

Introduction to Cisco Data Center Technology

Version 1.0

Fast Lane LAB Guide

Version 1.0.3

ATTENTION

The Information contained in this guide is intended for training purposes only. This guide contains information and activities that, while beneficial for purposes of training in a close, non-production environment, can result in downtime or other severe consequences and therefore are not intended as a reference guide. This guide is not a technical reference and should not, under any circumstances be used in a production environment. Customers should refer to the published specifications applicable to specific products for technical information. The information in this guide is distributed AS IS, and the use of this information or implementation of any recommendations or techniques herein is a customer's responsibility.

COPYRIGHT



© 2013 Fast Lane GmbH. All rights reserved.

All other brands and product names are trademarks of their respective owners.

No part of this book covered by copyright may be reproduced in any form or by any means (graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system) without prior written permission of the copyright owner. Fast Lane reserves the right to change any products described herein at any time and without notice. Fast Lane assumes no responsibility or liability arising from the use of products or materials described herein, except as expressly agreed to in writing by Fast Lane. The use or purchase of this product or materials does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Fast Lane products described in this manual may be protected by one or more patents, foreign patents, or pending applications.

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:

- Activity 1-1: Cisco Power Calculator (Instructor Demonstration Only)
- Lab 1-1: Connecting to a Cisco Nexus 7000 Series Switch Using SSH
- Lab 1-2: Cisco Nexus 5000 Series Switch Initial Setup Script
- Lab 1-3: Connecting to a Cisco Nexus 5000 Series Switch Using SSH
- Lab 1-4: Running CLI Commands
- Lab 1-5: Configuring vPCs
- Lab 1-6: Validating Cisco FabricPath Configuration
- Lab 1-7: Validating OTV Configuration
- Lab 2-1: Verifying Current VDC Settings
- Lab 2-2: Validating a Cisco Nexus 2000 Series Fabric Extender Configuration
- Lab 2-3: Validating a Cisco Nexus 1000V Series Switch Configuration
- Lab 3-1: Cisco MDS 9100 Series Multilayer Fabric Switch Initial Setup
- Lab 3-2: Validating a Cisco MDS 9100 Series Multilayer Fabric Switch License
- Lab 3-3: Configuring VSANs and Zoning
- Lab 3-4: Validating FLOGI and FCNS
- Lab 3-5: Viewing the tech-support Command Output
- Lab 4-1: Validating the Physical Connections for FCoE
- Lab 5-1: Cisco UCS
- Lab 5-2: Exploring the Cisco UCS Manager GUI
- Lab 5-3: Creating a Service Profile from a Template

DCICT	1
Overview	3
Outline	3
Job Aids.....	8
Lab Topology Diagram	8
Lab Topology – Lab Aids	9
Activity 1-1: Cisco Power Calculator (Instructor Demonstration Only).....	10
Activity Objective	10
Visual Objective.....	10
Required Resources.....	10
Command List	11
Job Aids.....	11
Task 1: Configure the Cisco Power Calculator (Instructor Demonstration Only)	12
Lab 1-1: Connecting to a Cisco Nexus 7000 Series Switch Using SSH.....	17
Activity Objective	17
Visual Objective.....	17
Required Resources.....	17
Command List	18
Job Aids.....	18
Task 1: Connect to the Cisco Nexus 7000 Series Switch Using SSH.....	19
Task 2: Verify Interface Management 0 Configuration	21
Task 3: Verify Management Connectivity	23
Lab 1-2: Cisco Nexus 5000 Series Switch Initial Setup Script.....	25
Activity Objective	25
Visual Objective.....	25
Required Resources.....	25
Command List	26
Job Aids.....	26
Task 1: Use Cisco Nexus 5000 Series Initial Setup Script.....	27
Lab 1-3: Connecting to a Cisco Nexus 5000 Series Switch Using SSH.....	31
Activity Objective	31
Visual Objective.....	31
Required Resources.....	31
Command List	32
Job Aids.....	32
Task 1: Connect to a Cisco Nexus 5000 Series Switch Using SSH.....	33
Task 2: Verify Interface Management 0 Configuration	36
Lab 1-4: Running CLI Commands	38
Activity Objective	38
Visual Objective.....	38
Required Resources.....	38
Command List	39
Job Aids.....	39
Task 1: Verify VLAN and VLAN Membership	40
Task 2: Verify Interface States	43
Task 3: Verify the MAC Address Table	46
Task 4: Verify the Cisco NX-OS Software.....	48
Task 5: Verify the Running and Startup Configuration	51
Task 6: Use the tech-support Command.....	56

Lab 1-5: Configuring vPCs.....	57
Activity Objective	57
Visual Objective.....	57
Required Resources	58
Command List	58
Job Aids	59
Task 1: Connect to Your Assigned Switch	60
Task 2: Verify Interswitch Connections	61
Task 3: Establish the vPC Domain	63
Task 4: Configure the Cisco Nexus 5000 Series Switch	66
Task 5: Configure the Cisco Nexus 7000 Series Switch vPCs.....	69
Task 6: Verify the Cisco Nexus 5000 Series Switch vPCs	75
Lab 1-6: Validating Cisco FabricPath Configuration	77
Activity Objective	77
Visual Objective.....	77
Required Resources	77
Command List	78
Job Aids.....	78
Task 1: Validate the Cisco FabricPath Configuration	79
Lab 1-7: Validating OTV Configuration.....	84
Activity Objective	84
Visual Objective.....	84
Required Resources	84
Command List	85
Job Aids.....	85
Task 1: Validate the OTV Configuration	86
Lab 2-1: Verifying Current VDC Settings.....	90
Activity Objective	90
Visual Objective.....	90
Required Resources	90
Command List	91
Job Aids	91
Task 1: Verify the Current VDC Settings	92
Lab 2-2: Validating a Cisco Nexus 2000 Series Fabric Extender Configuration.....	94
Activity Objective	94
Visual Objective.....	94
Required Resources	94
Command List	95
Job Aids.....	95
Task 1: Validate a Cisco Nexus 2000 Fabric Extender Configuration.....	96
Lab 2-3: Validating a Cisco Nexus 1000V Series Switch Configuration.....	102
Activity Objective	102
Visual Objective.....	102
Required Resources	102
Command List	103
Job Aids.....	103
Task 1: Validate a Cisco Nexus 1000V Series Switch Configuration	104
Lab 3-1: Cisco MDS 9100 Series Multilayer Fabric Switch Initial Setup.....	109
Activity Objective	109
Visual Objective.....	109
Required Resources	109
Command List	110
Job Aids.....	110
Task 1: Perform an Initial Setup on the Cisco MDS 9100 Series Multilayer Fabric Switch	111

Lab 3-2: Validating a Cisco MDS 9100 Series Multilayer Fabric Switch License.....	113
Activity Objective	113
Visual Objective.....	113
Required Resources.....	113
Command List	114
Job Aids.....	114
Task 1: Validate the License on the Cisco MDS 9100 Series Switch	115
Lab 3-3: Configuring VSANs and Zoning	118
Activity Objective	118
Visual Objective.....	118
Required Resources.....	119
Command List	120
Job Aids.....	121
Task 1: Connect to Your Switches	122
Task 2: Verify the Switch Model and configure FC ports.	123
Task 3: Verify Lab Connections	126
Task 4: Configure VSANs on a Cisco Nexus 5000 Series Switch	128
Task 6: Optimize VSAN Trunking.....	132
Task 7: Verify the Default Zoning	134
Task 8: Configure Zoning	135
Lab 3-4: Validating FLOGI and FCNS	138
Activity Objective	138
Visual Objective.....	138
Required Resources.....	138
Command List	139
Job Aids.....	139
Task 1: Verify the FLOGI and FCNS Database	140
Lab 3-5: Viewing the tech-support Command Output.....	143
Activity Objective	143
Visual Objective.....	143
Required Resources.....	143
Command List	144
Job Aids.....	144
Task 1: View the tech-support Command Output	145
Lab 4-1: Validating the Physical Connections for FCoE	150
Activity Objective	150
Visual Objective.....	150
Required Resources.....	150
Command List	151
Job Aids.....	151
Task 1: Validate FCoE Physical Connections	152

Lab 5-1: Cisco UCS.....	156
Activity Objective	156
Required Resources	156
Job Aids	156
Task 1: Connect to UCS Manager.....	157
Task 2: Validate Server Ports	159
Task 3: Observe Blade Server Discovery in Finite State Machine	162
Lab 5-2: Exploring the Cisco UCS Manager GUI	166
Activity Objective	166
Visual Objective	166
Required Resources	166
Command List	166
Job Aids	167
Implementation Sheet for Lab 5-2 Explore the Cisco UCS Manager GUI	167
Task 1: Connect to Cisco UCS Manager.....	168
Task 2: Explore the Equipment Tab	169
Task 3: Explore the Servers Tab	171
Task 4: Explore the LAN Tab	172
Task 5: Explore the SAN Tab	175
Task 6: Explore the VM Tab	176
Task 7: Explore the Admin Tab	177
Lab 5-3: Creating a Service Profile from a Template.....	180
Activity Objective	180
Required Resources	181
Command List	181
Job Aids	181
Implementation Sheet for Lab 5-3 Creating a Service Profile from a Template	181
Task 1: Connect to Cisco UCS Manager.....	182
Task 2: Generate a Service Profile from a Template	183
Task 3: Service Profile Management.....	185

Job Aids

Use the following job aids while performing the lab tasks in this lab guide.

Lab Topology Diagram

This diagram describes the physical topology of the lab that is used in this course:

FastLane 7K/5K/2K Nexus Lab (Rev. 4.1)

N7K to N7K:

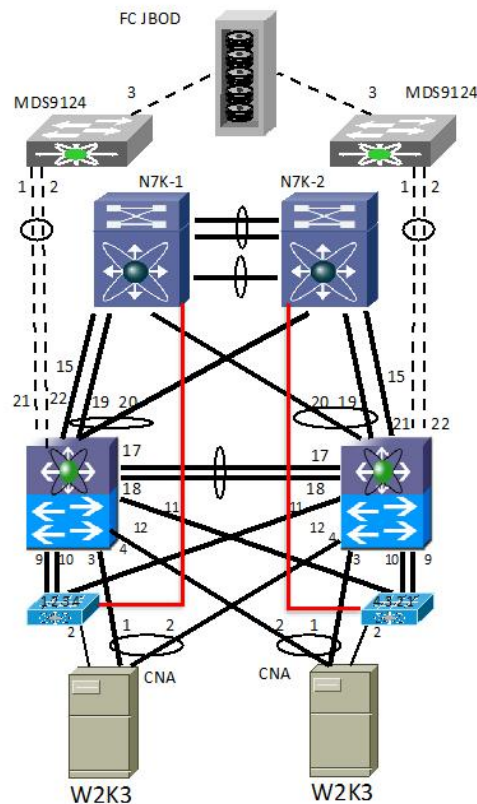
Pod1+2: 1/17 and 3/11-12
Pod3+4: 1/18 and 3/13-14
Pod5+6: 1/25 and 3/15-16
Pod7+8: 1/26 and 3/17-18

N7K to N5K:

Pod1: 1/1 on both N7K
3/1 on N7K-1
Pod2: 1/3 on both N7K
3/1 on N7K-2
Pod3: 1/2 on both N7K
3/3 on N7K-1
Pod4: 1/4 on both N7K
3/3 on N7K-2
Pod5: 1/9 on both N7K
3/5 on N7K-1
Pod6: 1/11 on both N7K
3/5 on N7K-2
Pod7: 1/12 on both N7K
3/7 on N7K-1
Pod8: 1/14 on both N7K
3/7 on N7K-2

N7K to N2K FEX:

Pod1&2: 1/5
Pod3&4: 1/6
Pod5&6: 1/13
Pod7&8: 1/14



Windows with CNA

For 4 Students

GE

FC

10GE

Uses dual fabric for FC
and vPC for Ethernet

Server port	Going to
Onboard1	Infrastructure access
Onboard2	Infrastructure mgmt
Singe GE intel	N2K port 2

(infrastructure Eth and
mgmt eth port on servers
not shown)

Lab Topology – Lab Aids

Management IP Addresses (P is always your Pod #)

<u>Device</u>	<u>IP Address</u>	
N7K-1 admin VDC	192.168.0.210/24	
N7K-1 CMP (slot5)	192.168.0.215/24	(not accessible)
N7K-2 admin VDC	192.168.0.220/24	
N7K-2 CMP (slot5)	192.168.0.225/24	(not accessible)
N7K Pod VDC	192.168.0.20P/24	
N5548 mgmt0	192.168.0.P8/24	
MDS9124 mgmt0	192.168.0.P9/24	
Windows Server	192.168.0.P1/24	
Mail Server	192.168.0.10/24	
NTP server	192.168.0.1/24	
UCS Demo System	192.168.0.100/24	
Nexus 1000v VSM	192.168.0.93/24	

Device Login Credentials

<u>Device</u>	<u>Username</u>	<u>Password</u>	
N7010 (default VDC)	podX	podX	(readonly access only)
N7010 (Pod VDC)	admin	1234QWer	
N5548	admin	1234QWer	
MDS9124	admin	1234QWer	
Windows Server	administrator	1234QWer	
Linux Server	root	1234QWer	
UCS	admin	admin	
Nexus 1000v	admin	admin	

Activity 1-1: Cisco Power Calculator (Instructor Demonstration Only)

The instructor will complete this lab activity to demonstrate what you learned in the related module.

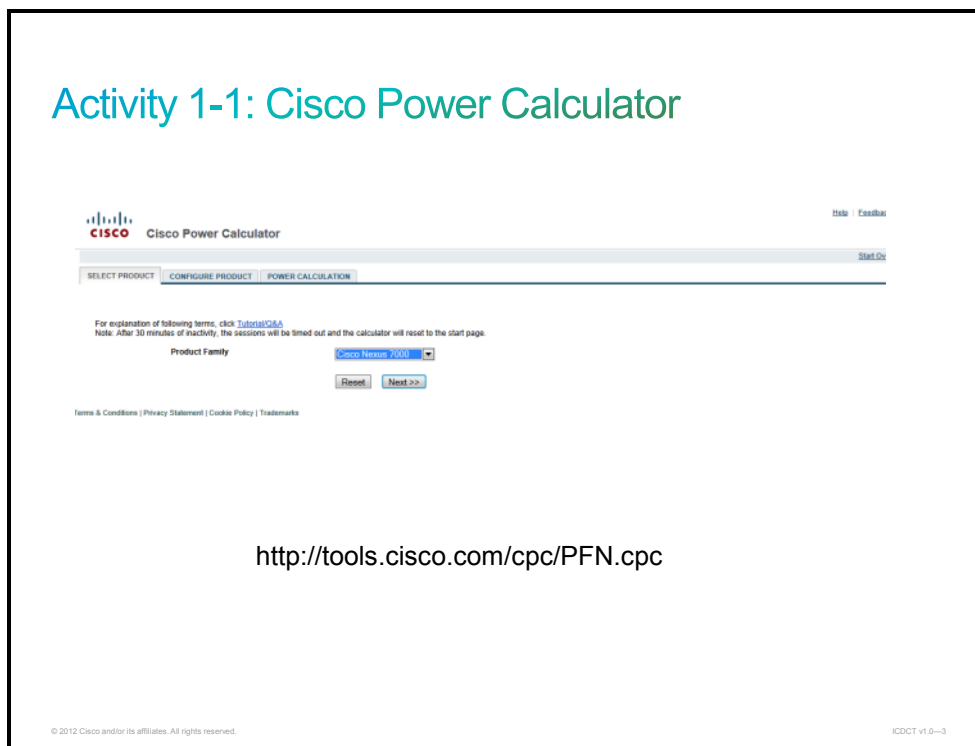
Activity Objective

In this activity, the instructor will demonstrate how to use the Cisco Power Calculator. After completing this activity, you will be able to meet these objectives:

- Describe how to access the Cisco Power Calculator
- Describe how to use the Cisco Power Calculator to identify the power requirements for a Cisco Nexus 7000 Series switch

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 PC with browser
- Internet connection

Command List

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

Command	Description
There are no commands used.	

Job Aids

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

- No job aids are required.

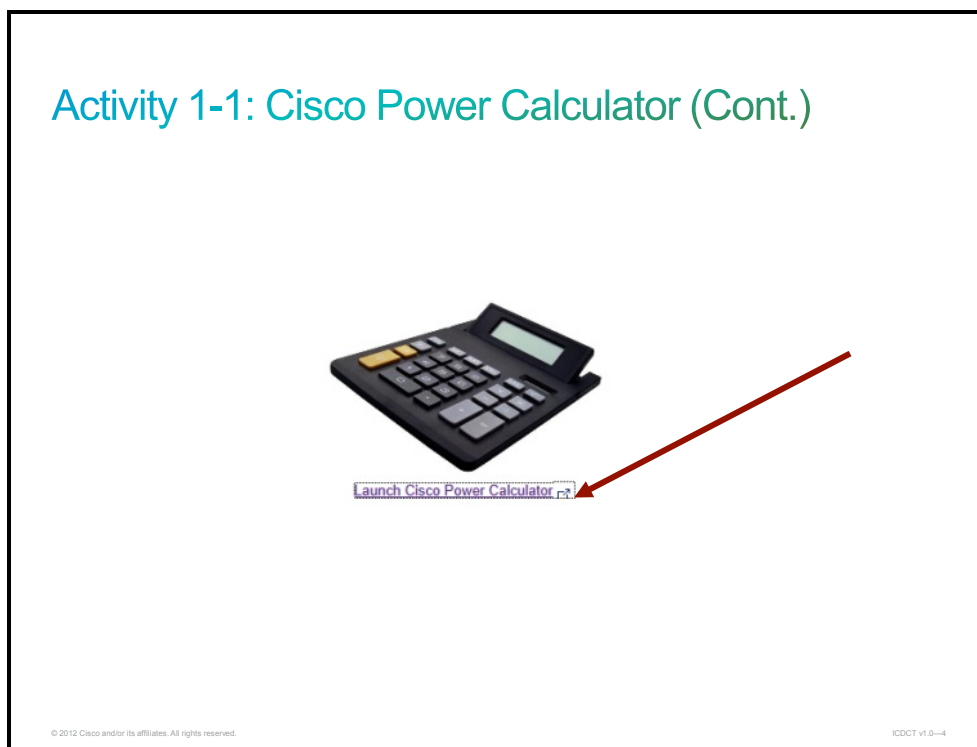
Task 1: Configure the Cisco Power Calculator (Instructor Demonstration Only)

During this task, your instructor will demonstrate how to use the Cisco Power Calculator.

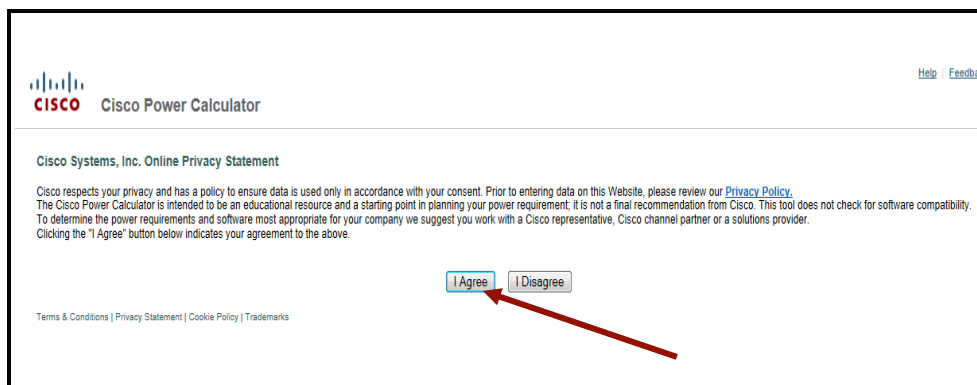
Activity Procedure

Complete these steps:

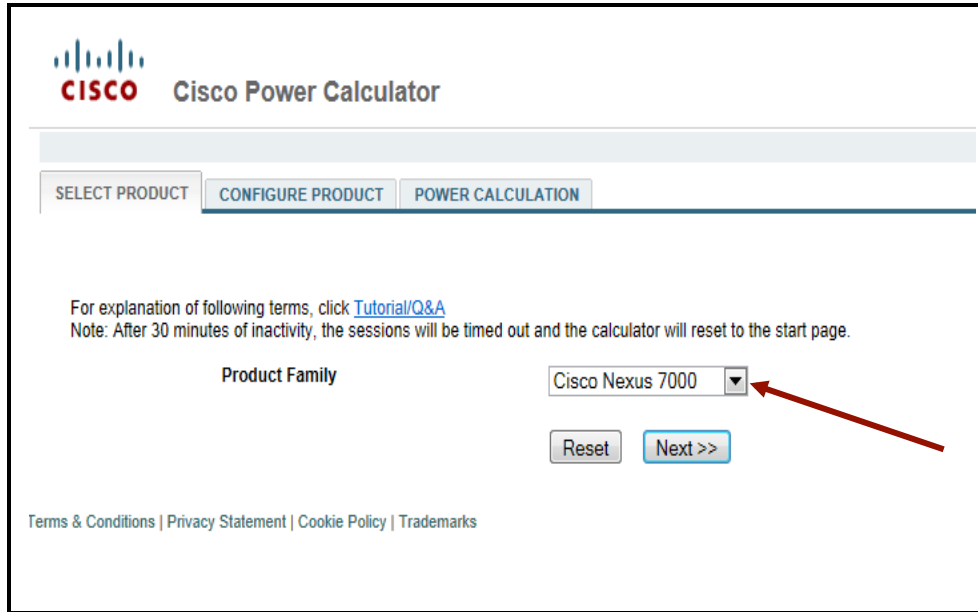
- Step 1** Connect to a pod PC and open an Internet browser.
- Step 2** Go to the Cisco website at **<http://www.cisco.com>** and log in using your Cisco.com account credentials.
- Step 3** Go to the following URL to access the Cisco Power Calculator:
<http://tools.cisco.com/cpc/>
- Step 4** Click the **Launch Cisco Power Calculator** to launch the calculator.



- Step 5** Click **I Agree** to accept or confirm acceptance of the online privacy policy.



Step 6 In the Product Family drop-down menu, choose **Cisco Nexus 7000**.



Step 7 Click the **Next** button.

Step 8 In the Configure Product tab, choose the following options:

Chassis:	N7K-C7009
Supervisor Engine:	N7K-SUP1
Redundant Supervisor Engine:	Yes
Fantray:	N7K-C7009-FAN
How many Fabric modules?	5
Input Voltage:	200-240 volts
Slot 3:	N7K-M148GT-11L
Slot 4:	N7K-M148GT-11L
Slot 5:	N7K-M132XP-12L
Slot 6:	N7K-F248XP-25
Slot 7:	N7K-F248XP-25
Slot 8:	N7K-M108X2-12L
Slot 9:	N7K-M108X2-12L

For explanation of following terms, click [Tutorial/Q&A](#)

Slot	Line Card
1	N7K-SUP1 ▼
2	N7K-SUP1 ▼
3	N7K-M148GT-11L ▼
4	N7K-M148GT-11L ▼
5	N7K-M132XP-12L ▼
6	N7K-F248XP-25 ▼
7	N7K-F248XP-25 ▼
8	N7K-M108X2-12L ▼
9	N7K-M108X2-12L ▼

Reset Next >>



Step 9 Click the **Next** button.

Step 10 The Power Calculation tab appears showing power supply recommendations.

 Cisco Power Calculator [Help](#) [Feedback](#)

[Start Over](#)

[SELECT PRODUCT](#) [CONFIGURE PRODUCT](#) **POWER CALCULATION**

For explanation of following terms, click [Tutorial/Q&A](#)

- [Power Consumption/Heat Dissipation Summary](#)
- [Quick Facts](#)
- [Power Supply Details](#)
- [Configuration Details](#)

[Download Data to Microsoft Excel File](#) 

[Download Data to Adobe PDF File](#) 

Power Consumption/Heat Dissipation Summary	
Slot	Line Card
1	N7K-SUP1
2	N7K-SUP1
3	N7K-M148GT-11L
4	N7K-M148GT-11L
5	N7K-M132XP-12L
6	N7K-F248XP-25
7	N7K-F248XP-25
8	N7K-M108X2-12L
9	N7K-M108X2-12L

Recommended Power Supply		Percentage of Power Used
Two N7K-AC-6.0KW in Full redundancy mode		86.58% 

First Alternative Power Supply		Percentage of Power Used
Two N7K-AC-6.0KW in Input Source redundancy mode		86.58% 

Total Output Current	Total Output Power	Total Typical Output Power	Total Heat Dissipation
103.90 Amps	5195.00 Watts	3907.00 Watts	19712.14 BTU/Hr

Step 11 View the supported redundancy options further down on the same page.

NOTE:
The system will support the following 4 power redundancy options:

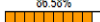
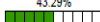
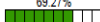
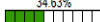
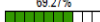
- Full Redundancy - guards the system against the failure of either a power supply or a grid.
- Input Source (Grid) Redundancy - guards the system against failure of a grid.
- Power Supply (N+1) Redundancy- guards the system against the failure of one power supply. This is the system default.
- Combined Mode, where the total power available is the sum of the outputs of all the power supplies installed; (There is no redundancy).

[\[Top \]](#)

Quick Facts		
	Selected Supervisor Engine	N7K-SUP1
	Selected Chassis	N7K-C7009
	Selected Voltage	200-240 Volts AC
	Selected Fantray	N7K-C7009-FAN
	Selected Number of Fabric Modules	5
	Chassis Slots	9
	Power Supply Options	Two N7K-AC-6.0KW in Full redundancy mode Two N7K-AC-6.0KW in Input Source redundancy mode Two N7K-AC-6.0KW in Power Supply redundancy mode Single N7K-AC-6.0KW in Combined mode Two N7K-AC-6.0KW in Combined mode Two N7K-AC-7.5KW in Input Source redundancy mode Two N7K-AC-7.5KW in Full redundancy mode Two N7K-AC-7.5KW in Combined mode Two N7K-AC-7.5KW in Power Supply redundancy mode Single N7K-AC-7.5KW in Combined mode
	Line Card Slots	7
	Rack Units	15

Step 12 View the information in the Total Output columns, which is based on the chosen power redundancy mode.

[\[Top \]](#)

Power Supply Details				
Recommended Power Supply	Percentage of Power used	Total Output Current for this PSU (A)	Total Output Current Used (A)	Total Output Current Remaining (A)
Two N7K-AC-6.0KW in Full redundancy mode	86.58% 	120.00	103.90	16.10
Other Power Supply Options				
Two N7K-AC-6.0KW in Input Source redundancy mode	86.58% 	120.00	103.90	16.10
Two N7K-AC-6.0KW in Power Supply redundancy mode	86.58% 	120.00	103.90	16.10
Single N7K-AC-6.0KW in Combined mode	86.58% 	120.00	103.90	16.10
Two N7K-AC-6.0KW in Combined mode	43.29% 	240.00	103.90	136.10
Two N7K-AC-7.5KW in Input Source redundancy mode	69.27% 	150.00	103.90	46.10
Two N7K-AC-7.5KW in Full redundancy mode	69.27% 	150.00	103.90	46.10
Two N7K-AC-7.5KW in Combined mode	34.63% 	300.00	103.90	196.10
Two N7K-AC-7.5KW in Power Supply redundancy mode	69.27% 	150.00	103.90	46.10
Single N7K-AC-7.5KW in Combined mode	69.27% 	150.00	103.90	46.10

Step 13 View how much power each item requires.

NOTE:
Chassis reserves power for two Supervisor Engines and five Fabric Modules regardless of the actual number of those modules in the system

Configuration Details					
Slot	Line Card	Output Current (A)	Output Power (W)	Typical Power Used (W)	Heat Dissipation (BTU/Hr)
SYSTEM-FAN	N7K-C7009-FAN	13.00	650.00	185.0	2466.39
FABRIC MODULE	N7K-C7009-FAB-2	1.50	75.00	55.0	284.58
FABRIC MODULE	N7K-C7009-FAB-2	1.50	75.00	55.0	284.58
FABRIC MODULE	N7K-C7009-FAB-2	1.50	75.00	55.0	284.58
FABRIC MODULE	N7K-C7009-FAB-2	1.50	75.00	55.0	284.58
FABRIC MODULE	N7K-C7009-FAB-2	1.50	75.00	55.0	284.58
1	N7K-SUP1	4.20	210.00	190.0	796.83
2	N7K-SUP1	4.20	210.00	190.0	796.83
3	N7K-M148GT-11L	8.00	400.00	358.0	1517.78
4	N7K-M148GT-11L	8.00	400.00	358.0	1517.78
5	N7K-M132XP-12L	15.00	750.00	611.0	2845.83
6	N7K-F248XP-25	9.00	450.00	350.0	1707.50
7	N7K-F248XP-25	9.00	450.00	350.0	1707.50
8	N7K-M108X2-12L	13.00	650.00	520.0	2466.39
9	N7K-M108X2-12L	13.00	650.00	520.0	2466.39
		Output Current (A)	Output Power (W)	Typical Power Used (W)	Heat Dissipation (BTU/Hr)
Total		103.90	5195.00	3907.00	19712.14

Step 14 Click the link to download the summary either to a Microsoft Excel or Adobe PDF file.

**Cisco Power Calculator**

[SELECT PRODUCT](#) [CONFIGURE PRODUCT](#) [POWER CALCULATION](#)

For explanation of following terms, click [Tutorial/Q&A](#)

- [Power Consumption/Heat Dissipation Summary](#)
- [Quick Facts](#)
- [Power Supply Details](#)
- [Configuration Details](#)

[Download Data to Microsoft Excel File](#) 

[Download Data to Adobe PDF File](#) 

Activity Verification

You have completed this task when you attain this result:

- You have used the Cisco Power Calculator to calculate power supply options for the Cisco Nexus 7000 9-Slot Switch chassis and selected modules.

Lab 1-1: Connecting to a Cisco Nexus 7000 Series Switch Using SSH

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

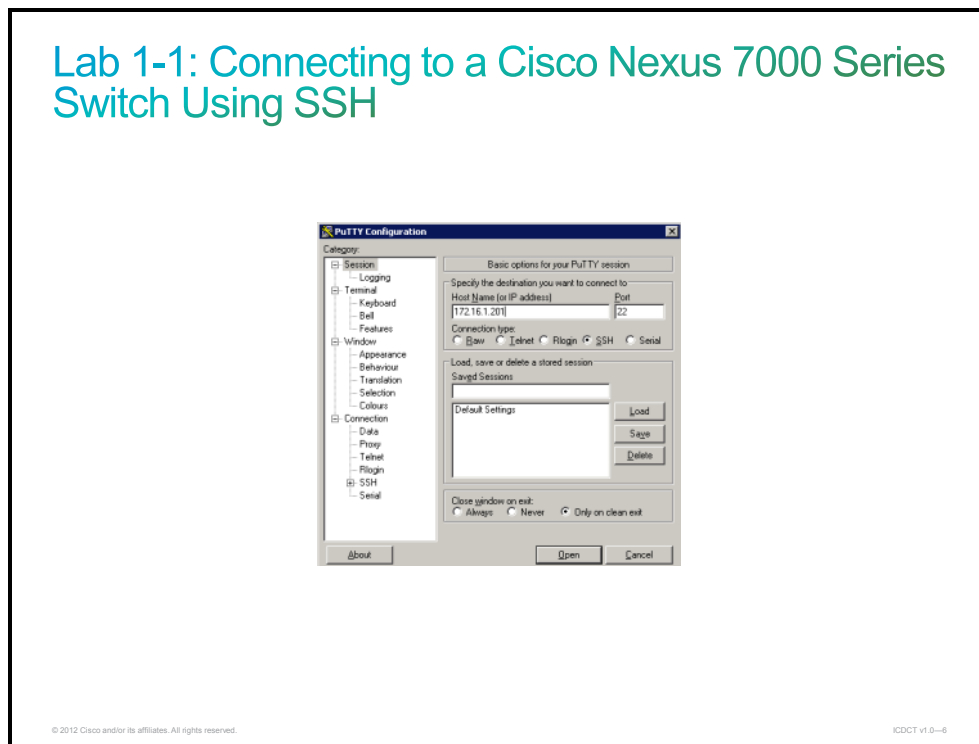
Activity Objective

In this activity, you will connect to the Cisco Nexus 7000 Series switch using SSH to run various **show** commands. After completing this activity, you will be able to meet these objectives:

- Connect to a Cisco Nexus 7000 Series switch using SSH
- Use **show** commands to verify the management 0 interface configuration
- Use the show commands to verify the management 0 interface connectivity

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 7000 Series VDC
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show running-config interface mgmt 0</code>	Displays the mgmt 0 configuration in the running configuration
<code>show running-config include route</code>	Displays the default route configuration in the running configuration
<code>show ip route</code>	Displays the IP routing table for the default VRF
<code>show ip route vrf management</code>	Displays the IP routing table for the management VRF
<code>show interface mgmt 0 brief</code>	Displays summary information about the mgmt 0 interface
<code>show interface mgmt 0</code>	Displays detailed information about the mgmt 0 interface
<code>ping <x.x.x.x></code>	Pings a remote address using the default VRF
<code>ping <x.x.x.x> vrf management</code>	Pings a remote address using the management VRF

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

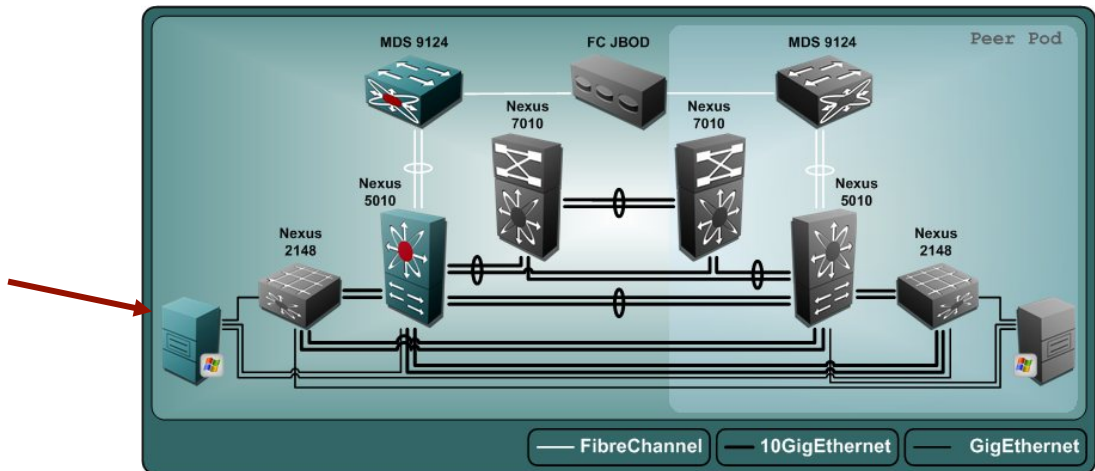
Task 1: Connect to the Cisco Nexus 7000 Series Switch Using SSH

During this task, you will use SSH to connect to the Out Of Band Management interface of your Cisco Nexus 7000 Series switch.

Activity Procedure

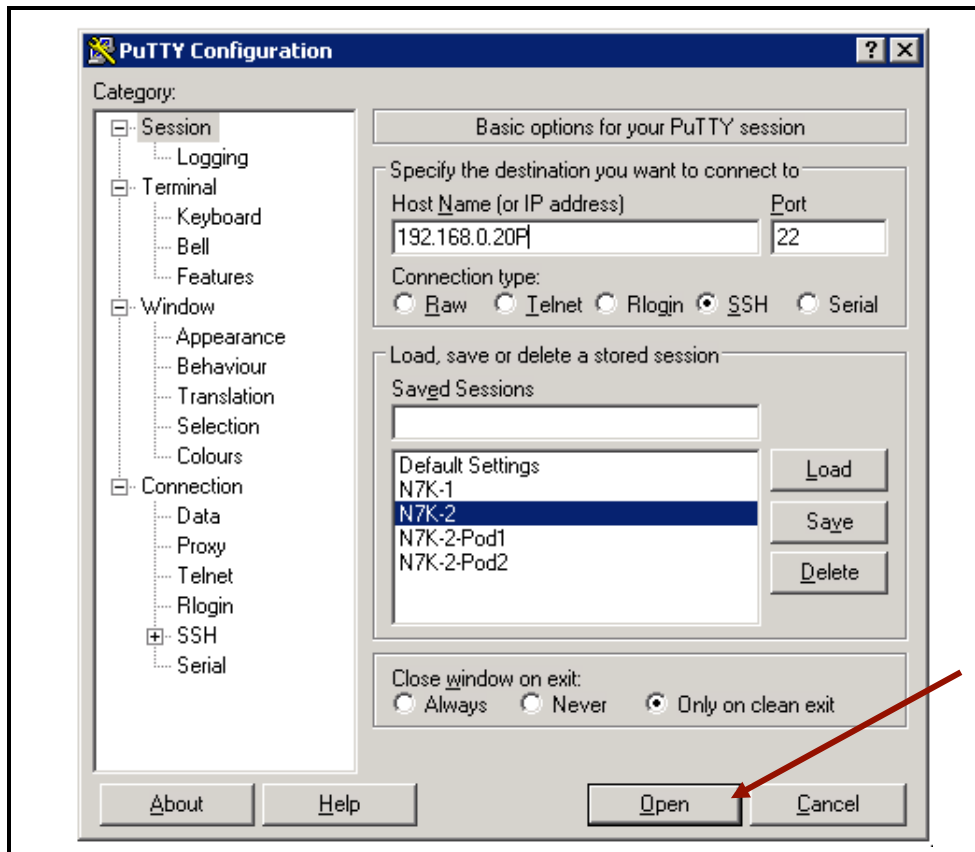
Complete these steps:

- Step 1** Connect to the remote lab GUI at <http://remotelabs.flane.de> using the credentials supplied by your instructor
- Step 2** Click on the **blue** Server icon in the remote lab GUI and wait for the NX window to open.



- Step 3** Log in to the PC using username **administrator** and password **1234QWer**.
- Step 4** Use Putty or Teraterm (or windows telnet) to connect to a Nexus 7010 switch.

Pod #	Telnet/ssh to
1	192.168.0.201
2	192.168.0.202
3	192.168.0.203
4	192.168.0.204
5	192.168.0.205
6	192.168.0.206
7	192.168.0.207
8	192.168.0.208



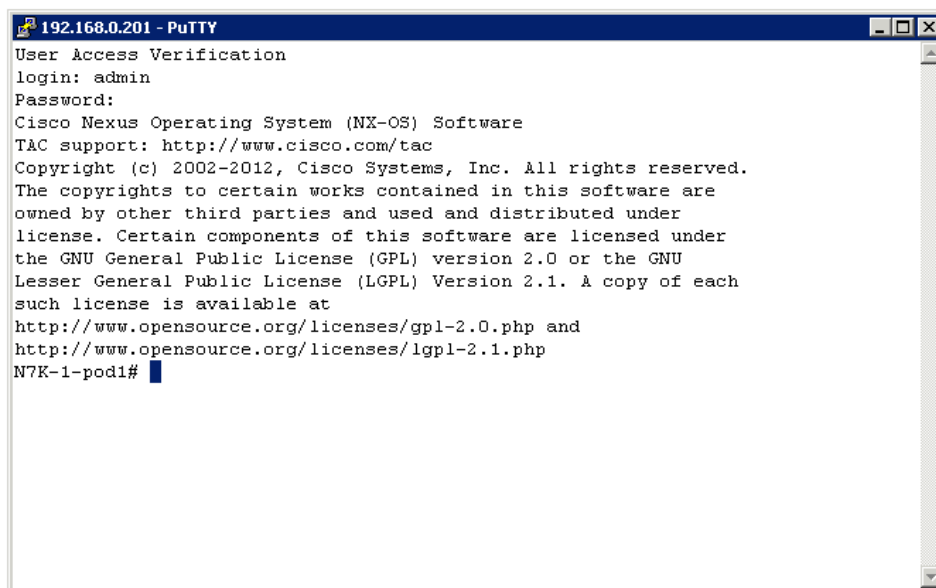
Step 5 Click the **Open** button to open the session.

Step 1 When the session opens you will be asked for credentials for logging into the switch. Log in as student using username **admin** and password **1234QWer**.

Activity Verification

You have completed this task when you attain these results:

- You have successfully logged into your Cisco Nexus 7000 Series switch.



Task 2: Verify Interface Management 0 Configuration

In this task, you will use **show** commands to verify the configuration that was applied to management 0 in the Cisco Nexus 7000 Series Switch Initial Script Setup lab.

Activity Procedure

Complete these steps on both N7K switches:

- Step 1** At the command prompt, enter the **show running-config interface mgmt 0** to verify the configuration of management 0.

```
N7K-X-PodY# show running-config interface mgmt 0
```

```
!Command: show running-config interface mgmt0
```

```
!Time: Wed Feb 22 10:07:43 2012
```

```
version 6.0(3)
```

```
interface mgmt0
```

```
ip address 192.168.0.201/24
```

```
N7K-X-PodY#
```

- Step 2** Verify that the IP address of each Cisco Nexus 7000 Series switch is as follows:

```
N7K-X-PodY#: 192.168.0.20P (P is your Pod#)
```

- Step 3** Verify that the default route has been correctly set using the command **show running-config | include route** on both N7K switches.

```
N7K-X-PodY# show running-config | include route
```

```
ip route 0.0.0.0/0 192.168.0.1
```

```
N7K-X-PodY#
```

- Step 4** The Cisco Nexus 7000 Series switch supports two default VRFs. One is called **management** and the other is called **default**. Use the following commands to verify that the default route has been set for the correct VRF.

```
N7K-X-Pod## sho ip route
```

```
IP Route Table for VRF "default"
```

```
'*' denotes best ucast next-hop
```

```
'**' denotes best mcast next-hop
```

```
'[x/y]' denotes [preference/metric]
```

```
'%<string>' in via output denotes VRF <string>
```

```
N7K-X-Pod##
```

```
N7K-X-Pod## sho ip route vrf management
```

```
IP Route Table for VRF "management"
```

```
'*' denotes best ucast next-hop
```

```
'**' denotes best mcast next-hop
```

```
'[x/y]' denotes [preference/metric]
```

```
'%<string>' in via output denotes VRF <string>
```

```
0.0.0.0/0, ubest/mbest: 1/0
```

```

        *via 192.168.0.1, [1/0], 00:05:48, static
192.168.0.0/24, ubest/mbest: 1/0, attached
        *via 192.168.0.201, mgmt0, [0/0], 00:05:48, direct
192.168.0.20P/32, ubest/mbest: 1/0, attached
        *via 192.168.0.20P, mgmt0, [0/0], 00:05:48, local
N7K-X-Pod##

```

- Q1) Which VRF is using the default route of 192.168.0.1? _____
- Q2) Is this VRF the correct VRF? _____
- Q3) Based on your answer, explain why this is, or is not, the correct VRF. _____

Step 5 Verify that the management 0 interface is administratively and operationally up using the **show interface mgmt 0 brief** command.

```
N7K-X-PodY# show interface mgmt 0 brief
```

```

-----
Port    VRF      Status IP Address      Speed    MTU
-----
mgmt0   --       up      192.168.0.20P   1000     1500
N7K-X-PodY#

```

Step 6 Check the management 0 interface details using the **show interface mgmt 0** command.

```
N7K-X-PodY# show interface mgmt 0
```

```

mgmt0 is up
Hardware: GigabitEthernet, address: 68bd.abd6.1f11 (bia 68bd.abd6.1f11)
Internet Address is 192.168.0.20P/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
full-duplex, 1000 Mb/s
Auto-Negotiation is turned on
EtherType is 0x0000
1 minute input rate 144 bits/sec, 0 packets/sec
1 minute output rate 120 bits/sec, 0 packets/sec
Rx
  16269 input packets 10685 unicast packets 3827 multicast packets
  1757 broadcast packets 2865910 bytes
Tx
  30351 output packets 7740 unicast packets 3839 multicast packets
  18772 broadcast packets 3027571 bytes

```

```
N7K-X-PodY#
```

Activity Verification

You have completed this task when you attain these results:

- You have confirmed that the IP configuration for the management 0 interface is correctly configured.
- You have confirmed that the IP default route is configured for the correct VRF.
- You have confirmed that the mgmt 0 interface is up both administratively and operationally.

Task 3: Verify Management Connectivity

In this task, you will test connectivity from the management 0 interface.

Activity Procedure

Complete these steps:

Step 7 Now that the mgmt 0 configuration has been verified, you need to verify that connectivity to remote devices is available.

Step 8 From the N7K SSH session, ping 192.168.0.1 using the **ping** command.

```
N7K-X-Pod## ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
ping: sendto 192.168.0.1 64 chars, No route to host
Request 0 timed out
ping: sendto 192.168.0.1 64 chars, No route to host
Request 1 timed out
ping: sendto 192.168.0.1 64 chars, No route to host
Request 2 timed out
ping: sendto 192.168.0.1 64 chars, No route to host
Request 3 timed out
ping: sendto 192.168.0.1 64 chars, No route to host
Request 4 timed out

--- 192.168.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
N7K-X-Pod##
```

Q1) Why did the ping fail? _____

Q2) What would you do to correct the problem? _____

Step 9 From the N7K SSH session, try using the following command to verify reachability to the default gateway: **ping 192.168.0.1 vrf management**.

```
N7K-X-Pod## ping 192.168.0.1 vrf management
PING 192.168.0.1 (192.168.0.1): 56 data bytes
Request 0 timed out
Request 1 timed out
64 bytes from 192.168.0.1: icmp_seq=2 ttl=254 time=0.967 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=254 time=0.877 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=254 time=0.897 ms

--- 192.168.0.1 ping statistics ---
5 packets transmitted, 3 packets received, 40.00% packet loss
round-trip min/avg/max = 0.877/0.913/0.967 ms
N7K-X-Pod##
```

- Q3) Why did this command work? _____

- Q4) Why could one or two pings fail in the beginning? _____

Activity Verification

You have completed this task when you attain this result:

- You have verified reachability to all devices in the lab on the 192.168.0.x network.

Lab 1-2: Cisco Nexus 5000 Series Switch Initial Setup Script

You will complete this lab activity to demonstrate what you learned in the related module.

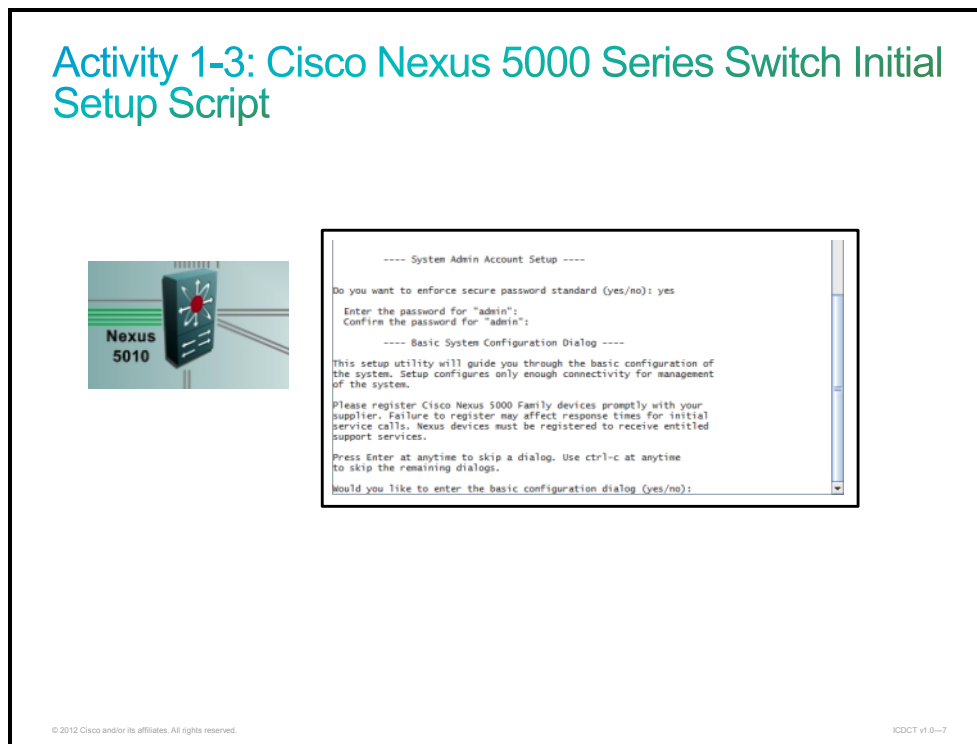
Activity Objective

In this activity, the you will perform an initial setup on a Cisco Nexus 5000 Series switch. After completing this activity, you will be able to meet these objectives:

- Describe how to use the initial setup script to perform an initial configuration on a Cisco Nexus 5000 Series switch
- Describe which parameters should be set during the initial configuration on a Cisco Nexus 5000 Series switch
- Describe which parameters have default settings in the initial setup script on a Cisco Nexus 5000 Series switch

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 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>setup</code>	Runs the setup script
<code>show running-config</code>	Displays the current running configuration

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

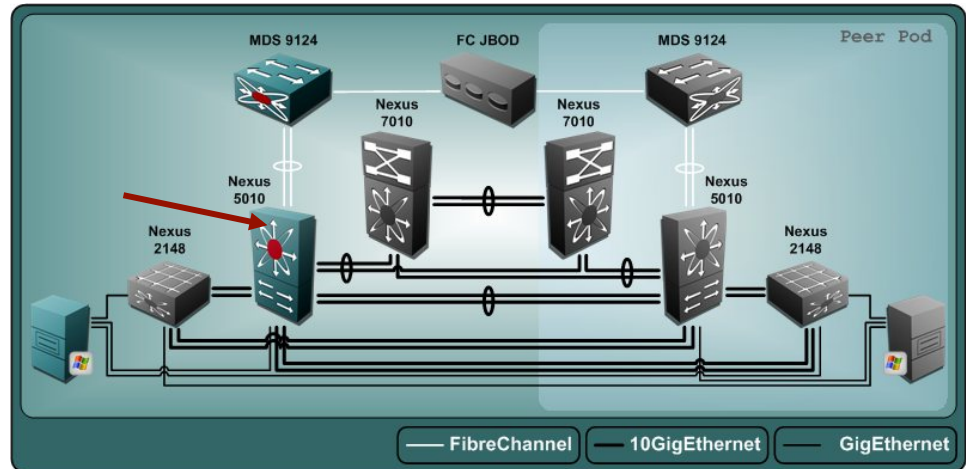
Task 1: Use Cisco Nexus 5000 Series Initial Setup Script

During this task, you will use the initial setup script on a Cisco Nexus 5000 Series switch.

Activity Procedure

Complete these steps:

- Step 1** Open the console window to your Cisco Nexus 5000 Series switch by clicking the nexus 5000 icon in the remote lab GUI.



Step 2

- Step 3** Log into your Pods Nexus 5000 with username “admin” and password “1234QWer”

- Step 4** If your N5K asks for an “strong passwords” or an admin password answer yes, define “1234QWer” as the password and log in with those credentials.

- Step 5** Reset the startup configuration.

```
switch# write erase
Warning: This command will erase the startup-configuration.
Do you wish to proceed anyway? (y/n) [n] y
```

- Step 6** Reload the system. When prompted to continue with the system reboot, type “y.”

```
switch# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y

...
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "statsclient" (PID 3862) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "licmgr" (PID 3790) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "AAA Daemon" (PID 3848) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "vshd" (PID 3785) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "vlan_mgr" (PID 3874) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "igmp" (PID 3977) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "netstack" (PID 3937) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "urib" (PID 3853) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "u6rib" (PID 3852) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "smm" (PID 3786) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "res_mgr" (PID 3826) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "npac1" (PID 3831) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "l3vm" (PID 3850) is forced exit.
```

```

Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "icmpv6" (PID 3936) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "fs-daemon" (PID 3791) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "eth_dstats" (PID 3839) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "Radius Daemon" (PID 3975) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "adjmgr" (PID 3900) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "Cert_enroll Daemon" (PID 3847) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "arp" (PID 3935) is forced exit.
Aug 3 13:11:58 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "Security Daemon" (PID 3846) is forced exit.
Aug 3 13:11:59 %LIBSYSMGR-3-SIGTERM_FORCE_EXIT Service "callhome server" (PID 3897) is forced exit.

INIT: Sending processes the KILL signal
Unexporting directories for NFS kernel daemon...done.
Stopping NFS kernel daemon: rpc.mountd rpc.nfsddone.
Unexporting directories for NFS kernel daemon...
done.
Stopping portmap daemon: portmap.
Stopping kernel log daemon: klogd.
Sending all processes the TERM signal... done.
Sending all processes the KILL signal... done.
Unmounting remote filesystems... done.
Deactivating swap...umount: none busy - remounted read-only
done.
Unmounting local filesystems...umount: none busy - remounted read-only
done.
mount: you must specify the filesystem type
Starting reboot command: reboot
Rebooting...
Restarting system.

Booting kickstart image: bootflash:/n5000-uk9-kickstart.4.2.1.N1.1.bin....
.....Image verification OK

Starting kernel...
Usage: init 0123456SsQqAaBbCcUu
INIT: version 2.85 booting
I2C - Mezz absent
blogger: /var/log/isan.log: No such file or directory (2).
Starting Nexus5010 POST...
  Executing Mod 1 1 SEEPROM Test.....done
  Executing Mod 1 1 GigE Port Test.....done
  Executing Mod 1 1 Inband GigE Test.....done
  Executing Mod 1 1 NVRAM Test....done
  Executing Mod 1 1 PCIE Test.....done
  Mod 1 1 Post Completed Successfully
  Mod 2 Post Completed Successfully
POST is completed
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Checking all filesystems..... done.
.
Loading system software
Uncompressing system image: bootflash:/n5000-uk9.4.2.1.N1.1.bin

Loading plugin 0: core_plugin...
plugin_link_to_exec_path: plugin_path = /isan/plugin/0, tar_log = /isan/plugin_extract_log/0
Loading plugin 1: eth_plugin...
plugin_link_to_exec_path: plugin_path = /isan/plugin/1, tar_log = /isan/plugin_extract_log/1
plugin_file_is_excluded_from_exec_path: /boot/ is excluded from linking
plugin_file_is_excluded_from_exec_path: /boot/etc/ is excluded from linking
plugin_file_is_excluded_from_exec_path: /boot/etc/plugin_exclude.conf is excluded from linking
plugin_file_is_excluded_from_exec_path: /boot/lib/ is excluded from linking
plugin_file_is_excluded_from_exec_path: /boot/lib/libplugin_sysreg.so is excluded from linking
plugin_file_is_excluded_from_exec_path: /boot/lib/libplugin_sysreg.so.0 is excluded from linking
plugin_file_is_excluded_from_exec_path: /boot/lib/libplugin_sysreg.so.0.0.0 is excluded from linking
INIT: Entering runlevel: 3
Exporting directories for NFS kernel daemon...done.
Starting NFS kernel daemon:rpc.nfsd.
rpc.mountddone.

Setting envvar: SYSMGR_SERVICE_NAME to muxif_service
Set envvar SYSMGR_SERVICE_NAME to muxif_service
/isan/bin/muxif_config: argc:2
muxif_init....vacl: ret: 0
Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan/config
Added VLAN with VID == 4042 to IF -:muxif:-
2010 Aug 3 13:14:36 $$ VDC-1 $$ %USER-2-SYSTEM_MSG: CLIS: loading cmd files begin - clis
2010 Aug 3 13:14:39 $$ VDC-1 $$ %KERN-2-SYSTEM_MSG: Starting kernel... - kernel
2010 Aug 3 13:14:39 $$ VDC-1 $$ %KERN-0-SYSTEM_MSG: I2C - Mezz absent - kernel
2010 Aug 3 13:14:49 $$ VDC-1 $$ %USER-2-SYSTEM_MSG: CLIS: loading cmd files end - clis
2010 Aug 3 13:14:49 $$ VDC-1 $$ %USER-2-SYSTEM_MSG: CLIS: init begin - clis
2010 Aug 3 13:15:05 $$ VDC-1 $$ %NOHMS-2-NOHMS_DIAG_ERR_PS_FAIL: System minor alarm on power supply
2: failed
Executing Port Power On Tests.....Done
2010 Aug 3 13:16:10 $$ VDC-1 $$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online

```

- Step 7** Use the strong password "1234QWer" for the admin user when prompted (using any other password will make support for the lab very difficult and the support team may have to clear your configuration!!!)
- Step 8** Use the basic system configuration dialog for initial setup. Enter the parameters as shown in bold typeface. (replace P with your Pod number during setup)

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

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

Enter the password for "admin": 1234QWer
Confirm the password for "admin": 1234QWer

----- Basic System Configuration Dialog -----

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 Nexus 5010 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus 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]: n

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

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

Enter the switch name : N5K-P    (P is your POD number!!)

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

Mgmt0 IPv4 address : 192.168.0.P8 (P is your Pod Number!!)

Mgmt0 IPv4 netmask : 255.255.255.0

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

IPv4 address of the default-gateway: 192.168.0.1

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

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

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

Number of rsa key bits <768-2048>: 1024

Configure the ntp server? (yes/no) [n]: n

Enter basic FC configurations (yes/no) [n]: n

The following configuration will be applied:
switchname N5K-P
interface mgmt0
```

```

ip address 192.168.0.18 255.255.255.0
no shutdown
  telnet server enable
  ssh key rsa 1024 force
  ssh server enable

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

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

[#####] 100%
Packaging and storing to flash: /

Nexus 5000 Switch
N5K-P login: admin
Password: 1234Qwer
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html
N5K-P#

```

Step 9 Use the command **show running-config** to verify that the configuration has been generated as expected.

Activity Verification

You have completed this task when you attain these results:

- You have successfully performed an initial configuration on the Cisco Nexus 5000 Series switch.
- You have verified the configuration using the **show running-config** command.

Lab 1-3: Connecting to a Cisco Nexus 5000 Series Switch Using SSH

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

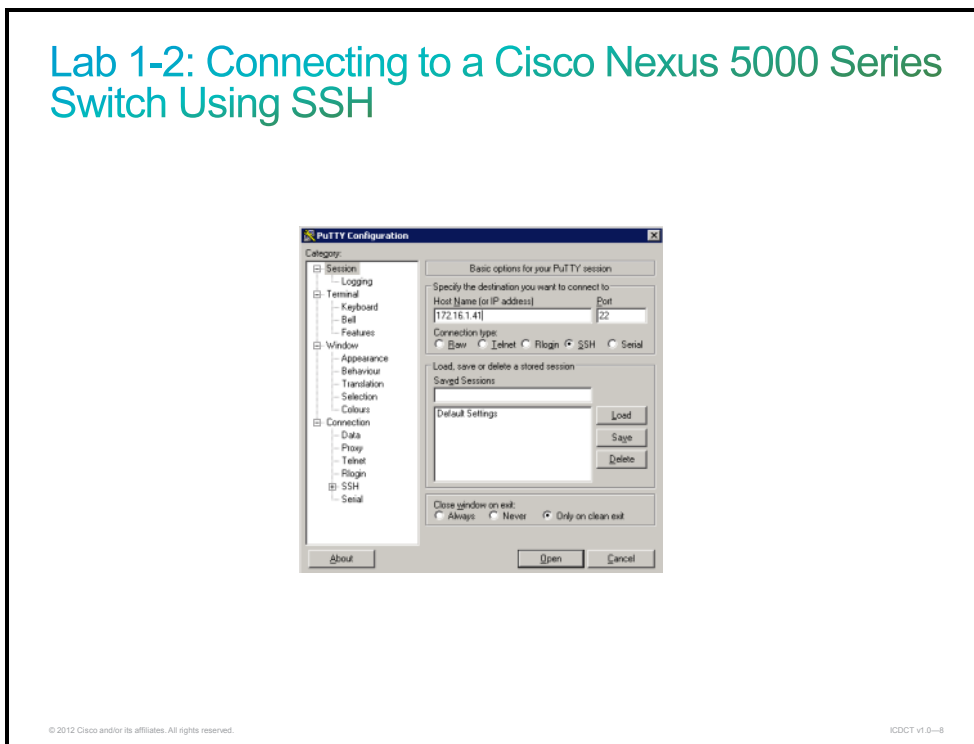
Activity Objective

In this activity, you will connect to a Cisco Nexus 5000 Series switch using SSH to verify the management 0 configuration and connectivity. After completing this activity, you will be able to meet these objectives:

- Connect to a Cisco Nexus 5000 Series switch using SSH
- Use **show** commands to verify the management 0 interface configuration
- Use **show** commands to verify the management 0 interface connectivity

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 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show running-config interface mgmt 0</code>	Displays the mgmt 0 configuration in the running configuration
<code>show running-config include route</code>	Displays the default route configuration in the running configuration
<code>show ip route</code>	Displays the IP routing table for the default VRF
<code>show ip route vrf management</code>	Displays the IP routing table for the management VRF
<code>show interface mgmt 0 brief</code>	Displays summary information about the mgmt 0 interface
<code>show interface mgmt 0</code>	Displays detailed information about the mgmt 0 interface
<code>ping <x.x.x.x></code>	Pings a remote address using the default VRF
<code>ping <x.x.x.x> vrf management</code>	Pings a remote address using the management VRF

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

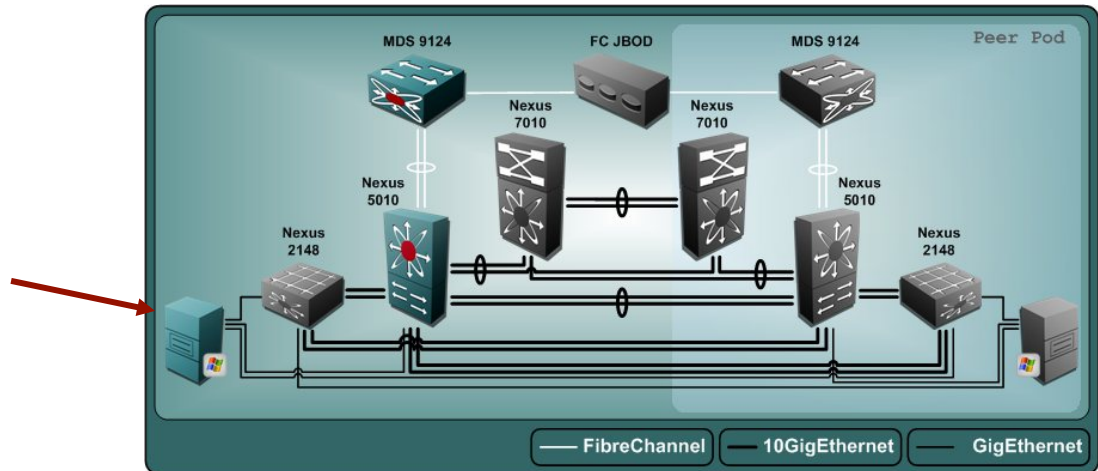
Task 1: Connect to a Cisco Nexus 5000 Series Switch Using SSH

In this task, you will use SSH to connect to a Cisco Nexus 5000 Series switch.

Activity Procedure

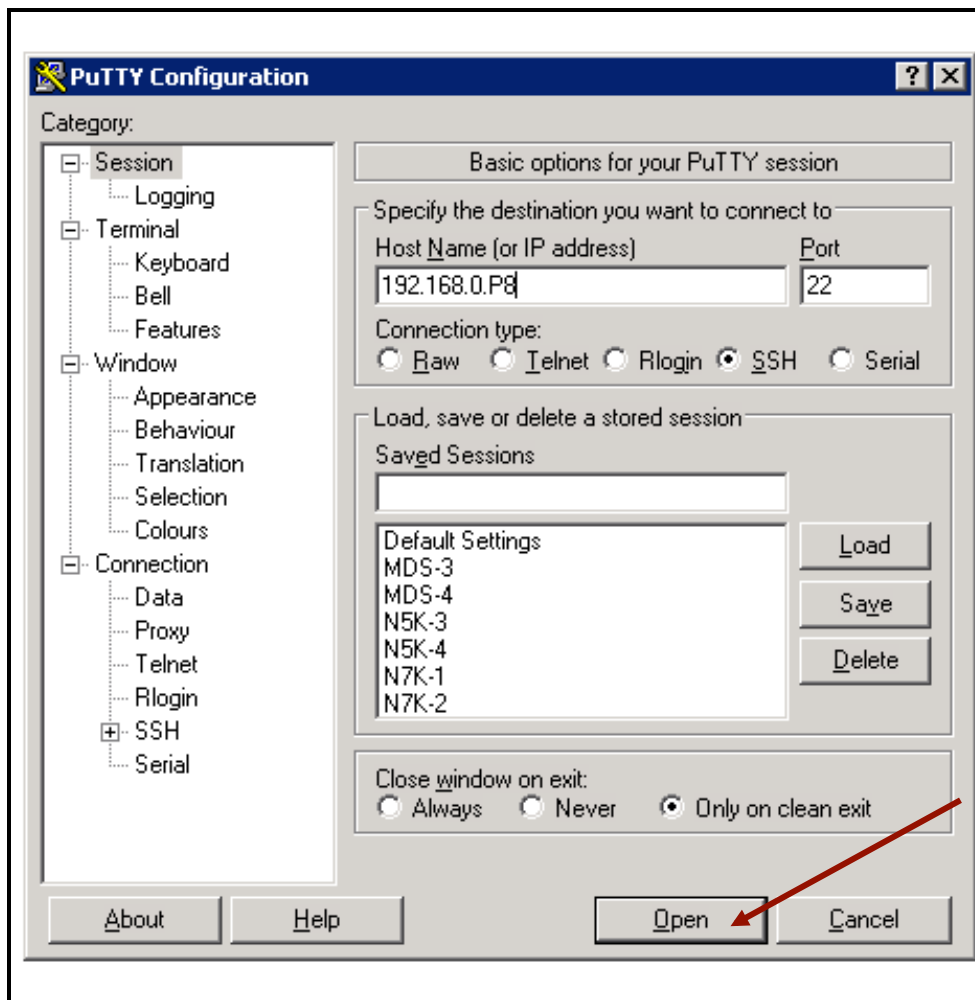
Complete these steps:

- Step 1** Connect to the remote lab GUI at <http://remotelabs.flane.de> using the credentials supplied by your instructor
- Step 2** Click on the **blue** Server icon in the remote lab GUI and wait for the NX window to open.



- Step 3** Log in to the PC using username **administrator** and password **1234QWer**.
- Step 4** Use Putty or Teraterm (or windows telnet) to connect to a Nexus 5000 switch. Use the IP address 192.168.1.P8 (or refer to the table below)

Pod #	Telnet/ssh to
1	192.168.0.18
2	192.168.0.28
3	192.168.0.38
4	192.168.0.48
5	192.168.0.58
6	192.168.0.68
7	192.168.0.78
8	192.168.0.88



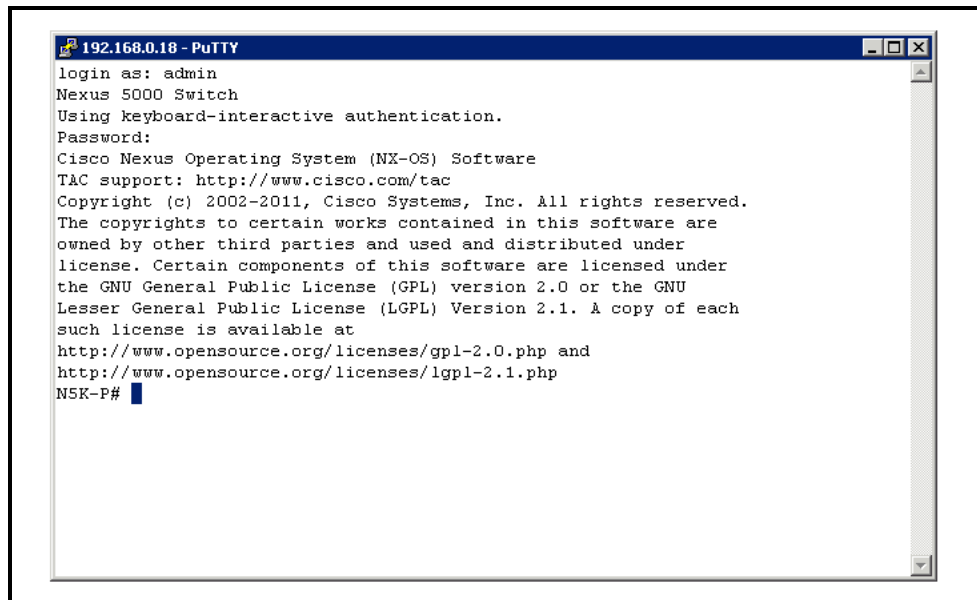
Step 5 Click the **Open** button to open the session.

Step 6 When the session opens you will be asked for credentials for logging into the switch. Log in as student using username **admin** and password **1234QWer**.

Activity Verification

You have completed this task when you attain this result:

- You have successfully logged into both switches.



```
192.168.0.18 - PuTTY
login as: admin
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
NSK-P#
```

Task 2: Verify Interface Management 0 Configuration

In this task, you will use **show** commands to verify the configuration that was applied to management 0 in the previous lab.

Activity Procedure

Complete these steps on both N5K switches:

- Step 1** At the command prompt, enter the **show running-config interface mgmt 0** to verify the configuration of management 0.

```
N5K-P # show running-config interface mgmt 0

!Command: show running-config interface mgmt0
!Time: Wed Feb 18 12:01:35 2009

version 5.1(3)N1(1)

interface mgmt0
  ip address 192.168.0.P8/24
```

```
N5K-P#
```

- Step 2** Verify that the IP address of each Cisco Nexus 5000 Series switch is as follows:

```
N5K:                192.168.0.P8
```

- Step 3** Verify that the default route has been correctly set using the command **show running-config | include route**.

```
N5K-P# show running-config | include route
ip route 0.0.0.0/0 192.168.0.1
N5K-P#
```

- Step 4** The Cisco Nexus 5000 Series switch supports two default VRFs. One is called **management** and the other is called **default**. Use the following commands to verify that the default route has been set for the correct VRF.

```
N5K-P# show ip route

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

```
N5K-P#
```

```
N5K-P# show ip route vrf management

IP Route Table for VRF "management"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
```

```
0.0.0.0/0, ubest/mbest: 1/0
  *via 192.168.0.1, mgmt0, [1/0], 00:15:15, static
192.168.0.0/24, ubest/mbest: 1/0, attached
  *via 192.168.0.18, mgmt0, [0/0], 00:15:15, direct
```

```
192.168.0.18/32, ubest/mbest: 1/0, attached
    *via 192.168.0.18, mgmt0, [0/0], 00:15:15, local
N5K-P#
```

Q1) Which VRF is using the default route of 192.168.0.1? _____

Q2) Is this VRF the correct VRF? _____

Q3) Based on your answer, explain why this is, or is not, the correct VRF.

Step 5 Verify that the management 0 interface is administratively and operationally up using the **show interface mgmt 0 brief**.

```
N5K-P# show interface mgmt 0 brief
```

```
-----
Port      VRF      Status IP Address      Speed      MTU
-----
mgmt0     --      up      192.168.0.P8    1000      1500
N5K-P#
```

Step 6 Check the management 0 interface details using the **show interface mgmt 0** command.

```
N5K-P# show interface mgmt 0
```

mgmt0 is up

```
Hardware: GigabitEthernet, address: 547f.ee5c.6ea1 (bia 547f.ee5c.6ea1)
```

```
Internet Address is 192.168.0.P8/24
```

```
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA
```

```
full-duplex, 1000 Mb/s
```

```
EtherType is 0x0000
```

```
1 minute input rate 1168 bits/sec, 1 packets/sec
```

```
1 minute output rate 816 bits/sec, 0 packets/sec
```

```
Rx
```

```
36258 input packets 293 unicast packets 33536 multicast packets
```

```
2429 broadcast packets 3189819 bytes
```

```
Tx
```

```
3470 output packets 207 unicast packets 3262 multicast packets
```

```
1 broadcast packets 804357 bytes
```

```
N5K-P#
```

Activity Verification

You have completed this task when you attain these results:

- You have confirmed that the IP configuration for the management 0 interface is correctly configured.
- You have confirmed that the IP default route is configured for the correct VRF.
- You have confirmed that the mgmt 0 interface is up both administratively and operationally.

Lab 1-4: Running CLI Commands

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

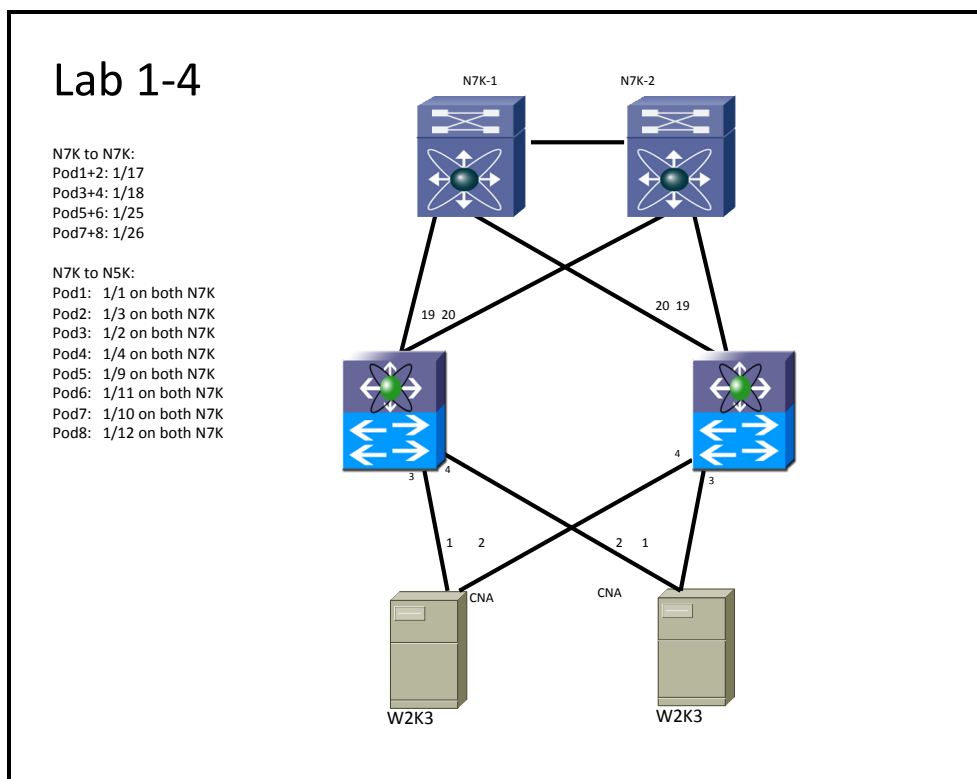
Activity Objective

In this activity, you will connect to a Cisco Nexus 7000 Series switch and a 5000 Series switch to run various **show** commands. After completing this activity, you will be able to meet these objectives:

- Use the **show** commands to verify VLANs and VLAN membership
- Use the **show** commands to verify which interfaces are operational
- Use the **show** commands to verify the MAC address table
- Verify which Cisco NX-OS Software version is running on the switch
- Verify the running and startup configurations
- Use the **show** commands to verify if there are any connectivity issues in the network

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

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

- One Cisco Nexus 7000 Series VDC
- One Cisco Nexus 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show vlan</code>	Displays the currently configured VLANs and the interfaces that are associated with those VLANs
<code>show vlan summary</code>	Displays a summary of the number of VLANs that are configured
<code>show interface brief</code>	Displays a summary of the interfaces, showing the status of those interfaces
<code>show interface trunk</code>	Displays details of which interfaces are trunking and if there are any issues with the VLANs that are on the trunks
<code>show mac address-table</code>	Displays the switch MAC address table
<code>show mac address-table learning-mode</code>	Displays the learning mode for MAC addresses on the VLANs
<code>show mac address-table vlan <x></code>	Displays the MAC address table for a given VLAN
<code>show mac address-table aging-time</code>	Displays how long MAC addresses will be kept in the table
<code>show version</code>	Displays details that are related to the Cisco NX-OS Software version that is being used
<code>show startup-config</code>	Displays the startup configuration of the switch
<code>show running-config</code>	Displays the running configuration of the switch
<code>show running-config <feature> <all></code>	Displays the running configuration of a specific feature on the switch
<code>show feature</code>	Displays the features that are currently enabled on the switch
<code>show tech-support</code>	Displays the output of the tech-support command
<code>show tech-support > volatile:<filename></code>	Directs the output of the tech-support command to a file in volatile memory
<code>show cdp neighbor</code>	Displays the neighbors that are found using Cisco Discovery Protocol
<code>show run vpc</code>	Displays the vPC configuration from the running configuration
<code>show tech vpc</code>	Displays the output of the tech-support command for the vPC configuration

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Verify VLAN and VLAN Membership

In this task, you will use CLI commands to verify the VLAN database and membership.

Activity Procedure

Complete these steps:

Step 7 On your Nexus 5000 switch load the configuration file for this lab.

```
N5K-P# rollback running-config file bootflash:DCICTv10/lab1-4
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
..
Collecting Running-Config
#Generating Rollback Patch

Rollback completed successfully.

N5K-P#
```

Step 8 On your Nexus 7000 VDC load the configuration file for this lab.

```
N7K-X-Pod## rollback running-config file bootflash:DCICTv10/lab1-4
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch

Rollback completed successfully.

N7K-X-Pod##
```

Step 9 On your Cisco Nexus 5000 Series Switch, identify which VLANs are currently check configured.

```
N5K-P# show vlan summary

Number of existing VLANs           : 3
Number of existing user VLANs      : 3
Number of existing extended VLANs  : 0
```

- Q1) How many VLANs have been configured on the switch? _____

- Q2) Have the same number of VLANs been configured on the Cisco Nexus 7000 Series switch?

- Q3) If you have a different number of VLANs between the switches, which VLANs are they? _____

Step 10 Use the **show vlan** command to find out which interfaces are members of which VLAN on both the Cisco Nexus 7000 Series and 5000 Series Switches.

N7K-X-Pod## **sh vlan**

VLAN	Name	Status	Ports
1	default	active	Eth1/1, Eth1/3, Eth1/17 Eth1/19, Eth3/1, Eth3/2, Eth3/11 Eth3/12
113	VLAN0113	active	Eth1/1, Eth1/3, Eth1/17 Eth1/19
114	VLAN0114	active	Eth1/1, Eth1/3, Eth1/17 Eth1/19

VLAN	Type	Vlan-mode
1	enet	CE
113	enet	CE
114	enet	CE

Remote SPAN VLANs

Primary	Secondary	Type	Ports
-----	-----	-----	-----

N7K-X-Pod##

N5K-P# **sh vlan**

VLAN	Name	Status	Ports
1	default	active	Eth1/1, Eth1/2, Eth1/5, Eth1/6 Eth1/7, Eth1/8, Eth1/9, Eth1/10 Eth1/11, Eth1/12, Eth1/13 Eth1/14, Eth1/15, Eth1/16 Eth1/17, Eth1/18, Eth1/19 Eth1/20, Eth1/21, Eth1/22 Eth1/23, Eth1/24, Eth1/25 Eth1/26, Eth1/27, Eth1/28 Eth1/29, Eth1/30, Eth1/31 Eth1/32
113	VLAN0113	active	Eth1/3, Eth1/19, Eth1/20
114	VLAN0114	active	Eth1/4, Eth1/19, Eth1/20
VLAN	Name	Status	Ports
----	-----	-----	-----

Remote SPAN VLANs

Primary	Secondary	Type	Ports
-----	-----	-----	-----

Q4) Are there any interfaces that are members of multiple VLANs? _____

Q5) What is the reason for this? _____

Step 11 Do not log out of the switches because you will be using the same connections and configurations for the following task.

Activity Verification

You have completed this task when you attain these results:

- You have successfully identified which VLANs have been configured and which interfaces are members of which VLAN.
- You have correctly identified why some interfaces are members of multiple VLANs.

Task 2: Verify Interface States

In this task, you will use CLI commands to verify the interface states.

Activity Procedure

Complete these steps:

- Step 1** If you logged out of your assigned switches, please log in again for this task.
- Step 2** The **show interface brief** command is used to provide a summary state of all interfaces on the switch. Run the **show interface brief** command on both the Cisco Nexus 7000 Series and 5000 Series Switches.

N5K-P# **show interface brief**

```
-----
Ethernet      VLAN   Type Mode   Status Reason                               Speed
Port
Interface                                           Ch #
-----
Eth1/1        1      eth  access down  SFP not inserted                    10G(D) --
Eth1/2        1      eth  access down  SFP not inserted                    10G(D) --
Eth1/3        113    eth  access up    none                                10G(D) --
Eth1/4        114    eth  access up    none                                10G(D) --
Eth1/5        1      eth  access down  SFP not inserted                    10G(D) --
Eth1/6        1      eth  access down  SFP not inserted                    10G(D) --
Eth1/7        1      eth  access down  SFP not inserted                    10G(D) --
Eth1/8        1      eth  access down  SFP not inserted                    10G(D) --
Eth1/9        1      eth  access down  Administratively down                10G(D) --
Eth1/10       1      eth  access down  Administratively down                10G(D) --
Eth1/11       1      eth  access down  Administratively down                10G(D) --
Eth1/12       1      eth  access down  SFP not inserted                    10G(D) --
Eth1/13       1      eth  access down  SFP not inserted                    10G(D) --
Eth1/14       1      eth  access down  SFP not inserted                    10G(D) --
Eth1/15       1      eth  access down  Administratively down                10G(D) --
Eth1/16       1      eth  access down  SFP not inserted                    10G(D) --
Eth1/17       1      eth  access down  Administratively down                10G(D) --
Eth1/18       1      eth  access down  Administratively down                10G(D) --
Eth1/19       1      eth  trunk up     none                                10G(D) --
Eth1/20       1      eth  trunk up     none                                10G(D) --
Eth1/21       1      eth  access down  Administratively down                10G(D) --
Eth1/22       1      eth  access down  Administratively down                10G(D) --
Eth1/23       1      eth  access down  SFP not inserted                    10G(D) --
...
Eth1/32       1      eth  access down  SFP not inserted                    10G(D) --
-----

Port   VRF      Status IP Address                               Speed   MTU
-----
mgmt0  --      up     192.168.0.18                             1000
1500
N5K-P#
```

N7K-X-Pod## **show interface brief**

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	192.168.0.201	1000	1500

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth1/1	1	eth	trunk	up	none	10G(S)	--
Eth1/3	1	eth	trunk	up	none	10G(S)	--
Eth1/5	--	eth	routed	down	Administratively down	auto(S)	--
Eth1/7	--	eth	routed	down	SFP not inserted	auto(S)	--
Eth1/17	1	eth	trunk	up	none	10G(S)	--
Eth1/19	1	eth	trunk	up	none	10G(S)	--
Eth1/21	--	eth	routed	down	SFP not inserted	auto(S)	--
Eth1/23	--	eth	routed	down	SFP not inserted	auto(S)	--
Eth3/1	1	eth	access	down	Administratively down	auto(D)	--
Eth3/2	1	eth	access	down	Administratively down	auto(D)	--
Eth3/11	1	eth	access	down	Administratively down	auto(D)	--
Eth3/12	1	eth	access	down	SFP not inserted	auto(D)	--

N7K-X-Pod##

Q1) What is the default mode for interfaces on the Cisco Nexus 5000 Series switch?

Q2) What is the default mode for interfaces on the Cisco Nexus 7000 Series switch?

Q3) When were these default modes set? _____

Step 3 Some of the interfaces on the switches are set as trunk interfaces. Check whether any of these interfaces have any VLAN errors disabled on the Trunk using the command **show interface trunk**.

Note Your output may not match the lab guide output exactly.

N5K-P# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/19	1	trunking	--
Eth1/20	1	trunking	--

Port	Vlans Allowed on Trunk
------	------------------------

```

-----
Eth1/19      1,113-114
Eth1/20      1,113-114

```

```

-----
Port          Vlans Err-disabled on Trunk
-----

```

```

Eth1/19      none
Eth1/20      none

```

```

-----
Port          STP Forwarding
-----

```

```

Eth1/19      none
Eth1/20      1,113-114

```

```

-----
Port          Vlans in spanning tree forwarding state and not pruned
-----

```

```

Eth1/19      --
Eth1/20      --
N5K-P#

```

Q4) Were there any VLANs disabled on the Cisco Nexus 5000 Series switch? _____

Q5) Were there any VLANs disabled on the Cisco Nexus 7000 Series switch? _____

Activity Verification

You have completed this task when you attain these results:

- You have successfully verified the state of the interfaces.
- You have successfully identified the device that is connected to the 1-Gb/s interface on the Cisco Nexus 5000 Series switch.
- You have successfully verified there are no error-disabled VLANs on the trunk interfaces.

Task 3: Verify the MAC Address Table

In this task, you will use CLI commands to verify the MAC address table.

Activity Procedure

Complete these steps:

- Step 1** If you logged out of your assigned switches, please log in again for this task.
- Step 2** As MAC addresses are discovered, they are put into a MAC address table. Use the following command to identify which MAC addresses are currently in the table on the Cisco Nexus 7000 Series switch: **show mac address-table**.

Note Your output may not match the lab guide output exactly.

N7K-X-Pod## **show mac address-table**

Legend:

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

VLAN	MAC Address	Type	age	Secure	NTFY	Ports/SWID.SSID.LID
G -	0026.51cc.de42	static	-	F	F	sup-eth1 (R)
* 113	00c0.dd11.2a18	dynamic	30	F	F	Eth1/3
* 113	00c0.dd11.2d14	dynamic	0	F	F	Eth1/3
* 114	00c0.dd11.2a1a	dynamic	30	F	F	Eth1/3
* 114	00c0.dd11.2d16	dynamic	0	F	F	Eth1/3

N7K-X-Pod##

- Step 3** Using the **show mac address-table aging-time** command, find out the aging time for entries in the MAC address table.

N7K-X-Pod## **show mac address-table aging-time**

Vlan	Aging Time
------	------------

----	-----
1	1800
113	1800
114	1800

N7K-X-Pod##

- Q1) What is the aging time value? _____

- Step 4** Use the **show mac address-table vlan number** command. Which MAC addresses are registered in VLAN 113?

N7K-X-Pod## **show mac address-table vlan 113**

Legend:

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

VLAN	MAC Address	Type	age	Secure	NTFY	Ports/SWID.SSID.LID
* 113	00c0.dd11.2a18	dynamic	30	F	F	Eth1/3
* 113	00c0.dd11.2d14	dynamic	0	F	F	Eth1/3

N7K-X-Pod##

Q2) How have the MAC addresses been discovered? _____

Q3) We have no Cisco FabricPath configured. Using the **show mac address-table learning-mode** command, what is the learning mode for MAC addresses on the Cisco Nexus 7000 Series switch? _____

```
N7K-X-Pod## show mac address-table learning-mode
Vlan      Learning Mode
----      -
1         Non-Conversational-Learning
113       Non-Conversational-Learning
114       Non-Conversational-Learning
N7K-X-Pod##
```

Activity Verification

You have completed this task when you attain these results:

- You have successfully verified the MAC address table.
- You have successfully identified the learning mode for MAC addresses.
- You have successfully identified how MAC addresses have been discovered.

Task 4: Verify the Cisco NX-OS Software

In this task, you will use CLI commands to verify the Cisco NX-OS version.

Activity Procedure

Complete these steps:

- Step 1** If you logged out of your assigned switches, please log in again for this task.
- Step 2** The **show version** command shows you which version of software you are running currently on the switch. Use the **show version** command to answer the following questions (the following output is an example of the output you will see on the switches):

Note Your output may not match the lab guide output exactly.

```
N7K-X-Pod## sh ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents:
http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:          version 3.22.0
  kickstart:     version 6.0(3)
  system:        version 6.0(3)
  BIOS compile time:    02/20/10
  kickstart image file is: bootflash:///n7000-s1-kickstart.6.0.3.bin
  kickstart compile time: 12/25/2020 12:00:00 [04/13/2012 01:44:26]
  system image file is:   bootflash:///n7000-s1-dk9.6.0.3.bin
  system compile time:    3/21/2012 19:00:00 [04/13/2012 03:09:27]

Hardware
  cisco Nexus7000 C7010 (10 Slot) Chassis ("Supervisor module-1X")
  Intel(R) Xeon(R) CPU          with 4110372 kB of memory.
  Processor Board ID JAF1311AFBL

  Device name: N7K-1
  bootflash:    2030616 kB
  slot0:        1013825 kB (expansion flash)

Kernel uptime is 19 day(s), 6 hour(s), 18 minute(s), 0 second(s)

Last reset
  Reason: Out of service
  System version: 6.0(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin
N7K-X-Pod##
```

```
N5K-P# sh ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2011, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:          version 3.5.0
  loader:        version N/A
  kickstart:     version 5.0(3)N2(1)
  system:        version 5.0(3)N2(1)
  power-seq:     Module 1: version v1.0
                  Module 3: version v2.0
  uC:            version v1.2.0.1
  SFP uC:        Module 1: v1.0.0.0
  BIOS compile time:    02/03/2011
  kickstart image file is: bootflash:/n5000-uk9-kickstart.5.0.3.N2.1.bin
  kickstart compile time: 6/13/2011 6:00:00 [06/13/2011 13:43:33]
  system image file is:   bootflash:/n5000-uk9.5.0.3.N2.1.bin
  system compile time:    6/13/2011 6:00:00 [06/13/2011 15:33:42]

Hardware
  cisco Nexus5548 Chassis ("O2 32X10GE/Modular Universal Platform Supervisor")
  Intel(R) Xeon(R) CPU          with 8299528 kB of memory.
  Processor Board ID JAF1522AFQN

  Device name: N5K-P
  bootflash:    1908736 kB

Kernel uptime is 0 day(s), 1 hour(s), 31 minute(s), 26 second(s)

Last reset at 364471 usecs after  Wed Dec 26 06:52:16 2012

Reason: Reset Requested by CLI command reload
System version: 5.0(3)N2(1)
Service:

plugin
  Core Plugin, Ethernet Plugin
N5K-P#
```

- Q1) Which version of the kickstart image is running on each of these switches?
Cisco Nexus 7000 Series switch: _____
Cisco Nexus 5000 Series switch: _____
- Q2) Which version of the system image is running on each of these switches?
Cisco Nexus 7000 Series switch: _____
Cisco Nexus 5000 Series switch: _____
- Q3) Are you running the same version of kickstart and system image on the switches?

- Q4) Are you running the same version of software on both the Cisco Nexus 7000 Series and 5000 Series Switches? _____

- Q5) How long has the switch been operating? _____

- Q6) What is the reason for the last switch reset? _____

Activity Verification

You have completed this task when you attain this result:

- You have successfully verified the Cisco NX-OS software image that is being used.

Task 5: Verify the Running and Startup Configuration

In this task, you will use CLI commands to verify the running and startup configuration.

Activity Procedure

Complete these steps:

Step 1 If you logged out of your assigned switches, please log in again for this task.

Step 2 The **show running-config** command is used to show the running configuration. Use the command to see what your current configuration looks like.

```
N7K-X-Pod## sh run
```

```
!Command: show running-config
!Time: Mon Jan 21 15:04:48 2013
```

```
version 6.0(3)
switchname Pod1
```

```
feature telnet
```

```
username admin password 5 $1$dHjqGxBx$T1pOIq3A6pTB208MBnMTQ0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x4e8ee60453a201525eba401aed299024
pri
v 0x4e8ee60453a201525eba401aed299024 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
```

```
vrf context management
 ip route 0.0.0.0/0 192.168.0.1
vlan 1,113-114
```

```
interface Ethernet1/1
 switchport
 switchport mode trunk
 no shutdown
```

```
interface Ethernet1/3
 switchport
 switchport mode trunk
 no shutdown
```

```
interface Ethernet1/5
```

```
interface Ethernet1/7
```

```
interface Ethernet1/17
 switchport
 switchport mode trunk
 no shutdown
```

```
interface Ethernet1/19
 switchport
 switchport mode trunk
 no shutdown
```

```
interface Ethernet1/21
```

```
interface Ethernet1/23
```

```
interface Ethernet3/1
```

```

interface Ethernet3/2

interface Ethernet3/11

interface Ethernet3/12

interface mgmt0
  ip address 192.168.0.201/24
  line vty

N7K-X-Pod##

```

- Q1) Use the **show startup-config** command to see the startup configurations.
- Q2) Use **show running-config diff** to see differences between startup and running configurations. Are the running and startup configurations the same?
-
-

Q3)

- Step 3** The configuration for this lab includes spanning-tree. Use the **show running-config spanning-tree** command on the Cisco Nexus 7000 Series switch to view the NONDEFAULT parameters that are configured for this feature.

```

N7K-X-Pod## sh run spanning-tree
N7K-X-Pod##

```

- Step 4** The **show running-config spanning-tree all** command shows you the DEFAULT configuration for spanning-tree.

```

N7K-X-Pod## sh run spanning-tree all
spanning-tree mode rapid-pvst
spanning-tree pathcost method short
no spanning-tree port type edge default
no spanning-tree port type network default
spanning-tree bridge assurance
no spanning-tree loopguard default
spanning-tree vlan 1,113-114
spanning-tree vlan 1,113-114 priority 32768
spanning-tree vlan 1,113-114 hello-time 2
spanning-tree vlan 1,113-114 forward-time 15
spanning-tree vlan 1,113-114 max-age 20
interface Ethernet1/1
  spanning-tree port-priority 128
  spanning-tree cost auto
  spanning-tree link-type auto
  no spanning-tree bpduguard
  no spanning-tree bpdufilter
interface Ethernet1/3
  spanning-tree port-priority 128
  spanning-tree cost auto
  spanning-tree link-type auto
  no spanning-tree bpduguard
  no spanning-tree bpdufilter
interface Ethernet1/17
  spanning-tree port-priority 128
  spanning-tree cost auto
  spanning-tree link-type auto
  no spanning-tree bpduguard
  no spanning-tree bpdufilter
interface Ethernet1/19
  spanning-tree port-priority 128

```

```

spanning-tree cost auto
spanning-tree link-type auto
no spanning-tree bpduguard
no spanning-tree bpdupfilter
N7K-X-Pod##

```

Q4) When you add the **all** parameter to the **show running-config <feature>** command, what additional configuration is actually being displayed? _____

Step 5 To be able to configure additional features, you would have had to switch on the feature. Use the **show feature** command on the Cisco Nexus 7000 Series switch to find out what other additional features are available for you to configure.

```

N7K-X-Pod## sh feature
Feature Name          Instance  State
-----
amt                   1         disabled
bfd                   1         disabled
bfd_app              1         disabled
bgp                   1         disabled
cts                   1         disabled
dhcp                 1         disabled
dot1x                 1         disabled
drap                  1         disabled
eigrp                 1         disabled
eigrp                 2         disabled
eigrp                 3         disabled
eigrp                 4         disabled
eou                   1         disabled
eth_port_sec         1         disabled
fex                   1         disabled
fipsm                 1         disabled
glbp                  1         disabled
hsrp_engine           1         disabled
interface-vlan        1         disabled
isis                  1         disabled
isis                  2         disabled
isis                  3         disabled
isis                  4         disabled
lacp                  1         disabled
ldap                  1         disabled
lisp                  1         disabled
lldp                  1         disabled
msdp                  1         disabled
netflow               1         disabled
oim                   1         disabled
ospf                  1         disabled
ospf                  2         disabled
ospf                  3         disabled
ospf                  4         disabled
ospfv3                1         disabled
ospfv3                2         disabled
ospfv3                3         disabled
ospfv3                4         disabled
otv                   1         disabled
pbr                   1         disabled

```

pim	1	disabled
pim6	1	disabled
pong	1	disabled
private-vlan	1	disabled
privilege	1	disabled
ptp	1	disabled
rip	1	disabled
rip	2	disabled
rip	3	disabled
rip	4	disabled
scheduler	1	disabled
scpServer	1	disabled
sftpServer	1	disabled
sshServer	1	enabled
tacacs	1	disabled
telnetServer	1	enabled
tunnel	1	disabled
udld	1	disabled
vpc	1	disabled
vrrp	1	disabled
vtp	1	disabled
wccp	1	disabled
N7K-X-Pod##		

Step 6 Use the same command on the Cisco Nexus 5000 Series switch. Are you running the same features? _____

```
N5K-P# sho feature
```

Feature Name	Instance	State
Flexlink	1	disabled
adapter-fex	1	disabled
bgp	1	disabled
dhcp	1	disabled
eigrp	1	disabled
eigrp	2	disabled
eigrp	3	disabled
eigrp	4	disabled
fcoe	1	disabled
fcoe-npv	1	disabled
fex	1	disabled
hsrp_engine	1	disabled
interface-vlan	1	disabled
lACP	1	disabled
ldap	1	disabled
lldp	1	enabled
msdp	1	disabled
ospf	1	disabled
ospf	2	disabled
ospf	3	disabled
ospf	4	disabled
pim	1	disabled
poe	1	disabled
private-vlan	1	disabled
privilege	1	disabled
rip	1	disabled
rip	2	disabled
rip	3	disabled
rip	4	disabled
sshServer	1	enabled
tacacs	1	disabled
telnetServer	1	enabled
udld	1	disabled
vem	1	disabled
vpc	1	disabled
vrrp	1	disabled

Activity Verification

You have completed this task when you attain these results:

- You have successfully verified the configuration that is being used in running and startup configuration.
- You have successfully verified which features are currently enabled on the Cisco Nexus 7000 Series and 5000 Series Switches.

Task 6: Use the tech-support Command

In this task, you will use CLI commands to view the tech-support command output.

Activity Procedure

Complete these steps:

- Step 1** If you logged out of your assigned switches, please log in again for this task.
- Step 2** The **show tech-support** command provides you with valuable information about the switch, and the output is often provided to Cisco TAC so that they have a complete picture of the switch that is having problems.
- Step 3** Run the **show tech-support** command on the Cisco Nexus 5000 Series switch.
- Step 4** Run the **show tech-support** command on the Cisco Nexus 7000 Series switch.
- Step 5** As you can see, there is a large amount of data to view. If you are looking for specific information, you can pull out the tech support details for a specific feature.
- Step 6** For example, run the **show tech-support vpc** on the Cisco Nexus 7000 Series switch. There is still a large amount of data, but it is now focused on a specific feature you may be having issues with.
- Step 7** It is often necessary to send this output to Cisco TAC, or you may wish to analyze the information offline. To be able to do this analysis, you can send the output to a file, which can then be copied to a TFTP server.
- Step 8** Run the **show tech-support > volatile:tech** command. In this command, you are sending the output of the command to a file called **tech**, which is being stored in **volatile** memory.

Activity Verification

You have completed this task when you attain this result:

- You have successfully run and viewed the output from the **show tech-support** command.

Lab 1-5: Configuring vPCs

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

Activity Objective

In this activity, you will connect to the Cisco Nexus 7000 Series and 5000 Series Switches and perform the tasks that are required to configure and verify vPCs.

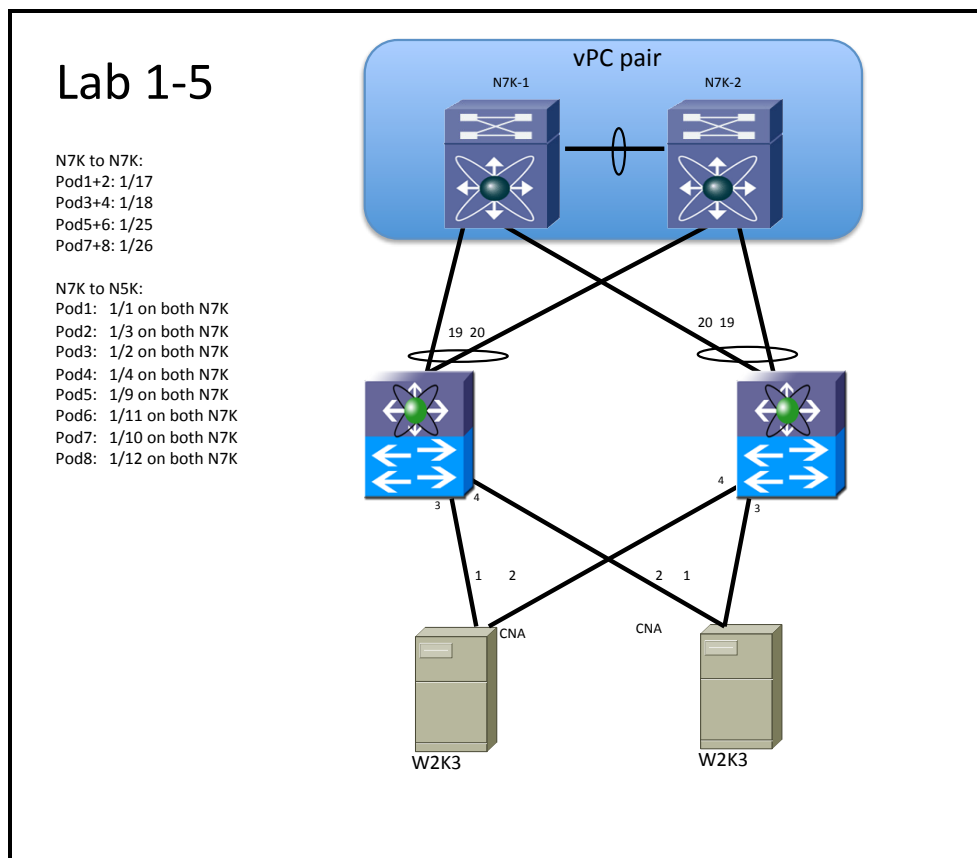
Note You will need to work with your partner workgroup to complete this task (Pods 1&2, 3&4, 5&6 and 7&8 will work together).

After completing this activity, you will be able to meet these objectives:

- Verify the existing topology and configuration
- Configure and verify the vPC domain, vPC peer link and vPC peer-keepalive link
- Configure and verify the vPCs to the downstream switches
- Use **show** commands to verify the overall vPC operation
- Save the running configurations

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 VDCs
- Two Cisco Nexus 5000 Series Switches
- One PC with an SSH application for remote connectivity
- Console connections if available

Command List

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

Command	Description
<code>show interface description</code>	Displays the description that is defined for the interfaces
<code>show interface brief</code>	Displays a summary of the interfaces, showing the status of those interfaces
<code>show cdp neighbor</code>	Displays the neighbors that are found using Cisco Discovery Protocol
<code>show ip interface brief</code>	Displays a summary of the interfaces that are configured with IP, showing the status of those interfaces
<code>ping <x.x.x.x></code>	Pings a remote address using the default VRF
<code>feature vpc</code>	Enables the vPC feature on the switch
<code>vpc domain n</code>	Defines the vPC domain on the switch
<code>peer-keepalive destination <x.x.x.x> [source <x.x.x.x> vrf <vrf-name>]</code>	Defines the vPC peer-keepalive link
<code>show running-config interface</code>	Displays the current running configuration for a specified interface
<code>channel-group n [mode active]</code>	Creates a port channel
<code>vpc peer-link</code>	Defines a port channel as a vPC peer link.
<code>description</code>	Assigns a description to an interface
<code>show port-channel summary</code>	Displays a summary of the port channels that are configured on the switch and their state
<code>show interface</code>	Displays the details of an interface
<code>show vpc brief</code>	Displays a summary of the vPC and its operating parameters
<code>copy running-config startup-config</code>	Saves the current configuration of the switch
<code>vpc n</code>	Defines a port channel as a vPC
<code>show port-channel traffic</code>	Displays the traffic utilization of the port channel
<code>show running-config vpc</code>	Displays the vPC portion of the running configuration
<code>show tech-support vpc</code>	Displays the output of the tech-support command for the vPC configuration

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Connect to Your Assigned Switch

In this task, you will be assigned a switch in the topology, which you are responsible for configuring, and you will connect to it.

Activity Procedure

Complete these steps:

Step 1 Using the credentials that are provided by your instructor, connect to the remote lab and your pod.

Note You will need to work with your partner workgroup to complete this task (Pods 1&2, 3&4, 5&6 and 7&8 will work together).

Step 2 Open an SSH session to your assigned switches and log in using the username **admin** and password **1234QWer**. Refer to the “Lab Addressing Plan: IP Addresses” section for the management IP address of your switch.

Note Not all of the following tasks in this lab exercise are performed on all switches.

Activity Verification

You have completed this task when you attain these results:

- You have successfully identified which switch you and your pod are responsible for configuring during this lab.
- You have successfully logged into that device via SSH.

Task 2: Verify Interswitch Connections

In this task, you will use CLI commands to verify the physical connections between the Cisco Nexus 7000 Series and Cisco Nexus 5000 Series Switches. This task will be performed on all switches.

Activity Procedure

Complete these steps on all switches:

Step 3 On your Nexus 5000 switch load the configuration file for this lab.

```
N5K-P# rollback running-config file bootflash:DCICTv10/lab1-5
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
..
Collecting Running-Config
#Generating Rollback Patch

Rollback completed successfully.
```

N5K-P#

Step 4 On your Nexus 7000 VDC load the configuration file for this lab.

```
N7K-X-Pod## rollback running-config file bootflash:DCICTv10/lab1-5
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch

Rollback completed successfully.
```

N7K-X-Pod##

Step 1 Review the interface connectivity by examining the descriptions that are assigned to the interfaces. Compare the output to your topology diagram for all interfaces that are in use.

Step 2 Verify that the required interfaces are operational by comparing the output of the **show interface brief** command to your topology diagram

```
N7K-X-Pod## sh int brief
```

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	192.168.0.201	1000	1500

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth1/1	1	eth	trunk	up	none	10G(S)	--
Eth1/3	1	eth	trunk	up	none	10G(S)	--
Eth1/5	--	eth	routed	down	Administratively down	auto(S)	--
Eth1/7	--	eth	routed	down	SFP not inserted	auto(S)	--
Eth1/17	1	eth	trunk	up	none	10G(S)	--
Eth1/19	1	eth	trunk	up	none	10G(S)	--
Eth1/21	--	eth	routed	down	SFP not inserted	auto(S)	--
Eth1/23	--	eth	routed	down	SFP not inserted	auto(S)	--

```

Eth3/1      1      eth  access down  Administratively down  auto(D)  --
Eth3/2      1      eth  access down  Administratively down  auto(D)  --
Eth3/11     1      eth  access down  Administratively down  auto(D)  --
Eth3/12     1      eth  access down  SFP not inserted      auto(D)  --
N7K-X-Pod##

```

Step 3 Determine which remote device is connected on each of the links and that the connection is on the correct interface.

```
N7K-X-Pod## sho cdp neigh
```

```

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

```

```

Device-ID          Local Intrfce Hldtme Capability Platform      Port ID
N5K-P (SSI151307WJ) Eth1/1         139    S I s      N5K-C5548UP  Eth1/19
N5K-Q (SSI15150M46) Eth1/3         139    S I s      N5K-C5548UP  Eth1/20
N7K-X-Pod# (TBM12368105)
                  Eth1/Z1         149    R S I s    N7K-C7010    Eth1/Z1
N7K-X-Pod# (TBM12368105)
                  Eth1/Z2         149    R S I s    N7K-C7010    Eth1/Z2
N7K-X-Pod##

```

Activity Verification

You have completed this task when you attain these results:

- You have verified that all interfaces between the switches are operational.
- You have verified that all links between the switches are connected to the correct device and interface.

Task 3: Establish the vPC Domain

In this task, you will use CLI commands to configure and verify the vPC domain between the Cisco Nexus 7000 Series Switches. This task will be performed only on the Cisco Nexus 7000 Series Switches.

Activity Procedure

Complete these steps on your Cisco Nexus 7000 Series Switches:

Step 1 Enable the vPC feature.

```
N7K-X-PodY# conf
Enter configuration commands, one per line. End with CNTL/Z.
N7K-X-PodY#(config)# feature vpc
N7K-X-PodY#(config)#
```

Step 2 Configure the vPC domain ID. This configuration must be the same on both Cisco Nexus 7000 Series Switches but unique in your data center. Use the number from the following table

Pod number	VPC domain ID
1 & 2	12
3 & 4	34
5 & 6	56
7 & 8	78

```
N7K-X-PodY#(config)# vpc domain ?
<1-1000> Domain id
```

```
N7K-X-PodY#(config)# vpc domain PQ
N7K-X-PodY#(config-vpc-domain)#
```

Note The domain ID can be any value if the same value is configured on both switches forming the vPC pair.

Step 3 Configure the vPC peer-keepalive link. The destination address used in this command is the IP address of the remote Cisco Nexus 7000 Series switch. Use the MANAGEMENT IP from your Partner Pod. (192.168.20Q)

```
N7K-X-PodY#(config-vpc-domain)# peer-keepalive destination 192.168.0.20Q
Note:
-----:: Management VRF will be used as the default VRF ::-----
N7K-X-PodY#(config-vpc-domain)#
```

Q1) Which VRF is used if you don not specify one in the peer-keepalive command?

Step 4 Refer to the previous task, or issue a command to verify the interswitch connectivity. Refer to your topology diagram.

Q2) Determine which interfaces of the local Cisco Nexus 7000 Series switch is used to connect to the remote Cisco Nexus 7000 Series switch.

Pod	Interface
1 & 2	Ethernet 1/17
3 & 4	Ethernet 1/18

5 & 6	Ethernet 1/25
7 & 8	Ethernet 1/26

Step 5 Determine the current configuration of these interfaces.

```
N7K-X-PodY#(config-vpc-domain) # show running-config interface e1/xx
```

```
!Command: show running-config interface Ethernet1/xx
!Time: Mon Jan 21 16:02:48 2013
```

```
version 6.0(3)
```

```
interface Ethernet1/xx
  switchport
  switchport mode trunk
  no shutdown
```

```
N7K-X-Pod#(config-vpc-domain) #
```

Step 6 A traditional port channel will be configured statically between the Cisco Nexus 7000 Series Switches using these interfaces. Use channel group number 7.

Note The channel group number can be any value between 1 and 4096. The system automatically creates a port channel interface using the same number.

```
N7K-X-PodY#(config-vpc-domain) # interface ethernet 1/xx
N7K-X-PodY#(config-if) # channel-group 999
N7K-X-PodY#(config-if) #
```

Step 7 Configure the port channel interface as a vPC peer link. Note the messages that are generated automatically by the system.

```
N7K-X-PodY#(config-if-range) # interface port-channel 999
N7K-X-PodY#(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.
N7K-X-PodY#(config-if) #
```

Step 8 Assign a description to the port channel interface.

```
N7K-X-PodY#(config-if) # description vpc peer-link between Cisco Nexus 7000
Series Switches
N7K-X-PodY#(config-if) # end
```

Step 9 Once both switches have completed the port channel configuration from the preceding steps, verify that the port channel interface is operational.

```
N7K-X-Pod#(config-if) # sho port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        S - Suspended     r - Module-removed
        U - Up            R - Routed
        M - Not in use.  Min-links not met
```

```
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
```

```
999  Po999(SU)  Eth      NONE      Eth1/xx(P)
```

```
N7K-X-Pod#(config-if) #
```

Step 10 Verify the details of the port channel interface.

```
N7K-X-Pod## sho int po 999
port-channel999 is up
```

```

Hardware: Port-Channel, address: 0026.0b91.6248 (bia 0026.0b91.6248)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s
Input flow-control is off, output flow-control is off
Switchport monitor is off
EtherType is 0x8100
Members in this channel: Eth1/17
Last clearing of "show interface" counters never
30 seconds input rate 1152 bits/sec, 1 packets/sec
30 seconds output rate 1152 bits/sec, 1 packets/sec
Load-Interval #2: 5 minute (300 seconds)
  input rate 2.29 Kbps, 1 pps; output rate 1.72 Kbps, 0 pps
-- output omitted --

```

Step 11 Verify that the vPC domain is operational.

N7K-X-Pod## **sho vpc brief**

Legend:

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

```

vPC domain id                : 99
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                      : 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    Po999  up      1,113-114
N7K-X-Pod##

```

Step 12 Save the configuration of the switch.

```

N7K-X-PodY# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...

```

Activity Verification

You have completed this task when you attain these results:

- You have configured a vPC domain between two Cisco Nexus Series Switches.
- You have verified that the vPC domain is operational.

Task 4: Configure the Cisco Nexus 5000 Series Switch

In this task, you will use CLI commands to configure and verify vPCs on devices that are connected to the vPC domain. This task will be performed only on the Cisco Nexus 5000 Series Switches.

Note The Nexus 5000 is also capable of vPC but in this lab it is used as a “normal” switch without a vPC configuration. DO NOT enable and configure vPC on the Nexus 5000.

Activity Procedure

Complete these steps on both Cisco Nexus 5000 Series Switches:

Note The **feature vpc** command is not required on the devices that are connected to the vPC domain. They are only configured with a traditional port channel.

Step 1 Interfaces of the local Cisco Nexus 5000 Series switch connect to the Cisco Nexus 7000 Series Switches. Find your Pod in the table to determine which interfaces on which devices will be used.

Pod & Switch	N5K Interface	N7K Interface
Pod1: N5K-1	Ethernet 1/19 and 1/20	Ethernet 1/1
Pod2: N5K-2	Ethernet 1/19 and 1/20	Ethernet 1/3
Pod3: N5K-3	Ethernet 1/19 and 1/20	Ethernet 1/2
Pod4: N5K-4	Ethernet 1/19 and 1/20	Ethernet 1/4
Pod5: N5K-5	Ethernet 1/19 and 1/20	Ethernet 1/9
Pod6: N5K-6	Ethernet 1/19 and 1/20	Ethernet 1/11
Pod7: N5K-7	Ethernet 1/19 and 1/20	Ethernet 1/10
Pod8: N5K-8	Ethernet 1/19 and 1/20	Ethernet 1/12

Step 2 Check connectivity with CDP (sample output for Pod1)

```
N5K-P# sho cdp neigh
```

```
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, M - Two-port Mac Relay
```

```
Device ID           Local Intrfce    Hldtme  Capability  Platform  Port ID  
N7K-X-Pod#(TBM12419159 Eth1/19        120     R S I s     N7K-C7010  Eth1/1  
  
N7K-X-Pod#(TBM12368105 Eth1/20        131     R S I s     N7K-C7010  Eth1/1
```

```
N5K-P#
```

Step 3 Determine the current configuration of these interfaces.

```
N5K-P# sho run interface e1/19-20
```

```
!Command: show running-config interface Ethernet1/19-20  
!Time: Wed Dec 26 09:35:40 2012
```

```
version 5.0(3)N2(1)
```

```
interface Ethernet1/19  
  switchport mode trunk
```

```
interface Ethernet1/20
```

```
switchport mode trunk
```

```
N5K-P#
```

Step 4 Verify that these interfaces are up.

```
N5K-P# show interface ethernet 1/19-20 brief
```

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch #
Eth1/19	1	eth	trunk	up	none	10G (D)	--
Eth1/20	1	eth	trunk	up	none	10G (D)	--

Step 5 Enable LACP on your Nexus 5000

```
N5K-P(config)# feature lacp
```

```
N5K-P(config)#
```

Step 6 A traditional port channel will be configured between your Cisco Nexus 5000 Series switch and the two Cisco Nexus 7000 Series Switches that are configured as part of a vPC domain using these interfaces. Use your Pod# as the channel group number.

```
N5K-P# conf
```

Enter configuration commands, one per line. End with CNTL/Z.

```
N5K-P(config)# interface ethernet 1/19-20
```

```
N5K-P(config-if-range)# channel-group P mode active
```

Note The active keyword specifies to use IEEE 802.1ax LACP to form the port channel.

Step 7 Assign a description to the port channel interface.

```
N5K-P(config-if-range)# interface port-channel P
```

```
N5K-P(config-if)# description PortChannel to vPC Domain
```

```
N5K-P(config-if)# end
```

```
N5K-P#
```

Step 8 Verify that the port channel interface is operational.

```
N5K-P# sho port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)
```

Group	Port-Channel	Type	Protocol	Member Ports
9	Po# (SD)	Eth	LACP	Eth1/19 (I) Eth1/20 (I)

```
N5K-P#
```

Q3) Why is the state of the port channel SD (Down)? If you are not sure, proceed to the next step then answer this question. _____

Step 9 Further details relating to the port channel state are visible in the output of other commands.

```
N5K-P# show interface port-channel #
```

```
port-channel# is down (No operational members)
```

```
Hardware: Port-Channel, address: 0005.73f6.7c1b (bia 0005.73f6.7c1b)
```

```
MTU 1500 bytes, BW 20000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA
```

```
Port mode is trunk
```

```

auto-duplex, 10 Gb/s
Beacon is turned off
Input flow-control is off, output flow-control is off
Switchport monitor is off
EtherType is 0x8100
Members in this channel: Eth1/19, Eth1/20
Last clearing of "show interface" counters never
30 seconds input rate 1048 bits/sec, 131 bytes/sec, 1 packets/sec
30 seconds output rate 1280 bits/sec, 160 bytes/sec, 1 packets/sec
Load-Interval #2: 5 minute (300 seconds)
  input rate 1.14 Kbps, 1 pps; output rate 1.30 Kbps, 1 pps
RX
  0 unicast packets  347 multicast packets  0 broadcast packets
  347 input packets  25320 bytes
  0 jumbo packets  0 storm suppression bytes
  0 giants  0 input error  0 short frame  0 overrun  0 underrun
  0 watchdog  0 if down drop
  0 input with dribble  0 input discard
  0 Rx pause
TX
  0 unicast packets  372 multicast packets  0 broadcast packets
  372 output packets  34652 bytes
  0 jumbo packets
  0 output errors  0 collision  0 deferred  0 late collision
  0 lost carrier  0 no carrier  0 babble
  0 Tx pause
  0 interface resets

```

N5K-P#

N5K-P# **show interface port-channel # brief**

```

-----
Port-channel VLAN  Type Mode    Status  Reason                               Speed Protocol
Interface
-----
Po#              1      eth  trunk  down    No operational members          10G(D)  lacp
N5K-P#

```

Step 10 Save the configuration of the switch.

```

N5K-P# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...

```

Activity Verification

You have completed this task when you attain these results:

- You have configured a port channel using IEEE 802.1ax LACP on the Cisco Nexus 5000 Series switch.
- You have verified that the vPC is not operational until the vPC is also configured on the other side of the links.

Task 5: Configure the Cisco Nexus 7000 Series Switch vPCs

In this task, you will use CLI commands to configure and verify vPCs on the switches that form the vPC domain. This task will be performed only on the Cisco Nexus 7000 Series Switches.

Activity Procedure

Complete these steps on both Cisco Nexus 7000 Series Switches:

Note	The correct configuration is required on both sides of the connections before it becomes operational.
-------------	---

Step 1 Interfaces of the local Cisco Nexus 5000 Series switch connect to the Cisco Nexus 7000 Series Switches. Find your Pod in the table to determine which interfaces on which devices will be used.

Pod & Switch	N5K Interface	N7K Interface
Pod1: N5K-1	Ethernet 1/19 and 1/20	Ethernet 1/1
Pod2: N5K-2	Ethernet 1/19 and 1/20	Ethernet 1/3
Pod3: N5K-3	Ethernet 1/19 and 1/20	Ethernet 1/2
Pod4: N5K-4	Ethernet 1/19 and 1/20	Ethernet 1/4
Pod5: N5K-5	Ethernet 1/19 and 1/20	Ethernet 1/9
Pod6: N5K-6	Ethernet 1/19 and 1/20	Ethernet 1/11
Pod7: N5K-7	Ethernet 1/19 and 1/20	Ethernet 1/10
Pod8: N5K-8	Ethernet 1/19 and 1/20	Ethernet 1/12

Step 2 Determine the current configuration of the interfaces connecting to your and your Partner Pod Nexus 5000.

N7K-X-Pod## **sh run int e1/x,e1/y**

```
!Command: show running-config interface Ethernet1/x, Ethernet1/y
!Time: Mon Jan 21 16:28:53 2013
```

```
version 6.0(3)
```

```
interface Ethernet1/x
  switchport
  switchport mode trunk
  no shutdown
```

```
interface Ethernet1/y
  switchport
  switchport mode trunk
  no shutdown
```

N7K-X-Pod##

Step 3 Verify that these interfaces are up.

```
N7K-X-Pod## sho int e1/x,e1/y brief
```

```
-----  
Ethernet      VLAN      Type Mode   Status Reason           Speed  Port  
Interface                                           Ch  #  
-----  
Eth1/x        1          eth  trunk  up      none              10G(S) --  
Eth1/y        1          eth  trunk  up      none              10G(S) --  
N7K-X-Pod##
```

Step 4 Double-check connectivity with CDP

```
N7K-X-Pod## sho cdp neigh
```

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

```
Device-ID          Local Intrfce Hldtme Capability Platform      Port ID  
N5K-P (SSI151307WJ)  Eth1/x        176    S I s      N5K-C5548UP  Eth1/19  
  
N5K-Q (SSI15150M46)  Eth1/y        135    S I s      N5K-C5548UP  Eth1/20  
  
N7K-X-Pod# (TBM12368105)  
                  Eth1/z1        177    R S s      N7K-C7010    Eth1/z1  
  
N7K-X-Pod# (TBM12368105)  
                  Eth1/z2        161    R S I s    N7K-C7010    Eth1/z2  
  
N7K-X-Pod##
```

Step 5 Enable LACP on your N7K

```
N7K-X-Pod# (config) # feature lacp
```

```
N7K-X-Pod# (config) #
```

Step 6 Two traditional port channels will be configured on each Cisco Nexus 7000 Series switch to the Cisco Nexus 5000 Series Switches using these interfaces. Use the Pod number as the channel group number.

Note For this step, the configuration for both Cisco Nexus 7000 Series Switches is shown.

```
N7K-X-PodY# conf  
Enter configuration commands, one per line. End with CNTL/Z.  
N7K-X-PodY# (config) # interface ethernet 1/X  
N7K-X-PodY# (config-if-range) # channel-group P mode active  
  
N7K-X-PodY# (config) # interface ethernet 1/Y  
N7K-X-PodY# (config-if-range) # channel-group Q mode active
```

Note The active keyword specifies to use IEEE 802.1ax LACP to form the port channel.

Step 7 Assign a description to the port channel interfaces.

```
N7K-X-PodY# (config-if-range) # interface port-channel P  
N7K-X-PodY# (config-if) # description vPC to N5K-P
```

```
N7K-X-PodY#(config-if)# interface port-channel Q
N7K-X-PodY#(config-if)# description vPC to N5K-Q
N7K-X-PodY#(config-if)# end
N7K-X-PodY#
```

Step 8 Verify that the port channel interfaces. ONE link will be operational, the other will show up as “suspended”! Why?

```
N7K-X-Pod## sh 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-Channel	Type	Protocol	Member Ports
P	PoP(SU)	Eth	LACP	Eth1/X(P)
Q	PoQ(SU)	Eth	LACP	Eth1/Y(P)
999	Po999(SU)	Eth	NONE	Eth1/z1(P)

```
N7K-X-Pod## sho 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-Channel	Type	Protocol	Member Ports
P	PoP(SD)	Eth	LACP	Eth1/X(s)
Q	PoQ(SD)	Eth	LACP	Eth1/Y(s)
999	Po999(SU)	Eth	NONE	Eth1/17(P)

```
N5K-P# sho port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)
```

Group	Port-Channel	Type	Protocol	Member Ports
9	Po9(SU)	Eth	LACP	Eth1/19(P) Eth1/20(s)

Step 9 Display the configuration of the port channel interfaces on the N7K.

```
N7K-X-Pod## sh running-config interface poP, poQ

!Command: show running-config interface port-channelP, port-channelQ
!Time: Mon Jan 21 16:41:16 2013

version 6.0(3)

interface port-channelP
 switchport
 switchport mode trunk

interface port-channelQ
 switchport
```

```
switchport mode trunk

N7K-X-Pod##
```

Step 10 Port channel interfaces are currently not vPCs. These two port channels have been configured independently on each of the Cisco Nexus 7000 Series Switches. To form a vPC, each of the port channels must be bound together as a single vPC within the vPC domain.

```
N7K-X-PodY# conf
Enter configuration commands, one per line. End with CNTL/Z.
N7K-X-PodY#(config)# interface port-channel P
N7K-X-PodY#(config-if)# vpc P
N7K-X-PodY#(config-if)# interface port-channel Q
N7K-X-PodY#(config-if)# vpc Q
N7K-X-PodY#(config-if)# end
N7K-X-PodY#
```

Note The port channel number and the vPC number do not have to be the same, but it is recommended that you keep them the same for consistency.

Note The vPC number must be the same on both switches for the same vPC (channel going to the same switch)

Step 11 Verify that the newly created vPCs are now part of the vPC domain.

```
N7K-X-Pod## sho vpc brief
```

Legend:

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

```
vPC domain id          : 99
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                : 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    Po999  up      1,113-114
```

```
vPC status
```

```
-----
id   Port   Status Consistency Reason          Active vlans
--   ---   -
P    PoP    up      success    success          1,113-114
Q    PoQ    up      success    success          1,113-114
```

```
N7K-X-Pod##
```

Step 12 Check the PortChannels on all switches.

```
N7K-X-Pod## sho 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-Channel	Type	Protocol	Member Ports
-------	--------------	------	----------	--------------

P	PoP(SU)	Eth	LACP	Eth1/X(P)
Q	PoQ(SU)	Eth	LACP	Eth1/Y(P)
999	Po999(SU)	Eth	NONE	Eth1/Z1(P)

N7K-X-Pod##

N7K-X-Pod## **sho 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-Channel	Type	Protocol	Member Ports
-------	--------------	------	----------	--------------

P	PoP(SU)	Eth	LACP	Eth1/1(P)
Q	PoQ(SU)	Eth	LACP	Eth1/3(P)
999	Po999(SU)	Eth	NONE	Eth1/17(P)

N7K-X-Pod##

N5K-P# **sho port-channel summary**

Flags: D - Down P - Up in port-channel (members)
 I - Individual H - Hot-standby (LACP only)
 s - Suspended r - Module-removed
 S - Switched R - Routed
 U - Up (port-channel)

Group	Port-Channel	Type	Protocol	Member Ports
-------	--------------	------	----------	--------------

9	Po9(SU)	Eth	LACP	Eth1/19(P)	Eth1/20(P)
---	---------	-----	------	------------	------------

N5K-P#

Step 13 Save the configuration of the switch.

N7K-X-PodY# **copy running-config startup-config**
[#####] 100%
Copy complete, now saving to disk (please wait)...

Activity Verification

You have completed this task when you attain these results:

- You have configured port channels using IEEE 802.1ax LACP on the Cisco Nexus 7000 Series Switches.
- You have configured two separate port channels configured on two physical switches that form a VPC domain to operate as a single vPC.
- You have verified that the vPC domain and all vPCs within the domain are operational.

Task 6: Verify the Cisco Nexus 5000 Series Switch vPCs

In this task, you will use CLI commands to verify vPCs on devices that are connected to the vPC domain. This task will be performed only on the Cisco Nexus 5000 Series Switches.

Activity Procedure

Complete these steps on both Cisco Nexus 5000 Series Switches:

Note	The vpc is now configured on both the Cisco Nexus 7000 and 5000 Series Switches and should be operational.
-------------	--

Step 1 Verify that the port channel interface is operational.

```
N5K-P# sho 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
-----
9      Po9(SU)    Eth       LACP      Eth1/19(P)  Eth1/20(P)
N5K-P#
```

Step 2 Further details relating to the port channel state are visible in the output of other commands.

```
N5K-P# sho int port-channel 9
port-channel9 is up
  Hardware: Port-Channel, address: 0005.73f6.7c1b (bia 0005.73f6.7c1b)
  MTU 1500 bytes, BW 20000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Switchport monitor is off
  EtherType is 0x8100
Members in this channel: Eth1/19, Eth1/20
  Last clearing of "show interface" counters never
  30 seconds input rate 1104 bits/sec, 138 bytes/sec, 1 packets/sec
  30 seconds output rate 176 bits/sec, 22 bytes/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 976 bps, 1 pps; output rate 872 bps, 0 pps
  -- output omitted -
```

```
N5K-P# sho int e1/19-20 brief
```

```
-----
Ethernet      VLAN   Type Mode   Status Reason              Speed
Port
Interface
#
-----
Eth1/19       1      eth  trunk  up      none                10G(D) 9
Eth1/20       1      eth  trunk  up      none                10G(D) 9
N5K-P#
```

Step 3 Verify if there is traffic flow traversing the port channel.

```
N5K-P# sho port-channel traffic
ChanId      Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
-----
          9  Eth1/19   0.33%   0.0%   25.12%  60.06%  56.18%  31.13%
          9  Eth1/20  99.66% 100.00% 74.87%  39.93%  43.81%  68.86%
N5K-P#
```

Note In this lab the traffic distribution will be very uneven since there is NO real traffic... in a real-world scenario the traffic distribution would be MUCH better.

Activity Verification

You have completed this task when you attain these results:

- You have verified port channel operation on the Cisco Nexus 5000 Series switch.
- You have verified traffic flow over the port channel interface.

Lab 1-6: Validating Cisco FabricPath Configuration

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

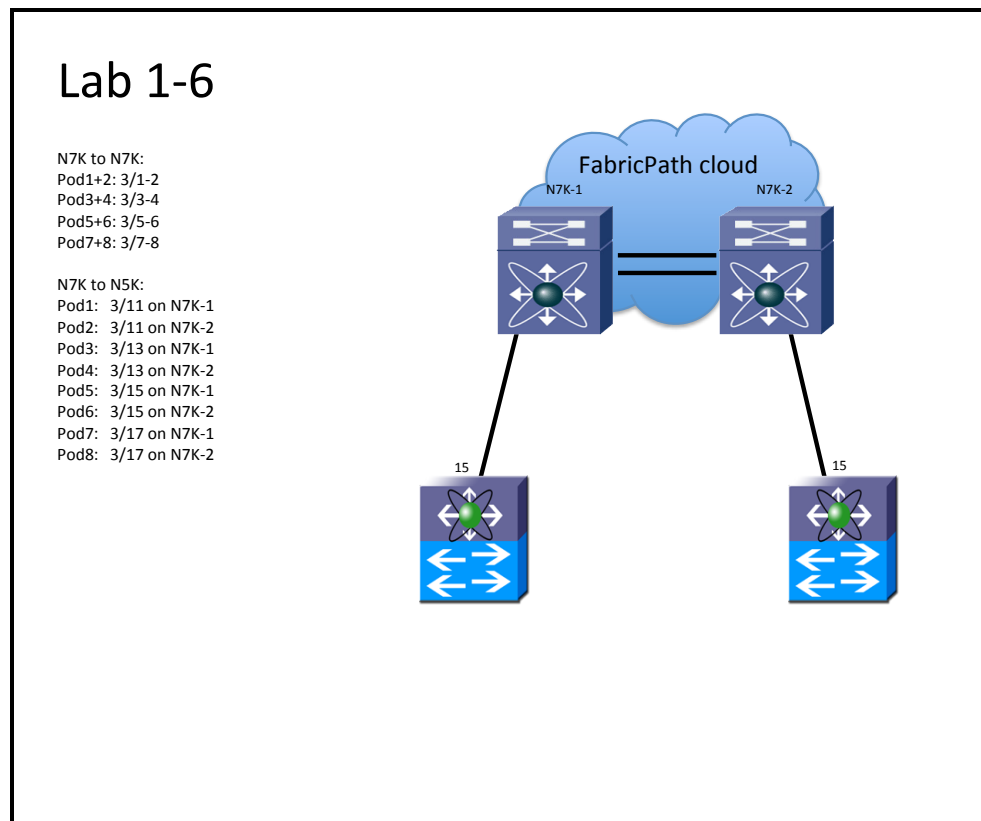
Activity Objective

In this activity, you will connect to the Cisco Nexus 7000 Series and 5000 Series Switches to validate a Cisco FabricPath configuration. After completing this activity, you will be able to meet this objective:

- Use the **show** commands to validate the Cisco FabricPath configuration

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 7000 Series VDC
- One Cisco Nexus 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show feature-set</code>	Displays which feature-set or sets have been enabled on the switch
<code>show fabricpath switch-id</code>	Displays the Cisco FabricPath switch IDs for each switch
<code>show fabricpath isis adjacency</code>	Displays the Cisco FabricPath adjacencies that have been formed
<code>show fabricpath route</code>	Displays the Cisco FabricPath routing table
<code>show mac address-table learning-mode</code>	Displays the learning mode for MAC addresses on the VLANs
<code>show spanning-tree [vlan <x>]</code>	Displays the spanning tree details for a given VLAN
<code>show cdp neighbor</code>	Displays the Cisco devices that have been discovered via Cisco Discovery Protocol
<code>show fabricpath conflict all</code>	Displays any Cisco FabricPath conflicts that have been discovered

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Validate the Cisco FabricPath Configuration

In this task, you will use CLI commands to validate the Cisco FabricPath configuration.

Activity Procedure

Complete these steps:

Step 1 Using the credentials that are provided by your instructor, connect to the remote lab and your pod PC and open SSH sessions to your N7K VDC and your N5K.

Step 2 Log into the switches using the username **admin** and password **1234QWer**.

Step 3 On your Nexus 5000 switch load the configuration file for this lab.

```
N5K-P# rollback running-config file bootflash:DCICTv10/lab1-6
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
..
Collecting Running-Config
#Generating Rollback Patch
```

Rollback completed successfully.

N5K-P#

Step 4 On your Nexus 7000 VDC load the configuration file for this lab.

```
N7K-X-Pod## rollback running-config file bootflash:DCICTv10/lab1-6
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
```

Rollback completed successfully.

N7K-X-Pod##

Note	Cisco FabricPath has been configured on both the N7K switches in the lab, with VLAN 42 configured as the FabricPath VLAN.
-------------	---

Step 5 One of the things to check when verifying a Cisco FabricPath configuration is whether the Cisco FabricPath feature set has been installed on the switch. Use the **show feature-set** command to check that this feature is enabled on each of the switches in the lab.

```
N7K-X-PodY# show feature-set
Feature Set Name      ID      State
-----
fcoe                  1      disabled
fabricpath            2      enabled
fex                   3      disabled
mpls                   4      disabled
N7K-X-PodY#
```

Step 6 Although the switch ID can be dynamically allocated, it has been configured on each switch. Using the **show fabricpath switch-id** command, verify that the switch ID for each switch has been configured as follows:

Switch	Switch-ID
N7K-X-PodY#	71
N7K-X-PodY#	72

Step 7 Using the **show fabricpath isis adjacency** command, verify that each switch has formed the correct adjacencies.

N7K-X-Pod## **sho fabricpath isis adjacency**

Fabricpath IS-IS domain: default Fabricpath IS-IS adjacency database:

System ID	SNPA	Level	State	Hold Time	Interface
N7K-X-Pod#	N/A	1	UP	00:00:23	Ethernet3/1
N7K-X-Pod#	N/A	1	UP	00:00:25	Ethernet3/2

N7K-X-Pod##

N7K-X-Pod## **sho fabricpath isis adjacency**

Fabricpath IS-IS domain: default Fabricpath IS-IS adjacency database:

System ID	SNPA	Level	State	Hold Time	Interface
N7K-X-Pod#	N/A	1	UP	00:00:29	Ethernet3/1
N7K-X-Pod#	N/A	1	UP	00:00:28	Ethernet3/2

N7K-X-Pod##

Step 8 Each switch should have four routes in the FabricPath routing table, indicating the paths that are available to each switch. Use the **show fabricpath route** to verify.

N7K-X-Pod## **sho 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

0/71/0, number of next-hops: 0

via ----, [60/0], 0 day/s 00:24:58, local

1/72/0, number of next-hops: 2

via Eth3/1, [115/40], 0 day/s 00:15:34, isis_fabricpath-default

via Eth3/2, [115/40], 0 day/s 00:15:34, isis_fabricpath-default

N7K-X-Pod##

Q4) Do any of the switches have multiple paths in the routing table to any other switch?

Q5) If so, why do these multiple paths exist?

- Step 9** When you enable Cisco FabricPath on a VLAN, the MAC address learning should change to conversational. Verify this change is the case on all switches for VLAN 42 using the command **show mac address-table learning-mode**.

```
N7K-X-Pod## sho mac address-table learning-mode
Vlan      Learning Mode
-----
1          Non-Conversational-Learning
42         Conversational-Learning
N7K-X-Pod##
```

- Step 10** When you enable Cisco FabricPath for a VLAN that VLAN is not bridged with spanning tree any more. Both N7K are edge switches and they both are the root bridge for a part of the attached (Nexus 5000) STP domain.

```
N7K-X-Pod## sho spanning-tree
```

```
VLAN0001
```

```
...
```

```
VLAN0042
```

```
Spanning tree enabled protocol rstp
```

```
Root ID      Priority      24618
```

```
Address      c84c.75fa.6000
```

```
This bridge is the root
```

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

```
15 sec
```

```
Bridge ID    Priority      24618 (priority 24576 sys-id-ext 42)
```

```
Address      c84c.75fa.6000
```

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

```
15 sec
```

```
Interface      Role Sts Cost      Prio.Nbr Type
-----
```

```
Eth3/11        Desg FWD 2          128.395 P2p
```

```
N7K-X-Pod##
```

```
N7K-X-Pod## sho spanning-tree
```

```
VLAN0001
```

```
...
```

```
VLAN0042
```

```
Spanning tree enabled protocol rstp
```

```
Root ID      Priority      24618
```

```
Address      c84c.75fa.6000
```

```
This bridge is the root
```

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

```
15 sec
```

```

      Bridge ID  Priority    24618  (priority 24576 sys-id-ext 42)
      Address    c84c.75fa.6000
      Hello Time  2   sec   Max Age 20 sec   Forward Delay
15 sec

```

```

Interface          Role Sts Cost          Prio.Nbr Type
-----
Eth3/11            Desg FWD 2          128.395 P2p

```

```
N7K-X-Pod##
```

Step 11 Verify that Cisco Discovery Protocol is still running between devices by using the command **show cdp neighbor**.

```

N7K-X-Pod## sho cdp neigh
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
N7K-X-Pod# (TBM12368105)
                  Eth3/1          172    R S I s    N7K-C7010      Eth3/1

N7K-X-Pod# (TBM12368105)
                  Eth3/2          172    R S I s    N7K-C7010      Eth3/2

N5K-P (SSI151307WJ)  Eth3/11       127    S I s      N5K-C5548UP     Eth1/15

N7K-X-Pod##

```

Step 12 Send a PING between your two N5Ks (IP 192.168.42.5Q, Q is your PEER Pod#)

```

N5K-P# ping 192.168.42.5Q
PING 192.168.42.5Q (192.168.42.5Q): 56 data bytes
64 bytes from 192.168.42.5Q: icmp_seq=0 ttl=254 time=3.432 ms
64 bytes from 192.168.42.5Q: icmp_seq=1 ttl=254 time=4.924 ms
64 bytes from 192.168.42.5Q: icmp_seq=2 ttl=254 time=4.972 ms
64 bytes from 192.168.42.5Q: icmp_seq=3 ttl=254 time=4.975 ms
64 bytes from 192.168.42.5Q: icmp_seq=4 ttl=254 time=4.972 ms

--- 192.168.42.5Q ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.432/4.655/4.975 ms
N5K-P#

```

Step 13 Check the mac address table on your N5K and N7K VDC, note the FabricPath information.

```

N5K-P# sho mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen, + - primary entry using vPC Peer-Link
VLAN      MAC Address      Type      age      Secure NTFY      Ports
-----+-----+-----+-----+-----+-----+-----

```

```
* 42      0005.73f6.4d3c    dynamic    60          F      F    Eth1/15
* 114     00c0.dd11.2d16    dynamic     0          F      F    Eth1/4
* 113     00c0.dd11.2a18    dynamic     0          F      F    Eth1/3
N5K-P#
```

N7K-X-Pod## **sho mac address-table**

Legend:

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

	VLAN	MAC Address	Type	age	Secure	NTFY	Ports	SWID.SSID.LID
-----+-----+-----+-----+-----+-----+-----								
G	-	0026.51cc.de42	static	-	F	F	sup-eth1 (R)	
	42	0005.73f6.4d3c	dynamic	90	F	F	72.0.10	
*	42	0005.73f6.7c41	dynamic	90	F	F	Eth3/11	

N7K-X-Pod##

Step 14 If any conflicts have been discovered within Cisco FabricPath, they can be displayed using the **show fabricpath conflict all** command. Run this command to verify that there are no conflicts on any switches in the lab.

N7K-X-PodY# **show fabricpath conflict all**

No Ports under Fabricpath control

No Switch id Conflicts

No transitions in progress

N7K-X-PodY#

Activity Verification

You have completed this task when you attain these results:

- You have successfully verified the Cisco FabricPath configuration and established that neighbor adjacencies have been formed.
- You have successfully verified that you can see all neighbors across the Cisco FabricPath network.
- You have successfully verified that there are no Cisco FabricPath conflicts in the network.

Lab 1-7: Validating OTV Configuration

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

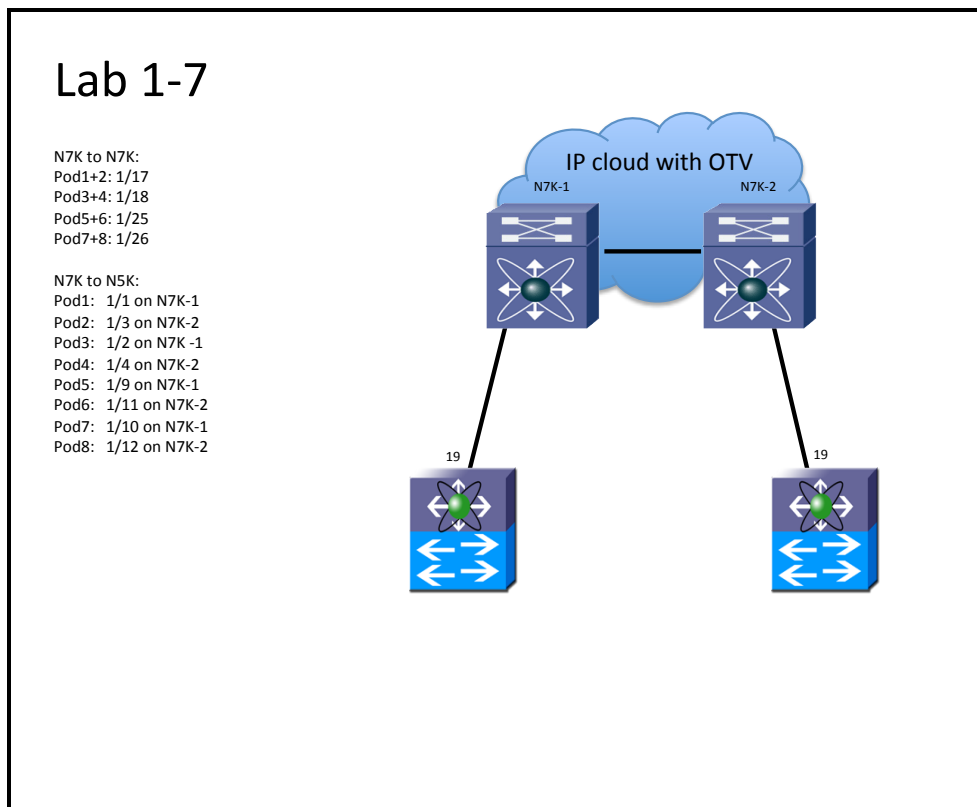
Activity Objective

In this activity, you will connect to a Cisco Nexus 7000 Series switch to validate a Cisco OTV configuration. After completing this activity, you will be able to meet this objective:

- Use the **show** commands to validate the Cisco OTV configuration

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 7000 Series VDC
- One Cisco Nexus 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show license usage</code>	Displays which licenses are available and currently being used
<code>show otv overlay 1</code>	Displays the overlay interface settings and verifies if the interface is up
<code>show vlan</code>	Displays the current VLANs
<code>show otv adjacency</code>	Displays the OTV adjacencies that have been established
<code>show otv route</code>	Displays the OTV routing table
<code>ping <x.x.x.x></code>	Tests connectivity to an IP address
<code>show otv arp-nd-cache</code>	Displays the OTV ARP cache

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Validate the OTV Configuration

In this task, you will use CLI commands to validate the Cisco OTV configuration.

Activity Procedure

Complete these steps:

Step 1 Using the credentials that are provided by your instructor, connect to the remote lab and your pod PC and open SSH sessions to your N7K VDC and your N5K.

Step 2 Log into the switches using the username **admin** and password **1234QWer**.

Step 3 On your Nexus 5000 switch load the configuration file for this lab.

```
N5K-P# rollback running-config file bootflash:DCICTv10/lab1-7
```

Note: Applying config parallelly may fail Rollback verification

Collecting Running-Config

Generating Rollback patch for switch profile

..

Collecting Running-Config

#Generating Rollback Patch

Rollback completed successfully.

```
N5K-P#
```

Step 4 On your Nexus 7000 VDC load the configuration file for this lab.

```
N7K-X-Pod## rollback running-config file bootflash:DCICTv10/lab1-7
```

Note: Applying config parallelly may fail Rollback verification

Collecting Running-Config

#Generating Rollback Patch

Rollback completed successfully.

```
N7K-X-Pod##
```

Step 5 Using the credentials provided by your instructor, connect to the remote lab and your pod and open an SSH session to all four switches.

Step 6 Log in using the username **student** and password **1234QWer**.

Note	OTV has been configured on the Nexue 7000 switches in the lab, with VLAN 10 configured as the extended VLAN across the OTV cloud.
-------------	---

Step 7 Check that the correct license is enabled for the OTV configuration using the command **show license usage**.

N7K-X-Pod## **sho 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	Yes	-	Unused	Never
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

N7K-X-Pod##

Q1) Which license does OTV require? _____

Step 8 To be able to create any OTV adjacencies, the overlay interface must be up and the site VLAN configured. Use the **show otv overlay 0** command to view the state of the overlay interface.

N7K-X-Pod## **sho otv overlay 0**

OTV Overlay Information

Site Identifier 0000.0000.0001

Overlay interface Overlay0

VPN name	: Overlay0
VPN state	: UP
Extended vlans	: 10 (Total:1)
Control group	: 239.1.1.1
Data group range(s)	: 232.0.0.0/24
Join interface(s)	: Eth1/17 (192.168.99.71)
Site vlan	: 999 (up)
AED-Capable	: Yes
Capability	: Multicast-Reachable

N7K-X-Pod##

Step 9 Identify the site VLAN from the output and run the **show vlan** command to verify that the VLAN is operational.

N7K-X-Pod## **sho vlan**

VLAN	Name	Status	Ports
1	default	active	Eth1/1, Eth1/3, Eth1/19, Eth3/1 Eth3/2, Eth3/11, Eth3/12
10	VLAN0010	active	Eth1/1, Eth1/3, Eth1/19
999	OTV-site-vlan	active	Eth1/1, Eth1/3, Eth1/19

```
VLAN Type  Vlan-mode
-----
1      enet   CE
10     enet   CE
999    enet   CE
```

```
Remote SPAN VLANs
-----
```

```
Primary  Secondary  Type          Ports
-----
```

```
N7K-X-Pod##
```

Step 10 Without an adjacency established, traffic cannot be forwarded over the OTV cloud. Verify the establishment of an adjacency between the two Cisco Nexus 7000 Series Switches using the **show otv adjacency** command.

```
N7K-X-Pod## sho otv adjacency
Overlay Adjacency database
```

```
Overlay-Interface Overlay0 :
Hostname                      System-ID      Dest Addr      Up Time      State
N7K-X-Pod#                    0026.51c8.cf42 192.168.99.72  00:07:50    UP
N7K-X-Pod##
```

Step 11 Make sure VLAN10 is extended over OTV.

```
N7K-X-Pod## sho otv vlan 10
```

```
OTV Extended VLANs and Edge Device State Information (* - AED)
```

```
VLAN    Auth. Edge Device          Vlan State      Overlay
-----
10*     N7K-X-Pod#                    active          Overlay0
```

```
N7K-X-Pod##
```

Step 12 Verify that MAC addresses are being discovered across the OTV cloud. Use the command **show otv route**.

```
N7K-X-Pod## sho otv route
```

```
OTV Unicast MAC Routing Table For Overlay0
```

```
VLAN MAC-Address      Metric  Uptime    Owner      Next-hop(s)
-----
10 0005.73f6.4d3c 42      00:07:51 overlay    N7K-X-Pod#
10 0005.73f6.4dfa 42      00:08:05 overlay    N7K-X-Pod#
10 0005.73f6.7c1a 1       00:08:04 site       Ethernet1/1
10 0005.73f6.7c41 1       00:07:50 site       Ethernet1/1
```

```
N7K-X-Pod##
```

Step 13 If you do not see any routes in the table, go to the Cisco Nexus 5000 Series switch and run the following two pings:

```
N5K-P# ping 192.168.10.5Q (Q is your PEER Pod#)
N5K-Q# ping 192.168.10.5P
```

Step 14 Redo the **show otv route** command.

Q2) Has anything changed (you should see some routes in the OTV routing table)? Why has it changed?

Step 15 Check the mac address table on the Nexus 7000 switch.

```
N7K-X-Pod## sho mac address-table
```

Legend:

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

VLAN	MAC Address	Type	age	Secure	NTFY
Ports/SWID.	SSID.LID				
G -	0026.51cc.de42	static	-	F	F sup-eth1 (R)
O 10	0005.73f6.4d3c	dynamic	0	F	F Overlay0
O 10	0005.73f6.4dfa	dynamic	0	F	F Overlay0
* 10	0005.73f6.7c1a	dynamic	600	F	F Eth1/1
* 10	0005.73f6.7c41	dynamic	0	F	F Eth1/1

```
N7K-X-Pod##
```

Step 16 The **show otv arp-nd-cache** command can show you which addresses have been seen through ARPs. Run this command to verify that addresses are being discovered through the ARP process.

```
N7K-X-Pod## sho otv arp-nd-cache
```

OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay0

VLAN	MAC Address	Layer-3 Address	Age	Expires In
10	0005.73f6.4d3c	192.168.10.5Q	00:08:43	Del Pend: 00:00:38 m

```
N7K-X-Pod##
```

Activity Verification

You have completed this task when you attain these results:

- You have examined OTV and verified that OTV adjacencies are in place.

Lab 2-1: Verifying Current VDC Settings

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

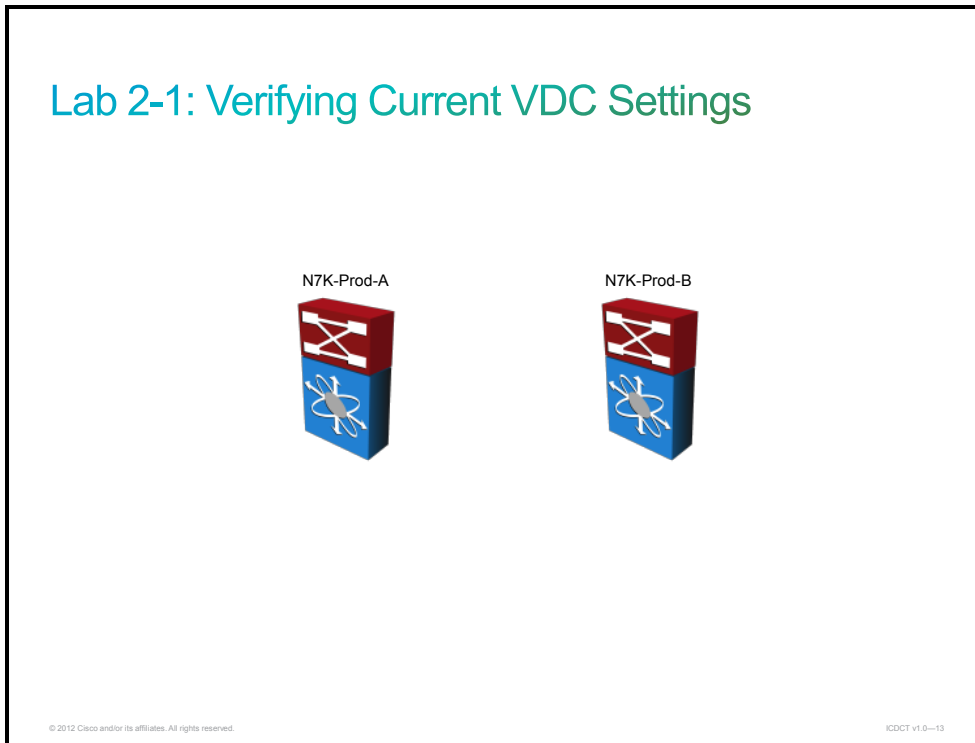
Activity Objective

In this activity, you will connect to a Cisco Nexus 7000 Series switch to verify the current VDC settings. After completing this activity, you will be able to meet this objective:

- Use the **show** commands to verify the settings that are configured for a 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:

- One Cisco Nexus 7000 Series VDC
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show vdc</code>	Displays a summary of the current VDC
<code>show vdc detail</code>	Displays detailed information of the current VDC
<code>show vdc feature-set</code>	Displays which feature sets have been enabled in the current VDC
<code>show vdc internal mac_address_table</code>	Displays the internal MAC address table of the current VDC
<code>show vdc membership</code>	Displays which interfaces are members of the current VDC

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Verify the Current VDC Settings

In this task, you will use CLI commands to verify the current VDC settings.

Activity Procedure

Complete these steps:

- Step 1** Using the credentials that are provided by your instructor, connect to the remote lab and your pod PC and open an SSH session to your N7K VDC using IP 192.168.0.20# (# is your Pod number)
- Step 2** Log in using username **admin** password **1234QWer**.
- Step 3** VDCs are created and modified in the default VDC. You are working in a nondefault VDC here in the lab. Use the **show vdc** command to identify which VDC you are working in.

```
N7K-X-Pod## sho vdc
```

vdc_id	vdc_name	state	mac	type	lc
-----	-----	-----	-----	-----	-----
2	Pod1	active	00:26:51:cc:de:42	Ethernet	m1 f1 m1x1

```
N7K-X-Pod##
```

Q1) Which VDC are you using? _____

- Step 4** VDCs are configured with a high availability policy. Use the command **show vdc detail** to identify which high availability policy your VDC is using.

```
N7K-X-Pod## sho vdc detail
```

```
vdc id: 2
vdc name: Pod1
vdc state: active
vdc mac address: 00:26:51:cc:de:42
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
vdc create time: Mon Jan 21 12:33:25 2013
vdc reload count: 1
vdc restart count: 0
vdc type: Ethernet
vdc supported linecards: m1 f1 m1x1
```

```
N7K-X-Pod##
```

Q2) Which high availability policy has been configured for the VDC?

Q3) Using the same output, what line cards are supported in your VDC?

- Step 5** Feature sets are used to enable specific features on the Cisco Nexus 7000 Series switch. These feature sets can be enabled on a per-VDC basis. Verify which feature sets you are running in your VDC using the command **show feature-set**.

Q4) Which feature sets are you running? _____

Step 6 Check what internal MAC addresses are being used in the VDC using the command **show vdc internal mac_address_table**.

```
N7K-X-Pod## sho vdc internal mac_address_table
00:26:51:cc:de:40
00:26:51:cc:de:41
00:26:51:cc:de:42
00:26:51:cc:de:43
00:26:51:cc:de:44
N7K-X-Pod##
```

Step 7 An easy way to find out which interfaces have been assigned to your VDC is through the **show vdc membership** command. Check which interfaces you have been assigned to use.

```
N7K-X-Pod## sho vdc membership

vdc_id: 2 vdc_name: Pod1 interfaces:
Ethernet1/1      Ethernet1/3      Ethernet1/5
Ethernet1/7      Ethernet1/17     Ethernet1/19
Ethernet1/21     Ethernet1/23
                Ethernet3/1      Ethernet3/2      Ethernet3/11
Ethernet3/12
```

N7K-X-Pod##

Tip If you also want to explore the default VDC you can SSH to 192.168.0.210 (N7K-1) or 192.168.0.220 (N7K-2) and use the username pod# with password pod# (# is your pod number) to get read-only access.

Activity Verification

You have completed this task when you attain these results:

- You have identified which VDC you are currently working with.
- You have successfully verified the VDC membership.
- You have successfully verified the high availability policy.
- You have successfully identified which feature sets are being used in your VDC.

Lab 2-2: Validating a Cisco Nexus 2000 Series Fabric Extender Configuration

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

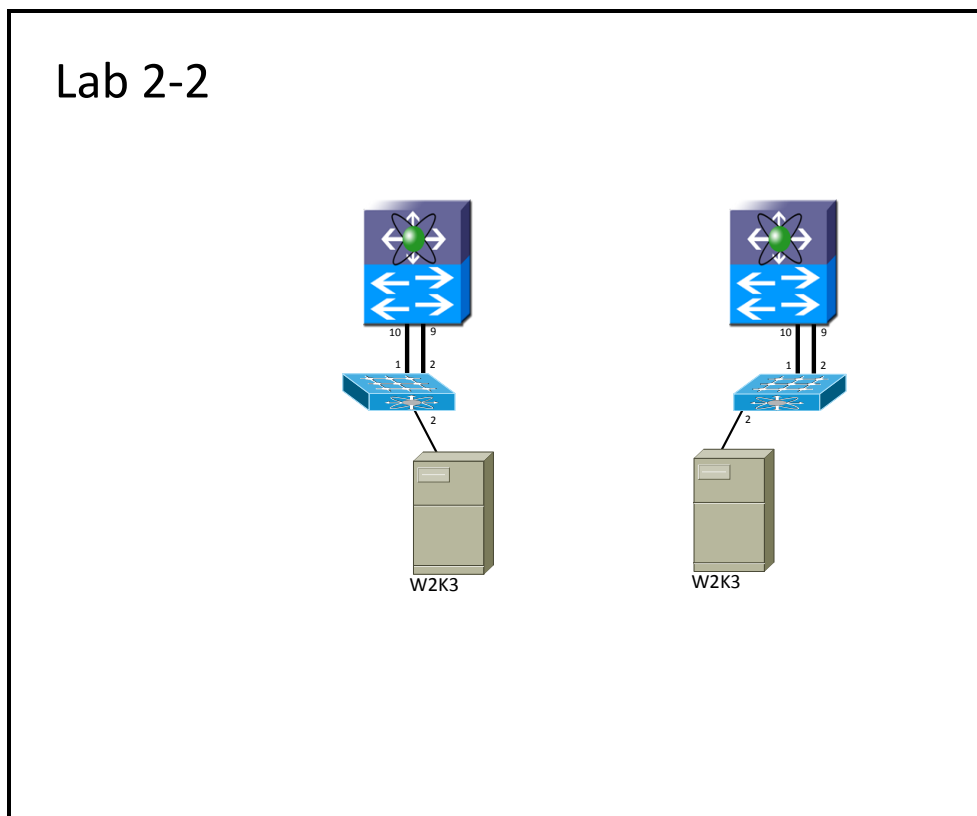
Activity Objective

In this activity, you will connect to a Cisco Nexus 5000 Series switch to validate a Cisco Nexus 2000 Series Fabric Extender configuration. After completing this activity, you will be able to meet this objective:

- Use the **show** commands to validate a Cisco Nexus 2000 Series Fabric Extender configuration

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 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show fex</code>	Displays a summary of which FEXs are online and discovered
<code>show run interface Ethernet 1/x-y</code>	Displays the running configuration for specific interfaces
<code>show fex detail</code>	Displays detailed information about discovered FEXs
<code>show running-config fex all</code>	Displays the FEX configuration in the running configuration file
<code>show interface Ethernet 1/x fex-intf</code>	Displays the FEX interfaces for a specific interface
<code>show interface brief</code>	Displays a summary of all interfaces known by the switch
<code>show module fex #</code>	Displays the FEX module details

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Validate a Cisco Nexus 2000 Fabric Extender Configuration

In this task, you will use CLI commands to validate the configuration of a Cisco Nexus 2000 Fabric Extender that is connected to a Cisco Nexus 5000 Series switch.

Activity Procedure

Complete these steps:

Step 1 Using the credentials that are provided by your instructor, connect to the remote lab and your pod and open an SSH session to your N5K. (the N7K will not be used in this lab)

Step 2 Log into the switch using the username **student** and password **1234QWer**.

Step 3 On your Nexus 5000 switch load the configuration file for this lab.

```
N5K-P# rollback running-config file bootflash:DCICTv10/lab2-2
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
..
Collecting Running-Config
#Generating Rollback Patch
```

Rollback completed successfully.

N5K-P#

Step 4 Using the credentials provided by your instructor, connect to the remote lab and your pod and open an SSH session to all four switches.

Step 5 Log in to the switches using the username **student** and password **1234QWer**.

Note The Cisco Nexus 2000 Series Fabric Extender is attached to the N5K switch via interface Ethernet 1/9 and interface Ethernet 1/10.

Step 6 Once the file has loaded, verify that the Cisco Nexus 2000 Series Fabric Extender is found using the **show fex** command. It will take a while for the FEX to come online, DO NOT wait but continue with the lab.

```
N5K-P# sho fex
FEX      FEX      FEX      FEX
Number   Description  State      Model      Serial
-----
---      -
          Discovered  N2K-C2248TP-1GE  SSI141605QQ
N5K-P#
```

```
N5K-P# sho fex
FEX      FEX      FEX      FEX
Number   Description  State      Model      Serial
-----
```

```
100          FEX0100          Connected      N2K-C2248TP-1GE      SSI141605QQ
N5K-P#
```

```
N5K-P# sho fex
```

FEX Number	FEX Description	FEX State	FEX Model	FEX Serial
100	FEX0100	Image Download	N2K-C2248TP-1GE	SSI141605QQ

```
N5K-P#
```

Q1) What is the current state of your FEX? Why? (Hint: use the **show running-config interface Ethernet 1/9-10** and **show fex** commands.)

```
_____
_____
_____
_____
```

```
N5K-P# sho running-config interface ethernet 1/9-10
```

```
!Command: show running-config interface Ethernet1/9-10
!Time: Wed Dec 26 12:39:05 2012
```

```
version 5.0(3)N2(1)
```

```
interface Ethernet1/9
  switchport mode fex-fabric
  fex associate 100
  channel-group 100
```

```
interface Ethernet1/10
  switchport mode fex-fabric
  fex associate 100
  channel-group 100
```

```
N5K-P#
```

```
N5K-P# sho run int port-channel 100
```

```
!Command: show running-config interface port-channel100
!Time: Wed Dec 26 12:40:06 2012
```

```
version 5.0(3)N2(1)
```

```
interface port-channel100
  switchport mode fex-fabric
  fex associate 100
```

```
N5K-P#
```

Step 7 Wait for the FEX to come online. A log message will be displayed when the FEX comes online.

```
2012 Dec 26 12:40:14 N5K-P %SATCTRL-FEX100-2-SATCTRL: FEX-100 Module
1: Cold boot
2012 Dec 26 12:40:27 N5K-P %PFMA-2-FEX_STATUS: Fex 100 is online
2012 Dec 26 12:40:27 N5K-P %NOHMS-2-NOHMS_ENV_FEX_ONLINE: FEX-100 On-
line
2012 Dec 26 12:40:28 N5K-P %PFMA-2-FEX_STATUS: Fex 100 is online
```

Step 8 Using the **show fex detail** command, identify the number of uplinks that are being used and which uplinks the FEX server interfaces are using.

N5K-P# **sho fex detail**

```
FEX: 100 Description: FEX0100    state: Online
  FEX version: 5.0(3)N2(1) [Switch version: 5.0(3)N2(1)]
  FEX Interim version: 5.0(3)N2(1)
  Switch Interim version: 5.0(3)N2(1)
  Extender Model: N2K-C2248TP-1GE,  Extender Serial: JAF1427AHQD
  Part No: 73-12748-05
  Card Id: 99, Mac Addr: d0:d0:fd:68:5e:02, 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: Eth1/9
  Fabric interface state:
    Po100 - Interface Up. State: Active
    Eth1/9 - Interface Up. State: Active
    Eth1/10 - Interface Up. State: Active
  Fex Port      State  Fabric Port
    Eth100/1/1  Down   Po100
    Eth100/1/2   Up    Po100
    Eth100/1/3  Down   Po100
    Eth100/1/4  Down   Po100
    Eth100/1/5  Down   Po100
```

...

Logs:

```
12/26/2012 12:31:28.915671: Module register received
12/26/2012 12:31:28.916496: Image Version Mismatch
12/26/2012 12:31:28.916781: Registration response sent
12/26/2012 12:31:28.917017: Requesting satellite to download image
12/26/2012 12:39:03.629568: Image preload successful.
12/26/2012 12:39:05.19172: Deleting route to FEX
12/26/2012 12:39:05.24189: Module disconnected
12/26/2012 12:39:05.25156: Module Offline
12/26/2012 12:39:05.94938: Deleting route to FEX
12/26/2012 12:39:05.99910: Module disconnected
12/26/2012 12:39:05.101295: Offlining Module
12/26/2012 12:40:22.953211: Module register received
12/26/2012 12:40:22.954328: Registration response sent
12/26/2012 12:40:23.151034: Module Online Sequence
12/26/2012 12:40:27.902700: Module Online
```

N5K-P#

Q2) Which command would you use to verify that the number of uplinks being used is the number that is specified in the pinning command for the FEX? _____

N5K-P# **sh run fex all**

```
!Command: show running-config fex all
!Time: Wed Dec 26 12:43:18 2012
```

```

version 5.0(3)N2(1)
feature flex

wrr-queue cos-map 0 0 1
wrr-queue cos-map 1 2 3
wrr-queue cos-map 2 4 5
wrr-queue cos-map 3 6 7
flex 100
    pinning max-links 1
    description "FEX0100"

interface port-channel100
    flex associate 100

interface Ethernet1/9
    flex associate 100

interface Ethernet1/10
    flex associate 100

N5K-P#

```

Step 9 Verify the mapping of FEX server interfaces to uplink channel using the **show interface Port-Channel 100 flex-intf**.

N5K-P# **show interface port-channel 100 flex-intf**

```

Fabric          FEX
Interface       Interfaces
-----
Po100           Eth100/1/1   Eth100/1/2   Eth100/1/3   Eth100/1/4
                Eth100/1/5   Eth100/1/6   Eth100/1/7   Eth100/1/8
                Eth100/1/9   Eth100/1/10  Eth100/1/11  Eth100/1/12
                Eth100/1/13  Eth100/1/14  Eth100/1/15  Eth100/1/16
                Eth100/1/17  Eth100/1/18  Eth100/1/19  Eth100/1/20
                Eth100/1/21  Eth100/1/22  Eth100/1/23  Eth100/1/24
                Eth100/1/25  Eth100/1/26  Eth100/1/27  Eth100/1/28
                Eth100/1/29  Eth100/1/30  Eth100/1/31  Eth100/1/32
                Eth100/1/33  Eth100/1/34  Eth100/1/35  Eth100/1/36
                Eth100/1/37  Eth100/1/38  Eth100/1/39  Eth100/1/40
                Eth100/1/41  Eth100/1/42  Eth100/1/43  Eth100/1/44
                Eth100/1/45  Eth100/1/46  Eth100/1/47  Eth100/1/48

```

N5K-P#

Step 10 Verify the Cisco Nexus 2000 Series Fabric Extender interfaces using the **show interface brief** command.

N5K-P# **sho int brief**

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch#
Eth1/1	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/2	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/3	113	eth	access	down	Administratively down	10G(D)	--
Eth1/4	114	eth	access	down	Administratively down	10G(D)	--
Eth1/5	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/6	1	eth	access	down	SFP not inserted	10G(D)	--

Interface	VLAN	Type	Mode	Status	Reason	Speed	Protocol
Eth1/7	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/8	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/9	1	eth	fabric	up	none	10G(D)	100
Eth1/10	1	eth	fabric	up	none	10G(D)	100
Eth1/11	1	eth	access	down	Administratively down	10G(D)	--
Eth1/12	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/13	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/14	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/15	1	eth	access	down	Administratively down	10G(D)	--
Eth1/16	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/17	1	eth	access	down	Administratively down	10G(D)	--
Eth1/18	1	eth	access	down	Administratively down	10G(D)	--
Eth1/19	1	eth	trunk	down	Administratively down	10G(D)	--
Eth1/20	1	eth	trunk	down	Administratively down	10G(D)	--
Eth1/21	1	eth	access	down	Administratively down	10G(D)	--
Eth1/22	1	eth	access	down	Administratively down	10G(D)	--
Eth1/23	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/24	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/25	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/26	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/27	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/28	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/29	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/30	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/31	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/32	1	eth	access	down	SFP not inserted	10G(D)	--

Port-channel Interface	VLAN	Type	Mode	Status	Reason	Speed	Protocol
Po100	1	eth	fabric	up	none	a-10G(D)	none

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	192.168.0.18	1000	1500

Ethernet Port Interface #	VLAN	Type	Mode	Status	Reason	Speed	Ch
Eth100/1/1	1	eth	access	down	Link not connected	auto(D)	--
Eth100/1/2	1	eth	access	up	none	1000(D)	--
Eth100/1/3	1	eth	access	down	Link not connected	auto(D)	--
Eth100/1/4	1	eth	access	down	Link not connected	auto(D)	--
Eth100/1/5	1	eth	access	down	Link not connected	auto(D)	--
...							
Eth100/1/48	1	eth	access	down	Link not connected	auto(D)	--

N5K-P#

Step 11 View the Cisco Nexus 2000 Series Fabric Extender modules using the **show module fex #** command. (On the N5K-P # is 151 and on the N5K-P # is 152.) You could also use the **show fex** command.

```
N5K-P# sho module fex 100
FEX Mod Ports Card Type Model Status.
---
100 1 48 Fabric Extender 48x1GE + 4x10G Module N2K-C2248TP-1GE
present

FEX Mod Sw Hw World-Wide-Name(s) (WWN)
---
```

```

100 1    5.0(3)N2(1)      3.5      --

FEX Mod  MAC-Address(es)      Serial-Num
--- ---  -
100 1    d0d0.fd68.5e00 to d0d0.fd68.5e2f  JAF1427AHQD
N5K-P#

```

Activity Verification

You have completed this task when you attain these results:

- Used the **show** commands to verify the connectivity between the Cisco Nexus 5000 Series switch and the Cisco Nexus 2000 Series Fabric Extender.
- Use the **show** commands to verify that the Cisco Nexus 5000 Series switch can see the interfaces on the Cisco Nexus 2000 Series Fabric Extender.

Lab 2-3: Validating a Cisco Nexus 1000V Series Switch Configuration

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

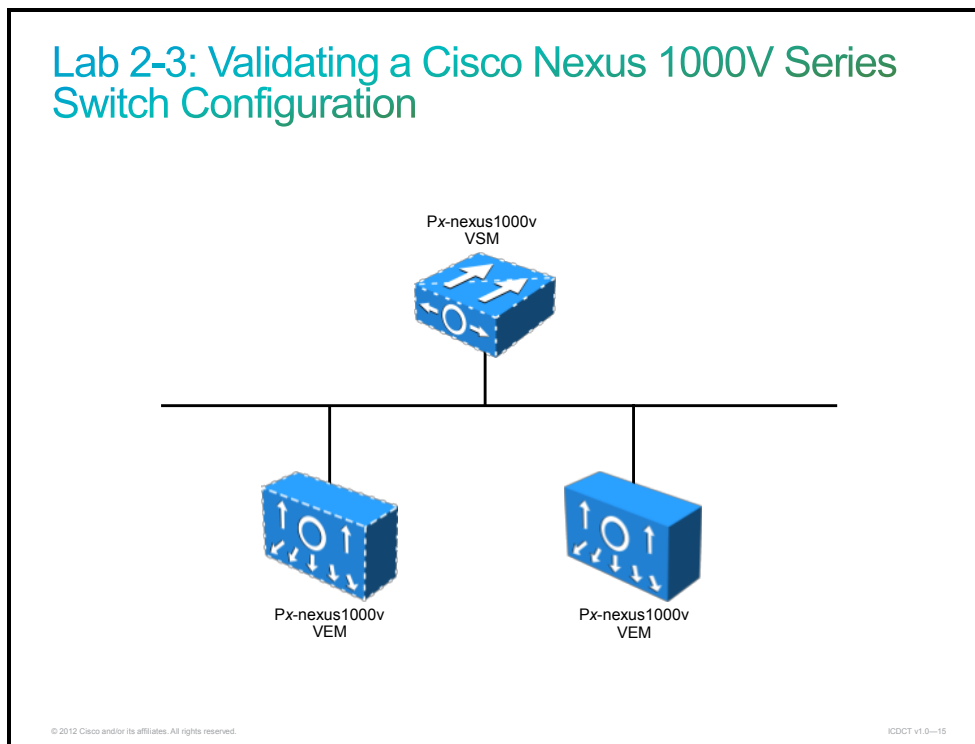
Activity Objective

In this activity, you will validate a Cisco Nexus 1000V Series switch configuration. After completing this activity, you will be able to meet this objective:

- Use the **show** commands to validate a Cisco Nexus 1000V Series switch configuration

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 1000V Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show module</code>	Displays the modules that are seen by the switch
<code>show port-profile</code>	Displays details of all the port profiles that are configured
<code>show port-profile brief</code>	Displays a summary of the port profiles that are configured
<code>show port-profile name <name></code>	Displays details of a specific port profile that is configured
<code>show port-profile usage</code>	Displays the interfaces using each port profile
<code>show running-config</code>	Displays the running configuration
<code>show svs domain</code>	Displays the SVS domain configuration
<code>show svs connection</code>	Displays the SVS connection to vCenter
<code>show interface Ethernet x/y</code>	Displays details of the physical interface
<code>show interface vethernet x</code>	Displays details of the logical interface

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Validate a Cisco Nexus 1000V Series Switch Configuration

In this task, you will use CLI commands to validate the configuration of a Cisco Nexus 1000V Series switch.

Activity Procedure

Caution The equipment used in the exercise is SHARED with all other students in the class, please DO NOT play around since that may break the lab for everybody.

Complete these steps:

Step 1 Using the credentials that are provided by your instructor, connect to the remote lab.

Step 2 Connect to your PC and log in using the username **administrator** and password **1234QWer**. Open a PuTTY connection to **192.168.0.93** (all pods!) and log in using username **admin** and password **admin**.

Step 3 The VSM has been installed in a VM, with the VEM installed on the VMware ESXi hosts. To verify that the hosts have the VEM installed, run the **show module** command.

```
N1000V# sho module
Mod  Ports  Module-Type                Model                Status
---  -
1    0      Virtual Supervisor Module  Nexus1000V          active *
2    0      Virtual Supervisor Module  Nexus1000V          ha-standby
3    248    Virtual Ethernet Module    NA                   ok
4    248    Virtual Ethernet Module    NA                   ok
```

```
Mod  Sw                Hw
---  -
1    4.2(1)SV2(1.1)    0.0
2    4.2(1)SV2(1.1)    0.0
3    4.2(1)SV2(1.1)    VMware ESXi 5.0.0 Releasebuild-914586 (3.0)
4    4.2(1)SV2(1.1)    VMware ESXi 5.0.0 Releasebuild-914586 (3.0)
```

```
Mod  MAC-Address(es)      Serial-Num
---  -
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA
4    02-00-0c-00-04-00 to 02-00-0c-00-04-80  NA
```

```
Mod  Server-IP          Server-UUID                Server-Name
---  -
1    192.168.0.93       NA                          NA
2    192.168.0.93       NA                          NA
3    192.168.0.95       4239d548-5515-d6c9-f9a8-6a678e24c9ff  NA
4    192.168.0.96       4239cb70-35f0-aaf0-1dc7-b14018cc5606  NA
```

* this terminal session
N1000V#

Q1) Which version of software are the VMware ESX hosts running? _____

Q2) Which hosts have a VEM installed? _____

Q3) Which version of software is the Cisco Nexus 1000V Series switch running?

Step 4 Port profiles are created on the Cisco Nexus 1000V Series switch and pushed down to vCenter for the VMware administrator to apply to the VMs that are created. Run the **show port-profile brief** command to find out which port profiles have been configured on your Cisco Nexus 1000V Series switch.

```
N1000V# sho port-profile brief
```

```
-----  
Port      Profile  Profile  Conf  Eval  Assigned  Child  
Profile   Type    State    Items Items  Intfs     Profs  
-----  
UPLINK    Ethernet 1         3      3      2         0  
Unused_Or_Quarantine_Uplink Ethernet 1         1      0      0         0  
Unused_Or_Quarantine_Veth Vethernet 1         1      0      0         0  
VM        Vethernet 1         3      3      1         0  
-----  
Profile   Assigned  Total  Sys   Parent  Child  UsedBy  
Type      Intfs     Prfls  Prfls Prfls   Prfls  Prfls  
-----  
Vethernet 1         2      0      2      0      1  
Ethernet  2         2      1      2      0      1  
N1000V#
```

Q4) Which port profiles have been configured? _____

Step 5 Display detailed information about the uplink and VM traffic port profiles using the **show port-profile name <name>** command.

```
N1000V# sho port-profile name UPLINK
```

```
port-profile UPLINK  
type: Ethernet  
description:  
status: enabled  
max-ports: 32  
min-ports: 1  
inherit:  
config attributes:  
  switchport mode access  
  switchport access vlan 1  
  no shutdown  
evaluated config attributes:  
  switchport mode access  
  switchport access vlan 1  
  no shutdown  
assigned interfaces:  
  Ethernet3/2  
  Ethernet4/2  
port-group: UPLINK  
system vlans: 1  
capability l3control: no  
capability iscsi-multipath: no  
capability vxlan: no  
capability l3-vservice: no  
port-profile role: none  
port-binding: static
```

```
N1000V#
```

```
N1000V# sho port-profile name VM
```

```
port-profile VM
  type: Vethernet
  description:
  status: enabled
  max-ports: 32
  min-ports: 1
  inherit:
  config attributes:
    switchport mode access
    switchport access vlan 1
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 1
    no shutdown
  assigned interfaces:
    Vethernet1
  port-group: VM
  system vlans: none
  capability l3control: no
  capability iscsi-multipath: no
  capability vxlan: no
  capability l3-vservice: no
  port-profile role: none
  port-binding: static
```

```
N1000V#
```

Q5) Which switchport mode has been configured for the uplink port profile? _____

Q6) Which switch port mode has been configured for the VM traffic port profile? _____

Q7) Which VLAN or VLANs are the VMs using? _____

Step 6 Verify which interfaces are using the port profiles using the **show port-profile usage** command.

```
N1000V# sho port-profile usage
```

```
port-profile UPLINK
  Ethernet3/2
  Ethernet4/2

port-profile Unused_Or_Quarantine_Uplink

port-profile Unused_Or_Quarantine_Veth

port-profile VM
  Vethernet1
```

```
N1000V#
```

Step 7 Gather further information about the VM interface using the command **show interface vethernet x**, where x is the virtual Ethernet port identified as using the VM traffic port profile.

```
N1000V# sho int vethernet 1
Vethernet1 is up
Port description is xp, Network Adapter 1
```

```

Hardware: Virtual, address: 0050.5682.7d5d (bia 0050.5682.7d5d)
Owner is VM "xp", adapter is Network Adapter 1
Active on module 3
VMware DVS port 224
Port-Profile is VM
Port mode is access
5 minute input rate 0 bits/second, 0 packets/second
5 minute output rate 2528 bits/second, 0 packets/second
Rx
  79 Input Packets 13 Unicast Packets
  6 Multicast Packets 113 Broadcast Packets
  11473 Bytes
Tx
  3875 Output Packets 183 Unicast Packets
  0 Multicast Packets 3765 Broadcast Packets 3835 Flood Packets
  1164540 Bytes
  0 Input Packet Drops 0 Output Packet Drops

```

N1000V#

Q8) What is the DVS port number this virtual interface is using? _____

Step 8 Using the output from the **show running-config** command, verify which VLANs are being used as the control and packet VLANs.

Q9) Which VLAN is being used as the control VLAN? _____

Q10) Which VLAN is being used as the packet VLAN? _____

Step 9 The Cisco Nexus 1000V Series switch needs to be configured with an SVS connection to the vCenter server. Use the **show svcs connection** command to verify the connectivity.

N1000V# **sho svcs connections**

```

connection vcenter:
  ip address: 192.168.0.94
  remote port: 80
  protocol: vmware-vim https
  certificate: default
  datacenter name: DCICT
  admin: nlkUser(user)
  max-ports: 8192
  DVS uuid: 26 36 02 50 36 70 78 0e-b9 ce ee 31 98 58 48 ac
  config status: Enabled
  operational status: Connected
  sync status: Complete
  version: VMware vCenter Server 5.0.0 Build-913577
  vc-uuid: 9DEC9371-5711-48EB-9E4F-E6101654D51F

```

N1000V#

Q11) What is the IP address of the vCenter server this switch is connected to? _____

Step 10 Verify that the SVS domain information has been successfully pushed to the vCenter server using the **show svcs domain** command.

N1000V# **sho svcs domain**

```

SVS domain config:
  Domain id: 1
  Control vlan: 1
  Packet vlan: 1
  L2/L3 Control mode: L2

```

```
L3 control interface: NA
Status: Config push to VC successful.
```

```
Note: Control VLAN and Packet VLAN are not used in L3 mode
N1000V#
```

Activity Verification

You have completed this task when you attain this result:

- You have verified the configuration on the Cisco Nexus 1000V Series switch.

Lab 3-1: Cisco MDS 9100 Series Multilayer Fabric Switch Initial Setup

You will complete this lab activity to demonstrate what you learned in the related module.

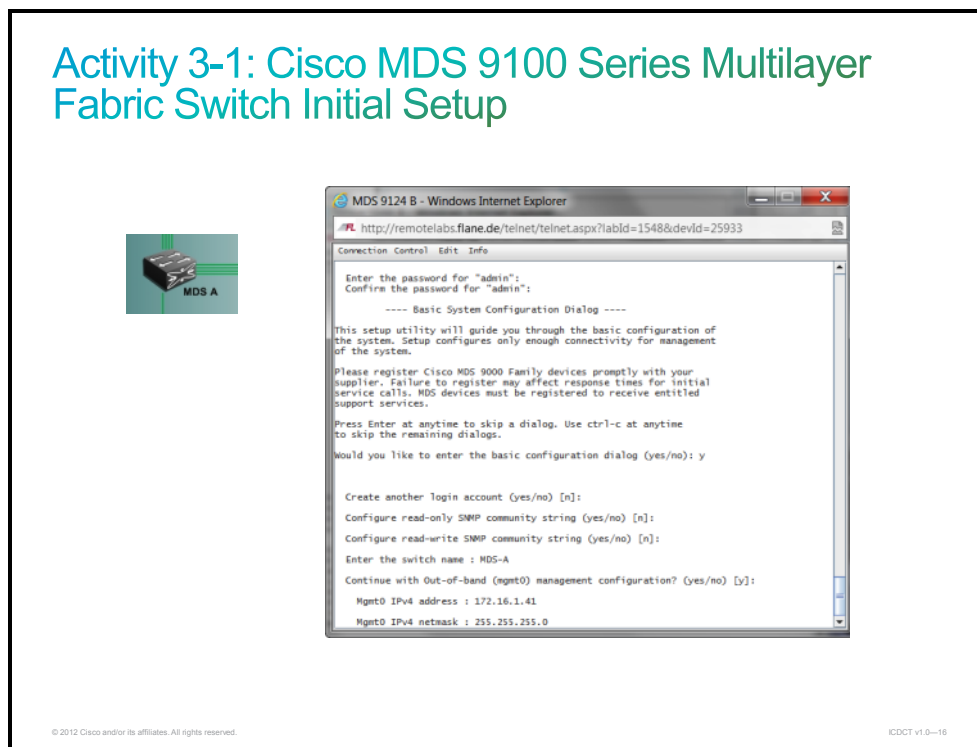
Activity Objective

In this activity, you will perform an initial configuration on a Cisco MDS 9100 Series Multilayer Fabric switch. After completing this activity, you will be able to meet these objectives:

- Describe how to use the initial setup script to perform an initial configuration on a Cisco MDS 9100 Series Multilayer Fabric switch
- Describe which parameters should be set during the initial configuration on the Cisco MDS 9100 Series Multilayer Fabric switch
- Describe which parameters have default settings in the initial setup script on the Cisco MDS 9100 Series Multilayer Fabric switch

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 MDS 9100 Series Multilayer Fabric switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>setup</code>	Runs the initial setup script
<code>show running-config</code>	Displays the current configuration on the switch

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

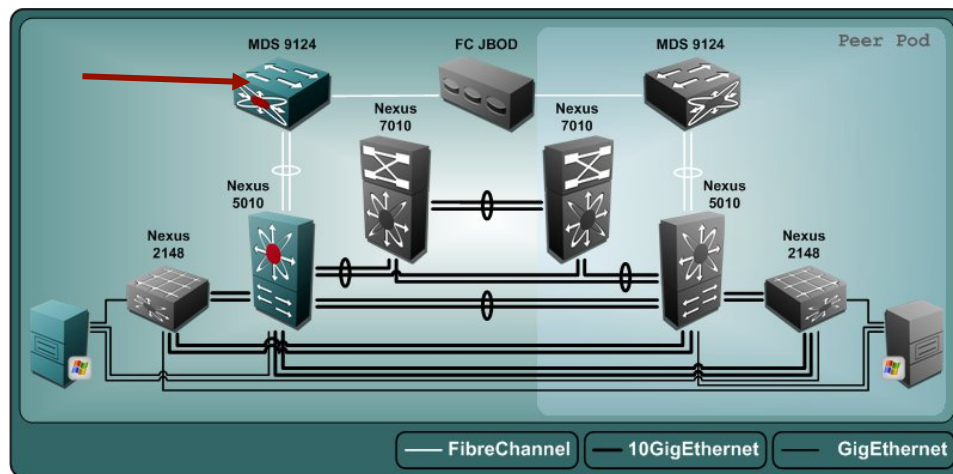
Task 1: Perform an Initial Setup on the Cisco MDS 9100 Series Multilayer Fabric Switch

During this task, you will perform an initial configuration on a Cisco MDS 9100 Series Multilayer Fabric switch.

Activity Procedure

Complete these steps:

- Step 1** Using the credentials that are provided by your instructor, connect to the remote lab and your pod.
- Step 2** Open a console connection to **Cisco MDS 9124** by clicking the MDS icon in the remote lab GUI.



- Step 3** Log in using username **admin** password **1234QWer**.
- Step 4** Perform a **write erase** and **reload** of the switch to clear any current configuration.

Note Instead of performing a write erase and reload, explain to the students the purpose of these commands and then issue the setup command.

- Step 5** Complete the initial configuration as follows:

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]: <enter>
Enter the password for "admin": 1234QWer
Confirm the password for "admin": 1234QWer
---- Basic System Configuration Dialog ----
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 MDS 9000 Family devices promptly with your supplier.
Failure to register may affect response times for initial service calls. MDS
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): yes
Create another login account (yes/no) [n]: <enter>
Configure read-only SNMP community string (yes/no) [n]: <enter>
Configure read-write SNMP community string (yes/no) [n]: <enter>
Enter the switch name : MDS-P (P is your POD#)
```

```

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
<enter>
Mgmt0 IPv4 address : 192.168.0.P9      P is your Pod#
Mgmt0 IPv4 netmask : 255.255.255.0
Configure the default gateway? (yes/no) [y]: <enter>
IPv4 address of the default gateway : 192.168.0.1
Configure advanced IP options? (yes/no) [n]: <enter>
Enable the ssh service? (yes/no) [y]: <enter>
Type of ssh key you would like to generate (dsa/rsa) [rsa]: <enter>
Number of rsa key bits <1024-2048> [1024]: <enter>
Enable the telnet service? (yes/no) [n]: y
Enable the http-server? (yes/no) [y]: n
Configure clock? (yes/no) [n]: <enter>
Configure timezone? (yes/no) [n]: <enter>
Configure summertime? (yes/no) [n]: <enter>
Configure the ntp server? (yes/no) [n]: <enter>
Configure default switchport interface state (shut/noshut) [shut]: <enter>
Configure default switchport trunk mode (on/off/auto) [on]: <enter>
Configure default switchport port mode F (yes/no) [n]: <enter>
Configure default zone policy (permit/deny) [deny]: <enter>
Enable full zoneset distribution? (yes/no) [n]: <enter>
Configure default zone mode (basic/enhanced) [basic]: <enter>

```

Step 6 You will be asked to verify if the proposed configuration is as required. Enter **no** to editing the configuration and **yes** to saving the configuration.

The following configuration will be applied:

```

password strength-check
switchname MDS-A
interface mgmt0
  ip address 192.168.0.P9 255.255.255.0
  no shutdown
ip default-gateway 192.168.0.1
ssh key rsa 1024 force
feature ssh
no feature telnet
no feature http-server
system default switchport shutdown
system default switchport trunk mode on
no system default zone default-zone permit
no system default zone distribute full
no system default zone mode enhanced

```

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

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

```

[#####] 100%
Copy complete, now saving to disk (please wait)...

```

Step 7 Once the configuration has been saved, log into the switch and verify the configuration using the **show running-config** command.

Step 8 Verify the configuration using the **show running-config** command.

Activity Verification

You have completed this task when you attain these results:

- You have successfully performed an initial configuration on the Cisco MDS 9100 Series Multilayer switch.
- You have verified the configuration using the **show running-config** command.

Lab 3-2: Validating a Cisco MDS 9100 Series Multilayer Fabric Switch License

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

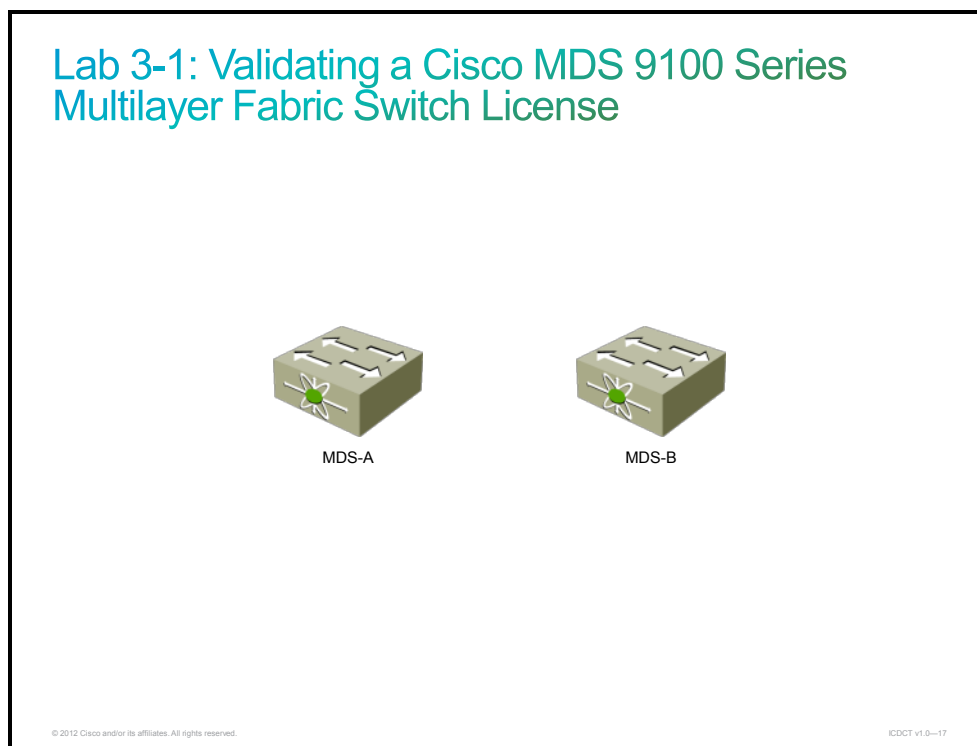
Activity Objective

In this activity, you will connect to a Cisco MDS 9100 Series Multilayer Fabric switch and validate the license and features. After completing this activity, you will be able to meet this objective:

- Validate the license on a Cisco MDS 9100 Series Multilayer Fabric switch.

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 MDS 9100 Series Multilayer Fabric switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show license</code>	Displays the license details
<code>show license usage</code>	Displays the license usage table
<code>show license default</code>	Displays which services are using default licenses
<code>show license host-id</code>	Displays the unique ID for this host for licensing

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Validate the License on the Cisco MDS 9100 Series Switch

In this task, you will use the CLI commands to validate the license on the Cisco MDS 9100 Series Multilayer Fabric switch.

Activity Procedure

Complete these steps:

- Step 1** Using the credentials that are provided by your instructor, connect to the remote lab and your pod PC.
- Step 2** Open an SSH session to your Cisco MDS 9100 Series Multilayer Fabric Switches using IP 192.168.0.19.
- Step 3** Log in using username **admin** and password **1234QWer**.
- Step 4** This command shows you what license is currently being used. To find out which licenses are available use the **show license default** command.

```
MDS-P# sho license default
Feature                                     Default License Count
-----
FM_SERVER_PKG                             -
ENTERPRISE_PKG                             -
PORT_ACTIVATION_PKG                        8
10G_PORT_ACTIVATION_PKG                    0
MDS-P#
```

- Step 5** To find out more details about the current license usage, use the command **show license usage**.

```
MDS-P# show license usage
Feature                                     Ins  Lic  Status Expiry Date Comments
                                     Count
-----
FM_SERVER_PKG                             No   -   Unused          -
ENTERPRISE_PKG                             No   -   Unused          -
PORT_ACTIVATION_PKG                        No   8   In use never    -
10G_PORT_ACTIVATION_PKG                    No   0   Unused          -
MDS-P#
```

- Step 6** Use the outputs from the previous two commands to answer the following questions:

- Q1) How many port licenses are available on the switch? _____
- Q2) How many port licenses have been activated on the switch? _____

- Step 7** Licenses are tied to the host ID of the switch. If you needed to purchase additional licenses, you would need to provide this ID. Use the **show license host-id** command to identify the switch ID.

```
MDS-A# show license host-id

License hostid: VDH=FOX1529H7N4
```

Step 8 Create a new VSAN according to the table below

Pod	VSAN
1, 3, 5	11
2, 4, 6	12

```
MDS-P# conf
Enter configuration commands, one per line. End with CNTL/Z.
MDS-P(config)# vsan database
MDS-P(config-vsan-db)# vsan 1X
MDS-P(config-vsan-db)#
```

Step 9 Place port fc1/3 in your VSAN

```
MDS-P(config-vsan-db)# vsan 1X interface fc1/3
MDS-P(config-vsan-db)#
```

Step 10 Enable Ports 1-3 on your MDS

```
MDS-P# conf
Enter configuration commands, one per line. End with CNTL/Z.
MDS-P(config)# int fc 1/1-3
MDS-P(config-if)# no shut
MDS-P(config-if)#
```

Step 11 Validate the Ports (keep in mind ports 1 and 2 connect to the Nexus 5000 which is not yet configured)

```
MDS-P(config-if)# sho int fc 1/1-3 brief
```

```
-----
Interface  Vsan    Admin  Admin  Status          SFP    Oper  Oper  Port
          Mode   Trunk                               Mode  Speed Channel
          Mode
-----
fc1/1      1       auto   on     notConnected    swl    --    --    --
fc1/2      1       auto   on     notConnected    swl    --    --    --
fc1/3      1X      auto   on     up              swl    FL    1    --
MDS-P(config-if)#
```

Step 12 Validate the JBOD disks have successfully logged into the MDS switch.

```
MDS-P(config-if)# sho flogi database
-----
INTERFACE      VSAN    FCID          PORT NAME          NODE NAME
-----
fc1/3          1X     0xaf019b     22:00:00:04:cf:2b:02:f7  20:00:00:04:cf:2b:02:f7
fc1/3          1X     0xaf01b3     22:00:00:04:cf:70:4c:15  20:00:00:04:cf:70:4c:15

Total number of flogi = 2.
```

Activity Verification

You have completed this task when you attain this result:

- You have successfully validated the license on the Cisco MDS 9100 Series Multilayer Fabric switch.

Lab 3-3: Configuring VSANs and Zoning

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

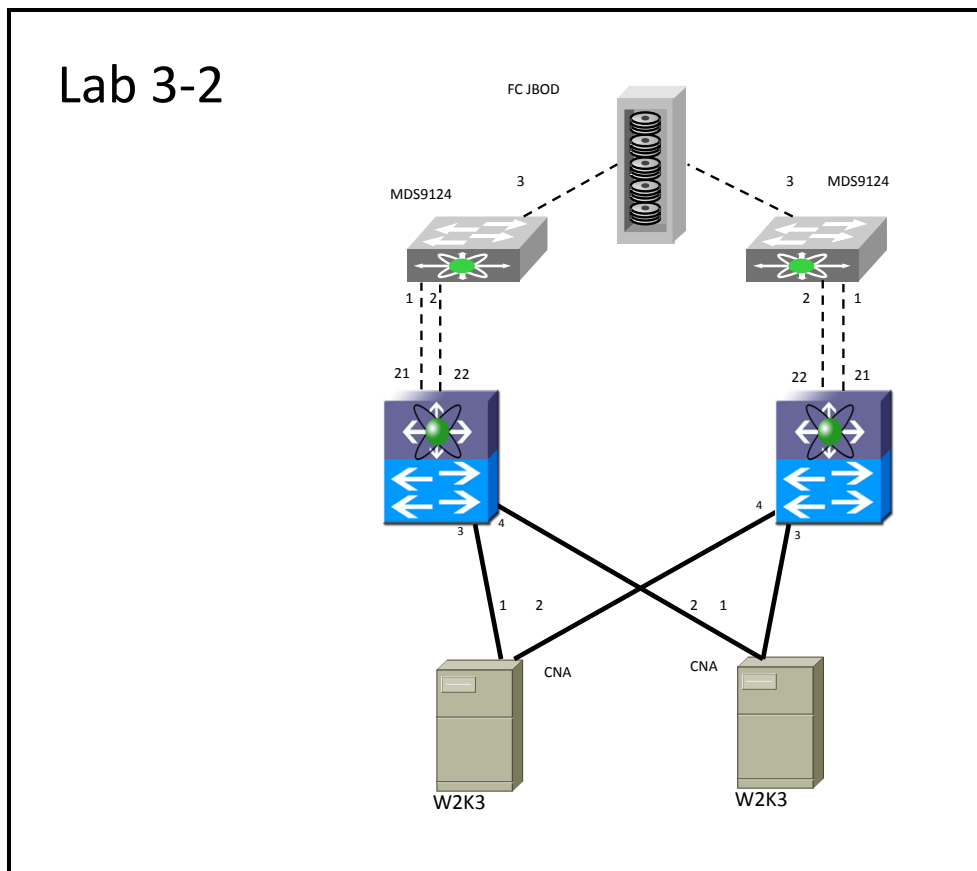
Activity Objective

In this activity, you will configure and verify VSANs in the switch fabric to logically isolate SAN traffic in SAN-A and SAN-B. You will then configure zone services, enabling initiators to have access to the proper storage targets. After completing this activity, you will be able to meet these objectives:

- Verify the existing topology and default configuration
- Configure and verify the VSANs to provide logical isolation for SAN traffic between SAN-A and SAN-B
- Optimize VSAN trunking
- Configure and verify the zone configuration to ensure that initiators can see their proper storage targets
- Use **show** commands to verify the configuration
- Save the running configurations

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 MDS 9100 Series Multilayer Fabric Switches
- Two Cisco Nexus 5000 Series Switches
- One PC with an SSH application for remote connectivity
- Console connections if available

Command List

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

Command	Description
show module	Displays the modules that are seen by the switch
show interface brief	Displays a summary of the interfaces, showing the status of those interfaces
show interface description	Displays the description that is defined for the interfaces
show ip interface brief [vrf vrf-name]	Displays the interfaces with IP addresses assigned in the specified VRF (Cisco Nexus Series switch)
show ip interface	Displays the interfaces with IP addresses assigned (Cisco MDS switch)
ping <x.x.x.x>[vrf vrf-name]	Tests connectivity to an IP address in the specified VRF (Cisco Nexus Series switch)
ping <x.x.x.x>	Tests connectivity to an IP address (Cisco MDS switch)
show feature	Displays the features that are enabled on the switch
show vsan	Displays the VSANs that are present on the switch
show vlan id n	Displays a VLAN
show vlan fcoe n	Displays the VLAN-VSAN mapping for FCoE
vsan database	Enters VSAN database configuration mode
vsan n	Creates a VSAN in the VSAN database
vsan n name VSAN-name	Assigns a name to a VSAN
show vsan membership	Displays the VSAN-to-interface associations
vsan n interface <interface slot/port>	Associates an interface to the specified VSAN
copy running-config startup-config	Saves the configuration of the switch
switchport trunk allowed vsan n	Defines the VSANs that are permitted to use a VSAN trunk
show zone policy	Displays the current zoning policy
show zone active	Displays the active zone set and zones
show zoneset active	Displays the active zone set
show device-alias database	Displays the device aliases that are known to the switch
zone name name vsan n	Defines a zone and associates the zone to a VSAN
member device-alias device-alias-name	Assigns a device to a zone based on the device alias
show zone	Displays all configured zones
zoneset name zoneset-name vsan n	Defines a zone set and associates the zone set to a VSAN
member zone-name	Assigns a zone to a zone set

zoneset activate name zoneset-name vsan n	Makes the specified zone set the active zone set for a VSAN
show zone status vsan n	Displays the zoning status for a VSAN
show zoneset	Displays all configured zone sets

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Connect to Your Switches

In this task you will connect to your assigned Nexus 5000 and MDS9124 switches.

Activity Procedure

Complete these steps:

- Step 1** Using the credentials that are provided by your instructor, connect to the remote lab and your pod PC.

Note Each Pod will configure one individual fabric.

- Step 2** Open an SSH session to your assigned switches and log in with username **admin** and password **1234QWer** using IP 192.168.0.P8 (P is your Pod #) and IP 192.168.0.P9 (P is your Pod #)

Note You can also use the console windows.

Activity Verification

You have completed this task when you attain these results:

- You have successfully identified which switch you and your pod are responsible for configuring during this lab.
- You have successfully logged into that device via SSH.

Task 2: Verify the Switch Model and configure FC ports.

In this task, you will use CLI commands to verify the model of a Cisco Nexus 5000 Series switch.

Activity Procedure

Complete these steps on the Cisco Nexus 5000 Series Switches only:

Step 1 Determine the model of the Cisco Nexus 5000 Series switch.

```
N5K-P# show module
Mod Ports  Module-Type                Model                Status
---
1      32      O2 32X10GE/Modular Universal Pla N5K-C5548UP-SUP    active *
3      0      O2 Non L3 Daughter Card        N55-DL2             ok

Mod  Sw                Hw      World-Wide-Name(s) (WWN)
---
1    5.1(3)N1(1a)      1.0     --
3    5.1(3)N1(1a)      1.0     --

Mod  MAC-Address(es)                Serial-Num
---
1    547f.ee5c.6ea8 to 547f.ee5c.6ec7  FOC154849HZ
3    0000.0000.0000 to 0000.0000.000f  FOC15475JZJ
```

Q1) What does “UP” in “N5K-C5548UP” mean? _____

Step 2 Determine if any of the physical ports have been configured as type fc.

```
N5K-P# show running-config | include slot next 1
N5K-P#
```

Q2) What is the default mode of all the physical ports on a UP platform? _____

Step 3 Enable the FCoE feature

```
N5K-P(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
Warning: Ensure class-fcoe is included in qos policy-maps of
all types
N5K-P(config)#
```

Step 4 Configure Ports 21-32 of slot 1 to be FC ports.

```
N5K-P(config)# slot 1
N5K-P(config-slot)# port 21-32 type fc
N5K-P(config-slot)#
```

Step 5 Save the configuration.

```
N5K-P(config-slot)# copy run start
[#####] 100%
N5K-P(config-slot)#
```

Step 6 Reload the Nexus 5000 switch to activate the FC ports. (this is currently a limitation in NX/OS)

```
N5K-P(config-slot)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

Step 7 Wait for the reboot to complete, the restart the session and log in with **admin** and **1234QWer**

Step 8 Verify the configuration includes the FC ports.

```
N5K-P# show running-config | include slot next 1
slot 1
port 29-32 type fc
```

Step 9 Verify that the fc ports are recognized by the switch.

```
N5K-P# sh int fc 1/21-32 brief
```

```
-----
-
Interface  Vsan    Admin  Admin  Status      SFP    Oper  Oper  Port
          Mode    Trunk                      Mode  Speed  Channel
          Mode                                (Gbps)
-----
-
fc1/21     1        auto   on     down        swl    --    --    --
fc1/22     1        auto   on     down        swl    --    --    --
fc1/23     1        auto   on     sfpAbsent   --     --    --    --
fc1/24     1        auto   on     sfpAbsent   --     --    --    --
fc1/25     1        auto   on     sfpAbsent   --     --    --    --
fc1/26     1        auto   on     sfpAbsent   --     --    --    --
fc1/27     1        auto   on     sfpAbsent   --     --    --    --
fc1/28     1        auto   on     sfpAbsent   --     --    --    --
fc1/29     1        auto   on     sfpAbsent   --     --    --    --
fc1/30     1        auto   on     sfpAbsent   --     --    --    --
fc1/31     1        auto   on     sfpAbsent   --     --    --    --
fc1/32     1        auto   on     sfpAbsent   --     --    --    --
N5K-P#
```

Step 10 On your Nexus 5000 switch load the configuration file for this lab

Note Ignore any error messages, they are just transient while the new configuration is applied

Note The Nexus 5000 does not support checkpoints and rollback with FCoE enabled, therefore we need to use the copy command.

```
N5K-P# copy bootflash:DCICTv10/lab3-3 running-config
```

```
Syntax error while parsing 'feature lldp'
```

```
2012 Dec 27 08:53:27 N5K-P %PORT-2-IF_DOWN_ERROR_DISABLED: %$VSAN 11%$
Interface vfc3 is down (Error disabled)
```

```
2012 Dec 27 08:53:28 N5K-P %PORT-2-IF_DOWN_ERROR_DISABLED: %$VSAN 11%$
Interface vfc4 is down (Error disabled)
```

```
N5K-P#
```

Activity Verification

You have completed this task when you attain these results:

- You have verified the model of the Cisco Nexus 5000 Series switch.
- You have verified the operation of the required unified ports in Fibre Channel (fc) mode.

Task 3: Verify Lab Connections

In this task, you will use CLI commands to verify the physical connections between the servers, the Cisco Nexus 5000 Series and Cisco MDS 9100 Series Multilayer Fabric Switches.

Activity Procedure

Note A configuration file that contains additional configuration relating to Fibre Channel, FCoE, and other technologies has been preloaded into the switches. The command outputs that are shown in this lab will reflect those configurations. Ask your instructor for further clarification if required.

Complete these steps on both the Cisco Nexus 5000 Series and Cisco MDS 9100 Series Multilayer Fabric Switches:

Step 1 Display the interface status for the fibre channel interfaces in use.

MDS-P# **sho int fc 1/1-3 brief**

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc1/1	1	auto	on	trunking	swl	TE	2	--
fc1/2	1	auto	on	trunking	swl	TE	2	--
fc1/3	1	auto	on	up	swl	FL	1	--

MDS-P#

N5K-P# **sho int fc 1/21-22 brief**

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc1/21	1	auto	on	trunking	swl	TE	2	--
fc1/22	1	auto	on	trunking	swl	TE	2	--

N5K-P#

Note The WWNs in the following screen shots will probably be different from your output.

Step 2 Verify the flogi database on both MDS and Nexus 5K.

N5K-P# **sho flogi database**

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
vfc3	11	0xe10000	21:00:00:c0:dd:11:2a:19	20:00:00:c0:dd:11:2a:19
vfc4	11	0xe10001	21:00:00:c0:dd:11:2d:17	20:00:00:c0:dd:11:2d:17

Total number of flogi = 2.

N5K-P#

MDS-P# **sho flogi database**

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
fc1/3	11	0xaf019b	22:00:00:04:cf:2b:02:f7	20:00:00:04:cf:2b:02:f7
fc1/3	11	0xaf01b3	22:00:00:04:cf:70:4c:15	20:00:00:04:cf:70:4c:15

Total number of flogi = 2.

MDS-P#

Step 3 Verify the FCNS database (it should be identical on both switches)

N5K-P# **sho fcns database**

VSAN 1X:

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x5e009b	NL	22:00:00:04:cf:2b:02:f7	(Seagate)	scsi-fcp:target
0x5e00b3	NL	22:00:00:04:cf:70:4c:15	(Seagate)	scsi-fcp:target
0xe10000	N	21:00:00:c0:dd:11:2a:19	(Qlogic)	scsi-fcp:init
0xe10001	N	21:00:00:c0:dd:11:2d:17	(Qlogic)	scsi-fcp:init

Total number of entries = 4

N5K-P#

MDS-P# **sho fcns database**

VSAN 1X:

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x5e009b	NL	22:00:00:04:cf:2b:02:f7	(Seagate)	scsi-fcp
0x5e00b3	NL	22:00:00:04:cf:70:4c:15	(Seagate)	scsi-fcp
0xe10000	N	21:00:00:c0:dd:11:2a:19	(Qlogic)	scsi-fcp:init
0xe10001	N	21:00:00:c0:dd:11:2d:17	(Qlogic)	scsi-fcp:init

Total number of entries = 4

MDS-P#

Activity Verification

You have completed this task when you attain these results:

- You have verified the interfaces that are in use.
- You have verified that all required interfaces are operational.
- You have verified Fibre channel FLOGI and FCNS information.

Task 4: Configure VSANs on a Cisco Nexus 5000 Series Switch

In this task, you will use the CLI commands to configure VSANs and assign Fibre Channel interfaces into the correct VSANs to complete the preloaded FCoE configuration of a Cisco Nexus 5000 Series switch.

Activity Procedure

Note A configuration file that contains configuration relating to Fibre Channel, FCoE, and related technologies has been preloaded into the switches. The command outputs that are shown here will reflect those configurations. Ask your instructor for further clarification if required.

Complete these steps on the Cisco Nexus 5000 Series Switches only:

Step 1 Determine the operating mode of the Cisco Nexus 5000 Series switch. When the NPV modes are disabled, the switch is operating in the default mode of switch mode.

```
N5K-P# show feature | include npv
fcoe-npv          1          disabled
npv               1          disabled
```

Note In switch mode, the Cisco Nexus 5000 Series switch operates as both an Ethernet switch and Fibre Channel (MDS) switch at the same time.

Step 2 Determine if the VFC interfaces are operational. They should **not** be operational at this time. The interfaces will be operational when the VSAN configuration performed in this task is completed.

```
N5K-P# sho int vfc 3-4 brief
```

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
vfc3	1X	F	on	trunking	--	TF	auto	--
vfc4	1X	F	on	trunking	--	TF	auto	--

```
N5K-P#
```

```
N5K-P# sho int vfc 3-4
```

```
vfc3 is trunking (Not all VSANs UP on the trunk)
  Bound interface is Ethernet1/3
  Hardware is Virtual Fibre Channel
  Port WWN is 20:02:00:05:73:f6:7c:3f
  Admin port mode is F, trunk mode is on
  snmp link state traps are enabled
  Port mode is TF
  Port vsan is 11
  Trunk vsans (admin allowed and active) (1,1X)
  Trunk vsans (up) (1X)
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) (1)
  1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    26 frames input, 4820 bytes
      0 discards, 0 errors
    26 frames output, 3640 bytes
      0 discards, 0 errors
  last clearing of "show interface" counters never
  Interface last changed at Thu Dec 27 08:53:31 2012
```

```
vfc4 is trunking (Not all VSANs UP on the trunk)
```

```

Bound interface is Ethernet1/4
Hardware is Virtual Fibre Channel
Port WWN is 20:03:00:05:73:f6:7c:3f
Admin port mode is F, trunk mode is on
snmp link state traps are enabled
Port mode is TF
Port vsan is 11
Trunk vsans (admin allowed and active) (1,1X)
Trunk vsans (up) (1X)
Trunk vsans (isolated) (1)
Trunk vsans (initializing) (1)
1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
26 frames input, 4820 bytes
0 discards, 0 errors
26 frames output, 3640 bytes
0 discards, 0 errors
last clearing of "show interface" counters never
Interface last changed at Thu Dec 27 08:53:30 2012

```

N5K-P#

Step 3 Determine the VSANs that are present.

```

N5K-P# sh vsan
vsan 1 information
    name:VSAN0001 state:active
    interoperability mode:default
    loadbalancing:src-id/dst-id/oxid
    operational state:up

vsan 1X information
    name:VSAN001X state:active
    interoperability mode:default
    loadbalancing:src-id/dst-id/oxid
    operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

N5K-P#

```

Step 4 Verify that the VLAN that will be used for FCoE is configured and active. Determine the appropriate VLAN for your assigned switch from the table.

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

N5K-P# **sho vlan id 101X**

```

VLAN Name                               Status    Ports
-----
1011 FCoE                               active    Eth1/3, Eth1/4, Eth1/19
                                           Eth1/20

Remote SPAN VLAN
-----
Disabled

Primary Secondary Type           Ports
-----

```

N5K-P#

Step 5 The VLAN that carries FCoE traffic must be translated to a VSAN. Verify the preconfigured VLAN to VSAN translation for the VLAN on your switch.

N5K-P# **show vlan fcoe 1011**

Original VLAN ID	Translated VSAN ID	Association State
-----	-----	-----
1011	11	Non-Operational

N5K-P# **show vlan fcoe 1012**

Original VLAN ID	Translated VSAN ID	Association State
-----	-----	-----
1012	12	Non-Operational

Note The Translated VSAN IDs that are configured on the switches are different VSANs. The association state is Non-Operational because the VSANs have not yet been created on the switches.

Step 6 Verify that the VLAN to VSAN association state is operational.

N5K-P# **sho vlan fcoe**

Original VLAN ID	Translated VSAN ID	Association State
-----	-----	-----
101X	1X	Operational

N5K-P#

Step 7 Similar to VLANs, all Fibre Channel interfaces are associated to VSAN 1 by default. Verify that all Fibre Channel (fc) interfaces are members of VSAN 1.

N5K-P# **sho vsan membership**

vsan 1 interfaces:

fc1/21	fc1/22	fc1/23	fc1/24
fc1/25	fc1/26	fc1/27	fc1/28
fc1/29	fc1/30	fc1/31	fc1/32

vsan 11 interfaces:

vfc3	vfc4
------	------

vsan 4079(evfp_isolated_vsan) interfaces:

vsan 4094(isolated_vsan) interfaces:

N5K-P#

Step 8 Verify that all VFC interfaces are operational.

N5K-P# **sho int vfc 3-4 brief**

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
-----	-----	-----	-----	-----	-----	-----	-----	-----
-								

```
vfc3      11      F      on      trunking      --      TF      auto  --
vfc4      11      F      on      trunking      --      TF      auto  --
N5K-P#
```

Step 9 Verify that the operating mode of the physical Fibre Channel (fc) interfaces of your switch that connect to the Cisco MDS 9100 Series Multilayer Fabric switch is “trunking.”

```
N5K-P# sho int fc 1/21-22 trunk vsan
fc1/21 is trunking
    Vsan 1 is up (None)
    Vsan 11 is up (None)
fc1/22 is trunking
    Vsan 1 is up (None)
    Vsan 11 is up (None)
N5K-P#
```

```
MDS-P# sho int fc1/1-2 trunk vsan
fc1/1 is trunking
    Vsan 1 is up (None)
    Vsan 11 is up (None)
fc1/2 is trunking
    Vsan 1 is up (None)
    Vsan 11 is up (None)
MDS-P#
```

Note On Cisco SAN switches, VSAN trunks allow all VSANs by default.

Step 10 Save the configuration of the switch.

```
N5K-P# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
```

Activity Verification

You have completed this task when you attain these results:

- You have successfully created the required VSAN on the Cisco Nexus 5000 Series switch.
- You have verified the FCoE VLAN to VSAN mapping on the Cisco Nexus 5000 Series switch.
- You have successfully configured the virtual Fibre Channel (fc) interfaces to be members of the FCoE VSAN.
- You have verified that the VSAN trunks between the Cisco Nexus 5000 Series switch and Cisco MDS 9100 Series Multilayer Fabric Switches are operational.

Task 6: Optimize VSAN Trunking

In this task, you will use the CLI commands to optimize VSAN trunking, minimizing the traffic that is utilizing a trunk connection.

Activity Procedure

Complete these steps on both the Cisco Nexus 5000 Series and Cisco MDS 9100 Series Multilayer Fabric Switches:

- Step 1** On each switch, only one VSAN, either VSAN 11 or VSAN 12 is in use. Configure the VSAN trunks of your switch to allow only the VSAN that is in use.

```
N5K-P# conf
Enter configuration commands, one per line. End with CNTL/Z.
N5K-P(config)# interface fc1/21-22
N5K-P(config-if)# switchport trunk allowed vsan 1X
N5K-P(config-if)# end
N5K-P#
```

```
MDS-A# conf
Enter configuration commands, one per line. End with CNTL/Z.
MDS-A(config)# interface fc1/1-2
MDS-A(config-if)# switchport trunk allowed vsan 1X
MDS-A(config-if)# end
MDS-A#
```

Note This configuration must be done on the switches at both ends of the trunk. A mismatched VSAN allowed list will cause the interface to fail.

- Step 2** Verify that the trunks between the switches remain operational.

```
N5K-P# sho int fc 1/21-22 brief
```

```
-----
Interface  Vsan    Admin  Admin  Status      SFP    Oper  Oper  Port
          Mode   Trunk  Mode                                     Mode  Speed  Channel
          Mode                                     (Gbps)
-----
fc1/21     1       auto   on     trunking    swl    TE    2     --
fc1/22     1       auto   on     trunking    swl    TE    2     --
N5K-P#
```

- Step 3** Verify the trunk configuration

```
N5K-P# sho int fc 1/21-22 trunk vsan
```

```
fc1/21 is trunking
      Vsan 1X is up (None)
fc1/22 is trunking
      Vsan 1X is up (None)
N5K-P#
```

- Step 4** For each of the interfaces, verify that only the desired list of VSANs is permitted.

```
N5K-P# sho int fc 1/21
fc1/21 is trunking
  Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
  Port WWN is 20:15:00:05:73:f6:7c:00
  Peer port WWN is 20:01:00:0d:ec:3e:c4:c0
  Admin port mode is auto, trunk mode is on
  snmp link state traps are enabled
  Port mode is TE
  Port vsan is 1
```

```

Speed is 2 Gbps
Transmit B2B Credit is 16
Receive B2B Credit is 16
Receive data field Size is 2112
Beacon is turned off
Trunk vsans (admin allowed and active) (11)
Trunk vsans (up) (11)
Trunk vsans (isolated) ()
Trunk vsans (initializing) ()
1 minute input rate 128 bits/sec, 16 bytes/sec, 0 frames/sec
1 minute output rate 40 bits/sec, 5 bytes/sec, 0 frames/sec
-- output omitted -

```

Step 5 Save the configuration of all switches.

```

N5K-P# copy running-config startup-config
[#####] 100%
N5K-P#

```

Activity Verification

You have completed this task when you attain these results:

- You have optimized the VSAN trunks between the Cisco Nexus 5000 Series and Cisco MDS 9100 Series Multilayer Fabric Switches to allow only the required VSANs.

Task 7: Verify the Default Zoning

In this task, you will use CLI commands to verify the default zoning configuration of the switches.

Activity Procedure

Complete these steps on both the Cisco Nexus 5000 Series and Cisco MDS 9100 Series Multilayer Fabric Switches:

Note	Zone sets and zones are used to ensure that a server has access to the correct disks, similar to ACLs.
-------------	--

Step 1 Verify the default zoning policy for each VSAN of your assigned switch.

```
N5K-P# show zone policy
Vsan: 1
  Default-zone: deny
  Distribute: active only
  Broadcast: disable
  Merge control: allow
  Generic Service: read-write
```

```
Vsan: 1X
  Default-zone: deny
  Distribute: active only
  Broadcast: disable
  Merge control: allow
  Generic Service: read-write
```

Q1) What is the default zone policy for each VSAN? _____

Step 2 Verify if there are any zones present on any of the switches.

```
N5K-P# show zone active
Zone not present
```

Note	Zones contain the devices that are permitted to communicate.
-------------	--

Step 3 Verify if there is an active zone set present on any of the switches.

```
N5K-P# show zoneset active
Zoneset not present
```

Note	A zone set contains one or more zones. There may be multiple zone sets present on a switch, but only one zone set is active.
-------------	--

Activity Verification

You have completed this task when you attain these results:

- You have verified that the default zone policy is deny.
- You have verified that zoning is not present on the switches by default.

Task 8: Configure Zoning

In this task, you will use CLI commands to configure and verify the zone set and active zone set of the fabric on the Cisco MDS 9100 Series Multilayer Fabric switch.

Activity Procedure

Complete these steps on the Cisco MDS 9100 Series Multilayer Fabric Switches only, unless otherwise noted:

Note Configuring zoning requires the administrator to have a complete list of all devices in the SAN. The common practice is to configure zones based on the device WWN or device aliases based on the WWNs. (these are not covered in this class and lab)

Step 1 Verify the FCNS database that has been distributed on **all** of your switches. The database will be different on each Fabric. Note we have 4 devices, two targets (disks) and two init(iators) (servers)

MDS-P# **sho fcns database**

VSAN 11:

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x5e009b	NL	22:00:00:04:cf:2b:02:f7	(Seagate)	scsi-fcp
0x5e00b3	NL	22:00:00:04:cf:70:4c:15	(Seagate)	scsi-fcp
0xe10000	N	21:00:00:c0:dd:11:2a:19	(Qlogic)	scsi-fcp:init
0xe10001	N	21:00:00:c0:dd:11:2d:17	(Qlogic)	scsi-fcp:init

Total number of entries = 4

MDS-P#

N5K-P# **sho fcns database**

VSAN 11:

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x5e009b	NL	22:00:00:04:cf:2b:02:f7	(Seagate)	scsi-fcp:target
0x5e00b3	NL	22:00:00:04:cf:70:4c:15	(Seagate)	scsi-fcp:target
0xe10000	N	21:00:00:c0:dd:11:2a:19	(Qlogic)	scsi-fcp:init
0xe10001	N	21:00:00:c0:dd:11:2d:17	(Qlogic)	scsi-fcp:init

Total number of entries = 4

N5K-P#

Note Devices that are permitted to communicate, for example a server and its assigned storage devices, are configured in the same zone.

Step 2 Configure a **unique** zone for each server to allow it to communicate with its storage device. Create a zone for the LOWER target WWPN and the LOWER initiator PWWN and ANOTHER zone for the HIGHER target WWPN and the HIGHER initiator PPWN. (copy&paste is REALLY helpful here ☺)

Note Zoning can be configured on any of the switches. For simplicity and to minimize errors, it is typically configured on one switch per fabric.

```

N5K-P# conf
Enter configuration commands, one per line. End with CNTL/Z.
N5K-P(config)# zone name LOWER vsan 1X
N5K-P(config-zone)# member pwnn 22:00:00:04:cf:2b:02:f7
N5K-P(config-zone)# member pwnn 21:00:00:c0:dd:11:2a:19
N5K-P(config-zone)# exit
N5K-P(config)# zone name HIGHER vsan 1X
N5K-P(config-zone)# member pwnn 22:00:00:04:cf:70:4c:15
N5K-P(config-zone)# member pwnn 21:00:00:c0:dd:11:2d:17
N5K-P(config-zone)# exit
N5K-P(config)#

```

Step 3 Verify that the zones have been created and the proper devices are assigned to each zone.

```

N5K-P(config)# sho zone
zone name LOWER vsan 11
  pwnn 22:00:00:04:cf:2b:02:f7
  pwnn 21:00:00:c0:dd:11:2a:19

zone name HIGHER vsan 11
  pwnn 22:00:00:04:cf:70:4c:15
  pwnn 21:00:00:c0:dd:11:2d:17
N5K-P(config)#

```

Note Zones are grouped in a zone set.

Step 4 Add all zones that were configured in the previous step to a zone set. The zone set is defined for a VSAN.

```

N5K-P(config)# zoneset name DCICT vsan 1X
N5K-P(config-zoneset)# member LOWER
N5K-P(config-zoneset)# member HIGHER
N5K-P(config-zoneset)# exit
N5K-P(config)#

```

Note A zone set contains one or more zones. There may be multiple zone sets present on a switch, but only one zone set is active. The active zone set is automatically distributed between devices within the same fabric.

Step 5 Activate the zone set in your VSAN, enabling it to be distributed automatically to the other switches in the same fabric.

```

N5K-P(config)# zoneset activate name DCICT vsan 1X
Zoneset activation initiated. check zone status
N5K-P(config)#

```

Step 6 Verify the status of the zoning for your VSAN.

```

N5K-P(config)# sho zone status vsan 1X
VSAN: 1X default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
Default zone:
  qos: none broadcast: disabled ronly: unsupported
Full Zoning Database :
  DB size: 200 bytes
  Zonesets:1 Zones:2 Aliases: 0
Active Zoning Database :
  DB size: 104 bytes
  Name: DCICT Zonesets:1 Zones:2
Status: Activation completed at 09:42:27 UTC Dec 27 2012

N5K-P(config)#

```

Step 7 Save the configuration Nexus 5000 switch.

```
N5K-P# copy running-config startup-config
[#####] 100%
N5K-P#
```

Step 8 Verify that the active zone set is present on the MDS switch.

Note	The zoning will be different on Fabric-A and Fabric-B.
-------------	--

```
MDS-P# sho zone status vsan 1X
VSAN: 1X default-zone: deny distribute: active only Interop: default
      mode: basic merge-control: allow
      session: none
      hard-zoning: enabled broadcast: unsupported
Default zone:
      qos: none broadcast: unsupported ronly: disabled
Full Zoning Database :
      DB size: 4 bytes
      Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
      DB size: 104 bytes
      Name: DCICT Zonesets:1 Zones:2
Status: Activation completed at 15:51:19 UTC Jan 22 2013

MDS-P#
```

```
MDS-P# show zoneset active vsan 1X
zoneset name DCICT vsan 1X
  zone name LOWER vsan 1X
    * fcid 0x5e009b [pwwn 22:00:00:04:cf:2b:02:f7]
    * fcid 0xe10000 [pwwn 21:00:00:c0:dd:11:2a:19]
  zone name HIGHER vsan 1X
    * fcid 0x5e00b3 [pwwn 22:00:00:04:cf:70:4c:15]
    * fcid 0xe10001 [pwwn 21:00:00:c0:dd:11:2d:17]

MDS-P#
```

Note	Devices seen as active in the fabric are indicated by an * (asterisk) beside the device name.
-------------	---

Activity Verification

You have completed this task when you attain these results:

- You have verified that the device-alias database is present on the switches.
- You have configured a zone for each server and its storage devices.
- You have configured a zone set that contains all configured zones.
- You have verified that the active zone set has been distributed across the fabric and is visible on the other switches.

Lab 3-4: Validating FLOGI and FCNS

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

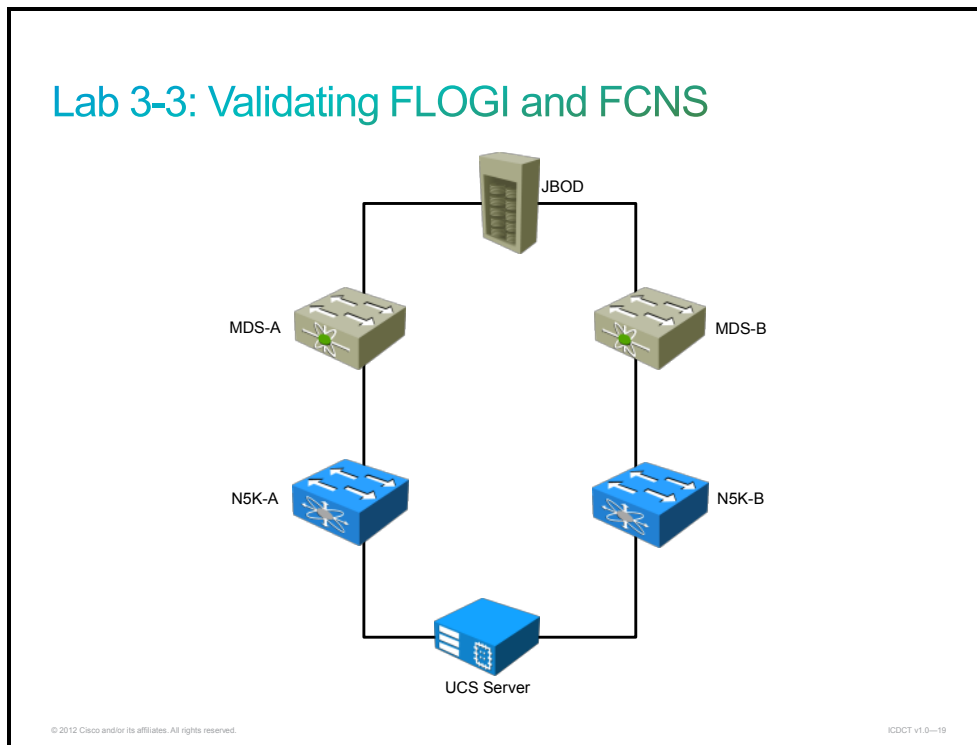
Activity Objective

In this activity, you will connect to a Cisco MDS 9100 Series switch and verify that initiators and targets have successfully logged into the fabric and that the devices have registered with the fabric. After completing this activity, you will be able to meet these objectives:

- Verify that initiators and targets have been able to successfully log into the fabric
- Verify FCNS to ensure that devices have registered with the 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:

- One Cisco MDS 9100 Series Multilayer Fabric switch
- One Cisco Nexus 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
show flogi database	Verifies which devices have logged into the switch
show fcns database	Verifies which devices have registered in the fabric

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Verify the FLOGI and FCNS Database

In this task, you will use the CLI commands to verify that initiators and targets have been able to successfully log in and register in the fabric.

Activity Procedure

Complete these steps:

- Step 1** Using the credentials that are provided by your instructor, connect to the remote lab and your pod PC and open SSH sessions to both your Cisco MDS 9100 Series Multilayer Fabric Switches and your N5K using 192.168.0.P8 and 192.168.0.P9
- Step 2** Log in using username **student** and password **1234QWer**.
- Step 3** The first step in verifying successful login to the fabric by devices is to run the **show flogi database** command. On the Cisco MDS 9100 Series switch, use this command to verify that devices have successfully logged into the fabric.

```
MDS-P# sho flogi database
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
fc1/3	1X	0x5e009b	22:00:00:04:cf:2b:02:f7	20:00:00:04:cf:2b:02:f7
fc1/3	1X	0x5e00b3	22:00:00:04:cf:70:4c:15	20:00:00:04:cf:70:4c:15

```
Total number of flogi = 2.
```

```
MDS-P#
```

Note Your output may be slightly different depending on which switch you perform the command from.

- Step 4** The device that is connected to the Cisco MDS 9100 Series Multilayer Fabric switch is the JBOD.
- Step 5** Verify that the servers have been able to successfully log in on the Cisco Nexus 5000 Series switch.

```
N5K-P# sho flogi database
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
vfc3	1X	0xe10000	21:00:00:c0:dd:11:2a:19	20:00:00:c0:dd:11:2a:19
vfc4	1X	0xe10001	21:00:00:c0:dd:11:2d:17	20:00:00:c0:dd:11:2d:17

```
Total number of flogi = 2.
```

```
N5K-P#
```

Note Your output may be slightly different depending on which switch you perform the command from.

- Step 6** The next step in verification is to confirm that all the devices have registered in the fabric. The output from the **show fcns database** command should be the same on all switches.
- Step 7** On the Cisco MDS 9100 Series Multilayer Fabric switch and Cisco Nexus 5000 Series switch, verify successful registration in the fabric for all devices.

```
MDS-P# sho fcns database
```

VSAN 1X:

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x5e009b	NL	22:00:00:04:cf:2b:02:f7	(Seagate)	scsi-fcp
0x5e00b3	NL	22:00:00:04:cf:70:4c:15	(Seagate)	scsi-fcp
0xe10000	N	21:00:00:c0:dd:11:2a:19	(Qlogic)	scsi-fcp:init
0xe10001	N	21:00:00:c0:dd:11:2d:17	(Qlogic)	scsi-fcp:init

Total number of entries = 4

MDS-P#

N5K-P# sho fcns database

VSAN 1X:

FCID	TYPE	PWWN	(VENDOR)	FC4-TYPE:FEATURE
0x5e009b	NL	22:00:00:04:cf:2b:02:f7	(Seagate)	scsi-fcp:target
0x5e00b3	NL	22:00:00:04:cf:70:4c:15	(Seagate)	scsi-fcp:target
0xe10000	N	21:00:00:c0:dd:11:2a:19	(Qlogic)	scsi-fcp:init
0xe10001	N	21:00:00:c0:dd:11:2d:17	(Qlogic)	scsi-fcp:init

Total number of entries = 4

N5K-P#

Note	Your output may be slightly different depending on which switch you perform the command from.
-------------	---

Q1) Do you see any differences? _____

Step 8 View the details of a target entry in the FCNS database.

N5K-P# **sho fcns database fcid 0x5e009b detail vsan 1X**

```
-----
VSAN:11      FCID:0x5e009b
-----
port-wwn (vendor)      :22:00:00:04:cf:2b:02:f7 (Seagate)
node-wwn               :20:00:00:04:cf:2b:02:f7
class                  :3
node-ip-addr           :0.0.0.0
ipa                    :ff ff ff ff ff ff ff ff
fc4-types:fc4_features :scsi-fcp:target
symbolic-port-name     :
symbolic-node-name     :
port-type              :NL
port-ip-addr           :0.0.0.0
fabric-port-wwn        :20:03:00:0d:ec:3e:c4:c0
```

```

hard-addr                :0x000000
permanent-port-wwn (vendor) :00:00:00:00:00:00:00:00
Connected Interface       :fc1/3
Switch Name (IP address)  :MDS-P (192.168.0.19)

```

```

Total number of entries = 1
N5K-P#

```

Step 9 View the details of an initiator entry in the FCNS database.

```
N5K-P# sho fcns database fcid 0xe10000 detail vsan 11
```

```

-----
VSAN:11      FCID:0xe10000
-----
port-wwn (vendor)        :21:00:00:c0:dd:11:2a:19 (Qlogic)
node-wwn                  :20:00:00:c0:dd:11:2a:19
class                     :3
node-ip-addr              :0.0.0.0
ipa                       :ff ff ff ff ff ff ff ff
fc4-types:fc4_features    :scsi-fcp:init
symbolic-port-name        :
symbolic-node-name        :QLE8152 FW:v5.01.03 DVR:v9.1.9.15
port-type                 :N
port-ip-addr              :0.0.0.0
fabric-port-wwn           :20:02:00:05:73:f6:7c:3f
hard-addr                 :0x000000
permanent-port-wwn (vendor) :21:00:00:c0:dd:11:2a:19 (Qlogic)
Connected Interface       :vfc3
Switch Name (IP address)  :N5K-P (192.168.0.18)

```

```

Total number of entries = 1
N5K-P#

```

Activity Verification

You have completed this task when you attain these results:

- You have successfully verified that devices have been able to log in and register in the fabric.
- You have displayed the databases that contain the login and fabric information.

Lab 3-5: Viewing the tech-support Command Output

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

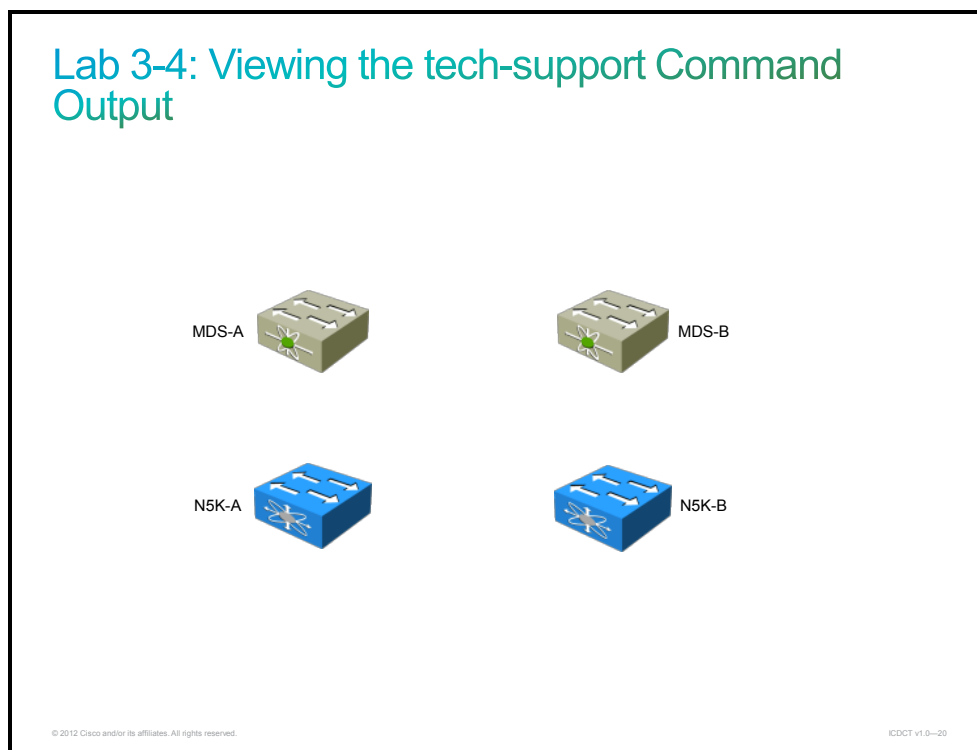
Activity Objective

In this activity, you will connect to a Cisco MDS 9100 Series Multilayer Fabric switch and view the **tech-support** command outputs. After completing this activity, you will be able to meet this objective:

- View the **tech-support** command outputs on the Cisco MDS 9100 Series switch

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 MDS 9100 Series Multilayer Fabric switch
- One Cisco Nexus 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show tech-support</code>	Displays the content of the tech-support output
<code>show tech-support brief</code>	Displays the switch summary
<code>show tech-support bootvar</code>	Gathers detailed information for boot variables troubleshooting
<code>show tech-support details</code>	Gathers detailed information for troubleshooting
<code>show tech-support device-alias</code>	Shows device-alias technical support information
<code>show tech-support license</code>	Displays license information

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: View the tech-support Command Output

In this task, you will use the CLI commands to view the **tech-support** command outputs on the Cisco MDS 9100 Series Multilayer Fabric Switch and the Cisco Nexus 5000 Series switch.

Activity Procedure

Complete these steps:

- Step 1** Using the credentials that are provided by your instructor, connect to the remote lab and your pod and open SSH sessions to your N5K switch and your Cisco MDS 9100 Series Multilayer Fabric Switch using IP 192.168.0.P8 and 192.168.0.P9.
- Step 2** Log in using username **admin** and password **1234QWer**.

Note The **show tech-support** command has a large amount of data to display because it covers all aspects of the switch that are needed during troubleshooting. Rather than display the output on the console, it is better to send the output to a file, which can then be copied off the switch for offline analysis.

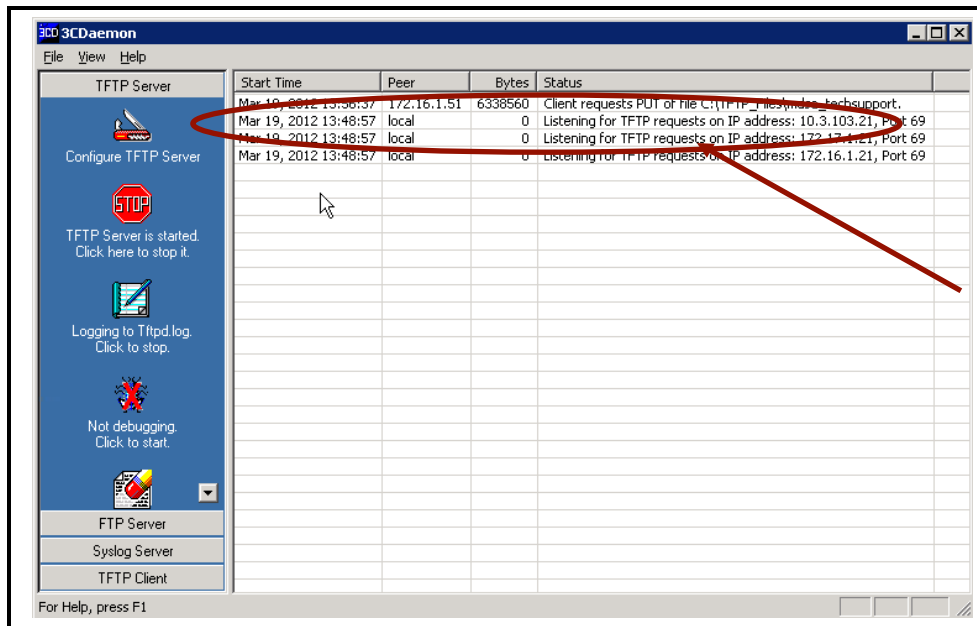
- Step 3** On your PC, start the 3CDaemon TFTP server and ensure it is running before performing Step 4.
- Step 4** Run the command **show tech-support > tftp://192.168.0.P1/mds_techsupport** (P is your Pod#)

```
MDS-P# show tech-support > tftp://192.168.0.P1/mdsa_techsupport
```

```
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
-
TFTP put operation was successful
```

Note The command may take a few minutes to complete.

- Step 5** This command will send the output to a file on the TFTP server. To verify that it is copying to the TFTP server, look at the TFTP server details on the Windows PC.



Step 6 Rather than perform a complete output of the **show tech-support** command, it is possible to filter it for specific areas that need further analysis.

Step 7 The **show tech-support brief** command displays a summary of the tech support details. Run this command on the Cisco MDS 9100 Series Multilayer Fabric switch.

```
MDS-P# sho tech-support brief
Switch Name       : MDS-P
Switch Type      :
Kickstart Image   : 5.0(4b) bootflash:/m9100-s2ek9-kickstart-mz.5.0.4b.bin
System Image      : 5.0(4b) bootflash:/m9100-s2ek9-mz.5.0.4b.bin
IP Address/Mask   : 192.168.0.19/24
No of VSANs      : 2
Configured VSANs : 1,11
```

```
VSAN    1:   name:VSAN0001, state:active, interop mode:default
          domain id:0xaf(175), WWN:20:01:00:0d:ec:3e:c4:c1 [Principal]
          active-zone:<NONE>, default-zone:deny
```

```
VSAN   11:   name:VSAN0011, state:active, interop mode:default
          domain id:0x5e(94), WWN:20:0b:00:0d:ec:3e:c4:c1
          active-zone:size:, default-zone:deny
```

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc1/1	1	auto	on	trunking	sw1	TE	2	--
fc1/2	1	auto	on	trunking	sw1	TE	2	--
fc1/3	11	auto	on	up	sw1	FL	1	--
fc1/4	1	auto	on	sfpAbsent	--	--	--	--
fc1/5	1	auto	on	sfpAbsent	--	--	--	--
fc1/6	1	auto	on	sfpAbsent	--	--	--	--
fc1/7	1	auto	on	sfpAbsent	--	--	--	--
fc1/8	1	auto	on	sfpAbsent	--	--	--	--
fc1/9	1	auto	on	sfpAbsent	--	--	--	--
fc1/10	1	auto	on	sfpAbsent	--	--	--	--
fc1/11	1	auto	on	sfpAbsent	--	--	--	--
fc1/12	1	auto	on	sfpAbsent	--	--	--	--
fc1/13	1	auto	on	sfpAbsent	--	--	--	--
fc1/14	1	auto	on	sfpAbsent	--	--	--	--
fc1/15	1	auto	on	sfpAbsent	--	--	--	--

fc1/16	1	auto	on	sfpAbsent	--	--	--
fc1/17	1	auto	on	sfpAbsent	--	--	--
fc1/18	1	auto	on	sfpAbsent	--	--	--
fc1/19	1	auto	on	sfpAbsent	--	--	--
fc1/20	1	auto	on	sfpAbsent	--	--	--
fc1/21	1	auto	on	sfpAbsent	--	--	--
fc1/22	1	auto	on	sfpAbsent	--	--	--
fc1/23	1	auto	on	sfpAbsent	--	--	--
fc1/24	1	auto	on	sfpAbsent	--	--	--

Interface	Status	Speed (Gbps)
sup-fc0	up	1

Interface	Status	IP Address	Speed	MTU
mgmt0	up	192.168.0.19/24	100 Mbps	1500

MDS-P#

Q1) How many VSANs have been configured on the switch? _____

Q2) What is the operational speed of the Fibre Channel interfaces? _____

Q3) Which software image is being used? _____

Q4) What is the default zone policy for each VSAN? _____

Step 8 The **show tech-support device-alias** can be used when troubleshooting different issues in the fabric. Run the command **show tech-support ?** on the Cisco MDS 9100 Series switch.

```
MDS-P# sho tech-support ?
<CR>
> Redirect it to a file
>> Redirect it to a file in append mode
aaa Display aaa information
acltkcam-soc Show information for acltkcam_soc technical support
assoc_mgr Gather detailed information for assoc_mgr troubleshooting
bootvar Gather detailed information for bootvar troubleshooting
brief Display the switch summary
callhome Callhome troubleshooting information
cdp Gather information for CDP trouble shooting
cert-enroll Display certificates information
cfs Gather detailed information for cfs troubleshooting
cli Gather information for parser troubleshooting
clis Gather information for CLI Server troubleshooting
commands Show commands executed as part of show tech-support commands
details Gather detailed information for troubleshooting
device-alias Show device-alias technical support information
dhcp Gather detailed information for dhcp troubleshooting
eem Show EEM tech-support information
epp Gather detailed information for EPP troubleshooting
ethport Gather detailed information for ETHPORT troubleshooting
fc2 Show information for fc2 technical support
fcdomain Gather detailed information for fcdomain troubleshooting
fcns Show information for fcns technical support
fcs Gather detailed information for fcs troubleshooting
```

```

flogi          Gather detailed information for flogi troubleshooting
fspf           Show information for fspf technical support
ha             Gather detailed information for HA troubleshooting
im             Gather detailed information for IM troubleshooting
include-time   Gather tech-support and capture time taken to execute each
               command
internal       Gather internal info for troubleshooting
l2fm           L2fm debug info
license        Display licensing information
logging        Show information on logging for technical support staff
module         Gather info related to a module
ntp            Gather information for NTP trouble shooting
port           Gather detailed information for port manager troubleshooting
port-channel   Gather detailed information for port channel troubleshooting
qos            Show information for QoS technical support
radius         Display radius information
rlir           Show information for rlir technical support
rscn           Show information for rscn technical support
security       Show tech support information for security
snmp           Gather info related to snmp
span           Gather detailed information for span troubleshooting
sysmgr        Gather detailed information for sysmgr troubleshooting
time-optimized Gather tech-support faster, requires more memory & disk
               space
vrrp           Show information for vrrp technical support
vsan           Gather detailed information for vsan troubleshooting
zbm            Show information for zbm technical support
zone           Show information for zoneserver technical support
|              Pipe command output to filter

```

MDS-P#

Step 9 The command **show tech-support license** is useful for troubleshooting licensing issues. Run the **show tech-support license** command on the Cisco MDS 9100 Series Multilayer Fabric switch.

```

MDS-P# sho tech-support license
`show license host-id`
License hostid: VDH=FOX10440AXS
`show license`
`show license usage`

```

Feature	Ins	Lic Count	Status	Expiry Date	Comments
FM_SERVER_PKG	No	-	Unused		-
ENTERPRISE_PKG	No	-	Unused		-
PORT_ACTIVATION_PKG	No	8	In use never		-
10G_PORT_ACTIVATION_PKG	No	0	Unused		-

```

-----
--
`show running-config license all`

!Command: show running-config license all
!Time: Tue Jan 22 16:15:29 2013

version 5.0(4b)
license grace-period

`show system internal license event-history`
1) Event:E_MTS_RX, length:60, at 461519 usecs after Tue Jan 22 16:15:29 2013
   [NOT] Opc:MTS_OPC_VSH_ACFG_GEN(7663), Id:0X00068509, Ret:SUCCESS
   Src:0x00000101/3305, Dst:0x00000101/106, Flags:None
   HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:2840
   Payload:

```

```

0x0000: 00 00 0c e9 00 00 02 00 ff ff ff ff ff ff ff
2) Event:E_MTS_TX, length:60, at 35111 usecs after Tue Jan 22 16:15:29 2013
   [RSP] Opc:MTS_OPC_LICMGR_CMI_SHOW_LIC_HOSTID(7958), Id:0X000684D5,
Ret:SUCCESS
   Src:0x00000101/106, Dst:0x00000101/3302, Flags:None
   HA_SEQNO:0X00000000, RRtoken:0x000684D4, Sync:UNKNOWN, Payloadsize:153
   Payload:
0x0000: 00 00 00 01 00 00 00 29 00 00 00 00 61 64 6d 69

3) Event:E_MTS_RX, length:60, at 34931 usecs after Tue Jan 22 16:15:29 2013
   [REQ] Opc:MTS_OPC_LICMGR_CMI_SHOW_LIC_HOSTID(7958), Id:0X000684D4,
Ret:SUCCESS
   Src:0x00000101/3302, Dst:0x00000101/0, Flags:None
   HA_SEQNO:0X00000000, RRtoken:0x000684D4, Sync:UNKNOWN, Payloadsize:112
   Payload:
0x0000: 00 00 00 01 00 00 00 00 10 04 d8 08 61 64 6d 69

4) Event:E_MTS_RX, length:60, at 856132 usecs after Tue Jan 22 16:15:25 2013
   [NOT] Opc:MTS_OPC_VSH_ACFG_GEN(7663), Id:0X000684AE, Ret:SUCCESS
   Src:0x00000101/3296, Dst:0x00000101/106, Flags:None
   HA_SEQNO:0X00000000, RRtoken:0x00000000, Sync:UNKNOWN, Payloadsize:2840
   Payload:
0x0000: 00 00 0c e0 00 00 02 00 ff ff ff ff ff ff ff ff

5) Event:E_MTS_TX, length:60, at 445145 usecs after Tue Jan 22 16:15:25 2013
   [RSP] Opc:MTS_OPC_LICMGR_CMI_SHOW_LIC_HOSTID(7958), Id:0X0006847C,
Ret:SUCCESS
   Src:0x00000101/106, Dst:0x00000101/3293, Flags:None
   HA_SEQNO:0X00000000, RRtoken:0x0006847B, Sync:UNKNOWN, Payloadsize:153
   Payload:
0x0000: 00 00 00 01 00 00 00 29 00 00 00 00 61 64 6d 69
-- remaining output removed -

```

Q5) How many ports are licensed? _____

Q6) There are a number of **show tech-support** commands. Which command would be used to troubleshoot the boot variables? _____

Activity Verification

You have completed this task when you attain this result:

- You have successfully viewed the output of the **show tech-support <variable>** command.

Lab 4-1: Validating the Physical Connections for FCoE

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

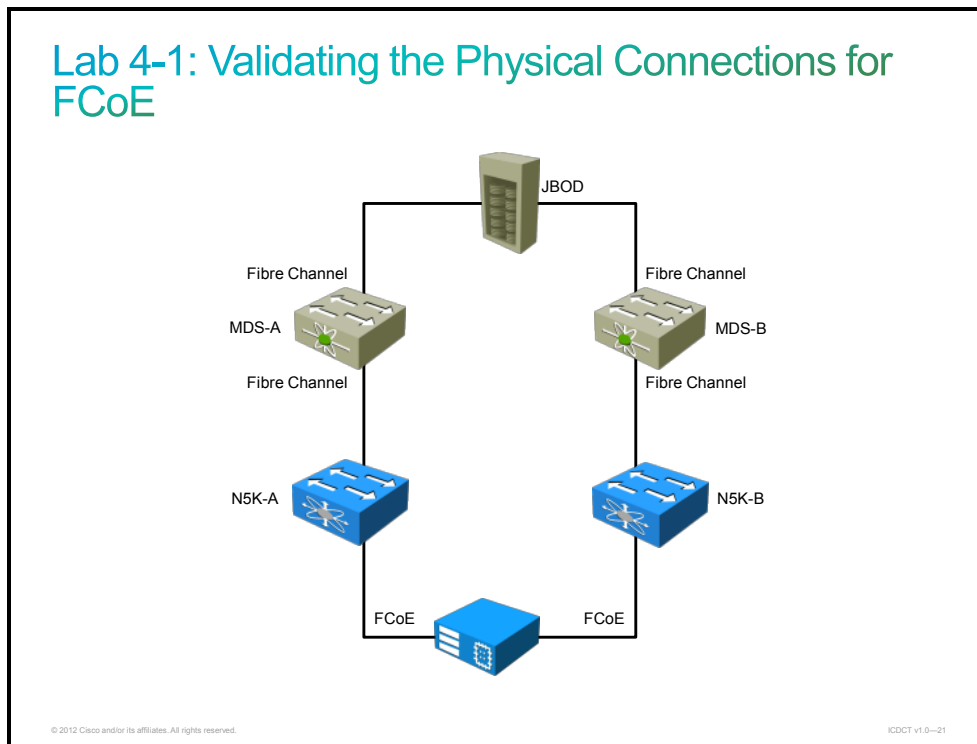
Activity Objective

In this activity, you will connect to a Cisco Nexus 5000 Series switch and validate the physical connections for FCoE. After completing this activity, you will be able to meet this objective:

- Verify the physical connections that are required for FCoE

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 5000 Series switch
- One PC with an SSH application for remote connectivity

Command List

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

Command	Description
<code>show interface brief</code>	Displays a brief summary of all interfaces
<code>show interface Ethernet x/y</code>	Displays detailed information for an interface
<code>show interface Ethernet x/y transceiver</code>	Displays the interface transceiver information
<code>show interface Ethernet x/y status</code>	Displays the interface line status
<code>show interface Ethernet x/y fcoe</code>	Displays the FCoE information for an interface
<code>show interface vfc x</code>	Displays the logical interface information

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Task 1: Validate FCoE Physical Connections

In this task, you will use the CLI commands to validate FCoE physical connections on the Cisco Nexus 5000 Series switch.

Activity Procedure

Complete these steps:

- Step 1** Using the credentials that are provided by your instructor, connect to the remote lab and your pod PC and open an SSH session to your Cisco Nexus 5000 Series Switch using IP 192.168.0.P8.
- Step 2** Log in using username **student** password **1234QWer**.
- Step 3** The **show interface brief** command displays summary information about all interfaces on the Cisco Nexus 5000 Series switch. Run the **show interface brief** command.

N5K-P# **sho int brief**

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
fc1/21	1	auto	on	trunking	swl	TE	2	--
fc1/22	1	auto	on	trunking	swl	TE	2	--
fc1/23	1	auto	on	sfpAbsent	--	--		--
...								
fc1/32	1	auto	on	sfpAbsent	--	--		--

Ethernet Interface	VLAN	Type	Mode	Status	Reason	Speed	Port Ch#
Eth1/1	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/2	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/3	42	eth	trunk	up	none	10G(D)	--
Eth1/4	42	eth	trunk	up	none	10G(D)	--
Eth1/5	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/6	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/7	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/8	1	eth	access	down	SFP not inserted	10G(D)	--
Eth1/9	1	eth	access	down	Administratively down	10G(D)	--
Eth1/10	1	eth	access	down	Administratively down	10G(D)	--
...							
Eth1/20	1	eth	trunk	down	Administratively down	10G(D)	--

Port	VRF	Status	IP Address	Speed	MTU
mgmt0	--	up	192.168.0.18	1000	1500

Interface	Vsan	Admin Mode	Admin Trunk Mode	Status	SFP	Oper Mode	Oper Speed (Gbps)	Port Channel
vfc3	11	F	on	trunking	--	TF	auto	--
vfc4	11	F	on	trunking	--	TF	auto	--

N5K-P#

Step 4 Ports are configured for trunking or access mode. Use the **show interface Ethernet 1/3** command to view details about the port the server is connected to.

```
N5K-P# sho int ethernet 1/3
Ethernet1/3 is up
  Hardware: 1000/10000 Ethernet, address: 0005.73f6.7c0a (bia 0005.73f6.7c0a)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
  Last link flapped 01:23:59
  Last clearing of "show interface" counters never
  30 seconds input rate 856 bits/sec, 107 bytes/sec, 0 packets/sec
  30 seconds output rate 1632 bits/sec, 204 bytes/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 120 bps, 0 pps; output rate 344 bps, 0 pps
  RX
    322 unicast packets  269 multicast packets  158 broadcast packets
    749 input packets  106018 bytes
    1 jumbo packets  0 storm suppression bytes
    0 giants  0 input error  0 short frame  0 overrun  0 underrun
    0 watchdog  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    418 unicast packets  3500 multicast packets  133 broadcast packets
    4051 output packets  408727 bytes
    5 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble
    0 Tx pause
  2 interface resets

N5K-P#
```

Q7) What speed is this interface running at? _____

Q8) What duplex mode is configured? _____

Q9) Have there been any link flaps identified? _____

Q10) If so, how many? _____

Q11) Is this interface up for FCoE? (Use the **show interface Ethernet 1/3 fcoe** to verify.) _____

Q12) What SFP is installed in the port? (Use the **show interface Ethernet 1/3 status** to identify the SFP.) _____

Step 5 Use the **show interface Ethernet 1/3 transceiver** command to identify the name and part number of the transceiver that is being used. _____

Step 6 Run the same commands on **interface Ethernet 1/4** to answer the same questions.

Q13) What speed is this interface running at? _____

Q14) What duplex mode is configured? _____

Q15) Have there been any link flaps identified? _____

Q16) Is this interface up for FCoE? (Use the **show interface Ethernet 1/4 fcoe** to verify.) _____

Q17) What SFP is installed in the port? (Use the **show interface Ethernet 1/4 status** to identify the SFP.) _____

Step 7 The virtual Fibre Channel interfaces connect to the servers. Run the **show interface vfc 3** command.

```
N5K-P# sho int vfc 3
vfc3 is trunking (Not all VSANs UP on the trunk)
  Bound interface is Ethernet1/3
  Hardware is Virtual Fibre Channel
  Port WWN is 20:02:00:05:73:f6:7c:3f
  Admin port mode is F, trunk mode is on
  snmp link state traps are enabled
  Port mode is TF
  Port vsan is 11
  Trunk vsans (admin allowed and active) (1,11)
  Trunk vsans (up) (11)
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) (1)
  1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    120 frames input, 13972 bytes
    0 discards, 0 errors
    176 frames output, 38052 bytes
    0 discards, 0 errors
  last clearing of "show interface" counters never
  Interface last changed at Thu Dec 27 08:53:31 2012
```

N5K-P#

Q18) Which physical interface is the virtual interface bound to? _____

Q19) What port mode is the interface running in? _____

Q20) What is the port VSAN number? _____

Q21) Which VSANs are active? _____

Step 8 Can you run the command **show interface vfc 3 transceiver** to view the transceiver details? _____

Q22) Why is it not possible to view the transceiver details?

Activity Verification

You have completed this task when you attain this result:

- You have successfully verified the physical and logical interface connections.

Lab 5-1: Cisco UCS

You will navigate the Cisco UCS.

Activity Objective

In this activity you will navigate Cisco UCS Manager and determine physical connectivity without the USC and to the outside world.

After completing this activity, you will be able to meet these objectives:

- Understand physical connectivity for Cisco UCS.

Required Resources

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

- Two Cisco UCS Fabric Interconnect Cluster
- One PC with access to the Cisco UCS Fabric Interconnect serial consoles

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab IP address plan

Task 1: Connect to UCS Manager

During this task, you will connect to UCS Manager.

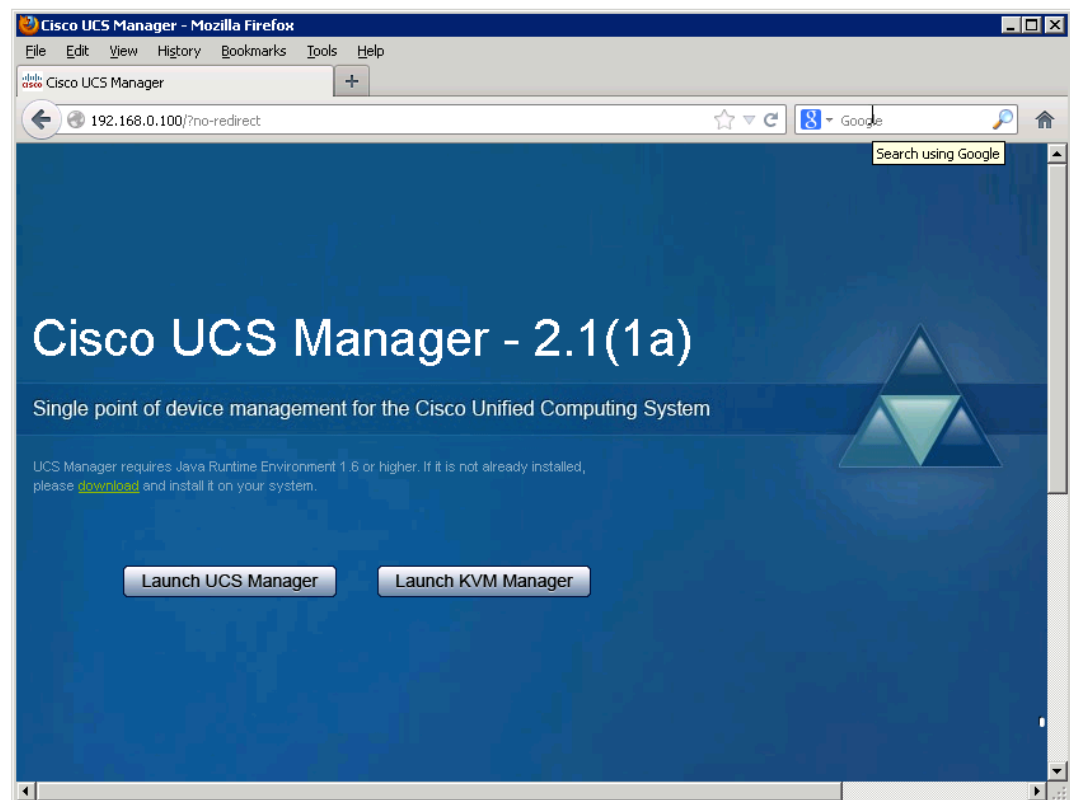
Activity Procedure

Caution The equipment used in the exercise is SHARED with all other students in the class, please DO NOT play around since that may break the lab for everybody.

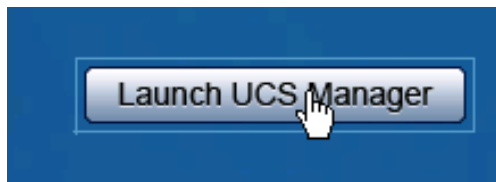
Complete these steps:

- Step 1** Log into the FastLane remote lab by starting internet explorer (or any other browser) and navigating to <http://remotelabs.flane.de>
- Step 2** Click the “login” button on the top right (or the “student login” link on the bottom of the page)
- Step 3** Login with the credentials of your workgroup (supplied by the instructor)
- Step 4** Click on the BLUE PC icon to start your remote access session to the remote lab. ALL lab exercises will be done on this PC, your local PC will only be used for accessing the remote lab GUI. (the GREY components are not manageable by you for now). Use username “Administrator” und passwort “1234QWer”
- Step 5** Open a browser window and open <http://192.168.0.100/?no-redirect>

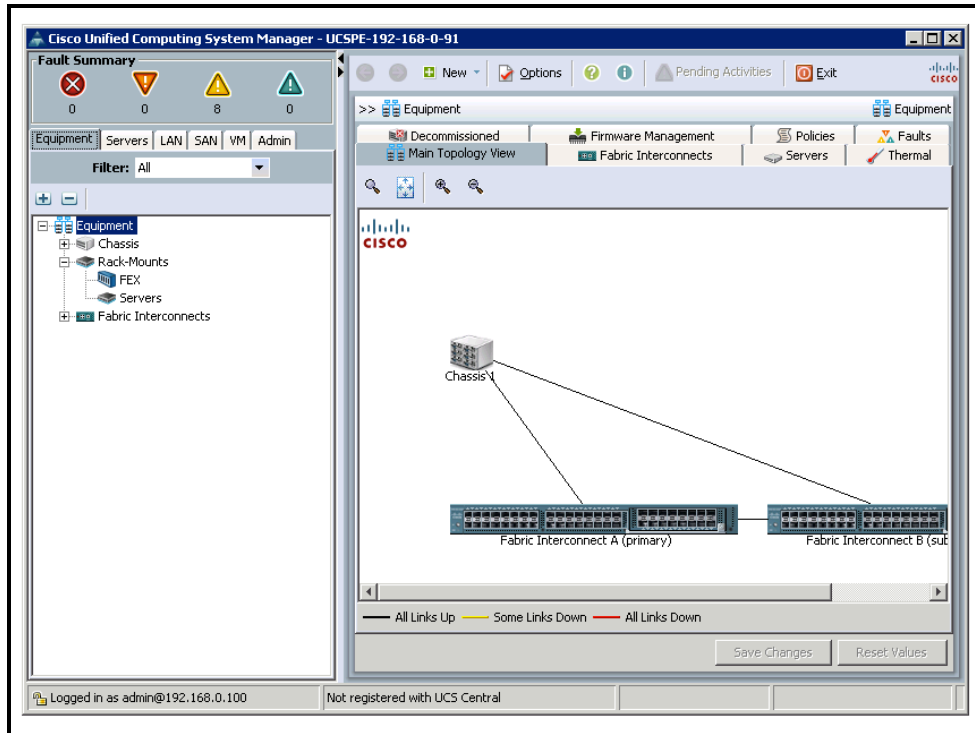
Note All Pods use share the same UCS system and therefore use the same IP address to connect.



- Step 6** Click the “Launch UCS Manager” Button.



Step 7 Wait for UCS Manager to load then login with user “admin” password “admin”



Note The UCS system (actually an emulator of the system) is partially preconfigured.

Activity Verification

You have completed this task when you attain these results:

- Logged into UCS manager.

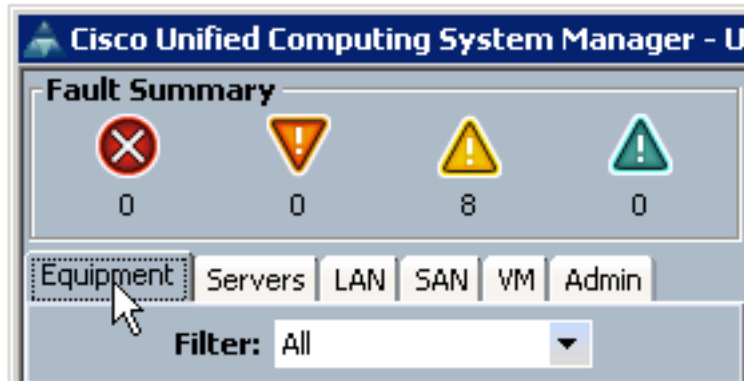
Task 2: Validate Server Ports

During this task, you will verify server ports on the Cisco UCS 6120XP Fabric Interconnects.

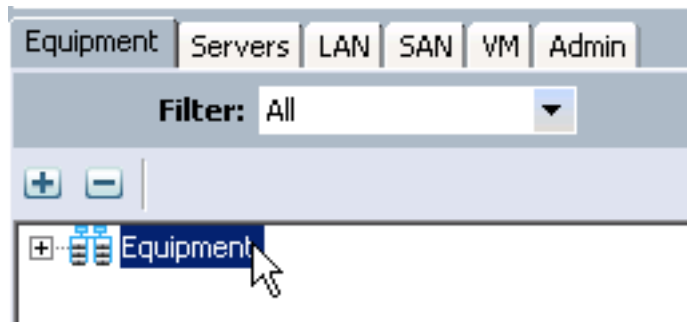
Activity Procedure

Complete these steps:

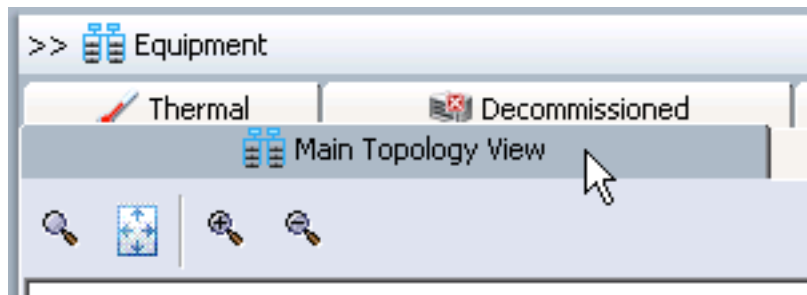
Step 1 Click the Equipment tab in UCS Manager



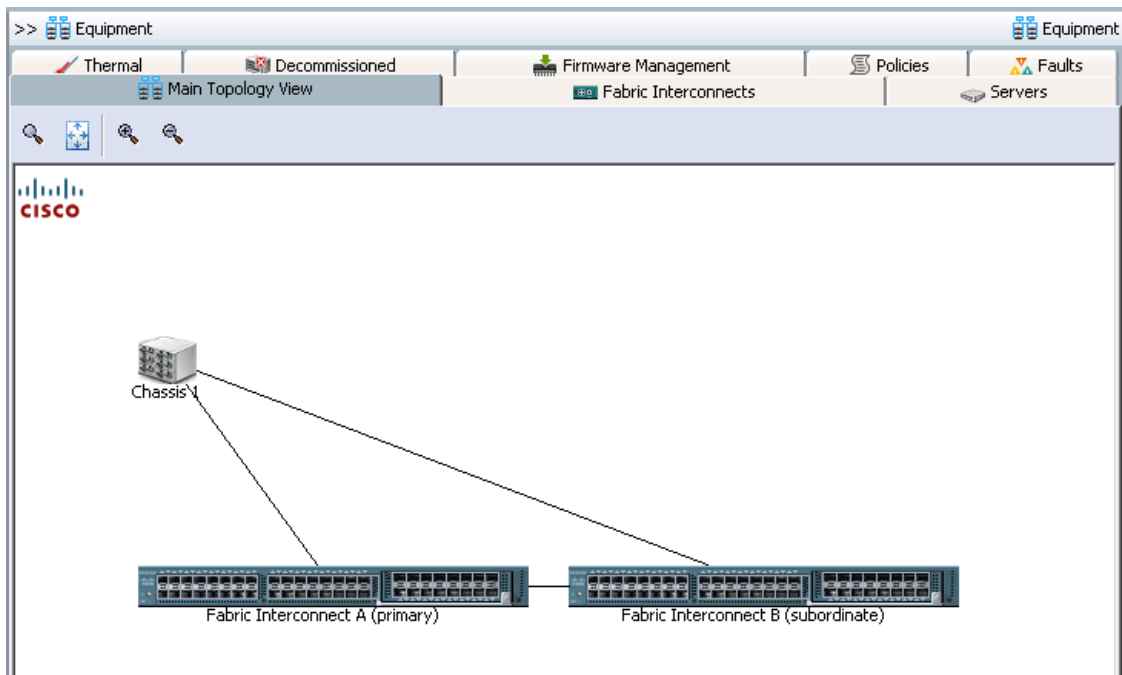
Step 2 Select “Equipment”



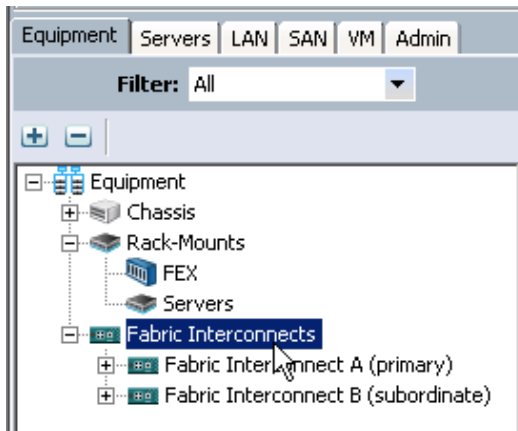
Step 3 In the right-hand content pane click “Main Topology View”



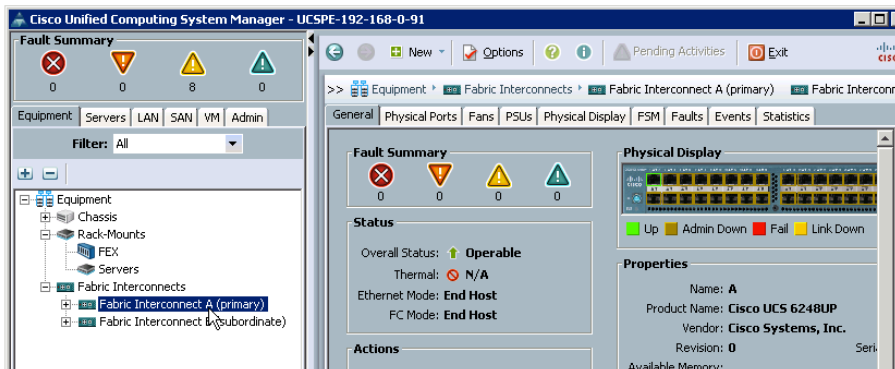
Step 4 The topology of this UCS demo system is displayed.



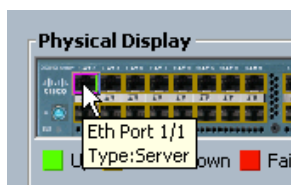
Step 5 In the equipment tab expand the tree and navigate to **Fabric Interconnects**.



Step 6 Click on primary Fabric Interconnect, note the content pane on the right is filled with information about this FI.

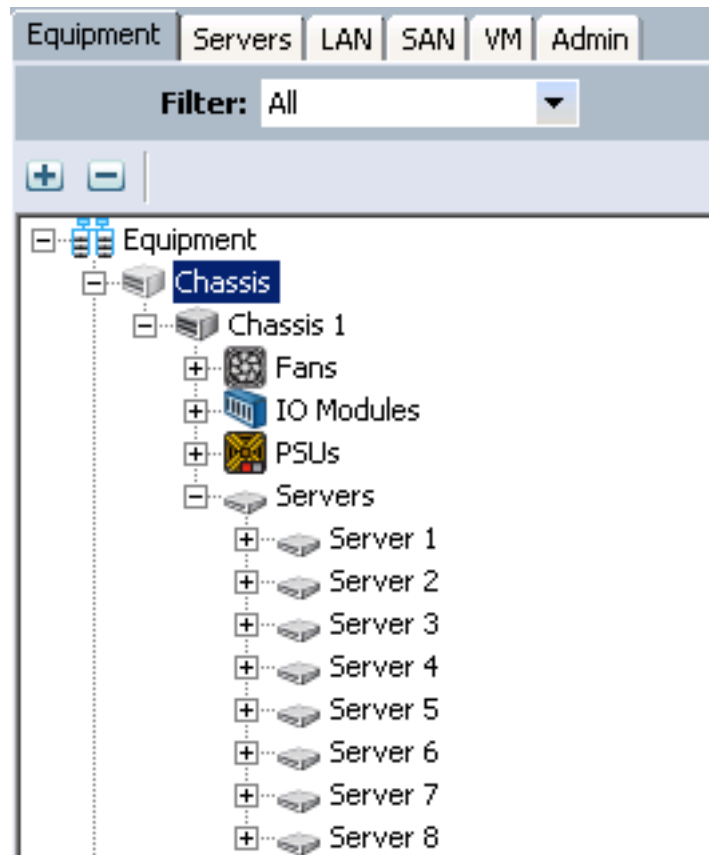


Step 7 Hover the mouse over Port1, note the tooltip – this is a server port.



Note In this lab this is the only active connections, in a real UCS system you would also see Uplink port (connecting the UCS system to the outside network world), FC Uplink ports (for connecting the UCS system to the FC SAN cloud) and even Appliance Ports (for connecting FC, FCoE and/or Ethernet devices like Firewalls, Load Balancers and IP Storage)

Step 8 Expand **Chassis** in the Equipment tab and note there is one chassis holding 8 servers.



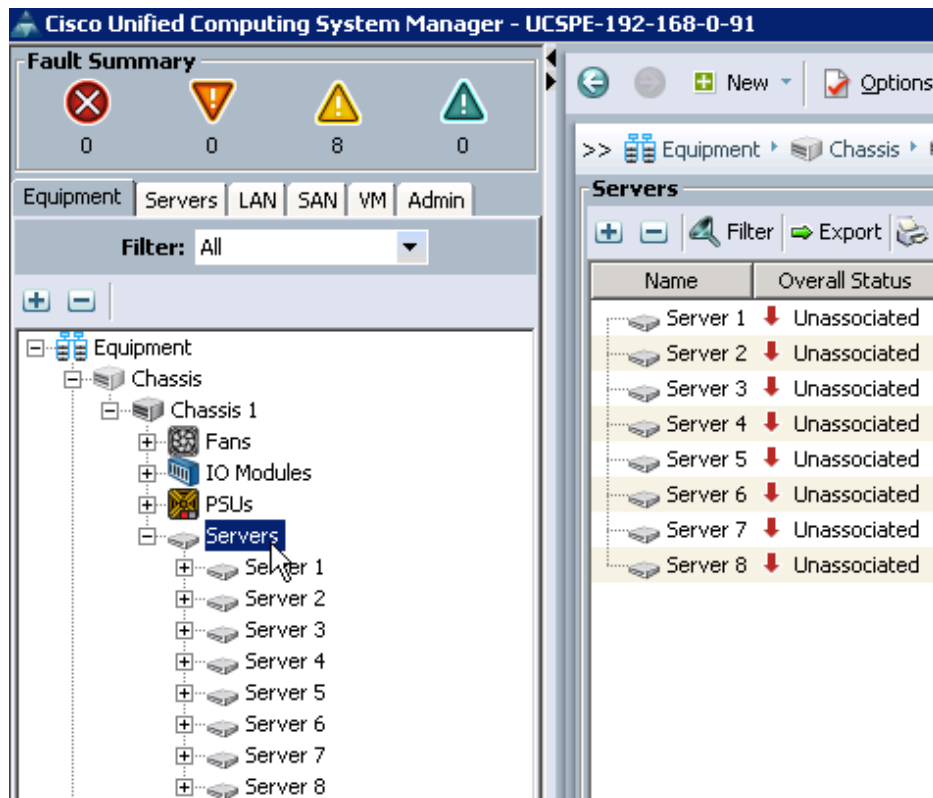
Task 3: Observe Blade Server Discovery in Finite State Machine

During this task, you will explore blade server discovery in Cisco UCS Manager.

Activity Procedure

Complete these steps:

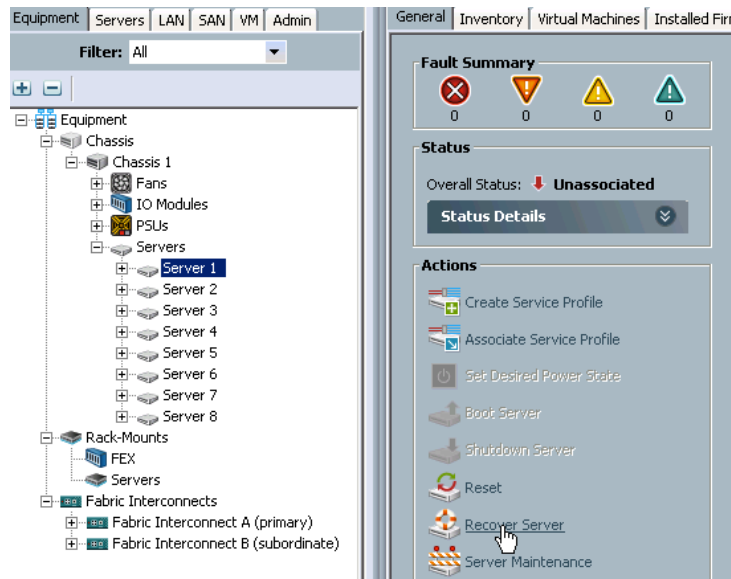
Step 1 Expand the **Chassis1** and select the **Servers** item.



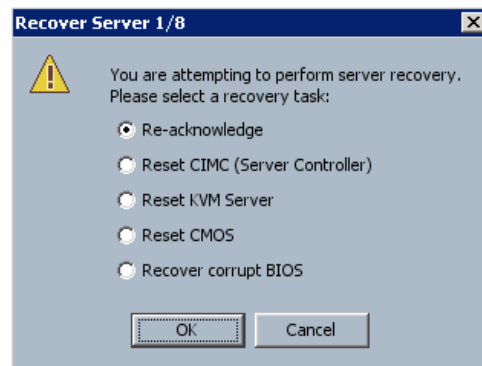
Step 2 Notice that the overall status of the server should be **Unassociated**. (if a service profile is assigned to your server ask your instructor to remove it for you.)

Note The Servers were automatically discovered during system installation. We will now simulate a hardware change by manually forcing the discovery process – under normal circumstances it is not necessary to re-acknowledge Servers.

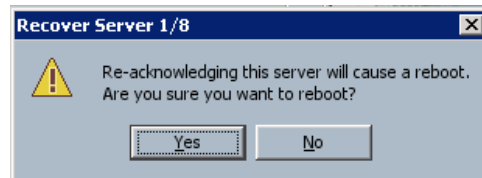
Step 3 Select the server with your Pod# and click the “Recover Server” Action item (or right-click your server and use the context menu)



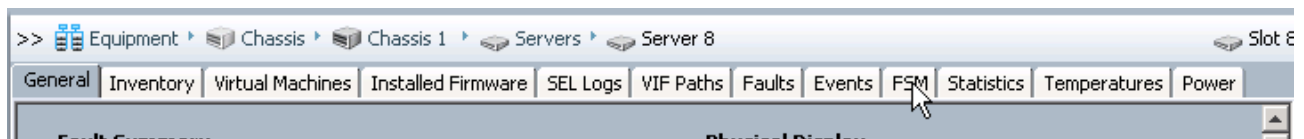
Step 4 Confirm **Re-acknowledge** with **OK**



Step 5 Confirm Reboot with **Yes** and dismiss the confirmation.



Step 6 Click the **FSM** tab to allow the class to observe state transitions as the Cisco UCS B200 is discovered.



Step 7 A Finite State Machine (FSM) is a process that tracks and validates state transitions. When the B200 M2 blade server is being observed, components are tested first for presence in the blade server and then the component is validated. This process continues until all of the components of the server are inventoried and added to the Cisco UCS Manager database.

General | Inventory | Virtual Machines | Installed Firmware | SEL Logs | VIF Paths | Faults | Events | **FSM** | Statistics | Temperatures | Power

FSM Status: **In Progress**
 Description:
 Current FSM Name: **Discover**
 Completed at:
 Progress Status: 96%
 Remote Invocation Result:
 Remote Invocation Error Code: **None**
 Remote Invocation Description:

Step Sequence

Order	Name	Description	Status	Timestamp
1	Discover Bmc Presence	checking CIMC of server 1/...	Success	2013-01-23T15:28
2	Discover Bmc Inventory	getting inventory of server...	Success	2013-01-23T15:28
3	Discover Pre Sanitize	Preparing to check hardwar...	Success	2013-01-23T15:28
4	Discover Sanitize	Checking hardware configu...	Success	2013-01-23T15:28
5	Discover Check Power Avail...	If explicit power capping is ...	Success	2013-01-23T15:28
6	Discover Blade Power On	power on server 1/8 for dis...	Success	2013-01-23T15:28
7	Discover Config Fe Local	configuring primary fabric i...	Success	2013-01-23T15:28
8	Discover Config Fe Peer	configuring secondary fabri...	Success	2013-01-23T15:28
9	Discover Config User Access	configuring external user a...	Success	2013-01-23T15:28
10	Discover Nic Presence Local	detect mezz cards in 1/8(F...	Success	2013-01-23T15:28
11	Discover Nic Presence Peer	detect mezz cards in 1/8(F...	Success	2013-01-23T15:28

Step 8 If the discovery process completes successfully, the Progress Status bar reaches 100% and the Status of Last Operation will indicate Discover Success.

>> Equipment > Chassis > Chassis 1 > Servers > Server 8

General | Inventory | Virtual Machines | Installed Firmware | SEL Logs | VIF Paths | Faults | Events | **FSM** | Statistics | Temperatures | Power

FSM Status: **Success**
 Description:
 Current FSM Name: **Discover**
 Completed at: **2013-01-23T15:30:34**
 Progress Status: 100%
 Remote Invocation Result:
 Remote Invocation Error Code: **None**
 Remote Invocation Description:

Step 9 Once all servers are discovered, service profiles are created to provision the server and prepare it for operating system or hypervisor installation.

Step 10 To display more detailed information on the actual state transitions that occurred during the discovery process click the **Events** tab.

>> Equipment > Chassis > Chassis 1 > Servers > Server 8							
General	Inventory	Virtual Machines	Installed Firmware	SEL Logs	VIF Paths	Faults	Events
Filter	Export	Print					
Affected object	Code	ID	Cause	Created at	User	Description	
sys/chassis-1/blad...	E4196486	37484	transition	2013-01-22T19:3...	internal	[FSM:STAGE:STA...	
sys/chassis-1/blad...	E4195074	38353	transition	2013-01-22T19:3...	internal	[FSM:STAGE:EN...	
sys/chassis-1/blad...	E4196502	39902	transition	2013-01-23T15:2...	internal	[FSM:STAGE:STA...	
sys/chassis-1/blad...	E4195073	38331	transition	2013-01-22T19:3...	internal	[FSM:STAGE:STA...	
sys/chassis-1/blad...	E4195060	39876	transition	2013-01-23T15:2...	internal	[FSM:STAGE:EN...	
sys/chassis-1/blad...	E4195058	39868	transition	2013-01-23T15:2...	internal	[FSM:STAGE:ASY...	
sys/chassis-1/blad...	E4195807	37295	transition	2013-01-22T19:3...	internal	[FSM:STAGE:EN...	
sys/chassis-1/blad...	E4195053	36725	transition	2013-01-22T19:3...	internal	[FSM:BEGIN]: bla...	
sys/chassis-1/blad...	E4196475	39917	transition	2013-01-23T15:2...	internal	[FSM:STAGE:STA...	
sys/chassis-1/blad...	E4195053	39848	transition	2013-01-23T15:2...	admin	[FSM:STAGE:EN...	
sys/chassis-1/blad...	E4195808	39885	transition	2013-01-23T15:2...	internal	[FSM:STAGE:EN...	
sys/chassis-1/blad...	E4195054	36705	transition	2013-01-22T19:3...	internal	[FSM:STAGE:ASY...	
sys/chassis-1/blad...	E4195056	39859	transition	2013-01-23T15:2...	internal	[FSM:STAGE:STA...	
sys/chassis-1/blad...	E4195085	39993	transition	2013-01-23T15:3...	internal	[FSM:STAGE:STA...	
sys/chassis-1/blad...	E4196477	39988	transition	2013-01-23T15:2...	internal	[FSM:STAGE:RE...	
sys/chassis-1/blad...	E4196620	39941	transition	2013-01-23T15:2...	internal	[FSM:STAGE:ASY...	
sys/chassis-1/blad...	E4195054	36787	transition	2013-01-22T19:3...	internal	[FSM:STAGE:RE...	
sys/chassis-1/blad...	E4195054	35715	transition	2013-01-22T19:3...	internal	[FSM:STAGE:RE...	
sys/chassis-1/blad...	E4195053	36583	transition	2013-01-22T19:3...	internal	[FSM:STAGE:RES...	
sys/chassis-1/blad...	E4196502	37385	transition	2013-01-22T19:3...	internal	[FSM:STAGE:EN...	
sys/chassis-1/blad...	E4195053	36824	transition	2013-01-22T19:3...	internal	[FSM:STAGE:RES...	
sys/chassis-1/blad...	E4195075	39939	transition	2013-01-23T15:2...	internal	[FSM:STAGE:STA...	

Activity Verification

You have completed this task when you attain these results:

- Verified d a server port in Cisco UCS Manager and that a new chassis appeared in the Cisco UCS Manager inventory.
- Observe the blade server discovery progress in the FSM tab of the server.

Lab 5-2: Exploring the Cisco UCS Manager GUI

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

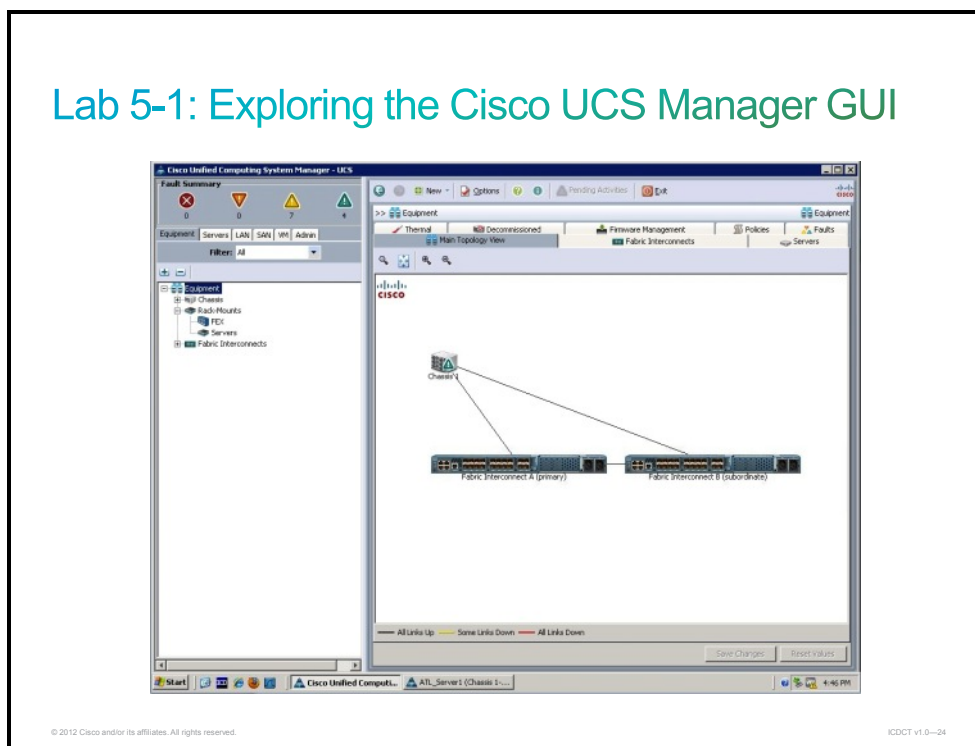
Activity Objective

In this activity, you will navigate through the Cisco UCS Manager GUI to learn where to locate, monitor, and configure various activities. After completing this activity, you will be able to meet these objectives:

- Interact with the various elements of the Cisco UCS Manager GUI
- Locate important functions within the Cisco UCS Manager GUI

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 UCS 6120XP Fabric Interconnect clusters
- One Cisco UCS 5108 Blade Server Chassis with two I/O modules
- One PC with access to the remote lab environment
- Lab resources sheet

Command List

All procedures in this lab are performed in the Cisco UCS Manager GUI.

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Implementation Sheet for Lab 5-2 Explore the Cisco UCS Manager GUI

Use this implementation sheet to aid in the configuration tasks in Lab 5-1.

Task 3: Pod Number to Organization Mapping

Pod	Organization
1	Pod1
2	Pod2
3	Pod3
4	Pod4
5	Pod5
6	Pod6
7	Pod7
8	Pod8

Task 1: Connect to Cisco UCS Manager

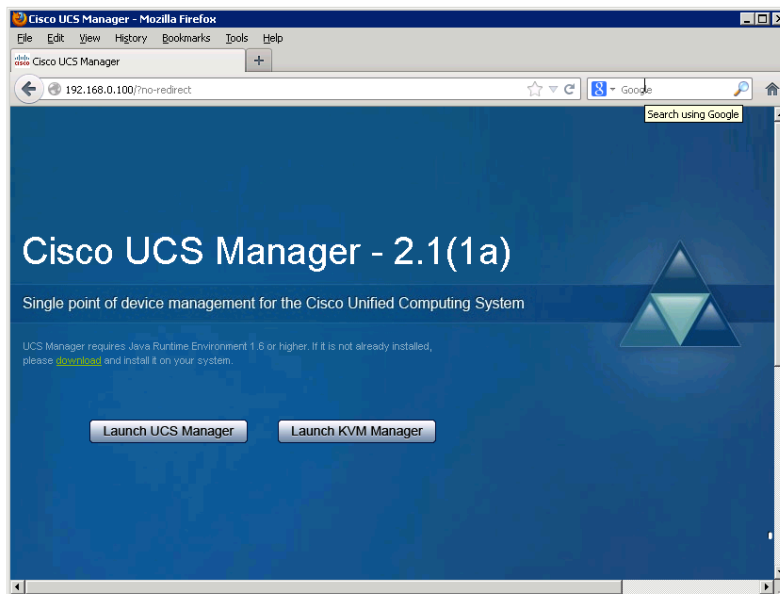
In this task, you will connect to the Cisco UCS Manager GUI.

Activity Procedure

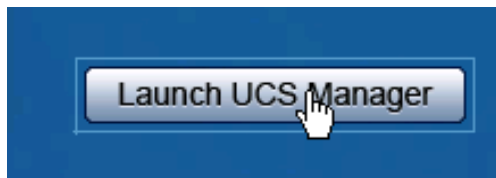
Complete these steps:

- Step 1** If you are still connected to UCS Manager go to Task 2.
- Step 2** Log into the FastLane remote lab by starting internet explorer (or any other browser) and navigating to <http://remotelabs.flane.de>
- Step 3** Click the “login” button on the top right (or the “student login” link on the bottom of the page)
- Step 4** Login with the credentials of your workgroup (supplied by the instructor)
- Step 5** Click on the BLUE PC icon to start your remote access session to the remote lab. ALL lab exercises will be done on this PC, your local PC will only be used for accessing the remote lab GUI. (the GREY components are not manageable by you for now). Use username “Administrator” und passwort “1234QWer”
- Step 6** Open a browser window and open <http://192.168.0.100/?no-redirect>

Note All Pods use share the same UCS system and therefore use the same IP address to connect.



- Step 7** Click the “Launch UCS Manager” Button.



- Step 8** Wait for UCS Manager to load then login with user “admin” password “admin”

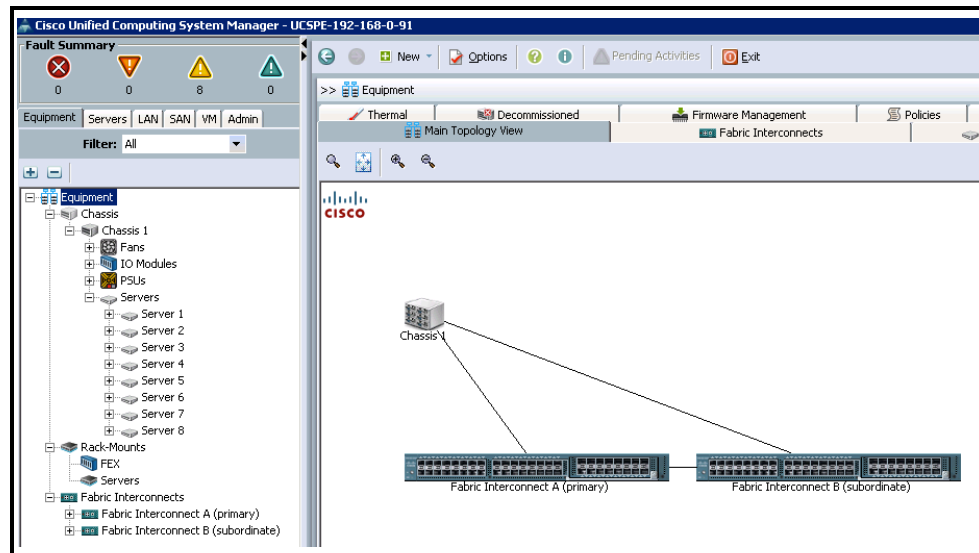
Task 2: Explore the Equipment Tab

In this task, you will explore the Cisco UCS Manager GUI from the equipment point of view.

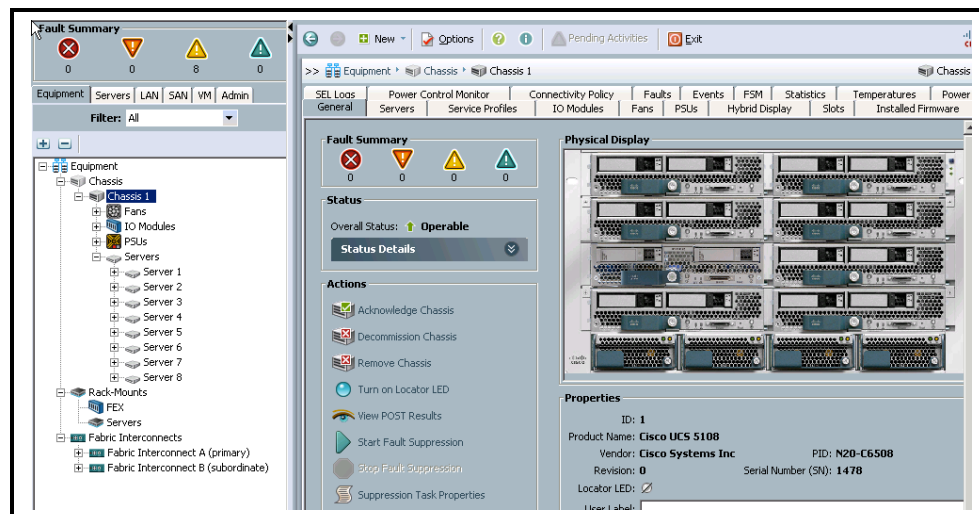
Activity Procedure

Complete these steps:

- Step 1** Expand the Equipment tab in the Navigation pane by clicking the + sign to the left of the word Equipment in the Cisco UCS Manager GUI.
- Step 2** Click **Equipment** at the top of the hierarchy, and then click the **Main Topology** tab on the Content pane. This tab provides a graphical view of connectivity from the fabric interconnects to the Cisco UCS 5108 Blade Server Chassis.

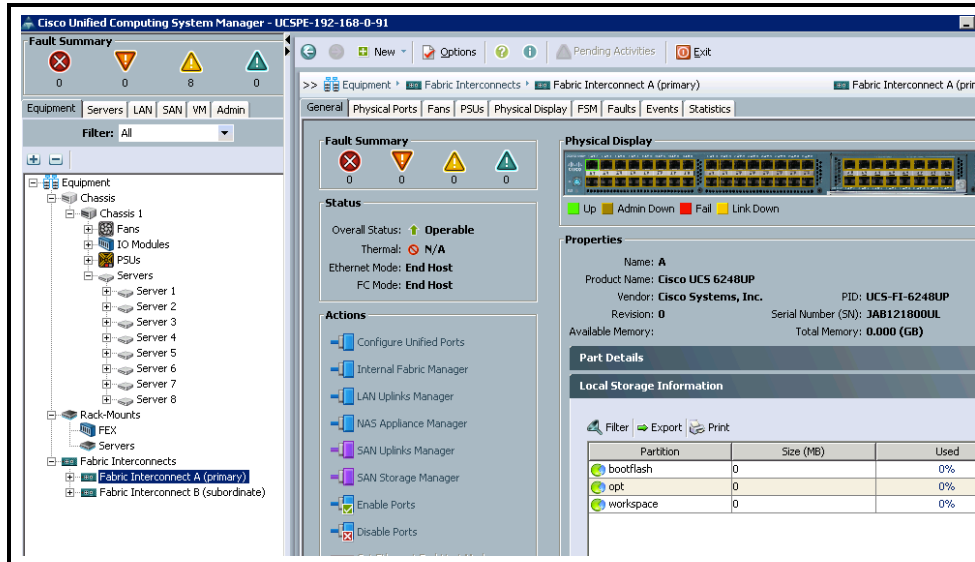


- Step 3** Select the **Chassis** list by clicking the + sign to the left of Chassis, then click the **General** tab if it is not already selected.



- Step 4** In the content pane, there is a graphical view of the chassis. Above the chassis, take a few minutes to explore the selection tabs that provide access to additional information about the chassis.

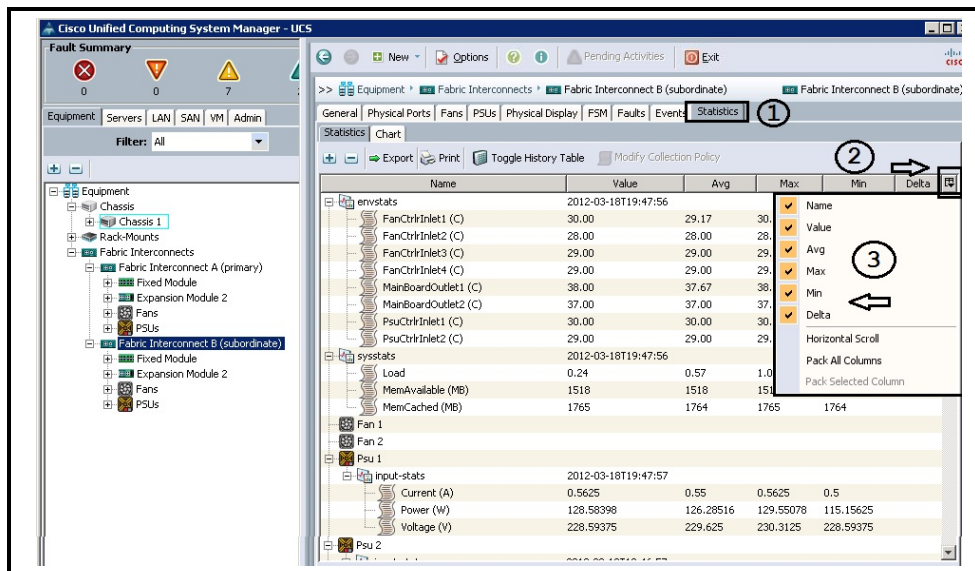
Step 5 Expand both fabric interconnects by clicking the + sign to the left of each fabric interconnect icon. (The hierarchy can be collapsed by clicking the – signs.)



Step 6 In the content pane, click the double chevron to open the information panel that is rolled up underneath it. Click the double chevron again to roll the window up. This behavior is uniform throughout Cisco UCS Manager.



Step 7 Next, click the **Statistics** tab in the content pane. A summary of environmental statistics appears. In the upper-right portion of the statistics window is a small black triangle on a chart. Click this **black triangle** to choose which columns you would like to display on the table. This menu is available on any screen that displays columnar data. Add or remove check marks to display or hide columns.



Task 3: Explore the Servers Tab

In this task, you will explore the Cisco UCS Manager GUI from the pools and policies perspective.

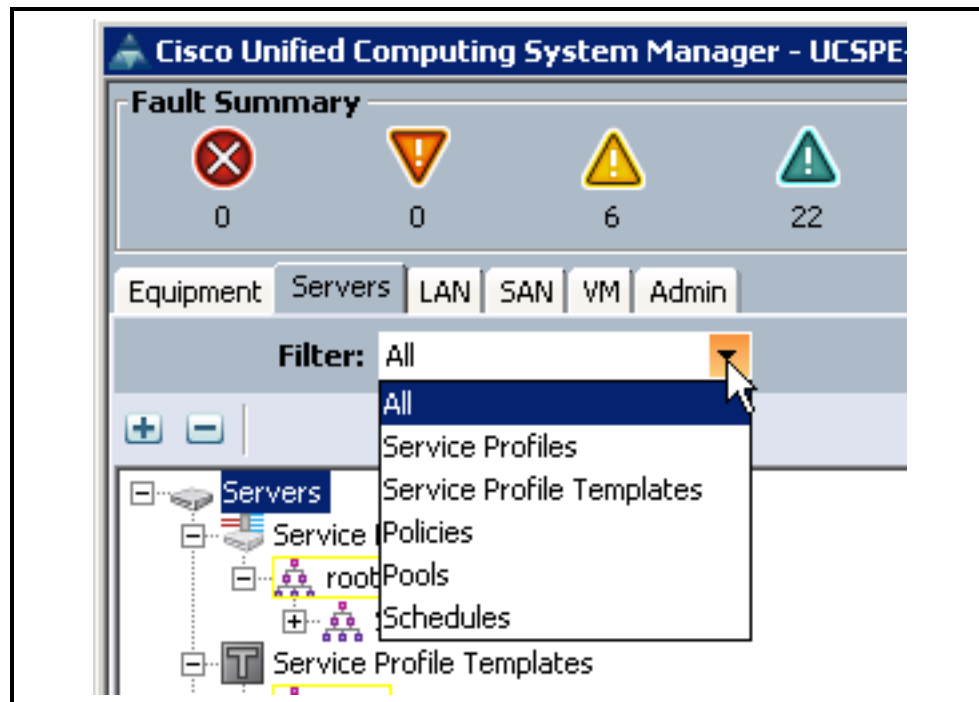
Activity Procedure

Complete these steps:

- Step 1** In the Cisco UCS Manager GUI, click the **Servers** tab in the Navigation pane and expand the following tree in the hierarchy: **Service Profiles > root -> Sub-Organizations > Pod#**.
- Step 2** Click the **Pod#-SP** service profile (where # = your assigned pod number). The example in the following figure is for pod 1.

Note Organizations are an optional configuration element that is available in the Servers, LAN, and SAN tabs. They allow the Cisco UCS administrator to create objects such as pools, policies, and profiles into separate folders. If organizations are not employed, all objects are created under the root organization. Root is always present and cannot be modified or deleted.

- Step 3** Take a few minutes to explore the tabs at the top of the content pane.
- Step 4** From the Servers tab, click the **Filters** drop-down menu.



- Step 5** Choose the **Pools** filter to reduce the view to only pools that are associated with the Servers tab.
- Step 6** Navigate to **Pools->root->Sub-Organizations-> Pod#**.
- Q1) What are the names of the Server Pool and UUID pools for your organization?
-

Task 4: Explore the LAN Tab

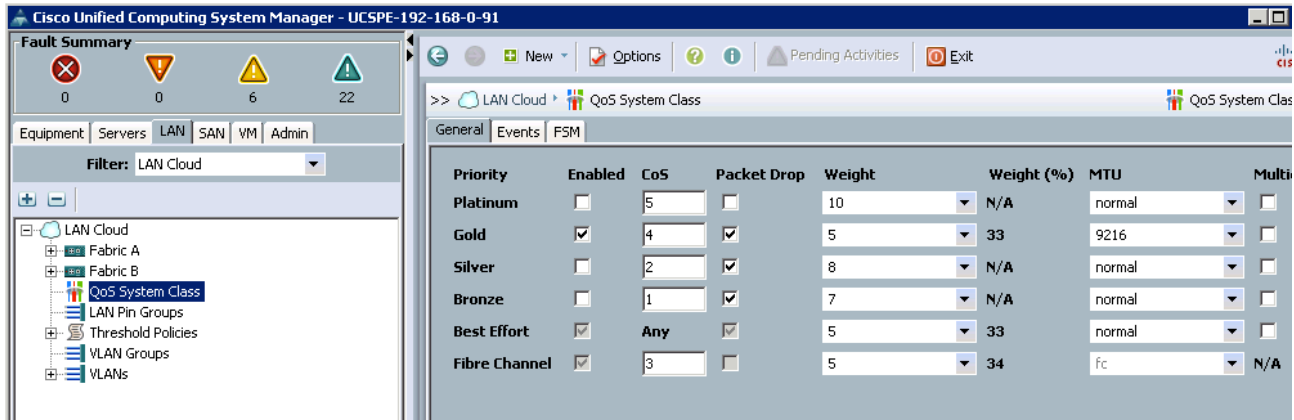
In this task, you will explore the Cisco UCS Manager GUI from the LAN perspective.

Activity Procedure

Complete these steps:

Step 1 Click the **LAN** tab in the Navigation pane and set the Filter to **LAN Cloud**.

Step 2 Expand the **LAN Cloud** and choose **QoS System Class**.

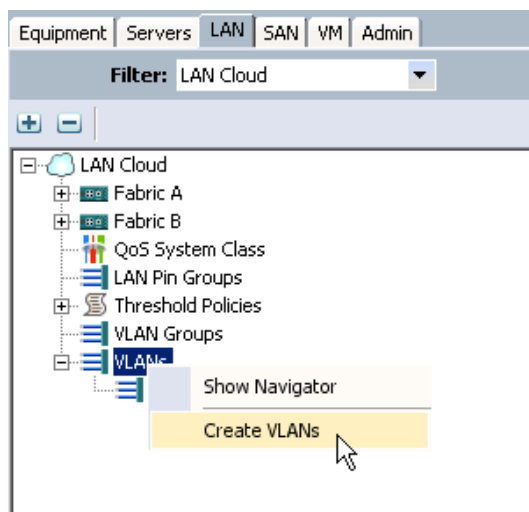


Step 3 This view allows the administrator to adjust Class of Service, MTU, and weighting. The example Gold class that is shown here is assigned CoS of 4 and an MTU of 9216 to allow the transmission and receipt of Jumbo frames. (Jumbos are greater than 1500 bytes.)

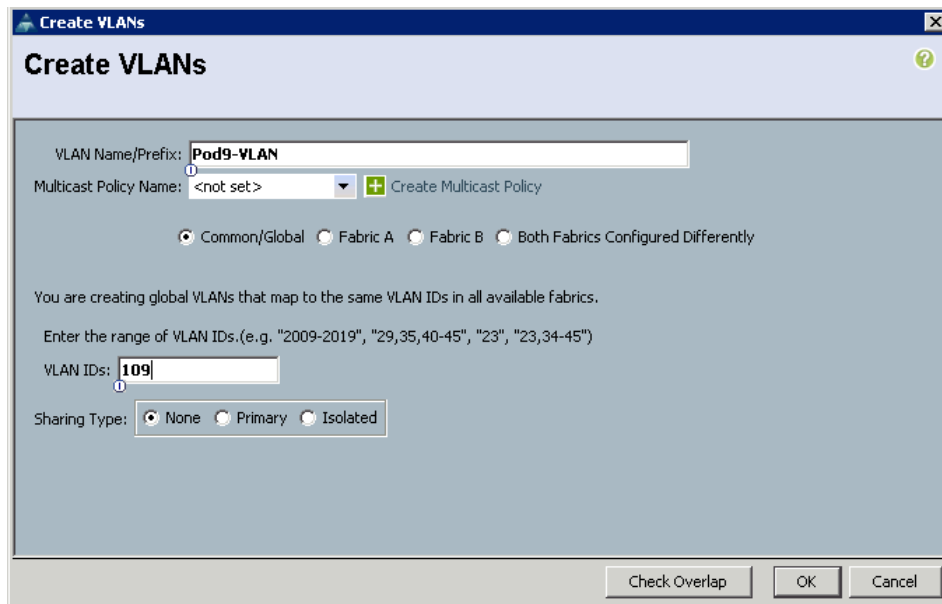
Step 4 Click the **+ sign** to the left of **VLANs** to expand that branch of the tree.

Q1) How many VLANs are configured?

Step 5 Right-click **VLANs** and click “**Create VLAN**”

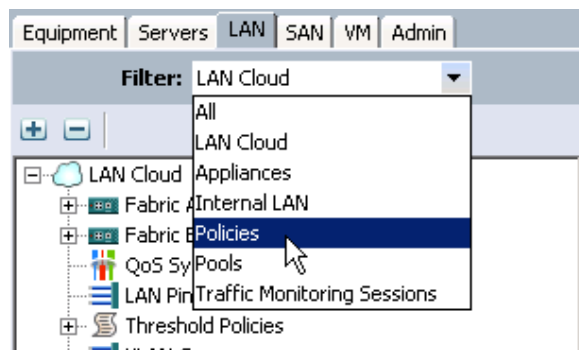


Step 6 Create VLAN 10P (P is your Pod#) for both FIs (common).



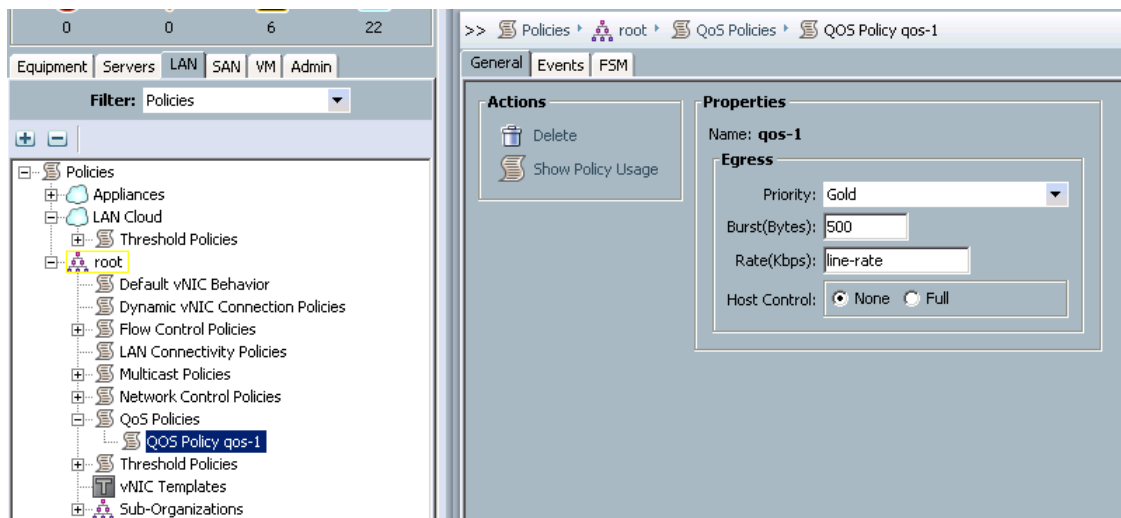
Step 7 Click OK to confirm and dismiss the confirmation.

Step 8 Click the **Filter** drop-down and choose **Policies**.



Step 9 Navigate to **Policies->root->QoS Policies**.

Step 10 Choose the QoS policy.



Q2) What Priority is assigned in the Egress area of the Content pane?

Note This step maps the policy that is enabled in QoS System Class and allows this policy to be consumed by your Service Profile to control traffic on Ethernet links.

Step 11 Click the **Filter** drop-down and choose **Pools**.

Step 12 Navigate to **Pools->root->Sub-Organizations-> Pod#**.

Q3) What is the range of MAC addresses in the MAC Pool for your pod?
_____ to _____

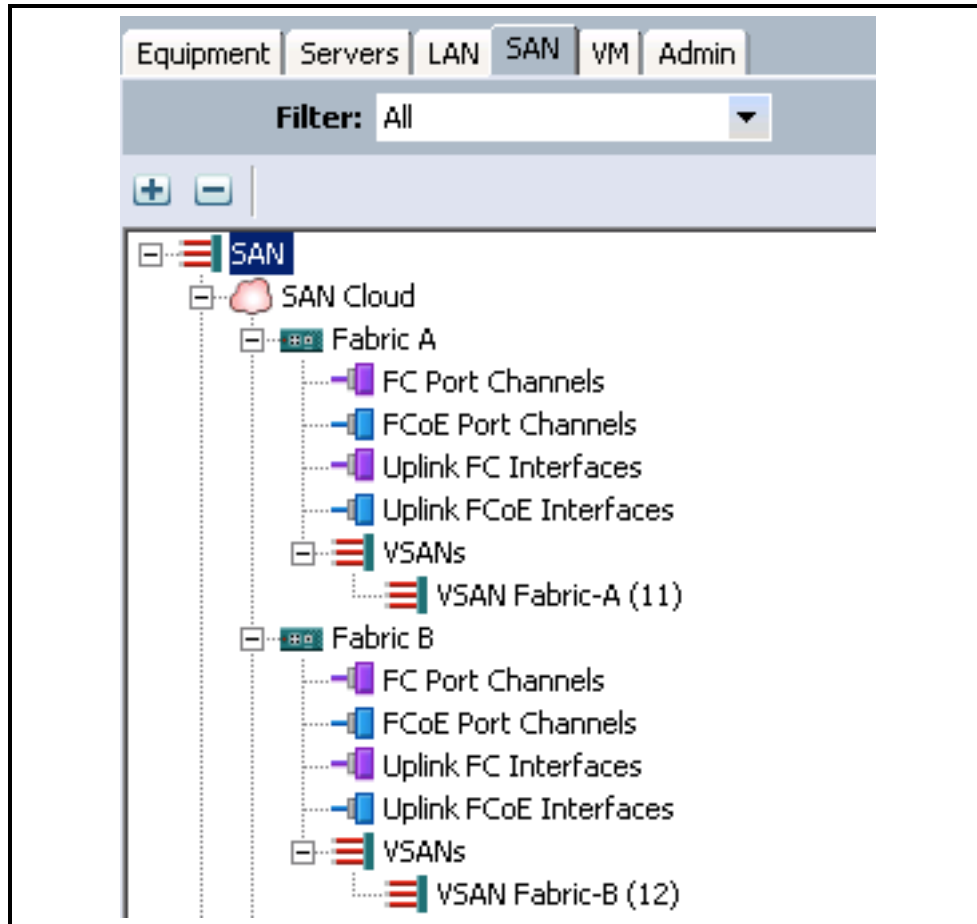
Task 5: Explore the SAN Tab

In this task, you will explore the Cisco UCS Manager GUI from the SAN perspective.

Activity Procedure

Complete these steps:

- Step 1** Click the **SAN** tab in the Navigation pane and choose the Filter **SAN Cloud**.
- Step 2** Expand **Fabric A** and **Fabric B**.



- Step 3** Expand the **VSANs**.

Q1) What VSANs are configured on each fabric interconnect?

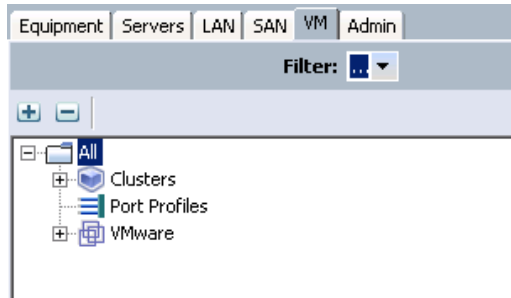
Task 6: Explore the VM Tab

In this task, you will briefly explore the SAN tab.

Activity Procedure

Complete these steps:

- Step 1** Click the **VM** tab in the Navigation pane and leave the Filter to set to **All**.



- Step 2** Expand **Clusters** and **VMware** elements.

- Step 3** The VM tab is used to configure a feature called VM-FEX, also known as VMware Pass-Through Switching (PTS). The VM tab will not be discussed further in this course, it is covered in the DCUCI class.

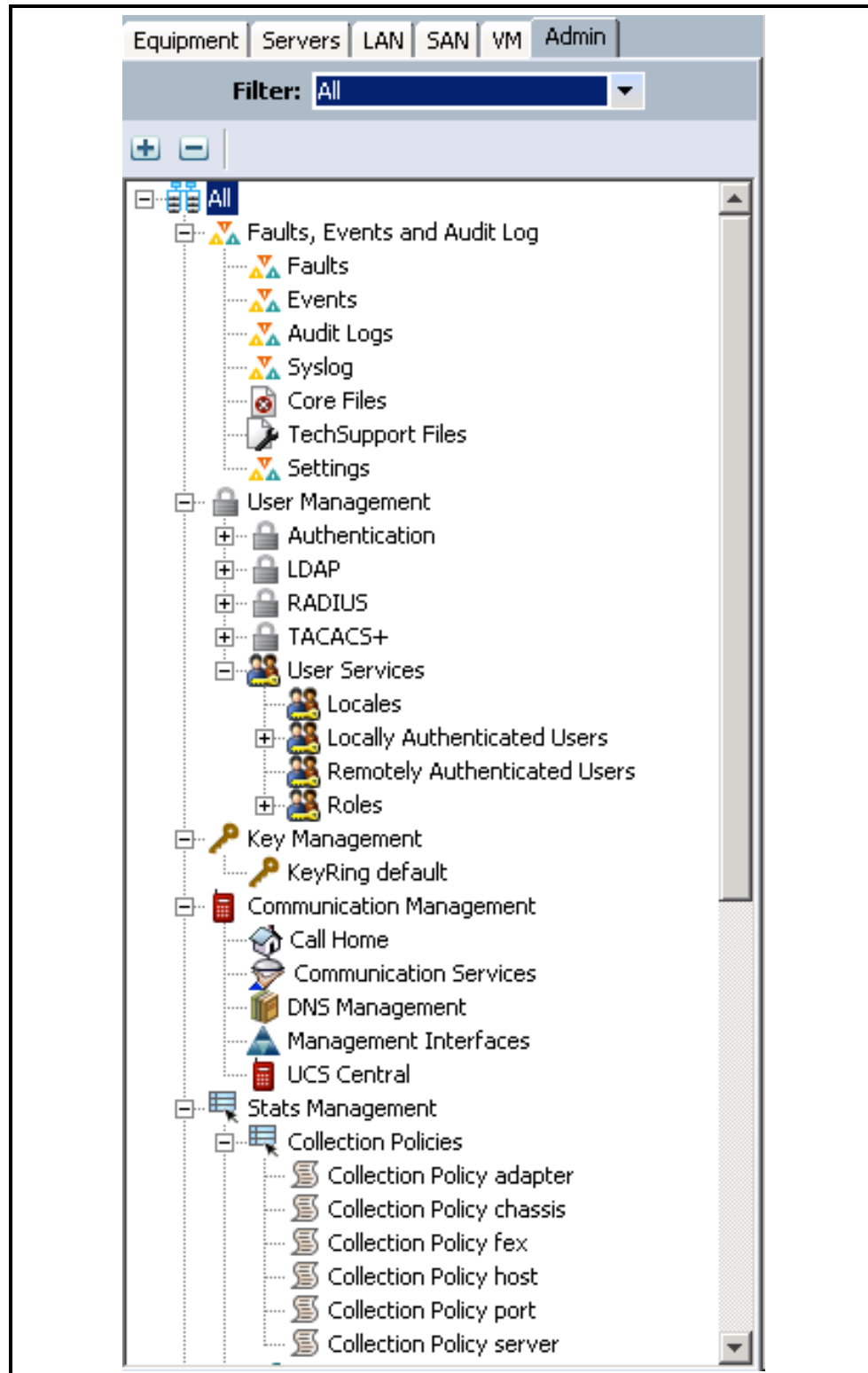
Task 7: Explore the Admin Tab

In this task, you will explore common administrative tasks.

Activity Procedure

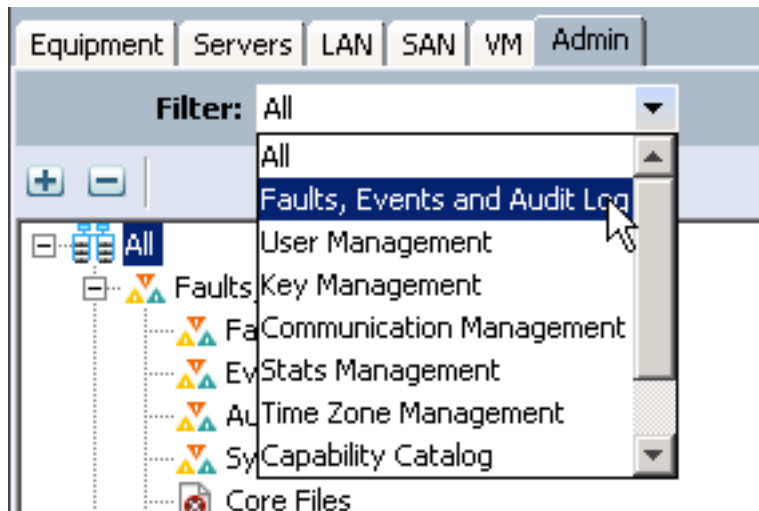
Complete these steps:

Step 1 Click the **Admin** tab in the Navigation pane and leave the Filter to set to **All**.

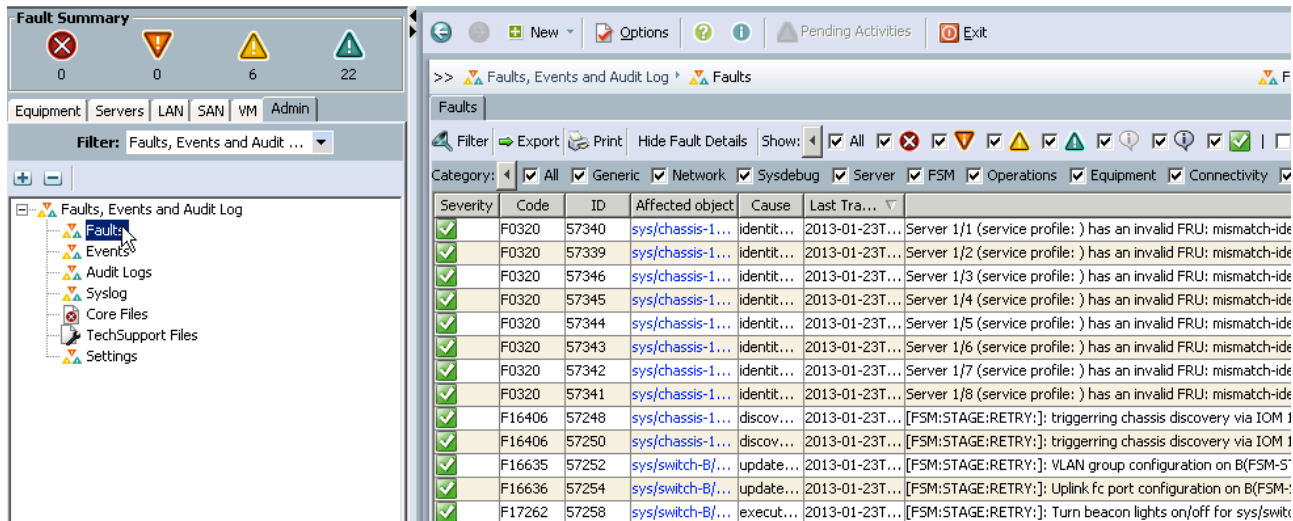


Step 2 The large number of options in the Admin tab makes the Filter menu very useful.

Step 3 Click the **Filter** drop-down and choose **Faults, Events and Audit Log**.

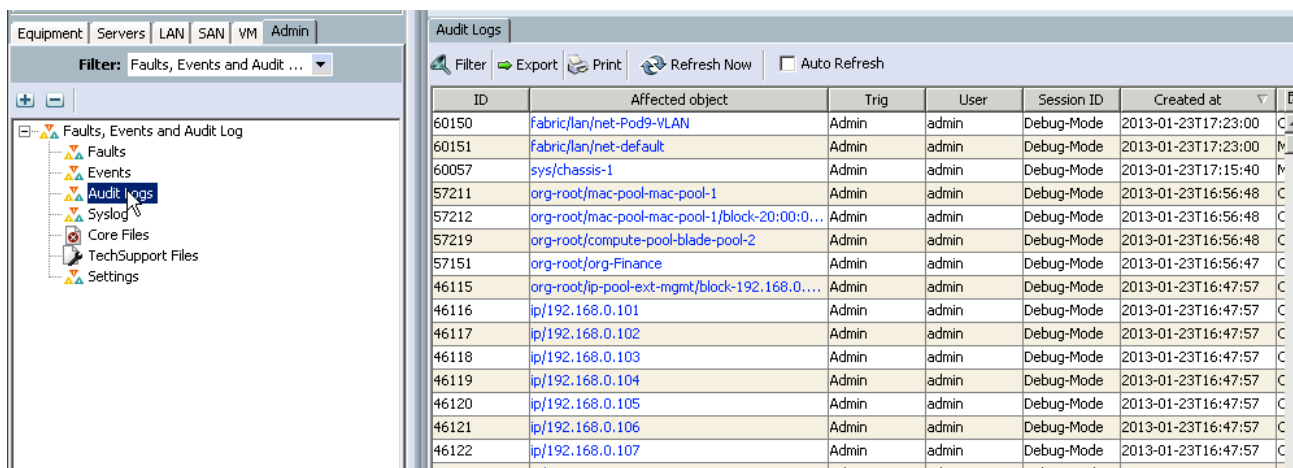


Step 4 When you choose a fault in the content pane, the fault detail appears in the **Details** panel of the **Content** pane.



Step 5 In the **Severity and Category** sections, there are check marks that allow granular filtering of events in the event log. Uncheck a few check marks and observe the results.

Step 6 Click the **Audit Log** link in the Navigation pane.



- Step 7** Every time a configuration change is made to the Cisco UCS Manager database, the Audit Log records the change. This can be a useful tool to discover which user created, modified, or deleted a particular object.
- Step 8** Click the **Filter** drop-down and choose **User Management**.
- Step 9** Expand **User Services** and **Locally Authenticated Users**.
- Step 10** This view is where you add, modify, and delete locally authenticated Cisco UCS Manager users. Although the admin user cannot be deleted, it is a best practice to disable it and assign individual users administrative privileges.

Activity Verification

You have completed this task when you attain these results:

- Successfully log in to Cisco UCS Manager.
- Explore the equipment hierarchy in the Equipment tab.
- Explore service profiles and pools in the Servers tab.
- Explore QoS system classes and pools in the LAN tab.
- Explore VSANs in the SAN tab.
- Explore where communications with VMware vCenter servers are configured.
- Explore faults, the audit log, and local users.

Lab 5-3: Creating a Service Profile from a Template

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

Activity Objective

In this activity, you will generate a service profile for your pod. After completing this activity, you will be able to meet these objectives:

- Explain how to spawn a service profile from a service profile template
- Explain how to monitor service profile association with the FSM tab
- Explain how to boot the server
- Explain how to disassociate a service profile from a blade server

Required Resources

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

- Two Cisco UCS 6120XP Fabric Interconnect clusters
- One Cisco UCS 5108 Blade Server Chassis with two I/O modules
- One PC with access to the remote lab environment
- Lab resource sheet

Command List

All procedures in this lab are performed in the Cisco UCS Manager GUI.

Job Aids

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

- Lab topology diagram
- Lab connections
- Lab addressing plan

Implementation Sheet for Lab 5-3 Creating a Service Profile from a Template

Use this implementation sheet to aid in the configuration tasks in Lab 5-2.

Task 1: Pod Number to Organization Mapping

Pod	Organization
1	Pod1
2	Pod2
3	Pod3
4	Pod4
5	Pod5
6	Pod6
7	Pod7
8	Pod8

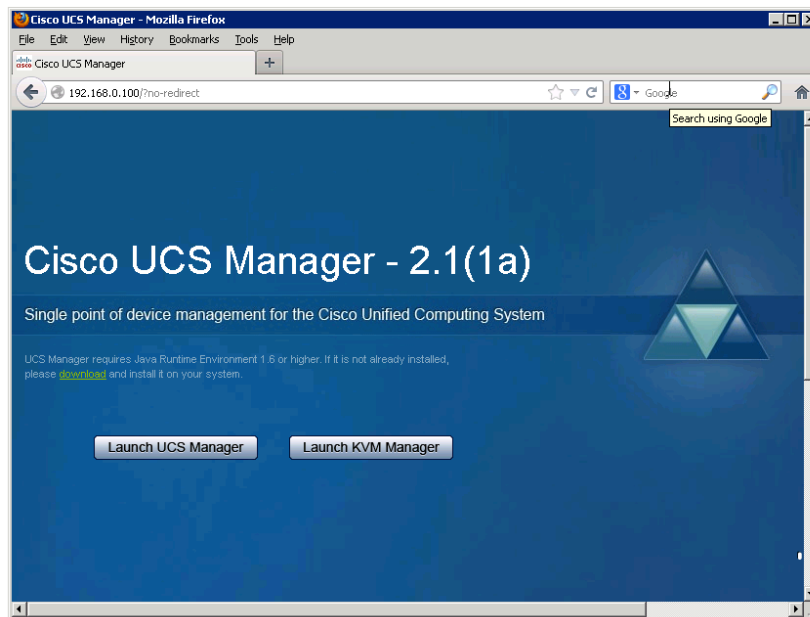
Task 1: Connect to Cisco UCS Manager

In this task, you will connect to the Cisco UCS Manager GUI.

Activity Procedure

Complete these steps:

- Step 1** If you are still connected to UCS manager go to Task 2.
- Step 2** Log into the FastLane remote lab by starting internet explorer (or any other browser) and navigating to <http://remotelabs.flane.de>
- Step 3** Click the “login” button on the top right (or the “student login” link on the bottom of the page)
- Step 4** Login with the credentials of your workgroup (supplied by the instructor)
- Step 5** Click on the BLUE PC icon to start your remote access session to the remote lab. ALL lab exercises will be done on this PC, your local PC will only be used for accessing the remote lab GUI. (the GREY components are not manageable by you for now). Use username “Administrator” und password “1234QWer”
- Step 6** Open a browser window and open <http://192.168.0.100/?no-redirect>



- Step 7** Click the “Launch UCS Manager” Button.



- Step 8** Wait for UCS Manager to load then login with user “admin” password “admin”

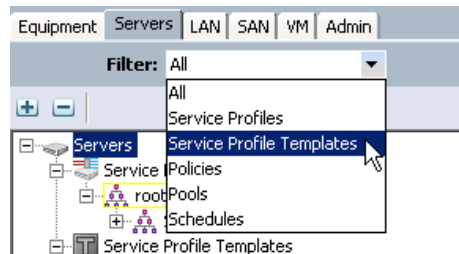
Task 2: Generate a Service Profile from a Template

In this task, you will generate a service profile from a template and observe the association process.

Activity Procedure

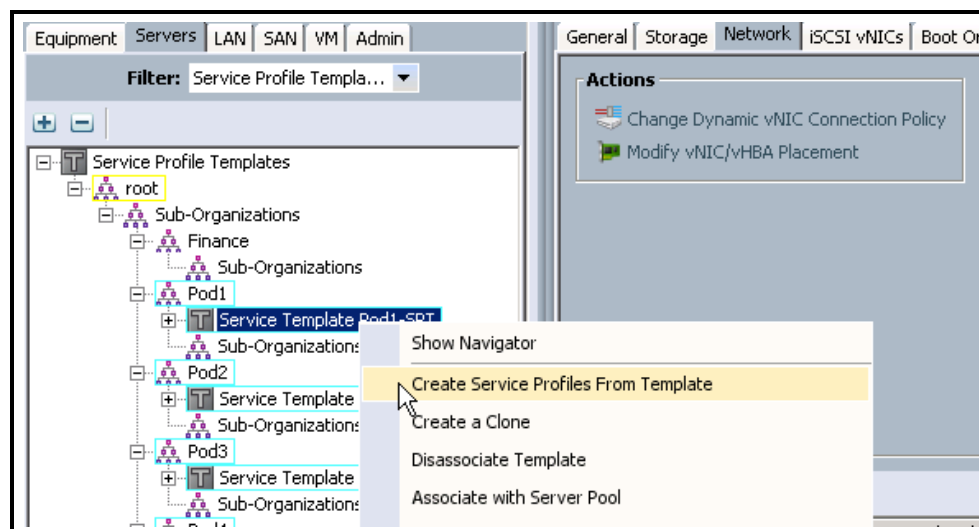
Complete these steps:

- Step 1** From the Servers tab, choose **Service Profile Templates** from the Filter drop-down menu.

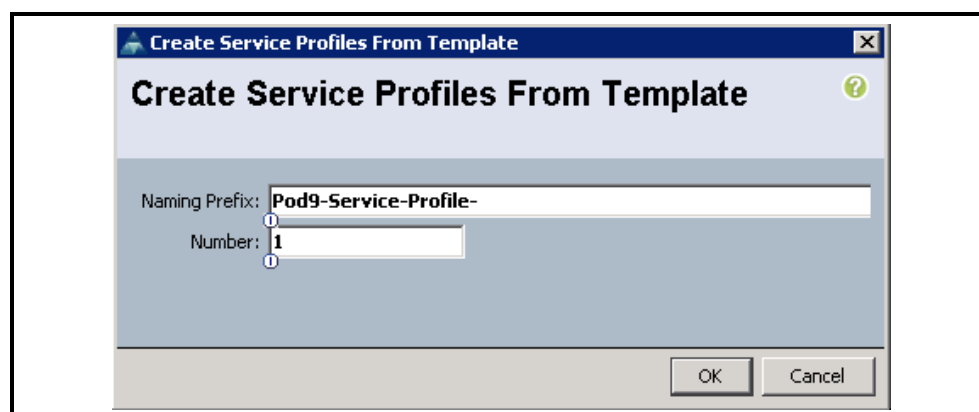


- Step 2** Navigate to **Service Profile Templates->root->Sub-Organizations->Pod#**.

- Step 3** Right-click the service profile template for your pod and choose **Create Service Profiles from Template**.

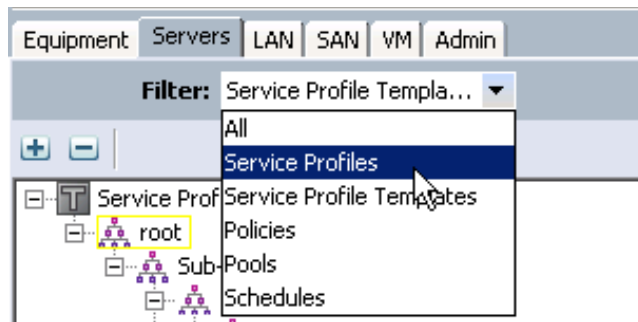


- Step 4** In the dialog box that appears, enter the server “Pod#-Service-Profile-” name (replace #with your pod number). Set the number in the **Number** field to **1**.



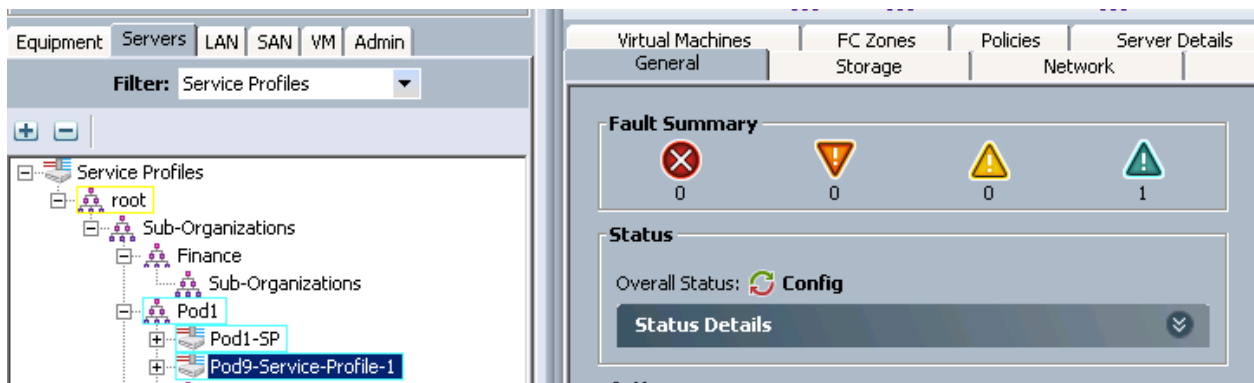
Step 5 Click the **OK** button on the dialog box indicating the service profile was created successfully.

Step 6 From the Servers tab, choose **Service Profiles** from the Filter drop-down menu.



Step 7 Navigate to **Service Profiles->root->Sub-Organizations-> Pod#**.

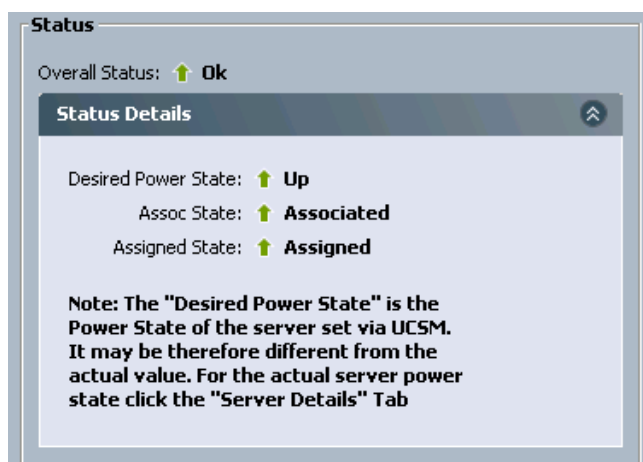
Step 8 Click the name of the service profile for your pod. Note the Status is "Config".



Step 9 Click the **FSM** tab in the Content pane to view the service profile associating with your blade.

Step 10 Once the Progress Status indicator reaches 100%, the Status of Last Operation should read Hard Shutdown Success.

Step 11 While still in the Content pane for your server, click the **General** tab. Expand the Status Details.



Note Normally you would now launch KVM and install an OS on your newly deployed server.

Step 12

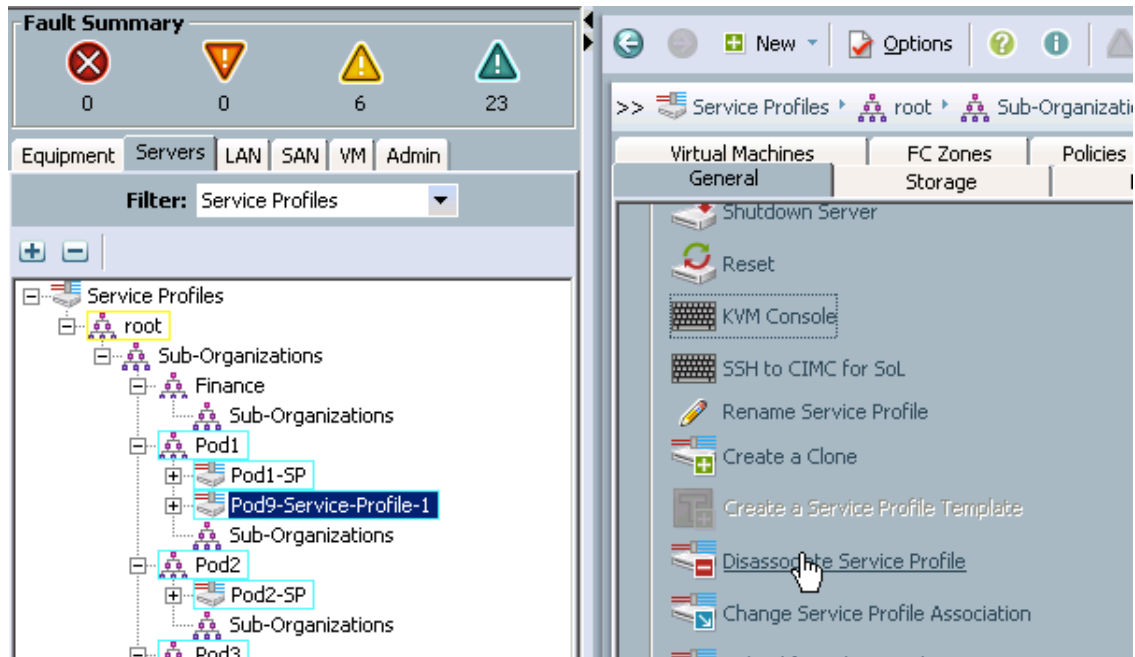
Task 3: Service Profile Management

In this task, you will disassociate and associate service profiles.

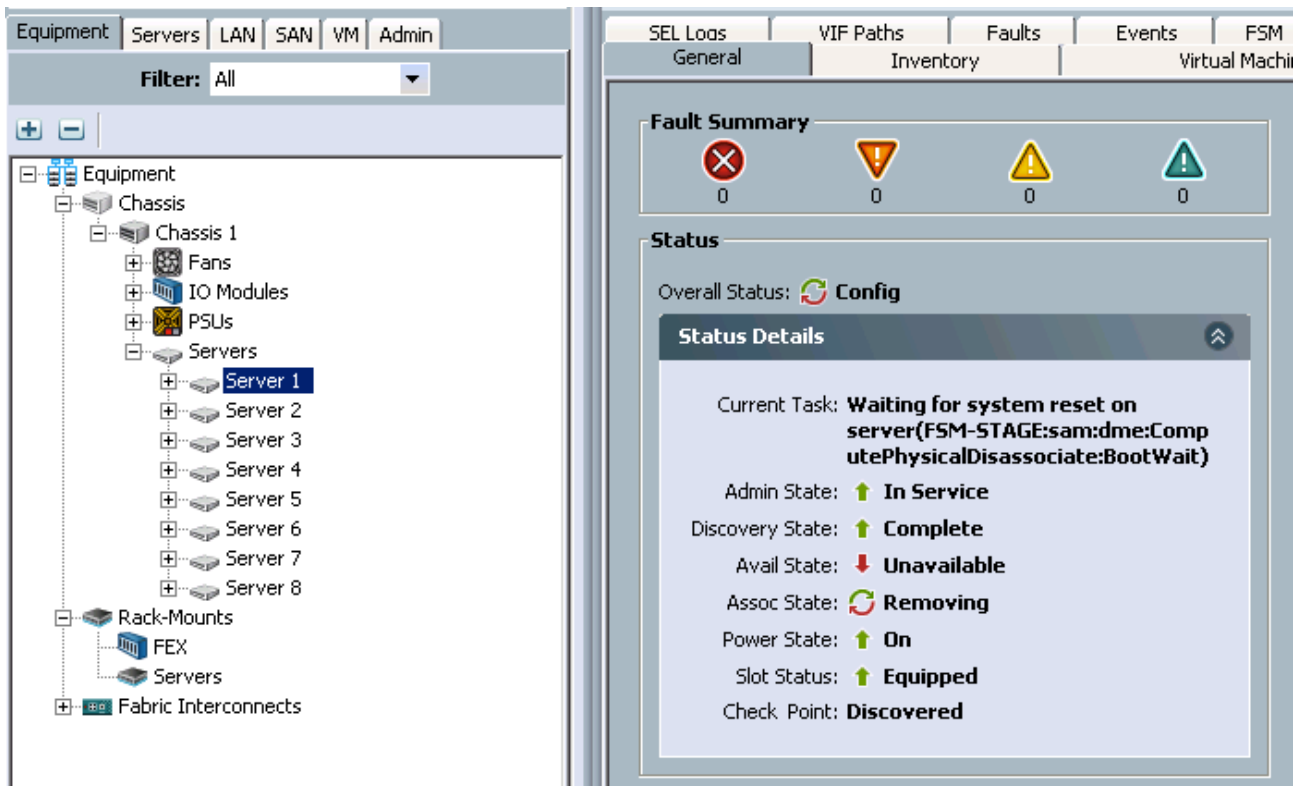
Activity Procedure

Complete these steps:

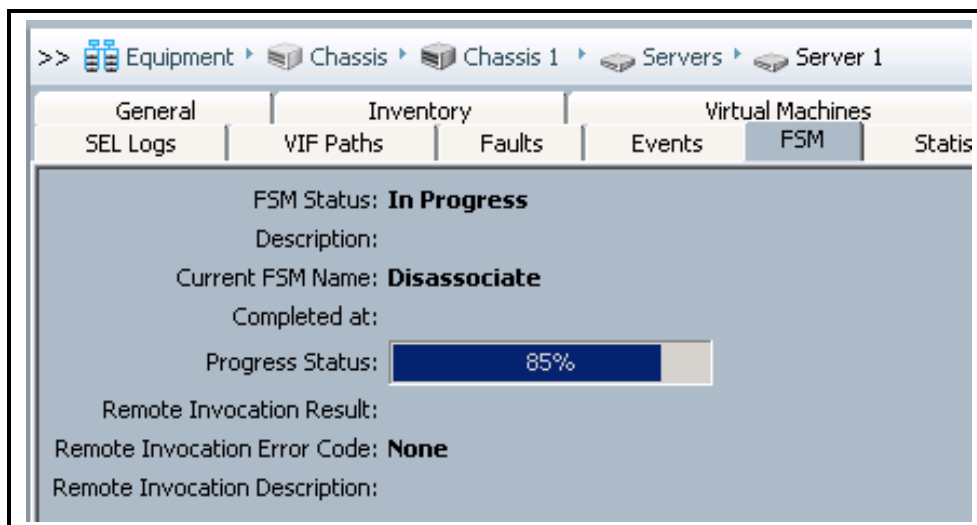
- Step 1** Navigate to **Service Profiles->root->Sub-Organizations-> Pod#**.
- Step 2** Click your Service Profile with the name **Pod#-Service-Profile-1** in the Navigation pane.
- Step 3** In the Content pane, click **Disassociate Service Profile**. (you may have to scroll down)



- Step 4** Click the **Yes** button to confirm disassociation.
- Step 5** The Service Profile will immediately report that it is unassociated. Because the service profile is no longer attached to a blade server, you will now need to switch to the **Equipment** tab to watch the disassociation process.
- Step 6** Navigate to **Equipment->Chassis->Chassis 1->Servers->Server P** (where P = your pod number). Note your server is in “config” again.



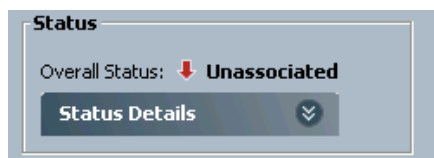
Step 7 Click the server in the Navigation pane, and then click the **FSM** tab in the Content pane.



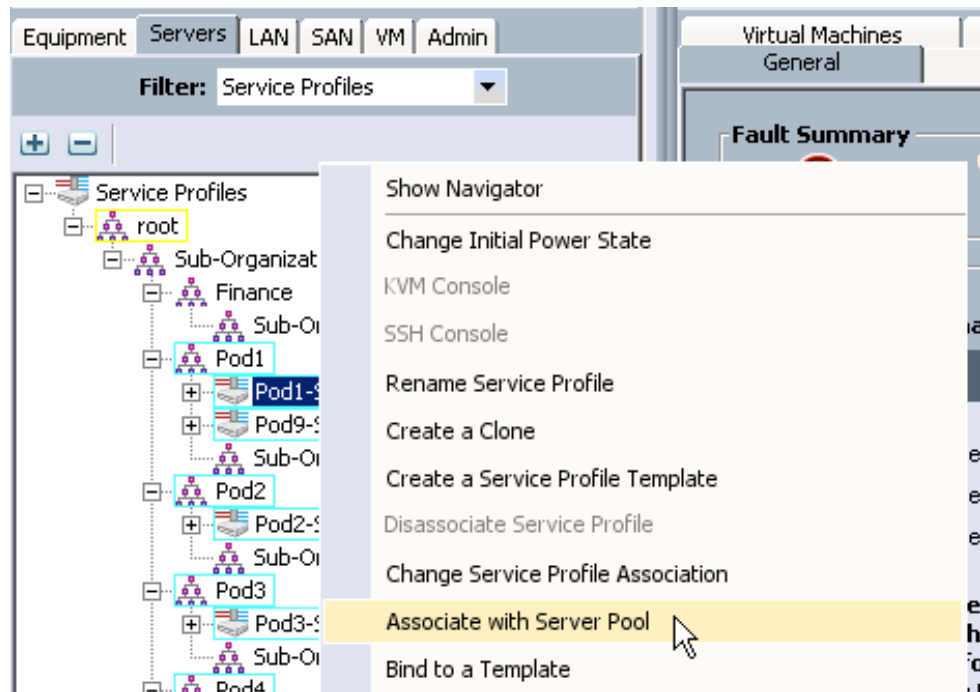
Step 8 You will view the process of disassociation. It should take 1 to 2 minutes.

Step 9 Once the Progress Status indicator reaches 100%, the Status of Last Operation should read Disassociate Success.

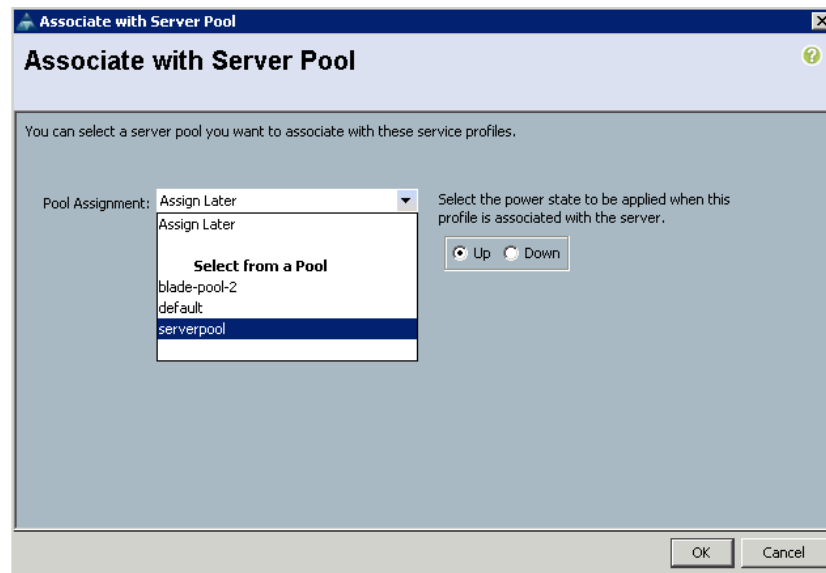
Step 10 Note in the general tab your server now is “Unassociated”.



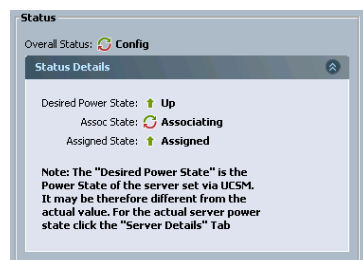
- Step 11** Now that the service profile is no longer associated, return to the service profile in the Servers tab.
- Step 12** Select Service Profile “Pod#-SP” and right-click.



- Step 13** Select “Associate with Server Pool”



- Step 14** Select Pool “serverpool” and click OK to assign.
- Step 15** Note the service profile status changes to “config” Your server is now reconfigured to support a totally different environment.



Activity Verification

You have completed this task when you attain these results:

- Successfully generate a service profile from a template and observe the association process.
- Successfully disassociate your service profile and observe the disassociation process in the FSM tab.