

# Converged Networks (LAN and SAN) User Guide for EX Series Switches

Published  
2021-04-18

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Converged Networks (LAN and SAN) User Guide for EX Series Switches*  
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

**About This Guide | vi**

1

## **Overview**

**Converged Networks Overview | 2**

Understanding FIP Snooping | 2

Understanding Using an FCoE Transit Switch | 5

Understanding Priority-Based Flow Control | 6

Understanding DCB Features and Requirements on EX Series Switches | 10

Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches | 12

Understanding DCBX Application Protocol TLV Exchange on EX Series Switches | 17

2

## **Configuration**

**Configuration Examples | 22**

Example: Configuring an FCoE Transit Switch | 22

Requirements | 23

Overview and Topology | 23

Configuration | 26

Verification | 35

Example: Configuring DCBX to Support an iSCSI Application | 39

Requirements | 40

Overview and Topology | 40

Configuration | 41

Verification | 43

**Configuration Tasks | 47**

Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch | 47

Considerations When Configuring VN2VF\_Port FIP Snooping | 47

Configure VN2VF\_Port FIP Snooping on ELS FCoE Transit Switches | 49

Configure VN2VF\_Port FIP Snooping on non-ELS FCoE Transit Switches | 50

Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure) | 51

Disabling DCBX to Disable PFC Autonegotiation on EX Series Switches (CLI Procedure)	55
Disabling DCBX Application Protocol Exchange on EX Series Switches (CLI Procedure)	56
Defining an Application for DCBX Application Protocol TLV Exchange	57
Configuring an Application Map for DCBX Application Protocol TLV Exchange	58
Applying an Application Map to an Interface for DCBX Application Protocol TLV Exchange	60
Disabling the ETS Recommendation TLV	61
<b>Configuration Statements  </b>	<b>62</b>
application (Applications)	63
application (Application Maps)	64
applications (Applications)	66
application-map	67
application-maps	69
code-point (Congestion Notification)	70
code-points (Application Maps)	72
congestion-notification-profile	73
dcbx	77
destination-port (Applications)	79
disable (DCBX)	80
ether-type	82
ethernet-switching-options	83
examine-fip	90
fc-map	92
fcoe	95
fcoe-trusted	96
ieee-802.1 (Congestion Notification)	98
input (Congestion Notification)	99

interface (Access Port Security) | 101

interface (DCBX) | 103

interfaces | 105

policy-options | 107

priority-flow-control | 108

protocol (Applications) | 110

secure-access-port | 112

vlan (Access Port Security) | 115

### 3

## Administration

**Operational Commands | 119**

clear fip snooping enode | 119

clear fip snooping statistics | 121

clear fip snooping vlan | 123

show dcbx neighbors | 124

show fip snooping | 160

show fip snooping enode | 167

show fip snooping fcf | 173

show fip snooping statistics | 177

show fip snooping vlan | 183

# About This Guide

Use this guide to configure data center bridging (DCB) functions to support storage area network (SAN) traffic on EX Series switches that do not use the Enhanced Layer 2 Software (ELS) configuration style. Supported features include DCB capabilities exchange (DCBX), Fibre Channel over Ethernet (FCoE) transit functions, FCoE Initialization Protocol (FIP) snooping, and Priority Flow Control (PFC) for managing lossless traffic classes.

**NOTE:** For configuring DCB functions on QFX Series switches and EX Series switches that support the Enhanced Layer 2 Software (ELS) configuration style, see [Storage User Guide](#).

# 1

PART

## Overview

---

[Converged Networks Overview](#) | 2

---

# Converged Networks Overview

## IN THIS CHAPTER

- Understanding FIP Snooping | 2
- Understanding Using an FCoE Transit Switch | 5
- Understanding Priority-Based Flow Control | 6
- Understanding DCB Features and Requirements on EX Series Switches | 10
- Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches | 12
- Understanding DCBX Application Protocol TLV Exchange on EX Series Switches | 17

## Understanding FIP Snooping

### IN THIS SECTION

- FC Network Security | 3
- FIP Snooping Functions | 3
- FIP Snooping Firewall Filters | 3
- FIP Snooping Implementation | 4
- T11 FIP Snooping Specification | 5

Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping is a security mechanism that is designed to prevent unauthorized access and data transmission to a Fibre Channel (FC) network. It works by filtering traffic to permit only servers that have logged in to the FC network to access the network. You enable FIP snooping on FCoE VLANs when the switch is being used as an FCoE transit switch connecting FC initiators (servers) on the Ethernet network to FCoE forwarders (FCFs) at the FC storage area network (SAN) edge.



Through the FIP process, servers that have a converged network adapter (CNA) present an FCoE Node (ENode) that can log in to the FC network. The login process establishes a dedicated virtual link between the ENode and the FCF to emulate a point-to-point connection that passes transparently through the FCoE transit switch.

The FCoE transit switch applies FIP snooping firewall filters at the edge access ports associated with the FCoE VLANs on which you enable FIP snooping. FIP snooping provides security for virtual links by automatically creating firewall filters based on information gathered (snooped) about FC devices during FIP transactions.

This topic describes:

## FC Network Security

In traditional pure FC networks, the FCF is a trusted entity and server ENodes connect directly to the FCF. After an ENode gains access to the network through the fabric login (FLOGI) process, the FCF enforces zoning configurations, ensures that the ENode uses valid addresses, monitors the connection, and performs other security functions to prevent unauthorized access.

FIP snooping firewall filters emulate these security functions by preventing unauthorized access to the FCF through the transit switch and by ensuring the security of the virtual link between each ENode and the FCF. FIP snooping also prevents man-in-the-middle attacks.

## FIP Snooping Functions

When you enable FIP snooping, the FCoE transit switch monitors FIP logins, solicitations, and advertisements that pass through it and gathers information about the ENode address and the address of the FCF. The transit switch uses the information to construct firewall filters that permit access only to logged-in ENodes. All other traffic on the VLAN is denied.

For example, when an ENode on an FCoE VLAN performs a successful login, the FCoE transit switch snoops the FIP information, constructs a *firewall filter* that permits access for the ENode, and adds the filter on all transit switch access ports associated with the FCoE VLAN.

The firewall filters allow FCoE frames to pass through the transit switch only between the server ENode FCoE port and the FCF FCoE port to which the server ENode has logged in. This ensures that ENodes can only connect to the FCFs they have successfully logged in to and that only valid FCoE traffic is transmitted. FIP snooping maintains the filters by tracking FCoE sessions.

## FIP Snooping Firewall Filters

The FIP snooping firewall filters deny any FCoE traffic on the VLAN except for traffic originating from ENodes that have already logged in to the FCF.

FIP snooping performs these actions and checks to ensure that FCoE traffic is valid:

- Denies ENodes that use the FCF media access control (MAC) address as the source address.
- Denies all traffic from the ENode other than traffic addressed to the FCF that the ENode has logged into.
- Restricts the ENode to sending only FCoE protocol traffic on the virtual link.
- Allows the ENode to transmit only FIP and FCoE frames to the FCF address.
- Ensures that the FCoE source address an ENode uses after fabric login and fabric discovery (FDISC) is the address the FCF assigned to that ENode.
- Ensures that the FCoE source address the FCF assigns or accepts is only used for FCoE traffic.
- Ensures that FCoE frames are only addressed to the accepting FCF.

## **FIP Snooping Implementation**

You enable FIP snooping on a per-VLAN basis. The FCoE transit switch snoops FIP frames at the access ports associated with the FIP snooping-enabled VLANs, then installs the resulting firewall filters on the access ports to ensure that all snooping occurs on the FCoE transit switch network edge.

FCoE VLANs can include both access ports and trunk ports. Access ports face the hosts (FCoE servers and other FCoE initiators), and trunk ports face the FCF. When FIP snooping is enabled, the FCoE transit switch inspects both FIP frames and FCoE frames.

The FIP snooping implementation includes these considerations:

### **Server ENode-Facing Interfaces**

We recommend that you enable FIP snooping on all FCoE access ports to ensure secure connections to FCFs. After you enable FIP snooping on an FCoE VLAN, the transit switch denies FCoE traffic from any server on that VLAN until the server performs a valid fabric login with an FCF.

### **FCF-Facing Interfaces**

You must configure the interface that you are using to connect to an FCF as FCoE trusted interface, and it must be a 10 Gigabit Ethernet interface.

An FCoE trusted interface receives FCoE traffic only from an FCF. The following conditions apply to FCFs and FCF-facing interfaces:

- By default, FCFs are trusted entities.

- The FCoE transit switch always processes FCF frames because they come from a trusted source.

## FCoE Mapped Address Prefix

When you enable FIP snooping on a VLAN, optionally you can specify the FCoE Mapped Address Prefix (FC-MAP) value for that VLAN if the network uses the fabric-provided MAC address (FPMA) addressing scheme. The FC-MAP value is a 24-bit value that identifies the FCF. The FCF combines the FC-MAP value with a unique 24-bit Fibre Channel ID (FCID) value for the server during the fabric login process, creating a unique 48-bit identifier. The FCF assigns the 48-bit value to the server ENode as its MAC address and unique identifier for the session. Each server session the ENode establishes with the FCF receives a unique FCID, so a server can host multiple virtual links to an FCF, each with a unique 48-bit address identifier.

The FIP snooping filter compares the configured FC-MAP value with the FC-MAP value in the header of frames coming from the server. If the values do not match, the FCoE transit switch denies access.

## T11 FIP Snooping Specification

For more details about FIP snooping, see the Technical Committee T11 organization document *Increasing FCoE Robustness using FIP Snooping* at <http://www.t11.org/ftp/t11/pub/fc/bb-5/08-264v3.pdf>.

## RELATED DOCUMENTATION

[Understanding Using an FCoE Transit Switch | 5](#)

[Example: Configuring an FCoE Transit Switch | 22](#)

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

## Understanding Using an FCoE Transit Switch

You can use an EX4500 switch as a Fibre Channel over Ethernet (FCoE) transit switch. An FCoE transit switch is a Layer 2 data center bridging (DCB) switch that can transport FCoE frames and implement FCoE Initialization Protocol (FIP) snooping. The switch can transport both FCoE and Ethernet LAN traffic over the same network infrastructure while preserving the class of service (CoS) that Fibre Channel (FC) traffic requires.

An FCoE transit switch does not encapsulate or decapsulate FC frames in Ethernet. It is an access switch that transports FC frames that have already been encapsulated in Ethernet between FCoE initiators such as servers and an FCoE forwarder (FCF), which is in an FC storage area network (SAN). The transit

switch acts as a passthrough switch and is transparent to the FCF, which detects each connection to an FCoE server as a direct point-to-point link.

When the switch acts as a transit switch, the VLANs you configure for FCoE traffic can use any of the switch ingress and egress ports, because the traffic in both directions is Ethernet traffic. FCoE traffic must use a VLAN dedicated only to FCoE traffic that does not carry any other traffic.

When the switch acts as a transit switch, you must enable *priority-based flow control* (PFC, IEEE standard 802.1Qbb) as a link-level flow control mechanism. See *Understanding Priority-Based Flow Control* for additional information. FIP snooping adds security by filtering access so that only traffic from servers that have successfully logged in to the FC network passes through the transit switch and reaches the FC network.

The transit switch transparently connects FCoE-capable servers in an Ethernet LAN to an FCF, which has both FCoE and FC interfaces and processes both the FCoE and FC protocol stacks. The transit switch acts as a transparent access layer between FCoE servers and the FCF.

Encapsulated FCoE server traffic flows through the transit switch to the FCoE ports on the FCF. The FCF removes the Ethernet encapsulation from the FCoE frames to restore the native FC frames. Native FC traffic travels out FCF FC ports to storage devices in the FC SAN.

Native FC traffic from storage devices flows to the FCF FC ports, and the FCF encapsulates that traffic in Ethernet as FCoE traffic. The FCoE traffic flows through the transit switch to the appropriate server, and the server decapsulates the traffic.

## RELATED DOCUMENTATION

[Understanding FIP Snooping](#) | 2

# Understanding Priority-Based Flow Control

## IN THIS SECTION

- [Reliability of Packet Delivery in Standard Ethernet Networks and in Layer 2 Networks](#) | 7
- [Calculations for Buffer Requirements When Using PFC PAUSE](#) | 7
- [How PFC and Congestion Notification Profiles Work With or Without DCBX](#) | 8

*Priority-based flow control* (PFC), IEEE standard 802.1Qbb, is a link-level flow control mechanism. The flow control mechanism is similar to that used by IEEE 802.3x Ethernet PAUSE, but it operates on individual priorities. Instead of pausing all traffic on a link, PFC allows you to selectively pause traffic according to its class.

This topic describes:

## Reliability of Packet Delivery in Standard Ethernet Networks and in Layer 2 Networks

Standard Ethernet does not guarantee that a packet injected into the network will arrive at its intended destination. Reliability is provided by upper-layer protocols. Generally, a network path consists of multiple hops between the source and destination. A problem arises when transmitters send packets faster than receivers can accept them. When receivers run out of available buffer space to hold incoming flows, they silently drop additional incoming packets. This problem is generally resolved by upper-layer protocols that detect the drops and request retransmission.

Applications that require reliability in Layer 2 must have flow control that includes feedback from a receiver to a sender regarding buffer availability. Using IEEE 802.3x Ethernet PAUSE control frames, a receiver can generate a MAC control frame and send a PAUSE request to a sender when a specified threshold of receiver buffer has been filled to prevent buffer overflow. Upon receiving a PAUSE request, the sender stops transmission of any new packets until the receiver notifies the sender that it has sufficient buffer space to accept them again. The disadvantage of using Ethernet PAUSE is that it operates on the entire link, which might be carrying multiple traffic flows. Some traffic flows do not need flow control in Layer 2, because they are carrying applications that rely on upper-layer protocols for reliability. PFC enables you to configure Layer 2 flow control selectively for the traffic that requires it, such as Fibre Channel over Ethernet (FCoE) traffic, without impacting other traffic on the link. You can also enable PFC for other traffic types, such as iSCSI.

## Calculations for Buffer Requirements When Using PFC PAUSE

The receive buffer must be large enough to accommodate all data that is received while the system is responding to a PFC PAUSE frame.

When you calculate buffer requirements, consider the following factors:

- Processing and queuing delay of the PFC PAUSE—In general, the time to detect the lack of sufficient buffer space and to transmit the PFC PAUSE is negligible. However, delays can occur if the switch detects a reduction in buffer space just as the transmitter is beginning to transmit a maximum length frame.
- Propagation delay across the media—The delay amount depends on the length and speed of the physical link.
- Response time to the PFC PAUSE frame

- Propagation delay across the media on the return path

**NOTE:** We recommend that you configure at least 20 percent of the buffer size for the queue that is using PFC and that you do not specify the **exact** option.

Because it is mandatory to explicitly configure a certain percentage of buffer size for PFC, you must also explicitly configure some buffer size for any other forwarding classes that you are planning to use (including the default forwarding classes and the user-defined forwarding classes). The percentage that you allocate depends on the usage of the respective classes.

## How PFC and Congestion Notification Profiles Work With or Without DCBX

PFC can be applied to an interface regardless of whether the Data Center Bridging Capability Exchange protocol (DCBX) is enabled (DCBX is enabled by default for 10-Gigabit Ethernet interfaces on EX4500 CEE-enabled switches).

However, automatic control and advertisement of PFC requires DCBX:

- When DCBX is enabled—DCBX detects the data center bridging (DCB) neighbor's PFC configuration, uses autonegotiation to advertise local and peer PFC configuration, and then enables or disables PFC depending on whether the configurations are compatible or not. When PFC is enabled, it uses the congestion notification profile, which you have configured and applied to the interface.
- When DCBX is not enabled—*Class of service* (CoS) triggers PFC when the incoming frame has a User Priority (UP) field that matches the three-bit pattern specified for the congestion notification profile.

To manually control the use of PFC on the interface regardless of the configuration of the peer data center devices, you can explicitly change the configuration of DCBX on the interface to disable PFC autonegotiation. See ["Disabling DCBX to Disable PFC Autonegotiation on EX Series Switches \(CLI Procedure\)" on page 55](#). When PFC autonegotiation is disabled, PFC is triggered by the congestion notification profile for PFC regardless of the configuration of the DCB peer.

**NOTE:** PFC functions effectively only when the peer devices connected to the local interface are also using PFC and are configured compatibly with the local interface. PFC must be symmetrical—if PFC is not configured to use the same traffic class (code point) on both the local and the peer interface, it does not have any impact on the traffic.

[Table 1 on page 9](#) shows the one-to-one mapping between the UP field of an IEEE 802.1Q tagged frame, the traffic class, and the egress queue. In addition to setting a PFC congestion notification profile on an ingress port, you must set a forwarding class to match the priority specified in the PFC congestion notification profile and to forward the frame to the appropriate queue.

Juniper Networks EX Series Ethernet Switches support up to six traffic classes and allow you to associate those classes with six different congestion notification profiles. (The switches support up to 16 forwarding classes.)

**Table 1: Input for PFC Congestion Notification Profile and Mapping to Traffic Class and Egress Queue**

UP Field of IEEE-802.1Q Tagged Frame	Traffic Class	Egress Queue
000	TC 0	queue 0
001	TC 1	queue 1
010	TC 2	queue 2
011	TC 3	queue 3
100	TC4	queue 4
101	TC 5	queue 5

## RELATED DOCUMENTATION

[Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches | 12](#)

[Example: Configuring an FCoE Transit Switch | 22](#)

*Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*

[schedulers](#)

*congestion-notification-profile*

## Understanding DCB Features and Requirements on EX Series Switches

### IN THIS SECTION

- [EX Series Switch DCB Features Overview | 10](#)
- [Physical Interfaces | 11](#)
- [DCBX | 11](#)
- [Lossless Transport | 11](#)

Data center bridging (DCB) is a set of enhancements to the IEEE 802.1 bridge specifications. DCB modifies and extends Ethernet behavior to support I/O convergence in the data center. I/O convergence includes but is not limited to the transport of Ethernet LAN traffic and Fibre Channel (FC) storage area network (SAN) traffic on the same physical Ethernet network infrastructure.

A converged architecture saves cost by reducing the number of networks and switches required to support both types of traffic, reducing the number of interfaces required, reducing cable complexity, and reducing administration activities.

You can use DCB features on CEE-enabled switches to transport converged Ethernet and FC traffic while providing the class-of-service (CoS) characteristics and other characteristics FC requires for transmitting storage traffic.

**NOTE:** This topic only applies to DCB features on EX Series switches that do not support the Enhanced Layer 2 Software (ELS) configuration style. EX4500 and EX4550 switches are the only non-ELS EX Series switches that support DCB features.

DCB features on ELS EX Series switches and QFX Series switches are described in *Understanding DCB Features and Requirements*.

This topic describes:

### EX Series Switch DCB Features Overview

To accommodate FC traffic, DCB specifications provide:

- High-bandwidth interface
- A discovery and exchange protocol for communicating configuration and capabilities among neighbors to ensure consistent configuration across the network, called Data Center Bridging



Capability Exchange protocol (DCBX), which is an extension of Link Layer Discovery Protocol (LLDP, described in IEEE 802.1AB).

- A flow control mechanism called *priority-based flow control* (PFC, described in IEEE 802.1Qbb) to help provide lossless transport.

**NOTE:** The switches support the DCBX standards and PFC, but do not support enhanced transmission selection (ETS) and quantized congestion notification (QCN).

## Physical Interfaces

The switches provide the high-bandwidth interfaces (10-Gigabit Ethernet interfaces) required to support DCB and converged traffic. Your switch can have both 1-gigabit and 10-gigabit interfaces, depending on the configuration. DCBX works only on 10-gigabit, full-duplex interfaces. However, LLDP and DCBX are enabled by default on all the interfaces.

## DCBX

DCB devices use DCBX to exchange configuration information with directly connected peers (switches and data center devices such as servers). DCBX is an extension of LLDP. If you attempt to enable DCBX on an interface on which LLDP is disabled, the configuration commit fails. See ["Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches" on page 12](#) for details.

## Lossless Transport

FC traffic requires lossless transport (defined as no frames dropped because of congestion). Standard Ethernet does not support lossless transport, but the DCB extensions to Ethernet along with proper buffer management enable an Ethernet network to provide the level of CoS necessary to transport FC frames encapsulated in Ethernet over an Ethernet network.

This section describes these factors in creating lossless transport over Ethernet:

## PFC

PFC is a link-level flow control mechanism similar to Ethernet PAUSE (described in IEEE 802.3x). Ethernet PAUSE stops all traffic on a link for a specified period of time. PFC allows you to assign special priority to a specific traffic class for a specified period of time without stopping the traffic assigned to other priorities on the link. You assign this priority by using a congestion notification profile.

The switches support up to six traffic classes and allow you to associate those classes with six different congestion notification profiles.

PFC enables you to provide lossless transport for traffic assigned to use the PFC congestion notification profile and to use standard Ethernet transport for the rest of the link traffic.

## Buffer Management

Buffer management is critical to the proper functioning of PFC, because if buffers are allowed to overflow, frames are dropped and transport is not lossless.

For each lossless flow priority, the switch requires sufficient buffer space to:

- Store frames sent during the time it takes to send the PFC PAUSE across the cable between devices
- Store frames that are already on the wire when the sender receives the PFC PAUSE

The amount of buffer space needed to prevent frame loss due to congestion depends on the cable length, cable speed, and processing speed.

The switch automatically sets the threshold for sending a PFC PAUSE frame to accommodate delay from cables as long as 984 feet (300 meters) and to accommodate large frames that might be on the wire when the switch sends the PAUSE. This ensures that the switch sends PAUSE frames early enough to allow the sender to stop transmitting before the receive buffers on the switch overflow.

## RELATED DOCUMENTATION

[Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches | 12](#)

[Example: Configuring an FCoE Transit Switch | 22](#)

# Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches

## IN THIS SECTION

- [Basic DCBX Functioning | 13](#)
- [DCBX and PFC | 14](#)
- [DCBX and FCoE | 14](#)
- [DCBX and iSCSI | 14](#)
- [How DCBX Is Implemented on the Switches | 15](#)

Data Center Bridging Capability Exchange protocol (DCBX) is a discovery and exchange protocol for communicating configuration and capabilities among neighbors to ensure consistent configuration across the data center bridging network. It is an extension of Link Layer Discovery Protocol (LLDP). If you attempt to enable DCBX on an interface on which LLDP is disabled, the configuration commit fails. Data center bridging devices use DCBX to exchange configuration information with directly connected peers (devices such as switches and servers in a data center bridging network).

**NOTE:** This topic applies only to DCBX on EX Series switches that do not support the Enhanced Layer 2 Software (ELS) configuration style. EX4500 and EX4550 switches are the only non-ELS EX Series switches that support DCBX.

DCBX support on ELS EX Series switches and QFX Series switches is described in *Understanding DCBX*.

You can use DCBX to:

- Discover the data center bridging capabilities of peers
- Detect data center bridging feature misconfiguration or mismatches between peers
- Automatically enable or disable *priority-based flow control* (PFC) on an interface depending on whether the PFC configuration of the local interface is the same as the PFC configuration of the DCB peer

This topic describes:

## Basic DCBX Functioning

DCBX features support PFC, the Fibre Channel over Ethernet (FCoE) application, and other Layer 2 or Layer 4 applications (such as iSCSI). DCBX is enabled or disabled on a per-interface basis. The default autonegotiation behavior is: DCBX is enabled if the peer device connected to the interface also supports DCBX.

If the peer device connected to the interface does not support DCBX, DCBX remains enabled on the switch, but the switch detects that DCBX is not enabled on the peer and reports a misconfiguration for that interface when you issue the `show dcbx neighbors` command.

During negotiation of capabilities, the switch pushes the PFC configuration to an attached peer if the peer is configured as *willing* to learn the PFC configuration from other peers. The switch does not

support autoprovisioning and does not change its own configuration during autonegotiation to match the peer configuration—that is, the switch is not *willing* to learn the PFC configuration from peers.

## DCBX and PFC

After you enable PFC on a switch interface, DCBX uses autonegotiation to control the operational state of PFC functionality.

DCB devices must use the same traffic class (code point) on both the local and peer device. If the peer device connected to the interface supports PFC and is provisioned for the same traffic class as the switch interface, DCBX sets the PFC operational state to enabled. If the peer device connected to the interface does not support PFC or is not provisioned for the same traffic class, DCBX sets the operational state to disabled.

If the peer advertises that it is *willing* to learn its PFC configuration from the switch, DCBX pushes the switch's PFC configuration to the peer and does not check the peer's administrative state.

You can manually override DCBX control of the PFC operational state on a per-interface basis by disabling autonegotiation. If you disable autonegotiation on an interface on which you have configured PFC, then PFC remains enabled on that interface regardless of the peer configuration. To disable PFC on an interface, delete any PFC configuration on the interface.

## DCBX and FCoE

DCBX is mandatory for running FCoE applications, because FCoE traffic requires PFC to ensure lossless transport and PFC is a component of DCBX.

The FCoE application is configured by default on DCBX interfaces. Because of the FCoE requirement for lossless transport, we recommend that you configure the interfaces that carry FCoE traffic for PFC. See *Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*.

DCBX advertisement of the FCoE application functions as follows:

- If you configure the **fcoe** forwarding class and PFC congestion notification profile and assign these components to the interfaces that carry FCoE traffic, DCBX advertises their FCoE capability and assigned 802.1p code points to the DCB peer, and DCBX reports the FCoE capability and assigned 802.1p code points of the DCB peer to the switch.

## DCBX and iSCSI

DCBX is not essential for iSCSI applications. These applications provide a method for linking data storage facilities over IP networks. Unlike Fibre Channel (FC) communications, which require special-purpose cabling, iSCSI can be run over long distances by using existing network infrastructure.

You might want to use iSCSI over DCB to reduce latency in a network that is oversubscribed. You might also want to use it to provide predictable and certain application responsiveness, eliminating Ethernet's dependence on TCP/IP for the retransmission of dropped Ethernet frames.

DCBX advertises switch interfaces that are configured to support the iSCSI application, their PFC capability, and their assigned 802.1p code points.

## How DCBX Is Implemented on the Switches

On the switches, the implementation of DCBX is:

- Supported on aggregated Ethernet interfaces composed of 10-Gigabit Ethernet interfaces
- Enabled by default on all 10-Gigabit Ethernet interfaces

On the switches, DCBX supports the application type-length-value (TLV) — thus, DCBX interfaces on the switch can exchange information with their DCB peers about application capability, PFC capability, and 802.1p code-point settings. This implementation includes the following:

- The FCoE application is enabled by default on DCBX interfaces on the switch. Therefore, you do not configure an application map for the default FCoE application.

The switches do not have a default FCoE forwarding class—therefore, you must explicitly configure a forwarding class with the name **fcoe** and associate that class with the interfaces carrying FCoE traffic. If PFC is enabled, the 802.1p code points are assigned, and the interfaces are associated with a forwarding class, the switch negotiates FCoE application capability on the DCBX interface.

- Do not explicitly configure an FCoE application map, because that generates a commit error.
- You can configure additional Layer 2 or Layer 4 applications to be supported by the DCBX application TLV feature. To do this, explicitly configure an application map and associate the application map with one of the DCBX interfaces. DCBX then advertises the application capabilities of the associated interface and checks the capabilities of the connected peer device.
- If the peer device connected to the local interface does not support PFC or the peer's PFC configuration is not the same as the local interface's PFC configuration, DCBX automatically disables PFC for the local interface.

**NOTE:** You can manually override DCBX control of the PFC operational state on a per-interface basis. See ["Disabling DCBX to Disable PFC Autonegotiation on EX Series Switches \(CLI Procedure\)" on page 55](#).

## Features That Are Not Fully Supported by DCBX on EX Series Switches

The implementation of DCBX on EX Series switches does not fully support the following features:

- Enhanced transmission selection (ETS) (IEEE 802.1Qaz)—ETS is a bandwidth management mechanism to support dynamic allocation of bandwidth for DCBX traffic classes.
  - EX Series switches do not support using ETS to dynamically allocate bandwidth to specified traffic classes. Instead, the switches handle all DCBX traffic as a single default traffic class, group 7.
  - However, the switches do support the ETS Recommendation TLV. The ETS Recommendation TLV communicates the ETS settings that the switch wants the connected DCBX peer interface to use.
  - If the peer interface is *willing*, it changes its configuration to match the configuration in the ETS Recommendation TLV sent by the switch (group 7).
  - The switch also advertises that it is not *willing* to change its ETS settings.
  - The advertisement of ETS TLV is enabled by default for DCBX interfaces. If you want, you can disable this advertisement. See *Disabling the ETS Recommendation TLV*.
- A default FCoE forwarding class—The switch does not have a default FCoE forwarding class with default mapping to a priority queue for FCoE traffic.

**NOTE:** Because the switches do not support a default FCoE forwarding class, you must explicitly configure a forwarding class and name it **fcoe**.

### RELATED DOCUMENTATION

[Understanding DCB Features and Requirements on EX Series Switches | 10](#)

[Understanding Using an FCoE Transit Switch | 5](#)

[Example: Configuring an FCoE Transit Switch | 22](#)

## Understanding DCBX Application Protocol TLV Exchange on EX Series Switches

### IN THIS SECTION

- [Basic Steps for Setting Up Application Protocol TLV Exchange | 17](#)
- [Applications | 18](#)
- [Application Maps | 19](#)
- [Classifying and Prioritizing Application Traffic | 19](#)
- [Requirements for Interfaces in Non-FCoE Applications to Exchange Application Protocol Information | 20](#)

Data Center Bridging Capability Exchange protocol (DCBX) discovers the data center bridging (DCB) capabilities of connected peers. DCBX also advertises the capabilities of applications on interfaces by exchanging application protocol information through application type, length, and value (TLV) elements. DCBX is an extension of Link Layer Discovery Protocol (LLDP). LLDP must remain enabled on every interface on which you want to use DCBX.

LLDP and DCBX are enabled by default on all 10-Gigabit Ethernet interfaces of EX4500 CEE-enabled switches.

**NOTE:** This topic applies only to DCBX on EX Series switches that do not support the Enhanced Layer 2 Software (ELS) configuration style. EX4500 and EX4550 switches are the only non-ELS EX Series switches that support DCBX.

DCBX TLV exchange on ELS EX Series switches and QFX Series switches is described in *Understanding DCBX Application Protocol TLV Exchange*.

This topic describes:

### Basic Steps for Setting Up Application Protocol TLV Exchange

Setting up application protocol exchange for FCoE applications consists of:

- Configuring the **fcoe** forwarding class for IEEE 802.1p code point **011**
- Configuring PFC for IEEE 802.1p code point **011**

We recommend that you use code point **011** for the **fcoe** forwarding class, because this is the conventional IEEE 802.1p code point for FCoE traffic. We recommend that you configure PFC to use the same code point. See "[Example: Configuring an FCoE Transit Switch](#)" on page 22.

Setting up application protocol exchange for non-FCoE applications consists of:

- Defining applications
- Mapping the applications to IEEE 802.1p code points
- Configuring classifiers to prioritize incoming traffic map and map the incoming traffic to the application by the traffic code points
- Applying the application maps and classifiers to interfaces

Except for FCoE applications, you must explicitly define and map all applications that you want an interface to advertise.

**NOTE:** Do not explicitly configure an FCoE application map, because doing that generates a commit error.

## Applications

Before an interface can exchange application protocol information, you must define the applications that you want to advertise, except for the FCoE application, which is defined by default. You can define:

- Layer 2 applications by EtherType
- Layer 4 applications (such as iSCSI applications) by a combination of protocol (TCP or UDP) and destination port

The EtherType is a two-octet field in the Ethernet frame that denotes the protocol encapsulated in the frame. For a list of common EtherTypes, see <http://standards.ieee.org/develop/regauth/ethertype/eth.txt> on the IEEE standards organization website. For a list of port numbers and protocols, see the *Service Name and Transport Protocol Port Number Registry* at [http://www.iana.org/assignments/service-names-port-numbers.xml](http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml) on the Internet Assigned Numbers Authority (IANA) website.

The switch automatically defines the FCoE application as EtherType 0x8906.



## Application Maps

An *application map* maps defined applications to one or more IEEE 802.1p code points. Each application map contains one or more applications. DCBX includes the configured application code points in the protocol TLVs exchanged with the connected peer.

To exchange protocol TLVs for an application, you must include the application in an application map (with the exception of the FCoE application).

Mapping an application to code points does two things:

- Maps incoming traffic with the same code points to that application.
- Allows you to configure classifiers that map incoming application traffic, by code point, to a forwarding class and a loss priority to apply *class of service* (CoS) to application traffic and prioritize application traffic.

You apply an application map to an interface to enable DCBX application protocol exchange on that interface for each application specified in the application map. Applications that you want an interface to advertise must be configured in the application map that you apply to the interface (except the FCoE application). Do not explicitly configure an FCoE application map, because doing that generates a commit error.

## Classifying and Prioritizing Application Traffic

When traffic arrives at an interface, the interface classifies the incoming traffic based on its code points. Classifiers map code points to loss priorities and forwarding classes. The loss priority prioritizes the traffic. The forwarding class determines the traffic output queue and CoS service level.

When you map an application to an IEEE 802.1p code point in an application map and apply the application map to an interface, incoming traffic on the interface that matches the application code points is mapped to the appropriate application. The application receives the loss priority and the CoS associated with the forwarding class for those code points, and its traffic is placed in the output queue associated with the forwarding class.

You can use the default classifier or you can configure a classifier to map the application code points defined in the application map to forwarding classes and loss priorities.

Traffic for the FCoE application is classified and prioritized by your configuration of the **fcoe** forwarding class.

## Requirements for Interfaces in Non-FCoE Applications to Exchange Application Protocol Information

For non-FCoE applications, interfaces on which you want to exchange application protocol TLVs must include the following two items:

- The application map that contains the application
- A classifier

See *Defining an Application for DCBX Application Protocol TLV Exchange* and *Configuring an Application Map for DCBX Application Protocol TLV Exchange*.

### RELATED DOCUMENTATION

---

[Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches | 12](#)

---

[Understanding DCB Features and Requirements on EX Series Switches | 10](#)

---

*Understanding Priority-Based Flow Control*

---

[Disabling DCBX Application Protocol Exchange on EX Series Switches \(CLI Procedure\) | 56](#)

# 2

PART

## Configuration

---

[Configuration Examples](#) | 22

[Configuration Tasks](#) | 47

[Configuration Statements](#) | 62

---

## CHAPTER 2

# Configuration Examples

**IN THIS CHAPTER**

- [Example: Configuring an FCoE Transit Switch | 22](#)
- [Example: Configuring DCBX to Support an iSCSI Application | 39](#)

## Example: Configuring an FCoE Transit Switch

**IN THIS SECTION**

- [Requirements | 23](#)
- [Overview and Topology | 23](#)
- [Configuration | 26](#)
- [Verification | 35](#)

You can use an EX4500 CEE-enabled switch as a Fibre Channel over Ethernet (FCoE) transit switch, enabling it to transport both FCoE and Ethernet LAN traffic. Using the same switch to support both your storage network and traditional IP-based data communications reduces the costs of powering, cooling, provisioning, maintaining, and managing your network.

This example includes:

- FIP snooping for security
- Priority-based flow control (PFC) for lossless transport
- The FCoE forwarding class for the DCBX application protocol type, length, value (TLV) exchange
- A trusted port connecting to the FCoE forwarder (FCF)
- Enlarged maximum transmission unit (MTU) size for handling FCoE traffic

This example shows how to configure an FCoE transit switch:

## Requirements

This example uses the following hardware and software components:

- One EX4500 switch (CEE-capable model)
- Junos OS Release 12.1 or later for EX Series switches
- One FCoE Node (ENode)
- One FCoE forwarder (FCF)

Before you begin, be sure you have:

- Configured the VLAN **fcoe-vlan** on the switch. See [Configuring VLANs for EX Series Switches](#).

## Overview and Topology

### IN THIS SECTION

- [Topology | 25](#)

FCoE transmissions are vulnerable to address spoofing and man-in-the-middle attacks, because they are not actually sent through point-to-point links. This example describes how to configure the switch so that it provides security similar to that provided by traditional Fibre Channel (FC) networks. The switch is transparent to the ENode and the FCF, so the ENode and FCF communicate just as they would for a point-to-point link.

FIP snooping is disabled by default. You enable FIP snooping on a per-VLAN basis for VLANs that carry FCoE traffic. Ensure that a VLAN that carries FCoE traffic carries only FCoE traffic, because enabling FIP snooping denies access for all other Ethernet traffic.

This example shows how to configure FIP snooping on a VLAN of the EX4500 switch that is connected with one ENode, that is, a server equipped with converged network adapters (CNAs). The setup for this example includes the VLAN **fcoe-vlan** on the switch.

This example also shows how to configure PFC on the interfaces that are being used for FCoE traffic and how to configure an FCoE trusted port to handle traffic between the switch and the FCF gateway to the storage area network (SAN).

You must configure PFC properties for the interfaces that are carrying FCoE traffic, because flow control must be implemented on the link level for this type of traffic.

**NOTE:** Data Center Bridging Capability Exchange protocol (DCBX) is enabled by default on all 10-Gigabit Ethernet interfaces on EX4500 switches. DCBX automatically controls whether PFC is enabled or disabled on the interface. However, you must configure the PFC properties selecting the traffic class and queue. See *Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*.

You configure trunk interfaces that connect to the FCF as trusted interfaces. The switch must use the same FCoE MAC Address Prefix (FC-MAP) value that is being used by the FCF. Therefore, if the FCF is using a nondefault FC-MAP value, you must configure the FC-MAP value on the switch to match that value.

You must also enlarge the MTU size for all interfaces (both access and trunk) that are handling FCoE traffic to accommodate the maximum FC frame and Ethernet header sizes.

This example also includes configuring the **fcoe** forwarding class to be used for the FCoE traffic, so that it can take advantage of DCBX support for the Application Protocol TLV Exchange. See ["Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches" on page 12](#) for additional information.

**NOTE:** Configuring and applying PFC and a forwarding class **fcoe** on the DCBX interfaces automatically enables the DCBX FCoE application protocol exchange on those interfaces. Do not explicitly configure an FCoE application map, because doing that generates a commit error. See ["Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches" on page 12](#) for additional information.

**NOTE:** PFC is supported only on 10-Gigabit Ethernet interfaces.

**NOTE:** We recommend that you also:

- Configure the PFC congestion notification profile for the same 802.1p code points that you are using for the **fcoe** forwarding class. We recommend code point **011**, because this is the conventional IEEE 802.1p code point for FCoE traffic.
- Configure at least 20 percent of the buffer for the queue that is using PFC.
- Do not specify the **exact** option when configuring the buffer for the queue that is using PFC.

- Configure the **loss-priority** statement to **low** for a traffic class that is using PFC.
- Configure an appropriate percent of the buffer for any other forwarding classes (default forwarding classes and the user-defined forwarding classes) that you are using

Topology

The components of the topology for this example are shown in [Table 2 on page 25](#).

Table 2: Components of the FCoE Security Topology

Properties	Settings
Switch hardware	One EX4500 CEE-enabled switch
VLAN name and ID	<b>fcoe-vlan</b> , tag <b>20</b>
Forwarding class for FCoE traffic	<b>fcoe</b> , code point <b>011</b>
Interfaces in <b>fcoe-vlan</b>	<b>xe-0/0/1</b>  <b>xe-0/0/2</b>  <b>xe-0/0/3</b>  <b>xe-0/0/30</b>
FCoE trusted port to the FCF	<b>xe-0/0/30</b>
PFC interfaces	<b>xe-0/0/1</b>  <b>xe-0/0/2</b>  <b>xe-0/0/3</b>  <b>xe-0/0/30</b>

Table 2: Components of the FCoE Security Topology *(Continued)*

Properties	Settings
CoS forwarding-class interface	xe-0/0/30
CoS scheduler-map interface	xe-0/0/30
Interfaces configured with MTU of 2500	xe-0/0/1 xe-0/0/2 xe-0/0/3 xe-0/0/30

In this example, the switch has already been configured as follows:

- All access ports are untrusted, which is the default setting.
- DCBX is enabled by default on all 10-Gigabit Ethernet interfaces.
- The port connecting the switch to the FCF is configured as a trunk port.

## Configuration

### IN THIS SECTION

- [Procedure | 27](#)

To configure an FCoE transit switch, perform these tasks:



## Procedure

### CLI Quick Configuration

To quickly configure an FCoE transit switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set ethernet-switching-options secure-access-port vlan fcoe-vlan examine-fip fc-map 0x0EFC03
set ethernet-switching-options secure-access-port interface xe-0/0/30 fcoe-trusted
set interfaces xe-0/0/1 ether-options no-flow-control
set interfaces xe-0/0/2 ether-options no-flow-control
set interfaces xe-0/0/3 ether-options no-flow-control
set interfaces xe-0/0/30 ether-options no-flow-control
set class-of-service congestion-notification-profile cn-profile input ieee-802.1 code-point 011 pfc
set class-of-service interfaces xe-0/0/1 congestion-notification-profile cn-profile
set class-of-service interfaces xe-0/0/2 congestion-notification-profile cn-profile
set class-of-service interfaces xe-0/0/3 congestion-notification-profile cn-profile
set class-of-service interfaces xe-0/0/30 congestion-notification-profile cn-profile
set class-of-service classifiers ieee-802.1 pfc-class import default
set class-of-service classifiers ieee-802.1 pfc-class forwarding-class fcoe loss-priority low code-points 011
set class-of-service interfaces xe-0/0/1 unit 0 classifiers ieee-802.1 pfc-class
set class-of-service interfaces xe-0/0/2 unit 0 classifiers ieee-802.1 pfc-class
set class-of-service interfaces xe-0/0/3 unit 0 classifiers ieee-802.1 pfc-class
set class-of-service interfaces xe-0/0/30 unit 0 classifiers ieee-802.1 pfc-class
set class-of-service forwarding-classes class fcoe queue-num 3
set class-of-service schedulers pfc-sched buffer-size percent 25
set class-of-service schedulers default-sched buffer-size percent 17
set class-of-service scheduler-maps pfc-map forwarding-class fcoe scheduler pfc-sched
set class-of-service scheduler-maps pfc-map forwarding-class assured-forwarding scheduler default-sched
set class-of-service scheduler-maps pfc-map forwarding-class best-effort scheduler default-sched
set class-of-service scheduler-maps pfc-map forwarding-class network-control scheduler default-sched
set class-of-service scheduler-maps pfc-map forwarding-class expedited-forwarding scheduler default-sched
set class-of-service interfaces xe-0/0/30 scheduler-map pfc-map
set interfaces xe-0/0/1 mtu 2500
set interfaces xe-0/0/2 mtu 2500
set interfaces xe-0/0/3 mtu 2500
set interfaces xe-0/0/30 mtu 2500
```

## Step-by-Step Procedure

To configure an FCoE transit switch:

1. Enable FIP snooping on the VLAN and modify the FC-MAP value to match the FC-MAP value being used by the FCF:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan fcoe-vlan examine-fip fc-map 0x0EFC03
```

2. Set the FCF-facing interface (**xe-0/0/30**) as FCoE-trusted:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface xe-0/0/30 fcoe-trusted
```

3. Configure a congestion notification profile, specifying the name of the profile and applying it to the traffic class that is indicated by the User Priority bits in the 802.1Q tagged frame of an incoming packet:

**NOTE:** The ENode and the switch must use the same traffic class for the FCoE traffic. DCBX advertises the traffic class being used by the switch and detects the traffic class being used by the ENode. If there is a mismatch, the switch disables the PFC capability of the switch interface.

```
[edit class-of-service]
user@switch# set congestion-notification-profile cn-profile input ieee-802.1 code-point 011 pfc
```

**NOTE:** The configuration of PFC includes two different **ieee-802.1** configuration statements:

- *ieee-802.1 (Congestion Notification)*—Use to configure the congestion notification profile.
- [ieee-802.1](#)—Use to configure the CoS classifier.

4. Disable standard flow control on the interfaces that you want to use for the FCoE VLAN.

**NOTE:** PFC and standard flow control cannot be enabled on the same interface, and you must use PFC for FCoE traffic.

```
[edit interfaces]
user@switch# set xe-0/0/1 ether-options no-flow-control
user@switch# set xe-0/0/2 ether-options no-flow-control
user@switch# set xe-0/0/3 ether-options no-flow-control
user@switch# set xe-0/0/30 ether-options no-flow-control
```

5. Bind the congestion notification profile to all interfaces of the FCoE VLAN:

```
[edit class-of-service]
user@switch# set interface xe-0/0/1 congestion-notification-profile cn-profile
user@switch# set interface xe-0/0/2 congestion-notification-profile cn-profile
user@switch# set interface xe-0/0/3 congestion-notification-profile cn-profile
user@switch# set interface xe-0/0/30 congestion-notification-profile cn-profile
```

6. Create a CoS classifier for the fcoe forwarding class:

```
[edit class-of-service]
user@switch# set forwarding-classes fcoe queue-num 3
```

7. Configure this forwarding class (**fcoe**) to use a low loss priority value and to use the same code point that is used for PFC:

**NOTE:** We recommend that you use code point 011, because this is the conventional IEEE 802.1p code point for FCoE traffic.

```
[edit class-of-service]
user@switch# set classifiers ieee-802.1 pfc-class forwarding-class fcoe loss-priority low code-points
011
```

8. Bind the **pfc-class** classifier to all interfaces of the FCoE VLAN:

```
[edit class-of-service]
user@switch# set interfaces xe-0/0/1 unit 0 classifiers ieee-802.1 pfc-class
user@switch# set interfaces xe-0/0/2 unit 0 classifiers ieee-802.1 pfc-class
user@switch# set interfaces xe-0/0/3 unit 0 classifiers ieee-802.1 pfc-class
user@switch# set interfaces xe-0/0/30 unit 0 classifiers ieee-802.1 pfc-class
```

9. Assign forwarding-class **fcoe** to an egress queue:

```
[edit class-of-service]
user@switch# set forwarding-classes fcoe queue-num 3
```

10. Set a scheduler for this queue, allocating at least 20 percent of the buffer to **pfc-sched**:

```
[edit class-of-service]
user@switch# set schedulers pfc-sched buffer-size percent 25
```

11. Set a scheduler for the default queue, allocating 17 percent of the buffer to that queue:

```
[edit class-of-service]
uuser@switch# set schedulers default-sched buffer-size percent 17
```

12. Configure a scheduler map (**pfc-map**) that associates the scheduler (**pfc-sched**) with the **fcoe** forwarding class and associates the default forwarding classes (assured-forwarding, best-effort and network-control) with the default schedule:

```
[edit class-of-service]
user@switch# set scheduler-maps pfc-map forwarding-class fcoe scheduler pfc-sched
user@switch# set scheduler-maps pfc-map forwarding-class assured-forwarding scheduler default-sched
user@switch# set scheduler-maps pfc-map forwarding-class best-effort scheduler default-sched
user@switch# set scheduler-maps pfc-map forwarding-class network-control scheduler default-sched
user@switch# set scheduler-maps pfc-map forwarding-class expedited-forwarding scheduler default-sched
```

13. Assign the scheduler map (**pfc-map**) to the FCF-facing interface (xe-0/0/30):

```
[edit class-of-service]
user@switch# set interfaces xe-0/0/30 scheduler-map pfc-map
```

14. Enlarge the MTU size to 2500 bytes for all the interfaces (both access and trunk) that are handling FCoE traffic:

```
[edit interfaces]
user@switch# set xe-0/0/1 mtu 2500
user@switch# set xe-0/0/2 mtu 2500
user@switch# set xe-0/0/3 mtu 2500
user@switch# set xe-0/0/30 mtu 2500
```

## Results

Display the results of the configuration:

```
[edit]
user@switch# show
```

```
interfaces {
  xe-0/0/1 {
    mtu 2500;
    ether-options {
      no-flow-control;
    }
    unit 0 {
      family ethernet-switching {
        vlan {
          members fcoe-vlan;
        }
      }
    }
  }
  xe-0/0/2 {
    mtu 2500;
    ether-options {
```

```

        no-flow-control;
    }
    unit 0 {
        family ethernet-switching {
            vlan {
                members fcoe-vlan;
            }
        }
    }
}
xe-0/0/3 {
    mtu 2500;
    ether-options {
        no-flow-control;
    }
    unit 0 {
        family ethernet-switching {
            vlan {
                members fcoe-vlan;
            }
        }
    }
}
xe-0/0/30 {
    mtu 2500;
    ether-options {
        no-flow-control;
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members fcoe-vlan;
            }
        }
    }
}
}
class-of-service {
    classifiers {
        ieee-802.1 pfc-class {
            import default;
            forwarding-class fcoe {

```

```

        loss-priority low code-points 011;
    }
    forwarding-classes {
        class fcoe queue-num 3;
    }
    congestion-notification-profile {
        cn-profile {
            input {
                ieee-802.1 {
                    code-point 011 {
                        pfc;
                    }
                }
            }
        }
    }
}
interfaces {
    xe-0/0/1 {
        congestion-notification-profile cn-profile;
        unit 0 {
            classifiers {
                ieee-802.1 pfc-class;
            }
        }
    }
    xe-0/0/2 {
        congestion-notification-profile cn-profile;
        unit 0 {
            classifiers {
                ieee-802.1 pfc-class;
            }
        }
    }
    xe-0/0/3 {
        congestion-notification-profile cn-profile;
        unit 0 {
            classifiers {
                ieee-802.1 pfc-class;
            }
        }
    }
    xe-0/0/30 {
        congestion-notification-profile cn-profile;
        scheduler-map pfc-map;
    }
}

```

```

        unit 0 {
            classifiers {
                ieee-802.1 pfc-class;
            }
        }
    }

    scheduler-maps {
        pfc-map {
            forwarding-class fcoe scheduler pfc-sched;
            forwarding-class assured-forwarding scheduler default-sched;
            forwarding-class best-effort scheduler default-sched;
            forwarding-class network-control scheduler default-sched;
            forwarding-class expedited-forwarding scheduler default-
sched;
        }
    }

    schedulers {
        pfc-sched {
            buffer-size percent 25;
        }
        default-sched {
            buffer-size percent 17;
        }
    }
}

ethernet-switching-options {
    secure-access-port {
        interface xe-0/0/30.0 {
            fcoe-trusted;
        }
        vlan fcoe-vlan {
            examine-fip {
                fc-map 0x0EFC03;
            }
        }
    }
}

```



## Verification

### IN THIS SECTION

- [Verifying That FIP Snooping Is Working Correctly on the Switch | 35](#)
- [Verifying That PFC is Enabled, That the FCoE Application Is Advertised, and That the Switch Interface and DCB Peer Are Using the Same 802.1p Code Points | 36](#)

Confirm that the configuration of the FCoE transit switch is working properly:

### Verifying That FIP Snooping Is Working Correctly on the Switch

#### Purpose

Verify that FIP snooping is being implemented on the appropriate VLAN.

#### Action

Send some requests from ENodes to the switch.

Display the FIP snooping information :

```
user@switch> show fip snooping vlan detail fcoe-vlan

VLAN: fcoe-vlan,    FC-MAP: 0e:fc:03
FCF Information
FCF-MAC             : 30:10:94:01:00:00
Active Sessions     : 2
Configured FKA-ADV  : 195
Running FKA-ADV     : 73
  Enode Information
    Enode-MAC: 10:10:94:01:00:01,      Interface: xe-0/0/1
    Configured FKA-ADV : 195
    Running FKA-ADV    : 103
      Session Information
        VN-Port MAC: 0E:FC:03:01:0A:01,  FKA-ADV : 178
        VN-Port MAC: 0E:FC:03:01:0B:01,  FKA-ADV : 194
FCF Information
FCF-MAC             : 40:10:94:01:00:00
```

```

Active Sessions      : 2
Configured FKA-ADV   : 258
Running FKA-ADV      : 212
  Enode Information
    Enode-MAC: 20:10:94:01:00:02,      Interface: xe-0/0/0
    Configured FKA-ADV : 258
    Running FKA-ADV    : 242
  Session Information
    VN-Port MAC: 0E:FC:03:02:0C:02,    FKA-ADV : 254
    VN-Port MAC: 0E:FC:03:02:0D:02,    FKA-ADV : 269

```

## Meaning

The output for this VLAN (**fcoe-vlan**) includes the FC MAP value that you configured. It shows the MAC addresses of the FCF and the ENode that are transmitting FCoE traffic through the switch.

## Verifying That PFC is Enabled, That the FCoE Application Is Advertised, and That the Switch Interface and DCB Peer Are Using the Same 802.1p Code Points

### Purpose

Verify that PFC is enabled on the local switch interface and on the peer interface, and that the local interface and the peer interface are using the same code point.

### Action

Send some requests from ENodes to the switch.

Display the DCBX information advertised by the configured CoS forwarding class interface (**xe-0/0/30**) and detected by the switch:

```

user@switch> show dcbx neighbors interface xe-0/0/30

Interface : xe-0/0/30.0

Protocol-State: in-sync

Local-Advertisement:
  Operational version: 0
  sequence-number: 1, acknowledge-id: 1

```

## Peer-Advertisement:

Operational version: 0

sequence-number: 1, acknowledge-id: 1

Feature: PFC, Protocol-State: in-sync

Operational State: Enabled

## Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 6

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Disabled
100	Disabled
011	Enabled
110	Disabled
111	Disabled

## Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 6

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Disabled
100	Disabled
011	Enabled
110	Disabled
111	Disabled

Feature: Application, Protocol-State: in-sync

## Local-Advertisement:

```
Enable: Yes, Willing: No, Error: No
```

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
FCoE	0x8906		00001000	Enabled

```
Peer-Advertisement:
```

```
Enable: Yes, Willing: No, Error: No
```

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
FCoE	0x8906		00001000	Enabled

## Meaning

PFC is a requirement for transmitting FCoE traffic and PFC works only when the local and peer devices are both enabled for PFC and are both using the same traffic class (code point) for transmitting the PFC traffic.

In the output for **Feature: PFC**, check the status of **Local-Advertisement** to verify that PFC is enabled. If DCBX detects a misconfiguration with the DCB peer, it disables the PFC capability. In this example, the PFC **Operational State** is **enabled**, because PFC is configured symmetrically on the switch and the DCB peer. Both devices are using code point **011** for forwarding the traffic.

If the results show that PFC is disabled, you can use the information provided by this command to reconfigure the congestion notification profile to match the code point being used for PFC by the peer device. See *Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*.

**Appl-Name** shows the default FCoE application. The FCoE application always indicates **Ethernet-Type 0x8906**. The **Priority-Map** for the FCoE application shows the 8-bit format of the code-point setting that was specified for the PFC congestion notification profile. In this case, the three bit code point is 3, **011**. So the **Priority-Map** for the default FCoE application is **00001000**.

The **fcoe** forwarding-class and PFC were configured; and the configuration of the application on the switch and on the DCB are synchronized. Therefore, the **Status** of the FCoE application is **Enabled**.

If the configuration of the FCoE application on the switch did not match the FCoE application of the DCB peer, the status of the application would appear as **Disabled**.

## RELATED DOCUMENTATION

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

*Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*

[Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches | 12](#)

*congestion-notification-profile*

## Example: Configuring DCBX to Support an iSCSI Application

### IN THIS SECTION

- [Requirements | 40](#)
- [Overview and Topology | 40](#)
- [Configuration | 41](#)
- [Verification | 43](#)

Data Center Bridging Capability Exchange protocol (DCBX) support for the application protocol type, length, and value (TLV) enables you to implement DCBX for various Layer 2 and Layer 4 applications. Internet small computer system interface (iSCSI) is a Layer 4 storage application that can benefit from DCBX. Implementing iSCSI over data center bridging (DCB) reduces latency in networks that are oversubscribed and provides a predictable and certain application responsiveness, eliminating Ethernet's dependence on TCP/IP for the retransmission of dropped Ethernet frames. Although DCBX is not a requirement for such applications, it adds the reliability required for enterprise data storage.

**NOTE:** You can configure and apply priority flow control (PFC) for any DCBX interfaces, but it is not a requirement for applications other than Fiber Channel over Ethernet (FCoE).

This example shows how to configure DCBX to support an iSCSI application:

## Requirements

This example uses the following hardware and software components:

- One EX4500 switch (CEE-capable model)
- Junos OS Release 12.1 or later for EX Series switches

## Overview and Topology

### IN THIS SECTION

- [Topology](#) | 41

You can use the same switch to support your LAN traffic and your storage area network (SAN) traffic—including both FCoE and iSCSI traffic. The DCBX application protocol TLV allows you to associate a specific DCBX interface with a specific application map.

DCBX discovers the DCB capabilities of peers by exchanging feature configuration information, detects feature misconfiguration and mismatches, and can configure DCB on peers. DCBX is an extension of Link Layer Discovery Protocol (LLDP). LLDP must remain enabled on every interface for which you want to use DCBX. If you attempt to enable DCBX on an interface on which LLDP is disabled, the configuration commit fails.

The switch supports DCBX information exchange for other applications, such as iSCSI, as specified in your configuration by EtherType or by the destination port and protocol.

To take advantage of this feature for non-FCoE applications, you must configure the application and application map and associate the application map with the interface that is carrying the application's traffic. This configuration includes specifying the 802.1 code points to be used for this application.

When you configure an iSCSI application, you must always designate **destination-port 3260**.

**NOTE:** DCBX is enabled by default on all 10-Gigabit Ethernet interfaces on EX4500 switches (CEE-capable models).

This example shows how to configure an iSCSI application on a DCBX interface of the EX4500 switch that is connected to an iSCSI storage device.

Topology

The components of the topology for this example are shown in [Table 3 on page 41](#).

Table 3: Components of the DCBX iSCSI Topology

Properties	Settings
Switch hardware	One EX4500 switch (CEE capable model)
Application	iSCSI
Application map code points	101
Interface for iSCSI application	xe-0/0/37
Destination port	3260

In this example, the switch has already been configured as follows:

- DCBX is enabled by default on all 10-Gigabit Ethernet interfaces.

Configuration

IN THIS SECTION

Procedure | 42

To configure DCBX to support an iSCSI application, perform these tasks:

## Procedure

### CLI Quick Configuration

To quickly configure a DCBX interface for an iSCSI application, copy the following commands and paste them into the switch terminal window:

```
[edit]
set applications application iscsi protocol tcp destination-port 3260
set policy-options application-maps iscsi-map application iscsi code-points 101
set protocols dcbx interface xe-0/0/37 application-map iscsi-map
```

### Step-by-Step Procedure

Configure a DCBX interface for an iSCSI application:

1. Create the application:

```
[edit]
user@switch# set applications application iscsi protocol tcp destination-port 3260
```

2. Create the application map:

```
[edit policy-options]
user@switch# set application-maps iscsi-map application iscsi code-points 101
```

3. Apply the application map to the DCBX interface that you want to use for iSCSI:

```
[edit protocols]
user@switch# set dcbx interface xe-0/0/37 application-map iscsi-map
```

## Results

Check the results of the configuration:

```
user@switch> show configuration
protocols {
```



```
dcbx {  
    interface all;  
    interface xe-0/0/37.0 {  
        application-map iscsi-map;  
    }  
}  
lldp {  
    interface all;  
}  
}  
policy-options {  
    application-maps {  
        iscsi-map {  
            application iscsi code-points 101;  
        }  
    }  
}  
applications {  
    application iscsi {  
        protocol tcp;  
        destination-port 3260;  
    }  
}
```

## Verification

### IN THIS SECTION

- [Verifying That the iSCSI Application Is Advertised and That the Switch Interface and DCB Peer Are Using the Same 802.1p Code Points | 44](#)

To confirm that the configuration is working properly:

## Verifying That the iSCSI Application Is Advertised and That the Switch Interface and DCB Peer Are Using the Same 802.1p Code Points

### Purpose

Verify that both the switch and the DCB peer are using a DCBX iSCSI application configured for the same 802.1p code points.

### Action

Send some requests from the switch to the DCB peer.

Display the DCBX information advertised by DCBX interface (**xe-0/0/37**) and detected by the switch:

```
user@switch> show dcbx neighbors interface

Interface : xe-0/0/37.0

Protocol-State: in-sync
Active-application-map: iscsi-map

Local-Advertisement:
  Operational version: 0
  sequence-number: 1, acknowledge-id: 1

Peer-Advertisement:
  Operational version: 0
  sequence-number: 1, acknowledge-id: 1

Feature: PFC, Protocol-State: in-sync

Operational State: Disabled

Local-Advertisement:
  Enable: Yes, Willing: No, Error: No
  Maximum Traffic Classes capable to support PFC: 6

Code Point      Admin Mode
-----
000             Disabled
001             Disabled
010             Disabled
```

011	Disabled
100	Disabled
101	Disabled
110	Disabled
111	Disabled

Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 6

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Disabled
100	Disabled
101	Disabled
110	Disabled
111	Disabled

Feature: Application, Protocol-State: in-sync

Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
iscsi		3260	00100000	Enabled

Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
-----------	---------------	---------------	--------------	--------

iscsi	3260	00100000	Enabled
-------	------	----------	---------

## Meaning

Check the status for **Local-Advertisement** in the section **Feature: Application**.

If there is misconfiguration between the switch and the DCB peer, the status displays **Error: Yes**.

In this example, there is no error. The output for **Feature: Application, Protocol-State**, displays a list of DCBX applications under **Appl-Name**.

This field displays information for the user-configured application **iscsi**. When you configure an iSCSI application, you must always designate the destination port as **3260**. The output displays this as the **Socket-Number**.

The **Priority-Map** for the iSCSI application reflects the 802.1p code points that were specified in this example for the **iSCSI-map**. The example specified **101** for the iSCSI application map code points. The **Priority-Map** is an 8-bit code point format of the 802.1p code points; thus, **00100000**.

The **Status** of the iSCSI application is **Enabled**, because the switch and the DCB are using the same code points for the iSCSI application.

## RELATED DOCUMENTATION

[Example: Configuring an FCoE Transit Switch | 22](#)

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Configuring an Application Map for DCBX Application Protocol TLV Exchange*

*Applying an Application Map to an Interface for DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches | 17](#)

## CHAPTER 3

# Configuration Tasks

**IN THIS CHAPTER**

- [Configuring VN2VF\\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch | 47](#)
- [Configuring Priority-Based Flow Control for an EX Series Switch \(CLI Procedure\) | 51](#)
- [Disabling DCBX to Disable PFC Autonegotiation on EX Series Switches \(CLI Procedure\) | 55](#)
- [Disabling DCBX Application Protocol Exchange on EX Series Switches \(CLI Procedure\) | 56](#)
- [Defining an Application for DCBX Application Protocol TLV Exchange | 57](#)
- [Configuring an Application Map for DCBX Application Protocol TLV Exchange | 58](#)
- [Applying an Application Map to an Interface for DCBX Application Protocol TLV Exchange | 60](#)
- [Disabling the ETS Recommendation TLV | 61](#)

## Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch

**SUMMARY**

On a Fibre Channel (FC) over Ethernet (FCoE) transit switch, VN\_Port to VF\_Port FCoE Initialization Protocol (FIP) snooping sets up firewall filters to prevent unauthorized access through the transit switch to an FC switch or FCoE forwarder (FCF). You configure FIP snooping using different commands on FCoE transit switches that use the Enhanced Layer 2 Software (ELS) configuration style than on switches that don't use ELS.

**IN THIS SECTION**

- [Considerations When Configuring VN2VF\\_Port FIP Snooping | 47](#)
- [Configure VN2VF\\_Port FIP Snooping on ELS FCoE Transit Switches | 49](#)
- [Configure VN2VF\\_Port FIP Snooping on non-ELS FCoE Transit Switches | 50](#)

### Considerations When Configuring VN2VF\_Port FIP Snooping

VN\_Port to VF\_Port (VN2VF\_Port) Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping uses information gathered during FIP discovery and login to create firewall filters that provide

security against unauthorized access to the FC switch or FCoE forwarder (FCF) through the switch when the switch is acting as an FCoE transit switch. The firewall filters allow only FCoE devices that successfully log in to the FC fabric to access the FCF through the transit switch. VN2VF\_Port FIP snooping provides security for the point-to-point virtual links that connect host FCoE Nodes (ENodes) and FCFs in the FCoE VLAN by denying access to any device that does not successfully log in to the FCF.

VN2VF\_Port FIP snooping is disabled by default. You enable VN2VF\_Port FIP snooping on a per-VLAN basis for VLANs that carry FCoE traffic. Ensure that a VLAN that carries FCoE traffic carries only FCoE traffic, because enabling VN2VF\_Port FIP snooping denies access for all other Ethernet traffic.

**NOTE:** All of the transit switch ports are untrusted by default. If an ENode on an FCoE device logs in to an FCF before you enable VN2VF\_Port FIP snooping on the VLAN and you then enable VN2VF\_Port FIP snooping, the transit switch denies traffic from the ENode because the transit switch has not snooped (learned) the ENode state. The following process automatically logs the ENode back in to the FCF to reestablish the connection:

1. VN2VF\_Port FIP snooping is enabled on an FCoE VLAN on the switch.
2. The switch denies existing connections between servers and the FCF on the FCoE VLAN by filtering the FCoE traffic and FIP traffic, so no keepalive messages from the ENodes reach the FCF.
3. The FCF port timer for each ENode and for each VN\_Port on each ENode expires.
4. The FCF sends each ENode whose port timer has expired a Clear Virtual Links (CVL) message.
5. The CVL message causes the ENode to log in again.

Because the FCF is a trusted source, you configure interfaces that connect to the FCF as FCoE trusted interfaces. FCoE trusted interfaces do not filter traffic (FIP snooping filtering should occur only at the FCoE access edge), but VN2VF\_Port FIP snooping continues to run on trusted interfaces so that the switch learns the FCF state.

**NOTE:** Do not configure ENode-facing interfaces both with FIP snooping enabled and as trusted interfaces. FCoE VLANs with interfaces that are directly connected to FCoE hosts should be configured with FIP snooping enabled and the interfaces should *not* be trusted interfaces. Ethernet interfaces that are connected to an FCF should be configured as trusted interfaces and should not have FIP snooping enabled. Interfaces that are connected to a transit switch that is performing FIP snooping can be configured as trusted interfaces if the FCoE VLAN is not enabled for FIP snooping.

Optionally, you can specify an FC-MAP value for each FCoE VLAN. On a given FCoE VLAN, the switch learns only FCFs that have a matching FC-MAP value. The default FC-MAP value is 0EFC00h for all FC devices. (Enter hexadecimal values for FC-MAP preceded by the hexadecimal indicator “0x”—for example, 0x0EFC00.) If you change the FC-MAP value of an FCF, change the FC-MAP value for the FCoE VLAN it belongs to on the switch and on the servers you want to communicate with the FCF. An FCoE VLAN can have one and only one FC-MAP value.

**NOTE:** The default enhanced FIP snooping scaling supports 2,500 sessions. On QFabric systems, starting with Junos OS Release 13.2X52, you can disable enhanced FIP snooping scaling on a per-VLAN basis if you want to do so, but only 376 sessions are supported if you disable enhanced FIP snooping scaling.

There are some differences in the CLI commands you use to configure FIP snooping and FCoE trusted interfaces on a transit switch depending on whether the switch uses the Enhanced Layer 2 Software (ELS) configuration style or the original non-ELS CLI.

### Configure VN2VF\_Port FIP Snooping on ELS FCoE Transit Switches

Configure the following to enable VN2VF\_Port FIP snooping on FCoE transit switches that run the Enhanced Layer 2 Software (ELS) CLI:

- Enable VN2VF\_Port FIP snooping on a VLAN and optionally specify the FC-MAP value:

```
[edit]
user@switch# set vlans vlan-name forwarding-options fip-security fc-map fc-map-value examine-
vn2vf
```

For example, to enable VN2VF\_Port FIP snooping on a VLAN named **san1\_vlan** and change the FC-MAP value to **0x0EFC03**:

```
[edit]
user@switch# set vlans san1_vlan forwarding-options fip-security fc-map 0x0EFC03 examine-vn2vf
```

**NOTE:** Changing the FC-MAP value causes all logins to drop and forces ENodes to log in again.

- Configure an interface as an FCoE trusted interface:

```
[edit]
user@switch# set vlans vlan-name forwarding-options fip-security interface interface-name fcoe-
trusted
```

For example, to configure interface **xe-0/0/30** on VLAN named **san1\_vlan** as an FCoE trusted interface:

```
[edit]
user@switch# set vlans san1_vlan forwarding-options fip-security interface xe-0/0/30 fcoe-trusted
```

## Configure VN2VF\_Port FIP Snooping on non-ELS FCoE Transit Switches

Configure either of the following to enable VN2VF\_Port FIP snooping on FCoE transit switches that don't use ELS, depending on whether you want to specify an FC-MAP value or use the default FC-MAP value:

- To enable VN2VF\_Port FIP snooping on a single VLAN and specify the optional FC-MAP value:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan vlan-name examine-fip fc-map fc-map-value
```

For example, to enable VN2VF\_Port FIP snooping on a VLAN named **san1\_vlan** and change the FC-MAP value to **0x0EFC03**:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan san1_vlan examine-fip fc-map 0x0EFC03
```

**NOTE:** Changing the FC-MAP value causes all logins to drop and forces ENodes to log in again.



- To enable VN2VF\_Port FIP snooping on all VLANs and use the default FC-MAP value:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all examine-fip
```

- Configure an interface as an FCoE trusted interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface interface-name fcoe-trusted
```

For example, to configure interface **xe-0/0/30** as an FCoE trusted interface:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface xe-0/0/30 fcoe-trusted
```

## RELATED DOCUMENTATION

[Example: Configuring an FCoE Transit Switch](#)

*Configuring an FCoE VLAN Interface on an FCoE-FC Gateway*

*Configuring VLANs for FCoE Traffic on an FCoE Transit Switch*

*Configuring an FCoE LAG*

*Disabling Enhanced FIP Snooping Scaling*

[Understanding FIP Snooping](#)

*Understanding VN\_Port to VF\_Port FIP Snooping on an FCoE Transit Switch*

*Understanding FCoE LAGs*

## Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)

You can configure priority-based flow control (PFC) on EX4500 switches to apply link-level flow control on a specific traffic class so that different types of traffic can efficiently use the same network interface card (NIC). You must configure PFC for all interfaces carrying Fibre Channel over Ethernet (FCoE) traffic.

You can also configure PFC on interfaces carrying other traffic types, such as Internet small computer system interface (iSCSI) traffic. Using PFC is optional for traffic types other than FCoE.

**NOTE:**

- PFC is supported only on 10-Gigabit Ethernet interfaces.
- If you are using PFC for a non-FCoE DCBX application, use the same 802.1p code points for the PFC congestion notification profile and for the application map that is carrying that application traffic.

Data Center Bridging Capability Exchange protocol (DCBX) is enabled by default on all 10-Gigabit Ethernet interfaces on EX4500 switches. DCBX enables or disables PFC on the local interface depending on whether the PFC configuration on that interface is the same as the PFC configuration of the connected interface on the data center bridging (DCB) peer.

**NOTE:** When you configure PFC, we recommend that you:

- Configure at least 20 percent of the buffer for the queue that is using PFC.
- Configure an appropriate percent of the buffer for any other forwarding classes (default forwarding classes and the user-defined forwarding classes) that you are using.
- Do not specify the **exact** option when configuring the buffer for the queue that is using PFC.
- Configure the **loss-priority** statement to **low** for a traffic class that is using PFC.
- Verify that the PFC configurations of the local interfaces are the same as the PFC configurations of the connected interfaces on the DCB peer. See *show dcbx neighbors*.

EX Series switches support up to six congestion notification profiles for PFC.

To configure PFC:

1. Configure a congestion notification profile, specifying the name of the profile and specifying the three-bit pattern of the User Priority bits in an incoming frame that will trigger the priority-based flow control on that traffic class:

```
[edit class-of-service]
user@switch# set congestion-notification-profile profile-name input ieee-802.1 code-point up-bits
pfc
```

2. Disable standard Ethernet flow control on the interfaces that will be used for the traffic class that you have selected for PFC:

```
[edit interfaces]
user@switch# set interface-name ether-options no-flow-control
```

**NOTE:** You cannot apply PFC to interfaces that are using standard Ethernet flow control. You must first disable flow control on those interfaces.

3. Bind the congestion notification profile to the interfaces that will be used for the traffic class that you have selected for PFC:

```
[edit class-of-service]
user@switch# set interfaces interface-name congestion-notification-profile profile-name
```

4. Create a CoS classifier for a traffic class that will use PFC:

```
[edit class-of-service]
user@switch# set classifiers ieee-802.1 classifier-name import default
```

5. Configure this traffic class (*classifier-name*) to use a user-defined or default forwarding class with a low loss priority value and specify the 802.1p code points::

```
[edit class-of-service]
user@switch# set classifiers ieee-802.1 classifier-name forwarding-class class-name loss-priority low
code-points 3 bit-patterns
```

6. Bind the *classifier-name* classifier to all interfaces that require PFC:

```
[edit class-of-service]
user@switch# set interfaces interface-name unit logical-unit-number classifiers ieee-802.1 classifier-name
```

7. Assign the specified forwarding-class to an egress queue:

```
[edit class-of-service]
user@switch# set forwarding-classes class-name queue-number
```

8. Set a scheduler for this queue, allocating at least 20 percent of the buffer to be used for FCoE traffic:

```
[edit class-of-service]
user@switch# set schedulers scheduler-name buffer-size percent
```

9. Set a scheduler to allocate buffer space for forwarding classes carrying other traffic:

**NOTE:** You must explicitly allocate some buffer space for the other forwarding classes. The default allocation of buffer space for forwarding classes is overridden when you manually configure the requisite amount of buffer space for the FCoE traffic.

```
[edit class-of-service]
user@switch# set scheduler-name buffer-size percent
```

10. Configure a scheduler map that associates the specified scheduler with the specified forwarding class:

```
[edit class-of-service]
user@switch# set scheduler-maps map-name forwarding-class class-name scheduler scheduler-name
```

For example:

```
[edit class-of-service]
user@switch# set scheduler-maps pfc-map forwarding-class af2 scheduler pfc-sched
user@switch# set scheduler-maps pfc-map forwarding-class best-effort scheduler default-sched
user@switch# set scheduler-maps pfc-map forwarding-class network-control scheduler default-sched
user@switch# set scheduler-maps pfc-map forwarding-class expedited-forwarding scheduler default-sched
```

11. Assign the scheduler map to the egress interface:

```
[edit class-of-service]
user@switch# set interfaces interface-name scheduler-map pfc-map
```

## RELATED DOCUMENTATION

[Example: Configuring an FCoE Transit Switch | 22](#)

*Understanding Priority-Based Flow Control*

*congestion-notification-profile*

## Disabling DCBX to Disable PFC Autonegotiation on EX Series Switches (CLI Procedure)

As part of its autonegotiation capabilities, the Data Center Bridging Capability Exchange protocol (DCBX) automatically does the following:

- Advertises the priority flow control (PFC) configuration of the local interfaces to directly connected peers (switches and data center devices such as servers)
- Detects the PFC capabilities of the connected peers
- Enables the local interface's PFC capabilities if DCBX detects that the peer interface's PFC configuration is the same as the PFC configuration of the local interface.
- Disables the local interface's PFC capabilities if DCBX detects that the peer interface's PFC configuration is not the same as the PFC configuration of the local interface.

DCBX is enabled by default on all 10-Gigabit Ethernet interfaces on EX4500 switches. You can manually override DCBX control of the PFC operational state on a per-interface basis. You might want to disable autonegotiation if the DCB peer does not support PFC.

To disable the DCBX control of the PFC operational state:

- On an individual interface:

```
[edit protocols]
user@switch# set dcbx interface interface-name priority-flow-control no-auto-negotiation
```

- On all 10-Gigabit Ethernet interfaces:

```
[edit protocols]
user@switch# set dcbx interface all priority-flow-control no-auto-negotiation
```

## RELATED DOCUMENTATION

*show dcbx neighbors*

[Understanding DCBX Features and Requirements on EX Series Switches | 10](#)

## Disabling DCBX Application Protocol Exchange on EX Series Switches (CLI Procedure)

You can disable the Data Center Bridging Capability Exchange protocol (DCBX) Application Protocol exchange on a specific interface or on all interfaces.

To disable the DCBX application protocol exchange for any DCBX application, do the following:

**NOTE:** The format of the configuration statement specifies the **fcoe** application, however, this applies to *any* DCBX application (both FCoE applications and non-FCoE applications) on that interface.

- For a specific interface:

```
[edit protocols]
user@switch# set dcbx interface interface-name applications fcoe no-auto-negotiation
```

- For all interfaces:

```
[edit protocols]
user@switch# set dcbx interface all applications fcoe no-auto-negotiation
```

**NOTE:** If you disable the DCBX application protocol exchange, the *show dcbx neighbors* command displays **Feature: Application, Protocol-State: not-applicable**.

## RELATED DOCUMENTATION

*show dcbx neighbors*

[Disabling DCBX to Disable PFC Autonegotiation on EX Series Switches \(CLI Procedure\) | 55](#)

## Defining an Application for DCBX Application Protocol TLV Exchange

Define each application for which you want DCBX to exchange application protocol information. You can define Layer 2 and Layer 4 applications. After you define applications, you map them to IEEE 802.1p code points, and then apply the application map to the interfaces on which you want DCBX to exchange application protocol information with connected peers. (See *Related Documentation* for how to configure application maps and apply them to interfaces, and for an example of the entire procedure that also includes classifier configuration.)

**NOTE:** In Junos OS Release 12.1, the FCoE application was configured by default, so you did not need to configure it in an application map. In Junos OS Release 12.2, if you want DCBX to advertise the FCoE application on an interface and you apply an application map to that interface, you must explicitly configure FCoE in the application map. You also must enable priority-based flow control (PFC) on the FCoE code point on all interfaces that you want to advertise FCoE. If you apply an application map to an interface, the interface sends DCBX TLVs only for the applications configured in the application map.

Define Layer 2 applications by mapping an application name to an EtherType. Define Layer 4 applications by mapping an application name to a protocol (TCP or UDP) and a destination port.

- To define a Layer 2 application, specify the name of the application and its EtherType:

```
[edit applications]
user@switch# set application application-name ether-type ether-type
```

For example, to configure an application named **PTP** (for Precision Time Protocol) that uses the EtherType **0x88F7**:

```
user@switch# set applications application ptp ether-type 0x88F7
```

- To define a Layer 4 application, specify the name of the application, its protocol (TCP or UDP), and its destination port:

```
[edit]
user@switch# set applications application application-name protocol (tcp | udp) destination-port
port-value
```

For example, to configure an application named **iscsi** (for Internet Small Computer System Interface) that uses the protocol **TCP** and the destination port **3260**:

```
user@switch# set applications application iscsi protocol tcp destination-port 3260
```

## RELATED DOCUMENTATION

*Configuring an Application Map for DCBX Application Protocol TLV Exchange*

*Applying an Application Map to an Interface for DCBX Application Protocol TLV Exchange*

*Configuring DCBX Autonegotiation*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

*show dcbx neighbors*

## Configuring an Application Map for DCBX Application Protocol TLV Exchange

After you define applications for which you want to exchange DCBX application protocol information, map the applications to IEEE 802.1p code points. The IEEE 802.1p code points identify incoming traffic and allow you to map that traffic to the desired application. You then apply the application map to the interfaces on which you want DCBX to exchange application protocol information with connected peers. (See *Related Documentation* for how to define applications and apply the application map to interfaces, and for an example of the entire procedure that also includes classifier configuration.)



**NOTE:** In Junos OS Release 12.1, the FCoE application was configured by default, so you did not need to configure it in an application map. In Junos OS Release 12.2, if you want DCBX to advertise the FCoE application on an interface and you apply an application map to that interface, you must explicitly configure FCoE in the application map. You also must enable priority-based flow control (PFC) on the FCoE code point on all interfaces that you want to advertise FCoE. If you apply an application map to an interface, the interface sends DCBX TLVs only for the applications configured in the application map.

Configure an application map by creating an application map name and mapping an application to one or more IEEE 802.1p code points.

- To define an application map, specify the name of the application map, the name of the application, and the IEEE 802.1p code points of the incoming traffic that you want to associate with the application in the application map:

```
[edit policy-options]
user@switch# set application-maps application-map-name application application-name code-points
[ aliases ] [ bit-patterns ]
```

For example, to configure an application map named **ptp-app-map** that includes an application named **PTP** (for Precision Time Protocol) and map the application to IEEE 802.1p code points **001** and **101**:

```
user@switch# set policy-options application-maps ptp-app-map application ptp code-points [ 001 101 ]
```

## RELATED DOCUMENTATION

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Applying an Application Map to an Interface for DCBX Application Protocol TLV Exchange*

*Configuring DCBX Autonegotiation*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*show dcbx neighbors*

## Applying an Application Map to an Interface for DCBX Application Protocol TLV Exchange

After you define applications and map them to IEEE 802.1p code points in an application map, apply the application map to the interfaces on which you want DCBX to exchange the application protocol information with connected peers. (See *Related Documentation* for how to define applications and configure application maps to interfaces, and for an example of the entire procedure that also includes classifier configuration.)

**NOTE:** In Junos OS Release 12.1, the FCoE application was configured by default, so you did not need to configure it in an application map. In Junos OS Release 12.2, if you want DCBX to advertise the FCoE application on an interface and you apply an application map to that interface, you must explicitly configure FCoE in the application map. You also must enable priority-based flow control (PFC) on the FCoE code point on all interfaces that you want to advertise FCoE. If you apply an application map to an interface, the interface sends DCBX TLVs only for the applications configured in the application map.

- To apply an application map to a DCBX interface, specify the DCBX interface and the application map name:

```
[edit protocols]
user@switch# set dcbx interface interface-name application-map application-map-name
```

For example, to apply an application map named **ptp-app-map** on interface **xe-0/0/11**:

```
user@switch# set protocols dcbx interface xe-0/0/11 application-map ptp-app-map
```

### RELATED DOCUMENTATION

[\*Defining an Application for DCBX Application Protocol TLV Exchange\*](#)

[\*Configuring an Application Map for DCBX Application Protocol TLV Exchange\*](#)

[\*Configuring DCBX Autonegotiation\*](#)

[\*Example: Configuring DCBX Application Protocol TLV Exchange\*](#)

[Example: Configuring DCBX to Support an iSCSI Application](#)

[\*show dcbx neighbors\*](#)

## Disabling the ETS Recommendation TLV

The enhanced transmission selection (ETS) Recommendation TLV communicates the ETS settings that the switch wants the connected peer interface to use. If the peer interface is “willing,” the peer interface changes its configuration to match the configuration in the ETS Recommendation TLV. By default, the switch interfaces send the ETS Recommendation TLV to the peer. The settings communicated are the egress ETS settings defined by configuring hierarchical scheduling on the interface.

We recommend that you use the same ETS settings on the connected peer that you use on the switch interface and that you leave the ETS Recommendation TLV enabled. However, on interfaces that use IEEE DCBX as the DCBX mode, if you want an asymmetric configuration between the switch interface and the connected peer, you can disable the ETS Recommendation TLV.

**NOTE:** Disabling the ETS Recommendation TLV on interfaces that use DCBX version 1.01 as the DCBX mode has no effect and does not change DCBX behavior.

If you disable the ETS Recommendation TLV, the switch still sends the ETS Configuration TLV to the connected peer. The result is that the connected peer is informed about the switch DCBX ETS configuration, but even if the peer is “willing,” the peer does not change its configuration to match the switch configuration. This is asymmetric configuration—the two interfaces can have different parameter values for the ETS attribute.

To disable the ETS Recommendation TLV:

- ```
[edit protocols dcbx interface interface-name]  
user@switch# set enhanced-transmission-selection no-recommendation-tlv
```

### RELATED DOCUMENTATION

*Configuring the DCBX Mode*

*Configuring DCBX Autonegotiation*

*Understanding DCBX*

[Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches](#)

# Configuration Statements

## IN THIS CHAPTER

- application (Applications) | 63
- application (Application Maps) | 64
- applications (Applications) | 66
- application-map | 67
- application-maps | 69
- code-point (Congestion Notification) | 70
- code-points (Application Maps) | 72
- congestion-notification-profile | 73
- dcbx | 77
- destination-port (Applications) | 79
- disable (DCBX) | 80
- ether-type | 82
- ethernet-switching-options | 83
- examine-fip | 90
- fc-map | 92
- fcoe | 95
- fcoe-trusted | 96
- ieee-802.1 (Congestion Notification) | 98
- input (Congestion Notification) | 99
- interface (Access Port Security) | 101
- interface (DCBX) | 103
- interfaces | 105
- policy-options | 107
- priority-flow-control | 108
- protocol (Applications) | 110
- secure-access-port | 112

- [vlan \(Access Port Security\) | 115](#)

## application (Applications)

### IN THIS SECTION

- [Syntax | 63](#)
- [Hierarchy Level | 63](#)
- [Description | 63](#)
- [Options | 64](#)
- [Required Privilege Level | 64](#)
- [Release Information | 64](#)

### Syntax

```
application application-name {  
    destination-port port-value;  
    protocol (tcp | udp);  
    ether-type type;  
}
```

### Hierarchy Level

```
[edit applications]
```

### Description

Configure properties to define an application.

## Options

*application-name*—Name of the application.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## application (Application Maps)

### IN THIS SECTION

- [Syntax | 65](#)
- [Hierarchy Level | 65](#)
- [Description | 65](#)
- [Options | 65](#)
- [Required Privilege Level | 65](#)
- [Release Information | 65](#)

## Syntax

```
application application-name {
    code-points [ aliases ] [ bit-patterns ];
}
```

## Hierarchy Level

```
[edit policy-options application-maps application-map-name]
```

## Description

Add an application to an application map and define the application's code points.

## Options

***application-name***—Name of the application.

The remaining statement is explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Configuring an Application Map for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## applications (Applications)

### IN THIS SECTION

- [Syntax | 66](#)
- [Hierarchy Level | 66](#)
- [Description | 66](#)
- [Options | 66](#)
- [Required Privilege Level | 67](#)
- [Release Information | 67](#)

### Syntax

```
applications {  
    application application-name {  
        destination-port port-value;  
        protocol (tcp | udp);  
        ether-type type;  
    }  
}
```

### Hierarchy Level

[edit]

### Description

Define applications that DCBX advertises.

### Options

The remaining statements are explained separately. See [CLI Explorer](#).



## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## application-map

### IN THIS SECTION

- [Syntax | 67](#)
- [Hierarchy Level | 68](#)
- [Description | 68](#)
- [Options | 68](#)
- [Required Privilege Level | 68](#)
- [Release Information | 68](#)

## Syntax

```
application-map application-map-name;
```

## Hierarchy Level

```
[edit protocols dcbx interface interface-name]
```

## Description

Specify an application map to apply to an interface.

## Options

*application-map-name*—Name of the application map.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

---

*show dcbx neighbors*

---

*Applying an Application Map to an Interface for DCBX Application Protocol TLV Exchange*

---

*Example: Configuring DCBX Application Protocol TLV Exchange*

---

[Example: Configuring DCBX to Support an iSCSI Application](#)

---

*Understanding DCBX Application Protocol TLV Exchange*

---

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## application-maps

### IN THIS SECTION

- [Syntax | 69](#)
- [Hierarchy Level | 69](#)
- [Description | 69](#)
- [Options | 69](#)
- [Required Privilege Level | 70](#)
- [Release Information | 70](#)

### Syntax

```
application-maps application-map-name {  
    application application-name {  
        code-points [ aliases ] [ bit-patterns ];  
    }  
}
```

### Hierarchy Level

```
[edit policy-options]
```

### Description

Define an application map by specifying the applications that belong to the application map.

### Options

***application-map-name***—Name of the application map.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Configuring an Application Map for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## code-point (Congestion Notification)

### IN THIS SECTION

- [Syntax | 70](#)
- [Hierarchy Level | 71](#)
- [Description | 71](#)
- [Options | 71](#)
- [Required Privilege Level | 71](#)
- [Release Information | 71](#)

## Syntax

```
code-point up-bits pfc;
```

## Hierarchy Level

```
[edit class-of-service congestion-notification-profile profile-name input
ieee-802.1],
[edit class-of-service interfaces interface-name congestion-notification-profile
profile-name input ieee-802.1]
```

## Description

Configure the IEEE 802.1p (User Priority) code point bits as input for creating the priority-based flow control (PFC) congestion notification profile, which you will associate with a particular traffic class.

## Options

- *pfc*—PFC flow control method
- *up-bits*—Three-bit pattern of the User Priority field in an IEEE 802.1Q tag

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

[Example: Configuring an FCoE Transit Switch | 22](#)

*Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*

## code-points (Application Maps)

### IN THIS SECTION

- [Syntax | 72](#)
- [Hierarchy Level | 72](#)
- [Description | 72](#)
- [Options | 72](#)
- [Required Privilege Level | 72](#)
- [Release Information | 73](#)

### Syntax

```
code-points [ aliases ] [ bit-patterns ];
```

### Hierarchy Level

```
[edit policy-options application-maps application-map-name application  
application-name]
```

### Description

Define one or more code-point aliases or bit sets for an application.

### Options

*aliases*—Name of the alias or aliases.

*bit-patterns*—Value of the code-point bits, in decimal form.

### Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Configuring an Application Map for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## congestion-notification-profile

### IN THIS SECTION

- [Syntax | 73](#)
- [EX4500 and EX4550 Switches | 74](#)
- [Hierarchy Level | 74](#)
- [Description | 75](#)
- [Options | 75](#)
- [Required Privilege Level | 76](#)
- [Release Information | 76](#)

## Syntax

```
congestion-notification-profile profile-name {
  input {
    (dscp | ieee-802.1) {
      code-point [code-point-bits] {
```

```

        pfc {
            mru mru-value;
        }
    }
}
cable-length cable-length-value;
}
output {
    ieee-802.1 {
        code-point [code-point-bits] {
            flow-control-queue [queue | list-of-queues];
        }
    }
}
pfc-watchdog {
    detection number of polling intervals;
    pfc-watchdog-action {
        drop;
    }
    poll-interval time;
    recovery time;
}
}

```

## EX4500 and EX4550 Switches

```

congestion-notification-profile profile-name {
    input {
        ieee-802.1 {
            code-point up-bits pfc;
        }
    }
}

```

## Hierarchy Level

```

[edit class-of-service],
[edit class-of-service interfaces interface-name]

```



## Description

Configure a congestion notification profile (CNP) to enable priority-based flow control (PFC) on traffic and apply the profile to an interface. You can apply a CNP to most interfaces, including aggregated ethernet (AE) interfaces and their individual members.

A congestion notification profile can be configured to enable PFC on incoming traffic (**input** stanza) that matches the following:

- A Differentiated Services code point (DSCP) value in the Layer 3 IP header (for traffic that is not VLAN-tagged).
- An IEEE 802.1 code point at Layer 2 in the VLAN header (for VLAN-tagged traffic).

A congestion notification profile can be configured to enable PFC on outgoing traffic (**output** stanza) specified only by an IEEE 802.1 code point at Layer 2 in the VLAN header.

**NOTE:** You must configure PFC for FCoE traffic. Each interface that carries FCoE traffic should be configured for PFC on the FCoE code point (usually **011**).

There is no limit to the total number of congestion notification profiles you can create. However:

- You can attach a maximum of one congestion notification profile to an interface.
- DSCP-based PFC and IEEE 802.1p PFC cannot be configured under the same congestion notification profile.

**NOTE:** Configuring or changing PFC on an interface blocks the entire port until the PFC change is completed. After a PFC change is completed, the port is unblocked and traffic resumes. Blocking the port stops ingress and egress traffic, and causes packet loss on all queues on the port until the port is unblocked.

## Options

***profile-name*** Name of the congestion notification profile.

***pfc-watchdog*** Enable the Priority Flow Control (PFC) watchdog. If you do not configure any options, the default values are used.

- **pfc-watchdog-action drop**—When the PFC watchdog detects that a PFC queue has stalled, it drops all queued packets and all newly arriving packets for the stalled PFC queue. This option is the default.
- **poll-interval *time***—How often the PFC watchdog checks the status of PFC queues. Configure the polling interval in milliseconds.
  - Default: 100
  - Range: 100-1000
- **detection *number of polling intervals***—How many polling intervals the PFC watchdog waits before it determines that a PFC queue has stalled.
  - Default: 2
  - Range: 2-10
- **recovery *time***—Configure in milliseconds how long the PFC watchdog disables the affected queues before it re-enables PFC.
  - Default: 200
  - Range: 200-10,000

The remaining statements are explained separately. Search for a statement in [CLI Explorer](#) or click a linked statement in the Syntax section for details.

## Required Privilege Level

**interface**—To view this statement in the configuration.

**interface-control**—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

Support for DSCP values introduced in Junos OS Release 17.4R1 for the QFX Series.

**pfc-watchdog** option introduced in Junos OS Evolved Release 20.4R1 for the PTX10008.

## RELATED DOCUMENTATION

[Configuring CoS PFC \(Congestion Notification Profiles\)](#)

*Understanding CoS Flow Control (Ethernet PAUSE and PFC)*

[Understanding CoS IEEE 802.1p Priorities for Lossless Traffic Flows](#)

[Understanding PFC Using DSCP at Layer 3 for Untagged Traffic](#)

[Configuring DSCP-based PFC for Layer 3 Untagged Traffic](#)

[PFC Watchdog](#)

## dcbx

### IN THIS SECTION

- [Syntax | 77](#)
- [Hierarchy Level | 78](#)
- [Description | 78](#)
- [Options | 78](#)
- [Required Privilege Level | 78](#)
- [Release Information | 78](#)

## Syntax

```
dcbx {
  disable;
  interface (interface-name | all) {
    disable;
    application-map application-map-name;
    applications {
      no-auto-negotiation;
    }
    enhanced-transmission-selection {
      no-auto-negotiation;
      no-recommendation-tlv;
      recommendation-tlv {
        no-auto-negotiation;
      }
    }
  }
}
```

```

    dcbx-version (auto-negotiate | ieee-dcbx | dcbx-version-1.01);
    priority-flow-control {
        no-auto-negotiation;
    }
}
}

```

## Hierarchy Level

[edit [protocols](#)]

## Description

Configure DCBX properties. DCBX is an extension of Link Layer Discovery Protocol (LLDP), and LLDP must remain enabled on every interface for which you want to use DCBX. If you attempt to enable DCBX on an interface on which LLDP is disabled, the configuration commit fails.

## Options

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.1.

**mode** and **recommendation-tlv** statements introduced in Junos OS Release 12.2 for the QFX Series.

## RELATED DOCUMENTATION

---

*show dcbx neighbors*

---

*Understanding DCB Features and Requirements*

---

*Configuring DCBX Autonegotiation*

## destination-port (Applications)

### IN THIS SECTION

- Syntax | 79
- Hierarchy Level | 79
- Description | 79
- Options | 80
- Required Privilege Level | 80
- Release Information | 80

### Syntax

```
destination-port port-value;
```

### Hierarchy Level

```
[edit applications application application-name]
```

### Description

Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) destination port number, which combines with **protocol** to identify an application type. The Internet Assigned Numbers Authority (IANA) assigns port numbers. See the IANA *Service Name and Transport Protocol Port Number Registry* at <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml> for a list of assigned port numbers.

**NOTE:** To create an application for iSCSI, use the protocol **tcp** with the destination port number **3260**.

## Options

*port-value*—Identifier for the port.

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## disable (DCBX)

### IN THIS SECTION

- [Syntax | 81](#)
- [Hierarchy Level | 81](#)
- [Description | 81](#)
- [Default | 81](#)
- [Required Privilege Level | 81](#)
- [Release Information | 81](#)

## Syntax

```
disable
```

## Hierarchy Level

```
[edit protocols dcbx]  
  
[edit protocols dcbx interface interface-name]
```

## Description

Disable Data Center Bridging Capability Exchange protocol (DCBX) on one or more 10-Gigabit Ethernet interfaces.

## Default

DCBX is enabled by default on all 10-Gigabit or higher Ethernet interfaces.

DCBX is enabled by default on all 10-Gigabit Ethernet interfaces on EX4500 CEE-enabled switches.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.1.

## RELATED DOCUMENTATION

---

*Configuring DCBX Autonegotiation*

---

[Disabling DCBX to Disable PFC Autonegotiation on EX Series Switches \(CLI Procedure\)](#)

---

*Understanding DCB Features and Requirements*

---

[Understanding DCB Features and Requirements on EX Series Switches](#)

## ether-type

### IN THIS SECTION

- Syntax | 82
- Hierarchy Level | 82
- Description | 82
- Options | 82
- Required Privilege Level | 83
- Release Information | 83

### Syntax

```
ether-type ether-type;
```

### Hierarchy Level

```
[edit applications application application-name]
```

### Description

Two-octet field in an Ethernet frame that defines the protocol encapsulated in the frame payload. See <http://standards.ieee.org/develop/regauth/ethertype/eth.txt> for a list of Institute of Electrical and Electronics Engineers (IEEE) EtherTypes.

**NOTE:** To create a FIP application, use the EtherType 0x8914.

### Options

*type*—Identifier for the EtherType.



## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

*Understanding DCBX Application Protocol TLV Exchange*

## ethernet-switching-options

### IN THIS SECTION

- [EX Series | 83](#)
- [QFX Series, QFabric, EX4600 | 87](#)
- [Hierarchy Level | 89](#)
- [Description | 89](#)
- [Required Privilege Level | 90](#)
- [Release Information | 90](#)

## EX Series

```
ethernet-switching-options {
  analyzer {
    name {
      loss-priority priority;
```

```

        ratio number;
    input {
        ingress {
            interface (all | interface-name);
            vlan (vlan-id | vlan-name);
        }
        egress {
            interface (all | interface-name);
        }
    }
    output {
        interface interface-name;
        vlan (vlan-id | vlan-name) {
            no-tag;
        }
    }
}

bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]) {
        (disable | drop | shutdown);
    }
}

dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
}

interfaces interface-name {
    no-mac-learning;
    no-mac-notification;
}

mac-lookup-length number-of-entries;
}

mac-notification {
    notification-interval seconds;
}

mac-table-aging-time seconds;
nonstop-bridging;
port-error-disable {
    disable-timeout timeout;
}

redundant-trunk-group {
    group name {

```

```

        interface interface-name <primary>;
        interface interface-name;
    }
}
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    dhcpv6-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
}
interface (all | interface-name) {
    allowed-mac {
        mac-address-list;
    }
    (dhcp-trusted | no-dhcp-trusted);
    fcoe-trusted;
    mac-limit limit action (drop | log | none | shutdown);
    no-allowed-mac-log;
    persistent-learning;
    static-ip ip-address {
        vlan vlan-name;
        mac mac-address;
    }
    static-ipv6 ip-address {
        vlan vlan-name;
        mac mac-address;
    }
}
vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) [
        forwarding-class class-name;
    ]
    dhcp-option82 {
        circuit-id {
            prefix hostname;
            use-interface-description;
            use-vlan-id;
        }
    }
}

```

```

        remote-id {
            prefix hostname | mac | none;
            use-interface-description;
            use-string string;
        }
        vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp) {
        forwarding-class class-name;
    }
    (examine-dhcpv6 | no-examine-dhcpv6) {
        forwarding-class class-name;
    }
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);
}
(neighbor-discovery-inspection | no-neighbor-discovery-inspection);
no-option-37;
static {
    vlan name {
        mac mac-address {
            next-hop interface-name;
        }
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        level level;
        multicast;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}
traceoptions {

```

```

        file filename <files number> <no-stamp> <replace> <size size> <world-
readable | no-world-readable>;
        flag flag <disable>;
    }
    unknown-unicast-forwarding {
        vlan (all | vlan-name) {
            interface interface-name;
        }
    }
    voip {
        interface (all | [interface-name | access-ports]) {
            forwarding-class forwarding-class;
            vlan vlan-name;
        }
    }
}

```

## QFX Series, QFabric, EX4600

```

ethernet-switching-options {
    analyzer {
        name {
            input {
                egress {
                    interface (all | interface-name);
                }
                ingress {
                    interface (all | interface-name);
                    vlan (vlan-id | vlan-name);
                }
            }
            output {
                interface interface-name;
                ip-address ip-address;
                vlan (vlan-id | vlan-name);
            }
        }
    }
    bpdu-block {
        interface (all | [interface-name]);
        disable-timeout timeout;
    }
}

```

```

dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100)
}
interfaces interface-name {
    no-mac-learning;
}
mac-table-aging-time seconds {
}
port-error-disable {
    disable-timeout timeout;
}
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action action;
        no-allowed-mac-log;
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection) [
            forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        ]
        dhcp-option82 {
            circuit-id {
                prefix (Circuit ID for Option 82) hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix (Remote ID for Option 82) hostname | mac | none;
                use-interface-description;
                use-string string;
            }
            vendor-id <string>;
        }
    }
}

```

```

        (examine-dhcp | no-examine-dhcp) {
            forwarding-class (for DHCP Snooping or DAI Packets) class-name;
        }
    examine-fip {
        examine-vn2vn {
            beacon-period milliseconds;
        }
        fc-map fc-map-value;
    }
    mac-move-limit limit <fabric-limit limit action action;
}
}
static {
    vlan vlan-id {
        mac mac-address next-hop interface-name;
    }
}
storm-control {
    interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-unknown-unicast;
    }
}
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-
readable | no-world-readable>;
    flag flag <disable>;
}
}

```

## Hierarchy Level

[edit]

## Description

Configure Ethernet switching options.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

|                                                                                |
|--------------------------------------------------------------------------------|
| <a href="#">Understanding Port Mirroring and Analyzers</a>                     |
| <a href="#">Understanding How to Protect Access Ports from Common Attacks</a>  |
| <a href="#">Port Security Features</a>                                         |
| <a href="#">Understanding BPDU Protection for STP, RSTP, and MSTP</a>          |
| <a href="#">Understanding Redundant Trunk Links (Legacy RTG Configuration)</a> |
| <a href="#">Understanding Storm Control</a>                                    |
| <a href="#">Understanding 802.1X and VoIP on EX Series Switches</a>            |
| <a href="#">Understanding Q-in-Q Tunneling and VLAN Translation</a>            |
| <a href="#">Understanding MAC Notification on EX Series Switches</a>           |
| <a href="#">Understanding FIP Snooping   2</a>                                 |
| <a href="#">Understanding Nonstop Bridging on EX Series Switches</a>           |

examine-fip

IN THIS SECTION

- Syntax | 91
- Hierarchy Level | 91
- Description | 91
- Required Privilege Level | 91
- Release Information | 92



## Syntax

```
examine-fip {
    examine-vn2vn {
        beacon-period milliseconds;
    }
    fc-map fc-map-value;
    no-fip-snooping-scaling;
}
```

## Hierarchy Level

```
[edit ethernet-switching-options secure-access-port vlan (all | vlan-name)]
```

## Description

**NOTE:** This statement supports the original CLI. If your switch runs the Enhanced Layer 2 Software (ELS) CLI, see *examine-vn2vf* for VN\_Port to VF\_Port (VN2VF\_Port) FIP snooping, and see *examine-vn2vn* for VN\_Port to VN\_Port (VN2VN\_Port) FIP snooping. For ELS details, see [Using the Enhanced Layer 2 Software CLI](#).

Enable FIP snooping on a specified VLAN. Ensure that the VLAN is a dedicated FCoE VLAN that transports only FCoE traffic.

(QFX Series only) Enable VN2VN\_Port FIP snooping on the specified VLAN. The VLAN must be a dedicated FCoE VLAN that transports only VN2VN\_Port traffic. One FCoE VLAN cannot support both VN2VF\_Port FIP snooping and VN2VN\_Port FIP snooping. Configure separate, dedicated FCoE VLANs for VN2VN\_Port FIP snooping and VN2VN\_Port FIP snooping.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

Statement **examine-vn2vn** introduced in Junos OS Release 12.2 for the QFX Series.

Statement **no-fip-snooping-scaling** introduced in Junos OS Release 13.2X52-D10 for the QFX Series.

## RELATED DOCUMENTATION

*vlan*

[Example: Configuring an FCoE Transit Switch | 22](#)

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

## fc-map

### IN THIS SECTION

- [Syntax | 92](#)
- [Hierarchy Level | 93](#)
- [Description | 93](#)
- [Options | 94](#)
- [Required Privilege Level | 94](#)
- [Release Information | 94](#)

## Syntax

```
fc-map fc-map-value;
```

## Hierarchy Level

### Original CLI

```
[edit ethernet-switching options secure-access-port vlan (all | vlan-name)  
  examine-fip]
```

### ELS CLI for Platforms that Support FCoE

```
[edit vlans vlan-name forwarding-options fip-security]
```

**NOTE:** The **fc-map** configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.

### QFX Series that Support FCoE-FC Gateway Configuration

```
[edit fc-fabrics fc-fabric-name protocols fip]
```

## Description

Set the FCoE mapped address prefix (FC-MAP) value for the FCoE VLAN to match the FC switch (or FCoE forwarder) FC-MAP value for the FC fabric. The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN).

You can configure the FC-MAP value or use the default value. The default FC-MAP value is different for VN\_Port to VF\_Port (VN2VF\_Port) FIP snooping (0x0EFC00) than for VN\_Port to VN\_Port (VN2VN\_Port) FIP snooping.

The FC switch provides the FC-MAP value to FCoE nodes (ENodes) in the FIP discovery advertisement message. If the EX Series switch or the QFX Series FCoE VLAN FC-MAP value does not match the FC switch FC-MAP value, neither device discovers the FC switch on that VLAN, and the ENodes on that VLAN cannot access the FC switch. The FC switch accepts only FCoE traffic that uses the correct FC-MAP value as part of the VN\_Port MAC address.

When the QFX Series acts as an FCoE-FC gateway, the FC-MAP value for the gateway and the FCoE devices must match the FC switch FC-MAP value in order to communicate with the FC switch.

**NOTE:** Changing the FC-MAP value causes all logins to drop and forces the ENodes to log in again.

## Options

*fc-map-value*—FC-MAP value, hexadecimal value preceded by “0x”.

- **Range:** 0x0EFC00 through 0x0EFCFF
- **Default:** 0x0EFC00 for VN2VF\_Port FIP snooping  
0x0EFD00 for VN2VN\_Port FIP snooping

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.

## RELATED DOCUMENTATION

[examine-fip](#)

[show fip snooping](#)

[Example: Configuring an FCoE Transit Switch](#)

[Configuring VN2VF\\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch](#)

## fcoe

### IN THIS SECTION

- [Syntax | 95](#)
- [Hierarchy Level | 95](#)
- [Description | 95](#)
- [Options | 95](#)
- [Required Privilege Level | 95](#)
- [Release Information | 96](#)

### Syntax

```
fcoe {  
    no-auto-negotiation;  
}
```

### Hierarchy Level

```
[edit protocols dcbx interface interface-name applications]
```

### Description

Disable advertising the FCoE state of the interface to the peer. To disable FCoE on the interface, do not configure the FCoE forwarding class on the interface.

### Options

**no-auto-negotiate**—Disable automatic negotiation of FCoE capability.

### Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.1.

## RELATED DOCUMENTATION

*show dcbx neighbors*

*Understanding DCB Features and Requirements*

[Understanding DCB Features and Requirements on EX Series Switches | 10](#)

## fcoe-trusted

### IN THIS SECTION

- [Syntax | 96](#)
- [Hierarchy Level | 96](#)
- [Description | 97](#)
- [Required Privilege Level | 97](#)
- [Release Information | 97](#)

## Syntax

```
fcoe-trusted;
```

## Hierarchy Level

Original CLI

```
[edit ethernet-switching-options secure-access-port interface interface-name]
```

## ELS CLI for Platforms that Support FCoE

```
[edit vlans vlan-name forwarding-options fip-security interface interface-name]
```

**NOTE:** The **fcoe-trusted** configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.

## QFX Series that Support FCoE-FC Gateway Configuration

```
[edit fc-fabrics fc-fabric-name protocols fip]
```

### Description

Configure the specified 10-Gigabit Ethernet interface to trust Fibre Channel over Ethernet (FCoE) traffic. If an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters.

(QFX Series FCoE-FC gateway) Configure the specified local Fibre Channel fabric to trust FCoE traffic on all ports in the fabric. Changing the fabric ports from untrusted to trusted removes any existing FIP snooping filters from the ports. Changing the fabric ports from trusted to untrusted by removing the **fcoe-trusted** configuration from the fabric forces all of the FCoE sessions on those ports to log out so that when the ENodes and VN\_Ports log in again, the switch can build the appropriate FIP snooping filters.

### Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

### Release Information

Statement introduced in Junos OS Release 10.4.

Statement introduced for the FC fabric in Junos OS Release 11.3 for the QFX Series.

Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.

## RELATED DOCUMENTATION

*show fip snooping*

[Example: Configuring an FCoE Transit Switch](#)

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

## ieee-802.1 (Congestion Notification)

### IN THIS SECTION

- [Syntax | 98](#)
- [Hierarchy Level | 98](#)
- [Description | 98](#)
- [Required Privilege Level | 99](#)
- [Release Information | 99](#)

### Syntax

```
ieee-802.1 {
    code-point up-bits pfc ;
}
```

### Hierarchy Level

```
[edit class-of-service congestion-notification-profile profile-name],
[edit class-of-service interfaces interface-name congestion-notification-profile
profile-name]
```

### Description

Set an association between the traffic class and the congestion notification profile.



The remaining statement is explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

[Example: Configuring an FCoE Transit Switch | 22](#)

*Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*

## input (Congestion Notification)

### IN THIS SECTION

- [Syntax | 99](#)
- [Hierarchy Level | 100](#)
- [Description | 100](#)
- [Required Privilege Level | 100](#)
- [Release Information | 100](#)

## Syntax

```
input {
  ieee-802.1 {
    code-point up-bits pfc ;
```

```
}
}
```

## Hierarchy Level

```
[edit class-of-service congestion-notification-profile profile-name],
[edit class-of-service interfaces interface-name congestion-notification-profile
profile-name]
```

## Description

Identify the three-bit pattern of the User Priority field that triggers the priority-based congestion notification profile for a specified traffic class.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

[Example: Configuring an FCoE Transit Switch | 22](#)

*Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)*

## interface (Access Port Security)

### IN THIS SECTION

- [Syntax | 101](#)
- [Hierarchy Level | 102](#)
- [Description | 102](#)
- [Options | 102](#)
- [Required Privilege Level | 102](#)
- [Release Information | 102](#)

### Syntax

```
interface (all | interface-name) {
    allowed-mac {
        mac-address-list;
    }
    (dhcp-trusted | no-dhcp-trusted);
    fcoe-trusted;
    mac-limit limit action (drop | log | none | shutdown);
    no-allowed-mac-log;
    persistent-learning;
    static-ip ip-address {
        vlan vlan-name;
        mac mac-address;
    }
    static-ipv6 ip-address {
        vlan vlan-name;
        mac mac-address;
    }
}
vlan vlan-name {
    mac-limit limit action (drop | log | none | shutdown);
}
```

## Hierarchy Level

```
[edit ethernet-switching-options secure-access-port]
```

## Description

Apply port security features to all interfaces or to the specified interface.

## Options

**all**—Apply port security features to all interfaces.

*interface-name*—Apply port security features to the specified interface.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

**system**—To view this statement in the configuration.

**system-control**—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.0.

Support for the **ipv6-source-guard** statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

## RELATED DOCUMENTATION

[Example: Configuring Port Security \(non-ELS\)](#)

[Example: Protecting Against DHCP Snooping Database Attacks](#)

[Example: Protecting against Ethernet Switching Table Overflow Attacks](#)

[Example: Protecting against DHCP Starvation Attacks](#)

[Example: Protecting against Rogue DHCP Server Attacks](#)

[Configuring MAC Limiting \(non-ELS\)](#)

[Enabling a Trusted DHCP Server \(non-ELS\)](#)

## interface (DCBX)

### IN THIS SECTION

- [Syntax | 103](#)
- [Hierarchy Level | 104](#)
- [Description | 104](#)
- [Options | 104](#)
- [Required Privilege Level | 104](#)
- [Release Information | 104](#)

### Syntax

```
interface (interface-name | all) {  
    disable;  
    application-map application-map-name;  
    applications {  
        no-auto-negotiation;  
    }  
    enhanced-transmission-selection {  
        no-auto-negotiation;  
        no-recommendation-tlv;  
        recommendation-tlv {  
            no-auto-negotiation;  
        }  
    }  
    dcbx-version (auto-negotiate | ieee-dcbx | dcbx-version-1.01);  
    priority-flow-control {  
        no-auto-negotiation;  
    }  
}
```

# Hierarchy Level

```
[edit protocols dcbx]
```

## Description

Configure DCBX properties on an interface.

## Options

*interface-name*—Name of the interface.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.1.

**Mode** and **recommendation-tlv** statements introduced in Junos OS Release 12.2 for the QFX Series.

## RELATED DOCUMENTATION

|                                                                                            |
|--------------------------------------------------------------------------------------------|
| <i>show dcbx neighbors</i>                                                                 |
| <i>Configuring DCBX Autonegotiation</i>                                                    |
| <a href="#">Example: Configuring DCBX to Support an iSCSI Application</a>                  |
| <i>Understanding DCB Features and Requirements</i>                                         |
| <a href="#">Understanding DCB Features and Requirements on EX Series Switches</a>          |
| <a href="#">Understanding DCBX Application Protocol TLV Exchange on EX Series Switches</a> |

## interfaces

### IN THIS SECTION

- [Syntax | 105](#)
- [Hierarchy Level | 106](#)
- [Description | 106](#)
- [Options | 106](#)
- [Required Privilege Level | 106](#)
- [Release Information | 106](#)

### Syntax

```

interfaces {
    interface-name {
        congestion-notification-profile profile-name {
            input {
                ieee-802.1 {
                    code-point up-bits pfc;
                }
            }
        }
        scheduler-map map-name;
        unit logical-unit-number {
            forwarding-class class-name;
            classifiers {
                (dscp | ieee-802.1 | inet-precedence) (classifier-name |
default);
            }
        }
    }
}

```

## Hierarchy Level

```
[edit class-of-service]
```

## Description

Configure interface-specific class-of-service (CoS) properties for incoming packets.

## Options

**interface-name** Name of the interface.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.0.

## RELATED DOCUMENTATION

[Example: Configuring CoS on EX Series Switches](#)

[Defining CoS Classifiers \(CLI Procedure\)](#)

[Defining CoS Classifiers \(J-Web Procedure\)](#)

[Defining CoS Forwarding Classes \(CLI Procedure\)](#)

[Defining CoS Forwarding Classes \(J-Web Procedure\)](#)

[Defining CoS Schedulers and Scheduler Maps \(CLI Procedure\)](#)

[Defining CoS Schedulers \(J-Web Procedure\)](#)

[Configuring Priority-Based Flow Control for an EX Series Switch \(CLI Procedure\)](#)



## policy-options

### IN THIS SECTION

- [Syntax | 107](#)
- [Hierarchy Level | 108](#)
- [Description | 108](#)
- [Required Privilege Level | 108](#)
- [Release Information | 108](#)

### Syntax

```

policy-options
  application-maps application-map-name {
    application application-name {
      code-points [ aliases ] [ bit-patterns ];
    }
  }
  policy-statement policy-name {
    term term-name {
      from {
        family family-name;
        match-conditions;
        policy subroutine-policy-name;
        prefix-list prefix-list-name;
        prefix-list-filter prefix-list-name match-type <actions>;
        route-filter destination-prefix match-type <actions>;
        source-address-filter source-prefix match-type <actions>;
      }
      to {
        match-conditions;
        policy subroutine-policy-name;
      }
      then actions;
    }
  }

```

## Hierarchy Level

[edit]

## Description

Configure options such as application maps for DCBX application protocol exchange and policy statements.

## Required Privilege Level

storage—To view this statement in the configuration.

storage-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## priority-flow-control

### IN THIS SECTION

● [Syntax | 109](#)

● [Hierarchy Level | 109](#)

- [Description | 109](#)
- [Options | 109](#)
- [Required Privilege Level | 109](#)
- [Release Information | 110](#)

## Syntax

```
priority-flow-control {
    no-auto-negotiation;
}
```

## Hierarchy Level

```
[edit protocols dcbx interface (all | interface-name)]
```

## Description

Disable autonegotiation of priority-based flow control (PFC) on one or more Ethernet interfaces. Autonegotiation enables PFC on an interface only if the switch and the peer device connected to the switch both support PFC and have the same PFC configuration. Disabling autonegotiation on an interface forces the interface to use the PFC state (enabled or disabled) that is configured on the switch by the configuration and assignment of the congestion notification profile.

## Options

**no-auto-negotiation**—Disable automatic negotiation of PFC.

## Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 11.1.

## RELATED DOCUMENTATION

*show dcbx neighbors*

[Configuring CoS PFC \(Congestion Notification Profiles\)](#)

[Configuring Priority-Based Flow Control for an EX Series Switch \(CLI Procedure\)](#)

*Configuring DCBX Autonegotiation*

*Example: Configuring CoS PFC for FCoE Traffic*

[Understanding Data Center Bridging Capability Exchange Protocol for EX Series Switches](#)

[Understanding Priority-Based Flow Control](#)

*Understanding DCB Features and Requirements*

## protocol (Applications)

### IN THIS SECTION

- [Syntax | 110](#)
- [Hierarchy Level | 111](#)
- [Description | 111](#)
- [Options | 111](#)
- [Required Privilege Level | 111](#)
- [Release Information | 111](#)

## Syntax

```
protocol (tcp | udp);
```

## Hierarchy Level

```
[edit applications application application-name]
```

## Description

Networking protocol type, which combines with **destination-port** to identify an application type.

**NOTE:** To create an application for iSCSI, use the protocol **tcp** with the destination port number **3260**.

## Options

**tcp**—Transmission Control Protocol

**udp**—User Datagram Protocol

## Required Privilege Level

**interface**—To view this statement in the configuration.

**interface-control**—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 12.1.

## RELATED DOCUMENTATION

*Defining an Application for DCBX Application Protocol TLV Exchange*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring DCBX to Support an iSCSI Application](#)

*Understanding DCBX Application Protocol TLV Exchange*

[Understanding DCBX Application Protocol TLV Exchange on EX Series Switches](#)

## secure-access-port

### IN THIS SECTION

- [Syntax | 112](#)
- [Hierarchy Level | 114](#)
- [Description | 114](#)
- [Required Privilege Level | 114](#)
- [Release Information | 114](#)

### Syntax

```
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    dhcpv6-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action (drop | log | none | shutdown);
        no-allowed-mac-log;
        persistent-learning;
        static-ipip-address {
            vlan vlan-name;
            mac mac-address;
        }
        static-ipv6ip-address {
```

```

        vlan vlan-name;
        mac mac-address;
    }
    voip-mac-exclusive;
    (dhcp-trusted | no-dhcp-trusted);
}
vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) [
        forwarding-class class-name;
    ]
    dhcp-option82 {
        circuit-id {
            prefix hostname;
            use-interface-description;
            use-vlan-id;
        }
        remote-id {
            prefix hostname | mac | none;
            use-interface-description;
            use-string string;
        }
        vendor-id <string>;
    }
    (examine-dhcp | no-examine-dhcp) {
        forwarding-class class-name;
    }
    (examine-dhcpv6 | no-examine-dhcpv6) {
        forwarding-class class-name;
    }
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
    no-option37;
}
}

```

## Hierarchy Level

```
[edit ethernet-switching-options]
```

## Description

Configure port security features, including MAC limiting, dynamic ARP inspection, whether interfaces can receive DHCP responses, DHCP snooping, IP source guard, DHCP option 82, MAC move limiting, and FIP snooping.

The remaining statements are explained separately. See [CLI Explorer](#).

## Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.0.

Support for IPv6 introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

## RELATED DOCUMENTATION

---

[Example: Configuring Port Security \(non-ELS\)](#)

---

[Example: Protecting Against Address Spoofing and Layer 2 DoS Attacks](#)

---

[Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN](#)

---

[Example: Setting Up DHCP Option 82 Using the Same VLAN](#)

---

[Example: Configuring an FCoE Transit Switch](#) | 22



## vlan (Access Port Security)

### IN THIS SECTION

- Syntax | 115
- Hierarchy Level | 116
- Description | 116
- Options | 117
- Required Privilege Level | 117
- Release Information | 117

### Syntax

```

vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection) {
        forwarding-class class-name;
    }
    dhcp-option82 {
        circuit-id {
            prefix hostname;
            use-interface-description;
            use-vlan-id;
        }
        remote-id {
            prefix hostname | mac | none;
            use-interface-description;
            use-string string;
        }
        vendor-id <string>;
    }
    (examine-dhcp | no-examine-dhcp) {
        forwarding-class class-name;
    }
    (examine-dhcpv6 | no-examine-dhcpv6) {
        forwarding-class class-name;
    }
    examine-fip {

```

```

        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    (ipv6-source-guard | no-ipv6-source-guard);
    mac-move-limit limit action (drop | log | none | shutdown);
    }
    (neighbor-discovery-inspection | no-neighbor-discovery-inspection);
    no-option37;
}

```

## Hierarchy Level

```
[edit ethernet-switching-options secure-access-port]
```

## Description

Apply any of the following security options to a VLAN:

- DHCP snooping
- DHCPv6 snooping with DHCP option 37
- DHCP option 82
- Dynamic ARP inspection (DAI)
- IPv6 neighbor discovery inspection
- FIP snooping
- IP source guard
- IPv6 source guard
- MAC move limiting

The remaining statements are explained separately. See [CLI Explorer](#).

**TIP:** To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type **?** after **vlan** or **vlangs** in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

## Options

**all**—Apply the feature to all VLANs.

*vlan-name*—Apply the feature to the specified VLAN.

## Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

## Release Information

Statement introduced in Junos OS Release 9.0.

Support for the **examine-dhcpv6**, **no-option37**, **neighbor-discovery-inspection**, and **ipv6-source-guard** statements introduced in Junos OS Release 14.1x53-D10 for EX Series switches.

## RELATED DOCUMENTATION

---

[Example: Configuring Port Security \(non-ELS\)](#)

---

[Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces](#)

---

[Example: Setting Up DHCP Option 82 Using the Same VLAN](#)

---

[Example: Configuring an FCoE Transit Switch](#) | 22

# 3

PART

## Administration

---

[Operational Commands](#) | 119

---

## CHAPTER 5

# Operational Commands

**IN THIS CHAPTER**

- [clear fip snooping enode | 119](#)
- [clear fip snooping statistics | 121](#)
- [clear fip snooping vlan | 123](#)
- [show dcbx neighbors | 124](#)
- [show fip snooping | 160](#)
- [show fip snooping enode | 167](#)
- [show fip snooping fcf | 173](#)
- [show fip snooping statistics | 177](#)
- [show fip snooping vlan | 183](#)

## clear fip snooping enode

**IN THIS SECTION**

- [Syntax | 120](#)
- [Syntax \(Junos Fusion\) | 120](#)
- [Description | 120](#)
- [Options | 120](#)
- [Required Privilege Level | 120](#)
- [Sample Output | 121](#)
- [Release Information | 121](#)

## Syntax

```
clear fip snooping enode enode-mac
<vlan vlan-name>
```

## Syntax (Junos Fusion)

```
clear fip snooping satellite enode enode-mac
<vlan vlan-name>
```

## Description

Clear FIP snooping information for the specified FCoE Node (ENode) or (optionally) only on a specified FCoE VLAN.

This operation deletes the ENode state from the switch database and from the FIP snooping firewall filters, which causes the ENode to lose its connection to the FCoE forwarder (FCF) and to log in to the FCF again.

The command syntax in a Junos Fusion environment includes the **satellite** keyword and clears FIP snooping Enode information on satellite device FCoE VLANs, which have FCoE and FIP functions and status information distributed between the aggregation devices and satellite devices. The command validates that a specified VLAN is a satellite FCoE VLAN, and displays an error message if the satellite syntax is not used for a satellite FCoE VLAN, or if the satellite syntax is used with a VLAN that is not a satellite FCoE VLAN.

## Options

|                       |                              |
|-----------------------|------------------------------|
| <i>enode-mac</i>      | MAC address of the ENode.    |
| vlan <i>vlan-name</i> | (Optional) Name of the VLAN. |

## Required Privilege Level

view

## Sample Output

**clear fip snooping enode enode-mac**

```
user@switch> clear fip snooping enode 00:10:94:00:00:02
```

## Release Information

Command introduced in Junos OS Release 10.4.

Command introduced with satellite keyword in Junos OS Release 17.4R1 for Junos Fusion Data Center.

## RELATED DOCUMENTATION

| *show fip snooping enode (or show fip snooping satellite enode)*

## clear fip snooping statistics

### IN THIS SECTION

- [Syntax | 121](#)
- [Syntax \(Junos Fusion\) | 122](#)
- [Description | 122](#)
- [Required Privilege Level | 122](#)
- [Sample Output | 122](#)
- [Release Information | 122](#)

## Syntax

**clear fip snooping statistics**

```
<vlan vlan-name>
```

## Syntax (Junos Fusion)

```
clear fip snooping satellite statistics  
<vlan vlan-name>
```

## Description

Clear FIP snooping statistics globally or on a specified VLAN.

The command syntax in a Junos Fusion environment includes the **satellite** keyword and clears FIP snooping information for satellite device FCoE VLANs, which have FCoE and FIP functions and status information distributed between the aggregation devices and satellite devices. The command validates that a specified VLAN is a satellite FCoE VLAN, and displays an error message if the satellite syntax is not used for a satellite FCoE VLAN, or if the satellite syntax is used with a VLAN that is not a satellite FCoE VLAN.

## Required Privilege Level

view

## Sample Output

**clear fip snooping statistics**

```
user@switch> clear fip snooping statistics
```

## Release Information

Command introduced in Junos OS Release 10.4.

Command introduced with satellite keyword in Junos OS Release 17.4R1 for Junos Fusion Data Center.

## RELATED DOCUMENTATION

| *show fip snooping statistics (or show fip snooping satellite statistics)*



## clear fip snooping vlan

### IN THIS SECTION

- [Syntax | 123](#)
- [Syntax \(Junos Fusion\) | 123](#)
- [Description | 123](#)
- [Options | 124](#)
- [Required Privilege Level | 124](#)
- [Sample Output | 124](#)
- [Release Information | 124](#)

### Syntax

```
clear fip snooping vlan vlan-name
```

### Syntax (Junos Fusion)

```
clear fip snooping satellite vlan vlan-name
```

### Description

Clear FIP snooping information for the specified FCoE VLAN.

This operation deletes all ENode and FCF information for the specified VLAN from the switch database and causes the ENodes to lose their connections to the FCFs. After clearing a VLAN, the switch relearns all of the FCFs and ENodes on the VLAN, and the ENodes must log in to the FCF again.

The command syntax in a Junos Fusion environment includes the **satellite** keyword to clear FIP snooping information for satellite device FCoE VLANs, which have FCoE and FIP functions distributed between the aggregation devices and satellite devices. The command validates that a specified VLAN is a satellite FCoE VLAN, and displays an error message if the satellite syntax is not used for a satellite FCoE VLAN, or if the satellite syntax is used with a VLAN that is not a satellite FCoE VLAN.

## Options

*vlan-name* Name of the VLAN.

## Required Privilege Level

view

## Sample Output

**clear fip snooping vlan vlan-name**

```
user@switch> clear fip snooping vlan fcoevlan1
```

## Release Information

Command introduced in Junos OS Release 10.4.

Command introduced with satellite keyword in Junos OS Release 17.4R1 for Junos Fusion Data Center.

## RELATED DOCUMENTATION

| *show fip snooping vlan (or show fip snooping satellite vlan)*

## show dcbx neighbors

### IN THIS SECTION

- [Syntax | 125](#)
- [Description | 125](#)
- [Options | 125](#)
- [Required Privilege Level | 125](#)
- [Output Fields | 125](#)

- [Sample Output | 147](#)
- [Release Information | 159](#)

### Syntax

```
show dcbx neighbors
<interface interface-name>
<terse>
```

### Description

Display information about Data Center Bridging Capability Exchange protocol (DCBX) neighbor interfaces.

### Options

<b>none</b>	Display information about all DCBX neighbor interfaces.
<b><i>interface-name</i></b>	(Optional) Display information for the specified interface.
<b>terse</b>	Display the specified level of output.

### Required Privilege Level

view

### Output Fields

[Table 4 on page 126](#) lists the output fields for the **show dcbx neighbors** command. Output fields are listed in the approximate order in which they appear.

Table 4: show dcbx neighbors Output Fields

Field Name	Field Description
<b>Interface</b>	Name of the interface.
<b>Parent Interface</b>	Name of the link aggregation group (LAG) interface to which the DCBX interface belongs.
<b>Active-application-map</b>	Name of the application map applied to the interface.
<b>Protocol-Mode</b>	<p>(QFX Series) DCBX protocol mode the interface uses:</p> <ul style="list-style-type: none"> <li>• IEEE DCBX Version—The interface uses IEEE DCBX mode.</li> <li>• DCBX Version 1.01—The interface uses DCBX version 1.01.</li> </ul> <p><b>NOTE:</b> On interfaces that use the IEEE DCBX mode, the <b>show dcbx neighbors interface <i>interface-name</i></b> operational command does not include application, PFC, or ETS operational state in the output.</p>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name		Field Description
<b>Protocol-State</b>		<p>(DCBX Version 1.01 only) DCBX protocol state synchronization status:</p> <ul style="list-style-type: none"> <li>• <b>in-sync</b>—The local interface received an acknowledge message from the peer to indicate that the peer received a state change message sent by the local interface.</li> <li>• <b>ack-pending</b>—The local interface has not yet received an acknowledge message from the peer to indicate that the peer received a state change message sent by the local interface.</li> </ul>
<b>Local-Advertisement</b>		<p>(DCBX Version 1.01 only)</p> <p>Status of advertisements that the local interface sends to the peer.</p>
	<b>Operational version</b>	Version of the DCBX standard used.
	<b>sequence-number</b>	<p>Number of state change messages sent to the peer.</p> <p>If the interface <b>Protocol-State</b> value is <b>in-sync</b>, this number should match the <b>acknowledge-id</b> number in the <b>Peer-Advertisement</b> section.</p> <p>If the interface <b>Protocol-State</b> value is <b>ack-pending</b>, this number does not match the <b>acknowledge-id</b> number in the <b>Peer-Advertisement</b> section.</p>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name		Field Description
	<b>acknowledge-id</b>	<p>Number of acknowledge messages received from the peer.</p> <p>If the <b>Protocol-State</b> value is <b>in-sync</b>, this number should match the <b>sequence-number</b> value in the <b>Peer-Advertisement</b> section.</p> <p>If the <b>Protocol-State</b> value is <b>ack-pending</b>, this number does not match the <b>sequence-number</b> value in the <b>Peer-Advertisement</b> section.</p>
<b>Peer-Advertisement</b>		<p>(DCBX Version 1.01 only)</p> <p>Status of advertisements that the peer sends to the local interface.</p>
	<b>Operational version</b>	Version of the DCBX standard used.
	<b>sequence-number</b>	<p>Number of state change messages the peer sent to the local interface.</p> <p>If this number matches the <b>acknowledge-id</b> number in the <b>Local-Advertisement</b> field, this indicates that the local interface has acknowledged all of the peer's state change messages and is synchronized.</p> <p>If this number does not match the <b>acknowledge-id</b> number in the <b>Local-Advertisement</b> field, this indicates that the peer has not yet received an acknowledgment for a state change message from the local interface.</p>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name		Field Description
	<b>acknowledge-id</b>	<p>Number of acknowledge messages the peer has received from the local interface.</p> <p>If this number matches the <b>sequence-number</b> value in the <b>Local-Advertisement</b> field, this indicates that the peer has acknowledged all of the local interface's state change messages and is in synchronization.</p> <p>If this number does not match the <b>sequence-number</b> value in the <b>Local-Advertisement</b> field, this indicates that the peer has not yet sent an acknowledgment for a state change message from the local interface.</p>
<b>Feature: PFC</b>		Priority-based flow control (PFC) feature DCBX state information.
	<b>Protocol-State</b>	<p>(DCBX Version 1.01 only)</p> <p>DCBX protocol state synchronization status:</p> <ul style="list-style-type: none"> <li>• <b>ack-pending</b>—The local interface has not yet received an acknowledge message from the peer to indicate that the peer received a PFC state change message sent by the local interface.</li> <li>• <b>in-sync</b>—The local interface received an acknowledge message from the peer to indicate that the peer received a PFC state change message sent by the local interface.</li> <li>• <b>not-applicable</b>—PFC autonegotiation is disabled.</li> </ul>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name		Field Description
	<b>Operational State</b>	(DCBX Version 1.01 only)  Operational state of the feature: <b>enabled</b> or <b>disabled</b> .
	<b>Local-Advertisement</b>	Status of advertisements that the local interface sends to the peer.
	<b>Enable</b>	(DCBX Version 1.01 only)  State that the local interface advertises to the peer: <ul style="list-style-type: none"> <li>• <b>Yes</b>—The feature is enabled.</li> <li>• <b>No</b>—The feature is disabled.</li> </ul>
	<b>Willing</b>	Willingness of the local interface to learn the PFC configuration from the peer using DCBX: <ul style="list-style-type: none"> <li>• <b>Yes</b>—The local interface is willing to learn the PFC configuration from the peer.</li> <li>• <b>No</b>—The local interface is not willing to learn the PFC configuration from the peer.</li> </ul>
	<b>Mac auth Bypass Capability</b>	(IEEE DCBX only)  (QFX Series) Media access controller (MAC) authentication bypass provides access to devices based on MAC address authentication. This is not supported, so the only value seen in the local advertisement field is <b>no</b> .



Table 4: show dcbx neighbors Output Fields (Continued)

Field Name		Field Description
	<b>Error</b>	(DCBX Version 1.01 only)  Configuration compatibility error status: <ul style="list-style-type: none"> <li>• <b>No</b>—No error detected. Local and peer configuration are compatible.</li> <li>• <b>Yes</b>—Error detected. Local and peer configuration are not compatible.</li> </ul>
	<b>Operational State</b>	PFC operational state on the interface: <ul style="list-style-type: none"> <li>• <b>Enabled</b>—PFC is enabled on the interface</li> <li>• <b>Disabled</b>—PFC is disabled on the interface</li> </ul>
	<b>Maximum Traffic Classes capable to support PFC</b>	Largest number of traffic classes the local interface supports for PFC: <ul style="list-style-type: none"> <li>• <b>6</b> (EX Series switches)</li> <li>• <b>6</b> (QFX Series)</li> </ul>
	<b>Code Point</b>	PFC code point, which is specified in the 3-bit class-of-service field in the VLAN header.
	<b>Admin Mode</b>	PFC administrative state for each code point on the local interface: <ul style="list-style-type: none"> <li>• <b>Enabled</b>—PFC is enabled for the code point.</li> <li>• <b>Disabled</b>—PFC is disabled for the code point.</li> </ul>

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name			Field Description
		<b>Operational Mode</b>	<p>(QFX Series) PFC operational mode for each code point:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>—PFC is enabled on the code point.</li> <li>• <b>Disable</b>—PFC is disabled on the code point.</li> </ul>
	<b>Peer-Advertisement</b>		Status of advertisements that the peer sends to the local interface.
		<b>Enable</b>	<p>(DCBX Version 1.01 only)</p> <p>State that the peer advertises to the local interface:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The feature is enabled.</li> <li>• <b>No</b>—The feature is disabled.</li> </ul>
		<b>Willing</b>	<p>Willingness of the peer to learn the PFC configuration from the local interface using DCBX:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The peer is willing to learn the PFC configuration from the local interface.</li> <li>• <b>No</b>—The peer is not willing to learn the PFC configuration from the local interface.</li> </ul>

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name			Field Description
		<b>Error</b>	<p>(DCBX Version 1.01 only)</p> <p>Configuration compatibility error status:</p> <ul style="list-style-type: none"> <li>• <b>No</b>—No error detected. Local and peer configuration are compatible.</li> <li>• <b>Yes</b>—Error detected. Local and peer configuration are not compatible.</li> </ul>
		<b>Operational State</b>	<p>PFC operational state on the interface:</p> <ul style="list-style-type: none"> <li>• Enabled—PFC is enabled on the interface</li> <li>• Disabled—PFC is disabled on the interface</li> </ul>
		<b>Mac auth Bypass Capability</b>	<p>(IEEE DCBX only)</p> <p>(QFX Series) Media access controller (MAC) authentication bypass provides access to devices based on MAC address authentication. Although the QFX Series does not support this feature, the connected peer might support it. This field reports the peer state:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The connected peer supports MAC authentication bypass.</li> <li>• <b>No</b>—The connected peer does not support MAC authentication bypass.</li> </ul>
		<b>Maximum Traffic Classes capable to support PFC</b>	<p>Largest number of traffic classes the peer supports for PFC:</p> <ul style="list-style-type: none"> <li>• 6 (EX Series switches)</li> <li>• 8 (QFX Series)</li> </ul>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name			Field Description
		<b>Code Point</b>	PFC code point, which is specified in the 3-bit class-of-service field in the VLAN header.
		<b>Admin Mode</b>	<p>PFC administrative state for each code point on the peer:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—PFC is enabled for the code point.</li> <li>• <b>Disabled</b>—PFC is disabled for the code point.</li> </ul>
<b>Feature: Application</b>			State information for the DCBX application.
	<b>Protocol-State</b>		<p>(DCBX Version 1.01 only)</p> <p>DCBX protocol state synchronization status:</p> <ul style="list-style-type: none"> <li>• <b>in-sync</b>—The local interface received an acknowledge message from the peer to indicate that the peer received an FCoE state change message sent by the local interface.</li> <li>• <b>ack-pending</b>—The local interface has not yet received an acknowledge message from the peer to indicate that the peer received an FCoE state change message sent by the local interface.</li> <li>• <b>not-applicable</b>—The local interface is set to <b>no-auto-negotiation</b> (autonegotiation is disabled). If the interface is associated with an FCoE forwarding class, the interface advertises FCoE capability even if the connected peer does not advertise FCoE capability.</li> </ul>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name		Field Description
	<b>Local-Advertisement</b>	<p>Status of advertisements that the local interface sends to the peer.</p> <p>If the local interface is set to <b>no-auto-negotiation</b> (autonegotiation is disabled), the local advertisement portion of the output is not shown.</p>
	<b>Enable</b>	<p>(DCBX Version 1.01 only)</p> <p>State that the local interface advertises to the peer:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The feature is enabled.</li> <li>• <b>No</b>—The feature is disabled.</li> </ul>
	<b>Willing</b>	<p>(DCBX Version 1.01 only)</p> <p>Willingness of the local interface to learn the FCoE interface state from the peer using DCBX:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The local interface is willing to learn the FCoE interface state from the peer.</li> <li>• <b>No</b>—The local interface is not willing to learn the FCoE interface state from the peer.</li> </ul>
	<b>Error</b>	<p>(DCBX Version 1.01 only)</p> <p>Configuration compatibility error status:</p> <ul style="list-style-type: none"> <li>• <b>No</b>—No error detected. The local and peer configuration are compatible.</li> <li>• <b>Yes</b>—Error detected. The local and peer configuration are not compatible.</li> </ul>

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name		Field Description
	<b>Appl-Name</b>	Name of the application:
	<b>Ethernet-Type</b>	(DCBX Version 1.01 only)  Ethernet type (EtherType) of the application. For example, <b>0x8906</b> indicates the EtherType for the FCoE application. Either the EtherType (for Layer 2 applications) or the Socket Number (for Layer 4 applications) of the application is displayed in the output.
	<b>Socket-Number</b>	Destination port socket number of the application, if applicable. Either the EtherType (for Layer 2 applications) or the Socket Number (for Layer 4 applications) of the application is displayed in the output.
	<b>Priority-Field or Priority-Map</b>	Priority assigned to the application.  For EX Series switches, the priority of the FCoE application is determined by the PFC congestion notification profile that has been configured and associated with the FCoE interface. For other applications, the priority is based on the application map.

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name			Field Description
		<b>Status</b>	<p>(DCBX Version 1.01 only)</p> <p>Local status when autonegotiation is enabled:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—The application feature is enabled on both the local interface and the peer interface. (The local configuration and the peer configuration match.)</li> <li>• <b>Disabled</b>—The local configuration and the peer configuration do not match.</li> </ul> <p><b>NOTE:</b> If there is a configuration mismatch in one application between the switch and the peer, all the other applications including FCoE are disabled.</p>
	<b>Peer-Advertisement</b>		Status of advertisements that the peer sends to the local interface.
		<b>Enable</b>	<p>(DCBX Version 1.01 only)</p> <p>State that the peer advertises to the local interface:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The feature is enabled.</li> <li>• <b>No</b>—The feature is disabled.</li> </ul>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name			Field Description
		<b>Willing</b>	<p>(DCBX Version 1.01 only)</p> <p>Willingness of the peer to learn the FCoE interface state from the local interface using DCBX:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The peer is willing to learn the FCoE interface state from the local interface.</li> <li>• <b>No</b>—The peer is not willing to learn the FCoE interface state from the local interface.</li> </ul>
		<b>Error</b>	<p>(DCBX Version 1.01 only)</p> <p>Configuration compatibility error status:</p> <ul style="list-style-type: none"> <li>• <b>No</b>—No error detected. Local and peer configuration are compatible.</li> <li>• <b>Yes</b>—Error detected. Local and peer configuration are not compatible.</li> </ul>
		<b>Appl-Name</b>	<p>Name of the application:</p> <ul style="list-style-type: none"> <li>• <b>FCoE</b>—Fibre Channel over Ethernet</li> </ul>
		<b>Ethernet-Type</b>	<p>Ethernet type (EtherType) of the application. For example, <b>0x8906</b> indicates the EtherType for the FCoE application. Either the EtherType (for Layer 2 applications) or the Socket-Number (for Layer 4 applications) of the application is displayed in the output.</p>



Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name		Field Description
	<b>Socket-Number</b>	Destination port socket number of the application, if applicable. Either the EtherType (for Layer 2 applications) or the Socket Number (for Layer 4 applications) of the application is displayed in the output.
	<b>Priority-Field or Priority-Map</b>	Priority assigned to the application.
	<b>Status</b>	(DCBX Version 1.01 only)  Peer interface status: <ul style="list-style-type: none"> <li>• <b>Enabled</b>—The application feature is enabled on both the local interface and the peer interface. (The local configuration and the peer configuration match.)</li> <li>• <b>Disabled</b>—The local configuration and the peer configuration do not match.</li> </ul>
<b>Feature: ETS</b>		Enhanced Transmission Selection (ETS) DCBX state information.

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name		Field Description
	<b>Protocol-State</b>	(DCBX Version 1.01 only)  ETS protocol state synchronization status: <ul style="list-style-type: none"> <li>• <b>in-sync</b>—The local interface received an acknowledge message from the peer to indicate that the peer received an ETS state change message sent by the local interface.</li> <li>• <b>ack-pending</b>—The local interface has not yet received an acknowledge message from the peer to indicate that the peer received an ETS state change message sent by the local interface.</li> </ul>
	<b>Operational State</b>	(DCBX Version 1.01 only)  Operational state of the feature, <b>enabled</b> or <b>disabled</b> .
	<b>Local-Advertisement</b>	Status of advertisements that the local interface sends to the peer.
	<b>Enable</b>	(DCBX Version 1.01 only)  State that the local interface advertises to the peer: <ul style="list-style-type: none"> <li>• <b>Yes</b>—The feature is enabled.</li> <li>• <b>No</b>—The feature is disabled.</li> </ul>

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name			Field Description
		<b>TLV Type</b>	<p>(IEEE DCBX only)</p> <p>Type of ETS TLV:</p> <ul style="list-style-type: none"> <li>• Configuration—Advertises the Configuration TLV, which communicates the local ETS configuration to the peer but does not ask the peer to use the configuration.</li> <li>• Recommendation—Advertises the Recommendation TLV, which communicates the local ETS configuration to the peer, and if the peer is “willing,” configures the peer interface to match the local ETS configuration.</li> <li>• Recommendation-or-Configuration—Advertises both TLVs.</li> </ul>
		<b>Willing</b>	<p>Willingness of the local interface to learn the ETS state from the peer using DCBX (EX Series switches always advertise <b>No</b> for this field):</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—Local interface is willing to learn the ETS state from the peer.</li> <li>• <b>No</b>—Local interface is not willing to learn the ETS state from the peer.</li> </ul>
		<b>Credit Based Shaper</b>	<p>(IEEE DCBX only)</p> <p>Alternative method of flow control to buffer-to-buffer credit. The QFX Series does not support a credit-based shaper, so the value of this field is always <b>No</b>.</p>

Table 4: show dcbx neighbors Output Fields (Continued)

Field Name			Field Description
		<b>Error</b>	(DCBX Version 1.01 only)  Configuration error status: <ul style="list-style-type: none"> <li>• <b>No</b>—No error. This should always be the switch ETS error state.</li> <li>• <b>Yes</b>—Error detected.</li> </ul>
		<b>Maximum Traffic Classes capable to support PFC</b>	(DCBX Version 1.01 only)  Largest number of traffic classes the local interface supports for PFC.
		<b>Maximum Traffic Classes supported</b>	(IEEE DCBX only)  Largest number of traffic classes the local interface supports for ETS. (EX Series switches support only one traffic class for ETS. However, a different value might be shown for this field.)
		<b>Code Point</b>	PFC code point, which is specified in the 3-bit class-of-service field in the VLAN header.
		<b>Priority-Group</b>	Class-of-service (CoS) priority group (forwarding class set) identification number.
		<b>Percentage B/W</b>	Configured minimum percentage of link bandwidth allocated to the priority group. Only explicitly configured values appear in this output column. If the link bandwidth is the default percentage, it is not shown. (EX Series switches allocate 100% of link bandwidth to the default priority group, group 7.)

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name			Field Description
		<b>Transmission Selection Algorithm</b>	<p>(IEEE DCBX only)</p> <p>The transmission selection algorithm used by the interface. The QFX Series supports ETS but does not support using the credit-based shaper algorithm, so the only value shown in this field is <b>ETS</b>.</p>
	<b>Peer-Advertisement</b>		Status of advertisements that the peer sends to the local interface.
		<b>Enable</b>	<p>(DCBX Version 1.01 only)</p> <p>State that the peer advertises to the local interface:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—The feature is enabled.</li> <li>• <b>No</b>—The feature is disabled.</li> </ul>

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name		Field Description
	<b>TLV Type</b>	<p>(IEEE DCBX only)</p> <p>Type of ETS TLV:</p> <ul style="list-style-type: none"> <li>• <b>Configuration</b>—Advertises the Configuration TLV, which communicates the local ETS configuration to the peer but does not ask the peer to use the configuration.</li> <li>• <b>Recommendation</b>—Advertises the Recommendation TLV, which communicates the local ETS configuration to the peer, and if the peer is “willing,” configures the peer interface to match the local ETS configuration.</li> <li>• <b>Configuration/Recommendation</b>—Advertises both TLVs.</li> </ul>
	<b>Willing</b>	<p>Willingness of the peer to learn the ETS state from the local interface using DCBX:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—Peer is willing to learn the ETS state from the local interface.</li> <li>• <b>No</b>—Peer is not willing to learn the ETS state from the local interface.</li> </ul>
	<b>Credit Based Shaper</b>	<p>(IEEE DCBX only)</p> <p>Alternative method of flow control to buffer-to-buffer credit. The QFX Series does not support a credit-based shaper, so the value of this field is always <b>No</b>.</p>

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name			Field Description
		<b>Error</b>	(DCBX Version 1.01 only)  Configuration error status of the peer: <ul style="list-style-type: none"> <li>• <b>No</b>—No error in peer ETS TLV.</li> <li>• <b>Yes</b>—Error in peer ETS TLV.</li> </ul>
		<b>Maximum Traffic Classes capable to support PFC</b>	(DCBX Version 1.01 only)  Largest number of traffic classes the local interface supports for PFC.
		<b>Maximum Traffic Classes supported</b>	(IEEE DCBX only)  Largest number of traffic classes the local interface supports for ETS. (EX Series switches support only one traffic class for ETS. However, a different value might be shown for this field.)
		<b>Code Point</b>	PFC code point, which is specified in the 3-bit class-of-service field in the VLAN header.
		<b>Priority-Group</b>	CoS priority group (forwarding class set) identification number.
		<b>Percentage B/W</b>	Configured minimum percentage of link bandwidth allocated to the priority group. (EX Series switches allocate 100% of link bandwidth to the default priority group, group 7.)

Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name			Field Description
		<b>Transmission Selection Algorithm</b>	<p>(IEEE DCBX only)</p> <p>Transmission selection algorithm used by the interface. The QFX Series supports ETS but does not support using the credit-based shaper algorithm, so the only value shown in this field is <b>ETS</b>.</p>
<b>PFC</b>			<p>(QFX Series, <b>terse</b> option only) DCBX TLV advertisement state for PFC:</p> <ul style="list-style-type: none"> <li>• Disabled—PFC configuration matches the configuration on the connected peer and PFC is disabled</li> <li>• Enabled—PFC configuration matches the configuration on the connected peer and PFC is enabled</li> <li>• Not Advt—Interface does not advertise PFC to the connected peer</li> </ul>
<b>ETS</b>			<p>(<b>terse</b> option only) Local DCBX TLV advertisement state for ETS:</p> <ul style="list-style-type: none"> <li>• Advt—Interface advertises ETS TLVs</li> <li>• Disabled—ETS is disabled on the interface (interface does not advertise ETS)</li> </ul>



Table 4: show dcbx neighbors Output Fields (*Continued*)

Field Name	Field Description
ETS Rec	<p>(<b>terse</b> option only) DCBX TLV peer advertisement state for ETS (state received from the connected DCBX peer):</p> <ul style="list-style-type: none"> <li>• Advt—Peer interface advertises ETS TLVs</li> <li>• Not Advt—Peer interface does not advertise ETS</li> </ul> <p><b>NOTE:</b> When the DCBX mode is DCBX version 1.01, no peer information is displayed.</p>
Version	<p>(<b>terse</b> option only) The DCBX version used on the interface and whether the DCBX version was autonegotiated or explicitly configured:</p> <ul style="list-style-type: none"> <li>• <b>IEEE</b>—The interface uses IEEE DCBX.</li> <li>• <b>1.01</b>—The interface uses DCBX version 1.01.</li> </ul> <p>When the DCBX version used is the result of autonegotiation, the term (<b>Auto</b>) appears next to the version. For example, <b>IEEE (Auto)</b> indicates that the interface autonegotiated with the connected peer to use IEEE DCBX. Autonegotiation is enabled by default.</p>

## Sample Output

### show dcbx neighbors interface (QFX Series, DCBX Version 1.01 Mode)

```

user@switch> show dcbx neighbors interface xe-0/0/0
Interface : xe-0/0/0.0 - Parent Interface: ae0.0
Active-application-map: app-map-1

```

Protocol-State: in-sync

Protocol-Mode: DCBX Version 1.01

Local-Advertisement:

Operational version: 1

sequence-number: 130, acknowledge-id: 102

Peer-Advertisement:

Operational version: 1

sequence-number: 102, acknowledge-id: 130

Feature: PFC, Protocol-State: in-sync

Operational State: Enabled

Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 8

Code Point	Admin Mode	Operational Mode
000	Disabled	Disable
001	Disabled	Disable
010	Disabled	Disable
011	Enabled	Enable
100	Enabled	Enable
101	Disabled	Disable
110	Disabled	Disable
111	Disabled	Disable

Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 8

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Enabled
100	Enabled
101	Disabled
110	Disabled
111	Disabled

Feature: Application, Protocol-State: in-sync

Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
FCoE	0x8906		00001110	Enabled
iSCSI		3260	10000000	Enabled

Peer-Advertisement:

Enable: Yes, Willing: Yes, Error: No

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
FCoE	0x8906	N/A	00001110	Enabled

Feature: ETS, Protocol-State: in-sync

Operational State: Enabled

Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 8

Code Point	Priority-Group
000	0
001	7
010	7
011	7
100	0
101	1
110	1
111	7

Priority-Group	Percentage B/W
0	40%
1	5%

Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 8

Code Point	Priority-Group
000	0

001	7
010	7
011	7
100	0
101	1
110	1
111	7
Priority-Group	Percentage B/W
0	40%
1	5%

### show dcbx neighbors interface (QFX Series, IEEE DCBX Mode)

```

user@switch> show dcbx neighbors interface xe-0/0/0
Interface : xe-0/0/0.0 - Parent Interface: ae0.0
  Active-application-map: app-map-1
  Protocol-Mode: IEEE-DCBX Version

  Feature: PFC

  Local-Advertisement:
    Willing: No
    Mac auth Bypass Capability: No
    Operational State: Enabled

  Maximum Traffic Classes capable to support PFC: 8

  Code Point      Admin Mode
    000           Disabled
    001           Disabled
    010           Disabled
    011           Enabled
    100           Enabled
    101           Disabled
    110           Disabled
    111           Disabled

  Peer-Advertisement:

```

Willing: No

Mac auth Bypass Capability: No

Operational State: Enabled

Maximum Traffic Classes capable to support PFC: 8

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Enabled
100	Enabled
101	Disabled
110	Disabled
111	Disabled

Feature: Application

Local-Advertisement:

Appl-Name	Ethernet-Type	Socket-Number	Priority-field
FCoE	0x8906		00001110
iSCSI		3260	10000000

Peer-Advertisement:

Appl-Name	Ethernet-Type	Socket-Number	Priority-field
FCoE	0x8906	N/A	00001110

Feature: ETS

Local-Advertisement:

TLV Type: Configuration/Recommendation

Willing: No

Credit Based Shaper: No

Maximum Traffic Classes supported: 3

Code Point	Priority-Group
000	0
001	7
010	7
011	7
100	0
101	1

110	1
111	7

Priority-Group	Percentage B/W
----------------	----------------

0	40%
---	-----

1	5%
---	----

Priority-Group	Transmission Selection Algorithm
----------------	----------------------------------

0	Enhanced Transmission Selection
---	---------------------------------

1	Enhanced Transmission Selection
---	---------------------------------

Peer-Advertisement:

TLV Type: Configuration

Willing: No

Credit Based Shaper: No

Code Point	Priority-Group
------------	----------------

000	0
-----	---

001	7
-----	---

010	7
-----	---

011	7
-----	---

100	0
-----	---

101	1
-----	---

110	1
-----	---

111	7
-----	---

Priority-Group	Percentage B/W
----------------	----------------

0	40%
---	-----

1	5%
---	----

Priority-Group	Transmission Selection Algorithm
----------------	----------------------------------

0	Enhanced Transmission Selection
---	---------------------------------

1	Enhanced Transmission Selection
---	---------------------------------

Peer-Advertisement:

TLV Type: Recommendation

Code Point	Priority-Group
------------	----------------

000	0
-----	---

001	7
-----	---

010	7
-----	---

011	7
-----	---

```

100          0
101          1
110          1
111          7

Priority-Group    Percentage B/W
0                 40%
1                 5%

Priority-Group    Transmission Selection Algorithm
0                 Enhanced Transmission Selection
1                 Enhanced Transmission Selection

```

### show dcbx neighbors terse (QFX Series)

```

user@switch> show dcbx neighbors terse
Interface  Parent      PFC      ETS      ETS      Version
           Interface
xe-0/0/8.0  -           Enabled  Advt     Advt     IEEE (Auto)
xe-0/0/9.0  -           Disabled Disabled
xe-0/0/11.0 ae0.0       Enabled  Advt     Advt     IEEE (Auto)
xe-0/0/12.0 ae0.0       Enabled  Advt     Advt     IEEE (Auto)
xe-0/0/32.0 -           Enabled  Advt     Not Advt IEEE
xe-0/0/36.0 -           Not Advt Advt     Advt     IEEE

```

### show dcbx neighbors (EX4500 Switch: FCoE Interfaces on Both Local and Peer with PFC Configured Compatibly)

```

user@switch> show dcbx neighbors interface xe-0/0/14

Interface : xe-0/0/14.0 - Parent Interface: ae0.0
Protocol-State: in-sync

Local-Advertisement:
  Operational version: 0
  sequence-number: 6, acknowledge-id: 6

```

## Peer-Advertisement:

Operational version: 0

sequence-number: 6, acknowledge-id: 6

Feature: PFC, Protocol-State: in-sync

Operational State: Enabled

## Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 6

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Enabled
100	Disabled
101	Disabled
110	Disabled
111	Disabled

## Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 6

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Enabled
100	Disabled
101	Disabled
110	Disabled
111	Disabled

Feature: Application, Protocol-State: in-sync



```

Local-Advertisement:
  Enable: Yes, Willing: No, Error: No   <<< Error bit will not be set as
there is no miss configuration between local and peer.

```

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
FCoE	0x8906		00001000	Enabled

```

Peer-Advertisement:
  Enable: Yes, Willing: No, Error: No

```

Status	Appl-Name	Ethernet-Type	Socket-Number	Priority-Map
Enabled	FCoE	0x8906		00001000

### show dcbx neighbors (EX4500 Switch: DCBX Interfaces on Local and Peer Are Configured Compatibly with iSCSI Application)

```

user@switch> show dcbx neighbors interface xe-0/0/14

```

```

Interface : xe-0/0/14.0 - Parent Interface: ae0.0

```

```

Protocol-State: in-sync

```

```

Active-application-map: iscsi-map

```

```

Local-Advertisement:
  Operational version: 0
  sequence-number: 9, acknowledge-id: 12

```

```

Peer-Advertisement:
  Operational version: 0
  sequence-number: 12, acknowledge-id: 9

```

```

Feature: PFC, Protocol-State: in-sync

```

Operational State: Enabled

Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 6

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Enabled
100	Disabled
101	Disabled
110	Disabled
111	Disabled

Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes capable to support PFC: 6

Code Point	Admin Mode
000	Disabled
001	Disabled
010	Disabled
011	Enabled
100	Disabled
101	Disabled
110	Disabled
111	Disabled

Feature: Application, Protocol-State: in-sync

Local-Advertisement:

Enable: Yes, Willing: No, Error: No

	Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
	FCoE	0x8906		00001000	
Enabled					
	iscsi		3260	00100000	
Enabled					

Peer-Advertisement:

Enable: Yes, Willing: No, Error: No

	Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
	FCoE	0x8906		00001000	
Enabled					
	iscsi		3260	00100000	
Enabled					

### show dcbx neighbors (EX4500 Switch: Includes ETS)

```
user@switch> show dcbx neighbors interface xe-0/0/3
```

```
Interface : xe-0/0/3.0
```

```
Protocol-State: in-sync
```

```
Active-application-map: map_iscsi
```

```
Local-Advertisement:
```

```
Operational version: 0
```

```
sequence-number: 1, acknowledge-id: 5
```

```
Peer-Advertisement:
```

```
Operational version: 0
```

```
sequence-number: 5, acknowledge-id: 1
```

```
Feature: PFC, Protocol-State: in-sync
```

```
Operational State: Enabled
```

```
Local-Advertisement:
```

```
Enable: Yes, Willing: No, Error: No
```

```
Maximum Traffic Classes capable to support PFC: 6
```

Code Point	Admin Mode
000	Enabled
001	Enabled
010	Disabled
011	Disabled
100	Disabled
101	Disabled
110	Disabled
111	Disabled

## Peer-Advertisement:

Enable: Yes, Willing: Yes, Error: No

Maximum Traffic Classes capable to support PFC: 8

Code Point	Admin Mode
000	Enabled
001	Disabled
010	Disabled
011	Disabled
100	Enabled
101	Disabled
110	Disabled
111	Disabled

Feature: Application, Protocol-State: in-sync

## Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
FCoE	0x8906		00000001	Enabled
iscsi		3260	00000010	Enabled

## Peer-Advertisement:

Enable: Yes, Willing: Yes, Error: No

Appl-Name	Ethernet-Type	Socket-Number	Priority-Map	Status
FCoE	0x8906		00001000	Enabled
iscsi		3260	00010000	Enabled

Feature: ETS, Protocol-State: in-sync

Operational State: Enabled

## Local-Advertisement:

Enable: Yes, Willing: No, Error: No

Maximum Traffic Classes supported : 3

Code Point	Priority-Group
000	7
001	7
010	7

011	7
100	7
101	7
110	7
111	7

Priority-Group	Percentage B/W
7	100%

Peer-Advertisement:

Enable: Yes, Willing: Yes, Error: No  
Maximum Traffic Classes supported : 8

Code Point	Priority-Group
000	0
001	1
010	0
011	0
100	2
101	0
110	0
111	0

Priority-Group	Percentage B/W
0	30%
1	40%
2	30%

## Release Information

Command introduced in Junos OS Release 11.1.

## RELATED DOCUMENTATION

*Configuring DCBX Autonegotiation*

*Example: Configuring DCBX Application Protocol TLV Exchange*

[Example: Configuring an FCoE Transit Switch](#)

[Example: Configuring DCBX to Support an iSCSI Application](#)

# show fip snooping

## IN THIS SECTION

- [Syntax | 160](#)
- [Description | 160](#)
- [Options | 160](#)
- [Required Privilege Level | 161](#)
- [Output Fields | 161](#)
- [Sample Output | 164](#)
- [Release Information | 167](#)

## Syntax

```
show fip snooping  
<brief | detail>
```

## Description

Display FIP snooping information.

## Options

- |                       |                                                   |
|-----------------------|---------------------------------------------------|
| <b>none</b>           | Display FIP snooping information.                 |
| <b>brief   detail</b> | (Optional) Display the specified level of output. |

## Required Privilege Level

view

## Output Fields

Table 5 on page 161 lists the output fields for the **show fip snooping** command. Output fields are listed in the approximate order in which they appear.

**Table 5: show fip snooping Output Fields**

Field Name	Field Description	Level of Output
<b>VLAN</b>	Name of the VLAN.	All
<b>Mode</b>	(QFX Series only)  Snooping mode enabled on the FCoE VLAN: <ul style="list-style-type: none"> <li>• VN2VF Snooping—The FCoE VLAN is configured for FIP snooping between an ENode VN_Port and a switch VF_Port.</li> <li>• VN2VN Snooping—The FCoE VLAN is configured for VN_Port to VN_Port FIP snooping between ENode VN_Ports.</li> </ul>	All
<b>FC-MAP</b>	FCoE mapped address prefix of the FCoE forwarder for the VLAN.	All
<b>FCF or FCF-MAC</b>	MAC address of the FCF.	All
<b>Session Count or Active Sessions</b>	Current number of virtual link sessions with VN_Ports.	All

Table 5: show fip snooping Output Fields *(Continued)*

Field Name	Field Description	Level of Output
<b>VN_Port Count</b>	(QFX Series only)  Number of VN_Ports active on an ENode.	<b>brief</b>
<b>Configured FKA-ADV</b>	FIP keepalive interval in seconds configured on the FCF multiplied by three. For example, if the FKA_ADV period configured on the FCF is 86 seconds, the value of this field is 258.  For the QFX Series only, the output of this field is always 0 (zero) if the VLAN is an FCoE-FC gateway VLAN. If the VLAN is a FIP snooping VLAN (a transit switch VLAN), then the output is accurate. This is because for an FCoE-FC gateway VLAN, FIP snooping is performed internally and the keepalive advertisements are not tracked by the switch's Ethernet module.	<b>detail</b>
<b>Running FKA-ADV</b>	Runtime interval in seconds of the last FIP keepalive advertisement the FCF received. This value changes every time the FCF receives an FKA_ADV.  For the QFX Series only, the output of this field is always 0 (zero) if the VLAN is an FCoE-FC gateway VLAN. If the VLAN is a FIP snooping VLAN (a transit switch VLAN), then the output is accurate. This is because for an FCoE-FC gateway VLAN, FIP snooping is performed internally and the keepalive advertisements are not tracked by the switch's Ethernet module.	<b>detail</b>
<b>Beacon Period</b>	(QFX Series only)  Beacon period interval in milliseconds.	<b>detail</b>



Table 5: show fip snooping Output Fields (*Continued*)

Field Name	Field Description	Level of Output
<b>VN2VN Mode</b>	<p>(QFX Series only)</p> <p>Mode of VN2VN_Port snooping:</p> <ul style="list-style-type: none"> <li>• Multi-Point—Multiple ENodes are connected to the network and form multiple virtual links. Each virtual link is created between one pair of VN_Ports. This is analogous to the loop mode in traditional FC networks.</li> <li>• Point-to-Point—Two ENodes are connected to the network and form a single VN_Port to VN_Port virtual link. This is analogous to the point-to-point FC link between an FC initiator and an FC target.</li> </ul>	<b>detail</b>
<b>ENode-MAC</b>	MAC address of the connected FCoE node (ENode).	All
<b>Interface</b>	<p>Interface connected to the ENode.</p> <p>(QFabric System or Junos Fusion <b>satellite</b> command output only)</p> <p>When an FCoE LAG has been configured, this field displays both the LAG interface and the LAG member interface connected to the ENode.</p>	<b>detail</b>
<b>VN-Port MAC</b>	MAC address of a VN_Port on the ENode.	All
<b>FKA-ADV</b>	Runtime interval in seconds of the last FIP keepalive advertisement the ENode sent to the FCF on behalf of the VN_Port (VN_Port FKA_ADV). This value changes every time the ENode sends a VN_Port FKA_ADV to the FCF.	<b>detail</b>

Table 5: show fip snooping Output Fields *(Continued)*

Field Name	Field Description	Level of Output
<b>Active VN_Ports</b>	(QFX Series only)  Number of VN_Ports active on an ENode.	<b>detail</b>
<b>Vlink far-end VN-Port-MAC</b>	(QFX Series only)  Media access control (MAC) address of the VN_Port at the other end of the virtual link.	<b>detail</b>

## Sample Output

### show fip snooping

```
user@switch> show fip snooping
VLAN : fcoevlan1      FC-MAP : 0e:fc:00
FCF : 00:10:94:00:00:01  Session Count : 2
Enode-MAC : 00:10:94:00:00:02
VN-Port-MAC : 0E:FC:00:01:00:05
VN-Port-MAC : 0E:FC:00:01:00:01
```

### show fip snooping brief (QFX Series)

```
user@switch> show fip snooping brief
VLAN: vlan100,      Mode: VN2VF Snooping
FC-MAP: 0e:fc:00
FCF: 30:10:94:01:00:00  Session Count: 2
Enode-MAC: 10:10:94:01:00:01
VN-Port-MAC: 0e:fc:00:01:0d:01
VN-Port-MAC: 0e:fc:00:01:0e:01
VLAN: vlan101,      Mode: VN2VN Snooping
FC-MAP: 0e:fc:00
Enode-MAC: 10:10:94:01:00:02 VN_Port count: 1
```

```

VN-Port-MAC: 0e:fc:00:01:0a:01  Session Count: 2
Enode-MAC: 10:10:94:01:00:03 VN_Port count: 0

```

### show fip snooping detail (QFX Series Switches)

```

user@switch> show fip snooping detail
root@sw-pa02v> show fip snooping detail
VLAN: vlan100,  Mode: VN2VF Snooping
  FC-MAP: 0e:fc:00
  FCF Information
    FCF-MAC          : 30:10:94:01:00:00
    Active Sessions  : 2
    Configured FKA-ADV : 258
    Running FKA-ADV   : 188
    Enode Information
      Enode-MAC: 10:10:94:01:00:01,      Interface: xe-0/0/10
      Configured FKA-ADV : 258
      Running FKA-ADV    : 230
      Session Information
        VN-Port MAC: 0e:fc:00:01:0d:01,  FKA-ADV : 230
        VN-Port MAC: 0e:fc:00:01:0e:01,  FKA-ADV : 245

VLAN: vlan101,  Mode: VN2VN Snooping
  FC-MAP: 0e:fd:00
  Beacon_Period: 90000
  VN2VN Mode: Multi-Point
  Enode Information
    Enode-MAC: 10:10:94:01:00:02,      Interface: xe-0/0/10
    Active VN_Ports : 1
    VN_Port Information
      VN-Port MAC: 0e:fd:00:01:0a:01
      Active Sessions : 2
      Session Information
        Vlink far-end VN-Port-MAC: 0e:fd:00:01:0b:01
        Vlink far-end VN-Port-MAC: 0e:fd:00:01:0c:01
    Enode-MAC: 10:10:94:01:00:02,      Interface: xe-0/0/11
    Active VN_Ports : 0

```

## show fip snooping detail (QFabric System FCoE with LAG Configured)

```
admin@qfabric> show fip snooping detail
VLAN: vlan_100, Mode: VN2VF Snooping
FC-MAP: 0e:fc:00
  FCF Information
    FCF-MAC          : 84:18:88:d1:f5:cc
    Active Sessions   : 2
    Configured FKA-ADV : 8000
    Running FKA-ADV    : 23962
  Enode Information
    Enode-MAC: 00:c0:dd:14:ae:6d,      Interface: P4546-C:ae0 P4546-C:xe-0/0/39
    Configured FKA-ADV : 8000
    Running FKA-ADV    : 16622
  Session Information
    VN-Port MAC: 0e:fc:00:6c:06:a5,    FKA-ADV : 246303
  Enode Information
    Enode-MAC: 00:c0:dd:14:ae:6f,      Interface: P4546-C:ae0 P4546-C:xe-0/0/38
    Configured FKA-ADV : 8000
    Running FKA-ADV    : 16512
  Session Information
    VN-Port MAC: 0e:fc:00:6c:06:a4,    FKA-ADV : 238150
```

## show fip snooping detail (EX Series Switches)

```
user@switch> show fip snooping detail
VLAN : fcoevlan1    FC-MAP : 0e:fc:00
  FCF Information
    FCF-MAC          : 00:10:94:00:00:01
    Active Sessions   : 2
    Configured FKA-ADV : 258
    Running FKA-ADV    : 244
  Enode Information
    Enode-MAC : 00:10:94:00:00:02      Interface : xe-0/0/1
    Configured FKA-ADV : 258
    Running FKA-ADV    : 248
  Session Information
    VN-Port MAC : 0E:FC:00:01:00:05    FKA-ADV : 264
    VN-Port MAC : 0E:FC:00:01:00:01    FKA-ADV : 260
```

## Release Information

Command introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

*Configuring an FCoE LAG*

*Example: Configuring an FCoE LAG on a Redundant Server Node Group*

*show fip snooping enode*

*show fip snooping fcf*

*show fip snooping statistics*

*show fip snooping vlan*

*show fip snooping interface*

## show fip snooping enode

### IN THIS SECTION

- [Syntax | 168](#)
- [Description | 168](#)
- [Options | 168](#)
- [Required Privilege Level | 168](#)
- [Output Fields | 168](#)
- [Sample Output | 172](#)
- [Release Information | 173](#)

Syntax

```
show fip snooping enode enode-mac
<brief | detail>
<vlan vlan-name>
```

Description

Display FIP snooping FCoE node (ENode) information.

Options

- brief | detail** (Optional) Display the specified level of output.
- enode-mac*** Display information for the ENode specified by the MAC address.
- vlan *vlan-name*** (Optional) Display FIP snooping information for the ENode on only the specified VLAN.

Required Privilege Level

view

Output Fields

Table 6 on page 168 lists the output fields for the **show fip snooping enode** command. Output fields are listed in the approximate order in which they appear.

Table 6: show fip snooping enode Output Fields

Field Name	Field Description	Level of Output
ENode and ENode MAC	MAC address of the ENode.	All
VLAN	Name of the VLAN.	All

Table 6: show fip snooping enode Output Fields *(Continued)*

Field Name	Field Description	Level of Output
<b>Interface</b>	Interface connected to the ENode.	All
<b>Mode</b>	(QFX Series only)  Snooping mode enabled on the FCoE VLAN: <ul style="list-style-type: none"> <li>• VN2VF Snooping—The FCoE VLAN is configured for FIP snooping between an ENode VN_Port and a switch VF_Port.</li> <li>• VN2VN Snooping—The FCoE VLAN is configured for VN_Port to VN_Port FIP snooping between ENode VN_Ports.</li> </ul>	All
<b>VN_Port Count</b>	(QFX Series only)  Number of VN_Ports active on an ENode.	<b>brief</b>
<b>Session Count</b>	Current number of virtual link sessions with VN_Ports.	All

Table 6: show fip snooping enode Output Fields *(Continued)*

Field Name	Field Description	Level of Output
<b>Configured FKA-ADV</b>	<p>FIP keepalive interval in seconds configured on the FCoE forwarder (FCF) multiplied by three. For example, if the FKA_ADV period configured on the FCF is 86 seconds, the value of this field is 258. This value remains constant.</p> <p>For the QFX Series only, the output of this field is always 0 (zero) if the VLAN is an FCoE-FC gateway VLAN. If the VLAN is a FIP snooping VLAN (a transit switch VLAN), then the output is accurate. This is because for an FCoE-FC gateway VLAN, FIP snooping is performed internally and the keepalive advertisements are not tracked by the switch's Ethernet module.</p>	<b>detail</b>
<b>Running FKA-ADV</b>	<p>Runtime interval in seconds of the last FIP keepalive advertisement the ENode sent to the FCF. This value changes every time the ENode sends an FKA_ADV to the FCF.</p> <p>For the QFX Series only, the output of this field is always 0 (zero) if the VLAN is an FCoE-FC gateway VLAN. If the VLAN is a FIP snooping VLAN (a transit switch VLAN), then the output is accurate. This is because for an FCoE-FC gateway VLAN, FIP snooping is performed internally and the keepalive advertisements are not tracked by the switch's Ethernet module.</p>	<b>detail</b>
<b>VN-Port or VN-Port-MAC</b>	MAC address of a VN_Port on the ENode.	All



Table 6: show fip snooping enode Output Fields (*Continued*)

Field Name	Field Description	Level of Output
<b>FKA-ADV</b>	Runtime interval in seconds of the last FIP keepalive advertisement the ENode sent to the FCF on behalf of the VN_Port (VN_Port FKA_ADV). This value changes every time the ENode sends a VN_Port FKA_ADV to the FCF.	<b>detail</b>
<b>FCF or FCF-MAC</b>	MAC address of the FCF to which the VN_Port is connected.	All
<b>Beacon Period</b>	(QFX Series only)  Beacon period interval in milliseconds.	<b>detail</b>
<b>VN2VN Mode</b>	(QFX Series only)  Mode of VN2VN_Port snooping: <ul style="list-style-type: none"> <li>• Multi-Point—Multiple ENodes are connected to the network and form multiple virtual links. Each virtual link is created between one pair of VN_Ports. This is analogous to the loop mode in traditional FC networks.</li> <li>• Point-to-Point—Two ENodes are connected to the network and form a single VN_Port to VN_Port virtual link. This is analogous to the point-to-point FC link between an FC initiator and an FC target.</li> </ul>	<b>detail</b>
<b>Vlink far-end VN-Port-MAC</b>	(QFX Series only)  Media access control (MAC) address of the VN_Port at the other end of the virtual link.	<b>detail</b>

## Sample Output

### show fip snooping enode

```
user@switch> show fip snooping enode 00:10:94:00:00:02
Enode : 00:10:94:00:00:02   VLAN : vlan1   Interface : xe-0/0/1
      VN-Port-MAC          FCF-MAC
      0E:FC:00:00:00:05    00:10:94:00:00:01
      0E:FC:00:00:00:01    00:10:94:00:00:01
```

### show fip snooping enode brief (QFX Series)

```
user@switch> show fip snooping enode 10:10:94:01:00:02 brief
Enode: 10:10:94:01:00:02 ,   VLAN: vlan101,   Interface: xe-0/0/10
  Mode: VN2VF Snooping      VN_Port Count: 1
    VN_Port Information
      VN_Port Mac: 0e:fc:00:01:0a:01      Session Count: 2
```

### show fip snooping enode detail (QFX Series)

```
user@switch> show fip snooping enode 10:10:94:01:00:02 detail
Enode MAC: 10:10:94:01:00:02,   VLAN: vlan101,   Interface: xe-0/0/10
  Mode: VN2VF Snooping      VN_Port Count: 1
  Beacon_Period: 90000      VN2VN Mode: Multi-Point
    VN_Port Information
      VN_Port Mac: 0e:fc:00:01:0a:01      Session Count: 2
      Vlink far-end VN-Port-MAC: 0e:fc:00:01:0b:01
      Vlink far-end VN-Port-MAC: 0e:fc:00:01:0c:01
```

### show fip snooping enode detail

```
user@switch> show fip snooping enode 00:10:94:00:00:02 detail
Enode MAC : 00:10:94:00:00:02   VLAN : vlan1   Interface : xe-0/0/1
Configured FKA-ADV : 258      Running FKA-ADV : 213
  Session Information
```

```
VN-Port : 0E:FC:00:00:00:05   FKA-ADV : 229   FCF : 00:10:94:00:00:01
VN-Port : 0E:FC:00:00:00:01   FKA-ADV : 225   FCF : 00:10:94:00:00:01
```

### Release Information

Command introduced in Junos OS Release 10.4.

### RELATED DOCUMENTATION

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

[Example: Configuring an FCoE Transit Switch](#)

*show fip snooping*

*show fip snooping fcf*

*show fip snooping statistics*

*show fip snooping vlan*

*show fip snooping interface*

## show fip snooping fcf

### IN THIS SECTION

- [Syntax | 174](#)
- [Description | 174](#)
- [Options | 174](#)
- [Required Privilege Level | 174](#)
- [Output Fields | 174](#)
- [Sample Output | 176](#)
- [Release Information | 177](#)

Syntax

```
show fip snooping fcf fcf-mac
<brief | detail>
<vlan vlan-name>
```

Description

Display FIP snooping FCoE forwarder (FCF) information.

Options

- brief | detail** (Optional) Display the specified level of output.
- fcf-mac*** Display information for the FCF specified by the MAC address.
- vlan-name*** (Optional) Display FIP snooping information for the FCF on only the specified VLAN.

Required Privilege Level

view

Output Fields

[Table 7 on page 174](#) lists the output fields for the **show fip snooping fcf** command. Output fields are listed in the approximate order in which they appear.

Table 7: show fip snooping fcf Output Fields

Field Name	Field Description	Level of Output
FCF or FCF-MAC	MAC address of the FCoE forwarder.	All
VLAN	Name of the VLAN.	All

Table 7: show fip snooping fcf Output Fields (*Continued*)

Field Name		Field Description	Level of Output
<b>Session Count</b>		Current number of virtual link sessions with VN_Ports.	None
<b>Configured FKA-ADV</b>		FIP keepalive interval in seconds configured on the FCF multiplied by three. For example, if the FKA_ADV period configured on the FCF is 86 seconds, the value of this field is 258.	<b>detail</b>
<b>Running FKA-ADV</b>		Runtime interval in seconds of the last FIP keepalive advertisement the FCF received. This value changes every time the FCF receives an FKA_ADV.	<b>detail</b>
<b>ENode-MAC</b>		MAC address of the connected ENode.	All
	• <b>Interface</b>	Interface connected to the ENode.	<b>detail</b>
	• <b>Configured FKA-ADV</b>	FIP keepalive interval in seconds configured on the FCF multiplied by three. For example, if the FKA_ADV period configured on the FCF is 86 seconds, the value of this field is 258. This value remains constant.	<b>detail</b>
	• <b>Running FKA-ADV</b>	Runtime interval in seconds of the last FIP keepalive advertisement the ENode sent to the FCF. This value changes every time the ENode sends an FKA_ADV to the FCF.	<b>detail</b>
	• <b>VN-Port MAC</b>	MAC address of a VN_Port on the ENode.	All

**Table 7: show fip snooping fcf Output Fields (Continued)**

Field Name	Field Description	Level of Output
<ul style="list-style-type: none"> <li><b>FKA-ADV</b></li> </ul>	Runtime interval in seconds of the last FIP keepalive advertisement the ENode sent to the FCF on behalf of the VN_Port (VN_Port FKA_ADV). This value changes every time the ENode sends a VN_Port FKA_ADV to the FCF.	<b>detail</b>

## Sample Output

### show fip snooping fcf

```

user@switch> show fip snooping fcf 00:10:94:00:00:01
FCF : 00:10:94:00:00:01   VLAN : vlan1   Session Count : 2
Enode-MAC : 00:10:94:00:00:02
VN-Port-MAC : 0E:FC:00:00:00:05
VN-Port-MAC : 0E:FC:00:00:00:01

```

### show fip snooping fcf detail

```

user@switch> show fip snooping fcf 00:10:94:00:00:01 detail
FCF-MAC : 00:10:94:00:00:01   VLAN : vlan1
Configured FKA-ADV : 258       Running FKA-ADV : 222
Enode Information
Enode-MAC : 00:10:94:00:00:02 Interface: xe-0/0/1
Configured FKA-ADV : 258
Running FKA-ADV      : 226
Session Information
VN-Port MAC : 0E:FC:00:00:00:05   FKA-ADV : 242
VN-Port MAC : 0E:FC:00:00:00:01   FKA-ADV : 238

```

## Release Information

Command introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

[Example: Configuring an FCoE Transit Switch](#)

*show fip snooping*

*show fip snooping enode*

*show fip snooping statistics*

*show fip snooping vlan*

*show fip snooping interface*

## show fip snooping statistics

### IN THIS SECTION

- [Syntax | 177](#)
- [Syntax \(Junos Fusion\) | 178](#)
- [Description | 178](#)
- [Options | 178](#)
- [Required Privilege Level | 178](#)
- [Output Fields | 178](#)
- [Sample Output | 181](#)
- [Release Information | 182](#)

## Syntax

```
show fip snooping statistics
```

```
<vlan vlan-name>
```

Syntax (Junos Fusion)

```
show fip snooping satellite statistics
<vlan  vlan-name>
```

Description

Display FIP snooping statistics.

The command syntax in a Junos Fusion environment includes the **satellite** keyword and displays FIP snooping statistics for satellite device FCoE VLANs, which have FCoE and FIP functions and status information distributed between the aggregation devices and satellite devices. The command validates that a specified VLAN is a satellite FCoE VLAN, and displays an error message if the satellite syntax is not used for a satellite FCoE VLAN, or if the satellite syntax is used with a VLAN that is not a satellite FCoE VLAN.

Options

**vlan *vlan-name*** (Optional) Display FIP snooping statistics for the specified VLAN.

Required Privilege Level

view

Output Fields

[Table 8 on page 178](#) lists the output fields for the **show fip snooping statistics** command. Output fields are listed in the approximate order in which they appear.

Table 8: show fip snooping statistics Output Fields

Field Name	Field Description
VLAN	Name of the VLAN for which a set of statistics is displayed.



Table 8: show fip snooping statistics Output Fields *(Continued)*

Field Name	Field Description
<b>Mode</b>	<p>(QFX Series only)</p> <p>Snooping mode enabled on the FCoE VLAN:</p> <ul style="list-style-type: none"> <li>• VN2VF Snooping—The FCoE VLAN is configured for FIP snooping between an ENode VN_Port and a switch VF_Port.</li> <li>• VN2VN Snooping—The FCoE VLAN is configured for VN_Port to VN_Port FIP snooping between ENode VN_Ports.</li> </ul>
<b>Number of MDS</b>	Number of multicast discovery solicitation messages sent on the VLAN.
<b>Number of UDS</b>	Number of unicast discovery solicitation messages sent on the VLAN.
<b>Number of FLOGI</b>	Number of fabric logins on the VLAN.
<b>Number of FDISC</b>	Number of fabric discovery logins on the VLAN.
<b>Number of LOGO</b>	Number of fabric logouts on the VLAN.
<b>Number of ENode-keep-alive</b>	Number of ENode keepalive messages sent on the VLAN.
<b>Number of VNPort-keep-alive</b>	Number of VN_Port keepalive messages sent on the VLAN.
<b>Number of MDA</b>	Number of multicast discovery advertisement messages sent on the VLAN.
<b>Number of UDA</b>	Number of unicast discovery advertisement messages sent on the VLAN.

Table 8: show fip snooping statistics Output Fields *(Continued)*

Field Name	Field Description
<b>Number of FLOGI_ACC</b>	Number of fabric logins accepted on the VLAN.
<b>Number of FLOGI_RJT</b>	Number of fabric logins rejected on the VLAN.
<b>Number of FDISC_ACC</b>	Number of fabric discoveries accepted on the VLAN.
<b>Number of FDISC_RJT</b>	Number of fabric discoveries rejected on the VLAN.
<b>Number of LOGO_ACC</b>	Number of fabric logouts accepted on the VLAN.
<b>Number of LOGO_RJT</b>	Number of fabric logouts rejected on the VLAN.
<b>Number of CVL</b>	Number of clear virtual links (CVL) actions on the VLAN.
<b>Number of VN_Port Probes Req</b>	(QFX Series only)  Number of multicast N_Port_ID probes sent to the ALL-VN2VN-ENode-MACs multicast address on the VLAN.
<b>Number of VN_Port Claim Notif</b>	(QFX Series only)  Number of multicast N_Port_ID claim notifications sent on the VLAN.
<b>Number of VN_Port Beacons</b>	(QFX Series only)  Number of multicast beacons sent on the VLAN.
<b>Number of VN_Port Probes Reply</b>	(QFX Series only)  Number of replies to N_Port_ID probes sent on the VLAN. Replies are unicast to the ENode MAC address of the probe requester.

Table 8: show fip snooping statistics Output Fields *(Continued)*

Field Name	Field Description
<b>Number of VN_Port Claim Reply</b>	(QFX Series only)  Number of replies to N_Port_ID claim notifications sent on the VLAN. Replies are unicast to the ENode MAC address of the claim notifier.

## Sample Output

### show fip snooping statistics (FIP Snooping)

```

user@switch> show fip snooping statistics
VLAN: fcoevlan1      Mode: VN2VF Snooping

    Number of MDS:                2
    Number of UDS:                2
    Number of FLOGI:              2
    Number of FDISC:              2
    Number of LOGO:               0
    Number of Enode-keep-alive: 200
    Number of VNPort-keep-alive: 200

    Number of MDA:                25
    Number of UDA:                2
    Number of FLOGI_ACC:          2
    Number of FLOGI_RJT:          0
    Number of FDISC_ACC:          2
    Number of FDISC_RJT:          0
    Number of LOGO_ACC:           0
    Number of LOGO_RJT:           0
    Number of CVL:                0

```

### show fip snooping statistics (VN2VN\_Port Snooping)

```

user@switch> show fip snooping statistics
VLAN: vlan101      Mode: VN2VN Snooping

```

Number of VN_Port Probes Req:	3
Number of VN_Port Claim Notif:	3
Number of VN_Port Beacons:	0
Number of VN_Port Probes Reply:	3
Number of VN_Port Claim Reply:	3
Number of FLOGI:	0
Number of FLOGI_ACC:	0
Number of FLOGI_RJT:	0
Number of FDISC:	0
Number of FDISC_ACC:	0
Number of FDISC_RJT:	0
Number of LOGO:	0
Number of LOGO_ACC:	0
Number of LOGO_RJT:	0

## Release Information

Command introduced in Junos OS Release 10.4.

Command introduced with satellite keyword in Junos OS Release 17.4R1 for Junos Fusion Data Center.

## RELATED DOCUMENTATION

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

[Example: Configuring an FCoE Transit Switch](#)

*show fip snooping*

*show fip snooping enode*

*show fip snooping fcf*

*show fip snooping vlan*

*show fip snooping interface*

# show fip snooping vlan

## IN THIS SECTION

- [Syntax | 183](#)
- [Description | 183](#)
- [Options | 183](#)
- [Required Privilege Level | 183](#)
- [Output Fields | 184](#)
- [Sample Output | 187](#)
- [Release Information | 189](#)

## Syntax

```
show fip snooping vlan vlan-name  
<brief | detail>
```

## Description

Display FIP snooping VLAN information.

## Options

- |                         |                                                   |
|-------------------------|---------------------------------------------------|
| <b>brief   detail</b>   | (Optional) Display the specified level of output. |
| <b><i>vlan-name</i></b> | Display information for the specified VLAN.       |

## Required Privilege Level

view

## Output Fields

Table 9 on page 184 lists the output fields for the **show fip snooping vlan** command. Output fields are listed in the approximate order in which they appear.

**Table 9: show fip snooping vlan Output Fields**

Field Name	Field Description	Level of Output
<b>VLAN</b>	Name of the VLAN.	All
<b>Mode</b>	<p>(QFX Series only)</p> <p>Snooping mode enabled on the FCoE VLAN:</p> <ul style="list-style-type: none"> <li>• VN2VF Snooping—The FCoE VLAN is configured for FIP snooping between an ENode VN_Port and a switch VF_Port.</li> <li>• VN2VN Snooping—The FCoE VLAN is configured for VN_Port to VN_Port FIP snooping between ENode VN_Ports.</li> </ul>	All
<b>VN_Port count</b>	<p>(QFX Series only)</p> <p>Number of VN_Ports active on an ENode when the mode is VN2VN_Port FIP snooping.</p>	
<b>FC-MAP</b>	FCoE mapped address prefix of the FCoE forwarder for the VLAN.	All
<b>Beacon_Period</b>	<p>(QFX Series only)</p> <p>Beacon period interval in milliseconds.</p>	<b>detail</b>

Table 9: show fip snooping vlan Output Fields (*Continued*)

Field Name	Field Description	Level of Output
<b>VN2VN Mode</b>	<p>(QFX Series only)</p> <p>Mode of VN2VN_Port snooping:</p> <ul style="list-style-type: none"> <li>• Multi-Point—Multiple ENodes are connected to the network and form multiple virtual links. Each virtual link is created between one pair of VN_Ports. This is analogous to the loop mode in traditional FC networks.</li> <li>• Point-to-Point—Two ENodes are connected to the network and form a single VN_Port to VN_Port virtual link. This is analogous to the point-to-point FC link between an FC initiator and an FC target.</li> </ul>	<b>detail</b>
<b>FCF or FCF-MAC</b>	MAC address of the FCF.	All
<b>Session Count or Active Sessions</b>	Current number of virtual link sessions with VN_Ports.	All
<b>Configured FKA-ADV</b>	FIP keepalive interval in seconds configured on the FCF multiplied by three. For example, if the FKA_ADV period configured on the FCF is 86 seconds, the value of this field is 258.	<b>detail</b>
<b>Running FKA-ADV</b>	Runtime interval in seconds of the last FIP keepalive advertisement the FCF received. This value changes every time the FCF receives an FKA_ADV.	<b>detail</b>

Table 9: show fip snooping vlan Output Fields (*Continued*)

Field Name		Field Description	Level of Output
ENode-MAC		MAC address of the connected ENode.	All
	• <b>Interface</b>	Interface connected to the ENode.	<b>detail</b>
	• <b>Configured FKA-ADV</b>	FIP keepalive interval in seconds configured on the FCF multiplied by three. For example, if the FKA_ADV period configured on the FCF is 86 seconds, the value of this field is 258. This value remains constant.	<b>detail</b>
	• <b>Running FKA-ADV</b>	Runtime interval in seconds of the last FIP keepalive advertisement the ENode sent to the FCF. This value changes every time the ENode sends an FKA_ADV to the FCF.	<b>detail</b>
	• <b>VN-Port MAC</b>	MAC address of a VN_Port on the ENode.	All
	• <b>FKA-ADV</b>	Runtime interval in seconds of the last FIP keepalive advertisement the ENode sent to the FCF on behalf of the VN_Port (VN_Port FKA_ADV). This value changes every time the ENode sends a VN_Port FKA_ADV to the FCF.	<b>detail</b>
	• <b>Active VN_Ports</b>	(QFX Series only)  Number of VN_Ports active on an ENode.	<b>detail</b>



Table 9: show fip snooping vlan Output Fields (*Continued*)

Field Name	Field Description	Level of Output
<ul style="list-style-type: none"> <li><b>Vlink far-end VN-Port-MAC</b></li> </ul>	(QFX Series only)  Media access control (MAC) address of the VN_Port at the other end of the virtual link.	<b>detail</b>

## Sample Output

### show fip snooping vlan

```

user@switch> show fip snooping vlan fcoevlan1
VLAN : fcoevlan1      FC-MAP : 0e:fc:00
FCF : 00:10:94:00:00:01  Session Count : 2
Enode-MAC : 00:10:94:00:00:02
VN-Port-MAC : 0E:FC:00:00:00:05
VN-Port-MAC : 0E:FC:00:00:00:01

```

### show fip snooping vlan (QFX Series, VN2VF\_Port FIP Snooping)

```

user@switch> show fip snooping vlan fcoevlan1
VLAN : fcoevlan1      Mode: VN2VF Snooping
FC-MAP : 0e:fc:00
FCF : 00:10:94:00:00:01  Session Count : 2
Enode-MAC : 00:10:94:00:00:02
VN-Port-MAC : 0E:FC:00:00:00:05
VN-Port-MAC : 0E:FC:00:00:00:01

```

### show fip snooping vlan (QFX Series, VN2VN\_Port FIP Snooping)

```

user@switch> show fip snooping vlan vlan101
VLAN: vlan101,      Mode: VN2VN Snooping
FC-MAP: 0e:fd:00

```

```

Enode-MAC: 10:10:94:01:00:02 VN_Port count: 1
  VN-Port-MAC: 0e:fd:00:00:0a:01 Session Count: 2
Enode-MAC: 10:10:94:01:00:03 VN_Port count: 0

```

### show fip snooping vlan detail (QFX Series, VN2VN\_Port FIP Snooping)

```

user@switch> show fip snooping vlan vlan101 detail
VLAN: vlan101, Mode: VN2VN Snooping
  FC-MAP: 0e:fd:00
  Beacon_Period: 90000
  VN2VN Mode: Multi-Point
    Enode Information
      Enode-MAC: 10:10:94:01:00:02, Interface: xe-0/0/10
      Active VN_Ports : 1
      VN_Port Information
        VN-Port MAC: 0e:fd:00:00:0a:01
        Active Sessions : 2
        Session Information
          Vlink far-end VN-Port-MAC: 0e:fd:00:00:0b:01
          Vlink far-end VN-Port-MAC: 0e:fd:00:00:0c:01
      Enode-MAC: 10:10:94:01:00:02, Interface: xe-0/0/11
      Active VN_Ports : 0

```

### show fip snooping vlan detail

```

user@switch> show fip snooping vlan fcoevlan1 detail
VLAN : fcoevlan1 FC-MAP : 0e:fc:00
  FCF Information
    FCF-MAC : 00:10:94:00:00:01
    Active Sessions : 2
    Configured FKA-ADV : 258
    Running FKA-ADV : 235
    Enode Information
      Enode-MAC : 00:10:94:00:00:02 Interface : xe-0/0/1
      Configured FKA-ADV : 258
      Running FKA-ADV : 239
      Session Information
        VN-Port MAC : 0E:FC:00:00:00:05 FKA-ADV : 255
        VN-Port MAC : 0E:FC:00:00:00:01 FKA-ADV : 251

```

## Release Information

Command introduced in Junos OS Release 10.4.

## RELATED DOCUMENTATION

---

*Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

---

[Example: Configuring an FCoE Transit Switch](#)

---

*show fip snooping*

---

*show fip snooping enode*

---

*show fip snooping fcf*

---

*show fip snooping statistics*

---

*show fip snooping interface*