



# Overview

---

This chapter provides an architectural overview of the Cisco Nexus 2000 Series Fabric Extender and includes the following sections:

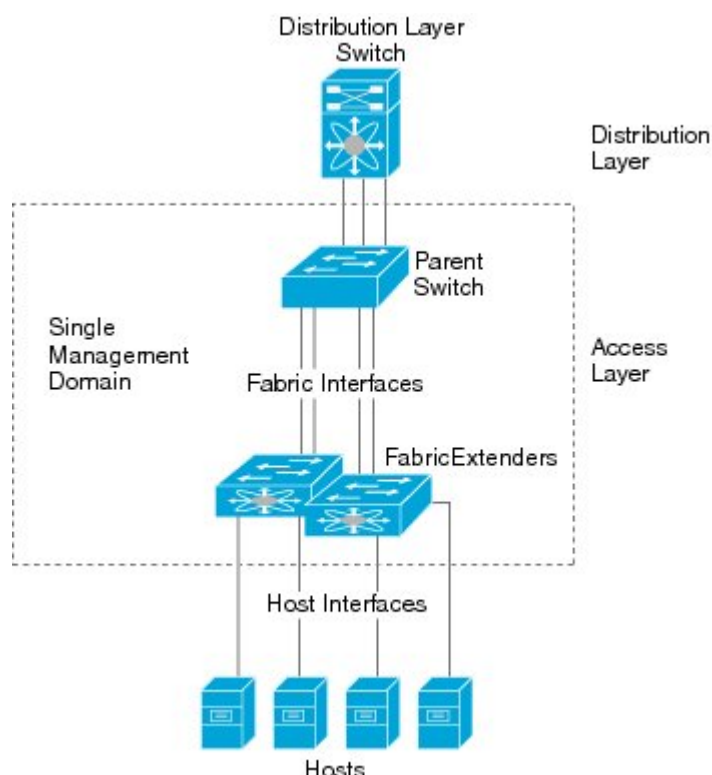
- [About the Cisco Nexus 2000 Series Fabric Extender, page 2](#)
- [Fabric Extender Terminology, page 3](#)
- [Fabric Interface Features , page 3](#)
- [Host Interfaces, page 4](#)
- [Host Interface Port Channels, page 5](#)
- [VLANs, page 5](#)
- [Protocol Offload, page 6](#)
- [Quality of Service, page 6](#)
- [Access Control Lists, page 6](#)
- [IGMP Snooping, page 6](#)
- [Switched Port Analyzer, page 6](#)
- [Oversubscription, page 7](#)
- [Management Model, page 7](#)
- [Forwarding Model, page 8](#)
- [Port Channel Fabric Interface Connection, page 9](#)
- [Port Numbering Convention, page 9](#)
- [Fabric Extender Image Management, page 10](#)
- [Licensing Requirements for the Fabric Extender, page 10](#)
- [Guidelines and Limitations, page 10](#)
- [Default Settings, page 11](#)

## About the Cisco Nexus 2000 Series Fabric Extender

The Cisco Nexus 2000 Series Fabric Extender is a highly scalable and flexible server networking solution that works with Cisco Nexus 7000 Series devices to provide high-density, low-cost connectivity for server aggregation. Scaling across 1-Gigabit Ethernet, 10-Gigabit Ethernet, unified fabric, rack, and blade server environments, the Fabric Extender is designed to simplify data center architecture and operations.

The Fabric Extender integrates with its parent switch, a Cisco Nexus 7000 Series device, to allow automatic provisioning and configuration taken from the settings on the parent switch. This integration allows large numbers of servers and hosts to be supported using the same feature set as the parent switch, including security and quality-of-service (QoS) configuration parameters, with a single management domain as shown in the following figure. The Fabric Extender and its parent switch enable a large multi-path, loop-free, active-active data center topology without the use of Spanning Tree Protocol (STP).

**Figure 1: Single Management Domain**



The Cisco Nexus 2000 Series Fabric Extender forwards all traffic to its parent Cisco Nexus 7000 Series device over 10-Gigabit Ethernet fabric uplinks, allowing all traffic to be inspected by policies established on the Cisco Nexus 7000 Series device.



### Note

The Fabric Extender must be connected to a parent Cisco Nexus 7000 Series device equipped with a 32-port 10-Gigabit M1 module (N7K-M132XP-12) and/or a 32-port 10-Gigabit M1 XL module (N7K-M132XP-12L).

No software is included with the Fabric Extender. Software is automatically downloaded and upgraded from its parent switch.

## Fabric Extender Terminology

Some terms used in this document are as follows:

- Fabric interface—A 10-Gigabit Ethernet uplink port designated for connection from the Fabric Extender to its parent switch. A fabric interface cannot be used for any other purpose. It must be directly connected to the parent switch.



---

**Note**

A fabric interface includes the corresponding interface on the parent switch. This interface is enabled when you enter the **switchport mode fex-fabric** command.

---

- Port channel fabric interface—A port channel uplink connection from the Fabric Extender to its parent switch. This connection consists of fabric interfaces bundled into a single logical channel.
- Host interface—An Ethernet host interface for connection to a server or host system.



---

**Note**

Do not connect a bridge or switch to a host interface. These interfaces are designed to provide end host or server connectivity.

---

- Port channel host interface—A port channel host interface for connection to a server or host system.

## Fabric Interface Features

The FEX fabric interfaces support static port channels. During the initial discovery and association process, SFP+ validation and digital optical monitoring (DOM) are performed as follows:

The FEX fabric interfaces support static port channels. During the initial discovery and association process, SFP+ validation and digital optical monitoring (DOM) are performed as follows:

- The FEX performs a local check on the uplink SFP+ transceiver. If it fails the security check, the LED flashes but the link is still allowed to come up.
- The FEX local check is bypassed if it is running its backup image.
- The parent switch performs SFP validation again when the fabric interface is brought up. It keeps the fabric interface down if SFP validation fails.

Once an interface on the parent switch is configured in fex-fabric mode, all other features that were configured on that port and are not relevant to this mode are deactivated. If the interface is reconfigured to remove fex-fabric mode, the previous configurations are reactivated.

# Host Interfaces

## Layer 3 Host Interfaces

Beginning in NX-OS Release 5.2, by default, all host interfaces on a Fabric Extender connected to a Cisco Nexus 7000 Series parent switch run in Layer 3 mode.

**Note**

If you have updated the parent switch to Cisco Nexus Release 5.2, previously configured Fabric Extender host interfaces will retain their default port mode, Layer 2. You can change these ports to Layer 3 mode with the **no switchport** command.

The host interfaces also support subinterfaces. You can create up to 32 subinterfaces on a Fabric Extender host interface.

For information about interfaces and subinterfaces, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*.

## Layer 2 Host Interfaces

In NX-OS Release 5.1 and earlier releases, the default port mode is Layer 2.

To run a host interface in Layer 2 mode, use the **switchport** command. For NX-OS Release 5.2 and later releases, to change the port mode to Layer 3, use the **no switchport** command.

The Fabric Extender provides connectivity for computer hosts and other edge devices in the network fabric. The following guidelines should be followed when connecting devices to Fabric Extender host interfaces:

- All Fabric Extender host interfaces run as spanning tree edge ports with BPDU Guard enabled and cannot be configured as Spanning Tree network ports.
- Servers utilizing active/standby teaming, 802.3ad port channels, or other host-based link redundancy mechanisms can be connected to Fabric Extender host interfaces.
- Any device running spanning tree connected to a Fabric Extender host interface will result in that host interface being placed in an error-disabled state when a BPDU is received.
- Any edge switch that leverages a link redundancy mechanism not dependent on Spanning Tree such as Cisco Flexlink or vPC (with BPDUFilter enabled) may be connected to a Fabric Extender host interface. Since spanning tree is not utilized to eliminate loops, care must be taken to ensure a loop-free topology below the Fabric Extender host interfaces.

Ingress and egress packet counters are provided on each host interface.

For more information about BPDU Guard, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*.

# Host Interface Port Channels

## Layer 3 Host Interface Port Channels

The Fabric Extender supports host interface port channel configurations. Up to eight interfaces can be combined in a standard mode port channel and 16 interfaces when configured with the Link Aggregation Control Protocol (LACP).

**Note**

Port channel resources are allocated when the port channel has one or more members.

All members of the port channel must be Fabric Extender host interfaces and all host interfaces must be from the same Fabric Extender. You also cannot mix interfaces from the Fabric Extender and the parent switch.

Layer 3 mode is supported on host interface port channels.

A host interface port channel also support subinterfaces. You can create up to 1000 subinterfaces on a Fabric Extender host interface port channel.

For more information about port channels, see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*.

## Layer 2 Host Interface Port Channels

The FEX supports host interface port channel configurations. Up to eight interfaces can be combined in a standard mode port channel and 16 interfaces when configured with the Link Aggregation Control Protocol (LACP).

**Note**

Port channel resources are allocated when the port channel has one or more members.

All members of the port channel must be Fabric Extender host interfaces and all host interfaces must be from the same Fabric Extender. You also cannot mix interfaces from the Fabric Extender and the parent switch.

Layer 2 mode is supported on host interface port channels.

Layer 2 port channels can be configured as access or trunk ports.

Beginning with NX-OS Release 5.2(1), Fabric Extenders support the host vPC feature where a server can be dual-attached to two different FEXs through a port channel. Parent switches connecting each FEX (one parent switch per FEX) must be configured in a vPC domain.

## VLANs

The Fabric Extender supports Layer 2 VLAN trunks and IEEE 802.1Q VLAN encapsulation.

For more information about VLANs, see the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*.

## Protocol Offload

To reduce the load on the control plane of the Cisco Nexus 7000 Series device, Cisco NX-OS provides the ability to offload link-level protocol processing to the Fabric Extender CPU. The following protocols are supported:

- Link Layer Discovery Protocol (LLDP)
- Link Aggregation Control Protocol (LACP)

## Quality of Service

The Fabric Extender uses IEEE 802.1p class of service (CoS) values to associate traffic with the appropriate class. Per-port QoS configuration is also supported.

Host interfaces support pause frames, which are implemented using IEEE 802.3x link-level flow control (LLC). By default, flow control send is on and flow control receive is off on all host interfaces. Autonegotiation is enabled on the host interfaces. Per-class flow control is set according to the QoS classes.

For more information about LLC and quality-of-service, see the *Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x*.

## Access Control Lists

The Fabric Extender supports the full range of ingress access control lists (ACLs) that are available on its parent Cisco Nexus 7000 Series device.

For more information about ACLs, see the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*.

## IGMP Snooping

IGMP snooping is supported on all host interfaces of the Fabric Extender.

The Fabric Extender and its parent switch support IGMPv2 and IGMPv3 snooping based only on the destination multicast MAC address. It does not support snooping based on the source MAC address or on proxy reports.

**Note**

For more information about IGMP snooping, see <http://tools.ietf.org/wg/magma/draft-ietf-magma-snoop/rfc4541.txt>. Also, see the *Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x*.

## Switched Port Analyzer

You can configure the host interfaces on the Fabric Extender as Switched Port Analyzer (SPAN) source ports. Fabric Extender ports cannot be configured as a SPAN destination. Only one SPAN session is supported for

all the host interfaces on the same Fabric Extender. Ingress source (Rx), egress source (Tx), or both ingress and egress monitoring are supported.

**Note**

All IP multicast traffic on the set of VLANs that a Fabric Extender host interface belongs to is captured in the SPAN session. You cannot separate the traffic by IP multicast group membership.

If ingress monitoring and egress monitoring is configured for host interfaces on the same Fabric Extender, you might see a packet twice: once as the packet ingresses on an interface with Rx configured, and again as the packet egresses on an interface with Tx configured.

For more information about SPAN, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*

## Oversubscription

In a switching environment, oversubscription is the practice of connecting multiple devices to the same interface to optimize port usage. An interface can support a connection that runs at its maximum speed. Because most interfaces do not run at their maximum speeds, you can take advantage of unused bandwidth by sharing ports. In the case of the Cisco Nexus 2000 Series Fabric Extender, oversubscription, which is a function of the available fabric interfaces to active host interfaces, provides cost-effective scalability and flexibility for Ethernet environments.

The Cisco Nexus 2248TP Fabric Extender has four 10-Gigabit Ethernet fabric interfaces and 48 100/1000BASE-T (100-Mb/1-Gigabit) Ethernet host interfaces. It offers the following configurations when its host interfaces are running in Gigabit Ethernet mode:

- No oversubscription (40 host interfaces for four fabric interfaces)
- 1.2 to 1 oversubscription (48 host interfaces for four fabric interfaces)
- 4.8 to 1 oversubscription (48 host interfaces for one fabric interface)

The Cisco Nexus 2248TP can be run with no oversubscription when its host interfaces are running in 100-Mb mode.

The Cisco Nexus 2232PP Fabric Extender has eight 10-Gigabit Ethernet fabric interfaces and 32 10-Gigabit Ethernet host interfaces. With this system, you can configure a 4 to 1 oversubscription (4 host interfaces for one fabric interface) or higher.

The Cisco Nexus 2224PP Fabric Extender has two 10-Gigabit Ethernet fabric interfaces and 24 100/1000BASE-T (100-Mb/1-Gigabit) Ethernet host interfaces. With this system, you can configure a 1.2 to 1 oversubscription (24 host interfaces for two fabric interfaces) or higher.

## Management Model

The Cisco Nexus 2000 Series Fabric Extender is managed by its parent switch over the fabric interfaces through a zero-touch configuration model. The switch discovers the Fabric Extender by detecting the fabric interfaces of the Fabric Extender.

After discovery, if the Fabric Extender has been correctly associated with the parent switch, the following operations are performed:

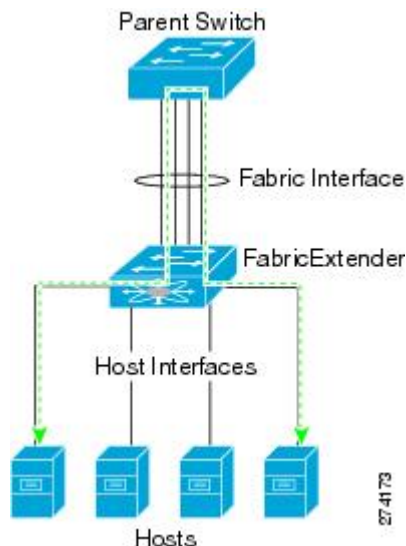
- 1 The switch checks the software image compatibility and upgrades the Fabric Extender if necessary.

- 2 The switch and Fabric Extender establish in-band IP connectivity with each other. The switch assigns an IP address in the range of loopback addresses (127.15.1.0/24) to the Fabric Extender to avoid conflicts with IP addresses that might be in use on the network.
- 3 The switch pushes the configuration data to the Fabric Extender. The Fabric Extender does not store any configuration locally.
- 4 The Fabric Extender updates the switch with its operational status. All Fabric Extender information is displayed using the switch commands for monitoring and troubleshooting.

## Forwarding Model

The Cisco Nexus 2000 Series Fabric Extender does not perform any local switching. All traffic is sent to the parent switch that provides central forwarding and policy enforcement, including host-to-host communications between two systems that are connected to the same Fabric Extender as shown in the following figure.

**Figure 2: Forwarding Model**



The forwarding model facilitates feature consistency between the Fabric Extender and its parent Cisco Nexus 7000 Series device.



### Note

The Fabric Extender provides end-host connectivity into the network fabric. As a result, BPDU Guard is enabled on all its host interfaces. If you connect a bridge or switch to a host interface, that interface is placed in an error-disabled state when a BPDU is received.

You cannot disable BPDU Guard on the host interfaces of the Fabric Extender.

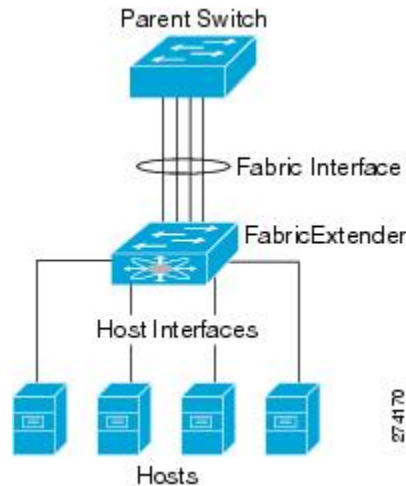
The Fabric Extender supports egress multicast replication from the network to the host. Packets sent from the parent switch for multicast addresses attached to the Fabric Extender are replicated by the Fabric Extender ASICs and then sent to corresponding hosts.



# Port Channel Fabric Interface Connection

To provide load balancing between the host interfaces and the parent switch, you can configure the Fabric Extender to use a port channel fabric interface connection. This connection bundles 10-Gigabit Ethernet fabric interfaces into a single logical channel as shown in the following figure.

**Figure 3: Port Channel Fabric Interface Connection**



When you configure the Fabric Extender to use a port channel fabric interface connection to its parent switch, the switch load balances the traffic from the hosts that are connected to the host interface ports by using the following load-balancing criteria to select the link:

- For a Layer 2 frame, the switch uses the source and destination MAC addresses.
- For a Layer 3 frame, the switch uses the source and destination MAC addresses and the source and destination IP addresses.



## Note

A fabric interface that fails in the port channel does not trigger a change to the host interfaces. Traffic is automatically redistributed across the remaining links in the port channel fabric interface. If all links in the fabric port channel go down, all host interfaces on the FEX are set to the down state.

## Port Numbering Convention

The following port numbering convention is used for the Fabric Extender:

**interface ethernet** *chassis/slot/port*

where

- *chassis* is configured by the administrator. A Fabric Extender must be directly connected to its parent Cisco Nexus 7000 Series device via a port channel fabric interface. You configure a chassis ID on a port channel on the switch to identify the Fabric Extender that is discovered through those interfaces.

The chassis ID ranges from 101 to 199.



**Note** The chassis ID is required only to access a host interface on the Fabric Extender. A value of less than 101 indicates a slot on the parent switch. The following port numbering convention is used for the interfaces on the switch:

**interface ethernet** *slot/port*

- *slot* identifies the slot number on the Fabric Extender.
- *port* identifies the port number on a specific slot and chassis ID.

## Fabric Extender Image Management

No software ships with the Cisco Nexus 2000 Series Fabric Extender. The Fabric Extender image is bundled into the system image of the parent device. The image is automatically verified and updated (if required) during the association process between the parent device and the Fabric Extender.

When you enter the **install all** command, it upgrades the software on the parent Cisco Nexus 7000 Series device and also upgrades the software on any attached Fabric Extender. To minimize downtime as much as possible, the Fabric Extender remains online while the installation process loads its new software image. Once the software image has successfully loaded, the FEX performs a nondisruptive upgrade.

This process is required to maintain version compatibility between the parent device and the Fabric Extender.

## Licensing Requirements for the Fabric Extender

The following table shows the licensing requirements for the Cisco Nexus 2000 Series Fabric Extender:

Product	License Requirement
Cisco NX-OS	The Cisco Nexus 2000 Series Fabric Extender requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For an explanation of the licensing scheme, see the <i>Cisco NX-OS Licensing Configuration Guide</i> .

## Guidelines and Limitations

The Cisco Nexus 2000 Series Fabric Extender has the following configuration guidelines and limitations:

- Beginning with NX-OS Release 5.2(1), the default port mode is Layer 3. Before NX-OS Release 5.2(1), the default port mode was Layer 2.
- You must install the Fabric Extender feature set in the default virtual device context (VDC) before you can enable the Fabric Extender in any VDC (including the default VDC).

- You must connect the Fabric Extender to its parent Cisco Nexus 7000 Series device equipped with a 32-port 10-Gigabit M1 module (N7K-M132XP-12) and/or a 32-port 10-Gigabit M1-XL module (N7K-M132XP-12L).
- The Fabric Extender feature set operation may cause the standby supervisor to reload if it is in an unstable state, such as following a service failure or powering up. You can check whether the standby supervisor is stable with the **show modules** command. When the standby supervisor is stable, it is indicated as "ha-standby".
- You can configure the Fabric Extender host interfaces as edge ports only. The interface is placed in an error disabled state if a downstream switch is detected.

## Configuration Limits

The following configuration limits apply to Fabric Extenders configured with Cisco Nexus 7000 Series switches:

- The maximum number of Fabric Extenders that can be configured with a single Cisco Nexus 7000 Series switch is 32.
- The maximum number of physical Fabric Extender Layer 3 subinterfaces is 32.
- The maximum number of Fabric Extender Layer 3 port channel subinterfaces is 1000.

## Default Settings

This table lists the default settings for the Fabric Extender parameters.

**Table 1: Default Cisco Nexus 2000 Series Fabric Extender Parameter Settings**

Parameters	Default
<b>feature-set fex</b> command	Disabled
Port mode	Layer 3 (NX-OS Release 5.2 and later releases). Layer 2 (NX-OS Release 5.1 and earlier releases).

