

Implementing Cisco Data Center Unified Fabric

Lab Guide

Version 5.0

Implementing Cisco Data Center Unified Fabric

Version 5.0

Lab Guide

Text Part Number: 97-3213-01



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)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS." CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Lab Guide	1
Overview	1
Outline	1
Lab 2-1: Configure Layer 2 Switching	5
Activity Objective	5
Visual Objective	5
Job Aids	6
Required Resources	6
Command List	7
Task 1: Management Connectivity	8
Task 2: Layer 2 Interfaces and Rapid PVST+	8
Task 3: STP Enhancements	15
Task 4: MST	17
Lab 2-2: Configure vPCs	22
Activity Objective	22
Visual Objective	22
Job Aids	23
Required Resources	23
Command List	24
Task 1: vPC Domain	26
Task 2: vPC Keepalive Link	27
Task 3: vPC Peer Link	28
Task 4: vPC Configuration	30
Task 5: FEX Configuration	35
Lab 2-3: Configure Cisco FabricPath	38
Activity Objective	38
Visual Objective	38
Required Resources	38
Command List	39
Task 1: Examine Spanning Tree Load Balancing	40
Task 2: Implement Cisco FabricPath	42
Task 3: Analyze Cisco FabricPath Load Balancing	46
Lab 2-4: Configure Layer 3 Switching	49
Activity Objective	49
Visual Objective	49
Job Aids	50
Required Resources	50
Task 1: Establish VRF Connectivity Between Your Nexus 7000 Series Switch VDC and Your Cisco Nexus 5500 Platform Switch	53
Task 2: Static Routing	55
Task 3: OSPFv2	58
Task 4: EIGRP	62
Lab 3-1: Configure OTV	66
Activity Objective	66
Visual Objective	66
Job Aids	67
Required Resources	67
Command List	68
Lab 3-2: Configure QoS	75
Activity Objective	75
Visual Objective	75
Command List	77
Task 1: Verify Baseline Connectivity	78
Task 2: Class Maps	79
Task 3: Policy Maps	80
Task 4: Service Policies	81
Lab 3-3: Configure Security Features	83
Activity Objective	83

Visual Objective	83
Job Aids	84
Required Resources	84
Command List	85
Task 1: Port Security	86
Task 2: Traffic Storm Control	88
Task 3: Configuring Access Control List Using Atomic Programming	89
Lab 4-1: Configure FCoE	91
Activity Objective	91
Visual Objective	91
Required Resources	91
Command List	92
Job Aids	93
Task 1: Preparing Cisco Nexus 5548UP and 5596UP Switches for Fibre Channel Services	93
Task 3: Implementing Fibre Channel Services	101
Lab 4-2: Configuring NPV	106
Activity Objective	106
Visual Objective	106
Command List	108
Task 1: Configure NPV Mode on the Cisco Nexus 5500 Platform Switch	110
Task 2: Configure NPIV on the Cisco MDS 9124 Switch	115
Lab 5-1: Configure System Management	118
Activity Objective	118
Visual Objective	118
Job Aids	119
Required Resources	119
Command List	120
Task 1: Configure Cisco Fabric Services	122
Task 2: Configure the Scheduler	127
Task 3: Configure Cisco Smart Call Home	129
Lab 5-2: Implement Cisco DCNM for LAN	134
Activity Objective	134
Visual Objective	134
Required Resources	134
Command List	135
Job Aids	135
Task 1: Network Discovery	135
Task 2: Platform Inventory	142
Task 3: Monitoring and Management	144
Answer Key	152
Lab 2-1 Answer Key: Configure Layer 2 Switching	152
Lab 2-2 Answer Key: Configure vPCs	155
Lab 2-3 Answer Key: Configure Cisco FabricPath	158
Lab 2-4 Answer Key: Configure Layer 3 Switching	162
Lab 3-1 Answer Key: Configure OTV	167
Lab 3-2 Answer Key: Configure QoS	171
Lab 3-3 Answer Key: Configure Security Features	173
Lab 4-1 Answer Key: Configure FCoE	177
Lab 4-2 Answer Key: Configure NPV	181
Lab 5-1 Answer Key: Configure System Management	183
Lab 5-2 Answer Key: Implement Cisco DCNM for LAN	185

Lab Guide

Overview

This guide presents the instructions and other information concerning the lab activities for this course. You can find the solutions in the lab activity Answer Key.

Outline

This guide includes these activities:

- Job Aids
- Lab 2-1: Configure Layer 2 Switching
- Lab 2-2: Configure vPCs
- Lab 2-3: Configure Cisco FabricPath
- Lab 2-4: Configure Layer 3 Switching
- Lab 3-1: Configure OTV
- Lab 3-2: Configure QoS
- Lab 3-3: Configure Security Features
- Lab 4-1: Configure FCoE
- Lab 4-2: Configure NPV
- Lab 5-1: Configure System Management
- Lab 5-2: Implement Cisco DCNM for LAN
- Answer Key

Job Aids

These job aids are available to help you complete the lab activity. You may tear these pages out of the Lab Guide for future reference.

Interface ID

Interface	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6	Description
Ethernet AA	E 4/9	E 4/11	E 4/13	E 4/15	E 4/21	E 4/23	Downlink from N7K to N5K in your own pod (access)
Ethernet AA	E 1/1	E 1/2	E 1/1	E 1/2	E 1/1	E 1/2	Uplink from N5K to N7K in your own pod (access)
Ethernet AB	E 4/11	E 4/9	E 4/15	E 4/13	E 4/23	E 4/21	Downlink from N7K to N5K in peer pod (access)
Ethernet AB	E 1/2	E 1/1	E 1/2	E 1/1	E 1/2	E 1/1	Uplink from N5K to N7K in peer pod (access)
Ethernet ITA	E 4/1	E 4/1	E 4/5	E 4/5	E 4/17	E 4/17	First inter-N7K-link 10 GB to peer VDC on other N7K
Ethernet ITB	E 4/3	E 4/3	E 4/7	E 4/7	E 4/19	E 4/19	Second inter-N7K-link 10 GB to peer VDC on other N7K
Ethernet IGA	E 1/41	E 3/41	E 1/43	E 3/43	E 1/45	E 3/45	Inter-N7K-link 1 GB to peer VDC on other N7K

Note The interface IDs depend on your pod number. Each pod VDC requires six ports, but additional ports have been automatically added as port group members. Refer to the following table to identify the interfaces used in the lab topology. The interface names, such as access (AA, AB), Inter-N7K 10 GB (ITA, ITB), and Inter-N7K 1 GB (IGA) will be used in the lab description.

Fibre Channel Connectivity

This table lists the **fc 1/FF** interfaces on the MDS 9124-X and MDS 9124-Y switches.

FC switch	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6	Description
MDS9124-1	FC1/7		FC1/7		FC1/7		Fibre Channel link towards SAN
MDS9124-2		FC1/7		FC1/7		FC1/7	Fibre Channel link towards SAN
MDS9124-1	FC1/11		FC1/12		FC1/13		Fibre Channel link towards pod Nexus 5548 switch
MDS9124-2		FC1/11		FC1/12		FC1/13	Fibre Channel link towards pod Nexus 5548 switch

Note The interface IDs depend on your pod number. On each N5548 switch port, **Ethernet 1/31 (Ethernet FF)** is connected to listed ports on the MDS9124-X or MDS9124-Y switch.

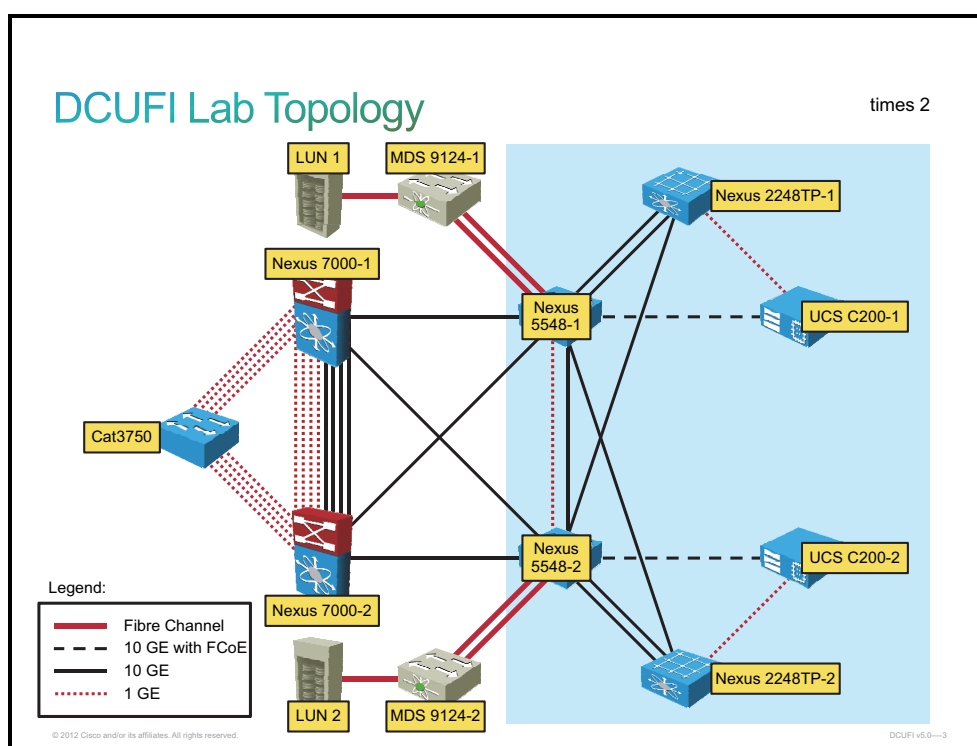
VSAN and FCoE VLAN Mappings

Pod	VSAN "X"	FCoE VLAN
Pod 1, 3, 5	11	1011
Pod 2, 4, 6	12	1012

IP Addresses

Device	Pod 1	Pod 2	Pod 3	Pod 4
N7K VDC	192.168.10.95	192.168.10.97	192.168.10.96	192.168.10.98
N5548	192.168.10.91	192.168.10.92	192.168.10.93	192.168.10.94
MDS9124	192.168.10.2	192.168.10.3	192.168.10.2	192.168.10.3
DCNM Server	192.168.10.121	192.168.10.122	192.168.10.123	192.168.10.124
Cisco UCS C-200 Server CIMC	192.168.10.41	192.168.10.42	192.168.10.43	192.168.10.44

Device	Pod 5	Pod 6
N7K VDC	192.168.10.103	192.168.10.104
N5548	192.168.10.99	192.168.10.100
MDS9124	192.168.10.2	192.168.10.3
DCNM Server	192.168.10.125	192.168.10.126
Cisco UCS C-200 Server CIMC	192.168.10.45	192.168.10.46



Username and Passwords

Device Type	Username	Password
N7K VDC	admin	NXos12345
N5548	admin	NXos12345
MDS9124	admin	NXos12345
DCNM server	admin	NXos12345
C200 Windows Server	admin	NXos12345

Allocated Interfaces

Pod	M Type Interface	F Type Interface
N7K1-Pod1	E1/1, E1/41, E1/43	E4/1, E4/2, E4/3, E4/4, E4/9, E4/10, E4/11, E4/12
N7K2-Pod2	E3/1, E3/41, E3/43	E4/1, E4/2, E4/3, E4/4, E4/9, E4/10, E4/11, E4/12
N7K1-Pod3	E1/3, E1/45, E1/47	E4/5, E4/6, E4/7, E4/8, E4/13, E4/14, E4/15, E4/16
N7K2-Pod4	E3/3, E3/45, E3/47	E4/5, E4/6, E4/7, E4/8, E4/13, E4/14, E4/15, E4/16

Lab 2-1: Configure Layer 2 Switching

Complete this lab activity to practice what you have learned in the related module.

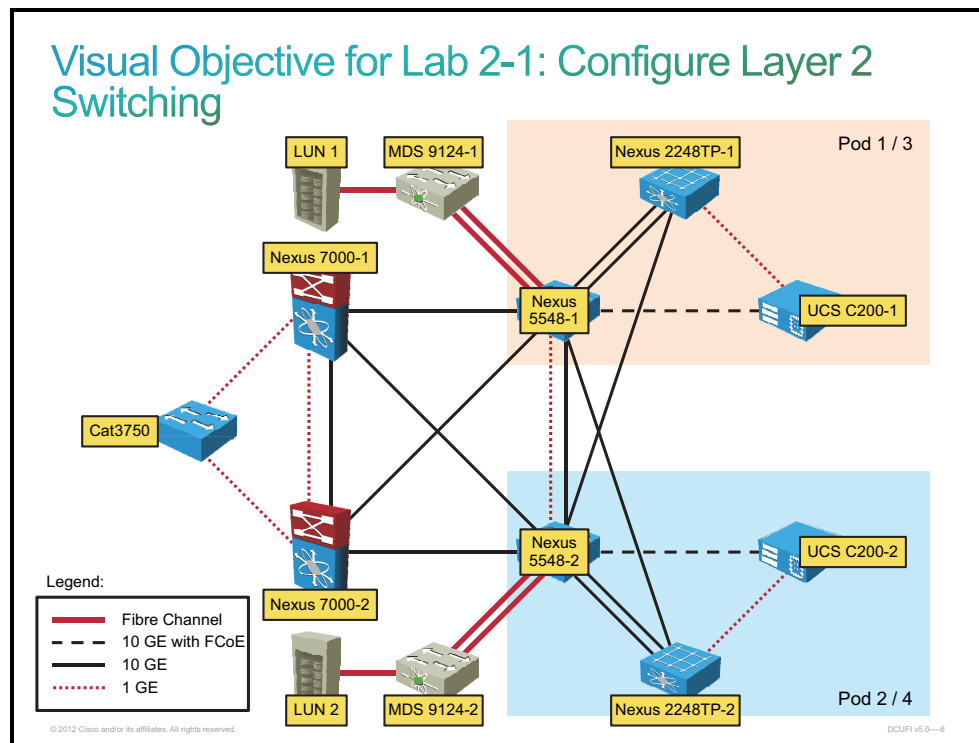
Activity Objective

In this activity, you will implement Layer 2 switching features on the Cisco Nexus 7000 Series and 5500 Platform switches. After completing this activity, you will be able to meet these objectives:

- Configure Layer 2 interfaces and implement and verify Rapid PVRST+
- Implement and verify spanning-tree enhancements in order to optimize and protect spanning-tree operation
- Implement and verify MST

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required to complete this activity:

- Two Cisco Nexus 7000 Series switch VDCs
- Two Cisco Nexus 5500 Platform switches

Command List

The table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>show interface brief</code>	Displays a summary of the interfaces
<code>show interface transceiver</code>	Displays detailed information about installed small form-factor pluggables (SFPs)
<code>rate-mode dedicated</code>	Sets the first port in a port group to dedicated mode
<code>switchport</code>	Configures an interface as a Layer 2 switch port
<code>switchport mode trunk</code>	Configures an interface as a trunk port
<code>show spanning-tree</code>	Displays information related to the Spanning Tree Protocol (STP)
<code>show vlan internal usage</code>	Displays the list of VLANs that are reserved for internal use
<code>vlan <vlan-list></code>	Creates one or more VLANs
<code>name <vlan-name></code>	Configures the VLAN name
<code>show spanning-tree summary</code>	Displays a summarized view of the spanning-tree operational status
<code>spanning-tree vlan <vlan-list> root primary</code>	Changes the priority of the switch in order to make it the root of the spanning tree for the listed VLANs
<code>spanning-tree vlan <vlan-list> root secondary</code>	Lowers the spanning-tree priority of the switch below the default value in order to make the switch the backup spanning-tree root for the listed VLANs
<code>spanning-tree guard root</code>	Enables root guard on an interface
<code>spanning-tree port type edge</code>	Configures an interface as a spanning-tree edge port
<code>feature udld</code>	Enables UniDirectional Link Detection (UDLD) on a switch
<code>udld aggressive</code>	Enables UDLD aggressive mode
<code>show udld neighbors</code>	Displays the list of current UDLD neighbors
<code>spanning-tree port type network</code>	Enables Bridge Assurance on an interface
<code>show spanning-tree inconsistentports</code>	Displays the switch ports that are in the spanning-tree inconsistent state
<code>spanning-tree mst configuration</code>	Enters configuration mode for Multiple Spanning Tree (MST)
<code>name <mst-region-name></code>	Configures the MST region name
<code>revision <mst-revision-nr></code>	Configures the MST revision number
<code>spanning-tree mode mst</code>	Changes the spanning-tree protocol to MST
<code>instance <nr> vlan <vlan-list></code>	Maps a list of VLANs to an MST instance
<code>spanning-tree mst <nr> root primary</code>	Changes the priority of the switch in order to make it the root of the spanning tree for the MST instance

Task 1: Management Connectivity

In this task, you will connect to the switch devices used in the lab.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide. The prompt of the device should be N5548-**P**, where **P** is your assigned pod number. The device should have basic configurations loaded that include the hostname, management IP settings, and admin user settings.

Note If this configuration is missing, the configuration contains more advanced feature configurations, or you cannot log in to the switch, contact the instructor.

- Step 2** Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide. The prompt of the device should be N7K**X**-pod**P**, where **P** is your assigned pod number and **X** is “1” if your pod number is odd and **X** is “2” if your pod number is even. The VDC should have assigned interfaces and a basic configuration loaded that includes the hostname, management IP settings, and admin user settings.

Note If this configuration is missing, the configuration contains more advanced feature configurations, or you cannot log in to the switch, contact the instructor.

Task 2: Layer 2 Interfaces and Rapid PVST+

In this task you will configure basic Layer 2 parameters, such as VLAN and trunk settings. You will also configure Rapid per VLAN Spanning Tree Plus (Rapid PVRST+) and verify proper spanning-tree operation both within your pod and between your pod and your peer pod.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC.
- Step 2** In your Cisco Nexus 7000 Series switch VDC, check the interface state of your assigned interfaces.

N7K**X**-pod**P**# **show interface brief**

Port	VRF	Status	IP Address			Speed	MTU
mgmt0	--	up	192.168.10.98			100	1500
Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth3/45	--	eth	routed	down	Administratively down	auto(D)	--
Eth3/47	--	eth	routed	down	Administratively down	auto(D)	--
Eth4/5	1	eth	access	down	Administratively down	auto(D)	--
Eth4/6	1	eth	access	down	SFP not inserted	auto(D)	--
Eth4/7	1	eth	access	down	Administratively down	auto(D)	--
Eth4/8	1	eth	access	down	SFP not inserted	auto(D)	--
Eth4/13	1	eth	access	down	Administratively down	auto(D)	--
Eth4/14	1	eth	access	down	SFP not inserted	auto(D)	--

Eth4/15	1	eth	access down	Administratively down	auto(D) --
Eth4/16	1	eth	access down	SFP not inserted	auto(D) --

Note This output will be different depending on your pod number. This is a pod 4 printout.

Step 3 Determine how many enhanced form-factor pluggable (SFP+) transceivers are installed in module 4.

Step 4 Determine which interfaces within module 4 have SFP+ transceivers installed.

Step 5 Determine if the I/O module interfaces are currently set to perform as Layer 2 or Layer 3 interfaces.

Step 6 Determine the SFP+ transceiver type(s) installed in your interfaces.

N7KX-podP# **show interface transceiver**

Ethernet **IGA**
transceiver is not applicable

Ethernet **ITA**
transceiver is present
type is SFP-H10GB-CU5M
name is CISCO-MOLEX
part number is 74752-9521
revision is --
serial number is MOC154901LW
nominal bitrate is 10300 MBit/sec
Link length supported for copper is 5 m
cisco id is --
cisco extended id number is 4

Ethernet **ITB**
transceiver is present
type is SFP-H10GB-CU5M
name is CISCO-MOLEX
part number is 74752-9521
revision is --
serial number is MOC154909PG
nominal bitrate is 10300 MBit/sec
Link length supported for copper is 5 m
cisco id is --
cisco extended id number is 4

Ethernet **AA**
transceiver is present
type is SFP-H10GB-CU3M
name is CISCO-MOLEX
part number is 74752-9520
revision is --
serial number is MOC16030BZ1
nominal bitrate is 10300 MBit/sec
Link length supported for copper is 3 m
cisco id is --
cisco extended id number is 4

Ethernet **AB**
transceiver is present
type is SFP-H10GB-CU3M
name is CISCO-MOLEX
part number is 74752-9520
revision is --

```

serial number is MOC16030BNA
nominal bitrate is 10300 MBit/sec
Link length supported for copper is 3 m
cisco id is --
cisco extended id number is 4

```

Step 7 Determine which types of SFP+ transceivers are installed in module 4.

Step 8 Determine what the maximum distance is between devices that these transceivers support.

Step 9 Change all 10-Gb interfaces in your VDC that have SFPs inserted to Layer 2 switch ports rather than routed ports, and then enable these interfaces.

```

N7KX-podP(config)# interface ethernet ITA, ethernet ITB, ethernet AA, ethernet AB
N7KX-podP(config-if-range)# switchport
N7KX-podP(config-if-range)# no shutdown

```

Note Do not enable the inter-N7K 1-GB interfaces.

Step 10 Verify that the interfaces have been enabled and changed to Layer 2 switch ports.

Note The following output is shown for pod 4. Your output may be different.

```
N7KX-podP# show interface brief
```

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	192.168.10.(95-98)	100	1500

Ethernet Interface #	VLAN	Type	Mode	Status	Reason	Speed	Port Ch
Eth3/45	--	eth	routed	down	Administratively down	auto(D)	--
Eth3/47	--	eth	routed	down	Administratively down	auto(D)	--
Eth4/5	1	eth	access	up	none	10G(D)	--
Eth4/6	1	eth	access	down	SFP not inserted	auto(D)	--
Eth4/7	1	eth	access	up	none	10G(D)	--
Eth4/8	1	eth	access	down	SFP not inserted	auto(D)	--
Eth4/13	1	eth	access	up	none	10G(D)	--
Eth4/14	1	eth	access	down	SFP not inserted	auto(D)	--
Eth4/15	1	eth	access	up	none	10G(D)	--
Eth4/16	1	eth	access	down	SFP not inserted	auto(D)	--

Step 11 Verify the CDP neighbors. The following example is taken from pod 4.

```
N7KX-podP# show cdp neighbors
```

```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

```

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
UCS-RL-MGMT	mgmt0	135	R S I	WS-C3550-48	Fas0/33
N7010-pod3 (TBM13384417)	Eth4/5	173	R S I s	N7K-C7010	Eth4/5
N7010-pod3 (TBM13384417)	Eth4/7	173	R S I s	N7K-C7010	Eth4/7

N5548-3 (SSI153702X9)	Eth4/13	173	S I s	N5K-C5548UP	Eth1/2
N5548-4 (SSI16010HKX)	Eth4/15	173	S I s	N5K-C5548UP	Eth1/2

Step 12 Configure all the Layer 2 interfaces in your VDCs as trunks, and verify that the change was successful.

```
N7KX-podP(config)# interface ethernet ITA, ethernet ITB, ethernet AA, ethernet AB
N7KX-podP(config-if-range)# switchport mode trunk
N7KX-podP(config-if-range)# show interface brief
```

Step 13 Connect to your assigned Cisco Nexus 5500 Platform switch.

Step 14 Check the state of the interfaces.

N5548-P# **show interface brief**

Ethernet Interface #	VLAN	Type	Mode	Status	Reason	Speed	Port Ch
Eth1/1	1	eth	access	up	none	10G (D)	--
Eth1/2	1	eth	access	up	none	10G (D)	--
Eth1/3	1	eth	access	down	Link not connected	10G (D)	--
<output omitted>							
Eth1/9	1	eth	access	up	none	10G (D)	--
Eth1/10	1	eth	access	up	none	1000 (D)	--
<output omitted>							
Eth1/15	1	eth	access	up	none	10G (D)	--
Eth1/16	1	eth	access	up	none	10G (D)	--
<output omitted>							

Note The output shown lists only the uplinks to N7K switches (E1/1-2), links to peer N5K (E1/9-10), and downlinks to N2K. Your output may be different.

Step 15 Determine if the Ethernet interfaces are configured as Layer 2 or Layer 3 ports.

Step 16 Determine in which mode the Ethernet interfaces are operating by default.

Step 17 Examine the CDP neighbors.

Note The following output is shown for pod 3. Your output might be different.

N5548-P# **show cdp neighbors**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
UCS-RL-MGMT	mgmt0	172	R S I	WS-C3550-48	Fas0/37
N7K1-pod3 (TBM13384417)	Eth1/1	169	R S I s	N7K-C7010	Eth4/15
N7K2-pod4 (JAF1602BGDB)	Eth1/2	146	R S I s	N7K-C7009	Eth4/15
N5548-4 (SSI153702X9)	Eth1/9	169	S I s	N5K-C5548UP	Eth1/9
N5548-4 (SSI153702X9)	Eth1/10	169	S I s	N5K-C5548UP	Eth1/10

Step 18 Configure the uplinks as Layer 3 interfaces.

```
N5548-P(config)# interface ethernet 1/1-2
N5548-P(config-if-range)# no switchport
```

Note Cisco Nexus 5500 Platform switches, unlike Nexus 5000 Series switches, support Layer 3 interfaces.

Step 19 Configure the uplinks as Layer 2 interfaces in trunk mode.

```
N5548-P(config)# interface ethernet 1/1-2
N5548-P(config-if-range)# switchport
N5548-P(config-if-range)# switchport mode trunk
```

Step 20 Verify that the uplinks operate as Layer 2 trunk interfaces.

```
N5548-P# show interface ethernet 1/1-2 brief
```

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

Step 21 Disable the interfaces connecting to your peer pod N5K switch.

```
N5548-P(config)# interface ethernet 1/9-10
N5548-P(config-if-range)# shutdown
```

Step 22 Switch back to your Nexus 7000 Series switch VDC and examine the spanning-tree operation for VLAN 1 by using the **show spanning-tree vlan 1** command.

```
N7KX-podP# show spanning-tree vlan 1
```

```
VLAN0001
Spanning tree enabled protocol rstp
Root ID    Priority    8193
           Address    0019.300e.aa00
           Cost      43
           Port      527 (AB)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
           Address    6c9c.ed46.52c3
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth ITA	Desg	FWD	2	128.517	P2p
Eth ITB	Desg	FWD	2	128.519	P2p
Eth AA	Altn	BLK	2	128.525	P2p
Eth AB	Root	FWD	2	128.527	P2p

Note Your output may be different.

Step 23 Determine which PVRST+ path cost method is being used.

Step 24 Determine which switch or VDC is the root bridge for VLAN 1 in your pod pair. Consult your peer student to determine what their output.

Step 25 Examine which VLANs are available for you and which are used internally.

```
N7KX-podP# show vlan internal usage
VLANs          DESCRIPTION
-----
3968-4031      Multicast
4032-4035,4048-4059 Online Diagnostic
4036-4039,4060-4087 ERSPAN
4042           Satellite
3968-4095      Current
```

Step 26 Create VLAN 10 with the name “TEST” on your Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP(config)# vlan 10
N7KX-podP(config-vlan)# name TEST
```

Step 27 Create VLAN 10 with the name “TEST” on your Cisco Nexus 5500 Platform Switch.

```
N55548-P(config)# vlan 10
N55548-P(config-vlan)# name TEST
```

Step 28 On Cisco Nexus 7000 Series switch VDC, examine spanning-tree operation for all VLANs.

```
N7KX-podP# show spanning-tree
```

```
VLAN0001
Spanning tree enabled protocol rstp
Root ID    Priority    8193
           Address    0019.300e.aa00
           Cost      43
           Port      527 (AB)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    6c9c.ed46.52c3
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth ITA	Desg	FWD	2	128.517	P2p
Eth ITB	Desg	FWD	2	128.519	P2p
Eth AA	Altn	BLK	2	128.525	P2p
Eth AB	Root	FWD	2	128.527	P2p

```
VLAN0010
Spanning tree enabled protocol rstp
Root ID    Priority    32778
           Address    547f.ee82.9f01
           Cost      2
           Port      527 (AB)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
           Address    6c9c.ed46.52c3
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth ITA	Desg	FWD	2	128.517	P2p
Eth ITB	Desg	FWD	2	128.519	P2p
Eth AA	Desg	FWD	2	128.525	P2p
Eth AB	Root	FWD	2	128.527	P2p

Note Your output may be different.

Step 29 Determine which switch or VDC is the root bridge for the spanning-tree instance for VLAN 10. Determine if it is the same or different from VLAN 1.

Step 30 Create additional VLANs 11–13 on your Cisco Nexus 7000 Series switch VDC.

N7KX-podP(config)# **vlan 11-13**

Step 31 Create additional VLANs 11–13 on your Cisco Nexus 5500 Platform switch.

N5548-P(config)# **vlan 11-13**

Step 32 Examine the spanning-tree instances running in your pod.

N7KX-podP# **show spanning-tree summary**

```
Switch is in rapid-pvst mode
Root bridge for: none
Port Type Default          is disable
Edge Port [PortFast] BPDU Guard Default is disabled
Edge Port [PortFast] BPDU Filter Default is disabled
Bridge Assurance           is enabled
Loopguard Default         is disabled
Pathcost method used       is short
STP-Lite                   is enabled
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	1	0	0	3	4
VLAN0010	0	0	0	4	4
VLAN0011	0	0	0	4	4
VLAN0012	0	0	0	4	4
VLAN0013	0	0	0	4	4
5 vlans	1	0	0	19	20

Note Your output may be different.

Step 33 Determine if there is a separate spanning-tree instance for each VLAN.

Step 34 Configure the spanning-tree root bridge for each VLAN according to the following table:

Pod	VLAN STP Root Primary	VLAN STP Root Secondary
N7K1-Pod1	VLAN11, VLAN13	VLAN10, VLAN12
N7K2-Pod2	VLAN10, VLAN12	VLAN11, VLAN13
N7K1-Pod3	VLAN11, VLAN13	VLAN10, VLAN12
N7K2-Pod4	VLAN10, VLAN12	VLAN11, VLAN13
N7K1-Pod5	VLAN11, VLAN13	VLAN10, VLAN12
N7K2-Pod6	VLAN10, VLAN12	VLAN11, VLAN13

N7KX-podP(config)# **spanning-tree vlan XX,XY root primary**

N7KX-podP(config)# **spanning-tree vlan YY,YX root secondary**

Step 35 Verify that the spanning tree for VLANs 10–13 is behaving as expected.

N7KX-podP# **show spanning-tree vlan 10-13**

Activity Verification

You have completed this task when you attain these results:

- You have configured the interface connecting to the peer Cisco Nexus 7000 Series switch VDC as rate-mode dedicated.
- You have verified basic interface operation and settings on your Cisco Nexus 7000 Series switch VDC and Cisco Nexus 5500 Platform switch.
- You have configured the links between the switches in your pod and your peer pod as 802.1Q trunks.
- You have created new VLANs.
- You have configured the odd VDC as the root for the odd VLANs and the even VDC as the backup root for the odd VLANs.
- You have configured the even VDC as the root for the even VLANs and the odd VDC as the backup root for the even VLANs.
- You have verified spanning-tree operation for selected VLANs.

Task 3: STP Enhancements

In this task, you will configure STP optimization and protection features and verify their operation.

Note	In the previous task, the Cisco Nexus 7000 VDCs were configured as the root and backup root for VLANs 10–13. Together they form the aggregation layer of the lab network. Now you will protect the spanning tree by preventing the access switches from becoming root bridges.
-------------	--

Activity Procedure

Complete these steps:

- Step 1** In your Cisco Nexus 7000 Series switch VDC, configure root guard on the trunk links connecting to the Cisco Nexus 5500 Platform switches in your pod as well as your peer pod.

```
N7KX-podP(config)# interface ethernet AA, ethernet AB  
N7KX-podP(config-if-range)# spanning-tree guard root
```

- Step 2** Configure the access ports on your Cisco Nexus 5500 Platform switch that connect to FEXs as spanning-tree edge ports.

```
N5548-P(config)# interface ethernet 1/15-16  
N5548-P(config-if-range)# spanning-tree port type edge  
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
```

Edge Port Type (Portfast) will be configured in 2 interfaces due to the range command but will only have effect when the interfaces are in a non-trunking mode.

Note	The spanning-tree edge port feature is also known as PortFast.
-------------	--

Step 3 Enable UDLD in aggressive mode on the devices in your pod and your peer pod in order to protect your switches against unidirectional link failures.

```
N7KX-podP(config)# feature udld
N7KX-podP(config)# udld aggressive
```

```
N5548-P(config)# feature udld
N5548-P(config)# udld aggressive
```

Step 4 Verify UDLD operation.

```
N7KX-podP# show udld neighbors
```

Port	Device Name	Device ID	Port ID	Neighbor State
Ethernet ITA	TBM13384417	1	Ethernet ITA	bidirectional
Ethernet ITB	TBM13384417	1	Ethernet ITB	bidirectional
Ethernet AA	SSI153702X9	1	Ethernet AA	bidirectional
Ethernet AB	SSI16010HKX	1	Ethernet AB	bidirectional

Step 5 Enable bridge assurance on the links between your N7K VDC and the VDC in the peer pod.

```
N7KX-podP(config)# interface ethernet ITA, ITB
N7KX-podP(config-if)# spanning-tree port type network
```

Note UDLD can protect against bridging loops caused by physical problems, but it cannot protect against software-caused spanning-tree failures. The bridge assurance feature can help protect against bridging loops caused by software failures.

Step 6 Verify that bridge assurance is enabled on the link between the VDCs by using the **show spanning-tree** command.

```
N7KX-podP# show spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol rstp
Root ID    Priority    8193
           Address    0019.300e.aa00
           Cost      47
           Port      517 (Ethernet ITA)
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
           Address    6c9c.ed46.52c3
Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth ITA	Root	FWD	2	128.517	Network P2p
Eth ITB	Desg	BKN*2		128.519	Network P2p *BA_Inc
Eth AA	Desg	BKN*2		128.525	P2p *ROOT_Inc
Eth AB	Desg	BKN*2		128.527	P2p *ROOT_Inc

```
<output omitted>
```

Step 7 Determine which keyword indicates that bridge assurance is enabled on the port.

Step 8 On your Cisco Nexus 7000 Series switch VDC, enable bridge assurance on the ports that are connected to the Cisco Nexus 5500 Platform switches in your pod and the peer pod.

```
N7KX-podP(config)# interface ethernet AA, ethernet AB
N7KX-podP(config-if-range)# spanning-tree port type network
```

Step 9 Check the spanning-tree inconsistencies:

```
N7KX-podP(config-if-range)# show spanning-tree inconsistentports
```

Step 10 Determine the misconfiguration.

Step 11 Repair the misconfiguration by enabling bridge assurance on your Cisco Nexus 5500 Platform switch for the ports that connect to the Cisco Nexus 7000 Series switch VDCs.

```
N5548-P(config)# interface ethernet 1/1-2
```

```
N5548-P(config-if-range)# spanning-tree port type network
```

Step 12 Ensure that the problem has been resolved by verifying inconsistent ports on your N7K VDC once again.

Activity Verification

You have completed this task when you attain these results:

- You have enabled root guard on the N7K VDC ports connecting to the Cisco Nexus 5500 Platform switches in your pod and the peer pod.
- You have configured the ports leading to the servers as spanning-tree edge ports.
- You have successfully enabled UDLD in aggressive mode between the switches in your pod and your peer pod.
- You have successfully enabled bridge assurance between the switches in your pod and your peer pod.
- You have observed the spanning-tree behavior when bridge assurance is only enabled on one side of a link.

Task 4: MST

In this task, you will configure and verify MST operation.

Activity Procedure

Complete these steps:

Step 1 Configure your Cisco Nexus 7000 Series switch VDC to participate in an MST region by using the following parameters, where **P** is your pod number and **Q** is your peer pod number:

Device	Region Name	Revision Number
N7K1-pod1	reg12	12
N7K2-pod2	reg12	12
N7K1-pod3	reg34	34
N7K2-pod4	reg34	34
N7K1-pod5	reg56	56
N7K2-pod6	reg56	56

```
N7KX-podP(config)# spanning-tree mst configuration
```

```
N7KX-podP(config-mst)# name regPQ
```

```
N7KX-podP(config-mst)# revision PQ
```

```
N7KX-podP(config-mst)# exit
```

Step 2 In your Cisco Nexus 7000 Series switch VDC, change the spanning-tree mode to MST.

```
N7KX-podP(config)# spanning-tree mode mst
```

Step 3 Repeat the same steps on your Cisco Nexus 5500 Platform switch:

```
N5548-P(config)# spanning-tree mst configuration
N5548-P(config-mst)# name regPQ
N5548-P(config-mst)# revision PQ
N5548-P(config-mst)# exit
N5548-P(config)# spanning-tree mode mst
```

Step 4 Verify that MST is operating correctly between the VDCs and switches in your pod and in your peer pod. Use the **show spanning-tree**, **show spanning-tree mst**, and **show spanning-tree mst configuration** commands to verify this. The example provided is for pod 4, but it may be different on your own pod.

```
N7KX-podP# show spanning-tree
```

```
MST0000
```

```
Spanning tree enabled protocol mstp
Root ID    Priority    32768
           Address    0026.51c9.78c4
           Cost        0
           Port        517 (Ethernet ITA)
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    32768 (priority 32768 sys-id-ext 0)
           Address    6c9c.ed46.52c3
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Eth ITA	Root	FWD	2000	128.517		Network P2p
Eth ITB	Altn	BLK	2000	128.519		Network P2p
Eth AA	Desg	BKN*2000		128.525		Network P2p *ROOT_Inc
Eth AB	Desg	BKN*2000		128.527		Network P2p *ROOT_Inc

```
N7KX-podP# show spanning-tree mst
```

```
MST0    vlans mapped:    1-4094
Bridge   address 6c9c.ed46.52c3 priority    32768 (32768 sysid 0)
Root     address 0026.51c9.78c4 priority    32768 (32768 sysid 0)
          port    Eth ITA    path cost    0
Regional Root address 0026.51c9.78c4 priority    32768 (32768 sysid 0)
          internal cost 2000    rem hops 19
Operational hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured  hello time 2 , forward delay 15, max age 20, max hops    20
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Eth ITA	Root	FWD	2000	128.517		Network P2p
Eth ITB	Altn	BLK	2000	128.519		Network P2p
Eth AA	Desg	BKN*2000		128.525		Network P2p *ROOT_Inc
Eth AB	Desg	BKN*2000		128.527		Network P2p *ROOT_Inc

Note Be aware that MST configuration is not applied until you exit MST configuration mode. Therefore, you should exit MST configuration mode before issuing any **show** commands in order to verify MST operation. The output may be different than that shown here.

Step 5 Determine which spanning-tree path cost method MST uses by default.

Step 6 Determine how many MST instances are currently being used and determine if you can achieve VLAN load balancing with this configuration.

Step 7 Change the MST configuration on your Cisco Nexus 7000 Series switch VDC to add two new MST instances. Map VLANs 11 and 13 to MST instance 1 and map VLANs 10 and 12 to MST instance 2.

```
N7KX-podP(config)# spanning-tree mst configuration
N7KX-podP(config-mst)# instance 1 vlan 11,13
N7KX-podP(config-mst)# instance 2 vlan 10,12
N7KX-podP(config-mst)# exit
```

Step 8 Verify MST operation on the switches in your pod to determine that it is operating as expected.

```
N7KX-podP# show spanning-tree
N5548-P# show spanning-tree
```

Step 9 On your Cisco Nexus 5500 Platform switch, change the MST configuration to match the configuration on your VDC by mapping VLANs 11 and 13 to MST instance 1 and mapping VLANs 10 and 12 to MST instance 2. Set the priority level to 61440 for each instance to ensure that the N5K does not become the root bridge.

```
N5548-P(config)# spanning-tree mst configuration
N5548-P(config-mst)# instance 1 vlan 11,13
N5548-P(config-mst)# instance 2 vlan 10,12
N5548-P(config-mst)# spanning-tree mst 1-2 priority 61440
N5548-P(config-mst)# exit
```

Step 10 Verify that MST is now operating properly on all devices in your pod as well as your peer pod.

```
N7KX-podP# show spanning-tree
N5548-P# show spanning-tree
```

Note You should not see any boundary ports in the output of the **show spanning-tree** commands.

Step 11 Determine which switches or VDCs are the root bridges for each of the MST instances. Determine if they are the same or different.

Step 12 Configure the VDC of switch N7K-1 as the root bridge for MST instance 1 and as the backup root bridge for MST instance 2.

```
N7K1-podP(config)# spanning-tree mst 1 root primary
N7K1-podP(config)# spanning-tree mst 2 root secondary
```

Step 13 Configure the VDC of switch N7K-2 as the root bridge for MST instance 2 and as the backup root bridge for MST instance 1.

```
N7K2-podQ(config)# spanning-tree mst 1 root secondary
N7K2-podQ(config)# spanning-tree mst 2 root primary
```

Step 14 Verify that the root bridges are selected as expected. Ensure that you have no spanning-tree inconsistent ports or boundary ports on the switches in your pod as well as your peer pod. The examples shown are for both Nexus 7000 Series switches VDCs.

```
N7K1-podP(config)# show spanning-tree
```

```
MST0000
```

```

Spanning tree enabled protocol mstp
Root ID      Priority      32768
             Address      0026.51c9.78c4
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority      32768 (priority 32768 sys-id-ext 0)
             Address      0026.51c9.78c4
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Eth ITA        Desg FWD 2000      128.517 Network P2p
Eth ITB        Desg FWD 2000      128.519 Network P2p
Eth AA         Desg BKN*2000      128.525 Network P2p *ROOT_Inc
Eth AB         Desg BKN*2000      128.527 Network P2p *ROOT_Inc

```

```

MST0001
Spanning tree enabled protocol mstp
Root ID      Priority      24577
             Address      0026.51c9.78c4
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority      24577 (priority 24576 sys-id-ext 1)
             Address      0026.51c9.78c4
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Eth ITA        Desg FWD 2000      128.517 Network P2p
Eth ITB        Desg FWD 2000      128.519 Network P2p
Eth AA         Desg BKN*2000      128.525 Network P2p *ROOT_Inc
Eth AB         Desg BKN*2000      128.527 Network P2p *ROOT_Inc

```

```

MST0002
Spanning tree enabled protocol mstp
Root ID      Priority      24578
             Address      6c9c.ed46.52c3
             Cost          2000
             Port          517 (Ethernet ITA)
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority      28674 (priority 28672 sys-id-ext 2)
             Address      0026.51c9.78c4
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Eth ITA        Root FWD 2000      128.517 Network P2p
Eth ITB        Altn BLK 2000      128.519 Network P2p
Eth AA         Desg BKN*2000      128.525 Network P2p *ROOT_Inc
Eth AB         Desg BKN*2000      128.527 Network P2p *ROOT_Inc

```

N7K2-podP(config)# **show spanning-tree**

```

MST0000
Spanning tree enabled protocol mstp
Root ID      Priority      32768
             Address      0026.51c9.78c4
             Cost          0
             Port          517 (Ethernet ITA)
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority      32768 (priority 32768 sys-id-ext 0)
             Address      6c9c.ed46.52c3

```

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth ITA	Root	FWD	2000	128.517	Network P2p
Eth ITB	Altn	BLK	2000	128.519	Network P2p
Eth AA	Desg	BKN*2000		128.525	Network P2p *ROOT_Inc
Eth AB	Desg	BKN*2000		128.527	Network P2p *ROOT_Inc

MST0001

Spanning tree enabled protocol mstp

Root ID Priority 24577
 Address 0026.51c9.78c4
 Cost 2000
 Port 517 (Ethernet4/5)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28673 (priority 28672 sys-id-ext 1)
 Address 6c9c.ed46.52c3
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth ITA	Root	FWD	2000	128.517	Network P2p
Eth ITB	Altn	BLK	2000	128.519	Network P2p
Eth AA	Desg	BKN*2000		128.525	Network P2p *ROOT_Inc
Eth AB	Desg	BKN*2000		128.527	Network P2p *ROOT_Inc

MST0002

Spanning tree enabled protocol mstp

Root ID Priority 24578
 Address 6c9c.ed46.52c3
 This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24578 (priority 24576 sys-id-ext 2)
 Address 6c9c.ed46.52c3
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth ITA	Desg	FWD	2000	128.517	Network P2p
Eth ITB	Desg	FWD	2000	128.519	Network P2p
Eth AA	Desg	BKN*2000		128.525	Network P2p *ROOT_Inc
Eth AB	Desg	BKN*2000		128.527	Network P2p *ROOT_Inc

Step 15 Verify the root bridges on Cisco Nexus 5500 Platform switches.

N5548-**P#** **show spanning-tree | include Bound**
N5548-**P#** **show spanning-tree inconsistentports**

Activity Verification

You have completed this task when you attain these results:

- You have successfully enabled MST on all switches in your pod.
- You have configured the odd VDC as the root for the MST instance that contains the odd VLANs and the even VDC as the backup root for this particular MST instance.
- You have configured the even VDC as the root for the MST instance that contains the even VLANs and the odd VDC as the backup root for this particular MST instance.

Lab 2-2: Configure vPCs

Complete this lab activity to practice what you have learned in the related module.

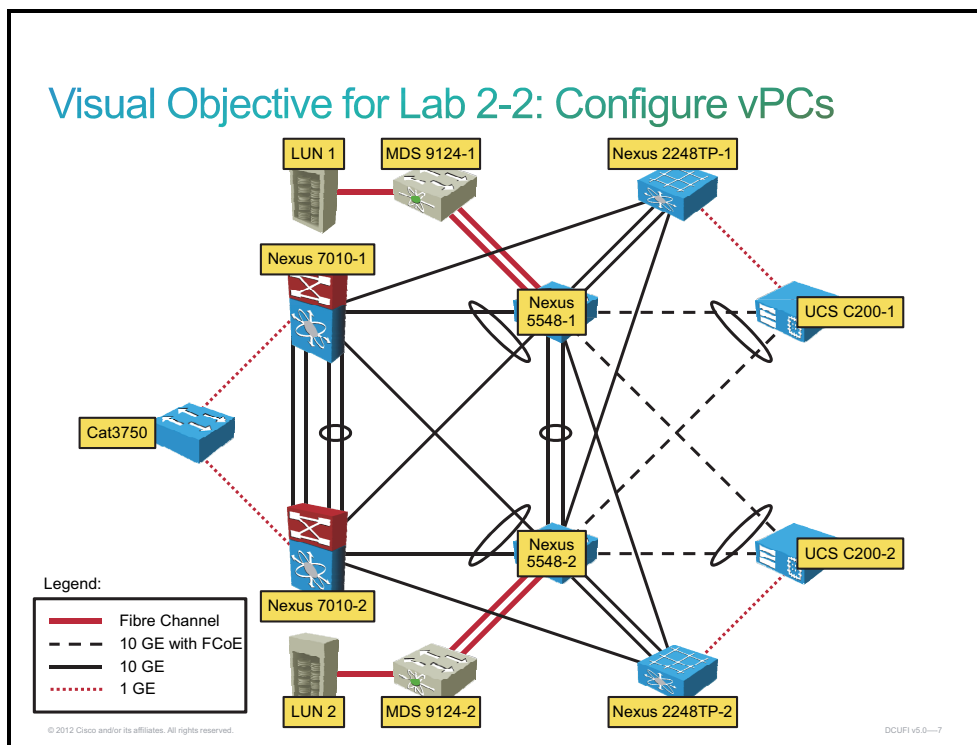
Activity Objective

In this activity, you will configure a virtual port channel (vPC) between the Cisco Nexus 7000 Series switch and the Cisco Nexus 5500 Platform switch at the access layer of the network and configure a Cisco Nexus 2000 Fabric Extender. After completing this activity, you will be able to meet these objectives:

- Create and verify a vPC domain on a Cisco Nexus switch
- Create a vPC peer keepalive link between two Cisco Nexus switches and verify proper operation
- Create a vPC peer link between two Cisco Nexus switches and verify proper operation
- Configure a vPC on a Cisco Nexus switch and verify proper operation
- Configure a Cisco Nexus 2000 Fabric Extender for operation with a Cisco Nexus 7000 Series switch VDC

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete this lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required to complete this activity:

- Two Cisco Nexus 7000 Series switches VDCs
- Two Cisco Nexus 5500 Platform switches
- Two Cisco Nexus 2000 Fabric Extenders

Command List

This table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>show license usage</code>	Displays the usage of licensed features
<code>feature vpc</code>	Enables the vPC feature
<code>vpc domain 56</code>	Creates a vPC domain
<code>peer-gateway</code>	Enables the peer-gateway feature
<code>peer-switch</code>	Enables the peer switch feature
<code>spanning-tree mst <mst-instances> priority <priority></code>	Changes the spanning-tree priority for a set of Multiple Spanning Tree (MST) instances
<code>ping <ip-address> vrf <vrf></code>	Verifies IP connectivity to an IP address in a virtual routing and forwarding (VRF) by using Internet Control Message Protocol (ICMP) echo messages
<code>peer-keepalive destination <vpc-peer-ip-address></code>	Enables the vPC peer keepalive link to the vPC peer IP address
<code>show vpc peer-keepalive</code>	Displays status information for the vPC peer keepalive link
<code>show interface <intf> brief</code>	Displays summarized status information for an interface.
<code>show running-config <intf></code>	Displays the current configuration for an interface
<code>channel-group <nr></code>	Adds an interface to a port channel
<code>vpc peer-link</code>	Defines a port channel interface as the vPC peer link
<code>show vpc consistency-parameters global</code>	Displays global vPC consistency status
<code>show vpc</code>	Displays vPC operational parameters
<code>feature lacp</code>	Enables the use of the Link Aggregation Control Protocol (LACP)
<code>channel-group <nr> mode active</code>	Adds an interface to a port channel that is dynamically negotiated through LACP
<code>show port-channel summary</code>	Displays a summarized view of port channel operation
<code>show lacp neighbor</code>	Displays a list of LACP neighbors and their operational parameters
<code>vpc <nr></code>	Adds a port channel interface to a vPC
<code>show vpc brief</code>	Displays a brief overview of vPC status
<code>show spanning-tree</code>	Displays information related to the STP
<code>show version</code>	Displays the software version running on the switch
<code>feature-set fex</code>	Enables the features that are necessary to support fabric extenders in a Cisco Nexus 7000 Series switch VDC
<code>fex <instance></code>	Creates an FEX instance
<code>switchport mode fex-fabric</code>	Changes a switch port into a fabric interface that can be used to connect to an FEX

fex associate <instance>	Associates a fabric interface with an FEX instance
show fem	Displays summarized status information for FEXs that are connected to the switch
show fem detail	Displays detailed status information for FEXs that are connected to the switch
show interface fem-fabric	Shows the FEX fabric interfaces on the switch
reload fem <instance>	Reloads an FEX
show inventory fem <instance>	Displays the hardware inventory for an FEX
show module fem <instance>	Displays the FEX modules, including basic hardware and software information
switchport mode access	Configures a switch port as an access port
switchport access vlan <vlan>	Sets the access VLAN when the interface is in access mode
no spanning-tree bpduguard	Disables the spanning-tree BPDU Guard feature on a switch port
spanning-tree port type normal	Changes a port to normal spanning-tree mode

Task 1: vPC Domain

In this task, you will define the vPC domain.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids section at the beginning of the Lab Guide.
- Step 2** Verify the current license usage on your Cisco Nexus 7000 Series switch VDC.

N7KX-podP# **show license usage**

Feature	Ins	Lic Count	Status	Expiry Date	Comments
MPLS_PKG	No	-	Unused		-
STORAGE-ENT	No	-	Unused		-
ENTERPRISE_PKG	No	-	Unused		-
FCOE-N7K-F132XP	No	0	Unused		-
ENHANCED_LAYER2_PKG	No	-	Unused		Grace 107D 2H
SCALABLE_SERVICES_PKG	No	-	Unused		-
TRANSPORT_SERVICES_PKG	No	-	Unused		-
LAN_ADVANCED_SERVICES_PKG	No	-	Unused		Grace 108D 0H
LAN_ENTERPRISE_SERVICES_PKG	No	-	Unused		-

- Step 3** Enable the vPC feature in your VDC.

N7KX-podP(config)# **feature vpc**

- Step 4** Check the license usage again. Determine if you require a license in order to enable vPC on a Cisco Nexus 7000 Series switch.

- Step 5** Configure a vPC domain.

N7KX-podP(config)# **vpc domain XY**

Note The vPC domain number should be the same on your pod and on your peer pod. Pods 1 and 2 use vPC domain number 12, and pods 3 and 4 use vPC domain number 34.

- Step 6** Enable the vPC peer-gateway feature in order to allow your switch to forward traffic for the peer switch router MAC addresses in order to support non-RFC-compliant devices.

N7KX-podP(config-vpc-domain)# **peer-gateway**

- Step 7** Enable the peer-switch feature to optimize spanning-tree processing for the vPC domain.

N7KX-podP(config-vpc-domain)# **peer-switch**

- Step 8** Set the priority for all MST instances to 8192 to ensure that the vPC peer switches will be the root for the spanning tree.

N7KX-podP(config)# **spanning-tree mst 0-4094 priority 8192**

Activity Verification

You have completed this task when you attain these results:

- You have configured a vPC domain on your Cisco Nexus 7000 VDC.
- You have enabled the peer-gateway and peer switch features.
- You have tuned the spanning-tree priority to ensure that the vPC switches will be the spanning-tree root.

Task 2: vPC Keepalive Link

In this task, you will configure the vPC keepalive link between the VDCs in your pod and in the peer pod.

Activity Procedure

Complete these steps:

- Step 1** Configure the first 1-Gb Ethernet link connecting your N7K VDC with the peer N7K VDC as a routed interface. Use IP addresses 192.168.100.**P**/24, where **P** is your pod number.

```
N7KX-podP(config)# interface ethernet IGA
N7KX-podP(config-if)# no switchport
N7KX-podP(config-if)# ip address 192.168.100.P/24
N7KX-podP(config-if)# no shutdown
```

- Step 2** Verify that you can ping the peer IP address on the keepalive link.

```
N7KX-podP# ping 192.168.100.Q
PING 192.168.100.2 (192.168.100.2): 56 data bytes
Request 0 timed out
64 bytes from 192.168.100.2: icmp_seq=1 ttl=254 time=1.298 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=254 time=0.615 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=254 time=0.585 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=254 time=0.594 ms

--- 192.168.100.2 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.585/0.773/1.298 msloss
round-trip min/avg/max = 0.602/0.74/1.087 ms
```

- Step 3** Configure the vPC peer keepalive link by using your peer IP address as the destination. (**Q** is the peer pod number.). Use the default VRF, and source the keepalive packets from the 1 Gigabit Ethernet interface dedicated to keepalives.

```
N7KX-podP(config-if)# vpc domain XY
N7KX-podP(config-vpc-domain)# peer-keepalive destination 192.168.100.Q source
192.168.100.P vrf default
```

- Step 4** Verify that the peer keepalive link between your pod and your peer pod is operational.

```
N7K-X-podP# show vpc peer-keepalive
```

```
vPC keep-alive status           : peer is alive
--Peer is alive for             : (30) seconds, (228) msec
--Send status                   : Success
--Last send at                  : 2012.06.09 07:30:17 492 ms
--Sent on interface             : IGA
--Receive status                : Success
--Last receive at               : 2012.06.09 07:30:17 491 ms
--Received on interface         : IGA
--Last update from peer        : (0) seconds, (217) msec
```

```
vPC Keep-alive parameters
--Destination          : 192.168.100.2
--Keepalive interval   : 1000 msec
--Keepalive timeout     : 5 seconds
--Keepalive hold timeout : 3 seconds
--Keepalive vrf         : default
--Keepalive udp port    : 3200
--Keepalive tos         : 192
```

Note This step requires configuration on your VDC and your peer pod VDC. Do not proceed to the next task until this task has been completed on both VDCs and the peer keepalive link is active.

Activity Verification

You have completed this task when you attain these results:

- You have successfully established the vPC peer keepalive link between your VDC and the VDC in your peer pod.

Task 3: vPC Peer Link

In this task, you will configure the vPC peer link between the VDC in your pod and the VDC in your peer pod.

Activity Procedure

Complete these steps:

- Step 1** In your Cisco Nexus 7000 Series switch VDC, verify that the interface connecting to your peer VDC is active and configured as a trunk.

Note In the first exercise, you configured two 10 Gigabit Ethernet interfaces that connect to your peer pod VDC. They are referred to as ITA and ITB.

```
N7KX-podP# show interface ethernet ITA, ITB brief
```

```
-----
Ethernet      VLAN    Type Mode   Status Reason           Speed   Port
Interface                                           Ch
#
-----
EthITA        1       eth  trunk  up      none             10G(D)  --
EthITB        1       eth  trunk  up      none             10G(D)  --
-----
```

Note The exact interface used to connect the two peer VDCs is different for each peer pod pair. Refer to the Lab Connections “Job Aids” at the beginning of the lab guide.

- Step 2** Try to configure this Ethernet interface as the vPC peer link.

```
N7KX-podP(config)# interface ethernet ITA
N7KX-podP(config-if)# vpc peer-link ?
^
% Invalid command at '^' marker.
N7KX-podP(config-if)# vpc ?
orphan-port  Orphan-port (non-vpc port)
```

Note The vPC peer link must be a port channel interface. An Ethernet port cannot be used as the peer link.

Step 3 Configure the 10-Gb interfaces that connect your VDC to the peer pod VDC as static port channel members. Use channel group 7 for this port channel.

```
N7KX-podP(config)# interface ethernet ITA, ethernet ITB
N7KX-podP(config-if)# channel-group 7
```

Step 4 Configure the port channel you just created as the vPC peer link.

```
N7KX-podP(config)# interface port-channel 7
N7KX-podP(config-if)# vpc peer-link
```

Please note that spanning tree port type is changed to "network" port type on vPC peer-link.

This will enable spanning tree Bridge Assurance on vPC peer-link provided the STP Bridge Assurance (which is enabled by default) is not disabled.

Step 5 Examine the global vPC consistency parameters.

```
N7KX-podP# show vpc consistency-parameters global
```

Legend:

Type 1 : vPC will be suspended in case of mismatch

Name	Type	Local Value	Peer Value
-----	----	-----	-----
--			
STP Mode	1	MST	MST
STP Disabled	1	None	None
STP MST Region Name	1	regPQ	regPQ
STP MST Region Revision	1	PQ	PQ
STP MST Region Instance to VLAN Mapping	1		
STP Loopguard	1	Disabled	Disabled
STP Bridge Assurance	1	Enabled	Enabled
STP Port Type, Edge	1	Normal, Disabled,	Normal, Disabled,
BPDUFILTER, Edge BPDUGuard		Disabled	Disabled
STP MST Simulate PVST	1	Enabled	Enabled
Allowed VLANs	-	1,10-13	1,10-13
Local suspended VLANs	-	-	-

Caution When Type 1 global consistency parameters are mismatched, all vPCs will be suspended.

Step 6 Verify the vPC status.

```
N7KX-podP# show vpc
```

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

```
vPC domain id : XY
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role : primary
Number of vPCs configured : 0
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
```

vPC Peer-link status

id	Port	Status	Active vlans
1	Po7	up	1,10-13

Note The peer status must appear as "peer adjacency formed ok" before you continue to the next task.

Activity Verification

You have completed this task when you attain these results:

- You have configured a port channel between your pod VDC and the peer pod VDC.
- You have successfully established the vPC peer link between the VDCs.

Task 4: vPC Configuration

In this task, you will configure a vPC between the Cisco Nexus 5500 Platform switch in your pod and the Cisco Nexus 7000 Series switch VDCs in your own pod and in the peer pod.

Activity Procedure

Complete these steps:

Step 1 Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 2 Create an LACP-based port channel containing the uplinks (Ethernet 1/1 and Ethernet 1/2). Use channel group 77 for this port channel.

```
N5548-P(config)# feature lacp
```

```
N5548-P(config)# interface ethernet 1/1-2
```

```
N5548-P(config-if-range)# channel-group 77 mode active
```

Step 3 Examine the state of the port channel.

```
N5548-P# show port-channel summary
```

```
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)
```

Group	Port-Channel	Type	Protocol	Member Ports
77	Po77 (SD)	Eth	LACP	Eth1/1 (I) Eth1/2 (I)

- Step 4** Switch to your Cisco Nexus 7000 Series switch VDC and configure an LACP-based port channel by using the downstream interfaces. Each pod has to configure two downstream port channels. Use the following table to determine port channel numbers used on each interface.

Pod	PortChannel 1	PortChannel 2	PortChannel 3	PortChannel 4	PortChannel 5	PortChannel 6
N7K1-pod1	ethernet4/9	ethernet4/11				
N7K2-pod2	ethernet4/9	ethernet4/11				
N7K1-pod3			ethernet4/13	ethernet4/15		
N7K2-pod4			ethernet4/13	ethernet4/15		
N7K1-pod3					ethernet4/17	ethernet4/19
N7K2-pod4					ethernet4/17	ethernet4/19

```

N7KX-podP(config)# feature lacp
N7KX-podP(config)# interface ethernet W
N7KX-podP(config-if)# channel-group X mode active
N7KX-podP(config-if)# interface ethernet Y
N7KX-podP(config-if)# channel-group Z mode active

```

Note The result of this configuration is that each Cisco Nexus 5500 Platform switch is reached by a port channel with the number of the Nexus 5500 Platform switch.

- Step 5** Check the configuration of your Nexus 7000 Series switch VDC to ensure that two port channel interfaces have been automatically created.

- Step 6** Switch to your Nexus 5500 Platform switch and examine the status of port channel 77. Ensure that the port channel formed correctly.

```

N5548-P# show port-channel summary
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)
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
77    Po77(SU)    Eth       LACP      Eth1/1(P)  Eth1/2(s)

```

Note Which port is up and which one is suspended will depend on the pod you are using.

- Step 7** Examine the LACP neighbors on your Cisco Nexus 5500 Platform switch.

```

N5548-P# show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
        A - Device is in Active mode         P - Device is in Passive mode
port-channel77 neighbors
Partner's information
Port      Partner
System ID System ID
Eth1/1    32768,0-26-51-c9-78-c4
Partner   Port Number  Age      Partner
System ID 32768,0-26-51-c9-78-c4 0x40d    0        Flags
SA
LACP Partner
Port Priority 32768
Partner       Oper Key    Partner
System ID 32768,0-26-51-c9-78-c4 0x2      0x5

```

Partner's information

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Eth1/2	32768,6c-9c-ed-46-52-c30x40d		393	SA
	LACP Partner Port Priority	Partner Oper Key		Partner Port State
	32768	0x2		0x3

Note Without the vPC enabled on the port channels of the Cisco Nexus 7000 Series switch VDCs, the Cisco Nexus 5500 Platform switch detects that it is connected to two different switches.

Step 8 Switch to your Cisco Nexus 7000 Series switch VDC and configure the vPC with the same number as the port channel number.

```
N7KX-podP(config)# interface port-channel P
N7KX-podP(config-if)# vpc P
N7KX-podP(config)# interface port-channel Q
N7KX-podP(config-if)# vpc Q
```

Step 9 Examine the status of the vPCs that you created.

```
N7KX-podP# show vpc brief
```

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

```
vPC domain id          : XY
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role               : primary
Number of vPCs configured : 2
Peer Gateway           : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status    : Disabled
```

vPC Peer-link status

```
-----
id   Port   Status Active vlans
--   ---   -
1    Po7    up      1,10-13
```

vPC status

```
-----
id   Port   Status Consistency Reason          Active vlans
--   ---   -
P    PoP    up      success    success          1,10-13
Q    PoQ    up      success    success          1,10-13
```

Note In the last section of the output (vPC status), the consistency results must be listed as "success" and the status as "up" for both vPCs before continuing. Use the **show vpc consistency-parameters vpc** command to examine potential failed consistency checks for a specific vPC.

Cisco Nexus 5500 Platform Switch

- Step 10** Switch to your Nexus 5500 Series Switch and examine the status of port channel 77 on your Cisco Nexus 5500 Platform Switch. Determine if the port channel now forms correctly.

N5548-*P*# **show port-channel summary**

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)

Group	Port-Channel	Type	Protocol	Member Ports
77	Po77(SU)	Eth	LACP	Eth1/1 (P) Eth1/2 (P)

- Step 11** Examine the LACP neighbors.

N5548-*P*# **show lacp neighbor**

Flags: S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

port-channel77 neighbors

Partner's information

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Eth1/1	32667,0-23-4-ee-be- HH	0x40d	1073	SA
	LACP Partner Port Priority 32768	Partner Oper Key 0x8003		Partner Port State 0x3d

Partner's information

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Eth1/2	32667,0-23-4-ee-be- HH	0x440d	1063	SA
	LACP Partner Port Priority 32768	Partner Oper Key 0x8003		Partner Port State 0x3d

Note Now the Cisco Nexus 5500 Platform switch sees the two Cisco Nexus 7000 Series switch VDCs as a single LACP neighbor. The last octet of the system ID equals the configured vPC domain number in hexadecimal notation.

- Step 12** Examine the spanning tree on your Cisco Nexus 5500 Platform switch to determine if there are any blocked ports.

N5548-*P*# **show spanning-tree**

MST0000

Spanning tree enabled protocol mstp

Root ID	Priority	8192
	Address	0023.04ee.be22
	Cost	0
	Port	4172 (port-channel77)
	Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID	Priority	32768 (priority 32768 sys-id-ext 0)
	Address	547f.0000.0000
	Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po77	Root	FWD	1000	128.4172	P2p
Eth1/14	Desg	FWD	2000	128.142	P2p
Eth1/15	Desg	FWD	2000	128.143	Edge P2p
Eth1/16	Desg	FWD	2000	128.144	Edge P2p
Eth1/28	Desg	FWD	2000	128.156	P2p

MST0001

Spanning tree enabled protocol mstp

Root ID	Priority	8193	
	Address	0023.04ee.be22	
	Cost	1000	
	Port	4172 (port-channel77)	
	Hello Time	2 sec	Max Age 20 sec Forward Delay 15 sec

Bridge ID	Priority	61441 (priority 61440 sys-id-ext 1)
	Address	547f.ee3e.6641
	Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po77	Root	FWD	1000	128.4172	P2p

MST0002

Spanning tree enabled protocol mstp

Root ID	Priority	8194	
	Address	0023.04ee.be22	
	Cost	1000	
	Port	4172 (port-channel77)	
	Hello Time	2 sec	Max Age 20 sec Forward Delay 15 sec

Bridge ID	Priority	61442 (priority 61440 sys-id-ext 2)
	Address	547f.ee3e.6641
	Hello Time	2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Po77	Root	FWD	1000	128.4172	P2p

Note The output may differ depending on your pod number.

Step 13 Determine what the spanning-tree port cost of the uplink to the Cisco Nexus 7000 Series switch VDCs is?

Step 14 Determine which switch is the spanning-tree root within the network and how the bridge ID of the root bridge was created.

Activity Verification

You have completed this task when you attain these results:

- You have successfully created a vPC between your Cisco Nexus 5500 Platform switch and the Cisco Nexus 7000 Series switch VDCs in your pod and in your peer pod.

Task 5: FEX Configuration

In this task, you will configure your Cisco Nexus 2000 Fabric Extender for use with your Cisco Nexus 5500 Series Switches by using dynamic pinning.

Note You will not configure static pinning because of its redundancy and load-balancing limitations. You will also not configure active-active FEX using vPC, because in this lab you will not configure another vPC on the Nexus 5500 Platform switches in addition to the one you configured on the Nexus 7000 Series Switches.

Activity Procedure

Complete these steps:

Step 1 Enable the FEX feature on your Cisco Nexus 5500 Series Switch.

```
N5548-P(config)# feature fex
```

Step 2 Create an FEX instance with the number 10**P**, where **P** is your assigned pod number. Set the maximum number of links for pinning at 1.

```
N5548-P(config)# fex 10P  
N5548-P(config)# pinning max-links 1
```

Step 3 Disable the port downlink port toward the peer pod Cisco Nexus 2000 Fabric Extender since it is not used in this lab.

```
N5548-P(config)# interface ethernet 1/14  
N5548-P(config-if)# shutdown
```

Step 4 Configure the two downlinks to your Cisco Nexus 2000 Fabric Extender as the Layer 2 switch port, and configure it as an FEX fabric interface.

```
N5548-P(config)# interface ethernet 1/15-16  
N5548-P(config-if)# switchport  
N5548-P(config-if)# switchport mode fex-fabric
```

Step 5 Assign the FEX fabric port to a channel group in order to create a port channel. Use 1**P** as the channel group number, where **P** is your pod number.

```
N5548-P(config-if)# channel-group 1P
```

Step 6 Associate the newly created port channel interface 1**P** with your FEX instance.

```
N5548-P(config)# interface port-channel 1P  
N5548-P(config-if)# fex associate 10P
```

Step 7 Enable the FEX fabric interface.

```
N5548-P(config)# interface ethernet 1/15-16  
N5548-P(config-if)# no shutdown
```

Step 8 Wait until your FEX is online. The state may remain as “image download” for up to 10 minutes if the FEX is running a lower software version than the switch.

```
N5548-P# show fex
```

FEX Number	FEX Description	FEX State	FEX Model	FEX Serial
10 P	FEX010 P	Online	N2K-C2248TP-1GE	SSI16020FCK

Note You may need to wait several minutes for FEX to become available. If the FEX software image differs from the Cisco Nexus 5500 Series Switch software image, an automatic upgrade will occur. Check FEX availability for five minutes; it should then be ready for you to continue with the lab.

Step 9 Examine the FEX parameters.

```
N5548-P# show fex detail
FEX: 10P Description: FEX010P state: Online
FEX version: 5.1(3)N1(1a) [Switch version: 5.1(3)N1(1a)]
  FEX Interim version: 5.1(3)N1(1a)
  Switch Interim version: 5.1(3)N1(1a)
  Extender Serial: SSI16020FCK
  Extender Model: N2K-C2248TP-1GE, Part No: 73-13232-01
  Card Id: 99, Mac Addr: 3c:ce:73:a1:67:42, Num Macs: 64
  Module Sw Gen: 12594 [Switch Sw Gen: 21]
  post level: complete
pinning-mode: static Max-links: 1
Fabric port for control traffic: Eth1/15
FCoE Admin: false
FCoE Oper: true
FCoE FEX AA Configured: false
Fabric interface state:
  PolP - Interface Up. State: Active
  Eth1/15 - Interface Up. State: Active
  Eth1/16 - Interface Up. State: Active
    Fex Port      State      Fabric Port
    Eth10P/1/1   Down      PolP
    Eth10P/1/2   Down      PolP
    Eth10P/1/3   Down      PolP
    Eth10P/1/4   Down      PolP
    ...
    Eth10P/1/47 Down      PolP
    Eth10P/1/48 Down      PolP
Logs:
<output truncated>
```

Step 10 Examine the FEX fabric ports.

```
N5548-P# show interface fex-fabric
```

	Fabric	Fabric	Fex		FEX	
Fex	Port	Port	State	Uplink	Model	Serial
10 P	Eth1/15		Active	1	N2K-C2248TP-1GE	SSI16020FCK
10 P	Eth1/16		Active	2	N2K-C2248TP-1GE	SSI16020FCK

Step 11 View the hardware inventory for the FEX.

```
N5548-P# show inventory fex 10P
NAME: "FEX 103 CHASSIS", DESCR: "N2K-C2248TP-1GE CHASSIS"
PID: N2K-C2248TP-1GE , VID: V03 , SN: SSI16020FCK

NAME: "FEX 103 Module 1", DESCR: "Fabric Extender Module: 48x1GE, 4x10GE
Supervisor"
PID: N2K-C2248TP-1GE , VID: V03 , SN: FOC16063CZU

NAME: "FEX 103 Fan 1", DESCR: "Fabric Extender Fan module"
PID: N2K-C2248-FAN , VID: N/A , SN: N/A

NAME: "FEX 103 Power Supply 1", DESCR: "Fabric Extender AC power supply"
PID: N2200-PAC-400W , VID: V03 , SN: DTN1602P0AG

NAME: "FEX 103 Power Supply 2", DESCR: "Fabric Extender AC power supply"
PID: N2200-PAC-400W , VID: V03 , SN: DTN1602P0A0
```

Step 12 Examine the modules on the FEX.

N5548-**P**# **show module fex 10P**

FEX	Mod	Ports	Card Type	Model	Status.
10P	1	48	Fabric Extender 48x1GE + 4x10G Module	N2K-C2248TP-1GE	present

FEX	Mod	Sw	Hw	World-Wide-Name(s) (WWN)
10P	1	5.1(3)N1(1a)	4.3	--

FEX	Mod	MAC-Address(es)	Serial-Num
10P	1	3cce.73a1.6740 to 3cce.73a1.676f	SSI16020FCK

Step 13 Configure interface Ethernet 1/1 on your FEX as an access port in VLAN 10, and then enable it.

N5548-**P**(config)# **interface ethernet 10P/1/1**

N5548-**P**(config-if)# **switchport mode access**

N5548-**P**(config-if)# **switchport access vlan 10**

N5548-**P**(config-if)# **no shutdown**

Note There is no server connected to port Ethernet 10P/1/1.

Step 14 Try to disable the BPDU Guard and spanning-tree edge port features on the interface.

N5548-**P**(config-if)# **interface ethernet 10P/1/1**

N5548-**P**(config-if)# **no spanning-tree bpduguard**

ERROR: Command not supported on fex port

N5548-**P**(config-if)# **spanning-tree port type normal**

ERROR: Command not supported on fex port

Note FEX ports are intended to connect servers only. BPDU Guard and spanning-tree port type edge are enabled by default and cannot be disabled.

Activity Verification

You have completed this task when you attain these results:

- You have successfully enabled a Cisco Nexus 2000 Fabric Extender on your Cisco Nexus 5500 Platform switch.
- You have configured a port on the FEX and examined the spanning-tree capabilities for the FEX ports.

Lab 2-3: Configure Cisco FabricPath

Complete this lab activity to practice what you learned in the related module.

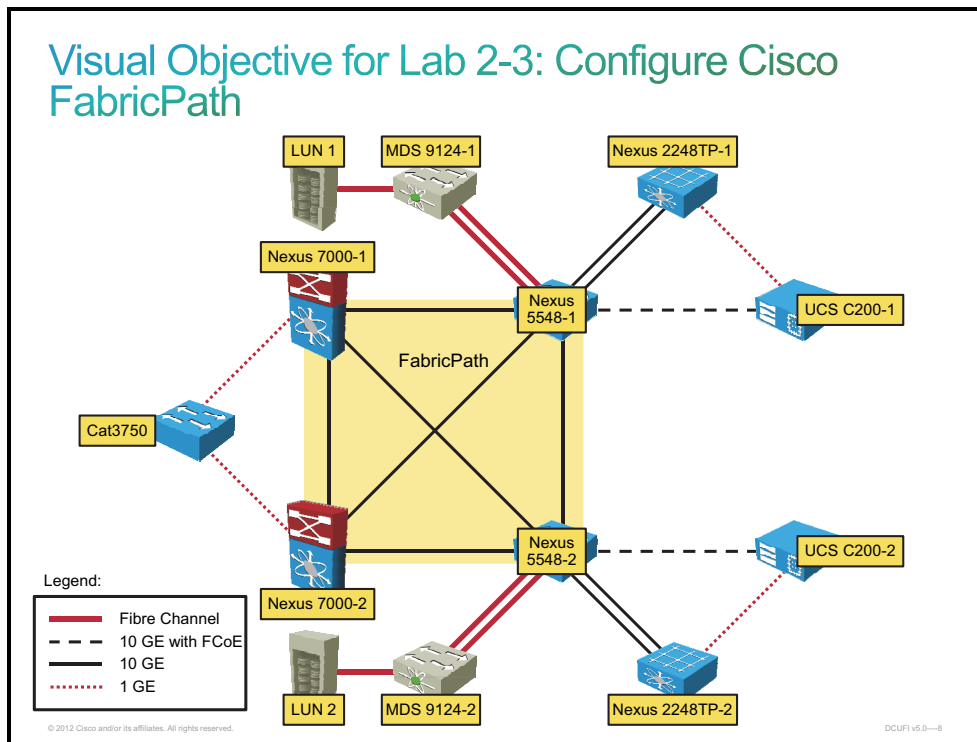
Activity Objective

In this activity, you will configure and verify Cisco FabricPath on the Cisco Nexus 5500 and 7000 Series switches. After completing this activity, you will be able to meet these objectives:

- Analyze spanning-tree load balancing
- Implement Cisco FabricPath
- Verify Cisco FabricPath
- Analyze Cisco FabricPath load balancing

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required in order to complete this activity:

- Two Cisco Nexus 2000 Fabric Extenders

Command List

The table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>install feature-set fabricpath</code>	Installs the FabricPath feature set on a Cisco Nexus 7000 Series switch
<code>feature-set fabricpath</code>	Enables the FabricPath feature set
<code>fabricpath switch-id</code>	Sets the FabricPath switch identifier (Note: The same command configured the virtual switch ID for vPC+ in the vPC domain configuration mode.)
<code>switchport mode fabricpath</code>	Configures the FabricPath mode on an interface (This command is available in interface configuration mode.)
<code>mode fabricpath</code>	Changes a VLAN to a Cisco FabricPath VLAN
<code>show mac address-table vlan <vlan></code>	Displays the MAC address table for a VLAN
<code>show spanning-tree vlan <vlan></code>	Displays the spanning-tree topology for a VLAN
<code>fabricpath load-balance unicast</code>	Configures the load-balancing method for unicast traffic
<code>show fabricpath switch-id</code>	Displays the FabricPath switch ID table
<code>show fabricpath isis route</code>	Displays the FabricPath Intermediate System-to-Intermediate System (IS-IS paths
<code>show fabricpath route</code>	Displays the FabricPath routing table

Task 1: Examine Spanning Tree Load Balancing

In this task, you will configure and examine the spanning-tree forwarding within the network.

Activity Procedure

Complete these steps:

Step 1 Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 2 Disable ports that are not used in this lab.

```
N5548-P(config) # interface ethernet1/9-10, ethernet1/14
N5548-P(config-if-range) # shutdown
```

Step 3 Configure VLAN 10 with the name FP-TEST.

```
N5548-P(config) # vlan 10
N5548-P(config-vlan) # name FP-TEST
```

Step 4 Configure the VLAN10 interface with the address 172.16.10.5**P**, where **P** is your pod number.

```
N5548-P(config) # feature interface-vlan
N5548-P(config) # interface vlan10
N5548-P(config-if) # ip address 172.16.10.5P/24
N5548-P(config-if) # no shutdown
```

Step 5 Remove the vPC configuration and enable spanning-tree protocol for VLAN10.

```
N5548-P(config) # no feature vpc
N5548-P(config) # spanning-tree vlan 10
```

Step 6 Enable uplink interfaces toward your switch as well as your peer Cisco Nexus 7000 Series switch, and configure them as trunks.

```
N5548-P(config) # interface ethernet1/1-2
N5548-P(config-if-range) # no channel-group
N5548-P(config-if-range) # switchport
N5548-P(config-if-range) # switchport mode trunk
N5548-P(config-if-range) # spanning-tree port type network
N5548-P(config-if-range) # no shutdown
```

Step 7 Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 8 Remove the vPC configuration and enable spanning-tree protocol for VLAN 10.

```
N7KX-podP(config) # no feature vpc
N7KX-podP(config) # spanning-tree vlan 10
N7KX-podP(config) # interface ethernetITA, ethernetITB, ethernetIGA
N7KX-podP(config-if-range) # shutdown
```

Note Although vPC+ is a Cisco FabricPath feature that combines the FabricPath functionality with vPC, you will not be able to test it due to the lab topology constraints. Do not remove the port channels on your Cisco Nexus 5500 Platform switch that are pointing to the Nexus 2000 Series FEXs.

- Step 9** Attempt to configure interfaces between your Cisco Nexus 7000 Series switch, your Cisco Nexus 5500 Platform switch and your peer Cisco Nexus 5500 Platform switch as routed ports. Determine if you are allowed to make this change and why.

```
N7KX-podP(config)# interface ethernetAA, ethernetAB
N7KX-podP(config-if-range)# no channel-group
N7KX-podP(config-if-range)# no switchport
ERROR: EthernetAA, EthernetAB: requested config change not allowed
```

- Step 10** Enable interfaces between your Cisco Nexus 7000 Series switch VDC, your Cisco Nexus 5500 Platform switch and your peer Cisco Nexus 5500 Platform switch, and configure them as trunks.

```
N7KX-podP(config)# interface ethernetAA, ethernetAB
N7KX-podP(config-if-range)# switchport
N7KX-podP(config-if-range)# switchport mode trunk
N7KX-podP(config-if-range)# spanning-tree port type network
N7KX-podP(config-if-range)# no shutdown
```

- Step 11** Create VLAN10 on the Cisco Nexus 7000 Series switch.

```
N7KX-podP(config)# vlan 10
N7KX-podP(config-vlan)# name FP-TEST
```

- Step 12** From your Cisco Nexus 5500 Platform switch, ping the IP address of your peer pod Cisco Nexus 5500 Platform switch, 172.16.10.5Q, where Q is your peer pod number, in order to confirm IP connectivity between the two pods.

```
N5548-P# ping 172.16.10.5Q
PING 172.16.10.5Q (172.16.10.5Q): 56 data bytes
64 bytes from 172.16.10.5Q: icmp_seq=0 ttl=254 time=1.377 ms
64 bytes from 172.16.10.5Q: icmp_seq=1 ttl=254 time=0.789 ms
64 bytes from 172.16.10.5Q: icmp_seq=2 ttl=254 time=0.746 ms
64 bytes from 172.16.10.5Q: icmp_seq=3 ttl=254 time=0.715 ms
64 bytes from 172.16.10.5Q: icmp_seq=4 ttl=254 time=0.718 ms

--- 172.16.10.5Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.715/0.868/1.377 ms
```

Note Make sure that you are able to ping the peer IP address. A successful ping will prove that all wiring and configurations so far are correct.

- Step 13** Examine the spanning-tree topology on the Cisco Nexus 5500 Platform switch and identity the links that are in a blocking state.

```
N5548-P# show spanning-tree vlan 10
N5548-P# show spanning-tree blockedports
```

- Step 14** Examine the spanning-tree topology on the Cisco Nexus 7000 Series switch and identity the links that are in a blocking state.

```
N7KX-podP# show spanning-tree vlan 10
N7KX-podP# show spanning-tree blockedports
```

Note Check spanning-tree topology together with your peer. Blocked ports may be present on the peer devices.

Activity Verification

You have completed this task when you attain these results:

- You have removed the vPC configuration from your Cisco Nexus 7000 Series switch and 5500 Platform switches.
- You have verified that the spanning-tree topology does not allow several active links between two switches or Layer 2 loops in the topology.

Task 2: Implement Cisco FabricPath

In this task, you will implement Cisco FabricPath technology in your Cisco Nexus 7000 Series switch VDC and on your Cisco Nexus 5500 Platform switch.

Activity Procedure

Complete these steps:

Step 1 Connect to your assigned Cisco Nexus 7000 Series switch VDC.

Step 2 Examine the license usage on your Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP# show license usage
```

Feature	Ins	Lic	Status	Expiry	Date	Comments
		Count				

MPLS_PKG	Yes	-	Unused	Never		-
STORAGE-ENT	Yes	-	Unused	Never		-
ENTERPRISE_PKG	No	-	Unused			-
FCOE-N7K-F132XP	Yes	1	Unused	Never		-
ENHANCED_LAYER2_PKG	Yes	-	Unused	Never		-
SCALABLE_SERVICES_PKG	Yes	-	Unused	Never		-
TRANSPORT_SERVICES_PKG	Yes	-	Unused	Never		-
LAN_ADVANCED_SERVICES_PKG	Yes	-	Unused	Never		-
LAN_ENTERPRISE_SERVICES_PKG	Yes	-	Unused	Never		-

Step 3 Determine which license is required to enable Cisco FabricPath.

Step 4 Enable the Cisco FabricPath feature set.

```
N7KX-podP(config)# feature-set fabricpath
```

Step 5 Examine the Cisco FabricPath switch ID of your Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP# show fabricpath switch-id
```

```
FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
```

SWITCH-ID	SYSTEM-ID	FLAGS	STATE	STATIC	EMULATED
*3938	0026.51c9.78c3	Primary	Confirmed	No	No
Total Switch-ids: 1					

Note The switch ID may be different than in the example.

Step 6 Configure the switch ID of your VDC to be **PQ**, where **P** is your pod number and **Q** is your peer pod number.

```
N7KX-podP(config)# fabricpath switch-id PQ
```

Step 7 Verify the configured Cisco FabricPath switch ID.

```
N7KX-podP# show fabricpath switch-id
```

FABRICPATH SWITCH-ID TABLE

Legend: '*' - this system

SWITCH-ID	SYSTEM-ID	FLAGS	STATE	STATIC	EMULATED
*PQ	0026.51c9.78c3	Primary	Confirmed	Yes	No
Total Switch-ids: 1					

Step 8 Configure the two interfaces on the F1 series I/O module that connect your VDC and your Cisco Nexus 5500 Platform switch, as well as the interface that connects your pod VDC and your peer pod VDC as Cisco FabricPath interfaces. Use the Lab Connections Job Aids to find the correct interfaces.

```
N7KX-podP(config)# interface ethernetAA,ethernetAB
```

```
N7KX-podP(config-if-range)# switchport mode fabricpath
```

```
N7KX-podP(config-if-range)# exit
```

Step 9 Enable Cisco FabricPath on your Cisco Nexus 5500 switch.

```
N5548-P(config)# install feature-set fabricpath
```

```
N5548-P(config)# feature-set fabricpath
```

Step 10 Configure the switch IP of your Cisco Nexus 5500 Platform switch to be PP, where P is your pod number.

```
N5548-P(config)# fabricpath switch-id PP
```

Step 11 Examine the Cisco FabricPath switch ID of your Cisco Nexus 5500 Platform switch.

```
N5548-P(config)# show fabricpath switch-id
```

FABRICPATH SWITCH-ID TABLE

Legend: '*' - this system

SWITCH-ID	SYSTEM-ID	FLAGS	STATE	STATIC	EMULATED
*PP	547f.ee83.2c01	Primary	Confirmed	Yes	No
Total Switch-ids: 1					

Step 12 Configure the uplinks toward Cisco Nexus 7000 Series switch VDC as Cisco FabricPath interfaces. Use the Lab Connections Job Aids to find the correct interfaces.

```
N5548-P(config)# interface ethernetAA, ethernetAB
```

```
N5548-P(config-if-range)# switchport mode fabricpath
```

Step 13 Reexamine the Cisco FabricPath switch IDs.

```
N7KX-podP# show fabricpath switch-id
```

FABRICPATH SWITCH-ID TABLE

Legend: '*' - this system

SWITCH-ID	SYSTEM-ID	FLAGS	STATE	STATIC	EMULATED
*PQ	a8b1.d455.6fc4	Primary	Confirmed	Yes	No
QP	0026.9804.a944	Primary	Confirmed	Yes	No
PP	547f.ee83.2c01	Primary	Confirmed	Yes	No
QQ	0026.9804.b772	Primary	Confirmed	Yes	No

Total Switch-ids: 4

Note Do not continue to the next step until you see your peer pod switch ID also listed in the output of the show fabricpath switch-id command.

- Step 14** Use the **show fabricpath isis adjacency** command to verify that Cisco FabricPath IS-IS adjacencies have been formed between all switches in the Cisco FabricPath cloud. Determine how many switches participate in Cisco FabricPath cloud.

N7KX-podP# show fabricpath isis adjacency

```
Fabricpath IS-IS domain: default Fabricpath IS-IS adjacency database:
System ID      SNPA          Level  State   Hold Time  Interface
N5548-P        N/A           1      UP      00:00:27   EthernetAA
N5548-Q        N/A           1      UP      00:00:29   EthernetAB
```

- Step 15** From your Cisco Nexus 5500 Platform switch, ping 172.16.10.5Q, the IP address of your peer pod Cisco Nexus 5500 Platform switch, where Q is your peer pod number, in order to confirm IP connectivity between the two pods. Determine if the ping was successful and why.

```
N5548-P# ping 172.16.10.5Q
PING 172.16.10.5Q (172.16.10.5Q): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out

--- 172.16.10.5Q ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

- Step 16** Examine the Cisco FabricPath routing table.

```
N7KX-podP# show 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/PQ/0, number of next-hops: 0
via ---- , [60/0], 0 day/s 01:11:54, local
```

Note The Cisco FabricPath routing table does not list any remote switches until at least one Cisco FabricPath VLAN has been configured.

- Step 17** Convert VLAN 10 to a Cisco FabricPath VLAN on both VDC and the Cisco Nexus 5500 Platform switch.

```
N7KX-podP(config)# vlan 10
N7KX-podP(config-vlan)# mode fabricpath
N7KX-podP(config-vlan)# exit

N5548-P(config)# vlan 10
N5548-P(config-vlan)# mode fabricpath
N5548-podP(config-vlan)# exit
```

- Step 18** Reexamine the Cisco FabricPath routing table.

```
N7KX-podP# show 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/PQ/0, number of next-hops: 0
    via ----, [60/0], 0 day/s 19:04:16, local
1/PP/0, number of next-hops: 1
    via EthAA, [115/40], 0 day/s 00:00:43, isis_fabricpath-default
1/QP/0, number of next-hops: 2
    via EthAA, [115/80], 0 day/s 00:00:28, isis_fabricpath-default
    via EthAB, [115/80], 0 day/s 00:00:15, isis_fabricpath-default
1/QQ/0, number of next-hops: 1
    via EthAB, [115/40], 0 day/s 00:00:15, isis_fabricpath-default
```

- Step 19** From your Cisco Nexus 5500 Platform switch, ping 172.16.10.5Q, the IP address of your peer pod Cisco Nexus 5500 Platform switch, where Q is your peer pod number, in order to confirm IP connectivity between the two pods. Determine if the ping was successful and why.

```
N5548-P# ping 172.16.10.5Q
PING 172.16.10.5Q (172.16.10.5Q): 56 data bytes
64 bytes from 172.16.10.5Q: icmp_seq=0 ttl=254 time=2.111 ms
64 bytes from 172.16.10.5Q: icmp_seq=1 ttl=254 time=0.789 ms
64 bytes from 172.16.10.5Q: icmp_seq=2 ttl=254 time=0.746 ms
64 bytes from 172.16.10.5Q: icmp_seq=3 ttl=254 time=0.737 ms
64 bytes from 172.16.10.5Q: icmp_seq=4 ttl=254 time=0.735 ms

--- 172.16.10.5Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.735/1.024/2.111 ms
```

- Step 20** Examine the spanning-tree topology for VLAN 10.

```
N7KX-podP# show spanning-tree vlan 10
Spanning tree instance(s) for vlan does not exist.
```

- Step 21** Examine the MAC address table for VLAN 10 on your VDC.

```
N7KX-podP# show mac address-table vlan 10
Legend:
    * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
    age - seconds since last seen, + - primary entry using vPC Peer-Link
VLAN    MAC Address      Type      age      Secure NTFY Ports/SWID.SSID.LID
-----+-----+-----+-----+-----+-----+-----+
10      547f.ee81.cb8c    dynamic   30       F      F      QQ.0.0
10      547f.ee83.2c01    dynamic   30       F      F      PP.0.0
```

Note Do not proceed to the next task until you succeed in pinging the peer pod Cisco Nexus 5500 Platform switch VLAN 10 IP address. Troubleshoot together with your peer as necessary.

Activity Verification

You have completed this task when you attain these results:

- You have implemented Cisco FabricPath on your Cisco Nexus 7000 Series switch VDC and Nexus 5500 Platform switch.
- You have established a Cisco FabricPath cloud with your peer pod.
- You have verified IP connectivity between your Cisco Nexus 5500 Platform switch and your peer pod Nexus 5500 Platform switch in VLAN across the Cisco FabricPath cloud.
- You have verified that spanning-tree protocol is not active for VLAN10.

Task 3: Analyze Cisco FabricPath Load Balancing

In this task, you will examine the traffic load balancing in a Cisco FabricPath environment.

Activity Procedure

Complete these steps:

- Step 1** On your Cisco Nexus 7000 Series switch VDC, configure the VLAN10 interface with the primary IP address of 172.16.10.15 P and the secondary IP address of 172.16.10.16 P , where P is your pod number.

```
N7KX-podP(config)# feature interface-vlan
N7KX-podP(config)# interface vlan10
N7KX-podP(config-if)# ip address 172.16.10.15P/24
N7KX-podP(config-if)# ip address 172.16.10.16P/24 secondary
Disabling IP Redirects on Vlan10 :secondary address configured.
N7KX-podP(config-if)# no shutdown
```

- Step 2** Configure Cisco FabricPath load balancing to use only Layer 3 for hash calculation.

```
N7KX-podP(config)# fabricpath load-balance unicast layer3
```

- Step 3** Determine which links Cisco FabricPath will use to forward traffic toward your peer pod Cisco Nexus 7000 Series switch VDC. Replace M with module number where F-type linecard is installed.

```
N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type L3 src-ip 172.16.10.15P dst-ip 172.16.10.15Q vlan 10
module M
N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type L3 src-ip 172.16.10.15P dst-ip 172.16.10.16Q vlan 10
module M
N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type L3 src-ip 172.16.10.16P dst-ip 172.16.10.15Q vlan 10
module M
N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type L3 src-ip 172.16.10.16P dst-ip 172.16.10.16Q vlan 10
module M
```

Source IP	Destination IP	Path That Will Be Used
172.16.10.15 P	172.16.10.15 Q	
172.16.10.15 P	172.16.10.16 Q	
172.16.10.16 P	172.16.10.15 Q	
172.16.10.16 P	172.16.10.16 Q	

- Step 4** From your Cisco Nexus 7000 Series switch VDC, ping both the IP address of your peer pod Cisco Nexus 7000 Series switch VDC, 172.16.10.15 Q , and 172.16.10.16 Q —where Q is your peer pod number—to confirm IP connectivity between the two pods. Determine if the ping was successful.

```
N7KX-podP# ping 172.16.10.15Q
PING 172.16.10.15Q (172.16.10.15Q): 56 data bytes
64 bytes from 172.16.10.15Q: icmp_seq=0 ttl=254 time=2.111 ms
64 bytes from 172.16.10.15Q: icmp_seq=1 ttl=254 time=0.789 ms
64 bytes from 172.16.10.15Q: icmp_seq=2 ttl=254 time=0.746 ms
64 bytes from 172.16.10.15Q: icmp_seq=3 ttl=254 time=0.737 ms
64 bytes from 172.16.10.15Q: icmp_seq=4 ttl=254 time=0.735 ms
```

```

--- 172.16.10.15Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.735/1.024/2.111 ms
N7KX-podP# ping 172.16.10.16Q
PING 172.16.10.16Q (172.16.10.16Q): 56 data bytes
64 bytes from 172.16.10.16Q: icmp_seq=0 ttl=254 time=0.792 ms
64 bytes from 172.16.10.16Q: icmp_seq=1 ttl=254 time=0.789 ms
64 bytes from 172.16.10.16Q: icmp_seq=2 ttl=254 time=0.716 ms
64 bytes from 172.16.10.16Q: icmp_seq=3 ttl=254 time=0.722 ms
64 bytes from 172.16.10.16Q: icmp_seq=4 ttl=254 time=0.735 ms

--- 172.16.10.15Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.735/0.751/0.792 ms

```

Step 5 To check high availability of the Cisco FabricPath cloud, disable one of the links being used.

```

N7KX-podP(config)# interface ethernetAA
N7KX-podP(config-if)# shutdown

```

Step 6 Examine the Cisco FabricPath routing table.

```

N7KX-podP# show 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/PQ/0, number of next-hops: 0
  via ----, [60/0], 0 day/s 19:23:18, local
1/PP/0, number of next-hops: 1
  via EthAB, [115/120], 0 day/s 00:00:10, isis_fabricpath-default
1/QP/0, number of next-hops: 1
  via EthAB, [115/80], 0 day/s 00:19:17, isis_fabricpath-default
1/QQ/0, number of next-hops: 1
  via EthAB, [115/40], 0 day/s 00:19:17, isis_fabricpath-default

```

Step 7 Determine which of the interfaces will be used to forward frames to your peer pod on Cisco Nexus 7000 Series switch VDC.

Step 8 Determine which links Cisco FabricPath will use to forward traffic toward your peer pod Cisco Nexus 7000 Series switch VDC. Replace *M* with the module number where the F-type line card is installed.

```

N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type 13 src-ip 172.16.10.15P dst-ip 172.16.10.15Q vlan 10
module M
N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type 13 src-ip 172.16.10.15P dst-ip 172.16.10.16Q vlan 10
module M
N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type 13 src-ip 172.16.10.16P dst-ip 172.16.10.15Q vlan 10
module M
N7KX-podP# show fabricpath load-balance unicast forwarding-path ftag 1
switchid QP flow-type 13 src-ip 172.16.10.16P dst-ip 172.16.10.16Q vlan 10
module M

```

Source IP	Destination IP	Path That Will Be Used
172.16.10.15P	172.16.10.15Q	
172.16.10.15P	172.16.10.16Q	
172.16.10.16P	172.16.10.15Q	
172.16.10.16P	172.16.10.16Q	

Step 9 From your Cisco Nexus 7000 Series switch VDC, ping both the IP address of your peer pod Cisco Nexus 7000 Series switch VDC, 172.16.10.15Q, and 172.16.10.16Q—where Q is your peer pod number—to confirm IP connectivity between the two pods. Determine if the ping was successful.

```
N7KX-podP# ping 172.16.10.15Q
PING 172.16.10.15Q (172.16.10.15Q): 56 data bytes
64 bytes from 172.16.10.15Q: icmp_seq=0 ttl=254 time=2.111 ms
64 bytes from 172.16.10.15Q: icmp_seq=1 ttl=254 time=0.789 ms
64 bytes from 172.16.10.15Q: icmp_seq=2 ttl=254 time=0.746 ms
64 bytes from 172.16.10.15Q: icmp_seq=3 ttl=254 time=0.737 ms
64 bytes from 172.16.10.15Q: icmp_seq=4 ttl=254 time=0.735 ms

--- 172.16.10.15Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.735/1.024/2.111 ms
N7KX-podP# ping 172.16.10.16Q
PING 172.16.10.16Q (172.16.10.16Q): 56 data bytes
64 bytes from 172.16.10.16Q: icmp_seq=0 ttl=254 time=0.792 ms
64 bytes from 172.16.10.16Q: icmp_seq=1 ttl=254 time=0.789 ms
64 bytes from 172.16.10.16Q: icmp_seq=2 ttl=254 time=0.716 ms
64 bytes from 172.16.10.16Q: icmp_seq=3 ttl=254 time=0.722 ms
64 bytes from 172.16.10.16Q: icmp_seq=4 ttl=254 time=0.735 ms

--- 172.16.10.15Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.735/0.751/0.792 ms.
```

Activity Verification

You have completed this task when you attain these results:

- You have examined the Cisco FabricPath load balancing.
- You have examined the high availability of the Cisco FabricPath links.

Lab 2-4: Configure Layer 3 Switching

Complete this lab activity to practice what you learned in the related module.

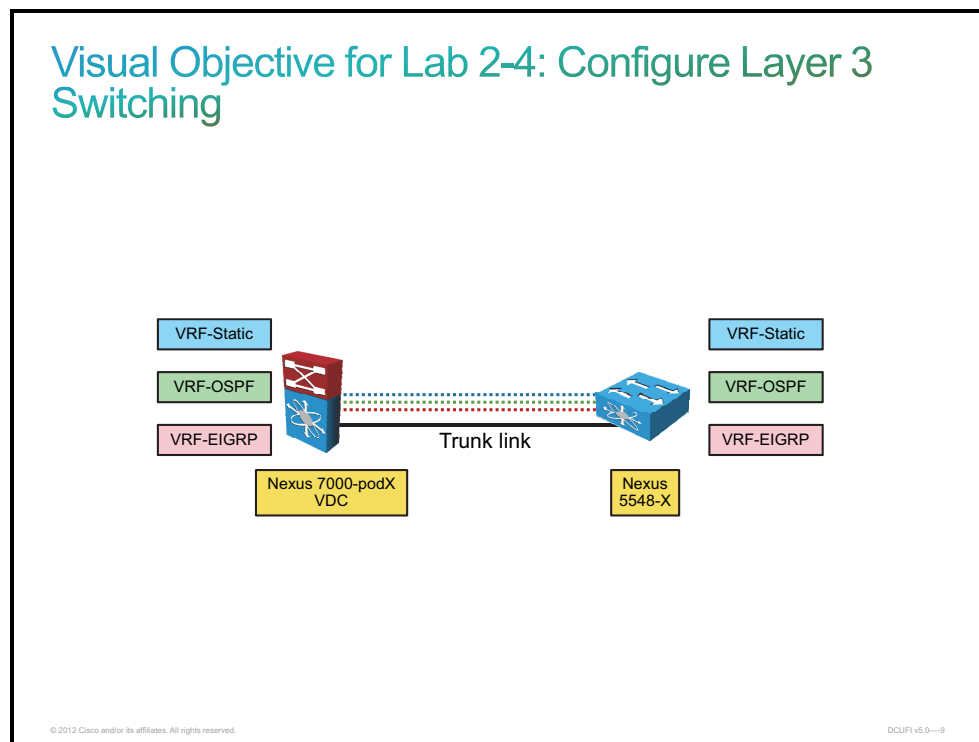
Activity Objective

In this activity, you will configure Layer 3 switching features between your Cisco Nexus 7000 Series switch VDC and your Cisco Nexus 5548 Platform switch. After completing this activity, you will be able to meet these objectives:

- Configure RIP and verify the configuration
- Configure VRF instances with static routing and verify the configuration
- Configure VRF instances with OSPFv2 and verify the configuration
- Configure VRF instances with EIGRP and verify the configuration

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required to complete this activity:

- Two Cisco Nexus 7000 Series switch VDCs
- Two Cisco Nexus 5500 Platform switches

Command List

This table describes the commands that are used in this activity.

Command	Description
feature interface-vlan	Enables the interface-vlan feature, which allows the creation of switched virtual interfaces (SVI)
ip address <address>/<prefix>	Configures an IP address and prefix on an interface
feature rip	Enables the Routing Information Protocol (RIP) feature
show license usage	Displays the license usage in a VDC
ip router rip <tag>	Activates a RIP process on an interface
show ip route	Displays the IP routing table
show ip rip	Displays basic parameters for a RIP process
router rip <tag>	Starts a RIP routing process
show vrf	Lists the virtual routing and forwarding (VRFs) that are present in a VDC
show vrf detail	Displays details for the VRFs in a VDC
show vrf <vrf> interface	Lists the interfaces that are associated with a VRF
vrf member <vrf>	Associates an interface with a VRF
vrf context <vrf>	Creates a new VRF context
ip route <subnet>/<prefix> <next-hop>	Creates a static route to a subnet using a specified next-hop router
show ip route vrf <vrf>	Displays the IP routing table for a VRF
routing-context vrf <vrf>	Sets the scope for routing-related commands to a specific VRF
feature ospf	Enables the Open Shortest Path First (OSPF) feature
ip router ospf <tag> area <area>	Enables an OSPF process on an interface for a specific area
show ip ospf	Displays basic parameters for an OSPF process
router ospf <tag>	Starts an OSPF routing process
show ip ospf vrf <vrf>	Displays basic parameters for an OSPF process in a VRF
show ip ospf neighbors vrf <vrf>	Displays the list of OSPF neighbors for a VRF
show ip ospf database vrf <vrf>	Lists the content of the OSPF database for a VRF
router-id <id>	Sets the router ID for an OSPF process
vrf <vrf>	Enters VRF configuration mode under a routing process
show ip ospf interface <intf>	Displays OSPF interface parameters
auto-cost reference-bandwidth <bw> <unit>	Changes the OSPF auto-cost reference bandwidth
show ip ospf interface brief	Displays an overview of the interfaces that are enabled for OSPF

feature eigrp	Enables the Enhanced Interior Gateway Routing Protocol (EIGRP) feature
router eigrp <tag>	Starts an EIGRP routing process
ip router eigrp <tag>	Activates an EIGRP routing process on an interface
show ip eigrp	Displays basic EIGRP parameters
autonomous-system <as-nr>	Sets the autonomous system (AS) number for EIGRP in a VRF
show ip eigrp neighbors	Displays the list of EIGRP neighbors

Task 1: Establish VRF Connectivity Between Your Nexus 7000 Series Switch VDC and Your Cisco Nexus 5500 Platform Switch

In this task, you will configure IP connections between your VDC and your Cisco Nexus 5500 Platform switch.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.
- Step 2** Change VLAN 10 back to Classic Ethernet (CE) mode and remove the entire Cisco FabricPath configuration.

```
N7KX-podP(config)# vlan 10
N7KX-podP(config-vlan)# mode ce
N7KX-podP(config-vlan)# exit
N7KX-podP(config-vlan)# no feature-set fabricpath
```

Feature-set Operation may take up to 30 minutes depending on the size of configuration.

- Step 3** Configure interface Ethernet *AA* as a trunk.

```
N7KX-podP(config)# interface ethernet AA
N7KX-podP(config-if)# switchport mode trunk
N7KX-podP(config-if)# no shutdown
```

- Step 4** Shut down the interface on your Cisco Nexus 7000 Series switch VDC that leads to your peer pod Cisco Nexus 5500 Platform switch. Use the Lab Connections Job Aids to find the correct interface.

```
N7KX-podP(config)# interface ethernet AB
N7KX-podP(config-if)# shutdown
```

- Step 5** Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

- Step 6** Change VLAN 10 back to CE mode and remove the entire Cisco FabricPath configuration.

```
N5548-P(config)# vlan 10
N5548-P(config-vlan)# mode ce
N5548-P(config-vlan)# exit
N5548-P(config-vlan)# no feature-set fabricpath
```

Feature-set Operation may take up to 30 minutes depending on the size of configuration.

```
N5548-P(config-vlan)# no install feature-set fabricpath
```

- Step 7** Configure interface Ethernet *AA* as a trunk.

```
N5548-P(config)# interface ethernet AA
N5548-P(config-if)# switchport mode trunk
N5548-P(config-if)# no shutdown
```

- Step 8** Disable the link toward your peer pod.

```
N5548-P(config)# interface ethernetAB
N5548-P(config-if)# shutdown
```

- Step 9** Check IP connectivity between your Cisco Nexus 7000 Series switch VDC and the Cisco Nexus 5500 Platform switch in your pod.

```
N7KX-podP# ping 172.16.10.51
PING 172.16.10.51 (172.16.10.51): 56 data bytes
Request 0 timed out
64 bytes from 172.16.10.51: icmp_seq=1 ttl=254 time=1.22 ms
64 bytes from 172.16.10.51: icmp_seq=2 ttl=254 time=0.701 ms
64 bytes from 172.16.10.51: icmp_seq=3 ttl=254 time=0.999 ms
64 bytes from 172.16.10.51: icmp_seq=4 ttl=254 time=1.023 ms

--- 172.16.10.51 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.701/0.985/1.22 ms
```

Note Do not proceed until you have confirmed IP connectivity on VLAN 10 between your Cisco Nexus 7000 Series switch VDC and the Cisco Nexus 5500 Platform switch.

- Step 10** Enable the RIP feature on both the Cisco Nexus 7000 Series switch VDC and the Cisco Nexus 5500 Platform switch.

```
N7KX-podP(config)# feature rip
```

```
N5548-P(config)# feature rip
```

- Step 11** Configure loopback interface 10 on your Cisco Nexus 7000 Series switch VDC. Assign address 192.168.10.P1/32—where **P** is your assigned pod number—and enable RIP on it.

```
N7KX-podP(config)# interface loopback 10
N7KX-podP(config-if)# ip address 192.168.10.P1/32
N7KX-podP(config-if)# ip router rip MYRIP
```

- Step 12** Enable RIP on interface VLAN 10 as well.

```
N7KX-podP(config)# interface vlan 10
N7KX-podP(config-if)# ip router rip MYRIP
```

- Step 13** Configure loopback interface 10 on your Cisco Nexus 5500 Platform switch. Assign the address 192.168.10.P2/32—where **P** is your assigned pod number—and enable RIP on it. Also enable RIP on interface VLAN 10.

```
N5548-P(config)# interface loopback 10
N5548-P(config-if)# ip address 192.168.10.P2/32
N5548-P(config-if)# ip router rip MYRIP
N5548-P(config)# interface vlan 10
N5548-P(config-if)# ip router rip MYRIP
```

- Step 14** Examine your routing table to determine if you received routes via the RIP protocol.

```
N5548-P# show ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

172.16.10.0/24, ubest/mbest: 1/0, attached
  *via 172.16.10.5P, Vlan10, [0/0], 2d08h, direct
172.16.10.5P/32, ubest/mbest: 1/0, attached
  *via 172.16.10.5P, Vlan10, [0/0], 2d08h, local
192.168.10.P2/32, ubest/mbest: 2/0, attached
  *via 192.168.10.P2, Lo10, [0/0], 00:03:32, local
  *via 192.168.10.P2, Lo10, [0/0], 00:03:32, direct
```

Step 15 Examine the RIP process.

```
N5548-P# show ip rip
Note: process currently not running
```

Step 16 Enable the RIP process by using the appropriate process tag on both the Cisco Nexus 7000 Series switch VDC and the Cisco Nexus 5500 Platform switch.

```
N5548-P(config)# router rip MYRIP
```

```
N7KX-podP(config)# router rip MYRIP
```

Step 17 Examine your routing table again.

```
N5548-P# sh ip route
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]

172.16.10.0/24, ubest/mbest: 1/0, attached
    *via 172.16.10.5P, Vlan10, [0/0], 2d11h, direct
172.16.10.5P/32, ubest/mbest: 1/0, attached
    *via 172.16.10.5P, Vlan10, [0/0], 2d11h, local
192.168.10.P1/32, ubest/mbest: 1/0
    *via 172.16.10.15P, Vlan10, [120/2], 01:59:20, rip-MYRIP, rip
192.168.10.12/32, ubest/mbest: 2/0, attached
    *via 192.168.10.P2, Lo10, [0/0], 03:05:26, local
    *via 192.168.10.P2, Lo10, [0/0], 03:05:26, direct
```

Step 18 Ping Cisco Nexus 7000 Series switch VDC loopback 10 IP address 192.168.10.P1 by using the Cisco Nexus 5500 Platform switch loopback 10 interface.

```
N5548-P# ping 192.168.10.P1 source 192.168.10.P2
PING 192.168.10.P1 (192.168.10.P1) from 192.168.10.P2: 56 data bytes
64 bytes from 192.168.10.P1: icmp_seq=0 ttl=254 time=1.021 ms
64 bytes from 192.168.10.P1: icmp_seq=1 ttl=254 time=1.334 ms
64 bytes from 192.168.10.P1: icmp_seq=2 ttl=254 time=0.917 ms
64 bytes from 192.168.10.P1: icmp_seq=3 ttl=254 time=4.385 ms
64 bytes from 192.168.10.P1: icmp_seq=4 ttl=254 time=9.602 ms

--- 192.168.10.P1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.917/3.451/9.602 ms
```

Activity Verification

You have completed this task when you attain these results:

- You have enabled Layer 3 connectivity over the trunk.
- You have configured RIP on your Cisco Nexus 7000 Series switch VDC and Cisco Nexus 5500 Platform switch.
- You have verified that RIP is exchanging routing information.
- You have a working ping between loopback 10 interfaces.

Task 2: Static Routing

In this task, you will configure static routing within one of the VRFs.

Activity Procedure

- Step 1** On your Cisco Nexus 7000 Series switch VDC, configure a VRF named **STATIC-VRF**. Then create a loopback 0 interface. Assign it to the just-created VRF and configure IP address 192.168.11.**P**1/32, where **P** is your assigned pod number.

```
N7KX-podP(config)# vrf context STATIC-VRF
N7KX-podP(config-vrf)# interface loopback 0
N7KX-podP(config-if)# vrf member STATIC-VRF
% Deleted all L3 config on interface loopback0
N7KX-podP(config-if)# ip address 192.168.11.P1/32
```

- Step 2** Examine the routing table for VRF **STATIC-VRF**.

```
N7KX-PODP(config-if)# show ip route vrf STATIC-VRF
IP Route Table for VRF "STATIC-VRF"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.11.P1/32, ubest/mbest: 2/0, attached
  *via 192.168.11.P1, Lo0, [0/0], 00:03:21, local
  *via 192.168.11.P1, Lo0, [0/0], 00:03:21, direct
```

- Step 3** Create VLAN 11 and a SVI for VLAN with the IP address 172.16.11.**P**1/24, where **P** is your assigned pod number. Assign VLAN 11 interface to the VRF **STATIC-VRF**.

```
N7KX-podP(config)# vlan 11
N7KX-podP(config-vlan)# exit
N7KX-podP(config)# interface vlan 11
N7KX-podP(config-if)# vrf member STATIC-VRF
% Deleted all L3 config on interface Vlan11
N7KX-podP(config-if)# ip address 172.16.11.P1/24
N7KX-podP(config-if)# no shutdown
```

- Step 4** On Cisco Nexus 7000 Series switch VDC, configure a static route for VRF **VRF-STATIC** that points to the loopback 0 interface on your Cisco Nexus 5500 Platform switch with the IP address 192.168.11.**P**2/32 via the VLAN 11 IP address (172.16.11.**P**2) of your Cisco Nexus 5500 Platform switch.

```
N7KX-podP(config)# vrf context STATIC-VRF
N7KX-podP(config-vrf)# ip route 192.168.11.P2/32 172.16.11.P2
```

- Step 5** On your Cisco Nexus 5500 Platform switch, configure a VRF named **STATIC-VRF**. Then create a loopback 0 interface. Assign it to the just-created VRF and configure the IP address 192.168.11.**P**2/32, where **P** is your assigned pod number.

```
N5548-P(config)# vrf context STATIC-VRF
N5548-P(config-vrf)# interface loopback 0
N5548-P(config-if)# vrf member STATIC-VRF
% Deleted all L3 config on interface loopback0
N5548-P(config-if)# ip address 192.168.11.P2/32
```

- Step 6** Create VLAN 11 and a SVI for VLAN with the IP address 172.16.11.**P**2/24, where **P** is your assigned pod number. Assign VLAN 11 interface to the VRF **STATIC-VRF**.

```
N5548-P(config)# vlan 11
N5548-P(config-vlan)# exit
N5548-P(config)# interface vlan 11
N5548-P(config-if)# vrf member STATIC-VRF
% Deleted all L3 config on interface Vlan11
N5548-P(config-if)# ip address 172.16.11.P2/24
N5548-P(config-if)# no shutdown
```

- Step 7** On the Cisco Nexus 5500 Platform switch, configure a static route in VRF **STATIC-VRF** that points to the loopback 0 interface on your Cisco Nexus 7000 Series switch VDC with IP address 192.168.11.P1/32 via the VLAN 11 IP address of your Cisco Nexus 7000 Series switch VDC (172.16.11.P1).

```
N5548-P(config)# vrf context STATIC-VRF
N5548-P(config-vrf)# ip route 192.168.11.P1/32 172.16.11.P1
```

- Step 8** Examine the routing table.

```
N5548-P# show ip route vrf STATIC-VRF
IP Route Table for VRF "STATIC-VRF"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

172.16.11.0/24, ubest/mbest: 1/0, attached
    *via 172.16.11.P2, Vlan11, [0/0], 00:19:27, direct
172.16.11.P2/32, ubest/mbest: 1/0, attached
    *via 172.16.11.P2, Vlan11, [0/0], 00:19:27, local
192.168.11.P1/32, ubest/mbest: 1/0
    *via 172.16.11.P1, Vlan11, [1/0], 00:19:26, static
192.168.11.P2/32, ubest/mbest: 2/0, attached
    *via 192.168.11.P2, Lo0, [0/0], 00:27:58, local
    *via 192.168.11.P2, Lo0, [0/0], 00:27:58, direct
```

Note If you do not specify the VRF, the default VRF is used for all IP routing-related commands.

- Step 9** Set the scope of all Cisco NX-OS IP routing-related commands to use the VRF **STATIC-VRF** for your current session.

```
N5548-P# routing-context vrf STATIC-VRF
```

- Step 10** Ping the IP address of VLAN 11 address on the Cisco Nexus 7000 Series switch VDC.

```
N5548-P%STATIC-VRF# ping 192.168.11.P1 source 192.168.11.P2
PING 192.168.11.P1 (192.168.11.P1) from 192.168.11.P2: 56 data bytes
64 bytes from 192.168.11.P1: icmp_seq=0 ttl=254 time=2.358 ms
64 bytes from 192.168.11.P1: icmp_seq=1 ttl=254 time=0.821 ms
64 bytes from 192.168.11.P1: icmp_seq=2 ttl=254 time=0.891 ms
64 bytes from 192.168.11.P1: icmp_seq=3 ttl=254 time=7.291 ms
64 bytes from 192.168.11.P1: icmp_seq=4 ttl=254 time=9.598 ms

--- 192.168.11.P1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.821/4.191/9.598 ms
```

- Step 11** Reset the command scope to the default VRF.

```
N5548-P%STATIC-VRF# routing-context vrf default
```

Activity Verification

You have completed this task when you attain these results:

- You have verified IP connectivity between the loopback IP addresses within the **STATIC-VRF**.

Task 3: OSPFv2

In this task, you will configure OSPF routing within one of your VRFs.

Activity Procedure

Step 1 On your Cisco Nexus 7000 Series switch VDC, configure VLAN 12.

```
N7KX-podP(config)# vlan 12
N7KX-podP(config-vlan)# exit
```

Step 2 Configure a VRF context named **OSPF-VRF**.

```
N7KX-podP(config)# vrf context OSPF-VRF
```

Step 3 Configure interface VLAN12, place it in **OSPF-VRF**, and assign IP address 172.16.12.P1/24, where **P** is your pod number.

```
N7KX-podP(config)# interface vlan 12
N7KX-podP(config-if)# vrf member OSPF-VRF
% Deleted all L3 config on interface Vlan12
N7KX-podP(config-if)# ip address 172.16.12.P1/24
N7KX-podP(config-if)# no shutdown
```

Step 4 Configure loopback interface 12, assign it to **VRF OSPF-VRF**, and assign the IP address 192.168.12.P1/32, where **P** is your assigned pod number.

```
N7KX-podP(config)# interface loopback 12
N7KX-podP(config-if)# vrf member OSPF-VRF
% Deleted all L3 config on interface loopback12
N7KX-podP(config-if)# ip address 192.168.12.P1/32
```

Step 5 Enable the OSPF feature.

```
N7KX-podP(config)# feature ospf
```

Step 6 Verify the license usage on your Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP# show license usage
```

Feature	Ins	Lic	Status	Expiry	Date	Comments
		Count				
MPLS_PKG	Yes	-	Unused	Never		-
STORAGE-ENT	Yes	-	Unused	Never		-
ENTERPRISE_PKG	No	-	Unused			-
FCOE-N7K-F132XP	Yes	1	Unused	Never		-
ENHANCED_LAYER2_PKG	Yes	-	Unused	Never		-
SCALABLE_SERVICES_PKG	Yes	-	Unused	Never		-
TRANSPORT_SERVICES_PKG	Yes	-	In use	Never		-
LAN_ADVANCED_SERVICES_PKG	Yes	-	Unused	Never		-
LAN_ENTERPRISE_SERVICES_PKG	Yes	-	In use	Never		-

--

Step 7 Verify which feature will cause the LAN_ENTERPRISE_SERVICES_PKG to be used.

```
N7KX-podP# show license usage LAN_BASE_SERVICES_PKG
```

```
Application          Vdc
```

```
-----
ospf                  PODP
-----
```

Step 8 Configure the OSPF process with the process ID **MYOSPF**.

```
N7KX-podP(config)# router ospf MYOSPF
```

Step 9 Configure OSPF in area 0 on interface VLAN12 with the process ID **MYOSPF**.

```
N7KX-podP(config)# interface vlan 12
N7KX-podP(config-if)# ip router ospf MYOSPF area 0
```

Step 10 Configure OSPF in area **P1** on interface loopback 12, where **P** is your assigned pod number and the process ID is **MYOSPF**.

```
N7KX-podP(config)# interface loopback 12
N7KX-podP(config-if)# ip router ospf MYOSPF area P1
```

Step 11 Examine the OSPF process.

```
N7KX-podP# sh ip ospf vrf OSPF-VRF

Routing Process MYOSPF with ID 172.16.12.P1 VRF OSPF-VRF
Stateful High Availability enabled
Graceful-restart is configured
  Grace period: 60 state: Inactive
  Last graceful restart exit status: None
Supports only single TOS(TOS0) routes
Supports opaque LSA
Administrative distance 110
Reference Bandwidth is 40000 Mbps
SPF throttling delay time of 200.000 msecs,
  SPF throttling hold time of 1000.000 msecs,
  SPF throttling maximum wait time of 5000.000 msecs
LSA throttling start time of 0.000 msecs,
  LSA throttling hold interval of 5000.000 msecs,
  LSA throttling maximum wait time of 5000.000 msecs
Minimum LSA arrival 1000.000 msec
LSA group pacing timer 10 secs
Maximum paths to destination 8
Number of external LSAs 0, checksum sum 0
Number of opaque AS LSAs 0, checksum sum 0
Number of areas is 2, 2 normal, 0 stub, 0 nssa
Number of active areas is 1, 1 normal, 0 stub, 0 nssa
  Area BACKBONE(0.0.0.0)
    Area has existed for 00:01:08
    Interfaces in this area: 1 Active interfaces: 1
    Passive interfaces: 1 Loopback interfaces: 1
    No authentication available
    SPF calculation has run 4 times
    Last SPF ran for 0.000363s
    Area ranges are
    Number of LSAs: 4, checksum sum 0x171e8
  Area (0.0.0.P1) (Inactive)
    Area has existed for 00:00:22
    Interfaces in this area: 1 Active interfaces: 0
    Passive interfaces: 1 Loopback interfaces: 0
    No authentication available
    SPF calculation has run 0 times
    Last SPF ran for 0.000000s
    Area ranges are
    Number of LSAs: 0, checksum sum 0
```

Note Make sure that you specify the correct VRF. Otherwise, the default VRF information will be presented.

Step 12 On your Cisco Nexus 5500 Platform switch, configure VLAN 12.

```
N5548-P(config)# vlan 12
N5548-P(config-vlan)# exit
```

Step 13 Configure a VRF context named **OSPF-VRF**.

```
N5548-P(config)# vrf context OSPF-VRF
```

Step 14 Configure interface VLAN12, place it in an **OSPF-VRF**, and assign the IP address 172.16.12.**P2**/24, where **P** is your pod number.

```
N5548-P(config)# interface vlan 12
N5548-P(config-if)# vrf member OSPF-VRF
% Deleted all L3 config on interface Vlan12
N5548-P(config-if)# ip address 172.16.12.P2/24
N5548-P(config-if)# no shutdown
```

Step 15 Ping the IP address of VLAN 12 on the Cisco Nexus 7000 Series switch VDC.

```
N5548-P# ping 172.16.12.P1 vrf ospf-vrf
PING 172.16.12.P1 (172.16.12.P1): 56 data bytes
Request 0 timed out
64 bytes from 172.16.12.P1: icmp_seq=1 ttl=254 time=1.079 ms
64 bytes from 172.16.12.P1: icmp_seq=2 ttl=254 time=0.744 ms
64 bytes from 172.16.12.P1: icmp_seq=3 ttl=254 time=0.752 ms
64 bytes from 172.16.12.P1: icmp_seq=4 ttl=254 time=7.48 ms

--- 172.16.12.P1 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.744/2.513/7.48 ms
```

Note On Cisco NX-OS, VRF naming is not case-sensitive.

Step 16 Configure loopback interface 12, assign it to **VRF OSPF-VRF**, and assign the IP address 192.168.12.**P2**/32, where **P** is your assigned pod number.

```
N5548-P(config)# interface loopback 12
N5548-P(config-if)# vrf member OSPF-VRF
% Deleted all L3 config on interface loopback12
N5548-P(config-if)# ip address 192.168.12.P2/32
```

Step 17 Enable the OSPF feature.

```
N5548-P(config)# feature ospf
```

Step 18 Verify the license usage on your Cisco Nexus 5500 Platform switch.

```
N5548-P# show license usage
```

Feature	Ins	Lic	Status	Expiry	Date	Comments
		Count				
FCOE_NPV_PKG	No	-	In use			Grace 117D 10H
FM_SERVER_PKG	Yes	-	Unused	Never		-
ENTERPRISE_PKG	Yes	-	Unused	Never		-
FC_FEATURES_PKG	Yes	-	Unused	Never		-
VMFEX_FEATURE_PKG	Yes	-	Unused	Never		-
ENHANCED_LAYER2_PKG	Yes	-	In use	Never		-
LAN_BASE_SERVICES_PKG	Yes	-	In use	Never		-
LAN_ENTERPRISE_SERVICES_PKG	Yes	-	Unused	Never		-

Step 19 Verify which feature will cause the LAN_BASE_SERVICES_PKG to be used.

```
N5548-P# show license usage LAN_BASE_SERVICES_PKG
```

Application

btcm
ospf

Step 20 Configure the OSPF process with the process ID **MYOSPF**.

```
N5548-P(config)# router ospf MYOSPF
```

Step 21 Configure OSPF in area 0 on interface VLAN12 with the process ID MYOSPF.

```
N5548-P(config)# interface vlan 12
N5548-P(config-if)# ip router ospf MYOSPF area 0
```

Step 22 Configure OSPF in area P2 on interface loopback 12, where P is your assigned pod number. Use and the process ID MYOSPF.

```
N5548-P(config)# interface loopback 12
N5548-P(config-if)# ip router ospf MYOSPF area P2
```

Step 23 Examine the routing table.

```
N5548-P(config)# sh ip route vrf OSPF-VRF
IP Route Table for VRF "OSPF-VRF"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

172.16.12.0/24, ubest/mbest: 1/0, attached
  *via 172.16.12.P2, Vlan12, [0/0], 01:02:09, direct
172.16.12.12/32, ubest/mbest: 1/0, attached
  *via 172.16.12.P2, Vlan12, [0/0], 01:02:09, local
192.168.12.P1/32, ubest/mbest: 1/0
  *via 172.16.12.P1, Vlan12, [110/41], 00:00:49, ospf-MYOSPF, inter
192.168.12.12/32, ubest/mbest: 2/0, attached
  *via 192.168.12.P2, Lo12, [0/0], 00:42:33, local
  *via 192.168.12.P2, Lo12, [0/0], 00:42:33, direct
```

Step 24 Ping the loopback 12 on your Cisco Nexus 7000 Series switch VDC. As a source, use loopback 12 on your Cisco Nexus 5500 Platform switch.

```
N5548-P# ping 192.168.12.P1 source 192.168.12.P2 vrf OSPF-VRF
PING 192.168.12.P1 (192.168.12.P1) from 192.168.12.12: 56 data bytes
64 bytes from 192.168.12.P1: icmp_seq=0 ttl=254 time=7.882 ms
64 bytes from 192.168.12.P1: icmp_seq=1 ttl=254 time=0.711 ms
64 bytes from 192.168.12.P1: icmp_seq=2 ttl=254 time=0.673 ms
64 bytes from 192.168.12.P1: icmp_seq=3 ttl=254 time=0.744 ms
64 bytes from 192.168.12.P1: icmp_seq=4 ttl=254 time=0.718 ms

--- 192.168.12.P1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.673/2.145/7.882 ms
```

Step 25 Examine the OSPF database for VRF OSPF-VRF.

```
N5548-P# show ip ospf database vrf OSPF-VRF
OSPF Router with ID (192.168.12.P2) (Process ID MYOSPF VRF OSPF-VRF)
```

Router Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	Checksum	Link Count
192.168.12. P1	192.168.12. P1	777	0x80000015	0xa3c9	1
192.168.12. P2	192.168.12. P2	596	0x80000017	0x9dca	1

Network Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	Checksum
172.16.12. P2	192.168.12. P2	767	0x80000014	0x07e7

Summary Network Link States (Area 0.0.0.0)

Link ID	ADV Router	Age	Seq#	Checksum
192.168.12. P1	192.168.12. P1	817	0x80000014	0x0840
192.168.12. P2	192.168.12. P2	596	0x80000014	0xf74e

Router Link States (Area 0.0.0.P2)

Link ID	ADV Router	Age	Seq#	Checksum	Link Count
192.168.12. P2	192.168.12. P2	596	0x80000014	0xd1e7	1

Summary Network Link States (Area 0.0.0.P2)

Link ID	ADV Router	Age	Seq#	Checksum
172.16.12.0	192.168.12.P2	596	0x80000014	0x24b3
192.168.12.P1	192.168.12.P2	596	0x80000014	0x938b

Activity Verification

You have completed this task when you attain these results:

- You have examined the OSPF topology information.
- You have verified IP connectivity within the **OSPF-VRF**.

Task 4: EIGRP

In this task, you will configure EIGRP routing within one of the VRFs.

Activity Procedure

Complete these steps:

Step 1 On your Cisco Nexus 7000 Series switch VDC, configure VLAN 13.

```
N7KX-podP(config)# vlan 13
N7KX-podP(config-vlan)# exit
```

Step 2 Configure a VRF context named **EIGRP-VRF**.

```
N7KX-podP(config)# vrf context EIGRP-VRF
```

Step 3 Configure interface VLAN13, place it in **EIGRP-VRF**, and assign the IP address 172.16.13.P1/24, where **P** is your pod number.

```
N7KX-podP(config)# interface vlan 13
N7KX-podP(config-if)# vrf member EIGRP-VRF
% Deleted all L3 config on interface Vlan13
N7KX-podP(config-if)# ip address 172.16.13.P1/24
N7KX-podP(config-if)# no shutdown
```

Step 4 Configure loopback interface 13, assign it to VRF **EIGRP-VRF**, and assign IP address 192.168.13.P1/32, where **P** is your assigned pod number.

```
N7KX-podP(config)# interface loopback 13
N7KX-podP(config-if)# vrf member EIGRP-VRF
% Deleted all L3 config on interface loopback13
N7KX-podP(config-if)# ip address 192.168.13.P1/32
```

Step 5 Enable the EIGRP feature.

```
N7KX-podP(config)# feature eigrp
```

Step 6 Verify which feature will cause the LAN_ENTERPRISE_SERVICES_PKG to be used.

```
N7KX-podP# show license usage LAN_ENTERPRISE_SERVICES_PKG
Application          Vdc
-----
ospf                  PODP
eigrp                 PODP
-----
```

Step 7 Set the scope of all Cisco NX-OS IP routing-related commands to use the VRF **EIGRP-VRF** for your current session.

```
N7KX-podP(config)# routing-context vrf EIGRP-VRF
```

Step 8 Configure an EIGRP process with the process tag **MYEIGRP**.

```
N7KX-podP%EIGRP-VRF(config)# router EIGRP MYEIGRP
```

Step 9 Activate EIGRP on interface VLAN13.

```
N7KX-podP%EIGRP-VRF(config)# interface vlan 13
N7KX-podP%EIGRP-VRF(config-if)# ip router eigrp MYEIGRP
```

Step 10 Activate EIGRP on interface loopback 13.

```
N7KX-podP%EIGRP-VRF(config)# interface loopback 13
N7KX-podP%EIGRP-VRF(config-if)# ip router eigrp MYEIGRP
```

Step 11 Examine the EIGRP process.

```
N7KX-podP%EIGRP-VRF# sh ip eigrp
Process-tag: MYEIGRP
Status: shutdown
Authentication mode: none
Authentication key-chain: none
Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
IP proto: 88 Multicast group: 224.0.0.10
Int distance: 90 Ext distance: 170
Max paths: 8
Number of EIGRP interfaces: 2 (1 loopbacks)
Number of EIGRP passive interfaces: 0
Number of EIGRP peers: 0
Graceful-Restart: Enabled
Stub-Routing: Disabled
NSF converge time limit/expiries: 120/0
NSF route-hold time limit/expiries: 240/0
NSF signal time limit/expiries: 20/0
Redistributed max-prefix: Disabled
```

Step 12 Determine why the EIGRP process shut down.

Step 13 Configure EIGRP autonomous system number 35 for the VRF EIGRP-VRF.

```
N7KX-podP%EIGRP-VRF(config)# router eigrp MYEIGRP
N7KX-podP%EIGRP-VRF(config-router)# vrf EIGRP-VRF
N7KX-podP%EIGRP-VRF(config-router-vrf)# autonomous-system 35
```

Step 14 Examine the EIGRP process once again.

```
N7K-X-podP%EIGRP-VRF# show ip eigrp
IP-EIGRP AS 35 ID 192.168.13.1 VRF EIGRP-VRF
Process-tag: MYEIGRP
Status: running
Authentication mode: none
Authentication key-chain: none
Metric weights: K1=1 K2=0 K3=1 K4=0 K5=0
IP proto: 88 Multicast group: 224.0.0.10
Int distance: 90 Ext distance: 170
Max paths: 8
Number of EIGRP interfaces: 2 (1 loopbacks)
Number of EIGRP passive interfaces: 0
Number of EIGRP peers: 0
Graceful-Restart: Enabled
Stub-Routing: Disabled
NSF converge time limit/expiries: 120/0
NSF route-hold time limit/expiries: 240/0
NSF signal time limit/expiries: 20/0
Redistributed max-prefix: Disabled
```

Step 15 On your Cisco Nexus 5500 Platform switch, configure VLAN 13.

```
N5548-P(config)# vlan 13
N5548-P(config-vlan)# exit
```

Step 16 Configure a VRF context named EIGRP-VRF.

```
N5548-P(config)# vrf context EIGRP-VRF
```

Step 17 Configure interface VLAN13, place it in **EIGRP-VRF**, and assign it the IP address 172.16.13.**P2**/24, where **P** is your pod number.

```
N5548-P(config)# interface vlan 13
N5548-P(config-if)# vrf member EIGRP-VRF
% Deleted all L3 config on interface Vlan13
N5548-P(config-if)# ip address 172.16.13.P2/24
N5548-P(config-if)# no shutdown
```

Step 18 Configure loopback interface 13, assign it to VRF **EIGRP-VRF**, and assign it the IP address 192.168.13.**P2**/32, where **P** is your assigned pod number.

```
N5548-P(config)# interface loopback 13
N5548-P(config-if)# vrf member EIGRP-VRF
% Deleted all L3 config on interface loopback13
N5548-P(config-if)# ip address 192.168.13.P2/32
```

Step 19 Ping VLAN 13 interface on the Cisco Nexus 7000 Series switch VDC.

Step 20 Enable the EIGRP feature.

```
N5548-P(config)# feature eigrp
```

Step 21 Set the scope of all Cisco NX-OS IP routing-related commands to use the VRF **EIGRP-VRF** for your current session.

```
N5548-P# routing-context vrf EIGRP-VRF
```

Step 22 Ping VLAN interface 13 on the Cisco Nexus 7000 Series switch VDC.

```
N5548-P%EIGRP-VRF# ping 172.16.13.P1
PING 172.16.13.P1 (172.16.13.P1): 56 data bytes
Request 0 timed out
64 bytes from 172.16.13.P1: icmp_seq=1 ttl=254 time=1.017 ms
64 bytes from 172.16.13.P1: icmp_seq=2 ttl=254 time=0.903 ms
64 bytes from 172.16.13.P1: icmp_seq=3 ttl=254 time=0.868 ms
64 bytes from 172.16.13.P1: icmp_seq=4 ttl=254 time=7.174 ms

--- 172.16.13.P1 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.868/2.49/7.174 ms
```

Step 23 Configure the EIGRP process with process tag **MYEIGRP**.

```
N5548-P%EIGRP-VRF(config)# router EIGRP MYEIGRP
```

Step 24 Activate EIGRP on interface VLAN13.

```
N5548-P%EIGRP-VRF(config)# interface vlan 13
N5548-P%EIGRP-VRF(config-if)# ip router eigrp MYEIGRP
```

Step 25 Activate EIGRP on interface loopback 13.

```
N5548-P%EIGRP-VRF(config)# interface loopback 13
N5548-P%EIGRP-VRF(config-if)# ip router eigrp MYEIGRP
```

Step 26 Configure EIGRP autonomous system number 35 for the VRF **EIGRP-VRF**.

```
N5548-P%EIGRP-VRF(config)# router eigrp MYEIGRP
N5548-P%EIGRP-VRF(config-router)# vrf EIGRP-VRF
N5548-P%EIGRP-VRF(config-router-vrf)# autonomous-system 35
```

Step 27 Verify that an EIGRP adjacency has been established between your Cisco Nexus 7000 Series switch VDC and your Cisco Nexus 5500 Platform switch.

```
N5548-P%EIGRP-VRF# sh ip eigrp neighbors
IP-EIGRP neighbors for process 35 VRF EIGRP-VRF
H   Address                Interface      Hold  Uptime  SRTT   RTO  Q  Seq
                               (sec)          (ms)    Cnt  Num
0   172.16.13.P1            Vlan13        11    00:00:03  2      200  0   3
```

Step 28 Examine the routing table for VRF **EIGRP-VRF**.

```
N5548-P%EIGRP-VRF# show ip route
IP Route Table for VRF "EIGRP-VRF"
'*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]

172.16.13.0/24, ubest/mbest: 1/0, attached
    *via 172.16.13.P2, Vlan13, [0/0], 00:05:04, direct
172.16.13.12/32, ubest/mbest: 1/0, attached
    *via 172.16.13.P2, Vlan13, [0/0], 00:05:04, local
192.168.13.0/24, ubest/mbest: 1/0
    *via 172.16.13.P1, Vlan13, [90/130816], 00:02:30, eigrp-MYEIGRP, internal
192.168.13.12/32, ubest/mbest: 2/0, attached
    *via 192.168.13.P2, Lo13, [0/0], 00:21:32, local
    *via 192.168.13.P2, Lo13, [0/0], 00:21:32, direct
```

Step 29 Reset the command scope on both the Cisco Nexus 7000 Series switch VDC and the Cisco Nexus 5500 Platform switch to the default VRF.

```
N5548-P%EIGRP-VRF# routing-context vrf default
```

```
N7KX-podP%EIGRP-VRF# routing-context vrf default
```

Step 30 Save the configuration on your Cisco Nexus 7000 Series switch VDC.

Activity Verification

You have completed this task when you attain these results:

- You have examined the EIGRP topology information.
- You have verified IP connectivity within the **EIGRP-VRF**.

Lab 3-1: Configure OTV

Complete this lab activity to practice what you learned in the related module.

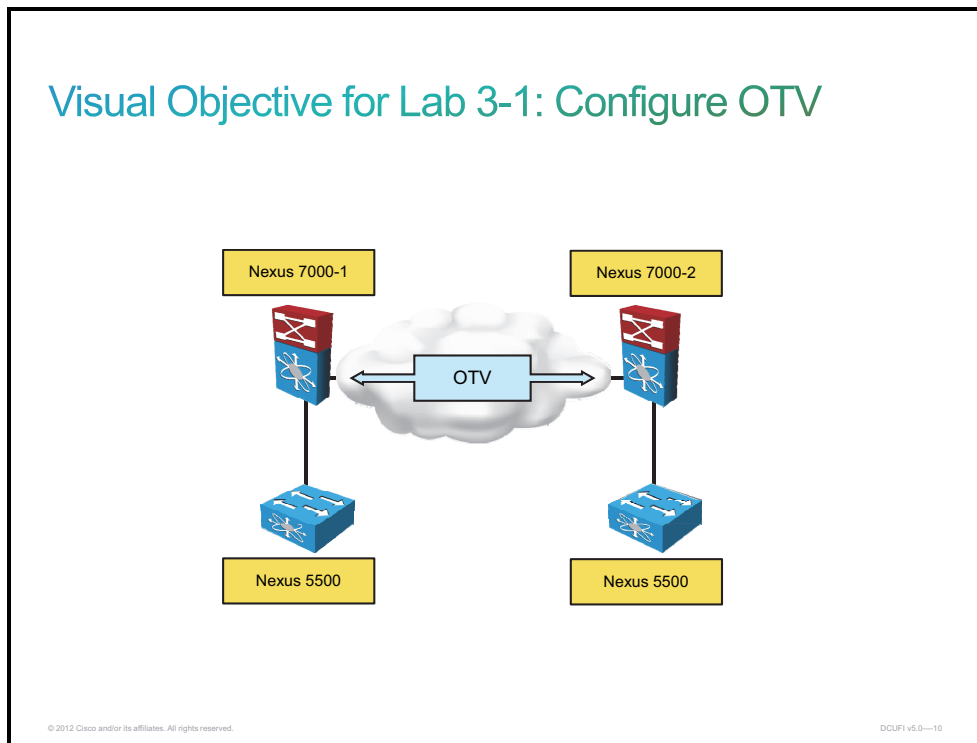
Activity Objective

In this activity, you will configure OTV between your Cisco Nexus 7000 Series switch VDC and your peer Cisco Nexus 7000 Series switch VDC. After completing this activity, you will be able to meet these objectives:

- Configure a Cisco Nexus 7000 Series switch to support OTV
- Verify the OTV operation

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required to complete this activity:

- Two Cisco Nexus 7000 Series switch VDCs
- Two Cisco Nexus 5500 Platform switches

Command List

The table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>feature interface-vlan</code>	Enables the interface-vlan feature, which allows SVIs to be created
<code>show license usage</code>	Displays the license usage in a VDC
<code>feature otv</code>	Enables the Overlay Transport Virtualization (OTV) feature
<code>otv site-vlan <vlan></code>	Defines the OTV site VLAN
<code>ip igmp version <version></code>	Configures the Internet Group Management Protocol (IGMP) version
<code>interface overlay <nr></code>	Creates an OTV overlay
<code>otv join-interface <intf></code>	Defines the OTV join interface for an overlay
<code>otv control-group <multicast-group></code>	Defines the OTV control multicast group for an overlay
<code>otv data-group <multicast-group-range></code>	Defines the range of multicast groups to be used for multicast forwarding on an overlay
<code>otv extend-vlan <vlan-range></code>	Defines the range of VLANs that are extended across an overlay
<code>show otv overlay <nr></code>	Displays basic parameters and status information for an OTV overlay
<code>show otv adjacency</code>	Displays the list of OTV adjacencies on a VDC
<code>show otv route</code>	Displays the OTV MAC routing table
<code>show otv arp-nd-cache</code>	Displays the content of the OTV Address Resolution Protocol (ARP) and neighbor discovery (ND) cache
<code>show spanning-tree vlan <vlan></code>	Displays the spanning-tree state for a VLAN

Task 1: Configuring Basic OTV

During this task, you will configure OTV on the Cisco Nexus 7000 Series switch VDC in your pod.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.
- Step 2** Remove the configuration from the previous lab, where *P* is your pod number and *Q* is your peer pod number.

```
N7KX-podP(config)# no feature rip
N7KX-podP(config)# no feature ospf
N7KX-podP(config)# no feature eigrp
N7KX-podP(config)# no interface port-channel P, port-channel Q, port-channel 7
N7KX-podP(config)# no vrf context STATIC-VRF
N7KX-podP(config)# no vrf context OSPF-VRF
N7KX-podP(config)# no vrf context EIGRP-VRF
N7KX-podP(config)# no interface loopback0, loopback10, loopback12, loopback13
N7KX-podP(config)# no feature interface-vlan
```

Note Currently, OTV and SVI cannot coexist within the same VDC. You must disable the interface VLAN feature in order for OTV to function properly.

- Step 3** Disable the interface on the F1 module on your Cisco Nexus 7000 Series switch VDC that leads to your peer pod Cisco Nexus 7000 Series switch VDC. Enable the interface on the M1 module on your Cisco Nexus 7000 Series switch VDC that leads to your peer pod Cisco Nexus 7000 Series switch VDC. Use the Lab Connections “Job Aids” to find the correct interface.

```
N7KX-podP(config)# interface ethernet ITA, ethernet ITB
N7KX-podP(config-if-range)# shutdown
N7KX-podP(config-if-range)# interface ethernet IGA
N7KX-podP(config-if)# switchport
N7KX-podP(config-if)# switchport mode trunk
N7KX-podP(config-if)# no shutdown
```

- Step 4** Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

- Step 5** Remove the configuration from the previous lab.

```
N5548-P(config)# no feature rip
N5548-P(config)# no feature ospf
N5548-P(config)# no feature eigrp
N5548-P(config)# no interface port-channel 77
N5548-P(config)# no vrf context STATIC-VRF
N5548-P(config)# no vrf context OSPF-VRF
N5548-P(config)# no vrf context EIGRP-VRF
N5548-P(config)# no interface vlan10, vlan11, vlan12, vlan13
N5548-P(config)# no interface loopback0, loopback12, loopback13
```

Note Do not remove PortChannel interface going toward FEX.

- Step 6** Configure an SVI on your Cisco Nexus 5500 Platform switch for VLAN10. Assign the IP address 172.16.10.5P/24 to it, where P is your pod number.

```
N5548-P(config)# feature interface-vlan
N5548-P(config)# interface vlan 10
N5548-P(config-if)# ip address 172.16.10.5P/24
N5548-P(config-if)# no shutdown
```

- Step 7** Ping the IP address of your peer pod, 172.16.10.5Q— where Q is your peer pod number, to confirm IP connectivity between the two pods.

```
N5548-P# ping 172.16.10.5Q
PING 172.16.10.5Q (172.16.10.5Q): 56 data bytes
Request 0 timed out
64 bytes from 172.16.10.5Q: icmp_seq=1 ttl=254 time=1.186 ms
64 bytes from 172.16.10.5Q: icmp_seq=2 ttl=254 time=0.84 ms
64 bytes from 172.16.10.5Q: icmp_seq=3 ttl=254 time=0.752 ms
64 bytes from 172.16.10.5Q: icmp_seq=4 ttl=254 time=0.714 ms

--- 172.16.10.5Q ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.714/0.872/1.186 ms
```

Note Do not proceed to the next step until you succeed in pinging the peer pod Cisco Nexus 5500 Platform switch VLAN10 IP address. Troubleshoot together with your peer pod as necessary.

- Step 8** Change the interface on your Cisco Nexus 7000 Series switch VDC that connects to your peer Cisco Nexus 7000 Series switch VDC to a routed port.

```
N7KX-podP(config)# interface ethernet IGA
N7KX-podP(config-if)# no switchport
```

- Step 9** Configure IP address 10.7.7.P/24—where P is your pod number—on the routed interface that connects to your peer Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP(config-if)# ip address 10.7.7.P/24
```

- Step 10** Ping the IP address of your peer pod, 10.7.7.Q—where Q is your peer pod number—to confirm IP connectivity between the VDCs.

```
N7KX-podP# ping 10.7.7.Q
PING 10.7.7.Q (10.7.7.Q): 56 data bytes
64 bytes from 10.7.7.Q: icmp_seq=0 ttl=254 time=1.18 ms
64 bytes from 10.7.7.Q: icmp_seq=1 ttl=254 time=0.697 ms
64 bytes from 10.7.7.Q: icmp_seq=2 ttl=254 time=0.846 ms
64 bytes from 10.7.7.Q: icmp_seq=3 ttl=254 time=0.849 ms
64 bytes from 10.7.7.Q: icmp_seq=4 ttl=254 time=0.725 ms

--- 10.7.7.Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.697/0.859/1.18 ms
```

Note This interface will be used as the OTV join interface. Do not proceed to the next step until you have verified IP connectivity between the VDCs for this link.

- Step 11** Switch to your Cisco Nexus 5500 Platform switch.

Step 12 Verify that you can no longer ping from your Cisco Nexus 5500 Platform switch to your peer pod Cisco Nexus 5500 Platform switch on VLAN 10.

```
N5548-P# ping 172.16.10.5Q
PING 172.16.10.5Q (172.16.10.5Q): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
```

```
--- 172.16.10.5Q ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

Step 13 Determine why you cannot ping between the Cisco Nexus 5500 Platform switches any longer.

Note Verify that you have shut down the trunk from your Cisco Nexus 7000 Series switch VDC to your peer pod Cisco Nexus 5500 Platform switch if you can still ping to the peer Cisco Nexus 5500 Platform switch. You should not be able to ping between the Cisco Nexus 5500 Platform switches in your pod and peer pod until OTV has been configured to extend VLAN 10 between the pods.

Step 14 Examine the license usage on your Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP# show license usage
Feature                               Ins Lic   Status Expiry Date Comments
                                Count
-----
--
ENHANCED_LAYER2_PKG                  No    -    Unused
SCALABLE_SERVICES_PKG                No    -    Unused
TRANSPORT_SERVICES_PKG               Yes    -    Unused Never
LAN_ADVANCED_SERVICES_PKG            Yes    -    Unused Never
LAN_ENTERPRISE_SERVICES_PKG           Yes    -    Unused Never
-----
--
```

Step 15 Enable the OTV feature.

```
N7KX-podP(config)# feature otv
```

Step 16 Examine the license usage again.

```
N7KX-podP# show license usage
Feature                               Ins Lic   Status Expiry Date Comments
                                Count
-----
--
ENHANCED_LAYER2_PKG                  No    -    Unused
SCALABLE_SERVICES_PKG                No    -    Unused
TRANSPORT_SERVICES_PKG               Yes    -    In use Never
LAN_ADVANCED_SERVICES_PKG            Yes    -    Unused Never
LAN_ENTERPRISE_SERVICES_PKG           Yes    -    Unused Never
-----
--
```

Determine which license the OTV feature requires.

Step 17 Configure the OTV site identifier, where *P* is your pod number.

```
N7KX-podP(config)# otv site-identifier P.P.P
% Site Identifier mismatch will prevent overlays from forwarding traffic.
```

Step 18 Configure VLAN 13 as the OTV site VLAN.

```
N7KX-podP(config)# vlan 13
N7KX-podP(config-vlan)# otv site-vlan 13
N7KX-podP(config-site-vlan)# exit
```

Step 19 Configure the OTV join interface to use IGMP Version 3.

```
N7KX-podP(config)# interface ethernet IGA
N7KX-podP(config-if)# ip igmp version 3
```

Step 20 Increase the maximum transmission unit (MTU) on this interface to the maximum of 9216 bytes.

```
N7KX-podP(config-if)# mtu 9216
```

Step 21 Create an OTV overlay interface 1. Configure it to use the interface that connects your Cisco Nexus 7000 Series switch VDC to your peer pod VDC as the join interface.

```
N7KX-podP(config)# interface overlay 1
N7KX-podP(config-if-overlay)# otv join-interface ethernet IGA
OTV needs join interfaces to be configured for IGMP version 3
```

Note A warning about using IGMPv3 on the join interface is displayed, regardless of the actual configuration of the join interface.

Step 22 Configure multicast group 239.7.7.7 as the OTV control multicast group.

```
N7KX-podP(config-if-overlay)# otv control-group 239.7.7.7
```

Step 23 Configure the multicast range 232.7.7.0/24 as the Source Specific Multicast (SSM) group range for OTV multicast data.

```
N7KX-podP(config-if-overlay)# otv data-group 232.7.7.0/24
```

Step 24 Extend VLANs 10–12 across the overlay.

```
N7KX-podP(config-if-overlay)# otv extend-vlan 10-12
```

Step 25 Examine the overlay interface.

```
N7KX-podP# show otv overlay 1
```

OTV Overlay Information

Overlay interface Overlay1

```
VPN name           : Overlay1
VPN state          : DOWN (admin down)
Extended vlans     : 10-12 (Total:3)
Control group      : 239.7.7.7
Data group range(s) : 232.7.7.0/24
Join interface(s)  : EthIGA(10.7.7.P)
Site vlan          : 13 (up)
AED-Capable        : No (Overlay is Down)
Capability          : Multicast-Reachable
```

Step 26 Enable the overlay interface.

```
N7KX-podP(config)# interface overlay 1
N7KX-podP(config-if-overlay)# no shutdown
```

Note You should wait at least 30 seconds for OTV to form adjacency.

Step 27 Examine the overlay interface again.

N7KX-podP# **show otv overlay 1**

OTV Overlay Information

Overlay interface Overlay1

```
VPN name           : Overlay1
VPN state          : UP
Extended vlans     : 10-12 (Total:3)
Control group      : 239.7.7.7
Data group range(s) : 232.7.7.0/24
Join interface(s)  : Eth1GA (10.7.7.P)
Site vlan          : 13 (up)
AED-Capable        : Yes
Capability          : Multicast-Reachable
```

Step 28 Verify that your VDC has established an OTV adjacency with the VDC in your peer pod.

N7KX-podP# **show otv adjacency**

Overlay Adjacency database

```
Overlay-Interface Overlay1 :
Hostname                     System-ID      Dest Addr      Up Time
State
N7KY-podQ                   0026.9804.a944 10.7.7.Q       00:01:30  UP
```

Step 29 Examine the OTV MAC routing table to see if any MAC addresses were learned.

N7KX-podP# **show otv route**

Determine if you see any MAC addresses in the OTV MAC routing table.

Step 30 Switch to your Cisco Nexus 5500 Platform switch.

Step 31 Ping the IP address of your peer pod, 172.16.10.5Q—where Q is your peer pod number—from your Cisco Nexus 5500 Platform switch.

```
N5548-P# ping 172.16.10.5Q
PING 172.16.10.5Q (172.16.10.5Q): 56 data bytes
Request 0 timed out
Request 1 timed out
64 bytes from 172.16.10.5Q: icmp_seq=2 ttl=254 time=1.189 ms
64 bytes from 172.16.10.5Q: icmp_seq=3 ttl=254 time=0.859 ms
64 bytes from 172.16.10.5Q: icmp_seq=4 ttl=254 time=0.8 ms

--- 172.16.10.5Q ping statistics ---
5 packets transmitted, 3 packets received, 40.00% packet loss
round-trip min/avg/max = 0.8/0.949/1.189 ms
```

Step 32 Switch back to your Cisco Nexus 7000 Series switch VDC.

Step 33 Examine the OTV MAC routing table again.

N7KX-podP# **show otv route**

OTV Unicast MAC Routing Table For Overlay1

VLAN	MAC-Address	Metric	Uptime	Owner	Next-hop(s)
10	0005.9b1f.7c7c	42	00:00:45	overlay	N7KY-podQ
10	0005.9b1f.89fc	1	00:00:46	site	EthernetAA

Step 34 Examine the OTV ARP cache.

```
N7KX-podP# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN  MAC Address      Layer-3 Address      Age      Expires In
10     0005.9b1f.7c7c       172.16.10.5Q         00:04:37 00:03:22
```

Step 35 Examine the spanning-tree topology for VLAN 10.

```
N7KX-podP# show spanning-tree vlan 10

MST0002
  Spanning tree enabled protocol mstp
  Root ID    Priority    8194
             Address     a8b1.d455.6fc4
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    8194 (priority 8192 sys-id-ext 2)
             Address     a8b1.d455.6fc4
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
EthAA Desg FWD 2000      128.137 Network P2p
```

Determine which bridge is the root of the spanning tree for VLAN 10.

Note	Ask your lab partners in the peer pod which bridge is listed as the root of the spanning tree on their VDCs. Is it the same? If not, can you explain why?
-------------	---

Save the configurations on your Cisco Nexus 7000 Series switch VDC and Cisco Nexus 5500 Platform switch.

Activity Verification

- You have completed this task when you attain these results:
- You have removed the unnecessary configurations from the previous lab.
- You have successfully established an OTV adjacency between your Cisco Nexus 7000 Series switch VDC and your peer pod VDC.
- You have successfully extended VLAN 10 across the OTV overlay.
- You have examined OTV and spanning-tree operation.

Lab 3-2: Configure QoS

Complete this lab activity to practice what you learned in the related module.

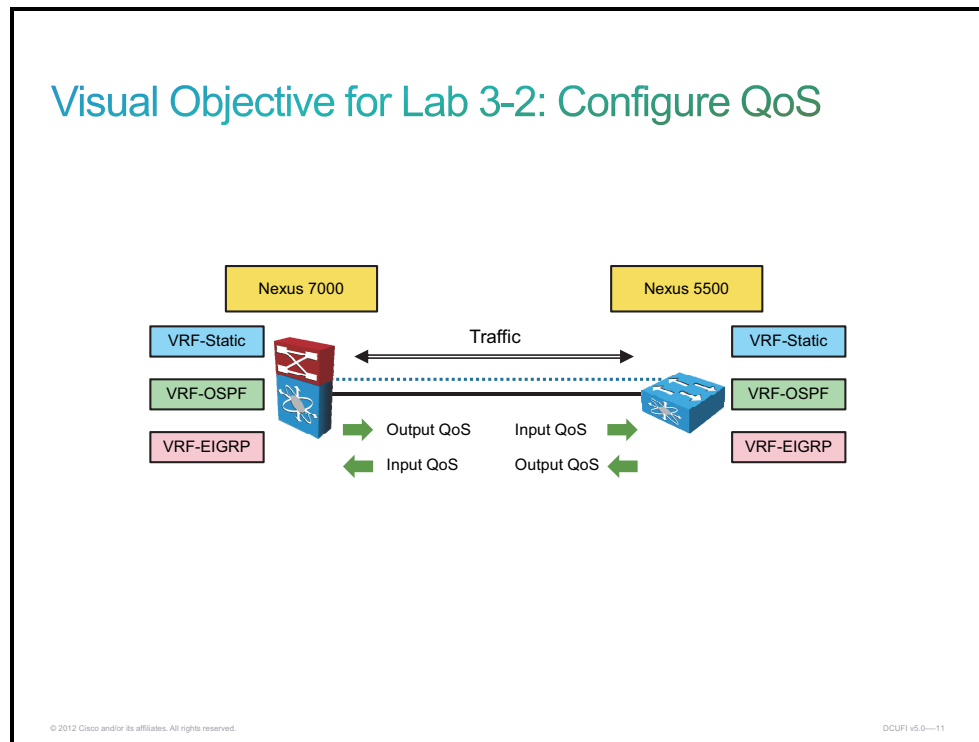
Activity Objective

In this activity, you will configure QoS features on a link between the Cisco Nexus 7000 Series switch VDC in your pod and Cisco Nexus 7000 Series switch VDC in your peer pod. After completing this activity, you will be able to meet these objectives:

- Generate some traffic against which the QoS configuration can be tested
- Configure type QoS class maps and verify the configuration
- Configure type QoS policy maps and verify the configuration
- Configure type QoS service policies and verify that the configuration has been applied to the correct traffic stream and is performing as expected

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required in order to complete this activity:

- Two Cisco Nexus 7000 Series switch VDCs

Command List

This table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>ip access-list <name></code>	Defines an IP access list
<code>statistics per-entry</code>	Enables the gathering of statistics for an access list
<code>class-map type qos <name></code>	Creates a class map of type QoS
<code>match access-group name <name></code>	Matches packets that are permitted by an access list
<code>show class-map type qos</code>	Displays the class maps of type QoS
<code>match cos <cos></code>	Matches packets with a specific class of service (CoS) value
<code>show class-map <name></code>	Displays all class maps on the switch
<code>show running-config ipqos</code>	Shows the elements of the running configuration that are related to QoS
<code>policy-map type qos <name></code>	Creates a policy map of type QoS
<code>class type qos <name></code>	Enters class configuration mode for a class within the policy map
<code>set qos-group <nr></code>	Sets the internal QoS group marker
<code>show policy-map type qos</code>	Displays all policy maps of type QoS on the switch
<code>class-map type network-qos <name></code>	Creates a class map of type network-qos
<code>match qos-group <nr></code>	Matches packets with a specific QoS group value
<code>policy-map type network-qos <name></code>	Creates a policy map of type network-qos
<code>class type network-qos <name></code>	Enters class configuration mode for a class within the policy map
<code>set cos <cos></code>	Sets the CoS value
<code>show policy-map type network-qos</code>	Displays all policy maps of type network-qos on the switch
<code>set dscp <dscp></code>	Sets the differentiated services code point (DSCP) value
<code>system qos</code>	Enters system QoS configuration
<code>service-policy type qos input <name></code>	Associates an ingress policy map of type QoS with an interface
<code>service-policy type network-qos <name></code>	Associates a policy map of type network QoS with the system QoS target
<code>show policy-map system</code>	Displays the policy maps that are associated with the system QoS target
<code>show policy-map interface <intf> type qos</code>	Displays the policy map of type QoS that is associated with an interface, including packet statistics for that interface

Task 1: Verify Baseline Connectivity

In this task, you will verify baseline connectivity between the Cisco Nexus 5500 Platform switch and the Cisco 7000 Series switch VDC in your pod.

Activity Procedure

Complete these steps:

Step 1 Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 2 Remove OTV configuration.

```
N7KX-podP(config)# no feature otv
```

Step 3 Configure a VRF named **QOS-VRF**. Then create a loopback 10 interface. Assign it to the just-created VRF and configure IP address 192.168.10.**P**/32, where **P** is your assigned pod number.

```
N7KX-podP(config)# vrf context QOS-VRF
N7KX-podP(config-vrf)# interface loopback 10
N7KX-podP(config-if)# vrf member QOS-VRF
% Deleted all L3 config on interface loopback10
N7KX-podP(config-if)# ip address 192.168.10.P1/32
```

Step 4 Create loopback 1 interface. Assign it to VRF **QOS-VRF**, and configure IP address 192.168.1.**P**/32, where **P** is your assigned pod number.

```
N7KX-podP(config-vrf)# interface loopback 1
N7KX-podP(config-if)# vrf member QOS-VRF
% Deleted all L3 config on interface loopback1
N7KX-podP(config-if)# ip address 192.168.1.P1/32
```

Step 5 Configure interface Ethernet **IGA** toward the peer pod and assign IP address 172.16.10.**P**/24, where **P** is your pod number. Assign it to the VRF context you just created.

```
N7KX-podP(config)# interface ethernet IGA
N7KX-podP(config-if)# vrf member QOS-VRF
% Deleted all L3 config on interface EthernetIGA
N7KX-podP(config-if)# ip address 172.16.10.P1/24
N7KX-podP(config-if)# no shutdown
```

Step 6 Create a default route for VRF **QOS-VRF** over IP address 172.16.10.**Q**1, where **Q** is your peer pod number.

```
N7KX-podP(config)# vrf context QOS-VRF
N7KX-podP(config-vrf)# ip route 0.0.0.0/0 172.16.10.Q1
```

Step 7 Verify connectivity between the loopback 10 IP addresses on your pod and a peer Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP# ping 192.168.10.Q1
PING 192.168.10.Q1 (192.168.10.Q1): 56 data bytes
ping: sendto 192.168.10.Q1 64 chars, No route to host
Request 0 timed out
ping: sendto 192.168.10.Q1 64 chars, No route to host
Request 1 timed out
ping: sendto 192.168.10.Q1 64 chars, No route to host
Request 2 timed out
ping: sendto 192.168.10.Q1 64 chars, No route to host
Request 3 timed out
ping: sendto 192.168.10.Q1 64 chars, No route to host
Request 4 timed out
```

```
--- 192.168.10.Q1 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
```

Determine why this ping was not successful.

Step 8 Change your routing context so that you have your execute commands placed in the correct VRF context.

```
N7KX-podP# routing-context vrf QOS-VRF
N7KX-podP%QOS-VRF# ping 192.168.10.Q1
PING 192.168.10.Q1 (192.168.10.Q1): 56 data bytes
64 bytes from 192.168.10.Q1: icmp_seq=0 ttl=254 time=1.038 ms
64 bytes from 192.168.10.Q1: icmp_seq=1 ttl=254 time=0.729 ms
64 bytes from 192.168.10.Q1: icmp_seq=2 ttl=254 time=0.718 ms
64 bytes from 192.168.10.Q1: icmp_seq=3 ttl=254 time=0.749 ms
64 bytes from 192.168.10.Q1: icmp_seq=4 ttl=254 time=9.17 ms

--- 192.168.10.Q1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.718/2.48/9.17 ms
```

Step 9 Verify connectivity between the loopback 1 IP addresses on your VDC and a peer Cisco Nexus 7000 Series switch VDC. Use appropriate ping options to source the traffic from the loopback 1 IP address.

Note Later, you will apply differentiated treatment to the two traffic flows between the different loopback interfaces. Do not proceed with the lab until you have established connectivity.

Activity Verification

You have completed this task when you attain these results:

- You have verified IP connectivity between the loopback 1 and loopback 10 IP addresses on your VDC and a peer Cisco Nexus 7000 Series switch VDC.

Task 2: Class Maps

In this task, you will configure type QoS class maps and verify the configuration.

Activity Procedure

Complete these steps:

- Step 1** On the Cisco Nexus 7000 Series switch VDC, configure two access lists:
- An ACL named ACL01, which permits ICMP traffic between **Loopback 1** interfaces
 - An ACL named ACL10, which permits ICMP traffic between **Loopback 10** interfaces

```
N7KX-podP%QOS-VRF(config)# ip access-list ACL01
N7KX-podP%QOS-VRF(config-acl)# permit icmp 192.168.1.0/24 192.168.1.0/24
N7KX-podP%QOS-VRF(config)# ip access-list ACL10
N7KX-podP%QOS-VRF(config-acl)# permit icmp 192.168.10.0/24 192.168.10.0/24
```

Step 2 Configure two class maps:

- A class map named CMAP01 that matches ACL01
- A class map named CMAP10 that matches ACL10

```
N7KX-podP%QOS-VRF(config)# class-map type qos CMAP01
N7KX-podP%QOS-VRF(config-cmap-qos)# match access-group name ACL01
N7KX-podP%QOS-VRF(config)# class-map type qos CMAP10
N7KX-podP%QOS-VRF(config-cmap-qos)# match access-group name ACL10
```

Step 3 Verify the class maps.

```
N7KX-podP%QOS-VRF(config-cmap-qos)# show class-map CMAP01
```

```
Type qos class-maps
=====
```

```
class-map type qos match-all CMAP01
  match access-group name ACL01
```

```
N7KX-podP%QOS-VRF(config-cmap-qos)# show class-map CMAP10
```

```
Type qos class-maps
=====
```

```
class-map type qos match-all CMAP10
  match access-group name ACL10
```

Activity Verification

You have completed this task when you attain these results:

- You have configured the access lists.
- You have configured and verified the class maps.

Task 3: Policy Maps

In this task, you will configure type QoS policy maps and verify the configuration.

Activity Procedure

Complete these steps:

- Step 1** On your Cisco Nexus 7000 Series switch VDC, configure a policy map that gives precedence of one traffic stream over the other.

```
N7KX-podP%QOS-VRF(config)# policy-map type qos PMAP
N7KX-podP%QOS-VRF(config-pmap-qos)# class type qos CMAP01
N7KX-podP%QOS-VRF(config-pmap-c-qos)# set precedence 5
N7KX-podP%QOS-VRF(config-pmap-c-qos)# class type qos CMAP10
N7KX-podP%QOS-VRF(config-pmap-c-qos)# set precedence 0
N7KX-podP%QOS-VRF(config-pmap-c-qos)# exit
N7KX-podP%QOS-VRF(config-pmap-qos)# exit
```

Step 2 Verify the policy map.

```
N7KX-podP%QOS-VRF(config)# show policy-map PMAP
```

```
Type qos policy-maps
=====

policy-map type qos PMAP
  class type qos CMAP01
    set prec 5
  class type qos CMAP10
    set prec 0
```

Activity Verification

You have completed this task when you attain these results:

- You have configured and verified the policy map.

Task 4: Service Policies

In this task, you will configure type QoS service policies and verify that the configuration has been applied to the correct traffic stream and is performing as expected.

Activity Procedure

Complete these steps:

- Step 1** On your Cisco Nexus 7000 Series switch VDC, apply the policy map you have created in input and output directions. The policy should be applied on an interface toward the peer Cisco Nexus 7700 Series switch VDC: Ethernet **IGA**.

```
N7KX-podP%QOS-VRF(config)# interface ethernet IGA
N7KX-podP%QOS-VRF(config-if)# service-policy type qos input PMAP
N7KX-podP%QOS-VRF(config-if)# service-policy type qos output PMAP
```

- Step 2** Verify the policy map.

```
N7KX-podP%QOS-VRF(config-if)# show policy-map interface ethernet IGA
```

```
Global statistics status : enabled
```

```
EthernetIGA
```

```
Service-policy (qos) input: PMAP
SNMP Policy Index: 285212759
```

```
Class-map (qos): CMAP01 (match-all)
```

```
Aggregate forwarded :
 0 packets 0 bytes
Match: access-group ACL01
set prec 5
```

```
Class-map (qos): CMAP10 (match-all)
```

```
Aggregate forwarded :
 0 packets 0 bytes
Match: access-group ACL10
set prec 0
```

```
<output omitted>
```

- Step 3** The even-numbered pods will start a continuous ping toward a peer Loopback 10 IP address, with a large packet size and large packet count. Use Loopback 10 IP address as a source address.

```
N7KX-podP%QOS-VRF# ping 192.168.10.21 count 10000 packet-size 10000 source 192.168.10.11
```

- Step 4** The odd-numbered pods will start a continuous ping toward a peer Loopback 1 IP address, with a large packet size and large packet count. Use Loopback 1 IP address as a source address.

```
N7KX-podP%QOS-VRF# ping 192.168.1.21 count 10000 packet-size 10000 source 192.168.1.11
```

- Step 5** By analyzing round-trip time (RTT), observe how two data flows require different amounts of time to send ping packets.

Note	Consult your peer workgroup for round-trip times they have recorded.
-------------	--

Activity Verification

You have completed this task when you attain these results:

- You have configured and verified the service policy.
- You have examined the policy map counters.
- You have observed differentiated traffic treatment.

Lab 3-3: Configure Security Features

Complete this lab activity to practice what you learned in the related module.

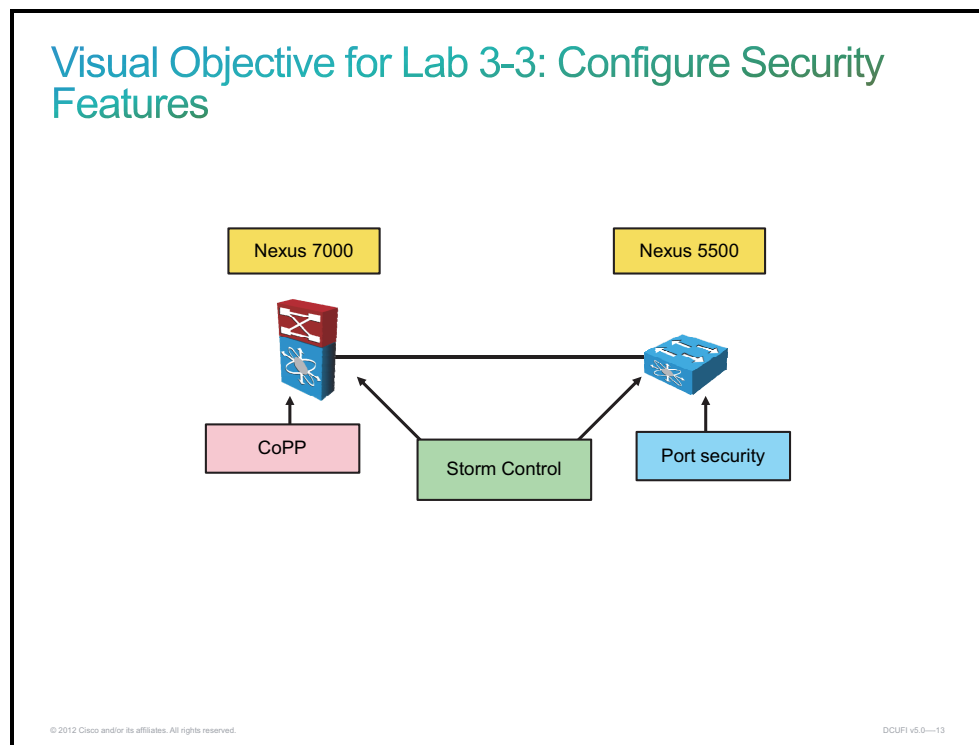
Activity Objective

In this activity, you will configure the Cisco NX-OS security features on your Cisco Nexus 5500 Platform switch and Cisco Nexus 7000 Series switch VDC. After completing this activity, you will be able to meet these objectives:

- Configure port security
- Configure traffic storm control
- Configure ACL using atomic programming

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required in order to complete this activity:

- Cisco Nexus 7000 Series switch VDC
- Cisco Nexus 5500 Platform switch

Command List

The table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>switchport access vlan <vlan></code>	Configures the VLAN for an access port
<code>spanning-tree port type edge</code>	Configures an interface as a spanning-tree edge port
<code>feature port-security</code>	Enables the port security feature
<code>switchport port-security</code>	Enables port security on an interface
<code>show running-config port-security all</code>	Shows the elements of the running configuration that are related to port security, including default values
<code>show port-security address</code>	Shows the static and dynamic port security addresses in the system
<code>switchport port-security mac-address <address></code>	Configures a static port security MAC address for an interface
<code>show logging last <nr></code>	Shows the last number of lines in the system log
<code>storm-control broadcast level <percent></code>	Enables traffic storm control for broadcast traffic at the configured level
<code>storm-control multicast level <percent></code>	Enables traffic storm control for multicast traffic at the configured level
<code>storm-control unicast level <percent></code>	Enables traffic storm control for unicast traffic at the configured level
<code>show interface <intf> counters storm-control</code>	Displays the operational traffic storm-control parameters and statistics

Task 1: Port Security

In this task, you will configure port security on your Cisco Nexus 5500 Platform switch.

Activity Procedure

Complete these steps:

Step 1 Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 2 Remove Cisco FabricPath configuration.

```
N5548-P(config)# vlan 10-13
N5548-P(config-vlan)# mode ce
N5548-P(config-vlan)# exit
N5548-P(config)# no feature-set fabricpath
N5548-P(config)# no install feature-set fabricpath
```

Step 3 Set the interface toward Cisco Nexus 7000 Series switch VDC (Ethernet AA) as a Layer 2 access port in VLAN 11.

```
N5548-P(config)# interface AA
N5548-P(config-if)# switchport
N5548-P(config-if)# switchport mode access
N5548-P(config-if)# switchport access vlan 11
N5548-P(config-if)# no spanning-tree port type network
N5548-P(config-if)# no shutdown
```

Step 4 Create an SVI interface for VLAN 11, and assign to it IP address 192.168.11.**P2**/24, where **P** is your pod number.

```
N5548-P(config)# feature interface-vlan
N5548-P(config)# interface vlan 11
N5548-P(config-if)# ip address 192.168.11.P2/24
N5548-P(config-if)# no shutdown
```

Step 5 Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 6 Set the interface toward the Cisco Nexus 5500 Platform switch (Ethernet AA) as a Layer 2 access port in VLAN 11.

```
N7KX-podP(config)# interface AA
N7KX-podP(config-if)# switchport
N7KX-podP(config-if)# switchport mode access
N7KX-podP(config-if)# switchport access vlan 11
N7KX-podP(config-if)# no spanning-tree port type network
N7KX-podP(config-if)# no shutdown
```

Step 7 Create an SVI interface for VLAN 11, and assign to it IP address 192.168.11.**P1**/24, where **P** is your pod number.

```
N7KX-podP(config)# feature interface-vlan
N7KX-podP(config)# interface vlan 11
N7KX-podP(config-if)# ip address 192.168.11.P1/24
N7KX-podP(config-if)# no shutdown
```

Step 8 Check the connectivity between VLAN 11 interfaces.

```
N7KX-podP(config-if)# ping 192.168.11.P2
PING 192.168.11.P2 (192.168.11.P2): 56 data bytes
Request 0 timed out
64 bytes from 192.168.11.P2: icmp_seq=1 ttl=254 time=1.158 ms
64 bytes from 192.168.11.P2: icmp_seq=2 ttl=254 time=0.738 ms
64 bytes from 192.168.11.P2: icmp_seq=3 ttl=254 time=0.71 ms
64 bytes from 192.168.11.P2: icmp_seq=4 ttl=254 time=13.558 ms
```

```
--- 192.168.11.P2 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.71/4.041/13.558 ms
```

Step 9 Record the MAC address of interface VLAN 11.

```
N7KX-podP(config)# show interface vlan 11
Vlan11 is up, line protocol is up
Hardware is EtherSVI, address is HHHH.HHHH.HHHH
Internet Address is 192.168.11.P1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
<output omitted>
```

Determine what the MAC address of VLAN 11 is.

Step 10 On the Cisco Nexus 5500 Platform switch, enable the port-security feature.

```
N5548-P(config)# feature port-security
```

Step 11 Configure port security on interface Ethernet AA, and permit incoming traffic only from the MAC address of VLAN 11 on the Cisco Nexus 7000 Series switch VDC (recorded in the previous step).

```
N5548-P(config)# interface AA
N5548-P(config-if)# switchport port-security mac-address HHHH.HHHH.HHHH
N5548-P(config-if)# switchport port-security
N5548-P(config-if)# exit
```

Step 12 On the Cisco Nexus 7000 Series switch VDC, ping address 192.168.11.P2 with a large packet size and large packet count.

```
N7KX-podP(config)# ping 192.168.11.P2 packet-size 65000 count 2000
PING 192.168.11.P2 (192.168.11.P2): 65000 data bytes
65008 bytes from 192.168.11.P2: icmp_seq=0 ttl=254 time=458.373 ms
65008 bytes from 192.168.11.P2: icmp_seq=1 ttl=254 time=453.249 ms
65008 bytes from 192.168.11.P2: icmp_seq=2 ttl=254 time=453.782 ms
65008 bytes from 192.168.11.P2: icmp_seq=3 ttl=254 time=453.122 ms
65008 bytes from 192.168.11.P2: icmp_seq=4 ttl=254 time=452.112 ms
65008 bytes from 192.168.11.P2: icmp_seq=5 ttl=254 time=451.467 ms
65008 bytes from 192.168.11.P2: icmp_seq=6 ttl=254 time=452.982 m
65008 bytes from 192.168.11.P2: icmp_seq=7 ttl=254 time=453.129 ms
65008 bytes from 192.168.11.P2: icmp_seq=8 ttl=254 time=453.722 m
<output omitted>
```

Step 13 While the pinging continues, on your Cisco Nexus 5500 Platform switch, reconfigure port security so that the permitted MAC address is 0000.1111.1111.

```
N5548-P(config)# interface AA
N5548-P(config-if)# no switchport port-security
N5548-P(config-if)# no switchport port-security mac-address HHHH.HHHH.HHHH
N5548-P(config-if)# switchport port-security mac-address 0000.1111.1111
N5548-P(config-if)# switchport port-security
```

What happened when port-security was enabled with different MAC address and why?

Step 14 Examine the port security status of interface Ethernet AA.

```
N5548-P(config-if)# show port-security interface ethernet AA
Configured Port Security      : Enabled
Operational Port Security     : Enabled
Port Status                   : Secure Down
Violation Mode                 : Shutdown
Aging Time                    : 0 mins
Aging Type                    : Absolute
Maximum MAC Addresses         : 1
Total MAC Addresses           : 1
Configured MAC Addresses      : 1
Sticky MAC Addresses          : 0
Security violation count      : 1
```

Step 15 Examine the interface status on the Cisco Nexus 5500 Platform switch.

```
N5548-P(config-if)# show interface brief
-----
Ethernet      VLAN    Type Mode   Status Reason                               Speed  Port
Interface                                           Ch #
-----
--
EthAA        11      eth  access down   Sec-violation errDisable      10G(D) --
Eth1/2        1       eth  access down   Administratively down          10G(D) --
Eth1/3        1       eth  access down   Link not connected             10G(D) --
Eth1/4        1       eth  access down   SFP not inserted               10G(D) --
Eth1/5        1       eth  access down   SFP not inserted               10G(D) --
Eth1/6        1       eth  access down   SFP not inserted               10G(D) --
Eth1/7        1       eth  access down   SFP not inserted               10G(D) --
<output omitted>
```

Note On your output, the other port may be disabled due to security violation.

Activity Verification

You have completed this task when you attain these results:

- You have removed the unnecessary configurations from the previous lab.
- You have successfully configured SVI interfaces for VLAN 11 on both devices.
- You have successfully configured access ports on both devices.
- You have examined port security configuration and operation.

Task 2: Traffic Storm Control

In this task, you will configure traffic storm control on a Cisco Nexus 5500 Platform switch.

Activity Procedure

Complete these steps:

- Step 1** Enable a directed broadcast on the VLAN11 interface on the Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP(config)# interface vlan 11
N7KX-podP(config)# ip directed-broadcast
```

- Step 2** Enable a directed broadcast on the VLAN11 interface on the Cisco Nexus 5500 Platform switch.

```
N5548-P(config)# interface vlan 11
N5548-P(config-if)# ip directed broadcast
```

- Step 3** On the Cisco Nexus 5500 Platform switch, re-enable port security for the recorded MAC address of the VLAN11 interface on the Cisco Nexus 7000 Series switch VDC.

```
N5548-P(config)# interface AA
N5548-P(config-if)# shutdown
N5548-P(config-if)# no switchport port-security
N5548-P(config-if)# no switchport port-security mac-address 0000.1111.1111
N5548-P(config-if)# switchport port-security mac-address HHHH.HHHH.HHHH
N5548-P(config-if)# switchport port-security
N5548-P(config-if)# no shutdown
```

- Step 4** Configure Traffic Storm Control for broadcast traffic to a level of 0.01 percent (on a 10-Gb link, 0.01 percent would be 1 Mb)

```
N5548-P(config)# interface AA
N5548-P(config-if)# storm-control broadcast level 0.01
```

- Step 5** On the Cisco Nexus 7000 Series switch VDC, start a ping toward network broadcast address with large packet size and large packet count”..

```
N7KX-podP# ping 192.168.11.255 count 10000 packet-size 1400
```

Note After several seconds, you will notice periodical pauses of ping responses.

- Step 6** Verify that the broadcast Traffic Storm Control has a limited amount of broadcast traffic.

```
N5548-P(config)# show interface AA counters storm-control
```

Port	UcastSupp %	McastSupp %	BcastSupp %	TotalSuppDiscards (bytes)
EthAA	100.00	100.00	0.01	165070

Activity Verification

You have completed this task when you attain these results:

- You have successfully configured broadcast Traffic Storm Control on the Cisco Nexus 5500 Platform switch.
- You have examined traffic storm control configuration and operation.

Task 3: Configuring Access Control List Using Atomic Programming

In this task, you will configure ACL using atomic programming.

Activity Procedure

Complete these steps:

- Step 1** On the Cisco Nexus 7000 Series switch VDC, initiate a configuration session, and configure ACL that will block all ICMP traffic.

```
N7KX-podP# configure session ATOMIC
Config Session started, Session ID is 1
Enter configuration commands, one per line. End with CNTL/Z.
N7KX-podP(config-s)# ip access-list ATOMIC_ACL
N7KX-podP(config-s-acl)# deny icmp any any
```

- Step 2** Apply ACL to interface VLAN11.

```
N7KX-podP(config-s-acl)# interface vlan 11
N7KX-podP(config-s-if)# ip access-group ATOMIC_ACL in
```

- Step 3** Verify the configuration session to assure that ACL changes will fit into ternary content addressable memory (TCAM) memory.

```
N7KX-podP(config-s-if)# verify  
Verification Successful
```

- Step 4** On the Cisco Nexus 5500 Platform switch, generate some ICMP traffic.

```
N5548-P# ping 192.168.11.P1  
PING 192.168.11.P1 (192.168.11.P1): 56 data bytes  
64 bytes from 192.168.11.P1: icmp_seq=0 ttl=254 time=1.014 ms  
64 bytes from 192.168.11.P1: icmp_seq=1 ttl=254 time=0.912 ms  
64 bytes from 192.168.11.P1: icmp_seq=2 ttl=254 time=0.904 ms  
64 bytes from 192.168.11.P1: icmp_seq=3 ttl=254 time=7.227 ms  
64 bytes from 192.168.11.P1: icmp_seq=4 ttl=254 time=9.586 ms  
  
--- 192.168.11.P1 ping statistics ---  
5 packets transmitted, 5 packets received, 0.00% packet loss  
round-trip min/avg/max = 0.904/3.928/9.586 ms.
```

Determine why the ping is still working.

Note	Configuration session verification only verifies ACL against TCAM. It does not apply ACL to the traffic path.
-------------	---

- Step 5** Commit ACL to TCAM memory.

```
N7KX-podP(config-s)# commit  
Commit Successful
```

- Step 6** Check to see if ICMP traffic is now flowing.

```
N5548-P# ping 192.168.11.P1  
PING 192.168.11.P1 (192.168.11.P1): 56 data bytes  
Request 0 timed out  
Request 1 timed out  
Request 2 timed out  
Request 3 timed out  
Request 4 timed out  
  
--- 192.168.11.P1 ping statistics ---  
5 packets transmitted, 0 packets received, 100.00% packet loss
```

Activity Verification

You have completed this task when you attain these results:

- You have successfully created ACL using a configuration session.

Lab 4-1: Configure FCoE

Complete this lab activity to practice what you learned in the related module.

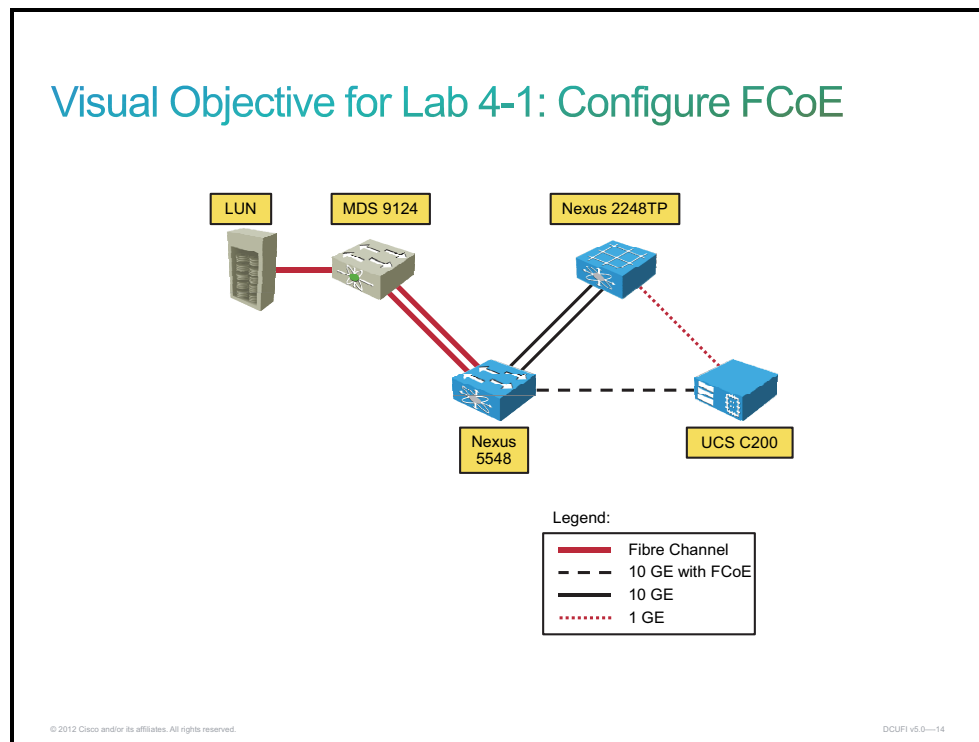
Activity Objective

In this activity, you will configure the Cisco Nexus 5500 Platform switch to support FCoE. After completing this activity, you will be able to meet these objectives:

- Configure FCoE on the Cisco Nexus 5500 Platform switch
- Configure a basic Fibre Channel and FCoE on a Cisco MDS 9124 Switch

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required in order to complete this activity:

- Cisco Nexus 5500 Platform switch
- Cisco Nexus 5500 Fibre Channel expansion module
- Cisco NX-OS Storage Protocols Services Package for the Cisco Nexus 5000 Series switch
- Cisco Nexus 2000 FEX
- Cisco UCS C200
- Cisco MDS 9124 switch
- Just a Bunch of Disks (JBOD)

Command List

The table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>how license usage</code>	Verify available licenses
<code>show npv status</code>	Verify net present value (NPV) operational mode
<code>[no] feature npv</code>	Disable/enable Fibre Channel NPV mode
<code>show feature</code>	Examine enabled features
<code>feature fcoe</code>	Enable Fibre Channel over Ethernet (FCoE)
<code>[no] shutdown</code>	Disable/enable interface/port
<code>show interface ethernet X/Y</code>	Verify Ethernet interface status
<code>switchport mode trunk</code>	Set the Ethernet interface mode to trunking
<code>spanning-tree port type edge trunk</code>	Set the spanning-tree port type to edge
<code>show interface Ethernet X/Y switchport</code>	Examine the Layer 2 information for the Ethernet
<code>vsan database</code>	Enter virtual storage area network (VSAN) database configuration
<code>vsan X</code>	Create VSAN with ID X
<code>show vsan</code>	Examine VSAN database
<code>vlan X</code>	Create VLAN with ID X
<code>fcoe vsan X</code>	Set the VLAN to be used as FCoE VLAN for VSAN X
<code>show vlan fcoe</code>	Examine the FCoE information for the given VLAN
<code>show interface Ethernet 1/3 fcoe</code>	Examine the FCoE information for the Data Center Bridging (DCB) Ethernet interface
<code>show interface Ethernet 1/3 priority-flow-control</code>	Examine the priority flow control for the given Ethernet interface
<code>interface Ethernet X/Y</code>	Enter Ethernet interface configuration mode
<code>bind interface ethernet X/Y</code>	Bind the physical Ethernet interface to the logical virtual Fibre Channel (vFC) interface
<code>interface vfc X</code>	Enter vFC interface configuration mode
<code>vsan X interface vfc fc X</code>	Associate vfc/fc interface to appropriate VSAN
<code>show interface vfc X</code>	Examine the vFC interface status
<code>show flogi database</code>	Examine the fabric login (FLOGI) database
<code>show zone status vsan X</code>	Examine the zone operational mode for a given VSAN
<code>zone mode enhanced vsan X</code>	Set the zone mode to enhanced
<code>show device-alias status</code>	Examine the device-alias database mode
<code>device-alias mode enhanced</code>	Set the device-alias database mode to enhanced
<code>device-alias commit</code>	Commit the configuration changes for the device-alias database

<code>show zone status vsan X</code>	Examine the zone configuration for a given VSAN
<code>slot 1</code>	Enter slot 1 Enter unified port configuration mode
<code>port 31-32 type fc</code>	Set ports 31 to 32 to operate as Fibre Channel interfaces
<code>show interface fc X/Y</code>	Examine the Fibre Channel interface status
<code>speed 4000</code>	Set the Fibre Channel interface speed to 4 Gb/s
<code>switchport trunk mode off</code>	Set the Fibre Channel interface trunking mode to off
<code>switchport mode E</code>	Set the Fibre Channel operational mode to E<
<code>switchport trunk allowed vsan X</code>	Set the allowed VSAN for the Fibre Channel interface
<code>no shutdown</code>	Enable the interface
<code>show zoneset active vsan X</code>	Examine the active zone set information
<code>zone name zone-name vsan X</code>	Create new zone for given VSAN
<code>member device-alias zone-name vsan X</code>	Add device-alias as a zone member
<code>zoneset name zoneset-name vsan X</code>	Enter the zone set configuration mode
<code>zoneset activate name zoneset-name vsan X</code>	Activate the zone set for a given VSAN
<code>zone commit vsan X</code>	Commit zoning configuration changes

Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Lab IP address plan

Task 1: Preparing Cisco Nexus 5548UP and 5596UP Switches for Fibre Channel Services

In this task, you will prepare a Cisco Nexus 5500UP Series switch for the FCoE deployment that includes verification of licenses, enabling proper features, and physical interface towards the assigned C-Series rack server.

Activity Procedure

Complete these steps:

- Step 1** Connect to the assigned Cisco Nexus 5500UP Series switch.
- Step 2** Verify the license availability on the assigned Cisco Nexus 5500UP Series switch. Use the command **show license usage** to verify that the **FC_FEATURES_PKG** feature package is present and available for use. (The **Status** should read either **In use** if FCoE is enabled or **Unused** if the FCoE is disabled, and the **Expiry** should read **Never**).

N5548-3# **show license usage**

Feature	Ins	Lic Count	Status	Expiry Date	Comments
FCOE_NPV_PKG	No	-	Unused		Grace 118D 22H
FM_SERVER_PKG	Yes	-	Unused	Never	-
ENTERPRISE_PKG	Yes	-	Unused	Never	-
FC_FEATURES_PKG	Yes	-	Unused	Never	-
VMFEX_FEATURE_PKG	Yes	-	Unused	Never	-
ENHANCED_LAYER2_PKG	Yes	-	In use	Never	-
LAN_BASE_SERVICES_PKG	Yes	-	In use	Never	-
LAN_ENTERPRISE_SERVICES_PKG	Yes	-	Unused	Never	-

Step 3 Verify the current status of FCoE functionality using the **show feature** command. Determine whether the FCoE functionality is enabled or disabled.

N5548-1# **show feature**

Feature Name	Instance	State
Flexlink	1	disabled
amt	1	disabled
bgp	1	disabled
cts	1	disabled
dhcp	1	disabled
dot1x	1	disabled
eigrp	1	disabled
eigrp	2	disabled
eigrp	3	disabled
eigrp	4	disabled
eth_port_sec	1	disabled
fabric-binding	1	disabled
fc-port-security	1	disabled
fcoe	1	disabled
fcoe-npv	1	disabled
fcsp	1	disabled
fex	1	disabled

Step 4 If the FCoE functionality is not enabled, enable it by using the **feature fcoe** command.

N5548-3(config)# **feature fcoe**

FC license checked out successfully

Step 5 Verify that the feature is enabled with the **show feature** command.

```
N5548-1# show feature
```

Feature Name	Instance	State
Flexlink	1	disabled
amt	1	disabled
bgp	1	disabled
cts	1	disabled
dhcp	1	disabled
dot1x	1	disabled
eigrp	1	disabled
eigrp	2	disabled
eigrp	3	disabled
eigrp	4	disabled
eth_port_sec	1	disabled
fabric-binding	1	disabled
fc-port-security	1	disabled
fcoe	1	enabled
fcoe-npv	1	disabled
fcsp	1	disabled
fex	1	disabled

Step 6 Enable the **Ethernet1/3** interface, which is used to connect the assigned Cisco UCS C-Series rack-mounted server, with the **no shutdown** command. Verify that after enabling the interface, the status transitions to UP.

Note The server connected to the interface **Ethernet 1/3** must be powered up for the interface to come online. If the server is not powered up, consult your instructor.

```
N5548-3# show interface ethernet 1/3
Ethernet1/3 is up
Hardware: 1000/10000 Ethernet, address: 547f.ee3e.660a (bia 547f.ee3e.660a)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is access
full-duplex, 10 Gb/s, media type is 10G
Beacon is turned off
Input flow-control is off, output flow-control is off
Rate mode is dedicated
Switchport monitor is off
EtherType is 0x8100
Last link flapped 00:00:28
Last clearing of "show interface" counters 00:00:02
30 seconds input rate 280 bits/sec, 0 packets/sec
30 seconds output rate 896 bits/sec, 0 packets/sec
Load-Interval #2: 5 minute (300 seconds)
  input rate 16 bps, 0 pps; output rate 1.41 Kbps, 3 pps
RX
  0 unicast packets  0 multicast packets  0 broadcast packets
  0 input packets  0 bytes
  0 jumbo packets  0 storm suppression bytes
  0 runts  0 giants  0 CRC  0 no buffer
  0 input error  0 short frame  0 overrun  0 underrun  0 ignored
  0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
  0 input with dribble  0 input discard
  0 Rx pause
TX
```

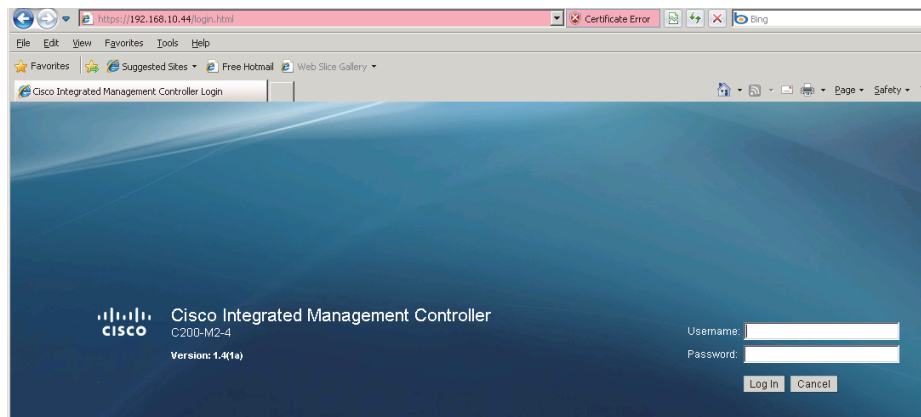
```

0 unicast packets 0 multicast packets 0 broadcast packets
0 output packets 0 bytes
0 jumbo packets
0 output errors 0 collision 0 deferred 0 late collision
0 lost carrier 0 no carrier 0 babble 0 output discard
0 Tx pause
0 interface resets

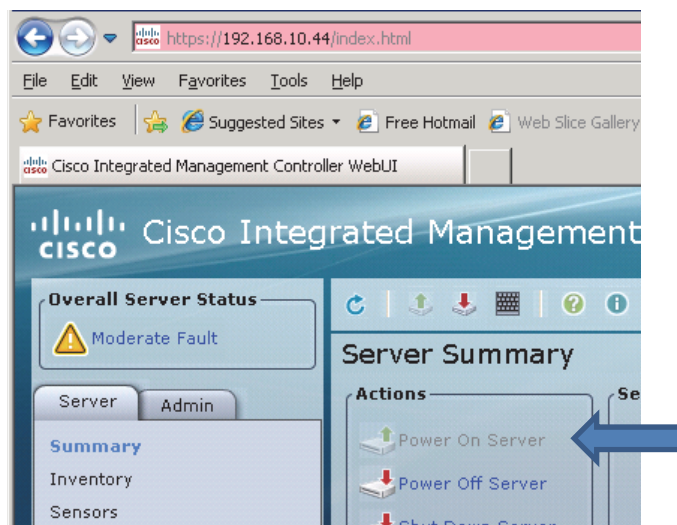
```

If the server is not powered up, you can power it up by connecting to your assigned C-Series server and then power it up. Log into the server web console. Navigate your web browser to the IP address of the assigned server, **https://192.168.10.4P**, and login with the **admin** username and the **NXos12345** password.

Note Refer to the Job Aids section in order to obtain the server Cisco Integrated Management Controller IP address.



Once you are logged into the web console, select the Power Cycle Server option in the Server Summary right pane under the Actions tab, and confirm the option with **OK** when presented with the dialog box.



Step 7 Set the **Ethernet 1/3** interface to manual trunking mode in order to force it to trunk 802.1q VLANs by using the command **switchport mode trunk**. Trunking is required for FCoE since VSAN is carried in the FCoE-assigned VLAN. Set the interface type to **edge** for the STP with the **spanning-tree port type edge trunk** command. Verify that trunking is administratively enabled and operational with the **show interface Ethernet 1/3 switchport** command.

```

N5548-3# show interface ethernet 1/3 switchport
Name: Ethernet1/3
Switchport: Enabled
Switchport Monitor: Not enabled
Operational Mode: trunk
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Allowed: 1-3967,4048-4093
Voice VLAN: none
Extended Trust State : not trusted [COS = 0]
Administrative private-vlan primary host-association: none
Administrative private-vlan secondary host-association: none
Administrative private-vlan primary mapping: none
Administrative private-vlan secondary mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

```

Activity Verification

You have completed this task when you attain these results:

- Verified the presence of a Fibre Channel license.
- Enabled the FCoE feature.
- Configured the relevant Ethernet interface as a trunk edge port.

Task 2: Configuring FCoE on the Cisco Nexus 5548UP and 5596UP Switches In this task, you will implement and configure FCoE functionality on a Cisco Nexus 5500UP Series switch towards the assigned Cisco UCS C-Series Rack-Mount server. This includes enabling the FCoE feature, the creation of appropriate VSAN and FCoE VLAN, enabling the physical server downlink, creating a vFC interface, and assigning it to the proper VSAN.

Pod	VSAN "X"	FCoE VLAN
Pod 1, 3, 5	11	1011
Pod 2, 4, 6	12	1012

Activity Procedure

Complete these steps:

- Step 1** Create the assigned VSAN that will be used by the server to connect to the remote storage. Enter the VSAN database with the **vsan database** command. Next, add the assigned VSAN to the VSAN database with the **vsan X** command. Verify the VSAN database with the **show vsan** command. Note that the operational state of the VSAN will be down since there are no assigned or operational interfaces.

```

N5548-3# show vsan
vsan 1 information
      name:VSAN0001  state:active
      interoperability mode:default
      loadbalancing:src-id/dst-id/oxid
      operational state:down

```

```

vsan 11 information
    name:VSAN0011  state:active
    interoperability mode:default
    loadbalancing:src-id/dst-id/oxid
    operational state:down

```

```
vsan 4079:evfp_isolated_vsan
```

```
vsan 4094:isolated_vsan
```

- Step 2** Create the FCoE VLAN for the VSAN by using the **vlan *VLAN-ID*** command. Set the newly created VLAN to be the FCoE VLAN for the VSAN you created in the previous step by using the **fcoe vsan *VSAN-ID*** command. Verify the configuration with the **show vlan fcoe** command. Note that the **Association State** of the VLAN should be **Operational**.

Note Refer to the Pod-VSAN-VLAN table at the beginning of this task.

```
N5548-3# show vlan fcoe
```

Original VLAN ID	Translated VSAN ID	Association State
-----	-----	-----
1011	11	Operational

- Step 3** Examine the status of the **Ethernet 1/3** interface for the FCoE functionality with the **show interface Ethernet 1/3 fcoe** command. You should see that the interface is operational for the FCoE and has the status **UP**.

```

N5548-3# show interface ethernet 1/3 fcoe
Ethernet1/3 is FCoE UP

```

- Step 4** Verify that the priority flow control is enabled for the **Ethernet 1/3**, which is required by the FCoE traffic that will be carried over the physical interface, by using the **show interface Ethernet 1/3 priority-flow-control** command.

```

N5548-4(config)# show interface ethernet 1/3 priority-flow-control
=====
Port                Mode Oper (VL bmap)  RxPPP  TxPPP
=====
Ethernet1/3         Auto On  (8)           0      0

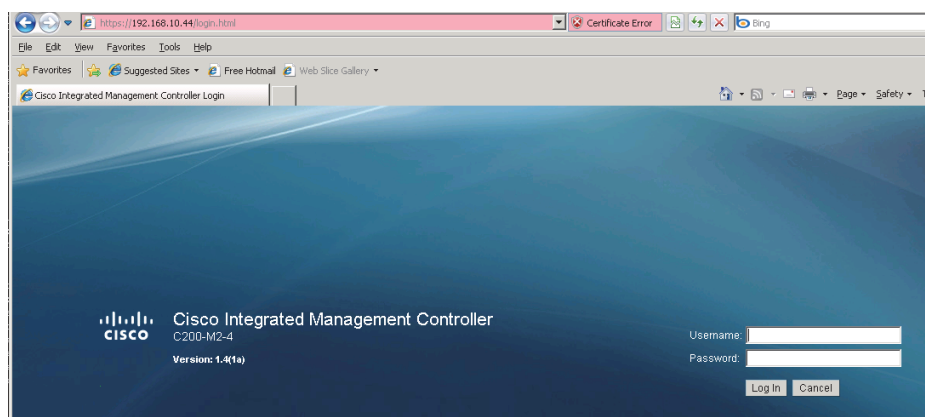
```

- Step 5** Create the vFC interface **vfc 3** that will be used to connect the assigned C-Series server. The virtual interface will have its counterpart in the C-Series server configuration: the virtual host bus adapter (vHBA) with the proper FCoE VLAN and VSAN ID. Bind the created **vfc 3** interface to the physical interface **Ethernet 1/3** to which the assigned C-Series server is connected by using the **bind interface ethernet 1/3** command.
- Step 6** Configure trunking of only the assigned VSAN with the **switchport trunk allowed vsan X** command (where X is the assigned VSAN), and enable it with the **no shutdown** command.
- Step 7** Assign the newly created **vfc 3** interface to the assigned VSAN. Enter the VSAN database with the **vsan database** command.

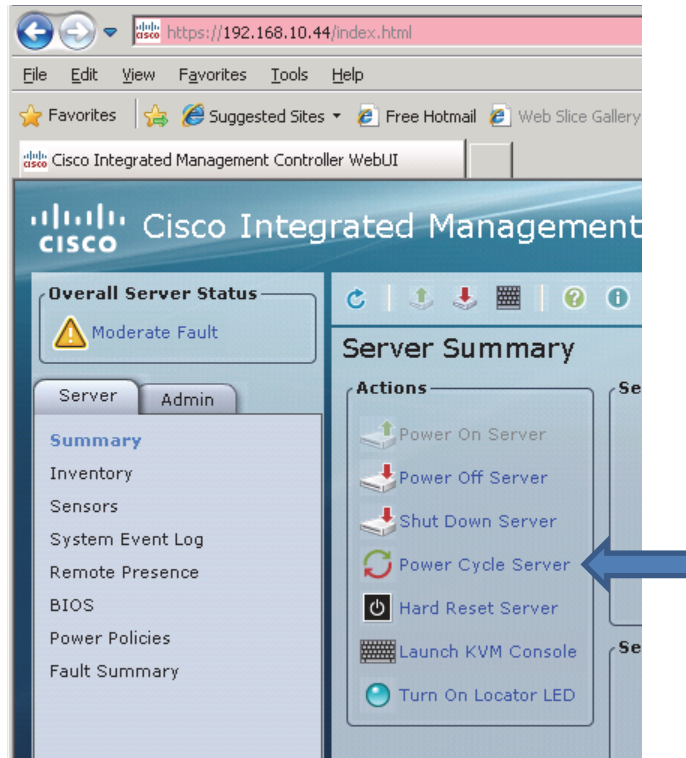
- Step 8** Assign the **vfc 3** interface to the assigned VSAN by using the **vsan X interface vfc 3** command (where X is the assigned VSAN).
- Step 9** Use the **show interface vfc 3** command to verify that the created virtual interface **vfc 3** is operating for the assigned VSAN. Note that the VSAN is stuck in the **initializing** mode.

```
N5548-4# show interface vfc 3
vfc3 is trunking (Not all VSANs UP on the trunk)
  Bound interface is Ethernet1/3
  Hardware is Ethernet
  Port WWN is 20:02:54:7f:ee:82:9e:ff
  Admin port mode is F, trunk mode is on
  snmp link state traps are enabled
  Port mode is TF
  Port vsan is 1
  Trunk vsans (admin allowed and active) (12)
  Trunk vsans (up) ()
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) (12)
  1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    8 frames input, 764 bytes
    0 discards, 0 errors
    9 frames output, 1288 bytes
    0 discards, 0 errors
  last clearing of "show interface" counters never
  Interface last changed at Wed May  6 11:04:19 2009
```

- Step 10** To enable the communication for the assigned VSAN towards the assigned C-Series server, you need to reset the server to enable the communication. Do this by logging into the server web console by navigating your web browser to the IP address of the assigned server, **https://192.168.10.4P**, and login with the **admin** username and **NXos12345** password.



- Step 11** When you are logged into the web console, select the **Power Cycle Server** option in the Server Summary right pane under the Actions and confirm the option with **OK** when presented with the dialog box.



- Step 12** Soon the server will reboot, and the communication between the server and the assigned Cisco Nexus 5500UP Series switch will come up. The server vHBA interface and the Cisco Nexus 5500UP Series switch **vfc 3** interface will come up and the assigned VSAN will be active on the connection. You can examine the status by inspecting **vfc 3** interface status with **show interface vfc 3** command. You should note that the assigned VSAN is now up.

```
N5548-4# show interface vfc 3
```

```
vfc3 is trunking
```

```
Bound interface is Ethernet1/3
```

```
Hardware is Ethernet
```

```
Port WWN is 20:02:54:7f:ee:82:9e:ff
```

```
Admin port mode is F, trunk mode is on
```

```
snmp link state traps are enabled
```

```
Port mode is TF
```

```
Port vsan is 12
```

```
Trunk vsans (admin allowed and active) (12)
```

```
Trunk vsans (up) (12)
```

```
Trunk vsans (isolated) ()
```

```
Trunk vsans (initializing) ()
```

```
1 minute input rate 24 bits/sec, 3 bytes/sec, 0 frames/sec
```

```
1 minute output rate 56 bits/sec, 7 bytes/sec, 0
```

```
frames/sec
```

```
16 frames input, 1528 bytes
```

```
0 discards, 0 errors
```

```
18 frames output, 2576 bytes
```

```
0 discards, 0 errors
```

```
last clearing of "show interface" counters never
Interface last changed at Wed May 6 12:10:43 2009
```

- Step 13** Once the server is successfully connected to the Cisco Nexus 5500UP Series switch (the Fibre Channel service), the server should log into the fabric and get its Fibre Channel ID (FCID) after the FLOGI is finished. You can inspect the fabric login by using the **show flogi database** command and see that the server is logged into the fabric.

```
N5548-4# show flogi database
```

```
-----
--
INTERFACE          VSAN      FCID          PORT NAME          NODE NAME
-----
--
vfc3                12       0x2c0000     20:00:00:25:b5:c0:40:04
20:00:00:25:b5:c0:30:04
```

```
Total number of flogi = 1.
```

Task 3: Implementing Fibre Channel Services

In this task, you will implement and configure the required Fibre Channel services in order to enable communication between the assigned Cisco UCS C-Series Rack-Mount Server and the storage target, which is the disk array. This will include enabling a proper interface between the assigned Cisco Nexus 5500UP Series switch and the core MDS Fibre Channel switch (thereby forcing the Fibre Channel Domain ID on the Cisco Nexus 5500UP Series switch), configuring and activating proper Fibre Channel zoning configuration, and verifying final FC configuration and operation.

Activity Procedure

Complete these steps:

- Step 1** Verify the zoning operational mode for the assigned VSAN on the Cisco Nexus 5500UP Series switch by using the **show zone status vsan X** (where X is the assigned VSAN ID). Note that zone mode is basic, whereas on the Cisco MDS 9124 Switch the zone mode is enhanced. N5548-4# **show zone status vsan 12**

```
VSAN: 12 default-zone: deny distribute: active only Interop:
default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
Default zone:
qos: none broadcast: disabled ronly: unsupported
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Status:
```

- Step 2** In order to enable proper Fibre Channel fabric operation, you need to tune the zoning operational mode on the Cisco Nexus 5500UP Series switch to enhanced mode by using the **zone mode enhanced vsan X** command (where X is the assigned VSAN ID).

- Step 3** Verify the device alias database mode on the Cisco Nexus 5500UP Series switch by using the **show device-alias status** command. You will notice that the mode is set to basic.

```
N5548-4# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 0 Mode: Basic
Checksum: 0xf6bd6b3389b87233d462029172c8612
```

- Step 4** Since the upstream core MDS switch has the device-alias database mode set to enhanced, you will need to change it on the Cisco Nexus 5500UP Series switch by using the **device-alias mode enhanced** command. Commit the configuration changes with the **device-alias commit** command.

- Step 5** Verify that the database mode has been changed to enhanced by using the **show device-alias status** command again.

```
N5548-4# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 0 Mode: Enhanced
Checksum: 0xb713791d47fd2d205e1a5fa01ea9c447
```

- Step 6** Verify that the zoning mode was changed to enhanced by using the **show zone status vsan X** command.

```
N5548-4# show zone status vsan 12
VSAN: 12 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
Default zone:
  qos: none broadcast: disabled ronly: unsupported
Full Zoning Database :
  DB size: 44 bytes
  Zonesets:0 Zones:0 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
  Database Not Available
Status: Set zoning mode complete at 13:21:07 UTC May 6 2009
```

- Step 7** Set the operational mode of the **Ethernet 1/31** unified port to Fibre Channel mode. Enter the slot 1 configuration mode by using the **slot 1** command.

- Step 8** Set the port type to Fibre Channel for ports 31 and 32 by using the **port 31-32 type fc** command. To activate the configuration, you will need to reload the assigned Nexus 5500 UP switch.

- Step 9** Once the Cisco Nexus 5500UP Series switch is back online, you must configure the remainder of the Fibre Channel parameters for that interface. Verify that you see port 1/31 as a Fibre Channel interface by using the **show interface fc1/31** command. Ensure that you get an output for the interface that indicates that port 1/31 now operates as a Fibre Channel interface.

```
N5548-4# show interface fc 1/31
fc1/31 is down (Administratively down)
Hardware is Fibre Channel, SFP is short wave laser w/o OFC
(SN)
Port WWN is 20:1f:54:7f:ee:82:9e:c0
Admin port mode is auto, trunk mode is on
```

```

snmp link state traps are enabled
Port vsan is 1
Receive data field Size is 2112
Beacon is turned off
1 minute input rate 392 bits/sec, 49 bytes/sec, 1
frames/sec
1 minute output rate 976 bits/sec, 122 bytes/sec, 1
frames/sec
1746 frames input, 55872 bytes
0 discards, 0 errors
0 CRC, 0 unknown class
0 too long, 0 too short
1746 frames output, 139680 bytes
0 discards, 0 errors
882 input OLS, 880 LRR, 0 NOS, 0 loop inits
885 output OLS, 7 LRR, 878 NOS, 0 loop inits
last clearing of "show interface" counters never

```

- Step 10** Move the interface **fc1/31** to the assigned VSAN by entering the VSAN database by using the **vsan database** command on the Cisco Nexus 5500UP Series switch. Move the interface to the VSAN by using the **vsan X interface fc 1/31** command (where X is the assigned VSAN ID).
- Step 11** Set the port speed to 4 Gb/s for interface **fc 1/31** on the Cisco Nexus 5500UP Series switch with the command **speed 4000** under the interface configuration mode.
- Step 12** The other side of the link (the port on the Cisco MDS 9124 Switch) is configured with the following parameters: Fibre Channel port mode is F, the allowed VSAN is the assigned one (so VSAN 11 for pods 1 and 3 and VSAN 12 for pods 2 and 4), and Fibre Channel port trunking is disabled. Set the Cisco Nexus 5500UP Series switch interface fc 1/31 with the same parameters. Set the trunking mode to off with the **switchport trunk mode off** command.
- Step 13** Set the port Fibre Channel mode to **E** with the **switchport mode E** command.
- Step 14** Set the allowed VSAN to the assigned VSAN ID with the **switchport trunk allowed vsan X** command (where X is the assigned VSAN ID), and enable the interface with **no shutdown** command.
- Step 15** Verify the interface status with the **show interface fc 1/31** command. Note that the interface is now up and operational.

```

N5548-4 # show interface fc1/31
fc1/31 is up
Hardware is Fibre Channel, SFP is short wave laser w/o OFC
(SN)
Port WWN is 20:1f:54:7f:ee:82:9e:c0
Peer port WWN is 20:0c:54:7f:ee:7a:c9:00
Admin port mode is E, trunk mode is off
snmp link state traps are enabled
Port mode is E
Port vsan is 12
Speed is 4 Gbps
Transmit B2B Credit is 16
Receive B2B Credit is 16

```

```

Receive data field Size is 2112
Beacon is turned off
1 minute input rate 200 bits/sec, 25 bytes/sec, 0
frames/sec
1 minute output rate 248 bits/sec, 31 bytes/sec, 0
frames/sec
2398 frames input, 108552 bytes
0 discards, 0 errors
0 CRC, 0 unknown class
0 too long, 0 too short
2395 frames output, 197752 bytes
0 discards, 0 errors
900 input OLS, 899 LRR, 1 NOS, 0 loop inits
908 output OLS, 19 LRR, 890 NOS, 0 loop inits
last clearing of "show interface" counters never
16 receive B2B credit remaining
16 transmit B2B credit remaining
0 low priority transmit B2B credit remaining
Interface last changed at Wed May 6 13:40:07 2009

```

- Step 16** Examine the zoning information for the assigned Cisco UCS C-Series Rack-Mount Server by using the **show zoneset active vsan X** command (where X is the assigned VSAN ID). You will see that there is no existing zone in the assigned VSAN active zone set.

```

N5548-4# show zoneset active vsan 12
zoneset name FabricB vsan 12

```

- Step 17** Create a zone named **znFabricB-dcuci-cP** (where **P** is your pod number) for the assigned Cisco UCS C-Series Rack-Mount Server, and put it together with the proper storage target. (Effectively, if in pod 1 or pod 3, the storage target device alias name is CX3-SPA, and if in pod 2 or 4, the storage target device alias name is CX3-SPB.) Use the command **zone name zone-name vsan X** (where X is the assigned VSAN ID).
- Step 18** Use the **member device-alias zone-name vsan X** command to add the Cisco UCS C-Series Rack-Mount Server defined with the device alias name **dcuci-cP** (where **P** is your pod number) and the storage target device defined with the aforementioned alias name
- Step 19** Commit the new zone into the fabric zone database with the **zone commit vsan X** command (where X is the assigned VSAN ID).
- Step 20** Add the created zone into the active zone set named **FabricW** (where W is either fabric A for VSAN 11 or B for VSAN 12) by entering the active zone set for the assigned VSAN ID by using the **zoneset name FabricW vsan X** command.
- Step 21** Add the created zone to the active zone set with the **member zone-name** command.
- Step 22** Activate the changed zone set for the assigned VSAN with the **zoneset activate name zoneset-name vsan X** command.
- Step 23** Commit the changes for the zone set into the fabric zone database with the **zone commit vsan X** command (where X is the assigned VSAN ID).

- Step 24** Verify that the newly created zone is active in the activated zone set and that the assigned Cisco UCS C-Series Rack-Mount Server and target storage device can communicate by using the **show zoneset active vsan X** command (where X is the assigned VSAN ID). You should see the zone being part of the active zone set and the * besides the assigned Cisco UCS C-Series Rack-Mount Server server pWWN and storage target, which indicates that the device are active in the fabric.

```
N5548-4# show zoneset active vsan 12
```

```
zoneset name FabricB vsan 12
```

```
... output omitted ...
```

```
zone name znFabricB-dcuci-c4 vsan 12
```

```
* fcid 0x2a0000 [device-alias CX3-SPB]
```

```
* fcid 0x2c0000 [device-alias dcuci-c4]
```

```
... output omitted ...
```

Activity Verification

You have completed this task when you attain these results:

- Configured the Cisco Nexus 5500UP Series switch interface towards the MDS 9124 as the FC interface.
- Applied proper FC configuration on the Cisco Nexus 5500UP Series switch interface connecting to Cisco MDS 9124 Switch.
- Configured and activated zoning information in order to allow communication between the assigned Cisco UCS C-Series Rack-Mount Server and the storage target.

Lab 4-2: Configuring NPV

Complete this lab activity to practice what you learned in the related module.

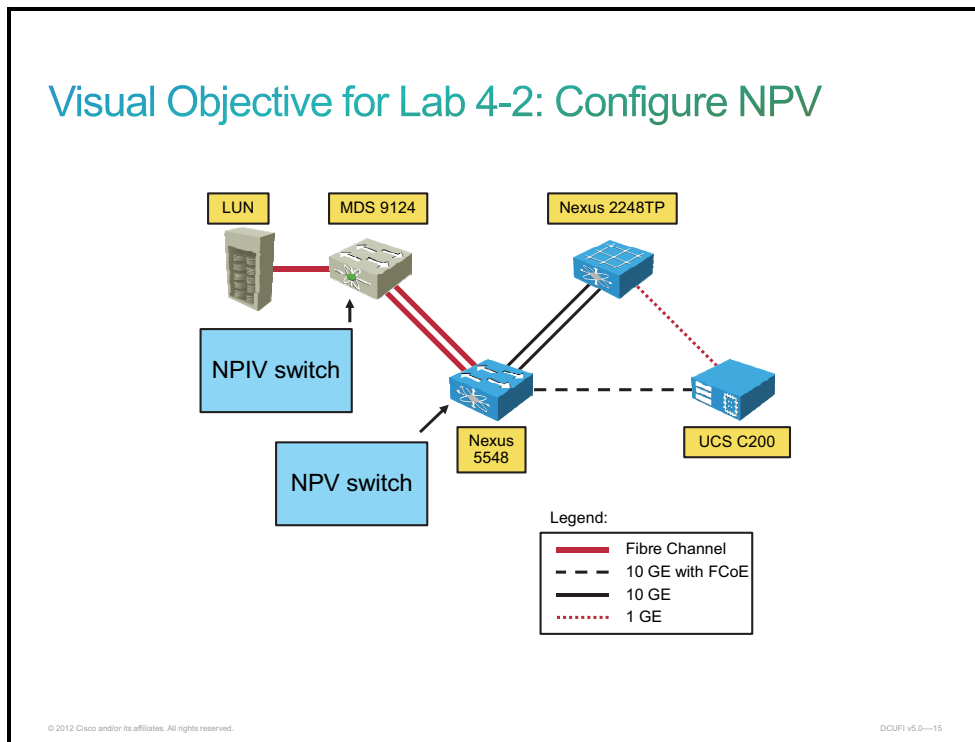
Activity Objective

In this activity, you will configure the Cisco Nexus 5500 Platform switch in NPV mode and verify the configuration by using the CLI. After completing this activity, you will be able to meet these objectives:

- Enable the NPV mode on the Cisco Nexus 5500 Platform switch
- Configure the Cisco Nexus 5500 Platform switch server-facing and fabric switch-facing interfaces for NPV
- Configure the Cisco MDS 9124 Switch to support NPIV
- Verify NPV and Fibre Channel operation

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required to complete this activity:

- Cisco UCS C200 server with Cisco Network Assistant
- Cisco Nexus 5500 Platform switch
- Cisco MDS 9124 Switch
- JBOD or a storage array

Command List

The table describes the commands that are used in this activity.

Cisco NX-OS Commands

Command	Description
<code>bind interface ethernet <x/y></code>	Bind the vFC interface to an Ethernet interface
<code>copy bootflash:temp running-config</code>	Copy a saved configuration from bootflash to the running configuration
<code>copy running-config bootflash:temp</code>	Copy the running configuration to a file in bootflash
<code>dir bootflash:</code>	Display the contents of bootflash
<code>feature fcoe</code>	Enable the FCoE feature
<code>interface ethernet <x/y></code>	Enter configuration mode for an Ethernet interface
<code>interface fc<x/y></code>	Enter configuration mode for a Fibre Channel interface
<code>interface vfc<x></code>	Enter configuration mode for a vFC interface
<code>no shutdown</code>	Enable an interface
<code>feature npiv</code>	Enable NPIV
<code>npv auto-load-balance disruptive</code>	Enable NPV load balancing
<code>feature npv</code>	Enable NPV
<code>npv traffic-map server-interface vfc<x> external-interface fc<x/y></code>	Configure traffic mapping for a server interface to an external interface
<code>show fcns database</code>	Display the FCNS database
<code>show fcoe</code>	Display the FCoE global details
<code>show flogi database</code>	Display the FLOGI database
<code>show interface fc<x/y></code>	Display the Fibre Channel interface details
<code>show interface vfc <x></code>	Display the vFC interface details
<code>show npv flogi-table</code>	Display the FLOGI table on the NPV-enabled switch
<code>show npv status</code>	Display the NPV status
<code>Show npv traffic-map</code>	Display the traffic mappings that have been configured
<code>show vlan fcoe</code>	Display the VLAN-to-VSAN mapping and status
<code>show vsan membership</code>	Display the VSAN membership details
<code>spanning-tree port type edge trunk</code>	Configure an interface as a spanning-tree trunk port at the edge
<code>switchport mode F</code>	Configure an interface in F Port mode.
<code>switchport mode NP</code>	Configure an interface in proxy N port (NP) port mode
<code>switchport mode trunk</code>	Configure an interface for trunking
<code>vlan <id></code>	Configure a VLAN

vsan <id>	Configure a VSAN
vsan <id> interface fc<x/y>	Associate a VSAN with a Fibre Channel interface
vsan <id> interface vfc <x>	Associate a VSAN with a vFC interface
vsan database	Enter VSAN database configuration mode

Task 1: Configure NPV Mode on the Cisco Nexus 5500 Platform Switch

In this task, you will back up the current configuration and then configure the Cisco Nexus 5500 Platform switch to operate in NPV mode.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.
- Step 2** Configuring the N Port Virtualization (NPV) feature will initiate a **write erase** and a system reboot. Save your running configuration to the bootflash memory before proceeding. Once the reboot is complete, you may retrieve your running configuration in order to complete the lab exercise.

```
N5548-P# copy running-config bootflash:temp
N5548-P# dir bootflash:
      13165      Apr 25 16:15:17 2009
20090425_161414_poap_3361_init.log
      91390      May 20 22:41:39 2009
20090520_223650_poap_3360_init.log
      15509      May 02 23:39:17 2009  N5548-4-running-config
      15509      May 02 23:40:35 2009  N5548-719-running-config
      1679       Mar 20 09:14:16 2012  license_SSI16010HKX_33.lic
      8759       May 29 12:11:50 2009  mts.log
      34358272    Mar 20 09:07:28 2012  n5000-uk9-
kickstart.5.1.3.N1.1a.bin
      34357760    Apr 22 13:31:33 2009  n5000-uk9-
kickstart.5.1.3.N2.1.bin
      147420604   Mar 20 09:08:16 2012  n5000-uk9.5.1.3.N1.1a.bin
      172662417   Apr 22 13:32:32 2009  n5000-uk9.5.1.3.N2.1.bin
      14568      May 24 07:38:40 2009  temp
Usage for bootflash://sup-local
626069504 bytes used
257282048 bytes free
883351552 bytes total
```

- Step 3** Enable the NPV feature.

```
N5548-P(config)# feature npv
Verify that boot variables are set and the changes are saved.
Changing to npv mode erases the current configuration and reboots the
switch in npv mode. Do you want to continue? (y/n):y
writing reset reason 90,

INIT: Sending processes the TERM signal
2011 Jan 25 03:40:53 N5K-5 %$ VDC-1 %$ %KERN-0-SYSTEM_MSG: writing
reset reason 90, - kernel
Jan 25 03:40:53 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "statsclient"
(PID 3833) is forced exit.

Jan 25 03:40:53 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "smm" (PID
3756) is forced exit.
```

```
Jan 25 03:40:53 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "rib" (PID 10878) is forced exit.
```

```
Jan 25 03:40:53 %LIBSYSMGR-3-SIG usdk_sse: mts_send failed:-32 sending to 0xfe000000.25e errno 32
```

Step 4 Once the switch has reloaded, access the Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 5 Enable the FCoE feature, and activate the interfaces that connect the Cisco Nexus 5500 Platform switch to the servers.

```
N5548-P(config)# feature fcoe
FC license checked out successfully
FCoE manager enabled successfully
N5548-P(config)# interface ethernet 1/3
N5548-P(config-if-range)# switchport mode trunk
N5548-P(config-if-range)# 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
```

```
N5548-P(config-if-range)# no shutdown
```

Step 6 Create the vFC interfaces, and bind them to the Ethernet interfaces.

```
N5548-P(config-if-range)# interface vfc 3
N5548-P(config-if)# bind interface ethernet 1/3
N5548-P(config-if)# no shutdown
```

Step 7 Verify that the vFC interfaces are bound correctly to the Ethernet interfaces.

```
N5548-P(config-if)# show interface vfc 3
vfc3 is down
Bound interface is Ethernet1/3
Hardware is Virtual Fibre Channel
Port WWN is 20:00:00:05:9b:1f:89:ff
Admin port mode is F, trunk mode is off
snmp link state traps are enabled
Port vsan is 1
5 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
5 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
0 frames input, 0 bytes
0 discards, 0 errors
0 frames output, 0 bytes
Port vsan is 1, 0 errors
```

Step 8 Create a VLAN-to-VSAN assignment, and bind the vFC interface to the VSAN.

Note Use the specified VSAN-FCoE VLAN mapping table in the Job Aids, and choose the appropriate VSAN or VLAN for your pod.

```
N5548-P(config-if)# vlan 1011
N5548-P(config-vlan)# fcoe vsan 11
N5548-P(config-vlan)# exit
N5548-P(config)# vsan database
N5548-P(config-vsan-db)# vsan 11
N5548-P(config-vsan-db)# vsan 11 interface vfc 3
N5548-P(config-vsan-db)# exit
```

Step 9 Display the interface membership for all VSANs.

```
N5548-5(config)# show vsan membership
vsan 1 interfaces:

vsan 11 interfaces:
    vfc3

vsan 4079(evfp_isolated_vsan) interfaces:

vsan 4094(isolated_vsan) interfaces:
```

Step 10 Confirm the VLAN-to-VSAN FCoE assignment.

```
N5548-P(config)# show vlan fcoe
VLAN      VSAN      Status
-----
1011      11        Operational
```

Step 11 Confirm the association of Ethernet-to-vFC interfaces.

```
N5548-P(config)# show interface vfc 3
vfc3 is down
    Bound interface is Ethernet1/3
    Hardware is Virtual Fibre Channel
    Port WWN is 20:00:00:05:9b:1f:89:ff
    Admin port mode is F, trunk mode is off
    snmp link state traps are enabled
    Port vsan is 2
    5 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
        0 frames input, 0 bytes
        0 discards, 0 errors
    0 frames output, 0 bytes
        0 discards, 0 errors
```

- Step 12** Configure unified ports 1/31–32 to operate as Fibre Channel ports. Accept the Fibre Channel enhanced form-factor pluggable (SFP+).

```
N5548-P(config-vsan-db) # slot 1
N5548-P(config-slot) # port 1-30 type ethernet
N5548-P(config-slot) # port 31-32 type fc
N5548-P(config-slot) # exit
```

- Step 13** In order for interfaces to change operational mode, write a configuration and reload switch.

```
N5548-P(config) # copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
N5548-P(config) # reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

- Step 14** Connect to your assigned Cisco Nexus 5500 Platform switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

- Step 15** Assign to VSAN 2 the Fibre Channel interface that connects the Cisco Nexus 5500 Platform switch to the Cisco MDS 9124 fabric switch.

```
N5548-P(config) # vsan database
N5548-P(config-vsan-db) # vsan 11 interface fc 1/31
N5548-P(config-vsan-db) # show vsan membership
vsan 1 interfaces:
    fc1/32
vsan 2 interfaces:
    fc1/31          vfc3

vsan 4079(evfp_isolated_vsan) interfaces:

vsan 4094(isolated_vsan) interfaces:
```

- Step 16** Configure the interfaces on your Cisco Nexus 5500 Platform switch for the proper Fibre Channel port types.

```
N5548-P(config-vsan-db) # interface fc1/31
N5548-P(config-if) # switchport mode NP
N5548-P(config-if) # no shutdown
N5548-P(config-if) # exit
N5548-P(config) # interface vfc 3
N5548-P(config-if) # switchport mode F
N5548-P(config-if) # no shutdown
N5548-P(config-if) # exit
```

- Step 17** Configure a mapping between the server and the NPV uplink interface. Enable disruptive load balancing.

```
N5548-P(config) # npv traffic-map server-interface vfc 1 external-
interface fc1/31
N5548-P(config) # npv traffic-map server-interface vfc 2 external-
interface fc1/32
N5548-P(config) # npv auto-load-balance disruptive
```

Enabling this feature may flap the server interfaces whenever load is not in a balanced state. This process may result in traffic disruption. Do you want to proceed? (y/n): **y**

N5548-**P**(config)# **show npv traffic-map**

NPV Traffic Map Information:

Server-If External-If(s)

vfcl fc1/31
vfc2 fc1/32

Step 18 View the NPV configuration details.

N5548-**P**(config)# **show npv status**

npiv is disabled

disruptive load balancing is enabled

External Interfaces:

=====

Interface: fc1/31, State: Failed(NPIV is not enabled in upstream switch)

Number of External Interfaces: 2

Server Interfaces:

=====

Number of Server Interfaces: 0

Activity Verification

You have completed this task when you attain these results:

- Enabled NPV mode on the Cisco Nexus 5500 Platform switch.
- Enabled FCoE and configured the server-facing interface as a trunk edge port.
- Created a VSAN.
- Created an FCoE VLAN and configured the VLAN-to-VSAN mapping.
- Configured the uplinks to the Cisco MDS 9124 Switch as NP ports.
- Enabled the uplinks to the Cisco MDS 9124 Switch.

Task 2: Configure NPIV on the Cisco MDS 9124 Switch

In this task, you will configure the Cisco MDS 9124 Switch to operate in NPIV mode.

Activity Procedure

Complete these steps:

Step 1 Connect to your assigned Cisco MDS 9124 Switch. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.

Step 2 Enable the NPIV feature on the Cisco MDS 9124 Switch.

```
MDS-P(config) # npiv enable
```

Note This feature might be already enabled as you are sharing the Cisco MDS 9124 Switch with another pod.

Step 3 Configure the interfaces on the core switch to operate in fabric (F) mode.

```
MDS-P(config) # feature npiv  
MDS-P(config) # interface fc 1/11-12  
MDS-P(config-if) # switchport mode F  
MDS-P(config-if) # no shutdown
```

Step 4 Configure VSAN 2, and assign the interfaces that connect the Cisco MDS 9124 Switch to the Cisco Nexus 5500 Platform switch to VSAN 11.

Note Consult the Job Aids at the beginning of the Lab Guide to find out which port you are using on the Cisco MDS 9124 Switch.

```
MDS-P(config-if) # vsan database  
MDS-P(config-vsan-db) # vsan 11  
MDS-P(config-vsan-db) # vsan 11 interface fc 1/FF  
Traffic on fc1/1 may be impacted. Do you want to continue? (y/n) [n]  
y
```

Step 5 Verify the VSAN membership.

```
MDS-P(config-vsan-db) # show vsan membership  
vsan 1 interfaces:  
    fc1/4          fc1/5          fc1/6          fc1/8  
vsan 11 interfaces:  
    fc1/7          fc1/11  
  
vsan 4079(evfp_isolated_vsan) interfaces:  
  
vsan 4094(isolated_vsan) interfaces:
```

Note Your output may look different depending on how far in the lab you and the other students are.

Step 6 Display the Fibre Channel Name Server (FCNS) tables and the FLOGI database.

```
MDS-P(config-vsan-db) # show fcns database
```

```
VSAN 2:
```

```
-----  
FCID          TYPE  PWWN                                (VENDOR)  FC4-TYPE:FEATURE  
-----  
0xe30000      N    20:41:00:05:9b:1f:89:c0 (Cisco)   npv  
0xe30001      N    21:00:00:c0:dd:12:b6:ad (Qlogic)  scsi-fcp:init  
0xe30100      N    20:42:00:05:9b:1f:89:c0 (Cisco)   npv  
0xe30101      N    21:00:00:c0:dd:12:b6:af (Qlogic)  scsi-fcp:init  
0xe3029b      NL   21:00:00:00:87:6d:a5:a8                scsi-fcp  
0xe302b3      NL   21:00:00:00:87:6f:13:21                scsi-fcp
```

```
Total number of entries = 6
```

```
MDS-P(config-vsan-db) # show flogi database
```

```
-----  
INTERFACE VSAN FCID          PORT NAME                                NODE NAME  
-----  
fc1/1      2 0xe30000 20:41:00:05:9b:1f:89:c0 20:02:00:05:9b:1f:89:c1  
fc1/1      2 0xe30001 21:00:00:c0:dd:12:b6:ad 20:00:00:c0:dd:12:b6:ad  
fc1/2      2 0xe30100 20:42:00:05:9b:1f:89:c0 20:02:00:05:9b:1f:89:c1  
fc1/2      2 0xe30101 21:00:00:c0:dd:12:b6:af 20:00:00:c0:dd:12:b6:af  
fc1/3      2 0xe3029b 21:00:00:00:87:6d:a5:a8 20:00:00:00:87:6d:a5:a8  
fc1/3      2 0xe302b3 21:00:00:00:87:6f:13:21 20:00:00:00:87:6f:13:21
```

```
Total number of flogi = 6.
```

Note Your output may look different depending on the number of devices connected to fabric.

Step 7 Reconnect to your assigned Cisco Nexus 5500 Platform switch, and then view the FLOGI table.

```
N5548-P(config) # show npv flogi-table
```

```
-----  
SERVER                                EXTERNAL  
INTERFACE VSAN FCID          PORT NAME                                NODE NAME  INTERFACE  
-----  
vfc3     11 0xe30001 20:00:00:25:b5:c0:40:04 20:00:00:25:b5:c0:30:04 fc1/31
```

```
Total number of flogi = 2.
```

Step 8 Verify the NPV status.

```
N5548-P(config) # show npv status

npiv is disabled

disruptive load balancing is enabled

External Interfaces:
=====
Interface:  fc1/31, VSAN:   11, FCID: 0xe30000, State: Up

Number of External Interfaces: 1

Server Interfaces:
=====
Interface:   vfc3, VSAN:   11, State: Up

Number of Server Interfaces: 1
```

Activity Verification

You have completed this task when you attain these results:

- Enabled NPIV on the Cisco MDS 9124 Switch.
- Configured the interfaces between the Cisco MDS 9124 Switch and the Cisco Nexus 5500 Platform Switch as F Ports.
- Associated the correct VSAN with the relevant interfaces.
- Confirmed that the hosts have successfully performed a FLOGI to the Cisco MDS 9124 Switch.
- Confirmed that the hosts and JBOD have successfully registered in the fabric.

Lab 5-1: Configure System Management

Complete this lab activity to practice what you learned in the related module.

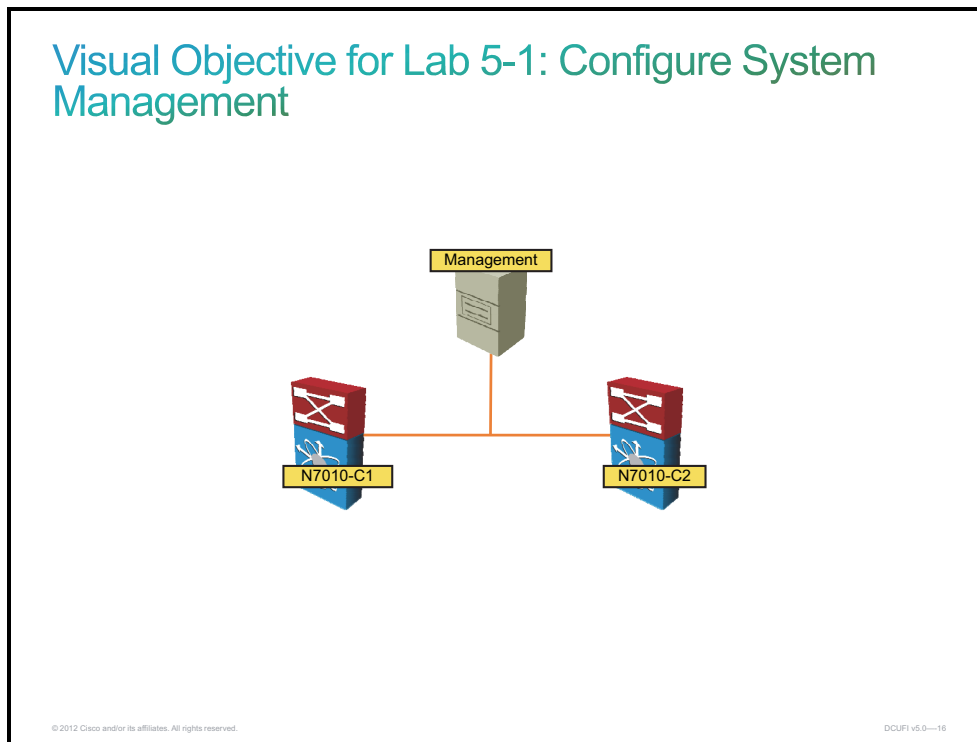
Activity Objective

In this activity, you will configure the system management features on the Cisco Nexus 7000 Series switch to support the implementation plan requirements. After completing this activity, you will be able to meet these objectives:

- Configure Cisco Fabric Services on the Cisco Nexus 7000 Series switch and verify the configuration
- Configure the scheduler to run a job periodically and on demand, and verify the job runs automatically when required
- Configure Cisco Smart Call Home to send an email message when an event occurs, and verify the configuration

Visual Objective

The figure illustrates what you will accomplish in this activity.



Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Job Aids at the beginning of the Lab Guide

Required Resources

These are the resources and equipment that are required in order to complete this activity:

- Two Cisco Nexus 7000 Series switch VDCs

Command List

The table describes the commands that are used in this activity.

Command	Description
cfs ipv4 mcast-address <group-address>	Changes the IP version 4 (IPv4) multicast address used for Cisco Fabric Services over IPv4
cfs ipv4 distribute	Enables Cisco Fabric Services distribution over IPv4
show cfs peers	Displays the active Cisco Fabric Services peers
cfs region <nr>	Creates a Cisco Fabric Services region
role	Assigns the role application to the Cisco Fabric Services region
radius	Assigns the RADIUS application to the Cisco Fabric Services region
show cfs regions	Displays the active Cisco Fabric Services regions
<application> distribute	Enables Cisco Fabric Services distribution for an application
role name <name>	Creates a user role
rule <nr> permit read feature <feature>	Creates a rule that grants read access for a specific feature
rule <nr> permit read-write feature <feature>	Creates a rule that grants read-write access for a specific feature
show role name <name>	Displays a specific user role on the switch
show <application> pending-diff	Displays the pending Cisco Fabric Services changes for an application
show cfs lock	Displays the Cisco Fabric Services locks in the fabric
<application> commit	Commits the pending changes for an application to the fabric
radius-server host <ip-address> key <key>	Configures a RADIUS server and key
show radius-server <ip-address>	Displays the RADIUS servers on the switch
show cli variables	Displays the Cisco NX-OS system and user-defined CLI variables
copy running-config bootflash: /<filename>	Copies the current running configuration to a file in bootflash
dir bootflash:	Lists the files in bootflash
feature scheduler	Enables the scheduler feature
scheduler job name <name>	Creates a scheduler job
scheduler schedule name <name>	Creates a schedule
job name <name>	Assigns a job to a schedule
time start +<time>	Sets the start time for a schedule as an offset to the current time
show scheduler schedule	Displays the configured schedules on the switch
show scheduler logfile	Displays the scheduler log

time weekly <day-and-time>	Sets a weekly recurring time for a schedule
callhome	Enters Cisco Smart Call Home configuration mode
email-contact <email-address>	Sets the email contact for Cisco Smart Call Home
phone-contact <phone-number>	Sets the contact phone number for Cisco Smart Call Home
streetaddress <address>	Sets the contact address for Cisco Smart Call Home
destination-profile <name> format <format>	Creates a Cisco Smart Call Home destination profile using XML, short text, or full text format
destination-profile <name> message-level <level>	Sets the Cisco Smart Call Home message level for a destination profile
destination-profile <name> alert-group <groups>	Sets the Cisco Smart Call Home alert groups for a destination profile
destination-profile <name> email-addr <email-address>	Sets the email address to send Cisco Smart Call Home messages to a destination profile
show callhome destination-profile profile <name>	Displays the operational parameters for a Cisco Smart Call Home destination profile
destination-profile <name> message-size <size>	Sets the maximum message size for a Cisco Smart Call Home destination profile
transport email smtp-server <ip-address> use-vrf <vrf>	Sets the IP address for the Simple Mail Transfer Protocol (SMTP) server that is used to send Cisco Smart Call Home messages
transport email from <email-address>	Sets the "from" email address used in Cisco Smart Call Home messages
transport email reply-to <email-address>	Sets the "reply-to" email address used in Cisco Smart Call Home messages
show callhome transport	Displays the transport settings for Cisco Smart Call Home messages
enable	Enables Cisco Smart Call Home
snmp-server contact <contact-name>	Sets the Simple Network Management Protocol (SNMP) sysContact name
callhome test	Generates a Cisco Smart Call Home message for testing purposes

Task 1: Configure Cisco Fabric Services

During this task, you will configure Cisco Fabric Services on the Cisco Nexus 7000 Series switch VDC in your pod.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.
- Step 2** Change the multicast address used for Cisco Fabric Services over IPv4 according to the following table:

Device	Cisco Fabric Services Multicast Address
N7K-1- pod1	239.255.12.12
N7K-2- pod2	239.255.12.12
N7K-1- pod3	239.255.34.34
N7K-2- pod4	239.255.34.34

```
N7KX-podP(config)# cfs ipv4 mcast-address 239.255.YZ.YZ
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
N7KX-podP(config)#
```

- Step 3** Enable Cisco Fabric Services distribution over IPv4 on your Cisco Nexus 7000 Series switch VDC.

```
N7KX-podP(config)# cfs ipv4 distribute
```

- Step 4** Examine the Cisco Fabric Services peers that were discovered.

```
N7KX-podP#sh cfs peers
```

Physical Fabric

```
-----
Switch WWN                IP Address
-----
20:00:00:26:51:c9:78:c3 192.168.10.9P [Local]
20:00:6c:9c:ed:46:52:c3 192.168.10.9Q
```

```
Total number of entries = 2
```

Note Do not continue on to the next step until this command lists exactly two entries—your own Cisco Nexus 7000 Series switch VDC and your peer pod Cisco Nexus 7000 Series switch VDC. Each pair of peer pods uses a unique multicast address to separate them from other pairs of peer pods within the same lab. In this lab task, you will be working very closely with your peer pod, and it is important that you progress through the lab at the same pace.

Step 5 Define a Cisco Fabric Services region on your Cisco Nexus 7000 Series switch VDC according to the following table.

Device	Cisco Fabric Services Region
N7K-1-pod1	12
N7K-2-pod2	12
N7K-1-pod3	34
N7K-2-pod4	34

```
N7KX-podP(config)# cfs region YZ
```

Step 6 Add the applications “role” and “radius” to the Cisco Fabric Services region.

```
N7KX-podP(config-cfs-region)# role
```

```
WARNING: If an Application is moved/assigned to a new region,
its scope is restricted to that region and it ignores all other regions
for distribution or merge.
Are you sure? (y/n) [n] y
```

```
N7KX-podP(config-cfs-region)# radius
```

```
WARNING: If an Application is moved/assigned to a new region,
its scope is restricted to that region and it ignores all other regions
for distribution or merge.
Are you sure? (y/n) [n] y
```

Step 7 Examine the Cisco Fabric Services region you have created.

```
N7KX-podP# show cfs regions
```

Note	Even though the applications have been assigned to the region, they have not been activated for Cisco Fabric Services distribution yet. Therefore, they do not show up in the output of the show cfs regions command.
-------------	--

Step 8 Enable Cisco Fabric Services distribution for the applications “role” and “radius.”

```
N7KX-podP(config)# role distribute
```

```
N7KX-podP(config)# radius distribute
```

Step 9 Reexamine the Cisco Fabric Services region.

```
N7KX-podP# sh cfs regions
```

```
Region-ID : XY
```

```
Application: role
```

```
Scope : Physical-fc-ip
```

```
-----
Switch WWN                IP Address
-----
20:00:00:26:51:c9:78:c3 192.168.10.9P [Local]
20:00:6c:9c:ed:46:52:c3 192.168.10.9Q
```

```
Total number of entries = 2
```

```

Region-ID   : XY
Application: radius
Scope       : Physical-fc-ip
-----
Switch WWN          IP Address
-----
20:00:00:26:51:c9:78:c3 192.168.10.9P [Local]
20:00:6c:9c:ed:46:52:c3 192.168.10.9Q

```

Total number of entries = 2

Step 10 Define a user role named TIER-2-OPS. This can result in two possible outcomes.

First possible result:

```
N7KX-podP(config)# role name TIER-2-OPS
```

Second possible result:

```

N7KX-podP(config)# role name TIER-2-OPS
ERROR: Operation failed. Fabric is already locked

```

Note	The outcome of this command depends on who enters the role command first. Cisco Fabric Services locks the fabric for the application as soon as you start configuring it. Other switches cannot make changes as long as the lock remains.
-------------	--

Step 11 If you got the first result on the previous step, continue on to the next step. If however you get the second result in the previous step, skip the next series of steps and continue at Step 22.

Step 12 Add a rule to the role TIER-2-OPS that adds read access to the role for all features.

```
N7KX-podP(config-role)# rule 1 permit read
```

Step 13 Add three more rules to add read-write rights for the “diagnostics,” “ping,” and “vlan” features.

```

N7KX-podP(config-role)# rule 2 permit read-write feature diagnostics
N7KX-podP(config-role)# rule 3 permit read-write feature ping
N7KX-podP(config-role)# rule 4 permit read-write feature vlan

```

Step 14 Examine the role TIER-2-OPS.

```
N7KX-podP# show role name TIER-2-OPS
```

```

      ^
% Invalid command at '^' marker.

```

Step 15 Determine why you get an error message.

Step 16 Examine the pending Cisco Fabric Services changes for the “role” application.

```

N7KX-podP# show role pending-diff
+Role: TIER-2-OPS
+ Description: new role
+ Vlan policy: permit (default)
+ Interface policy: permit (default)
+ Vrf policy: permit (default)
+ -----
+ Rule      Perm    Type      Scope      Entity
+ -----
+ 4          permit  read-write feature    vlan
+ 3          permit  read-write feature    ping
+ 2          permit  read-write feature    diagnostics
+ 1          permit  read

```

Step 17 Examine the Cisco Fabric Services locks for the fabric.

N7KX-podP# **show cfs lock**

Application: role
Scope : Physical-fc-ip

Switch WWN	IP Address	User Name	User Type
20:00:00:26:51:c9:78:c3	192.168.10.9P	admin	CLI/SNMP v3

Total number of entries = 1

Note Depending on the step that your peer pod is at during the exercise, you may also see a lock for the “radius” application. Allow some time for peers to establish communication.

Step 18 Commit the pending Cisco Fabric Services changes for the “role” application to the fabric.

N7KX-podP(config)# **role commit**

Step 19 Examine the role TIER-2-OPS again.

N7KX-podP# **show role name TIER-2-OPS**

Role: TIER-2-OPS
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)

Rule	Perm	Type	Scope	Entity
4	permit	read-write	feature	vlan
3	permit	read-write	feature	ping
2	permit	read-write	feature	diagnostics
1	permit	read		

Step 20 Ask your lab partners in the peer pod to execute the **show role name TIER-2-OPS** command on their Cisco Nexus 7000 Series switch VDCs. Determine if they see the newly created role in their VDCs.

Step 21 Skip the next series of steps and continue at Step 32.

Step 22 Examine the Cisco Fabric Services locks for the fabric.

N7KX-podP(config)# **show cfs lock**

Application: role
Scope : Physical-fc-ip

Switch WWN	IP Address	User Name	User Type
20:00:6c:9c:ed:46:52:c3	192.168.10.9Q	admin	CLI/SNMP v3

Total number of entries = 1

Note You cannot configure anything for the “role” application until your peer pod releases the lock by committing or aborting the configuration. Your output may be different.

Step 23 Configure a RADIUS server with the IP address 192.168.0.**P**1, where **P** is your pod number. Configure **Se3cr3t-K3y** as the RADIUS server key.

```
N7KX-podP(config)# radius-server host 192.168.10.P1 key S3cr3t-K3y
```

Step 24 Add a second RADIUS server with the IP address 192.168.0.**Q**1, where **Q** is your peer pod number. Again, configure **S3cr3t-K3y** as the RADIUS server key.

```
N7KX-podP(config)# radius-server host 192.168.10.Q1 key S3cr3t-K3y
```

Step 25 Examine the RADIUS servers that you configured.

```
N7KX-podP# show radius-server 192.168.10.P1
RADIUS server not found
N7KX-podP# show radius-server 192.168.10.Q1
RADIUS server not found
```

Step 26 Determine why you do not see the configured RADIUS servers.

Step 27 Examine the pending Cisco Fabric Services changes for the “radius” application.

```
N7KX-podP# show radius pending-diff
+radius-server host 192.168.0.P1 authentication accounting
+radius-server host 192.168.0.Q1 authentication accounting
```

Step 28 Examine the Cisco Fabric Services locks for the fabric.

```
N7KX-podP# show cfs lock

Application: radius
Scope      : Physical-fc-ip
-----
--
Switch WWN          IP Address          User Name      User Type
-----
--
20:00:00:26:51:c9:78:c3 192.168.10.9P      admin          CLI/SNMP v3

Total number of entries = 1
```

Note Depending on the step that your peer pod is at during the exercise, you may also see a lock for the “role” application.

Step 29 Commit the pending Cisco Fabric Services changes for the “radius” application to the fabric.

```
N7KX-podP(config)# radius commit
```

Step 30 Examine the RADIUS servers again.

```
N7KX-podP# show radius-server
retransmission count:1
timeout value:5
deadtime value:0
source interface:any available
total number of servers:2

following RADIUS servers are configured:
192.168.10.P1:
    available for authentication on port:1812
    available for accounting on port:1813
    RADIUS shared secret:*****
192.168.10.Q1:
    available for authentication on port:1812
    available for accounting on port:1813
    RADIUS shared secret:*****
```

- Step 31** Ask your lab partners in the peer pod to execute the **show radius-server** command on their Cisco Nexus 7000 Series switch VDCs. Determine if they see the newly created RADIUS servers in their VDCs. Determine if the RADIUS secret keys also exchanged through Cisco Fabric Services.

Caution The RADIUS server information is exchanged through Cisco Fabric Services, but the RADIUS server keys are not included. The global **radius-server key** command can be used to set a default key for all RADIUS servers.

- Step 32** Verify with your peer pod that you see the role and RADIUS servers that were distributed through Cisco Fabric Services in this exercise in both Cisco Nexus 7000 Series switch VDCs before moving on to the next task.

Activity Verification

You have completed this task when you attain these results:

- You have enabled Cisco Fabric Services distribution using IPv4 and configured a Cisco Fabric Services region and IPv4 multicast group.
- You have created a new role, distributed the role configuration through Cisco Fabric Services between your pod and peer pod VDCs, and verified the operation of Cisco Fabric Services.
- You have configured two RADIUS servers, distributed the RADIUS configuration through Cisco Fabric Services between your pod and peer pod VDCs, and verified the operation of Cisco Fabric Services.

Task 2: Configure the Scheduler

During this task, you will configure the Cisco NX-OS scheduler on the Cisco Nexus 7000 Series switch VDCs in your pod.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC.
- Step 2** Examine the default CLI variables that are available on your VDC.

```
N7KX-podP(config)# show cli variables
VSH Variable List (* = session vars)
-----
SWITCHNAME="N7KX-podP"
TIMESTAMP="2012-06-20-15.22.50"
```

- Step 3** Copy the running configuration to a file in bootflash on the supervisor module that uses the SWITCHNAME and TIMESTAMP variables to create the filename. Use “\$(SWITCHNAME)-\$(TIMESTAMP).cfg” as the name for the file in bootflash.

```
N7KX-podP# copy running-config bootflash:/${SWITCHNAME}-${TIMESTAMP}.cfg
Copy complete, now saving to disk (please wait)...
```

- Step 4** List the files in bootflash in order to verify that the file has been created with the correct hostname and timestamp.

```
N7KX-podP# dir bootflash: | i N7K
2182 Jun 20 15:24:32 2012 N7KX-podP-2012-06-20-15.24.31.cfg
```

Step 5 Enable the scheduler feature.

```
N7KX-podP(config)# feature scheduler
```

Create a scheduler job named BACKUP-CONFIG and copy the running configuration to bootflash using “\$(SWITCHNAME)-\$(TIMESTAMP).cfg” as the filename.

```
N7KX-podP(config)# scheduler job name BACKUP-CONFIG
N7KX-podP(config-job)# copy running-config bootflash:/${SWITCHNAME}-
$(TIMESTAMP).cfg
N7KX-podP(config-job)# exit
```

Step 6 Create a schedule named TEST-BACKUP that runs the job BACKUP-CONFIG once, starting one minute after you configure the schedule.

```
N7KX-podP(config)# scheduler schedule name TEST-BACKUP
N7KX-podP(config-schedule)# job name BACKUP-CONFIG
N7KX-podP(config-schedule)# time start +1
```

Step 7 Examine the schedule.

```
N7KX-podP# show scheduler schedule
Schedule Name      : TEST-BACKUP
-----
User Name          : admin
Schedule Type       : Run once on Mon Jul 23 14:14:00 2012
Last Execution Time : Yet to be executed
-----
Job Name            Last Execution Status
-----
BACKUP-CONFIG       -NA-
=====
```

Step 8 After a moment, examine the schedule again.

```
N7KX-podP# show scheduler schedule
Schedule Name      : TEST-BACKUP
-----
User Name          : admin
Schedule Type       : Run once on Mon Jul 23 14:14:00 2012
Last Execution Time : Mon Jul 23 14:14:00 2012
Last Completion Time: Mon Jul 23 14:14:04 2012
Execution count     : 1
-----
Job Name            Last Execution Status
-----
BACKUP-CONFIG       Success (0)
=====
```

Step 9 Determine if the backup job succeeded.

Step 10 Examine the scheduler log.

```
N7KX-podP# show scheduler logfile
=====
Job Name           : BACKUP-CONFIG                      Job Status: Success (0)
Schedule Name      : TEST-BACKUP                        User Name : admin
Completion time: Mon Jul 23 14:14:04 2012
----- Job Output -----
`copy running-config bootflash:/N7KX-podP-2012-06-23-14.14.00.cfg`
Copy complete, now saving to disk (please wait)...
`end`
=====
```

- Step 11** Remove the schedule TEST-BACKUP and create a new schedule named WEEKLY-BACKUP, which runs the job BACKUP-CONFIG every Sunday at 10:00 p.m. (2200).

```
N7KX-podP(config)# no scheduler schedule name TEST-BACKUP
N7KX-podP(config)# scheduler schedule name WEEKLY-BACKUP
N7KX-podP(config-schedule)# job name BACKUP-CONFIG
N7KX-podP(config-schedule)# time weekly 1:22:00
```

- Step 12** Examine the WEEKLY-BACKUP schedule.

```
N7KX-podP# show scheduler schedule name WEEKLY-BACKUP
Schedule Name       : WEEKLY-BACKUP
-----
User Name           : admin
Schedule Type       : Run on every Sunday at 22 Hrs 0 Mins
Last Execution Time : Yet to be executed
-----
Job Name             Last Execution Status
-----
BACKUP-CONFIG        -NA-
=====
```

Activity Verification

You have completed this task when you attain these results:

- You have created a manual backup of the configuration using the system CLI variables in bootflash.
- You have created a scheduler job that creates a backup of the running configuration in bootflash and successfully run the scheduler job as a one-time job.
- You have configured a weekly backup schedule for the backup scheduler job.

Task 3: Configure Cisco Smart Call Home

During this task, you will configure the Cisco Smart Call Home feature on the Cisco Nexus 7000 Series switch VDC in your pod.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC. For IP address and user credentials, consult the Job Aids at the beginning of the Lab Guide.
- Step 2** Enter Cisco Smart Call Home configuration mode and specify customer information according to the following table:

Parameter	Value
Email contact	podP-admin@example.net, where P is your pod number
Phone contact	+1-555-012-3456
Street address	123 Main Street, Sometown, USA

```
N7KX-podP(config)# callhome
N7KX-podP(config-callhome)# email-contact podP-admin@example.net
N7KX-podP(config-callhome)# phone-contact +1-555-012-3456
N7KX-podP(config-callhome)# streetaddress 123 Main Street, Sometown, USA
```

Step 3 Verify the operational Cisco Smart Call Home parameters.

```
N7KX-podP# show callhome
callhome disabled
Callhome Information:
contact person name(sysContact):
contact person's email:podP-admin@example.net
contact person's phone number:+1-555-012-3456
street addr:123 Main Street, Sometown, USA
site id:
customer id:
contract id:
switch priority:7
duplicate message throttling : enabled
periodic inventory : enabled
periodic inventory time-period : 7 days
periodic inventory timeofday : 08:00 (HH:MM)
Distribution : Disabled
```

Step 4 Create a destination profile named NEXUS-LAB by using the information in the following table.

Parameter	Value
Profile name	NEXUS-LAB
Message format	Full text
Message level	2
Alert group	All
Destination email address	podP@cisco.com, where P is your pod number

```
N7KX-podP(config)# callhome
N7KX-podP(config-callhome)# destination-profile NEXUS-OPS format full-txt
N7KX-podP(config-callhome)# destination-profile NEXUS-OPS message-level 2
N7KX-podP(config-callhome)# destination-profile NEXUS-OPS alert-group all
N7KX-podP(config-callhome)# destination-profile NEXUS-OPS email-addr
podP@cisco.com
```

Step 5 Examine the Cisco Smart Call Home destination profile NEXUS-LAB.

```
N7KX-podP# show callhome destination-profile profile NEXUS-OPS
NEXUS-OPS destination profile information
maximum message size:2500000
message format:full-txt
message-level:2
transport-method:email
email addresses configured:
podP@cisco.com

url addresses configured:

alert groups configured:
all
```

Step 6 Configure two more destination profiles according to the following table.

Parameter	Value
Profile name	SMS
Message format	Short text
Message level	6
Message size	160 characters
Alert group	All
Destination email address	podP@cisco.com, where P is your pod number
Parameter	Value
Profile name	TICKETING-SYSTEM
Message format	XML
Message level	1
Alert group	All
Destination email address	podP@cisco.com, where P is your pod number

Note The three destination profiles represent three different uses of Cisco Smart Call Home. The NEXUS-OPS profile is used to send email to a group of network operators. The SMS profile is used to send high-priority messages to a select group of users via an email-to-SMS gateway. The TICKETING-SYSTEM profile is used to send messages to a ticketing system that can parse XML-based messages. Normally, each of these profiles would use a separate destination email address, but in this lab exercise, the same email address is used for all three profiles.

```
N7KX-podP(config)# callhome
N7KX-podP(config-callhome)# destination-profile SMS format short-txt
N7KX-podP(config-callhome)# destination-profile SMS message-level 6
N7KX-podP(config-callhome)# destination-profile SMS message-size 160
N7KX-podP(config-callhome)# destination-profile SMS alert-group all
N7KX-podP(config-callhome)# destination-profile SMS email-addr podP@cisco.com
N7KX-podP(config-callhome)# destination-profile TICKETING-SYSTEM format XML
N7KX-podP(config-callhome)# destination-profile TICKETING-SYSTEM message-level 1
N7KX-podP(config-callhome)# destination-profile TICKETING-SYSTEM alert-group all
N7KX-podP(config-callhome)# destination-profile TICKETING-SYSTEM email-addr podP@cisco.com
```

Step 7 Configure the global Cisco Smart Call Home email settings according to the following table.

Parameter	Value
SMTP server	192.168.10.10
VRF	Management
From email address	callhome@example.net
Reply-to email address	podP-admin@example.net, where P is your pod number

```
N7KX-podP(config-callhome)# transport email smtp-server 192.168.10.10 use-vrf management
N7KX-podP(config-callhome)# transport email from callhome@example.com
N7KX-podP(config-callhome)# transport email reply-to podP-admin@example.com
```

Step 8 Examine the Cisco Smart Call Home transport parameters.

```
N7KX-podP# show callhome transport
http vrf:default

from email addr:callhome@example.com
reply to email addr:podP-admin@example.com

smtp server:192.168.10.10
smtp server port:25
smtp server vrf:management
smtp server priority:0

http proxy server:
http proxy server port:
http proxy status:Disabled
```

Step 9 Enable Cisco Smart Call Home.

```
N7KX-podP(config)# callhome
N7KX-podP(config-callhome)# enable
sysContact is not configured
callhome can not be enabled on the switch,
because necessary configuration has not been done
Please check if all of following configuration is done
contact person name(sysContact)
contact person's email
contact person's phone number
street addr
To configure sysContact, please use snmp-server command
```

Note In addition to the Cisco Smart Call Home parameters, the Cisco Smart Call Home feature also requires the SNMP sysContact variable to be set.

Step 10 Configure the SNMP sysContact to be “Pod P Administrator,” where P is your pod number.

```
N7KX-podP(config)# snmp-server contact Pod P Administrator
```

Step 11 Enable Cisco Smart Call Home.

```
N7KX-podP(config)# callhome
N7KX-podP(config-callhome)# enable
```

Step 12 Generate test messages to verify the operation of Cisco Smart Call Home.

```
N7KX-podP# callhome test
trying to send test callhome message
warning:no callhome message sent
The specified message level for destination profile: SMS is higher than the
level for alert Test(2)
The specified message level for destination profile: SMS is higher than the
level for alert Test(2)
no email address configured for destination profile:full_txt
The specified message level for destination profile: SMS is higher than the
level for alert Test(2)
no email address configured for destination profile:short_txt
The specified message level for destination profile: SMS is higher than the
level for alert Test(2)
no email address configured for destination profile:CiscoTAC-1
Error in transporting email message for TICKETING-SYSTEM
SMTPclient: Host:192.168.10.10:Invalid hostname or address for mailhost
Error in transporting email message for NEXUS-OPS
SMTPclient: Host:192.168.10.10:Invalid hostname or address for mailhost
```

Note	Cisco Smart Call Home messages will only be sent successfully for the profiles NEXUS-OPS and TICKETING-SYSTEM. No messages will be sent for the profile SMS, because the inventory message that is sent by the test has a lower level (2) than the configured Call Home level for the destination profile SMS (6). The other error messages are related to destination profiles that are predefined but not configured.
-------------	---

Activity Verification

You have completed this task when you attain these results:

- You have configured and tested Cisco Smart Call Home on your Cisco Nexus 7000 Series switch VDC.

Lab 5-2: Implement Cisco DCNM for LAN

Complete this lab activity to practice what you learned in the related module.

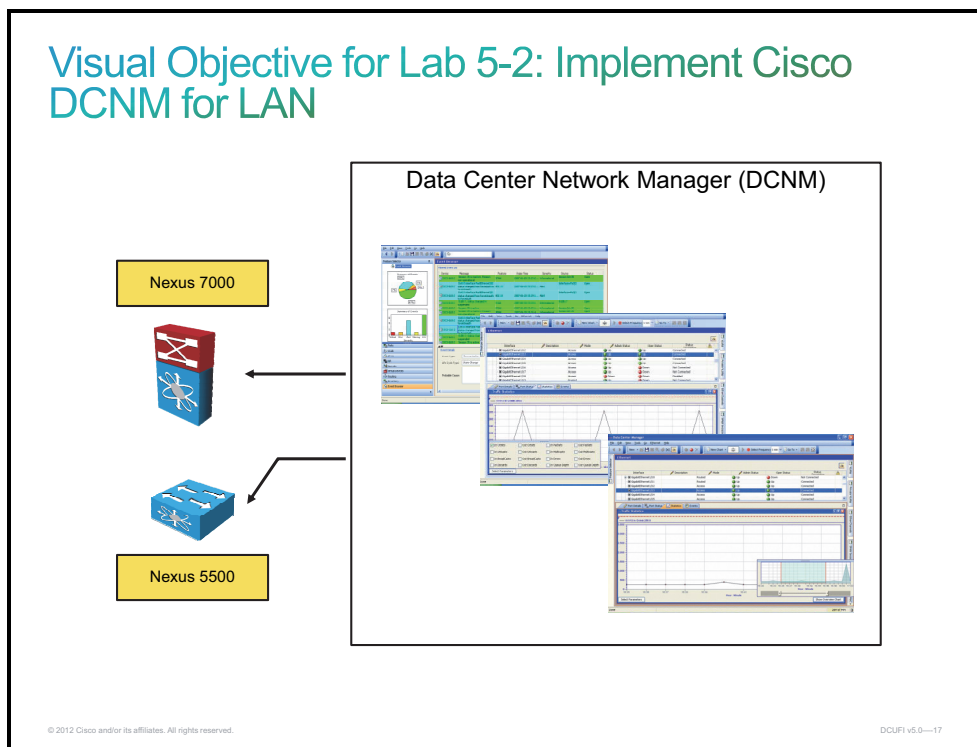
Activity Objective

In this activity, you will use Cisco DCNM for LAN to perform network discovery and network management of the Cisco Nexus product range. After completing this activity, you will be able to meet these objectives:

- Use Cisco DCNM to perform a network discovery of the network infrastructure
- Use Cisco DCNM to perform a platform inventory of the Cisco Nexus product range
- Use Cisco DCNM to monitor and manage the discovered network

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

- Cisco Nexus 7000 Series switch VDC
- Cisco Nexus 5500 Platform switch
- DCNM server

Command List

The table describes the commands that are used in this activity.

NX-OS Commands

Command	Description
<code>show cdp neighbors</code>	Displays the list of Cisco Discovery Protocol neighbors
<code>show diff rollback-patch startup-config running-config</code>	Displays the differences between the running configuration and startup configuration
<code>show vlan id <vlan-id></code>	Displays the properties of a specific VLAN
<code>show running-config interface <intf></code>	Displays the running configuration for a specific interface
<code>show startup-config vlan</code>	Displays the startup configuration for a specific VLAN
<code>show logging last <nr></code>	Displays the last number of lines in the system log file
<code>show running-config vlan <vlan-id></code>	Displays the running configuration for a specific VLAN
<code>copy bootflash:<filename> running-config</code>	Merges the configuration in a file in bootflash with the current running configuration
<code>checkpoint <name></code>	Creates a configuration checkpoint

Job Aids

These job aids are available to help you complete the lab activity.

- Lab topology diagram
- Lab IP address plan

Task 1: Network Discovery

In this task, you will use Cisco DCNM for LAN to perform a network discovery of your Nexus 7000 Series switch VDC and your Nexus 5500 Platform switch.

Activity Procedure

Complete these steps:

- Step 1** Connect to your assigned Cisco Nexus 7000 Series switch VDC.
- Step 2** Configure the interface that connects your Cisco Nexus 7000 Series switch VDC to the peer pod Cisco Nexus 7000 Series switch VDC as a trunk and enable bridge assurance on the port. Refer to the Lab Connections job aid to determine the correct interface.
- ```
N7K-X-podP(config)# interface ethernet 1/ITA
N7K-X-podP(config-if)# switchport
N7K-X-podP(config-if)# switchport mode trunk
N7K-X-podP(config-if)# spanning-tree port type network
```
- Step 3** Ensure that the interfaces that connect your Cisco Nexus 7000 Series switch VDC to your Cisco Nexus 5500 Platform switch and to your peer pod Cisco Nexus 5000 Series Switch are enabled. Refer to the Lab Connections job aid to determine the correct interfaces.
- ```
N7K-X-podP(config)# interface ethernet 1/AA, ethernet 1/AB
N7K-X-podP(config-if-range)# no shutdown
```

Step 4 Use Cisco Discovery Protocol to verify that the links between the devices in your pod and the peer pod are operational.

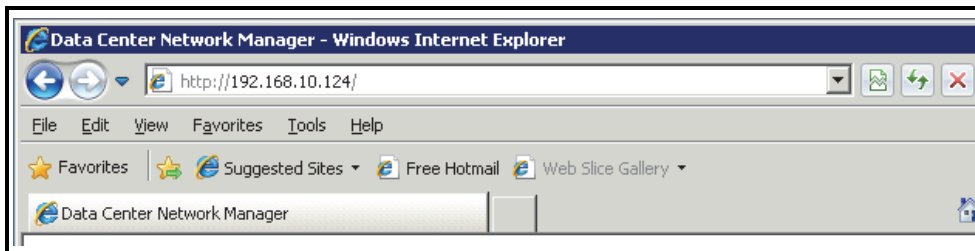
N7K-**X**-pod**P**# **show cdp neighbors**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

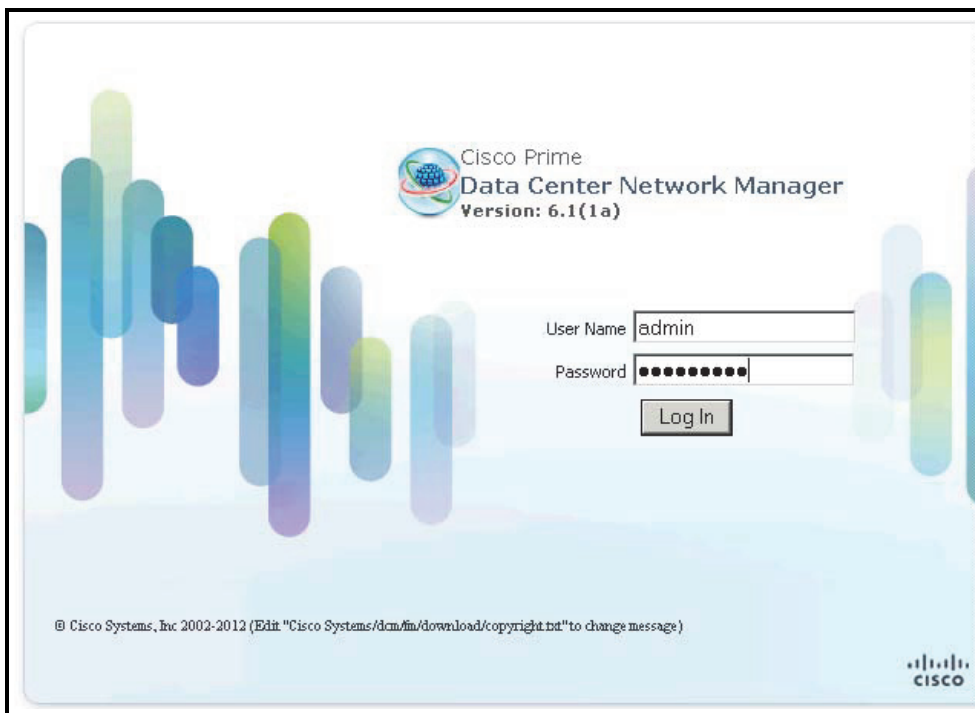
Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
N5K- P (SSI143207FZ)	Eth1/ AA	159	S I s		
N5K- Q (SSI14310363)	Eth1/ AB	146	S I s		
N7K- Y -pod Q (JAF1448AADT)	Eth1/ ITA	146	R S I s		

Note You should see three devices in the output of this command: your Cisco Nexus 5500 Platform switch, your peer pod Cisco Nexus 5500 Platform switch, and your peer pod Cisco Nexus 7000 Series switch VDC. If this is not the case, troubleshoot with your lab partners in the peer pod until all three connections are operational.

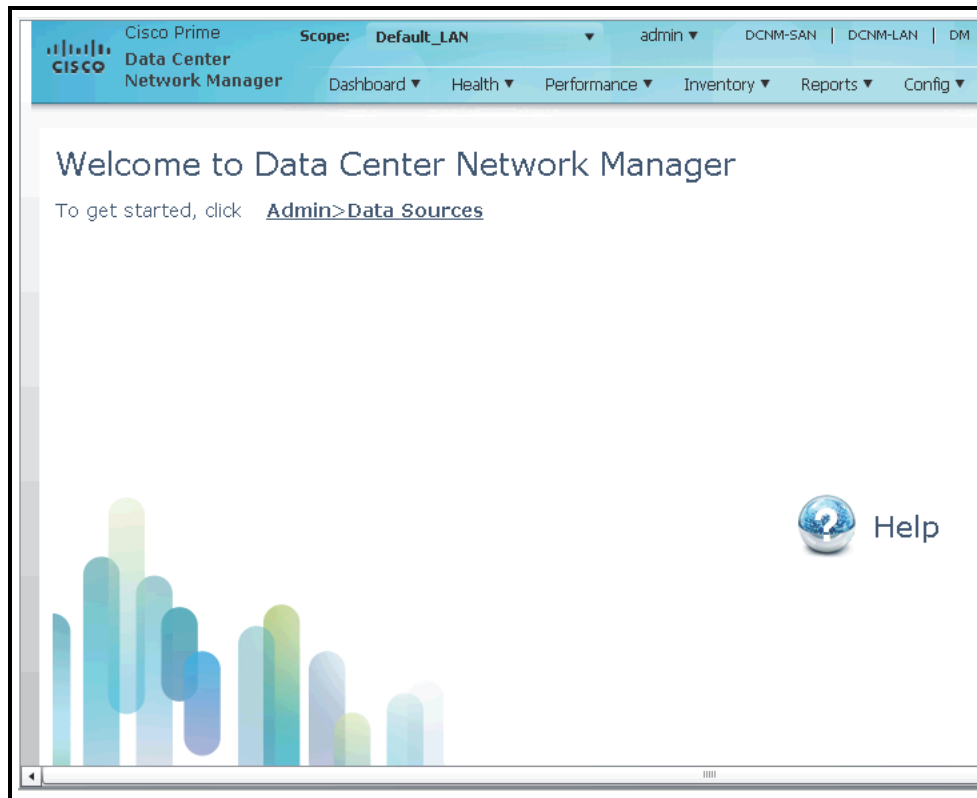
Step 5 Connect to the Cisco DCNM server by using a web browser and connecting to the following IP address: <http://192.168.10.12P>, where **P** represents your assigned pod number. In the example, pod 4 is used.



Step 6 Log in to the DCNM server.



Step 7 Wait for the application to open to the welcome screen.



Start adding network devices by clicking on the **Admin > Data Sources** link.

Step 8 Under **Admin > Data Sources > LAN**, click the “+” icon to add a data source.

Name	Switch	Manag	Discovery Status		Last Updated T	Group	SNMPv3	User	Auth/Pri	Max T
			SNMP	SSH/Telnet						

Start with adding your Cisco Nexus 7000 Series switch VDC. Fill in the required access information:

- Select zero hops from the seed switch.
- Enter the management IP address
- Select detailed discovery
- Enter the access credentials

Add LAN

Discovery Type: ☒ Hops from Seed Switch ☐ Switch List ☐ FWSM

Seed Switch: 192.168.10.98

Max Hops from Seed: 0 1 2 3 4 5 6 7

Protocol: ☐ Fast, Shallow (SNMPv1: No DCM-LAN Discovery) ☐ Fast (SNMPv3/CLI: No DCM-LAN Discovery. Edit task to select switches for DCM-LAN Discovery) ☒ Detailed (SNMPv3/CLI: Automatic DCM-LAN Discovery for all valid switches)

User Name: admin

Password: *****

Optional Enable Password:

Add Switches To Group: Default_LAN

Add **Close**

Wait for the discovery to finish.

Step 9 In the same way, add your pod Nexus 5500 Platform switch.

Add LAN

Discovery Type: ☒ Hops from Seed Switch ☐ Switch List ☐ FWSM

Seed Switch: 192.168.10.94

Max Hops from Seed: 0 1 2 3 4 5 6 7

Protocol: ☐ Fast, Shallow (SNMPv1: No DCM-LAN Discovery) ☐ Fast (SNMPv3/CLI: No DCM-LAN Discovery. Edit task to select switches for DCM-LAN Discovery) ☒ Detailed (SNMPv3/CLI: Automatic DCM-LAN Discovery for all valid switches)

User Name: admin

Password: *****

Optional Enable Password:

Add Switches To Group: Default_LAN

Add **Close**

Wait for discovery to finish.

Step 10 Return to the **Inventory** menu and click **Switches**. Select your Nexus 7000 Series switch VDC and explore the collected information.

Cisco Prime Data Center Network Manager

Scope: Default_LAN admin DCM-SAN | DCM-LAN |

Dashboard Health Performance Inventory Reports Conf

Inventory > Switches (1 items)

	Group	Name	IP Address	WWN/Chassis Id	#Ports
1	Default_LAN	N7K2-POD4	192.168.10.98	JAF1602BGDB	10

Review the collected information about the switch:

The screenshot shows the Cisco Prime Data Center Network Manager interface. On the left, a sidebar displays details for switch N7K2-POD4, including its IP address (192.168.10.98), group (Default_LAN), model (N7K-C7009), uptime (3 days, 00:14:54), serial number (JAF1602B8DB), version (6.0(1)), and status (Unlicensed). The main area shows a table of modules installed on the switch.

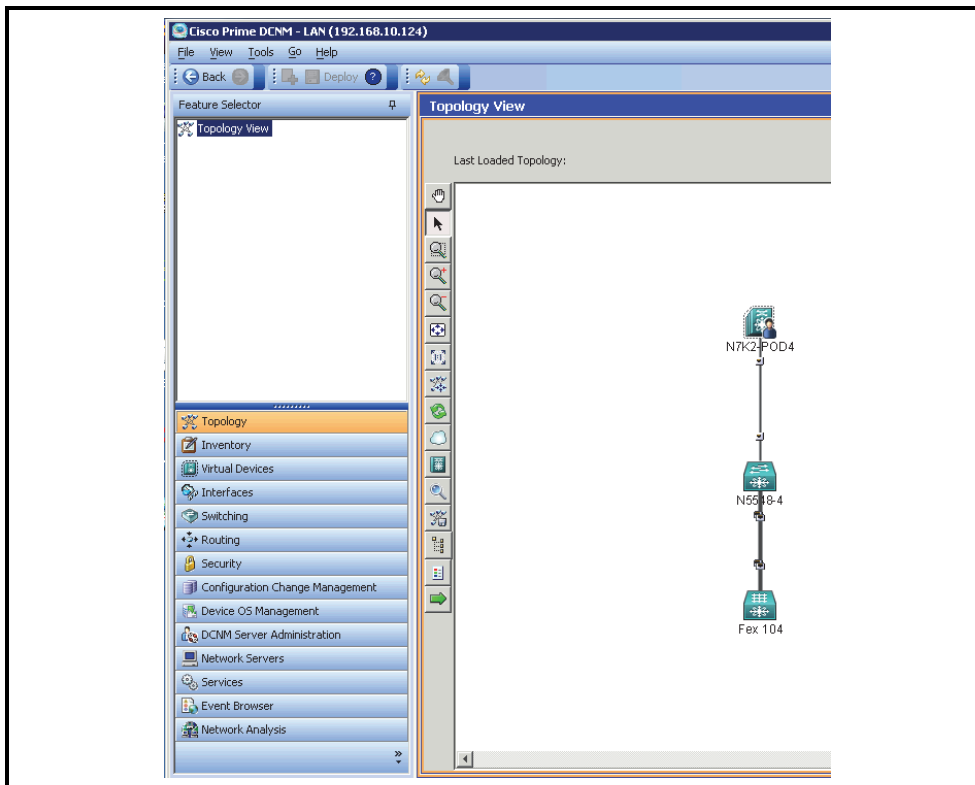
Name	ModelName	SerialNum	2nd SerialNum	Type	Slot	H/W...	S/W...	AssetID
PowerSupply-2	N7K-AC-6.0KW	AZS160300YP		powerSupply		3.0		341-02
Fan Module-1	N7K-C7009-FAN	JAF1607AFLH		fan		1.0		73-127
PowerSupply-1	N7K-AC-6.0KW	AZS160300YK		powerSupply		3.0		341-02
Nexus7000 C7009 (9)	N7K-C7009	JAF1602B8DB	JAF1606AABC	chassis		1.0		73-125
Supervisor module-1X	N7K-SUP1	JAF1610AMBN		module	1	2.3	6.0(1)	73-108
10/100/1000 Mbps Et	N7K-M148GT-11L	JAF1552BRKP		module	3	1.2	6.0(1)	73-128
1/10 Gbps Ethernet M	N7K-F132XP-15	JAF1601ARBB		module	4	1.2	6.0(1)	73-116
Fabric card module	N7K-C7009-FAB-2	JAF1609ACNN		module	10	2.0		73-127
Fabric card module	N7K-C7009-FAB-2	JAF1609AQED		module	11	2.0		73-127
Fabric card module	N7K-C7009-FAB-2	JAF1609ALSI		module	12	2.0		73-127
Fabric card module	N7K-C7009-FAB-2	JAF1609AQEG		module	13	2.0		73-127
Fabric card module	N7K-C7009-FAB-2	JAF1610AENA		module	14	2.0		73-127

Step 11 Start the Cisco DCNM for LAN application by clicking on the “DCNM-LAN” link on the top of the page:

The screenshot shows the Cisco Prime Data Center Network Manager - LAN login window. It includes fields for DCNM Server (192.168.10.124), Username (admin), and Password (masked with asterisks). A red message indicates the required JRE version is 1.6.0_29, and the detected version is 1.6.0_17. There are Login, Cancel, and More >> buttons at the bottom.

A new application window will then open.

- Step 12** On the left of your screen, select the **Topology** tab and examine the Topology View of your pod and peer pod. Rearrange the topology to your liking. When you are satisfied with the result, save the topology layout using the **Save Layout** button.



- Step 13** Move some devices in the layout, and then return to the saved layout by using the **Reload Layout** button.
- Step 14** Use the **Export as JPG** button to save the visible area of your topology to the desktop as a JPG picture named “Topology Diagram.jpg.”
- Step 15** Determine the significance of the puppet icon that is displayed on your Cisco Nexus 7000 Series switch.

Tip Use the **Legend** button to find out the meaning of the different types of icons in the topology view.

Step 16 Connect to your Cisco Nexus 7000 Series switch VDC.

Step 17 Examine the differences between the running configuration and the startup configuration that you saved in the previous lab.

```
N7K-X-podP# show diff rollback-patch startup-config running-config
Collecting Running-Config
Collecting Startup-Config
#Generating Rollback Patch
```

```
!!
!
logging level aaa 5
logging level cdp 6
logging level otm 5
logging level radius 5
logging level monitor 6
logging level port-security 5
logging level spanning-tree 6
!
interface Ethernet1/C
  no cdp enable
!
radius commit
```

Step 18 Determine any significant differences.

Note	During device discovery, if Cisco DCNM finds that a logging level on a discovered device is below the minimum logging-level requirement for that logging facility, Cisco DCNM raises the logging level in order to meet the minimum requirement. If logging levels meet or exceed the requirements, Cisco DCNM does not change the logging levels during discovery.
-------------	---

Step 19 Save the configurations on your Cisco Nexus 7000 Series switch VDC and Cisco Nexus 5000 Series switch.

Step 20 Go back to your Cisco DCNM client and spend some time examining the various options in the topology view of Cisco DCNM before moving on to the next task.

Activity Verification

You have completed this task when you attain these results:

- You have logged in to your assigned Cisco DCNM server by using the Cisco DCNM client.
- You have performed a device discovery using your Cisco Nexus 7000 Series switch VDC as the seed device.
- You have discovered the Cisco Nexus 7000 Series switch VDCs, the Cisco Nexus 5000 Series switches, and the Cisco Nexus 2000 Fabric Extenders in your pod and in your peer pod.
- You have examined the network map in the topology view of Cisco DCNM.

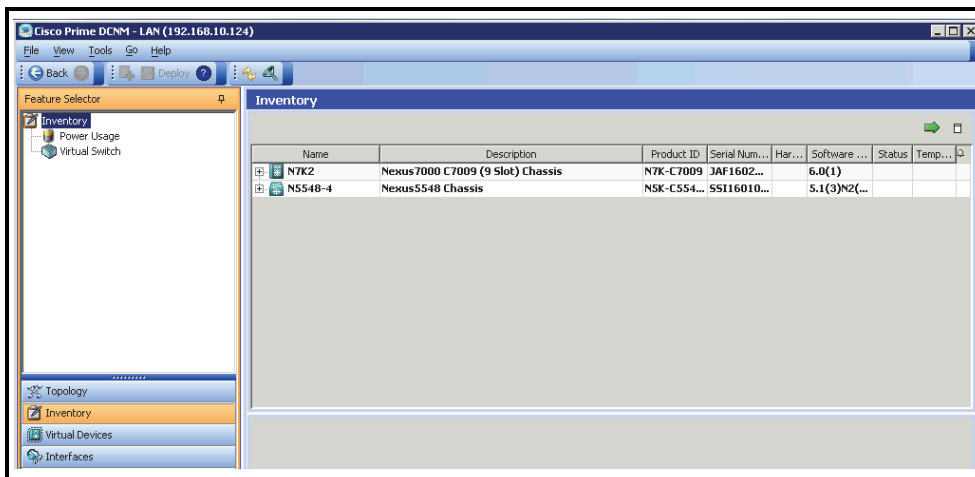
Task 2: Platform Inventory

In this task, you will use Cisco DCNM for LAN to perform a platform inventory of the Cisco Nexus product range.

Activity Procedure

Complete these steps:

- Step 21** Connect to your assigned Windows server and open the Cisco DCNM client for your Cisco DCNM server.
- Step 22** On the left of your screen, select the **Inventory** tab.



- Step 23** Open the inventory of your Cisco Nexus 7000 Series switch and your Cisco Nexus 5500 Platform switch and examine the components.

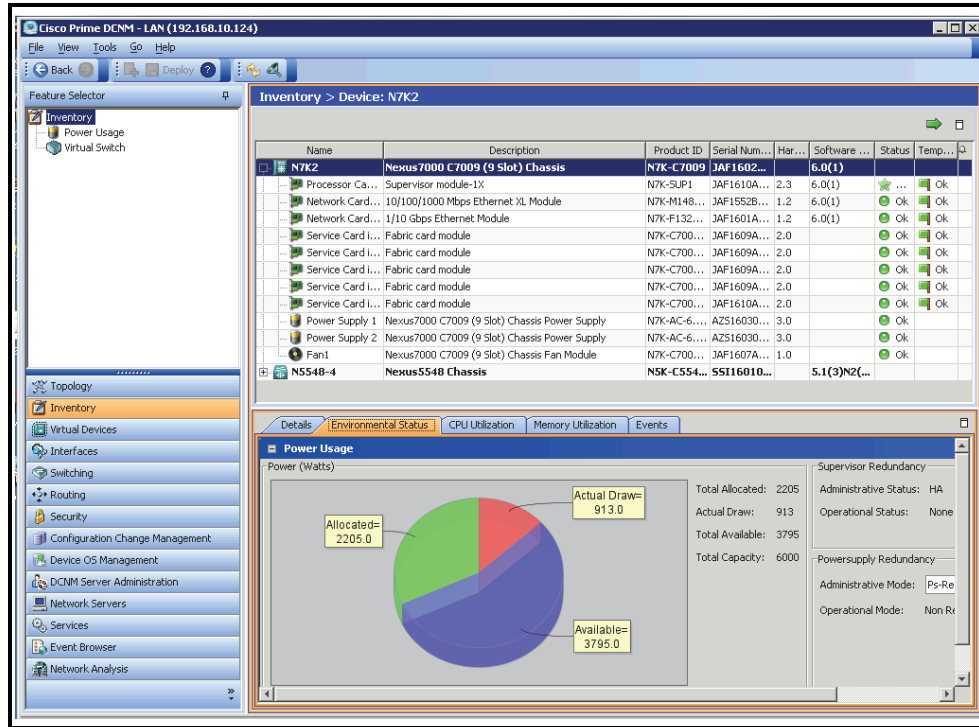
- Step 24** Determine how many fabric modules are installed in your assigned Cisco Nexus 7000 Series switch.

-
- Step 25** Determine how many power supplies are present in your Cisco Nexus 7000 Series switch. Determine the capacity of the power supplies and what the actual power draw of the switch is.

-
- Step 26** Determine where you can find the Cisco Nexus 2000 Fabric Extender in the inventory view and why it is displayed in this particular position.

-
- Step 27** Determine the product ID of the Fibre Channel module in your Cisco Nexus 5500 Platform switch in case you need to order a replacement.
-

Step 28 Go to the **Environmental Status** section of your assigned Cisco Nexus 7000 Series switch.

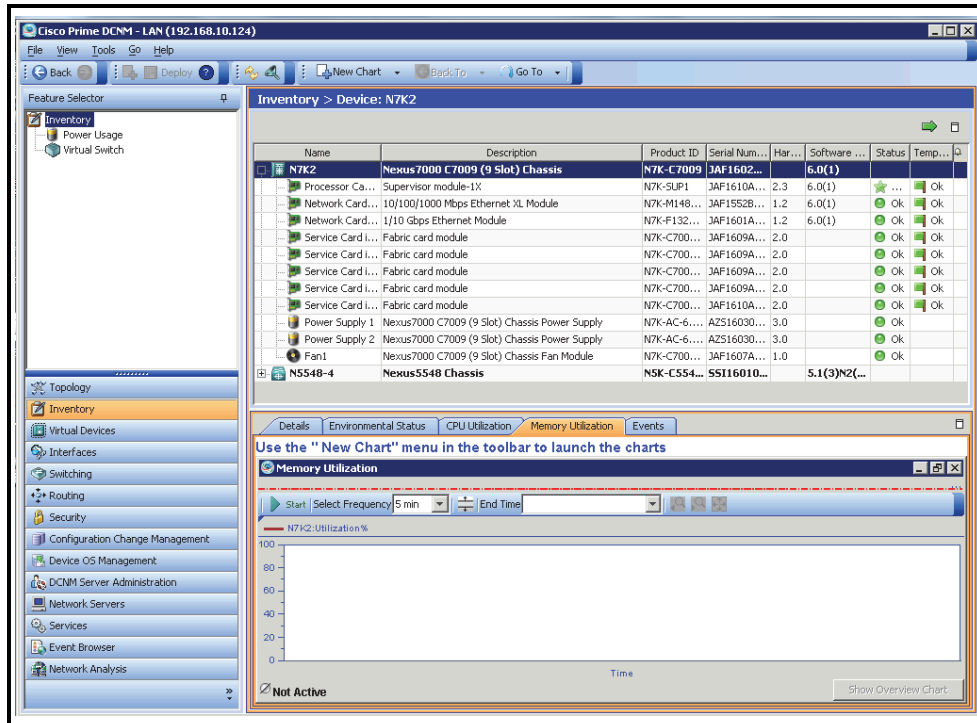


Step 29 Determine the administrative and operational power supply redundancy modes for the switch.

Step 30 Try to change the administrative power supply redundancy setting for the switch by selecting a different power supply redundancy mode and then selecting **Deploy** in the **File** menu.

Step 31 Determine if you succeeded in changing the power supply redundancy mode and why you could or could not change this setting.

Step 32 Go to the **Memory Utilization** tab of your assigned Cisco Nexus 7000 Series switch. Click **New Charts** in the toolbar and create a chart that graphs the memory utilization on the switch. Set the frequency to 30 seconds, and start the data collection for the chart. Wait for a few minutes in order to allow the chart to collect some data.



Step 33 Spend some time examining the various options in the inventory view of Cisco DCNM before moving on to the next task.

Activity Verification

You have completed this task when you attain these results:

- You have reviewed the hardware inventory of the devices in your pod and the peer pod.
- You have created a chart of the memory usage on your Cisco Nexus 7000 Series switch.

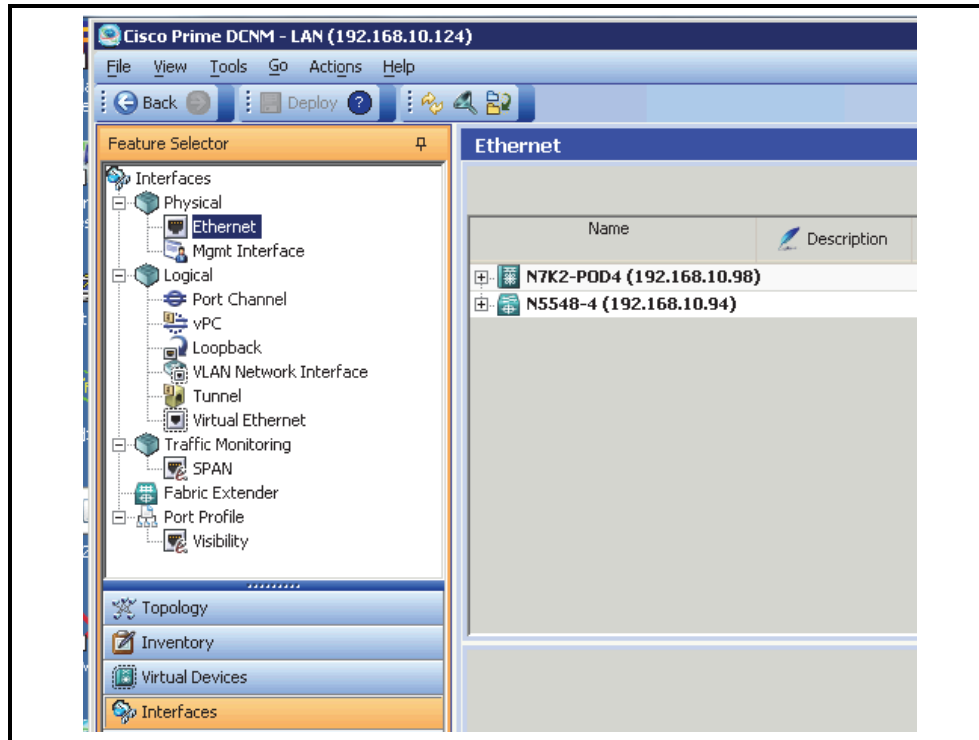
Task 3: Monitoring and Management

In this task, you will use Cisco DCNM for LAN to monitor and manage the discovered network.

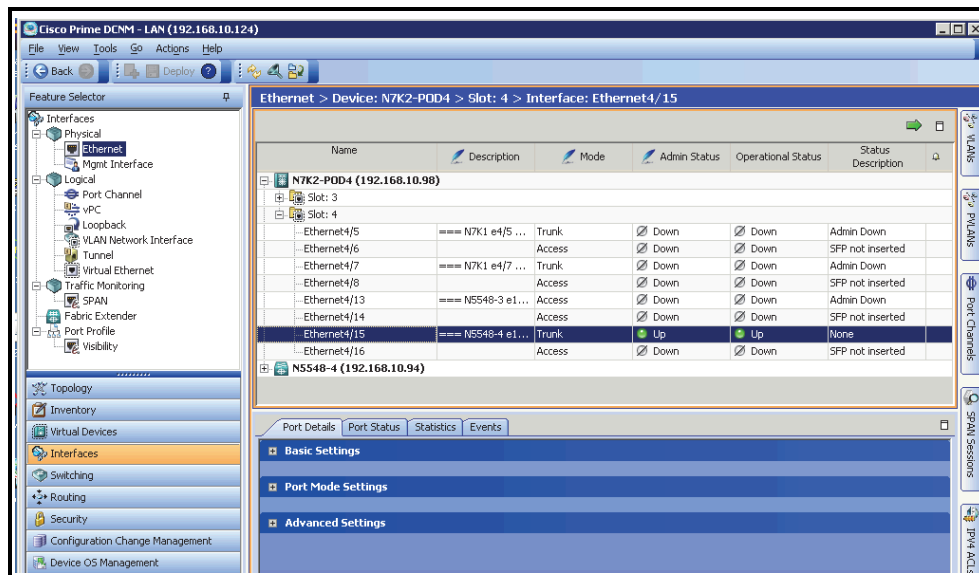
Activity Procedure

Complete these steps:

- Step 1** On the left of your screen, select the **Interfaces** tab. Select the item for the physical Ethernet interfaces within the tab.

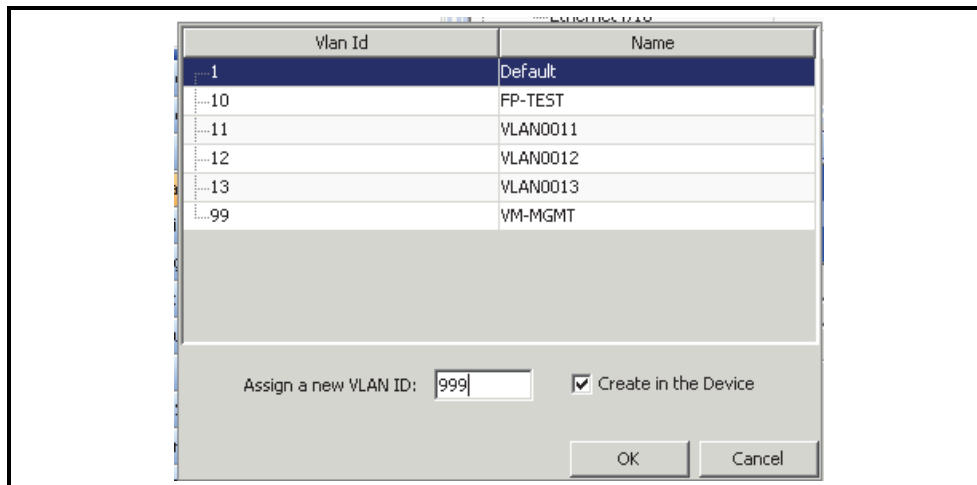
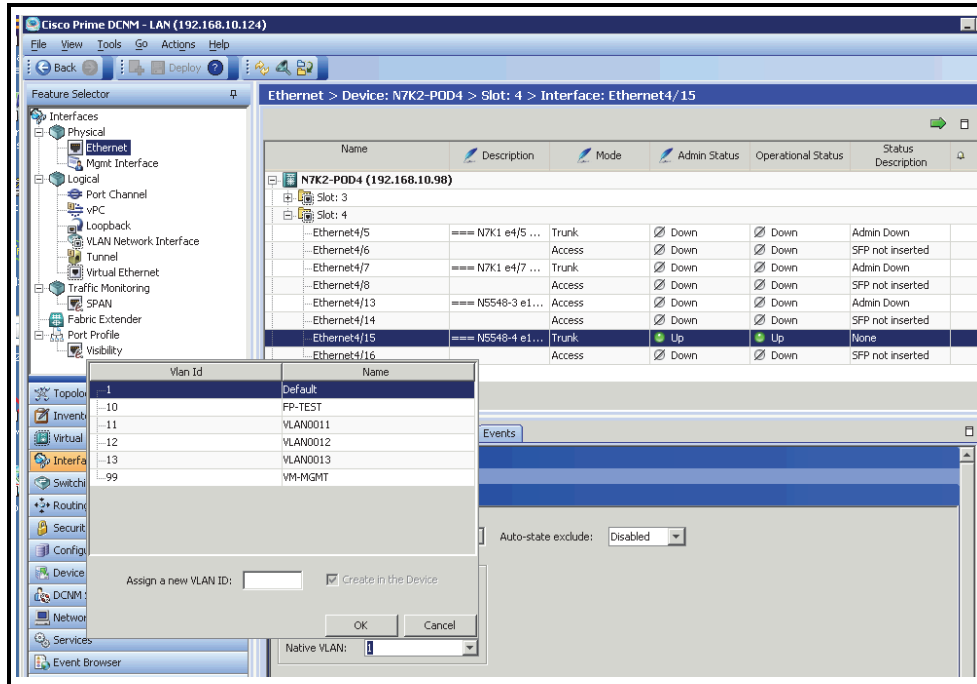


- Step 2** Select your Cisco Nexus 7000 Series switch VDC, and select the interface that connects your Cisco Nexus 7000 Series switch VDC to your Cisco Nexus 5000 Series switch. Refer to the Lab Connections job aid to find the correct interface.



Step 3 Examine the port details and status to determine which type of transceiver is plugged into this port.

Step 4 Go to the port mode settings. Create a new VLAN 999 and assign it as the native VLAN for the trunk. Do not leave the **Interfaces** tab to accomplish this task.



Step 5 Connect to your Cisco Nexus 7000 Series switch VDC.

Step 6 Verify that the new VLAN 999 exists and that the configuration for the port was changed.

N7K-**X**-pod**P**# **show vlan id 999**

VLAN	Name	Status	Ports
999	VLAN0999	active	Eth1/ AA , Eth1/ AB , Eth1/ ITA

VLAN Type	Vlan-mode
999	enet CE

Remote SPAN VLAN

Disabled

Primary	Secondary	Type	Ports
---	---	---	---

--

N7K-**X**-pod**P**# **show running-config interface ethernet 1/AA or AB**

!Command: show running-config interface Ethernet1/**AA or AB**
!Time: Tue Feb 22 14:42:10 2011

version 5.1(2)

```
interface Ethernet1/AA or AB
  switchport
  switchport mode trunk
  switchport trunk native vlan 999
  spanning-tree port type network
  storm-control broadcast level 40
  storm-control multicast level 40
  storm-control unicast level 40
  service-policy type qos input MARKING
  no shutdown
```

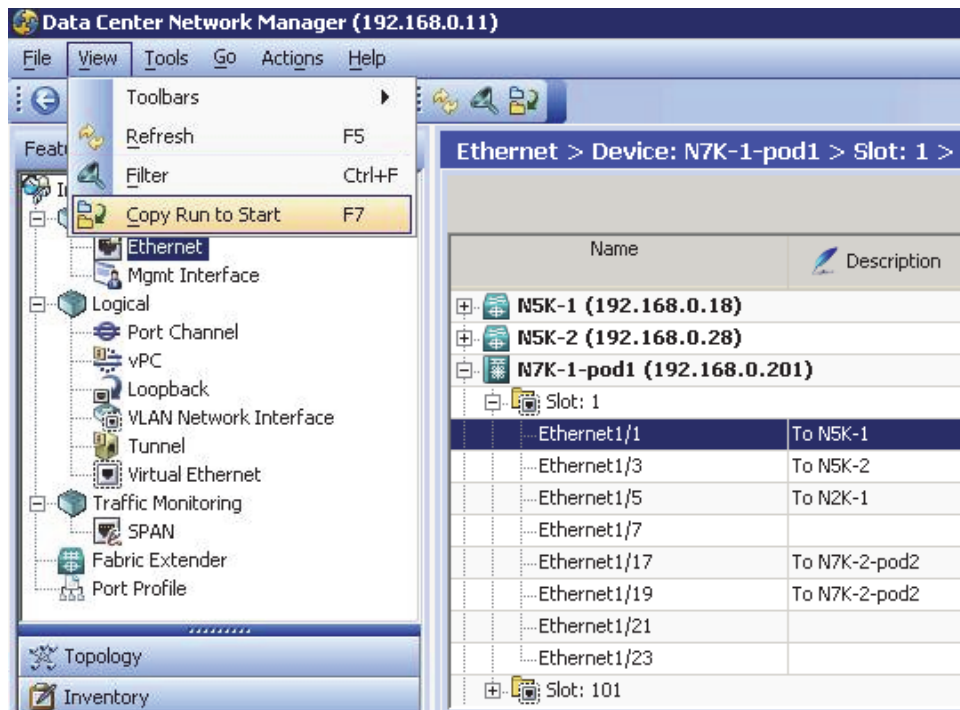
Step 7 Determine if the changed configuration was saved to the startup configuration automatically.

N7K-**X**-pod**P**# **show startup-config vlan**

!Command: show startup-config vlan
!Time: Tue Feb 22 14:52:41 2011
!Startup config saved at: Tue Feb 22 01:40:26 2011

```
version 5.1(2)
vlan configuration 1,10-13
vlan 1
vlan 10
  name TEST
vlan 11-13
```

- Step 8** Return to the Cisco DCNM client and use the option **Copy Run to Start** from the View menu in order to save the configuration.



- Step 9** Return to your Cisco Nexus 7000 Series switch VDC in order to verify that the configuration was saved.

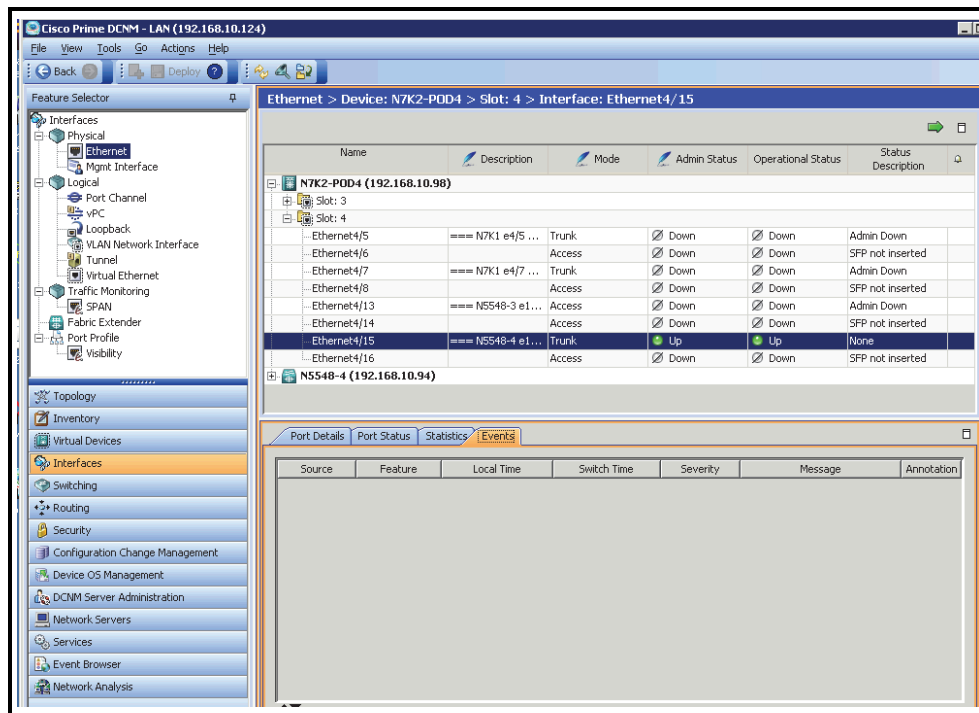
- Step 10** Try again, but make sure that you have selected your Cisco Nexus 7000 Series switch VDC in the View menu instead of the interface. Determine if the configuration is now saved.

```
N7K-X-podP# show startup-config vlan
```

```
!Command: show startup-config vlan
!Time: Tue Feb 22 15:08:49 2011
!Startup config saved at: Tue Feb 22 15:07:48 2011
```

```
version 5.1(2)
vlan configuration 1,10-13
vlan 1
vlan 10
    name TEST
vlan 11-13,999
```

- Step 11** Return to the Cisco DCNM client and select the interface that connects your VDC to your Cisco Nexus 5500 Platform switch once again. Select the **Events** tab for the interface and review the events.



- Step 12** Determine if you see any problems with the port.

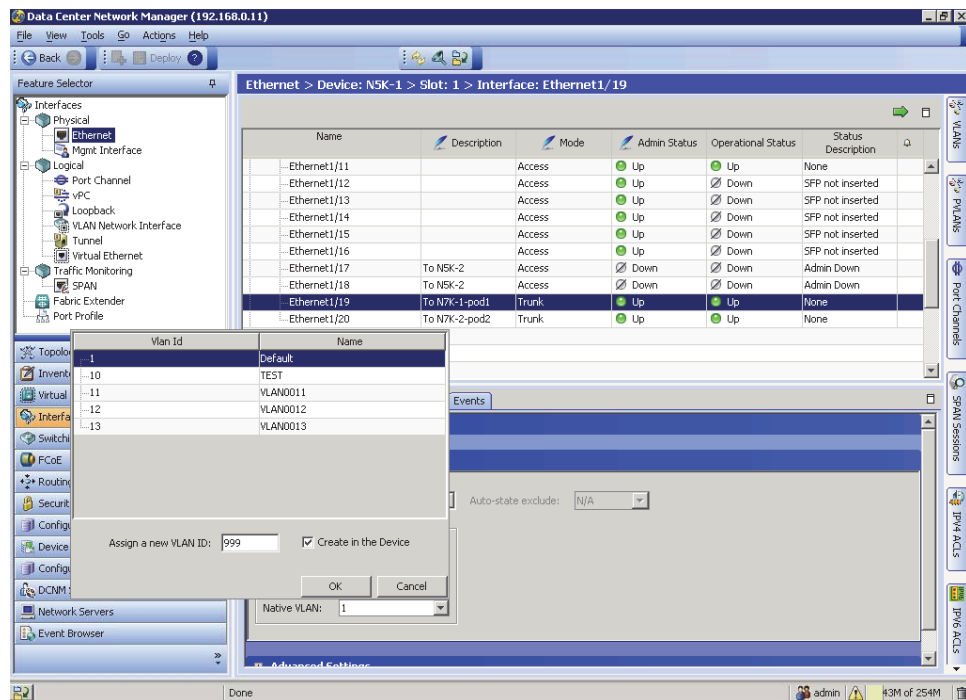
- Step 13** Return to your Cisco Nexus 7000 Series switch VDC and examine the log file.

N7K-X-podP# **show logging last 10**

```
2011 Feb 22 15:08:48 N7K-1-pod1 %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1(999), with Ethernet1/19(1)
2011 Feb 22 15:10:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:12:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:14:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:16:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:18:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:20:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:22:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:24:48 N7K-1-pod1 last message repeated 2 times
2011 Feb 22 15:26:48 N7K-1-pod1 last message repeated 2 times
```

- Step 14** Determine if there are any problems here.

- Step 15** Return to the Cisco DCNM client and change the native VLAN on your Cisco Nexus 5000 Series switch in order to match the value on the Cisco Nexus 7000 Series switch VDC for the link that connects the two devices.



- Step 16** Save the running configuration to the startup configuration for your Cisco Nexus 5000 Series switch by using DCNM.

- Step 17** Connect to your Cisco Nexus 5000 Series switch.

- Step 18** Verify that the changes were made and that the configuration was saved.

```
N5K-P# show running-config vlan 999
```

```
!Command: show running-config vlan 999
!Time: Tue Feb 22 10:40:05 2011
```

```
vlan 999
```

```
N5K-P# show running-config interface ethernet 1/AA or AB
```

```
!Command: show running-config interface Ethernet1/AA or AB
!Time: Tue Feb 22 10:40:22 2011
```

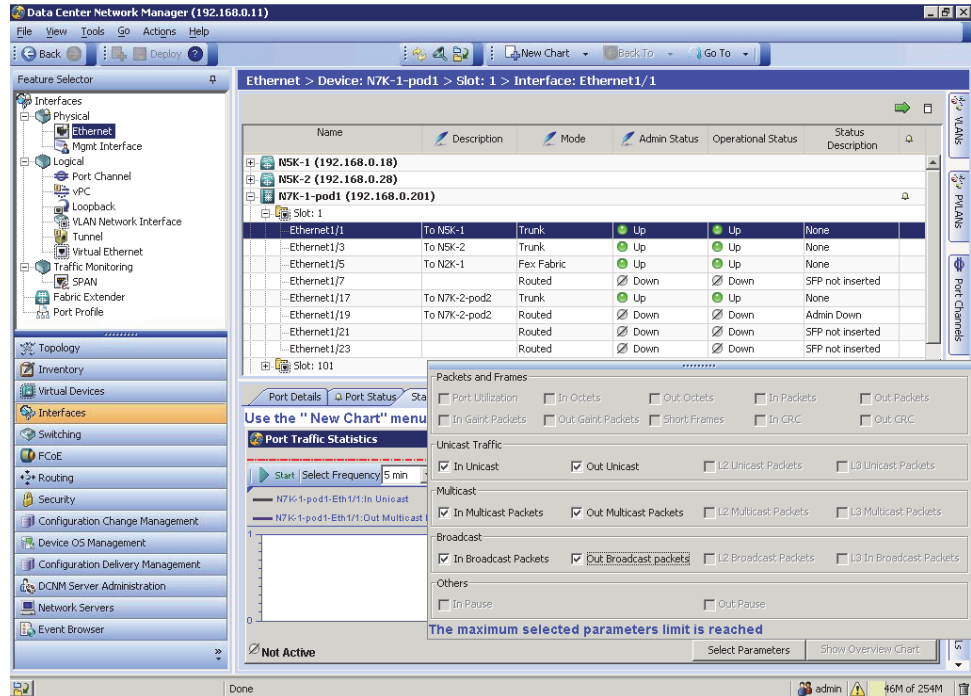
```
version 5.0(2)N1(1)
```

```
interface Ethernet1/AA or AB
  switchport mode trunk
  switchport trunk native vlan 999
  spanning-tree port type network
```

```
N5K-P# show startup-config | include vlan
```

```
feature interface-vlan
logging level interface-vlan 5
vlan 1
vlan 10
vlan 11-13,999
  instance 1 vlan 11,13
  instance 2 vlan 10,12
  switchport access vlan 10
  switchport trunk native vlan 999
```

- Step 19** Return to the Cisco DCNM client and select the interface on your Cisco Nexus 7000 Series switch VDC that connects to your Cisco 5000 Series switch. Go to the **Statistics** tab for the interface, and create a chart that graphs unicast, multicast, and broadcast ingress and egress traffic.



- Step 20** Determine the maximum number of parameters that can be graphed in a single chart.

- Step 21** Configure the chart to collect data every 30 seconds, and let it run for a couple of minutes in order to collect some statistics.

- Step 22** Spend some time examining the various options in the interface view of Cisco DCNM before moving on to the next task.

Activity Verification

You have completed this task when you attain these results:

- You have examined the interface status and parameters of the devices in your pod.
- You have changed the native VLAN for a trunk port by using the Cisco DCNM client.
- You have created a chart of the unicast, multicast, and broadcast interface utilization for an interface on your Cisco Nexus 7000 Series switch.

Answer Key

The correct answers and expected solutions for the activities that are described in this guide appear here.

Lab 2-1 Answer Key: Configure Layer 2 Switching

When you complete this activity, your Cisco Nexus 5500 Platform switch configuration and Cisco Nexus 7000 Series switch VDC configuration will be similar to the results here, with differences that are specific to your device or workgroup.

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N7K-2-pod4

```
version 6.0(1)
hostname pod4

feature telnet
feature udld

username admin password 5 $1$qtEBicif$eakEw71bocYQRm2KO88DG0 role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x224f77b9ca4e03868690ald688a346d3
priv 0x224f77b9ca4e03868690ald688a346d3 localizedkey
<rmon event configuration omitted>

vrf context management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  name TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 1 priority 28672
spanning-tree mst 2 priority 24576
spanning-tree vlan 10,12 priority 24576
spanning-tree vlan 11,13 priority 28672
spanning-tree mst configuration
  name reg34
  revision 34
  instance 1 vlan 11,13
  instance 2 vlan 10,12
udld aggressive

interface Ethernet3/45

interface Ethernet3/47

interface Ethernet4/5
  switchport mode trunk
  spanning-tree port type network
```

```

no shutdown

interface Ethernet4/6

interface Ethernet4/7
  switchport mode trunk
  spanning-tree port type network
  no shutdown

interface Ethernet4/8

interface Ethernet4/13
  switchport mode trunk
  spanning-tree port type network
  spanning-tree guard root
  no shutdown

interface Ethernet4/14

interface Ethernet4/15
  switchport mode trunk
  spanning-tree port type network
  spanning-tree guard root
  no shutdown

interface Ethernet4/16

interface mgmt0
  vrf member management
  ip address 192.168.10.98/24
  line vty

```

5548-4

```

version 5.1(3)N1(1a)
switchname N5548-4

feature telnet
no feature http-server
feature udd

username admin password 5 $1$g4rJcQDB$fd5s.h58sxDpbgqgVF2UL0 role network-admin

<some default configuration omitted>
vrf context management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  name TEST
vlan 11-13
  spanning-tree mode mst
  spanning-tree mst 1-2 priority 61440
  spanning-tree mst configuration

```

```

    name reg34
    revision 34
    instance 1 vlan 11,13
    instance 2 vlan 10,12
udld aggressive

interface Ethernet1/1
    switchport mode trunk
    spanning-tree port type network

interface Ethernet1/2
    switchport mode trunk
    spanning-tree port type network

interface Ethernet1/3
interface Ethernet1/4
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
interface Ethernet1/12
interface Ethernet1/13
interface Ethernet1/14
interface Ethernet1/15
    spanning-tree port type edge
interface Ethernet1/16
    spanning-tree port type edge
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
interface Ethernet1/25
interface Ethernet1/26
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
interface Ethernet1/30
interface Ethernet1/31
interface Ethernet1/32
interface mgmt0
    ip address 192.168.10.94/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin

```

Lab 2-2 Answer Key: Configure vPCs

When you complete this activity, your Cisco Nexus 5500 Platform switch configuration and Cisco Nexus 7000 Series switch VDC configuration will be similar to the results here, with differences that are specific to your device or workgroup.

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N7K-1-pod3

```
version 6.0(1)
hostname pod3

feature telnet
feature uddl
feature lacp
feature vpc

username admin password 5 $1$qtEBicif$eakEw71bocYQRm2K088DG0 role vdc-admin
no password strength-check
ip domain-lookup
<snmp and rmon setting omitted>

vrf context management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  name TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 0-4094 priority 8192
spanning-tree mst configuration
  name Pod3and4
  revision 34
  instance 1 vlan 11,13
  instance 2 vlan 10,12
udld aggressive
vpc domain 34
  peer-switch
  peer-keepalive destination 192.168.100.2 source 192.168.100.1 vrf default
  peer-gateway

interface port-channel3
  switchport
  switchport mode trunk
  vpc 3

interface port-channel4
  switchport
  switchport mode trunk
  vpc 4
```

```

interface port-channel7
  switchport
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link

interface Ethernet1/45
  ip address 192.168.102.1/30
  no shutdown

interface Ethernet1/47

interface Ethernet4/5
  switchport mode trunk
  spanning-tree port type network
  channel-group 7
  no shutdown

interface Ethernet4/6

interface Ethernet4/7
  switchport mode trunk
  spanning-tree port type network
  channel-group 7
  no shutdown

interface Ethernet4/8

interface Ethernet4/13
  switchport mode trunk
  spanning-tree port type network
  channel-group 3 mode active
  no shutdown

interface Ethernet4/14

interface Ethernet4/15
  switchport mode trunk
  spanning-tree port type network
  channel-group 4 mode active
  no shutdown

interface Ethernet4/16

interface mgmt0
  vrf member management
  ip address 192.168.10.97/24

```

N5K-pod3

```

version 5.1(3)N1(1a)
feature fcoe

```

```

switchname N5548-3

feature telnet
no feature http-server
feature udlld
feature lacp
feature fex

username admin password 5 $1$cvW.5dGi$x fyMB/XY9Sb.EPQafVl3X1 role network-
admin

banner motd #Nexus 5500 Switch
#
fex 103
    pinning max-links 1
    description "FEX0103"
snmp-server user admin network-admin auth md5
0x14aea44621ca1848faf3553d59b1a1a2
priv 0x14aea44621ca1848faf3553d59b1a1a2 localizedkey

vrf context management
    ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
    name TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 1-2 priority 61440
spanning-tree mst configuration
    name Pod3and4
    revision 34
    instance 1 vlan 11,13
    instance 2 vlan 10,12
udld aggressive

interface port-channel13
    switchport mode fex-fabric
    fex associate 103

interface port-channel77
    switchport mode trunk

interface Ethernet1/1
    switchport mode trunk
    spanning-tree port type network
    channel-group 77 mode active

interface Ethernet1/2
    switchport mode trunk
    spanning-tree port type network
    channel-group 77 mode active
<some interfaces omitted>
interface Ethernet1/15

```

```

switchport mode fex-fabric
fex associate 103
spanning-tree port type edge
channel-group 13

interface Ethernet1/16
  switchport mode fex-fabric
  fex associate 103
  spanning-tree port type edge
  channel-group 13
<some interfaces omitted>
interface mgmt0
  ip address 192.168.10.93/24

interface Ethernet103/1/1
  switchport access vlan 10
<some interfaces omitted>
interface Ethernet103/1/48
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
  ip route 0.0.0.0/0 192.168.10.254

```

Lab 2-3 Answer Key: Configure Cisco FabricPath

When you complete this activity, your Cisco Nexus 5500 Platform switch configuration and Cisco Nexus 7000 Series switch VDC configuration will be similar to the results here, with differences that are specific to your device or workgroup.

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N7K1-pod1

```

version 6.0(1)
feature-set fabricpath
hostname POD1

cfs eth distribute
feature interface-vlan

username admin password 5 $1$smLI8sPX$AMUZa.8cSQ.I1okw4oTWS1 role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x26298a08bec5aa6689576c4a38c9c1b2
pri
v 0x26298a08bec5aa6689576c4a38c9c1b2 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 management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  mode fabricpath

```

```

    name FP-TEST
vlan 110
spanning-tree mode mst

interface Vlan1

interface Vlan10
    no shutdown
    no ip redirects
    ip address 172.16.10.151/24
    ip address 172.16.10.161/24 secondary

interface Ethernet1/1

interface Ethernet1/41

interface Ethernet4/1

interface Ethernet4/2

interface Ethernet4/3

interface Ethernet4/4

interface Ethernet4/9
    switchport mode fabricpath
    spanning-tree port type network

interface Ethernet4/10

interface Ethernet4/11
    switchport mode fabricpath
    spanning-tree port type network
    no shutdown

interface Ethernet4/12

interface mgmt0
    ip address 192.168.10.95/24
line vty
fabricpath domain default
fabricpath switch-id 12
fabricpath load-balance unicast layer3

```

N5548-1

```

version 5.1(3)N1(1a)
no license grace-period

install feature-set fabricpath
feature-set fabricpath
switchname N5548-1

feature telnet
no feature http-server
cfs eth distribute
feature interface-vlan
feature lacp
feature lldp
feature fex

username admin password 5 $1$QiUqoLlo$91tBLbbAIG08SMq2JepqX. role network-
admin

banner motd #Nexus 5000 Switch
#

```

```

ip domain-lookup
logging event link-status default
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
system qos
    service-policy type queuing input fcoe-default-in-policy
    service-policy type queuing output fcoe-default-out-policy
    service-policy type qos input fcoe-default-in-policy
    service-policy type network-qos fcoe-default-nq-policy
fex 101
    pinning max-links 1
    description "FEX0101"
slot 1
    port 1-30 type ethernet
    port 31-32 type fc
snmp-server user admin network-admin auth md5
0xeb77058d50c8b810d36a3c51180660c7
priv 0xeb77058d50c8b810d36a3c51180660c7 localizedkey

vrf context vpc
vrf context management
    ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
    mode fabricpath
    name FP-TEST
vlan 101
vlan 1011
    fcoe vsan 11
vlan 3900-3901
vsan database
    vsan 11

interface Vlan1

interface Vlan10
    no shutdown
    ip address 172.16.10.51/24

interface Vlan3900
    no shutdown
    vrf member vpc
    ip address 198.18.1.1/24

interface port-channel9
    switchport mode trunk
    spanning-tree port type network

interface port-channel100
    switchport mode fex-fabric
    fex associate 101

interface fcl/31
    no shutdown

```

```

interface fc1/32

interface Ethernet1/1
  switchport mode fabricpath
  spanning-tree port type network
  no shutdown

interface Ethernet1/2
  switchport mode fabricpath
  spanning-tree port type network
  no shutdown

interface Ethernet1/3
  no shutdown

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9
  switchport mode trunk
  channel-group 9

interface Ethernet1/10
  switchport mode trunk
  speed 1000

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15
  switchport mode fex-fabric
  fex associate 101
  no shutdown

interface Ethernet1/16
  switchport mode fex-fabric
  fex associate 101
  no shutdown

interface Ethernet1/17

<some interfaces omitted>

interface Ethernet1/30

interface mgmt0
  ip address 192.168.10.91/24

interface Ethernet101/1/1

<some interfaces omitted>

interface Ethernet101/1/48
  cli alias name cdp show cdp nei
  line console

```

```

line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
fabricpath domain default
ip route 0.0.0.0/0 192.168.10.254
system default switchport shutdown
fabricpath switch-id 11
interface fc1/31
    switchport mode E
interface fc1/32
logging monitor 7

```

Lab 2-4 Answer Key: Configure Layer 3 Switching

When you complete this activity, your Cisco Nexus 7000 Series switch VDC and Cisco Nexus 5548 Platform switch configuration will be similar to the results here, with differences that are specific to your device or workgroup.

Note The sections of the configuration that are most relevant for this lab exercise have been highlighted in **bold**.

N7K1-pod1

```

version 6.0(1)
hostname POD1

cfs eth distribute
feature ospf
feature eigrp
feature rip
feature otv
feature interface-vlan
feature vpc

username admin password 5 $1$sm1I8sPX$AMUZa.8cSQ.IlokW4oTWS1 role vdc-admin
no password strength-check
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x26298a08bec5aa6689576c4a38c9c1b2
priv 0x26298a08bec5aa6689576c4a38c9c1b2 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 OSPF-VRF
vrf context EIGRP-VRF
vrf context STATIC-VRF
    ip route 192.168.11.12/32 172.16.11.12
vrf context management
    ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
    name FP-TEST
vlan 11-13
vlan 110,3900
spanning-tree mode mst
vpc domain 11
    peer-keepalive destination 192.168.10.97

interface Vlan1

interface Vlan10
    no shutdown

```

```

no ip redirects
ip address 172.16.10.151/24
ip address 172.16.10.161/24 secondary
ip router rip MYRIP

interface Vlan11
  no shutdown
  vrf member STATIC-VRF
  ip address 172.16.11.11/24

interface Vlan12
  no shutdown
  vrf member OSPF-VRF
  ip address 172.16.12.11/24
  ip router ospf MYOSPF area 0.0.0.0

interface Vlan13
  no shutdown
  vrf member EIGRP-VRF
  ip address 172.16.13.11/24
  ip router eigrp MYEIGRP

interface Vlan3900
  ip address 172.16.10.53/24

interface Ethernet1/1

interface Ethernet1/41

interface Ethernet4/1
  switchport mode trunk
  spanning-tree port type network

interface Ethernet4/2
  no shutdown

interface Ethernet4/3

interface Ethernet4/4

interface Ethernet4/9
  switchport mode trunk
  spanning-tree port type network
  no shutdown

interface Ethernet4/10

interface Ethernet4/11
  spanning-tree port type network

interface Ethernet4/12

interface mgmt0
  ip address 192.168.10.95/24

interface loopback0
  vrf member STATIC-VRF
  ip address 192.168.11.11/32

interface loopback10
  ip address 192.168.10.11/32
  ip router rip MYRIP

interface loopback12
  vrf member OSPF-VRF
  ip address 192.168.12.11/32
  ip router ospf MYOSPF area 0.0.0.11

```

```

interface loopback13
  vrf member EIGRP-VRF
  ip address 192.168.13.11/24
  ip router eigrp MYEIGRP
logging monitor 7
line vty
  exec-timeout 14400
router eigrp MYEIGRP
  vrf EIGRP-VRF
  autonomous-system 35
router ospf MYOSPF
router rip MYRIP

```

N5548-1

```

version 5.1(3)N1(1a)

hostname N5548-1

feature telnet
no feature http-server
feature ospf
feature eigrp
feature rip
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex

username admin password 5 $1$QiUqoLlo$91tBLbbAIG08SMq2JepqX. role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
fex 101
  pinning max-links 1
  description "FEX0101"
slot 1
  port 1-32 type ethernet
snmp-server user admin network-admin auth md5
0xeb77058d50c8b810d36a3c51180660c7 priv 0xeb77058d50c8b810d36a3c51180660c7
localizedkey

vrf context vpc
vrf context OSPF-VRF
vrf context EIGRP-VRF
vrf context STATIC-VRF
  ip route 192.168.11.11/32 172.16.11.11
vrf context management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10

```

```

    name FP-TEST
vlan 11-13
vlan 3900-3901

interface Vlan1

interface Vlan10
    no shutdown
    ip address 172.16.10.51/24
    ip router rip MYRIP

interface Vlan11
    no shutdown
    vrf member STATIC-VRF
    ip address 172.16.11.12/24

interface Vlan12
    no shutdown
    vrf member OSPF-VRF
    ip address 172.16.12.12/24
    ip router ospf MYOSPF area 0.0.0.0

interface Vlan13
    no shutdown
    vrf member EIGRP-VRF
    ip address 172.16.13.12/24
    ip router eigrp MYEIGRP

interface Vlan3900
    no shutdown
    vrf member vpc
    ip address 198.18.1.1/24

interface port-channel9
    switchport mode trunk
    spanning-tree port type network

interface port-channel100
    switchport mode fex-fabric
    fex associate 101

interface vfc3
    bind interface Ethernet1/3
    no shutdown

interface vfc28
    bind interface Ethernet1/28
    switchport mode NP
    no shutdown
vsan database
    vsan 11 interface vfc3
    vsan 11 interface vfc28

interface Ethernet1/1
    switchport mode trunk
    spanning-tree port type network

interface Ethernet1/2
    shutdown
    spanning-tree port type network

interface Ethernet1/3
    switchport mode trunk

interface Ethernet1/4

```

```

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9
    switchport mode trunk
    channel-group 9

interface Ethernet1/10
    switchport mode trunk
    speed 1000

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14
interface Ethernet1/15
    switchport mode fex-fabric
    fex associate 101

interface Ethernet1/16
    switchport mode fex-fabric
    fex associate 101
interface Ethernet1/17

<some interfaces omitted>

interface Ethernet1/28
    description FCoE-only connection to N5010-C1 e1/15 (VSAN 11)
    shutdown
    switchport mode trunk
    switchport trunk allowed vlan 1011

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
    ip address 192.168.10.91/24

interface loopback0
    vrf member STATIC-VRF
    ip address 192.168.11.12/32

interface loopback10
ip address 192.168.10.12/32
    ip router rip MYRIP

interface loopback12
    vrf member OSPF-VRF
    ip address 192.168.12.12/32
    ip router ospf MYOSPF area 0.0.0.12

interface loopback13
    vrf member EIGRP-VRF
    ip address 192.168.13.12/32
    ip router eigrp MYEIGRP

```

```

interface Ethernet101/1/1

<some interfaces omitted>

interface Ethernet101/1/48
line console
line vty
  exec-timeout 14400
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
router eigrp MYEIGRP
  vrf EIGRP-VRF
    autonomous-system 35
router ospf MYOSPF
router rip MYRIP
logging monitor 7

```

Lab 3-1 Answer Key: Configure OTV

When you complete this activity, your Cisco Nexus 7000 Series switch VDC configuration will be similar to the results here, with differences that are specific to your device or workgroup.

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N7K1-pod1

```

version 6.0(1)
hostname POD1

feature telnet
cfs eth distribute
feature otv
feature uddl
feature lacp

username admin password 5 $1$smlI8sPX$AMUZa.8cSQ.IlokW4oTWS1 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x26298a08bec5aa6689576c4a38c9c1b2
pri
v 0x26298a08bec5aa6689576c4a38c9c1b2 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 management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  name FP-TEST
vlan 11-13
otv site-vlan 13
spanning-tree mode mst
spanning-tree mst 0-4094 priority 8192
spanning-tree vlan 10,12 priority 28672
spanning-tree vlan 11,13 priority 24576
spanning-tree mst configuration
  name reg12
  revision 12
  instance 1 vlan 11,13
  instance 2 vlan 10,12
uddl aggressive

```

```

interface Overlay1
  otv join-interface Ethernet1/41
  otv control-group 239.7.7.7
  otv data-group 232.7.7.0/24
  otv extend-vlan 10-12
  no shutdown

interface Ethernet1/1
  description === C3550 fa0/25 ===

interface Ethernet1/41
  description === N7K2 e3/41 ===
  mtu 9216
  ip address 10.7.7.1/24
  ip igmp version 3
  no shutdown

interface Ethernet1/43
  description === N7K2 e3/43 ===
  switchport

interface Ethernet4/1
  description === N7K2 e4/1 ===
  switchport mode trunk
  spanning-tree port type network

interface Ethernet4/2

interface Ethernet4/3
  description === N7K2 e4/3 ===
  switchport mode trunk
  spanning-tree port type network

interface Ethernet4/4

interface Ethernet4/9
  description === N5548-1 e1/1 ===
  switchport mode trunk
  spanning-tree port type network
  spanning-tree guard root
  no shutdown

interface Ethernet4/10

interface Ethernet4/11
  description === N5548-2 e1/1 ===
  spanning-tree port type network
  spanning-tree guard root

interface Ethernet4/12

interface mgmt0
  ip address 192.168.10.95/24
  line vty
  otv site-identifier 0001.0001.0001

```

N5548-1

```

version 5.1(3)N1(1a)
hostname N5548-1

feature telnet
no feature http-server
feature udld
feature interface-vlan
feature lacp

```

```

feature lldp
feature fex

username admin password 5 $1$ZyeJfPMJ$f.7T43Ld6tTlKF..DP6fp0 role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
system qos
    service-policy type qos input fcoe-default-in-policy
    service-policy type queuing input fcoe-default-in-policy
    service-policy type queuing output fcoe-default-out-policy
    service-policy type network-qos fcoe-default-nq-policy
fex 101
    pinning max-links 1
    description "FEX0101"
snmp-server user admin network-admin auth md5
0xeb77058d50c8b810d36a3c51180660c7
priv 0xeb77058d50c8b810d36a3c51180660c7 localizedkey

vrf context management
    ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
    name FP-TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 1-2 priority 61440
spanning-tree mst configuration
    name reg12
    revision 12
    instance 1 vlan 11,13
    instance 2 vlan 10,12
udld aggressive

interface Vlan1

interface Vlan10
    no shutdown
    ip address 172.16.10.51/24

interface port-channel11
    switchport mode fex-fabric
    fex associate 101

interface Ethernet1/1
    switchport mode trunk
    spanning-tree port type network

interface Ethernet1/2
    shutdown
    spanning-tree port type network

```

```

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9
  shutdown

interface Ethernet1/10
  shutdown

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14
  shutdown

interface Ethernet1/15
  switchport mode fex-fabric
  fex associate 101
  spanning-tree port type edge
  channel-group 11

interface Ethernet1/16
  switchport mode fex-fabric
  fex associate 101
  spanning-tree port type edge
  channel-group 11

interface Ethernet1/17

<output omitted>

interface Ethernet1/32

interface mgmt0
  ip address 192.168.10.91/24

interface Ethernet101/1/1
  switchport access vlan 10

interface Ethernet101/1/2

<output omitted>

interface Ethernet101/1/48
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin

N5548-1(config)#

```

Lab 3-2 Answer Key: Configure QoS

When you complete this activity, your Cisco Nexus 7000 Series switch VDC configuration will be similar to the results here, with differences that are specific to your device or workgroup.

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N7K1-pod1

```
version 6.0(1)
hostname POD1

feature telnet
cfs eth distribute
feature uddl
feature lacp

username admin password 5 $1$smlI8sPX$AMUZa.8cSQ.IlokW4oTWS1 role vdc-admin
ip domain-lookup
ip access-list ACL01
  10 permit icmp 192.168.1.0/24 192.168.1.0/24
ip access-list ACL10
  10 permit icmp 192.168.10.0/24 192.168.10.0/24
class-map type qos match-all CMAP01
  match access-group name ACL01
class-map type qos match-all CMAP10
  match access-group name ACL10
policy-map type qos PMAP
  class CMAP01
    set precedence 5
  class CMAP10
    set precedence 0
snmp-server user admin vdc-admin auth md5 0x26298a08bec5aa6689576c4a38c9c1b2
pri
v 0x26298a08bec5aa6689576c4a38c9c1b2 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 QOS-VRF
  ip route 0.0.0.0/0 172.16.10.21
vrf context management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  name FP-TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 0-4094 priority 8192
spanning-tree vlan 10,12 priority 28672
spanning-tree vlan 11,13 priority 24576
spanning-tree mst configuration
  name reg12
  revision 12
  instance 1 vlan 11,13
  instance 2 vlan 10,12
udld aggressive

interface Vlan1

interface Ethernet1/1
  description === C3550 fa0/25 ===
```

```

interface Ethernet1/41
  description === N7K2 e3/41 ===
  service-policy type qos input PMAP
  service-policy type qos output PMAP
  vrf member QOS-VRF
  ip address 172.16.10.11/24
  no shutdown

interface Ethernet1/43
  description === N7K2 e3/43 ===
  switchport

interface Ethernet4/1
  description === N7K2 e4/1 ===
  switchport mode trunk
  spanning-tree port type network

interface Ethernet4/2

interface Ethernet4/3
  description === N7K2 e4/3 ===
  switchport mode trunk
  spanning-tree port type network

interface Ethernet4/4

interface Ethernet4/9
  description === N5548-1 e1/1 ===
  switchport mode trunk
  spanning-tree port type network
  spanning-tree guard root
  no shutdown

interface Ethernet4/10

interface Ethernet4/11
  description === N5548-2 e1/1 ===
  spanning-tree port type network
  spanning-tree guard root

interface Ethernet4/12

interface mgmt0
  ip address 192.168.10.95/24

interface loopback1
  vrf member QOS-VRF
  ip address 192.168.1.11/32

interface loopback10
  vrf member QOS-VRF
  ip address 192.168.10.11/32
line vty

```

Lab 3-3 Answer Key: Configure Security Features

When you complete this activity, your Cisco Nexus 5000 Series switch configuration and Cisco Nexus 7000 Series switch VDC configuration will be similar to the results here, with differences that are specific to your device or workgroup.

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N7K1-pod1

```
version 6.0(1)
hostname POD1

feature telnet
cfs eth distribute
feature udld
feature interface-vlan
feature lacp

username admin password 5 $1$smlI8sPX$AMUza.8cSQ.I1okw4oTWS1 role vdc-admin
ip domain-lookup
ip access-list ACL01
  10 permit icmp 192.168.1.0/24 192.168.1.0/24
ip access-list ACL10
  10 permit icmp 192.168.10.0/24 192.168.10.0/24
ip access-list ATOMIC_ACL
  10 deny icmp any any
class-map type qos match-all CMAP01
  match access-group name ACL01
class-map type qos match-all CMAP10
  match access-group name ACL10
policy-map type qos PMAP
  class CMAP01
    set precedence 5
  class CMAP10
    set precedence 0
snmp-server user admin vdc-admin auth md5 0x26298a08bec5aa6689576c4a38c9c1b2
pri
v 0x26298a08bec5aa6689576c4a38c9c1b2 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 QOS-VRF
  ip route 0.0.0.0/0 172.16.10.21
vrf context management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  name FP-TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 0-4094 priority 8192
spanning-tree vlan 10,12 priority 28672
spanning-tree vlan 11,13 priority 24576
spanning-tree mst configuration
  name reg12
  revision 12
  instance 1 vlan 11,13
  instance 2 vlan 10,12
udld aggressive
```

```

interface Vlan1

interface Vlan11
  no shutdown
  ip access-group ATOMIC_ACL in
  ip address 192.168.11.11/24
  ip directed-broadcast

interface Ethernet1/1
  description === C3550 fa0/25 ===

interface Ethernet1/41
  description === N7K2 e3/41 ===
  service-policy type qos input PMAP
  service-policy type qos output PMAP
  vrf member QOS-VRF
  ip address 172.16.10.11/24
  no shutdown

interface Ethernet1/43
  description === N7K2 e3/43 ===
  switchport

interface Ethernet4/1
  description === N7K2 e4/1 ===
  switchport mode trunk
  spanning-tree port type network

interface Ethernet4/2

interface Ethernet4/3
  description === N7K2 e4/3 ===
  switchport mode trunk
  spanning-tree port type network

interface Ethernet4/4

interface Ethernet4/9
  description === N5548-1 e1/1 ===
  switchport access vlan 11
  no shutdown

interface Ethernet4/10

interface Ethernet4/11
  description === N5548-2 e1/1 ===
  spanning-tree port type network
  spanning-tree guard root

interface Ethernet4/12

interface mgmt0
  ip address 192.168.10.95/24

interface loopback1
  vrf member QOS-VRF
  ip address 192.168.1.11/32

interface loopback10
  vrf member QOS-VRF
  ip address 192.168.10.11/32
line vty

```

N5548-1

```

version 5.1(3)N1(1a)
hostname N5548-1

```

```

feature telnet
no feature http-server
feature port-security
feature udld
feature interface-vlan
feature lacp
feature lldp
feature fex

username admin password 5 $1$ZyeJfPMJ$f.7T43Ld6tTlKF..DP6fp0 role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
fex 101
    pinning max-links 1
    description "FEX0101"
snmp-server user admin network-admin auth md5
0xeb77058d50c8b810d36a3c51180660c7
priv 0xeb77058d50c8b810d36a3c51180660c7 localizedkey

vrf context QOS-VRF
    ip route 0.0.0.0/0 172.16.10.11
vrf context management
    ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
    name FP-TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 1-2 priority 61440
spanning-tree mst configuration
    name reg12
    revision 12
    instance 1 vlan 11,13
    instance 2 vlan 10,12
udld aggressive

interface Vlan1

interface Vlan10
    no shutdown
    vrf member QOS-VRF
    ip address 172.16.10.12/24

interface Vlan11
    no shutdown
    ip address 192.168.11.12/24
    ip directed-broadcast

interface port-channel11
    switchport mode fex-fabric

```

```

fex associate 101

interface Ethernet1/1
  switchport port-security
  switchport port-security mac-address 0026.51C9.78C3
  switchport access vlan 11
  storm-control broadcast level 0.01

interface Ethernet1/2
  shutdown
  spanning-tree port type network

interface Ethernet1/3

<output omitted>

interface Ethernet1/8

interface Ethernet1/9
  shutdown

interface Ethernet1/10
  shutdown

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14
  shutdown

interface Ethernet1/15
  switchport mode fex-fabric
  fex associate 101
  spanning-tree port type edge
  channel-group 11

interface Ethernet1/16
  switchport mode fex-fabric
  fex associate 101
  spanning-tree port type edge
  channel-group 11

interface Ethernet1/17

<output omitted>

interface Ethernet1/32

interface mgmt0
  ip address 192.168.10.91/24

interface loopback1
  vrf member QOS-VRF
  ip address 192.168.1.12/32

interface loopback10
  vrf member QOS-VRF
  ip address 192.168.10.12/32

interface Ethernet101/1/1
  switchport access vlan 10

interface Ethernet101/1/2

<output omitted>

```

```

interface Ethernet101/1/48
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin

```

Lab 4-1 Answer Key: Configure FCoE

When you complete this activity, your Cisco Nexus 5500 Platform switch configuration and Cisco MDS 9124 Switch configuration will be similar to the results here, with differences that are specific to your device or workgroup.

N5548-1

```

feature fcoe
!
slot 1
    port 1-30 type ethernet
    port 31-32 type fc
!
vlan 1011
    fcoe vsan 11
!
vsan database
    vsan 11
!
device-alias mode enhanced
!
device-alias commit
!
interface vfc3
    bind interface Ethernet1/3
    switchport trunk allowed vsan 11
    no shutdown
vsan database
    vsan 12 interface vfc3
    vsan 12 interface fc1/31
!
interface fc1/31
    switchport trunk allowed vsan 11
    switchport trunk mode off
    no shutdown
!
interface fc1/31
    switchport speed 4000
interface fc1/31
    switchport mode E
!
zone mode enhanced vsan 11
!
zone name znFabricA-dcuci-c1 vsan 11
    member device-alias CX3-SPA
    member device-alias dcuci-c1
!
zoneset name FabricA vsan 11

```

```

        member znFabricA-dcuci-c1
    !
zoneset activate name FabricA vsan 11
!
zone commit vsan 11

```

N5548-2

```

feature fcoe
!
slot 1
    port 1-30 type ethernet
    port 31-32 type fc
!
vlan 1012
    fcoe vsan 12
!
vsan database
    vsan 12
!
device-alias mode enhanced
!
device-alias commit
!
interface vfc3
    bind interface Ethernet1/3
    switchport trunk allowed vsan 12
    no shutdown
vsan database
    vsan 12 interface vfc3
    vsan 12 interface fc1/31
!
interface fc1/31
    switchport trunk allowed vsan 12
    switchport trunk mode off
    no shutdown
!
interface fc1/31
    switchport speed 4000
interface fc1/31
    switchport mode E
!
zone mode enhanced vsan 12
!
zone name znFabricB-dcuci-c2 vsan 12
    member device-alias CX3-SPB
    member device-alias dcuci-c2
!
zoneset name FabricB vsan 12
    member znFabricB-dcuci-c2
!
zoneset activate name FabricB vsan 12
!
zone commit vsan 12

```

N5548-3

```
feature fcoe
!
slot 1
  port 1-30 type ethernet
  port 31-32 type fc
!
vlan 1011
  fcoe vsan 11
!
vsan database
  vsan 11
!
device-alias mode enhanced
!
device-alias commit
!
interface vfc3
  bind interface Ethernet1/3
  switchport trunk allowed vsan 11
  no shutdown
vsan database
  vsan 12 interface vfc3
  vsan 12 interface fc1/31
!
interface fc1/31
  switchport trunk allowed vsan 11
  switchport trunk mode off
  no shutdown
!
interface fc1/31
  switchport speed 4000
interface fc1/31
  switchport mode E
!
zone mode enhanced vsan 11
!
zone name znFabricA-dcuci-c3 vsan 11
  member device-alias CX3-SPA
  member device-alias dcuci-c3
!
zoneset name FabricA vsan 11
  member znFabricA-dcuci-c3
!
zoneset activate name FabricA vsan 11
!
zone commit vsan 11
```

N5548-4

```
feature fcoe
!
slot 1
```

```

    port 1-30 type ethernet
    port 31-32 type fc
!
vlan 1012
    fcoe vsan 12
!
vsan database
    vsan 12
!
device-alias mode enhanced
!
device-alias commit
!
interface vfc3
    bind interface Ethernet1/3
    switchport trunk allowed vsan 12
    no shutdown
vsan database
    vsan 12 interface vfc3
    vsan 12 interface fc1/31
!
interface fc1/31
    switchport trunk allowed vsan 12
    switchport trunk mode off
    no shutdown
!
interface fc1/31
    switchport speed 4000
interface fc1/31
    switchport mode E
!
zone mode enhanced vsan 12
!
zone name znFabricB-dcuci-c4 vsan 12
    member device-alias CX3-SPB
    member device-alias dcuci-c4
!
zoneset name FabricB vsan 12
    member znFabricB-dcuci-c4
!
zoneset activate name FabricB vsan 12
!
zone commit vsan 12

```

Lab 4-2 Answer Key: Configure NPV

When you complete this activity, your Cisco Nexus 5500 Platform switch configuration will be similar to the results here, with differences that are specific to your device or workgroup:

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N5548-P

```
version 5.0(2)N1(1)
version 5.1(3)N1(1a)
feature fcoe

hostname N5548-1

feature telnet
no feature http-server
cfs ipv4 distribute
feature lldp

username admin password 5 $1$ZyeJfPMJ$F.7T43Ld6tTlKF..DP6fp0 role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
system qos
    service-policy type queuing input fcoe-default-in-policy
    service-policy type queuing output fcoe-default-out-policy
    service-policy type qos input fcoe-default-in-policy
    service-policy type network-qos fcoe-default-nq-policy
slot 1
    port 31-32 type fc
snmp-server user admin network-admin auth md5
0xeb77058d50c8b810d36a3c51180660c7
priv 0xeb77058d50c8b810d36a3c51180660c7 localizedkey

vrf context QOS-VRF
    ip route 0.0.0.0/0 172.16.10.11
vrf context management
    ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 200
    fcoe vsan 2
vsan database
    vsan 2

interface vfc1
    bind interface Ethernet1/3
    no shutdown
```

```

interface vfc2
  bind interface Ethernet1/4
  no shutdown
vsan database
  vsan 2 interface vfc1
  vsan 2 interface vfc2
  vsan 2 interface fc1/31
  vsan 2 interface fc1/32

feature npv
npv traffic-map server-interface vfc1 external-interface fc1/31
npv traffic-map server-interface vfc2 external-interface fc1/32
npv auto-load-balance disruptive

interface fc1/31
  switchport mode NP
  no shutdown

interface fc1/32
  switchport mode NP
  no shutdown

interface Ethernet1/1

interface Ethernet1/2

interface Ethernet1/3
  switchport mode trunk
  spanning-tree port type edge trunk
  no shutdown

interface Ethernet1/4
  switchport mode trunk
  spanning-tree port type edge trunk
  no shutdown

interface Ethernet1/5

<output omitted>

interface Ethernet1/30

interface mgmt0
  ip address 192.168.10.91/24
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
interface fc1/31
  switchport mode NP
interface fc1/32
  switchport mode NP

```

Lab 5-1 Answer Key: Configure System Management

When you complete this activity, your Cisco Nexus 5000 Series switch configuration and Cisco Nexus 7000 Series switch VDC configuration will be similar to the results here, with differences that are specific to your device or workgroup:

Note	The sections of the configuration that are most relevant for this lab exercise have been highlighted in bold .
-------------	---

N7K1-pod1

```
version 6.0(1)
hostname POD1

feature telnet
cfs ipv4 mcast-address 239.255.12.12
cfs ipv4 distribute
cfs region 12
role
radius
exit
cfs eth distribute
feature scheduler
feature udlld
feature interface-vlan
feature lacp

role distribute
role name TIER-2-OPS
    rule 4 permit read-write feature vlan
    rule 3 permit read-write feature ping
    rule 2 permit read-write feature diagnostics
    rule 1 permit read
role commit
username admin password 5 $1$smLI8sPX$AMUZa.8cSQ.IlokW4oTWS1 role vdc-admin
ip domain-lookup
radius distribute
radius-server host 192.168.10.21 key 7 "V3gw3t-P3b" authentication accounting
radius-server host 192.168.10.11 authentication accounting
radius commit
ip access-list ACL01
    10 permit icmp 192.168.1.0/24 192.168.1.0/24
ip access-list ACL10
    10 permit icmp 192.168.10.0/24 192.168.10.0/24
ip access-list ATOMIC_ACL
    10 deny icmp any any
class-map type qos match-all CMAP01
    match access-group name ACL01
class-map type qos match-all CMAP10
    match access-group name ACL10
policy-map type qos PMAP
    class CMAP01
        set precedence 5
    class CMAP10
        set precedence 0
snmp-server contact Pod 1 Administrator
snmp-server user admin vdc-admin auth md5 0x26298a08bec5aa6689576c4a38c9c1b2
priv
0x26298a08bec5aa6689576c4a38c9c1b2 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
callhome
    email-contact pod1-admin@example.com
```

```

phone-contact +1-555-012-3456
streetaddress 123 Main Street, Sometown, USA
destination-profile NEXUS-OPS
destination-profile NEXUS-OPS format full-txt
destination-profile NEXUS-OPS message-level 2
destination-profile SMS
destination-profile SMS format short-txt
destination-profile SMS message-size 160
destination-profile SMS message-level 6
destination-profile TICKETING-SYSTEM
destination-profile TICKETING-SYSTEM format XML
destination-profile TICKETING-SYSTEM message-level 1
destination-profile NEXUS-OPS email-addr pod1@cisco.com
destination-profile SMS email-addr pod1@cisco.com
destination-profile TICKETING-SYSTEM email-addr pod1@cisco.com
destination-profile NEXUS-OPS alert-group all
destination-profile SMS alert-group all
destination-profile TICKETING-SYSTEM alert-group all
transport email from callhome@example.com
transport email reply-to pod1-admin@example.com
transport email smtp-server 192.168.10.10 port 25 use-vrf management
enable

vrf context QOS-VRF
  ip route 0.0.0.0/0 172.16.10.21
vrf context management
  ip route 0.0.0.0/0 192.168.10.254
vlan 1
vlan 10
  name FP-TEST
vlan 11-13
spanning-tree mode mst
spanning-tree mst 0-4094 priority 8192
spanning-tree vlan 10,12 priority 28672
spanning-tree vlan 11,13 priority 24576
spanning-tree mst configuration
  name reg12
  revision 12
  instance 1 vlan 11,13
  instance 2 vlan 10,12
udld aggressive

interface Vlan1

interface Vlan11
  no shutdown
  ip access-group ATOMIC_ACL in
  ip address 192.168.11.11/24
  ip directed-broadcast

interface Ethernet1/1
  description === C3550 fa0/25 ===

interface Ethernet1/41
  description === N7K2 e3/41 ===
  service-policy type qos input PMAP
  service-policy type qos output PMAP
  vrf member QOS-VRF
  ip address 172.16.10.11/24
  no shutdown

interface Ethernet1/43
  description === N7K2 e3/43 ===
  switchport

interface Ethernet4/1
  description === N7K2 e4/1 ===

```

```

        switchport mode trunk
        spanning-tree port type network

interface Ethernet4/2

interface Ethernet4/3
    description === N7K2 e4/3 ===
    switchport mode trunk
    spanning-tree port type network

interface Ethernet4/4

interface Ethernet4/9
    description === N5548-1 e1/1 ===
    switchport access vlan 11
    no shutdown

interface Ethernet4/10

interface Ethernet4/11
    description === N5548-2 e1/1 ===
    spanning-tree port type network
    spanning-tree guard root

interface Ethernet4/12

interface mgmt0
    ip address 192.168.10.95/24

interface loopback1
    vrf member QOS-VRF
    ip address 192.168.1.11/32

interface loopback10
    vrf member QOS-VRF
    ip address 192.168.10.11/32
line vty

scheduler job name BACKUP-CONFIG
copy running-config bootflash:/${(SWITCHNAME)}-${(TIMESTAMP)}.cfg

end-job

scheduler schedule name WEEKLY-BACKUP
    job name BACKUP-CONFIG
    time weekly 01:22:00

```

Lab 5-2 Answer Key: Implement Cisco DCNM for LAN

The tasks are procedural, so there is no answer key.

CSDCUFI50LAB

