

Lab Guide

Overview

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

Outline

This guide includes these activities:

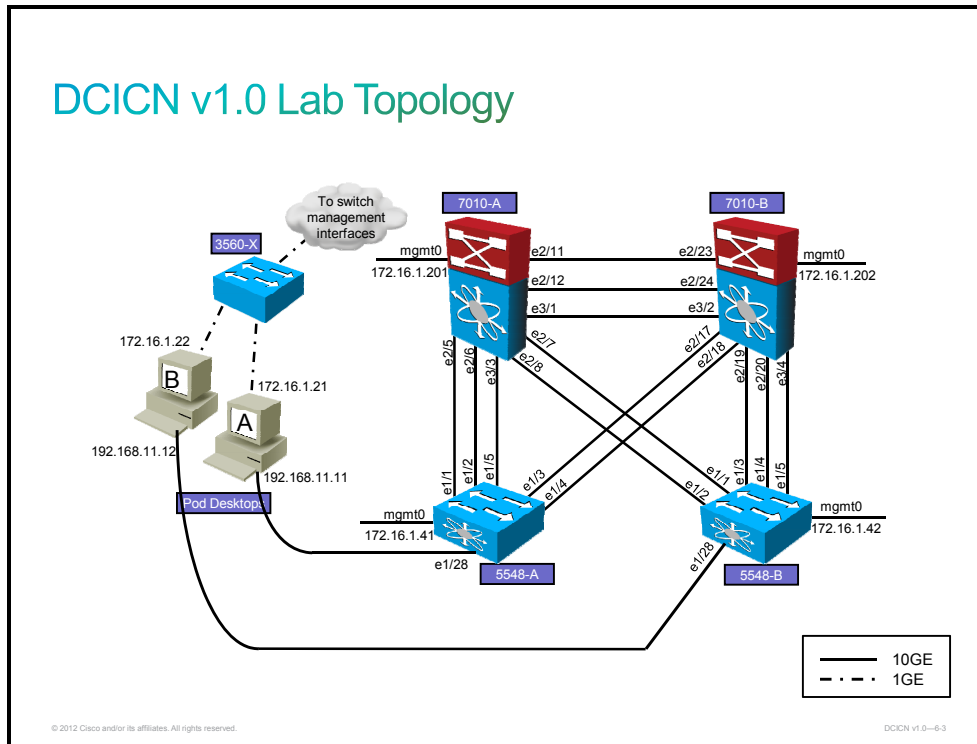
- Lab 1-1: Using Windows Applications as Network Tools
- Lab 1-2: Observing the TCP Three-Way Handshake
- Lab 1-3: Observing Extended PC Network Information
- Lab 2-1: Connecting to Cisco Nexus Switches
- Lab 2-2: Configuring Cisco Nexus Switches
- Lab 2-3: Configuring VLANs and Trunks
- Lab 2-4: Verifying and Configuring Spanning Tree
- Lab 2-5: Configuring EtherChannel
- Lab 3-1: Converting Decimal to Binary and Binary to Decimal
- Lab 3-2: Classifying Network Addressing
- Lab 3-3: Computing Usable Subnetworks and Hosts
- Lab 3-4: Calculating Subnet Masks
- Lab 4-1: Configuring Multilayer Switching
- Answer Key

Job Aids

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

Lab Topology Diagram

The following figure shows the physical topology of the lab that is used in this course.



Lab Connections

The following table lists the physical connections between the devices that are used in this course.

From		To	
Device	Interface	Device	Interface
N7K Prod-A	Ethernet 2/5	N5K-A	Ethernet 1/1
	Ethernet 2/6	N5K-A	Ethernet 1/2
	Ethernet 2/7	N5K-B	Ethernet 1/1
	Ethernet 2/8	N5K-B	Ethernet 1/2
	Ethernet 2/11	N7K Prod-B	Ethernet 2/23
	Ethernet 2/12	N7K Prod-B	Ethernet 2/24
	Ethernet 3/1	N7K Prod-B	Ethernet 3/2
	Ethernet 3/3	N5K-A	Ethernet 1/5
Device	Interface	Device	Interface
N7K Prod-B	Ethernet 2/17	N5K-A	Ethernet 1/3
	Ethernet 2/18	N5K-A	Ethernet 1/4
	Ethernet 2/19	N5K-B	Ethernet 1/3
	Ethernet 2/20	N5K-B	Ethernet 1/4
	Ethernet 2/23	N7K Prod-A	Ethernet 2/11
	Ethernet 2/24	N7K Prod-A	Ethernet 2/12
	Ethernet 3/2	N7K Prod-A	Ethernet 3/1
	Ethernet 3/4	N5K-B	Ethernet 1/5
Device	Interface	Device	Interface
N5K-A	Ethernet 1/1	N7K Prod-A	Ethernet 2/5
	Ethernet 1/2	N7K Prod-A	Ethernet 2/6
	Ethernet 1/3	N7K Prod-B	Ethernet 2/17
	Ethernet 1/4	N7K Prod-B	Ethernet 2/18
	Ethernet 1/5	N7K Prod-A	Ethernet 3/3
	Ethernet 1/28	PC A	Lab2
Device	Interface	Device	Interface
N5K-B	Ethernet 1/1	N7K Prod-A	Ethernet 2/7
	Ethernet 1/2	N7K Prod-A	Ethernet 2/8
	Ethernet 1/3	N7K Prod-B	Ethernet 2/19
	Ethernet 1/4	N7K Prod-B	Ethernet 2/20
	Ethernet 1/5	N7K Prod-B	Ethernet 3/4
	Ethernet 1/28	PC B	Lab2

Lab IP Address Plan

The following table lists the IP addresses that are configured on the devices in this course.

Device	Interface	IP Address	Prefix Length	Default Gateway
N7K Prod-A	Mgmt0	172.16.1.201	/24	172.16.1.1
N7K Prod-B	Mgmt0	172.16.1.202	/24	172.16.1.1
N5K-A	Mgmt0	172.16.1.41	/24	172.16.1.1
N5K-B	Mgmt0	172.16.1.42	/24	172.16.1.1
Pod 1 PC	Mgmt NIC	172.16.1.21	/24	172.16.1.1
Pod 2 PC	Mgmt NIC	172.16.1.22	/24	172.16.1.1
Pod 3 PC	Mgmt NIC	172.16.1.23	/24	172.16.1.1
Pod 4 PC	Mgmt NIC	172.16.1.24	/24	172.16.1.1
Pod 1 PC	Lab	172.17.1.21	/24	
Pod 2 PC	Lab	172.17.1.22	/24	
Pod 3 PC	Lab	172.17.1.23	/24	
Pod 4 PC	Lab	172.17.1.24	/24	
Pod 5 PC	Lab	172.17.1.25	/24	
Pod 6 PC	Lab	172.17.1.26	/24	
Pod 7 PC	Lab	172.17.1.27	/24	
Pod 8 PC	Lab	172.17.1.28	/24	

Lab 1-1: Using Windows Applications as Network Tools

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

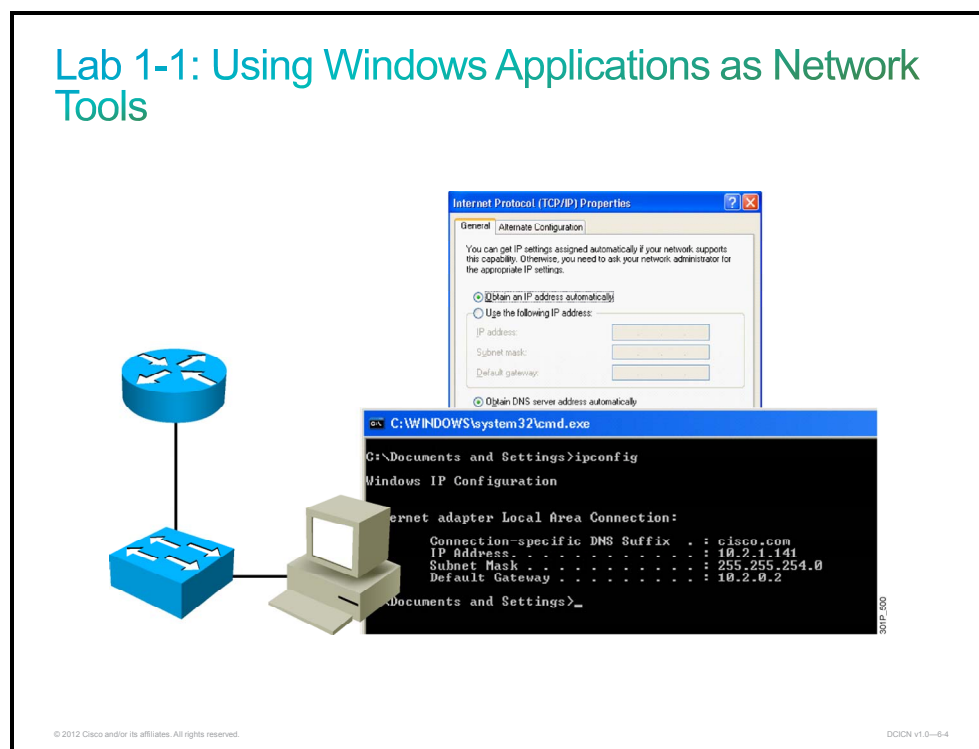
Activity Objective

In this activity, you will be able to use Windows applications and commands to investigate the IP configuration of your PC and your local network. After completing this activity, you will be able to meet these objectives:

- Using the Windows command **ipconfig**, determine the current network addressing information of a PC.
- Using the Windows command **ping**, determine test connectivity to the default gateway router.
- Using the Windows command **arp -a**, view the ARP table of the local PC and determine the association between the IP address and the MAC address of the default gateway.

Visual Objective

The following figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- PC connected to a functioning network, with connectivity to the Internet

Command List

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

Command	Description
<code>arp -a</code>	Obtains the output of the ARP table. Entries to the ARP table are removed after 5 minutes of inactivity.
<code>ipconfig</code>	Outputs the current IP address, network mask, and default gateway IP address
<code>ping</code>	Tests IP connectivity between hosts

Task 1: Obtain the Current IP Address Information

To obtain the current IP address information, use the Windows **ipconfig** command. First, you need to open a command window to access Windows commands.

Activity Procedure

Complete these steps:

Step 1 On the Windows desktop, click **Start**.

Step 2 Choose **Run**, and enter **cmd** in the Run window dialog box. Click **OK** to continue.

Step 3 At the command window prompt, enter **ipconfig**.

Your output should resemble one of the following four examples.

Nonworking example 1: The output indicates no connectivity. The Ethernet cable is probably not physically connected.

```
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
```

Nonworking example 2: The output indicates that the PC is waiting to obtain its IP address information automatically. This will be a transient output; it will either successfully get an address or retry the **ipconfig** command periodically until it changes to one of the following examples.

```
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :
```

Nonworking example 3: The output indicates that the PC network adapter was unable to obtain an IP address automatically, so the PC will use a generated link-local address. Getting a link-local address might seem like success, but it really indicates that there is no connectivity to an IP address server. This address will not be useful for network connectivity. If you see an IP address beginning with 169.254.x.x, you do not have a valid address.

```
C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.249.221
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
```

Working example 1: The output indicates that the PC either has a preconfigured IP address or that it successfully obtained its IP address automatically. Your IP address, subnet mask, or default gateway will most likely be different from what is shown.

```
C:\Documents and Settings>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix  . : cisco.com
IP Address. . . . . : 192.168.1.105
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Activity Verification

You have completed this task when you attain this result:

- You obtained valid IP address information from the **ipconfig** command.

Step 4 If you have a problem, ask your instructor for assistance. Continue only if you have a valid IP address.

Step 5 Write the values that you obtained from the **ipconfig** command in the following spaces, because you will be using them in later tasks.

PC IP address: _____

IP default gateway address: _____

Note There might be more than one network adapter available on a PC. The output of the **ipconfig** command will show a different IP configuration for each network adapter.

Task 2: View the Network Properties of the PC Ethernet Adapter

In this task you will use the Windows operating system Network Properties dialog window. You will only view the configuration, but you would follow the same process if you needed to modify or supply new IP network address values.

Activity Procedure

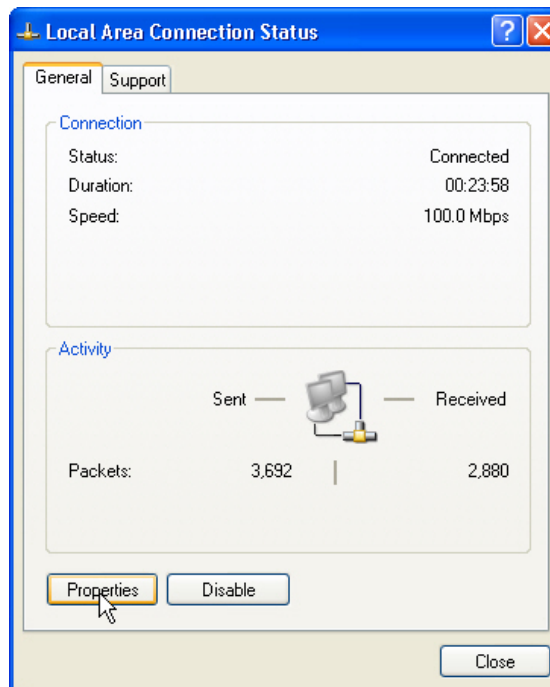
Complete these steps:

- Step 1** On the Windows desktop, double-click the **Local Area Connection** shortcut on your desktop. If there is no shortcut on the desktop, use the **Network Connections** icon in the Control Panel.

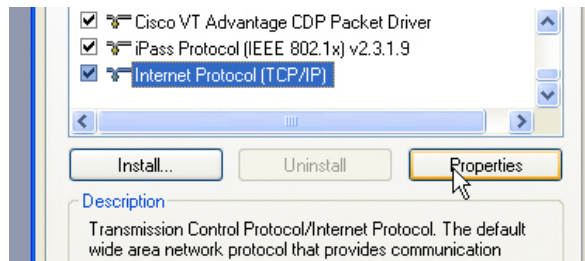


Note The icon can also be found on the Network Connections dialog box on the Windows desktop or in the Control Panel.

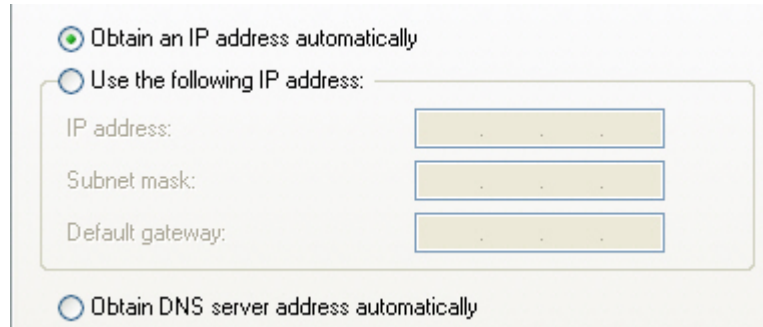
- Step 2** In the Local Area Connection status window, click the **Properties** button.



- Step 3** In the Local Area Connection Properties window, scroll to the bottom and click **Internet Protocol (TCP/IP)** to highlight it. Then click the **Properties** button.

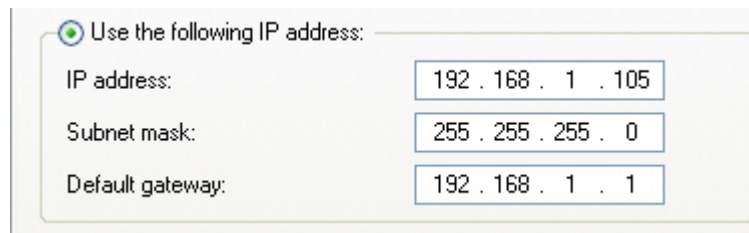


- Step 4** In the Internet Protocol (TCP/IP) Properties window, you might find that the Obtain an IP Address Automatically radio button is already set, as shown here.



- Step 5** Alternatively, you might see that the Use the Following IP Address radio button is chosen, and that the fields are configured with IP address information matching the output that you obtained from the **ipconfig** command.

Note This is an example only. Do *not* change your settings.



- Step 6** Close all the dialog boxes and return to the Windows desktop.

Activity Verification

You have completed this task when you attain these results:

- You used the Windows TCP/IP properties to view the current configuration for the local area connection.
- The values that were set in the TCP/IP properties were consistent with the information that you obtained using the **ipconfig** command.

Task 3: Test Connectivity to the Default Gateway Router

The Windows **ping** command allows you to test the connectivity of the network. Its output demonstrates success or failure, and gives an indication of the round-trip time taken.

Activity Procedure

Complete these steps:

- Step 1** At the command window prompt, enter **ping** followed by the address of your default gateway that you obtained in Task 1.
- Step 2** The first of the two following examples is an unsuccessful **ping**. If you get this output, ask your instructor for assistance.

Nonworking example: The following output indicates that no reply was received from the target IP address.

```
C:\Documents and Settings>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Working example: The following output indicates successful receipt of replies from the target IP address.

```
C:\Documents and Settings>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Note	Notice that, by default, the Windows ping command sends four ping packets (ICMP echo requests).
-------------	--

Activity Verification

You have completed this task when you attain these results:

- You used the Windows **ping** command to test the connectivity to your default gateway router.
- The round-trip time should be less than 10 ms.

Task 4: View the ARP Bindings of the IP Address to the MAC Address

The Windows **arp -a** command allows you to view the binding of the logical IP address and the physical MAC address.

Activity Procedure

Complete these steps:

Step 1 At the command window prompt, enter **arp -a**. It is necessary to use the **-a** parameter to receive the output of the ARP table.

```
C:\Documents and Settings>arp -a
```

```
Interface: 192.168.1.125 --- 0x2
    Internet Address      Physical Address      Type
    192.168.1.1           00-00-0c-07-ac-04     dynamic
```

Your output should resemble the output in Step 1. If you did not receive any values, the ARP table might have timed out the entry, and you need to repeat Step 1.

Step 2 Close your command window by entering **exit** at the prompt.

Activity Verification

You have completed this task when you attain this result:

- You were able to view the binding of the IP address to the MAC address.

Lab 1-2: Observing the TCP Three-Way Handshake

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

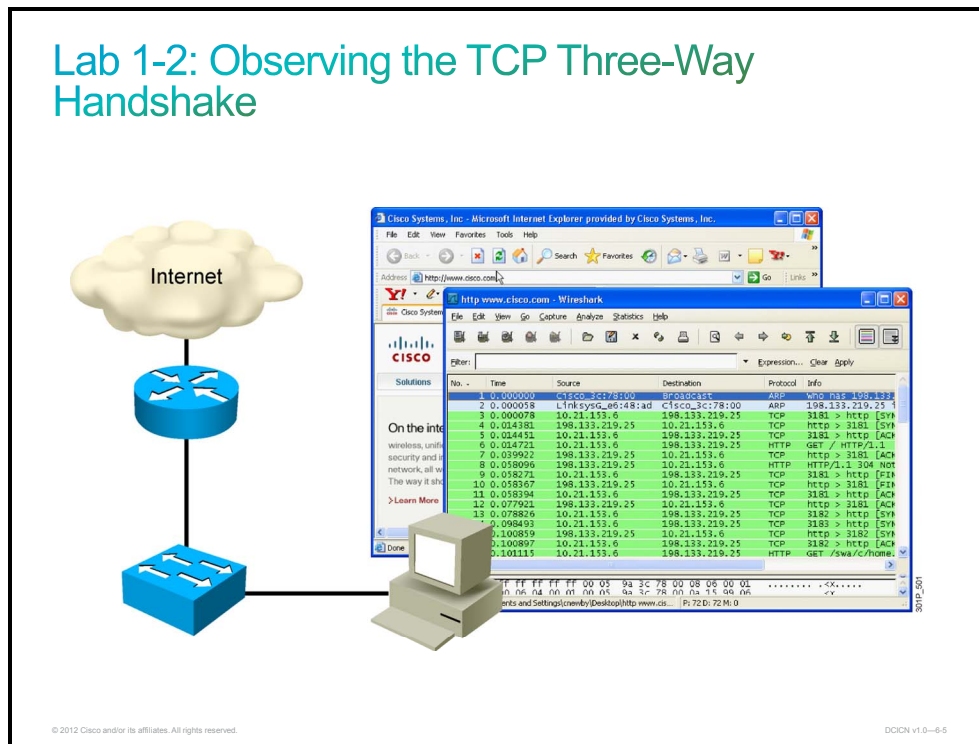
Activity Objective

In this activity, you will use a packet sniffer application to view the TCP initial three-way handshake. After completing this activity, you will be able to meet these objectives:

- Start the packet sniffer application, to monitor the appropriate Ethernet interface for recording the packet flow.
- Generate a TCP connection using a web browser.
- Observe the initial packets of the TCP flow, especially the SYN packet, the SYN-ACK packet, and finally the ACK packet.

Visual Objective

The following figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- PC with access to the Internet
- The Wireshark packet sniffer Windows application
- Student Guide Module 1, Lesson 1

Application List

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

PC Applications

Windows Application	Description
Internet Explorer	A web browser
Wireshark	A packet sniffer application

Caution Installing or using a packet sniffer application may be considered a breach of a security policy, leading to serious legal and financial consequences. It is recommended that before downloading, installing, or running such an application, you obtain permission to do so.

Job Aids

There are no job aids for this lab.

Task 1: Prepare the Sniffer Software to Capture a TCP Flow

In this task, you will open the Wireshark application and apply the packet capture to your active Ethernet interface.

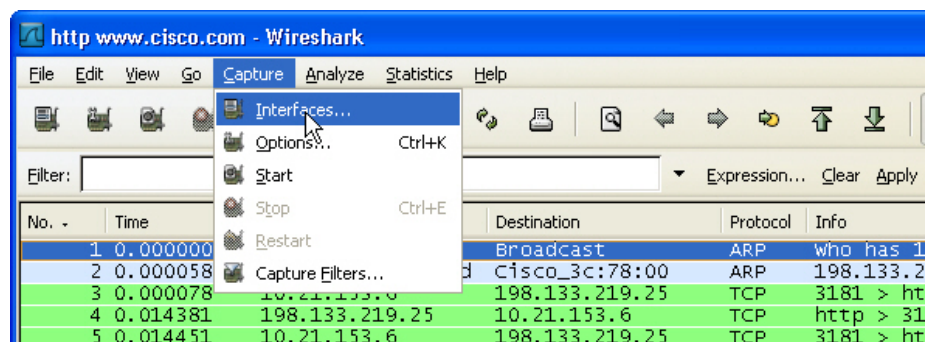
Activity Procedure

Complete these steps:

Step 1 Open the Wireshark application by double-clicking its icon on your desktop.

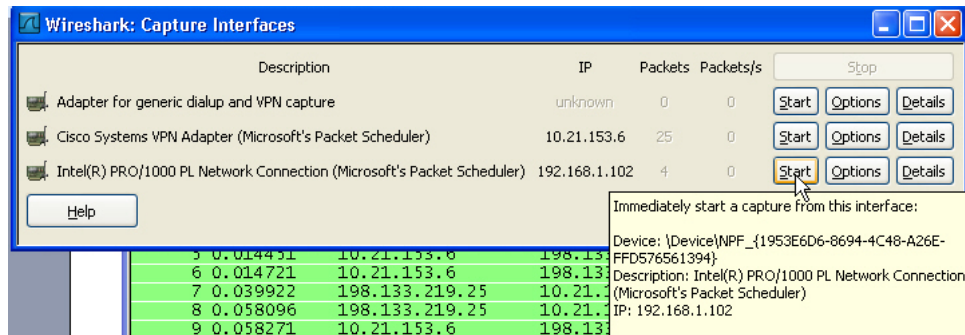


Step 2 Choose **Capture**, and then choose **Interfaces** from the drop-down menu.

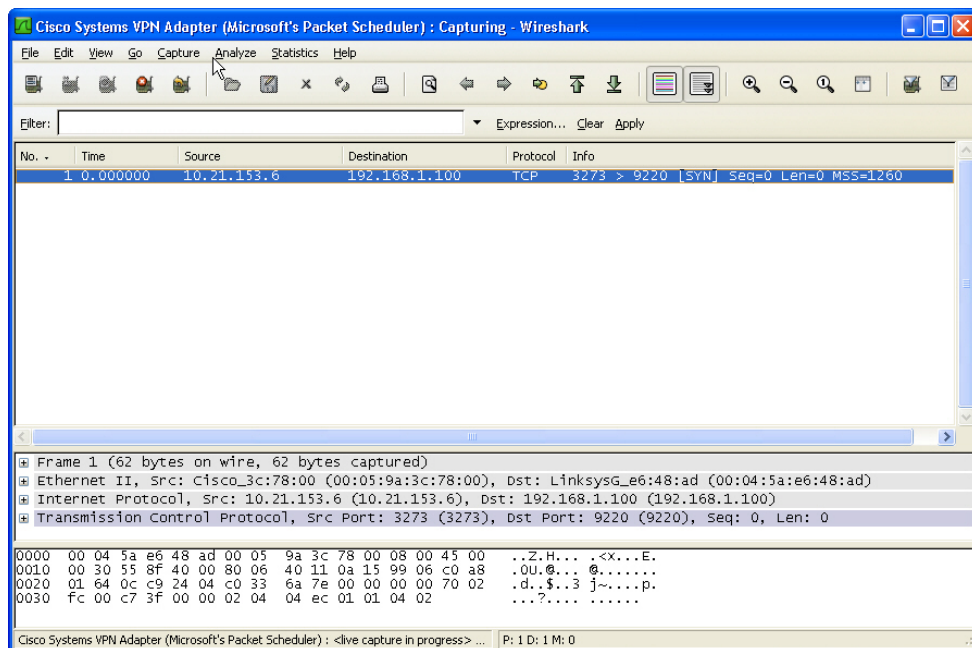


Step 3 Choose your local network Ethernet interface adapter. If this process is unclear, ask the instructor for assistance. Click the **Start** button that is associated with the chosen interface. Make a note of the IP address associated with your chosen Ethernet adapter, because it will be the source IP address that you will look for when you are examining captured packets.

Note your IP address here: _____



Note The capture windows are now active.



You will look more closely at the capture windows after you have captured the TCP flow.

You might see some packets filling up the uppermost window. This will depend on the level of background activity on the network to which you are attached.

Activity Verification

You have completed this task when you attain this result:

- You have an open packet-capture window, associated with the Ethernet interface connected to your default router.

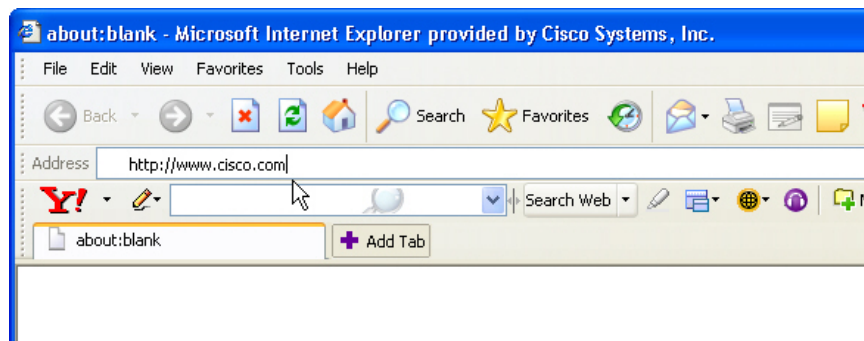
Task 2: Generate the TCP Flow to Be Captured

You will use the Internet Explorer web browser to connect to a web server. The actual web server that is chosen is not important. The HTTP data that is used to carry web page text and graphics uses TCP transport for reliability. The alternative best-effort protocol is UDP. You are interested only in the initial exchange that is performed by TCP to set up the connection.

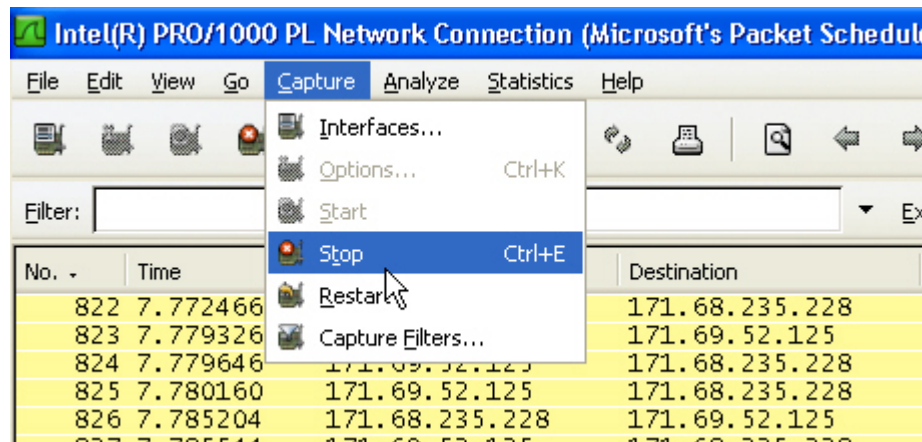
Activity Procedure

Complete these steps:

- Step 1** On the PC desktop, double-click the **Internet Explorer** icon to launch the web browser.
- Step 2** Enter the destination name or address. The instructor might provide you with a name or address different from `www.cisco.com`. If so, write down this information here:



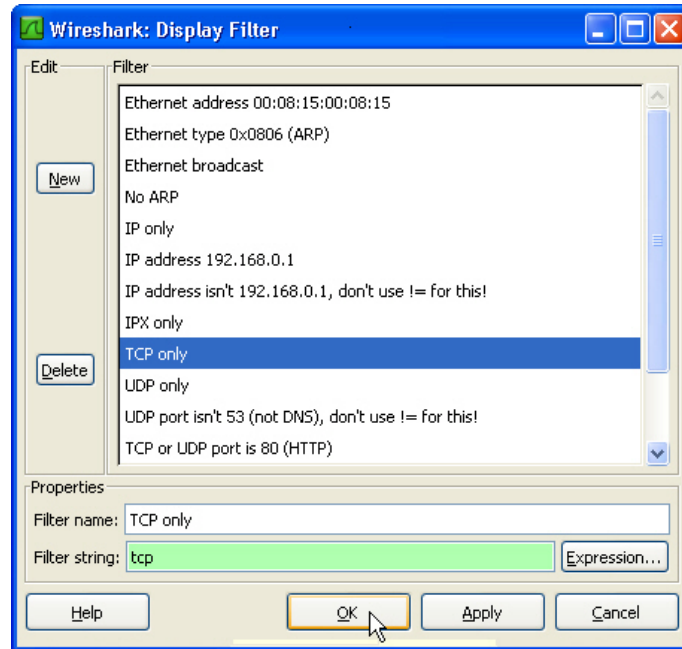
- Step 3** Return to the already open Wireshark application and choose **Capture > Stop** from the drop-down menu.



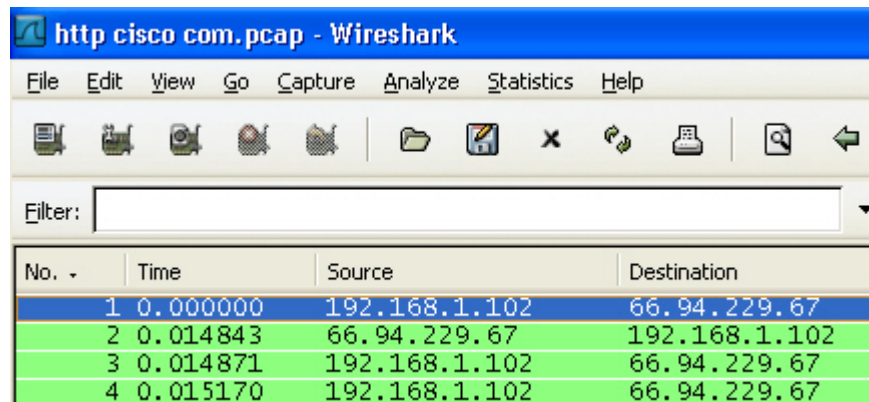
If you have many TCP packets that are unrelated to your TCP connection, you might need to use the filter capability of Wireshark.

- Step 4** To use a preconfigured filter, click the **Analyze** tab. Then click **Display Filters**.

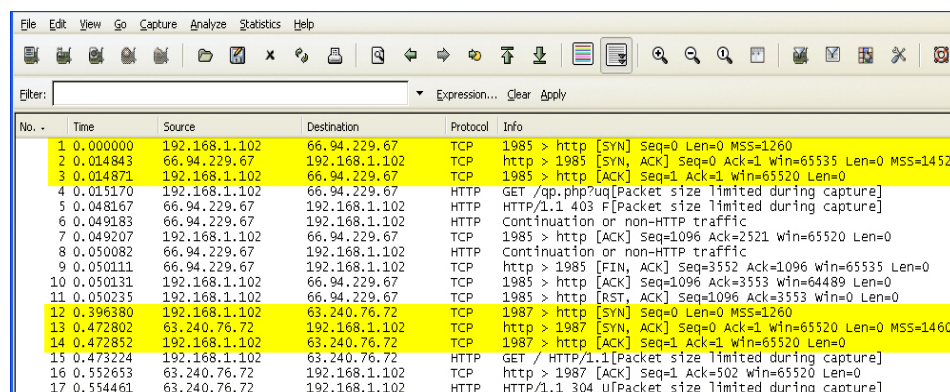
Step 5 In the **Wireshark: Display Filter** window, click **TCP only** and then click the **OK** button.



Step 6 In the top window of the Wireshark application, use the scroll bar to place the first captured TCP packet at the top of the window. This should be the first packet in the flow.

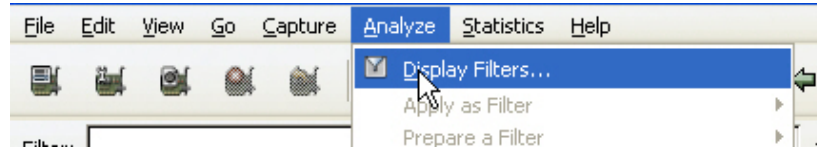


Step 7 Observe the Info column of the captured packets in the top window. Look for three packets similar to those shown here. Two groups of three packets are highlighted here as an example.



Step 8 Note the first packet number in the sequence that you have identified in your capture window. There is no need to find more than one sequence of packets. In the previous example, packet 1 and packet 12 both begin a sequence. You will observe the contents of these packets in detail in the next task.

Write down the packet number of the first packet in the TCP sequence here:



Step 9 To filter another protocol, return to Step 4 in this task.

Activity Verification

You have completed this task when you attain these results:

- You have identified that you have captured the packet sequence described in Step 8.
- You have noted the first packet in the sequence to be inspected in detail.

Task 3: Inspect the TCP Initialization Sequence

You will use the Packet Details window of the Wireshark application to view the TCP parameters exchanged during the initial startup sequence. This exchange is often referred to as the three-way handshake.

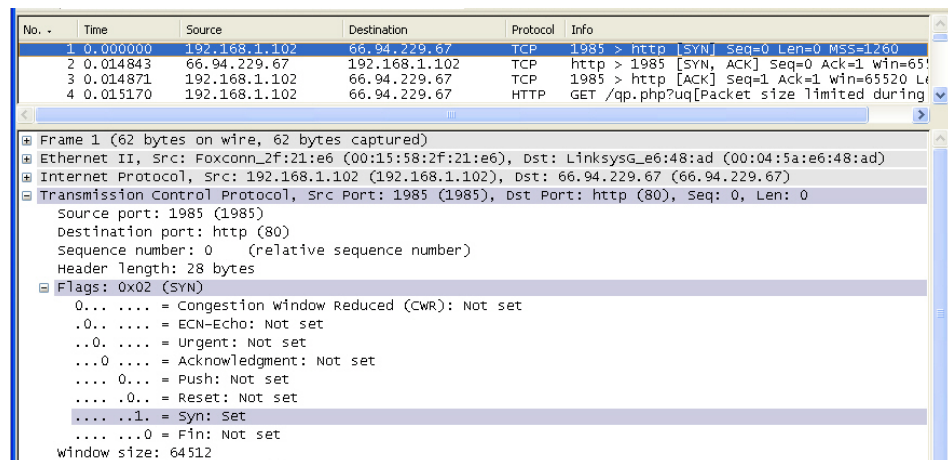
Activity Procedure

Complete these steps:

- Step 1** In the top window of the Wireshark application, click anywhere on the line containing the first packet that was identified in the previous task. This will highlight the line and make the two lower windows display the decoded information from that packet.

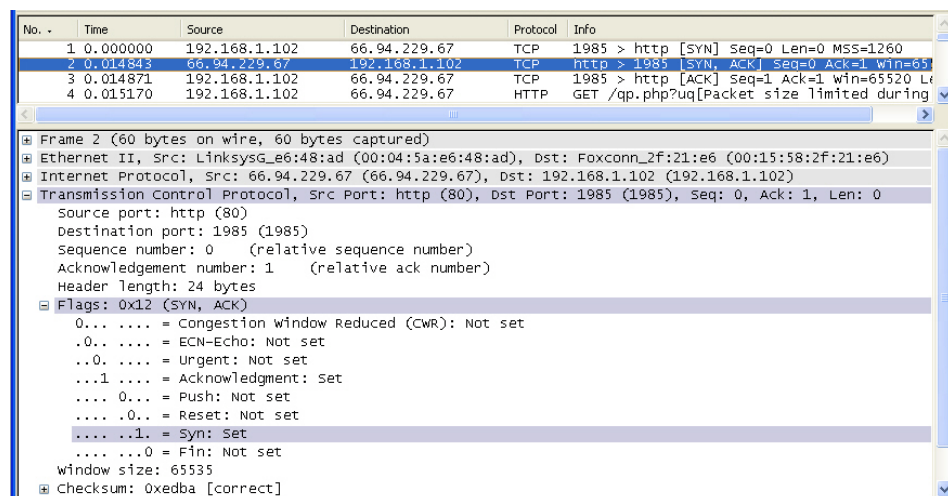
Note In the example that follows, the Wireshark windows were adjusted to allow the information to be viewed in a compact size. The second window contains the detailed decoding of the packet.

Note Clicking the + icon at the left expands the view of the TCP information. The view is contracted by clicking the – icon.



In this example, the forward sequence number is set to 0, and the SYN bit is set to 1 in the Flags field.

- Step 2** In the top window, click the next packet in the sequence. The detailed information changes to match the new values.



In the reply packet, the backward sequence number is set to 0, and the acknowledgment number is set to 1. In the Flags field, the acknowledgment bit and the SYN bit are set to 1.

Step 3 In the top window, click the next packet in the sequence. The detailed information changes to match the new values.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.102	66.94.229.67	TCP	1985 > http [SYN] Seq=0 Len=0 MSS=1260
2	0.014843	66.94.229.67	192.168.1.102	TCP	http > 1985 [SYN, ACK] Seq=0 Ack=1 win=65520
3	0.014871	192.168.1.102	66.94.229.67	TCP	1985 > http [ACK] Seq=1 Ack=1 win=65520
4	0.015170	192.168.1.102	66.94.229.67	HTTP	GET /qp.php?uq[Packet size limited during

Frame 3 (54 bytes on wire (54 bytes captured))
Ethernet II, Src: Foxconn_2f:21:e6 (00:15:58:2f:21:e6), Dst: LinksysG_e6:48:ad (00:04:5a:e6:48:ad)
Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 66.94.229.67 (66.94.229.67)
Transmission Control Protocol, Src Port: 1985 (1985), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
Source port: 1985 (1985)
Destination port: http (80)
Sequence number: 1 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x10 (ACK)
0... .. = Congestion window Reduced (CWR): Not set
.0.. .. = ECN-Echo: Not set
.0.. .. = Urgent: Not set
...1 .. = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
.... ..0 = Syn: Not set
.... ...0 = Fin: Not set
Window size: 65520
Checksum: 0x057f [correct]

In the third and final packet in the exchange, the forward sequence number is now set to 1. The acknowledgment number is set to 1. In the Flags field, only the acknowledgment bit is set to 1. At this point, the TCP connection is said to be established, because both ends have synchronized their sequence and acknowledgment numbers, as well as other parameters.

Step 4 Close the Wireshark application and all other open windows.

Activity Verification

You have completed this task when you attain this result:

- You have selected and decoded your three identified captured packets, and the values match those shown and discussed in the examples within the task.

Lab 1-3: Observing Extended PC Network Information

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

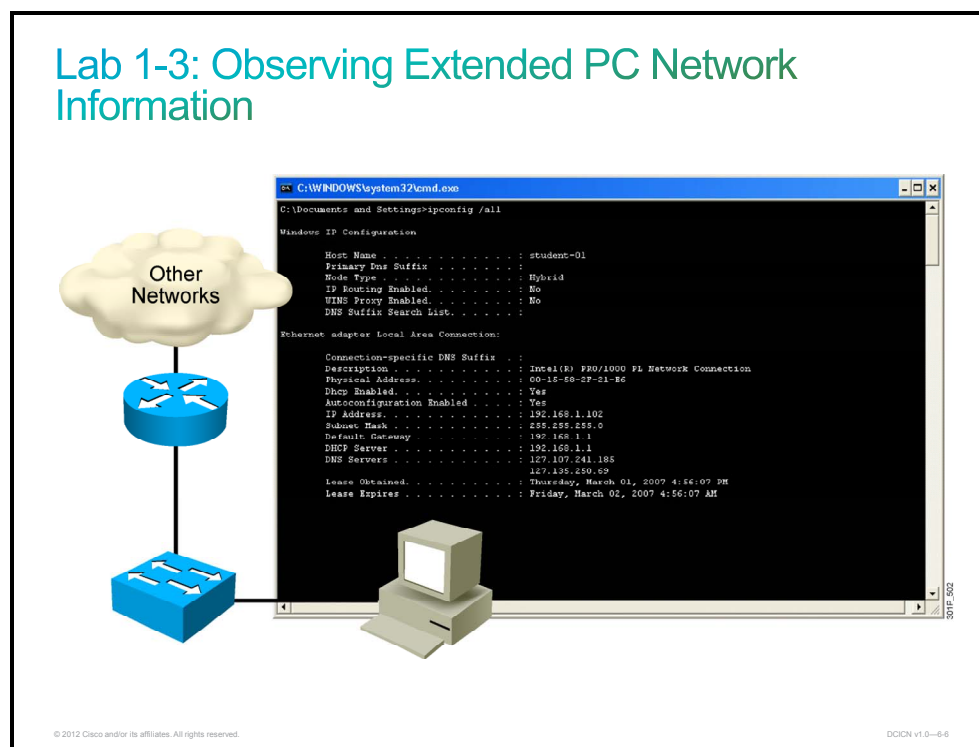
Activity Objective

In this activity, you will use PC tools to gather network-related information. After completing this activity, you will be able to meet these objectives:

- Using the Windows **ipconfig /all** command, determine the IP addresses of the DNS servers that are available to your PC.
- Using the IP address of one of the DNS servers from Task 1, test the connectivity to the DNS servers by using the Windows **ping** command.
- Using the Windows **tracert-d** command, obtain the IP addresses of the routers that were traversed to reach the DNS server that was tested in Task 2.

Visual Objective

This figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- PC connected to a functioning network, with connectivity to the Internet

Command List

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

Windows Commands

Command	Description
<code>ipconfig /all</code>	Outputs all the current IP network information
<code>ping</code>	Tests IP connectivity between hosts
<code>tracert /d ip Address</code>	Displays the IP address of the router at each hop as a packet traverses the network toward the destination IP address

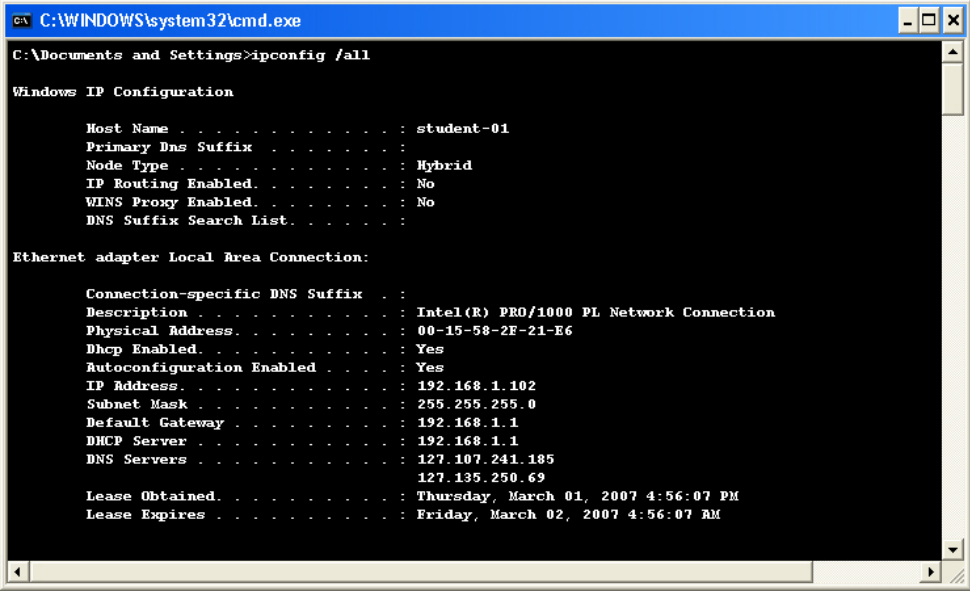
Task 1: Obtain the Complete Current IP Addressing Information

To obtain the complete current IP address information on your PC, it is necessary to use the Windows **ipconfig /all** command. To access Windows commands, it is necessary to open a command window.

Activity Procedure

Complete these steps:

- Step 1** On the Windows desktop, click **Start**.
- Step 2** Choose **Run**, and enter **cmd** in the Run window dialog box. Click **OK** to continue.
- Step 3** At the command window prompt, enter **ipconfig /all**. The **/all** parameter is used to show the complete output.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : student-01
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Intel(R) PRO/1000 PL Network Connection
    Physical Address. . . . . : 00-15-58-2F-21-E6
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 192.168.1.102
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 127.107.241.185
                           127.135.250.69
    Lease Obtained. . . . . : Thursday, March 01, 2007 4:56:07 PM
    Lease Expires . . . . . : Friday, March 02, 2007 4:56:07 AM
```

You will see from your own output that some extra, useful information is now visible.

From this output, note the IP address of the first DNS server here:

Activity Verification

You have completed this task when you attain this result:

- You have obtained the IP address of a DNS server from the output of the **ipconfig /all** command on your PC.

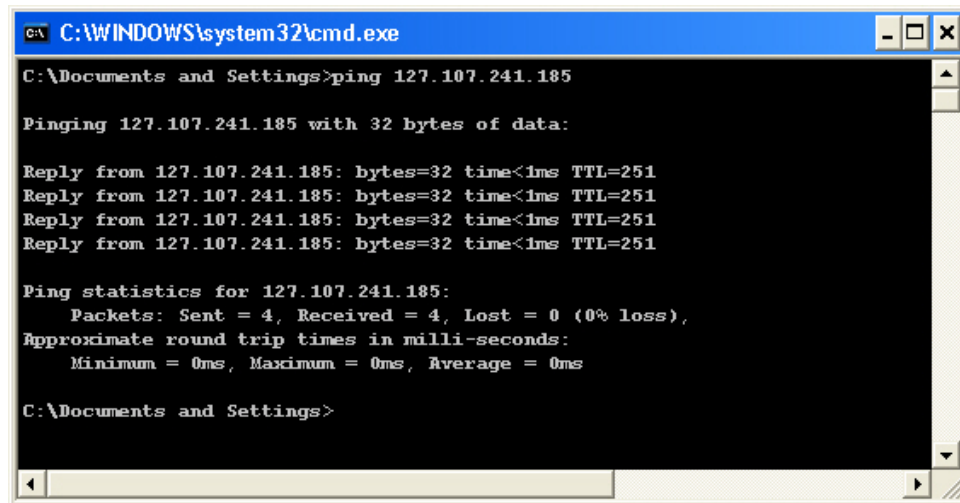
Task 2: Test Connectivity to the DNS Server

In this task, you will use the **ping** command to test the connectivity.

Activity Procedure

Complete these steps:

- Step 1** At the command window prompt, enter **ping DNS IP Address**. Your output should be similar to the example here, which uses a fictitious IP address.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>ping 127.107.241.185

Pinging 127.107.241.185 with 32 bytes of data:

Reply from 127.107.241.185: bytes=32 time<1ms TTL=251
Reply from 127.107.241.185: bytes=32 time<1ms TTL=251
Reply from 127.107.241.185: bytes=32 time<1ms TTL=251
Reply from 127.107.241.185: bytes=32 time<1ms TTL=251

Ping statistics for 127.107.241.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings>
```

- Step 2** A successful ping indicates that both of the packets are being received and that the return packets are being routed back to your PC successfully.
- Step 3** The implications of an unsuccessful ping sequence require more investigation. If it is assumed that the ping attempts are unsuccessful, the next step is to try to see where in the network the problem is occurring.

Activity Verification

You have completed this task when you attain this result:

- You have used the Windows **ping** command to successfully test connectivity to the IP address of the DNS server that you noted in Task 1.

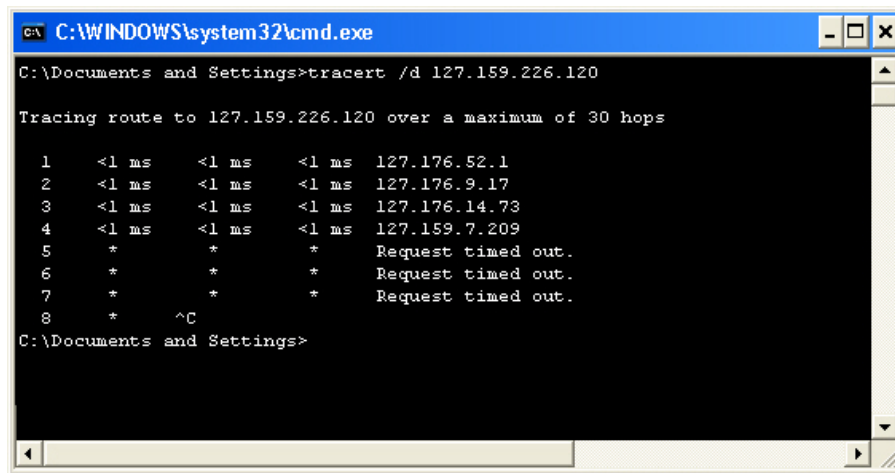
Task 3: Tracing Connectivity to the DNS Server

In this task, you will use the **tracert /d** command to trace the path to the DNS server that you noted in the previous task. The **/d** parameter in the command stops the attempt to use DNS to look up the IP addresses that were discovered along the path and put them in the output. In this scenario, DNS is not working, so attempting a lookup would waste time. You will use **tracert** without **/d** to see what the output would look like when DNS is able to resolve some or all of the IP addresses.

Activity Procedure

Complete these steps:

This is an example of an unsuccessful trace attempt to the DNS server. The sequence would have continued until 30 hops had been tried. You will see that pressing **Ctrl-C** was used to terminate the command earlier than the default number.

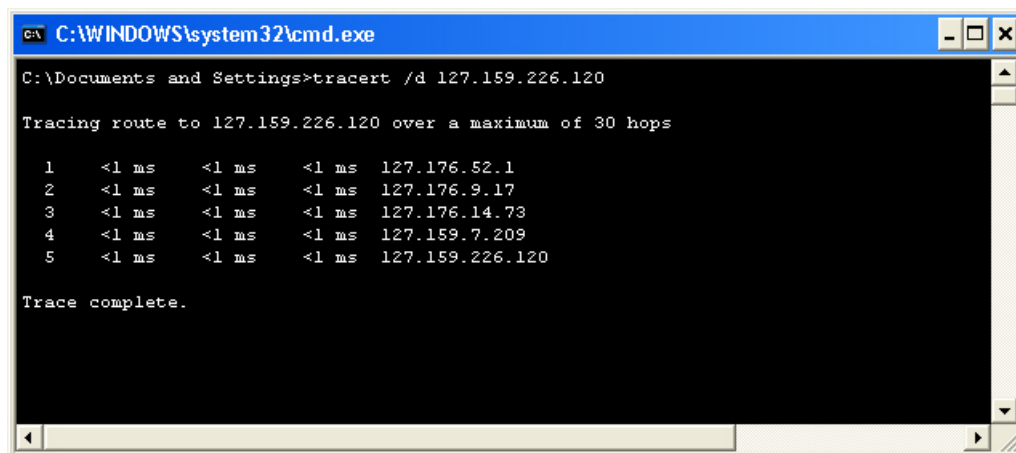


```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>tracert /d 127.159.226.120

Tracing route to 127.159.226.120 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  127.176.52.1
  2  <1 ms  <1 ms  <1 ms  127.176.9.17
  3  <1 ms  <1 ms  <1 ms  127.176.14.73
  4  <1 ms  <1 ms  <1 ms  127.159.7.209
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
      ^C
C:\Documents and Settings>
```

Step 1 At the command window prompt, enter **tracert /d DNS IP Address**. Your output should be similar to the example here, which uses fictitious IP addresses.



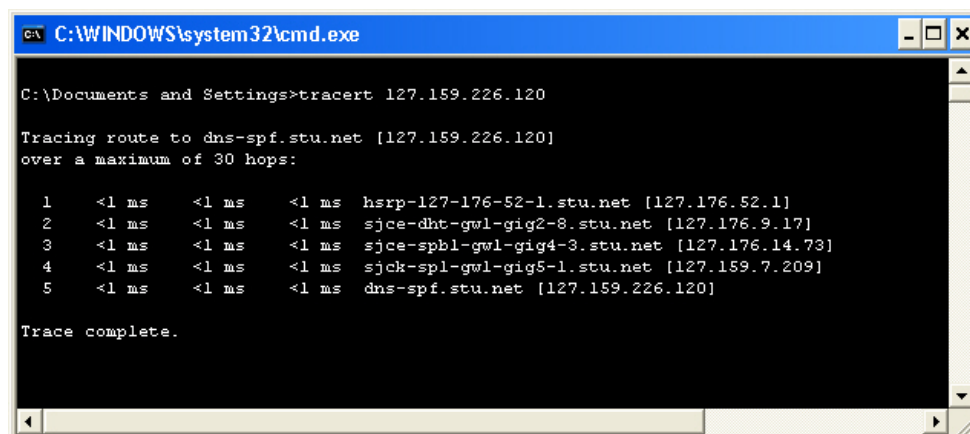
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>tracert /d 127.159.226.120

Tracing route to 127.159.226.120 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  127.176.52.1
  2  <1 ms  <1 ms  <1 ms  127.176.9.17
  3  <1 ms  <1 ms  <1 ms  127.176.14.73
  4  <1 ms  <1 ms  <1 ms  127.159.7.209
  5  <1 ms  <1 ms  <1 ms  127.159.226.120

Trace complete.
```

Now that you have seen that the route to the DNS server is working, use the **tracert** command without the **/d** parameter to see what the output looks like when symbolic names are available. Your output should be similar to the example here, which uses fictitious IP addresses.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings>tracert 127.159.226.120

Tracing route to dns-spf.stu.net [127.159.226.120]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  hsrp-127-176-52-1.stu.net [127.176.52.1]
  2  <1 ms  <1 ms  <1 ms  sjce-dht-gw1-gig2-8.stu.net [127.176.9.17]
  3  <1 ms  <1 ms  <1 ms  sjce-spb1-gw1-gig4-3.stu.net [127.176.14.73]
  4  <1 ms  <1 ms  <1 ms  sjck-spl-gw1-gig5-1.stu.net [127.159.7.209]
  5  <1 ms  <1 ms  <1 ms  dns-spf.stu.net [127.159.226.120]

Trace complete.
```

Step 2 Close the command window.

Activity Verification

You have completed this task when you attain these results:

- You have used the **tracert /d** command on your PC to suppress DNS lookup during the trace to the destination address.
- You have used the **tracert** command without the **/d** parameter on your PC to display the symbolic names that were associated with specific IP addresses that were discovered during the trace to the destination address.

Lab 2-1: Connecting to Cisco Nexus Switches

In this lab, you will use an SSH application to connect to the Cisco Nexus. The instructor will have loaded base configurations on the switches to provide basic connectivity.

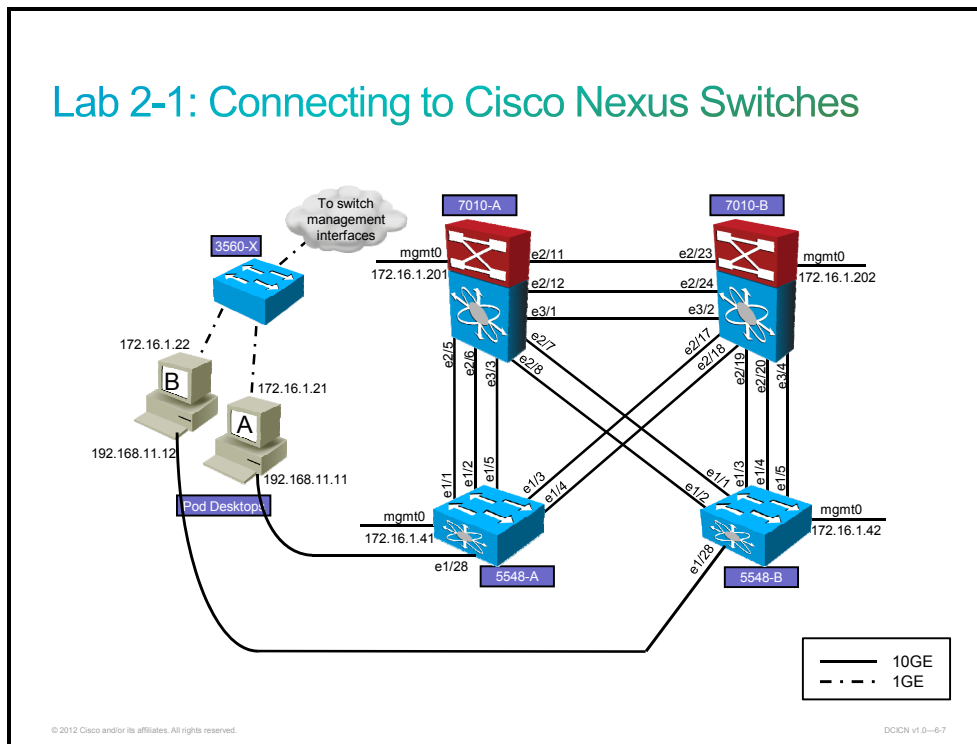
Activity Objective

In this activity, you will connect to the Cisco Nexus 7000 Series Switch using SSH. After completing this activity, you will be able to meet these objectives:

- Understand how to connect to the Out-Of-Band Management interface of Cisco Nexus Series Switches using SSH.

Visual Objective

The following figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco Nexus 7000 Series switches
- Cisco Nexus 5000 Series switches
- One PC with an SSH application for remote connectivity to the Cisco Nexus switches

Application List

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

Application	Description
PuTTY SSH Client	Terminal emulation application that supports SSH Protocol

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 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

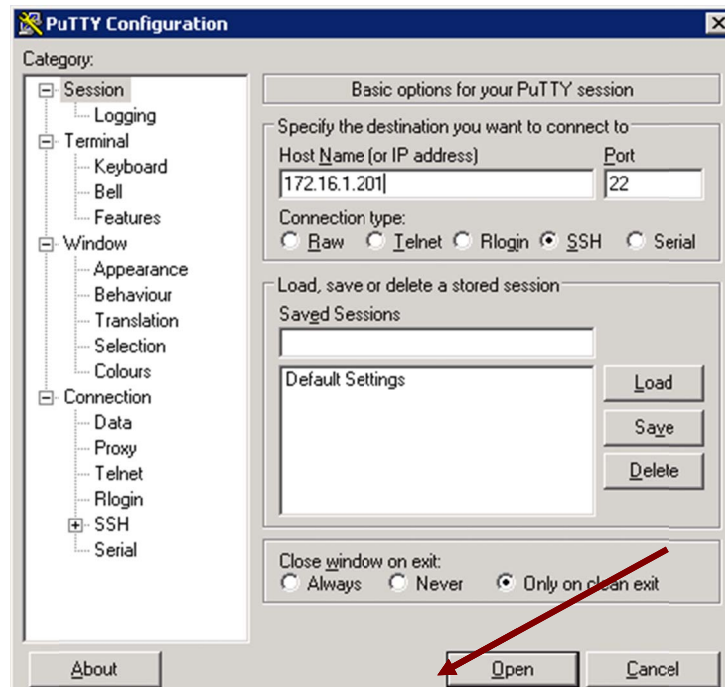
Complete these steps:

- Step 1** Using the credentials provided by your instructor, connect to the remote lab and your pod.
- Step 2** The pod consists of two PCs (A & B), two Cisco Nexus 7000 Series Switches (A & B) and two Cisco Nexus 5000 Series Switches (A & B). Each group of students in a pod will be responsible for a PC, a Cisco Nexus 7000 Series Switch, and a Cisco Nexus 5000 Series Switch. Management and communications will be performed from the PC. PC A will be used for the “A” switches and PC B will be used for the “B” switches. Your instructor has assigned you with the list of devices that you will be managing. Connect to your assigned PC.
- Step 3** Log into the PC using username **administrator** and password **1234QWer**.
- Step 4** Double-click the **PuTTY** shortcut on the desktop. (If the icon is missing, contact your instructor.)



Enter the following details in the PuTTY configuration dialog box for your Cisco Nexus 7000 Series Switch:

Host Name (or IP address):	172.16.1.201 (N7K-A) 172.16.1.202 (N7K-B)
Port	22
Connection Type	SSH



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 your Cisco Nexus 7000 Series Switch.

```

172.16.1.201 - PuTTY
login as: student
User Access Verification
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
F103-Nexus-7010-PROD-A#
  
```

Task 2: Connect to the Cisco Nexus 5000 Series Switch Using SSH

During this task, you will use SSH to connect to the Cisco Nexus 5000 Series Switch.

Activity Procedure

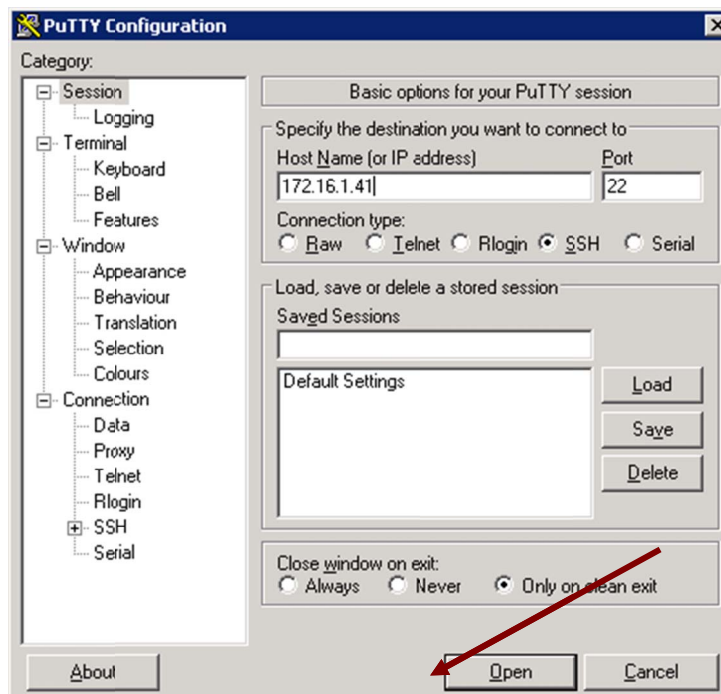
Complete these steps:

- Step 1** Double-click the **PuTTY** shortcut on the desktop. (If the icon is missing, contact your instructor.)



Enter the following details in the PuTTY configuration dialog box for your Cisco Nexus 5000 Series Switch:

Host Name (or IP address):	172.16.1.41 (N5K-A) 172.16.1.42 (N5K-B)
Port	22
Connection Type	SSH



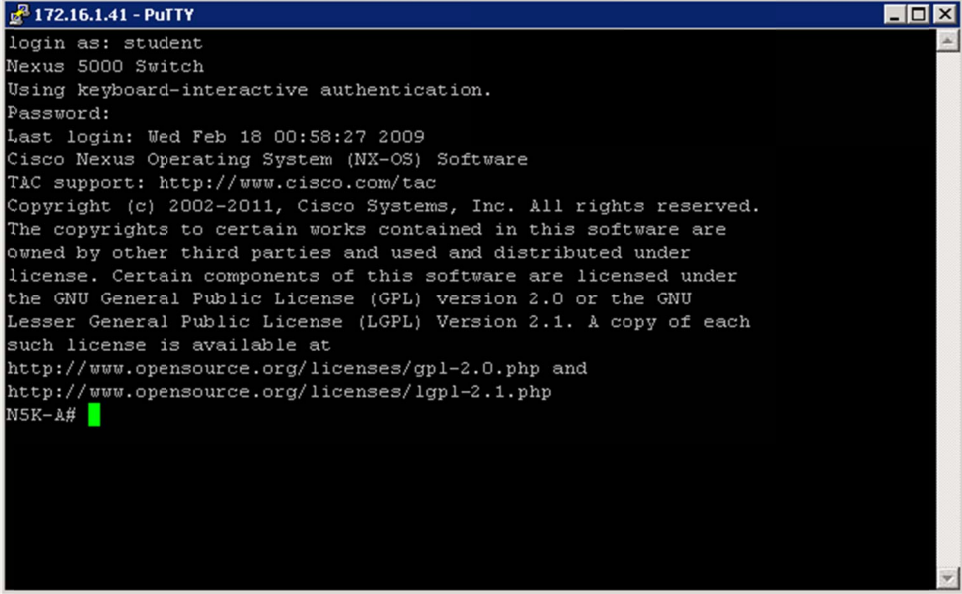
- Step 2** Click the **Open** button to open the session.

- Step 3** 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 your Cisco Nexus 5000 Series Switch.



```
172.16.1.41 - PuTTY
login as: student
Nexus 5000 Switch
Using keyboard-interactive authentication.
Password:
Last login: Wed Feb 18 00:58:27 2009
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-A#
```

Lab 2-2: Configuring Cisco Nexus Switches

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

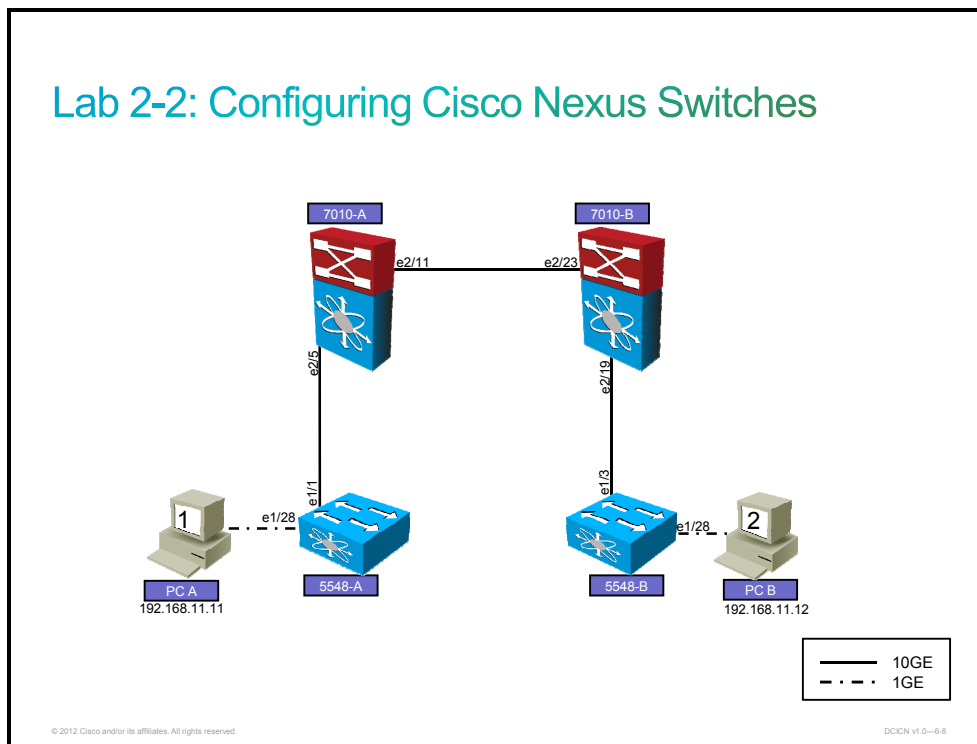
Activity Objective

In this activity, you will connect to the Cisco Nexus switch management interface using SSH to perform basic configuration tasks. After completing this activity, you will be able to meet these objectives:

- Understand how to perform basic configuration tasks on the Cisco Nexus 7000 Series Switch.
- Understand how to perform basic configuration tasks on the Cisco Nexus 5000 Series Switch.

Visual Objective

The following figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 5000 Series Switches
- One PC with an SSH application for remote connectivity to the Cisco Nexus switches

Command List

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

Command	Description
<code>clear user</code>	Disconnects the specified user
<code>configure</code>	Enters global configuration mode
<code>copy running-config startup-config</code>	Saves the running configuration to NVRAM
<code>description</code>	Creates a description on the current interface
<code>interface type mod/port</code>	Enters interface configuration mode for the specified port type, module, and port
<code>show inventory</code>	Displays inventory information on all switch hardware
<code>show interface</code>	Displays interface information
<code>show interface status</code>	Displays interface status
<code>show mac address-table</code>	Displays the current MAC address table
<code>show module</code>	Displays information on the installed modules
<code>show processes cpu history</code>	Displays information about CPU utilization for the last 60 seconds, 60 minutes, and 72 hours
<code>show running-config</code>	Displays the running configuration
<code>show users</code>	Displays user session information
<code>show user-account</code>	Displays the defined users and their roles
<code>show version</code>	Displays the version of system software that is currently running on the switch
<code>[no] shutdown</code>	Enables the current interface; disables current interface using the “no” prefix
<code>speed</code>	Defines the speed of the current interface
<code>username</code>	Creates account for the specified username

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: Perform Initial Configuration of the Switches

In this task, you will enable the ISLs and verify connectivity between the PCs.

Activity Procedure

Complete these steps:

Note The switch outputs and configuration steps are samples. Your actual input and output might be different from the samples shown.

Step 1 On your PC, open the window to your Cisco Nexus 7000 Series Switch.

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

F103-Nexus-7010-Prod_A# **show interface status**

```
-----  
Port          Name              Status    Vlan    Duplex  Speed  Type  
-----  
mgmt0         --                connected routed   full    1000   --  
Eth2/1        --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/2        --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/3        --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/4        --                disabled  1       full    auto   SFP-H10GB-C  
Eth2/5        --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/6        --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/7        --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/8        --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/9        --                disabled  1       full    auto   1000base-T  
Eth2/10       --                sfpAbsent 1       auto    auto   --  
Eth2/11       --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/12       --                disabled  1       auto    auto   SFP-H10GB-C  
Eth2/25       --                sfpAbsent 1       auto    auto   --  
Eth2/26       --                sfpAbsent 1       auto    auto   --  
Eth3/1        --                disabled  1       full    auto   SFP-H10GB-C  
Eth3/3        --                disabled  1       full    auto   SFP-H10GB-C  
Eth3/5        --                sfpAbsent 1       full    auto   --  
Eth3/7        --                sfpAbsent 1       full    auto   --  
Eth3/9        --                sfpAbsent 1       full    auto   --  
Eth3/11       --                sfpAbsent 1       full    auto   --  
Eth3/13       --                sfpAbsent 1       full    auto   --  
-output omitted-
```

Note The interfaces will be different for the two Cisco Nexus 7000 Series Switches.

Step 3 By default, all the interfaces are disabled except the mgmt0 interface. Enable the interfaces on your Cisco Nexus 7000 Series Switch listed in the table below that connect to the neighboring switches.

Device	Interface	Neighbor
N7K-A	e2/11	N7K-B e2/23
N7K-A	e2/5	N5K-A e1/1
N7K-B	e2/23	N7K-A e2/11
N7K-B	e2/19	N5K-B e1/3

```
F103-Nexus-7010-Prod_A# configure
F103-Nexus-7010-Prod_A(config-if)# interface e2/11,e2/5
F103-Nexus-7010-Prod_A(config-if-range)# no shutdown
```

Step 4 Create a description for the interfaces.

```
F103-Nexus-7010-Prod_A(config-if)# interface e2/11
F103-Nexus-7010-Prod_A(config-if)# description Link to N7K-B 2/23
F103-Nexus-7010-Prod_A(config-if)# interface e2/5
F103-Nexus-7010-Prod_A(config-if)# description Link to N5K-A 1/1
```

Step 5 Display the interface status to verify the configuration..

```
F103-Nexus-7010-Prod_A(config-if)# show interface status
```

```
-----
Port          Name                Status    Vlan    Duplex  Speed  Type
-----
mgmt0         --                  connected routed   full    1000   --
Eth2/1        --                  disabled  1       auto    auto   SFP-H10GB-C
Eth2/2        --                  disabled  1       auto    auto   SFP-H10GB-C
Eth2/3        --                  disabled  1       auto    auto   SFP-H10GB-C
Eth2/4        --                  disabled  1       full    auto   SFP-H10GB-C
Eth2/5        Link to N5K-A 1/1   notconnec 1       auto    auto   SFP-H10GB-C
Eth2/6        --                  disabled  1       auto    auto   SFP-H10GB-C
Eth2/7        --                  disabled  1       auto    auto   SFP-H10GB-C
Eth2/8        --                  disabled  1       auto    auto   SFP-H10GB-C
Eth2/9        --                  disabled  1       full    auto   1000base-T
Eth2/10       --                  sfpAbsent 1       auto    auto   --
Eth2/11       Link to N7K-B 2/23  connected 1       auto    auto   SFP-H10GB-C
Eth2/12       --                  disabled  1       auto    auto   SFP-H10GB-C
Eth2/25       --                  sfpAbsent 1       auto    auto   --
-output omitted-
```

Note The interfaces will not show as “connected” until the devices at each end of the link are enabled.

Step 6 Open the window to your Cisco Nexus 5000 Series Switch.

Step 7 Enable and assign descriptions to the interfaces that connect to the neighboring switch and the lab2 NIC of the PC.

Device	Interface	Neighbor
N5K-A	e1/1	N7K-A e2/5
N5K-A	e1/28	PC-A lab2
N5K-B	e1/3	N7K-B e2/19
N5K-B	e1/28	PC-B lab2

```
N5K-B# config
Enter configuration commands, one per line. End with CNTL/Z.
N5K-B(config)# interface e1/3
N5K-B(config-if)# desc Link to N7K-B 2/19
N5K-B(config-if)# no shutdown
N5K-B(config-if)# interface e1/28
N5K-B(config-if)# desc Link to PC-B
N5K-B(config-if)# no shutdown
N5K-B(config-if)# show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Eth1/1	--	disabled	1	full	10G	SFP-H10GB-C
Eth1/2	--	disabled	1	full	10G	SFP-H10GB-C
Eth1/3	Link to N7K-B 2/19	connected	1	full	10G	SFP-H10GB-C
Eth1/4	--	disabled	1	full	10G	SFP-H10GB-C
Eth1/5	--	disabled	1	full	10G	SFP-H10GB-C
Eth1/6	--	disabled	1	full	10G	SFP-1000BAS
Eth1/7	--	sfpAbsent	1	full	10G	--
Eth1/8	--	sfpAbsent	1	full	10G	--
(output omitted)						
Eth1/24	--	sfpAbsent	1	full	10G	--
Eth1/25	--	sfpAbsent	1	full	10G	--
Eth1/26	--	sfpAbsent	1	full	10G	--
Eth1/27	--	sfpAbsent	1	full	10G	--
Eth1/28	Link to PC-B	sfpInvalid	1	full	10G	SFP-1000BAS

Step 8 Because of the link used to connect to the PC, the interface does not function until the speed is manually set.

```
N5K-B(config)# interface e1/28
N5K-B(config-if)# speed 1000
```

Step 9 Verify that the e1/28 interface is shown as “connected.” If it is not, notify the instructor.

Step 10 Determine the IP address of the lab2 NIC on your PC by opening a command prompt on the PC and using the **ipconfig** command.

```
C:\Documents and Settings\Administrator>ipconfig
```

Windows IP Configuration

Ethernet adapter management:

```
Connection-specific DNS Suffix . :
IP Address. . . . . : 172.16.1.22
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Ethernet adapter lab:

```
Connection-specific DNS Suffix . :
IP Address. . . . . : 172.17.1.22
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Ethernet adapter do not change:

```
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.3.103.22
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.3.103.1
```

Ethernet adapter Lab2:

```
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.11.12
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Step 11 Exchange the IP address with your pod partner.

Step 12 Verify connectivity between the two PCs in your pod by pinging the NIC IP address of the other PC.

Activity Verification

You have completed this task when you attain these results:

- You have enabled the ISLs.
- You have verified the status of the interfaces that connect to neighboring switches and PCs.
- You have verified connectivity between the PCs.

Task 2: Create Management Accounts on the Cisco Nexus 7000 Series Switch

In this task, you will create accounts that are used to manage the switches.

Complete these steps:

Step 1 Open the window to your Cisco Nexus 7000 Series Switch.

Step 2 Use the **show user-account** command to display a list of the user accounts for the switch.

```
F103-Nexus-7010-Prod_B# show user-account
user:admin
      this user account has no expiry date
      roles:vdc-admin
```

Step 3 Create a new account named “student” that can be used to administer the switch. Your output should resemble this example:

```
F103-Nexus-7010-Prod_A# config
Enter configuration commands, one per line. End with CNTL/Z.
F103-Nexus-7010-Prod_A(config)# username student password 1234QWer role vdc-
admin
```

Step 4 Create a new account that will have limited capability. This account will be able to view most parameters but will not be able to change the configuration.

```
F103-Nexus-7010-Prod_A(config)# username intern password 1234ASdf role vdc-
operator
```

Step 5 Verify the new user accounts by using the **show user-account** command.

```
F103-Nexus-7010-Prod_A(config)# show user-account
user:admin
      this user account has no expiry date
      roles:vdc-admin
user:student
      this user account has no expiry date
      roles:vdc-admin
user:intern
      this user account has no expiry date
      roles:vdc-operator
```

Step 6 Open a new session in PuTTY to the Cisco Nexus 7000 Series Switch (keep the existing sessions open). Log in using the intern credentials (intern/1234ASdf).

Step 7 When logged in, display the user accounts by using the **show user-account** command.

Step 8 Display a list of currently connected users by using the **show users** command.

```
F103-Nexus-7010-Prod_A# show users
NAME      LINE      TIME      IDLE      PID COMMENT
admin     pts/0      Jun  8 09:02 00:04     1049 (172.16.1.21) session=ssh
intern    pts/1      Jun  8 09:33 .          2151 (172.16.1.21) session=ssh *
```

Notice that there are currently two users connected to the Switch (admin and intern). The “*” indicates the current user.

Step 9 Attempt to disconnect the admin user with the **clear user admin** command.

```
F103-Nexus-7010-Prod_A# clear user admin
% Permission denied for the role
```

Now, open the terminal window for the session that was connected with the admin credentials. Attempt to disconnect the intern user with the **clear user intern** command. Notice that no “Permission denied” message is displayed and the intern session window is closed.

Activity Verification

You have completed this task when you attain these results:

- You created a nondefault admin and operator account on the Cisco Nexus 7000 Series Switch.
- You verified the limited functionality of the operator role.
- You cleared a connection.

Note The accounts that you created on the Cisco Nexus 7000 Series Switch can also be created on the Cisco Nexus 5000 Series Switch.

Task 3: Explore Context-Sensitive Help

In this task, you will use context-sensitive help to locate commands and complete command syntax.

Complete these steps:

Step 1 Open the window to the Cisco Nexus 5000 Series Switch.

Step 2 Enter ? at the user prompt. You should see a list of available commands. Your output should resemble this example.

```
N5K-B# ?
callhome          Callhome commands
cd                Change current directory
cfs               CFS parameters
checkpoint         Create configuration rollback checkpoint
clear             Reset functions
cli              CLI commands
clock             Manage the system clock
configure         Enter configuration mode
copy             Copy from one file to another
debug            Debugging functions
debug-filter      Enable filtering for debugging functions
delete           Delete a file or directory
diff-clean        Remove temp files created by '| diff' filters
dir              List files in a directory
dos2nxos          DOS to NXOS text file format converter
echo             Echo argument back to screen (useful for scripts)
ethanalyzer       Configure cisco packet analyzer
event            Event Manager commands
find             Find a file below the current directory
fips             Enable/Disable FIPS mode
gunzip           Uncompresses LZ77 coded files
gzip             Compresses file using LZ77 coding
hardware         Change hardware usage settings
5K-A# ?
-output omitted-
```

Step 3 Enter **s?** (no space between “s” and ?). You should see the context-sensitive help. Your output should resemble this example.

```
N5K-A# s?
scripting  Configure scripting parameters
send       Send message to open sessions
setup      Run the basic SETUP command facility
show       Show running system information
sleep      Sleep for the specified number of seconds
sockets    Display sockets status and configuration
ssh        SSH to another system
system     System management commands
system     System configuration commands
```

```
N5K-A# s
```

There are approximately nine commands available that begin with the letter *s*.

Step 4 At the prompt, enter **sh** and then press the **Tab** key. You should see the command-completion feature in operation. When enough letters of a command or keyword have been entered, the Tab key completes the word and places a space so that it is ready to receive further input.

Step 5 Enter the **show ?** command. A list of possible **show** commands is displayed. Press **Spacebar** to see the next page of commands or press **Enter** to see the next line. Ctrl+C will terminate the output.

Step 6 Enter the **show p?** command. A list of possible **show** commands that begin with the letter *p* will be displayed. Your output should look like this:

```
N5K-A# show p?
password      Password for the user
platform      Shows list of events received by Platform Manager
policy-map    Show policy maps
port          Show port information
port-channel  Show port-channel information
port-profile  Show port-profile
port-resources Show information about Port Resources
privilege     Display privilege information
processes     Show processes
provision     Show information about provision
ptplc        Show ptpkc related information
```

```
N5K-A# show p
```

Step 7 Enter the **show processes ?** command. A list of possible **show processes** commands will be displayed. Your output should look like this:

```
N5K-A# show processes ?
<CR>
>      Redirect it to a file
>>    Redirect it to a file in append mode
cpu     Show processes CPU Info
log     Show information about process logs
memory  Show processes Memory Info
vdc     Show processes in vdc
|       Pipe command output to filter
```

```
N5K-A# show processes
```

Note The <CR> indicates that no further input is required. The current command would be accepted. In this case, however, there are additional commands that can be appended.

Step 8 Enter the **show processes cpu ?** command. A list of possible **show processes cpu** commands will be displayed. Your output should look like this:

```
N5K-A# show processes cpu ?
<CR>
>          Redirect it to a file
>>         Redirect it to a file in append mode
  history   Show processes CPU Util History
  sort      Show processes CPU Info (Sorted by Cpu Util)
  |         Pipe command output to filter

N5K-A# show processes cpu
```

Step 9 Enter the **show processes cpu history** command. This will generate an ASCII graph of the cpu utilization for the past 60 seconds, 60 minutes, and 72 hours.

Activity Verification

You have completed this task when you attain this result:

- You used the system help and the command-completion functions.

Task 4: Explore the Cisco Nexus Switch

In this task, you will use Cisco NX-OS Software to explore the switch. Most of these commands can also be run from the Cisco Nexus 5000 Series Switches.

Activity Procedure

Complete these steps:

Step 1 Open the window for one of the Cisco Nexus 7000 Series Switches. At the switch command prompt, enter the **show version** command and determine the software version that is currently running on the Cisco Nexus 7000 Series Switch.

Note	Your version might be different from the output shown here.
-------------	---

```
F103-Nexus-7010-Prod_A# show version
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.ht
ml
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
```

```
Software
  BIOS:          version 3.22.0
  kickstart:     version 6.0(2)
  system:        version 6.0(2)
  BIOS compile time:      02/20/10
  kickstart image file is: bootflash:///n7000-s1-kickstart.6.0.2.bin
  kickstart compile time: 12/25/2010 12:00:00 [12/22/2011 06:56:22]
  system image file is:   bootflash:///n7000-s1-dk9.6.0.2.bin
  system compile time:    11/15/2011 12:00:00 [12/22/2011 08:46:28]
```

```
Hardware
  cisco Nexus7000 C7010 (10 Slot) Chassis ("Supervisor module-1X")
```

Intel(R) Xeon(R) CPU with 8251592 kB of memory.
Processor Board ID JAF1551ASRN

Device name: F103-Nexus-7010
bootflash: 2048256 kB
slot0: 0 kB (expansion flash)

Kernel uptime is 4 day(s), 12 hour(s), 20 minute(s), 7 second(s)

Last reset
Reason: Unknown
System version: 6.0(2)
Service:

plugin
Core Plugin, Ethernet Plugin
F103-Nexus-7010-Prod_B#

Step 2 Answer the following questions:

1. Which version of Cisco NX-OS Software is currently running?

2. How long has the switch been running?

Step 3 Display the currently installed modules in the switch by using the **show modules** command.

Note Your output might vary.

```
F103-Nexus-7010-Prod_A# show module
Mod Ports Module-Type Model Status
---
2 32 1/10 Gbps Ethernet Module N7K-F132XP-15 ok
3 32 10 Gbps Ethernet XL Module N7K-M132XP-12L ok
5 0 Supervisor module-1X N7K-SUP1 active *
6 0 Supervisor module-1X N7K-SUP1 ha-standby
-output omitted-
```

In the preceding example, the card in slot 2 is an N7K-F132XP-15 line card. This card has 32 Layer 2, 10-Gb/s ports. The card in slot 3 is an N7K-M132XP-12L. This card has 32 multilayer 10-Gb/s ports.

Step 4 The information from the previous step can also be obtained by using the **show inventory** command.

```
F103-Nexus-7010-Prod_A# show inventory
NAME: "Chassis", DESCR: "Nexus7000 C7010 (10 Slot) Chassis "
PID: N7K-C7010 , VID: V02 , SN: JAF1545CJAM

NAME: "Slot 2", DESCR: "1/10 Gbps Ethernet Module"
PID: N7K-F132XP-15 , VID: V02 , SN: JAF1552AJKS

NAME: "Slot 3", DESCR: "10 Gbps Ethernet XL Module"
PID: N7K-M132XP-12L , VID: V02 , SN: JAF1550BBKM

NAME: "Slot 5", DESCR: "Supervisor module-1X"
```

```

PID: N7K-SUP1          ,   VID: V14 ,   SN: JAF1551ASRN

NAME: "Slot 6",  DESCR: "Supervisor module-1X"
PID: N7K-SUP1          ,   VID: V11 ,   SN: JAF1508AJQR

NAME: "Slot 11",  DESCR: "Fabric card module"
PID: N7K-C7010-FAB-1   ,   VID: V04 ,   SN: JAF1551AMLC

NAME: "Slot 12",  DESCR: "Fabric card module"
PID: N7K-C7010-FAB-1   ,   VID: V04 ,   SN: JAF1550CAKS

NAME: "Slot 13",  DESCR: "Fabric card module"
PID: N7K-C7010-FAB-1   ,   VID: V04 ,   SN: JAF1550CAKE
-output omitted-

```

Step 5 Display detailed information about one of the interfaces connecting to the other 7K in the pod by using the **show interface interface** command. Note the status of the interface along with the packet counters.

```

F103-Nexus-7010-PROD-A# show interface ethernet 2/11
Ethernet2/11 is up
  Dedicated Interface
  Hardware: 1000/10000 Ethernet, address: c464.13ba.fe92 (bia c464.13ba.fe92)
  Description: Link to N7K-B 2/23
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is access
  full-duplex, 10 Gb/s, media type is 10G
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
  Last link flapped 00:39:36
  Last clearing of "show interface" counters 4d01h
  30 seconds input rate 32 bits/sec, 0 packets/sec
  30 seconds output rate 264 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 40 bps, 0 pps; output rate 304 bps, 0 pps
  RX
    49 unicast packets  17995 multicast packets  234 broadcast packets
    18278 input packets  3246043 bytes
    0 jumbo packets  0 storm suppression packets
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun  0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    218 unicast packets  20792 multicast packets  707 broadcast packets
    21717 output packets  3482483 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
  19 interface resets

```

Step 6 Determine the MAC address of the lab2 NIC on the PC by opening a command prompt and using the **ipconfig /all** command. Record the MAC address of the interface here and provide it to your pod partners.

MAC Address: _____

Step 7 Display the MAC address table of the switches by using the **show mac address-table** command.

```
F103-Nexus-7010-Prod_A# 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      -      64a0.e743.03c2      static      -      F      F      sup-eth1 (R)
* 1      0050.5680.7974      dynamic      270      F      F      Eth2/5
* 1      0050.5680.7975      dynamic      270      F      F      Eth2/11
```

Note The dynamic entries will age out after 1800 seconds on a Cisco Nexus 7000 Series Switch (300 seconds on a Cisco Nexus 5000 Series Switch). Your output might look different. To create entries, generate traffic by opening a command prompt on the PC and pinging the other PC in the pod. Then display the MAC address table again.

Step 8 Verify that the MAC addresses are associated with the expected ports. For example, on the N7K-A switch, the PC-A MAC address should be learned on the e2/5 port.

Step 9 Display the running configuration of the switch by using the **show running-config** command.

```
F103-Nexus-7010-Prod_A# show running-config
```

```
!Command: show running-config
!Time: Wed Feb 29 13:28:00 2012
```

```
version 6.0(2)
hostname Prod_A
```

```
username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
```

```
ip domain-lookup
-output omitted-
```

Step 10 Rather than scroll through the configuration, you can filter the output by section.

```
F103-Nexus-7010-PROD-A# show running-config interface ethernet 2/11
```

```
!Command: show running-config interface Ethernet2/11
!Time: Fri Mar 2 10:36:42 2012
```

```
version 6.0(2)
```

```
interface Ethernet2/11
  description Link to N7K-B 2/23
  no shutdown
```

```
F103-Nexus-7010-PROD-A#
```

Step 11 Save the running-config by using the **copy running-config startup-config** command. Perform this step on all switches!

```
F103-Nexus-7010-Prod_A# copy running-config startup-config
```

```
[#####] 100%
Copy complete, now saving to disk (please wait)...
F103-Nexus-7010-Prod_A#
```

Activity Verification

You have completed this task when you attain these results:

- You have connected to the two Cisco Nexus 7000 Series Switches and the two Cisco Nexus 5000 Series Switches.
- You have explored the CLI and the help function.
- You have explored the status of the switch using **show** commands.
- You have used the system help and the command-completion functions.
- You have saved the running configuration.

Switch Configurations

When you complete this lab activity, your switch configurations will be like the following, with differences that are specific to your switch.

Lab 2-2 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:09:58 2012

version 6.0(2)
hostname Prod_A

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1
vlan 1

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
description Link to N5K-A 1/1
no shutdown

interface Ethernet2/6

interface Ethernet2/7
```

```
interface Ethernet2/8

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
  description Link to N7K-B 2/23
  no shutdown

interface Ethernet2/12

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  switchport

interface Ethernet3/3
  switchport

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

interface Ethernet3/11
  switchport

interface Ethernet3/13
  switchport

interface Ethernet3/15
  switchport

interface Ethernet3/17
  switchport

interface Ethernet3/19
  switchport

interface Ethernet3/21
  switchport

interface Ethernet3/23
  switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
  ip address 172.16.1.201/24
  line vty
```

Lab 2-2 Cisco Nexus 5000 Series Switch Configuration

```
!Command: show running-config
!Time: Sat Jun 9 14:02:39 2012

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lldp

username admin password 5 $1$aS0dB0mR$h7immj0YTBsjhQlsiy/hR/ role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
  ip route 0.0.0.0/0 172.16.1.1
vlan 1

interface Ethernet1/1
  description Link to N7K-A 2/5

interface Ethernet1/2

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14
```

```
interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28
  description Link to PC-A Lab2
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 2-3: Configuring VLANs and Trunks

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

Note This lab builds on the configurations of the previous labs.

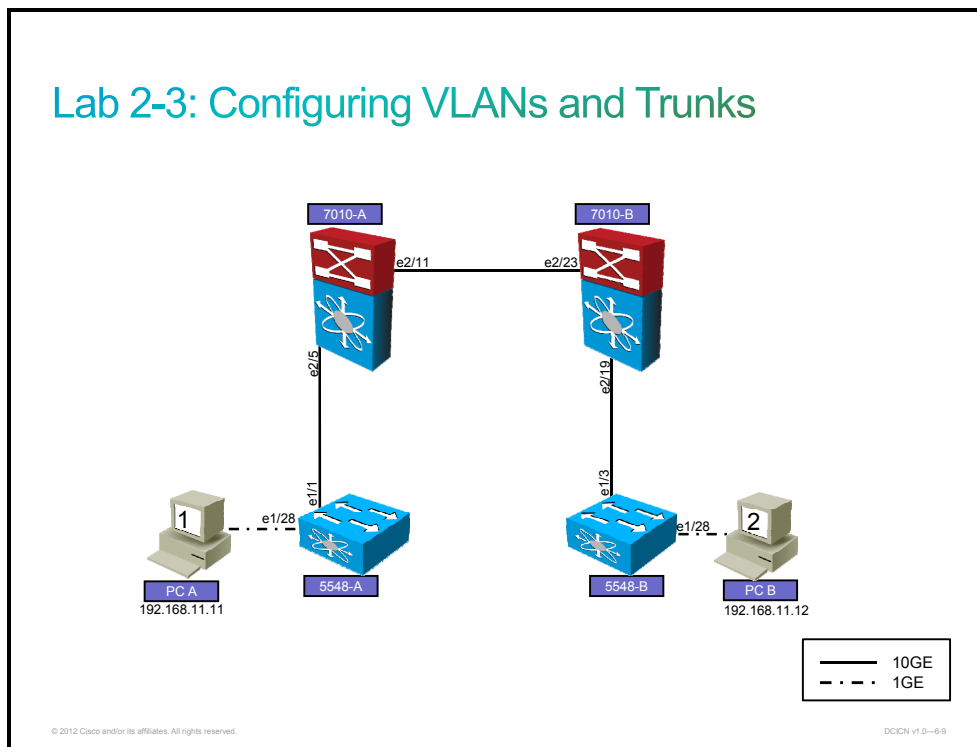
Activity Objective

In this activity, you will connect to the Cisco Nexus 5000 Series Switches and Cisco Nexus 7000 Series Switches and create VLANs and trunks. You will use the **show** commands to verify configurations. After completing this activity, you will be able to meet these objectives:

- Understand how to create VLANs and configure VLAN membership
- Understand how to verify VLANs and VLAN membership.
- Understand how to create trunks
- Understand how to use **show** commands to verify trunking

Visual Objective

This figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 5000 Series Switches
- PC with an SSH application for remote connectivity to the Cisco Nexus switches

Command List

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

Command	Description
feature <i>name</i>	Enables the specified feature
interface <i>type num</i>	Enters interface configuration mode for the specified interface
show interface status	Displays status information on all interfaces
show interface trunk	Displays trunking information on all interfaces
show vlan [<i>num</i>]	Displays information on all configured VLANs
show vlan brief	Displays a summary of all configured VLANs
show vtp status	Displays the current VTP configuration and status
switchport access vlan <i>num</i>	Defines the current interface as a member of the specified VLAN
switchport mode trunk	Defines the current interface as an 802.1q trunk
vlan [<i>num</i>]	Creates the specified VLAN
vtp domain <i>name</i>	Defines the VTP domain name
show running-config	Displays the current configuration

Task 1: Configure VLANs

In this task, you will create VLANs on the switches, and you will make ports members of the VLANs. The configuration of this lab is built on the configuration of the previous labs.

Note This lab builds on the configurations of the previous labs.

Activity Procedure

Complete these steps:

Note The switch outputs and configuration steps are samples. Your actual input and output might be different from the samples shown.

Step 1 If an SSH session from the PC to both switches is not already established, open an SSH session to both Cisco Nexus switches that you are configuring. (This step is described in Lab 2-1.)

Step 2 On the Cisco Nexus 7000 Switch, display the interface status by using the **show interface status** command. Note the “Vlan” column for the connected links.

F103-Nexus-7010-Prod_A# **show interface status**

Port	Name	Status	Vlan	Duplex	Speed	Type
mgmt0	--	connected	routed	full	1000	--
Eth2/1	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/2	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/3	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/4	--	disabled	1	full	auto	SFP-H10GB-C
Eth2/5	Link to N5K-A 1/1	connected	1	full	10G	SFP-H10GB-C
Eth2/6	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/7	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/8	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/9	--	disabled	1	full	auto	1000base-T
Eth2/10	--	sfpAbsent	1	auto	auto	--
Eth2/11	Link to N7K-B 2/23	connected	1	full	10G	SFP-H10GB-C
Eth2/12	--	disabled	1	auto	auto	SFP-H10GB-C

-output omitted-

Step 3 Display the list of VLANs by using the **show vlan brief** command.

F103-Nexus-7010-Prod_A# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Eth2/1, Eth2/2, Eth2/3, Eth2/4 Eth2/5, Eth2/6, Eth2/7, Eth2/8 Eth2/9, Eth2/10, Eth2/11 Eth2/12, Eth2/25, Eth2/26 Eth3/1, Eth3/3, Eth3/5, Eth3/7 Eth3/9, Eth3/11, Eth3/13 Eth3/15, Eth3/17, Eth3/19 Eth3/21, Eth3/23

At this time, VLAN 1 is the only VLAN, and all ports are members of VLAN 1.

Step 4 On all the switches, create VLAN 11 from global configuration mode using the **vlan 11** command and name the VLAN “lab-a.”

Note The naming of the VLAN will not take effect until you exit from VLAN configuration mode.

```
F103-Nexus-7010-Prod_A# configure
F103-Nexus-7010-Prod_A(config)# vlan 11
F103-Nexus-7010-Prod_A(config-vlan)# name lab-a
F103-Nexus-7010-Prod_A(config-vlan)# exit
F103-Nexus-7010-Prod_A(config)#
```

Step 5 Verify the VLANs by using the **show vlan brief** command. Notice the new VLAN displayed below VLAN 1. However, VLAN 11 has no member ports on any of the switches.

```
F103-Nexus-7010-Prod_A(config)# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Eth2/1, Eth2/2, Eth2/3, Eth2/4 Eth2/5, Eth2/6, Eth2/7, Eth2/8 Eth2/9, Eth2/10, Eth2/11 Eth2/12, Eth2/25, Eth2/26 Eth3/1, Eth3/3, Eth3/5, Eth3/7 Eth3/9, Eth3/11, Eth3/13 Eth3/15, Eth3/17, Eth3/19 Eth3/21, Eth3/23
11	lab-a	active	

Step 6 On the two Cisco Nexus 5000 Series Switches, make the port that is connected to the PC a member of VLAN 11 by using the **switchport access vlan 11** command in interface configuration mode.

```
N5K-A(config)# interface e1/28
N5K-A(config-if)# switchport access vlan 11
N5K-A(config-if)#
```

Step 7 Verify the VLAN membership of the port by using the **show vlan brief** command and the **show interface status** command.

```
N5K-A(config-if)# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 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, Eth1/29, Eth1/30 Eth1/31, Eth1/32
11	lab-a	active	Eth1/28

```
N5K-A(config-if)# show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Eth1/1	Link to N7K-A 2/5	connected	1	full	10G	SFP-H10GB-C
Eth1/2	--	disabled	1	full	10G	SFP-H10GB-C
Eth1/3	--	disabled	1	full	10G	SFP-H10GB-C
Eth1/4	--	disabled	1	full	10G	SFP-H10GB-C

```

Eth1/5      --      disabled 1      full 10G SFP-H10GB-C
Eth1/6      --      disabled 1      full 10G SFP-1000BAS
-output omitted-
Eth1/26     --      sfpAbsent 1      full 10G --
Eth1/27     --      sfpAbsent 1      full 10G --
Eth1/28     Link to PC-A connected 11 full 1000 SFP-1000BAS
Eth1/29     --      disabled 1      full 10G 10Gbase- (un
-output omitted-

```

Step 8 At a command prompt on one of the PCs, ping the other PC in the pod. Is the ping successful? (Refer to Lab 2-2, Task 1, Steps 11 and 12 for the IP address.)

3. Why?

4. Is there a path for the VLAN 11 traffic from the PC that is connected to N5K-A to the PC that is connected to N5K-B?

Activity Verification

You have completed this task when you attain these results:

- You have created VLAN 11 on all switches.
- You have verified VLAN 11 on all switches.
- You have configured the e1/28 port on both Cisco Nexus 5000 Series Switches as members of VLAN 11.
- You have verified the port membership of the e1/28 ports on the Cisco Nexus 5000 Series Switches.

Task 2: Configure Trunks

In this task, you will create trunks between the Cisco Nexus switches.

Activity Procedure

Complete these steps:

Step 1 From the previous task, we know that the ISLs are members of VLAN 1. Use the **show interface status** command to review this information. Because of this, no VLAN 11 traffic can cross these links. On the Cisco Nexus 5000 Series Switches, configure the interface that connects to your Cisco Nexus 7000 Series Switch as a trunk by using the **switchport mode trunk** command. The following table lists the interfaces configured in this step.

Device	Interface
N5K-A	e1/1
N5K-A	e1/3

```

N5K-A(config)# int e1/1
N5K-A(config-if)# switchport mode trunk
N5K-A(config-if)#

```

Step 2 On the Cisco Nexus 5000 Series Switches, verify the interface configuration using the **show interface status** command.

```

N5K-A(config-if)# show interface status

```

Port	Name	Status	Vlan	Duplex	Speed	Type
Eth1/1	Link to N7K-A 2/5	connected	trunk	full	10G	SFP-H10GB-C
Eth1/2	--	disabled	1	full	10G	SFP-H10GB-C
Eth1/3	--	disabled	1	full	10G	SFP-H10GB-

-output omitted-

Step 3 On the Cisco Nexus 5000 Series Switches, view the trunking status using the **show interface trunk** command.

N5K-A(config-if)# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Port	Vlans Allowed on Trunk		
Eth1/1	1-3967,4048-4093		
Port	Vlans Err-disabled on Trunk		
Eth1/1	none		
Port	STP Forwarding		
Eth1/1	1,11		
Port	Vlans in spanning tree forwarding state and not pruned		
Eth1/1	--		
Port	Vlans Forwarding on FabricPath		

Step 4 On the Cisco Nexus 7000 Series Switches, configure the remaining ISLs on the 7Ks using the same command.

Device	Interface
N7K-A	e2/5, e2/11
N&K-B	e2/19, e2/23

F103-Nexus-7010-Prod_A(config)# **int e2/5,e2/11**

F103-Nexus-7010-Prod_A(config-if-range)# **switchport mode trunk**

Step 5 On all switches, verify that all ISLs are trunking by using the **show interface trunk** command.

F103-Nexus-7010-Prod_A# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth2/5	1	trunking	--
Eth2/11	1	trunking	--
Port	Vlans Allowed on Trunk		
Eth2/5	1-4094		
Eth2/11	1-4094		

Port	Vlans Err-disabled on Trunk
Eth2/5	none
Eth2/11	none
Port	STP Forwarding
Eth2/5	1,11
Eth2/11	1,11
Port	Vlans in spanning tree forwarding state and not pruned
Eth2/5	1,11
Eth2/11	1,11
Port	Vlans Forwarding on FabricPath
Eth2/5	none
Eth2/11	none

Step 6 Answer the following questions:

- Which VLANs are allowed over the trunk between the Cisco Nexus 5000 Series Switches and the Cisco Nexus 7000 Series Switches?

- What is the native VLAN on the trunk between N7K-A and N7K-B?

Step 7 From a command prompt on the PC, ping the other PC in the pod. Is the ping successful?

3.

Activity Verification

You have completed this task when you attain these results:

- You have created trunks between the switches.
- You have verified the trunks between the switches.
- You have verified connectivity between the PCs.

Task 3: Configure VTP

In this task, you will configure VTP.

Activity Procedure

Complete these steps:

Step 1 Enable the VTP feature by using the **feature vtp** command on all the switches.

```
N5K-B# configure
N5K-B(config)# feature vtp
N5K-B(config)
```

Step 2 Verify the VTP status using the **show vtp status** command.

```
N5K-B(config)# sh vtp status
VTP Status Information
-----
VTP Version                : 2 (capable)
Configuration Revision      : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 6
VTP Operating Mode          : Server
VTP Domain Name             : <VTP domain not acquired/configured yet>
VTP Pruning Mode            : Disabled (Operationally Disabled)
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 Digest                  : 0x6E 0x99 0xFC 0xBD 0x0F 0xE0 0x5C 0xA1
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0
VTP version running         : 1
```

Step 3 Notice that the mode is set to Server, and the domain name is not yet defined.

Step 4 On the N5K-B only, define the domain name as DCICN.

```
N5K-B(config)# vtp domain DCICN
N5K-B(config)#
```

Step 5 View the VTP status again on all switches. Note that all switches now have a domain name defined.

```
F103-Nexus-7010-Prod_B(config)# show vtp status
VTP Status Information
-----
VTP Version                : 2 (capable)
Configuration Revision      : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 6
VTP Operating Mode          : Server
VTP Domain Name             : DCICN
VTP Pruning Mode            : Disabled (Operationally Disabled)
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 Digest                  : 0x8F 0x4B 0x77 0x30 0x67 0x32 0xDB 0x27
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0
```

Note Depending on the timing, it might take a couple of minutes before the domain name is acquired by all the switches. When you have observed the domain name propagating to the neighboring switch, you can either wait for the domain name to be acquired by the remaining switches, or you can manually assign the domain name.

Step 6 After you have confirmed that all switches have the domain name DCICN, on the N7K-A switch, create VLAN 12 and name it lab-12.

```
F103-Nexus-7010-Prod_A(config)# vlan 12
F103-Nexus-7010-Prod_A(config-vlan)# name lab-12
F103-Nexus-7010-Prod_A(config-vlan)# exit
F103-Nexus-7010-Prod_A(config)#
```

Step 7 On all switches, display the VLAN database using the **show vlan brief** command.

Step 8 VLAN 12 now exists on all switches in the VTP domain.

- Step 9** Display the VTP status and compare the configuration revision number to the value in Step 6.
- Step 10** Create two or three additional VLANs on any of the switches and view the VLAN database and configuration revision numbers as the VLANs are created.
- Step 11** On the N5K-A switch, delete VLAN 11.
- Step 12** Answer the following questions:
1. What happens to VLAN 11 on the other three switches?
-
2. Will the PCs be able to ping each other now?
-

- Step 13** On the N7K-A switch, delete the VLANs that were created in steps 9 and 11.
- Step 14** On the N7K-B switch, re-create VLAN 11.
- Step 15** Verify that the VLAN database contains VLAN 11 on all switches and ping between the two PCs to confirm connectivity.
- Step 16** Save the running-config using the **copy running-config startup-config** command. Perform this step on all switches!

```
F103-Nexus-7010-Prod_A# 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 enabled VTP.
- You have observed the propagation of the VLAN database between switches.

Switch Configurations

When you complete this lab activity, your switch configurations will be like the following, with differences that are specific to your switch.

Lab 2-3 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:31:17 2012

version 6.0(2)
hostname Prod_A

feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
```

```

v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
  description Link to N5K-A 1/1
  switchport mode trunk
  no shutdown

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
  description Link to N7K-B 2/23
  switchport mode trunk
  no shutdown

interface Ethernet2/12

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  switchport

interface Ethernet3/3
  switchport

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

interface Ethernet3/11
  switchport

```

```

interface Ethernet3/13
  switchport

interface Ethernet3/15
  switchport

interface Ethernet3/17
  switchport

interface Ethernet3/19
  switchport

interface Ethernet3/21
  switchport

interface Ethernet3/23
  switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
  ip address 172.16.1.201/24
  line vty

```

Lab 2-3 Cisco Nexus 5000 Series Switch Configuration

```

!Command: show running-configz
!Time: Sat Jun  9 14:30:23 2012z

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lldp
feature vtp

username admin password 5 $1$aSOdBomR$h7immj0YTBsjhQlsiy/hR/  role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management

```

```
ip route 0.0.0.0/0 172.16.1.1

interface Ethernet1/1
  description Link to N7K-A 2/5
  switchport mode trunk

interface Ethernet1/2

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28
  description Link to PC-A Lab2
  switchport access vlan 11
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31
```

```
interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 2-4: Verifying and Configuring Spanning Tree

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

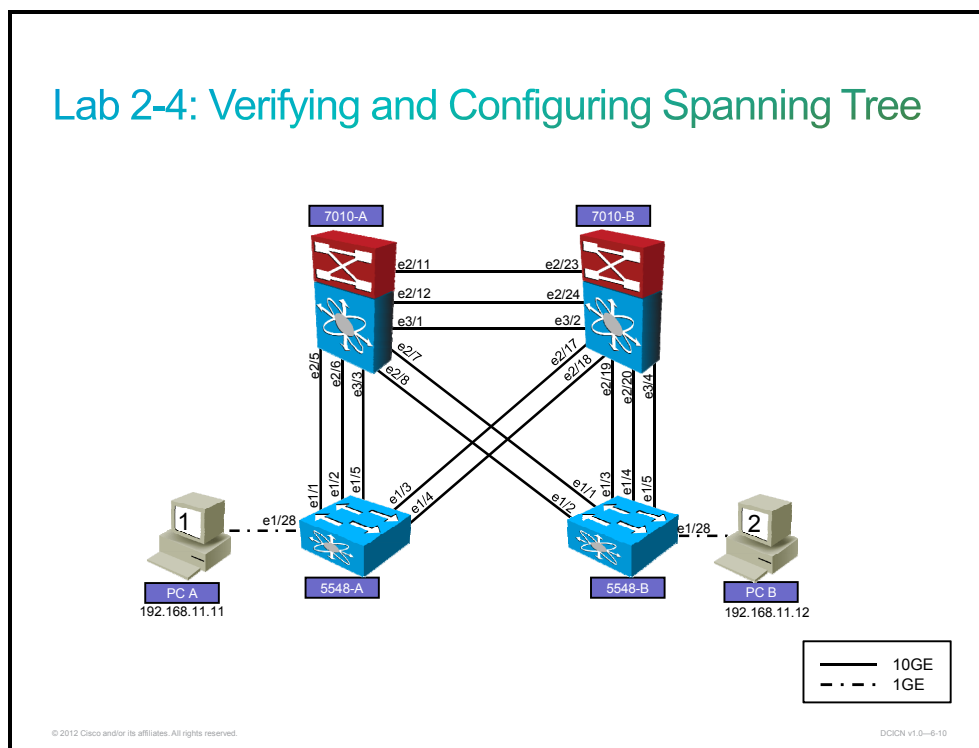
Activity Objective

In this lab, you will connect to the Cisco Nexus 5000 Series Switches and Cisco Nexus 7000 Series Switches to configure and validate spanning tree configurations. After completing this activity, you will be able to meet these objectives:

- Configure spanning tree parameters
- Use the **show** commands to validate spanning tree configuration

Visual Objective

The following figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 5000 Series Switches
- One PC with an SSH application for remote connectivity to the Cisco Nexus Switches

Command List

This table describes the commands used in this activity.

Command	Description
<code>description <i>string</i></code>	Assigns the specified description to the current interface
<code>interface <i>type num</i></code>	Enters interface configuration mode for the specified interface
<code>show interface status</code>	Displays status information on all interfaces
<code>show running-config</code>	Displays current running configuration
<code>show spanning-tree</code>	Displays spanning tree information
<code>[no] shutdown</code>	Disables the current interface
<code>spanning-tree port type edge</code>	Defines the current interface as an edge port
<code>switchport mode trunk</code>	Defines the current interface as an 802.1q trunk

Task 1: Configure Redundant Links

In this task, you will use CLI commands to enable the redundant links between switches.

Note This lab builds on the configurations of the previous labs.

Activity Procedure

Complete the following steps on all switches.

Note The switch outputs and configuration steps are samples. Your actual input and output might be different from the samples shown.

Step 1 Configure and enable the redundant ISLs. The following table shows the links for each switch.

N7K-A

Device	Interface	Neighbor & Interface
N7K-A	e2/6	N5K-A e1/2
N7K-A	e2/7	N5K-B e1/1
N7K-A	e2/8	N5K-B e1/2
N7K-A	e2/12	N7K-B e2/24
N7K-A	e3/1	N7K-B e3/2
N7K-A	e3/3	N5K-A e1/5

N5K-A

Device	Interface	Neighbor & Interface
N5K-A	e1/2	N7K-A e2/6
N5K-A	e1/3	N7K-B e2/17
N5K-A	e1/4	N7K-B e2/18
N5K-A	e1/5	N7K-A e3/3

N7K-B

Device	Interface	Neighbor & Interface
N7K-B	e2/17	N5K-A e1/3
N7K-B	e2/18	N5K-A e1/4
N7K-B	e2/20	N5K-B e1/4
N7K-B	e2/24	N7K-A e2/12
N7K-B	e3/2	N7K-A e3/1
N7K-A	e3/4	N5K-B e1/5

Device	Interface	Neighbor & Interface
N5K-B	e1/1	N7K-A e2/7
N5K-B	e1/2	N7K-A e2/8
N5K-B	e1/4	N7K-B e2/20
N5K-B	e1/5	N7K-B e3/4

```

F103-Nexus-7010-Prod_A(config)# int e2/6
F103-Nexus-7010-Prod_A(config-if)# description Link to N5K-A 1/2
F103-Nexus-7010-Prod_A(config-if)# switchport mode trunk
F103-Nexus-7010-Prod_A(config-if)# no shut
F103-Nexus-7010-Prod_A(config-if)# int e2/7
F103-Nexus-7010-Prod_A(config-if)# description Link to N5K-B 1/1
F103-Nexus-7010-Prod_A(config-if)# switchport mode trunk
F103-Nexus-7010-Prod_A(config-if)# no shut
F103-Nexus-7010-Prod_A(config-if)# int e2/8
F103-Nexus-7010-Prod_A(config-if)# description Link to N5K-B 1/2
F103-Nexus-7010-Prod_A(config-if)# switchport mode trunk
F103-Nexus-7010-Prod_A(config-if)# no shut
F103-Nexus-7010-Prod_A(config-if)# int e2/12
F103-Nexus-7010-Prod_A(config-if)# description Link to N7K-B 2/24
F103-Nexus-7010-Prod_A(config-if)# switchport mode trunk
F103-Nexus-7010-Prod_A(config-if)# no shut
F103-Nexus-7010-Prod_A(config-if)# int e3/1
F103-Nexus-7010-Prod_A(config-if)# description Link to N7K-B 3/2
F103-Nexus-7010-Prod_A(config-if)# switchport mode trunk
F103-Nexus-7010-Prod_A(config-if)# no shut
F103-Nexus-7010-Prod_A(config-if)# int e3/3
F103-Nexus-7010-Prod_A(config-if)# description Link to N5K-A 1/D
F103-Nexus-7010-Prod_A(config-if)# switchport mode trunk
F103-Nexus-7010-Prod_A(config-if)# no shut

```

Step 2 Verify the interface status on all switches by using the **show interface status** command.

```
F103-Nexus-7010-Prod_A(config-if)# show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
mgmt0	--	connected	routed	full	1000	--
Eth2/1	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/2	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/3	--	disabled	1	auto	auto	SFP-H10GB-C
Eth2/4	--	disabled	1	full	auto	SFP-H10GB-C
Eth2/5	Link to N5K-A 1/1	connected	trunk	full	10G	SFP-H10GB-C
Eth2/6	Link to N5K-A 1/2	connected	trunk	full	10G	SFP-H10GB-C
Eth2/7	Link to N5K-B 1/1	connected	trunk	full	10G	SFP-H10GB-C
Eth2/8	Link to N5K-B 1/2	connected	trunk	full	10G	SFP-H10GB-C
Eth2/9	--	disabled	1	full	auto	1000base-T
Eth2/10	--	sfpAbsent	1	auto	auto	--
Eth2/11	Link to N7K-B 2/23	connected	trunk	full	10G	SFP-H10GB-C
Eth2/12	Link to N7K-B 2/24	connected	trunk	full	10G	SFP-H10GB-C
Eth2/25	--	sfpAbsent	1	auto	auto	--
Eth2/26	--	sfpAbsent	1	auto	auto	--
Eth3/1	Link to N7K-B 3/2	connected	trunk	full	10G	SFP-H10GB-C
Eth3/3	Link to N5K-A 1/5	connected	trunk	full	10G	SFP-H10GB-C
Eth3/5	--	sfpAbsent	1	full	auto	--
Eth3/7	--	sfpAbsent	1	full	auto	--

-output omitted-

Step 3 Determine the spanning tree topology for vlan 11 using the **show spanning-tree vlan 11** command on all the switches.

F103-Nexus-7010-Prod_A(config)# **show spanning-tree vlan 11**

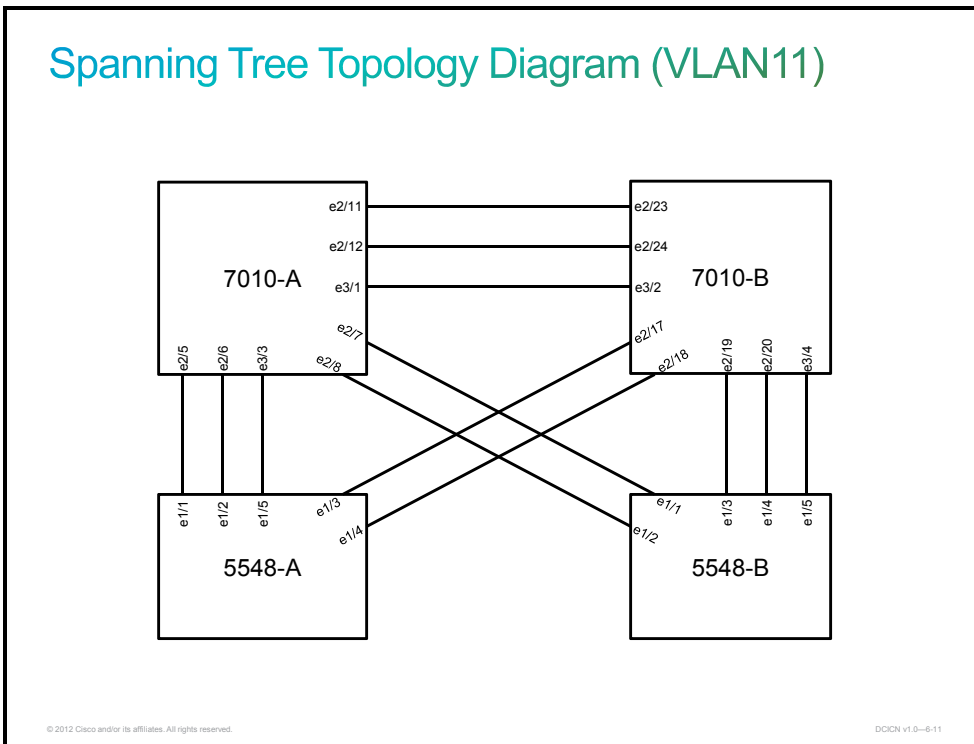
VLAN0011

Spanning tree enabled protocol rstp

Root ID Priority 32779
 Address 547f. ee5c. 6efc
 Cost 2
 Port 261 (Ethernet2/5)
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32779 (priority 32768 sys-id-ext 11)
 Address 64a0. e743. 03c2
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth2/5	Root	FWD	2	128.261	P2p
Eth2/6	Altn	BLK	2	128.262	P2p
Eth2/7	Desg	FWD	2	128.263	P2p
Eth2/8	Desg	FWD	2	128.264	P2p
Eth2/11	Desg	FWD	2	128.267	P2p
Eth2/12	Desg	FWD	2	128.268	P2p
Eth3/1	Desg	FWD	2	128.385	P2p
Eth3/3	Altn	BLK	2	128.387	P2p



Step 4 Using the topology diagram for VLAN11, indicate which switch is the root for VLAN11.

Step 5 Using the topology diagram, indicate which port on each switch is the root port for VLAN 11.

Step 6 Using the topology diagram, indicate which ports are blocking by placing an “X” over the interfaces.

Step 7 Answer the following questions:

3. Which Spanning Tree Protocol is running?

4. Which switch is the root?

5. What is the root port on the N7K-B switch?

6. What is the root port on the 7K-A switch?

7. What is the cost to the root from the 5K-B switch?

8. Using the information from the topology diagram for VLAN 11, how many paths are there from the PC connected to the N5K-A switch to the PC connected to the N5K-B switch?

Activity Verification

You have completed this task when you attain these results:

- You have enabled the redundant ISLs.
- You have determined the cost to the root bridge.
- You have determined that the topology is loop free.

Task 2: Optimize Spanning Tree

In this task, you will use CLI commands to optimize the spanning tree configuration.

Activity Procedure

Complete the following steps on all switches.

Step 1 To insure optimal traffic flow in a spanning tree network, the location of the root bridge must sometimes be configured. Typically, the root bridge will be in the core or close to the core of the network. In the lab topology, the root should be one of the Cisco Nexus 7000 Series Switches. In this step, the N7K-A switch is configured to be the root of the spanning tree topology for VLAN 11.

```
F103-Nexus-7010-Prod_A(config)# spanning-tree vlan 11 priority 16384
```

Note This step can also be done using the **spanning-tree vlan 11 root primary** command.

Step 2 Verify the new spanning tree topology using the **show spanning-tree vlan 11** command.

Step 3 Using the topology diagram for VLAN11, indicate which switch is the root for VLAN11.

- Step 4** Using the topology diagram, indicate which port on each switch is the root port for VLAN 11.
- Step 5** Using the topology diagram, indicate which ports are blocking by placing an “X” over the interfaces.
- Step 6** Compare the current topology with the topology determined in Task 1.
- Step 7** On the Cisco Nexus 50000 Series Switches, determine the port type for the ports that are connected to the PCs.

```
N5K-A(config-if)# show spanning-tree vlan 11
```

```
VLAN0011
  Spanning tree enabled protocol rstp
  Root ID    Priority    16395
            Address     64a0.e743.03c2
            Cost        2
            Port        129 (Ethernet1/1)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32779 (priority 32768 sys-id-ext 11)
            Address     547f.ee5c.6efc
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Eth1/1	Root	FWD	2	128.129	P2p
Eth1/2	Altn	BLK	2	128.130	P2p
Eth1/3	Desg	FWD	2	128.131	P2p
Eth1/4	Desg	FWD	2	128.132	P2p
Eth1/5	Altn	BLK	2	128.133	P2p
Eth1/28	Desg	FWD	4	128.156	P2p Peer (STP)

- Step 8** Ports that are not connected to other spanning tree-capable devices should be configured as edge ports. On the Cisco Nexus 5000 Series Switches, configure the e1/28 ports as edge ports by using the **spanning-tree port type edge** command.

```
N5K-A(config-if)# interface e1/28
N5K-A(config-if)# spanning-tree port type edge
Warning: Edge port type (portfast) should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches, bridges, etc...
to this interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
Use with CAUTION
```

Edge Port Type (Portfast) has been configured on Ethernet1/28 but will only have effect when the interface is in a non-trunking mode.

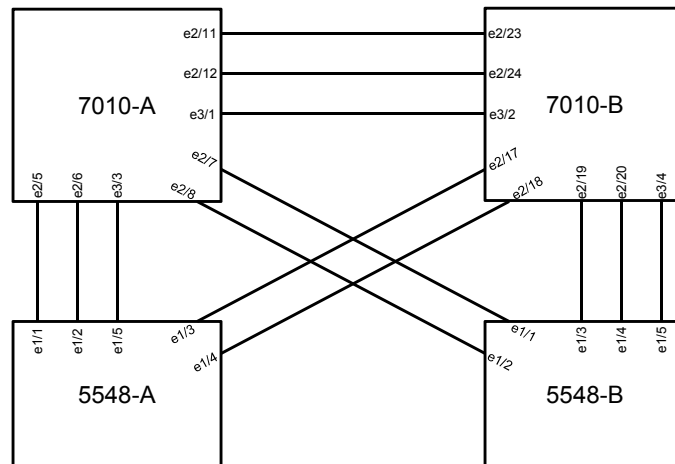
```
N5K-A(config-if)#
```

- Step 9** Verify that the port N5K e1/28 ports are now edge ports by using the **show spanning-tree interface e1/28** command.

```
N5K-A(config-if)# show spanning-tree interface e1/28
```

Vlan	Role	Sts	Cost	Prio.Nbr	Type
VLAN0011	Desg	FWD	4	128.156	Edge P2p Peer (STP)

Spanning Tree Topology Diagram (VLAN1)



© 2012 Cisco and/or its affiliates. All rights reserved.

DCICN v1.0--6-12

- Step 10** Using the topology diagram for VLAN1, indicate which switch is the root for VLAN1.
- Step 11** Using the topology diagram, indicate which port on each switch is the root port for VLAN 1.
- Step 12** Using the topology diagram, indicate which ports are blocking by placing an “X” over the interfaces.
- Step 13** Compare the VLAN 1 topology with the VLAN 11 topology from task 1.

Activity Verification

You have completed this task when you attain these results:

- You have configured the root bridge for VLAN 11.
- You have determined the new VLAN 11 topology.
- You have configured the e1/28 ports on the Cisco Nexus 5000 Series Switches as edge ports.
- You have validated that there are two separate spanning tree instances: one for VLAN 1 and another for VLAN 11.

Task 3: Verify Spanning Tree Failover

In this task, you will verify the failover capability of the STP.

Activity Procedure

Complete the following steps on all switches.

- Step 1** Determine which ports on the Cisco Nexus 5000 Series Switches are the root ports using the **show spanning-tree vlan 11** command or by using the topology diagram from the previous task.
- Step 2** From a command prompt on the PC, start a continuous ping to the other PC using the **ping 192.168.11.x -t** command where x = the last octet of the neighbor PC.
- Step 3** With the command prompt window visible, shut down the root port of the Cisco Nexus 5000 Series Switch and observe if there are any dropped pings.
- Step 4** View the spanning tree topology using the **show spanning-tree vlan 11** command and verify that a new root port has been selected.
- Step 5** Enable the port that was shut down in Step 3.

When spanning tree converges, it is not unusual to have a brief interruption in traffic flow. This can show up as a single dropped ping. However, it is also possible that no packets are dropped.

- Step 6** Save the running-config using the **copy running-config startup-config** command. Perform this step on all switches!

```
F103-Nexus-7010-Prod_A# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
```

Activity Verification

You have completed this task when you attain this result:

- You have validated the failover of the STP.

Lab 2-4 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:45:16 2012

version 6.0(2)
hostname Prod_A

feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1  
spanning-tree vlan 11 priority 16384
```

```
interface Ethernet2/1
```

```
interface Ethernet2/2
```

```
interface Ethernet2/3
```

```
interface Ethernet2/4
```

```
interface Ethernet2/5  
  description Link to N5K-A 1/1  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet2/6  
  description Link to N5K-A 1/2  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet2/7  
  description Link to N5K-B 1/1  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet2/8  
  description Link to N5K-B 1/2  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet2/9
```

```
interface Ethernet2/10
```

```
interface Ethernet2/11  
  description Link to N7K-B 2/23  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet2/12  
  description Link to N7K-B 2/24  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet2/25
```

```
interface Ethernet2/26
```

```
interface Ethernet3/1  
  description Link to N7K-B 3/2  
  switchport  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet3/3  
  description Link to N5K-A 1/5  
  switchport  
  switchport mode trunk  
  no shutdown
```

```
interface Ethernet3/5  
  switchport
```

```

interface Ethernet3/7
    switchport

interface Ethernet3/9
    switchport

interface Ethernet3/11
    switchport

interface Ethernet3/13
    switchport

interface Ethernet3/15
    switchport

interface Ethernet3/17
    switchport

interface Ethernet3/19
    switchport

interface Ethernet3/21
    switchport

interface Ethernet3/23
    switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
    ip address 172.16.1.201/24
    line vty

```

Lab 2-4 Cisco Nexus 5000 Series Switch Configuration

```

!Command: show running-config
!Time: Sat Jun  9 14:44:05 2012

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lldp
feature vtp

username admin password 5 $1$aSodBomR$h7immj0YTBsjhQlsiy/hR/ role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1

```

```

class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
  ip route 0.0.0.0/0 172.16.1.1

interface Ethernet1/1
  description Link to N7K-A 2/5
  switchport mode trunk

interface Ethernet1/2
  description Link to N7K-A 2/6
  switchport mode trunk

interface Ethernet1/3
  description Link to N7K-B 2/17
  switchport mode trunk

interface Ethernet1/4
  description Link to N7K-B 2/18
  switchport mode trunk

interface Ethernet1/5
  description Link to N7K-A 3/3
  switchport mode trunk

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

```

```
interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28
  description Link to PC-A Lab2
  switchport access vlan 11
  spanning-tree port type edge
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 2-5: Configuring EtherChannel

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

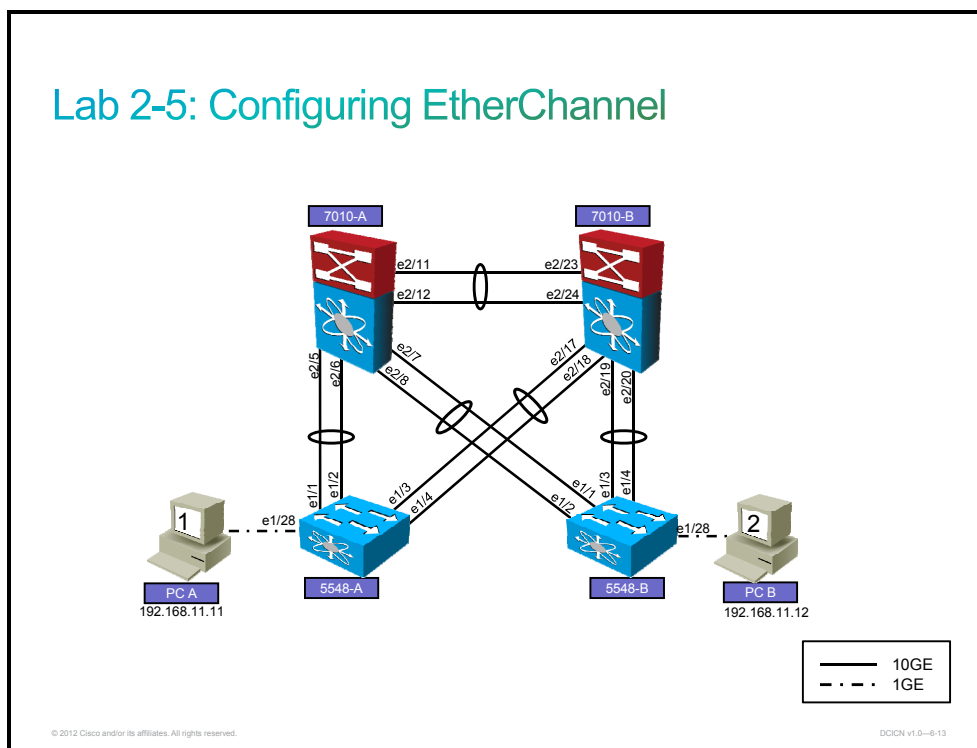
Activity Objective

In this lab, you will connect to the Cisco Nexus 5000 Series and Cisco Nexus 7000 Series Switches to configure and validate EtherChannel. After completing this activity, you will be able to meet these objectives:

- Configure EtherChannel
- Use the **show** commands to validate EtherChannel configuration

Visual Objective

The figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 5000 Series Switches
- One PC with an SSH application for remote connectivity to the Cisco Nexus switches

Command List

This table describes the commands used in this activity.

Command	Description
channel-group <i>num</i> mode active	Defines current interface as a member of specified EtherChannel group in LACP active mode
feature <i>name</i>	Enables the specified feature
interface <i>type num</i>	Enters interface configuration mode for the specified interface
show spanning-tree	Displays spanning tree information
show port-channel summary	Displays EtherChannel summary information
spanning-tree pathcost method long	Enables long path cost algorithm

Task 1: Prepare Topology for EtherChannel

In this task, you will use CLI commands to set up the topology for EtherChannel.

Note	This lab builds on the configurations of the previous labs.
-------------	---

Activity Procedure

Complete the following steps on all switches.

Note	The switch outputs and configuration steps are samples. Your actual input and output may be different from the samples shown.
-------------	---

While EtherChannel can work with two to eight physical links, the hashing algorithm is optimized for bundles of two, four, or eight links. Using the following table, disable the third ISLs.

Device	Interface
N7K-A	e3/1
N7K-A	e3/3
N7K-B	e3/2
N7K-B	e3/4
N5K-A	e1/5
N5K-B	e1/5

```
F103-Nexus-7010-Prod_A(config)# int e3/1,e3/3
F103-Nexus-7010-Prod_A(config-if)# shut
```

```
F103-Nexus-7010-Prod_B(config)# int e3/2,e3/4
F103-Nexus-7010-Prod_B(config-if)# shut
```

```
N5K-A(config)# int e1/5
N5K-A(config-if)# shut
```

```
N5K-B(config)# int e1/5
N5K-B(config-if)# shut
```

Step 7 Review the spanning tree topology using the **show spanning-tree vlan 11** command.

The topology is basically the same as the previous lab. The only difference is the absence of the third links between some of the switches that were blocking in the previous labs. Even though there are two 10-Gb/s links between the Cisco Nexus 5000 Series Switches and the Cisco Nexus 7000 Series Switches, only one is forwarding traffic.

Activity Verification

You have completed this task when you attain this result:

- You have only two ISLs between all switches.

Task 2: Configure EtherChannel

In this task, you will use CLI commands to configure EtherChannel.

Activity Procedure

Complete the following steps on all switches.

Step 1 LACP is used to negotiate the EtherChannel groups between the switches. Enable the LACP feature using the **feature lacp** command on all switches.

```
F103-Nexus-7010-Prod_A(config)# feature lacp
```

Step 2 Configure the physical interface on the switches to be grouped into EtherChannel groups (also known as port channels). The following table lists the interfaces and group numbers.

Device	Interface	Group
N7K-A	e2/5-6	1
N7K-A	e2/7-8	5
N7K-A	e2/11-12	2
N7K-B	e2/17-18	3
N7K-B	e2/19-20	4
N7K-B	e2/23-24	2
N5K-A	e1/1-2	1
N5K-A	e1/3-4	3
N5K-B	e1/1-2	5
N5K-B	e1/3-4	4

```
F103-Nexus-7010-Prod_A(config)# int e2/5-6
F103-Nexus-7010-Prod_A(config-if-range)# channel-group 1 mode active
F103-Nexus-7010-Prod_A(config-if-range)# int e2/7-8
F103-Nexus-7010-Prod_A(config-if-range)# channel-group 5 mode active
F103-Nexus-7010-Prod_A(config-if-range)# int e2/11-12
F103-Nexus-7010-Prod_A(config-if-range)# channel-group 2 mode active
```

Step 3 Verify that the EtherChannel groups are functional using the **show port-channel summary** command on all switches.

```
F103-Nexus-7010-Prod_A(config-if-range)# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```
-----
Group Port-      Type      Protocol  Member Ports
      Channel
-----
1      Po1 (SU)    Eth       LACP      Eth2/5 (P)  Eth2/6 (P)
2      Po2 (SU)    Eth       LACP      Eth2/11 (P) Eth2/12 (P)
5      Po5 (SU)    Eth       LACP      Eth2/7 (P)  Eth2/8 (P)
```

An upper-case “U” in the Group Port-Channel column indicates that the EtherChannel group is up. An upper-case “P” next to each port in the Member Ports column indicates that the physical port is part of the EtherChannel group.

Step 4 Verify the spanning tree topology using the **show spanning-tree vlan 11** command.

```
N5K-A(config-if-range)# show spanning-tree vlan 11
```

```
VLAN0011
```

```
Spanning tree enabled protocol rstp
Root ID    Priority    16395
           Address    64a0.e743.03c2
           Cost        1
           Port        4096 (port-channel1)
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID  Priority    32779 (priority 32768 sys-id-ext 11)
           Address    547f.ee5c.6efc
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Po1	Root	FWD	1	128.4096	P2p	
Po3	Desg	FWD	1	128.4098	P2p	
Eth1/28	Desg	FWD	4	128.156	P2p	Peer (STP)

Notice the physical interfaces that are part of the EtherChannel group no longer appear in the spanning tree topology. They have been replaced by the virtual “Port-Channel” interfaces.

A potential issue is the costing method used by spanning tree. An interface with a speed greater than 10 Gb/s has a cost of 1. In this topology, the EtherChannel links, which are presented as 20 Gb/s, are showing a cost of 1. As an example, if there were a 40-Gb/s link, spanning tree might not select that link as better than a 20-Gb/s link. This potential issue can be resolved by changing the costing method from short (the RSTP default) to long.

Step 5 On all switches, change the costing method to long using the **spanning-tree pathcost method long** command.

```
F103-Nexus-7010-Prod_A(config)# spanning-tree pathcost method long
```

Step 6 Verify the new spanning tree cost using the **show spanning-tree vlan 11** command.

```
N5K-A(config)# show spanning-tree vlan 11
```

```
VLAN0011
```

```
Spanning tree enabled protocol rstp
Root ID    Priority    16395
           Address    64a0.e743.03c2
           Cost        1000
           Port        4096 (port-channel1)
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID  Priority    32779 (priority 32768 sys-id-ext 11)
           Address    547f.ee5c.6efc
           Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Po1	Root	FWD	1000	128.4096	P2p	
Po3	Desg	FWD	1000	128.4098	P2p	
Eth1/28	Desg	FWD	20000	128.156	P2p	Peer (STP)

Step 7 Save the running-config using the **copy running-config startup-config** command.
Perform this step on all switches!

```
F103-Nexus-7010-Prod_A# 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 created EtherChannel links between the switches.
- You have changed the pathcost method used by spanning tree.

Lab 2-5 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:52:59 2012

version 6.0(2)
hostname Prod_A

feature lacp
feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long
spanning-tree vlan 11 priority 16384

interface port-channel1
switchport
switchport mode trunk

interface port-channel2
switchport
switchport mode trunk

interface port-channel5
switchport
switchport mode trunk

interface Ethernet2/1

interface Ethernet2/2
```

```

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
  description Link to N5K-A 1/1
  switchport mode trunk
  channel-group 1 mode active
  no shutdown

interface Ethernet2/6
  description Link to N5K-A 1/2
  switchport mode trunk
  channel-group 1 mode active
  no shutdown

interface Ethernet2/7
  description Link to N5K-B 1/1
  switchport mode trunk
  channel-group 5 mode active
  no shutdown

interface Ethernet2/8
  description Link to N5K-B 1/2
  switchport mode trunk
  channel-group 5 mode active
  no shutdown

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
  description Link to N7K-B 2/23
  switchport mode trunk
  channel-group 2 mode active
  no shutdown

interface Ethernet2/12
  description Link to N7K-B 2/24
  switchport mode trunk
  channel-group 2 mode active
  no shutdown

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  description Link to N7K-B 3/2
  switchport
  switchport mode trunk

interface Ethernet3/3
  description Link to N5K-A 1/5
  switchport
  switchport mode trunk

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

```

```

interface Ethernet3/11
    switchport

interface Ethernet3/13
    switchport

interface Ethernet3/15
    switchport

interface Ethernet3/17
    switchport

interface Ethernet3/19
    switchport

interface Ethernet3/21
    switchport

interface Ethernet3/23
    switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
    ip address 172.16.1.201/24
    line vty

```

Lab 2-5 Cisco Nexus 5000 Series Switch Configuration

```

!Command: show running-config
!Time: Sat Jun  9 14:52:05 2012

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lacp
feature lldp
feature vtp

username admin password 5 $1$aS0dB0mR$h7immj0YTBsjhQlsiy/hR/ role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2

```

```

snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
  ip route 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long

interface port-channel1
  switchport mode trunk

interface port-channel3
  switchport mode trunk

interface Ethernet1/1
  description Link to N7K-A 2/5
  switchport mode trunk
  channel-group 1 mode active

interface Ethernet1/2
  description Link to N7K-A 2/6
  switchport mode trunk
  channel-group 1 mode active

interface Ethernet1/3
  description Link to N7K-B 2/17
  switchport mode trunk
  channel-group 3 mode active

interface Ethernet1/4
  description Link to N7K-B 2/18
  switchport mode trunk
  channel-group 3 mode active

interface Ethernet1/5
  description Link to N7K-A 3/3
  shutdown
  switchport mode trunk

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

```

```
interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28
  description Link to PC-A Lab2
  switchport access vlan 11
  spanning-tree port type edge
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 3-1: Converting Decimal to Binary and Binary to Decimal

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

Activity Objective

In this activity, you will convert decimal and binary numbers. After completing this activity, you will be able to meet these objectives:

- Convert decimal numbers to binary
- Convert binary numbers to decimal

Visual Objective

This figure shows what you will accomplish in this activity.

Lab 3-1: Converting Decimal to Binary, and Binary to Decimal

Converting Decimal to Binary

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Decimal	128	64	32	16	8	4	2	1	Binary
48	0	0	1	1	0	0	0	0	48 = 32 + 16 = 00110000

Converting Binary to Decimal

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Binary	128	64	32	16	8	4	2	1	Decimal
11001100	1	1	0	0	1	1	0	0	128+64+8+4= 204

© 2012 Cisco and/or its affiliates. All rights reserved. DCICN v1.0--6-14

Required Resources

No resources are required for this activity.

Command List

No commands are used in this activity.

Task 1: Convert from Decimal Notation to Binary Format

Activity Procedure

Complete the following table, which provides practice in converting a number from decimal notation to binary format.

Base 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Decimal	128	64	32	16	8	4	2	1	Binary
48	0	0	1	1	0	0	0	0	48 = 32 + 16 = 00110000
146	1	0	0	1					
222									
119									
135									
60									

Task 2: Convert from Binary Notation to Decimal Format

Activity Procedure

Complete the following table, which provides practice in converting a number from binary notation to decimal format.

Base 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	128	64	32	16	8	4	2	1	Decimal
11001100	1	1	0	0	1	1	0	0	128 + 64 + 8 + 4 = 204
10101010	1	0	1	0					
11100011									
10110011									
00110101									
10010111									

Activity Verification

You have completed this lab when you attain these results:

- You can accurately convert decimal format numbers to binary notation.
- You can accurately convert binary notation numbers to decimal format.

Lab 3-2: Classifying Network Addressing

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

Activity Objective

In this activity, you will classify network addresses with IPv4 and IPv6. After completing this activity, you will be able to meet these objectives:

- Convert decimal IP addresses to binary numbers
- Convert binary numbers to IP addresses
- Identify classes of IP addresses
- Identify valid and invalid host IP addresses

Visual Objective

This figure shows what you will accomplish in this activity.

Lab 3-2: Classifying Network Addressing

Convert decimal IP address to binary

- 145.32.59.21 =
10010001.00100000._____._____

Convert binary IP address to decimal

- 10010001.00011011.00111101.10001001 =
216.____.____.____

Identify IP Address Classes

	Decimal IP Address	Address Class	Number of Bits in Network ID	Maximum Number of Hosts (2 ⁿ -2)
10010001.00100000.00111011.00011000	145.32.59.24	Class B	16	
11001000.00101010.10000001.00010000	200.42.129.16			

23.75.345.200? 0.124.0.0? 255.255.255.255?

© 2012 Cisco and/or its affiliates. All rights reserved. DCICN v1.0-6-15

Required Resources

No resources are required for this activity.

Command List

No commands are used in this activity.

Task 1: Convert from Decimal IP Address to Binary Format

Activity Procedure

Complete the following table to express 145.32.59.24 in binary format.

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Decimal	128	64	32	16	8	4	2	1	Binary
145	1	0	0	1	0	0	0	1	10010001
32	0	0	1	0	0	0	0	0	00100000
59									
24									
Binary Format IP Address						10010001. 00100000. _____ . _____			

Complete the following table to express 200.42.129.16 in binary format.

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Decimal	128	64	32	16	8	4	2	1	Binary
200									
42									
129									
16									
Binary Format IP Address									

Complete the following table to express 14.82.19.54 in binary format.

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Decimal	128	64	32	16	8	4	2	1	Binary
14									
82									
19									
54									
Binary Format IP Address									

Task 2: Convert from Binary Format to Decimal IP Address

Activity Procedure

Complete the following table to express 11011000.00011011.00111101.10001001 in decimal IP address format.

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Binary	128	64	32	16	8	4	2	1	Decimal
11011000	1	1	0	1	1	0	0	0	216
00011011									
00111101									
10001001									
Decimal Format IP Address						216.____.____.____			

Complete the following table to express 11000110.00110101.10010011.00101101 in decimal IP address format.

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Binary	128	64	32	16	8	4	2	1	Decimal
11000110									
00110101									
10010011									
00101101									
Decimal Format IP Address									

Complete the following table to express 01111011.00101101.01000011.01011001 in decimal IP address format.

Base 2	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	
Binary	128	64	32	16	8	4	2	1	Decimal
01111011									
00101101									
01000011									
01011001									
Decimal Format IP Address									

Task 3: Identify IP Address Classes

Activity Procedure

Complete this table to identify the address class, number of bits in the network ID, and maximum number of hosts.

Binary IP Address	Decimal IP Address	Address Class	Number of Bits in Network ID	Maximum Number of Hosts ($2^h - 2$)
10010001.00100000.00111011.00011000	145.32.59.24	Class B	16	
11001000.00101010.10000001.00010000	200.42.129.16			
00001110.01010010.00010011.00110110	14.82.19.54			
11011000.00011011.00111101.10001001	216.27.61.137			
10110011.00101101.01000011.01011001	179.45.67.89			
11000110.00110101.10010011.00101101	198.53.147.45			

Task 4: Identify Valid and Invalid Host IP Addresses

Activity Procedure

Complete the following table to identify which host IP addresses are valid and which are not valid.

Decimal IP Address	Valid or Invalid	If Invalid, Indicate Reason
23.75.345.200		
216.27.61.134		
102.54.94		
255.255.255.255		
142.179.148.200		
200.42.129.16		
0.124.0.0		

Activity Verification

You have completed this lab when you attain these results:

- You can accurately convert decimal format IP addresses to binary format.
- You can accurately convert binary format IP addresses to decimal format.
- You can identify the address class of a given IP address.
- You can identify valid and invalid IP addresses.

Lab 3-3: Computing Usable Subnetworks and Hosts

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

Activity Objective

In this activity, you will determine the number of bits to borrow from the host ID to create the required number of subnets for a given IP address. After completing this activity, you will be able to meet these objectives:

- Determine the number of bits that are required to create different subnets
- Determine the maximum number of host addresses that are available in a given subnet

Visual Objective

This figure shows what you will accomplish in this activity.

Lab 3-3: Computing Usable Subnetworks and Hosts

Given the following information:

- Class C network address of 192.168.89.0
- Class B network address of 172.25.0.0
- Class A network address of 10.0.0.0

How many subnets can you create?

How many hosts per subnet can you create?

© 2012 Cisco and/or its affiliates. All rights reserved. DCICN v1.0--6-16

Required Resources

No resources are required for this lab activity.

Command List

No commands are used in this activity.

Task 1: Determine the Number of Bits Required to Subnet a Class C Network

Activity Procedure

Given a Class C network address of 192.168.89.0, complete the table to identify the number of bits that are required to define the specified number of subnets for the network. Then, determine the number of hosts per subnet.

Number of Subnets	Number of Bits to Borrow	Number of Hosts Per Subnet ($2^h - 2$)
2		
5		
12		
24		
40		

Task 2: Determine the Number of Bits Required to Subnet a Class B Network

Activity Procedure

Given a Class B network address of 172.25.0.0, complete the table to identify the number of bits that are required to define the specified number of subnets for the network. Then, determine the number of hosts per subnet.

Number of Subnets	Number of Bits to Borrow	Number of Hosts Per Subnet ($2^h - 2$)
5		
8		
14		
20		
35		

Task 3: Determine the Number of Bits Required to Subnet a Class A Network

Activity Procedure

Given a Class A network address of 10.0.0.0, complete the table to identify the number of bits that are required to define the specified number of subnets for the network. Then, determine the number of hosts per subnet.

Number of Subnets	Number of Bits to Borrow	Number of Hosts Per Subnet ($2^h - 2$)
10		
14		
20		
40		
80		

Activity Verification

You have completed this lab when you attain these results:

- Given a Class A, B, or C network, you can identify the number of bits to borrow to create a given number of subnets.
- Given a Class A, B, or C network, with a specified number of subnets and number of bits to borrow, you can determine the total number of hosts and the number of hosts per subnet .

Lab 3-4: Calculating Subnet Masks

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

Activity Objective

In this activity, you will calculate subnet masks. After completing this activity, you will be able to meet these objectives:

- Given a network address, determine the number of possible network addresses and the binary subnet mask to use
- Given a network IP address and subnet mask, determine the range of subnet addresses
- Identify the host addresses that can be assigned to a subnet and the associated broadcast addresses

Visual Objective

This figure shows what you will accomplish in this activity.

Lab 3-4: Calculating Subnet Masks

- Given a network address, determine the number of possible network addresses and the binary subnet mask to use.
- Given a network IP address and subnet mask, determine the range of subnet addresses.
- Identify the host addresses that can be assigned to a subnet and the associated broadcast addresses.

Remember

Eight Easy Steps to Determining
Subnet Addresses

© 2012 Cisco and/or its affiliates. All rights reserved. DOCN v1.0-6-17

Required Resources

No resources are required for this lab activity.

Command List

No commands are used in this activity.

Task 1: Determine the Number of Possible Network Addresses

Activity Procedure

Given a Class A network and the net bits identified, complete this table to identify the subnet mask and the possible number of host addresses for each mask.

Classful Address	Decimal Subnet Mask	Binary Subnet Mask	Number of Hosts Per Subnet ($2^h - 2$)
/20			
/21			
/22			
/23			
/24			
/25			
/26			
/27			
/28			
/29			
/30			

Task 2: Given a Network Address, Define Subnets

Activity Procedure

Assume that you have been assigned the 172.25.0.0 /16 network. You need to establish 12 subnets. Complete the following questions.

- How many bits do you need to borrow to define 12 subnets?

- Specify the classful address and subnet mask in binary and decimal that allows you to create 12 subnets.

- Use the eight-step method to define the 12 subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write down the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits 4 times.	
5.	In the first line, define the network address by placing 0s in the remaining host bits.	

Step	Description	Example
6.	In the last line, define the directed-broadcast address by placing 1s in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by 1 to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			
...			

Task 3: Given Another Network Address, Define Subnets

Activity Procedure

Assume that you have been assigned the 192.168.1.0 /24 network.

- How many bits do you need to borrow to define six subnets? _____
- Specify the classful address and subnet mask in binary and decimal that allows you to create six subnets.

- Use the eight-step method to define the six subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write down the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits 4 times.	
5.	In the first line, define the network address by placing 0s in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing 1s in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by 1 to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

- Complete this table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Task 4: Given a Network Address and Classful Address, Define Subnets

Activity Procedure

Assume that you have been assigned the 192.168.111.129 address in a /28 network block.

- Specify the subnet mask in binary and decimal.

- How many subnets can you define with the specified mask?

3. How many hosts will be in each subnet?

4. Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write down the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits 4 times.	
5.	In the first line, define the network address by placing 0s in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing 1s in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by 1 to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

5. Complete this table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Task 5: Given a Network Block and Classful Address, Define Subnets

Activity Procedure

Assume that you have been assigned the 172.25.112.0 address in a /23 network block.

1. Specify the subnet mask in binary and decimal.

2. How many subnets can you define with the specified mask?

3. How many hosts will be in each subnet?

4. Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write down the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits 4 times.	
5.	In the first line, define the network address by placing 0s in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing 1s in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by 1 to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

5. Complete this table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Task 6: Given a Network Block and Classful Address, Define Subnets

Activity Procedure

Assume that you have been assigned the 172.20.0.129 address in a /25 network block.

1. Specify the subnet mask in binary and decimal.

2. How many subnets can you define with the specified mask?

3. How many hosts will be in each subnet?

4. Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write down the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits 4 times.	
5.	In the first line, define the network address by placing 0s in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing 1s in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by 1 to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

5. Complete this table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Activity Verification

You have completed this lab when you attain these results:

- Given a network address, you can determine the number of possible network addresses and the binary subnet mask to use.
- Given a network IP address and subnet mask, you can apply the mask to determine the range of subnet addresses.
- You can apply subnet masks to identify the host addresses that can be assigned to a subnet and the associated broadcast addresses.

Lab 4-1: Configuring Multilayer Switching

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

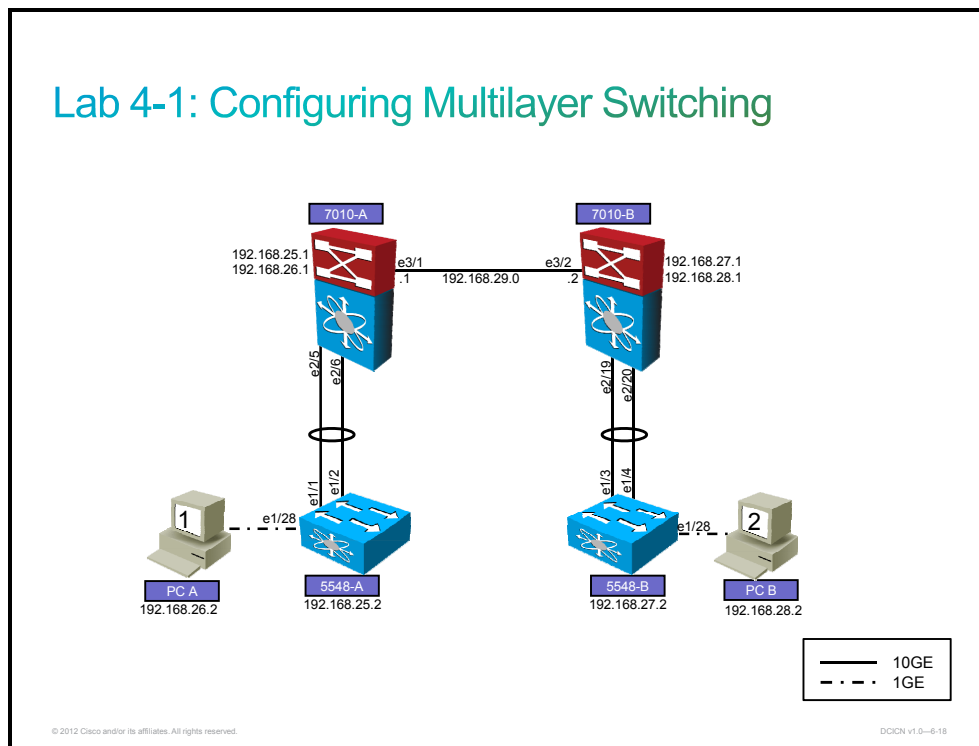
Activity Objective

In this lab, you will connect to the Cisco Nexus 5000 Series Switches and Cisco Nexus 7000 Series Switches to configure and verify multilayer switching. After completing this activity, you will be able to meet these objectives:

- Create Switched Virtual Interfaces (SVI)
- Create Layer 3 interfaces
- Use the **show** commands to verify multilayer switching and view the routing table

Visual Objective

The following figure shows what you will accomplish in this activity.



Required Resources

These resources and equipment are required to complete this activity:

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 5000 Series Switches
- One PC with an SSH application for remote connectivity to the Cisco Nexus switches

Command List

This table describes the commands used in this activity.

Command	Description
feature <i>name</i>	Enables the specified feature
interface <i>type number</i>	Enters interface configuration mode for the specified interface
ip address <i>address/prefix</i>	Assigns the specified IP address to the current interface
router eigrp <i>PID</i>	Creates an EIGRP routing process with the specified process ID
ping <i>address</i>	Sends ICMP echo requests to the specified address
ip router eigrp <i>PID</i>	Enables EIGRP on the current interface
show interface status	Displays the interface status
[no] shutdown	Disables the current interface
show ip eigrp neighbors	Displays information about EIGRP neighbors
show ip interface brief	Displays a summary of the IP interface configuration
show ip route	Displays the IP routing table
show ip route eigrp	Displays the EIGRP IP routing table
show interface status	Displays the interface status
show running-config	Displays the current configuration
[no] switchport	Defines the current interface as Layer 2
switchport access vlan <i>number</i>	Defines the current interface as member of the specified VLAN

Task 1: Configure Multilayer Switching

In this task, you will use CLI commands to configure and verify multilayer switching.

Note This lab builds on the configurations of the previous labs.

Activity Procedure

Complete the following steps on all the switches.

Note The switch outputs and configuration steps are samples. Your actual input and output might be different from the samples shown.

Step 1 Disable the Layer 2 ISLs between the Cisco Nexus 7000 Series Switches and the links between your Cisco Nexus 7000 Series Switch and your neighbor's Cisco Nexus 5000 Series Switch. The following table summarizes the interfaces that are disabled in this step.

N7K-A

Device	Interface	Neighbor & Interface
N7K-A	e2/7	N5K-B e1/1
N7K-A	e2/8	N5K-B e1/2
N7K-A	e2/11	N7K-B e2/23
N7K-A	e2/12	N7K-B e2/24

N5K-A

Device	Interface	Neighbor & Interface
N5K-A	e1/3	N7K-B e2/17
N5K-A	e1/4	N7K-B e2/18

N7K-B

Device	Interface	Neighbor & Interface
N7K-B	e2/17	N5K-A e1/3
N7K-B	e2/18	N5K-A e1/4
N7K-B	e2/23	N7K-A e2/11
N7K-B	e2/24	N7K-A e2/12

N5K-B

Device	Interface	Neighbor & Interface
N5K-B	e1/1	N7K-A e2/7
N5K-B	e1/2	N7K-A e2/8

```
F103-Nexus-7010-Prod_A# config
Enter configuration commands, one per line. End with CNTL/Z.
F103-Nexus-7010-Prod_A(config-if-range)# int e2/7-8,e2/11-12
F103-Nexus-7010-Prod_A(config-if-range)# shutdown
^
```

```
F103-Nexus-7010-Prod_B# config
```

```
Enter configuration commands, one per line. End with CNTL/Z.
F103-Nexus-7010-Prod_A(config-if-range)# int e2/17-18,e2/23-24
F103-Nexus-7010-Prod_A(config-if-range)# shutdown
```

```
N5K-A# config
Enter configuration commands, one per line. End with CNTL/Z.
N5K-A(config)# int e1/3-4
N5K-A(config-if-range)# shutdown
```

```
N5K-B# config
Enter configuration commands, one per line. End with CNTL/Z.
N5K-B(config)# int e1/1-2
N5K-B(config-if-range)# shutdown
```

Step 2 On the Cisco Nexus 5000 Series Switches, create two VLANs. One will be used by the PC and the other will be for in-band communications to the Cisco Nexus 5000 Series Switch. Refer to the following table for the VLAN assignments. You will not need to create the VLANs on the Cisco Nexus 7000 Series Switches because VTP will propagate these VLANs.

Device	Interface
N5K-A	25, 26
N5K-B	27, 28

```
N5K-A(config)# vlan 25-26
N5K-A(config-vlan)# exit
N5K-A(config)#
```

```
N5K-B(config)# vlan 27-28
N5K-B(config-vlan)# exit
N5K-B(config)#
```

Step 3 Make the interface that connects to the PCs a member of the even-numbered VLAN that you just created.

Device	VLANs	Interface
N5K-A	26	e1/28
N5K-B	28	e1/28

```
N5K-A(config)# interface e1/28
N5K-A(config-if)# switchport access vlan 26
-or-
N5K-B(config)# interface e1/28
N5K-B(config-if)# switchport access vlan 28
```

Step 4 Configure the link between the two Cisco Nexus 7000 Series Switches as a Layer 3 link, assign an IP address and enable the interface.

Device	Interface	IP Address
N7K-A	e3/1	192.168.29.1/24
N7K-B	e3/2	192.168.29.2/24

```
F103-Nexus-7010-Prod_B(config)# int e3/2
F103-Nexus-7010-Prod_B(config-if)# no switchport
F103-Nexus-7010-Prod_B(config-if)# ip address 192.168.29.2/24
F103-Nexus-7010-Prod_B(config-if)# no shut
```

Step 5 Verify the Layer 3 link using the **show interface status** and **show ip interface brief** commands.

```
F103-Nexus-7010-Prod_B(config-if)# show interface status
```

```
-----
Port          Name                Status      Vlan      Duplex  Speed  Type
-----
-output omitted-
Eth2/23       Link to N7K-A e2/1 disabled trunk    auto    auto   SFP-H10GB-C
Eth2/24       Link to N7K-A 2/12 disabled trunk    auto    auto   SFP-H10GB-C
Eth3/2       Link to N7K-A 3/1 connected routed    full    10G    SFP-H10GB-C
Eth3/4       Link to N5K-B 1/5 disabled trunk    full    auto   SFP-H10GB-C
Eth3/6       --                  sfpAbsent 1          full    auto   --
-output omitted-
```

```
F103-Nexus-7010-Prod_B(config-if)# show ip interface brief
```

```
IP Interface Status for VRF "default"(1)
```

```
Interface      IP Address      Interface Status
Eth3/2       192.168.29.2   protocol-up/link-up/admin-up
```

Step 6 Validate connectivity over the Layer 3 link by pinging the IP address assigned to the other end of the link. If the ping fails, verify that you have assigned the correct IP address to your interface and that you are pinging the correct IP address.

```
F103-Nexus-7010-Prod_B(config-if)# ping 192.168.29.1
```

```
PING 192.168.29.1 (192.168.29.1): 56 data bytes
64 bytes from 192.168.29.1: icmp_seq=0 ttl=254 time=1.045 ms
64 bytes from 192.168.29.1: icmp_seq=1 ttl=254 time=0.817 ms
64 bytes from 192.168.29.1: icmp_seq=2 ttl=254 time=0.71 ms
64 bytes from 192.168.29.1: icmp_seq=3 ttl=254 time=0.725 ms
64 bytes from 192.168.29.1: icmp_seq=4 ttl=254 time=0.728 ms
```

```
--- 192.168.29.1 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.71/0.805/1.045 ms
```

Step 7 Enable the SVI feature (interface-vlan) on all the switches using the **feature interface-vlan** command.

```
N5K-A(config)# feature interface-vlan
```

Step 8 The Cisco Nexus 5000 Series Switches do not have Layer 3 routing capabilities. However, it is possible to create an SVI and assign an IP address. This interface will be used as a destination for ping traffic. Create an SVI on the Cisco Nexus 5000 Series Switch and assign the IP address shown in the following table for the appropriate switch.

Device	Interface	IP Address
N5K-A	vlan 25	192.168.25.2/24
N5K-B	vlan 27	192.168.27.2/24

```
N5K-A(config)# interface vlan 25
```

```
N5K-A(config-if)# ip address 192.168.25.2/24
```

```
N5K-A(config-if)# no shut
```

- Step 9** The Cisco Nexus 5000 Series Switches will also need a default route that will forward nonlocal traffic to the Cisco Nexus 7000 Series Switch.

Device	Default Gateway
N5K-A	192.168.25.1
N5K-B	192.168.27.1

```
N5K-A(config-if)# ip route 0.0.0.0 0.0.0.0 192.168.25.1
-or-
N5K-B(config-if)# ip route 0.0.0.0 0.0.0.0 192.168.27.1
```

- Step 10** The Cisco Nexus 7000 Series Switches will be performing the routing between the networks. Create two SVIs on each Cisco Nexus 7000 Series Switch and assign the IP addresses listed here.

Device	Interface	IP Address
N7K-A	vlan 25	192.168.25.1/24
N7K-A	vlan 26	192.168.26.1/24
N7K-B	vlan 27	192.168.27.1/24
N7K-B	vlan 28	192.168.28.1/24

```
F103-Nexus-7010-Prod_A(config)# interface vlan 25
F103-Nexus-7010-Prod_A(config-if)# ip address 192.168.25.1/24
F103-Nexus-7010-Prod_A(config-if)# no shut
F103-Nexus-7010-Prod_A(config-if)# interface vlan 26
F103-Nexus-7010-Prod_A(config-if)# ip address 192.168.26.1/24
F103-Nexus-7010-Prod_A(config-if)# no shut
```

- Step 11** Configure the IP address on the Lab2 NIC of the PCs. Click **Start > Control Panel > Network Connections > Lab2** to open the Lab2 Status dialog window.
- Step 12** In the **Lab2 Status** window, click the **Properties** button.
- Step 13** In the **Lab2 Properties** window, highlight **Internet Protocol (TCP/IP)** and click the **Properties** button.
- Step 14** Change the IP address from 192.168.11.xx to the appropriate address shown in the following table. Leave the mask at 255.255.255.0 and do not define a default gateway. Static routes have already been added, so there is no need for a default gateway.

Device	Default Gateway
PC A	192.168.26.2
PC B	192.168.28.2

- Step 15** Click **OK**, click **OK** again, and close.

Step 16 Display the routing table on the two Cisco Nexus 7000 Series Switches.

```
F103-Nexus-7010-Prod_A(config-if)# show 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>

192.168.25.0/24, ubest/mbest: 1/0, attached
    *via 192.168.25.1, Vlan25, [0/0], 00:22:40, direct
192.168.25.1/32, ubest/mbest: 1/0, attached
    *via 192.168.25.1, Vlan25, [0/0], 00:22:40, local
192.168.26.0/24, ubest/mbest: 1/0, attached
    *via 192.168.26.1, Vlan26, [0/0], 00:22:29, direct
192.168.26.1/32, ubest/mbest: 1/0, attached
    *via 192.168.26.1, Vlan26, [0/0], 00:22:29, local
192.168.29.0/24, ubest/mbest: 1/0, attached
    *via 192.168.29.1, Eth3/1, [0/0], 00:22:16, direct
192.168.29.1/32, ubest/mbest: 1/0, attached
    *via 192.168.29.1, Eth3/1, [0/0], 00
```

Step 17 Notice that two entries correspond to each connected network. One is identified as “direct,” which indicates the network, and the other is identified as “local,” which shows the IP address assigned to the interface that is connected to that network. You can filter the output by appending the keyword **direct** to the **show ip route** command.

```
F103-Nexus-7010-Prod_A(config-if)# show ip route direct
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>

192.168.25.0/24, ubest/mbest: 1/0, attached
    *via 192.168.25.1, Vlan25, [0/0], 00:26:06, direct
192.168.26.0/24, ubest/mbest: 1/0, attached
    *via 192.168.26.1, Vlan26, [0/0], 00:25:55, direct
192.168.29.0/24, ubest/mbest: 1/0, attached
    *via 192.168.29.1, Eth3/1, [0/0], 00:25:42, direct
```

Step 18 View the IP-specific configuration by using the **show running-config ip** command.

```
F103-Nexus-7010-Prod_A(config-if-range)# sh run ip

!Command: show running-config ip
!Time: Sat Jun  9 15:19:47 2012

version 6.0(2)
vrf context management
    ip route 0.0.0.0/0 172.16.1.1

interface Vlan25
    ip address 192.168.25.1/24

interface Vlan26
    ip address 192.168.26.1/24

interface Ethernet3/1
    ip address 192.168.29.1/24

interface mgmt0
    ip address 172.16.1.201/24
```

Step 19 Open a command prompt on the PC and attempt to ping the IP address assigned to the Cisco Nexus 5000 Series Switch that the PC is connected to.

Device	Destination
PC A	192.168.25.2
PC B	192.168.27.2

```
C:\WINDOWS>ping 192.168.25.2
```

```
Pinging 192.168.25.2 with 32 bytes of data:
```

```
Reply from 192.168.25.2: bytes=32 time<1ms TTL=254
Reply from 192.168.25.2: bytes=32 time=1ms TTL=254
Reply from 192.168.25.2: bytes=32 time=1ms TTL=254
Reply from 192.168.25.2: bytes=32 time=1ms TTL=254
```

```
Ping statistics for 192.168.25.2:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Step 20 The pings should be successful. Now, attempt to ping the other N5K switch.

```
C:\WINDOWS>ping 192.168.27.2
```

```
Pinging 192.168.27.2 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 192.168.27.2:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Step 21 These pings should fail. The reason is that the Cisco Nexus 7000 Series Switches are not exchanging routes. The switches only know about directly connected networks at this time.

Activity Verification

You have completed this task when you attain these results:

- You have configured Layer 3 interfaces on the Cisco Nexus 7000 Series Switches.
- You have created and configured SVI interfaces on all switches.
- You have verified connectivity between your PC and one Cisco Nexus 5000 Series Switch.

Task 2: Configure EIGRP Routing Protocol

In this task, you will use CLI commands to configure and verify EIGRP.

Activity Procedure

Complete the following steps on both Cisco Nexus 7000 Series Switches.

Step 1 Enable the EIGRP feature on the Cisco Nexus 7000 Series Switches using the **feature eigrp** command.

```
N5K-A(config)# feature eigrp
```

Step 2 Create an EIGRP process and define the autonomous system number.

```
F103-Nexus-7010-Prod_A(config)# router eigrp DCICN
F103-Nexus-7010-Prod_A(config-router)# autonomous-system 100
```

Enable the routing process on all Layer 3 interfaces using the **ip router eigrp DCICN** command. Refer to the following table for the VLAN assignments.

Device	Interfaces
N7K-A	e3/1, VLAN 25, VLAN 26
N7K-B	e3/2, VLAN 27, VLAN 28

```
F103-Nexus-7010-Prod_A(config-router)# int e3/1
F103-Nexus-7010-Prod_A(config-if)# ip router eigrp DCICN
F103-Nexus-7010-Prod_A(config-if)# int vlan 25-26
F103-Nexus-7010-Prod_A(config-if-range)# ip router eigrp DCICN
```

Step 3 Display the routing table on the two Cisco Nexus 7000 Series Switches.

```
F103-Nexus-7010-Prod_A# show 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>

192.168.25.0/24, ubest/mbest: 1/0, attached
    *via 192.168.25.1, Vlan25, [0/0], 01:00:04, direct
192.168.25.1/32, ubest/mbest: 1/0, attached
    *via 192.168.25.1, Vlan25, [0/0], 01:00:04, local
192.168.26.0/24, ubest/mbest: 1/0, attached
    *via 192.168.26.1, Vlan26, [0/0], 00:59:53, direct
192.168.26.1/32, ubest/mbest: 1/0, attached
    *via 192.168.26.1, Vlan26, [0/0], 00:59:53, local
192.168.27.0/24, ubest/mbest: 1/0
    *via 192.168.29.2, Eth3/1, [90/3072], 00:00:06, eigrp-DCICN, internal
192.168.28.0/24, ubest/mbest: 1/0
    *via 192.168.29.2, Eth3/1, [90/3072], 00:00:06, eigrp-DCICN, internal
192.168.29.0/24, ubest/mbest: 1/0, attached
    *via 192.168.29.1, Eth3/1, [0/0], 00:59:40, direct
192.168.29.1/32, ubest/mbest: 1/0, attached
    *via 192.168.29.1, Eth3/1, [0/0], 00:59:40, local
F103-Nexus-7010-Prod_A(config-if-range)#
```

Step 4 Notice that two entries correspond to each nondirectly connected network. They are identified as “eigrp-DCICN,” which shows that the network was learned through the EIGRP routing protocol with the process ID of DCICN. You can filter the output by appending the keyword **eigrp** to the **show ip route** command.

```
F103-Nexus-7010-Prod_A# show ip route eigrp
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>

192.168.27.0/24, ubest/mbest: 1/0
    *via 192.168.29.2, Eth3/1, [90/3072], 00:10:37, eigrp-DCICN, internal
192.168.28.0/24, ubest/mbest: 1/0
    *via 192.168.29.2, Eth3/1, [90/3072], 00:10:37, eigrp-DCICN, internal
```

Step 5 View the EIGRP configuration by using the **show running-config eigrp** command.

```
F103-Nexus-7010-Prod_A(config-if-range)# show run eigrp
```

```
!Command: show running-config eigrp
```

```
!Time: Sat Jun 9 15:22:16 2012
```

```
version 6.0(2)
```

```
feature eigrp
```

```
router eigrp DCICN
```

```
 autonomous-system 100
```

```
interface Vlan25
```

```
 ip router eigrp DCICN
```

```
interface Vlan26
```

```
 ip router eigrp DCICN
```

```
interface Ethernet3/1
```

```
 ip router eigrp DCICN
```

Step 6 Open a command prompt on the PC and attempt to ping the IP addresses of all devices in the pod.

Device	Destination
PC A	192.168.26.2
PC B	192.168.28.2
N5K-A	192.168.25.2
N5K-B	192.168.28.2

Step 7 All the pings to all devices should be successful. If any pings fail, verify the configuration of the EIGRP routing protocol. If you are still unable to resolve the issue, notify the instructor.

Device	VLANs	Interface
N5K-A	26	e1/28
N5K-B	28	e1/28

Step 8 Save the running-config using the **copy running-config startup-config** command. Perform this step on all switches!

```
F103-Nexus-7010-Prod_A# 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 created and configured EIGRP processes on the Cisco Nexus 7000 Series Switches.
- You have verified connectivity between all devices in the pod.

Lab 4-1 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sat Jun  9 15:27:40 2012

version 6.0(2)
hostname Prod_A

feature telnet
feature eigrp
feature interface-vlan
feature lacp
feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$J9lXpUUN$hRsWCwwMBKwiJ75tqhaok0 role vdc-
operator
username student password 5 $1$J0atuBhn$6/LkqdW9c97u2R4BK/7Zn0 role vdc-admin

banner motd #Nexus 7010-A Lab2-1
#

ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long
spanning-tree vlan 11 priority 16384

interface Vlan1

interface Vlan25
no shutdown
ip address 192.168.25.1/24
ip router eigrp DCICN

interface Vlan26
no shutdown
ip address 192.168.26.1/24
ip router eigrp DCICN

interface port-channel1
switchport
switchport mode trunk

interface port-channel2
switchport
switchport mode trunk

interface port-channel5
switchport
switchport mode trunk
```

```

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
  description Link to N5K-A 1/1
  switchport mode trunk
  channel-group 1 mode active
  no shutdown

interface Ethernet2/6
  description Link to N5K-A 1/2
  switchport mode trunk
  channel-group 1 mode active
  no shutdown

interface Ethernet2/7
  description Link to N5K-B 1/1
  switchport mode trunk
  channel-group 5 mode active

interface Ethernet2/8
  description Link to N5K-B 1/2
  switchport mode trunk
  channel-group 5 mode active

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
  description Link to N7K-B 2/23
  switchport mode trunk
  channel-group 2 mode active

interface Ethernet2/12
  description Link to N7K-B 2/24
  switchport mode trunk
  channel-group 2 mode active

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  description Link to N7K-B 3/2
  ip address 192.168.29.1/24
  ip router eigrp DCICN
  no shutdown

interface Ethernet3/3
  description Link to N5K-A 1/5
  switchport
  switchport mode trunk

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

```

```
interface Ethernet3/11
  switchport

interface Ethernet3/13
  switchport

interface Ethernet3/15
  switchport

interface Ethernet3/17
  switchport

interface Ethernet3/19
  switchport

interface Ethernet3/21
  switchport

interface Ethernet3/23
  switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
  ip address 172.16.1.201/24
  line vty
  router eigrp DCICN
    autonomous-system 100
```

Lab 4-1 Cisco Nexus 5000 Series Switch Configuration

```
!Command: show running-config
!Time: Fri Jun  5 20:54:19 2009

version 5.1(3)N1(1a)
switchname N5K-A

feature telnet
no feature http-server
feature interface-vlan
feature lacp
feature lldp
feature vtp

username admin password 5 $1$2KKLDzdx$IkJAYPoK8xgbKxan539r. role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
    ip route 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long

interface Vlan1

interface Vlan25
    no shutdown
    ip address 192.168.25.2/24

interface port-channel1
    switchport mode trunk

interface port-channel3
    switchport mode trunk

interface Ethernet1/1
    description Link to N7K-A 2/5
    switchport mode trunk
    channel-group 1 mode active

interface Ethernet1/2
    description Link to N7K-A 2/6
    switchport mode trunk
    channel-group 1 mode active

interface Ethernet1/3
    description Link to N7K-B 2/17
```

```
shutdown
switchport mode trunk
channel-group 3 mode active

interface Ethernet1/4
description Link to N7K-B 2/18
shutdown
switchport mode trunk
channel-group 3 mode active

interface Ethernet1/5
description Link to N7K-B 3/4
shutdown
switchport mode trunk

interface Ethernet1/6
shutdown

interface Ethernet1/7
shutdown

interface Ethernet1/8
shutdown

interface Ethernet1/9
shutdown

interface Ethernet1/10
shutdown

interface Ethernet1/11
shutdown

interface Ethernet1/12
shutdown

interface Ethernet1/13
shutdown

interface Ethernet1/14
shutdown

interface Ethernet1/15
shutdown

interface Ethernet1/16
shutdown

interface Ethernet1/17
shutdown

interface Ethernet1/18
shutdown

interface Ethernet1/19
shutdown

interface Ethernet1/20
shutdown

interface Ethernet1/21
shutdown

interface Ethernet1/22
shutdown

interface Ethernet1/23
shutdown
```

```
interface Ethernet1/24
 shutdown

interface Ethernet1/25
 shutdown

interface Ethernet1/26
 shutdown

interface Ethernet1/27
 shutdown

interface Ethernet1/28
 description Link to PC A
 switchport access vlan 26
 spanning-tree port type edge
 speed 1000

interface Ethernet1/29
 shutdown

interface Ethernet1/30
 shutdown

interface Ethernet1/31
 shutdown

interface Ethernet1/32
 shutdown

interface mgmt0
 ip address 172.16.1.41/24
 line console
 line vty
 boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
 boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
 ip route 0.0.0.0/0 192.168.25.1
```

Answer Key

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

Lab 2-2 Answer Key: Configuring Cisco Nexus Switches

Lab 2-2 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:09:58 2012

version 6.0(2)
hostname Prod_A

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1
vlan 1

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
description Link to N5K-A 1/1
no shutdown

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
description Link to N7K-B 2/23
no shutdown

interface Ethernet2/12
```

```

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  switchport

interface Ethernet3/3
  switchport

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

interface Ethernet3/11
  switchport

interface Ethernet3/13
  switchport

interface Ethernet3/15
  switchport

interface Ethernet3/17
  switchport

interface Ethernet3/19
  switchport

interface Ethernet3/21
  switchport

interface Ethernet3/23
  switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
  ip address 172.16.1.201/24
line vty

```

Lab 2-2 Cisco Nexus 5000 Series Switch Configuration

```

!Command: show running-config
!Time: Sat Jun 9 14:02:39 2012

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lldp

username admin password 5 $1$aS0dBomR$h7immj0YTBsjhQlsiy/hR/ role network-
admin

```

```

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
    ip route 0.0.0.0/0 172.16.1.1
vlan 1

interface Ethernet1/1
    description Link to N7K-A 2/5

interface Ethernet1/2

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

```

```
interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28
  description Link to PC-A Lab2
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 2-3 Answer Key: Configuring VLANs and Trunks

Lab 2-3 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:31:17 2012

version 6.0(2)
hostname Prod_A

feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
description Link to N5K-A 1/1
switchport mode trunk
no shutdown

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
description Link to N7K-B 2/23
switchport mode trunk
no shutdown

interface Ethernet2/12

interface Ethernet2/25

interface Ethernet2/26
```

```

interface Ethernet3/1
  switchport

interface Ethernet3/3
  switchport

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

interface Ethernet3/11
  switchport

interface Ethernet3/13
  switchport

interface Ethernet3/15
  switchport

interface Ethernet3/17
  switchport

interface Ethernet3/19
  switchport

interface Ethernet3/21
  switchport

interface Ethernet3/23
  switchport

interface Ethernet3/25
  switchport

interface Ethernet3/27
  switchport

interface Ethernet3/29
  switchport

interface Ethernet3/31
  switchport

interface mgmt0
  ip address 172.16.1.201/24
  line vty

```

Lab 2-3 Cisco Nexus 5000 Series Switch Configuration

```

!Command: show running-config
!Time: Sat Jun 9 14:30:23 2012z

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lldp
feature vtp

username admin password 5 $1$aS0dB0mR$h7immj0YTBSjhQlsiy/hR/ role network-
admin

banner motd #Nexus 5000 Switch
#

```

```

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
    ip route 0.0.0.0/0 172.16.1.1

interface Ethernet1/1
    description Link to N7K-A 2/5
    switchport mode trunk

interface Ethernet1/2

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

```

```
interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28
  description Link to PC-A Lab2
  switchport access vlan 11
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 2-4 Answer Key: Verifying and Configuring Spanning Tree

Lab 2-4 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:45:16 2012

version 6.0(2)
hostname Prod_A

feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1
spanning-tree vlan 11 priority 16384

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
description Link to N5K-A 1/1
switchport mode trunk
no shutdown

interface Ethernet2/6
description Link to N5K-A 1/2
switchport mode trunk
no shutdown

interface Ethernet2/7
description Link to N5K-B 1/1
switchport mode trunk
no shutdown

interface Ethernet2/8
description Link to N5K-B 1/2
switchport mode trunk
no shutdown

interface Ethernet2/9

interface Ethernet2/10
```

```

interface Ethernet2/11
  description Link to N7K-B 2/23
  switchport mode trunk
  no shutdown

interface Ethernet2/12
  description Link to N7K-B 2/24
  switchport mode trunk
  no shutdown

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  description Link to N7K-B 3/2
  switchport
  switchport mode trunk
  no shutdown

interface Ethernet3/3
  description Link to N5K-A 1/5
  switchport
  switchport mode trunk
  no shutdown

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

interface Ethernet3/11
  switchport

interface Ethernet3/13
  switchport

interface Ethernet3/15
  switchport

interface Ethernet3/17
  switchport

interface Ethernet3/19
  switchport

interface Ethernet3/21
  switchport

interface Ethernet3/23
  switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
  ip address 172.16.1.201/24
  line vty

```

Lab 2-4 Cisco Nexus 5000 Series Switch Configuration

```
!Command: show running-config
!Time: Sat Jun  9 14:44:05 2012

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lldp
feature vtp

username admin password 5 $1$aSOdBomR$h7immj0YTBsjhQlsiy/hR/  role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
  match qos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-fcoe
  match qos-group 1
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
  ip route 0.0.0.0/0 172.16.1.1

interface Ethernet1/1
  description Link to N7K-A 2/5
  switchport mode trunk

interface Ethernet1/2
  description Link to N7K-A 2/6
  switchport mode trunk

interface Ethernet1/3
  description Link to N7K-B 2/17
  switchport mode trunk

interface Ethernet1/4
  description Link to N7K-B 2/18
  switchport mode trunk

interface Ethernet1/5
  description Link to N7K-A 3/3
  switchport mode trunk

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9
```

```
interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28
  description Link to PC-A Lab2
  switchport access vlan 11
  spanning-tree port type edge
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 2-5 Answer Key: Configuring EtherChannel

Lab 2-5 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sun Jun 10 14:52:59 2012

version 6.0(2)
hostname Prod_A

feature lacp
feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$9WYIRBFm$tQ.N4r2bsykhxGWSq9YgO/ role vdc-
operator
username student password 5 $1$GGGXAkEy$y37bGOM2RNB.pvbzKxphM0 role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long
spanning-tree vlan 11 priority 16384

interface port-channel1
switchport
switchport mode trunk

interface port-channel2
switchport
switchport mode trunk

interface port-channel5
switchport
switchport mode trunk

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
description Link to N5K-A 1/1
switchport mode trunk
channel-group 1 mode active
no shutdown

interface Ethernet2/6
description Link to N5K-A 1/2
switchport mode trunk
channel-group 1 mode active
```

```

no shutdown

interface Ethernet2/7
  description Link to N5K-B 1/1
  switchport mode trunk
  channel-group 5 mode active
  no shutdown

interface Ethernet2/8
  description Link to N5K-B 1/2
  switchport mode trunk
  channel-group 5 mode active
  no shutdown

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
  description Link to N7K-B 2/23
  switchport mode trunk
  channel-group 2 mode active
  no shutdown

interface Ethernet2/12
  description Link to N7K-B 2/24
  switchport mode trunk
  channel-group 2 mode active
  no shutdown

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  description Link to N7K-B 3/2
  switchport
  switchport mode trunk

interface Ethernet3/3
  description Link to N5K-A 1/5
  switchport
  switchport mode trunk

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9
  switchport

interface Ethernet3/11
  switchport

interface Ethernet3/13
  switchport

interface Ethernet3/15
  switchport

interface Ethernet3/17
  switchport

interface Ethernet3/19
  switchport

```

```

interface Ethernet3/21
    switchport

interface Ethernet3/23
    switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
    ip address 172.16.1.201/24
    line vty

```

Lab 2-5 Cisco Nexus 5000 Series Switch Configuration

```

!Command: show running-config
!Time: Sat Jun  9 14:52:05 2012

version 5.1(3)N1(1a)
switchname N5K-A

no feature telnet
no feature http-server
feature lacp
feature lldp
feature vtp

username admin password 5 $1$aSOdBomR$h7immj0YTBsjhQlsiy/hR/ role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
    match qos-group 1
class-map type queuing class-all-flood
    match qos-group 2
class-map type queuing class-ip-multicast
    match qos-group 2
class-map type network-qos class-fcoe
    match qos-group 1
class-map type network-qos class-all-flood
    match qos-group 2
class-map type network-qos class-ip-multicast
    match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
    ip route 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long

interface port-channel1
    switchport mode trunk

interface port-channel3
    switchport mode trunk

interface Ethernet1/1

```

```

    description Link to N7K-A 2/5
    switchport mode trunk
    channel-group 1 mode active

interface Ethernet1/2
    description Link to N7K-A 2/6
    switchport mode trunk
    channel-group 1 mode active

interface Ethernet1/3
    description Link to N7K-B 2/17
    switchport mode trunk
    channel-group 3 mode active

interface Ethernet1/4
    description Link to N7K-B 2/18
    switchport mode trunk
    channel-group 3 mode active

interface Ethernet1/5
    description Link to N7K-A 3/3
    shutdown
    switchport mode trunk

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

```

```
interface Ethernet1/28
  description Link to PC-A Lab2
  switchport access vlan 11
  spanning-tree port type edge
  speed 1000

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface mgmt0
  ip address 172.16.1.41/24
  line console
  line vty
  boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
  boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
```

Lab 3-1 Answer Key: Converting Decimal to Binary and Binary to Decimal

Task 1: Convert from Decimal Notation to Binary Format

Base-2	27	26	25	24	23	22	21	20	
Decimal	128	64	32	16	8	4	2	1	Binary
48	0	0	1	1	0	0	0	0	$48 = 32+16 = 00110000$
146	1	0	0	1	0	0	1	0	$146 = 128+16+2 = 10010010$
222	1	1	0	1	1	1	1	0	$222 = 128+64+16+8+4+2 = 1101110$
119	0	1	1	1	0	1	1	1	$119 = 64+32+16+4+2+1 = 01110111$
135	1	0	0	0	0	1	1	1	$135 = 128+4+2+1 = 10000111$
60	0	0	1	1	1	1	0	0	$60 = 32+16+8+4 = 00111100$

Task 2: Convert from Binary Notation to Decimal Format

Base-2	27	26	25	24	23	22	21	20	
Binary	128	64	32	16	8	4	2	1	Decimal
11001100	1	1	0	0	1	1	0	0	$128+64+8+4 = 204$
10101010	1	0	1	0	1	0	1	0	$128+32+8+2 = 170$
11100011	1	1	1	0	0	0	1	1	$128+64+32+2+1 = 227$
10110011	1	0	1	1	0	0	1	1	$128+32+16+2+1 = 179$
00110101	0	0	1	1	0	1	0	1	$32+16+4+1 = 53$
10010111	1	0	0	1	0	1	1	1	$128+16+4+2+1 = 151$

Lab 3-2 Answer Key: Classifying Network Addressing

Task 1: Convert from Decimal IP Address to Binary Format

Table to express 145.32.59.24 in binary format:

Base-2	27	26	25	24	23	22	21	20	
Decimal	128	64	32	16	8	4	2	1	Binary
145	1	0	0	1	0	0	0	1	10010001
32	0	0	1	0	0	0	0	0	00100000
59	0	0	1	1	1	0	1	1	00111011
24	0	0	0	1	1	0	0	0	00011000
Binary Format IP Address						10010001.00100000.00111011.00011000			

Table to express 200.42.129.16 in binary format:

Base-2	27	26	25	24	23	22	21	20	
Decimal	128	64	32	16	8	4	2	1	Binary
200	1	1	0	0	1	0	0	0	11001000
42	0	0	1	0	1	0	1	0	00101010
129	1	0	0	0	0	0	0	1	10000001
16	0	0	0	1	0	0	0	0	00010000
Binary Format IP Address						11001000.00101010.10000001.00010000			

Table to express 14.82.19.54 in binary format:

Base-2	27	26	25	24	23	22	21	20	
Decimal	128	64	32	16	8	4	2	1	Binary
14	0	0	0	0	1	1	1	0	00001110
82	0	1	0	1	0	0	1	0	01010010
19	0	0	0	1	0	0	1	1	00010011
54	0	0	1	1	0	1	1	0	00110110
Binary Format IP Address						00001110.01010010.00010011.00110110			

Task 2: Convert from Binary Format to Decimal IP Address

Table to express 11011000.00011011.00111101.10001001 in decimal IP address format:

Base-2	27	26	25	24	23	22	21	20	
Binary	128	64	32	16	8	4	2	1	Decimal
11011000	1	1	0	1	1	0	0	0	216
00011011	0	0	0	1	1	0	1	1	27
00111101	0	0	1	1	1	1	0	1	61
10001001	1	0	0	0	1	0	0	1	137
Decimal Format IP Address						216.27.61.137			

Table to express 11000110.00110101.10010011.00101101 in decimal IP address format:

Base-2	27	26	25	24	23	22	21	20	
Binary	128	64	32	16	8	4	2	1	Decimal
11000110	1	1	0	0	0	1	1	0	198
00110101	0	0	1	1	0	1	0	1	53
10010011	1	0	0	1	0	0	1	1	147
00101101	0	0	1	0	1	1	0	1	45
Decimal Format IP Address						198.53.147.45			

Table to express 01111011.00101101.01000011.01011001 in decimal IP address format:

Base-2	27	26	25	24	23	22	21	20	
Binary	128	64	32	16	8	4	2	1	Decimal
01111011	0	1	1	1	1	0	1	1	123
00101101	0	0	1	0	1	1	0	1	45
01000011	0	1	0	0	0	0	1	1	67
01011001	0	1	0	1	1	0	0	1	89
Decimal Format IP Address						123.45.67.89			

Task 3: Identify IP Address Classes

Binary IP Address	Decimal IP Address	Address Class	Number of Bits in Network ID	Maximum Number of Hosts (2h-2)
10010001.00100000.00111011.00011000	145.32.59.24	Class B	16	$2^{16}-2 = 65,534$
11001000.00101010.10000001.00010000	200.42.129.16	Class C	24	$2^8-2 = 254$
00001110.01010010.00010011.00110110	14.82.19.54	Class A	8	$2^{24}-2 = 16,777,214$
11011000.00011011.00111101.10001001	216.27.61.137	Class C	24	$2^8-2 = 254$
10110011.00101101.01000011.01011001	179.45.67.89	Class B	16	$2^{16}-2 = 65,534$
11000110.00110101.10010011.00101101	198.53.147.45	Class C	24	$2^8-2 = 254$

Task 4: Identify Valid and Invalid Host IP Addresses

Decimal IP Address	Valid or Invalid	If Invalid, Indicate Reason
23.75.345.200	Invalid	"345" exceeds an 8-bit value (max = 255).
216.27.61.134	Valid	
9102.54.94	Invalid	One octet is missing.
255.255.255.255	Invalid	Number is valid, but it is an administrative number that should not be assigned to a host.
142.179.148.200	Valid	
200.42.129.16	Valid	
0.124.0.0	Invalid	A Class A address cannot use 0 as the first octet.

Lab 3-3 Answer Key: Computing Usable Subnetworks and Hosts

Task 1: Determine the Number of Bits Required to Subnet a Class C Network

Given a Class C network address of 192.168.89.0, the completed table is:

Number of Subnets	Number of Bits to Borrow(s)	Number of Hosts per Subnet (2h-2)
2	1	$2^7-2 = 126$
5	3	$2^5-2 = 30$
12	4	$2^4-2 = 14$
24	5	$2^3-2 = 6$
40	6	$2^2-2 = 2$

Task 2: Determine the Number of Bits Required to Subnet a Class B Network

Given a Class B network address of 172.25.0.0, the completed table is:

Number of Subnets	Number of Bits to Borrow(s)	Number of Hosts per Subnet (2h-2)
5	3	$2^{13}-2 = 8,190$
8	3	$2^{13}-2 = 8,190$
14	4	$2^{12}-2 = 4,094$
20	5	$2^{11}-2 = 2,046$
35	6	$2^{10}-2 = 1,022$

Task 3: Determine the Number of Bits Required to Subnet a Class A Network

Given a Class A network address of 10.0.0.0, the completed table is:

Number of Subnets	Number of Bits to Borrow(s)	Number of Hosts per Subnet (2h-2)
10	4	$2^{20}-2 = 1,048,574$
14	4	$2^{20}-2 = 1,048,574$
20	5	$2^{19}-2 = 524,286$
40	6	$2^{18}-2 = 262,142$
80	7	$2^{17}-2 = 131,070$

Lab 3-4 Answer Key: Calculating Subnet Masks

Task 1: Determine the Number of Possible Network Addresses

Prefix Length	Decimal Subnet Mask	Binary Subnet Mask	Number of Hosts per Subnet (2h-2)
/20	255.255.240.0	11111111.11111111.11110000.00000000	4,094
/21	255.255.248.0	11111111.11111111.11111000.00000000	2,046
/22	255.255.252.0	11111111.11111111.11111100.00000000	1,022
/23	255.255.254.0	11111111.11111111.11111110.00000000	510
/24	255.255.255.0	11111111.11111111.11111111.00000000	254
/25	255.255.255.128	11111111.11111111.11111111.10000000	126
/26	255.255.255.192	11111111.11111111.11111111.11000000	62
/27	255.255.255.224	11111111.11111111.11111111.11100000	30
/28	255.255.255.240	11111111.11111111.11111111.11110000	14
/29	255.255.255.248	11111111.11111111.11111111.11111000	6
/30	255.255.255.252	11111111.11111111.11111111.11111100	2

Task 2: Given a Network Block, Define Subnets

Assume that you have been assigned the 172.25.0.0 /16 network block. You need to establish eight subnets. Complete the following questions.

- How many bits do you need to borrow to define 12 subnets? 4
- Specify the prefix length and subnet mask in binary and decimal that allows you to create 12 subnets.
Prefix length: /20
Subnet mask (binary): 11111111.11111111.11110000.00000000
Subnet mask (decimal): 255.255.240.0
- Use the eight-step method to define the 12 subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000
2.	Write the mask or classful prefix length in binary.	11110000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	0000 0000 ~~1111 0000~~
4.	Copy the significant bits four times.	0000 0000 (first subnet)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	0000 0001 (first host address)
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	0000 1110 (last host address)
7.	In the middle lines, define the first and last host ID for this subnet.	0000 1111 (broadcast address)

Step	Description	Example
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	0001 0000 (next subnet)

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.25.0.0	172.25.0.1 to 172.25.15.254	172.25.15.255
1	172.25.16.0	172.25.16.1 to 172.25.31.254	172.25.31.255
2	172.25.32.0	172.25.32.1 to 172.25.47.254	172.25.47.255
3	172.25.48.0	172.25.48.1 to 172.25.63.254	172.25.63.255
4	172.25.64.0	172.25.64.1 to 172.25.79.254	172.25.79.255
5	172.25.80.0	172.25.80.1 to 172.25.95.254	172.25.95.255
6	172.25.96.0	172.25.96.1 to 172.25.111.254	172.25.111.255
7	172.25.112.0	172.25.112.1 to 172.25.143.254	172.25.143.255

Task 3: Given Another Network Block, Define Subnets

Assume that you have been assigned the 192.168.1.0 /24 network block.

- How many bits do you need to borrow to define six subnets? 3
- Specify the classful address and subnet mask in binary and decimal that allows you to create six subnets.

Classful address: /27

Subnet mask (binary): 11111111.11111111.11111111.11100000

Subnet mask (decimal): 255.255.255.224

- Use the eight-step method to define the six subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000
2.	Write the mask or classful prefix length in binary.	11100000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	000 00000 ~~111 00000~~
4.	Copy the significant bits four times.	000 00000 (first subnet)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	000 00001 (first host address)
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	000 11110 (last host address)
7.	In the middle lines, define the first and last host ID for this subnet.	000 11111 (broadcast address)

Step	Description	Example
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	001 00000 (next subnet)

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	192.168.1.0	192.168.1.1 to 192.168.1.30	192.168.1.31
1	192.168.1.32	192.168.1.33 to 192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65 to 192.168.1.94	192.168.1.95
3	192.168.1.96	192.168.1.97 to 192.168.1.126	192.168.1.127
4	192.168.1.128	192.168.1.129 to 192.168.1.158	192.168.1.159
5	192.168.1.160	192.168.1.161 to 192.168.1.190	192.168.1.191

Task 4: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 192.168.111.0 /28 network block.

- Specify the subnet mask in binary and decimal.
Subnet mask (binary): 11111111.11111111.11111111.11110000
Subnet mask (decimal): 255.255.255.240
- How many subnets can you define with the specified mask? 16
- How many hosts will be in each subnet? 14
- Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	10000001
2.	Write the mask or classful prefix length in binary.	11110000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	1000 0001 ~~1111 0000~~
4.	Copy the significant bits four times.	1000 0000 (first subnet)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	1000 0001 (first host address)
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	1000 1110 (last host address)
7.	In the middle lines, define the first and last host ID for this subnet.	1000 1111 (broadcast address)
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	1001 0000 (next subnet)

5. Complete the following table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	192.168.111.0	192.168.111.1 to 192.168.111.126	192.168.111.127
1	192.168.111.128	192.168.111.129 to 192.168.111.142	192.168.111.143
2	192.168.111.144	192.168.111.145 to 192.168.111.158	192.168.111.159
3	192.168.111.160	192.168.111.161 to 192.168.111.174	192.168.111.175
4	192.168.111.176	192.168.111.177 to 192.168.111.190	192.168.111.191
5	192.168.111.192	192.168.111.193 to 192.168.111.206	192.168.111.207
6	192.168.111.208	192.168.111.209 to 192.168.111.222	192.168.111.223

Task 5: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.25.0.0 /23 network block.

- Specify the subnet mask in binary and decimal.
Subnet mask (binary): 11111111.11111111.11111110.00000000
Subnet mask (decimal): 255.255.254.0
- How many subnets can you define with the specified mask?
126
- How many hosts will be in each subnet?
510
- Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	01110000.00000000
2.	Write the mask or classful prefix length in binary.	11111110.00000000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	0111000 0.00000000 ~~1111111 0~~ .00000000
4.	Copy the significant bits four times.	0111000 0.00000000 (first subnet)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	0111000 0.00000001 (first host address)
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	0111000 1.11111110 (last host address)
7.	In the middle lines, define the first and last host ID for this subnet.	0111000 1.11111111 (broadcast address)
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	0111001 0.00000000 (next subnet)

5. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.25.0.0	172.25.0.1 to 172.25.1.254	172.25.1.255
1	172.25.2.0	172.25.2.1 to 172.25.3.254	172.25.3.255
2	172.25.4.0	172.25.4.1 to 172.25.5.254	172.25.5.255
3	172.25.6.0	172.25.6.1 to 172.25.7.254	172.25.7.255
4	172.25.8.0	172.25.8.1 to 172.25.9.254	172.25.9.255

Task 6: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.20.0.0 /25 network block.

- Specify the subnet mask in binary and decimal.
Subnet mask (binary): 11111111.11111111.11111111.10000000
Subnet mask (decimal): 255.255.255.128
- How many subnets can you define with the specified mask?
510
- How many hosts will be in each subnet?
126
- Use the eight-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000.10000001
2.	Write the mask or classful prefix length in binary.	11111111.10000000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	1 0000001 ~~1 0000000~~
4.	Copy the significant bits four times.	00000000.10000000 (first subnet)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	00000000.10000001 (first host address)
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	00000000.11111111 (broadcast address)
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	00000001.10000000 (next subnet)

5. Complete the following table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.20.0.0	172.20.0.1 to 172.20.0.126	172.20.0.127
1	172.20.0.128	172.20.0.129 to 172.20.0.254	172.20.0.255
2	172.20.1.0	172.20.1.1 to 172.20.1.126	172.20.1.127
3	172.20.1.128	172.20.1.129 to 172.20.1.254	172.20.1.255
4	172.20.2.0	172.20.2.1 to 172.20.2.126	172.20.2.127
5	172.20.2.128	172.20.2.129 to 172.20.2.254	172.20.2.255

Lab 4-1: Answer Key: Configuring Multilayer Switching

Lab 4-1 Cisco Nexus 7000 Series Switch Configuration

```
!Command: show running-config
!Time: Sat Jun  9 15:27:40 2012

version 6.0(2)
hostname Prod_A

feature telnet
feature eigrp
feature interface-vlan
feature lacp
feature vtp

username admin password 5 $1$A4XvuSsm$HWRb2FVZURjX6p6CzLaqL0 role vdc-admin
username intern password 5 $1$J9lXpUUN$hRsWCwwMBKwiJ75tqhaok0 role vdc-
operator
username student password 5 $1$J0atuBhn$6/LkqdW9c97u2R4BK/7Zn0 role vdc-admin

banner motd #Nexus 7010-A Lab2-1
#

ip domain-lookup
snmp-server user admin vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
pri
v 0xd9a69b00aa3809c0fe97007d8c262085 localizedkey
snmp-server user intern vdc-operator auth md5
0xe806e6958079ce4218351abf13035d37
priv 0xe806e6958079ce4218351abf13035d37 localizedkey
snmp-server user student vdc-admin auth md5 0xd9a69b00aa3809c0fe97007d8c262085
p
riv 0xd9a69b00aa3809c0fe97007d8c262085 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 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long
spanning-tree vlan 11 priority 16384

interface Vlan1

interface Vlan25
no shutdown
ip address 192.168.25.1/24
ip router eigrp DCICN

interface Vlan26
no shutdown
ip address 192.168.26.1/24
ip router eigrp DCICN

interface port-channel1
switchport
switchport mode trunk

interface port-channel2
switchport
switchport mode trunk

interface port-channel5
switchport
```

```

switchport mode trunk

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5
  description Link to N5K-A 1/1
  switchport mode trunk
  channel-group 1 mode active
  no shutdown

interface Ethernet2/6
  description Link to N5K-A 1/2
  switchport mode trunk
  channel-group 1 mode active
  no shutdown

interface Ethernet2/7
  description Link to N5K-B 1/1
  switchport mode trunk
  channel-group 5 mode active

interface Ethernet2/8
  description Link to N5K-B 1/2
  switchport mode trunk
  channel-group 5 mode active

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11
  description Link to N7K-B 2/23
  switchport mode trunk
  channel-group 2 mode active

interface Ethernet2/12
  description Link to N7K-B 2/24
  switchport mode trunk
  channel-group 2 mode active

interface Ethernet2/25

interface Ethernet2/26

interface Ethernet3/1
  description Link to N7K-B 3/2
  ip address 192.168.29.1/24
  ip router eigrp DCICN
  no shutdown

interface Ethernet3/3
  description Link to N5K-A 1/5
  switchport
  switchport mode trunk

interface Ethernet3/5
  switchport

interface Ethernet3/7
  switchport

interface Ethernet3/9

```

```

switchport

interface Ethernet3/11
switchport

interface Ethernet3/13
switchport

interface Ethernet3/15
switchport

interface Ethernet3/17
switchport

interface Ethernet3/19
switchport

interface Ethernet3/21
switchport

interface Ethernet3/23
switchport

interface Ethernet3/25

interface Ethernet3/27

interface Ethernet3/29

interface Ethernet3/31

interface mgmt0
ip address 172.16.1.201/24
line vty
router eigrp DCICN
autonomous-system 100

```

Lab 4-1 Cisco Nexus 5000 Series Switch Configuration

```

!Command: show running-config
!Time: Fri Jun  5 20:54:19 2009

version 5.1(3)N1(1a)
switchname N5K-A

feature telnet
no feature http-server
feature interface-vlan
feature lacp
feature lldp
feature vtp

username admin password 5 $1$2KKLDzdx$IkJAYPoK8xgbKxan539r. role network-
admin

banner motd #Nexus 5000 Switch
#

ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
match qos-group 1
class-map type queuing class-all-flood
match qos-group 2
class-map type queuing class-ip-multicast
match qos-group 2
class-map type network-qos class-fcoe
match qos-group 1

```

```

class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user admin network-admin auth md5
0x61b7d5b611af6597bb94ea2dd9a6594a priv 0x61b7d5b611af6597bb94ea2dd9a6594a
localizedkey

vrf context management
  ip route 0.0.0.0/0 172.16.1.1
spanning-tree pathcost method long

interface Vlan1

interface Vlan25
  no shutdown
  ip address 192.168.25.2/24

interface port-channel1
  switchport mode trunk

interface port-channel3
  switchport mode trunk

interface Ethernet1/1
  description Link to N7K-A 2/5
  switchport mode trunk
  channel-group 1 mode active

interface Ethernet1/2
  description Link to N7K-A 2/6
  switchport mode trunk
  channel-group 1 mode active

interface Ethernet1/3
  description Link to N7K-B 2/17
  shutdown
  switchport mode trunk
  channel-group 3 mode active

interface Ethernet1/4
  description Link to N7K-B 2/18
  shutdown
  switchport mode trunk
  channel-group 3 mode active

interface Ethernet1/5
  description Link to N7K-B 3/4
  shutdown
  switchport mode trunk

interface Ethernet1/6
  shutdown

interface Ethernet1/7
  shutdown

interface Ethernet1/8
  shutdown

interface Ethernet1/9
  shutdown

interface Ethernet1/10
  shutdown

interface Ethernet1/11

```

```
shutdown

interface Ethernet1/12
shutdown

interface Ethernet1/13
shutdown

interface Ethernet1/14
shutdown

interface Ethernet1/15
shutdown

interface Ethernet1/16
shutdown

interface Ethernet1/17
shutdown

interface Ethernet1/18
shutdown

interface Ethernet1/19
shutdown

interface Ethernet1/20
shutdown

interface Ethernet1/21
shutdown

interface Ethernet1/22
shutdown

interface Ethernet1/23
shutdown

interface Ethernet1/24
shutdown

interface Ethernet1/25
shutdown

interface Ethernet1/26
shutdown

interface Ethernet1/27
shutdown

interface Ethernet1/28
description Link to PC A
switchport access vlan 26
spanning-tree port type edge
speed 1000

interface Ethernet1/29
shutdown

interface Ethernet1/30
shutdown

interface Ethernet1/31
shutdown

interface Ethernet1/32
shutdown
```

```
interface mgmt0
  ip address 172.16.1.41/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.1.3.N1.1a.bin
boot system bootflash:/n5000-uk9.5.1.3.N1.1a.bin
ip route 0.0.0.0/0 192.168.25.1
```