APPENDIX **D**

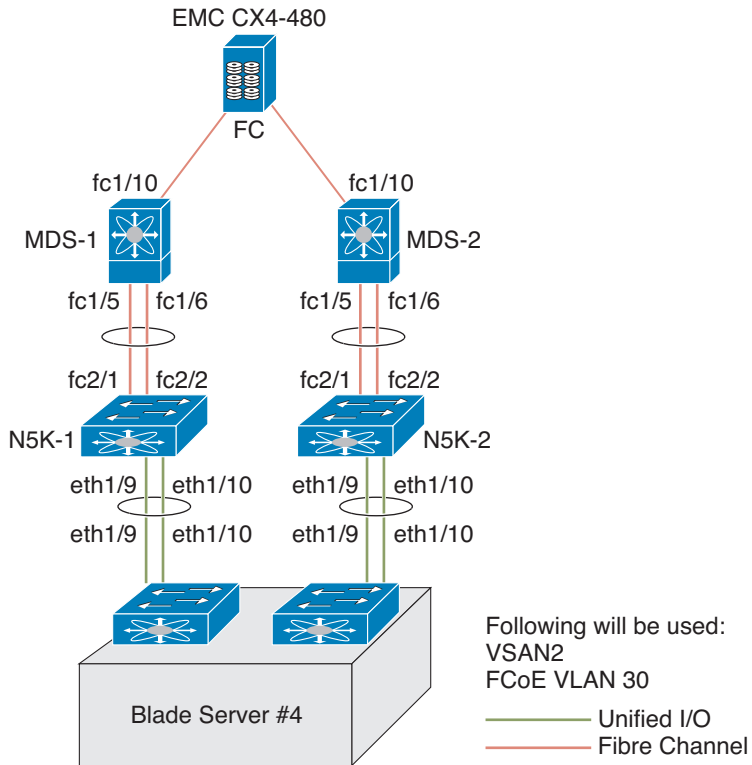# FCoE with Cisco Nexus 4000 Series Switch Configuration Example

This section includes a configuration example on how to configure an IBM blade server connecting to a Cisco Nexus 4000 Series switch which is then connected to a Cisco Nexus 5000 Series switch which accesses FC storage on a Cisco MDS 9000 Series Family switch using FCoE. Because the Cisco Nexus 4000 Series switch is a FIP snooping bridge, the FLOGI done by the CNAs do not login on the Cisco Nexus 4000 Series switch but onto the Cisco Nexus 5000 Series switch, which is the FCF. Creation of the vFC interface for the Cisco Nexus 4000 Series switch blade servers does not change whether the Cisco Nexus 5000 Series switch is in switching or NPV mode. Where the actual fabric login happens is determined by the mode on the Cisco Nexus 5000 Series switch.

- Cisco Nexus 5000 Series switch in switching mode—Login is on the Cisco Nexus 5000 Series switch.

- Cisco Nexus 5000 Series switch in NPV mode—Login will be on the Cisco MDS 9000 Series Family switch or any FC switch upstream with NPIV configured.

In this example, the Cisco Nexus 5000 Series switch in switching mode. Figure D-1 shows the topology used in the example.

Figure D-1   Nexus 4000 FCoE Lab Topology

The following hardware was used:

- IBM Blade Chassis model BCH
- IBM HS22 blade server running Windows 2003 using the Qlogic QMI8142
- Cisco Nexus 4000 Series switch running Cisco NX-OS Release 4.1(2)E1(1)
- Cisco Nexus 5010 switch running Cisco NX-OS Release 4.1(3)N1(1)
- Cisco MDS 9124 Director switch running Cisco SAN-OS Release 4.1(3a)
- EMC CX4-480

This appendix includes the following sections:

Cisco Nexus 5000 Series Switch in Switching Mode

Before following the steps in this example, be sure to complete a basic configuration on the Cisco Nexus 5000 Series switch (for example, IP Address (mgmt0), switch name, and password for the administrator) and FCoE has not been enabled.

To use this configuration example in production, you must have the FC Features Package license installed otherwise there will be a temporary license that expires after 90 days. When the license expires, the feature is disabled.

On the Cisco Nexus 5000 Series switch, by default FCoE is not enabled.

This example shows how to enable FCoE:

```
n5k-2# show interface brief
-------------------------------------------------------------------------------------
-----------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface                Ch #
Eth1/1 1 eth access up none 10G(D) --
Eth1/2 1 eth access up none 10G(D) --
[snip]
Eth2/4 1 eth access down SFP not inserted 10G(D) --
-------------------------------------------------------------------------------
Port VRF Status IP Address Speed MTU
-------------------------------------------------------------------------------
mgmt0 -- up 172.25.182.164 1000 1500
```

Note   There are no FC interfaces, even though there is a 4x4 GEM card installed in the Cisco Nexus 5010 switch.

```
n5k-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n5k-2(config)# feature fcoe
FC license checked out successfully fc_plugin extracted successfully FC plugin loaded
successfully FCoE manager enabled successfully FC enabled on all modules successfully
```

Note   Beginning with Cisco NX-OS Release 4.1(3)N1(1), the switch does not need to be reboot when you enable FCoE. The Cisco Nexus 5000 Series switch is in switching mode by default when FCoE is enabled.

```
n5k-2(config)# show feature
Feature Name Instance State
fcsp 1 disabled
fcoe 1 enabled
fex 1 enabled

n5k-2(config)# show interface brief
-------------------------------------------------------------------------------------
-----------------------
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
-------------------------------------------------------------------------------------
-----------------------
fc2/1 1 auto on down swl -- --
fc2/2 1 auto on down swl -- --
fc2/3 1 auto on down swl -- --
fc2/4 1 auto on sfpAbsent -- -- --
```

```
--------------------------------------------------------------------------------
--------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
--------------------------------------------------------------------------------
--------------------
Eth1/1 1 eth access up none 10G(D) --
Eth1/2 1 eth access up none 10G(D) --
```

Note   Use the **show interface brief** command to show the FC interfaces.

Configuring a SAN Port Channel on the Cisco Nexus 5000 Series Switch to the Cisco MDS Directory Series

This example shows how to configure a SAN port channel on the Cisco Nexus 5000 Series switch that is connected to a Cisco MDS 9000 Director. For redundancy, Cisco recommends that you create a SAN port channel from the FC interfaces.

Step 1   Configure a SAN port channel on the Cisco Nexus 5000 Series switch.

```
Fn5k-2# configure terminal
n5k-2(config)# interface san-port-channel 1
n5k-2(config-if)# interface fc2/1-2
n5k-2(config-if)# channel-group 1
```

Note   After you add fc2/1 fc2/2 to san-port-channel 1 you need to disable the port channel. This must also be done on the switch at the other end of the port channel. Then, shut the interfaces at both ends to bring them up.

```
n5k-2(config-if)# no shut
n5k-2(config-if)# interface san-port-channel 1
n5k-2(config-if)# no shut
n5k-2(config-if)# show san-port-channel database
san-port-channel 1
Administrative channel mode is on Operational channel mode is on Last membership
update is successful 2 ports in total, 0 ports up Age of the port-channel is
0d:00h:17m:14s
Ports: fc2/1 [down] fc2/2 [down]
n5k-2(config-if)#
```

Note   The SAN port channel is currently down because the Cisco MDS 9000 Series Director has not been configured.

Step 2   Configure the Cisco MDS 9124 switch to create a port channel between the Cisco Nexus 5000 Series switch and the Cisco MDS 9124 switch.

Note   With the SAN port channel on the Cisco Nexus 5000 configured to the MDS, you will need to perform the same configuration on the Cisco MDS 9000 Series switch. A SAN port channel configuration on the Cisco MDS 9000 Series switch is called a port channel.

```
mds9124-2# configure terminal
```

```
mds9124-2(config)# interface port-channel 1
mds9124-2(config-if)# interface fc1/5, fc1/6
mds9124-2(config-if)# channel-group 1 force
```

Note After you add fc1/5 fc1/6 to port-channel 1 you need to disable the port channel. This must also be done on the switch at the other end of the port channel. Then, shut the interfaces at both ends to bring them up.

Note

```
mds9124-2(config-if)# no shut
mds9124-2(config-if)# interface port-channel 1
mds9124-2(config-if)# no shut
```

Step 3 Verify that the SAN port channel on the Cisco Nexus 5000 Series switch is up and running. Use the **show san-port-channel database** command to show the SAN port channel configuration.

```
n5k-2(config-if)# show san-port-channel database
san-port-channel 1
Administrative channel mode is on
Operational channel mode is on
Last membership update is successful
2 ports in total, 2 ports up
First operational port is fc2/2
Age of the port-channel is 0d:00h:25m:10s
Ports: fc2/1 [up]
fc2/2 [up] *
```

Configuring a Port Channel on a Cisco Nexus 5000 Series Switch to a Cisco Nexus 4000 Series Switch

This example shows how to configure a port channel on the Cisco Nexus 5000 Series switch that is connected to the Cisco Nexus 4000 Series switch.

Step 1 Configure the port channel on the Cisco Nexus 5000 Series switch.

The port channel is configured to provide redundancy for traffic coming from the Cisco Nexus 4000 Series switch to the Cisco Nexus 5000 Series switch. In this example, all VLANs can traverse the port channel. The FCoE VLAN and the native VLAN must be allowed to traverse the port channel.In production environments, Network Administrators may designate other VLANs to traverse this network.

```
n5k-2# configure terminal
n5k-2(config)# feature lacp
n5k-2(config)# interface port-channel 2 mode active
n5k-2(config-if)# interface eth1/9-10
n5k-2(config-if)# channel-group 2
n5k-2(config)# interface port-channel 2
n5k-2(config-if)# switchport mode trunk
n5k-2(config-if)# no shut
n5k-2#
```

Step 2 Configure the port channel on the Cisco Nexus 4000 Series switch.

```
bch1-n4k-b9# configure terminal
bch1-n4k-b9(config)# feature lacp
bch1-n4k-b9(config)# interface port-channel 20
```

```
bch1-n4k-b9(config-if)# interface eth1/15-16
bch1-n4k-b9(config-if)# channel-group 2 mode active
bch1-n4k-b9(config)# interface port-channel 2
bch1-n4k-b9(config-if)# switchport mode trunk
bch1-n4k-b9(config-if)# no shut
bch1-n4k-b9(config-if)#
```

Configuring a Virtual Fibre Channel Interface on a Cisco Nexus 4000 Series Switch

This example shows how to configure a vFC interface on a Cisco Nexus 4000 Series switch.

Step 1   On the Cisco Nexus 5000 Series switch, configure a VSAN to match the production VSAN on the Cisco MDS 9000 Series switch. This is a one-time configuration.

Step 2   On the Cisco Nexus 5000 Series switch, configure an FCoE VLAN to map to the VSAN (VLAN-to-VSAN mapping). This is one-time configuration.

Step 3   On the Cisco Nexus 4000 Series switch, configure a FIP snooping VLAN that matches the FCoE VLAN on the Nexus 5000 Series switch. This is a one-time configuration.

Step 4   On the Cisco Nexus 4000 Series switch, configure the uplinks to allow FCoE traffic (FIP snooping).

Step 5   On the Cisco Nexus 4000 Series switch blade server, configure the Ethernet interfaces for FCoE traffic.

Step 6   On the Cisco Nexus 5000 Series switch, configure the vFCs.

Step 7   On the Cisco Nexus 4000 Series switch blade server, bind the vFC to the MAC address of the blade server.

Step 8   Verify that the vFC is in the correct VSAN.

Note   Completing the above tasks ensure that the connection to an FCoE CNA on the blade server from the Nexus 4000 is successful.

Configuring a VSAN on the Cisco Nexus 5000 Series Switch

You can configure a VSAN on the Cisco Nexus 5000 Series switch using Fabric Manager, Device Manager, or the CLI. This example shows CLI configuration tasks and Fabric Manager or Device Manager GUI tasks.

This example shows the storage on the Cisco MDS 9000 Series resides on VSAN 2. Configure the VSAN to ensure that the vFCs configured on the Cisco Nexus 5000 Series switch can communicate with the storage device.

```
n5k-2# configure terminal
n5k-2(config)# vsan database
n5k-2(config-vsan-db)# vsan 2
n5k-2(config-vsan-db)# show vsan vsan 1 information
name:VSAN0001 state:active
interoperability mode:default
loadbalancing:src-id/dst-id/oxid
operational state:up
vsan 2 information
```

```
name:VSAN0002 state:active
interoperability mode:default
loadbalancing:src-id/dst-id/oxid
 operational state:down
        vsan 4079:evfp_isolated_vsan
        vsan 4094:isolated_vsan
```

Configuring An FCoE VLAN on the Cisco Nexus 5000 Series Switch

You can configure a VLAN and then map the VLAN to a particular VSAN using the CLI. Fabric Manager and Device Manager can not be used for this configuration. Cisco recommends that you configure a separate VLAN for FCoE traffic and separate VLANs for standard Ethernet traffic.

This example shows how to create the FCoE VLAN:

```
n5k-2# configure terminal
        n5k-2(config)# vlan 30
        n5k-2(config-vlan)# fcoe vsan 2
        n5k-2(config-vlan)# show vlan fcoe
VLAN
VSAN
Status
--------
--------
--------
30
2
Operational
```

Configuring a FIP Snooping VLAN on the Cisco Nexus 4000 Series Switch

On the Cisco Nexus 4000 Series switch, by default the FIP snooping feature is disabled. Cisco recommends that during the basic configuration, when prompted, you should enable FCoE and FIP snooping and configure, for example, the appropriate Class of Service (CoS) no drop, MTU, and QoS, without having to manually configure these features after the initial configuration.

The example shows how to verify that FIP snooping is enabled:

```
bch1-n4k-b9# show feature
Feature Name Instance State
tacacs 1 disabled lacp 1 enabled [snip] fipsm 1 enabled
```

With the FCoE VLAN configured on the Cisco Nexus 5000 Series switch as VLAN 30, then the same VLAN number must be used to create the VLAN on the Cisco Nexus 4000 Series switch and the VLAN must be configured as a FIP snooping VLAN.

This example shows how to configure the VLAN on the Cisco Nexus 4000 Series switch:

```
bch1-n4k-b9# configure terminal
bch1-n4k-b9(config)# vlan 30
bch1-n4k-b9(config-vlan)# fip-snooping enable
```

Send documentation comments to n5kdocfeedback@cisco.com

Configuring the Cisco Nexus 4000 Series Switch Uplinks To Allow FCoE Traffic

In this example, we have already created the port channel that allows all VLANs to traverse the uplink between the Cisco Nexus 4000 Series switch and the Cisco Nexus 5000 Series switch from the previous section. The uplink (in this case a port channel) must be enabled to do FIP snooping with a port type mode of fcf.

This example shows how to configure the uplink:

```
bch1-n4k-b9# configure terminal
bch1-n4k-b9(config)# interface port-channel 20
bch1-n4k-b9(config-if)# fip-snooping port-mode fcf
```

Configuring Blade Server Ethernet Interfaces on the Cisco Nexus 4000 Series Switch For FCoE Traffic

You can configure the blade server using the CLI. Fabric Manager and Device Manager can not be used for this configuration.

Ensure that the FCoE VLAN (VLAN 30) can traverse the Ethernet interface on the blade server (Ethernet 1/4). In most cases, the CNA ports allow for both regular Ethernet traffic and FCoE traffic that resides on different VLANs. By default, all Ethernet interfaces on the Cisco Nexus 4000 Series switch is in access mode and resides on VLAN 1.

This example shows how to configure the Ethernet interface to allow multiple VLANs (trunk):

```
bch1-n4k-b9#configure terminal
bch1-n4k-b9(config)#interface ethernet 1/4
bch1-n4k-b9(config-if)# switchport mode trunk
bch1-n4k-b9(config-if)# switchport trunk allowed vlan 1,30
```

✎
Note   The above command is not needed but if you want to specify the allowed VLANs, make sure the FCoE VLAN is on the allowed list as shown in the example.

```
bch1-n4k-b9(config-if)# spanning-tree port type edge trunk
Warning: Edge port type (portfast) should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this  interface when
edge port type (portfast) is enabled, can cause temporary bridging loops.
Use with CAUTION

Creating vFC Interfaces on the Nexus 5000 - CLI
```

When the trunk configuration is complete, create the vFC interface on the Cisco Nexus 5000 Series switch. You can use Device Manager or the CLI to configure the vFC interface.

Because the CNA is connected on Ethernet interface eth1/4 on the Cisco Nexus 4000 Series switch and is not physically connected to the Cisco Nexus 5000 Series switch, you must bind the vFC to the MAC address of the CNA that is doing FCoE. At this time, Qlogic is the only vendor that does FCoE on the blade server that is interoperable with the Cisco Nexus 4000 Series switch. Qlogic provides 2 separate MAC addresses, one for the standard Ethernet traffic and another specifically for FCoE.

This example shows how to identify the MAC address from the specific blade server in the IBM blade chassis.

```
bch1-n4k-b9# show fip-snooping vlan-discovery
 Legend:
Interface VLAN FIP MAC
Eth1/4 1 00:c0:dd:04:0c:df
 Eth1/5 1 00:c0:dd:04:0d:13
```

Use the MAC address that has been identified on the blade server to create the vFC for this blade server on the Cisco Nexus 5000 series switch.

This example shows that the vFC is moved into VSAN 2. As a best practice in creating the vFC number to devices on the Cisco Nexus 4000 Series switch, you should create a numbering scheme that can easily identify where the vFCs are mapped to which blade server on which blade chassis. For this example, we are using the blade server in slot 4 on the first IBM blade chassis, which we have named BCH1. In this example, the vFC for this blade server is interface vfc104.

```
n5k-2# configure terminal
n5k-2(config)# interface vfc 104
n5k-2(config-if)# bind mac-address 00:c0:dd:04:0c:df
n5k-2(config-if)# no shutdown
n5k-2(config-if)# show vsan membership
vsan 1 interfaces:
fc2/1 fc2/2 fc2/3 fc2/4 san-port-channel 1 vfc104
vsan 2 interfaces:
vsan 4079(evfp_isolated_vsan) interfaces:
vsan 4094(isolated_vsan) interfaces:
n5k-2(config-if)# vsan database ð
this will get to the VSAN database
 n5k-2(config-vsan-db)# vsan 2 interface vfc104
n5k-2(config-vsan-db)# show vsan membership
vsan 1 interfaces: fc2/1 fc2/2 fc2/3 fc2/4 san-port-channel 1
 vsan 2 interfaces:
vfc104
vsan 4079(evfp_isolated_vsan) interfaces:
n5k-2# show interface vfc104
vfc104 is up
```

Bound MAC is 00:c0:dd:04:0c:df FCF priority is 128 Hardware is Virtual Fibre Channel Port WWN is 20:67:00:0d:ec:b2:b9:bf Admin port mode is F, trunk mode is on snmp link state traps are enabled Port mode is F, FCID is 0xcd0000 Port vsan is 2 [snip]

Configuring The vFC Interface Using Device Manager

This example shows how to use Device Manager to create the vFC interface.

*Send documentation comments to n5kdocfeedback@cisco.com*

Step 1   Open Device Manager and login to the Cisco Nexus 5000 Series switch.

*Figure D-2   Device Manager Login Window*

Step 2   From the Device Manager menu, choose Interface > Virtual Interfaces > Fibre Channel to configure one vFC. You can also use the Quick Configuration Tool to configure multiple vFCs and bind them to physical interfaces at one time.

Figure D-3   Device Manager Menu
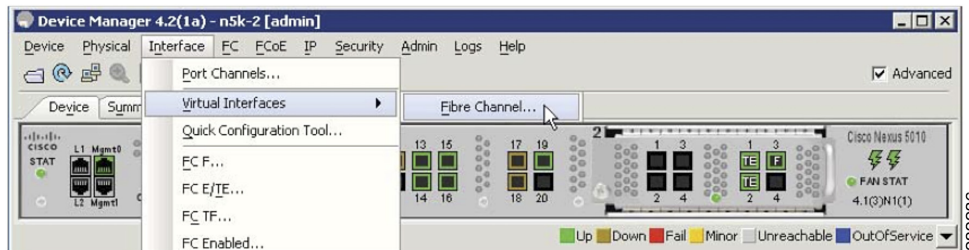
Step 3   From the Virtual FC Interfaces window, click Create to create the vFC.

Figure D-4   Virtual FC Interfaces Window
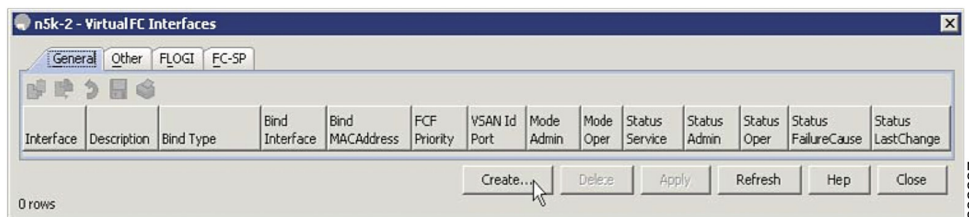
Step 4   In the Create Virtual FC Interfaces General window, enter the VFC Id, Bind Type and the interface (physical or MAC address depending on the bind type) and click Create. The window is redisplayed showing the vFCs with the new vFC ID.

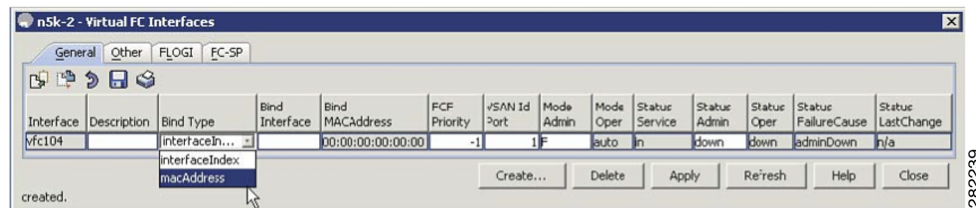*Figure D-5   Create Virtual FC Interfaces General Window*
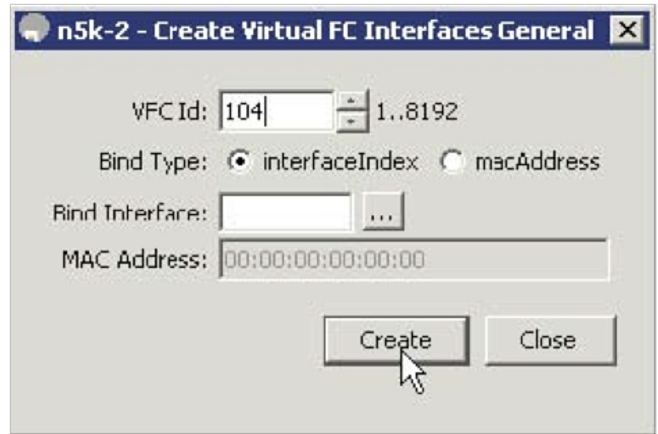
> **Note** As a best practice, create a vFC that is recognizable of the vFC back to the blade server. For example, 104 correlates to BCH1 on blade server 4.

**Step 5** From the Virtual FC Interfaces window, choose Bind Type > macAddress.

Figure D-6   Changing The Bind Type From Interface to Mac Address

Once the Bind Type is set to macAddress, you can enter the MAC address for the blade server in the Bind MAC Address column. In this example, 00:c0:dd:04:0c:df is the MAC address. By default, the VSAN membership is set down and VSAN 1. You can edit these sections for example, VSAN 2 and up).

Step 6 Click on Apply to commit the changes and then click Refresh to validate the vFC is up.

Figure D-7   The Configured vFC MAC Address in Device Manager
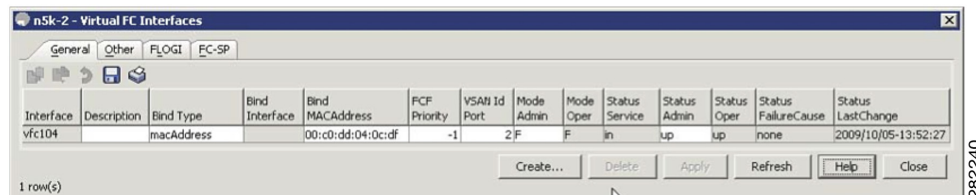
This completes the configuration of FCoE on the Cisco Nexus 4000 Series switch uplinked to the Cisco Nexus 5000 Series switch. The fabric management, for example, zoning and LUN masking, is managed with the existing SAN administrators tools. The vFC appear in Fabric Manager as a normal FC device but instead of a solid line to the host, a dash line is shown from the Cisco Nexus 5000 Series switch to the host.

Send documentation comments to n5kdocfeedback@cisco.com

Figure D-8   Fabric Manager View With FCoE Devices