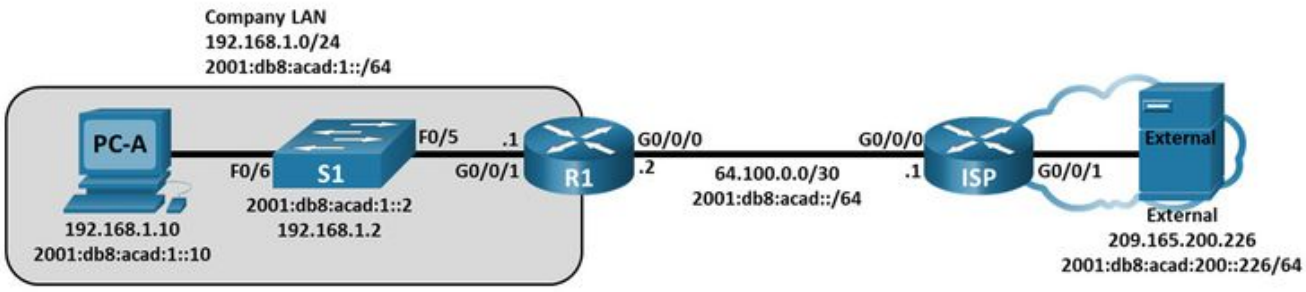
13.3.2 Lab – Use Ping and Traceroute to Test Network Connectivity (Answers)

August 7, 2020

13.3.2 Lab – Use Ping and Traceroute to Test Network Connectivity

Topology



Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	64.100.0.2 /30	N/A
		2001:db8:acad::2 /64	
		fe80::2	
R1	G0/0/1	192.168.1.1 /24	N/A
		2001:db8:acad:1::1 /64	
		fe80::1	
ISP	G0/0/0	64.100.0.1 /30	N/A
		2001:db8:acad::1 /64	
		fe80::1	
ISP	G0/0/1	209.165.200.225 /27	N/A
		2001:db8:acad:200::225 /64	
		fe80::225	

Device	Interface	IP Address / Prefix	Default Gateway
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
		2001db8:acad:1::2 /64	fe80::1
		fe80::10	
PC-A	NIC	2001:db8:acad:1::10 /64	fe80::1
		64.100.0.2 /30	N/A
External	NIC	209.165.200.226 /27	209.165.200.225
		2001:DB8:ACAD:200::226 /64	FE80::225

Objectives

- **Part 1: Build and Configure the Network**
- **Part 2: Use Ping Command for Basic Network Testing**
- **Part 3: Use Tracert and Traceroute Commands for Basic Network Testing**
- **Part 4: Troubleshoot the Topology**

Background / Scenario

Ping and traceroute are two tools that are indispensable when testing TCP/IP network connectivity. Ping is a network administration utility used to test the reachability of a device on an IP network. This utility also measures the round-trip time for messages sent from the originating host to a destination computer. The ping utility is available on Windows, Unix-like operating systems (OS), and the Cisco Internetwork Operating System (IOS).

The traceroute utility is a network diagnostic tool for displaying the path or route and measuring the transit delays of packets travelling an IP network. The tracert utility is available on Windows, and a similar utility, traceroute, is available on Unix-like OS and Cisco IOS.

In this lab, the **ping** and **traceroute** commands are examined and command options are explored to modify the command behavior. Cisco devices and PCs are used in this lab for command exploration. The necessary Cisco device configurations are provided in this lab.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

The **default bias** template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Instructions

Part 1: Build and Configure the Network

In Part 1, you will set up the network in the topology and configure the PCs and Cisco devices. The initial configurations for the routers and switches are provided for your reference. In this topology, static routing is used to route packets between networks.

Step 1: Cable the network as shown in the topology.

Step 2: Erase the configurations on the routers and switches, and reload the devices.

Step 3: Configure PC IP addresses and default gateways according to the Addressing Table.

Step 4: Configure the R1 and ISP routers and S1 switch using the initial configurations provided below.

At the switch or router global configuration mode prompt, copy and paste the configuration for each device. Save the configuration to startup-config.

Initial configurations for the R1 router:

```
hostname R1
no ip domain lookup
ipv6 unicast-routing
interface g0/0/0
 ip address 64.100.0.2 255.255.255.252
 ipv6 address 2001:db8:acad::2/64
 ipv6 address fe80::2 link-local
 ip nat outside
 no shutdown
interface g0/0/1
 ip add 192.168.1.1 255.255.255.0
 ipv6 address 2001:db8:acad:1::1/64
 ipv6 address fe80::1 link-local
 ip nat inside
 no shutdown
ip route 0.0.0.0 0.0.0.0 64.100.0.1
ipv6 route 0::/0 2001:db8:acad::1
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface g0/0/0 overload
```

Initial configurations for ISP:

```
hostname ISP
no ip domain lookup
ipv6 unicast-routing
interface g0/0/0
 ip address 64.100.0.1 255.255.255.252
 ipv6 address 2001:db8:acad::1/64
 ipv6 address fe80::1 link-local
 no shutdown
interface g0/0/1
 ip add 209.165.200.225 255.255.255.224
 ipv6 address 2001:db8:acad:200::225/64
 ipv6 address fe80::225 link-local
 no shutdown
ipv6 route ::/0 2001:db8:acad::2
```

Instructor Note: If Netlab is used, switch interfaces that are not in use should be shut down for this lab. As an example, the following commands can be used on S1:

```
Switch(config)# interface range f0/1 – 4, f0/7 – 24, g0/1 - 2
Switch(config)# shutdown
```

Initial configurations for S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.2 255.255.255.0
 ipv6 address 2001:db8:acad:1::2/64
 ipv6 address fe80::2 link-local
 no shutdown
 exit
ip default-gateway 192.168.1.1
end
```

Step 5: Configure an IP host table on the R1 router.

The IP host table allows you to use a hostname to connect to a remote device rather than an IP address. The host table provides name resolution for the device with the following configurations. Copy and paste the following configurations for the R1 router. The configurations will allow you to use the hostnames for **ping** and **traceroute** commands on the R1 router.

```
ip host Externalv4 209.165.200.226
ip host Externalv6 2001:db8:acad:200::226
ip host ISPv4 64.100.0.1
ip host ISPv6 2001:db8:acad::1
ip host PC-Av4 192.168.1.10
ip host PC-Av6 2001:db8:acad:1::10
ip host R1v4 64.100.0.2
ip host R1v6 2001:db8:acad::2
ip host S1v4 192.168.1.2
ip host S1v6 2001:db8:acad:1::2
end
```

Part 2: Use Ping Command for Basic Network Testing

In Part 2 of this lab, use the ping command to verify end-to-end connectivity. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and then waiting for an ICMP response. It can record the round trip time and any packet loss or routing loops.

IP packets have a limited lifetime on the network. IP packets use an 8 bit Time to Live (IPv4) or Hop Limit (IPv6) header field value which specifies the maximum number of layer three hops that can be traversed on the path to their destination. Hosts on a network will set its own 8 bit value with a maximum value of 255.

So each time an IP packet arrives at a layer three network device this value is reduced by one before it is forwarded to its destination. So if this value eventually reaches zero the IP packet is discarded.

You will examine the results with the **ping** command and the additional ping options that are available on Windows-based PCs and Cisco devices.

Step 1: Test network connectivity from the R1 network using PC-A.

All the pings from PC-A to other devices in the topology should be successful. If they are not, check the topology and the cabling, as well as the configuration of the Cisco devices and the PCs.

a. Ping from PC-A to its default gateway using the IPv4 address (R1's GigabitEthernet 0/0/1 interface).

```
C:\> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

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

In this example, four (4) ICMP requests, 32 bytes each, were sent and the responses were received in less than one millisecond with no packet loss. The transmission and reply time can increase as the ICMP requests and responses are processed by more devices during the journey to and from the final destination.

This can also be done using the IPv6 address of the default gateway (R1's GigabitEthernet 0/0/1 interface).

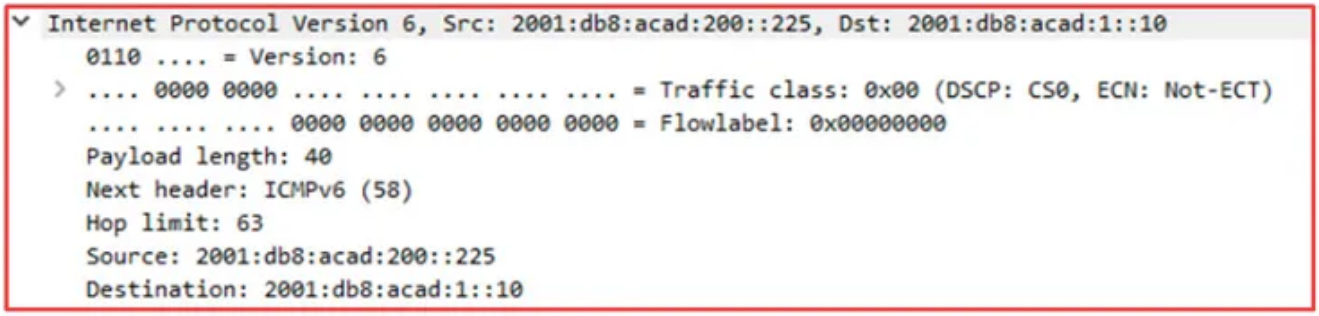
```
C:\> ping 2001:db8:acad:1::1
Pinging 2001:db8:acad:1::1 with 32 bytes of data:
Reply from 2001:db8:acad:1::1: time=5ms
Reply from 2001:db8:acad:1::1: time=1ms
Reply from 2001:db8:acad:1::1: time=1ms
Reply from 2001:db8:acad:1::1: time=1ms

Ping statistics for 2001:db8:acad:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

b. From PC-A, ping the addresses listed in the following table and record the average round trip time and IPv4 Time to Live (TTL) or IPv6 Hop Limit. **Optional:** Use WireShark to see the IPv6 Hop Limit value.

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
192.168.1.10	<1	128
2001:db8:acad:1::10	<1	128
192.168.1.1 (R1)	<1	255
2001:db8:acad:1::1 (R1)	1	64
192.168.1.2 (S1)	1	255
2001:db8:acad:1::2(S1)	1	64
64.100.0.2 (R1)	1	255
2001:DB8:ACAD::2 (R1)	<1	64
64.100.0.1 (ISP)	<1	254
2001:DB8:ACAD::1 (ISP)	1	63
209.165.200.225 (ISP G0/0/1)	1	254
2001:DB8:ACAD:200::225 (ISP G0/0/1)	1	63
209.165.200.226 (External)	1	126
2001:DB8:ACAD:200::226 (External)	01	126

Instructor Note: The average round trip time was increased if the message “Request timed out” was displayed during the first ICMP request. ARP caused the delay, and this resulted in packet loss.

Below is a sample WireShark capture of the ping reply from External to PC-A with a Hop limit of 63.



Step 2: Use extended ping commands on PC-A.

The default **ping** command sends four requests at 32 bytes each. It waits 4,000 milliseconds (4 seconds) for each response to be returned before displaying the “Request timed out” message. The **ping** command can be fine-tuned for troubleshooting a network.

a. At the command prompt, type ping and press Enter.

```
C:\> ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

b. Using the **–t** option, ping External to verify that External is reachable.

```
C:\Users\User1> ping –t 209.165.200.226
Pinging 209.165.200.226 with 32 bytes of data:
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
```

To illustrate the results when a host is unreachable, disconnect the cable between the ISP router and External, or shut down the GigabitEthernet 0/0/1 interface on the ISP router.

```
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
Reply from 64.100.0.1: Destination host unreachable.
Reply from 64.100.0.1: Destination host unreachable.
```

While the network is functioning correctly, the **ping** command can determine whether the destination responded and how long it took to receive a reply from the destination. If a network connectivity problem exists, the **ping** command displays an error message.

c. Reconnect the Ethernet cable or enable the GigabitEthernet 0/0/1 interface on the ISP router (using the **no shutdown** command) before moving onto the next step. After about 30 seconds, the ping should be successful again.

```
Reply from 64.100.0.1: Destination host unreachable.
Request timed out.
Request timed out.
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
Reply from 209.165.200.226: bytes=32 time<1ms TTL=126
```

d. Press **Ctrl+C** to stop the ping command.

e. The above steps can be repeated for IPv6 address to obtain ICMP error message.

What ICMP error messages did you receive?
Destination net unreachable, request timed out.

f. Enable the GigabitEthernet 0/0/1 interface on the ISP router (using the **no shutdown** command) before moving onto the next step. After about 30 seconds, the ping should be successful again.

Step 3: Test network connectivity from the R1 network using Cisco devices.

The **ping** command is also available on Cisco devices. In this step, the **ping** command is examined using the R1 router and the S1 switch.

a. Ping External on the external network using the IP address of 209.165.200.226 from the R1 router.

```
R1# ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The exclamation point (!) indicates that the ping was successful from the R1 router to External. The round trip takes an average of 1 ms with no packet loss, as indicated by a 100% success rate.

b. Because a local host table was configured on the R1 router, you can ping Externalv4 on the external network using the hostname configured from the R1 router.

Note: The hostname is not case-sensitive. You can substitute the hostname for the IP address if desired on R1 in this lab.

```
R1# ping externalv4
```

What is the IP address used?
209.165.200.226

c. There are more options available for the **ping** command. At the CLI, type **ping** and press Enter. Use **ipv6** as the protocol. Input **2001:DB8:ACAD:200::226** or **external** for the Target IPv6 address. Press Enter to accept the default value for other options.

```
R1# ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acad:200::226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:200::226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

d. You can use an extended ping to observe when there is a network issue. Start the **ping** command to 209.165.200.226 with a repeat a count of 50000. Then, disconnect the cable between the ISP router and EXTERNAL or shut down the GigabitEthernet 0/0/1 interface on the ISP router.

Reconnect the Ethernet cable or enable the GigabitEthernet 0/0/1 interface on the ISP router after the exclamation points (!) have replaced by the letter U and periods (.). After about 30 seconds, the ping should be successful again. Press **Ctrl**+**Shift**+**6** to stop the **ping** command if desired.

```
R1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]: 10000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.U.U.U.U.U.
U.U.............!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 99 percent (9970/10000), round-trip min/avg/max = 1/1/10 ms
```

The letter U in the results indicates that a destination is unreachable. An error protocol data unit (PDU) was received by the R1 router. Each period (.) in the output indicates that the ping timed out while waiting for a reply from External. In this example, 1% of the packets were lost during the simulated network outage.

Note: You can also use the following commands for the same results:

```
R1# ping 209.165.200.226 repeat 10000
or
R1# ping 2001:db8:acad:200::226 repeat 10000
```

Close configuration window
The **ping** command is extremely useful when troubleshooting network connectivity. However, ping cannot indicate the location of problem when a ping is not successful. The **tracert** (or **traceroute**) command can display network latency and path information.

Part 3: Use Tracert and Traceroute Commands for Basic Network Testing

The commands for tracing routes can be found on PCs and network devices. For a Windows-based PC, the **tracert** command uses ICMP messages to trace the path to the final destination. The **traceroute** command utilizes the User Datagram Protocol (UDP) datagrams for tracing routes to the final destination for Cisco devices and other Unix-like PCs.

In Part 3, you will examine the traceroute commands and determine the path that a packet travels to its final destination. You will use the **tracert** command from the Windows PCs and the **traceroute** command from the Cisco devices. You will also examine the options that are available for fine tuning the traceroute results.

Step 1: Use the tracert command from PC-A to EXTERNAL.

a. At the command prompt, type **tracert 209.165.200.226.**

```
C:\> tracert 209.165.200.226
Tracing route to EXTERNAL [209.165.200.226]
Over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2     1 ms    <1 ms    <1 ms    64.100.0.1
  3     1 ms    <1 ms    <1 ms    [209.165.200.226]

Trace complete.
```

The tracert results indicates the path from PC-A to EXTERNAL is from PC-A to R1 to ISP to EXTERNAL. The path to EXTERNAL traveled through two router hops to the final destination of EXTERNAL.

Step 2: Explore additional options for the tracert command.

a. At the command prompt, type **tracert** and press Enter to see the available options.

```
C:\> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

b. Use the **-d** option. Notice that the IP address of 209.165.200.226 is not resolved as EXTERNAL.

```
C:\> tracert –d 209.165.200.226
Tracing route to 209.165.200.226 over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2     1 ms    <1 ms    <1 ms    64.100.0.1
  3     1 ms    <1 ms    <1 ms    209.165.200.226

Trace complete.
```

Step 3: Use the traceroute command from the R1 router to External.

At the command prompt, type **traceroute 209.165.200.226** or **traceroute 2001:db8:acad:200::226** on the R1 router. The hostnames are resolved because a local IP host table was configured on the R1 router.

```
R1# traceroute 209.165.200.226
Type escape sequence to abort.
Tracing the route to Externalv4 (209.165.200.226)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISPv4 (64.100.0.1) 1 msec 1 msec 1 msec
  2 Externalv4 (209.165.200.226) 1 msec 1 msec 1 msec

R1# traceroute 2001:db8:acad:200::226
Type escape sequence to abort.
Tracing the route to EXTERNAL (2001:DB8:ACAD:200::226)

  1 ISPv6 (2001:DB8:ACAD::1) 8 msec 1 msec 1 msec
  2 Externalv6 (2001:DB8:ACAD:200::226) 0 msec 0 msec 0 msec
```

Step 4: Use the traceroute command from the S1 switch to External.

On the S1 switch, type **traceroute 209.165.200.226** or **traceroute 2001:db8:acad:200::226**. The hostnames are not displayed in the traceroute results because a local IP host table was not configured on this switch

```
S1# traceroute 209.165.200.226
Type escape sequence to abort.
Tracing the route to 209.165.200.226

  1 192.168.1.1 0 msec 0 msec 0 msec
  2 64.100.0.1 8 msec 0 msec 0 msec
  3 209.165.200.226 0 msec *  0 msec

S1# traceroute 2001:db8:acad:200::226
Type escape sequence to abort.
Tracing the route to 2001:DB8:ACAD:200::226

  1 2001:DB8:ACAD:1::1 0 msec 0 msec 0 msec
  2 2001:DB8:ACAD::1 8 msec 0 msec 0 msec
  3 2001:DB8:ACAD:200::226 0 msec 0 msec 0 msec
```

The **traceroute** command has additional options. You can use the ? or just press Enter after typing **traceroute** at the prompt to explore these options.

The following link provides more information regarding the ping and traceroute commands for a Cisco device:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Part 4: Troubleshoot the Topology

Step 1: Copy and paste the following configuration into the ISP router.

```
hostname ISP
interface g0/0/0
 ip address 64.100.0.1 255.255.255.252
 ipv6 address 2001:db8:acad::1/64
 no shutdown
interface g0/0/1
 ip address 192.168.8.1 255.255.255.0
 no ipv6 address 2001:db8:acad:200::225/64
 ipv6 address 2001:db8:acad:201::225/64
 no shutdown
end
```

Step 2: From the R1 network, use ping and tracert or traceroute commands to troubleshoot and correct the problem on the ISP network.

a. Use the **ping** and **tracert** commands from PC-A.

You can use the **tracert** command to determine end-to-end network connectivity. This tracert result indicates that PC-A can reach its default gateway of 192.168.1.1, but PC-A does not have network connectivity with External.

```
C:\> tracert 209.165.200.226

Tracing route to 209.165.200.226 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    <1 ms    <1 ms    <1 ms  64.100.0.1
  3  64.100.0.1  reports: Destination host unreachable.

Trace complete.
```

One way to locate the network issue is to ping each hop in the network to EXTERNAL. First determine if PC-A can reach the ISP router g0/0/0 interface with an IP address of 64.100.0.1.

```
C:\> ping 64.100.0.1
```

b. PC-A can reach the ISP router. Based on the successful ping results from PC-A to the ISP router, the network connectivity issue is with 209.165.200.224/24 network. Ping the default gateway to External, which is the GigabitEthernet 0/0/1 interface of the ISP router.

```
C:\> ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

PC-A cannot reach the GigabitEthernet 0/0/1 interface of the ISP router, as displayed by the results from the **ping** command.

The tracert and ping results conclude that PC-A can reach the R1 and ISP routers, but not the External or default gateway for External.

c. Use the **show** commands to examine the running configurations for the ISP router

```
ISP# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   64.100.0.1      YES manual up                    up
GigabitEthernet0/0/1   192.168.8.1     YES manual up                    up
Serial0/1/0            unassigned      YES unset  up                    up
Serial0/1/1            unassigned      YES unset  up                    up
GigabitEthernet0       unassigned      YES unset  down                  down

ISP# show run

interface GigabitEthernet0/0/0
 ip address 64.100.0.1 255.255.255.252
 negotiation auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD::1/64
!
interface GigabitEthernet0/0/1
 ip address 192.168.8.1 255.255.255.0
 negotiation auto
 ipv6 address FE80::225 link-local
 ipv6 address 2001:DB8:ACAD:201::225/64
!
interface Serial0/1/0
 no ip address
!
interface Serial0/1/1
 no ip address
<output omitted>
```

The outputs of the **show run** and **show ip interface brief** commands indicate that the GigabitEthernet 0/0/1 interface is up/up, but was configured with an incorrect IP address.

d. Correct the found issues.

```
ISP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)# interface GigabitEthernet 0/0/1
ISP(config-if)# no ip address 192.168.8.1 255.255.255.0
ISP(config-if)# ip address 209.165.200.225 255.255.255.224
```

e. Verify that PC-A can ping and tracert to EXTERNAL.

```
C:\> ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:
Reply from 209.165.200.226: bytes=32 time=44ms TTL=126
Reply from 209.165.200.226: bytes=32 time=41ms TTL=126
Reply from 209.165.200.226: bytes=32 time=40ms TTL=126
Reply from 209.165.200.226: bytes=32 time=41ms TTL=126

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\> tracert 209.165.200.226

Tracing route to EXTERNAL [209.165.200.226]
Over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2     1 ms    <1 ms    <1 ms    64.100.0.1
  3     1 ms    <1 ms    <1 ms     [209.165.200.226]
Trace complete.
```

Note: This can also be accomplished using **ping** and **traceroute** commands from the CLI on the ISP router and the S1 switch after verifying that there are no network connectivity issues on the 192.168.1.0/24 network.

f. Now repeat the process for IPv6 connectivity. **Note**: If you find an incorrect IPv6 address, you will need to remove it because it is not replaced by a new ipv6 address command

Reflection Questions

1. What could prevent ping or traceroute responses from reaching the originating device beside network connectivity issues?
Firewall on the PCs, access lists command, routing issues, interface is down, network delay

2. If you ping a non-existent address on the remote network, such as 209.165.200.227, what is the message displayed by the **ping** command? What does this mean? If you ping a valid host address and receive this response, what should you check?
Request timed out or periods (.). This means that there was no response in the default time period. Some of the items you may check: router is down, destination host is down, return route to your device and latency of the response is not more than the default time period

3. If you ping an address that does not exist in any network in your topology, such as 192.168.5.3, from a Windows-based PC, what is the message displayed by the **ping** command? What does this message indicate?
Destination host unreachable. This message indicates that there is no route to the destination as the network is not listed by the routing table.

4. What is the IPv4 TTL value set on the Windows host? What is the IPv4 TTL value set on a Cisco device?
Windows sets the TTL value to 128 and the Cisco device will set the TTL value to 255.

5. What is the IPv6 Hop Limit value set on the Windows host? What is the IPv6 Hop Limit value set on a Cisco device?
Windows sets the TTL value to 128, which is the same as IPv4 TTL value and the Cisco device will set the TTL value to 64.

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs

Router R1

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

Current configuration : 1806 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip host Externalv4 209.165.200.226
ip host Externalv6 2001:DB8:ACAD:200::226
ip host ISPv4 64.100.0.1
ip host ISPv6 2001:DB8:ACAD::1
ip host PC-Av4 192.168.1.10
ip host PC-Av6 2001:DB8:ACAD:1::10
ip host S1v4 192.168.1.2
ip host S1v6 2001:DB8:ACAD:1::2
no ip domain lookup
!
login on-success log
!
subscriber templating
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
 mode none
!
interface GigabitEthernet0/0/0
 ip address 64.100.0.2 255.255.255.252
 ip nat outside
 negotiation auto
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD::2/64
!
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
```

```
 ip nat inside
 negotiation auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Serial0/1/0
 no ip address
!
interface Serial0/1/1
 no ip address
!
ip nat inside source list 1 interface GigabitEthernet0/0/0 overload
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 64.100.0.1
!
access-list 1 permit 192.168.1.0 0.0.0.255
ipv6 route ::/0 2001:DB8:ACAD::1
!
control-plane
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

Router ISP

```
ISP# show run
Building configuration...

Current configuration : 1337 bytes
!
version 16.9
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
no ip domain lookup
!
login on-success log
!
subscriber templating
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
 mode none
!
interface GigabitEthernet0/0/0
 ip address 64.100.0.1 255.255.255.252
 negotiation auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD::1/64
!
interface GigabitEthernet0/0/1
 ip address 209.165.200.225 255.255.255.224
 negotiation auto
 ipv6 address FE80::225 link-local
 ipv6 address 2001:DB8:ACAD:200::225/64
!
interface Serial0/1/0
 no ip address
!
interface Serial0/1/1
 no ip address
```

```
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
ipv6 route 2001:db8:acad:1::/64 2001:db8:acad::2
!
control-plane
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end
```

Switch S1

```
S1# show run brief
Building configuration...

Current configuration : 1699 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
no ip domain-lookup
!
crypto pki trustpoint TP-self-signed-3822041216
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3822041216
 revocation-check none
 rsakeypair TP-self-signed-3822041216
!
crypto pki certificate chain TP-self-signed-3822041216
 certificate self-signed 01
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
```

```
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:ACAD:1::2/64
!
ip default-gateway 192.168.1.1
ip classless
ip http server
ip http secure-server
!
line con 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
!
end
```