



CHAPTER 3

FabricPath Interfaces

This chapter describes how to configure the FabricPath interfaces on the Cisco NX-OS devices.

This chapter includes the following sections:

- [Information About FabricPath Interfaces, page 3-1](#)
- [Licensing Requirements for FabricPath Interfaces, page 3-7](#)
- [Prerequisites for FabricPath Interfaces, page 3-7](#)
- [Guidelines and Limitations for FabricPath Interfaces, page 3-8](#)
- [Configuring FabricPath Interfaces, page 3-8](#)
- [Verifying FabricPath Interface Configuration, page 3-15](#)
- [Displaying FabricPath Interface Statistics, page 3-16](#)
- [FabricPath Interface Example Configuration, page 3-16](#)
- [Feature History for Configuring FabricPath Using the CLI, page 3-18](#)

Information About FabricPath Interfaces

This section includes the following sections:

- [FabricPath Interfaces, page 3-2](#)
- [STP and the FabricPath Network, page 3-2](#)
- [vPC+, page 3-4](#)
- [High Availability, page 3-6](#)
- [Virtual Device Contexts, page 3-6](#)



Note

You must have an F Series module installed in the Cisco Nexus 7000 Series device to run FabricPath.

Send document comments to nexus7k-docfeedback@cisco.com

FabricPath Interfaces

After you enable FabricPath on the devices that you are using, you can configure an Ethernet interface or a port-channel interface as a FabricPath interface. If one member of the port channel is in FabricPath mode, all the other members will be in FabricPath mode. After you configure the interface as a FabricPath interface, it automatically becomes a trunk port, capable of carrying traffic for multiple VLANs. You can also configure all the ports on the F Series module as FabricPath interfaces simultaneously.

The following interface modes carry traffic for the following types of VLANs:

- Interfaces on the F Series modules that are configured as FabricPath interfaces can carry traffic only for FP VLANs.
- Interfaces on the F Series modules that are not configured as FabricPath interfaces carry traffic for the following:
 - FP VLANs
 - Classical Ethernet (CE) VLANs
- Interfaces on the M Series modules carry traffic only for CE VLANs.

**Note**

See [Chapter 4, “FabricPath Forwarding”](#) for information about FP and CE VLANs.

The FabricPath interfaces connect only to other FabricPath interfaces within the FabricPath network. These FabricPath ports operate on the information in the FabricPath headers and Layer 2 Intermediate System-to-Intermediate System (IS-IS) only, and they do not run STP. These ports are aware only of FP VLANs; they are unaware of any CE VLANs. By default, all VLANs are allowed on a trunk port, so the FabricPath interface carries traffic for all FP VLANs.

**Note**

You cannot configure FabricPath interfaces as shared interfaces. See *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on shared interfaces.

STP and the FabricPath Network

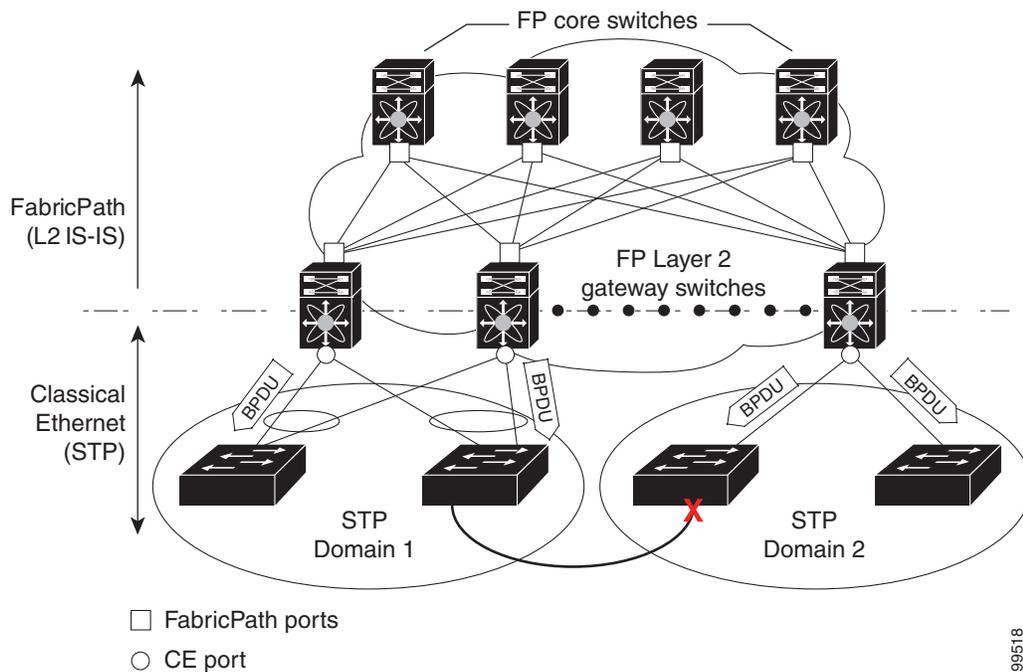
**Note**

The Layer 2 gateway switches, which are on the edge between the CE and the FabricPath network, must be the root for all STP domains that are connected to a FabricPath network.

The Spanning Tree Protocol (STP) domains do not cross into the FabricPath network (see [Figure 3-1](#)).

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Figure 3-1 STP Boundary Termination at FabricPath Network Border



You must configure the FabricPath Layer 2 gateway device to have the lowest STP priority of all the devices in the STP domain to which it is attached. You must also configure all the FabricPath Layer 2 gateway devices connected to one FabricPath network to have the *same* priority. The system assigns the bridge ID for the Layer 2 gateway devices from a pool of reserved MAC addresses.

To have a loop-free topology for the CE/FabricPath hybrid network, the FabricPath network automatically displays as a single bridge to all connected CE devices.



Note

You must set the STP priority on all FabricPath Layer 2 gateway switches to a value low enough to ensure that they become root for any attached STP domains.

Other than configuring the STP priority on the FabricPath Layer 2 gateway switches, you do not need to configure anything for the STP to work seamlessly with the FabricPath network. Only connected CE devices form a single STP domain. Those CE devices that are not interconnected form separate STP domains (see [Figure 3-1](#)).

All CE interfaces should be designated ports, which occurs automatically, or they are pruned from the active STP topology. If the system does prune any port, the system returns a syslog message. The system clears the port again only when that port is no longer receiving superior BPDUs.

The FabricPath Layer 2 gateway switch also propagates the Topology Change Notifications (TCNs) on all its CE interfaces.

The FabricPath Layer 2 gateway switches terminate STP. The set of FabricPath Layer 2 gateway switches that are connected by STP forms the STP domain. Because there can be many FabricPath Layer 2 gateway switches attached to a single FabricPath network, there may also be many separate STP domains (see [Figure 3-1](#)). The devices in the separate STP domains need to know the TCN information only for the domain to which they belong. You can configure a unique STP domain ID for each separate STP

Send document comments to nexus7k-docfeedback@cisco.com

domain that connects to the same FabricPath network. The Layer 2 IS-IS messages carry the TCNs across the FabricPath network. Only those FabricPath Layer 2 gateway switches in the same STP domain as the TCN message need to act and propagate the message to connected CE devices.

When a FabricPath Layer 2 gateway switch receives a TCN for the STP domain it is part of, it takes the following actions:

- Flushes all remote MAC addresses for that STP domain and the MAC addresses on the designated port.
- Propagates the TCN to the other devices in the specified STP domain.

The devices in the separate STP domains need to receive the TCN information and then flush all remote MAC addresses reachable by the STP domain that generated the TCN information.

vPC+

A virtual port channel+ (vPC+) domain allows a classical Ethernet (CE) vPC domain and a Cisco FabricPath cloud to interoperate. A vPC+ also provides a First Hop Routing Protocol (FHRP) active-active capability at the FabricPath to Layer 3 boundary.



Note

vPC+ is an extension to virtual port channels (vPCs) that run CE only (see the “Configuring vPCs” chapter in the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*). You cannot configure a vPC+ domain and a vPC domain on the same Cisco Nexus 7000 Series device.

A vPC+ domain enables Cisco Nexus 7000 Series enabled with FabricPath devices to form a single vPC+, which is a unique virtual switch to the rest of the FabricPath network. You configure the same domain on each device to enable the peers to identify each other and to form the vPC+. Each vPC+ has its own virtual switch ID.



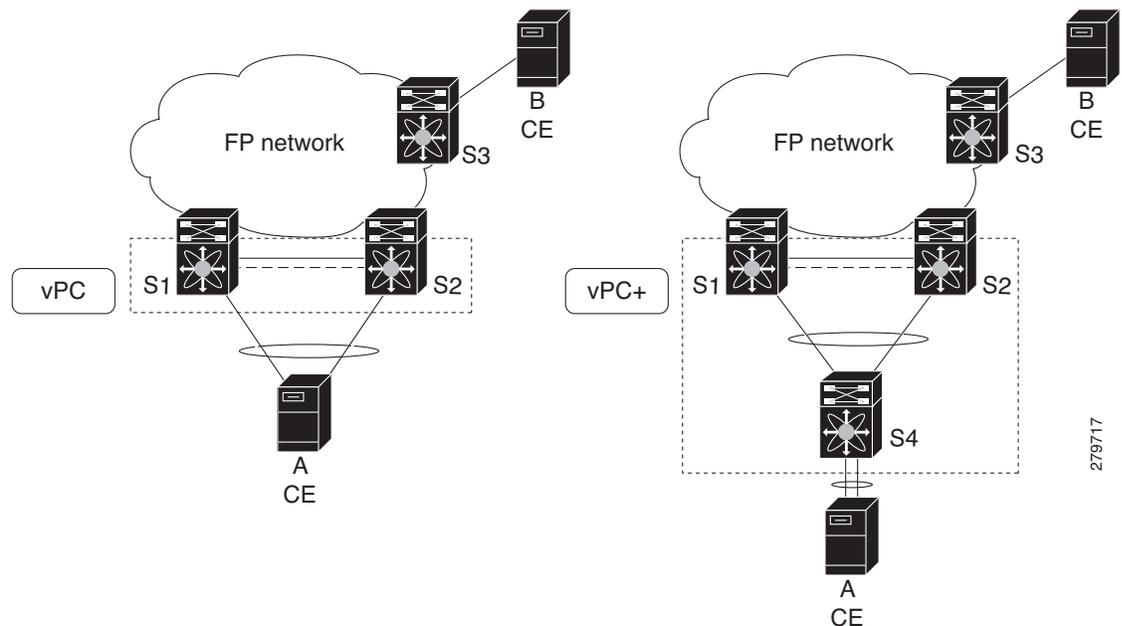
Note

We do not recommend enabling the vPC peer switch feature when you are using vPC+.

A vPC+ must still provide active-active Layer 2 paths for dual-homed CE devices or clouds, even though the FabricPath network allows only 1-to-1 mapping between the MAC address and the switch ID. vPC+ provides the solution by creating a unique virtual switch to the FabricPath network (see [Figure 3-2](#)).

Send document comments to nexus7k-docfeedback@cisco.com

Figure 3-2 vPC/vPC+



The FabricPath switch ID for the virtual switch becomes the outer source MAC address (OSA) in the FabricPath encapsulation header. Each vPC+ domain must have its own virtual switch ID.

Layer 2 multipathing is achieved by emulating a single virtual switch. Packets forwarded from host A to host B are tagged with the MAC address of the virtual switch as the transit source, and traffic from host B to host A is now load balanced.

You must have all interfaces in the vPC+ peer link as well as all the downstream vPC+ links on an F Series module with FabricPath enabled. The vPC+ downstream links will be FabricPath edge interfaces, which connect to the CE hosts.

The vPC+ virtual switch ID is used to assign the FabricPath Outer Source Address (OSA) to the FabricPath vPC+ peer devices (see [Chapter 2, “Configuring FabricPath Switching”](#), for information on FabricPath encapsulation). You must assign the same switch ID to each of the two vPC+ peer devices so the peer link can form.

The F1 Series modules have only Layer 2 interfaces. To use routing with a vPC+, you must have an M Series module inserted into the same Cisco Nexus 7000 Series chassis. The system then performs proxy routing using both the N7K-F132-15 module and the M Series modules in the chassis (see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x* for information on proxy routing with the F1 Series modules).

The First Hop Routing Protocols (FHRP) and the Hot Standby Routing Protocol (HSRP) interoperate with a vPC+. You should dual-attach all Layer 3 devices to both vPC+ peer devices.



Note

You must enable the Layer 3 connectivity from each vPC+ peer device by configuring a VLAN network interface for the same VLAN from both devices.

The primary FHRP device responds to ARP requests, even though the secondary vPC+ device also forwards the data traffic. Both the primary and secondary vPC+ devices forward traffic, but only the primary FHRP device responds to ARP requests.

Send document comments to nexus7k-docfeedback@cisco.com

To simplify initial configuration verification and vPC+/HSRP troubleshooting, you can configure the primary vPC+ peer device with the FHRP active router highest priority.

In addition, you can use the priority command in the if-hsrp configuration mode to configure failover thresholds for when a group state enabled on a vPC+ peer is in standby or in listen state. You can configure lower and upper thresholds to prevent the group state flap, if there is an interface flap (this feature is useful when there is more than one tracking object per group).

When the primary vPC+ peer device fails over to the secondary vPC+ peer device, the FHRP traffic continues to flow seamlessly.

You should configure a separate Layer 3 link for routing from the vPC+ peer devices, rather than using a VLAN network interface for this purpose.

We do not recommend that you configure the burnt-in MAC address option (use-bia) for hot standby router protocol HSRP or manually configure virtual MAC addresses for any FHRP protocol in a vPC+ environment because these configurations can adversely affect the vPC+ load balancing. The HSRP use-bia is not supported with a vPC+. When you are configuring custom MAC addresses, you must configure the same MAC address on both vPC+ peer devices.

You can configure a restore timer that delays the vPC+ coming back up until after the peer adjacency forms and the VLAN interfaces are back up. This feature allows you to avoid packet drops if the routing tables do not converge before the vPC+ is once again passing traffic.

Use the **delay restore** command to configure this feature.



Note

If a data center outage occurs and you enable HSRP before the vPC+ successfully comes up, traffic loss can occur. You need to enable an HSRP delay to give the vPC time to stabilize. If you enable both an HSRP delay and a preemption delay, the Cisco Nexus 7000 Series devices will allow Layer 2 switching only after both timers expire.

The delay option is only available with HSRP. If you use any other FHRP, traffic loss is still possible.

See the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*, for more information on FHRPs and routing.

High Availability

The FabricPath topologies retain their configuration through an in-service software upgrade (ISSU).

See the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*, for more information on high availability.

Virtual Device Contexts

You must install the FabricPath feature set before you enable FabricPath on the switch. See *Configuring Feature Set for FabricPath* for information on installing the FabricPath feature set.

Because of the multiple forwarding engines (FEs) on the F Series modules, the following port pairs must be in the same VDC:

- Ports 1 and 2
- Ports 3 and 4

Send document comments to nexus7k-docfeedback@cisco.com

- Ports 5 and 6
- Ports 7 and 8
- Ports 9 and 10
- Ports 11 and 12
- Ports 13 and 14
- Ports 15 and 16
- Ports 17 and 18
- Ports 19 and 20
- Ports 21 and 22
- Ports 23 and 24
- Ports 25 and 26
- Ports 27 and 28
- Ports 29 and 30
- Ports 31 and 32

See the *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 5.x*, for more information on VDCs.

Licensing Requirements for FabricPath Interfaces

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	FabricPath requires an Enhanced Layer 2 license. For a complete explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series Licensing Guide</i> .

Prerequisites for FabricPath Interfaces

FabricPath interfaces have the following prerequisites:

- You should have a working knowledge of Classical Ethernet Layer 2 functioning.
- You must install the FabricPath feature set on the default and non-default VDC before you enable FabricPath on the switch. See *Configuring Feature-Set for FabricPath* for complete information on installing and enabling the FabricPath feature set.
- The FabricPath feature set operation might cause the standby supervisor to reload if it is in an unstable state, such as following a service failure or powering up.
- You are logged onto the device.
- Ensure that you have installed the Enhanced Layer 2 license.
- You are in the correct virtual device context (VDC). A VDC is a logical representation of a set of system resources. You can use the **switchto vdc** command with a VDC number.
- You are working on the F Series module.

Send document comments to nexus7k-docfeedback@cisco.com

Guidelines and Limitations for FabricPath Interfaces

FabricPath has the following configuration guidelines and limitations:

- FabricPath interfaces carry only FabricPath-encapsulated traffic.
- You must enable FabricPath on each device before you can view or access the commands. Enter the **feature-set fabricpath** command to enable FabricPath on each device.
- STP does not run inside a FabricPath network.
- Set the STP priority value on all FabricPath Layer 2 gateway devices to 8192.
- The F Series modules do not support multiple SPAN destination ports or virtual SPAN. If a port on the F Series module is in a VDC and that VDC has multiple SPAN destination ports, that SPAN session is not brought up.
- The following guidelines apply to private VLAN configurations when you are running FabricPath:
 - All VLANs in a private VLAN must be in the same VLAN mode; either CE or FP. If you attempt to put different types of VLANs into a private VLAN, these VLANs will not be active in the private VLAN. The system remembers the configurations, and if you change the VLAN mode later, that VLAN becomes active in the specified private VLAN.
 - FabricPath ports cannot be put into a private VLAN.
- The system does not support hierarchical static MAC addresses. That is, you cannot configure static FabricPath ODAs or OSAs; you can only configure CE static MAC addresses.
- On the F Series modules, user-configured static MAC addresses are programmed on all forwarding engines (FEs) that have ports in that VLAN.

Configuring FabricPath Interfaces



Note

You must have an F Series module in the chassis and enabled FabricPath on all the devices before you can see the FabricPath commands on the devices.

This section includes the following topics:

- [Configuring FabricPath Interfaces, page 3-9](#)
- [Configuring the STP Priority with Rapid PVST+, page 3-10](#)
- [Configuring the STP Priority with MST, page 3-11](#)
- [\(Optional\) Configuring the STP Domain ID for STP Domains Connected to the Layer 2 Gateway Switch, page 3-13](#)
- [Configuring a vPC+ Switch ID, page 3-14](#)



Note

You must make these configurations on each switch that you want to participate in the FabricPath network.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Configuring FabricPath Interfaces



Note

By default, all the interfaces on the N7K-F132XP-15 module are Layer 2 access interfaces.

You configure the interfaces for the FabricPath network to be FabricPath interfaces.

BEFORE YOU BEGIN

Ensure that you are working on an F Series module.

Ensure that you have enabled the FabricPath feature on all devices.

Ensure that you have installed the Enhanced Layer 2 license.

SUMMARY STEPS

1. **config terminal**
2. **interface** [ethernet *slot/port* | **port-channel** *channel-no*]
3. [**no**] **switchport mode fabricpath**
4. (Optional) **system default switchport fabricpath**
5. **exit**
6. (Optional) **show interface**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config terminal Example: switch# config terminal switch(config)#	Enters global configuration mode.
Step 2	interface [ethernet <i>slot/port</i> port-channel <i>channel-no</i>] Example: switch(config)# interface ethernet 2/11-15 switch(config-if)#	Specifies the interfaces that you want to configure as FabricPath.
Step 3	[no] switchport mode fabricpath Example: switch(config-if)# switchport mode fabricpath switch(config-if)#	Specifies interfaces as FabricPath port. Note The no keyword returns the interface to the default CE access interface. The FabricPath ports carry traffic only for those VLANs that are configured as FabricPath VLANs.
Step 4	system default switchport fabricpath Example: switch(config-if)# system default switchport fabricpath switch(config-if)#	(Optional) Converts all CE interfaces on the F Series module to FabricPath interfaces simultaneously.

Send document comments to nexus7k-docfeedback@cisco.com

	Command	Purpose
Step 5	exit Example: switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 6	show interface Example: switch(config)# show interface	(Optional) Displays information on all interfaces.
Step 7	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure specified interfaces as FabricPath interfaces:

```
switch# config terminal
switch(config)# interface ethernet 2/11-15
switch(config-if)# switchport mode fabricpath
switch(config-if)#
```

Configuring the STP Priority with Rapid PVST+

All Layer 2 gateway devices must have the same bridge priority when they are in the same STP domain. Make sure that the STP priority configured for the Layer 2 gateway devices on a FabricPath network is the lowest value in the Layer 2 network. Additionally, the priorities must match.

We recommend that you configure the STP priority on all FabricPath Layer 2 gateway devices to 8192.

BEFORE YOU BEGIN

Ensure that you are working on an F Series module.

Ensure that you have enabled the FabricPath feature on all devices.

Ensure that you have installed the Enhanced Layer 2 license.

SUMMARY STEPS

1. **config terminal**
2. **spanning-tree vlan [vlan-id] priority [value]**
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

	Command	Purpose
Step 1	config terminal Example: switch# config terminal switch(config)#	Enters global configuration mode.
Step 2	spanning-tree vlan [vlan-id] priority [value] Example: switch(config)# spanning-tree vlan 11-20 priority 8192 switch(config)#	You must configure all the Rapid PVST+ VLANs on all the FabricPath Layer 2 gateway interfaces to a lower STP priority. We recommend that you configure the priority to be 8192.
Step 3	exit Example: switch(config-if)# exit switch(config)#	Exits the interface configuration mode.
Step 4	show spanning-tree summary Example: switch# show spanning-tree summary	(Optional) Displays information on STP.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure the Rapid PVST+ VLANs on the FabricPath Layer 2 gateway devices to have an STP priority of 8192:

```
switch# config terminal
switch(config)# spanning-tree vlan 11-20 priority 8192
switch(config)#
```

See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference* for more information on this command.

Configuring the STP Priority with MST

All Layer 2 gateway devices must have the same bridge priority when they are in the same STP domain. Make sure that the STP priority configured for the Layer 2 gateway devices on a FabricPath network is the lowest value in the Layer 2 network. Additionally, the priorities must match.

You configure the STP priority for all Multiple Spanning-Tree (MST) instances on all FabricPath Layer 2 gateway devices to 8192.

BEFORE YOU BEGIN

Ensure that you are working on an F Series module.

Ensure that you have enabled the FabricPath feature on all devices.

Send document comments to nexus7k-docfeedback@cisco.com

Ensure that you have installed the Enhanced Layer 2 license.

SUMMARY STEPS

1. **config terminal**
2. **spanning-tree mst** [*instance-id*] **priority** [*value*]
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config terminal Example: switch# config terminal switch(config)#	Enters global configuration mode.
Step 2	spanning-tree mst [<i>instance-id</i>] priority [<i>value</i>] Example: switch(config)# spanning-tree mst 1-5 priority 8192 switch(config)#	Configures all the MST VLANs on all the FabricPath Layer 2 gateway interfaces to a lower STP priority. We recommend that you configure the priority to be 8192.
Step 3	exit Example: switch(config-if)# exit switch(config)#	Exits interface configuration mode.
Step 4	show spanning-tree summary Example: switch# show spanning-tree summary	(Optional) Displays information on STP.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

This example shows how to configure the MST instances on the FabricPath Layer 2 gateway devices to have an STP priority of 8192:

```
switch# config terminal
switch(config)# spanning-tree mst 1-5 priority 8192
switch(config)#
```

See the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference* for more information on this command.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

(Optional) Configuring the STP Domain ID for STP Domains Connected to the Layer 2 Gateway Switch

Because there can be many FabricPath Layer 2 gateway switches attached to a single FabricPath network, there are also many separate STP domains that are each connected to a Layer 2 gateway switch. You can configure a unique STP domain ID in the FabricPath network to propagate TCNs across all the STP domains that are connected to the FabricPath network. To ensure that all the MAC addresses are flushed when the system receives a TCN.

BEFORE YOU BEGIN

Ensure that you are working on an F Series module.

Ensure that you have enabled the FabricPath feature on all devices.

Ensure that you have installed the Enhanced Layer 2 license.

SUMMARY STEPS

1. **config terminal**
2. **spanning-tree domain *domain-id***
3. **exit**
4. (Optional) **show spanning-tree summary**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config terminal Example: switch# config terminal switch(config)#	Enters global configuration mode.
Step 2	spanning-tree domain <i>domain-id</i> Example: switch(config)# spanning-tree domain 5 switch(config)#	Assigns an STP domain ID to the different STP domains attached to FabricPath Layer 2 gateway switches that are connected to a single FabricPath network. The range is from 1 to 1023.
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	show spanning-tree summary Example: switch# show spanning-tree summary	(Optional) Displays information on STP.
Step 5	copy running-config startup-config Example: switch# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to configure the STP domain ID attached to the FabricPath Layer 2 gateway device:

```
switch# config terminal
switch(config)# spanning-tree domain 5
switch(config)# exit
switch
```

Configuring a vPC+ Switch ID



Note

All the peer link and downstream links in the virtual private channel (vPC+) must be on the F Series module.

You configure the vPC+ switch ID by using the **fabricpath switch-id** command.



Note

You cannot configure a vPC+ domain and a vPC domain in the same virtual device context (VDC).

See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*, for complete information on configuring vPCs.

BEFORE YOU BEGIN

Ensure that you are working on an F Series module.

Ensure that you have enabled the vPC feature.

Ensure that you have enabled the FabricPath feature.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **vpc domain** *domain-id*
3. **fabricpath switch-id** *switch-id*

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal	Enters global configuration mode.

Send document comments to nexus7k-docfeedback@cisco.com

	Command	Purpose
Step 2	<code>vpc domain domain-id</code> Example: <code>switch(config)# vpc domain 1</code>	Creates a vPC+ domain on the device, and enters the vpc-domain configuration mode for configuration purposes.
Step 3	<code>fabricpath switch-id switch-id</code> Example: <code>switch(config-vpc-domain)# fabricpath switch-id 1</code>	Assigns a static vPC+ ID to the vPC+ peer. The range is from 0 to 4094. This static ID is the virtual switch ID for FabricPath encapsulation. Note You must assign the same vPC+ switch ID to each of the two vPC+ peer devices before they can form an adjacency.

This example shows how to configure a vPC+ switch ID on each vPC+ peer device:

```
switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# fabricpath switch-id 1
```

Verifying FabricPath Interface Configuration

To display FabricPath interfaces information, perform one of the following tasks:

Command	Purpose
<code>show feature-set</code>	Displays whether FabricPath is enabled on the device or not.
<code>show interface brief</code>	Displays information on all interfaces.
<code>show interface switchport</code>	Displays information, including access and trunk interface, for all the Layer 2 interfaces.
<code>show interface type {slot/port \ channel-number} [trunk]</code>	Displays interface configuration information.
<code>show interface capabilities</code>	Displays information on the capabilities of the interfaces.
<code>show interface status</code>	Displays information on the status of the interfaces.
<code>show spanning-tree summary</code>	Displays STP information.
<code>show fabricpath is-is database</code>	Displays STP TCN information.
<code>show vpc brief</code>	Displays brief information on the vPC+ domains.
<code>show vpc consistency-parameters</code>	Displays the status of those parameters that must be consistent across all vPC+ domain interfaces.
<code>show vpc peer-keepalive</code>	Displays information on the peer-keepalive messages.
<code>show vpc role</code>	Displays the peer status, the role of the local device, the vPC+ domain's system MAC address and system priority, and the MAC address and priority for the local vPC+ domain's device.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Purpose
show vpc statistics	Displays statistics on the vPC+ domains.
show running-config vpc	Displays running configuration information for vPCs and vPC+ domains.

For information on the above commands, see the *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference* and the *Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*.

Displaying FabricPath Interface Statistics

Use the following command to display FabricPath statistics:

- **clear counters** [**ethernet** *slot/port* | **port-channel** *channel-no*]
- **show interface counters** [**module** *module*]
- **show interface counters detailed** [**all**]
- **show interface counters errors** [**module** *module*]

FabricPath Interface Example Configuration

To configure FabricPath interfaces, perform the following tasks on each device:

- Enable FabricPath on each device.
- Configure the interfaces that you want to designate as FabricPath interfaces.
- Set the STP priority device to 8192 on all FabricPath Layer 2 gateway devices.
- (Optional) Set the STP domain ID for each of the separate STP domains that are connected to the FabricPath network.
- (Optional) Configure a vPC+ switch ID.

To configure FabricPath interfaces, follow these steps:

Step 1 (Optional) Enable FabricPath on each device.

```
switch# config terminal
switch(config)# feature fabricpath
switch(config-lldp)# exit
switch(config)#
```

Step 2 After you enable FabricPath on the device, configure the specified interface as FabricPath interfaces.

```
switch(config)# interface ethernet 1/2
switch(config-if)# switchport mode fabricpath
switch(config-if)# exit
switch(config)#
```

Step 3 Configure the STP priority for all Rapid PVST+ VLANs as 8192.

```
switch# config terminal
```

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# spanning-tree vlan 11-20 priority 8192
switch(config)#
```

Step 4 Configure the STP priority for all MST instances as 8192.

```
switch# config terminal
switch(config)# spanning-tree mst 1-5 priority 8192
switch(config)#
```

Step 5 (Optional) Configure the STP domain ID on each FabricPath Layer 2 gateway switch attached to the FabricPath network.

```
switch# config terminal
switch(config)# spanning-tree domain 5
switch(config)
```

Step 6 (Optional) Configure the vPC+ switch ID.

```
switch# config terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# fabricpath switch-id 100
switch(config-vpc-domain)# exit
switch(config)
```



Note

See the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*, for information on configuring vPC.

If you are configuring the vPC+ with no existing vPC+, follow these steps:

1. In the vPC domain configuration mode, enter the **fabricpath switch-id** *switch-id* command.
2. On each of the vPC+ peer link interfaces in interface configuration mode, enter the **switchport mode fabricpath** command.
3. On each vPC+ peer link port channel, enter the **vpc peer-link** command.

If you are changing an existing vPC configuration to a vPC+ on an F Series module, follow these steps:

1. On each vPC peer link port channel, enter the **shutdown** command.
2. In the vPC domain configuration mode, enter the **fabricpath switch-id** *switch-id* command.
3. On each of the vPC+ peer link interfaces in interface configuration mode, enter the **switchport mode fabricpath** command.
4. On each vPC+ peer link port channel, enter the **no shutdown** command.

Step 7 Save the configuration.

```
switch(config)# save running-config startup-config
switch(config)#
```

When you are configuring vPC+, and you see the following situations, you must enter the **shutdown** command and then the **no shutdown** command on all the peer-link interfaces:

- There is no switchport mode FabricPath configuration on the peer-link interfaces, but the FabricPath switch ID is configured in the vPC domain.
- The **switchport mode fabricpath** configuration is on the peer-link interfaces, but there is no FabricPath switch ID in the vPC domain.

Send document comments to nexus7k-docfeedback@cisco.com

Feature History for Configuring FabricPath Using the CLI

Table 3-1 lists the release history for this feature.

Table 3-1 *Feature History for FabricPath*

Feature Name	Releases	Feature Information
FabricPath Interfaces	5.1(1)	These features were introduced.