CCNAX

Interconnecting Cisco Networking Devices: Accelerated

Lab Guide

Version 3.0

Part Number: 97-3640-01

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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

Table of Contents

Module 3: Summary Challenge

Lesson 1: Establish Internet Connectivity

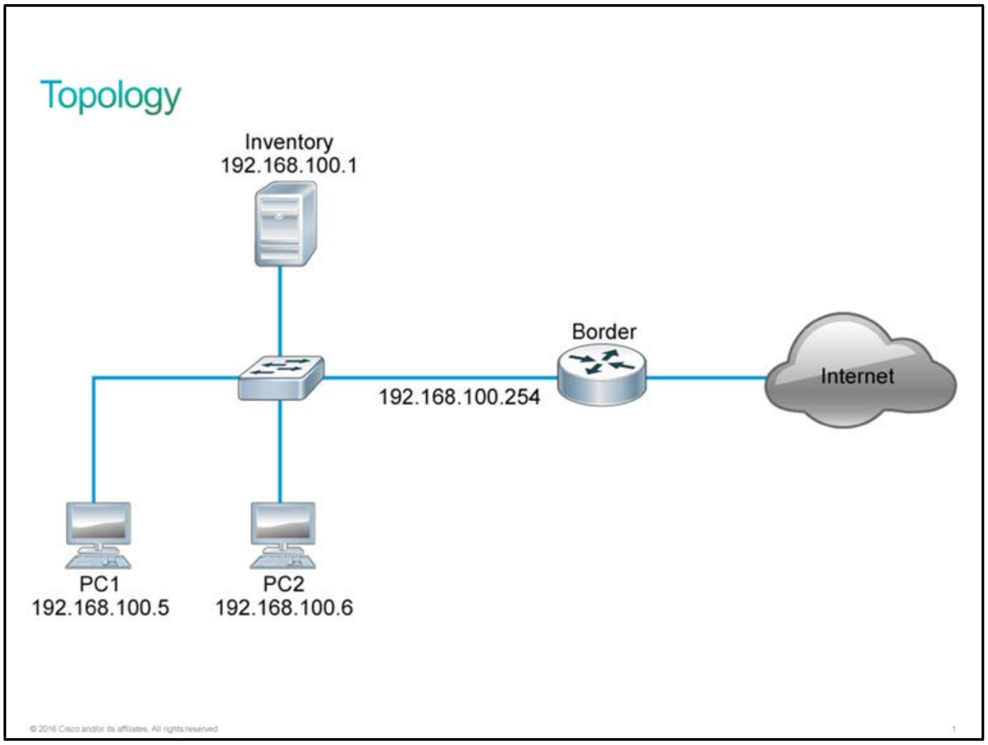
Challenge 1: Summary Challenge Lab: 1

Introduction

A Supermarket in your neighborhood has decided to expand into franchises. They have also decided to open an operations headquarters in a small office that is set up in a nearby building.
One of their new employee named Mark has working knowledge about computers, so he is working as their temporary Network administrator. He has set up the basic structure of the network, which includes a couple of servers and a switch. Mark has knowledge about DSL environments only and he has not configured a router before. Therefore, they have asked you to help.
The customer has purchased a router that is still in the box. You need to set up the basic configuration on the router before setting it as a gateway to the Internet. The router must receive a DHCP assigned IP Address from the ISP router. The ISP has also provided a public IP Address for additional use.

The customer requires that you must make one of the servers available through the Internet to POS systems in their franchises using the public IP Address.
There is also a list of public IP addresses that will be used by those POS systems that you will be limiting access to.
In addition to it, the remaining server and PC must have access to the internet using the IP address of the Interface on the router that faces the Internet.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
SW1	Ethernet0/0	VLAN 1	Border	Ethernet0/0	192.168.100.254/24
SW1	Ethernet0/1	VLAN 1	Inventory	Ethernet0/0	192.168.100.1/24
SW1	Ethernet0/2	VLAN 1	PC1	Ethernet0/0	192.168.100.5/24
SW1	Ethernet0/3	VLAN 1	PC2	Ethernet0/0	192.168.100.6/24
SW1	VLAN 1	192.168.100.10/24	_	_	_
Inventory	Ethernet0/0	192.168.100.1/24	SW1	Ethernet0/0	VLAN 1

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
Border	Ethernet0/0	192.168.100.254/24	SW1	Ethernet0/0	VLAN 1
Border	Ethernet0/1	DHCP	Internet	Ethernet0/0	209.165.200.227/27
Internet	Loopback 0	209.165.201.1/32	_	_	_
Internet	Loopback 1	209.165.201.226	_	_	_
Internet	Loopback 2	209.165.202.226	_	_	_
Internet	Loopback 3	209.165.203.226	_	_	_
PC1	Ethernet0/0	192.168.100.5/24	SW1	Ethernet0/2	VLAN 1
PC2	Ethernet0/0	192.168.100.6/24	SW1	Ethernet0/3	VLAN 1

Note 1: Use public IP address 209.165.200.226 for static NAT translation for Inventory server when traffic sent from inside to outside network.

Note 2: The public IP addresses 209.165.201.226, 209.165.202.226 and 209.165.203.226 are configured on the internet router emulating POS systems address. These addresses need to be permitted on Border router to access the Inventory server after it has been provided a static NAT address.

Task 1: Evaluation Lab Procedure

Activity

Step 1 Configure the router with an appropriate hostname and also set up the interfaces with appropriate address.

Step 2 Configure the Border router with a default route to the Internet and confirm connectivity to internet loopback 0 interface.

Step 3 Configure the Border router with a static NAT for the Inventory server using the public IP Address that is assigned by the ISP. The static NAT translation for the Inventory server must be configured for the traffic sent from inside network to outside network. (Refer to Job aid for ISP assigned public IP address for NAT translation.)

Step 4 Create a Standard ACL that is named as NAT_ACL to allow only three public IP addresses that POS client machines will use to access the Inventory server. Ensure that the ACL allows DHCP packets and other traffic from IP address 209.165.200.227 and allows ICMP packets and other traffic from IP address 209.165.201.1. Apply this ACL to the interface on Border router that faces the ISP.

Step 5 Configure a standard ACL that is named as PAT_ACL, which matches the IP addresses of PC1 and PC2. Create a PAT statement that uses PAT_ACL to translate the IP addresses of PC1 and PC2 to the IP Address of Border router that is connected to the Internet.

Verification

Step 1 Verify that the router is configured with the correct hostname and ensure that the interfaces on the router are working properly.

Substep 1

Use the **show run | include hostname** command to verify that the hostname is configured as "Border."

```
Border# show run | include hostname
hostname Border
```

Use the **show ip interface brief** command to check the status of the interfaces E0/0 and E0/1**.**

```
Border# show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.100.254 YES manual up                    up
Ethernet0/1                209.165.200.225 YES DHCP   up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
```

If the command output does not show the desired result, it indicates that the hostname is not configured correctly, or the interfaces are not enabled and assigned with the correct IP Addresses.

Step 2 Verify that the router is correctly configured with the default route to the Internet.

Substep 1

The default route configuration on the router can be verified by performing the following:
Use the **show ip route** command to verify the routing table.

```
Border# show ip route
Gateway of last resort is 209.165.200.227 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.227
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, Ethernet0/0
L        192.168.100.254/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Ethernet0/1
L        209.165.200.225/32 is directly connected, Ethernet0/1
```

Issue a ping command from Border router to the Internet test IP address 209.165.201.1 to verify that the default route to the internet is configured correctly.

```
Border# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

If the command output does not show the desired result, it indicates that the default route is not configured properly, or the interface E0/1 on Border router is still administratively shut down.

Step 3 Verify that the router is NATing the Inventory Server correctly.

Substep 1

You can verify that the task is completed successfully by performing the following steps:
Issue a ping command from the Inventory server to the Internet test IP address.

```
Inventory# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Use the **show ip nat translation** command to check the NAT translation table on Border router to ensure that the router is NATing the Inventory server correctly

```
Border # show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.226:11 192.168.100.1:11  209.165.201.1:11   209.165.201.1:11
--- 209.165.200.226    192.168.100.1      ---                ---
Border#
```

If the command output does not show the desired result, it indicates that the NAT statement is not configured correctly.

Step 4 Verify that the three public IP addresses that are mentioned earlier are allowed to access the Inventory server.

Substep 1

You can verify this task by performing the following steps:
Issue a ping command from the Internet router to the Inventory server using each of the public IP Address as a source. You need to be in privileged mode to do this command.

```
Internet# ping 209.165.200.226 source 209.165.201.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 209.165.201.226
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Internet# ping 209.165.200.226 source 209.165.202.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 209.165.202.226
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Internet# ping 209.165.200.226 source 209.165.203.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 209.165.203.226
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Internet#
```

Use the **show ip access-list** command on the Border router to check the hits on the ACL to verify that the specified public IP addresses are allowed to access the Inventory server.

```
Border#show ip access-lists
Standard IP access list NAT_ACL
    20 permit 209.165.202.226 (5 matches)
    30 permit 209.165.203.226 (5 matches)
    10 permit 209.165.201.226 (5 matches)
    40 permit 209.165.200.227
    50 permit 209.165.201.1
```

Issue ping commands from the Border router to the Internet router interface IP address 209.165.200.227 and Internet router loopback 0 IP address 209.165.201.1.

```
Border# ping 209.165.200.227
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
Border# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Use the **show ip access-list** command on the Border router to check the hits on the ACL to verify that the specified Internet router IP addresses are allowed on the Border router.

```
Border# show ip access-lists
Standard IP access list NAT_ACL
    20 permit 209.165.202.226 (5 matches)
    30 permit 209.165.203.226 (10 matches)
    10 permit 209.165.201.226 (5 matches)
    40 permit 209.165.200.227 (5 matches)
    50 permit 209.165.201.1 (5 matches)
```

If the command output does not show the desired result, it indicates that the ACL is not configured correctly or applied properly to the correct interface.

Step 5

Verify that the two PCs are able to use the Border Router's internet facing interface's IP address to access the Internet.

Substep 1

You can verify the connectivity between the specified PCs and the Internet test IP address by performing the following steps:
Issue a ping command from PC1 and PC2 to the Internet test IP address to verify that these PCs have access to Internet.

```
PC1# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

PC2# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Use the **show ip nat translation** command on the Border router to verify that PC1 and PC2 have access to the Internet.

```
Border# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.226    192.168.100.1      ---                ---
icmp 209.165.200.225:7 192.168.100.5:7    209.165.201.1:7    209.165.201.1:7
icmp 209.165.200.225:0 192.168.100.6:0    209.165.201.1:0    209.165.201.1:0
Border#
```

If the command output does not show the desired result, it indicates that the interfaces are not assigned with the correct NAT roles, the PAT statement is not configured correctly, or the interface E0/1 is not configured correctly to receive the DHCP IP address from the Internet router.

Answer Key

Challenge 1: Summary Challenge Lab: 1

Task 1: Evaluation Lab Procedure

Activity

Step 1 Configure the router with hostname as "Border" and turn on both ethernet interfaces. Configure interface E0/0 with IP address 192.168.100.254/24, and configure interface E0/1 in such a way that it accepts an IP address from the ISP router.

Configure the hostname as "Border."

```
Router(config)# hostname Border
Border(config)#
```

Configure interface E0/0 to be enabled and also provide it with the IP Address 192.168.100.254/24.

```
Border(config)# interface e0/0
Border(config-if)# no shut
Border(config-if)# ip address 192.168.100.254 255.255.255.0
```

Configure interface E0/1 to be enabled and also ensure that it receives an IP Address via DHCP.

```
Border(config)# interface E0/1
Border(config-if)# no shut
Border(config-if)# ip address dhcp
```

Step 2 Configure a default route to the interface on the ISP's Border router that is connected to interface E0/1 on router .

```
Border(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.227
```

Step 3 NAT the IP address of the Inventory Server 192.168.100.1 to the public IP address of 209.165.200.226.

```
Border(config)# ip nat inside source static 192.168.100.1 209.165.200.226
```

Enable the interfaces to take the appropriate NAT role (inside and outside).

```
Border(config)# interface E0/0
Border(config-if)# ip nat inside
Border(config)# interface E0/1
Border(config-if)# ip nat outside
```

Step 4 The three IP addresses that are assigned to the POS machines are 209.165.201.226, 209.165.202.226, and 209.165.203.226. Create an ACL that permits the IP traffic between these IP addresses and the Inventory server's public IP address 209.165.200.226. Also, ensure that the ACL does not block the other necessary traffic.
Apply this ACL to the interface E0/1 on the Border router.

Create the ACL using three ACL Statements given below.

```
Border(config)# ip access-list standard NAT_ACL
Border(config-std-nacl)# permit host  209.165.201.226
Border(config-std-nacl)# permit host  209.165.202.226
Border(config-std-nacl)# permit host  209.165.203.226
```

Add an ACL statement that allows DHCP packets and other traffic from IP address 209.165.200.227.

```
Border(config)# ip access-list standard NAT_ACL
Border(config-std-nacl)# permit host 209.165.200.227
```

Add an ACL statement that allows ICMP packets and other traffic from IP address 209.165.201.1.

```
Border(config)# ip access-list standard NAT_ACL
Border(config-std-nacl)#  permit host 209.165.201.1
```

Apply the ACL to the correct interface.

```
Border(config)# interface E0/1
Border(config-if)# ip access-group NAT_ACL in
```

Step 5 The IP addresses of PC1 and PC2 are 192.168.100.5 and 192.168.100.6 respectively. Create PAT_ACL to match these two IP Addresses and also configure the PAT statement.

Create the ACL. The following example shows a way to create an ACL with only one optimum and efficient ACL Statement.

```
Border(config)# ip access-list standard PAT_ACL
Border(config-std-nacl)# permit host 192.168.100.5
Border(config-std-nacl)# permit host 192.168.100.6
```

Create the PAT statement using the PAT_ACL.

```
Border(config)# ip nat inside source list PAT_ACL interface e0/1 overload
```

Lesson 2: Troubleshoot Internet Connectivity

Challenge 2: Summary Challenge Lab: 2

Introduction

An Application Startup company have just received funding and have started setting up their new office. The network manager is out of town, so he asked a network engineer trainee to rack mount, cable, and configure the routers and switches that are purchased to set up the network. The manager felt that this task is a great learning opportunity for the trainee, and it will save the time as well.

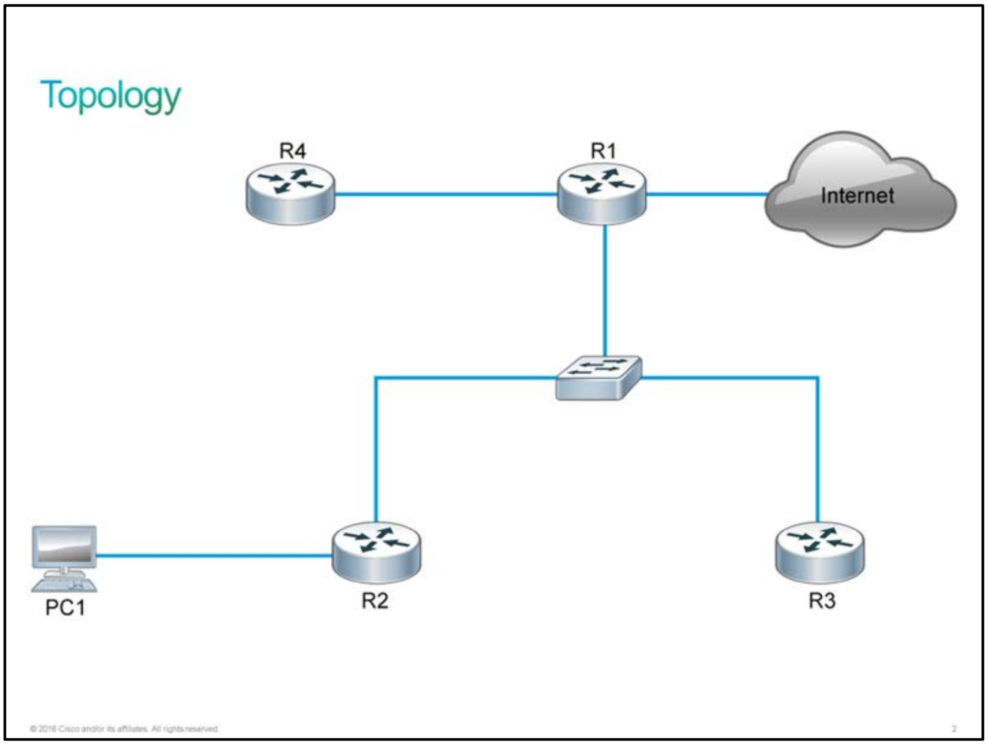
The network requirement is given below:
There are four routers, R1, R2, R3, and R4. The interface E0/1 on router R1 will be used to connect a WAN link that the ISP will provide in few days.
The network must use the static routing at the initial stage, till some of the management decisions are made. After the management decisions are made, the dynamic routing protocol must be implemented on the network.

The network is expected to perform the following:

- Router R1 is supposed to connect to the Internet. The ISP will assign a dynamic IP address to router R1 and the PAT is enabled on router R1.
- Route the traffic will be sourced from routers R2 and R3 that is destined to the subnets 172.16.5.0/24 and 172.16.6.0/24 to router R4 and forward all other traffic to Internet cloud.
- Apply filtering on router R1 to prevent traffic from the subnet 10.0.0.0/8 that might enter the network through R4.
- Translate the IP addresses of R2 and R3 routers when traffic forwarded to the internet.

The trainee has tried his best to implement the configuration to fulfill these requirements but has committed a few mistakes. Therefore, you must identify the issues and misconfiguration and help the trainee in troubleshooting the Internet connectivity.

Topology



Topology

2

Job Aid

Note	If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
R1	Ethernet0/0	192.168.123.1/24	SW1	Ethernet0/0	VLAN 1
R1	Ethernet0/1	DHCP	Internet	Ethernet0/0	209.165.200.227/27
R1	Ethernet0/2	192.168.14.1/24	R4	Ethernet0/0	192.168.14.4/24
R2	Ethernet0/0	192.168.123.2/24	SW1	Ethernet0/1	VLAN 1
R2	Ethernet0/1	192.168.20.2/24	PC1	Ethernet0/0	192.168.20.1/24
R3	Ethernet0/0	192.168.123.3/24	SW1	Ethernet0/2	VLAN 1

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
R4	Ethernet0/0	192.168.14.4/24	R1	Ethernet0/2	192.168.14.1/24
R4	Loopback 1	172.16.5.5/24	_	_	_
R4	Loopback 2	172.16.6.6/24	_	_	_
R4	Loopback 3	10.0.0.1/8	_	_	_
PC1	Ethernet0/0	192.168.20.1/24	R2	Ethernet0/1	192.168.20.2/24
Internet	Ethernet0/0	209.165.200.227/27	R1	Ethernet0/1	DHCP
Internet	Loopback 0	209.165.201.1	_	_	_

Task 1: Evaluation Lab Procedure

Activity

Step 1 Isolate and fix the issue that is related to router R1 as the gateway to the Internet for the network.

Step 2 Isolate and fix the issue such that traffic from any of the internal routers are forwarded to networks 172.16.5.0/24 and 172.16.6.0/24 through R1 router. (Both these networks are simulated on R4 by configuring loopback 1 & 2 interfaces.)

Step 3 Isolate and fix the issue that is related to filtering the traffic from 10.0.0.0/8, which is entering the network through router R4. The traffic form 10.0.0.0/8 on R4 is simulated by configuring loopback 3 interface on R4.

Step 4 Isolate and fix the issue that is related to translating the IP addresses of R2 (IP 192.168.123.2) and R3 (IP 192.168.123.3) when traffic forwarded to the internet.

Verification

Step 1 Verify that the issue preventing R1 from functioning as the gateway to the internet for the whole network is resolved.

Substep 1

Check the interface E0/1 to confirm that R1 is receiving the DHCP IP address from the Internet Router.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.123.2 YES NVRAM  up                    up
Ethernet0/1                209.165.200.225 YES DHCP   up                    up
```

Check the routing table to see the default route present.

```
R1# show ip route
Gateway of last resort is 209.165.200.227 to network 0.0.0.0
```

```
S*    0.0.0.0/0 [1/0] via 209.165.200.227
S     10.0.0.0/8 [1/0] via 192.168.14.4
      172.16.0.0/24 is subnetted, 2 subnets
S        172.16.6.0 [1/0] via 192.168.123.2
S        172.16.15.0 [1/0] via 192.168.14.4
      192.168.14.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.14.0/24 is directly connected, Ethernet0/2
L        192.168.14.1/32 is directly connected, Ethernet0/2
      192.168.123.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.123.0/24 is directly connected, Ethernet0/0
L        192.168.123.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Ethernet0/1
L        209.165.200.225/32 is directly connected, Ethernet0/1
```

From R1, ping the test address on the internet 209.165.201.1 to check if connectivity exists.

```
R1# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

If the pings from R1 router to the test address on the internet do not work, then verify if dhcp enabled on the R1 router interface connected to Internet router.

Step 2 Verify that the issue preventing the routing of traffic to 172.16.5.0/24 through R4 is resolved.

Substep 1

Check the routing table to verify correct routing table entries for 172.16.5.0/24 and 172.16.6.0/24 on Router R1.

```
R1# show ip route
Gateway of last resort is 209.165.200.227 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.227
S     10.0.0.0/8 [1/0] via 192.168.14.4
      172.16.0.0/24 is subnetted, 2 subnets
S        172.16.5.0 [1/0] via 192.168.14.4
S        172.16.6.0 [1/0] via 192.168.14.4
      192.168.14.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.14.0/24 is directly connected, Ethernet0/2
L        192.168.14.1/32 is directly connected, Ethernet0/2
      192.168.123.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.123.0/24 is directly connected, Ethernet0/0
L        192.168.123.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Ethernet0/1
L        209.165.200.225/32 is directly connected, Ethernet0/1
```

From R2 or R3, ping the test addresses of 172.16.5.5 and 172.16.6.6.

```
R2#ping 172.16.5.5
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R2#ping 172.16.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R3# ping 172.16.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.5.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R3# ping 172.16.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

If R2 and R3 are not able to ping the test address of 172.16.5.4, then there must be some problems with the way traffic to 172.16.5.0/24 is being handled by the network.

Step 3 Verify that the issue preventing the filtration of traffic from 10.0.0.0/8 coming through R4 is resolved.

Substep 1

From R4, Issue a ping using the source address 10.0.0.1 to R2 or R3. The ping should be blocked by the ACL on R4.

```
R4# ping 192.168.123.2 source 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.123.2, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
U.U.U
Success rate is 0 percent (0/5)
```

If Pings from R4, using the source IP Address 10.0.0.1 are successful, then the traffic is not being filtered correctly.

Step 4 Verify that the issue preventing the translation of IP Addresses belonging to R2 and R3 while going out to the internet is resolved.

Substep 1

From R2 and R3 ping the internet test address of 209.165.204.1. On The internet router, check the ACL to verify the source IP address of the ping packets.

```
R2# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R3# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Check the IP NAT Table on R1 immediately after the ping

```
R1# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:3 192.168.123.2:3    209.165.201.1:3    209.165.201.1:3
icmp 209.165.200.225:0 192.168.123.3:0    209.165.201.1:0    209.165.201.1:0
```

If the pings from R2 and R3 are not successful or ICMP packets from them do not have a public IP address as source address, then there is some problem with the NAT configuration.

Answer Key

Challenge 2: Summary Challenge Lab: 2

Task 1: Evaluation Lab Procedure

Activity

Step 1 In order to fix this issue, you must check connectivity between router R1 and the Internet router.

Use the **show ip route** command to check the routing table on router R1 to ensure that the default route exists.

```
R1# show ip route

Gateway of last resort is not set

S     10.0.0.0/8 [1/0] via 192.168.14.4
      172.16.0.0/24 is subnetted, 2 subnets
S        172.16.6.0 [1/0] via 192.168.123.2
S        172.16.15.0 [1/0] via 192.168.14.4
      192.168.14.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.14.0/24 is directly connected, Ethernet0/2
L        192.168.14.1/32 is directly connected, Ethernet0/2
      192.168.123.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.123.0/24 is directly connected, Ethernet0/0
L        192.168.123.1/32 is directly connected, Ethernet0/0
```

The command output shows that the default route does not exist in the routing table. Verify that the default route command is issued to the router.

```
R1# show run | include ip route 0.0.0.0
ip route 0.0.0.0 0.0.0.0 209.165.200.227
```

The default route command is configured, but it does not exist in the routing table. Use the **show ip interface brief** command to check the status of the interfaces of the router.

```
R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.123.1   YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
Ethernet0/2                192.168.14.1    YES NVRAM  up                    up
Ethernet0/3                unassigned      YES NVRAM  administratively down down
NVI0                       192.168.123.1   YES unset  up                    up
```

The command output shows that the interface E0/1 is enabled, but does not have an IP address assigned.
As per the scenario, DHCP on the Internet router should assign an IP Address to interface E0/1.
The interface E0/1 needs to be configured as a DHCP client.
Use the configuration commands that are shown below to enable it.

```
R1(config)# int e0/1
R1(config-if)# ip add dhcp
```

Step 2 In order to fix this issue, you must check if static routes are configured correctly on R1 router.

Use the **show ip route** command to check the routing table on router R1 to verify that the traffic is being sent to the IP addresses, 172.16.5.0/24 and 172.16.6.0/24.

```
R1# show ip route static

Gateway of last resort is 209.165.200.227 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.227
S     10.0.0.0/8 [1/0] via 192.168.14.4
      172.16.0.0/24 is subnetted, 2 subnets
S        172.16.6.0 [1/0] via 192.168.123.2
S        172.16.15.0 [1/0] via 192.168.14.4
```

The output of **show ip route** command shows that the route that was configured for 172.16.5.0/24 has one subnet value that is specified in the route statement is incorrect. Remove the existing static route and configure a new one with the correct IP Address and subnet mask using the configuration commands that are shown below:

```
R1(config)# no ip route 172.16.15.0 255.255.255.0 192.168.14.4
R1(config)# ip route 172.16.5.0 255.255.255.0 192.168.14.4
```

The output of **show ip route** command shows that the route for 172.16.6.0/24 is pointing to the wrong gateway. Remove the existing static route and configure a new one with correct next hop IP address using the configuration commands that are shown below:

```
R1(config)# no ip route 172.16.6.0 255.255.255.0 192.168.123.2
R1(config)# ip route 172.16.6.0 255.255.255.0 192.168.14.4
```

Step 3 As explained in the introduction, the traffic from 10.0.0.0/8, which is entering the network through router R4 configured to be blocked on router R1. This means that the ACL must block this traffic from entering interface E0/2 on router R1.

Use **show access-list** command to verify that the ACL is configured correctly to block the appropriate traffic.

```
R1# show access-list
Standard IP access list 10
    10 deny   11.0.0.0, wildcard bits 0.255.255.255
    20 permit any
```

The output of the show access-list command shows that the ACL is not blocking the traffic correctly.
Use the configuration commands that are shown below to remove the incorrect ACL entry and configure the correct ACL entry.

```
R1(config)# ip access-list standard 10
R1(config-std-nacl)# no 10 deny 11.0.0.0 0.255.255.255
R1(config-std-nacl)# 10 deny 10.0.0.0 0.255.255.255
```

Check the interface E0/2 on router R1 to ensure that the ACL is applied properly.

```
R1# sh run int e0/2
Building configuration...

Current configuration : 92 bytes
!
interface Ethernet0/2
 ip address 192.168.14.1 255.255.255.0
 ip access-group 10 out
end
```

The command output shows that the ACL is applied in the wrong direction.
Use the configuration commands that are shown below to remove the existing ACL application command and re-apply so that it filters out the incoming traffic on interface E0/1.

```
R1(config)# int e0/2
R1(config-if)# no ip access-group 10 out
R1(config-if)# ip access-group 10 in
```

Step 4 Verify NAT configuration on router R1.

Verify the NAT statement on router R1.

```
R1# sh run | i ip nat
 ip nat inside
 ip nat outside
ip nat source list NAT_ACL interface Ethernet0/1 overload
```

The command output shows that the NAT statement is missing the keyword "inside."

```
R1(config)# no ip nat source list NAT_ACL interface Ethernet0/1 overload
R1(config)# ip nat inside source list NAT_ACL interface Ethernet0/1 overload
```

Use the configuration commands that are shown below to remove the existing NAT statement, and to configure the correct NAT statement.

```
R1# show run int e0/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet0/0
 ip address 192.168.123.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
end

R1#show run int e0/1
Building configuration...

Current configuration : 86 bytes
!
interface Ethernet0/1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
end
```

The command outputs show that the interfaces are assigned with the appropriate NAT roles. Verify the access list that identifies the addresses of router R2 (IP 192.168.123.2) and router R3 (IP 192.168.123.3).

```
R1# show access-list NAT_ACL
Standard IP access list NAT_ACL
    10 permit host 192.168.20.1
```

The command output shows that the ACL is incorrectly identifying the IP Address of PC1. Use the configuration commands that are shown below to remove the incorrect ACL entry and add the entries with correct IP addresses of the routers R2 and R3.

```
R1(config)# no ip access-list standard NAT_ACL
R1(config)# ip access-list standard NAT_ACL
R1(config-std-nacl)# 10 permit host 192.168.123.2
R1(config-std-nacl)# 20 permit host 192.168.123.3
```

Module 4: Implementing Scalable Medium-Sized Networks

Lesson 7: Implementing RIPv2

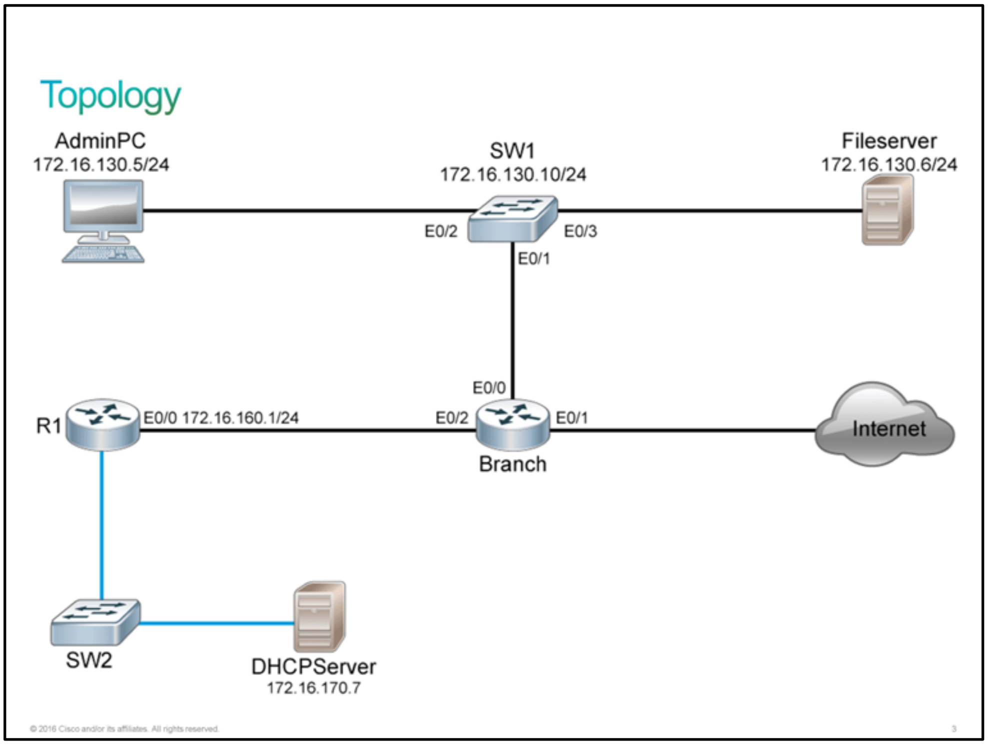
Challenge 3: Implementing RIPv2

Introduction

The customer wants to implement a dynamic routing protocol on the network. Until now, static routing was being used, but the static routing needs to be removed to make way for RIP.
The customer wants to enable RIP version 2 and disable auto-summarization. Also, it is not a best practice for all the routers in the network to point to the ISP router, so it is decided that:
Branch router will retain its default route to the ISP, and it will advertise a default route to the network.

The customer has one more caveat: There are plans to expand the network by adding routers and connecting them to switch SW2. Until the network has been stabilized, it is advised that the new routers must not receive the advertisements from the rest of the network, so that the network expansion does not send additional traffic to the live network.

Topology



Job Aid

Device Information

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
SW1	VLAN 1	172.16.130.10/24	VLAN 1	_	_
SW1	Ethernet0/1	VLAN 1	Branch	Ethernet0/0	172.16.130.3/24
SW1	Ethernet0/2	VLAN 1	AdminPC	Ethernet0/0	172.16.130.5/24
SW1	Ethernet0/3	VLAN 1	Fileserver	Ethernet0/0	172.16.130.6/24
Branch	Ethernet0/0	172.16.130.3/24	SW1	Ethernet0/1	VLAN 1
Branch	Ethernet0/1	209.165.200.226/27	Internet	Ethernet0/0	209.165.200.225/27
Branch	Ethernet0/2	172.16.160.3/24	R1	Ethernet0/0	172.16.160.1/24
Branch	Loopback 0	172.16.2.2/32	_	_	_
R1	Ethernet0/0	172.16.160.1/24	Branch	Ethernet0/2	172.16.160.3/24
R1	Loopback 0	172.16.1.1/32	_	_	_

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
AdminPC	Ethernet0/0	172.16.130.5/24	SW1	Ethernet0/2	_
Fileserver	Ethernet0/0	172.16.130.6/24	SW1	Ethernet0/3	_
Internet	Loopback 0	209.165.201.1/32	_	_	_

Task 1: Evaluation Lab Procedure

Activity

Step 1 Remove the static routes from the Branch router and router R1. Do not remove the default route on the Branch router that points to the Internet Router.

Step 2 Implement RIPv2 on the Branch router and router R1 with auto summarization disabled. Configure RIP so that it is advertised on all interfaces using a single command.

Step 3 Enable RIPv2 to originate a default route from the Branch router to Router R1.

Step 4 Ensure that the RIPv2 not enabled between switch SW2.

Verification

Step 1 Verify that the static routes are removed from the Branch router and router R1.

Substep 1

Verify the routing table on the router R1. Verify that the default route to the Branch router is removed and only the connected and loopback networks are displayed in the output of the **show ip route** command.

```
R1# show ip route

      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.1.1/32 is directly connected, Loopback0
C        172.16.160.0/24 is directly connected, Ethernet0/0
L        172.16.160.1/32 is directly connected, Ethernet0/0
```

Verify the routing table on Branch router. Use the **show ip route** command to verify that the static route to router R1 is removed and the default route to the Internet router still exists along with the connected and loopback networks.

```
Branch# show ip route
Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.225
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.2.2/32 is directly connected, Loopback0
C        172.16.130.0/24 is directly connected, Ethernet0/0
L        172.16.130.3/32 is directly connected, Ethernet0/0
C        172.16.160.0/24 is directly connected, Ethernet0/2
L        172.16.160.3/32 is directly connected, Ethernet0/2
```

```
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Ethernet0/1
L        209.165.200.226/32 is directly connected, Ethernet0/1
```

If the command output does not show the desired output, it indicates that the static and default routes are not removed from the respective routers.

Step 2 Verify that the RIPv2 enabled between router R1 and Branch router.

Substep 1

Verify that the Branch router is able to establish RIPv2 with router R1. You can verify it by checking the router R1's loopback address in routing table on the Branch router.

```
Branch# show ip route
Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.225
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
R        172.16.1.1/32 [120/1] via 172.16.160.1, 00:00:05, Ethernet0/2
C        172.16.2.2/32 is directly connected, Loopback0
C        172.16.130.0/24 is directly connected, Ethernet0/0
L        172.16.130.3/32 is directly connected, Ethernet0/0
C        172.16.160.0/24 is directly connected, Ethernet0/2
L        172.16.160.3/32 is directly connected, Ethernet0/2
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Ethernet0/1
L        209.165.200.226/32 is directly connected, Ethernet0/1
```

If the command output does not show the desired result, it indicates that the Branch router is not able to peer with router R1.

Step 3 Verify that the default route that is originated from the Branch router exists on router R1.

Substep 1

Check the routing table on Router R1 to see that a default route exists that points to router Branch.

```
R1# show ip route

Gateway of last resort is 172.16.160.3 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 172.16.160.3, 00:00:22, Ethernet0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.1.1/32 is directly connected, Loopback0
R        172.16.2.2/32 [120/1] via 172.16.160.3, 00:00:22, Ethernet0/0
R        172.16.130.0/24 [120/1] via 172.16.160.3, 00:00:22, Ethernet0/0
C        172.16.160.0/24 is directly connected, Ethernet0/0
L        172.16.160.1/32 is directly connected, Ethernet0/0
      209.165.200.0/27 is subnetted, 1 subnets
R        209.165.200.224 [120/1] via 172.16.160.3, 00:00:22, Ethernet0/0
```

If the command output does not show the desired result, it is because of one of the following reasons:
1) the default route has not been originated properly on Branch router,

2) and router R1 is not peering with Branch router using RIP .

Step 4 Verify that the proper measures have been taken to prevent RIPv2 being enabled between switch SW2 and router R1.

Substep 1

Use the **passive-interface** command to ensure that RIPv2 updates are suppressed on a particular interface.

```
R1# show run | begin router rip
router rip
  version 2
  passive-interface ethernet0/1
  no auto-summary
  network 0.0.0.0
```

If this task is not completed successfully, then the interface E0/1 will peer with any of the routers using RIP. It indicates that the interface is not configured as a passive interface under the routing protocol instance of RIP on router R1.

Command List

The table describes the commands that are used in the activity. Refer to the list if you need configuration command assistance during the lab activity.

Command	Description
ip route *prefix mask*	To configure static routes, use the **ip route** command in global configuration mode. Prefix denotes IP route prefix for the destination and mask denotes prefix mask for the destination.
router rip	Enables a RIP routing process, which places you in router configuration mode.
network *ip-address*	Associates a network with a RIP routing process.
version 2	Configures the software to receive and send only RIP Version 2 packets.
no auto-summary	Disables automatic summarization.
default-information originate	Generates a default route into Routing Information Protocol (RIP), use the **default-information originate** command in router configuration mode.
passive-interface *interface*	Specifying an interface name sets only that interface to passive RIP mode. In passive mode, RIP routing updates are accepted by, but not sent out of, the specified interface.
show ip rip database	Display the contents of the RIP routing database.

Answer Key

Challenge 3: Implementing RIPv2

Task 1: Evaluation Lab Procedure

Activity

Step 1 Static routes are used initially till dynamic routing is established. Remove the static routes and default routes that are present on Branch router and router R1, except the default route on the Branch router that points to the Internet.

Use the command that is shown below, to remove the default route on router R1.

```
R1(config)# no ip route 0.0.0.0 0.0.0.0 172.16.160.3
```

Use the command that is shown below, to remove the static route on Branch router for the loopback address of router R1.

```
Branch(config)# no ip route 172.16.1.1 255.255.255.255 172.16.160.1
```

Step 2 Remember the following parameters when enabling RIP:
1) Enable RIPv2 protocol using **router rip** command.
2) Ensure that the version of RIP is version 2 using the **version 2** command.
3) Ensure that autosummarization is disabled using the **no auto-summary** command.

Enable RIPv2 with auto-summarization disabled, on Branch router.

```
Branch(config)# router rip
Branch(config-router)# version 2
Branch(config-router)# no auto
```

Enable RIPv2 on Branch router to advertise on the all networks.

```
Branch(config)# router rip
Branch(config-router)# network 0.0.0.0
```

Enable RIPv2 with auto-summarization disabled, on router R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# no auto
```

Enable RIPv2 on router R1 to advertise on all networks.

```
R1(config)# router rip
R1(config-router)# network 0.0.0.0
```

Step 3 Since, the Branch router is configured as a default router for the network, all other routers in the network must point to the Branch router as their default gateway.

Use the **default-information originate** command, under the RIP process.

```
Branch(config)# router rip
Branch(config-router)# default-information originate
```

Step 4 In a previous task, you configured Router R1 to advertise RIP on all interfaces. You need to implement a RIP configuration to prevent R1 being enabled between SW2 through the interface E0/1.

Use the **passive-interface** command to disable RIP Advertisements on interface E0/1 on Router R1.

```
R1(config)# router rip
R1(config-router)# passive-interface e0/1
```

Module 5: Introducing IPv6

Lesson 3: Configuring IPv6 Static Routes

Challenge 4: Implement IPv6 Static Routing

Introduction

You are piloting the IPv6 implementation along with IPv4, and ISP has provided you with the following IPv6 addresses for testing purpose during the pilot phase, to make sure that these IPv6 addresses are reachable from your network.

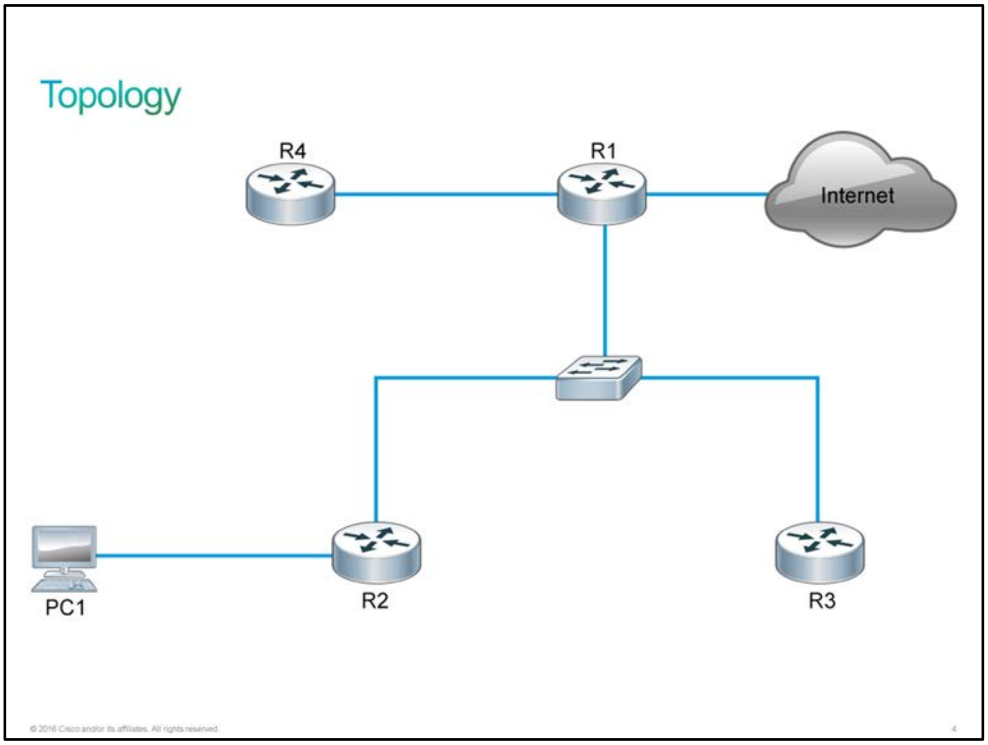
The following are the IPv6 global addresses that are configured on the Internet router for testing purpose.

- 2001:DB8:0:1A::1/64
- 2001:DB8:0:1B::1/64
- 2001:DB8:0:1C::1/64

You must implement IPv6 static routing to ensure that the above mentioned IPv6 addresses are reachable from devices R1, R2, R3, R4, and PC1.

- You are recommended to use the stateless autoconfiguration method to implement IPv6 addressing and to receive a default route on router R4.
- You must configure a default route using IPv6 global address on router R1 to establish the connectivity with Internet router. Do not use the autoconfiguration method on router R1.
- You must configure a default route using link local address on router R3 to establish the connectivity with Internet router. Do not use the autoconfiguration method on router R3.
- IPv6 configurations are already configured on the other devices. However, you need to investigate any incomplete or misconfigurations. Also, ensure that the connectivity from all devices exists to the IPv6 addresses that are provided by the ISP.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	Interface	IPv6 Address	Remote	Interface	IPv6 Address
R1	Ethernet0/0	2001:DB8:0:4::1/64	SW1	Ethernet0/0	VLAN 1
R1	Ethernet0/1	2001:DB8:0:6::2/64	Internet	Ethernet0/0	2001:DB8:0:6::1/64
R1	Ethernet0/2	2001:DB8:0:3::1/64	R4	Ethernet0/0	Autoconfig
R2	Ethernet0/0	2001:DB8:0:4::2/64	SW1	Ethernet0/1	VLAN 1
R2	Ethernet0/1	2001:DB8:0:5::1/64	PC1	Ethernet0/0	Autoconfig
R3	Ethernet0/0	2001:DB8:0:4::3/64	SW1	Ethernet0/2	VLAN 1

Device	Interface	IPv6 Address	Remote	Interface	IPv6 Address
R4	Ethernet0/0	Autoconfig	R1	Ethernet0/2	2001:DB8:0:3::1/64
PC1	Ethernet0/0	Autoconfig	R2	Ethernet0/1	2001:DB8:0:5::1/64
Internet	Ethernet0/0	2001:DB8:0:6::1/64	R1	Ethernet0/1	2001:DB8:0:6::2/64
Internet	Loopback 1	2001:DB8:0:1A::1/64	_	_	_
Internet	Loopback 2	2001:DB8:0:1B::1/64	_	_	_
Internet	Loopback 3	2001:DB8:0:1C::1/64	_	_	_

Task 1: Evaluation Lab Procedure

Activity

Step 1 Configure a default route command on router R1 that points to the Internet router, in the default route configuration command use a global ipv6 address for the next hop address. Verify that the connectivity exists between the Internet router and ISP provided IPv6 addresses.

Step 2 Configure router R4 to receive an IPv6 address and default route, from router R1 through stateless autoconfiguration method. Verify that the connectivity exists to ISP provided IPv6 addresses.

Step 3 Configure a default route on router R3 that points to router R1, in default route configuration include an exit interface and use a link local address for the next hop address. Verify that the connectivity exists between router R3 and ISP provided IPv6 addresses.

Step 4 Verify the configurations on router R1 and R2 to identify, and fix the issues that are related to static route misconfigurations.

Verification

Step 1 Verify that the IPv6 default route that points to Internet router is configured on router R1.

Substep 1

Use the **show run** and **show ipv6 route** commands to verify that the IPv6 default route is configured correctly. Ping the ISP provided IPv6 addresses such as 2001:DB8:0:1A::1, 2001:DB8:0:1B::1, and 2001:DB8:0:1C::1 to verify the connectivity.

```
R1# show run | incl ipv6 route ::/0
ipv6 route ::/0 2001:DB8:0:6::1


R1# show ipv6 route static
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
S   ::/0 [1/0]
     via 2001:DB8:0:6::1
S   2001:DB8:0:5::/64 [1/0]
     via 2001:DB8:0:6::1

R1# ping 2001:DB8:0:1A::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1A::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/18 ms
R1# ping 2001:DB8:0:1B::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1B::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
R1# ping 2001:DB8:0:1C::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1C::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
R1#
```

If the command output does not show the desired result, it indicates that the IPv6 default route with the global ipv6 address for the next hop address is not configured correctly.

Step 2

Verify that the IPv6 address and the default route are received on router R4 from router R1 through the stateless autoconfiguration method.

Substep 1

Use the **show run interface e0/0** and **show ipv6 route** commands to verify that the IPv6 address and the default route are received from router R1. Ping the ISP provided IPv6 addresses such as 2001:DB8:0:1A::1, 2001:DB8:0:1B::1, and 2001:DB8:0:1C::1 to verify the connectivity.

```
R4# show run interface e0/0
Building configuration...

Current configuration : 101 bytes
!
interface Ethernet0/0
 ip address 192.168.14.4 255.255.255.0
 ipv6 address autoconfig default


R4# show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
ND  ::/0 [2/0]
     via FE80::A8BB:CCFF:FE00:120, Ethernet0/0
NDp 2001:DB8:0:3::/64 [2/0]
     via Ethernet0/0, directly connected
L   2001:DB8:0:3:A8BB:CCFF:FE00:400/128 [0/0]
     via Ethernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive

R4# ping 2001:DB8:0:1A::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1A::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R4# ping 2001:DB8:0:1B::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1B::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R4# ping 2001:DB8:0:1C::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1C::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/17 ms
```

If the command output does not show the desired result, it indicates that the **ipv6 address autoconfig default** command is not configured correctly on router R4.

Step 3

Verify that the IPv6 default route that points to R3 is configured on router R1.

Substep 1

Use the **show run** and **show ipv6 route** commands to verify that the IPv6 default route configured correctly on router R3. Ping the ISP provided IPv6 addresses such as 2001:DB8:0:1A::1, 2001:DB8:0:1B::1, and 2001:DB8:0:1C::1 to verify the connectivity.

```
R3# show run | incl ipv6 route ::/0
ipv6 route ::/0 Ethernet0/0 FE80::A8BB:CCFF:FE00:100
!
R3#show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
S   ::/0 [1/0]
     via FE80::A8BB:CCFF:FE00:100, Ethernet0/0
C   2001:DB8:0:4::/64 [0/0]
     via Ethernet0/0, directly connected
L   2001:DB8:0:4::3/128 [0/0]
     via Ethernet0/0, receive
L   FF00::/8 [0/0]
```

```
     via Null0, receive
R3#

R3# ping 2001:DB8:0:1A::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1A::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
R3# ping 2001:DB8:0:1B::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1B::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R3# ping 2001:DB8:0:1C::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1C::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R3#
```

If the command output does not show the desired result, it indicates that the ipv6 default route command with an exit interface and link local address for the next hop address are not configured correctly.

Step 4 Verify that the static route configurations are correct and any misconfigurations that are on routers R1 and R2 are corrected.

Substep 1

Use **show ipv6 route** and **show run** commands to verify that the static route configurations are correct. Ping from PC1 to ISP provided IPv6 addresses such as 2001:DB8:0:1A::1, 2001:DB8:0:1B::1, and 2001:DB8:0:1C::1 to verify the connectivity.

```
R2# show run
Building configuration...
Current configuration : 1201 bytes
!
!
ipv6 route 2001:DB8:0:1A::/64 2001:DB8:0:4::1
ipv6 route 2001:DB8:0:1B::/64 2001:DB8:0:4::1
ipv6 route 2001:DB8:0:1C::/64 2001:DB8:0:4::1
!
!

R2# show ipv6 route static
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
S   2001:DB8:0:1A::/64 [1/0]
     via 2001:DB8:0:4::1
S   2001:DB8:0:1B::/64 [1/0]
```

```
     via 2001:DB8:0:4::1
S   2001:DB8:0:1C::/64 [1/0]
     via 2001:DB8:0:4::1
R2#
```

```
R1# show run | incl ipv6 route
ipv6 route 2001:DB8:0:5::/64 2001:DB8:0:4::2
ipv6 route ::/0 2001:DB8:0:6::1
```

```
R1# show ipv6 route static
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
S   ::/0 [1/0]
     via 2001:DB8:0:6::1
S   2001:DB8:0:5::/64 [1/0]
     via 2001:DB8:0:4::2

PC1# ping 2001:DB8:0:1A::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1A::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/19 ms
PC1# ping 2001:DB8:0:1B::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1B::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PC1# ping 2001:DB8:0:1C::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:1C::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PC1#
```

If the command output does not show the desired result, it indicates that the static route misconfigurations on routers R1 and R2 are not corrected.

Command List

The table describes the commands that are used in this activity.Refer to this list if you need configuration command assistance during the lab activity.

Command	Description
ipv6 unicast-routing	Used in global configuration mode to enable the forwarding of IPv6 unicast datagrams.
ipv6 address {*ipv6-address/prefix-*	Used in interface configuration mode to configure an IPv6 address based

Command	Description
length | prefix-name sub-bits/prefix-length}	on an IPv6 general prefix and to enable IPv6 processing on an interface.
show ipv6 route	Used in user EXEC or privileged EXEC mode to display the current contents of the IPv6 routing table.
ipv6 route *ipv6-prefix/prefix-length ipv6-address*	Used in global configuration mode to create static IPv6 routes. To remove a previously configured static route, use the no form of this command.
ipv6 address autoconfig [default]	Used in interface configuration mode to enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and to enable IPv6 processing on the interface. To remove the address from the interface, use the no form of this command.

Answer Key

Challenge 4: Implement IPv6 Static Routing

Task 1: Evaluation Lab Procedure

Activity

Step 1 Configure a default route on router R1 that points to the Internet router. Use global ipv6 address for the next hop address.

Use the command that is shown below to accomplish the task.

```
R1(config)# ipv6 route ::/0 2001:DB8:0:6::1
```

Step 2 Configure router R4 to receive an IPv6 address, and a default route through the stateless autoconfiguration method.

Use the commands that are shown below to accomplish the task.

```
R4(config)# int e0/0
R4(config-if)# ipv6 address autoconfig default
```

Step 3 Configure a default route on router R3 that points to the router R1. Include an exit interface and use a link local address for the next hop address.

Use the **show ipv6 interface brief** command on router R1, to identify the link local address of the next hop interface.

```
R1# show ipv6 int brief
Ethernet0/0            [up/up]
    FE80::A8BB:CCFF:FE00:100
    2001:DB8:0:4::1
Ethernet0/1            [up/up]
    FE80::A8BB:CCFF:FE00:110
    2001:DB8:0:6::2
Ethernet0/2            [up/up]
    FE80::A8BB:CCFF:FE00:120
    2001:DB8:0:3::1
Ethernet0/3            [administratively down/down]
    unassigned
NVI0                   [up/up]
    unassigned
```

Use the command that is shown below to configure a default route on router R3.

```
R3(config)# ipv6 route ::/0 e0/0 FE80::A8BB:CCFF:FE00:100
```

Step 4 Identify and fix any static route misconfigurations on routers R1 and R2. Verify connectivity from PC1 to ISP provided IP addresses on the Internet router.

Examine configurations on router R2, observe that static route that is configured on R2 has an incorrect exit interface and an incorrect IPv6 global address configured for the next hop address.

```
R2#show run
Building configuration...

Current configuration : 1201 bytes
!
! Last configuration change at 04:54:55 PST Wed Dec 30 2015

ipv6 route 2001:DB8:0:1A::/64 2001:DB8:0:4::3
ipv6 route 2001:DB8:0:1B::/64 2001:DB8:0:4::3
ipv6 route 2001:DB8:0:1C::/64 2001:DB8:0:4::3
!
```

The output of the show run command shows that the static route has an exit interface that is pointing incorrectly to interface E0/2 instead of interface E0/0, and the next hop IPv6 global address is pointing to router R2 instead of next hop global IPv6 address of router R1.

Use the configuration commands that are shown below to fix static route configuration on router R2.

```
R2(config)# no ipv6 route 2001:DB8:0:1A::/64 2001:DB8:0:4::3
R2(config)# no ipv6 route 2001:DB8:0:1B::/64 2001:DB8:0:4::3
R2(config)# no ipv6 route 2001:DB8:0:1C::/64 2001:DB8:0:4::3
R2(config)# ipv6 route 2001:DB8:0:1A::/64 2001:DB8:0:4::1
R2(config)# ipv6 route 2001:DB8:0:1B::/64 2001:DB8:0:4::1
R2(config)# ipv6 route 2001:DB8:0:1C::/64 2001:DB8:0:4::1
```

Examine configurations on router R1, observe that the static route that is configured on router R1 for the reverse traffic flow to IP address 2001:DB8:0:5::/64 from the ISP provided IP address has an incorrect exit interface and an incorrect IPv6 global address configured for the next hop address.

```
R1#show run
Building configuration...

Current configuration : 1629 bytes

ipv6 route 2001:DB8:0:5::/64 2001:DB8:0:6::1
```

Use the configuration commands that are shown below to fix static route configuration on route R1.

The static route has an exit interface that is configured incorrectly, it is pointing to interface E0/1 instead of pointing to interface E0/0, and the next hop IPv6 global address is pointing to the Internet router instead of pointing to the next hop IPv6 global address of router R2.

```
R1(config)# no ipv6 route 2001:DB8:0:5::/64 2001:DB8:0:6::1
R1(config)# ipv6 route 2001:DB8:0:5::/64 2001:DB8:0:4::2
```

Module 6: Troubleshooting Basic Connectivity

Lesson 1: Troubleshooting IPv4 Network Connectivity

Challenge 5: Troubleshooting IPv4 Connectivity

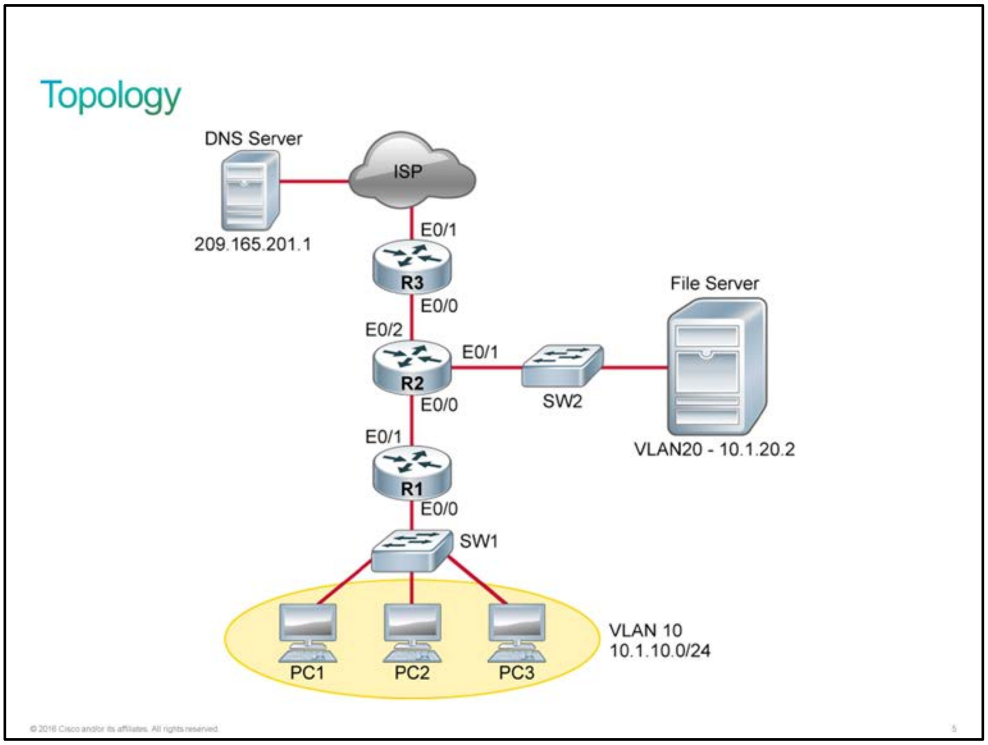
Introduction

ABC network has just completed its network implementation and has run into few issues. You have been contracted to work with ABC to resolve all network issues. They are running RIPv2 as the routing protocol. R3 is the edge router and it should be injecting a default route in RIP. The PCs are in VLAN 10 on switch SW1. The File Server is in VLAN 20 on switch SW2. The router R3 is connected to the ISP gateway. The DNS server is in the ISP cloud. Router R2 is the DHCP server for the PCs in the network. You are allowed to make changes in the access-list if required but not delete any line from the access-list or remove the access-lists.

Following are the network issues that you need to resolve.

- PC1 cannot get to internet. Use IP address, 209.165.202.225 to test internet connectivity.
- PC2 cannot ping the test host *icnd2.com*.
- PC3 cannot ping the File Server.
- There is intermittent connectivity to the internet at certain times of the day. It is suspected that it could be an issue at the ISP end. You have been asked to set up an IP SLA with number 1 and frequency 15 to perform an ICMP echo test to the ISP default gateway on router, R3. The IP SLA schedule should start immediately and run indefinitely.

Topology



Job Aid

Note	If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Note	The PCs may take a few minutes to get the IP address from the DHCP server.

Device Information

Local		**Remote**	
Device	IP Address	Device	IP Address
R1 (Ethernet 0/0)	_	SW1 (Ethernet 0/0)	Trunk
R1 (Ethernet 0/0.1)	192.168.1.2/30	SW1 via VLAN 1	192.168.1.1/30
R1 (Ethernet 0/0.10)	10.1.10.1/24	PC1, PC2, and PC3 via VLAN 10	DHCP

Local		Remote	
R1 (Ethernet 0/1)	10.1.1.1	R2 (Ethernet 0/0)	10.1.1.2
R2 (Ethernet 0/1)	_	SW2 (Ethernet 0/0)	Trunk
R2 (Ethernet 0/1.1)	192.168.1.6/30	SW2 (VLAN 1)	192.168.1.5/30
R2 (Ethernet 0/1.20)	10.1.20.1/24	File Server	10.1.20.2/24
R2 (Ethernet 0/2)	10.1.1.5/30	R3 (Ethernet 0/0)	10.1.1.6/30
R3 (Ethernet 0/1)	209.165.200.226/30	ISP	209.165.200.225/30

The DNS server IP address is 209.165.201.1

To test internet connectivity, ping the IP address 209.165.202.225.

Task 1: Troubleshooting IPv4 Connectivity Lab Procedure

Activity

Step 1 Troubleshoot and resolve the loss of connectivity between PC1 and internet. Make sure that the routers are learning the default route from RIP. R3 should be injecting the default route in RIP.

Step 2 Identify and correct the issue that is related to the inability of PC2 to ping test host *icnd2.com*. Make sure that the DNS server has been configured correctly on R2 which is the DHCP server for PC2.

Step 3 Troubleshoot and resolve the loss of connectivity between PC3 and File server. Make sure that the routes are configured correctly and there are no access-lists blocking the packets.

Step 4 Enable IP SLA monitoring for the ISP gateway on R3.

Verification

Step 1 Verify that PC1 is able to get to the internet.

Substep 1

On PC1, use **ping** command to verify that the connectivity issue is resolved.

```
PC1# ping  209.165.202.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
PC1#
```

If you do not get the desired result, check if the default route has been injected in RIP on R3.

Step 2 Verify that PC2 can ping the test host "icnd2.com."

Substep 1

On PC2, use **ping** command to verify that the connectivity issue is resolved.

```
PC2# ping icnd2.com
Translating "icnd2.com"...domain server (209.165.201.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PC2#
```

If you do not get the desired result, check the DNS setting on R2.

Step 3 Verify that PC3 can ping the File server.

Substep 1

On PC3, use **ping** command to verify that the connectivity issue is resolved.

```
PC3# ping 10.1.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

If you do not get the desired result, check the access-list configuration on R2.

Step 4 Verify that IP SLA has been configured on R3 to monitor the ISP gateway.

Substep 1

On R3, use the following commands to verify your configuration changes.

```
R3# show ip sla configuration
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 5000
Type of operation to perform: icmp-echo
Target address/Source address: 209.165.200.225/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 15  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None
```

```
R3# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: 1 milliseconds
Latest operation start time: 03:39:03 PST Thu Nov 12 2015
Latest operation return code: OK
Number of successes: 5
Number of failures: 0
Operation time to live: Forever
```

If you do not get the desired result, check the configuration on R3.

Command List

The table describes the commands that are used in the activity. Refer to this list if you need configuration command assistance during the lab activity.

Command	Description
ping {*host-name* | *system-address*}	Used in user EXEC or privileged EXEC mode to diagnose basic network connectivity
show ip route	Used in EXEC mode to display the current state of the routing table
ip route 0.0.0.0 0.0.0.0 <*next hop IP address*>	Used to configure default route in global configuration mode.
ip dhcp pool *name*	Used in global configuration mode to configure a DHCP address pool on a DHCP server and to enter DHCP pool configuration mode
dns-server *address [address2 ... address8]*	Used in DHCP pool configuration mode to specify the DNS IP servers available to a DHCP client; use the no form of this command to remove the DNS server list
ip access-list {**standard** | **extended**} {*access-list-name* | *access-list-number}*	Used in global configuration mode to define an IP access list by name or number
permit *protocol* [*source-addr source-wildcard*] { **any** | **host** { *address* | *name* } } { *destination-addr destination-*	Used in ACL configuration mode to set conditions in a named IP access list that will permit packets

Command	**Description**
wildcard | **any** | **host** { *address* | *name* } }	
show access-lists [*access-list-number* | *access-list-name*]	Used in user EXEC or privileged EXEC mode to display the contents of current ACLs
ip sla *operation-number*	Creates an IP SLAs operation, and enter IP SLAs configuration mode.
icmp-echo *destination-ip-address*	Configures ICMP Echo test for the specified destination.
frequency *seconds*	(Optional) Set the rate at which a specified IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.
ip sla schedule *operation-number* [**life {forever** | *seconds***}**][**start-time {***hh:mm[:ss] [month day* | *day month*] | **pending | now | after** *hh:mm:ss***}**] [**ageout** *seconds*] **[recurring**]	Configure the scheduling parameters for an individual IP SLAs operation. With the life keyword, you set how long the IP SLA test will run. If you choose forever, the test will run until you manually remove it. By default IP SLA test will run for 1 hour. With the **start-time** keyword, you will set when the IP SLA test should start. You can start the test right away by issuing now keyword, or you can configure a delayed start. With the age out keyword, you can control how long the collected data is kept. With the recurring keyword, you can schedule a test to run periodically—for example the same time each day.

Answer Key

Challenge 5: Troubleshooting IPv4 Connectivity

Task 1: Troubleshooting IPv4 Connectivity Lab Procedure

Activity

Step 1 Check the routing path from PC1 to the internet to resolve the connectivity issue.

Use **traceroute** command to check the path from PC1 to internet.

```
PC1# traceroute 209.165.202.225
Type escape sequence to abort.
Tracing the route to 209.165.202.225
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.10.1 0 msec 1 msec 1 msec
  2  *  !H  *
PC1#
```

The packet drops at the first hop which is the default gateway for the PC1. R1 is 10.1.10.1. Check the routing table on R1.

```
R1# show ip route 0.0.0.0
% Network not in table
```

R1 should be learning the default route from RIPv2. R3 is the edge router and it should be injecting the default route into RIP. Make the configuration change in R3 to ensure that the routers get the default route.

```
R3(config)# router rip
R3(config-router)# default-information originate
```

Now, there should be connectivity from PC1 to internet.

Step 2 Isolate the connectivity issue to host *icnd2.com* from PC2.

Use **ping** command to check the connectivity to host "icnd2.com."

```
PC2# ping icnd2.com
Translating "icnd2.com"...domain server (209.165.201.2)
% Unrecognized host or address, or protocol not running.
```

The DNS server IP address is incorrect. Router, R2 is the DHCP server for PC2. Check the DHCP configuration on R2 and correct the DNS server IP address

```
R2(config)# ip dhcp pool Workstations
R2(dhcp-config)# no  dns-server 209.165.201.2
R2(dhcp-config)# dns-server 209.165.201.1
```

Now, you need to reset the interface E0/0 on PC2 to ensure that DHCP occurs with revised information.

```
PC2(config)# interface ethernet 0/0
PC2(config-if)# shutdown
PC2(config-if)# no shutdown
```

You should be able to **ping** the host icnd2.com now.

Step 3 Resolve the connectivity issue between PC3 and File server by checking the routing path and access-lists.

First, use **ping** and **traceroute** command on PC3 to check the connectivity.

```
PC3# ping 10.1.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.20.2, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

```
PC3# traceroute 10.1.20.2
Type escape sequence to abort.
Tracing the route to 10.1.20.2
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.10.1 1 msec 1 msec 0 msec
  2 10.1.1.2 1 msec 1 msec 1 msec
  3 10.1.1.2 !A  !A  *
```

The packet is getting to R2 and so you need to check the configuration on R2. File server is connected to Interface E0/1.20 on R2 via SW2. Check this interface, E0/1.20 configuration on R2.

```
R2# show run interface ethernet 0/1.20
Building configuration...

Current configuration : 154 bytes
!
interface Ethernet0/1.20
 description to FileServer
 encapsulation dot1Q 20
 ip address 10.1.20.1 255.255.255.0
 ip access-group to_FileServer out
end
```

There is an access-list in applied to this interface. ICMP needs to be allowed in this access-list so that PC3 can ping the File server.

```
R2(config)# ip access-list extended to_FileServer
R2(config-ext-nacl)# 20 permit icmp 10.1.10.0 0.0.0.255 host 10.1.20.2
```

Now, PC3 should be able to ping the File server. There are various ways in which this access-list can be modified but you need to make sure that you do not delete any line from this access-list.

Step 4 Configure IP SLA to perform an echo test to ISP gateway on R3.

On R3, enter the following commands:

```
R3(config)# ip sla 1
R3(config-ip-sla)# icmp-echo 209.165.200.225
R3(config-ip-sla-echo)# frequency 15
R3(config-ip-sla-echo)# exit
R3(config)# ip sla schedule 1 life forever start-time now
```

Lesson 2: Troubleshooting IPv6 Network Connectivity

Challenge 6: Troubleshooting IPv6 Connectivity

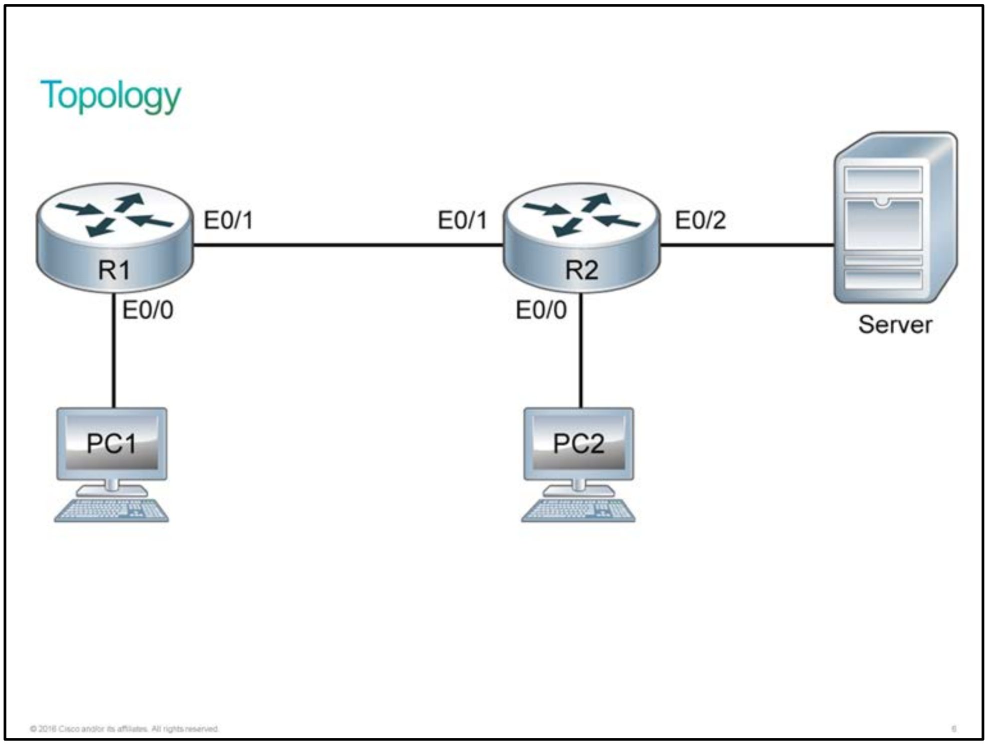
Introduction

Senior Engineer, Chris wants to test your skills in IPv6 Troubleshooting. He has set up a lab and injected some errors. You are required to resolve the issues in the lab. There are IPv6 static routes in the network.

Following are the issues that you need to resolve :

- PC1 is unable to telnet to Server. The telnet password for Server is *cisco123*.
- PC2 cannot ping PC1.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Local Device (Interface)	IPv6 Address	Remote Device (Interface)
R1 (Ethernet0/1)	2001:DB8:A:C1C2::1/64	R2 (Ethernet0/1)
R1 (Ethernet0/0)	2001:DB8:A:C1::1/64	PC1
R2 (Ethernet0/0)	2001:DB8:A:C2::1/64	PC2
R2 (Ethernet0/1)	2001:DB8:A:C1C2::2/64	R1 (Ethernet0/1)
R2 (Ethernet0/2)	2001:DB8:A:C3::1/64	Server
PC1	2001:DB8:A:C1::2	_
PC2	2001:DB8:A:C2::2	_
Server	2001:DB8:A:C3::2	_

The telnet password for Server is *cisco123*.

Task 1: Troubleshooting IPv6 Connectivity Lab Procedure

Activity

Step 1 Troubleshoot the IPv6 connectivity issue between PC1 and Server. Ensure that you can reach the server IPv6 address and the TCP traffic for port 23 is allowed for telnet access.

Step 2 Troubleshoot the IPv6 connectivity issue between PC2 and PC1. Ensure that IPv6 static routes are configured correctly on each router.

Verification

Step 1 Verify that PC1 can access the Server.

Substep 1

Use **telnet** command to verify that the connectivity issue is resolved. Telnet password is *cisco123*.

```
PC1# telnet 2001:DB8:A:C3::2
Trying 2001:DB8:A:C3::2 ... Open

User Access Verification

Password:
Server>exit
```

If you do not get the desired result, check the configuration on R1 and R2.

Step 2 Verify the connectivity between PC2 and PC1

Substep 1

Use **ping** command to verify that the connectivity issue is resolved.

```
PC2# ping 2001:DB8:A:C1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:A:C1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
PC2#
```

If you do not get the desired result, check the configuration on R1 and R2.

Command List

The table describes the commands that are used in activity. Refer to the list if you need configuration command assistance during lab activity.

Command	Description
ping {*host-name* | *system-address*}	Used in user EXEC or privileged EXEC mode to diagnose basic network connectivity
show ipv6 route	Used in EXEC mode to display the current state of the routing table
ipv6 unicast-routing	Enable forwarding of IPv6 unicast data packets.
ipv6 route *ipv6-prefix/prefix length {ipv6-address | interface-id [ipv6-address]} [administrative distance]*	Configure a static IPv6 route. •ipv6-prefix—The IPv6 network that is the destination of the static route. It can also be a hostname when static host routes are configured. •/prefix length—The length of the IPv6 prefix. •ipv6-address—The IPv6 address of the next hop that can be used to reach the specified network. •interface—Specify direct static routes from point-to-point and broadcast interfaces.
show ipv6 access-list *<name>*	Use this command to display the access-list configuration.
ipv6 access-list *access-list-name*	Define an IPv6 access list name, and enter IPv6 access-list configuration mode.

Command	**Description**
deny | permit *protocol {source-ipv6-prefix/prefix-length* | **any | host** *source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length* **| any | host** *destination-ipv6-address} [operator [port-number]] [dscp value] [fragments] [log] [log-input] [sequence value] [time-range name]*	Enter deny or permit statement to specify whether to deny or permit the packet if conditions are matched.

Answer Key

Challenge 6: Troubleshooting IPv6 Connectivity

Task 1: Troubleshooting IPv6 Connectivity Lab Procedure

Activity

Step 1 Isolate and correct the IPv6 connectivity between PC1 and Server.

On PC1, use **traceroute** command to trace the path to the Server IP address.

```
PC1# traceroute 2001:DB8:A:C3::2
Type escape sequence to abort.
Tracing the route to 2001:DB8:A:C3::2

  1 2001:DB8:A:C1::1 18 msec 5 msec 5 msec
  2 2001:DB8:A:C1C2::2 27 msec 4 msec 5 msec
  3 2001:DB8:A:C3::2 18 msec 5 msec 5 msec
```

From the output, it implies that the Server can be reached and so routing is working fine. Now, check the configuration on router R2 interface Ethernet0/2. There is an access-list that is configured on interface, E0/2 that denies all TCP traffic. You need to modify this access-list to allow TCP traffic so that PC1 can telnet to the Server.

```
R2(config)# ipv6 access-list  FILTER
R2(config-ipv6-acl)# sequence 5 permit tcp any any
R2(config-ipv6-acl)# no sequence 10
```

Now, you should be able to telnet.

Step 2 Isolate and correct the IPv6 connectivity between PC2 and PC1.

Use **traceroute** command on PC2 to check if it can reach PC1.

```
PC2# traceroute  2001:DB8:A:C1::2
Type escape sequence to abort.
Tracing the route to 2001:DB8:A:C1::2

  1 2001:DB8:A:C2::1 18 msec 5 msec 4 msec
  2  *  *  *
  3  *  *  *
  4  *  *  *
```

Now, check routing on routers, R2 and R1 for the remote subnets.

```
R2# show ipv6 route  2001:DB8:A:C1::2
Routing entry for 2001:DB8:A:C1::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:A:C1C2::1, Ethernet0/1
      Last updated 18:22:58 ago
```

```
R1# show ipv6 route  2001:DB8:A:C2::2
% Route not found
```

R1 does not have a route for the subnet connected to R2. Configure the IPv6 static route on R1.

```
R1(config)# ipv6 route  2001:DB8:A:C2::/64  2001:DB8:A:C1C2::2
```

Now, there should be IPv6 connectivity between PC1 and PC2.

Module 7: Implementing Network Device Security

Lesson 1: Securing Administrative Access

Challenge 7: Securing Device Administrative Access

Introduction

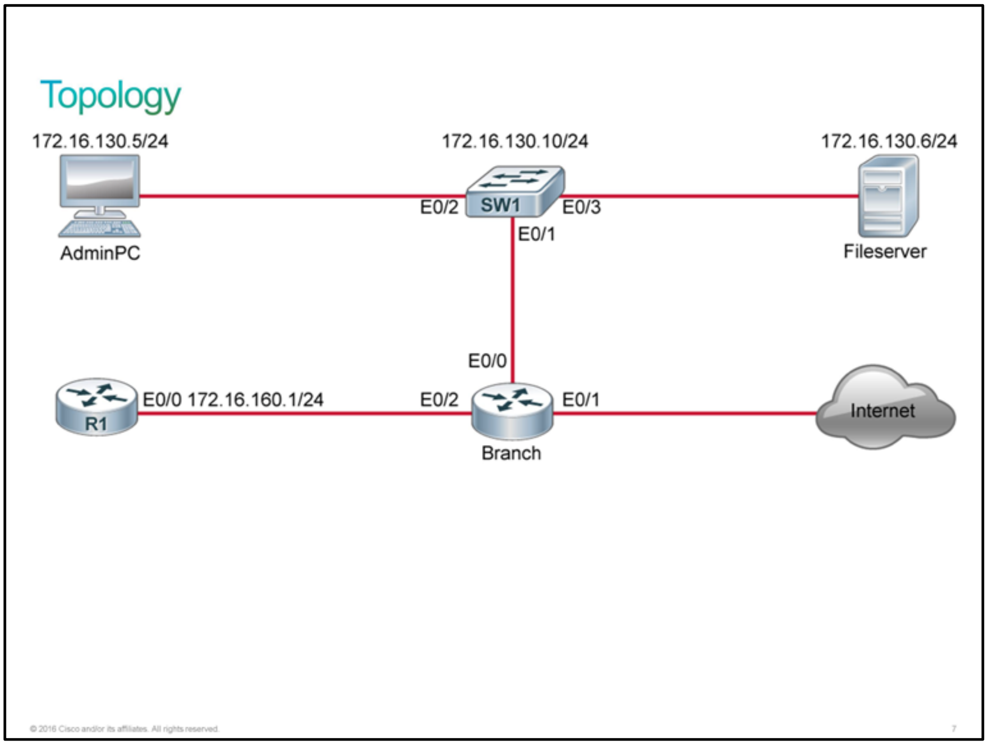
The basic network security policy was configured on the devices by your colleague, but you can still see that the configurations are incomplete as per the standard basic security policy adopted by CCS for customer environment. Identify and fix issues with the configurations.

The security policy that is adopted by CCS for router R1, Branch router, and switch SW1 is given below.

- Access to privilege mode must be secured using a password on all devices.
- Passwords must be encrypted on all devices.
- Access to the console and vty lines must be secured on all devices.
- Remote access must be secured by enabling SSH on vty 0 to 4.
- A standard IP ACL must be used to restrict remote access.
- A login banner must be present on all devices.

Refer to the Job aid section for login credential Information.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Login Credential & Device Information

Access Level	Username	Password
Console access	admin	AdminIcnd123
Remote access	admin	AdminIcnd123
Privileged mode	None	Icnd1

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
SW1	VLAN 1	172.16.130.10/24	VLAN 1	_	_
SW1	Ethernet0/1	VLAN 1	Branch	Ethernet0/0	172.16.130.3/24
SW1	Ethernet0/2	VLAN 1	AdminPC	Ethernet0/0	172.16.130.5/24

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
SW1	Ethernet0/3	VLAN 1	Fileserver	Ethernet0/0	172.16.130.6/24
Branch	Ethernet0/0	172.16.130.3/24	SW1	Ethernet0/1	VLAN 1
Branch	Ethernet0/1	209.165.200.226/27	Internet	Ethernet0/0	209.165.200.225/27
Branch	Ethernet0/2	172.16.160.3/24	R1	Ethernet0/0	172.16.160.1/24
Branch	Loopback 0	172.16.2.2/32	_	_	_
R1	Ethernet0/0	172.16.160.1/24	Branch	Ethernet0/2	172.16.160.3/24
R1	Loopback 0	172.16.1.1/32	_	_	_
AdminPC	Ethernet0/0	172.16.130.5/24	SW1	Ethernet0/2	_
Fileserver	Ethernet0/0	172.16.130.6/24	SW1	Ethernet0/3	_
Internet	Loopback 0	209.165.201.1/32	_	_	_

Task 1: Evaluation Lab Procedure

Activity

Step 1 Identify and troubleshoot the local authentication issue on router R1.

Step 2 Initiate an SSH session from AdminPC to router R1's IP address 172.16.160.1. If it fails, identify, and fix the issue.

Step 3 Enable password encryption on switch SW1 and Branch router, to encrypt the passwords on these devices.

Step 4 Initiate an SSH session from AdminPC to Branch router. If it fails, identify and fix the issue.

Step 5 Generate a pair of RSA keys on switch SW1 that allows the switch to support SSH version 2. Also, ensure that all the remote terminal sessions to the device take place over SSH. Use the domain name as "example.com," and use 768 bits in the modulus.

Verification

Step 1 Verify that the local authentication is enabled on the console and vty lines.erify that the local authentication is enabled on the console and vty lines.

Substep 1

Verify that the local authentication enabled on the console and vty lines on router R1.

```
R1# show run | begin line
line con 0
 logging synchronous
 login local
line aux 0
line vty 0 4
 access-class 11 in
 login local
```

Save the configuration and logout the router to verify that the local authentication works correctly.

```
!!! WARNING: ACCESS TO THIS DEVICE IS ONLY FOR AUTHORIZED PERSONNEL!!!

User Access Verification

Username: admin
Password:
R1>
```

If the command output does not show desired result, it indicates that the local authentication is not enabled on router R1.

Step 2 Verify that transport input protocol is configured as SSH on vty lines on router R1.

Substep 1

Verify that the vty lines on router R1 are configured with transport input protocol as SSH instead of telnet.

```
R1# show run | begin line vty
!
line vty 0 4
 access-class 11 in
 login local
 transport input ssh
```

If the command output does not show the desired result, it indicates that SSH is not enabled as transport input protocol on vty lines on router R1.

Step 3 Verify that the enable and local authentication passwords are encrypted.

Substep 1

Verify that the enable and local authentication passwords that are on switch SW1 and Branch router are encrypted.

```
Branch# show run
Building configuration...
service password-encryption
!
!
enable password 7 05220501251D
!
username admin password 7 0025170B0D55220501251D1C5A

SW1# show run
service password-encryption
```

```
!
enable password 7 062F0C2F481F
!
username admin password 7 15330F010D2402272637647040
```

If the command output does not show the desired result, it indicates that the service password encryption is not enabled on the switch SW1 and Branch router.

Step 4

Verify that the ACL statement that is configured to permit the traffic from IP address 172.16.130.5 to allow remote access on line vty on the Branch router

Substep 1

Verify that the traffic from IP address 172.16.130.5 is allowed on the vty lines on the Branch router. Initiate a SSH session on the port 22 (SSH) to IP address 172.16.160.3 from AdminPC.

```
Branch# show access-lists
Standard IP access list 11
    10 permit 172.16.130.5 (2 matches)

AdminPC# ssh -l admin 172.16.160.3

!!! WARNING: ACCESS TO THIS DEVICE IS ONLY FOR AUTHORIZED PERSONNEL!!!
Password:
```

If the command output does not show the desired result, it indicates that the configured ACL statement is not allowing the traffic from IP address 172.16.130.5 to router R1 for remote access via SSH.

Step 5

Verify that a pair of RSA keys is generated that allows the switch to support SSH and all remote terminal sessions to the device to take place over SSH. Also, verify that the domain name "example.com" and 768 bits in the modulus are configured.

Substep 1

Verify that a pair of RSA keys is generated that allows the switch to support SSH and vty lines to allow the remote access on SSH port instead of telnet.

```
SW1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAYQDbJgNFQuoArSM0jaTS5tcru6uDO3pZNki7VXnS2bL6
CloJxS5i8XbtabPGJtxOHEmuxtRbicL8PyqtL4o0qsqctrLwUDVALNVGWfxy45r2nh6ucTYCkqzHpobO
mhsXMEc=

SW1# show run | incl domain-name
ip domain-name example.com

SW1# show run | begin line
line con 0
 logging synchronous
 login local
line aux 0
line vty 0 4
 access-class 11 in
 login local
 transport input ssh
```

If the command output does not show the desired result, it indicates that the RSA keys are not generated and transport input protocol is not configured as SSH on the vty lines of the Branch router.

Command List

The table describes the commands that are used in the activity.Refer to the list if you need configuration command assistance during the lab activity.

Command	Description
line console 0	Changes the context to console configuration mode.
line vty *1st-vty 2nd-vty*	Changes the context to vty configuration mode for the range of vty lines listed in the command.
login	Console and vty configuration mode; tells Cisco IOS Software to prompt for a password.
login *local*	Console and vty configuration mode; tells Cisco IOS Software to prompt for a username and password, to be checked against locally configured **username** global configuration commands on this switch or router.
password *pass-value*	Console and vty configuration mode; lists the password that is required if the **login** command (with no other parameters) is configured.
username *name* **password** *pass-value*	Global command; defines one of possibly multiple usernames and associated passwords used for user authentication. It is used when the **login local** line configuration command has been used.
enable	A user in user mode can gain access to enable mode by using the **enable** command.
enable password *actual-password*	If the global configuration command **enable password** *actual-password* is used, it defines the password required when using the **enable** EXEC command.
enable secret *pass-value*	Global command; sets this switch password that is required for any user to reach enable mode
service password-encryption	The **service password-encryption** global configuration command directs the Cisco IOS Software to encrypt the passwords, CHAP secrets, and similar data that are saved in its configuration file.
ip domain-name *name*	Configure a DNS domain name with the **ip domain-name** *name* global configuration command.

Command	Description
crypto key generate rsa	Global command; creates and stores (in a hidden location in flash memory) the keys that are required by SSH.
transport input *{telnet | ssh}*	Used in vty line configuration mode; defines whether Telnet or SSH access, or both, is allowed into this switch. Both values can be configured on one command to allow both Telnet and SSH access (the default).
access-list *access-list-number* **{deny | permit} source** *[source-wildcard] [log]*	To define a standard IP access list, use the standard version of the access-list command in global configuration mode.
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list

Answer Key

Challenge 7: Securing Device Administrative Access

Task 1: Evaluation Lab Procedure

Activity

Step 1 Configure local authentication on console and virtual terminal (vty) lines.

Use enable password to log in to the device in order to address the issue faced with local authentication.

```
R1# show run | begin line
line con 0
 logging synchronous
line aux 0
line vty 0 4
 access-class 11 in
 no login
 transport input telnet
```

The output of the **show run** command shows that the local authentication is not enabled on console and vty lines.

Enable local authentication on the console and vty lines using the commands shown below.

```
R1(config)# line con 0
R1(config-line)# login local
R1(config-line)# line vty 0 4
R1(config-line)# login local
```

It is always good practice to reconfigure username, and correct password to make sure that your password is correct after enabling the local authentication for console and vty lines.

```
R1(config)# username admin password AdminIcnd123
```

Step 2 Verify that SSHv2 is enabled on router R1, and ACL is configured to allow the traffic from AdminPC. Also, verify that transport input protocol is configured as SSH.

Initiate an SSH session from AdminPC to IP address 172.16.160.1 that is configured on port 22, and verify the configurations on the router R1.

```
AdminPC# ssh -l admin 172.16.160.1
[Connection to 172.16.160.1 closed by foreign host]
```

Verify that SSHv2 is enabled and a pair of rsa key is generated on router R1.

```
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAYQDElDRvN8EftcrKYhAfuXOR7s4g8QeRa6ZDay1PjvUL
Rh76Qe6ENf702ZZOTmQfyK9lPqAIjDPlM+/OHtvw/2Fz9bNQxJ6WpKCnFNz/XJub5+I6zexNLZD511A0
rRcF6rE=
```

Examine the configuration for vty lines and verify that the ACL is configured to allow the traffic from AdminPC.

```
R1# show run | begin line
line con 0
 logging synchronous
 login local
line aux 0
line vty 0 4
 access-class 11 in
 login local
 transport input telnet
!

R1# show run | incl access-list
access-list 11 permit 172.16.130.5
R1# show access-lists
Standard IP access list 11
    10 permit 172.16.130.5 (3 matches)
```

The output of the show run command shows that even though the ACL permits the traffic from Admin PC (172.16.130.5) for line vty access on the router R1, the transport input protocol is configured for telnet protocol instead of SSH.

Configure transport input protocol as SSH for line vty 0 4 to allow SSH connection from AdminPC.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

Step 3 Verify the configuration and configure password encryption on switch SW1 and Branch router.

```
Branch# show run
Building configuration...
username admin password 0 AdminIcnd123
!
enable password Icnd1
!

SW1# show run
Building configuration...

enable password Icnd1
!
username admin password 0 AdminIcnd123
```

The output of the show run command shows that the enable password and local authentication password is not encrypted.

Use the commands shown below to enable password encryption on switch SW1 and Branch router.

```
SW1(config)# service password-encryption

Branch(config)# service password-encryption
```

Step 4 Verify that the ACL is configured to allow remote access on the Branch router.

Initiate an SSH session from AdminPC to IP address 172.16.160.3.

```
AdminPC# ssh -l admin 172.16.160.3
% Connection refused by remote host

Branch# show run | begin line
line con 0
 logging synchronous
 login local
line aux 0
line vty 0 4
 access-class 11 in
 login local
 transport input ssh
!

Branch# show access-lists
Standard IP access list 11
    10 deny   172.16.130.5 (1 match)
```

The output of the show access-lists command on Branch router shows that the ACL is configured to deny the traffic from IP address 172.16.130.5.

Correct the ACL statement to permit the traffic from IP address 172.16.130.5. You must remove the deny statement and permit the traffic from IP address 172.16.130.5 only.

```
Branch(config)# no access-list 11 deny 172.16.130.5 0.0.0.0
Branch(config)# access-list 11 permit 172.16.130.5 0.0.0.0
```

Step 5 Enable SSHv2 and generate a pair of RSA keys to allow the switch to support SSH, use domain name as example.com and 768 bits in the modulus.

```
SW1(config)# ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
SW1(config)# ip domain-name example.com
SW1(config)# crypto key generate rsa
The name for the keys will be: SW1.example.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

SW1(config)#
*Dec 20 19:56:52.530: %SSH-5-ENABLED: SSH 2.0 has been enabled
```

Also, configure vty lines to accept SSH session only.

```
SW1(config)# line vty 0 4
SW1(config-line)# transport input ssh
```

Lesson 2: Implementing Device Hardening

Challenge 8: Implementing Device Hardening

Introduction

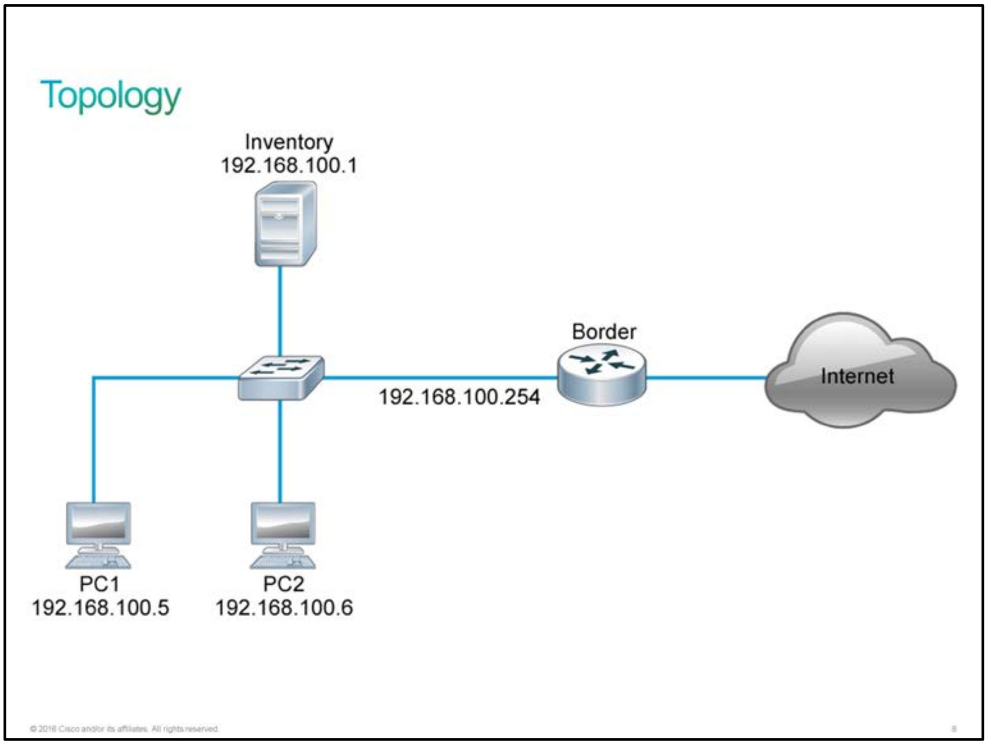
On a previous trip, you successfully added basic security to the law firm’s network, and Li has asked you to come back and add additional security. Bob tells you that you will need to perform the following tasks:

The tasks are:

- Enable the Border router as an NTP client of Internet router.
- Configure switch SW1 as follows:
  - Enable switch SW1 as an NTP client of Border router.
  - Secure all unused ports.
  - Configure dynamic (sticky) port security.
  - Disable Cisco Discovery Protocol (CDP) on the port connected to Inventory server.

Note Devices may take 60 to 240 seconds to get its clock synchronized with the NTP server or with its peers.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
SW1	Ethernet0/0	VLAN 1	Border	Ethernet0/0	192.168.100.254/24
SW1	Ethernet0/3	VLAN 1	Inventory	Ethernet0/0	192.168.100.1/24
SW1	Ethernet0/1	VLAN 1	PC1	Ethernet0/0	192.168.100.5/24
SW1	Ethernet0/2	VLAN 1	PC2	Ethernet0/0	192.168.100.6/24
SW1	VLAN 1	192.168.100.10/24	_	_	_
Inventory	Ethernet0/0	192.168.100.1/24	SW1	Ethernet0/3	VLAN 1
Border	Ethernet0/0	192.168.100.254/24	SW1	Ethernet0/0	VLAN 1

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
Border	Ethernet0/1	DHCP	Internet	Ethernet0/0	209.165.200.227/27
Internet	Loopback 0	209.165.204.1	_	_	_
Internet	Loopback 1	209.165.201.226	_	_	_
Internet	Loopback 2	209.165.202.226	_	_	_
Internet	Loopback 3	209.165.203.226	_	_	_

Task 1: Evaluation Lab Procedure

Activity

Step 1 Configure the Border router to synchronize its clock with the Internet router. Use the IP address 209.165.201.1.

Step 2 Configure the switch SW1 to synchronize its clock with the Border router. Use the IP address 192.168.100.254.

Step 3 Disable (shut down) all unused interfaces on the switch.

Step 4 Create a VLAN 99 that is named as "VLAN99", and assign all unused ports to VLAN 99.

Step 5 Configure port security on the switch SW1, on the port that is connected to the Inventory server to allow the MAC address of Inventory server only. If any other device is connected to this port, then the port must drop all the packets and increment the security-violation count.

Step 6 Configure port security on the switch SW1, on the port that is connected to PC1 to allow the MAC address of PC1 only. If any other device is connected to this port, then the port must drop all the packets, but must not increment the security-violation count.

Step 7 Configure port security on the switch SW1, on the port that is connected to PC2 to allow the MAC address of PC2 only. If any other device is connected to this port, then the port must drop all the packets, and place the port in an error-disabled state immediately.

Step 8 Disable Cisco CDP on the port that is connected to the Inventory server.

Verification

Step 1 Verify on the border router whether NTP updates are received from Internet router.

Substep 1

Use the **show ntp status** and **show ntp associations** commands on the Border router.

```
Border# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.201.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 5300 (1/100 of seconds), resolution is 4000
```

```
reference time is DA5A95DD.BDF3B850 (18:41:33.742 PST Mon Feb 1 2016)
clock offset is 0.0000 msec, root delay is 1.00 msec
root dispersion is 7943.03 msec, peer dispersion is 189.45 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 64, last update was 54 sec ago.

Border# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~209.165.201.1   .LOCL.           1     52     64     1  0.000   0.000 189.45
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Border#
```

If the command output does not show the desired result, it indicates that the NTP configuration is not configured correctly on the Border router.

Step 2 Verify that the NTP updates are received on the switch SW1 from the Border router.

Substep 1

Use the s**how ntp status** and s**how ntp associations** commands on the switch SW1 to verify the NTP status.

```
SW1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.100.254
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 9200 (1/100 of seconds), resolution is 4000
reference time is DA5A97D7.0B851ED8 (18:49:59.045 PST Mon Feb 1 2016)
clock offset is -0.5000 msec, root delay is 1.00 msec
root dispersion is 199.42 msec, peer dispersion is 189.44 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000000 s/s
system poll interval is 64, last update was 16 sec ago.

SW1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.168.100.254 209.165.201.1    2     20     64     1  1.000  -0.500 189.44
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
SW1#
```

It takes few minutes for switch SW1 to synchronize its clock with Border router.

If the command output does not show the desired result, it indicates that NTP configuration is not configured correctly on switch SW1.

Step 3 Verify that all unused interfaces on switch SW1 are placed in shutdown mode.

Substep 1

Use the **show ip interface brief** command to verify that all unused interfaces are placed in shutdown mode.

```
SW1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
```

```
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  administratively down down
Ethernet1/1            unassigned      YES unset  administratively down down
Ethernet1/2            unassigned      YES unset  administratively down down
Ethernet1/3            unassigned      YES unset  administratively down down
Vlan1                  192.168.100.10  YES NVRAM  up                    up
```

If the command output does not show the desired result, it indicates that the unused interfaces are not placed in shutdown mode.

Step 4

Verify that the VLAN that is named as "VLAN99" is created on switch SW1. Also, verify that all of the unused ports are assigned to VLAN 99.

Substep 1

Use the **show vlan brief** command to verify that the VLAN99 is created, and all of the unused ports are assigned to VLAN99.

```
SW1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
99   VLAN99                           active    Et1/0, Et1/1, Et1/2, Et1/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW1#
```

If the command output does not show the desired result, it indicates that the unused ports are not assigned to VLAN 99.

Step 5

Verify that the port security is enabled on switch SW1 for the port E0/3, which is connected to the Inventory server.

Substep 1

Use the **show port-security** and **show port-security interface** commands to verify that the port security is enabled on the port E0/3 of the switch SW1, which is connected to the Inventory server.

```
SW1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Et0/3              1            1                  0         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW1#

SW1# show port-security interface e0/3
Port Security              : Enabled
Port Status                : Secure-up
```

```
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : aabb.cc00.0400:1
Security Violation Count   : 0
```

If the command output does not show the desired output, it indicates that the port security is not enabled for the switch port e0/3 that is connected to the Inventory server.

Step 6 Verify that the port security is enabled on the port E0/1 of the switch SW1, which is connected to PC1.

Substep 1

Use the **show port-security** and **show port-security interface** commands to verify that the port security is enabled on the switch SW1 for the port E0/1 that is connected to PC1.

```
SW1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Et0/1              1            1                  0          Protect
      Et0/3              1            1                  0         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW1#
```

```
SW1# show port-security interface e0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : aabb.cc00.0200:1
Security Violation Count   : 0
```

If the command output does not show the desired result, it indicates that the port security is not enabled for the switch port E0/1 that is connected to PC1.

Step 7 Verify that the port security enabled for the port E0/2 on the switch SW1, which is connected to PC2.

Substep 1

Verify using **show port-security** command and show port-security interface command.

```
SW1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Et0/1              1            1                  0          Protect
      Et0/2              1            1                  0         Shutdown
      Et0/3              1            1                  0         Restrict
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW1#

SW1# show port-security interface e0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : aabb.cc00.0300:1
Security Violation Count   : 0
```

If the command output does not show the desired result, it indicates that the port security is not enabled for the port E0/2 that is connected to PC2.

Step 8 Verify that Cisco CDP is disabled on the port that is connected to the Inventory server.

Substep 1

Use the **show run int e0/3** and **show cdp neighbors** commands to verify that Cisco CDP is disabled on the port that is connected to the Inventory server. You must wait till the CDP holdtime expires, to check that the entry in the **show cdp neighbors** command output is removed.

```
SW1# show run int e0/3
Building configuration...

Current configuration : 306 bytes
!
interface Ethernet0/3
 description ***Connected to Inventory server***
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky aabb.cc00.0b00
 duplex auto
 no cdp enable


SW1# show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
```

```
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
PC2              Eth 0/2           139                    Linux Uni Eth 0/0
PC1              Eth 0/1           149                    Linux Uni Eth 0/0
Border           Eth 0/0           138               R    Linux Uni Eth 0/0
SW1#
```

If the command output does not show the desired result, it indicates that Cisco CDP is not enabled for the switch port E0/3 that is connected to the Inventory server.

Command List

The table describes the commands that are used in this activity. Refer to this list if you need configuration command assistance during the lab activity.

Command	Description
ntp server <*ip-address*>	Used in global configuration mode to allow the software clock to be synchronized by an NTP time server
ntp peer <*ip-address*>	Used in global configuration mode to configure the software clock to synchronize a peer or to be synchronized by a peer
interface *type number*	Used in global configuration mode to enter configuration mode for an interface
shutdown	Used in interface configuration mode to shut down the interface
vlan {*vlan-id* | *vlan-range*}	Used in global configuration mode to add a VLAN and enter configuration mode for the VLAN
name *name*	Used in VLAN configuration mode to name a VLAN
switchport access vlan *vlan-id*	Used in interface configuration mode to assign the interface to a VLAN
switchport port-security	Used in interface configuration mode to enable port security on the interface
switchport port-security maximum *maximum*	Used in interface configuration mode to set the maximum number of secure MAC addresses on the port
switchport port-security mac-address {*mac-addr* **| {sticky [***mac-addr***]}}**	Used in interface configuration mode to add a MAC address to the list of secure MAC addresses. The sticky option configures the MAC addresses as sticky on the interface.
switchport port-security violation {**shutdown** | **restrict** | **protect**}	Used in interface configuration mode to set the action to be taken when a security violation is detected

Answer Key

Challenge 8: Implementing Device Hardening

Task 1: Evaluation Lab Procedure

Activity

Step 1 Configure the Border router to receive NTP updates from Internet router.

Use following command on the border router to configure Internet router as NTP server.

```
Border(config)# ntp server 209.165.201.1
```

Step 2 Configure the switch SW1 to receive NTP updates from Border router.

Use following command to configure the switch SW1 and Border router as NTP clients.

```
SW1(config)# ntp server 192.168.100.254
```

Step 3 Disable all unused interfaces on the switch SW1.

Use the commands that are shown below to accomplish the task.

```
SW1(config)# int range e1/0 - 3
SW1(config-if-range)# shutdown
```

Step 4 Assign all unused ports to VLAN 99.

Use the commands that are shown below to accomplish the task.

```
SW1(config)# vlan 99
SW1(config-vlan)# name VLAN99

SW1(config)# int range e1/0 - 3
SW1(config-if-range)# switchport access vlan 99
```

Step 5 Configure port security to allow the MAC address of the Inventory server only. Ensure that all the packets are dropped and security-violation count is incremented, if any other device is connected to this port.

```
SW1(config)# int e0/3
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 1
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# switchport port-security violation restrict
```

Step 6 Configure port security to allow the MAC address of PC1 only. Ensure that all the packets are dropped and security-violation count is not incremented, if any other device is connected to this port.

```
SW1(config)# int e0/1
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 1
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# switchport port-security violation protect
```

Step 7 Configure port security to allow the MAC address of PC2 only. Ensure that all the packets are dropped and port is moved to error-disabled state, if another device is connected to this port.

```
SW1(config)# int e0/2
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 1
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# switchport port-security violation shutdown
```

Step 8 Disable Cisco CDP on the port E0/3 on switch SW1, which is connected to the Inventory server.

Use the commands that are shown below, to disable Cisco CDP on the port E0/1.

```
SW1(config)# int e0/3
SW1(config-if)# no cdp enable
```

Module 8: Implementing an EIGRP-Based Solution

Lesson 3: Troubleshooting EIGRP

Challenge 9: Troubleshooting EIGRP

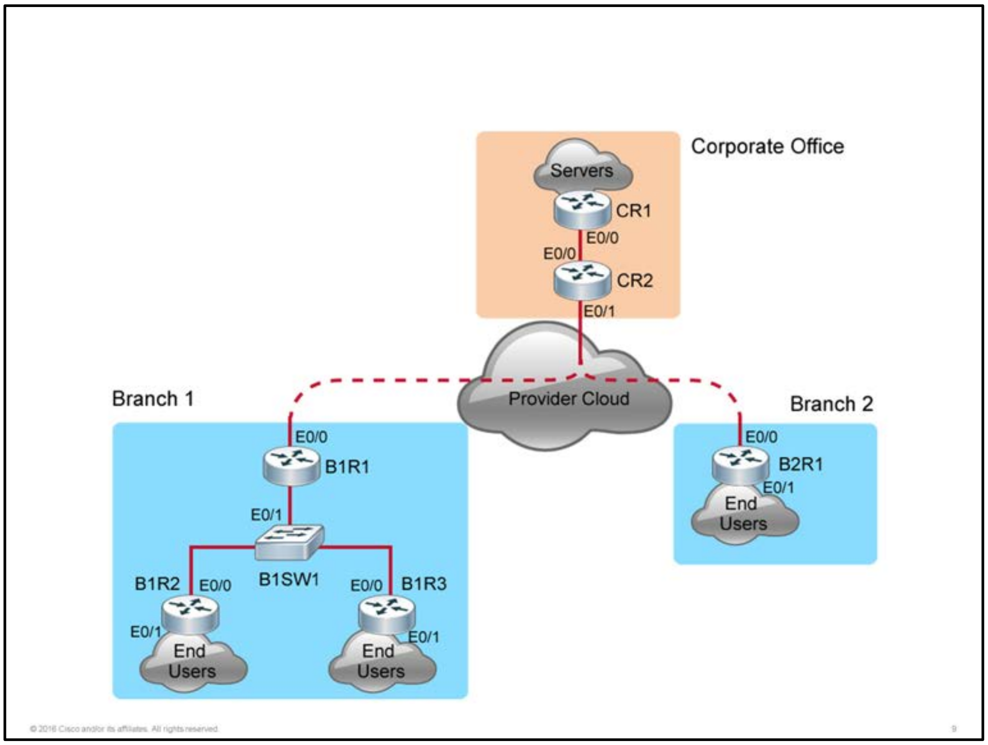
Introduction

Rahul, who is a network engineer at CCS has recently completed an EIGRP implementation for a new customer. Network connectivity verification has encountered some issues. You need to isolate and correct all issues before leaving the site.

Following are the issues that you need to resolve :

- A ping from CR1 to the loopback interface on B1R2 (192.168.1.2) fails.
- A ping from CR1 to the loopback interface on B2R1 (192.168.1.4) fails.
- There is no IPv6 connectivity between B1R3 and CR1. You should be able to ping 2001:0db8:a:c1::1/64 from B1R3.
- The end users have no IPv6 connectivity between B2R1 and B1R2. You should be able to ping 2001:DB8:A:B1::1 from B2R1.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information for IPv4 Addressing

Device	IP Address	Remote Device	Remote Device IP address
CR1 (Ethernet0/0)	172.16.0.1/30	CR2 (Ethernet0/0)	172.16.0.2/30
CR1 (Ethernet0/1)	172.16.10.1/24	Servers	_
CR1 (Loopback 0)	172.16.1.1/32	_	_
CR2 (Ethernet0/1)	_	Provider	
CR2 (Ethernet0/1.10)	172.16.0.5/30	B1R1 (Ethernet0/0) via Provider	172.16.0.6/30

Device	IP Address	Remote Device	Remote Device IP address
CR2 (Ethernet0/1.20)	172.16.0.9/30	B2R1 (Ethernet0/0) via Provider	172.16.0.10/30
CR2 (Loopback 0)	172.16.1.1/32	_	_
CR2 (Loopback 1)	172.16.0.11/32	_	_
B1R1 (Ethernet0/1)	_	B1SW1	_
B1R1 (Ethernet0/1.11)	192.168.1.13/30	B1R2 (Ethernet0/0) via B1SW1	192.168.1.14/30
B1R1 (Ethernet0/1.12)	192.168.1.17/30	B1R3 (Ethernet0/0) via B1SW1	192.168.1.18/30
B1R1 (Loopback 0)	192.168.1.1/32	_	_
B1R2 (Ethernet0/1)	192.168.1.33/27	End users	_
B1R2 (Loopback 0)	192.168.1.2/32	_	_
B1R3 (Ethernet0/1)	192.168.1.65/27	End users	_
B1R3 (Loopback 0)	192.168.1.3/32	_	_
B2R1 (Ethernet0/1)	192.168.1.97/27	End users	_
B2R1 (Loopback 0)	192.168.1.4/32	_	_

Device Information for IPv6 Addressing

Device	IPv6 Address	Device	Interface
CR1 (Ethernet0/0)	2001:0db8:a:c1c2::1/64	CR2 (Ethernet0/0)	2001:0db8:a:c1c2::2/64
CR1 (Ethernet0/1)	2001:0db8:a:c1::1/64	Servers	_
CR2 (Ethernet0/1.10)	2001:0db8:a:c2b1::2/64	B1R1 (Ethernet0/0)	2001:0db8:a:c2b1::1/64
CR2 (Ethernet0/1.20)	2001:0db8:a:c2b2::2/64	B2R1 (Ethernet0/0)	2001:0db8:a:c2b2::1/64
B1R1 (Ethernet0/1.11)	2001:0db8:a:b1b2::1/64	B1R2 (Ethernet0/0)	2001:0db8:a:b1b2::2/64
B1R1 (Ethernet0/1.12)	2001:0db8:a:b1b3::1/64	B1R3 (Ethernet0/0)	2001:0db8:a:b1b3::2/64
B1R2 (Ethernet0/1)	2001:0db8:a:b1::1/64	End User	_
B1R3 (Ethernet0/1)	2001:0db8:a:b2::1/64	End User	_
B2R1 (Ethernet0/1)	2001:0db8:a:b3::1/64	End User	_

Task 1: Troubleshooting EIGRP Lab Procedure

Activity

Step 1 Isolate and correct the issue that is related to the loss of connectivity between CR1 and B1R2 (192.168.1.2). Make sure that the EIGRP neighborship is not flapping on any device.

Step 2 Isolate and correct the issue that is related to the loss of connectivity between CR1 and B2R1 (192.168.1.4). Make sure that CR1 is learning about this network 192.168.1.4/32 from B2R1.

Step 3 Isolate and correct the issue that is related to the loss of IPv6 connectivity between B1R3 and CR1 (2001:0db8:a:c1::1). Make sure that the IPv6 EIGRP neighbors are formed in the Branch 1.

Step 4 Isolate and correct the issue that is related to the loss of IPv6 connectivity between B2R1 and B1R2 (2001:DB8:A:B1::1). Make sure that you fix the EIGRP neighbor relationship between B2R1 and CR2. Also on B1R2, advertise the network on Ethernet0/1 in EIGRP process 65010.

Verification

Step 1 Verify that the connectivity issue is resolved between CR1 and B1R2.

Substep 1

Use **ping** command to verify that the connectivity issue is resolved.

```
CR1# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Also, on CR1, verify that the EIGRP neighbor relationship is formed between CR1 and CR2.

```
CR1# show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(65010)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   172.16.0.2              Et0/0                    14 00:04:15    9   100  0  887
```

If you do not get the desired result, verify that EIGRP neighbor relationship is up on all routers connecting CR1 and B1R2.

Step 2 Verify that the connectivity issue has been resolved between CR1 and B2R1.

Substep 1

Use **ping** and **show ip route** command to verify that the connectivity issue is resolved.

```
CR1# ping 192.168.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Verify that CR1 has 192.168.1.4/32 in its routing table.

```
CR1# show ip route 192.168.1.4
Routing entry for 192.168.1.4/32
  Known via "eigrp 65010", distance 90, metric 435200, type internal
  Redistributing via eigrp 65010
  Last update from 172.16.0.2 on Ethernet0/0, 00:00:14 ago
  Routing Descriptor Blocks:
  * 172.16.0.2, from 172.16.0.2, 00:00:14 ago, via Ethernet0/0
      Route metric is 435200, traffic share count is 1
      Total delay is 7000 microseconds, minimum bandwidth is 10000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

If you do not get the desired result, verify that CR1 has 192.168.1.4/32 network in its routing table.

Step 3 Verify that the IPv6 connectivity has been resolved between CR1 and B1R3.

Substep 1

Use the following commands to verify that the connectivity issue is resolved.

```
B1R3# ping 2001:DB8:A:C1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:A:C1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
```

If you do not get the desired result, verify that the IPv6 EIGRP neighbor relationship is formed between B1R1 and B1R3.

Step 4 Verify that IPv6 connectivity between B1R2 and B2R1 is resolved.

Substep 1

Use **ping** command to verify that the connectivity issue is resolved.

```
B2R1# ping 2001:DB8:A:B1::1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:A:B1::1, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:A:B3::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

If you do not get the desired result, verify that the IPv6 EIGRP neighbor relationship is formed between CR2 and B2R1.

Command List

The table describes the commands that are used in this activity. Refer to this list if you need configuration command assistance during the lab activity.

Command	Description
show ip eigrp neighbor	Use this command to display the neighbors that are discovered by EIGRP.
show ipv6 eigrp neighbor	Use this command to display the neighbors that are discovered by IPv6 EIGRP.
show ip route	Use this command to display current state of routing table,
show ipv6 route	Use this command to display current state of IPv6 routing table,
show ip eigrp interfaces	Use this command to display information about interfaces that are configured for EIGRP.
show ip interface brief	Use this command to display the interface status and IP address.
show ipv6 interface brief	Use this command to display the interface status and IPv6 address.
show access-lists	Use this command to display all IPv4 access control lists (ACLs) or a specific IPv4 ACL
network *network-number [network-mask]*	Configures a list of networks for the EIGRP. Use this command in router configuration mode.
passive interface [default] *interface*	Suppresses EIGRP hello packets and routing updates on specified interfaces (or on all interfaces, when the default option is used). Use this command in router configuration mode
ipv6 eigrp *as-number*	Enables IPv6 EIGRP process on the interface.

Answer Key

Challenge 9: Troubleshooting EIGRP

Task 1: Troubleshooting EIGRP Lab Procedure

Activity

Step 1 To resolve the connectivity issue between CR1 and B1R2, you need to fix the neighbor relationship between CR1 and CR2.

Look at the EIGRP neighbor table on CR1 . Here is the output of that table:

```
CR1# show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(65010)
```

The EIGRP neighbor is flapping between CR1 and CR2.

Now, check the interface Ethernet0/0 configuration on CR1.

```
CR1# show run interface ethernet 0/0
Building configuration...

Current configuration : 185 bytes
!
interface Ethernet0/0
 description link  to CR2
 ip address 172.16.0.1 255.255.255.252
 ip access-group 101 in
 ipv6 address 2001:DB8:A:C1C2::1/64
 ipv6 enable
 ipv6 eigrp 65010
end
```

There is an access-list 101 configured on interface Ethernet0/0. Check the access-list configuration.

```
CR1# show access-list 101
Extended IP access list 101
    10 deny eigrp any any (29801 matches)
    20 permit ip any any
```

The access-list is denying EIGRP packets.

NOTE: The match count in the access-list line 10 may differ in your output.

Remove the access-list from the interface.

```
CR1(config)# interface ethernet 0/0
CR1(config-if)# no ip access-group 101 in
CR1(config-if)#
*Sep 11 05:07:45.643: %DUAL-5-NBRCHANGE: EIGRP-IPv4 65010: Neighbor 172.16.0.2
(Ethernet0/0) is up: new adjacency
```

The neighbor relationship comes up between CR1 and CR2 and you can now ping 192.168.1.2 on B1R2.

Step 2 To resolve the connectivity issue between CR1 and B2R1, you need to make sure that CR1 has IP address 192.168.1.4 in its routing table.

Check the routing table on CR1.

```
CR1# show ip route 192.168.1.4
% Network not in table
```

The route does not exist on CR1. Next, check the EIGRP configuration of B2R1.

```
B2R1# show run | begin router eigrp
router eigrp 65010
 network 172.16.0.10 0.0.0.0
 network 192.168.1.97 0.0.0.0
 eigrp router-id 192.168.1.4
```

The interface, loopback 0 IP address is not being advertised in EIGRP. Advertise this network in EIGRP.

```
B2R1(config)# router eigrp 65010
B2R1(config-router)# network 192.168.1.4 0.0.0.0
```

Also, check the interface status of loopback 0.

```
B2R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                172.16.0.10     YES NVRAM  up                    up
Ethernet0/1                192.168.1.97    YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Loopback0                  192.168.1.4     YES NVRAM  administratively down down
B2R1#
```

The interface, loopback 0 has been shut down. You need to enable this interface.

```
B2R1(config)# interface loopback 0
B2R1(config-if)# no shutdown
*Sep 11 07:45:36.107: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Sep 11 07:45:37.113: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to up
```

Now, you will see the network, 192.68.1.4/32 in the routing table of CR1.

Step 3 To resolve the IPv6 connectivity issue between B1R3 and CR1 , you need to fix the neighbor relationship between B1R1 and B1R3.

Check the EIGRP neighbor table on B1R3 . Here is the output of that table:

```
B1R3# show ipv6 eigrp neighbor
EIGRP-IPv6 Neighbors for AS(65010)
```

B1R3 is not forming IPv6 neighbor relationship with B1R1.

Now, look at the IPv6 EIGRP configuration on B1R1

```
B1R1# show run | section  ipv6 router eigrp
ipv6 router eigrp 65010
 passive-interface default
 no passive-interface Ethernet0/1.11
 no passive-interface Ethernet0/0
 eigrp router-id 192.168.1.1
B1R1#
```

Notice that the interface Ethernet0/1.12 is passive. This setting will prevent an EIGRP neighbor relationship from being formed on that interface. In the EIGRP configuration, the interface Ethernet0/1.12 needs to be set to not be passive. Here is an example of the configuration:

```
B1R1(config)# ipv6 router eigrp 65010
B1R1(config-rtr)# no passive-interface ethernet0/1.12
B1R1(config-rtr)#
*Sep 11 05:18:54.473: %DUAL-5-NBRCHANGE: EIGRP-IPv6 65010: Neighbor 
FE80::A8BB:CCFF:FE00:1400 (Ethernet0/1.12) is up: new adjacency
B1R1(config-rtr)#
```

```
B1R3# show ipv6 eigrp neighbor
EIGRP-IPv6 Neighbors for AS(65010)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   Link-local address:     Et0/0                    12 00:02:32    1   100  0  45
    FE80::A8BB:CCFF:FE00:1210
B1R3#
```

NOTE: Link local IPv6 address may be different in the output above.

The IPv6 EIGRP neighbor relationship is formed between B1R1 and B1R3. This will resolve the IPv6 connectivity between CR1 and B1R3.

Step 4 To resolve the connectivity issue between B1R2 and B2R1 , you need to fix the neighbor relationship between B2R1 and CR2. Also on B1R2, advertise the network on E0/1 in EIGRP process 65010.

Look at the IPv6 EIGRP neighbor table on B2R1 . Here is the output of that table:

```
B2R1# show ipv6 eigrp neighbor
EIGRP-IPv6 Neighbors for AS(65010)
```

Notice that the IPv6 EIGRP neighbor relationship is not formed between CR2 and B2R1.

On CR2, look at the interface configuration of E0/1.20 which is connected to B2R1.

```
CR2# show run interface ethernet 0/1.20
Building configuration...

Current configuration : 175 bytes
!
interface Ethernet0/1.20
 description link to B2R1
 encapsulation dot1Q 20
 ip address 172.16.0.9 255.255.255.252
 ipv6 address 2001:DB8:A:C2B2::2/64
 ipv6 eigrp 65011
end
```

You will notice that the EIGRP AS number is not configured correctly.

Configure the interface E0/1.20 with the correct EIGRP AS number to form neighbor relationship with B2R1.

```
CR2(config)# interface Ethernet0/1.20
CR2(config-subif)# no ipv6 eigrp 65011
CR2(config-subif)# ipv6 eigrp 65010
CR2(config-subif)#
*Sep 11 05:39:22.209: %DUAL-5-NBRCHANGE: EIGRP-IPv6 65010: Neighbor
FE80::A8BB:CCFF:FE00:1600 (Ethernet0/1.20) is up: new adjacency
```

```
B2R1# show ipv6 eigrp neighbor
EIGRP-IPv6 Neighbors for AS(65010)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   Link-local address:     Et0/0                    11 00:21:57    6   100  0  55
    FE80::A8BB:CCFF:FE00:1810
```

NOTE: Link local IPv6 address may be different in the output above.

The end users are connected to interface, Ethernet0/1 on B1R2 and B2R1. On B1R2, the interface Ethernet0/1 is not enabled for EIGRP IPv6 routing.

```
B1R2# show run interface Ethernet0/1
Building configuration...
Current configuration : 135 bytes
!
interface Ethernet0/1
 description link to end users
 ip address 192.168.1.33 255.255.255.224
 ipv6 address 2001:DB8:A:B1::1/64
end
```

Enable IPv6 EIGRP for AS 65010 on interface Ethernet0/1 on B1R2

```
B1R2(config)# interface Ethernet0/1
B1R2(config-if)# ipv6 eigrp 65010
```

Now, there should be IPv6 connectivity between end users on B1R2 and B2R1.

Module 9: Summary Challenge

Lesson 1: Troubleshooting a Medium-Sized Network

Challenge 10: Summary Challenge Lab: 3

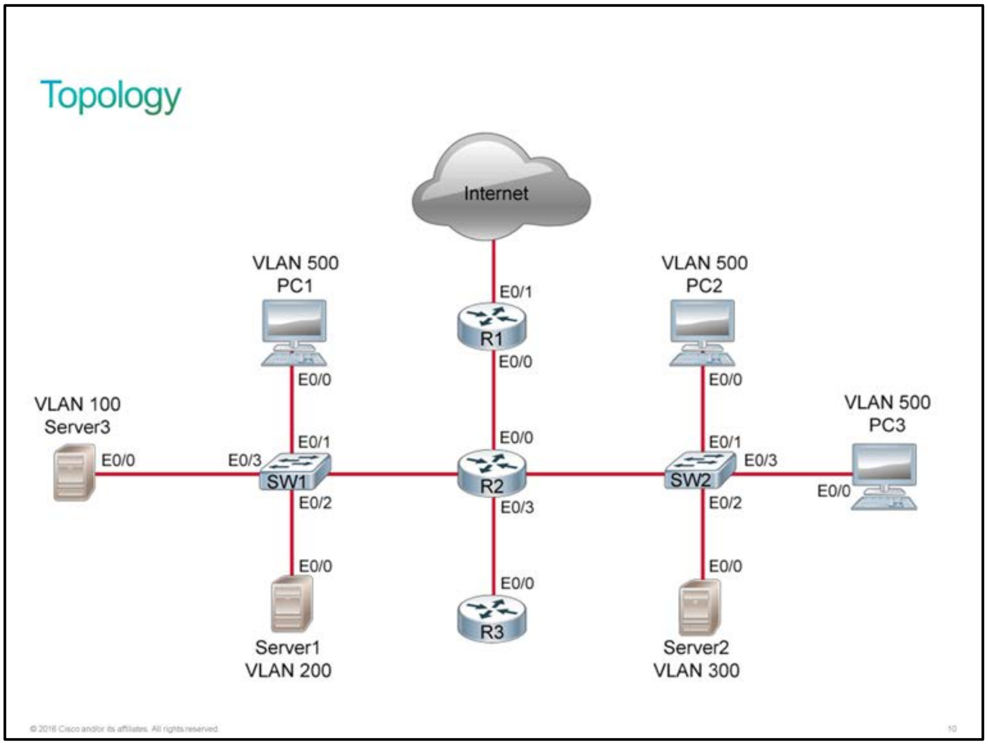
Scenario

CCS has been contracted by a trading company. As per the contract, the engineer has configured the network, but the customer has reported issues related to the connectivity. You must identify and fix the issues.

The network implementation details that are provided by the customer are given below.

- The PCs and servers are configured in their respective VLANs and default gateway for the VLANs is configured on router R2 using the "router on a stick" method.
- Router R1 connects to Internet, and the PAT is enabled on router R1.
- Routing protocol RIPv2 is enabled between routers R1, R2, and R3.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
R1	Ethernet0/0	10.16.140.1/30	R2	Ethernet0/0	10.16.140.2/30
R1	Ethernet0/1	209.165.200.226/27	Internet	Ethernet0/0	209.165.200.227/27
R1	Loopback 0	10.16.1.1/32	_	_	_
R2	Ethernet0/0	10.16.140.2/30	R1	Ethernet0/0	10.16.140.1/30
R2	Ethernet0/1.1	10.16.132.1	SW2	Ethernet0/0	Trunk
R2	Ethernet0/2.10	10.16.10.1/24	SW1	Ethernet0/0	Trunk
R2	Ethernet0/2.20	10.16.20.1/24	SW1	Ethernet0/0	Trunk

Device	Interface	IPv4 Address	Remote	Interface	IPv4 Address
R2	Ethernet0/2.1	10.16.131.1/24	SW1	Ethernet0/0	Trunk
R2	Ethernet0/2.10	10.16.10.1/24	SW1	Ethernet0/0	Trunk
R2	Ethernet0/2.20	10.16.20.1/24	SW1	Ethernet0/0	Trunk
R2	Ethernet0/2.40	10.16.40.1/24	SW1	Ethernet0/0	Trunk
R2	Ethernet0/3	10.16.12.1/30	R3	Ethernet0/0	10.16.12.2/30
R3	Ethernet0/0	10.16.12.2/30	R2	Ethernet0/3	10.16.12.1/30
R3	Loopback0	10.16.2.2/32	_	_	_
SW1	Ethernet0/0	Trunk	R2	Ethernet0/2.40	10.16.40.1/24
SW1	Ethernet0/0	Trunk	R2	Ethernet0/2.10	10.16.10.1/24
SW1	Ethernet0/0	Trunk	R2	Ethernet0/2.20	10.16.20.1/24
SW1	Ethernet0/1	VLAN 400	PC1	Ethernet0/0	10.16.40.2/24
SW1	Ethernet0/2	VLAN 200	Server1	Ethernet0/0	10.16.20.2/24
SW1	Ethernet0/3	VLAN 100	Server3	Ethernet0/0	10.16.10.2/24
SW2	Ethernet0/0	Trunk	R2	Ethernet0/1.30	10.16.30.1/24
SW2	Ethernet0/0	Trunk	R2	Ethernet0/1.50	10.16.50.1/24
SW2	Ethernet0/1	VLAN 500	PC2	Ethernet0/0	10.16.50.2/24
SW2	Ethernet0/2	VLAN 300	Server2	Ethernet0/0	10.16.30.2/24
SW2	Ethernet0/3	VLAN 500	PC3	Ethernet0/0	10.16.50.3/24
Internet	Ethernet0/0	209.165.200.227/27	R1	Ethernet0/1	209.165.200.226/27
Internet	Loopback0	209.165.201.1/32	_	_	_
PC1	Ethernet0/0	10.16.40.2/24	SW1	Ethernet0/1	VLAN 400
PC2	Ethernet0/0	10.16.50.2/24	SW2	Ethernet0/1	VLAN 500
PC3	Ethernet0/0	10.16.50.3/24	SW2	Ethernet0/3	VLAN 500
Server1	Ethernet0/0	10.16.20.2/24	SW1	Ethernet0/2	VLAN 200
Server2	Ethernet0/0	10.16.30.2/24	SW2	Ethernet0/2	VLAN 300
Server3	Ethernet0/0	10.16.10.2/24	SW1	Ethernet0/3	VLAN 100

Task 1: Evaluation Lab Procedure

Activity

Step 1 Server2 is unable to communicate with rest of the network, ping to its default gateway fails. Identify and fix the issue.

Step 2 Examine routing table on router R3. Router R3 does not send and receive RIPv2 routing updates. Identify and fix the issue. Note: You must use /8 network in the network statement and disable autosummarization.

Step 3 Server1 is unable to communicate with rest of the network, ping to its default gateway fails. Isolate and fix the issue.

Verification

Step 1 Issue a ping command from Server 1 to the default gateway address and Internet IP address, to verify that the ping responses to default gateway address and Internet IP address 209.165.201.1, are successful.

Substep 1

Verify the ping responses to IP addresses, 10.16.30.1 and 209.165.201.1.

```
Server2# ping 10.16.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.16.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1008 ms

Server2# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Server2#
```

If the command output does not show the desired result, it indicates that the IP address on the subinterface E0/1.30 is not configured correctly, on router R2.

Step 2 Verify that RIPv2 configured with the correct network statement. Also, verify that the RIPv2 routes from the routers R1 and R2 are updated in the routing table on router R3.

Substep 1

Verify using **show run**, **show ip route and show ip rip database** commands.

```
R3# show run | sec rip
router rip
 version 2
 network 10.0.0.0
 no auto-summary
```

```
R3#

R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.16.12.1 to network 0.0.0.0

R*    0.0.0.0/0 [120/2] via 10.16.12.1, 00:00:00, Ethernet0/0
      10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
R        10.16.1.1/32 [120/2] via 10.16.12.1, 00:00:00, Ethernet0/0
C        10.16.2.2/32 is directly connected, Loopback0
R        10.16.10.0/24 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
C        10.16.12.0/30 is directly connected, Ethernet0/0
L        10.16.12.2/32 is directly connected, Ethernet0/0
R        10.16.20.0/24 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
R        10.16.30.0/24 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
R        10.16.40.0/24 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
R        10.16.50.0/24 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
R        10.16.131.0/24 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
R        10.16.132.0/24 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
R        10.16.140.0/30 [120/1] via 10.16.12.1, 00:00:00, Ethernet0/0
R3# show ip rip database
0.0.0.0/0    auto-summary
0.0.0.0/0
    [2] via 10.16.12.1, 00:00:05, Ethernet0/0
10.0.0.0/8    auto-summary
10.16.1.1/32
    [2] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.2.2/32    directly connected, Loopback0
10.16.10.0/24
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.12.0/30    directly connected, Ethernet0/0
10.16.20.0/24
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.30.0/24
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.40.0/24
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.50.0/24
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.131.0/24
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.132.0/24
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
10.16.140.0/30
    [1] via 10.16.12.1, 00:00:05, Ethernet0/0
```

If the command output does not show the desired result, it indicates that RIPv2 is not configured correctly, on router R3.

Step 3 Issue a ping command from Server1 to the default gateway address and Internet IP address 209.165.201.1, to verify that the ping responses are successful.

Substep 1

Verify the ping responses to IP addresses,10.16.20.1 and 209.165.201.1. (Note: You need wait for ping responses.)

```
Server1# ping 10.16.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.16.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms
Server1# ping 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Server1#
```

If the command output does not show the desired result, it indicates that the switch port that is connected to Server 1 is configured in the wrong VLAN.

Answer Key

Challenge 10: Summary Challenge Lab: 3

Task 1: Evaluation Lab Procedure

Activity

Step 1 Verify that the VLAN configuration, trunk on SW2, and IP address that is configured on the corresponding subinterface on router R2, are correct as per the information given in the Job aid section.

Use the **show vlan brief** and **show interface trunk** commands on switch SW1, and the show ip interface brief command on router R2 to verify the configuration details.

```
SW2#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,300,400,500

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,300,400,500
SW2#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
300  VLAN300                          active    Et0/2
400  VLAN500                          active
500  VLAN0500                         active    Et0/1, Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW2#
```

```
R2#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.16.140.2     YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
Ethernet0/1.1              10.16.132.1     YES NVRAM  up                    up
Ethernet0/1.30             10.16.230.5     YES manual up                    up
Ethernet0/1.50             10.16.50.1      YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  up                    up
Ethernet0/2.1              10.16.131.1     YES NVRAM  up                    up
Ethernet0/2.10             10.16.10.1      YES NVRAM  up                    up
Ethernet0/2.20             10.16.20.1      YES NVRAM  up                    up
Ethernet0/2.40             10.16.40.1      YES NVRAM  up                    up
Ethernet0/3                10.16.12.1      YES NVRAM  up                    up
R2#
```

The output of the **show ip interface brief** command shows that, the IP address that is configured on the subinterface E0/1.30 on router R2 is 10.16.230.5 instead of 10.16.30.1, which is mentioned in the Job aid section.

Use the commands that are shown below to configure the correct IP address.

```
R2(config)#  int e0/1.30
R2(config-subif)# no ip add
R2(config-subif)# ip add 10.16.30.1 255.255.255.0
R2(config-subif)#
```

Step 2 Verify the configuration on router R3 to ensure that the RIPv2 is configured with autosummarization disabled.

Use the **show ip protocols** and **show ip route** commands to verify the configuration.

```
R3#show ip protocols
*** IP Routing is NSF aware ***

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.16.2.2/32 is directly connected, Loopback0
C        10.16.12.0/30 is directly connected, Ethernet0/0
L        10.16.12.2/32 is directly connected, Ethernet0/0
R3#
```

Observe that RIPv2 is not configured on R3. Use the commands that are shown below to configure RIPv2.

```
R3(config)# router rip
R3(config-router)# version 2
R3(config-router)# no auto
R3(config-router)# network 10.0.0.0
```

Step 3 Verify that the VLAN configuration, trunk on switch SW1, and IP address that is configured on the corresponding subinterface on R2, are correct as per information given in the Job aid section.

Use the **show vlan brief** and **show interface trunk** commands on switch SW1, and the show ip interface brief command on router R2 to verify the configuration.

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
100  VLAN100                          active    Et0/2, Et0/3
200  VLAN200                          active
400  VLAN400                          active    Et0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW1#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,100,200,400

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,100,200,400
SW1#

R2#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                10.16.140.2     YES NVRAM  up                    up
Ethernet0/1                unassigned      YES NVRAM  up                    up
Ethernet0/1.1              10.16.132.1     YES NVRAM  up                    up
Ethernet0/1.30             10.16.30.1      YES manual up                    up
Ethernet0/1.50             10.16.50.1      YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  up                    up
Ethernet0/2.1              10.16.131.1     YES NVRAM  up                    up
Ethernet0/2.10             10.16.10.1      YES NVRAM  up                    up
Ethernet0/2.20             10.16.20.1      YES NVRAM  up                    up
Ethernet0/2.40             10.16.40.1      YES NVRAM  up                    up
Ethernet0/3                10.16.12.1      YES NVRAM  up                    up
R2#
```

Verify that the VLAN configuration, trunk on switch SW1, and IP address that is configured on the corresponding subinterface on R2, are correct as per information given in the Job aid section.

```
SW1(config)# int e0/2
SW1(config-if)# switchport access vlan 200
```

The output of the commands that are shown above shows that instead of VLAN 200, VLAN 100 is assigned to the port E0/2. Use the commands that are shown below on switch SW1, to configure correct VLAN assignment for the port E0/2.

Lesson 2: Troubleshooting Scalable Medium-Sized Network

Challenge 11: Summary Challenge Lab: 4

Scenario

You work for DENTIC Networking. Your colleague, Andy did some maintenance on the network over the weekend. On Monday morning, he is seeing certain issues in the network and needs your help in troubleshooting it.

He gives you the following information about the network :

- Routers R1, R2, R3, and R4 are enabled for EIGRP routing with AS number 1023.
- R4 has been configured to get the IP address dynamically from the ISP. R4 also has NAT configured.
- Please refer to the topology for the VLAN information. R1 is the DHCP server for VLAN10 (PC1) and VLAN 20 (PC2).

Following are the issues that you need to resolve :

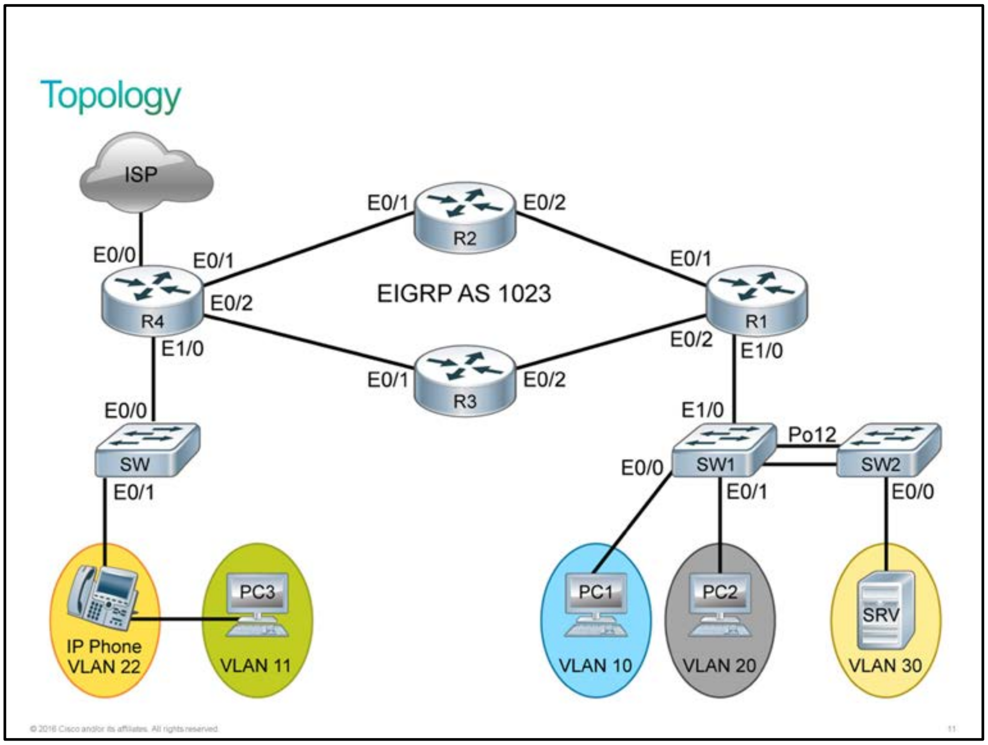
- PC1 cannot access internet. To test internet connectivity, use IP address 209.165.201.225.
- R4 should be load balancing the networks advertised by R1. The routing table for the following networks should look like:

```
R4#show ip route eigrp
<output omitted>

D     192.168.1.0/24 [90/332800] via 172.16.2.5, 00:00:24, Ethernet0/2
                     [90/332800] via 172.16.1.5, 00:00:24, Ethernet0/1
D     192.168.10.0/24 [90/332800] via 172.16.2.5, 00:00:24, Ethernet0/2
                      [90/332800] via 172.16.1.5, 00:00:24, Ethernet0/1
D     192.168.20.0/24 [90/332800] via 172.16.2.5, 00:00:24, Ethernet0/2
                      [90/332800] via 172.16.1.5, 00:00:24, Ethernet0/1
D     192.168.30.0/24 [90/337920] via 172.16.2.5, 00:00:24, Ethernet0/2
                      [90/337920] via 172.16.1.5, 00:00:24, Ethernet0/1
```

- Server SRV cannot reach PC3 (192.168.11.11).
- R2 is not forming IPv6 EIGRP neighbor with R1. Also, the neighborship with R4 on interface Ethernet0/1 on R2 is continuously flapping.

Topology



Job Aid

Note	If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

IPv4 Addressing

Device	**IP Address**	**Remote Device**	**IP Address**
R1 (Ethernet0/1)	172.16.1.1	R2 (Ethernet0/2)	172.16.1.2
R1 (Ethernet0/2)	172.16.2.1	R3 (Ethernet0/2)	172.16.2.2
R2 (Ethernet0/1)	172.16.1.5	R4 (Ethernet0/1)	172.16.1.6
R3 (Ethernet0/1)	172.16.2.5	R4 (Ethernet0/2)	172.16.2.6
R1 (Ethernet1/0.1)	192.168.1.1/24	SW1	_
R1 (Ethernet1/0.10)	192.168.10.1/24	SW1	_

Device	IP Address	Remote Device	IP Address
R1 (Ethernet1/0.20)	192.168.20.1/24	SW1	_
R1 (Ethernet1/0.30)	192.168.30.1/24	SW1	_
R4 (Ethernet1/0.1)	192.168.4.1/24	_	_
R4 (Ethernet1/0.11)	192.168.11.1/24	_	_
R4 (Ethernet1/0.22)	192.168.22.1/24	_	_
SW (VLAN 1)	192.168.4.2/24	_	_
PC3	192.168.11.11	_	_
SRV	192.168.30.33	_	_

IPv6 Addressing

Device	IPv6 Address	Remote Device	IPv6 Address
R1 (Ethernet0/1)	2001:DB8:A:B1B2::1/64	R2 (Ethernet0/2)	2001:DB8:A:B1B2::2/64
R1(Ethernet0/2)	2001:DB8:A:B1C2::1/64	R3 (Ethernet0/2)	2001:DB8:A:B1C2::2/64
R4 (Ethernet0/1)	2001:DB8:A:C1B2::1/64	R2 (Ethernet0/1)	2001:DB8:A:C1B2::2/64
R4 (Ethernet0/2)	2001:DB8:A:C1C2::1/64	R3 (Ethernet0/1)	2001:DB8:A:C1C2::2/64

VLAN Information

Device	VLAN Information
PC1	VLAN10
PC2	VLAN20
SRV	VLAN30
PC3	VLAN11
IP Phone	VLAN22

Task 1: Summary Challenge Lab Procedure

Activity

Step 1 Isolate and resolve the connectivity issue between PC1 and ISP (209.165.201.225). Make sure PC1 is getting IP address from DHCP server on R1.

Step 2 Isolate and resolve the EIGRP routing issue to enable load balancing of routes on R4. Check the EIGRP configuration on R4.

Step 3 Isolate and resolve the connectivity issue between PC3 (192.168.11.11) and SRV(192.168.30.33). Make sure that the networks are advertised in EIGRP. Also, check the configuration on the switches.

Step 4 Isolate and resolve the IPv6 EIGRP neighbor issue on R2.

Verification

Step 1 Verify that PC1 can reach internet.

Substep 1

From PC1, use **ping** command to verify that the connectivity issue is resolved.

```
PC1# ping 209.165.201.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1006 ms
PC1#
```

If you do not get the desired result, check the configuration on R1 and R4.

Step 2 Verify that all routes advertised by R1 are load balanced on R4.

Substep 1

Use **show ip route eigrp** command on R4 to verify that routes are load balanced.

```
R4# show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
D        172.16.1.0/30 [90/307200] via 172.16.1.5, 00:00:06, Ethernet0/1
```

```
D        172.16.2.0/30 [90/307200] via 172.16.2.5, 00:00:06, Ethernet0/2
D     192.168.1.0/24 [90/332800] via 172.16.2.5, 00:00:06, Ethernet0/2
                     [90/332800] via 172.16.1.5, 00:00:06, Ethernet0/1
D     192.168.10.0/24 [90/332800] via 172.16.2.5, 00:00:06, Ethernet0/2
                      [90/332800] via 172.16.1.5, 00:00:06, Ethernet0/1
D     192.168.20.0/24 [90/332800] via 172.16.2.5, 00:00:06, Ethernet0/2
                      [90/332800] via 172.16.1.5, 00:00:06, Ethernet0/1
D     192.168.30.0/24 [90/337920] via 172.16.2.5, 00:00:06, Ethernet0/2
                      [90/337920] via 172.16.1.5, 00:00:06, Ethernet0/1
R4#
```

If you do not get the desired result, check the EIGRP topology table on R4.

Step 3 Verify that SRV can reach PC3.

Substep 1

From SRV, use **ping** command to verify that the connectivity issue is resolved.

```
SRV# ping 192.168.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
SRV#
```

If you do not get the desired result, check the configuration on the switches.

Step 4 Verify that R2 has formed IPv6 EIGRP neighborship with R1 and R4.

Substep 1

Use the **show ipv6 eigrp neighbor** command to verify your configuration changes.

```
R2# show ipv6 eigrp neighbor
EIGRP-IPv6 Neighbors for AS(1023)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   Link-local address:     Et0/2                    13 00:00:32    6   100  0  14
    FE80::A8BB:CCFF:FE00:110
0   Link-local address:     Et0/1                    12 00:03:00    6   100  0  27
    FE80::A8BB:CCFF:FE00:410
R2#
```

If you do not get the desired result, check the IPv6 EIGRP configuration.

Answer Key

Challenge 11: Summary Challenge Lab: 4

Task 1: Summary Challenge Lab Procedure

Activity

Step 1 Troubleshoot the connectivity issue by tracing the path between PC1 and ISP gateway.

PC1 is not getting an IP address from R1 which is the DHCP server. On R1, the interface Ethernet0/1.10 has not been configured correctly. Configure the interface with VLAN ID as 10 and assign the IP address.

```
R1(config)# interface  Ethernet1/0.10
R1(config-subif)# no encapsulation dot1Q 12
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
```

You may have to reset the interface on PC1 to ensure that DHCP occurs with revised information.

```
PC1(config)# interface e0/0
PC1(config-if)# shutdown
PC1(config-if)# no shutdown
```

Now, you should be able to reach internet from PC1.

Step 2 Troubleshoot EIGRP routing to make sure that routes advertised by R1 are load balanced on R4.

On R4,check the EIGRP router configuration. You will see that EIGRP has been configured with **maximum path 1** command. Hence, it is not load balancing the networks.

```
R4(config)# router eigrp 1023
R4(config-router)# no  maximum-paths 1
```

Once you remove this command, you will see that the networks are being load balanced. By default, Cisco router supports up to 16 paths.

Step 3 Troubleshoot the connectivity issue by tracing the path between PC3 and Server SRV.

PC3 is in VLAN 11. The switch SW has interface Ethernet0/0 that is configured as trunk. This port only allows VLAN 1 and VLAN 22.

```
SW# show run interface ethernet0/0
Building configuration...

Current configuration : 145 bytes
!
interface Ethernet0/0
  switchport trunk allowed vlan 1,22
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

You need to allow VLAN 11 on this port.

```
SW(config)# interface ethern0/0
SW(config-if)# switchport trunk allowed vlan add 11
```

Now, you should be able to reach PC3 from SRV.

Step 4 Troubleshoot the IPv6 EIGRP neighbor issue.

On R1, the IPv6 EIGRP process has been shut down. You need to undo it so that EIGRP neighbor is formed.

```
R1(config)# ipv6 router eigrp 1023
R1(config-rtr)# no shutdown
```

On R4, there is an access-list applied on the interface Ethernet0/1. It is denying the IPv6 EIGRP multicast address FF02::A. You need to remove this access-list or allow this address for EIGRP neighbor to be formed.

```
R4(config)# interface e0/1
R4(config-if)# no ipv6 traffic-filter FILTER in
```

Module 10: Implementing a Scalable OSPF-Based Solution

Lesson 4: Troubleshooting Multiarea OSPF

Challenge 12: Troubleshooting OSPF

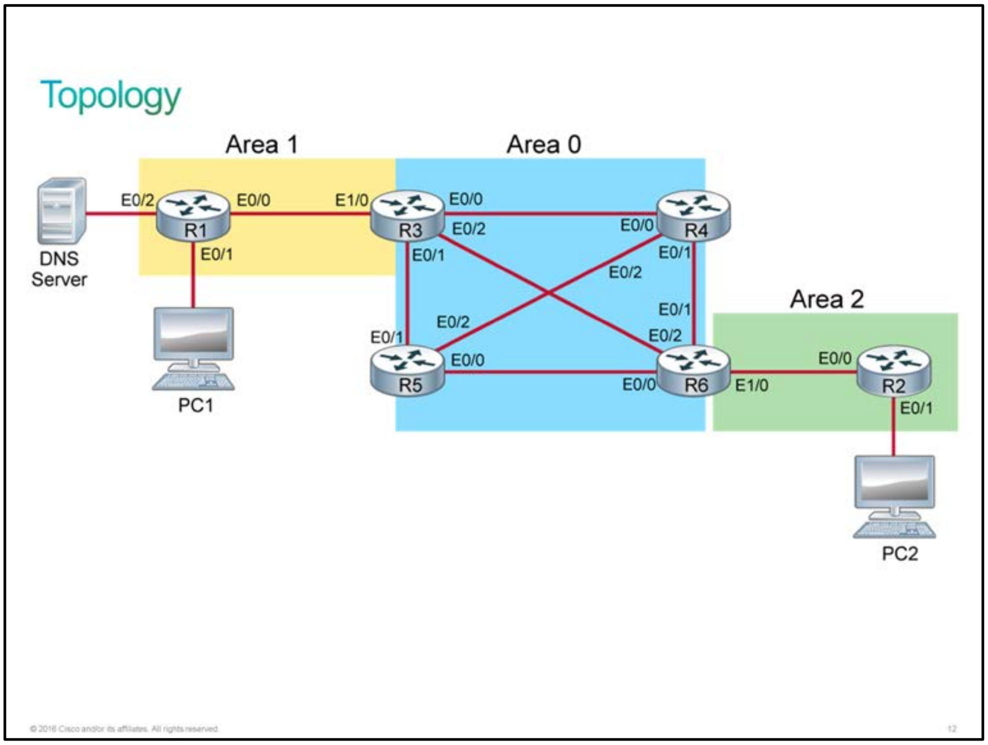
Introduction

Susan who is a network engineer at GCE has recently completed an OSPF implementation for a new customer. All routers are running OSPF as shown in the diagram. Network connectivity verification has encountered some issues. You need to isolate and correct all issues before leaving the site.

Following are the issues that you need to resolve:

- PC1 cannot ping PC2 (192.168.20.2).
- PC2 cannot ping the IP address 192.168.33.1 (R1 E0/2). There will be a DNS server added to network subnet 192.168.33.0/24.You need to make sure that PC2 can reach this network.
- In future, GCE will be enabling OSPFv3 routing for IPv6. For testing, they enabled OSPFv3 for IPv6 on R1 and R3. You need to fix the OSPFv3 neighbor issue between R1 and R3.

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	IP Address	Remote Device	IP address
R1 (Ethernet0/0)	172.16.1.2/30	R3 (Ethernet1/0)	172.16.1.1/30
R1 (Ethernet0/1)	192.168.10.1/24	To PC1	_
R1 (Ethernet0/2)	192.168.33.1/24	To Server	_
R3 (Ethernet0/0)	10.10.1.1/24	R4 (Ethernet0/0)	10.10.1.2/24
R3 (Ethernet0/1)	10.10.3.1/24	R5 (Ethernet0/1)	10.10.3.2/24
R3 (Ethernet0/2)	10.10.2.1/24	R6 (Ethernet0/2)	10.10.2.2/24
R4 (Ethernet0/1)	10.10.4.1/24	R6 (Ethernet0/1)	10.10.4.2/24

Device	IP Address	Remote Device	IP address
R4 (Ethernet0/2)	10.10.5.1/24	R5 (Ethernet0/2)	10.10.5.2/24
R5 (Ethernet0/0)	10.10.6.1/24	R6 (Ethernet0/0)	10.10.6.2/24
R2	172.16.2.2/30	R6 (Ethernet0/0)	172.16.2.1/30
R2	192.168.20.1/24	To PC2	_
R1 (Ethernet0/0)	2001:DB8:A:C1C2::2/64	R3 (Ethernet1/0)	2001:DB8:A:C1C2::1/64

OSPF Router IDs

Device	Router ID
R1	11.11.11.11
R2	22.22.22.22
R3	3.3.3.3
R4	4.4.4.4
R5	5.5.5.5
R6	6.6.6.6

Task 1: Troubleshooting OSPF Lab Procedure

Activity

Step 1 Isolate and correct the issue that is related to the loss of IPv4 connectivity between PC1 and PC2 (192.168.20.2). Make sure that the OSPF neighbors are formed between devices in the network.

Step 2 Isolate and correct the issue that is related to the loss of connectivity between PC2 and network 192.168.33.0/24. Check OSPF routing for these networks using **show ip route** command on R3 and R6.

Step 3 Isolate and correct the IPv6 OSPF neighbor issue between R1 and R3.

Verification

Step 1 To verify the connectivity between PC1 and PC2.

Substep 1

Use **ping** command to verify that the connectivity issue is resolved.

```
PC1# ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PC1#
```

If you do not get the desired result, check that the OSPF neighborship is formed between all devices.

Step 2 Verify that PC2 can ping 192.168.33.1 IP address on R1 E0/2.

Substep 1

Use **ping** command on PC2 to verify that the connectivity issue is resolved.

```
PC2# ping 192.168.33.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.33.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PC2#
```

If you do not get the desired result, check the routing path from PC2 to the destination network.

Step 3 Verify that the IPv6 OSPFv3 neighbor is formed between R3 and R1.

Substep 1

On R1, use **show ipv6 ospf neighbor** command to verify your configuration changes.

```
R1# show ipv6 ospf neighbor

            OSPFv3 Router with ID (10.10.10.10) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
3.3.3.3           1   FULL/DR         00:00:31    13              Ethernet0/0
R1#
```

If you do not get the desired result, check the IPv6 OSPF router configuration on R1.

Command List

The table describes the commands that are used in this activity. Refer to this list if you need configuration command assistance during the lab activity.

Command	Description
interface *interface-name*	To specify the interface, use the **interface** command in quota server configuration mode. To remove the interface, use the **no** form of this command.
router ospf *process-id* [**vrf** *vpn-name*]	To configure an OSPF routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

Command	Description
network {*IPv4 address netmask* | *IPv6 address netmask*}	To configure either an IPv4 or IPv6 network on a redundant peer, use the **network** command in configuration mode. To deconfigure a network, use the **no** form of this command.
show ip ospf [*process-id*]	To display general information about OSPF routing processes, use the **show ip ospf** command in user EXEC or privileged EXEC mode.
show ip ospf [*process-id*] **interface** *[type number*] [**brief**] [**multicast**] [**topology** {*topology-name* | **base**}]	To display interface information that is related to OSPF, use the **show ip ospf interface** command in user EXEC or privileged EXEC mode.
show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**]	To display OSPF neighbor information on a per-interface basis, use the **show ip ospf neighbor** command in privileged EXEC mode.
show ip protocols	To display the parameters and the current state of the active routing protocol process, use the **show ip protocols** command in privileged EXEC mode.
show ip route	To display the current state of the routing table, use the **show ip route** command in EXEC mode.

Answer Key

Challenge 12: Troubleshooting OSPF

Task 1: Troubleshooting OSPF Lab Procedure

Activity

Step 1 Make sure that the neighborship is formed between all devices between PC1 and PC2.

R3 is not forming neighborship with the R1. Check the OSPF configuration.

```
R3# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
6.6.6.6           1   FULL/DR         00:00:33    10.10.2.2       Ethernet0/2
5.5.5.5           1   FULL/DR         00:00:35    10.10.3.2       Ethernet0/1
4.4.4.4           1   FULL/DR         00:00:34    10.10.1.2       Ethernet0/0
R3#
```

You need to add the network 172.16.1.0/30 to OSPF process for area 1.

```
R3(config)# router ospf 1
R3(config-router)# network 172.16.1.0 0.0.0.3 area 1

*Jan 28 13:48:05.352: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Ethernet1/0 from
LOADING to FULL, Loading Done
```

Now, PC1 should be able to ping PC2.

Step 2 You need to check the routing path from PC2 to the destination network.

Use **traceroute** command on PC2 to check the path to the destination.

```
PC2# traceroute 192.168.33.1
Type escape sequence to abort.
Tracing the route to 192.168.33.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.20.1 1 msec 0 msec 1 msec
  2 172.16.2.1 1 msec 1 msec 0 msec
  3 10.10.2.1 1 msec 1 msec 0 msec
  4 10.10.2.2 1 msec 2 msec 0 msec
  5 10.10.2.1 1 msec 1 msec 1 msec
  6 10.10.2.2 1 msec 1 msec 1 msec
  7 10.10.2.1 1 msec 1 msec 1 msec
  8 10.10.2.2 1 msec 1 msec 1 msec
  9 10.10.2.1 1 msec 1 msec 1 msec
 10 10.10.2.2 1 msec 0 msec 0 msec
 11 10.10.2.1 1 msec 1 msec 0 msec
```

There is a routing loop between R3 and R6. To resolve it, check the routing table on R3 and R6.

```
R6# show ip route 192.168.33.1
Routing entry for 192.168.33.0/24
  Known via "ospf 1", distance 110, metric 30, type inter area
  Last update from 10.10.2.1 on Ethernet0/2, 00:04:07 ago
  Routing Descriptor Blocks:
  * 10.10.2.1, from 3.3.3.3, 00:04:07 ago, via Ethernet0/2
      Route metric is 30, traffic share count is 1
```

```
R3# show ip route 192.168.33.0
Routing entry for 192.168.33.0/24
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 10.10.2.2
      Route metric is 0, traffic share count is 1
R3#
```

On R3, there is a static route for network 192.168.33.0/24 pointing to R6. This route needs to be removed. R3 should be learning about this network from R1.

```
R3(config)# no ip route 192.168.33.0 255.255.255.0 10.10.2.2
```

Now, PC2 should be able to get to 192.168.33.0/24 network.

Step 3 Check the IPv6 OSPF configuration on R1.

On R1, you will see that passive interface has been enabled for all interfaces. This is preventing R1 from forming OSPF neighbor with R3.

```
R1(config)# ipv6 router ospf 1
R1(config-rtr)# no passive-interface ethernet0/0
R1(config-rtr)#
*Jan 28 14:04:47.197: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Ethernet0/0 from
LOADING to FULL, Loading Done
```

Module 11: Implementing Wide-Area Networks

Lesson 4: Configuring Single-Homed EBGP

Challenge 13: Implementing Single-Homed EBGP

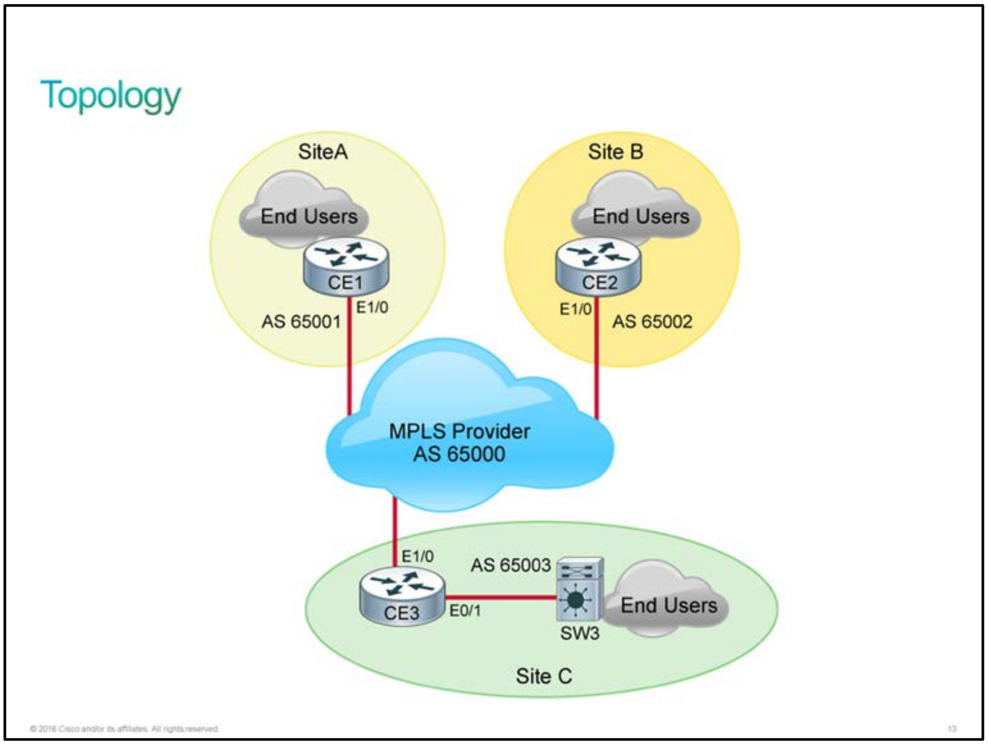
Introduction

The ABC Networks company is adding a new remote site, Site C to their network. They have all these sites connected via an MPLS provider and running EBGP with the ISP. The internal network has been set up for Site C. They are running EIGRP internally. You have been contracted to complete the BGP configuration.

Following are the requirements for Site C :

- Establish EBGP with the MPLS provider on CE3. The neighbor IP is 209.165.202.225.
- On CE3, advertise the networks learned from EIGRP into BGP on CE3 using network commands in BGP. You should see these networks in the routing table on CE1 and CE2.
- You should see the following networks in CE3 routing table once the BGP session is established. If not, you can troubleshoot the issue by logging into routers, CE1 and CE2.
  - 192.168.1.0/24 (from Site A)
  - 192.168.2.0/24(from Site B)
  - 192.168.11.0/26 (from Site A)
  - 192.168.22.0/28 (from Site B)

Topology



Job Aid

Note If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	IP Address	Remote Device
CE1 (Ethernet1/0)	209.165.200.226/30	MPLS Cloud (209.165.200.225/30)
CE1 (Ethernet0/0)	192.168.1.1/24	_
CE1 (Ethernet0/1)	192.168.11.1/26	_
CE2 (Ethernet1/0)	209.165.201.226/30	MPLS Cloud (209.165.201.225/30)
CE1 (Ethernet0/0)	192.168.2.1/24	_
CE2 (Ethernet0/0)	192.168.22.1/28	_

Device	IP Address	Remote Device
CE3 (Ethernet1/0)	209.165.200.226/30	MPLS Cloud (209.165.202.225/30)
CE3 (Ethernet1/0)	192.168.3.1/24	SW3 (Ethernet0/0)
SW3 (VLAN 1)	192.168.3.2/24	CE3 (Ethernet0/1)
SW3 (VLAN 10)	10.10.0.0/19	End Users
SW3 (VLAN 20)	10.11.0.0/17	End Users

Task 1: Implementing Single-Homed EBGP Lab Procedure

Activity

Step 1 Enable EBGP on router, CE3 to establish BGP session with MPLS provider.

Step 2 Advertise the internal networks learned from EIGRP in Site C into BGP using **network** commands. Use **show ip route eigrp** command to check the networks learned from EIGRP. Make sure that the subnet mask is correct when you are using the network command in BGP. BGP will advertise only those networks that have matching route in its routing table.

Step 3 Troubleshoot and make sure that Site C is learning the networks from Site A and Site B. On CE1 and CE2, make sure that the networks have been advertised in BGP using **network** command and that the subnet mask used is correct.

Verification

Step 1 Verify that BGP session is established between CE3 and MPLS.

Substep 1

Use **show ip bgp summary** command to verify your configuration changes.

```
CE3# show ip bgp summary
BGP router identifier 209.165.202.226, local AS number 65003
BGP table version is 3, main routing table version 3
2 network entries using 296 bytes of memory
2 path entries using 128 bytes of memory
2/2 BGP path/bestpath attribute entries using 272 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 744 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.202.225 4        65000       8       5        3    0    0 00:01:32        2
CE3#
```

If you do not get the desired result, check the BGP configuration on CE3.

Step 2 Verify that CE3 is advertising the EIGRP learned routes into BGP.

Substep 1

On CE3, use **show ip bgp** command to verify your configuration changes.

```
CE3# show ip bgp
BGP table version is 5, local router ID is 209.165.202.226
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.10.0.0/19     192.168.3.2         281856         32768 i
 *>  10.11.0.0/17     192.168.3.2         281856         32768 i
 *>  192.168.1.0      209.165.202.225                        0 65000 65001 i
 *>  192.168.2.0      209.165.202.225                        0 65000 65002 i
```

On CE1 and CE2, check the routing table to see if they are receiving these routes from CE3.

```
CE1# show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B        10.10.0.0/19 [20/0] via 209.165.200.225, 00:01:18
B        10.11.0.0/17 [20/0] via 209.165.200.225, 00:00:47
B     192.168.2.0/24 [20/0] via 209.165.200.225, 00:05:41
```

```
CE2# show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B        10.10.0.0/19 [20/0] via 209.165.201.225, 00:00:52
B        10.11.0.0/17 [20/0] via 209.165.201.225, 00:00:22
B     192.168.1.0/24 [20/0] via 209.165.201.225, 00:05:15
```

If you do not get the desired result, check the BGP configuration on CE3.

Step 3 Verify that CE3 is receiving all routes from Site A and Site B.

Substep 1

Use **show ip route bgp** and **show ip bgp** commands to verify your configuration changes.

```
CE3# show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     192.168.1.0/24 [20/0] via 209.165.202.225, 00:12:18
B     192.168.2.0/24 [20/0] via 209.165.202.225, 00:12:18
      192.168.11.0/26 is subnetted, 1 subnets
B        192.168.11.0 [20/0] via 209.165.202.225, 00:02:18
      192.168.22.0/28 is subnetted, 1 subnets
B        192.168.22.0 [20/0] via 209.165.202.225, 00:00:41
```

```
CE3# show ip bgp
BGP table version is 7, local router ID is 209.165.202.226
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.10.0.0/19     192.168.3.2         281856         32768 i
 *>  10.11.0.0/17     192.168.3.2         281856         32768 i
 *>  192.168.1.0      209.165.202.225                        0 65000 65001 i
 *>  192.168.2.0      209.165.202.225                        0 65000 65002 i
 *>  192.168.11.0/26  209.165.202.225                        0 65000 65001 i
 *>  192.168.22.0/28  209.165.202.225                        0 65000 65002 i
```

If you do not get the desired result, check the bgp configuration on CE1 and CE2.

Command List

The table describes the commands that are used in activity. Refer to the list if you need configuration command assistance during the lab activity.

Command	Description
router bgp *autonomous-system*	The command defines the router process and the AS number to which the routers belong

Command	Description
neighbor *ip-address* **remote-as** *number*	This **neighbor** command is used to establish a TCP connection with the BGP neighbor. The number in the command is the AS number of the router to which you want to connect with BGP. The ip-address is the next hop address with direct connection for eBGP.
network *network-number* **[mask** *network-mask*]	The network command controls the networks that originate from the device. With this command, you do not try to run BGP on a certain interface. Instead, you try to indicate to BGP what networks BGP should originate from this device. The command uses a mask portion because BGP version 4 (BGP4) can handle subnetting and supernetting. The **network** command works if the router knows the network that you attempt to advertise, whether connected, static, or learned dynamically.
show ip bgp summary	To display the status of all Border Gateway Protocol (BGP) connections, use the **show ip bgp summary** command in user EXEC or privileged EXEC mode.
show ip bgp	To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC or privileged EXEC mode.
show ip bgp neighbors	To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.
show ip route	To display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

Answer Key

Challenge 13: Implementing Single-Homed EBGP

Task 1: Implementing Single-Homed EBGP Lab Procedure

Activity

Step 1 Configure EBGP on CE3 with AS number of 65003.

On CE3, enter the following commands:

```
CE3(config)# router bgp 65003
CE3(config-router)# neighbor 209.165.202.225 remote-as 65000
CE3(config-router)#
*Oct 13 09:28:19.891: %BGP-5-ADJCHANGE: neighbor 209.165.202.225 Up
```

Step 2 On CE3, configure **network** command to advertise the internal networks learned from EIGRP.

On CE3, use **show ip route eigrp** command to check the networks learned from EIGRP.

```
CE3# show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D        10.10.0.0/19 [90/281856] via 192.168.3.2, 02:37:53, Ethernet0/1
D        10.11.0.0/17 [90/281856] via 192.168.3.2, 02:37:53, Ethernet0/1
CE3#
```

In the BGP router configuration mode, advertise these networks with correct subnet mask.

```
CE3(config)# router bgp 65003
CE3(config-router)# network 10.10.0.0 mask  255.255.224.0
CE3(config-router)# network 10.11.0.0 mask 255.255.128.0
```

Make sure that the subnet mask is correct. BGP will advertise only those networks that have matching route in its routing table.

Step 3 Check if CE3 is learning the routes from Site A and Site B.

On CE3 , use **show ip route bgp** command to check the routes learned from BGP.

```
CE3#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     192.168.1.0/24 [20/0] via 209.165.202.225, 00:07:22
B     192.168.2.0/24 [20/0] via 209.165.202.225, 00:07:22
```

Notice that only two networks are being learned. Check the BGP configuration on CE1 and CE2.

On CE1, the subnet mask for the network 192.168.11.0/26 is not correct. Change the subnet mask and then check if CE3 is receiving this route.

```
CE1(config)# router bgp 65001
CE1(config-router)# no network 192.168.11.0
CE1(config-router)# network  192.168.11.0 mask 255.255.255.192
```

On CE2, the subnet mask for the network 192.168.22.0/28 is not correct. Change the subnet mask and then check if CE3 is receiving this route.

```
CE2(config)# router bgp 65002
CE2(config-router)# no  network 192.168.22.0 mask 255.255.255.252
CE2(config-router)# network 192.168.22.0 mask  255.255.255.240
```

Module 13: Summary Challenge

Lesson 1: Troubleshooting Scalable Multiarea Network

Challenge 14: Summary Challenge Lab: 5

Scenario

You work for RMZ Networking. Your colleague, Peter did some improvements on the network over the weekend. On Monday morning, he is seeing certain issues in the network and needs your help in troubleshooting it.

He gives you the following information about the network :

- There are two sites, Site A and Site B, connected via serial links that are bundled into a multilink interface.
- Site A has OSPF routing configured while Site B has EIGRP running on the devices.
- CE1 should establish a PPPoE session with the ISP and the dialer interface should be configured to allow a dynamic IP address to be assigned.
- The edge routers, CE1 and CE2 are injecting default route into OSPF and EIGRP respectively.
- The serial links between CE1-R1 and CE1-R2 have PPP enabled. They are authenticating using CHAP. CHAP password is **c1sc0**.
- Routers, R4 and R5 are running HSRP with standby group number 10.

Following are the issues that you need to resolve:

- On R4 and R5, following error message is seen :

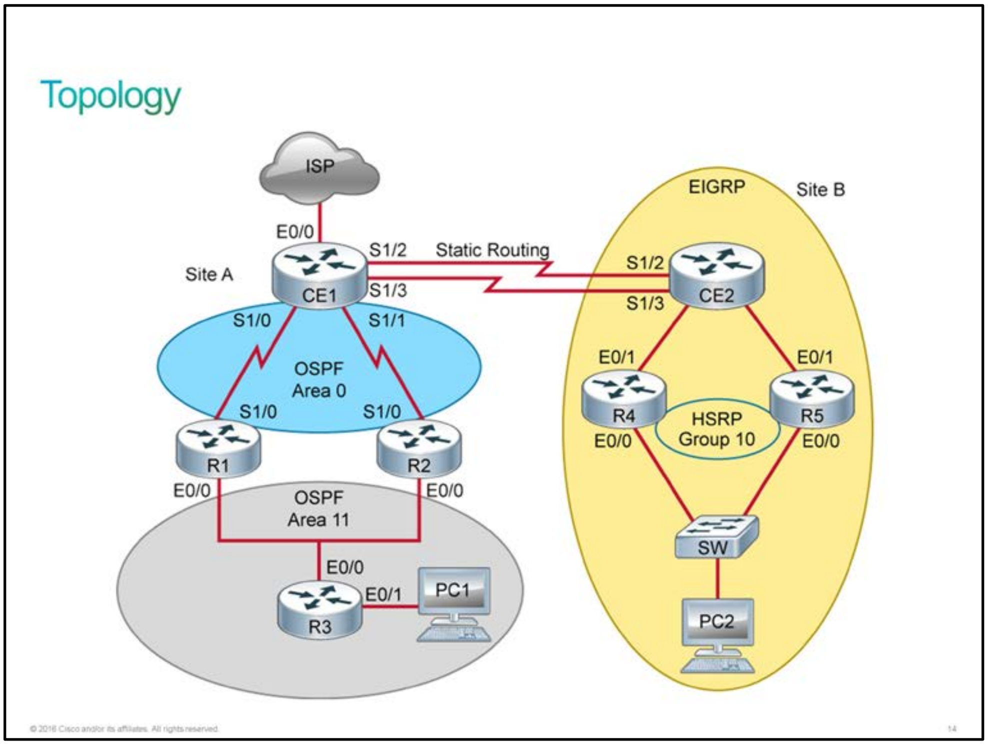
```
R4#
*Dec  9 06:09:00.695: %IP-4-DUPADDR: Duplicate address 192.168.10.1 on Ethernet0/0,
sourced by 0000.0c07.ac01
```

```
R5#
*Dec  9 06:10:00.693: %IP-4-DUPADDR: Duplicate address 192.168.10.1 on Ethernet0/0,
sourced by 0000.0c07.ac0a
R5#
```

- PC2 cannot reach internet. To test internet connectivity, use IP address 209.165.200.225.

- CE1 is not forming OSPF neighbors with R1 and R2.
- PC1 cannot reach PC2.

Topology



Job Aid

Note	If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

Device	IP address	Remote Device
CE1 (Multilink 12)	172.16.1.1/30	CE2 (Multilink 12)
CE2 (Multilink 12)	172.16.1.2/30	CE1 (Multilink 12)
CE1 (Loopback 0)	101.1.1.1	_
CE2 (Loopback 0)	102.1.1.1	_
CE1 (Serial 1/0)	10.1.1.1/30	R1 (Serial 1/0)

Device	IP address	Remote Device
CE1 (Serial 1/1)	10.2.1.1/30	R2 (Serial 1/0)
R1 (E0/0)	10.10.10.1/24	_
R2 (E0/0)	10.10.10.2/24	_
R3 (E0/0)	10.10.10.3/24	_
R3 (E0/1)	10.10.30.3/24	To PC1
CE2 (E0/0)	192.168.1.1/24	R4 (E0/1)
CE2 (E0/1)	192.168.2.1/24	R5 (E0/1)
R4(E0/1)	192.168.1.2/24	CE2 (E0/0)
R4 (E0/0)	192.168.10.2/24	SW2
R5 (E0/1)	192.168.2.2/24	CE2(E0/1)
R5 (E0/0)	192.168.10.3/24	SW2
R1 (Loopback 0)	1.1.1.1	_
R2 (Loopback 0)	2.2.2.2	_
R3 (Loopback 0)	3.3.3.3	_
R4 (Loopback 0)	4.4.4.4	_
R5 (Loopback 0)	5.5.5.5	_
PC1	10.10.30.1	_
PC2	192.168.10.5	_

Task 1: Summary Challenge Lab Procedure

Activity

Step 1 Ensure that interface Ethernet0/0 on R4 and R5 has been configured correctly for HSRP with standby group number 10.

Step 2 Ensure that PC2 in Site B has internet connectivity (209.165.200.225). Make sure that the Multilink interface on CE2 has been configured correctly.

Step 3 Ensure that CE1 forms OSPF neighbor with R1 and R2. Make sure that the OSPF has been configured correctly. Also, make sure that PPP has been configured correctly on the serial links. CHAP password should be "**c1sco**."

Step 4 Ensure that PC2 can reach PC1. Make sure that PC1 and PC2 IP addresses are being advertised by the routing protocols.

Verification

Step 1 Verify that HSRP is configured correctly.

Substep 1

Use the following command to verify your configuration changes.

```
R4# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0       10   150 P Active  local           192.168.10.3    192.168.10.1
R4#
```

Use the following command to verify your configuration changes.

```
R5# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0       10   110 P Standby 192.168.10.2    local           192.168.10.1
R5#
```

If you do not get the desired result, check the HSRP configuration on R4 and R5 interface E0/0.

Step 2 Verify that PC2 can get to the Internet.

Substep 1

Use **ping** command to test the internet connectivity from PC2.

```
PC2# ping 209.165.200.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms
```

If you do not get the desired result, check the configuration on CE1 and CE2.

Step 3 Verify that CE1 forms OSPF neighborship with R1 and R2.

Substep 1

On CE1, use **show ip ospf neighbor** command to verify your configuration changes.

```
CE1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:37    10.2.1.2        Serial1/1
1.1.1.1           0   FULL/  -        00:00:32    10.1.1.2        Serial1/0
```

```
CE1#
```

If you do not get the desired result, check the configuration on R1 and R2.

Step 4 Verify that PC2 can reach the PC1.

Substep 1

Use **ping** command to verify that the connectivity is resolved.

```
PC2# ping 10.10.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms
```

If you do not get the desired result, check the configuration on R3 and CE1.

Answer Key

Challenge 14: Summary Challenge Lab: 5

Task 1: Summary Challenge Lab Procedure

Activity

Step 1 The duplicate IP address in the error message is that of the HSRP virtual IP. On R4 and R5, the HSRP standby group number is not configured correctly. Therefore, both routers are in ACTIVE state. The HSRP standby group number should be the same on both routers.

Following configuration change is required on R5 :

```
R5(config)# interface ethernet 0/0
R5(config-if)# no  standby 1 ip 192.168.10.1
R5(config-if)#
*Dec  1 09:24:48.424: %HSRP-5-STATECHANGE: Ethernet0/0 Grp 1 state Active -> Disabled
R5(config-if)# no standby 1 priority 110
R5(config-if)# no standby 1 preempt
R5(config-if)# standby 10  ip 192.168.10.1
R5(config-if)# standby 10 priority 110
R5(config-if)# standby 10 preempt
R5(config-if)#
*Dec  1 09:25:39.472: %HSRP-5-STATECHANGE: Ethernet0/0 Grp 10 state Speak -> Standby
R5(config-if)#
```

Notice that the HSRP state changes to STANDBY on R5. Now, you should not see the error message.

Step 2 Troubleshoot the connectivity issue by tracing the path from PC2.

On CE2, the interface, Multilink 12 is in "down/down" state. This is why CE2 does not have a default route. The next hop is connected to this interface. The interfaces, Serial 1/2 and Serial 1/3 are in "up/down" state. These interfaces on CE2 should be configured correctly.

```
CE2(config)# interface serial 1/2
CE2(config-if)# encapsulation ppp
CE2(config-if)# ppp multilink group 12
CE2(config-if)# ppp multilink


CE2(config)# interface serial 1/3
CE2(config-if)# encapsulation ppp
CE2(config-if)# ppp multilink group 12
CE2(config-if)# ppp multilink
```

Now, PC2 should be able to reach internet.

Step 3 Isolate and troubleshoot the OSPF neighbor issue on CE1, R1, and R2.

On R1, the interface Serial 1/0 connected to CE1 is in passive state in OSPF. You need to make sure that this interface is not passive so that it forms OSPF neighbor with CE1.

```
R1(config)# router ospf 1
R1(config-router)# no passive-interface serial 1/0
R1(config-router)#
*Dec  1 12:15:41.014: %OSPF-5-ADJCHG: Process 1, Nbr 101.1.1.1 on Serial1/0 from LOADING
to FULL, Loading Done
R1(config-router)#
```

On R2, the OSPF configuration is correct. You will notice that you cannot ping the directly connected serial interface on CE1 from R2. The PPP authentication protocol that is used is CHAP. The username and password has not been configured on R2. You need to make the following configuration change on R2.

```
R2(config)# username CE1 password c1sc0
R2(config)#
*Dec  1 12:21:53.297: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed
state to up
*Dec  1 12:21:53.346: %OSPF-5-ADJCHG: Process 1, Nbr 101.1.1.1 on Serial1/0 from LOADING
to FULL, Loading Done
R2(config)#
```

Step 4 Isolate and troubleshoot the connectivity issue between PC1 and PC2.

On R3, the PC1 network has been advertised with wrong OSPF area ID. It should be in OSPF area 11.

```
R3(config)# router ospf 1
R3(config-router)# no network 10.10.30.0 0.0.0.0 area 1
R3(config-router)# network 10.10.30.0 0.0.0.0 area 11
```

Lesson 2: Implementing and Troubleshooting Scalable Multiarea Network

Challenge 15: Summary Challenge Lab: 6

Scenario

You work for TMC Networking. Your colleague, Peter did some improvements on the network over the weekend. On Monday morning, he is seeing certain issues in the network and needs your help in troubleshooting it.

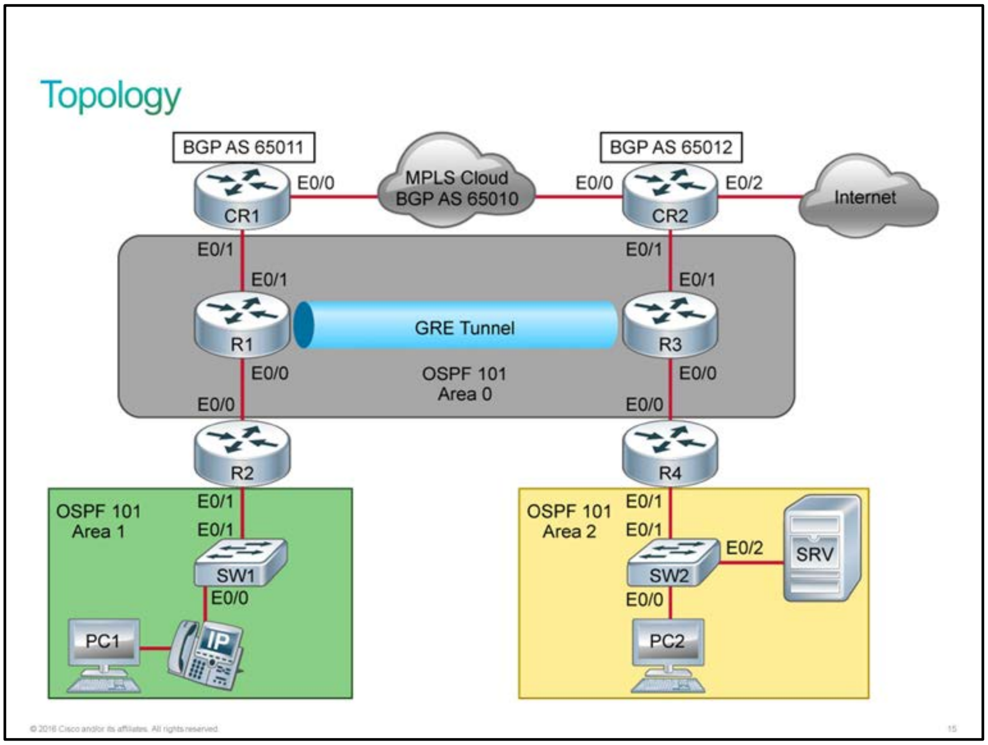
He is giving you the following information about the network :

- The routers, CR1 and CR2 are the two edge routers that are connected via MPLS cloud running EBGP.
- CR2 is acting as the PPPoE client. It is dynamically getting IP address from the ISP for internet access. CR2 is authenticating using PAP. The PAP username is **admin** and password is **c1sc0**.
- Routers, CR1 and CR2 should be injecting the default route into OSPF.
- The routers R1 and R2 should have a GRE tunnel configured. OSPF is enabled on the tunnel interface. The Loopback 10 interface on these routers should be used as the tunnel source and destination address.
- The routers are running OSPF as shown in the topology.
- For IPv6 routing, refer to the topology in Job Aids.

Following are the issues that you need to resolve:

- The EBGP session is not established between CR1 and MPLS router.
- The routers, R1 and R3 are not forming OSPF neighbor on the interface, tunnel 12.
- PC1 cannot reach internet. To test internet connectivity, use IP address 209.165.200.225.
- There is no IPv6 connectivity between PC1 and Server (2001:DB8:A:C1E3::2).

Topology



Job Aid

Note	If you shut down an interface on a real router or switch, the connected device will see it as "down/down." Due to virtualization specifics, IOL behavior is slightly different. If you shut down an interface on a router or switch, the connected device will see it as "up/up." In IOL, the status of an interface can only be "up/up" or "administratively down/down."

Device Information

IPv4 Addressing

Device	IP address	Remote Device	Remote Device IP address
CR1 (E0/0)	172.16.1.1	MPLS	172.16.1.2
CR1 (E0/1)	192.168.1.1	R1 (E0/1)	192.168.1.2
R1 (E0/0)	192.168.1.5	R2 (E0/0)	192.168.1.6
R2 (E0/1.1)	192.168.1.10	SW1 (VLAN1)	192.168.1.9
R2 (E0/1.10)	192.168.10.1	SW1 (to Workstations)	_
R2 (E0/1.10)	192.168.20.1	SW1 (to IP Phones)	_

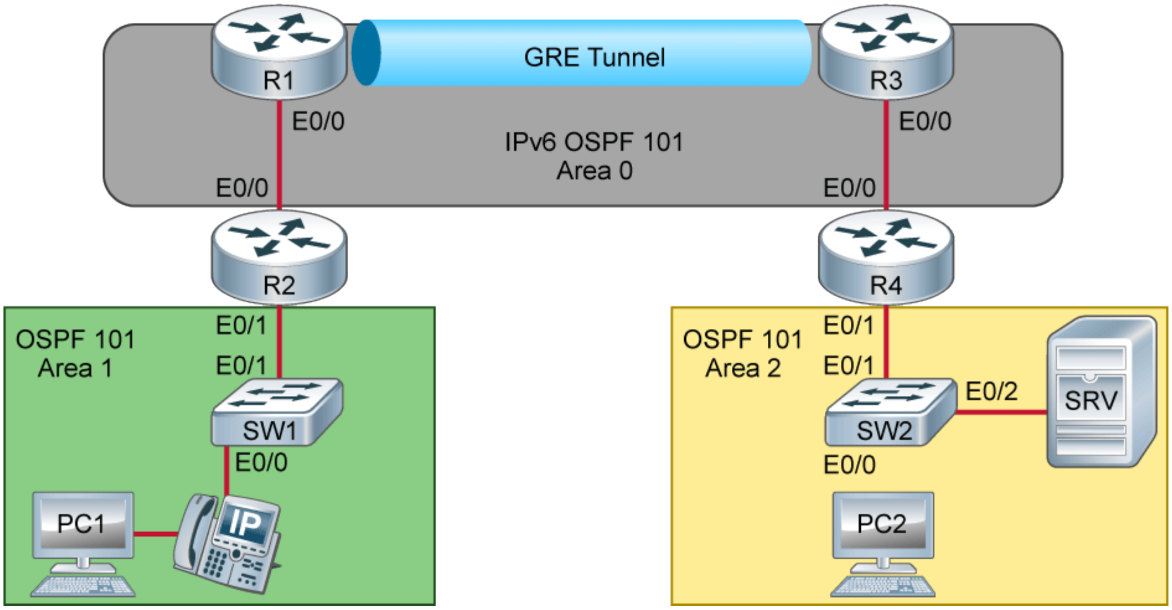
Device	IP address	Remote Device	Remote Device IP address
CR2 (E0/0)	172.16.2.1	MPLS	172.16.2.2
CR2 (E0/1)	192.168.2.1	R3(E0/1)	192.168.2.2
R3 (E0/0)	192.168.2.5	R4 (E0/0)	192.168.2.6
R4 (E0/1.1)	192.168.2.10	SW2	192.168.2.9
R4(E0/1.30)	192.168.30.1	SW2(to Workstations)	_
R4 (E0/1.33)	192.168.33.1	SW2 (to Server)	_
R1 (Loopback 10)	10.100.1.1	_	_
R3 (Loopback 10)	10.200.1.1	_	_
R1 (Tunnel 12)	10.1.1.1	R2 (Tunnel 12)	10.1.1.1.2
R1 (Loopback 0)	1.1.1.1	_	_
R2 (Loopback 0)	2.2.2.2	_	_
R3 (Loopback 0)	3.3.3.3	_	_
R4 (Loopback 0)	4.4.4.4	_	_
CR1(Loopback 0)	11.11.11.11	_	_
CR2 (Loopback 0)	22.22.22.22	_	_
PC1	192.168.10.5	_	_
Server	192.168.33.3	_	_

IPv6 Addressing

Device	IP address	Remote Device	Remote Device IP address
R1(Tunnel 12)	2001:DB8:A:B1B2::1/64	R3 (Tunnel 12)	2001:DB8:A:B1B2::2/64
R1 (E0/0)	2001:DB8:A:B1C2::1/64	R2 (E0/0)	2001:DB8:A:B1C2::2/64
R2 (E0/1.1)	2001:DB8:A:C2D1::1/64	SW1	_
R2 (E0/1.10)	2001:DB8:A:C2D2::1/64	SW1	PC1
R2 (E0/1.20)	2001:DB8:A:C2D3::1/64	SW1	IP Phones

Device	IP address	Remote Device	Remote Device IP address
R3 (E0/0)	2001:DB8:A:B2C1::1/64	R4 (E0/0)	2001:DB8:A:B2C1::2/64
R4 (E0/1.1)	2001:DB8:A:C1E1::1/64	SW2	_
R4 (E0/1.30)	2001:DB8:A:C1E3::1/64	SW2	PC2
R4 (E0/1.33)	2001:DB8:A:C1E3::1/64	SW2	SRV
PC1	2001:DB8:A:C2D2::2/64	_	_
PC2	2001:DB8:A:C1E2::2/64	_	_
SRV	2001:DB8:A:C1E3::2/64	_	_

IPv6 OSPF Routing



Task 1: Summary Challenge Lab Procedure

Activity

Step 1 Ensure that the EBGP session is established between CR1 and MPLS router. Make sure that BGP has been configured correctly on CR1. Also, the interface connecting to the MPLS router, Ethernet0/0 should be configured correctly.

Step 2 Ensure that R1 and R3 form an OSPF neighbor on the GRE tunnel 12. Make sure that the tunnel interface has been configured with the correct source and destination.

Step 3 Ensure that PC1 can reach internet(209.165.200.225). Make sure that the dialer interface is getting the IP address from the ISP. PAP authentication should be configured correctly.

Step 4 Ensure that there is IPv6 connectivity between PC1 and Server(2001:DB8:A:C1E3::2). Make sure that the IPv6 OSPF neighborship is formed between all connected device.

Verification

Step 1 Verify that BGP session is established on CR1

Substep 1

Use the following command on CR1 to verify your configuration changes.

```
CR1# show ip bgp summary
BGP router identifier 11.11.11.11, local AS number 65011
BGP table version is 6, main routing table version 6
5 network entries using 700 bytes of memory
5 path entries using 380 bytes of memory
2/2 BGP path/bestpath attribute entries using 280 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1384 total bytes of memory
BGP activity 5/0 prefixes, 5/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.2      4        65010      12       8        6    0    0 00:03:45        4
CR1#
```

If you do not get the desired result, check the interface configuration on CR1.

Step 2 Verify that OSPF neighborship is formed between R1 and R3.

Substep 1

Use the following command on R1 and R3 to verify your configuration changes.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
11.11.11.11       1   FULL/DR         00:00:35    192.168.1.1     Ethernet0/1
 2.2.2.2           1   FULL/DR         00:00:37    192.168.1.6     Ethernet0/0
 3.3.3.3           0   FULL/  -        00:00:39    10.1.1.2        Tunnel12
R1#
```

```
R3# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
22.22.22.22       1   FULL/BDR        00:00:37    192.168.2.1     Ethernet0/1
4.4.4.4           1   FULL/DR         00:00:36    192.168.2.6     Ethernet0/0
1.1.1.1           0   FULL/  -        00:00:37    10.1.1.1        Tunnel12
R3#
```

If you do not get the desired result, check the tunnel configuration.

Step 3 Verify that PC1 can reach internet.

Substep 1

Use the following command on PC1 to verify that the connectivity issue is resolved.

```
PC1# ping 209.165.200.225
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
PC1#
```

If you do not get the desired result, check the configuration CR1 and CR2.

Step 4 Verify that there is IPv6 connectivity between PC1 and Server.

Substep 1

Use the following command on PC1 to verify that the connectivity issue is resolved.

```
PC1# ping 2001:DB8:A:C1E3::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:A:C1E3::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
PC1#
```

If you do not get the desired result, check the configuration R1 and R4.

Answer Key

Challenge 15: Summary Challenge Lab: 6

Task 1: Summary Challenge Lab Procedure

Activity

Step 1 Troubleshoot and resolve the BGP peering issue between CR1 and MPLS router.

The BGP configuration on CR1 looks good. The interface, E0/0 on CR1, which connects to the MPLS provider has an access-list. This access-list denies all TCP traffic. BGP peers are established by manual configuration between routers to create a TCP session on port 179. You need to allow TCP traffic for BGP session to be established. This access-list should be removed from the interface.

```
CR1(config)# interface ethernet 0/0
CR1(config-if)# no ip access-group FILTER in
CR1(config-if)#
CR1#
*Dec 17 11:56:07.800: %BGP-5-NBR_RESET: Neighbor 172.16.1.2 active reset (BGP
Notification sent)
*Dec 17 11:56:07.800: %BGP-5-ADJCHANGE: neighbor 172.16.1.2 Up
```

Step 2 Troubleshoot and resolve the OSPF neighbor issue on R1 and R3.

Check the Tunnel 12 interface on both routers. The tunnel 12 is in up and down state. The tunnel source on R1 has not been configured correctly. The tunnel source should be interface loopback 10 and not loopback 100. Change the configuration on Tunnel 12 interface on R1.

```
R1(config)# interface tunnel 12
R1(config-if)# no tunnel source Loopback100
R1(config-if)# tunnel source loopback 10
R1(config-if)#
*Dec 21 04:27:50.025: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel12, changed
state to up
```

Step 3 Troubleshoot and resolve the internet connectivity issue from PC1.

CR2 is the router connected to the ISP gateway. The dialer interface on CR2 is not getting an IP address from the ISP. It is because the PPP PAP authentication is failing. You need to correct the PAP password on the dialer interface.

```
CR2(config)# interface Dialer1
CR2(config-if)# no ppp pap sent-username admin password 0 cisco
CR2(config-if)# ppp pap sent-username admin password c1sc0
```

Now, PC1 should be able to get to the internet.

Step 4 Troubleshoot and resolve the IPv6 connectivity issue between PC1 and Server.

R3 and R4 are not IPv6 OSPF neighbors. It is because the interface E0/0 on R4 has been made passive. Enter the following commands on R4:

```
R4(config)# ipv6 router ospf 101
R4(config-rtr)# no passive-interface ethernet 0/0
```

Now, the IPv6 OSPF neighbors should be formed and PC1 should be able to reach the Server.