# Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide, Release 5.1(3)N1(1)

**First Published:** December 05, 2011

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25843-01

# CONTENTS

# Preface

This preface contains the following sections:



## Audience

This publication is for experienced network administrators who configure and maintain Cisco Nexus Series switches and Cisco Nexus 2000 Series Fabric Extenders.

## Document Conventions

Command descriptions use the following conventions:

| Convention | Description |
|---|---|
| **bold** | Bold text indicates the commands and keywords that you enter literally as shown. |
| *Italic* | Italic text indicates arguments for which the user supplies the values. |
| [x] | Square brackets enclose an optional element(keyword or argument). |
| [x \| y] | Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice. |
| {x \| y} | Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice. |

| Convention | Description |
|---|---|
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| `variable` | Indicates a variable for which you supply values, in context where italics cannot be used. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |

Examples use the following conventions:

| Convention | Description |
|---|---|
| `screen font` | Terminal sessions and information the switch displays are in screen font. |
| **`boldface screen font`** | Information you must enter is in boldface screen font. |
| *italic screen font* | Arguments for which you supply values are in italic screen font. |
| < > | Nonprinting characters, such as passwords, are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

This document uses the following conventions:

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

# Related Documentation

The entire Cisco NX-OS 5000 documentation set is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

### Release Notes

The release notes are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

### Configuration Guides

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

The documents in this category include:

- *Adapter-FEX Configuration Guide*
- *Cisco Fabric Manager Configuration Guide*
- *Cisco Nexus 5000 Series NX-OS Software Configuration Guide*
- *Configuration Limits for Cisco NX-OS*
- *FabricPath Configuration Guide*
- *Fibre Channel over Ethernet Configuration Guide*
- *Layer 2 Switching Configuration Guide*
- *Multicast Routing Configuration Guide*
- *Operations Guide*
- *SAN Switching Configuration Guide*
- *Quality of Service Configuration Guide*
- *Security Configuration Guide*
- *System Management Configuration Guide*
- *Unicast Routing Configuration Guide*

### Maintain and Operate Guides

Cisco Nexus 5000 Series NX-OS Operations Guides for various features are available at http://www.cisco.com/en/US/products/ps9670/prod_maintenance_guides_list.html.

### Installation and Upgrade Guides

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/prod_installation_guides_list.html

The documents in this category include:

- *FabricPath Command Reference*
- *Software Upgrade and Downgrade Guides*
- *Regulatory Compliance and Safety Information*

### Licensing Guide

The *License and Copyright Information for Cisco NX-OS Software* is available at http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html.

### Command References

These guides are available at the following URL:

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

The documents in this category include:

- *Command Reference Master Index*
- *Fabric Extender Command Reference*
- *FabricPath Command Reference*
- *Fibre Channel Command Reference*
- *Fundamentals Command Reference*
- *Layer 2 Interfaces Command Reference*
- *Multicast Routing Command Reference*
- *QoS Command Reference*
- *Security Command Reference*
- *System Management Command Reference*
- *TrustSec Command Reference*
- *Unicast Routing Command Reference*
- *vPC Command Reference*

### Technical References

The *Cisco Nexus 5000 and Cisco Nexus 2000 MIBs Reference* is available at http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mib/reference/NX5000_MIBRef.html.

### Error and System Messages

The *Nexus 5000 Series NX-OS System Message Reference* is available at http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/system_messages/reference/sl_nxos_book.html.

### Troubleshooting Guide

The *Cisco Nexus 5000 Troubleshooting Guide* is available at http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide.html.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

# New and Changed Information

This chapter contains the following sections:



# New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide*.

The latest version of this document is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

To check for additional information about Cisco NX-OS software, see the *Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes* available at the following URL:

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

The following table summarized the changes in this book for release 5.1(3)N1(1):

| Feature | Description | Where Documented |
|---|---|---|
| Cisco Adapter FEX with FCoE | Support has been added for FCoE connections between a Cisco Nexus Series switch using a Cisco Nexus 2000 Series Fabric Extender and a Virtual Interface Card (VIC). | Configuring Cisco Adapter FEX with FCoE, on page 35 |
| FCoE with an Enhanced vPC Topology | Support has been added for using FCoE in an enhanced vPC topology. This new feature replaces the FEX straight-through and host CNA active-active topologies. | FCoE over Enhanced vPC, on page 29 and Configuring FCoE over Enhanced vPC, on page 30 |
| SAN Boot with vPC | You can now use a virtual port channnel to boot the switch from a SAN boot image. | SAN Boot with vPC, on page 32 |

| Feature | Description | Where Documented |
|---|---|---|
| Quality of Service policies | The Cisco Nexus 5500 Platform switch now has default QoS policies. You no longer need to change the defaults when you enable FCoE. | |

CHAPTER 2

# Overview

This chapter contains the following sections:



## Overview

Fibre Channel over Ethernet (FCoE) allows Fibre Channel traffic to be encapsulated over a physical Ethernet link. FCoE frames use a unique EtherType so that FCoE traffic and standard Ethernet traffic can be carried on the same link.

Classic Ethernet is a best-effort protocol; in the event of congestion, Ethernet will discard packets, relying on higher level protocols to provide retransmission and other reliability mechanisms. Fibre Channel traffic requires a lossless transport layer; as a data storage protocol, it is unacceptable to lose a single data packet. Native Fibre Channel implements a lossless service at the transport layer using a buffer-to-buffer credit system.

For FCoE traffic, the Ethernet link must provide a lossless service. Ethernet links on Cisco Nexus 5000 Series switches provide two mechanisms to ensure lossless transport for FCoE traffic: link-level flow control (LL-FC) and priority flow control (PFC).

IEEE 802.3x link-level flow control allows a congested receiver to signal the far end to pause the data transmission for a short period of time. The pause functionality is applied to all the traffic on the link.

The priority flow control feature applies pause functionality to specific classes of traffic on the Ethernet link. For example, PFC can provide lossless service for the FCoE traffic and best-effort service for the standard Ethernet traffic. PFC can provide different levels of service to specific classes of Ethernet traffic (using IEEE 802.1p traffic classes).

Cisco Nexus Series switches support T11-compliant FCoE on all 10-Gigabit Ethernet interfaces.

# FCoE Initiation Protocol

The FCoE Initialization Protocol (FIP) allows the switch to discover and initialize FCoE-capable entities that are connected to an Ethernet LAN. Two versions of FIP are supported by the Cisco Nexus 5000 Series switch:

- FIP—The Converged Enhanced Ethernet Data Center Bridging Exchange (CEE-DCBX) protocol supports T11-compliant Gen-2 CNAs.
- Pre-FIP—The Cisco, Intel, Nuova Data Center Bridging Exchange (CIN-DCBX) protocol supports Gen-1 converged network adapters (CNAs).

The Cisco Nexus 5000 Series switch detects the capabilities of the attached CNA and switches to the correct FIP mode.

## FIP Virtual Link Instantiation

Cisco NX-OS Release 4.1(3)N1(1) adds support for the T11-compliant FIP on the Cisco Nexus 5000 Series switch.

FIP is used to perform device discovery, initialization, and link maintenance. FIP performs the following protocols:

- FIP Discovery—When a FCoE device is connected to the fabric, it sends out a Discovery Solicitation message. A Fibre Channel Forwarder (FCF) or a switch responds to the message with a Solicited Advertisement that provides an FCF MAC address to use for subsequent logins.
- FCoE Virtual Link instantiation— FIP defines the encapsulation of fabric login (FLOGI) , fabric discovery (FDISC), logout (LOGO), and exchange link parameters (ELP) frames along with the corresponding reply frames. The FCoE devices use these messages to perform a fabric login.
- FCoE Virtual Link maintenance— FIP periodically sends maintenance messages between the switch and the CNA to ensure the connection is still valid.

## FCoE Frame Format

FCoE is implemented by encapsulating a Fibre Channel frame in an Ethernet packet with a dedicated Ethertype, 0x8906. That packet has a 4-bit version field. The other header fields in the frame (the source and destination MAC addresses, VLAN tags, and frame markers) are all standard Ethernet fields. Reserved bits pad the FCoE frame to the IEEE 802.3 minimum packet length of 64 bytes.

A Fibre Channel frame consists of 36 bytes of headers and up to 2112 bytes of data for a total maximum size of 2148 bytes. The encapsulated Fibre Channel frame has all the standard headers, which allow it to be passed to the storage network without further modification. To accomodate the maximum Fibre Channel frame in an FCoE frame, the class-fcoe is defined with a default MTU of 2240 bytes.

# VLAN Tagging for FCoE Frames

The Ethernet frames that are sent by the switch to the adapter may include the IEEE 802.1Q tag. This tag includes a field for the class of service (CoS) value used by the priority flow control (PFC). The IEEE 802.1Q tag also includes a VLAN field.

The Cisco Nexus 5000 Series switch expects frames from a FIP T11-compliant CNA to be tagged with the VLAN tag for the FCoE VLAN. Frames that are not correctly tagged are discarded.

The switch expects frames from a pre-FIP CNA to be priority tagged with the FCoE CoS value. The switch will still accept untagged frames from the CNA.

# FIP Ethernet Frame Format

FIP is encapsulated in an Ethernet packet with a dedicated EtherType, 0x8914. The packet has a 4-bit version field. Along with the source and destination MAC addresses, the FIP packet also contains a FIP operation code and a FIP operation subcode. The following table describes the FIP operation codes.

***Table 1: FIP Operation Codes***

| FIP Operation Code | FIP Subcode | FIP Operation |
|---|---|---|
| 0x0001 | 0x01 | Discovery Solicitation |
| | 0x02 | Discovery Advertisement |
| 0x0002 | 0x01 | Virtual Link Instantiation Request |
| | 0x02 | Virtual Link Instantiation Reply |
| 0x0003 | 0x01 | FIP Keep Alive |
| | 0x02 | FIP Clear Virtual Links |
| 0x0004 | 0x01 | FIP VLAN Request |
| | 0x02 | FIP VLAN Notification |

# Pre-FIP Virtual Link Instantiation

Pre-FIP virtual link instantiation consists of two phases; link discovery using the Data Center Bridging Exchange protocol (DCBX), which is followed by Fabric Login.

The Cisco Nexus 5000 Series switch is backward compatible with Gen-1 CNAs that operate in pre-FIP mode.

**Note** Pre-FIP is also known as the Cisco, Intel, Nuova Data Center Bridging Exchange (CIN-DCBX) protocol.

# Data Center Bridging Exchange Protocol

The Data Center Bridging Exchange (DCBX) protocol is an extension of the Link Layer Discovery Protocol (LLDP). DCBX end points exchange request and acknowledgment messages. For flexibility, parameters are coded in a type-length-value (TLV) format.

The Cisco Nexus 5000 Series switch supports two versions of DCBX:

- CEE-DCBX—The Converged Enhanced Ethernet DCBX is supported on all T11-compliant Gen-2 CNAs
- CIN-DCBX—The Cisco, Intel, Nuova DCBX is supported on Gen-1 converged network adapters (CNAs). CIN-DCBX is used to perform link detection in addition to other functions.

DCBX runs on the physical Ethernet link between the Cisco Nexus 5000 Series switch and the CNA. By default, DCBX is enabled on Ethernet interfaces. When an Ethernet interface is brought up, the switch automatically starts to communicate with the CNA.

During the normal operation of FCoE between the switch and the CNA, DCBX provides link-error detection.

DCBX is also used to negotiate capabilities between the switch and the CNA and to send configuration values to the CNA.

The CNAs that are connected to a Cisco Nexus 5000 Series switch are programmed to accept the configuration values sent by the switch, allowing the switch to distribute configuration values to all attached CNAs, which reduces the possibility of configuration errors and simplifies CNA administration.

## DCBX Feature Negotiation

The switch and CNA exchange capability information and configuration values. The Cisco Nexus 5000 Series switches support the following capabilities:

- FCoE—If the CNA supports FCoE capability, the switch sends the IEEE 802.1p CoS value to be used with FCoE packets.
- Priority Flow Control (PFC)—If the adapter supports PFC, the switch sends the IEEE 802.1p CoS values to be enabled with PFC.
- Priority group type-length-value (TLV)
- Ethernet logical link up and down signal
- FCoE logical link up and down signal for pre-FIP CNAs

The following rules determine whether the negotiation results in a capability being enabled:

- If a capability and its configuration values match between the switch and the CNA, the feature is enabled.
- If a capability matches, but the configuration values do not match, the following occurs:
  - If the CNA is configured to accept the switch configuration value, the capability is enabled using the switch value.
  - If the CNA is not configured to accept the switch configuration value, the capability remains disabled.

- If the CNA does not support a DCBX capability, that capability remains disabled.
- If the CNA does not implement DCBX, all capabilities remain disabled.

**Note** The Cisco Nexus 5000 Series switch provides CLI commands to manually override the results of the PFC negotiation with the adapter. On a per-interface basis, you can force capabilities to be enabled or disabled.

# Lossless Ethernet

Standard Ethernet is a best-effort medium which means that it lacks any form of flow control. In the event of congestion or collisions, Ethernet will drop packets. The higher level protocols detect the missing data and retransmit the dropped packets.

To properly support Fibre Channel, Ethernet has been enhanced with a priority flow control (PFC) mechanism.

## Logical Link Up/Down

The following expansion modules provide native Fibre Channel ports to connect the Cisco Nexus 5000 Series switch to other Fibre Channel devices.

- N5K-M1404 Cisco Nexus 5000 1000 Series Module 4x10GE 4xFC 4/2/1
- N5K-M1008 Cisco Nexus 5000 1000 Series Module 8xFC 4/2/1
- N5K-M1060 Cisco Nexus 5000 1000 Series Module 6xFC 8/4/2/1

On a native Fibre Channel link, some configuration actions (such as changing the VSAN) require that you reset the interface status. When you reset the interface status, the switch disables the interface and then immediately reenables the interface.

If an Ethernet link provides FCoE service, do not reset the physical link because this action is disruptive to all traffic on the link.

The logical link up/down feature allows the switch to reset an individual virtual link. The logical link down is signaled with a FIP Clear Virtual Link message.

For pre-FIP CNAs, the switch sends a DCBX message to request the CNA to reset only the virtual Fibre Channel interface.

**Note** If the CNA does not support the logical link level up/down feature, the CNA resets the physical link. In this case, all traffic on the Ethernet interface is disrupted.

DCBX-based FC Logical Link Status signaling only applies to FCoE sessions to pre-FIP CNAs.

## Converged Network Adapters

The following types of CNAs are available:

- Hardware adapter
  - Works with the existing Fibre Channel host bus adapter (HBA) driver and Ethernet Network Interface Card (NIC) driver in the server.
  - Server operating system view of the network is unchanged; the CNA presents a SAN interface and a LAN interface to the operating system.
- FCoE software stack
  - Runs on existing 10-Gigabit Ethernet adapters.

Two generations of CNAs are supported by the Cisco Nexus 5000 Series switch:

- A FIP adapter uses the FIP to exchange information about its available capabilities and to negotiate the configurable values with the switch.
- A pre-FIP adapter uses DCBX to exchange information about its available capabilities and to negotiate the configurable values with the switch.

To reduce configuration errors and simplify administration, the switch distributes the configuration data to all the connected adapters.

CHAPTER 3

# Configuring FCoE

This chapter contains the following sections:



## Licensing Requirements for FCoE

On Cisco Nexus 5000 Series switches, FCoE capability is included in the Storage Protocol Services License.

Before using FCoE capabilities, you must ensure the following:

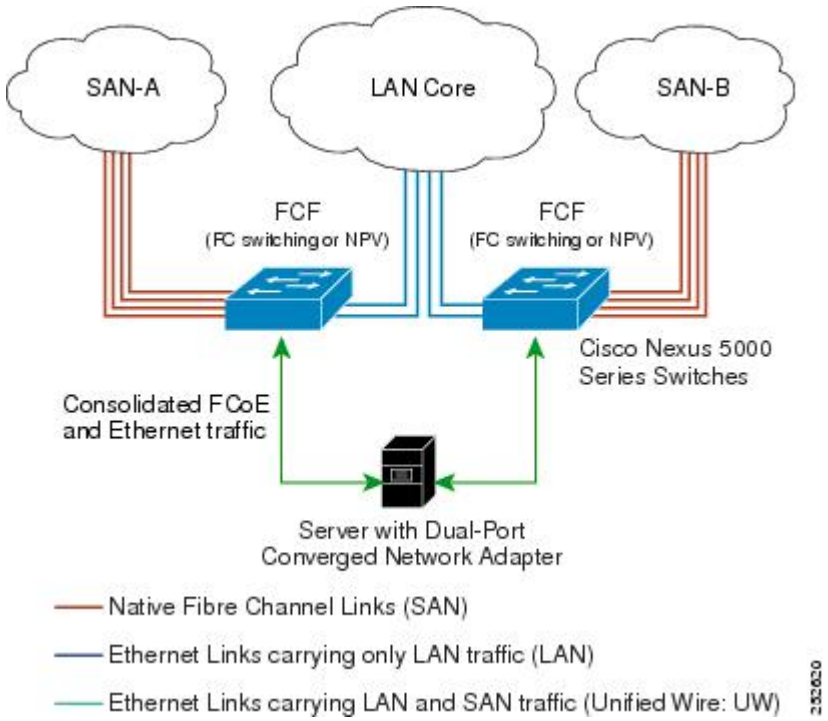
- The correct license is installed (N5010SS or N5020SS).
- FCoE has been activated on the switch by entering the **feature fcoe** command in configuration mode.

# FCoE Topologies

## Directly Connected CNA Topology

The Cisco Nexus 5000 Series switch can be deployed as a Fibre Channel Forwarder (FCF) as shown in the following figure.

***Figure 1: Directly Connected Fibre Channel Forwarder***




The following rules are used to process FIP frames to avoid the FCF being used as a transit between an FCoE node (ENode) and another FCF. These rules also prevent login sessions between ENodes and FCFs in different fabrics.

- FIP solicitation and login frames received from the CNAs are processed by the FCF and are not forwarded.
- If an FCF receives solicitations and advertisements from other FCFs over an interface, the following occurs:
  - The frames are ignored and discarded if the FC-MAP value in the frame matches the value of the FCF (the FCF is in the same fabric)
  - The interface is placed in the "FCoE Isolated" state if the FC-MAP value in the FIP frame does not match that of the FCF (the FCF is in a different fabric)

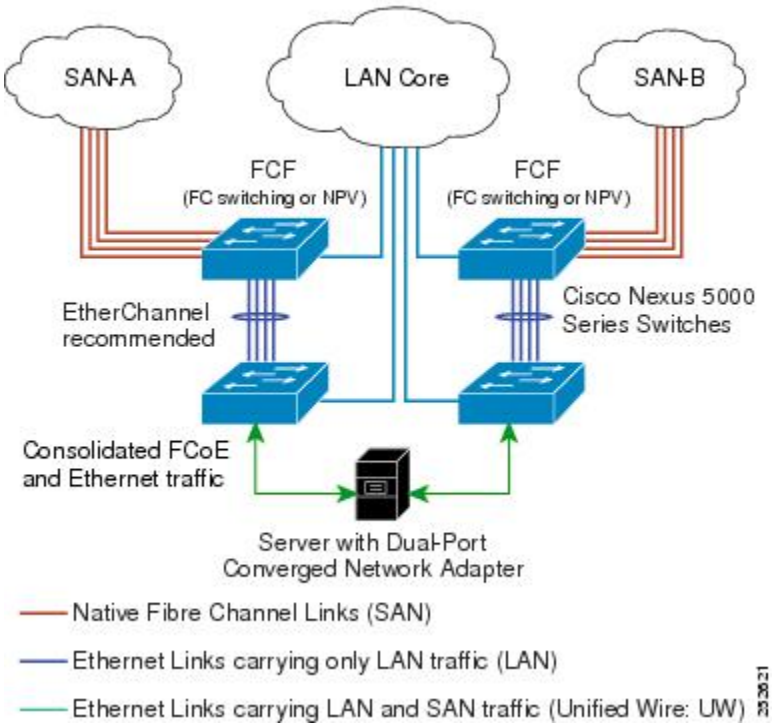
CNAs cannot discover or login to FCFs that are reachable only through a transit Cisco Nexus 5000 Series FCF. The Cisco Nexus 5000 Series switch cannot perform the FCoE transit function between a CNA and another FCF due to hardware limitations.

Because the Cisco Nexus 5000 Series FCF cannot perform the transit FCoE function, you must design your network topology so that the active STP path of FCoE VLANs is always over the directly connected links between the CNA and the FCF. Make sure that you configure the FCoE VLAN on the directly connected links only.

# Remotely Connected CNA Topology

The Cisco Nexus 5000 Series switch can be deployed as a Fibre Channel Forwarder (FCF) for remotely connected CNAs, but not as a FIP Snooping Bridge, as shown in the following figure.

***Figure 2: Remotely Connected Fibre Channel Forwarder***




The following rules are used to process FIP frames to avoid the FCF being used as a transit between an ENode and another FCF. These rules also prevent login sessions between ENodes and FCFs in different fabrics.

- FIP solicitation and login frames received from the CNAs are processed by the FCF and are not forwarded.
- If an FCF receives solicitations and advertisements from other FCFs over an interface, the following occurs:
  - The frames are ignored and discarded if the FC-MAP value in the frame matches the value of the FCF (the FCF is in the same fabric)

- The interface is placed in the "FCoE Isolated" state if the FC-MAP value in the FIP frame does not match that of the FCF (the FCF is in a different fabric)

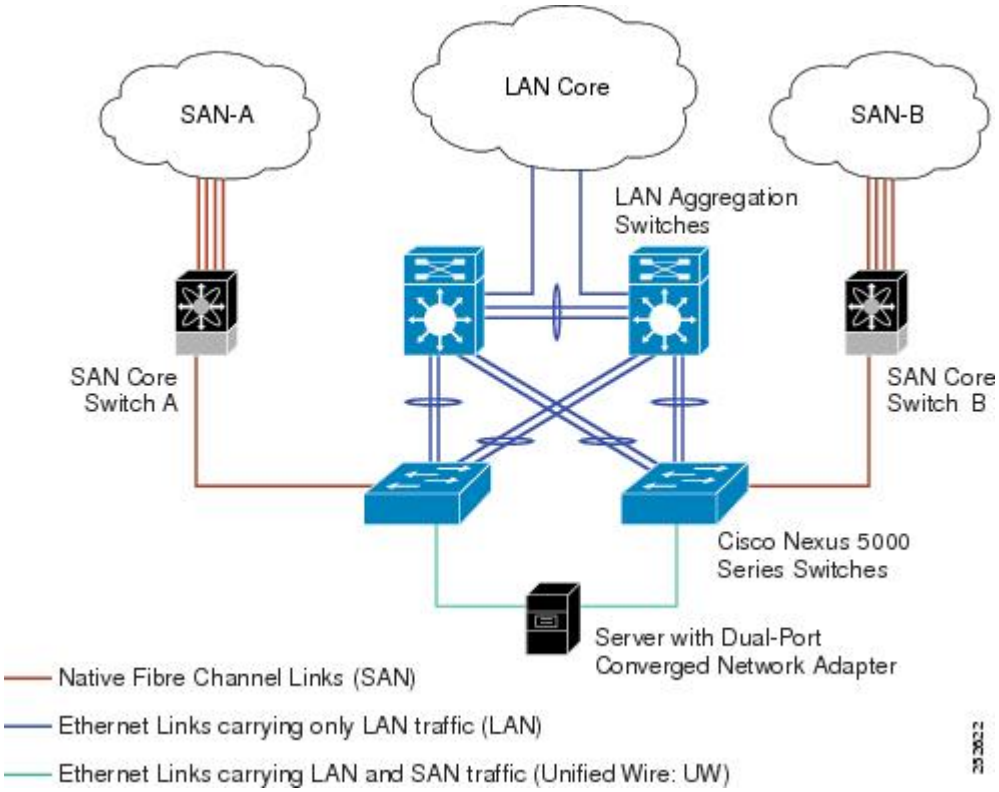
Because the Cisco Nexus 5000 Series FCF cannot perform the transit FCoE function, you must design your network topology so that the active STP path of FCoE VLANs is always over the directly connected links between the CNA and the FCF. Make sure that you configure the FCoE VLAN on the directly connected links only.

# FCoE Best Practices

## Directly Connected CNA Best Practice

The following figure shows a best practices topology for an access network using directly connected CNAs with Cisco Nexus 5000 Series switches.

***Figure 3: Directly Connected CNA***




Follow these configuration best practices for the deployment topology in the preceding figure:

1. You must configure a unique dedicated VLAN at every converged access switch to carry traffic for each Virtual Fabric (VSAN) in the SAN (for example, VLAN 1002 for VSAN 1, VLAN 1003 for VSAN 2, and so on). If you enable Multiple Spanning Tree (MST), you must use a separate MST instance for FCoE VLANs.

2 You must configure the unified fabric (UF) links as trunk ports. Do not configure the FCoE VLAN as a native VLAN. You must configure all FCoE VLANs as members of the UF links to allow extensions for VF_Port trunking and VSAN management for the virtual Fibre Channel interfaces.

**Note** A unified wire carries both Ethernet and FCoE traffic.

3 You must configure the UF links as spanning-tree edge ports.

4 You must not configure the FCoE VLANs as members of Ethernet links that are not designated to carry FCoE traffic because you want to ensure the scope of the STP for the FCoE VLANs is limited to UF links only.

5 If the converged access switches (in the same SAN fabric or in another) need to be connected to each other over Ethernet links for a LAN alternate path, then such links must explicitly be configured to exclude all FCoE VLANs from membership. This action ensures that the scope of the STP for the FCoE VLANs is limited to UF links only.

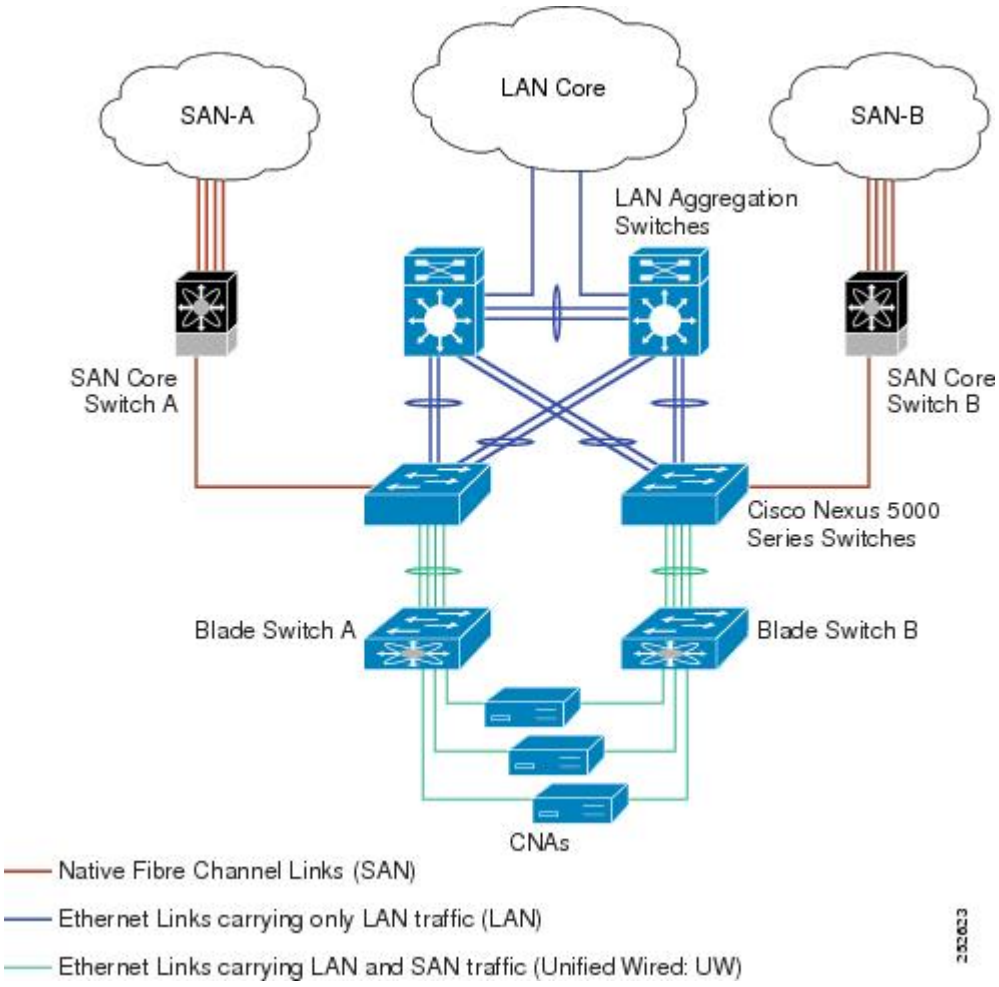
6 You must use separate FCoE VLANs for FCoE in SAN-A and SAN-B.

**Note** All Gen-1 (pre-FIP) and Gen-2 (FIP) CNAs are supported in a directly connected topology.

# Remotely Connected CNA Best Practice

The following figure shows a best practices topology for an access network using remotely connected CNAs with Cisco Nexus 5000 Series switches.

***Figure 4: Remotely Connected CNAs***




Follow these configuration best practices for the deployment topology in the preceding figure:

1. You must configure a unique dedicated VLAN at every converged access switch to carry traffic for each Virtual Fabric (VSAN) in the SAN (for example, VLAN 1002 for VSAN 1, VLAN 1003 for VSAN 2, and so on). If you enable MST, you must use a separate MST instance for FCoE VLANs.
2. You must configure the unified fabric (UF) links as trunk ports. Do not configure the FCoE VLAN as a native VLAN. You must configure all FCoE VLANs as members of the UF links to allow extensions for VF_Port trunking and VSAN management for the virtual Fibre Channel interfaces.

**Note** A unified fabric link carries both Ethernet and FCoE traffic.

3 You must configure the CNAs and the blade switches as spanning-tree edge ports.

4 A blade switch must connect to exactly one Cisco Nexus 5000 Series converged access switch, preferably over an EtherChannel, to avoid disruption due to STP reconvergence on events such as provisioning new links or blade switches.

5 You must configure the Cisco Nexus 5000 Series converged access switch with a better STP priority than the blade switches that are connected to it. This requirement allows you to create an island of FCoE VLANs where the converged access switch is the spanning-tree root and all the blade switches connected to it become downstream nodes.

6 Do not configure the FCoE VLANs as members of Ethernet links that are not designated to carry FCoE traffic because you want to ensure that the scope of the STP for the FCoE VLANs is limited to UF links only.

7 If the converged access switches and/or the blade switches need to be connected to each over Ethernet links for the purposes of LAN alternate pathing, then such links must explicitly be configured to exclude all FCoE VLANs from membership. This will ensure the scope of the spanning-tree protocol for FCoE VLANs is limited to UF links only.

8 You must use separate FCoE VLANs for FCoE in SAN-A and SAN-B.

**Note** A remotelyconnected topology is supported only with Gen-2 (FIP) CNAs.

# Guidelines and Limitations

FCoE has the following guidelines and limitations:

- FCoE on the Nexus 5000 Series supports the Gen-1 (pre-FIP) and Gen-2 (FIP) CNAs. FCoE on the Nexus 2232PP fabric extender supports Gen-2 CNAs only.
- Enabling FCoE on VLAN 1 is not supported.
- FCoE is not supported on a fabric extender interface or port channel when the fabric extender is connected to two switches in a fabric extender active-active topology.
- A combination of straight-through and active-active topologies is not supported on the same fabric extender.
- Direct connect FCoE (that is, a direct connect to CNAs through a bind interface) is not supported on a port channel of a Nexus 5000 Series or fabric extender interface if it is configured to have more than one interface. Direct connect FCoE is supported on port channels with a single link to allow for FCoE from a CNA connected through a vPC with one 10GB link to each upstream switch/fabric extender.

**Note** For a description of the default Quality of Service (QoS) policies for FCoE, see the *Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide* for the Nexus software release that you are using. The available versions of this document can be found at the following URL: http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html..

# Configuring FCoE

## Enabling FCoE

You can enable FCoE on the switch; however, enabling FCoE on VLAN 1 is not supported.

**Note** All the Fibre Channel features of the Cisco Nexus 5000 Series switch are packaged in the FC Plugin. When you enable FCoE, the switch software checks for the FC_FEATURES_PKG license. If it finds the license, the software loads the plugin. If the license is not found, the software loads the plugin with a grace period of 180 days.

After the FC Plugin is loaded, the following occurs:

- All Fibre Channel and FCoE related CLI are available
- The Fibre Channel interfaces of any installed Expansion Modules are available

If after 180 days, a valid license is not found, the FC Plugin is disabled. At the next switch reboot, all FCoE commands are removed from the CLI and the FCoE configuration is deleted.

### Before You Begin

You need to have the FC_FEATURES_PKG (N5010SS or N5020SS) license installed.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature fcoe**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **feature fcoe** | Enables the FCoE capability. |

This example shows how to enable FCoE on the switch:

```
switch# configure terminal
switch(config)# feature fcoe
```

# Disabling FCoE

After you disable FCoE, all FCoE commands are removed from the CLI and the FCoE configuration is deleted .

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature fcoe**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **no feature fcoe** | Disables the FCoE capability. |

This example shows how to disable FCoE on the switch:

```
switch# configure terminal
switch(config)# no feature fcoe
```

# Disabling LAN Traffic on an FCoE Link

You can disable LAN traffic on an FCoE link.

DCBX allows the switch to send a LAN Logical Link Status (LLS) message to a directly-connected CNA. Enter the **shutdown lan** command to send an LLS-Down message to the CNA. This command causes all VLANs on the interface that are not enabled for FCoE to be brought down. If a VLAN on the interface is enabled for FCoE, it continues to carry SAN traffic without any interruption.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot*/*port*
3. switch(config-if)# **shutdown lan**
4. (Optional) switch(config-if)# **no shutdown lan**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **interface ethernet** *slot*/*port* | Specifies an interface to configure, and enters interface configuration mode. |
| **Step 3** | switch(config-if)# **shutdown lan** | Shuts down Ethernet traffic on the interface. If the interface is part of an FCoE VLAN, the shutdown has no impact on the FCoE traffic. |
| **Step 4** | switch(config-if)# **no shutdown lan** | (Optional)<br>Reenables Ethernet traffic on the interface. |

# Configuring the FC-Map

You can prevent data corruption due to cross-fabric talk by configuring an FC-Map which identifies the Fibre Channel fabric for this Cisco Nexus 5000 Series switch. When the FC-Map is configured, the switch discards the MAC addresses that are not part of the current fabric.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fcmap** *fabric-map*
3. (Optional) switch(config)# **no fcoe fcmap** *fabric-map*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **fcoe fcmap** *fabric-map* | Configures the global FC-Map. The default value is 0E.FC.00. The range is from 0E.FC.00 to 0E.FC.FF. |
| **Step 3** | switch(config)# **no fcoe fcmap** *fabric-map* | (Optional)<br>Resets the global FC-Map to the default value of 0E.FC.00. |

This example shows how to configure the global FC-Map:

```
switch# configure terminal
switch(config)# fcoe fcmap 0e.fc.2a
```

# Configuring the Fabric Priority

The Cisco Nexus 5000 Series switch advertises its priority. The priority is used by the CNAs in the fabric to determine the best switch to connect to.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fcf-priority** *fabric-priority*
3. (Optional) switch(config)# **no fcoe fcf-priority** *fabric-priority*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **fcoe fcf-priority** *fabric-priority* | Configures the global fabric priority. The default value is 128. The range is from 0 (higher) to 255 (lower). |
| **Step 3** | switch(config)# **no fcoe fcf-priority** *fabric-priority* | (Optional)<br>Resets the global fabric priority to the default value of 128. |

This example shows how to configure the global fabric priority:

```
switch# configure terminal
switch(config)# fcoe fcf-priority 42
```

# Setting the Advertisment Interval

You can configure the interval for Fibre Channel fabric advertisment on the switch.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **fcoe fka-adv-period** *inverval*
3. (Optional) switch(config)# **no fcoe fka-adv-period** *interval*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | switch(config)# **fcoe fka-adv-period** *inverval* | Configures the advertisement interval for the fabric. The default value is 8 seconds. The range is from 4 to 60 seconds. |
| **Step 3** | switch(config)# **no fcoe fka-adv-period** *interval* | (Optional)<br>Resets the advertisement interval for the fabric to its default value of 8 seconds. |

This example shows how to configure the advertisement interval for the fabric:

```
switch# configure terminal
switch(config)# fcoe fka-adv-period 42
```

# Verifying FCoE Configuration

To verify FCoE configuration information, perform one of these tasks:

| Command | Purpose |
|---|---|
| switch# **show fcoe** | Displays whether FCoE is enabled on the switch. |
| switch# **show fcoe database** | Displays the contents of the FCoE database. |
| switch# **show interface** [*interface number*] **fcoe** | Displays the FCoE settings for an interface or all interfaces. |

This example shows how to verify that the FCoE capability is enabled:

```
switch# show fcoe
Global FCF details
        FCF-MAC is 00:0d:ec:6d:95:00
        FC-MAP is 0e:fc:00
        FCF Priority is 128
        FKA Advertisement period for FCF is 8 seconds
```

This example shows how to display the FCoE database:

```
switch# show fcoe database
------------------------------------------------------------------------------
INTERFACE       FCID            PORT NAME               MAC ADDRESS
------------------------------------------------------------------------------
vfc3            0x490100        21:00:00:1b:32:0a:e7:b8 00:c0:dd:0e:5f:76
```

This example shows how to display the FCoE settings for an interface.

```
switch# show interface ethernet 1/37 fcoe
Ethernet1/37 is FCoE UP
    vfc3 is Up
        FCID is 0x490100
        PWWN is 21:00:00:1b:32:0a:e7:b8
        MAC addr is 00:c0:dd:0e:5f:76
```

CHAPTER 4

# Configuring FCoE VLANs and Virtual Interfaces

This chapter contains the following sections:



## Information About Virtual Interfaces

Cisco Nexus 5000 Series switches support Fibre Channel over Ethernet (FCoE), which allows Fibre Channel and Ethernet traffic to be carried on the same physical Ethernet connection between the switch and the servers.

The Fibre Channel portion of FCoE is configured as a virtual Fibre Channel interface. Logical Fibre Channel features (such as interface mode) can be configured on virtual Fibre Channel interfaces.

A virtual Fibre Channel interface must be bound to an interface before it can be used. The binding is to a physical Ethernet interface (when the converged network adapter (CNA) is directly connected to the Cisco Nexus 5000 Series switch), a MAC address (when the CNA is remotely connected over a Layer 2 bridge), or an EtherChannel when the CNA connects to the Fibre Channel Forwarder (FCF) over a virtual port channel (vPC).

## Guidelines for FCoE VLANs and Virtual Interfaces

Follow these guidelines when configuring FCoE VLANs and Virtual Fiber Channel (vFC) Interfaces:

- Each vFC interface must be bound to an FCoE-enabled Ethernet or EtherChannel interface or to the MAC address of a remotely connected adapter. FCoE is supported on 10-Gigabit Ethernet interfaces.

  The Ethernet or EtherChannel interface that you bind to the vFC interface must be configured as follows:

- The Ethernet or EtherChannel interface must be a trunk port (use the **switchport mode trunk** command).
- The FCoE VLAN that corresponds to a vFC's VSAN must be in the allowed VLAN list.
- You must not configure an FCoE VLAN as the native VLAN of the trunk port.

**Note** The native VLAN is the default VLAN on a trunk. Any untagged frames transit the trunk as native VLAN traffic.

- You should use an FCoE VLAN only for FCoE.
- Do not use the default VLAN, VLAN1, as an FCoE VLAN.
- You must configure the Ethernet interface as PortFast (use the **spanning-tree port type edge trunk** command).

**Note** You are not required to configure trunking on the server interface even if the switch interface is configured with trunking enabled. All non-FCoE traffic from the server will be passed on the native VLAN.

- The vFC interface can be bound to Ethernet port-channels with multiple member ports connected to FIP snooping bridges.
- Each vFC interface is associated with only one VSAN.
- You must map any VSAN with associated vFC interfaces to a dedicated FCOE-enabled VLAN.
- FCoE is not supported on private VLANs.
- If the converged access switches (in the same SAN fabric or in another) need to be connected to each other over Ethernet links for a LAN alternate path, then you must explicitly configure such links to exclude all FCoE VLANs from membership.
- You must use separate FCoE VLANs for FCoE in SAN-A and SAN-B fabrics.
- FCoE connectivity to pre-FIP CNAs over virtual port channels (vPCs) is not supported.

**Note** Virtual interfaces are created with the administrative state set to down. You must explicitly configure the administrative state to bring the virtual interface into operation.

# Configuring Virtual Interfaces

## Mapping a VSAN to a VLAN

A unique, dedicated VLAN must be configured at every converged access switch to carry traffic for each Virtual Fabric (VSAN) in the SAN (for example, VLAN 1002 for VSAN 1, VLAN 1003 for VSAN 2, and so on). If MST is enabled, a separate MST instance must be used for FCoE VLANs.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan** *vlan-id*
3. switch(config-vlan)# **fcoe** [**vsan** *vsan-id*]
4. switch(config-vlan)# **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **vlan** *vlan-id* | Enters VLAN configuration mode. The VLAN number range is from 1 to 4096. |
| **Step 3** | switch(config-vlan)# **fcoe** [**vsan** *vsan-id*] | Enables FCoE for the specified VLAN. If you do not specify a VSAN number, a mapping is created from this VLAN to the VSAN with the same number.<br>Configures the mapping from this VLAN to the specified VSAN. |
| **Step 4** | switch(config-vlan)# **exit** | Exits VLAN configuration mode. |

This example shows how to map VLAN 200 to VSAN 2:

```
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
```

## Creating a Virtual Fibre Channel Interface

You can create a virtual Fibre Channel interface. You must bind the virtual Fibre Channel interface to a physical interface before it can be used.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface vfc** *vfc-id*
3. switch(config-if)# **bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*}
4. (Optional) switch(config-if)# **no bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*}
5. (Optional) switch(config)# **no interface vfc** *vfc-id*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **interface vfc** *vfc-id* | Creates a virtual Fibre Channel interface (if it does not already exist) and enters interface configuration mode.<br>The virtual Fibre Channel interface ID range is from 1 to 8192. |
| **Step 3** | switch(config-if)# **bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*} | Binds the virtual Fibre Channel interface to the specified interface. |
| **Step 4** | switch(config-if)# **no bind** {**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} | **mac-address** *MAC-address*} | (Optional)<br>Unbinds the virtual Fibre Channel interface from the specified interface. |
| **Step 5** | switch(config)# **no interface vfc** *vfc-id* | (Optional)<br>Deletes a virtual Fibre Channel interface. |

This example shows how to bind a virtual Fibre Channel interface to an Ethernet interface:

```
switch# configure terminal
switch(config)# interface vfc 4
switch(config-if)# bind interface ethernet 1/4
```

This example shows how to bind a virtual Fibre Channel interface to a Nexus 2232PP fabric extender Ethernet interface:

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind interface ethernet 100/1/1
```

This example shows how to bind a virtual Fibre Channel interface to create a vPC:

```
switch# configure terminal
switch(config)# interface vfc 3
switch(config-if)# bind interface port-channel 1
```

This example shows how to bind a virtual Fibre Channel interface on a Nexus 2232PP fabric extender to create a vPC:

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind interface ethernet 100/1/1
```

**Note** An error message is displayed if you attempt to bind the interface to a Nexus fabric extender that does not support FCoE.

This example shows how to bind a virtual Fibre Channel interface to a MAC address:

```
switch# configure terminal
switch(config)# interface vfc 2
switch(config-if)# bind mac-address 00:0a:00:00:00:36
```

This example shows how to bind a virtual Fibre Channel interface to a Nexus 2232PP fabric extender MAC address:

```
switch# configure terminal
switch(config)# interface vfc 1001
switch(config-if)# bind mac-address 00:01:0b:00:00:02
```

This example shows how to delete a virtual Fibre Channel interface:

```
switch# configure terminal
switch(config)# no interface vfc 4
```

# Associating a Virtual Fibre Channel Interface to a VSAN

A unique, dedicated VLAN must be configured at every converged access switch to carry traffic for each Virtual Fabric (VSAN) in the SAN (for example, VLAN 1002 for VSAN 1, VLAN 1003 for VSAN 2, and so on). If MST is enabled, a separate MST instance must be used for FCoE VLANs.

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vsan database**
3. switch(config-vsan)# **vsan** *vsan-id* **interface vfc** *vfc-id*
4. (Optional) switch(config-vsan)# **no vsan** *vsan-id* **interface vfc** *vfc-id*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | switch# **configure terminal** | Enters configuration mode. |
| **Step 2** | switch(config)# **vsan database** | Enters VSAN configuration mode. |
| **Step 3** | switch(config-vsan)# **vsan** *vsan-id* **interface vfc** *vfc-id* | Configures the association between the VSAN and virtual Fibre Channel interface. |

| | Command or Action | Purpose |
|---|---|---|
| | | The VSAN number must map to a VLAN on the physical Ethernet interface that is bound to the virtual Fibre Channel interface. |
| **Step 4** | switch(config-vsan)# **no vsan** *vsan-id* **interface vfc** *vfc-id* | (Optional)<br>Disassociates the connection between the VSAN and virtual Fibre Channel interface. |

This example shows how to associate a virtual Fibre Channel interface to a VSAN:

```
switch# configure terminal
switch(config)# vsan database
switch(config-vsan)# vsan 2 interface vfc 4
```

# Verifying the Virtual Interface

To display configuration information about virtual interfaces, perform one of the following tasks:

| Command | Purpose |
|---|---|
| switch# **show interface vfc** *vfc-id* | Displays the detailed configuration of the specified Fibre Channel interface. |
| switch# **show interface brief** | Displays the status of all interfaces. |
| switch# **show vlan fcoe** | Displays the mapping of FCoE VLANs to VSANs. |

This example shows how to display a virtual Fibre Channel interface bound to an Ethernet interface:

```
switch# show interface vfc 3
vfc3 is up
    Bound interface is Ethernet1/37
    Hardware is Virtual Fibre Channel
    Port WWN is 20:02:00:0d:ec:6d:95:3f
    Admin port mode is F, trunk mode is on
    snmp link state traps are enabled
    Port mode is F, FCID is 0x490100
    Port vsan is 931
    1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
      0 frames output, 0 bytes
        0 discards, 0 errors
    Interface last changed at Thu May 21 04:44:42 2009
```

This example shows how to display a virtual Fibre Channel interface bound to a MAC address:

```
switch# show interface vfc 1001
vfc1001 is down
    Bound MAC is 00:0a:00:00:00:01
    Hardware is Virtual Fibre Channel
    Port WWN is 23:e8:00:0d:ec:6d:95:3f
    Admin port mode is F, trunk mode is on
    snmp link state traps are enabled
    Port vsan is 901
    1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
      0 frames output, 0 bytes
        0 discards, 0 errors
```

This example shows how to display the status of all the interfaces on the switch (some output has been removed for brevity):

```
switch# show interface brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc3/1      1      auto   on      trunking         swl    TE      2    --
fc3/2      1      auto   on      sfpAbsent        --     --           --
...
fc3/8      1      auto   on      sfpAbsent        --     --           --
--------------------------------------------------------------------------------
Interface                Status     IP Address        Speed    MTU   Port
                                                                    Channel
--------------------------------------------------------------------------------
Ethernet1/1              hwFailure  --                --       1500  --
Ethernet1/2              hwFailure  --                --       1500  --
Ethernet1/3              up         --                10000    1500  --
...
Ethernet1/39             sfpIsAbsen --                --       1500  --
Ethernet1/40             sfpIsAbsen --                --       1500  --
--------------------------------------------------------------------------------
Interface                Status     IP Address        Speed    MTU
--------------------------------------------------------------------------------
mgmt0                    up         172.16.24.41      100      1500
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
vfc 1        1      F      --      down             --     --           --
...
```

This example shows how to display the mapping between the VLANs and VSANs on the switch:

```
switch# show vlan fcoe
VLAN      VSAN      Status
--------  --------  --------
15        15        Operational
20        20        Operational
25        25        Operational
30        30        Non-operational
```

# Mapping VSANs to VLANs Example Configuration

The following example shows how to configure the FCoE VLAN and a virtual Fibre Channel interface:

## SUMMARY STEPS

1. Enable the associated VLAN and map the VLAN to a VSAN.
2. Configure the VLAN on a physical Ethernet interface.
3. Create a virtual Fibre Channel interface and bind it to a physical Ethernet interface.
4. Associate the virtual Fibre Channel interface to the VSAN.
5. (Optional) Display membership information for the VSAN.
6. (Optional) Display the interface information for the virtual Fibre Channel interface.

## DETAILED STEPS

**Step 1** Enable the associated VLAN and map the VLAN to a VSAN.

```
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
switch(config-vlan)# exit
```

**Step 2** Configure the VLAN on a physical Ethernet interface.

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# spanning-tree port type edge trunk
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1,200
switch(config-if)# exit
```

**Step 3** Create a virtual Fibre Channel interface and bind it to a physical Ethernet interface.

```
switch(config)# interface vfc 4
switch(config-if)# bind interface ethernet 1/4
switch(config-if)# exit
```

**Note** By default, all virtual Fibre Channel interfaces reside on VSAN 1. If the VLAN to VSAN mapping is to a VSAN other than VSAN 1, then proceed to Step 4.

**Step 4** Associate the virtual Fibre Channel interface to the VSAN.

```
switch(config)# vsan database
switch(config-vsan)# vsan 2 interface vfc 4
switch(config-vsan)# exit
```

**Step 5** (Optional) Display membership information for the VSAN.

```
switch# show vsan 2 membership
vsan 2 interfaces
            vfc 4
```

**Step 6** (Optional) Display the interface information for the virtual Fibre Channel interface.

```
switch# show interface vfc 4

vfc4 is up
Bound interface is Ethernet1/4
Hardware is Virtual Fibre Channel
Port WWN is 20:02:00:0d:ec:6d:95:3f
Port WWN is 20:02:00:0d:ec:6d:95:3f
```

```
snmp link state traps are enabled
Port WWN is 20:02:00:0d:ec:6d:95:3f
APort WWN is 20:02:00:0d:ec:6d:95:3f
snmp link state traps are enabled
Port mode is F, FCID is 0x490100
Port vsan is 931
1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
0 frames input, 0 bytes 0 discards, 0 errors
0 frames output, 0 bytes 0 discards, 0 errors
Interface last changed at Thu Mar 11 04:44:42 2010
```

# FCoE over Enhanced vPC

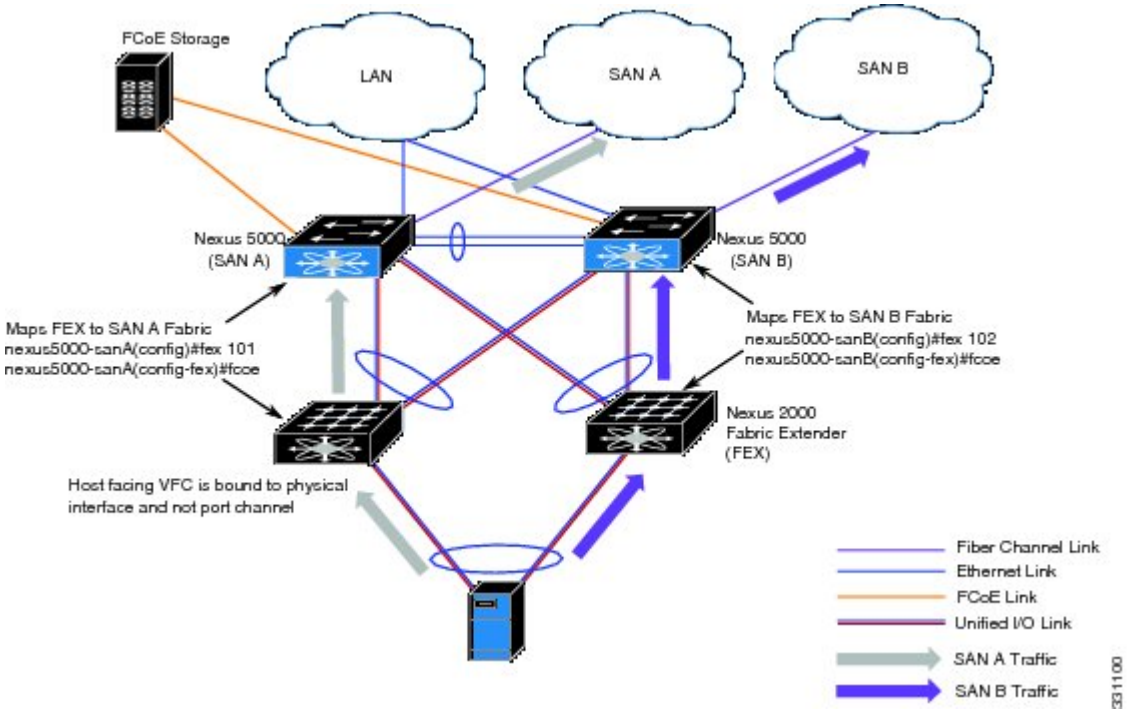
Although Ethernet traffic is dual homed between a FEX and a switch pair in an enhanced vPC topology, FCoE traffic must be single homed to maintain SAN isolation. Therefore, while enhanced vPC supports FCoE, a single homed FEX topology can be a better choice when SAN isolation and high FCoE bandwidth are required.

Consider the following disadvantages of enhanced vPC relative to a single homed topology:

- A typical SAN network maintains two fabrics, SAN A and SAN B, with traffic isolated between the two. In an enhanced vPC topology, each switch must be paired (single homed) with a FEX to ensure that FCoE traffic from one FEX is sent to only one switch, while Ethernet traffic is dual homed between each FEX and both switches. Because FCoE traffic from the FEX flows to only one switch while Ethernet traffic flows to both, the traffic load for the FEX uplinks is not evenly balanced.
- In a FEX with eight uplink ports, Ethernet traffic can use all eight ports, while the single homed FCoE traffic is limited by this topology to using only four of those ports, restricting the maximum bandwidth available for FCoE. As a further restriction, the default QoS template for the shared link allocates only half the link bandwidth to FCoE traffic, with the other half allocated to Ethernet traffic.
- In an enhanced vPC topology with FCoE, the host vPC is limited to two ports, one to each FEX.

The following network diagram shows the FCoE traffic flow in a system with two Nexus 2000 Fabric Extenders, each associated with a different Nexus 5000 switch.

***Figure 5: FCoE over Enhanced vPC***




# Configuring FCoE over Enhanced vPC

FCoE traffic must be single homed to maintain SAN isolation. You must first associate a FEX with only one switch. When the FEX and switch are associated, you can then create a virtual Fibre Channel (vFC) interface and bind it to a port.

After pairing the FEX and switch on the first peer, you repeat the configuration on the second peer using a different port number to ensure SAN traffic isolation. The different configuration will not cause a consistency error because the FCoE portion of the enhanced vPC configuration is not subject to the vPC consistency check.

## Before You Begin

Review the limitations in FCoE over Enhanced vPC, on page 29.

## SUMMARY STEPS

1. **configure terminal**
2. **fex** *fex-chassis_ID*
3. **fcoe**
4. **interface vfc** *vfc-id*
5. **bind interface ethernet** [*fex-chassis-ID*/]*slot*/*port*
6. **no shutdown**
7. (Optional) **end**
8. (Optional) **copy running-config startup-config**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config) #` | Enters global configuration mode. |
| **Step 2** | **fex** *fex-chassis_ID*<br><br>**Example:**<br>`switch(config) # fex 101`<br>`switch(config-fex) #` | Enters configuration mode for the specified FEX.<br>The range for *fex-chassis_ID* is 100 to 199. |
| **Step 3** | **fcoe**<br><br>**Example:**<br>`switch(config-fex) # fcoe`<br>`switch(config-fex) #` | Configures the FEX to send FCoE traffic only to this switch. |
| **Step 4** | **interface vfc** *vfc-id*<br><br>**Example:**<br>`switch(config-fex) # interface vfc 1`<br>`switch(config-if) #` | Enters configuration mode for the virtual Fibre Channel interface. If the interface does not already exist, this command also creates that interface.<br>The range of *vfc-id* is 1 to 8192. |
| **Step 5** | **bind interface ethernet** [*fex-chassis-ID*/]*slot*/*port*<br><br>**Example:**<br>`switch(config-if) # bind interface ethernet 101/1/1`<br>`switch(config-if) #` | Binds the vFC interface to the specified physical Ethernet interface.<br>The range for *fex-chassis_ID* is 100 to 199. For Cisco Nexus 5000 Platform, *slot* must be 1. For FCoE, the range for *port* is 1 to 32. |
| **Step 6** | **no shutdown**<br><br>**Example:**<br>`switch(config-if) # no shutdown`<br>`switch(config-if) #` | Returns the interface to its default operational state. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **end**<br><br>**Example:**<br>`switch(config-if) # end`<br>`switch#` | (Optional)<br>Return to privileged EXEC mode. |
| **Step 8** | **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config startup-config` | (Optional)<br>Copies the running configuration to the startup configuration. |

This example shows how to pair each FEX to a switch for FCoE traffic:

```
nexus5000-sanA# configure terminal
nexus5000-sanA(config) # fex 101
nexus5000-sanA(config-fex) # fcoe
nexus5000-sanA(config-fex) # interface vfc 1
nexus5000-sanA(config-if) # bind interface ethernet 101/1/1
nexus5000-sanA(config-if) #no shutdown
nexus5000-sanA(config-if) # end
nexus5000-sanA# copy running-config startup-config
nexus5000-sanA#

nexus5000-sanB# configure terminal
nexus5000-sanB(config) # fex 102
nexus5000-sanB(config-fex) # fcoe
nexus5000-sanB(config-fex) # interface vfc 1
nexus5000-sanB(config-if) # bind interface ethernet 102/1/1
nexus5000-sanB(config-if) #no shutdown
nexus5000-sanB(config-if) # end
nexus5000-sanB# copy running-config startup-config
nexus5000-sanB#
```

# SAN Boot with vPC

A Cisco Nexus Series switch can use SAN boot if the following conditions are met:

- The Cisco Nexus 2000 Series Fabric Extender (FEX) that contains the port assigned to the vPC must be associated with the Nexus switch.
- Only one VFC interface is bound to a vPC member. You cannot bind multiple interfaces to multiple members.

**Note** If you want to ensure backward compatibility for all previous configurations and supported topologies, you must configure the FEX in a straight-through FEX topology that does not use Enhanced vPC.

# SAN Boot with vPC Configuration Example

In this example, virtual Fibre Channel interface 1 is bound to physical Ethernet interface 101/1/1 on Fabric A and on interface 102/1/1 on Fabric B. The interface is also associated with virtual port channel 1 on both fabrics.

```
nexus5000-sanA(config) # interface vfc 1
nexus5000-sanA(config-if) # bind interface eth 101/1/1
nexus5000-sanA(config) # interface eth 101/1/1
nexus5000-sanA(config-if) # channel-group 1 mode active
nexus5000-sanA(config-if) # interface port-channel 1
nexus5000-sanA(config-if) # vpc 1
nexus5000-sanA(config-if) #

nexus5000-sanB(config) # interface vfc 1
nexus5000-sanB(config-if) # bind interface eth 102/1/1
nexus5000-sanB(config) # interface eth 102/1/1
nexus5000-sanB(config-if) # channel-group 1 mode active
nexus5000-sanB(config-if) # interface port-channel 1
nexus5000-sanB(config-if) # vpc 1
nexus5000-sanB(config-if) #
```

CHAPTER 5

# Configuring Cisco Adapter FEX with FCoE

This chapter contains the following sections:



## Overview

The Cisco Adapter FEX with FCoE feature allows you to create an FCoE connection to a Cisco Nexus 2000 Series Fabric Extender (FEX) which in turn can establish an FCoE connection to a server with a virtual interface card (VIC) adapter.

For example, you could use this feature to connect your Nexus switch to a Cisco UCS C-Series Rack-Mount Server containing a Cisco UCS P81E Virtual Interface Card, or you could connect it to a third-party server that has a Broadcom BCM57712 Convergence Network Interface Card (C-NIC) installed.

The switch connects to the FEX through a virtual port channel (vPC) while the FEX connects to the server using a standard FCoE link between the FEX and the VIC adapter.

## Guidelines and Limitations

If you are using Enhanced vPC, the FEX can be associated with one and only one Nexus 5000 fabric for FCoE forwarding.

If you are using FabricPath, you must use a dedicated link for FCoE traffic.

If you are using a Cisco UCS C-Series Rack-Mount Server with a Cisco UCS P81E Virtual Interface Card (VIC):

- The VIC must be configured in Network Interface Virtualization (NIV) mode, which makes the two unified ports appear to the system as virtual Host Bus Adapters (vHBAs).
- The VIC cannot be connected to the FEX through a VNP port. If this type of connection is used, NIV mode cannot be enabled on the VIC.
- The NIC mode on the Cisco UCS C-Series Rack-Mount Server must be set to **active-standby**.

# Configuring Cisco Adapter FEX with FCoE

## SUMMARY STEPS

1. **configure terminal**
2. **install feature-set virtualization**
3. **feature-set virtualization**
4. **fex** *fex-chassis-ID*
5. **fcoe**
6. **interface ethernet** [*fex-chassis-ID/*]*slot*/*port*
7. **switchport mode vntag**
8. **interface vethernet** *veth-id*
9. **bind interface ethernet** [*fex-chassis-ID/*]*slot*/*port* **channel** *channel-no*
10. **switchport mode {trunk|access}**
11. (Optional) **switchport trunk allowed vlan** *vlan-ID*
12. (Optional) **switchport access vlan** *vlan-ID*
13. **interface vfc** *vfc-id*
14. **bind interface vethernet** *veth-num*
15. **no shutdown**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config) #` | Enters global configuration mode. |
| **Step 2** | **install feature-set virtualization**<br><br>**Example:**<br>`switch(config) # install feature-set virtualization`<br>`switch(config) #` | Installs the virtualization feature set. |
| **Step 3** | **feature-set virtualization**<br><br>**Example:**<br>`switch(config) # feature-set virtualization`<br>`switch(config)#` | Enables the virtualization feature. |
| **Step 4** | **fex** *fex-chassis-ID*<br><br>**Example:**<br>`switch(config) # fex 101`<br>`switch(config-fex) #` | Enters configuration mode for the specified FEX.<br>The range for *fex-chassis_ID* is 100 to 199. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **fcoe**<br><br>**Example:**<br>`switch(config-fex) # fcoe`<br>`switch(config-fex) #` | Enables Fibre Channel over Ethernet traffic on the FEX. |
| **Step 6** | **interface ethernet** [*fex-chassis-ID*/]*slot*/*port*<br><br>**Example:**<br>`switch(config-fex) # interface ethernet 101/1/1`<br>`switch(config-if) #` | Enters configuration mode for the specified Ethernet interface.<br>The range for *fex-chassis_ID* is 100 to 199. For Cisco Nexus 5000 Platform, *slot* must be 1. For FCoE, the range for *port* is 1 to 32. |
| **Step 7** | **switchport mode vntag**<br><br>**Example:**<br>`switch(config-if) # switchport mode vntag`<br>`switch(config-if) #` | Configures the interface in port mode. |
| **Step 8** | **interface vethernet** *veth-id*<br><br>**Example:**<br>`switch(config-if) # interface vethernet 2`<br>`switch(config-if) #` | Creates a virtual Ethernet interface and enters configuration mode for that interface.<br>The range of *veth-id* is from 1 to 1,048,575.<br>**Note** If you have two Cisco Nexus Series switches configured for redundancy, the virtual Ethernet interface ID must be unique on each switch. |
| **Step 9** | **bind interface ethernet** [*fex-chassis-ID*/]*slot*/*port* **channel** *channel-no*<br><br>**Example:**<br>`switch(config-if) # bind interface ethernet 101/1/1 channel 1`<br>`switch(config-if) #` | Binds the specified Ethernet interface to the specified port channel.<br>The range for *fex-chassis_ID* is 100 to 199. For Cisco Nexus 5000 Platform, *slot* must be 1. For FCoE, the range for *port* is 1 to 32. The range for *channel-no* is from 1 to 4096. |
| **Step 10** | **switchport mode {trunk\|access}**<br><br>**Example:**<br>`switch(config-if) # switchport mode trunk`<br>`switch(config-if) #` | Configures the interface as a trunk port or an access port. |
| **Step 11** | **switchport trunk allowed vlan** *vlan-ID*<br><br>**Example:**<br>`switch(config-if) # switchport trunk allowed vlan 33`<br>`switch(config-if) #` | (Optional)<br>If you configured the interface as a trunk port, use this command to specify the VLAN for FCoE traffic.<br>The range for *vlan-ID* is from 1 to 4094, except for the VLANs reserved for internal use. |
| **Step 12** | **switchport access vlan** *vlan-ID*<br><br>**Example:**<br>`switch(config-if) # switchport access vlan 33`<br>`switch(config-if) #` | (Optional)<br>If you configured the interface as an access port, use this command to specify the VLAN for FCoE traffic. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **interface vfc** *vfc-id*<br><br>**Example:**<br>`switch(config-if) # interface vfc 4`<br>`switch(config-if) #` | Creates a virtual Fibre Channel interface on the switch and enters configuration mode.<br><br>The range of *vfc-id* is from 1 to 8192. |
| **Step 14** | **bind interface vethernet** *veth-num*<br><br>**Example:**<br>`switch(config-if) # bind interface veth 2`<br>`switch(config-if) #` | Binds the virtual Fibre Channel interface to the specified virtual Ethernet interface.<br><br>The range of *veth-num* is from 1 to 1048575. |
| **Step 15** | **no shutdown**<br><br>**Example:**<br>`switch(config-if) # no shutdown`<br>`switch(config-if) #` | Returns the interface to its default operational state. |

This example configures Cisco Adapter FEX with FCoE on SAN fabric A using FEX 101 and the Ethernet interface on channel 1 configured as a trunk port.

```
nexus5000-sanA(config)#configure terminal
nexus5000-sanA(config)#install feature-set virtualization
nexus5000-sanA(config)#feature-set virtualization
nexus5000-sanA(config)#fex 101
nexus5000-sanA(config-fex)#fcoe
nexus5000-sanA(config-fex)#interface ethernet 101/1/1
nexus5000-sanA(config-if)#switchport mode vntag
nexus5000-sanA(config-if)#interface veth 2
nexus5000-sanA(config-if)#bind interface eth 101/1/1 channel 1
nexus5000-sanA(config-if)#switchport mode trunk
nexus5000-sanA(config-if)#switchport trunk allowed vlan 33
nexus5000-sanA(config-if)#interface vfc 4
nexus5000-sanA(config-if)#bind interface veth 2
nexus5000-sanA(config-if)#no shutdown
```

This example configures Cisco Adapter FEX with FCoE on SAN fabric B using FEX 102 and Ethernet interface on channel 2 configured as an access port.

```
nexus5000-sanB(config)#configure terminal
nexus5000-sanB(config)#install feature-set virtualization
nexus5000-sanB(config)#feature-set virtualization
nexus5000-sanB(config)#fex 102
nexus5000-sanB(config-fex)#fcoe
nexus5000-sanB(config-fex)#interface ethernet 102/1/1
nexus5000-sanB(config-if)#switchport mode vntag
nexus5000-sanB(config-if)#interface veth 5
nexus5000-sanB(config-if)#bind interface eth 102/1/1 channel 2
nexus5000-sanB(config-if)#switchport mode access
nexus5000-sanB(config-if)#switchport access vlan 40
nexus5000-sanB(config-if)#interface vfc 6
nexus5000-sanB(config-if)#bind interface veth 5
nexus5000-sanB(config-if)#no shutdown
```