

Cisco FabricPath Best Practices

What You Will Learn

Cisco® FabricPath has been deployed and running in the field since end of 2010, and thousands of customers have now acquired Cisco FabricPath licenses for their networks. This document introduces some best practices that are mainly the results of their experiences.

A best practice is a recommendation based on Cisco internal testing and the experience accumulated by customers in their production networks. A best practice is not a rule. A configuration that is beneficial for the majority of the use cases can be described as a best practice but may not be applicable to a particular network design. To help customers determine whether a best practice is applicable, this document details the rationale for each best practice. Cisco support is not bound to strict compliance with the best practices listed in this document.

This document is not an introduction to Cisco FabricPath. A basic knowledge of Cisco FabricPath is assumed. Refer to the [Cisco FabricPath white paper](#) for more information.

This document is not a network design guide either. It does not attempt to describe each and every possible use case of the technology, and the network topology presented here simply illustrates the use of some common recommended configurations.

Following a high-level overview of the network topology that will be used as an example, the best practices are introduced. The best practices are discussed in more detail in the latter part of this document.

- [Configure Active-Active Default Gateways with vPC+](#)
- [Attach Devices Other Than Cisco FabricPathDevices Redundantly with VPC+](#)
- [Configure the Cisco FabricPathRegion as the Spanning Tree Root of the Network](#)
- [Disable Optimized Multicast Flooding](#)

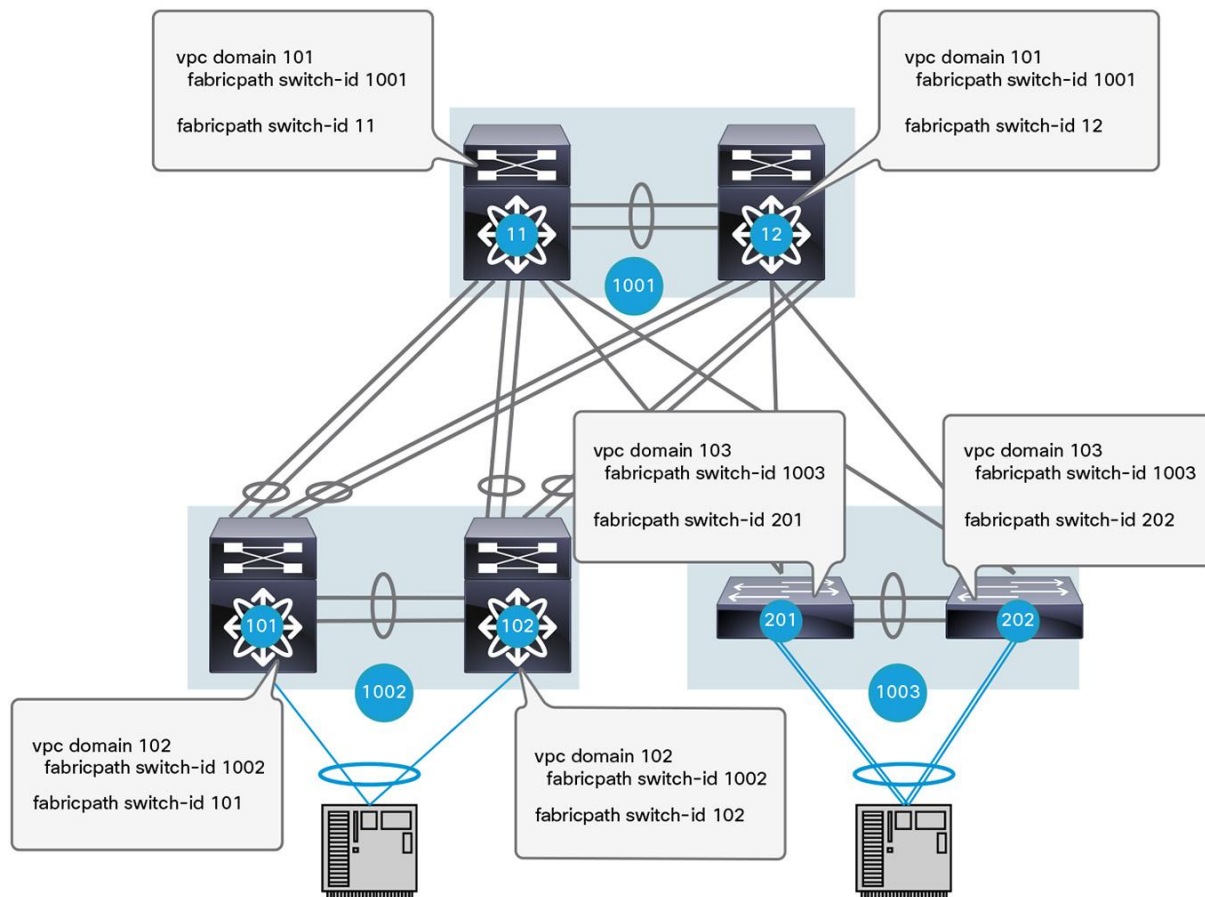
Assign Switch IDs Manually

Cisco FabricPath can assign switch IDs to all the devices in the network automatically; however, it is convenient to use a meaningful numbering scheme. During network troubleshooting, having a distinct numbering scheme allows faster and easier switch role identification. For example, in this network:

- The devices in the core have been assigned a two-digit ID
- The devices at the access have been assigned a three-digit ID
- The switches forming a vPC+ domain have been assigned consecutive switch IDs. For instance, the pair of Cisco Nexus 7000 Series access switches received 101 and 102 as IDs
- The virtual switch for this domain has a four-digit ID: 1002

Figure 2 shows the switched IDs assigned in the sample network.

Figure 2. Switch ID Examples



Here is the configuration:

```
SW-101# sh run fabricpath

feature-set fabricpath

vlan 10-100
  mode fabricpath

fabricpath switch-id 101

vpc domain 102
fabricpath switch-id 1002

-- output omitted -

fabricpath domain default
  root-priority 150
```

```
SW-102# sh run fabricpath

feature-set fabricpath

vlan 10-100
  mode fabricpath
fabricpath switch-id 102
vpc domain 102
  fabricpath switch-id 1002

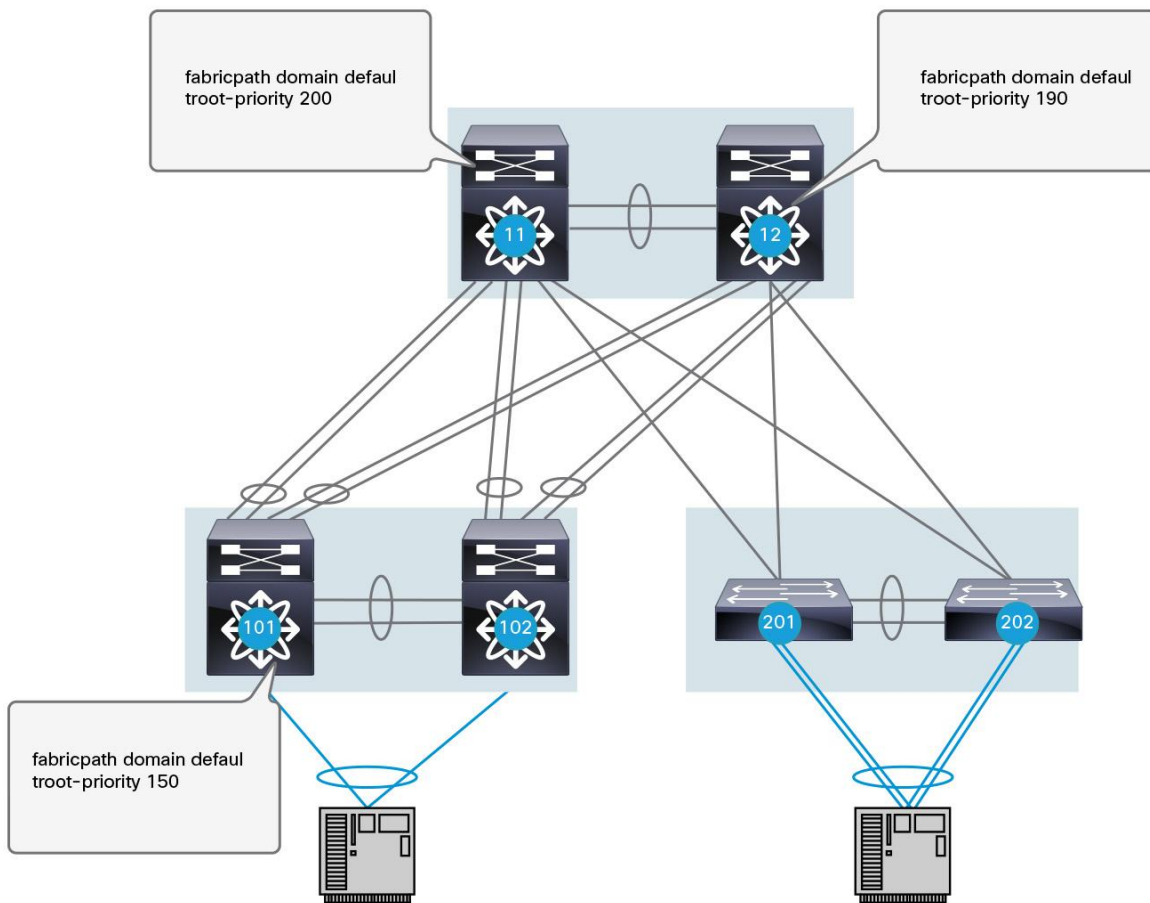
-- output omitted --

fabricpath domain default
```

Configure the Root for Multidestination Trees

Two multidestination trees are defined in this network by default, and multidestination traffic is mapped to either of those trees for load-balancing purposes. You should explicitly set the root of those multidestination trees in the network so that they provide an optimal topology (Figure 3).

Figure 3. Root Configuration for Multidestination Trees



In this example, switches 11 and 12 are set as the root for the two multidestination trees. If either of those switches fails, a replacement root would have to be elected out of the access switches. You should configure this backup root in advance so that the system falls back to a predetermined topology in a failure scenario.

Cisco FabricPath Intermediate Switch-to-Intermediate Switch (IS-IS) Protocol elects the switch with the highest configured root priority as the root for multidestination tree 1. The switch with the second-highest root priority becomes the root for multidestination tree 2.

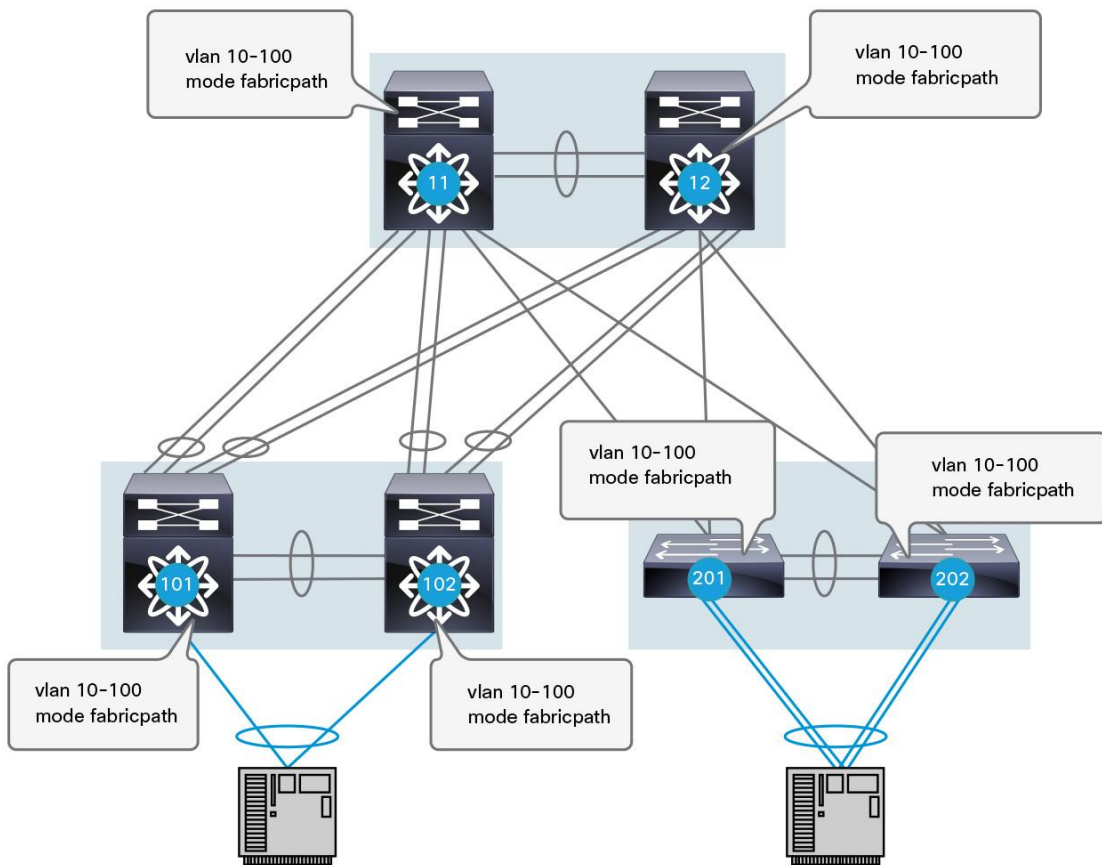
More information is provided in the section “Additional Details Supporting the Best Practices” later in this document.

Configure All VLANs Consistently in a Topology in the Network

You should configure the Cisco FabricPath VLANs consistently on all the Cisco FabricPath switches in a particular topology (Figure 4). In this example, VLANs 10 to 100 are Cisco FabricPath VLANs, so they must be configured as such on every switch running Cisco FabricPath in the network (the network has only a single topology).

This recommendation is only applicable to Cisco FabricPath VLANs, not Classic Ethernet (CE) VLANs.

Figure 4. Consistent Configuration of Cisco FabricPath VLANs



Use PortChannels Between Leaves and Spines

You should group the uplinks to spine switches in a PortChannel. When design requirements demand high-performance, reliable paths, statically hard-code bandwidth on each of the uplink PortChannels.

More information is provided in the section "Additional Details Supporting the Best Practices" later in this document.

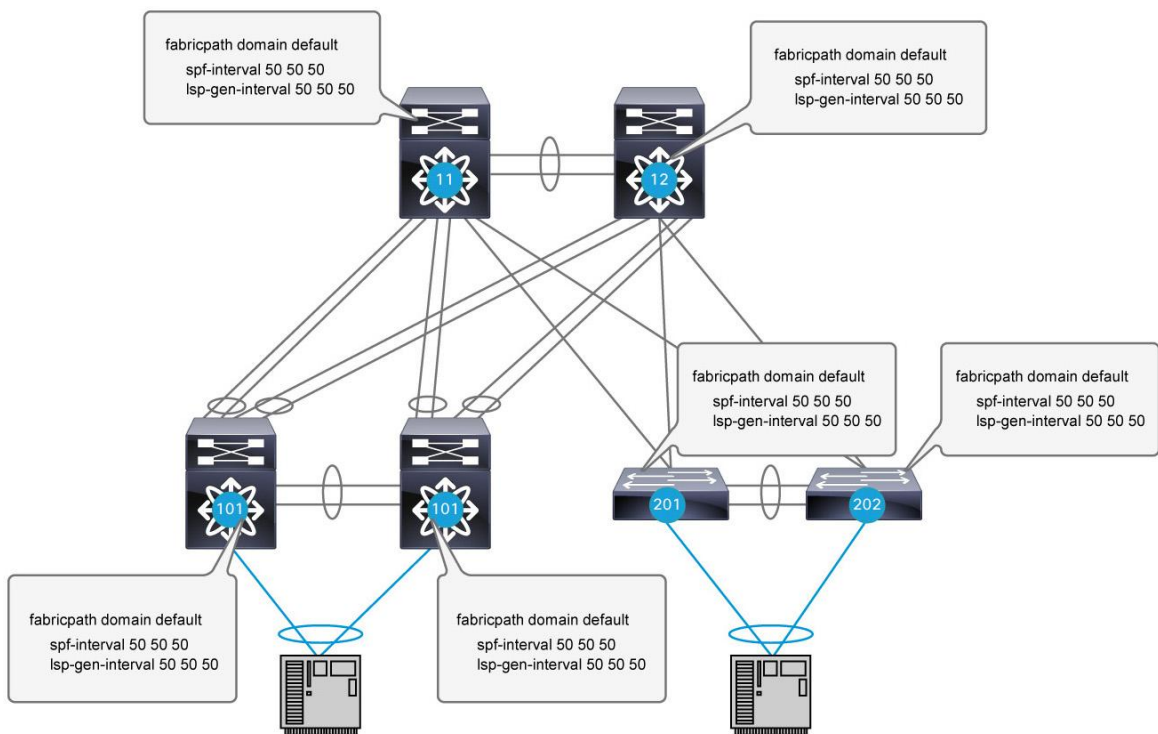
Tune Timers for Fast Convergence

To achieve fast convergence, it is recommended to tune the IS-IS timers in Cisco FabricPath (Figure 5). This tuning is particularly important when a switch is inserted in the topology.

The following configuration is recommended for all switches in the network:

```
fabricpath domain default
spf-interval 50 50 50
lsp-gen-interval 50 50 50
```

Figure 5. Tuning the IS-IS Timers



Also, to provide better network convergence upon a Cisco FabricPath switch restart, you should set a Cisco FabricPath linkup-delay timer to 60 as shown in the following example:

```
SW-11(config)# fabricpath timers linkup-delay 60
```

For more information, see the section “Additional Details Supporting the Best Practices” later in this document.

Configure Active-Active Default Gateways with vPC+

You should configure a vPC+ in conjunction with Hot Standby Router Protocol (HSRP) on Layer 2 and Layer 3 switches to actively use both switches default gateways.

For example, the vPC+ and HSRP configurations on Cisco FabricPathswitches 11 and 12 are shown here.

Switch 11 Configuration

```
SW-11# sh run vpc

feature vpc

vpc domain 101
  peer-keepalive destination 10.10.10.2 source 10.10.10.1 vrf PKL
  fabricpath switch-id 1001

interface port-channel10
  description vPC+ Peer-Link
  switchport
  switchport mode fabricpath
  vpc peer-link

SW-11# sh run hsrp

feature hsrp

interface Vlan10
  hsrp 10
  ip 10.100.10.1
```

Switch 12 Configuration

```
SW-12# sh run vpc

feature vpc

vpc domain 101
  peer-keepalive destination 10.10.10.1 source 10.10.10.2 vrf PKL
  fabricpath switch-id 1001

interface port-channel10
  description vPC+ Peer-link
  switchport
  switchport mode fabricpath
  vpc peer-link
```



```
SW-12# sh run hsrp

feature hsrp

interface Vlan10
  hsrp 10
  ip 10.100.10.1
```

More information is provided in the section “Additional Details Supporting the Best Practices” later in this document.

Attach Devices Other Than Cisco FabricPath Devices Redundantly with VPC+

Devices other than Cisco FabricPath devices can be dual-attached to vPC+ switches using IEEE standard PortChannels without the need to use Spanning Tree Protocol to provide redundancy. VLANs carried on vPC+ member ports must be Cisco FabricPath mode VLANs.

Since Cisco FabricPath does not rely on Spanning Tree Protocol, and the vPC+ peer link is in fact a Cisco FabricPath Core port, so a **peer-switch** command is not needed.

For hardware-related vPC+ requirements, please refer to the Cisco [NX-OS Software release notes](#) and [configuration guide](#).

Here are sample interfaces configurations of vPC+ peers:

SW-201 :

```
interface Ethernet6/8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  channel-group 20 mode active
  no shutdown
```

```
interface port-channel20
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  vpc 20
```

SW-202 :

```
interface Ethernet6/19
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  channel-group 20 mode active
  no shutdown
```

```
interface port-channel20
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  vpc 20
```

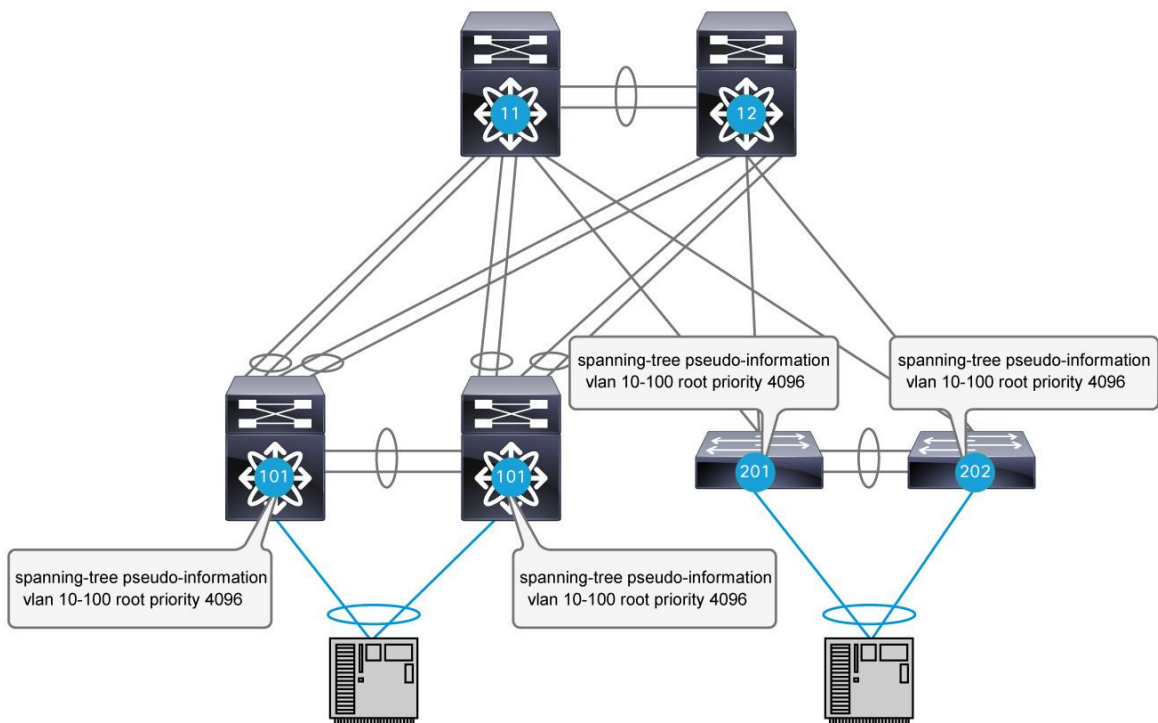
Configure the Cisco FabricPathRegion as the Spanning Tree Root of the Network

On all the Cisco FabricPath switches that have Classic Ethernet ports, configure the same root priority using the **spanning-tree pseudo-information** command shown here. Make sure that this root priority is the best (lowest) in the network so that the Cisco FabricPath region is the root of the spanning tree. If the Classic Ethernet edge ports receive a superior Bridge Protocol Data Unit (BPDU), those ports will be blocked from forwarding traffic. Also, those Classic Ethernet edge ports connecting to the same Layer 2 domain that is not a Cisco FabricPath domain, should be configured with the spanning-tree domain number. This approach will allow proper BPDU Propagation through the Cisco FabricPath network and help ensure a loop-free environment within that Layer 2 domain.

Figure 6 shows the configuration presented here.

```
switch(config)# spanning-tree pseudo-information
switch(config-pseudo)# vlan 10-100 root priority 4096
```

Figure 6. Cisco FabricPath Region Configured as Spanning Tree Root for Network



Disable Optimized Multicast Flooding

When IPv6 is used in a network, the Internet Group Management Protocol (IGMP) Optimized Multicast Flooding (OMF) feature must be disabled for that VLAN:

```
N7K-2-VDC3(config)# vlan configuration 10
N7K-2-VDC3(config-vlan-config)# no ip igmp snooping optimise-multicast-flood
```

More information is provided in the section “Additional Details Supporting the Best Practices.”

Additional Details Supporting the Best Practices

Considerations Regarding Multidestination Trees

Cisco FabricPath computes several trees that are used to forward multidestination traffic. This discussion assumes that the network contains only two of those trees, but the considerations presented are independent of the actual number of trees in the network (an upcoming software release will allow the creation of a variable number of trees per topology).

Multidestination traffic is basically anything that is not known unicast traffic:

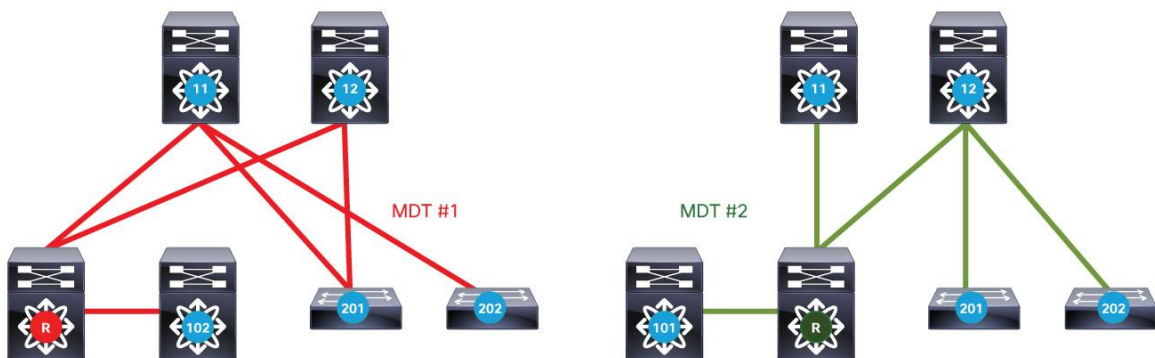
- Classic Ethernet unknown unicast (Layer 2 traffic destined for a unicast MAC address that is not associated with a particular switch ID)
- Broadcast traffic
- Multicast traffic

Set the Location of the Root Switches

To compute the two trees, Cisco FabricPath first sets up two distinct root switches. This is a particular property of Cisco FabricPath. With the Spanning Tree Protocol, for example, the same switch can be elected as root for different VLANs or different Multiple Spanning Tree (MST) instances. Here, there are dependencies between the trees, and Cisco FabricPath helps ensure that all the trees have different roots. The goal is to automatically introduce some variety into the different MDT tree topologies so that, by default, multidestination traffic is load balanced across different links.

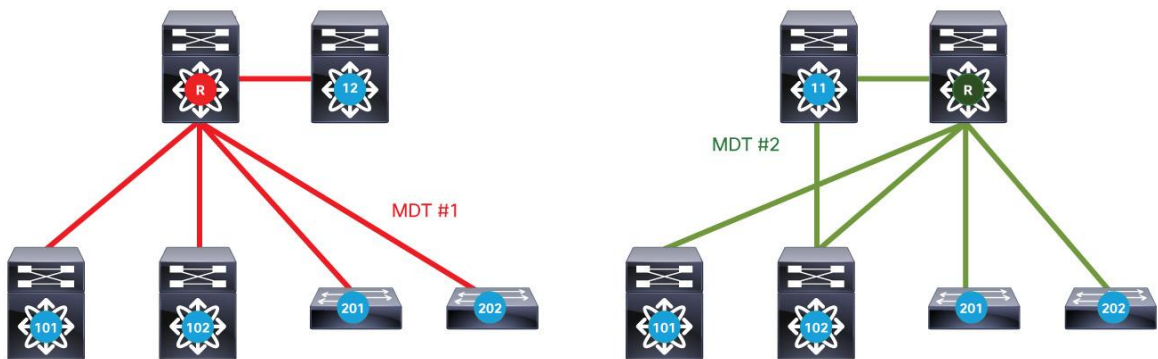
Cisco FabricPath sets up the two multidestination trees automatically, without user configuration. However, just as with Spanning Tree Protocol, it is desirable to influence the root selection to get optimal trees. For example, without any additional configuration, Cisco FabricPath could select its root switches at the access layer and compute the two trees shown in Figure 7 for the sample network.

Figure 7. Two Trees Set by Cisco FabricPath without Additional Configuration



There is nothing really wrong with those two trees. They will provide connectivity between all the switches in the network. Note, however, that the Clos fabric that is typically used in data center designs should optimize communication between leaf switches. Here, assume that the source for multidestination traffic is likely to be a leaf (access) switch, and the receivers for this traffic will be other leaf switches. In the example shown in Figure 7, notice that traffic may need to pass through up to three links when it is transmitted from one leaf to another. However, if you locate the root of the multidestination trees on the spines, as represented in Figure 8, communication between leaf switches is consistently achieved in two hops.

Figure 8. Locating the Root on the Spines to Optimize Communication



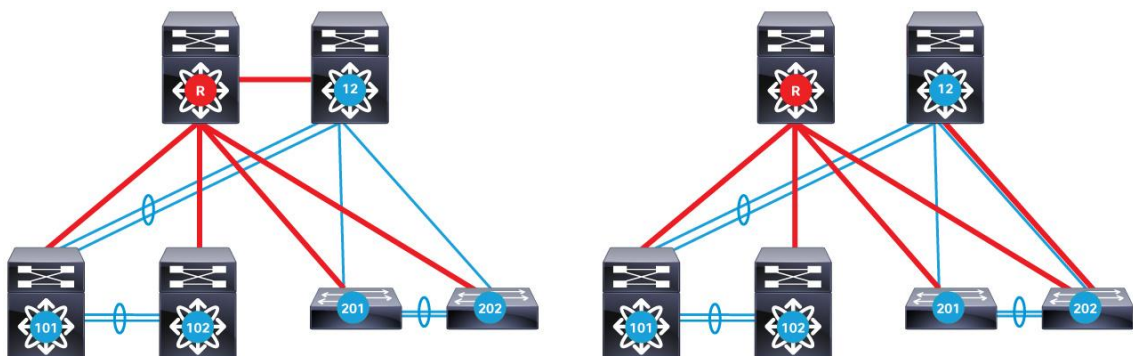
Locating the root on the spine switches of a Clos fabric is thus recommended to influence the tree topology and achieve the most efficient forwarding path between the leaf switches.

Note that Cisco FabricPath does not assume that the network is a Clos fabric. Even if there is no obvious “spine” switch in the network, you still should explicitly configure the root for the different multidestination trees in the network. You should do so because arbitrary root placement will most likely result in suboptimal multidestination trees. Also, a known, deterministic, tree topology will aid troubleshooting.

Configure All Cisco FabricPath VLANs Consistently Across the Network

Consistent VLAN configuration across the network is critical because Cisco FabricPath does not compute a network topology on a per-VLAN basis. Therefore, if a VLAN is not defined on a particular Cisco FabricPath switch, the control plane will not be aware of it and may try to forward traffic for this VLAN through this particular switch, with the result that the traffic is black-holed. Note that with Cisco FabricPath, core ports forward traffic only for VLANs that are defined in the switch. The loss of traffic which is caused by lack of the required VLANs in the VLAN database is especially difficult to troubleshoot. Figure 9 shows the red tree in stable conditions (on the left), and after a failure of the link between the two spine switches (on the right).

Figure 9. Tree in Stable Conditions (Left) and After a Link Failure (Right)



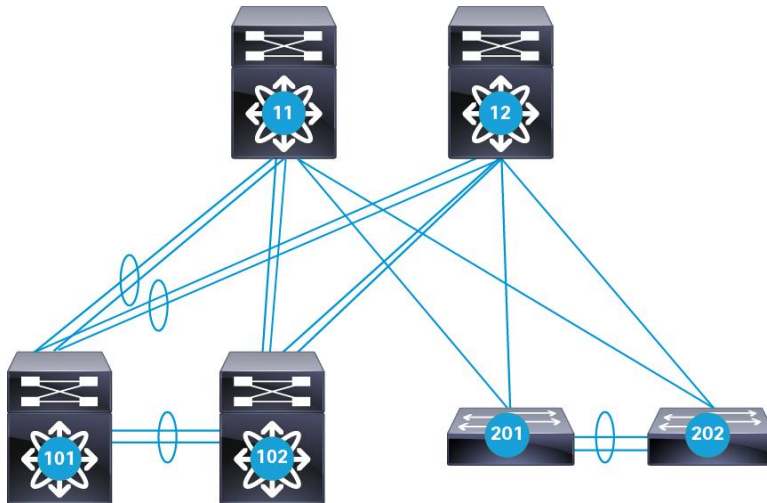
Suppose that VLAN 1 has not been defined on switches 201 and 202 because no host on this VLAN is defined on those switches. Everything is fine in stable conditions. However, because the control plane of Cisco FabricPath is not aware that VLAN 1 is not present on switch 202, it might still try to use it as a transit switch between the root and switch 12 in the failure scenario represented on the right in Figure 9. As a result, the two spine switches lose the capability to exchange multidestination traffic. Their HSRP adjacency will fail, for example.

You may be able to engineer the trees so that if any link or switch failure occurs, they never try to forward traffic through switch 202. However, it is simpler to make sure that all Cisco FabricPath VLANs are consistently configured on all switches.

Use PortChannels for Links Between Leaf and Spine

Cisco FabricPath can implement equal-cost multipath (ECMP). Figure 10 shows the benefits for the sample network.

Figure 10. Benefits of ECMP

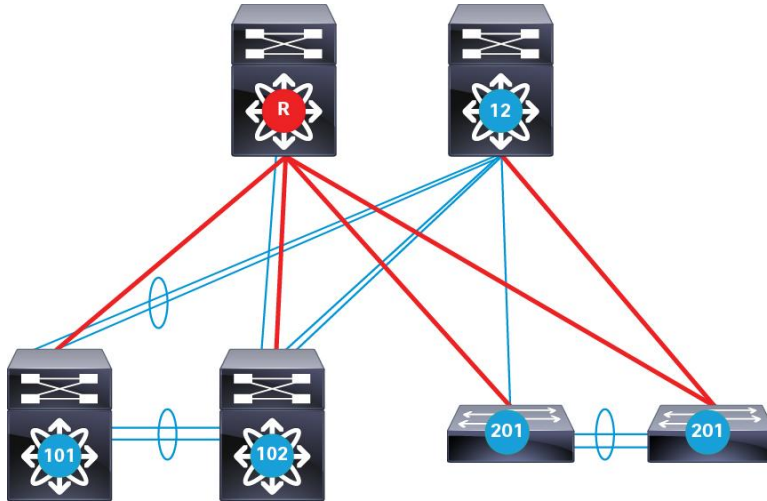


Here, switch 101 has its uplinks to 11 and 12 bundled in a PortChannel, whereas switch 102 has four independent uplinks. Both switches 101 and 102 can load-balance their traffic on up to four different physical links when targeting switch 201, for example. In the case of switch 101, there are two equal-cost paths to switch 201, whereas in the case of switch 102, there are four equal-cost paths to 201. From a data-plane forwarding perspective, there is hardly any difference in the way the traffic is load-balanced across the uplinks. However, you should use the configuration represented for switch 101, with PortChannels, for two main reasons:

- With PortChannels configured, the IS-IS protocol has to handle fewer links (and thus fewer link-state advertisements [LSAs]) and can converge faster and scale better. In the example in Figure 10, IS-IS sees only two links between switch 101 and the spine, and IS-IS has to handle four links between switch 102 and the spine.
- PortChannels provide more bandwidth for the multidestination trees, because the PortChannel is treated as a single logical link in Cisco FabricPath IS-IS.

Figure 11 shows one of the multideestination trees in the sample network. Because the four uplinks of switch 102 are seen as individual parallel links by IS-IS, only one physical port can be part of the multideestination tree. However, from the perspective of IS-IS, switch 101 has two logical uplinks (its two PortChannels), one of which is kept in the final multideestination tree. As a result, switch 101 can use two physical links (the ones forming the PortChannel to switch 11) for its multideestination traffic.

Figure 11. Multideestination Tree in the Sample Network



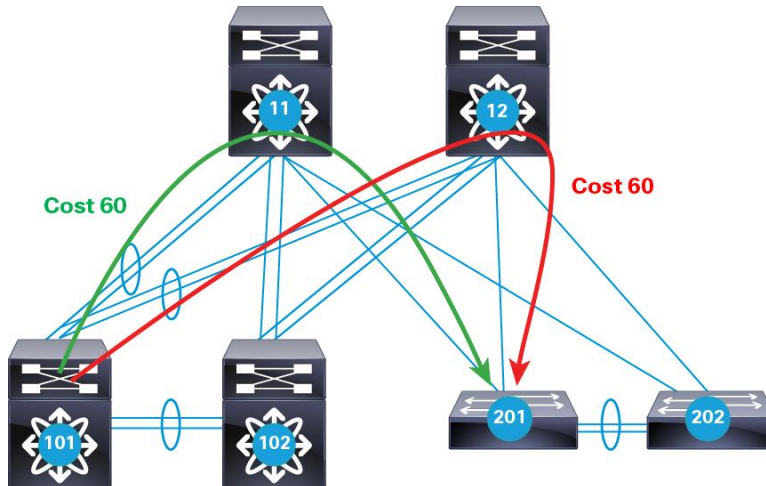
Note that this recommendation represents a trade-off between performance and multideestination tree bandwidth and simple operation. In a relatively small network, the benefits of PortChannels for the leaf switch uplinks may not be worth the configuration overhead.

Also, when configuring the uplinks of a leaf switch as a PortChannel, you should hard-code the IS-IS cost of the Port Channel. You should do so because IS-IS recomputes the cost of a channel dynamically based on the availability of its members. If a single link of a channel fails, the resulting cost of the bundle immediately increases. In the case of switch 101, such a link failure on an uplink would immediately remove this uplink from the list of equal-cost paths to the other leaf switches. In other words, a failure of a single member of the PortChannel causes IS-IS to avoid the whole PortChannel, as if the PortChannel had failed. Hard-coding a cost on the PortChannel prevents dynamic recomputation and keeps the uplink in the routing table.

Consider the following example:

Leaf switch 101 is dual homed through two PortChannels to spine switches. Each PortChannel has two 10Gigabit Ethernet links. Leaf switch 201, however, is dual homed only with a single 10 Gigabit Ethernet link to each of the spine switches (Figure 12).

Figure 12. Equal Cost Multi Pathing Example Between Switch 101 and Switch 201



There are two equal-cost paths between Cisco FabricPath switch 101 to Cisco FabricPath switch 201, and the metric is 60 for each path:

```
SW-101# sh fabricpath isis route
Fabricpath IS-IS domain: default MT-0
Topology 0, Tree 0, Swid routing table

-- output omitted --

201, L1
  via port-channel15, metric 60
  via port-channel13, metric 60

-- output omitted -
```

Cisco FabricPath IS-IS calculates the link metrics based on the number of active members in the PortChannel. In the next example, the PortChannel between Cisco FabricPath switches 101 and 11 is displayed:

```
SW-101# sh port-channel summary interface port-channel 13
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```



```

-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
13   Po13(SU)    Eth       LACP      Eth6/11 (P)  Eth6/12 (P)
SW-101#
SW-101# sh fabricpath isis interface port-channel 13
Fabricpath IS-IS domain: default
Interface: port-channel13
  Status: protocol-up/link-up/admin-up
  Index: 0x0001, Local Circuit ID: 0x01, Circuit Type: L1
  No authentication type/keychain configured
  Authentication check specified
  Extended Local Circuit ID: 0x1600000C, P2P Circuit ID: 0000.0000.0000.00
  Retx interval: 5, Retx throttle interval: 66 ms
  LSP interval: 33 ms, MTU: 1500
  P2P Adjs: 1, AdjsUp: 1, Priority 64
  Hello Interval: 10, Multi: 3, Next IIH: 00:00:04
Level  Adjs  AdjsUp  Metric  CSNP  Next CSNP  Last LSP ID
1       1      1       20     60    00:00:49  ffff.ffff.ffff.ff-ff
Topologies enabled:
  Topology Metric  MetricConfig Forwarding
0           20      no             UP

```

When one of the two links within the PortChannel fails, you can see that the metric changes appropriately:

```

SW-101# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-101(config)# int e6/11
SW-101(config-if)# shut
2013 Apr 10 23:24:41 N7K-1-VDC3 %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel13:
Ethernet6/11 is down
SW-101(config-if)# 2013 Apr 10 23:24:42 N7K-1-VDC3 %ETHPORT-5-IF_DOWN_CFG_CHANGE:
Interface Ethernet6/11 is down(Config change)
2013 Apr 10 23:24:42 N7K-1-VDC3 %ETHPORT-5-IF_DOWN_ADMIN_DOWN: Interface
Ethernet6/11 is down (Administratively down)
SW-101(config-if)# sh port-channel summary interface port-channel 13
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
-----
Group Port-      Type      Protocol  Member Ports

```



```

Channel
-----
13    Po13(SU)    Eth        LACP        Eth6/11(D)   Eth6/12(P)
SW-101(config-if)#
SW-101(config-if)# sh fabricpath isis interface port-channel 13
Fabricpath IS-IS domain: default
Interface: port-channel13
  Status: protocol-up/link-up/admin-up
  Index: 0x0001, Local Circuit ID: 0x01, Circuit Type: L1
  No authentication type/keychain configured
  Authentication check specified
  Extended Local Circuit ID: 0x1600000C, P2P Circuit ID: 0000.0000.0000.00
  Retx interval: 5, Retx throttle interval: 66 ms
  LSP interval: 33 ms, MTU: 1500
  P2P Adjs: 1, AdjsUp: 1, Priority 64
  Hello Interval: 10, Multi: 3, Next IIH: 00:00:08
  Level  Adjs  AdjsUp  Metric  CSNP  Next CSNP  Last LSP ID
  1      1      1      40     60   00:00:42  ffff.ffff.ffff.ff-ff
  Topologies enabled:
    Topology Metric  MetricConfig Forwarding
    0          40      no             UP

```

Now there are two paths with the following characteristics:

- With the metric of 80 (1x10-GbpsPortChannel 13 between switches 101 and 11 + 1x10-Gbps link between switches 11 and 201)
- With the metric of 60 (2x10-GbpsPortChannel 15 between switches 101 and 12 + 1x10-Gbps link between switches 12 and 201)

Because the paths are no longer equal, only the one with the best metric is used:

```

SW-101# sh fabricpath isis route
Fabricpath IS-IS domain: default MT-0
Topology 0, Tree 0, Swid routing table

-- output omitted --

201, L1
  via port-channel15, metric 60

-- output omitted --

```

As mentioned earlier, you can hard-code metrics on a PortChannel, using the Link Aggregation Control Protocol (LACP) min-links feature, to help ensure that Cisco FabricPath uses PortChannels only as long as they conform to the configured bandwidth limits:

```
interface port-channel13
  lacp min-links 2
  fabricpath isis metric 20
```

Now, when you look at the Cisco FabricPath IS-IS metric for this PortChannel, you see that even when one of the channel members is down, the metric is still equal to the full PortChannel capacity and two equal-cost paths in the Cisco FabricPath routing table:

```
SW-101(config-if)#sh fabricpath isis interface port-channel 13
Fabricpath IS-IS domain: default
Interface: port-channel13
  Status: protocol-up/link-up/admin-up
  Index: 0x0001, Local Circuit ID: 0x01, Circuit Type: L1
  No authentication type/keychain configured
  Authentication check specified
  Extended Local Circuit ID: 0x1600000C, P2P Circuit ID: 0000.0000.0000.00
  Retx interval: 5, Retx throttle interval: 66 ms
  LSP interval: 33 ms, MTU: 1500
  P2P Adjs: 1, AdjsUp: 1, Priority 64
  Hello Interval: 10, Multi: 3, Next IIH: 00:00:03
  Level  Adjs  AdjsUp  Metric  CSNP  Next CSNP  Last LSP ID
  1      1      1      20     60    00:00:57  ffff.ffff.ffff.ff-ff
  Topologies enabled:
    Topology Metric  MetricConfig Forwarding
    0         20     yes          UP

SW-101# sh fabricpath route switchid 201
-- output omitted --

FabricPath Unicast Route Table for Topology-Default

1/201/0, number of next-hops: 2
  via Po13, [115/60], 0 day/s 00:03:20, isis_fabricpath-default
  via Po15, [115/60], 19 day/s 00:13:18, isis_fabricpath-default
```

When configuring static metrics for PortChannels, consider the importance of that path remaining active. It would be suboptimal to remove a PortChannel with 16 members from the forwarding topology because of the failure of a single member. The removal of a PortChannel with two members would be much less problematic, and the explicit configuration of the cost may not be necessary in that case.

With careful consideration, you can configure **lacp min-links** command, which will bring down the PortChannel after the number of active member links falls below the configured threshold.

Configuring vPC+ for Active-Active Default Gateways

When configured on Layer 2 and Layer 3 boundary switches, vPC+ enables active-active default gateways. All devices, whether they are connected through vPC+ or native Cisco FabricPath ports can now use multiple paths to two active gateways for the routed traffic (north-south and inter-VLAN traffic).

From a leaf switch's point of view, the HSRP gateway is reached through an emulated switch ID of a configured vPC+ domain:

```
SW-101(config)# sh mac address-table
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen, + - primary entry using vPC Peer-Link,
    (T) - True, (F) - False
    VLAN      MAC Address      Type      age      Secure NTFY Ports/SWID.SSID.LID
    -----+-----+-----+-----+-----+-----+-----
G    -      d867.d90a.0b44    static    -        F    F    sup-eth1(R)
10    0000.0c07.ac0a    dynamic    0        F    F    1001.0.4306
10    d867.d903.f342    dynamic    0        F    F    12.0.4306
10    d867.d90a.0b42    dynamic    60       F    F    11.0.4306
```

Also, because there are two switches with emulated switch IDs, two equal-cost paths are installed in the Cisco FabricPath routing table:

```
SW-101# sh fabricpath route
FabricPath Unicast Route Table
'a/b/c' denotes ftag/switch-id/subswitch-id
'[x/y]' denotes [admin distance/metric]
ftag 0 is local ftag
subswitch-id 0 is default subswitch-id

FabricPath Unicast Route Table for Topology-Default

0/101/0, number of next-hops: 0
    via ---- , [60/0], 6 day/s 16:37:35, local
0/1002/1, number of next-hops: 0
1/11/0, number of next-hops: 1
    via Po13, [115/20], 6 day/s 16:34:26, isis_fabricpath-default
1/12/0, number of next-hops: 1
    via Po15, [115/20], 6 day/s 16:34:26, isis_fabricpath-default
1/102/0, number of next-hops: 1
    via Po17, [115/20], 6 day/s 16:34:25, isis_fabricpath-default
1/201/0, number of next-hops: 2
    via Po13, [115/60], 6 day/s 16:21:13, isis_fabricpath-default
    via Po15, [115/60], 6 day/s 16:21:13, isis_fabricpath-default
1/202/0, number of next-hops: 2
```

```

via Po13, [115/60], 6 day/s 16:21:28, isis_fabricpath-default
via Po15, [115/60], 6 day/s 16:21:28, isis_fabricpath-default
1/1001/0, number of next-hops: 2
via Po13, [115/20], 6 day/s 16:34:26, isis_fabricpath-default
via Po15, [115/20], 6 day/s 16:34:26, isis_fabricpath-default
1/1002/0, number of next-hops: 0
via ---- , [60/0], 6 day/s 16:34:26, local
1/1003/0, number of next-hops: 2
via Po13, [115/60], 6 day/s 16:21:18, isis_fabricpath-default
via Po15, [115/60], 6 day/s 16:21:18, isis_fabricpath-default
2/1002/0, number of next-hops: 0
via ---- , [60/0], 6 day/s 16:34:26, local

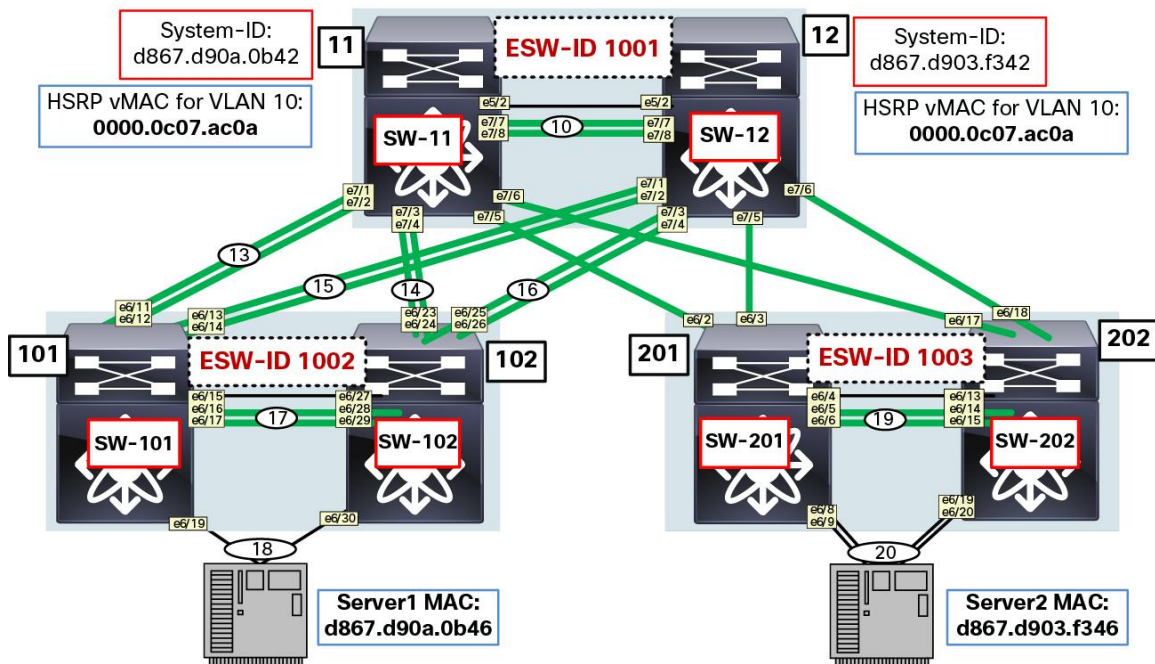
```

Because both HSRP peers are actively forwarding traffic, there is no need to configure preemption, different priorities, and fast hello timers.

Consider an example in which Cisco FabricPath switches with switch IDs 11 and 12 are configured with vPC+, HSRP, and an emulated switch ID (ESW-ID) of 1001 on both peers; Cisco FabricPath switches with switch IDs 101 and 102 are configured with vPC+ and an ESW-ID of 1002; and Cisco FabricPath switches with switch IDs 201 and 202 are configured with vPC+ and an ESW-ID of 1003.

Figure 13 shows the vPC+ components.

Figure 13. vPC+ Example



When a Cisco FabricPath edge switch needs to send a frame to the HSRP virtual MAC (vMAC) address, the MAC address table lookup returns the vPC+ emulated switch ID as the destination switch. Because both vPC+ peers have that emulated switch ID configured, they both can receive and actively route the traffic.

Following is the output of one of the leaf switches with switch ID 201. As you can see, the HSRP vMAC address is originating traffic on behalf of ESW-ID 1001, the Server1 MAC address is originating on behalf of ESW-ID 1002, and the Server2 MAC address is local to that switch:

```
SW-201# sh mac address-table
```

Legend:
 * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
 age - seconds since last seen, + - primary entry using vPC Peer-Link,
 (T) - True, (F) - False

VLAN	MAC Address	Type	age	Secure	NTFY	Ports/SWID.SSID.LID
G -	d867.d903.f344	static	-	F	F	sup-eth1(R)
10	0000.0c07.ac0a	dynamic	30	F	F	1001.0.4306
10	d867.d903.f342	dynamic	30	F	F	12.0.4306
* 10	d867.d903.f346	dynamic	870	F	F	Po20
10	d867.d90a.0b46	dynamic	870	F	F	1002.11.65535

Some additional commands show the system ID and switch ID and ESW-ID association:

```
SW-201# sh fabricpath switch-id
```

FABRICPATH SWITCH-ID TABLE

Legend: '*' - this system

SWITCH-ID	SYSTEM-ID	FLAGS	STATE	STATIC	EMULATED
11	d867.d90a.0b42	Primary	Confirmed	Yes	No
12	d867.d903.f342	Primary	Confirmed	Yes	No
101	d867.d90a.0b44	Primary	Confirmed	Yes	No
102	d867.d90a.0b45	Primary	Confirmed	Yes	No
*201	d867.d903.f344	Primary	Confirmed	Yes	No
202	d867.d903.f345	Primary	Confirmed	Yes	No
1001	d867.d903.f342	Primary	Confirmed	No	Yes
1001	d867.d90a.0b42	Primary	Confirmed	No	Yes
1002	d867.d90a.0b44	Primary	Confirmed	No	Yes
1002	d867.d90a.0b45	Primary	Confirmed	No	Yes
1003	d867.d903.f344	Primary	Confirmed	No	Yes
1003	d867.d903.f345	Primary	Confirmed	No	Yes

Total Switch-ids: 12

In the following output, you can see that a leaf switch with switch ID 201 has two equal-cost paths to ESW-ID 1001:

```
SW-201# sh fabricpath route
FabricPath Unicast Route Table
'a/b/c' denotes ftag/switch-id/subswitch-id
'[x/y]' denotes [admin distance/metric]
ftag 0 is local ftag
subswitch-id 0 is default subswitch-id

FabricPath Unicast Route Table for Topology-Default

0/201/0, number of next-hops: 0
    via ---- , [60/0], 7 day/s 23:36:05, local
0/1003/1, number of next-hops: 0
0/1003/11, number of next-hops: 1
    via Po20, [80/0], 1 day/s 05:19:15, vpcm
1/11/0, number of next-hops: 1
    via Eth6/2, [115/40], 7 day/s 23:24:54, isis_fabricpath-default
1/12/0, number of next-hops: 1
    via Eth6/3, [115/40], 7 day/s 23:24:54, isis_fabricpath-default
1/101/0, number of next-hops: 2
    via Eth6/2, [115/60], 1 day/s 00:49:47, isis_fabricpath-default
    via Eth6/3, [115/60], 7 day/s 23:24:54, isis_fabricpath-default
1/102/0, number of next-hops: 2
    via Eth6/2, [115/60], 7 day/s 23:24:54, isis_fabricpath-default
    via Eth6/3, [115/60], 7 day/s 23:24:54, isis_fabricpath-default
1/202/0, number of next-hops: 1
    via Po19, [115/20], 7 day/s 23:24:54, isis_fabricpath-default
1/1001/0, number of next-hops: 2
    via Eth6/2, [115/40], 7 day/s 23:24:54, isis_fabricpath-default
    via Eth6/3, [115/40], 7 day/s 23:24:54, isis_fabricpath-default
1/1002/0, number of next-hops: 2
    via Eth6/2, [115/60], 7 day/s 23:24:54, isis_fabricpath-default
    via Eth6/3, [115/60], 7 day/s 23:24:54, isis_fabricpath-default
1/1003/0, number of next-hops: 0
    via ---- , [60/0], 7 day/s 23:24:58, local
2/1003/0, number of next-hops: 0
    via ---- , [60/0], 7 day/s 23:24:58, local
```

In a Classic Ethernet environment, in which in a single VLAN only one HSRP gateway can be active at a time, fast failover between the remaining peers is essential. Typically, fast hello timers and preemption is configured to enforce the required behavior. Because In a Cisco FabricPath vPC+ environment, both HSRP peers are actively forwarding, fast hello timers and preemption is no longer required, and configurations can be left at their defaults.

As in Classic Ethernet vPC environments, you should implement a Layer 3 backup routing path between vPC+ peers. This path is used when local Layer 3 uplinks are down, in which case traffic will be redirected to other peer devices.

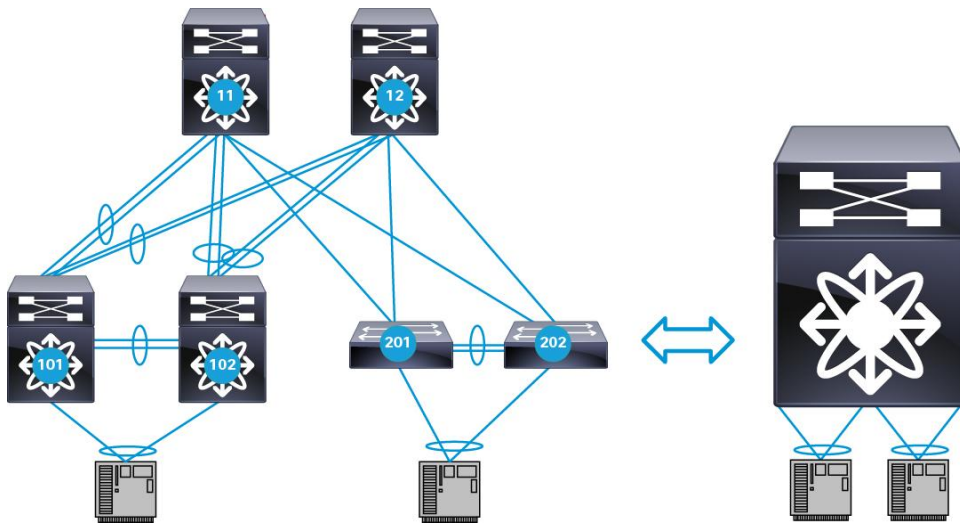
Connecting Devices Other Than Cisco FabricPath Devices at the Edge

Just like the Classic Ethernet vPC feature, Cisco FabricPath vPC+ allows dual-attachment of servers and switches with an industry-standard IEEE LACP or static PortChannel. The examples and console output presented earlier show that the rest of the network sees devices connected with vPC+ as if they were connected to an ESW-ID. For devices other than Cisco FabricPath devices attached with vPC+, both peers of vPC+ domain appear to be a single device. This approach avoids the complexities of spanning-tree domain configurations and prevents the forwarding of spanning-tree topology change notifications (TCNs) through the Cisco FabricPath cloud.

Cisco FabricPath and Spanning Tree Protocol Interaction

The current interaction between Spanning Tree Protocol and Cisco FabricPath is straightforward: the Cisco FabricPath region looks like a single bridge to the Spanning Tree Protocol. When a switch is running Cisco FabricPath, its edge ports automatically enter a mode in which they send the same information (called pseudo-information) in their BPDUs. The root and sender bridge MAC addresses of this pseudo-information are the same on every switch in the Cisco FabricPath domain, even if the information is generated independently by different physical switches. As a result, those BPDUs appear to originate from the same switch: a virtual switch representing the region (Figure 14).

Figure 14. From STP Perspective, FabricPath Domain Looks Like a Single Layer 2 Switch



Another requirement imposed by the Spanning Tree Protocol interaction model is that this virtual bridge must be the root of the spanning tree. The reason for this rule is that if the virtual bridge were not the root, it would have to be capable of receiving better spanning-tree information on an edge port (the root port) and propagating it to the other edge ports running Spanning Tree Protocol. Because one of the goals in the design of Cisco FabricPath was to remove Spanning Tree Protocol from the network, the model avoids the creation of a root port by mandating that the virtual bridge be the root of the spanning tree. Enforcing this restriction is very easy: all ports at the edge of a Cisco FabricPath network are configured with the equivalent of root guard, a feature that would block a port should it receive superior Spanning Tree Protocol BPDUs.

How is this virtual bridge configured as the root bridge? There is no centralized management for this distributed virtual switch. All the switches at the edge of the Cisco FabricPath network need a spanning-tree priority that makes them the root of the network. If all those switches are set up consistently with the same priority, they will send the same, better spanning-tree information on all the edge ports, and the Cisco FabricPath region will look like a virtual switch with a bridge ID of c84c.75fa.6000. The recommended way to set the priority on the edge switches is through the use of the **spanning-tree pseudo-information** command:

```
spanning-tree pseudo-information
root priority 16384
```

Note that the **spanning-tree priority** command would also work; however, it would change the priority for the spanning tree regardless of whether the switch were sending regular BPDUs (when Cisco FabricPath is not running) or sending BPDUs with the pseudo-information (when Cisco FabricPath is operational on the switch). In some scenarios, this change can have undesirable side effects.

Multicast Considerations

IPv6 Neighbor Discovery Protocol relies on neighbor solicitation and neighbor advertisement messages. These messages are sent in multicast Ethernet frames. You must disable IGMP OMF for VLANs that require any IPv6 packet forwarding to enable proper handling of Neighbor Discovery Protocol packets in the network.

Unlike IPv4 networks, IPv6 networks do not have formal broadcast addresses. Packets destined for all nodes in the network are encapsulated with an “all-nodes address”: FF01:0:0:0:0:0:1. Refer to <http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml> **IPv6 Multicast Address Space Registry** for details. The inability to send multicast frames while OMF is enabled for a specific VLAN stops IPv6 forwarding completely:

```
SW-201(config)# no ip igmp snooping optimise-multicast-flood
```

Timer Tuning

The linkup delay timer starts when the Cisco FabricPath core link is brought up. After the timer expires, the Cisco FabricPath switch starts shortest-path-first (SPF) calculations. You can configure the timer with a value greater than default value (the default value is 10) to give switch time to complete initial CPU-intensive tasks that need to be accomplished when switch is cold booted. After the timer expires, the system has more available CPU cycles and SPF processing runs faster, leading to faster convergence.

Another way to achieve faster convergence is to lower the maximum time that the shortest-path-first algorithm takes to perform calculations. By default, the SP interval and link-state packet (LSP) generation interval maximum wait times are set to 8 seconds. If you lower these timers to 50 milliseconds (ms), the SPF algorithm does not need wait the default 8 seconds before it can start generating LSP updates and start topology computations. Overall, this approach will lead to faster convergence at the cost price of more intense CPU utilization.

For example, consider what happens if one of the spine switches (SW-ID 11) loses power and then comes back up. After the supervisors and I/O modules are initialized, Cisco FabricPath IS-IS starts tracking interfaces. After the interfaces come up, Cisco FabricPath IS-IS uses the timers, among other parameters, to start generating LSP updates, and after the LSP updates are received from other switches, to start computing topology. There may be other processes that consume CPU cycles, and to avoid high CPU utilization, the IS-IS SPF algorithm does not calculate topology right away, but waits for expiration of up to the maximum SPF-interval timer. With the default configuration of 8 seconds, in some cases convergence may take a long time.

Lowering this timer to 50ms forces the SPF algorithm to run more often, providing faster convergence. You should remember, however, that in topologies with large numbers of switches and links, this approach may spike the CPU load.

With the continuous development of the protocol, Cisco FabricPath will introduce an overload bit in an upcoming software release. The overload bit serves the same purpose as in the IPv4 IS-IS protocol. The overload bit prevents other peers in the network from using the originating switch as a transit path. Upon switch restart, all LSP updates sent from that switch will contain the overload bit, and other peers will converge with this switch; however, they will not use it as a transit path. After a preconfigured amount of time passes, the originating switch will remove the overload bit from the LSP updates, and peers will begin using the switch as a transit path for data traffic.

Switch Configuration

This section presents configurations for switches in the sample topology.

SW-11

```
SW-11# sh running-config

!Command: show running-config
!Time: Tue Apr 23 03:34:22 2013

version 6.1(2)
feature-set fabricpath
hostname SW-11

feature telnet
cfs eth distribute
feature interface-vlan
feature hsrp
feature lacp
feature vpc

username admin password 5 $1$jYrGH1de$SOOZJwUJvt4D741eGmrRG. role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x528fe13771ce847ccd784ce9353139e3 priv
0x528fe13771ce847ccd784ce9353139e3 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vrf context PKL
vrf context management
vlan 1,10-100,110-200
```

```
vlan configuration 10
vlan 10-100
    mode fabricpath

fabricpath timers linkup-delay 60
fabricpath switch-id 11
vpc domain 101
    peer-keepalive destination 10.10.10.2 source 10.10.10.1 vrf PKL
    fabricpath switch-id 1001

interface Vlan1

interface Vlan10
    no shutdown
    ip address 10.100.10.253/24
    hsrp 10
        ip 10.100.10.1

interface port-channel10
    description vPC+ Peer-Link
    switchport
    switchport mode fabricpath
    vpc peer-link

interface port-channel13
    switchport
    switchport mode fabricpath

interface port-channel14
    switchport
    switchport mode fabricpath

interface Ethernet5/1

interface Ethernet5/2
    vrf member PKL
    ip address 10.10.10.1/30
    no shutdown

interface Ethernet5/3

interface Ethernet5/4
```

```
interface Ethernet5/5

interface Ethernet5/6

interface Ethernet5/7

interface Ethernet5/8

interface Ethernet5/9

interface Ethernet5/10

interface Ethernet5/11

interface Ethernet5/12

interface Ethernet5/13

interface Ethernet5/14

interface Ethernet5/15

interface Ethernet5/16

interface Ethernet7/1
  switchport mode fabricpath
  channel-group 13 mode active
  no shutdown

interface Ethernet7/2
  switchport mode fabricpath
  channel-group 13 mode active
  no shutdown

interface Ethernet7/3
  switchport mode fabricpath
  channel-group 14 mode active
  no shutdown

interface Ethernet7/4
  switchport mode fabricpath
  channel-group 14 mode active
  no shutdown
```

```
interface Ethernet7/5
  switchport mode fabricpath
  no shutdown

interface Ethernet7/6
  switchport mode fabricpath
  no shutdown

interface Ethernet7/7
  switchport mode fabricpath
  channel-group 10 mode active
  no shutdown

interface Ethernet7/8
  switchport mode fabricpath
  channel-group 10 mode active
  no shutdown

interface Ethernet7/9

interface Ethernet7/10

interface Ethernet7/11

interface Ethernet7/12

interface Ethernet7/13

interface Ethernet7/14

interface Ethernet7/15

interface Ethernet7/16

interface mgmt0
  ip address 10.1.1.11/24
  logging server 10.1.1.254 5 use-vrf management
  line vty
    exec-timeout 0
  fabricpath domain default
  root-priority 200
```

SW-12

```
SW-12#
SW-12# sh running-config

!Command: show running-config
!Time: Tue Apr 23 09:34:51 2013

version 6.1(2)
feature-set fabricpath
hostname SW-12

feature telnet
cfs eth distribute
feature interface-vlan
feature hsrp
feature lacp
feature vpc

username admin password 5 $1$PJNEU3Zp$7bFzJ7oakC0k3IrgsV53z. role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xa3bb1cb3e8b595a5cd7116c113db173c priv
0xa3bb1cb3e8b595a5cd7116c113db173c localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vrf context PKL
vrf context management
vlan 1,10-100,110-200
vlan 10-100,110-200
  mode fabricpath

fabricpath switch-id 12
vpc domain 101
  peer-keepalive destination 10.10.10.1 source 10.10.10.2 vrf PKL
  fabricpath switch-id 1001

interface Vlan1
```

```
interface Vlan10
  no shutdown
  ip address 10.100.10.254/24
  hsrp 10
    ip 10.100.10.1

interface port-channel10
  description vPC+ Peer-link
  switchport
  switchport mode fabricpath
  vpc peer-link

interface port-channel15
  switchport
  switchport mode fabricpath

interface port-channel16
  switchport
  switchport mode fabricpath

interface Ethernet5/1

interface Ethernet5/2
  vrf member PKL
  ip address 10.10.10.2/30
  no shutdown

interface Ethernet5/3

interface Ethernet5/4

interface Ethernet5/5

interface Ethernet5/6

interface Ethernet5/7

interface Ethernet5/8

interface Ethernet5/9

interface Ethernet5/10

interface Ethernet5/11
```

```
interface Ethernet5/12

interface Ethernet5/13

interface Ethernet5/14

interface Ethernet5/15

interface Ethernet5/16

interface Ethernet7/1
  switchport mode fabricpath
  channel-group 15 mode active
  no shutdown

interface Ethernet7/2
  switchport mode fabricpath
  channel-group 15 mode active
  no shutdown

interface Ethernet7/3
  switchport mode fabricpath
  channel-group 16 mode active
  no shutdown

interface Ethernet7/4
  switchport mode fabricpath
  channel-group 16 mode active
  no shutdown

interface Ethernet7/5
  switchport mode fabricpath
  no shutdown

interface Ethernet7/6
  switchport mode fabricpath
  no shutdown

interface Ethernet7/7
  switchport mode fabricpath
  channel-group 10 mode active
  no shutdown
```

```
interface Ethernet7/8
  switchport mode fabricpath
  channel-group 10 mode active
  no shutdown

interface Ethernet7/9

interface Ethernet7/10

interface Ethernet7/11

interface Ethernet7/12

interface Ethernet7/13

interface Ethernet7/14

interface Ethernet7/15

interface Ethernet7/16

interface mgmt0
  ip address 10.1.1.21/24
  logging server 10.1.1.254 5 use-vrf management
  line vty
    exec-timeout 0
  fabricpath domain default
  root-priority 190
```

SW-101

```
SW-101# sh running-config

!Command: show running-config
!Time: Tue Apr 23 03:39:16 2013

version 6.1(2)
feature-set fabricpath
hostname SW-101

feature telnet
cfs eth distribute
feature lacp
feature vpc
```



```
username admin password 5 $1$Pi9vrvbw$wAnLOtbsEKektF2fulAJ60 role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xaa2b473e3bb92447eb971c499cddce38 priv
0xaa2b473e3bb92447eb971c499cddce38 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vrf context PKL
vrf context management
vlan 1,10-100,110-200
vlan 10-100
mode fabricpath

fabricpath switch-id 101
vpc domain 102
 peer-keepalive destination 10.10.2.2 source 10.10.2.1 vrf PKL
 fabricpath switch-id 1002

interface port-channel13
 switchport
 switchport mode fabricpath
 fabricpath isis metric 20

interface port-channel15
 switchport
 switchport mode fabricpath

interface port-channel17
 description vPC+ Peer-link
 switchport
 switchport mode fabricpath
 vpc peer-link

interface port-channel18
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 10-100
 vpc 18
```

```
interface Ethernet6/9

interface Ethernet6/10

interface Ethernet6/11
  switchport
  switchport mode fabricpath
  channel-group 13 mode active

interface Ethernet6/12
  switchport
  switchport mode fabricpath
  channel-group 13 mode active
  no shutdown

interface Ethernet6/13
  switchport
  switchport mode fabricpath
  channel-group 15 mode active
  no shutdown

interface Ethernet6/14
  switchport
  switchport mode fabricpath
  channel-group 15 mode active
  no shutdown

interface Ethernet6/15
  vrf member PKL
  ip address 10.10.2.1/30
  no shutdown

interface Ethernet6/16
  switchport
  switchport mode fabricpath
  channel-group 17 mode active
  no shutdown

interface Ethernet6/17
  switchport
  switchport mode fabricpath
  channel-group 17 mode active
  no shutdown
```

```
interface Ethernet6/18

interface Ethernet6/19
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  channel-group 18 mode active
  no shutdown

interface Ethernet6/20

interface mgmt0
  ip address 10.1.1.13/24
line vty
  exec-timeout 0
fabricpath domain default
  root-priority 150
```

SW-102

```
SW-102# sh running-config

!Command: show running-config
!Time: Tue Apr 23 03:40:40 2013

version 6.1(2)
feature-set fabricpath
hostname SW-102

feature telnet
cfs eth distribute
feature lacp
feature vpc

username admin password 5 $1$D3q7uNV7$gjb.34cW/OZNH1szlurvpl. role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x92043a687294cd5f44785cc3076b250f priv
0x92043a687294cd5f44785cc3076b250f localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
```

```
vrf context PKL
vrf context management
vlan 1,10-100,110-200
vlan 10-100
  mode fabricpath

fabricpath switch-id 102
vpc domain 102
  peer-keepalive destination 10.10.2.1 source 10.10.2.2 vrf PKL
  fabricpath switch-id 1002

interface port-channel14
  switchport
  switchport mode fabricpath

interface port-channel16
  switchport
  switchport mode fabricpath

interface port-channel17
  description vPC+ Peer-link
  switchport
  switchport mode fabricpath
  vpc peer-link

interface port-channel18
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  vpc 18

interface Ethernet6/21

interface Ethernet6/22

interface Ethernet6/23
  switchport
  switchport mode fabricpath
  channel-group 14 mode active
  no shutdown

interface Ethernet6/24
  switchport
```

```
switchport mode fabricpath
channel-group 14 mode active
no shutdown

interface Ethernet6/25
switchport
switchport mode fabricpath
channel-group 16 mode active
no shutdown

interface Ethernet6/26
switchport
switchport mode fabricpath
channel-group 16 mode active
no shutdown

interface Ethernet6/27
vrf member PKL
ip address 10.10.2.2/30
no shutdown

interface Ethernet6/28
switchport
switchport mode fabricpath
channel-group 17 mode active
no shutdown

interface Ethernet6/29
switchport
switchport mode fabricpath
channel-group 17 mode active
no shutdown

interface Ethernet6/30
switchport
switchport mode trunk
switchport trunk allowed vlan 10-100
channel-group 18 mode active
no shutdown

interface Ethernet6/31

interface Ethernet6/32
```

```
interface mgmt0
  ip address 10.1.1.14/24
line vty
  exec-timeout 0
fabricpath domain default
```

SW-201

```
SW-201# sh running-config

!Command: show running-config
!Time: Tue Apr 23 09:37:40 2013

version 6.1(2)
feature-set fabricpath
hostname SW-201

feature telnet
cfs eth distribute
feature lacp
feature vpc

username admin password 5 $1$/dnxKH9p$8wmpSmOUgfIah84R6bOQ.1 role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x747b6191c960ad74ccc56edd325cabae priv
0x747b6191c960ad74ccc56edd325cabae localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vrf context PKL
vrf context management
vlan 1,10-200
vlan configuration 10
  no ip igmp snooping optimise-multicast-flood
vlan 10-109
  mode fabricpath

fabricpath switch-id 201
vpc domain 103
  peer-keepalive destination 10.10.3.2 source 10.10.3.1 vrf PKL
  fabricpath switch-id 1003
```

```
interface port-channel19
  description vPC+ Peer-link
  switchport
  switchport mode fabricpath
  vpc peer-link

interface port-channel20
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  vpc 20

interface Ethernet6/1

interface Ethernet6/2
  switchport
  switchport mode fabricpath
  no shutdown

interface Ethernet6/3
  switchport
  switchport mode fabricpath
  no shutdown

interface Ethernet6/4
  vrf member PKL
  ip address 10.10.3.1/30
  no shutdown

interface Ethernet6/5
  switchport
  switchport mode fabricpath
  channel-group 19 mode active
  no shutdown

interface Ethernet6/6
  switchport
  switchport mode fabricpath
  channel-group 19 mode active
  no shutdown

interface Ethernet6/7
```

```
interface Ethernet6/8
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  channel-group 20 mode active
  no shutdown

interface Ethernet6/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10-100
  channel-group 20 mode active
  no shutdown

interface Ethernet6/10

interface Ethernet6/11

interface Ethernet6/12

interface mgmt0
  ip address 10.1.1.23/24
  line vty
  exec-timeout 0
  fabricpath domain default
```

SW-202

```
SW-202# sh running-config

!Command: show running-config
!Time: Tue Apr 23 09:38:06 2013

version 6.1(2)
feature-set fabricpath
hostname SW-202

feature telnet
cfs eth distribute
feature lacp
feature vpc

username admin password 5 $1$C9Q8924.$SCTLWrmdrkJi/0FAFk5P50 role vdc-admin
no password strength-check
```



```
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x6bfba7f3f042285bdc33277616c2fe97 priv
0x6bfba7f3f042285bdc33277616c2fe97 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vrf context PKL
vrf context management
vlan 1,10-100,110-200
vlan 10-100
    mode fabricpath

fabricpath switch-id 202
vpc domain 103
    peer-keepalive destination 10.10.3.1 source 10.10.3.2 vrf PKL
    fabricpath switch-id 1003

interface port-channel19
    description vPC+ Peer-link
    switchport
    switchport mode fabricpath
    vpc peer-link

interface port-channel20
    switchport
    switchport mode trunk
    switchport trunk allowed vlan 10-100
    vpc 20

interface Ethernet6/13
    vrf member PKL
    ip address 10.10.3.2/30
    no shutdown

interface Ethernet6/14
    switchport
    switchport mode fabricpath
    channel-group 19 mode active
    no shutdown

interface Ethernet6/15
```

```
switchport
switchport mode fabricpath
channel-group 19 mode active
no shutdown

interface Ethernet6/16

interface Ethernet6/17
switchport
switchport mode fabricpath
no shutdown

interface Ethernet6/18
switchport
switchport mode fabricpath
no shutdown

interface Ethernet6/19
switchport
switchport mode trunk
switchport trunk allowed vlan 10-100
channel-group 20 mode active
no shutdown

interface Ethernet6/20
switchport
switchport mode trunk
switchport trunk allowed vlan 10-100
channel-group 20 mode active
no shutdown

interface Ethernet6/21

interface Ethernet6/22

interface Ethernet6/23

interface Ethernet6/24

interface mgmt0
ip address 10.1.1.24/24
line vty
exec-timeout 0
fabricpath domain default
```




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)