DCUFD

Designing Cisco Data Center Unified Fabric

Version 5.0

Lab Guide

Text Part Number: 97-3186-02

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.**

Table of Contents

DCUFD

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:

- Case Study 1-1: Design a Migration to vPC
- Lab 1-2: Become Familiar with the Lab Equipment
- Lab 3-1: Explore VDCs
- Lab 3-2: Examine vPC
- Lab 3-3: Explore Cisco FabricPath
- Lab 3-4: Connect Cisco FEXs
- Lab 3-5: Interconnect Data Centers with Cisco OTV
- Case Study 3-6: Design VLAN Extension
- Case Study 4-1: Design Cisco Unified Fabric
- Answer Key

Case Study 1-1: Design a Migration to vPC

Complete this case study to practice what you learned in the related module.

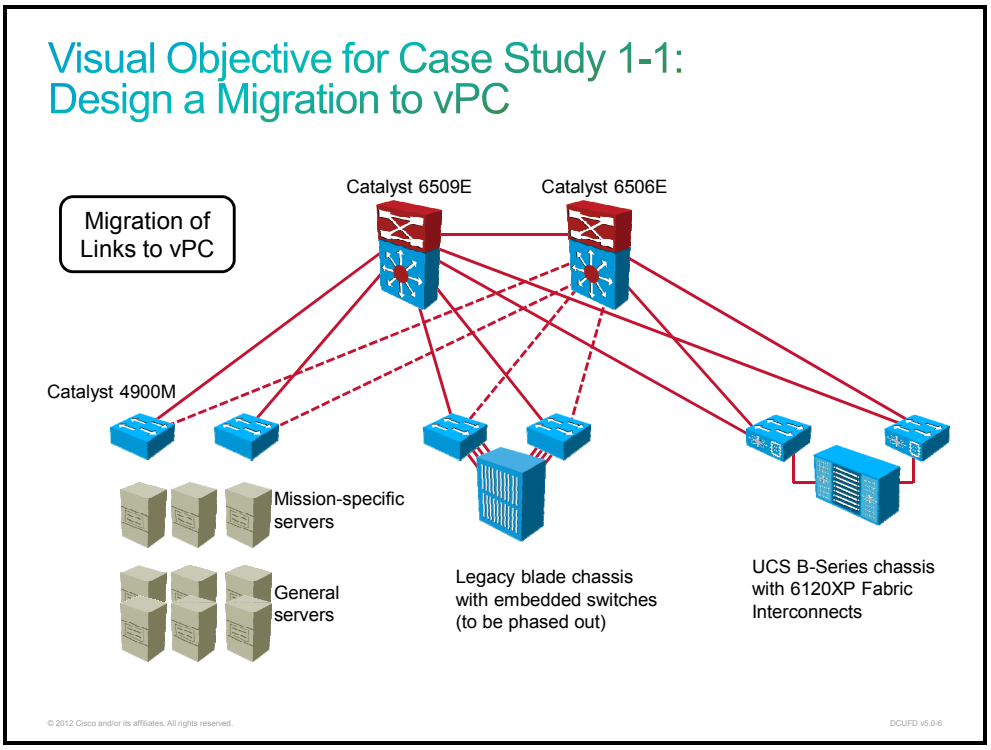
Activity Objective

In this activity, you will design a migration from the classical spanning tree-based topology to vPC. After completing this activity, you will be able to meet these objectives:

- Analyze the spanning tree network topology
- Design a solution using the Cisco Nexus family of switches with vPC

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:

- No resources are required.

Command List

There are no commands used in this activity as it is a purely paper-based activity and does not include any device configuration.

Job Aids

There are no particular job aids in this activity.

Task 1: Analyze the Spanning Tree Topology

Introduction

A mid-sized company working in the manufacturing sector has been growing over the past five years due to an increased demand in foreign markets.

The company has 200 employees in their main location.

The company manufactures power cables of various types for high-voltage applications. They expanded their product portfolio to include other products, mainly cabling solutions for new construction.

The growth of the company has shown the need to upgrade the company data center.

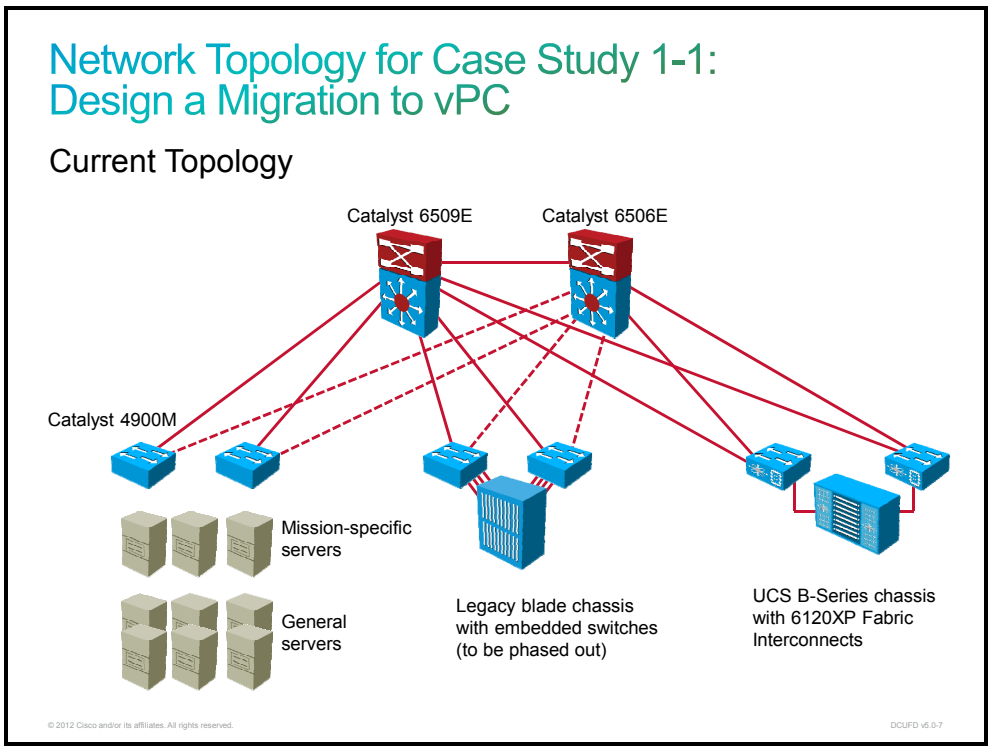
The company uses the data center for business support applications, where they run their ERP and CRM systems.

The industrial production network is separated from the business support network.

In the last four years, the company has been gradually implementing server virtualization as their old servers have been phasing out. Now they have enough capacity for growth on the computing side, and the budget plans for this year are to upgrade the data center aggregation and core layers to match the growing network demands from the virtualized servers.

Currently Installed Equipment

The topology of the company data center is shown in this figure:



Network Equipment

The company has been using the Cisco Catalyst 6509E and 6506E switches as their core and aggregation data center switches, forming a logical topology of a collapsed core. These switches use the Supervisor 720 engine with the PFC-3B forwarding card.

They have been adding 10-Gb line cards to their switches to accommodate bandwidth requirements. These connections are utilized as downlinks to the servers and as uplinks to their campus network.

Computing Equipment

One set of servers is the Cisco UCS B-Series blade server system with the Cisco UCS 6120XP Fabric Interconnect.

The company has another blade server chassis with an embedded third-party Ethernet switch that does support link bundling. This chassis will be phased out and the workload will be migrated to the Cisco UCS blade chassis.

Standalone rack servers are connected to a pair of Cisco Catalyst 4900M switches. Some of the servers in the rack utilize Gigabit Ethernet links on the switch. Some application-specific standalone servers utilize 10 Gigabit Ethernet ports. The Catalyst 4900M connects to the Catalyst 6500 chassis using 10 Gigabit Ethernet connections.

Challenges

Since the core switches are the Catalyst 6500 with the supervisor engine that does not support multichassis EtherChannel, they depend on STP and its behavior used on the links.

They are facing high utilization of their uplinks, but have no additional spare room on the 10-Gb line cards to accommodate the additional bandwidth requirement. Adding a line card is not an easy option because the second chassis is a Catalyst 6506 and they do not have the slots available there at this moment.

Questions

- What are the main congestion points in this network?
- What could be improved?

Task 2: Design a vPC Topology

In this task, you will design a vPC-based topology to optimize the use of all downlinks from the data center collapsed core.

Equipment Considerations

The company is replacing the Catalyst 6500 core switches with a pair of Cisco Nexus 7009 switches with the following configuration:

- A pair of Cisco Nexus 7009 switches with the following configuration:
  - Supervisor Engine 2
  - 32-port 10 Gigabit Ethernet I/O module: N7K-M132XP-12L
  - 48-port Gigabit Ethernet I/O module: N7K-M148GT-11L
- A pair of Cisco Nexus 2248TP Fabric Extenders (FEXs)

The Catalyst 6500 chassis will be retained, but will perform only auxiliary services with the service modules.

vPC Design Activity:

Consider the following:

- With the installation of the Nexus 7009, how can you benefit from the congested uplinks?
- How will the Catalyst 4900M connect to the Nexus 7009? Is vPC a viable option?
- How will the existing blade chassis connect to the core switch?
- How can you utilize the Cisco FEXs?
- How will the Cisco UCS chassis connect to the core switch?

Task 3: Future Readiness Assessment

In this task, you will examine the possibilities that the company has with its new equipment.

Nexus 7009 Chassis

The Cisco Nexus 7009 currently has installed the 32-port 10 Gigabit Ethernet I/O module, and the 48-port 1 Gigabit Ethernet I/O module. There is plenty of room for future expansion.

How can this company benefit from use of the following options?

- Cisco Unified Fabric
- Virtual port channels
- Cisco FabricPath
- Virtual device contexts

Current Catalyst 6500 Chassis

The current Catalyst 6509 and 6506 chassis can be repurposed and given other tasks.

Which of these components can be upgraded to extend the useful life of both chassis?

- Supervisor Engine
- Line cards
- Service modules

Catalyst 4900M Switches

The current switches can be retained to accommodate bandwidth requirements of the application-specific servers that connect to the 10 Gigabit Ethernet interfaces.

To free up these uplinks, some of the servers that use 1 Gigabit Ethernet interfaces can be moved to the Cisco FEXs.

Lab 1-2: Become Familiar with the Lab Equipment

In this lab, you will connect to the lab equipment and become familiar with it.

The lab consists of two Cisco Nexus 7000 Series Switches that are shared, and a Cisco Nexus 5548 Switch that is available to each POD. Additionally, there are available the Cisco Nexus 2248TP FEXs, and a Cisco UCS C-200 Series Server for every POD.

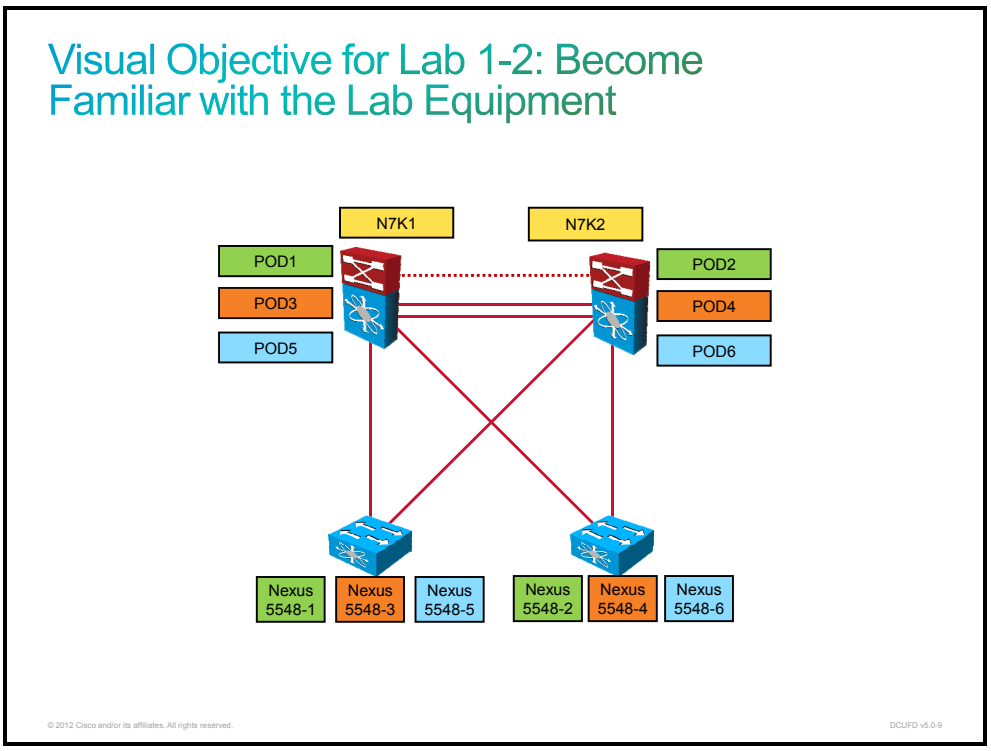
Activity Objective

In this activity, you will explore the lab.

- Connect and explore Cisco Nexus 7000 Series Switches
- Connect and explore Cisco Nexus 5548 Switches

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:

- Two Cisco Nexus 7000 Series Switches
- One Cisco Nexus 5548 Switch per POD
- Student PC

Command List

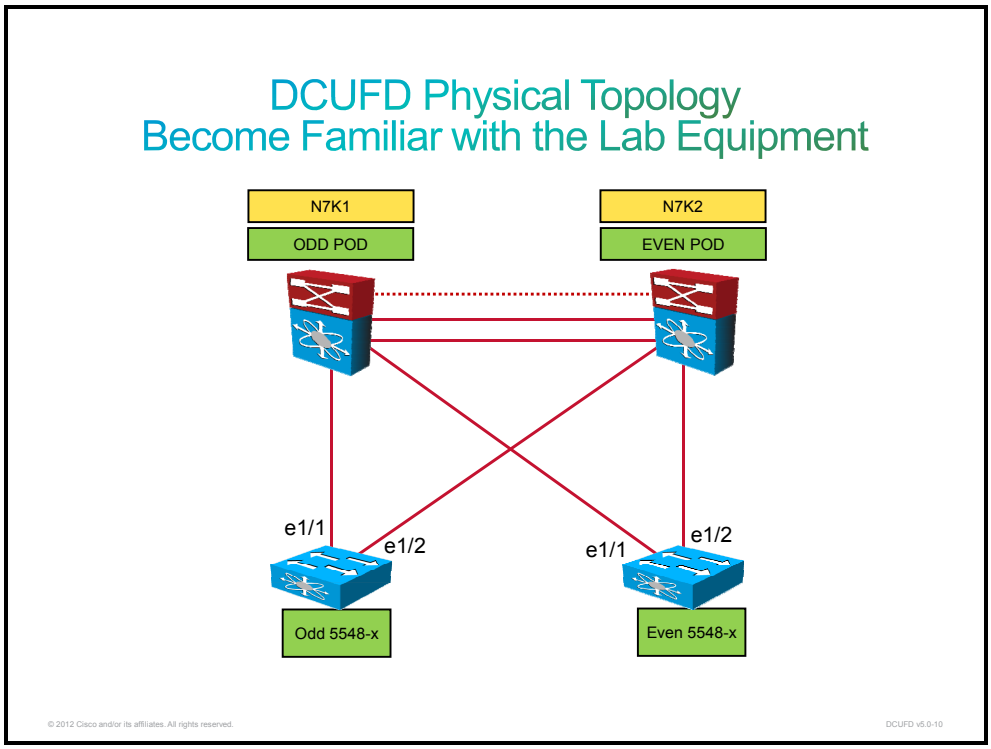
The table describes the commands that are used in this activity.

Commands Used in the Lab

Command	Description
`show cdp neighbors [detail]`	This command displays the list of neighbor network devices.
`show interfaces brief`	This command displays a table with interface statuses.
`show vlan`	This command displays the VLANs that are configured on the system or in the current VDC.

Job Aids

These job aids are available to help you complete all of the lab activities in this Lab Guide. You should consider marking up the following topology with the interface numbering of your specific POD to assist you with the remainder of this lab.



- Management IP addressing:

POD	Device	IP Address	Login
PODs 1, 3, 5	Cisco Nexus 7000 Series Switch 1 (N7K1)	192.168.10.89	admin / NXos12345
PODs 2, 4, 6	Cisco Nexus 7000 Series Switch 2 (N7K2)	192.168.10.90	admin / NXos12345
POD 1	N5548-1	192.168.10.91	admin / NXos12345
POD 2	N5548-2	192.168.10.92	admin / NXos12345
POD 3	N5548-3	192.168.10.93	admin / NXos12345
POD 4	N5548-4	192.168.10.94	admin / NXos12345
POD 5	N5548-5	192.168.10.99	admin / NXos12345
POD 6	N5548-6	192.168.10.100	admin / NXos12345

- Interface assignments per POD:

POD 1

Device	Interface	Device	Interface	Comment
N7K1-POD1	e4/1	N7K2-POD2	e4/1	vPC peer link
N7K1-POD1	e4/3	N7K2-POD2	e4/3	vPC peer link
N7K1-POD1	e1/41	N7K2-POD2	e3/41	vPC peer-keepalive link
N7K1-POD1	e4/9	N5548-1	e1/1	Member link
N7K1-POD1	e4/11	N5548-2	e1/1	Member link

POD 2

Device	Interface	Device	Interface	Comment
N7K2-POD2	e4/1	N7K1-POD1	e4/1	vPC peer link
N7K2-POD2	e4/3	N7K1-POD1	e4/3	vPC peer link
N7K2-POD2	e3/41	N7K1-POD1	e1/41	vPC peer-keepalive link
N7K2-POD2	e4/9	N5548-1	e1/2	Member link
N7K2-POD2	e4/11	N5548-2	e1/2	Member link

POD 3

Device	Interface	Device	Interface	Comment
N7K1-POD3	e4/5	N7K2-POD4	e4/5	vPC peer link
N7K1-POD3	e4/7	N7K2-POD4	e4/7	vPC peer link
N7K1-POD3	e1/45	N7K2-POD4	e3/45	vPC peer-keepalive link
N7K1-POD3	e4/13	N5548-3	e1/1	Member link
N7K1-POD3	e4/15	N5548-4	e1/1	member link

POD 4

Device	Interface	Device	Interface	Comment
N7K2-POD4	e4/5	N7K1-POD3	e4/5	vPC peer link
N7K2-POD4	e4/7	N7K1-POD3	e4/7	vPC peer link
N7K2-POD4	e3/45	N7K1-POD3	e1/45	vPC peer-keepalive link
N7K2-POD4	e4/13	N5548-3	e1/2	Member link
N7K2-POD4	e4/15	N5548-4	e1/2	Member link

POD 5

Device	Interface	Device	Interface	Comment
N7K1-POD5	e4/17	N7K1-POD6	e4/17	vPC peer link
N7K1-POD5	e4/19	N7K1-POD6	e4/19	vPC peer link
N7K1-POD5	e1/47	N7K1-POD6	e3/47	vPC peer-keepalive link
N7K1-POD5	e4/21	N5548-5	e1/1	Member link
N7K1-POD5	e4/23	N5548-6	e1/1	Member link

POD 6

Device	Interface	Device	Interface	Comment
N7K2-POD6	e4/17	N7K1-POD5	e4/17	vPC peer link
N7K2-POD6	e4/19	N7K1-POD5	e4/19	vPC peer link
N7K2-POD6	e3/47	N7K1-POD5	e1/47	vPC peer-keepalive link
N7K2-POD6	e4/21	N5548-5	e1/2	Member link
N7K2-POD6	e4/23	N5548-6	e1/2	Member link

Task 1: Connect to the Cisco Nexus 7000 Series Switch

In this task, you will connect to the switch in the main VDC and create additional VDCs that you will use in further exercises.

Activity Procedure

Complete these steps:

Step 1 Log into your Cisco Nexus 7000 Series Switch. Connect, using Telnet, to the management IP address. Refer to the lab access instructions for addresses, usernames, and passwords.

Note In general, the outputs that are shown are for POD 1 only. Perform the activities on your assigned equipment.

Step 2 Display the status of interfaces. Use the **show interface brief** command.

```
N7K1# show interface brief
```

Note	See the Job Aids section for device interfaces that are assigned to your POD. If you do not see any of the interfaces online or available for you to view, contact your instructor. The interface might be assigned to a VDC, in which case it must be brought into VDC 1 to be able to continue with the exercises.

Step 3 Display and examine the list of switch neighbors (if there are any).

```
N7K1# show cdp neighbors
```

Step 4 Display the features that are available and the installed licenses.

```
N7K1# 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   -   In use Never       -
SCALABLE_SERVICES_PKG         Yes   -   Unused Never       -
TRANSPORT_SERVICES_PKG        Yes   -   Unused Never       -
LAN_ADVANCED_SERVICES_PKG     Yes   -   In use Never       -
LAN_ENTERPRISE_SERVICES_PKG   Yes   -   Unused Never       -
--------------------------------------------------------------
```

Activity Verification

You have completed this task when you attain these results:

- Verify the interfaces and neighbors on the Cisco Nexus 7000 Series Switch.

Task 2: Connect to the Cisco Nexus 5548 Switch

In this task, you will connect to the Cisco Nexus 5548 access switch and examine it.

Activity Procedure

Complete these steps:

Step 1 Log into your Cisco Nexus 5548 Switch. Connect, using Telnet, to the management IP address.

With the Cisco Nexus 5548 Switch, every POD has its own device with which to connect. Refer to the Job Aids section for the IP addresses, usernames, and passwords for connection.

Step 2 Display the status of interfaces. Use the **show interface brief** command.

```
N5548-1# show interface brief
```

Step 3 Display and examine the list of switch neighbors.

```
N5548-1# show cdp neighbors
```


Step 4 Display the features that are available and the installed licenses.

```
N5548-1# show license usage
Feature                      Ins  Lic   Status Expiry Date
Comments
                                 Count
--------------------------------------------------------------
FCOE_NPV_PKG                  No    -   Unused             -
FM_SERVER_PKG                 Yes   -   Unused Never       -
ENTERPRISE_PKG                Yes   -   Unused Never       -
FC_FEATURES_PKG               Yes   -   In use 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       -
--------------------------------------------------------------
```

Activity Verification

You have completed this task when you attain these results:

- Verify the interfaces and neighbors on the Cisco Nexus 5548 Switch.

Lab 3-1: Explore VDCs

In this lab, you will be creating a VDC and assigning interfaces to it.

Virtual device contexts provide a means of virtualization of a Cisco Nexus 7000 Series Switch, allowing you to create up to four VDCs. These VDCs are independent from each other and provide isolation in management and control plane, as well as data plane separation and fault protection.

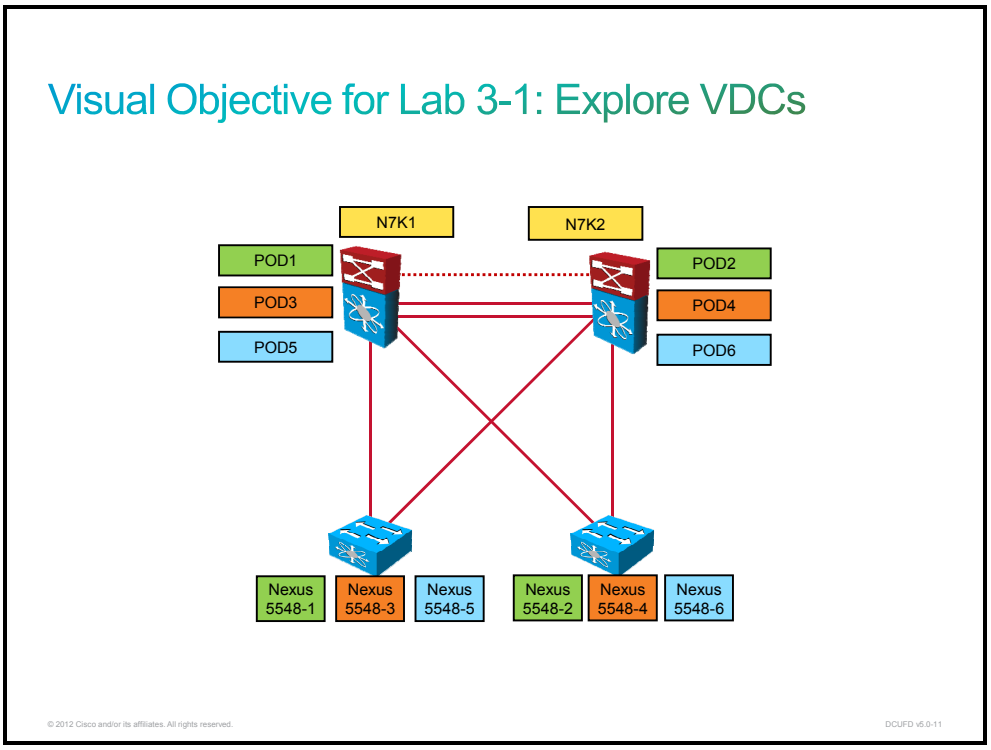
Activity Objective

In this activity, you will explore network device virtualization using VDCs on Cisco Nexus 7000 Series Switches. After completing this activity, you will be able to meet these objectives:

- Create a VDC on a Cisco Nexus 7000 Series Switch
- Assign physical interfaces to the VDC

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:

- Two Cisco Nexus 7000 Series Switches
- Student PC

Command List

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

Commands Used in the Lab

Command	Description
allocate interface ethernet X	This command allocates an interface to a VDC.
show cdp neighbors [detail]	This command displays the list of neighbor network devices.
show interfaces brief	This command displays a table with interface statuses.
show vlan	This command displays the VLANs that are configured on the system or in the current VDC.
switchback	This command switches the console from the VDC to VDC1.
switchto vdc name	This command switches the console to the console of the VDC.
vdc name	This command creates a VDC.

Job Aids

These job aids are available to help you complete the lab activity. You should also refer to the management addressing and POD-specific interface numbering from the Job Aids section of Lab 1-2.

- POD assignment:
  - PODs 1, 3, and 5 will work on the N7K1 switch.
  - PODs 2, 4, and 6 will work on the N7K2 switch.

Note When required, PODs 1 and 2, 3 and 4, and 5 and 6 will work as teams.

- Management IP addressing and login credentials per VDC:

POD	Device-VDC	Management IP	Login
PODs 1, 3, 5	N7K1	192.168.10.89	admin / NXos12345
PODs 2, 4, 6	N7K2	192.168.10.90	admin / NXos12345
POD 1	N7K1-POD1	192.168.10.95	admin / NXos12345
POD 2	N7K2-POD2	192.168.10.96	admin / NXos12345
POD 3	N7K1-POD3	192.168.10.97	admin / NXos12345
POD 4	N7K2-POD4	192.168.10.98	admin / NXos12345
POD 5	N7K1-POD5	192.168.10.103	admin / NXos12345
POD 6	N7K2-POD6	192.168.10.104	admin / NXos12345

Task 1: Create a VDC

In this task, you will connect to the switch in the main VDC, and create additional VDCs that you will use in further exercises.

Activity Procedure

Complete these steps:

Step 1 Log into your Cisco Nexus 7000 Series Switch and create the VDC. Connect, using Telnet, to the management IP address of the main VDC.

Refer to the lab access instructions for addresses, usernames, and passwords.

Note	Refer to the Job Aids section on which VDC to create. X is your POD number.

```
N7K1(config)# vdc PODX
Note:  Creating VDC, one moment please ...
```

Step 2 Allocate the downstream interfaces that will belong to every VDC. Study the warning that is generated from this configuration.

Note	Refer to the Job Aids section on which interfaces need to be assigned to your VDC.

```
N7K1(config-vdc)# allocate interface eX/X, eX/X, …
Moving ports will cause all config associated to them in
source vdc to be removed. Are you sure you want to move the
ports (y/n)?  [yes]
N7K1(config-vdc)#
```

Step 3 Repeat this process for all interfaces that need to be assigned to your POD VDC.

Step 4 Switch to the console of each VDC and review the configuration. Perform the first-time configuration wizard for that VDC. Set the management IP address.

```
N7K1(config-vdc)# switchto vdc PODX

         ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]:

  Enter the password for "admin": NXos12345
  Confirm the password for "admin": NXos12345

         ---- Basic System Configuration Dialog VDC: X ----

This setup utility will guide you through the basic
configuration of the system. Setup configures only enough
connectivity for management of the system.

Please register Cisco Nexus7000 Family devices promptly with
your supplier. Failure to register may affect response times
for initial service calls. Nexus7000 devices must be
registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```



```
Would you like to enter the basic configuration dialog
(yes/no): y


  Create another login account (yes/no) [n]:

  Configure read-only SNMP community string (yes/no) [n]:

  Configure read-write SNMP community string (yes/no) [n]:

  Enter the switch name : POD X
```

Step 5 Configure the management IP address as found in the Job Aids section. The default gateway IP address is **192.168.10.254**.

Note	Set the correct management IP address for your POD as found in the Job Aids section.

```
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:

    Mgmt0 IPv4 address : 192.168.10.XX

    Mgmt0 IPv4 netmask : 255.255.255.0

  Configure the default gateway? (yes/no) [y]: y

    IPv4 address of the default gateway : 192.168.10.254

  Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [n]: y

  Enable the ssh service? (yes/no) [y]:

    Type of ssh key you would like to generate (dsa/rsa)
[rsa]:

    Number of rsa key bits <1024-2048> [1024]:

  Configure default interface layer (L3/L2) [L3]: L2

  Configure default switchport interface state (shut/noshut)
[shut]:

The following configuration will be applied:
  password strength-check
  switchname PODX
interface mgmt0
```

```
ip address 192.168.10.XX 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 192.168.10.254
exit
  feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown

Would you like to edit the configuration? (yes/no) [n]: n

Use this configuration and save it? (yes/no) [y]: y
```

Activity Verification

You have completed this task when you attain these results:

- Display the VDC configuration on both switches from the default VDC. The output below is taken from N7K1 with the odd PODs configured.

```
N7K1-PODX#switchback
N7K1# show vdc

vdc_id  vdc_name                          state
mac
  type        lc
------  --------                          -----
----------
  ---------   ------
1       N7KX                              active
00:26:51:c9:78:c1
  Ethernet    m1 f1 m1xl
3       POD1                              active
00:26:51:c9:78:c3
  Ethernet    m1 f1 m1xl
4       POD3                              active
00:26:51:c9:78:c4
  Ethernet    m1 f1 m1xl
```

- Use Telnet to connect to your VDC from the student desktop. You should connect using the IP address that you previously configured for your VDC. If you are unable to connect via Telnet, troubleshoot your configuration wizard input; otherwise, contact your instructor.
- Display the interfaces that are in your VDC; POD 1 is shown here as an example:

```
N7K1-POD1# show interface status

--------------------------------------------------------------------
Port          Name               Status    Vlan      Duplex
Speed   Type
--------------------------------------------------------------------
```



```
mgmt0         --                 connected routed    full
100     --
Eth1/41       --                 disabled  1         full
auto    10/100/1000
Eth4/1        --                 disabled  1         auto
auto    SFP-H10GB-C
Eth4/2        --                 sfpAbsent 1         auto
auto    --
Eth4/9        --                 disabled  1         auto
auto    SFP-H10GB-C
Eth4/10       --                 sfpAbsent 1         auto
auto    --
Eth4/11       --                 disabled  1         auto
auto    SFP-H10GB-C
Eth4/12       --                 sfpAbsent 1         auto
auto    --
```

- Display the list of neighboring devices to which your VDC is connected; POD1 is shown here as an example. If you do not see any neighbors, it is likely that either of the interfaces are shut down between your Cisco Nexus 7000 Series VDC and the Cisco Nexus 5548 Switches or peer Cisco Nexus 7000 Series VDC:

```
N7K1-POD1# 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
N5548-1(SSI16010PVG)   Eth4/9        160    S I s     N5K-
C5548UP   Eth1/1

N5548-2(SSI16010Q23)   Eth4/11       160    S I s     N5K-
C5548UP   Eth1/1
```

- Connect to the Cisco Nexus 5548 Switch and examine interface statuses and neighbor tables on the switch.

```
N5548-1# show interface status
N5548-1# show cdp neighbors
```

  You should be able to see the neighboring VDCs as the connected devices. If not, verify that the interfaces are not shut down and otherwise troubleshoot the problem, or ask your instructor for help.

Lab 3-2: Examine vPC

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

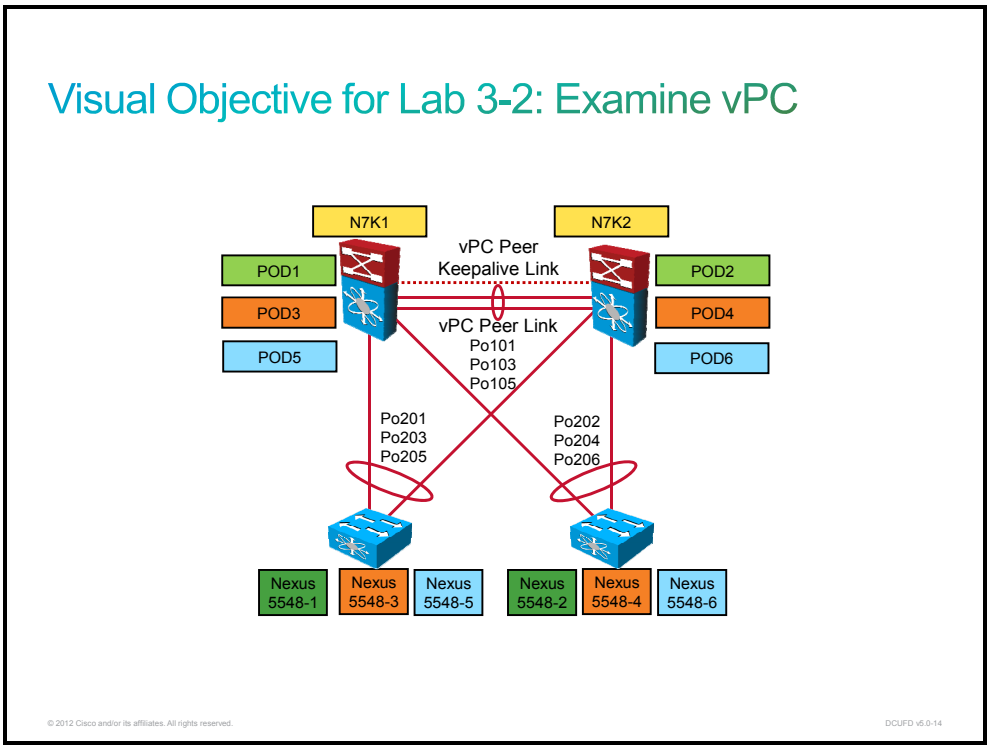
Activity Objective

In this activity, you will explore how vPCs allow simultaneous use of all uplinks between the switches. After completing this activity, you will be able to meet these objectives:

- Design access networks and determine the number of uplinks to the aggregation layer
- Verify the functioning of vPC on network equipment

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:

- Two Cisco Nexus 7000 Series Switches
- One Cisco Nexus 5548 Switch per POD
- Student PC

Command List

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

The Commands Used in the Examine vPC Lab

Command	Description
channel-group num mode active	This command configures an Ethernet interface to be a member of a port channel.
feature vpc	This command enables the vPC feature on the switch.
interface ethernet **channel-group mode active**	This command configures a physical interface to be a member of a port channel.
interface ethernet **fex associate 100** **switchport mode fex-fabric**	This command configures a physical interface to attach a FEX.
interface port-channel **vpc**	This command creates a port channel interface and configures it as a member of a vPC.
peer-keepalive destination	This command configures the keepalive destination address for a vPC domain
show feature	This command displays the enabled features on a switch.
show port-channel summary	This command displays all active port channel interfaces.
show vpc	This command displays the active vPCs.
show vpc peer-keepalive	This command displays the vPC peer keepalive information.
vpc domain num	This command creates a vPC domain.
vpc num	This command configures a port channel interface to be a member of a vPC.
vpc peer-link	This command configures the interface to be the vPC peer link.

Job Aids

These job aids are available to help you complete the lab activity. Also refer to the Job Aid for Lab 1-2 for the addressing and interface numbering per POD.

- Virtual port channel (vPC)-related configuration and values

POD	vPC Domain	vPC Peer Link	Cisco Nexus 5548 Port Channel
POD 1	12	Po101	Po201
POD 2	12	Po101	Po202
POD 3	34	Po103	Po203
POD 4	34	Po103	Po204
POD 5	56	Po105	Po205
POD 6	56	Po105	Po206

Task 1: Configure a vPC Domain Between the Cisco Nexus 7000 Series Aggregation Switches

In this task, you will configure a vPC domain between your Cisco Nexus 7000 Series VDC and your peer Cisco Nexus 7000 Series VDC. You will be working with your peer POD (1-2, 3-4, 5-6) during this task.

Activity Procedure

Complete these steps:

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

Step 2 Verify that the vPC feature on the switch is enabled. If the feature is not enabled, enable it. POD 1 is shown here as an example.

```
N7K1-POD1# show feature
Feature Name          Instance  State
--------------------  --------  --------
amt                   1         disabled
...
udld                  1         disabled
vpc                   1         disabled
vrrp                  1         disabled
vtp                   1         disabled
wccp                  1         disabled
N7K1-POD1(config)# feature vpc
```

Step 3 Configure a vPC domain on the switch. Refer to the Job Aids section for the domain number to use.

```
N7K1-POD1(config)# vpc domain XY
```

Step 4 Create the VRF that will be used for the peer-keepalive IP addressing. Put the physical interface into routed mode and in the correct VRF. Refer to the Job Aids section in Lab 1-2 to determine the interfaces that you should use between Cisco Nexus 7000 Series Switches for the vPC peer-keepalive. Set the IP address of the vPC peer-keepalive interfaces. Even-numbered PODs will use the address 10.99.99.2, while odd-numbered PODs will use the address 10.99.99.1 for the peer-

keepalive Layer 3 interface.

```
N7K1-POD1(config)# vrf context VPC
N7K1-POD1(config-vrf)# interface eX/X
N7K1-POD1(config-if)# no switchport
N7K1-POD1(config-if)# vrf member VPC
% Deleted all L3 config on interface EthernetX/X
N7K1-POD1(config-if)# ip address 10.99.99.X/24
N7K1-POD1(config-if)# no shut
```

Step 5 Configure the vPC peer-keepalive source and destination for the domain.

```
N7K1-POD1(config)# vpc domain XY
N7K1-POD1(config-vpc-domain)# peer-keepalive destination
10.99.99.X vrf VPC source 10.99.99.Y
```

Note The other POD should use a mirrored configuration.

Step 6 Test the connectivity across the peer-keepalive link:

```
N7K1-POD1# ping 10.99.99.X vrf VPC
PING 10.99.99.X (10.99.99.X): 56 data bytes
64 bytes from 10.99.99.X: icmp_seq=0 ttl=254 time=10.775 ms
64 bytes from 10.99.99.X: icmp_seq=1 ttl=254 time=0.576 ms
64 bytes from 10.99.99.X: icmp_seq=2 ttl=254 time=0.596 ms
64 bytes from 10.99.99.X: icmp_seq=3 ttl=254 time=0.61 ms
64 bytes from 10.99.99.X: icmp_seq=4 ttl=254 time=0.606 ms

--- 10.99.99.X ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.576/2.632/10.775 ms
```

Step 7 Verify the functioning of the vPC peer-keepalive link:

```
N7K1-POD1# show vpc peer-keepalive

vPC keep-alive status             : peer is alive
--Peer is alive for             : (414) seconds, (451) msec
--Send status                   : Success
--Last send at                  : 2012.05.21 00:59:30 186 ms
--Sent on interface             : EthX/XX
--Receive status                : Success
--Last receive at               : 2012.05.21 00:59:30 186 ms
--Received on interface         : EthX/XX
--Last update from peer         : (0) seconds, (222) msec

vPC Keep-alive parameters
--Destination                   : 10.99.99.X
--Keepalive interval            : 1000 msec
--Keepalive timeout             : 5 seconds
--Keepalive hold timeout        : 3 seconds
--Keepalive vrf                 : VPC
```

```
--Keepalive udp port            : 3200
--Keepalive tos                 : 192
```

Step 8 Verify from the Job Aids in Lab 1-2 the two interfaces that you will be using as the vPC peer link between your Cisco Nexus 7000 Series VDC and your peer Cisco Nexus 7000 Series VDC. Configure them as trunks.

```
N7K1-POD1(config)# interface eX/Y, eX/Z
N7K1-POD1(config-if-range)# switchport mode trunk
N7K1-POD1(config-if-range)# spanning-tree port type network
N7K1-POD1(config-if-range)# no shut
```

Step 9 Make the peer link physical interfaces a member of the port channel as specified in the previous Job Aid.

```
N7K1-POD1(config-if-range)# channel-group 10X
```

Step 10 Create the vPC peer link using the port channel interface.

```
N7K1-POD1(config-if-range)# interface port-channel 10X
N7K1-POD1(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.
```

Activity Verification

You have completed this task when you attain this result:

- Display the configuration of your vPC domain.

```
N7K1-POD1(config-if)# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC
peer-link

vPC domain id                     : XX
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 (or secondary)
Number of vPCs configured         : 0
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled

vPC Peer-link status
---------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------
1    Po10X  up     1
```


- Display the list of active port channel interfaces:

```
N7K1-POD1(config-if)# 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)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
10X   Po10X(SU)   Eth      NONE      EthX/X(P)  EthX/Y(P)
```

Task 2: Configure a vPC Between Access and Aggregation Switches

In this task, you will configure and verify vPC between your Cisco Nexus 5548 Switch and your Cisco Nexus 7000 Series VDC, as well as your peer Cisco Nexus 7000 Series VDC.

Activity Procedure

Complete these steps:

Step 1 On your Cisco Nexus 7000 Series VDC switch, configure the interface that connects to the Cisco Nexus 5548 access switch in the odd POD (this might be your POD). Use the Cisco Nexus 5548 port channel number X for the odd POD from the previous Job Aids.

```
N7K1-POD1(config)# interface e4/Y
N7K1-POD1(config-if)# switchport mode trunk
N7K1-POD1(config-if)# no shut
N7K1-POD1(config-if)# channel-group 20X mode active
```

If you get an error message saying that the LACP process must be started, enable the LACP feature.

```
N7K1-POD1(config-if)# channel-group 20X mode active
LACP process needs to be started before configuring active
mode
N7K1-POD1(config-if)# feature lacp
```

You might need to retry creating the port channel interface.

Note On the peer Cisco Nexus 7000 Series Switch, your colleague from the peer POD should perform the same configuration using the same channel-group number.

Step 2 On your Cisco Nexus 7000 Series VDC switch, configure the interface that connects to the Cisco Nexus 5548 access switch in the even POD (this might be your POD). Use the Cisco Nexus 5548 port channel number Y for the even POD from the previous Job Aids.

```
N7K1-POD1(config)# interface e4/X
N7K1-POD1(config-if)# switchport mode trunk
N7K1-POD1(config-if)# no shut
N7K1-POD1(config-if)# channel-group 20Y mode active
```

Note On the peer Cisco Nexus 7000 Series Switch, your colleague from the peer POD should perform the same configuration using the same channel-group number. Steps 1 and 2 should *not* be using the same channel-group number.

Step 3 Connect to your Cisco Nexus 5548 Switch. Prepare your Cisco Nexus 5548 access switch for vPC configuration:

```
N5548-1(config)# feature lacp
N5548-1(config)# interface e1/1, e1/2
N5548-1(config-if-range)# switchport mode trunk
N5548-1(config-if-range)# no shut
```

Step 4 Create a port channel X on the access switch, where X is the POD number. Use LACP for negotiation.

```
N5548-1(config-if-range)# channel-group 20X mode active
```

Step 5 Display the summary of port channel configuration; your output might look like one of these two displays:

```
N5548-1(config-if-range)# 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)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
20X   Po20X(SU)   Eth      LACP      Eth1/1(P)    Eth1/2(s)

N5548-1(config-if-range)# 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)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
20X   Po20X(SD)   Eth      LACP      Eth1/1(I)    Eth1/2(I)
```

What is the problem?

Note If you do not enable vPC on the individual port channels of the Cisco Nexus 7000 Series Switches, the access Cisco Nexus 5548 Switch will recognize two distinct upstream switches instead of one single vPC domain, which will cause a port channel error.

Step 6 Return to your Cisco Nexus 7000 Series VDC switch and verify the vPC status:

```
N7K1-POD1(config-if)# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC
peer-link

vPC domain id                     : XX
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 (or secondary)
Number of vPCs configured         : 0
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------------
1    Po10X  up     1
```

Note The port channels that are connecting the Cisco Nexus 5548 Switches are not on the list of vPCs. Also, the number of vPCs configured is 0.

Step 7 Configure the port-channel interface X for the even-numbered Cisco Nexus 5548 Switch to be a member of the vPC. (Refer to the previous Job Aids; the vPC number should match the port channel number.):

```
N7K1-POD1(config-if)# interface port-channel 20X
N7K1-POD1(config-if)# vpc 20X
```

Step 8 Configure the port-channel interface Y for the odd-numbered Cisco Nexus 5548 Switch to be a member of the vPC. (Refer to the previous Job Aids.):

```
N7K1-POD1(config-if)# interface port-channel 20Y
N7K1-POD1(config-if)# vpc 20Y
```

Step 9 Verify the vPC status again:

```
N7K1-POD1(config-if)# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC
peer-link

vPC domain id                     : XX
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 (or secondary)
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po10X  up     1

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason
Active vlans
--   ----   ------ ----------- ------                     ----
20X  Po20X  up     success     success                    1
20Y  Po20Y  up     success     success                    1
```

Step 10 Verify the port-channel configuration on the access switch:

```
N5548-1(config-if-range)# 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)
        M - Not in use. Min-links not met
----------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
----------------------------------------------------------------------
20X   Po20X(SU)   Eth      LACP      Eth1/1(P)    Eth1/2(P)
```

Activity Verification

You have completed this task when you attain this result:

- Verify the configuration of your vPC:

```
N7K1-POD1# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC
peer-link

vPC domain id                     : XX
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 (or secondary)
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------------
1    Po101  up     1

vPC status
---------------------------------------------------------------------
id   Port   Status Consistency Reason
Active vlans
--   ----   ------ ----------- ------                    ----
20X  Po20X  up     success     success                   1
20Y  Po20Y  up     success     success                   1
```

- Display information about the peer keepalive link.

```
N7K1-POD1# show vpc peer-keepalive

vPC keep-alive status             : peer is alive
--Peer is alive for              : (2818) seconds, (620) msec
--Send status                    : Success
--Last send at                   : 2012.05.21 01:39:34 89 ms
--Sent on interface              : EthX/XX
--Receive status                 : Success
--Last receive at                : 2012.05.21 01:39:34 297 ms
--Received on interface          : EthX/XX
--Last update from peer          : (0) seconds, (281) msec

vPC Keep-alive parameters
--Destination                    : 10.99.99.X
--Keepalive interval             : 1000 msec
--Keepalive timeout              : 5 seconds
--Keepalive hold timeout         : 3 seconds
--Keepalive vrf                  : VPC
--Keepalive udp port             : 3200
--Keepalive tos                  : 192
```

- Display the summary of port channels on the aggregation switch.

```
N7K1-POD1# 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)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
10X   Po10X(SU)   Eth      NONE      Eth4/X(P) Eth4/Y(P)
20X   Po20X(SU)   Eth      LACP      Eth4/X(P)
20Y   Po20Y(SU)   Eth      LACP      Eth4/X(P)
```

- Display the summary of port channels on the access switch.

```
N5548-1# 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)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
20X   Po20X(SU)   Eth      LACP      Eth1/1(P)    Eth1/2(P)
```


Lab 3-3: Explore Cisco FabricPath

In this lab, you will configure and explore Cisco FabricPath on Cisco Nexus 7000 Series Switches and Cisco Nexus 5548 Switches.

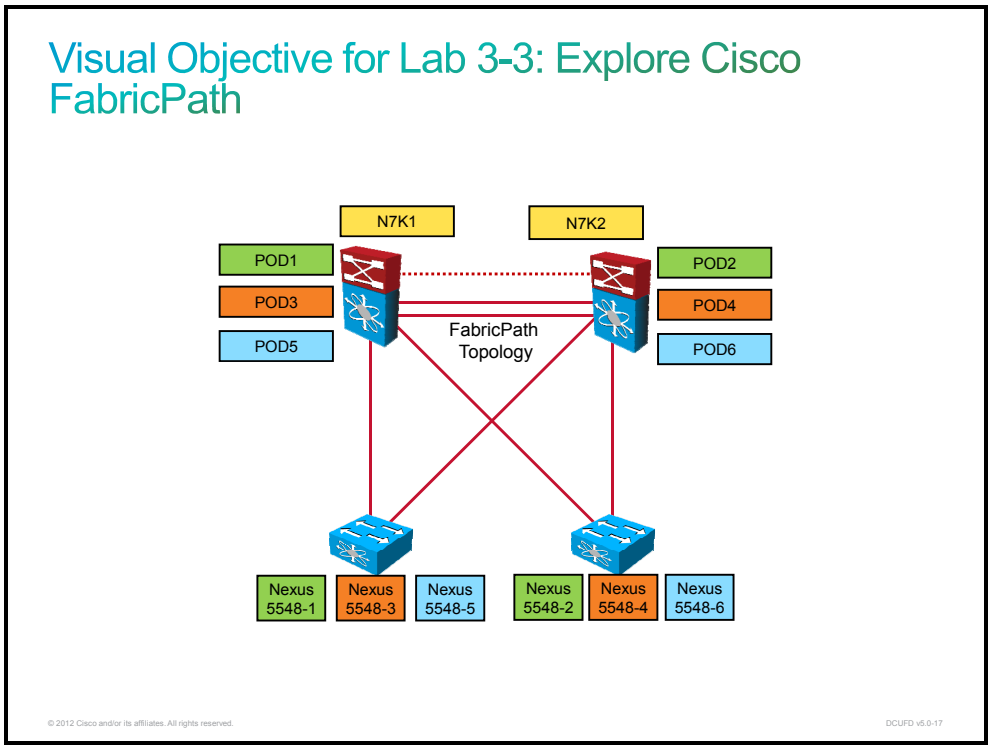
Activity Objective

In this activity, you will configure and explore FabricPath frame forwarding and Layer 2 multipathing. After completing this activity, you will be able to meet these objectives:

- Configure Cisco FabricPath on Cisco Nexus 7000 Series Switches and Cisco Nexus 5548 Switches
- Monitor Cisco FabricPath operation
- Design topologies with Cisco FabricPath

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:

- Two Cisco Nexus 7000 Series Switches with 32-port 10 Gigabit Ethernet F1 I/O Module
- One Cisco Nexus 5548 Switch per POD
- Student PC

Command List

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

The Commands Used in the Explore Cisco FabricPath Lab

Command	Description
fabricpath switch-id id	This command changes the Cisco FabricPath switch ID of a switch.
feature-set fabricpath	This command enables the Cisco FabricPath feature set.
mode fabricpath	This command changes a VLAN to a Cisco FabricPath VLAN.
show fabricpath isis adjacency	This command displays the list of Cisco FabricPath IS-IS neighbors.
show fabricpath loadbalance unicast forwarding-path flow	This command displays the interface that will be selected by the Cisco FabricPath load-balancing algorithm to forward packets for a specific flow.
show fabricpath route	This command displays the Cisco FabricPath routing table.
show fabricpath switch-id	This command lists the switch IDs of all switches in the Cisco FabricPath network.
show license usage	This command displays the license usage in a VDC.
show mac address-table address mac-address	This command displays the MAC address table entry for a specific MAC address.
show mac address-table vlan vlan	This command displays the MAC address table for a VLAN.
show spanning-tree inconsistentports	This command displays the ports that are in spanning-tree inconsistent state.
show spanning-tree vlan vlan	This command displays the spanning-tree topology for a VLAN.
spanning-tree mst instance-list priority priority	This command changes the spanning-tree priority for the selected MST instances.
switchport mode fabricpath	This command configures an interface as a Cisco FabricPath port.

Job Aids

These job aids are available to help you complete the lab activity. Refer also to the addressing and interface Job Aids from Lab 1-2.

- FabricPath switch IDs:

Device	FabricPath Switch ID
N7K1-POD1	1
N7K2-POD2	2
N7K1-POD3	3
N7K2-POD4	4
N7K1-POD5	5
N7K2-POD6	6
N5548-1	11
N5548-2	12
N5548-3	13
N5548-4	14
N5548-5	15
N5548-6	16

Task 1: Configure Cisco FabricPath Topology on the Cisco Nexus 7000 Series Switch

In this task, you will configure a FabricPath topology on Cisco Nexus 7000 Series Switches.

Your topology will consist of a pair of Cisco Nexus 7000 Series Switches acting as spine switches. Your topology will also include a pair of Cisco Nexus 5548 Switches that act as leaf switches and are connected to both Cisco Nexus 7000 Series Switches.

The topology provides two paths from one Cisco Nexus 5548 Switch to the other, which can perform load balancing over any of the two Cisco Nexus 7000 Series spine switches.

Activity Procedure

Complete these steps:

Step 1 Log into the lab and connect to your VDC on the Cisco Nexus 7000 Series Switch. Remove all of the vPC configuration from the Cisco Nexus 7000 Series Switches. Refer to the Job Aids from Lab 3-2 or utilize the appropriate **show** commands to identify the VPC domain and port channel numbers.

N7K1-POD1(config)# **no vpc domain *XY***
N7K1-POD1(config)# **no vrf context VPC**
N7K1-POD1(config)#**no interface port-channel 10X**
N7K1-POD1(config)#**no interface port-channel 20X**

Step 2 Verify that the interfaces between the Cisco Nexus 7000 Series Switch and the interfaces to the Cisco Nexus 5548 Switches are configured as trunks.

```
N7K1-POD1(config)# interface e4/X , e4/X , e4/X , e4/X
N7K1-POD1(config-if-range)# switchport mode trunk
```

Note Use the correct interface numbering for your POD.

Step 3 Verify licenses that allow you to use the Cisco FabricPath feature:

```
N7K1-POD1# show license usage
Feature                      Ins  Lic   Status Expiry Date
Comments
                                 Count
--------------------------------------------------------------------
MPLS_PKG                      No    -   Unused             -
STORAGE-ENT                   No    -   Unused             -
ENTERPRISE_PKG                No    -   Unused             -
FCOE-N7K-F132XP               No    0   Unused             -
ENHANCED_LAYER2_PKG           No    -   Unused             -
SCALABLE_SERVICES_PKG         No    -   Unused             -
TRANSPORT_SERVICES_PKG        No    -   Unused             -
LAN_ADVANCED_SERVICES_PKG     Yes   -   Unused Never       -
LAN_ENTERPRISE_SERVICES_PKG   Yes   -   Unused Never       -
--------------------------------------------------------------------
```

Which license is required to use Cisco FabricPath?

Step 4 Display the available feature sets. Enable FabricPath within the VDC.

```
N7K1-POD1# show feature-set
Feature Set Name      ID        State
--------------------  --------  --------
fcoe                   1          disabled
fabricpath             2          disabled
fex                    3          disabled
mpls                   4          disabled
```

Note Contact your instructor if the Cisco FabricPath feature set shows up as being uninstalled.

```
N7K1-POD1(config)# feature-set fabricpath
N7K1-POD1(config)# show feature-set
Feature Set Name      ID        State
--------------------  --------  --------
fcoe                   1          disabled
fabricpath             2          enabled
fex                    3          disabled
mpls                   4          disabled
```

Step 5 Display the Cisco FabricPath switch ID:

```
N7K1-POD1# show fabricpath switch-id
                        FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
============================================================
SWITCH-ID      SYSTEM-ID       FLAGS         STATE    STATIC
EMULATED
----------+---------------+-----------+----------+---------
*2838        6c9c.ed46.52c2    Primary     Confirmed    No
No
Total Switch-ids: 1
```

Step 6 Change the switch ID to match your POD number.

```
N7K1-POD1(config)# fabricpath switch-id P
```

Step 7 Display the switch ID again to verify the change:

```
N7K1-POD1(config)# show fabricpath switch-id
                        FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
============================================================
SWITCH-ID      SYSTEM-ID       FLAGS         STATE    STATIC
EMULATED
----------+---------------+-----------+----------+---------
*P           6c9c.ed46.52c2    Primary     Confirmed    Yes
No
Total Switch-ids: 1
```

Step 8 Configure the interfaces that connect your VDC and your peer POD VDC as Cisco FabricPath interfaces.

Note Insert the correct port number based on the physical topology for your POD.

```
N7K1-POD1(config)# interface e4/X, e4/Y
N7K1-POD1(config-if-range)# switchport mode fabricpath
```

Step 9 Re-examine the Cisco FabricPath switch ID again. If your colleagues in your peer POD Q have configured the interfaces for Cisco FabricPath, you should also see their switch:

```
N7K1-POD1(config)# show fabricpath switch-id
FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
==============================================================
SWITCH-ID SYSTEM-ID FLAGS STATE STATIC EMULATED
---------+---------------+-----------+----------+---------
*P a8b1.d455.6fc4 Primary Confirmed Yes No
 Q 0026.9804.a944 Primary Confirmed Yes No
Total Switch-ids: 2
```

Step 10 Configure the interface that connects to your Cisco Nexus 5548 POD access switch:

```
N7K1-POD1(config)# interface e4/X
N7K1-POD1(config-if)# switchport mode fabricpath
```

Note Insert the correct port number based on the physical topology for your POD.

Step 11 Configure the interface that connects to your peer POD Cisco Nexus 5548 access switch (the “cross” connection):

```
N7K1-POD1(config)# interface ethernet 4/X
N7K1-POD1(config-if)# switchport mode fabricpath
```

Note Insert the correct port number based on the physical topology.

Step 12 Verify that Cisco FabricPath IS-IS adjacencies have been formed on the interface between your VDC and your peer POD VDC.

```
N7K1-POD1# show fabricpath isis adjacency
```

Why do you not see the adjacency with the Cisco Nexus 5548 Switch?

Step 13 Examine the Cisco FabricPath routing table:

```
N7K1-POD1# 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/X/0, number of next-hops: 0
        via ---- , [60/0], 0 day/s 00:23:28, local
```

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

Step 14 Create a Cisco FabricPath VLAN. PODs 1 and 2 use VLAN 100; PODs 3 and 4 use VLAN 102; and PODs 5 and 6 use VLAN 104.

```
N7K1-POD1(config)# vlan 10X
N7K1-POD1(config-vlan)# mode fabricpath
```

Step 15 Re-examine the Cisco FabricPath routing table:

```
N7K1-POD1(config-vlan)# 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/X/0, number of next-hops: 0
        via ---- , [60/0], 0 day/s 00:23:28, local
1/X/0, number of next-hops: 4
        via Eth4/X, [115/40], 0 day/s 00:01:40,
isis_fabricpath-default
        via Eth4/X, [115/40], 0 day/s 00:01:40,
isis_fabricpath-default
        via Eth4/X, [115/40], 0 day/s 00:01:40,
isis_fabricpath-default
        via Eth4/X, [115/40], 0 day/s 00:01:40,
isis_fabricpath-default
```

Step 16 Examine the MAC address table for VLAN 100 / 102 / 104.

```
N7K1-POD1# show mac address-table vlan 10X
```

Were any MAC addresses learned for VLAN 10X?

Step 17 Examine the spanning tree topology for VLAN 10X.

```
N7K1-POD1# show spanning-tree vlan 10X
Spanning tree instance(s) for vlan does not exist.
```

Note	The relevant ports are not listed in the Spanning Tree Protocol list because they are now Cisco FabricPath ports, and STP does not run on those ports anymore.

Activity Verification

You have completed this task when you attain these results:

- Configure Cisco FabricPath on the Cisco Nexus 7000 Series Switch.

Task 2: Configure Cisco FabricPath Topology on the Cisco Nexus 5548 Switches

In this task, you will continue the configuration of a Cisco FabricPath topology on the Cisco Nexus 5548 Switches.

The topology provides two paths from one Cisco Nexus 5548 Switch to the other, which can perform load balancing over any of the two Cisco Nexus 7000 Series spine switches.

Activity Procedure

Complete these steps:

Step 1 Connect to your Cisco Nexus 5548 Switch. Remove the EtherChannel configuration from the switch. Use the appropriate **show** command to figure out which port channel number to use.

```
N5548-1(config)# no interface port-channel 20X
```

Step 2 Install and enable the Cisco FabricPath feature set.

```
N5548-1(config)# install feature-set fabricpath
N5548-1(config)# feature-set fabricpath
```

Step 3 Display the Cisco FabricPath switch ID:

```
N5548-1(config)# show fabricpath switch-id
```

Step 4 Change the switch ID. Use switch ID 1P, where P is your POD number, for the access switches.

```
N5548-1(config)# fabricpath switch-id 1P
```

Step 5 Display the switch ID again to verify the change:

```
N5548-1(config)# show fabricpath switch-id
                        FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
================================================================
SWITCH-ID      SYSTEM-ID       FLAGS         STATE    STATIC
EMULATED
---------+---------------+-----------+----------+---------
*1P          547f.ee81.cbbc    Primary     Confirmed    Yes
No
Total Switch-ids: 1
```

Step 6 Configure the links toward the Cisco Nexus 7000 Series Switches in Cisco FabricPath mode:

```
N5548-1(config)# interface e1/1 , e1/2
N5548-1(config-if-range)# switchport mode fabricpath
```


Step 7 Display the Cisco FabricPath switch ID table again. You should now see both Cisco Nexus 7000 Series Switches and your peer Cisco Nexus 5548 Switch:

```
N5548-1# show fabricpath switch-id
                        FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
================================================================
SWITCH-ID      SYSTEM-ID       FLAGS          STATE    STATIC
EMULATED
----------+---------------+-----------+----------+---------
P           6c9c.ed46.52c2    Primary     Confirmed     Yes
No
Q           6c9c.ed61.73c8    Primary     Confirmed     Yes
No
1Q          547f.ee83.2c01    Primary     Confirmed     Yes
No
*1P          547f.ee81.cbbc    Primary     Confirmed     Yes
No
Total Switch-ids: 4
```

Step 8 Create the VLANs 10X and configure them for Cisco FabricPath mode:

Note	Recall that PODs 1 and 2 use VLAN 100; PODs 3 and 4 use VLAN 102; and PODs 5 and 6 use VLAN 104.

```
N5548-1(config)# vlan 10X
N5548-1(config-vlan)# mode fabricpath
```

Activity Verification

You have completed this task when you attain these results.

- Display and examine the Cisco FabricPath topology table on the Cisco Nexus 7000 Series (aggregation) switch in your POD VDC. You should see four adjacencies, where P is your POD number and Q is your peer POD number:

```
N7K-POD1# show fabricpath isis adjacency
Fabricpath IS-IS domain: default Fabricpath IS-IS adjacency
database:
System ID       SNPA            Level  State  Hold Time
Interface
N7K-PODQ    N/A             1      UP     00:00:28
Ethernet4/X
N7K-PODQ    N/A             1      UP     00:00:28
Ethernet4/X
N5548-P         N/A             1      UP     00:00:30
Ethernet4/X
N5548-Q         N/A             1      UP     00:00:27
Ethernet4/X
```

- Display and examine the Cisco FabricPath topology table on the Cisco Nexus 5548 access switch:

```
N5548-1# show fabricpath isis adjacency
Fabricpath IS-IS domain: default Fabricpath IS-IS adjacency
database:
```

```
System ID       SNPA            Level  State  Hold Time
Interface
N7K-PODP    N/A             1      UP     00:00:33
Ethernet1/1
N7K-PODQ    N/A             1      UP     00:00:36
Ethernet1/2
```

- Display and compare the Cisco FabricPath routing tables on the Cisco Nexus 7000 Series Switch and Cisco Nexus 5548 Switch:

```
N5548-1# 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

0/1P/0, number of next-hops: 0
        via ---- , [60/0], 0 day/s 00:14:35, local
1/P/0, number of next-hops: 1
        via Eth1/1, [115/40], 0 day/s 00:04:24,
isis_fabricpath-default
1/Q/0, number of next-hops: 1
        via Eth1/2, [115/40], 0 day/s 00:04:24,
isis_fabricpath-default
1/1Q/0, number of next-hops: 2
        via Eth1/1, [115/80], 0 day/s 00:04:10,
isis_fabricpath-default
        via Eth1/2, [115/80], 0 day/s 00:04:10,
isis_fabricpath-default


N7K1-POD1# 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/P/0, number of next-hops: 0
        via ---- , [60/0], 0 day/s 00:48:51, local
1/Q/0, number of next-hops: 2
        via Eth4/X, [115/40], 0 day/s 00:27:03,
isis_fabricpath-default
        via Eth4/X, [115/40], 0 day/s 00:27:03,
isis_fabricpath-default
1/1P/0, number of next-hops: 1
```



```
        via Eth4/X, [115/40], 0 day/s 00:04:59,
isis_fabricpath-default
1/1Q/0, number of next-hops: 1
        via Eth4/X, [115/40], 0 day/s 00:04:45,
isis_fabricpath-default
```

- Display the Cisco FabricPath VLAN on one of the switches:

```
N5548-1# show fabricpath topology vlan active
Topo-Description                 Topo-ID   Active VLAN List
-------------------------------- --------- --------------------
------------------
0                                0         10X


N5548-1(config)# show vlan id 10X

VLAN Name                             Status    Ports
---- -------------------------------- --------- --------------
-----------------
10X  VLAN010X                         active    Eth1/1, Eth1/2

VLAN Type  Vlan-mode
---- ----- ----------
10X  enet  FABRICPATH
```

Note	Note that VLAN 10X is in Cisco FabricPath mode.

Lab 3-4: Connect Cisco FEXs

In this exercise, you will connect a Cisco FEX to the Cisco Nexus 5548 Switch. There are three possibilities to connect the Cisco FEX: using standalone links and host interface pinning; using a port channel; and using vPC where the Cisco FEX is multihomed to two managing switches.

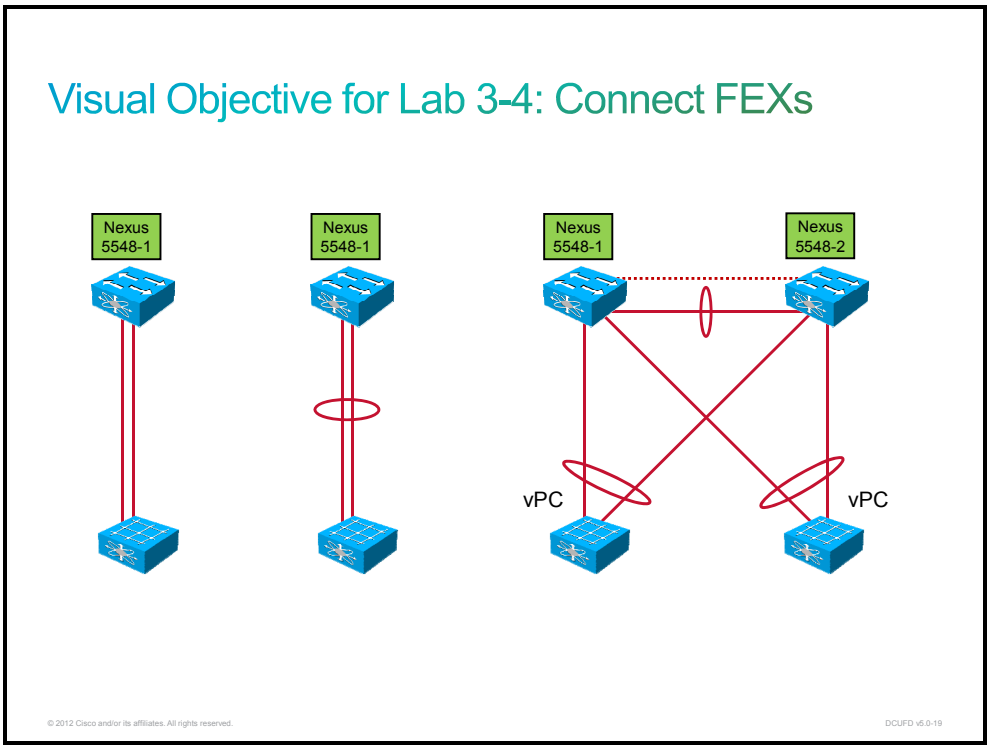
Activity Objective

In this activity, you will connect Cisco Nexus 2248TP FEX switches to extend the access layer. After completing this activity, you will be able to meet these objectives:

- Connect the Cisco FEX using straight-through links
- Connect the Cisco FEX using a port channel
- Connect the Cisco FEX using vPC

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:

- One Cisco Nexus 5548 Switch per POD
- One Cisco Nexus 2248 FEX per POD
- Student PC

Command List

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

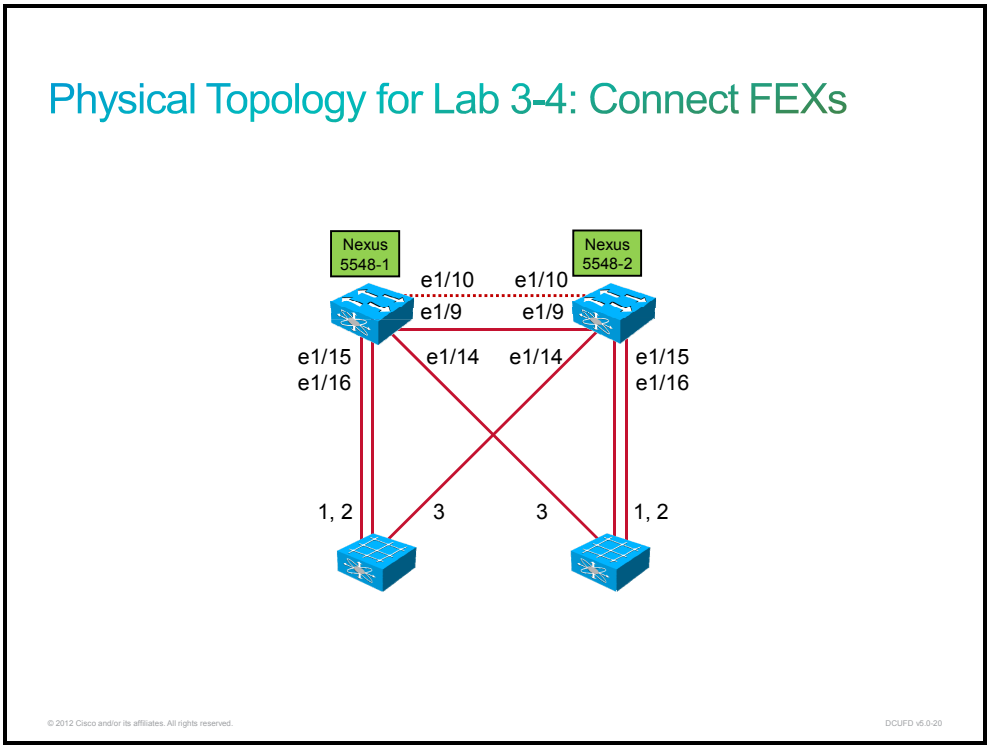
The Commands Used in the Connect FEXs Lab

Command	Description
channel-group num mode active	This command configures an Ethernet interface to be a member of a port channel.
feature fex	This command enables FEX support.
feature vpc	This command enables the vPC feature on the switch.
fex num	This command defines a FEX in the running configuration.
interface ethernet **channel-group mode active**	This command configures a physical interface to be a member of a port channel.
interface ethernet **fex associate 101**	This command configures a physical interface to attach a FEX.
interface ethernet **fex associate 101** **switchport mode fex-fabric**	This command configures a physical interface to attach a FEX.
interface port-channel **vpc**	This command creates a port channel interface and configures it as a member of vPC.
peer-keepalive destination	This command configures the keepalive destination address for a vPC domain.
pinning max-links num	This command configures how many links the FEX can use for pinning.
show feature	This command displays the enabled features on a switch.
show fex [detail]	This command displays all connected FEXs.
show port-channel summary	This command displays all active port channel interfaces.
show vpc	This command displays the active vPCs.
show vpc peer-keepalive	This command displays the vPC peer keepalive information.
switchport mode fex-fabric	This command configures the switch port to connect a FEX.
vpc domain num	This command creates a vPC domain.
vpc num	This command configures a port channel interface to be a member of a vPC.
vpc peer-link	This command configures the interface to be the vPC peer link.

Job Aids

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

- Physical topology (all PODs):



- Port assignments:

All PODs

Device	Interface	Comment
N5548-X	e1/15	Connection to the first downlink of your POD N2248
N5548-X	e1/16	Connection to the second downlink of your POD N2248
N5548-X	e1/14	Connection to the third downlink *of your peer* POD N2248
N5548-X	e1/9	Connection to your peer POD N5548 for vPC peer link
N5548-X	e1/10	Connection to your peer POD N5548 for vPC peer keepalive link

- FEX number assignments:

POD	FEX Number
POD 1	101
POD 2	102
POD 3	103
POD 4	104
POD 5	105
POD 6	106

- vPC domain assignments (Task 3):

POD	vPC Domain	vPC Peer Link	vPC
POD 1	112	Po101	Po201
POD 2	112	Po101	Po202
POD 3	134	Po103	Po203
POD 4	134	Po103	Po204
POD 5	156	Po105	Po205
POD 6	156	Po105	Po206

Task 1: Connect a Cisco Nexus 2248 FEX

In this task, you will configure the Cisco Nexus 5548 Switch to connect a Cisco Nexus 2248 FEX using straight-through links.

Activity Procedure

Complete these steps:

Step 1 Log into your POD Cisco Nexus 5548 Switches.

Step 2 Verify that the FEX feature support is enabled. If FEX support is disabled, enable it.

```
N5548-1# show feature
Feature Name          Instance  State
--------------------  --------  --------
assoc_mgr             1         enabled
cimserver             1         disabled
fabric-binding        1         disabled
fc-port-security      1         disabled
fcoe                  1         enabled
fcsp                  1         disabled
fex                   1         enabled
fport-channel-trunk   1         disabled
http-server           1         enabled
interface-vlan        1         enabled
lacp                  1         enabled
ldap                  1         disabled
lldp                  1         enabled
niv                   1         disabled
npiv                  1         disabled
npv                   1         disabled
port_track            1         disabled
private-vlan          1         disabled
privilege             1         disabled
sshServer             1         enabled
tacacs                1         disabled
telnetServer          1         disabled
udld                  1         enabled
vpc                   1         disabled
vtp                   1         disabled
```

Step 3 Start configuring the Cisco FEX. Assign the number "10P" to the FEX, where P is your POD number, with a maximum of two downlinks.

```
N5548-1(config)# fex 10P
N5548-1(config-fex)# pinning max-links 2
Change in Max-links will cause traffic disruption.
```

Step 4 Configure the downlink interfaces to your POD FEX to be FEX fabric ports:

```
N5548-1(config)# interface ethernet e1/15-16
N5548-1(config-if-range)# switchport mode fex-fabric
N5548-1(config-if-range)# fex associate 10P
```

This is the initial configuration required on an interface that the switch needs to detect and initialize the Cisco FEX. After 1 to 2 minutes, you should see messages similar to these:

```
2012 Nov 13 10:24:29 N5548-1 %PFMA-2-FEX_STATUS: Fex 10P is
online
2012 Nov 13 10:24:29 N5548-1 %NOHMS-2-NOHMS_ENV_FEX_ONLINE:
FEX-10P On-line
2012 Nov 13 10:24:31 N5548-1 %PFMA-2-FEX_STATUS: Fex 10P is
online
```

Activity Verification

You have completed this task when you attain these results:

- Display the associated FEX:

```
N5548-1# show fex detail
FEX: 10P Description: FEX010P   state: Online
  FEX version: 5.0(2)N1(1) [Switch version: 5.0(2)N1(1)]
  FEX Interim version: 5.0(2)N1(1)
  Switch Interim version: 5.0(2)N1(1)
  Extender Model: N2K-C2248TP-1GE,  Extender Serial:
JAF1430AJFP
  Part No: 73-12748-05
  Card Id: 99, Mac Addr: f8:66:f2:27:f7:02, Num Macs: 64
  Module Sw Gen: 12594  [Switch Sw Gen: 21]
  post level: complete
 pinning-mode: static    Max-links: 2
  Fabric port for control traffic: Eth1/15
  Fabric interface state:
    Eth1/15 - Interface Up. State: Active
    Eth1/16 - Interface Up. State: Active
  Fex Port        State  Fabric Port
       Eth10P/1/1    Up     Eth1/15
       Eth10P/1/2    Up     Eth1/15
       …
       Eth10P/1/24   Up     Eth1/15
       Eth10P/1/25   Up     Eth1/16
       Eth10P/1/26    Up     Eth1/16
       Eth10P/1/27    Up     Eth1/16
      …
```



```
Eth10P/1/48    Up      Eth1/16
```

You should confirm that the state of the FEX is online.

- Display the fabric ports:

```
N5548-1# show interface fex-fabric
     Fabric      Fabric       Fex                 FEX
Fex  Port      Port State    Uplink    Model          Serial
--------------------------------------------------------------
-
101   Eth1/15        Active     1    N2K-C2248TP-1GE
SSI161500N7
101   Eth1/16        Active     2    N2K-C2248TP-1GE
SSI161500N7
```

- Display the associated ports to one uplink: Ethernet 1/15 interface

```
N5548-1# show interface ethernet 1/15 fex-intf
Fabric          FEX
Interface       Interfaces
---------------------------------------------------
 Eth1/15        Eth101/1/1    Eth101/1/2    Eth101/1/3
Eth101/1/4
                Eth101/1/5    Eth101/1/6    Eth101/1/7
Eth101/1/8
                Eth101/1/9    Eth101/1/10   Eth101/1/11
Eth101/1/12
                Eth101/1/13   Eth101/1/14   Eth101/1/15
Eth101/1/16
                Eth101/1/17   Eth101/1/18   Eth101/1/19
Eth101/1/20
                Eth101/1/21   Eth101/1/22   Eth101/1/23
Eth101/1/24
```

Task 2: Connect a Cisco Nexus 2248 FEX Using a Port Channel

In this task, you will configure the Cisco Nexus 5548 Switch to connect a Cisco Nexus 2248 FEX using a port channel.

Step 1 Remove the FEX configuration from Task 1 from the physical interfaces:

```
N5548-1(config)# interface ethernet e1/15-16
N5548-1(config-if-range)# no switchport mode fex-fabric
N5548-1(config-if-range)# no fex associate 10X
```

Step 2 Change the fabric configuration on the FEX to allow for only one single link between the FEX and the managing switch:

```
N5548-1(config)# fex 10X
N5548-1(config-fex)# pinning max-links 1
Change in Max-links will cause traffic disruption.
```

This will allow a port channel interface to be the uplink for the FEX.

Step 3 Configure the physical interfaces to be members of the port channel. Use port channel interface number 100:

```
N5548-1(config-if)# interface e1/15-16
N5548-1(config-if-range)# channel-group 100
```

Note All PODs can use the same port channel number because it has only local meaning.

Step 4 Configure a port channel interface to be the downlink interface for the FEX. After 1 to 2 minutes, you should see the FEX come online.

```
N5548-1(config)# interface portchannel 100
N5548-1(config-if)# switchport mode fex-fabric
N5548-1(config-if)# fex associate 10X

2012 Nov 13 10:40:27 N5548-1 %PFMA-2-FEX_STATUS: Fex 10P is
online
2012 Nov 13 10:40:27 N5548-1 %NOHMS-2-NOHMS_ENV_FEX_ONLINE:
FEX-10P On-line
2012 Nov 13 10:40:30 N5548-1 %PFMA-2-FEX_STATUS: Fex 10P is
online
```

Activity Verification

You have completed this task when you attain these results:

- Display the associated FEX.

```
N5548-1# 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: SSI160301NQ
  Extender Model: N2K-C2248TP-1GE,  Part No: 73-13232-01
  Card Id: 99, Mac Addr: 3c:ce:73:04:83:82, 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:
    Po100 - 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       Po100
       Eth10P/1/2  Down       Po100
       Eth10P/1/3  Down       Po100

     ...
```



```
Eth10P/1/48   Down       Po100
```

You should confirm that the state of the FEX is online.

- Display the associated ports to one uplink: Ethernet 1/15 interface

```
N5548-1# show interface ethernet 1/15 fex-intf
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
 Eth1/15
```

Why do you not see any host ports?

- Display the associated ports for the port channel interface:

```
N5548-1# show interface portchannel 100 fex-intf
Fabric           FEX
Interface        Interfaces
---------------------------------------------------
 Po100           Eth101/1/1    Eth101/1/2    Eth101/1/3
Eth101/1/4
                 Eth101/1/5    Eth101/1/6    Eth101/1/7
Eth101/1/8
                 Eth101/1/9    Eth101/1/10   Eth101/1/11
Eth101/1/12
                 Eth101/1/13   Eth101/1/14   Eth101/1/15
Eth101/1/16
                 Eth101/1/17   Eth101/1/18   Eth101/1/19
Eth101/1/20
                 Eth101/1/21   Eth101/1/22   Eth101/1/23
Eth101/1/24
                 Eth101/1/25   Eth101/1/26   Eth101/1/27
Eth101/1/28
                 Eth101/1/29   Eth101/1/30   Eth101/1/31
Eth101/1/32
                 Eth101/1/33   Eth101/1/34   Eth101/1/35
Eth101/1/36
                 Eth101/1/37   Eth101/1/38   Eth101/1/39
Eth101/1/40
                 Eth101/1/41   Eth101/1/42   Eth101/1/43
Eth101/1/44
                 Eth101/1/45   Eth101/1/46   Eth101/1/47
Eth101/1/48
```

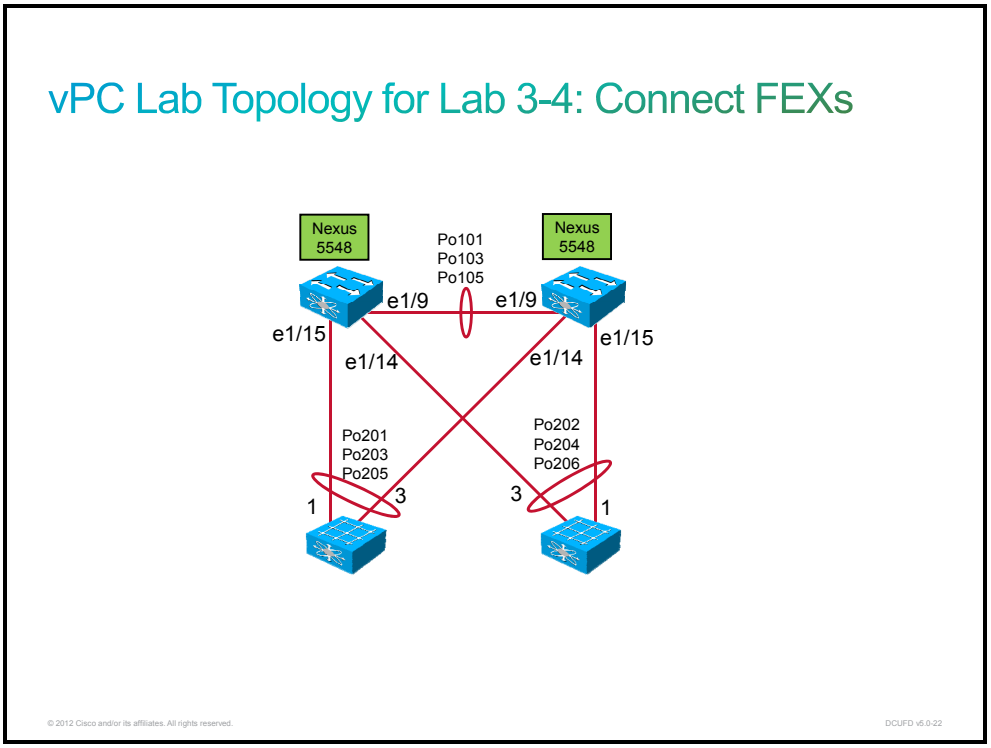
- Shut down one of the downlinks and display the information about the FEX:

```
N5548-1(config)# interface e1/15
N5548-1(config-if)# shutdown
N5548-1(config-if)# show interface portchannel 100 fex-intf
```

Re-enable the interface e1/15.

Task 3: Configure a vPC Between Cisco Nexus 5548 Switches and a Cisco Nexus 2248 FEX

In this task, you will multihome the FEX between a pair of Cisco Nexus 5548 Switches. You will configure the link to the Cisco Nexus 2248 FEX to be a vPC. In this task, you will need to work with your peer POD.



Activity Procedure

Complete these steps:

Step 1 On the Cisco Nexus 5548 Switch, remove the FEX configurations from the previous step. Also, e1/16 will not be used in this task.

```
N5548-1(config)# no interface portchannel 100
N5548-1(config)# interface e 1/16
N5548-1(config-if)# shut
```

Step 2 On the Cisco Nexus 5548 Switch, verify that the vPC feature has been enabled. If it is disabled, enable it.

```
N5548-1# show feature
Feature Name          Instance  State
--------------------  --------  --------
assoc_mgr             1         enabled
cimserver             1         disabled
fabric-binding        1         disabled
fc-port-security      1         disabled
fcoe                  1         enabled
fcsp                  1         disabled
fex                   1         enabled
fport-channel-trunk   1         disabled
```



```
http-server           1         enabled
interface-vlan        1         enabled
lacp                  1         enabled
ldap                  1         disabled
lldp                  1         enabled
niv                   1         disabled
npiv                  1         disabled
npv                   1         disabled
port_track            1         disabled
private-vlan          1         disabled
privilege             1         disabled
sshServer             1         enabled
tacacs                1         disabled
telnetServer          1         disabled
udld                  1         enabled
vpc                   1         disabled
vtp                   1         disabled

N5548-1(config)# feature vpc
```

Step 3 Create a vPC domain on the Cisco Nexus 5548 Switch.

Note Use the Job Aids section to determine the vPC domain ID.

```
N5548-1(config)# vpc domain 1XX
```

Step 4 Configure the keepalive link. You will use the management interface as a keepalive interface.

```
N5548-1(config-vpc-domain)# peer-keepalive destination
192.168.10.XX vrf management
```

Note Use the correct management IP address of your peer POD Cisco Nexus 5548 Switch. Refer to the Job Aids from Lab 1-2.

Step 5 Configure the vPC peer link that interconnects the Cisco Nexus 5548 Switches to be a port channel member. Refer to the Job Aids for the correct channel-group number to use.

```
N5548-1(config-vpc-domain)# interface e1/9
N5548-1(config-if)# channel-group 10X mode active
```

Step 6 Configure the vPC peer link.

```
N5548-1(config-if)# interface port-channel 10X
N5548-1(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.
N5548-1(config-if)# switchport mode trunk
```

Note Your peer POD must configure the vPC peer link on the peer Cisco Nexus 5548 Switch.

Step 7 Reconfigure the Cisco FEX links that you configured previously to attach the FEX. For this task, we will not use the second FEX link e1/16; rather, we will use the FEX interconnect interface e1/14. Note that e1/15 and e1/14 will *not* be in the same channel group. Refer to the Job Aids for the correct channel group number.

```
N5548-1(config)# interface e1/15
N5548-1(config-if)# channel-group 20P
N5548-1(config-if)# interface e1/14
N5548-1(config-if)# channel-group 20Q
```

Step 8 Create the port channel interfaces that will be used to connect both Cisco FEXs, and associate each FEX to that interface. Refer to the Job Aids for the vPC numbers.

```
N5548-1(config-if)# interface port-channel 20P
N5548-1(config-if)# switchport mode fex-fabric
N5548-1(config-if)# fex associate 10X
N5548-1(config-if)# vpc 20P

N5548-1(config-if)# interface port-channel 20Q
N5548-1(config-if)# switchport mode fex-fabric
N5548-1(config-if)# fex associate 10X
N5548-1(config-if)# vpc 20Q
```

Step 9 Change the fabric configuration on the Cisco FEX to allow for only one single link between the FEX and the managing switch:

```
N5548-1(config)# fex 10X
N5548-1(config-fex)# pinning max-links 1
Change in Max-links will cause traffic disruption.
```

Step 10 Verify the FEX status.

```
N5548-1# show fex
  FEX         FEX           FEX                      FEX
Number     Description      State            Model
Serial
------------------------------------------------------------------
10P        FEX010P               Online     N2K-C2248TP-1GE
SSI161500N7
10Q        FEX010Q               Online     N2K-C2248TP-1GE
SSI161507S2
```

Activity Verification

You have completed this task when you attain these results:

- Display the status of the vPC domain.

```
N5548-1# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC
peer-link

vPC domain id                     : 1XX
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : success
Type-2 consistency status         : success
```



```
vPC role                          : primary (or secondary)
Number of vPCs configured         : 98
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------------------
1    Po10P  up     1

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason
Active vlans
------ ----------- ------ ----------- ------------------------
-- -----------
20P    Po20P       up     success     success
-
20Q    Po20Q       up     success     success
-
102400 Eth10P/1/1  down*  Not         Consistency Check Not
-
                          Applicable  Performed
102401 Eth10P/1/2  down*  Not         Consistency Check Not
-
                          Applicable  Performed
….
102447 Eth10P/1/48 down*  Not         Consistency Check Not
-
                          Applicable  Performed
103424 Eth10Q/1/1  down*  Not         Consistency Check Not
-
                          Applicable  Performed
….
103471 Eth10Q/1/48 down*  Not         Consistency Check Not
-
                          Applicable  Performed
```

- Display the port channel summary information.

```
N5548-1# 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
--------------------------------------------------------------------
10X   Po10X(SU)   Eth      LACP      Eth1/9(P)
20P   Po20P(SU)   Eth      NONE      Eth1/15(P)
20Q   Po20Q(SU)   Eth      NONE      Eth1/14(P)
```

- Display the FEX information. You should see your FEX and the peer POD FEX.

```
N5548-1# show fex
  FEX         FEX           FEX                  FEX
Number    Description      State           Model
Serial
------------------------------------------------------------------
10P        FEX010P               Online     N2K-C2248TP-1GE
SSI161500N7
10Q        FEX010Q               Online     N2K-C2248TP-1GE
SSI161507S2
```


Lab 3-5: Interconnect Data Centers with Cisco OTV

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

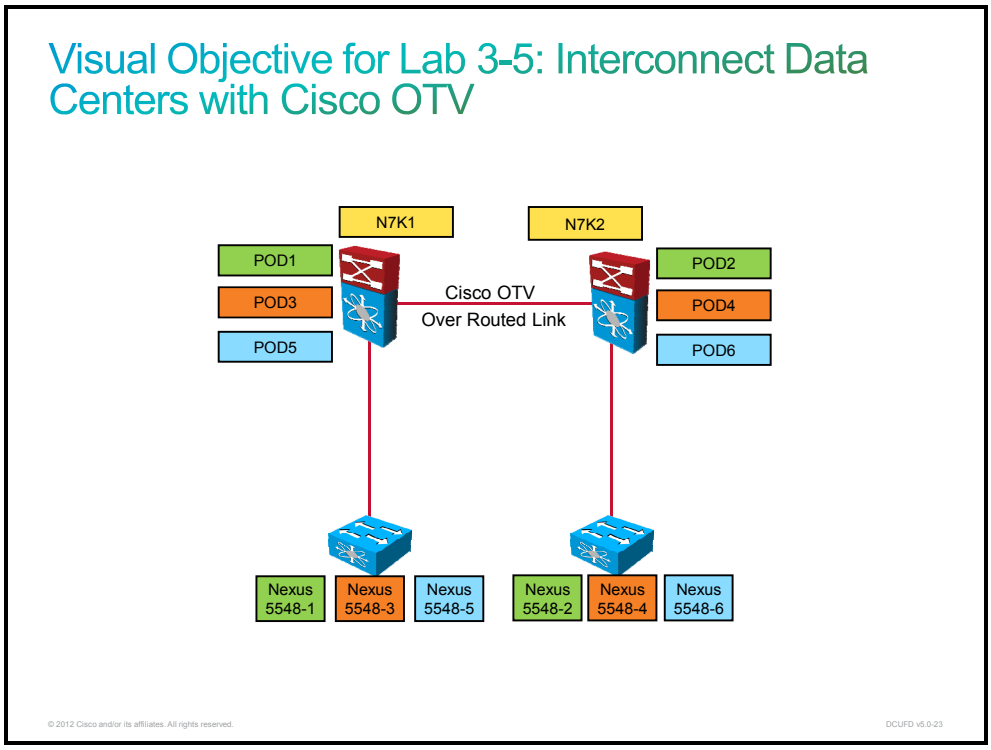
Activity Objective

In this activity, you will explore the data center interconnect with Cisco OTV. After completing this activity, you will be able to meet these objectives:

- Configure Cisco OTV between the two Cisco Nexus 7000 Series Switches

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:

- Two Cisco Nexus 7000 Series Switches with 32-port 10 Gigabit Ethernet F1 I/O Module
- One Cisco Nexus 5548 Switch per POD
- Student PC

Command List

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

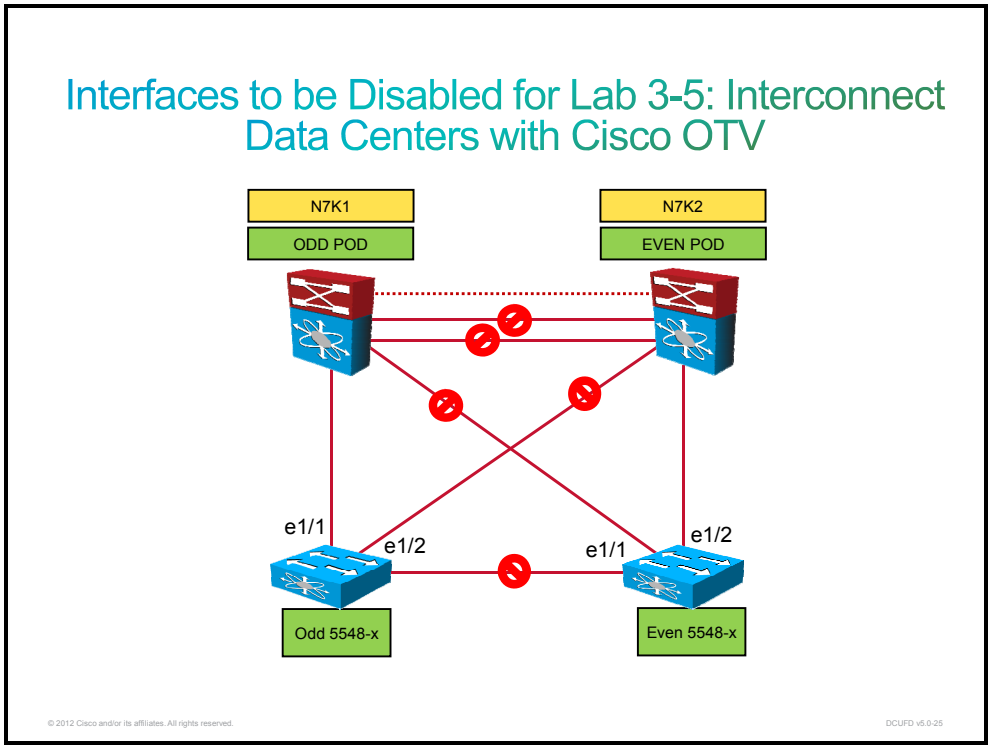
The Commands Used in the Interconnect Data Centers with Cisco OTV Lab

Command	Description
[no] shutdown	This command disables or enables an interface.
[no] switchport	This command enables or disables switched port mode (as opposed to routed port mode).
feature otv	This command enables the Cisco OTV feature.
interface ethernet num	This command enters interface configuration mode.
interface overlay num	This command creates an Cisco OTV overlay interface.
ip address ip/mask	This command configures an IP address on the interface.
ip igmp version 3	This command enables IGMPv3 on the interface.
ip route dest/mask nh	This command configures a static route.
otv control-group	This command configures an Cisco OTV control multicast group address.
otv data-group	This command configures an Cisco OTV data multicast group address.
otv extend-vlan num	This command defines which VLANs get extended over Cisco OTV.
otv join-interface num	This command defines the Cisco OTV join interface.
otv site-vlan num	This command sets the local Cisco OTV site VLAN number.
show otv overlay num	This command displays the status of the Cisco OTV overlay interface.
show port-channel summary	This command displays port channel summary information.
switchport trunk allowed vlan remove num	This command removes an allowed VLAN from a trunk link.

Job Aids

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

- Interfaces to be disabled to prepare the Cisco OTV topology:



- Cisco Nexus 5548 SVI IP addressing:

POD	Device	VLAN 10 SVI IP
POD 1	N5548-1	172.16.10.51
POD 2	N5548-2	172.16.10.52
POD 3	N5548-3	172.16.10.53
POD 4	N5548-4	172.16.10.54
POD 5	N5548-5	172.16.10.55
POD 6	N5548-6	172.16.10.56

- Cisco Nexus 7000 and Cisco OTV join interface IP addressing:

POD	Device-VDC	Cisco Nexus 7000 Interface	Cisco OTV Join Interface IP
POD 1	N7K1-POD1	e1/41	10.7.7.1
POD 2	N7K2-POD2	e3/41	10.7.7.2
POD 3	N7K1-POD3	e1/45	10.7.7.3
POD 4	N7K2-POD4	e3/45	10.7.7.4
POD 5	N7K2-POD5	e1/47	10.7.7.5

POD	Device-VDC	Cisco Nexus 7000 Interface	Cisco OTV Join Interface IP
POD 6	N7K2-POD6	e3/47	10.7.7.6

- Cisco Nexus 7000 Series Switch multicast IP addressing:

POD	Cisco OTV Multicast Control Group	Cisco OTV Multicast Data Group IP Range
All PODs	239.7.7.7	232.7.7.0/24

Task 1: Configure Cisco OTV

In this task, you will configure Cisco OTV between two Cisco Nexus 7000 Series VDCs in your lab. You will extend a VLAN from one access POD to another access POD across a Layer 3 routed network.

Activity Procedure

Complete these steps:

Step 1 Connect to your assigned Cisco Nexus 7000 Series VDC and remove the vPC configuration from the previous lab.

```
N7K1-POD1(config)# no feature vpc
```

Step 2 Check if there are any configured port channels that were created in previous labs. If there are, remove them. Also, configure the interface to your Cisco Nexus 7000 Series Switch peer.

```
N7K1-POD1(config)# show port-channel summary
N7K1-POD1(config)# no interface port-channel XXX
N7K1-POD1(config)# interface e X/XX
N7K1-POD1(config-if)# switchport mode trunk
N7K1-POD1(config-if)# no shut
```

Note Refer to the Job Aid for the correct interface to use between the POD Cisco Nexus 7000's. Removing a port channel interface also automatically removes the channel group commands from the physical interfaces that are associated with that port channel.

Step 3 Create VLANs 10 through 13 on both Cisco Nexus 7000 Series VDCs.

```
N7K1-POD1(config)# vlan 10-13
```

Step 4 Shut down the interface on your Cisco Nexus 7000 Series VDC that leads to your peer POD Cisco Nexus 5548 Switch. Also shut down the two interfaces on each pair of peer Cisco Nexus 7000 Series switches. Use the "Interfaces to be disabled" job aid to find the correct interface.

```
N7K1-POD1(config)# interface ethernet 4/XX, e 4/XX, e 4/XX
N7K1-POD1(config-if)# shutdown
```

Step 5 Configure the interface that is going to your Cisco Nexus 5548 Switch.

```
N7K1-POD1(config-if)# interface Ethernet 4/XX
N7K1-POD1(config-if)# switchport mode trunk
```

Step 6 Connect to your assigned Cisco Nexus 5548 Switch. Verify that there is no residual port channel configuration on it. Also, shut down the interfaces to your peer Cisco Nexus 5548 Switch and to the Cisco FEX interfaces from the previous lab.


```
N5548-1#show port-channel summary
N5548-1(config)# no interface port-channel XXX
N5548-1(config)# interface e1/9-10
N5548-1(config-if-range)# shut
N5548-1(config-if-range)# interface e1/14-16
N5548-1(config-if-range)# shut
```

Step 7 Configure the interface to your Cisco Nexus 7000 Series POD.

```
N5548-1(config-if-range)# interface e 1/X
N5548-1(config-if-range)# switchport mode trunk
N5548-1(config-if-range)# no shut
```

Step 8 Create VLAN 10 on the Cisco Nexus 5548 Switch.

```
N5548-1(config)# vlan 10
```

Step 9 Configure an SVI on your Cisco Nexus 5548 Switch for VLAN 10. Assign IP address 172.16.10.5P/24 to it, where P is your POD number.

```
N5548-1(config)# feature interface-vlan
N5548-1(config)# interface vlan 10
N5548-1(config-if)# ip address 172.16.10.5P/24
N5548-1(config-if)# no shutdown
```

Step 10 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.

```
N5548-1# 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
```

Step 11 Do *not* proceed to the next step until you succeed in pinging the peer POD Cisco Nexus 5548 Switch VLAN 10 IP address. Troubleshoot together with your peer POD, as necessary.

Step 12 Change the interface on your Cisco Nexus 7000 Series VDC that connects your peer Cisco Nexus 7000 Series VDC to a routed port. Use the "Lab Connections" job aid to determine the correct interface.

```
N7K1-POD1(config)# interface ethernet X/XX
N7K1-POD1(config-if)# no switchport
```

Step 13 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 VDC.

```
N7K1-POD1(config-if)# ip address 10.7.7.P/24
```

Step 14 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.

```
N7K1-POD1# 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 Cisco OTV join interface. Do not proceed to the next step until you have verified IP connectivity between the VDCs for this link.

Step 15 Verify that you can no longer ping from your Cisco Nexus 5548 Switch to your peer POD Cisco Nexus 5548 Switch on VLAN 10.

```
N5548-1# 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 Why are you now unable to ping between the Cisco Nexus 5548 Switches?

Note If you can still ping to the peer Cisco Nexus 5548 Switch, verify that you have shut down the trunk from your Cisco Nexus 7000 Series VDC to your peer POD Cisco Nexus 5548 Switch. You should not be able to ping between the Cisco Nexus 5548 Switches in your POD and peer POD until Cisco OTV has been configured to extend VLAN 10 between the PODs.

Step 17 Examine the license usage on your Cisco Nexus 7000 Series VDC.

```
N7K1-POD1# 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 18 Enable the Cisco OTV feature.

```
N7K1-POD1(config)# feature otv
```

Step 19 Examine the license usage again.

```
N7K1-POD1# 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 -
--------------------------------------------------------------
```

Q1) Which license does the OTV feature require?

Step 20 Configure VLAN 13 as the Cisco OTV site VLAN.

```
N7K1-POD1(config)# otv site-vlan 13
```

Step 21 Configure the Cisco OTV join interface to use IGMP version 3. Refer to the Job Aids to confirm the interface that you should use.

```
N7K1-POD1(config)# interface ethernet X/XX
N7K1-POD1(config-if)# ip igmp version 3
```

Step 22 Increase the MTU on this interface to the maximum of 9216 bytes.

```
N7K1-POD1(config-if)# mtu 9216
```

Step 23 Create a Cisco OTV overlay interface 1. Configure it to use the interface that connects your Cisco Nexus 7000 Series VDC to your peer POD VDC as the join interface.

```
N7K1-POD1(config)# interface overlay 1
N7K1-POD1(config-if-overlay)# otv join-interface ethernet X/XX
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 24 Configure multicast group 239.7.7.7 as the Cisco OTV control multicast group.

```
N7K1-POD1(config-if-overlay)# otv control-group 239.7.7.7
```

Step 25 Configure the multicast range 232.7.7.0/24 as the SSM group range for Cisco OTV multicast data.

```
N7K1-POD1(config-if-overlay)# otv data-group 232.7.7.0/24
```

Step 26 Extend VLANs 10–12 across the overlay.

```
N7K1-POD1(config-if-overlay)# otv extend-vlan 10-12
```

Step 27 Configure the OTV site identifier, where P is your POD number. Even though there is only a single edge device, the lack of a site identifier will not bring up the extended VLANs into the active state (confirm with **show otv vlan**).

```
N7K1-POD1(config-if-overlay)# otv site-identifer 0xP
```

Step 28 Examine the overlay interface.

```
N7K1-POD1# show otv overlay 1
OTV Overlay Information
Site Identifier 0000.0000.000P

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) : EthX/X (10.7.7.P)
Site vlan : 13 (up)
AED-Capable          : No (Overlay is Down)
Capability           : Multicast-Reachable
```

Step 29 Enable the overlay interface.

```
N7K1-POD1(config)# interface overlay 1
N7K1-POD1(config-if-overlay)# no shutdown
```

Step 30 Examine the overlay interface again.

```
N7K1-POD1# show otv overlay 1
OTV Overlay Information
Site Identifier 0000.0000.000P

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) : EthX/X (10.7.7.P)
Site vlan : 13 (up)
AED-Capable          : No (Site id is not configured)
Capability           : Multicast-Reachable
```

Step 31 Verify that your VDC has established a Cisco OTV adjacency with the VDC in your peer POD.

```
N7K1-POD1# show otv adjacency
Overlay Adjacency database
Overlay-Interface Overlay1 :
Hostname System-ID Dest Addr Up Time
State
N7K2-PODX 0026.9804.a944 10.7.7.Q 00:01:30 UP
```

Step 32 Examine the Cisco OTV MAC routing table to see if any MAC addresses were learned.

```
N7K1-POD1# show otv route
```

Step 33 Do you see any MAC addresses in the Cisco OTV MAC routing table? Why or why not?

Step 34 Switch to your Cisco Nexus 5548 Switch. Ping the IP address of your peer POD 172.16.10.5Q from your Cisco Nexus 5548 Switch, where Q is your peer POD number.

```
N5548-1# 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 35 Switch back to your Cisco Nexus 7000 Series VDC. Examine the Cisco OTV MAC routing table again.

```
N7K1-POD1# show otv route
OTV Unicast MAC Routing Table For Overlay1
VLAN MAC-Address     Metric  Uptime    Owner      Next-hop(s)
---- --------------  ------  --------  ---------  -----------
  10 547f.eea4.4a69  42      00:04:12  overlay    N7K2-PODQ
  10 547f.eea4.4abc  42      00:03:44  overlay    N7000-2-PODQ
  10 547f.eea4.d968  1       00:04:19  site       Ethernet4/X
  10 547f.eea4.d9bc  1       00:03:43  site       Ethernet4/X
```

Step 36 Examine the Cisco OTV ARP cache.

```
N7K1-POD1# 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 547f.eea4.4abc 172.16.10.5Q 00:04:37 00:03:22
```

Step 37 Examine the spanning-tree topology for VLAN 10.

```
N7K1-POD1# 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
---------------- ---- --- --------- -------- --------------------
Eth4/X Desg FWD 2000 128.137 Network P2p
```

Step 38 Which bridge is the root of the spanning tree for VLAN 10?

Step 39 Ask your lab partners in the peer POD which bridge is listed as the root of the spanning tree on their VDC. Is it the same? If not, can you explain why?

Activity Verification

You have completed this task when you attain these results:

- Remove the unnecessary configurations from the previous lab.
- Successfully establish a Cisco OTV adjacency between your Cisco Nexus 7000 Series VDC and your peer POD VDC.
- Successfully extend VLAN 10 across the Cisco OTV overlay.
- Examine Cisco OTV and spanning-tree operation.

Case Study 3-6: Design VLAN Extension

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

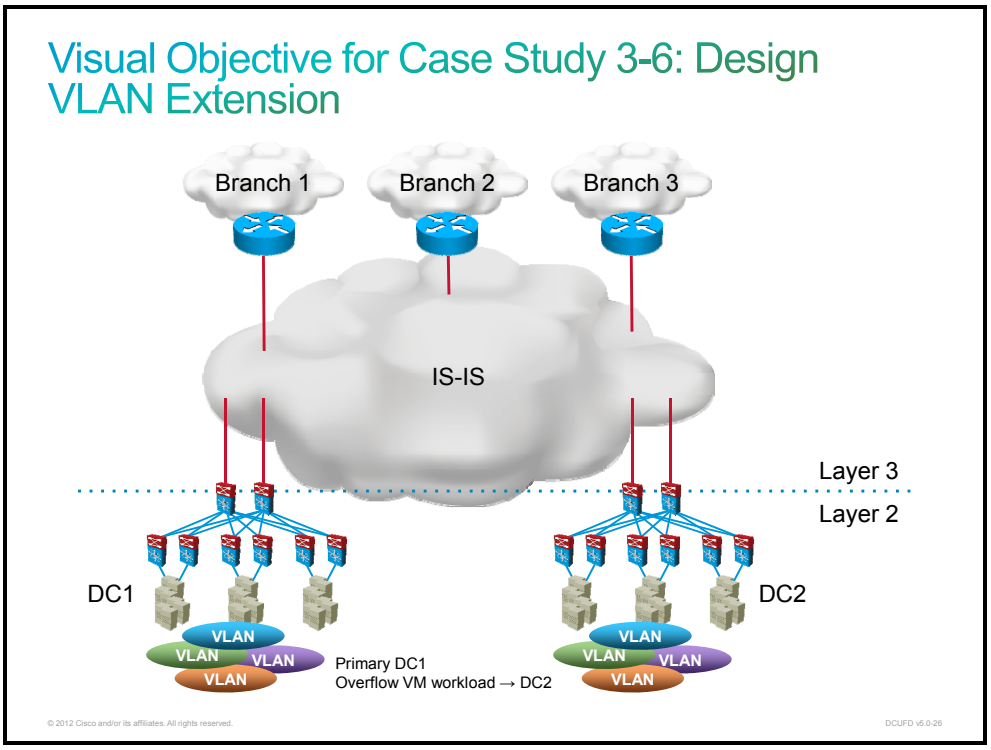
Activity Objective

In this activity, you will design the deployment of a VLAN extension between data centers. After completing this activity, you will be able to meet these objectives:

- List the reasons for VLAN extension between data centers
- Evaluate potential solutions for VLAN extension

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:

- No resources are required.

Command List

There are no commands used in this activity as it is purely a paper-based activity and does not include any device configuration.

Job Aids

There are no particular job aids for this activity.

Task 1: Become Familiar with the Network

Introduction

The company ACME Enterprises has upgraded their data center with Cisco Nexus 7000 Series Switches as core switches and Cisco Nexus 5548 Switches as their aggregation switches. This has been a considerable expense for the company and they have run out of the CAPEX budget expenses for the year.

The company has two data centers and both have been upgraded with new Nexus switches, replacing the previous Catalyst 6500-based data center core.

The company has a network that interconnects the main location with the primary data center, the location of the secondary data center, and three other locations where they have branch offices of various sizes.

Altogether, some 700 employees use the services of the data center. Some of their customers also use the data center to facilitate essential business processes of ACME Enterprises.

ACME Enterprises uses virtualization extensively for the compute layer. During the previous year they invested in virtualization and most of their servers are now virtualized.

Requirements

The company wants to take advantage of new equipment and would like to start using virtual machine mobility between data centers. This would help them greatly in situations where the virtualization hosts cluster would be at its maximum capacity during peak utilization times. The primary services would be provided by their primary data center.

Investing in a new link between data centers is not an option at this moment. However, they have purchased the following licenses for their Cisco Nexus 7000 Series Switches because they were in a promotion bundle:

- LAN_ADVANCED_SERVICES_PKG
- LAN_TRANSPORT_SERVICES_PKG

Additional requirements for the solution would be redundancy and load sharing between the two data centers.

Ideally, the company would like to have no manual intervention be necessary to the VM when a virtual machine is moved from one data center to another, for example, no change in IP address or default gateway configuration.

Task 2: Evaluate the Options for the Inter-Data Center Link

The company has considered a couple of options:

- Dark fiber between their Cisco Nexus 7000 Series Switches
- Overlay Transport Virtualization

Dark Fiber

The company would use dark fiber to interconnect the Cisco Nexus 7000 Series Switches. The first Cisco Nexus 7000 Series Switch in DC1 would be connected to the first Cisco Nexus 7000 Series Switch in DC2, and the second Cisco Nexus 7000 Series Switches would be interconnected in the same way.

The links would then be configured as a vPC to ensure load balancing on the link, and link redundancy.

However, the dark fiber link would require a substantial investment and the company is out of budget for this year.

Overlay Transport Virtualization

The company has its own network that interconnects the sites and is based on IS-IS. As already mentioned, the company has purchased the Cisco Nexus 7000 Series Switches with a promotional license bundle that allows them to use VDCs and Cisco OTV.

Describe a solution that would take the advantage of the Cisco Nexus 7000 Series Switch features.

How many VDCs would be needed to accommodate Cisco OTV on the Cisco Nexus 7000 Series Switch?

Do they need support for jumbo frames over the data center interconnect link?

Task 3: Determine the Paths for Outgoing Traffic

The Cisco Nexus 7000 Series Switches are configured with HSRP and provide a redundant default gateway service.

The company has tested a couple of virtual machine move events across the test deployment of the inter-data center link and has discovered that virtual machines use the default gateway in their original data center regardless of their location.

Connecting to the VM and setting the new IP default gateway is one solution, but this has to be repeated every time a virtual machine moves.

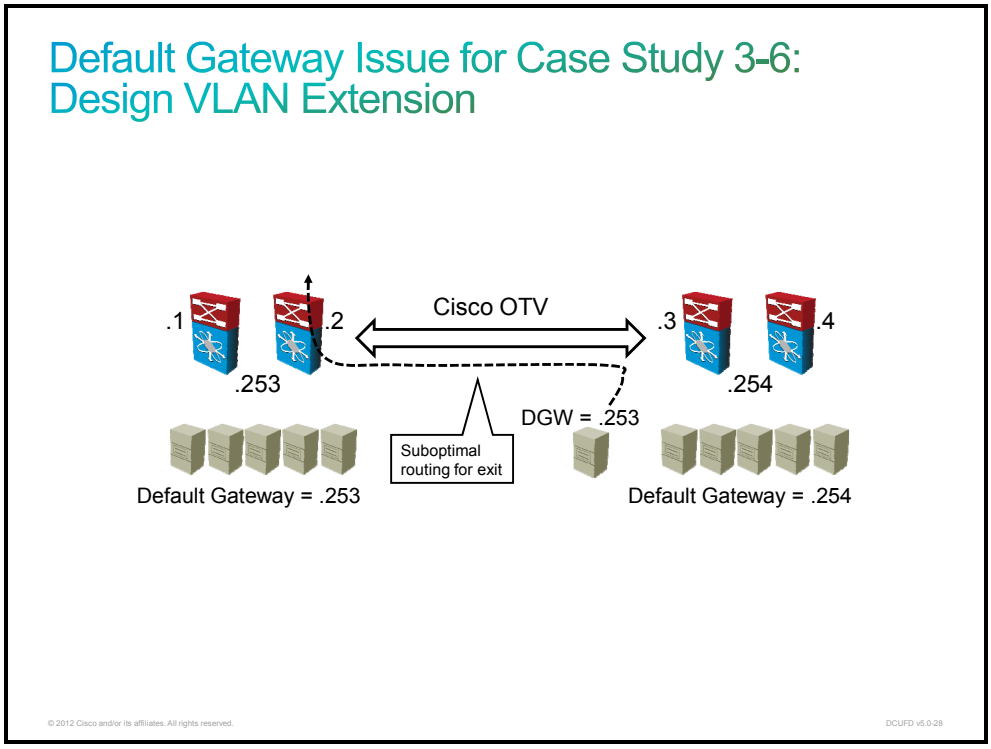
How can this problem be solved? Consider the following options:

- Run HSRP/GLBP only in DC1.
- Run HSRP with different groups and IP addresses for both data centers.
- Run the same HSRP group IP address.

Elaborate on the best option.

Task 4: Optimize the Traffic Between Branch and Data Center

With the data center interconnect and default gateway issues in place, you would like to optimize the flow of data from the branch offices to particular virtual machines that can move between data centers.



The company is considering two options:

- Add a host route to the IS-IS routing domain when a virtual machine moves, and remove the host route when the VM moves back to the primary data center
- Use LISP VM mobility between the data center and branch offices

Elaborate on the best option. How would you implement traffic flow optimization?

Case Study 4-1: Design Cisco Unified Fabric

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

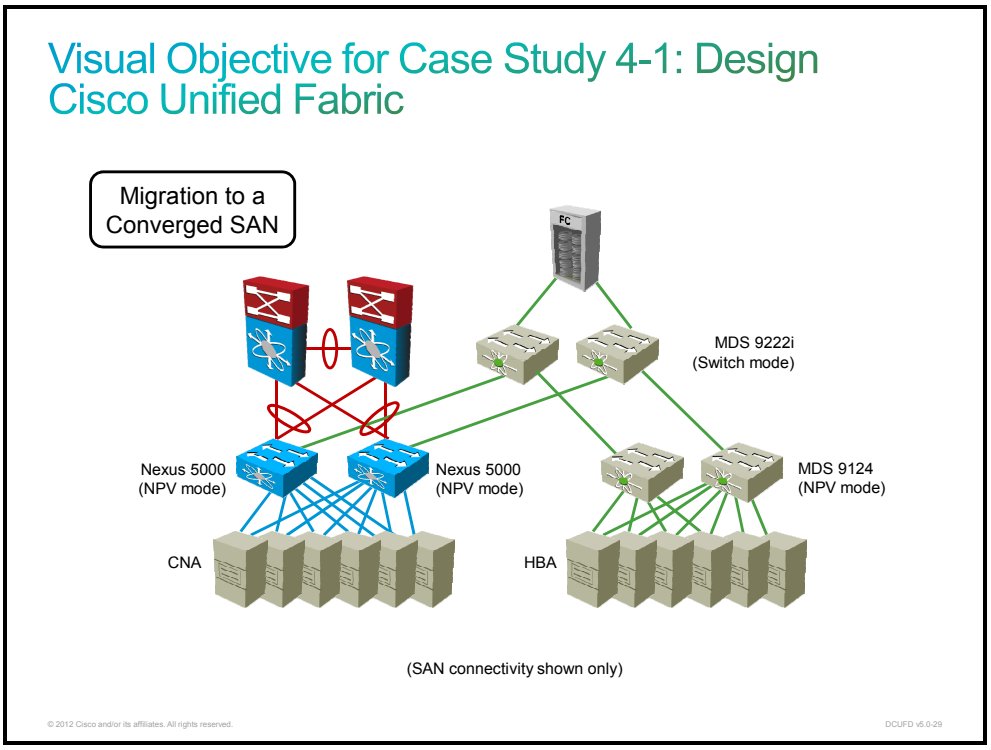
Activity Objective

In this activity, you will design the deployment of Cisco Unified Fabric. After completing this activity, you will be able to meet these objectives:

- Evaluate a design using Cisco Unified Fabric

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:

- No resources are required.

Command List

There are no commands used in this activity as it is purely a paper-based activity and does not include any device configuration.

Job Aids

There are no particular job aids for this activity.

Task 1: Examine the Current Topology

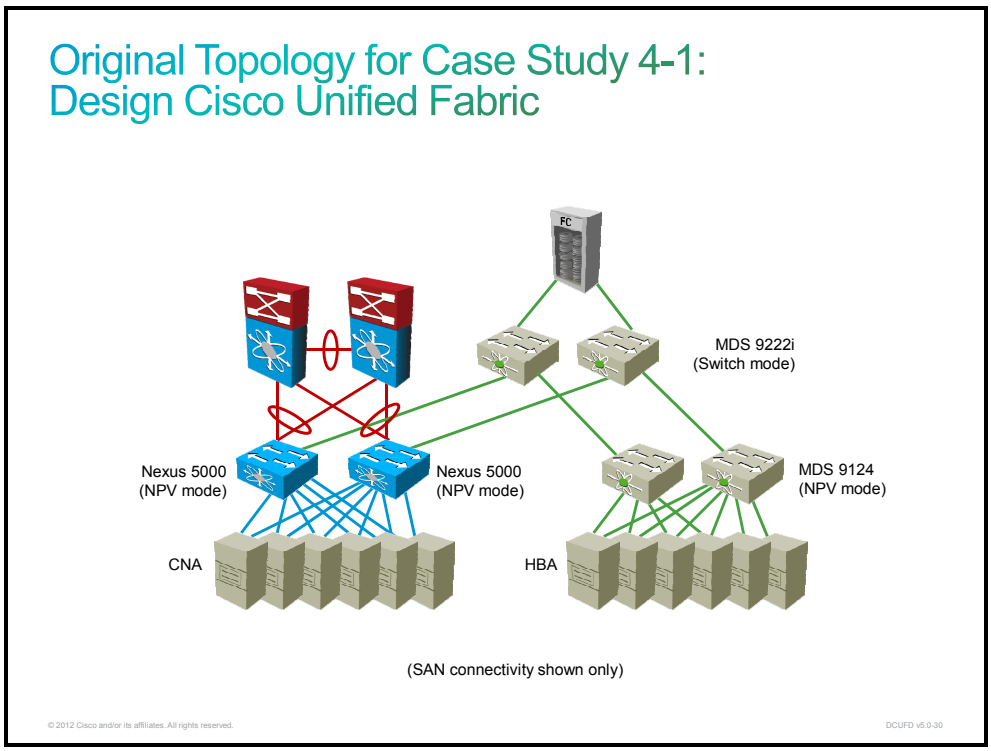
Introduction

The Relaxo Company is a medium-sized company that operates in the cosmetics industry. At their central office, they are using a data center that was established four years ago when the company had to restructure to cope with its own growth.

At that time they deployed state-of-the-art equipment in their data center, which featured Cisco Unified Fabric.

Their data center consisted of two aggregation blocks that were linked by a small core. The first block consisted of their existing equipment, and the new block was constructed using a pair of Cisco Nexus 7000 Series aggregation and collapsed core switches.

Cisco Unified Fabric was implemented using the only approach that was available at the time. The "direct attach" approach was used, where servers were attached to the Cisco Nexus 5548 Switches, and those were connected to the MDS Fibre Channel fabric.



The new servers were attached using CNAs to the Cisco Nexus 5548 Switch, which was connected to the Cisco MDS switch.

The older servers were attached traditionally, with a NIC connecting them to the data network, and with an HBA connecting them to the storage fabric.

Storage Upgrade

The old storage is running out of capacity and the company has been looking for options to procure modern storage with the following characteristics:

- Multitiered storage with automatic tiering, with the following three storage tiers:
  - High-speed SSD Flash drives
  - High-speed SAS hard drives for data that is often accessed
  - High-capacity, lower-cost SATA drives for storage of bulk data

- Converged interfaces on the storage processor, allowing for both Fibre Channel native connectivity and FCoE connectivity

The upgraded storage features both native Fibre Channel and converged FCoE connectivity. The company is considering extending the FCoE network to the storage directly, bypassing the MDS switch for traffic originating on CNA-attached servers.

Cisco Nexus 7000 Series Switches Upgrade

Along with the new storage, the company has acquired a pair of 32-port 10 Gigabit Ethernet I/O modules with an F1 forwarding engine for their Cisco Nexus 7000 Series Switches. These switches are intended to perform SAN aggregation.

Task 2: Evaluate Multiple Converged SAN Solutions

In this task, you will draft and evaluate multiple converged SAN solutions for CNA-connected servers.

Converged SAN Topology

Outline the new SAN topology. Consider the intent that the Cisco Nexus 7000 Series Switch can form SAN aggregation in a storage VDC.

Cisco MDS 9222i SAN-Based Services

The Cisco MDS 9222i Modular Switch offers SAN-based services that can be useful tools to perform data migration, write acceleration, and so on.

The new storage array has ample capacity at this moment. Considering that the new storage has multiple tiers, is it worth migrating data from the old storage array to the new one? What are the possible uses of the current (old) storage appliance?

With the help of the Cisco MDS 9222i Modular Switch, how can the company consolidate its storage space?

Task 3: Evaluate Future Expansion Readiness

In addition to FCoE, the storage array has the possibility to add iSCSI connectivity to the storage processors in the same way as the FCoE connectivity is added.

Assess the value of iSCSI connectivity.

From the migration to the converged SAN, the company has a pair of Cisco MDS 9222i Modular Switches that have IP connectivity. Because they have the new primary storage, they could relocate the old storage array to one of the branch offices and replicate critical data.

Outline a possible solution.

Answer Key

The correct answers and expected solutions for the activities that are described in this guide appear here.

Case Study 1-1 Answer Key: Design a Migration to vPC

This is an example solution for the specifications stated in the case study:

Task 1: Analyze the Spanning Tree Topology

The supervisor engine on the Catalyst 6500 uses the PFC-3B hardware forwarding engine, which does not support multilink aggregation. Instead, it runs pure Spanning Tree Protocol, which blocks half of the links from access to the aggregation and collapsed core.

To support VSS, the Catalyst 6500 supervisors would need to be one of the following types:

- Supervisor Engine 720-10GE with PFC-3C or 3CXL
- Supervisor Engine 2T

Q1) What are the main congestion points in this network?

A) The main congestion points are the links between the Catalyst 4900M and the Catalyst 6500, and the links from the existing blade chassis.

Cisco UCS uses its interfaces in EHV mode and uses both uplinks from every switch for forwarding.

Q2) What could be improved?

A) The easiest improvement is enabling vPCs whenever possible. By installing the Nexus 7009 as the core switch, you can enable VSS from the Catalyst 4900M switches, and to the blade chassis embedded switches.

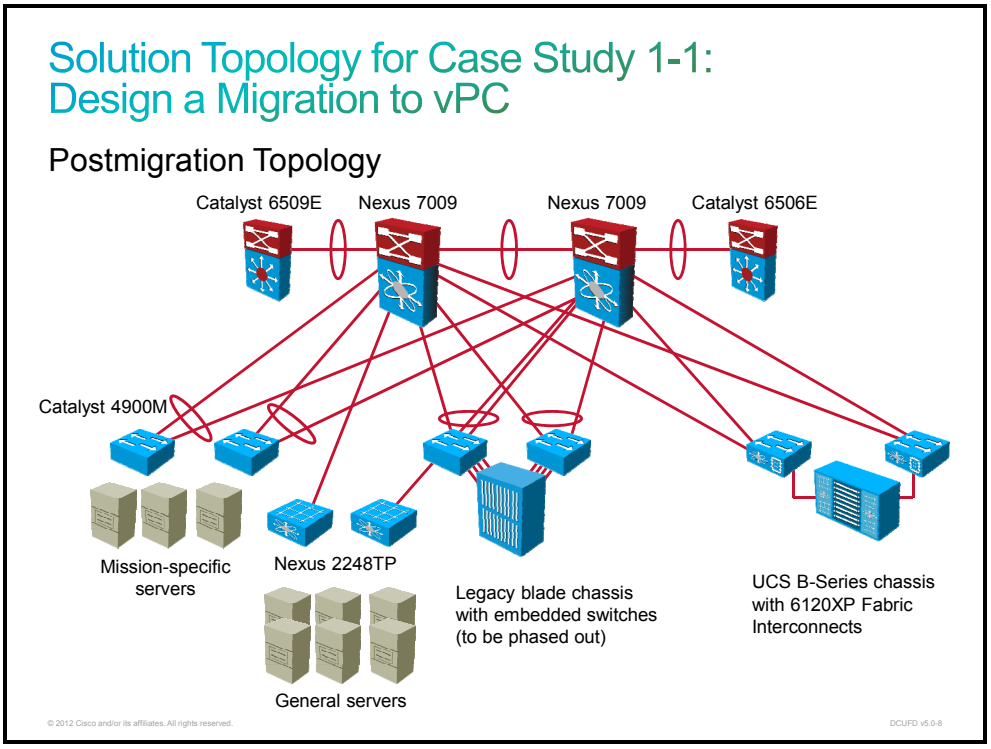
Additionally, you can move some of the 1 Gigabit Ethernet attached servers from the Catalyst 4900M to the FEX, further relieving the uplinks from the Catalyst 4900M to reduce the possibility of the congestion for the mission-specific servers.

Task 2: Design a vPC Topology

vPC connections will be configured toward the following switches:

- A pair of Catalyst 4900M switches
- A pair of blade switches on the existing blade chassis
- Regular port channel will be deployed for the connections to the FEX
- No changes to the uplinks of the Cisco UCS 6120XP fabric interconnects, because they use the EHV mode, which is the recommended operation mode.

The Cisco Nexus 7009 uses the M1 I/O modules with the M1 forwarding engine to retain routing capabilities that were previously used on the Cisco Catalyst 6500. The N7K-M132XP-12L is necessary to connect the FEXs.



The upgrade of the core switches achieved the following:

- Higher bandwidth is available to the mission-specific server on the Cisco Catalyst 4900M because both uplinks are in forwarding mode through the vPC and because general servers were moved to the Cisco FEXs.
- There is no added network complexity due to the Cisco FEXs. They are managed through the Cisco Nexus 7009 Switches.
- Higher bandwidth is available for the existing blade chassis.
- Services that are still running on the Cisco Catalyst 6500 chassis can be connected to the core switches using a vPC or using a port channel until a decision is made to upgrade or phase out these switches.

Task 3: Future Readiness Assessment

The Cisco Nexus 7000 Series Switches can be used in many other ways:

- By implementing vPCs, you can further segment the core switch into several logical switches, allowing for better separation of the data center network into security zones, or to perform a migration to a more structured network (core VDC to aggregation VDC).
- Cisco FabricPath can be used if the access switches are migrated to Cisco Nexus 5548 Switches, or if the data center expands further.
- The Cisco Catalyst 6500 chassis can be repurposed by installing new supervisor engines and a conversion to the service chassis. The current firewall module (the FWSM) can be upgraded to a new Cisco ASA-SM module. The switch can be put in VSS mode, and connected using a MEC to the pair of Cisco Nexus 7009 Switches.

Lab 1-2 Answer Key: Become Familiar with the Lab Equipment

The tasks in this lab are procedural and guide the student to the solution. Therefore, the lab has no answer key.

Lab 3-1 Answer Key: Explore VDCs

The tasks in this lab are procedural and guide the student to the solution. Therefore, the lab has no answer key.

Lab 3-2 Answer Key: Examine vPC

The tasks in this lab are procedural and guide the student to the solution. Therefore, the lab has no answer key.

Lab 3-3 Answer Key: Explore Cisco FabricPath

The tasks in this lab are procedural and guide the student to the solution. Therefore, the lab has no answer key.

Lab 3-4 Answer Key: Connect FEXs

The tasks in this lab are procedural and guide the student to the solution. Therefore, the lab has no answer key.

Lab 3-5 Answer Key: Interconnect Data Centers with Cisco OTV

The tasks in this lab are procedural and guide the student to the solution. Therefore, the lab has no answer key.

Task 1: Configure Cisco OTV

Q1) Which license does the OTV feature require?

The Transport Services Package (LAN_TRANSPORT_SERVICES_PKG) license is required to run OTV.

Case Study 3-6 Answer Key: Design VLAN Extension

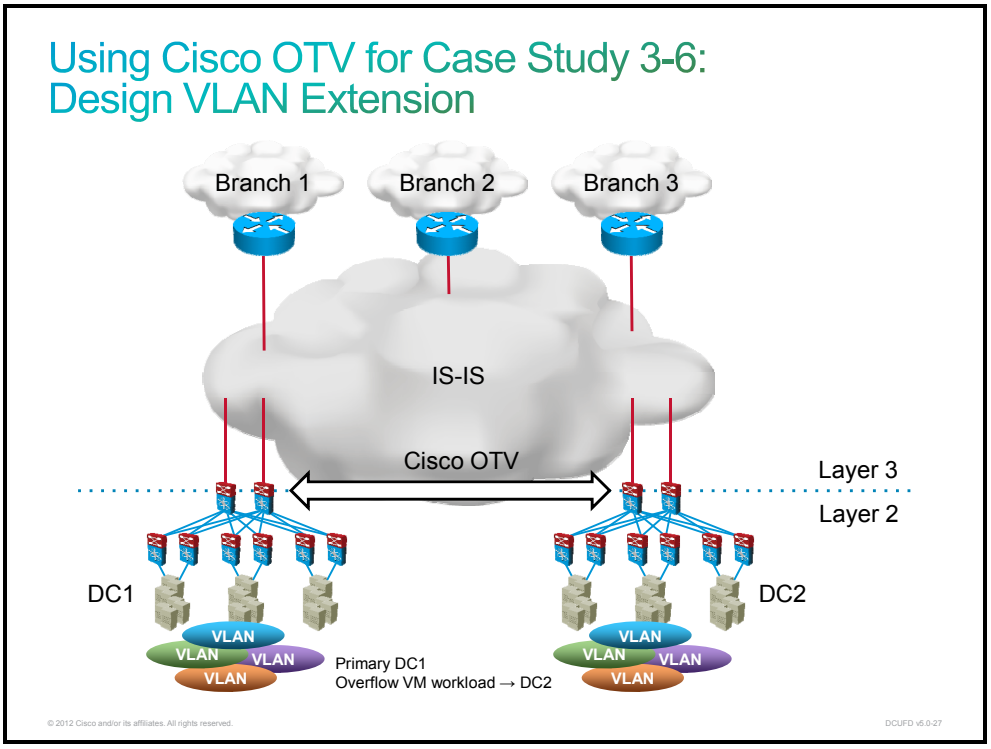
This is an example solution for the specifications stated in the case study:

Task 1: Become Familiar with the Network

- Both licenses allow deployment of Cisco OTV, VDCs, and Cisco FabricPath.

Task 2: Evaluate the Options for the Inter-Data Center Link

- The best solution in these circumstances would be Cisco OTV deployment because no additional investment is required.



- Multicast control plane data would need to be carried across the IS-IS domain.
- Two VDCs would be needed, with Cisco OTV being deployed in a dedicated VDC. This is because Cisco OTV and SVI interfaces cannot coexist for the same VLAN in the same VDC.

Task 3: Determine the Paths for Outgoing Traffic

- Running different HSRP group IP addresses in both data centers would require changing the VM default gateway configuration, either manually or by using a script.
- Running the same HSRP group in both data centers solves this issue, but requires HSRP traffic to be blocked over the Cisco OTV link.

Task 4: Optimize the Traffic Between Branch and Data Center

- The host route could be added for a VM that has moved between data centers. The same script that corrects the VM default gateway IP address could perform this action.
- Alternatively, an LISP infrastructure can be deployed, where LISP monitors movement of virtual machines and routes traffic to the correct location.

Case Study 4-1 Answer Key: Design Cisco Unified Fabric

This is an example solution for the specifications stated in the case study:

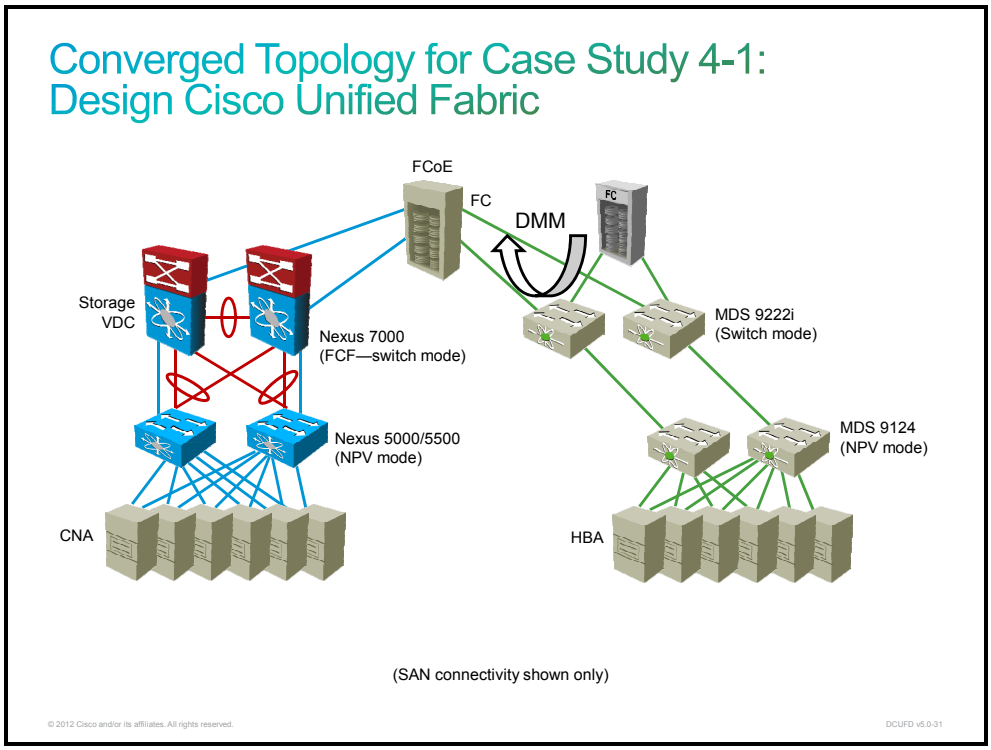
Task 1: Examine the Current Topology

This task is procedural and guides the student to the solution. Therefore, the task has no answer key.

Task 2: Evaluate Multiple Converged SAN Solutions

- Converged SAN topology:

The migration to the new storage array and the migration to the FCoE SAN aggregation can be done as shown in the figure:



This solution provides the best scalability for the Cisco Unified Fabric part of the network, and retains the same configuration for the part of the network without unified fabric, requiring no changes to the nonconverged fabric.

FCoE connections are aggregated on the Cisco Nexus 7000 Series Switches and perform the FCoE FCF role. Additional links are provisioned from the Cisco Nexus 5548 Switch to transport SAN traffic. These are VE-to-VE links and are topologically equivalent to the links from the Cisco Nexus 5548 Switch to the Cisco MDS 9222i Modular Switch. These links are 10 Gigabit Ethernet with DCB (FCoE).

- Cisco MDS 9222i SAN-Based Services

Using the dynamic mobility manager feature on the Cisco MDS 9222i Modular Switch, the company can migrate the LUNs from the old storage array to the new storage array. The replication is SAN-based and performed by the Cisco MDS 9222i. Once the LUNs are migrated, the servers can use the new storage.

Task 3: Evaluate Future Expansion Readiness

- iSCSI connectivity:

At this point, the iSCSI connectivity available on the storage array does not have much value. New servers in the future will be connected to the converged SAN using FCoE. Old servers will slowly be phased out and virtualized.

- Storage replication of critical data:

The pair of Cisco MDS 9222i Modular Switches can be used to provide transport of Fibre Channel traffic over the WAN. The new storage array can be configured to replicate to the old storage array, and the Cisco MDS 9222i switches can be configured to encapsulate Fibre Channel traffic over IP using the FCIP protocol.