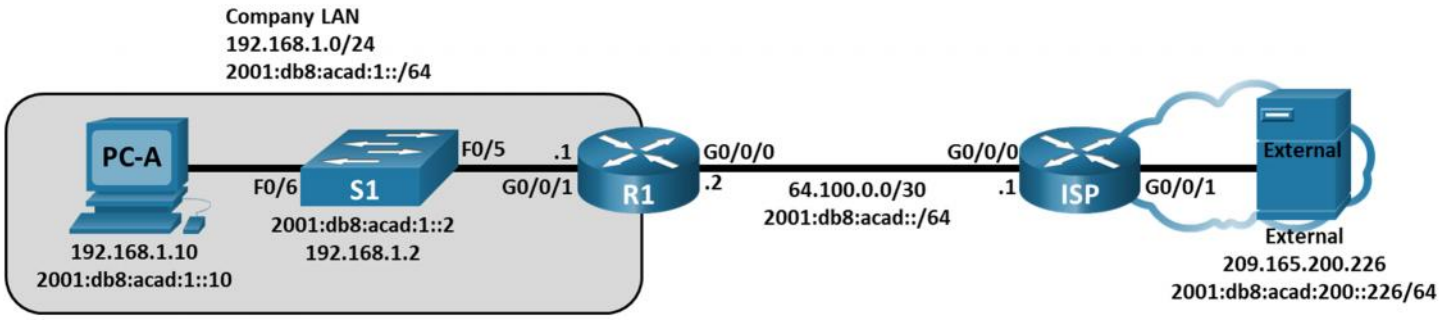
Lab 13.3.2 - Use Ping and Traceroute to Test Network Connectivity

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

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::1	
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::225	
ISP	G0/0/1	209.165.200.225 /27	N/A
		2001:db8:acad:200::225 /64	
		fe80::225	
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
		192.168.1.10 /24	192.168.1.1

Device	Interface	IP Address / Prefix	Default Gateway
External	NIC	209.165.200.226 /27	209.165.200.225
		2001:DB8:ACAD:200::226 /64	FE80::225

Objectives

Part 1: 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.

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
```

Instructions

Part 1: Configure the Network

In Part 1, you will 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: Configure PC IP addresses and default gateways according to the Addressing Table.

Step 2: Configure the S1 switch using the initial configurations provided below.

At the switch global configuration mode prompt, copy and paste the configuration. Save the configuration to the startup-config.

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::10 link-local
 no shutdown
 exit
ip default-gateway 192.168.1.1
end
```

Step 3: 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 into the global configuration mode prompt. 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	0	128
2001:db8:acad:1::10	0	128
192.168.1.1 (R1)	0	255
2001:db8:acad:1::1 (R1)	1	64
192.168.1.2 (S1)	1	255
2001:db8:acad:1::2(S1)	1	64

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
64.100.0.2 (R1)	1	255
2001:DB8:ACAD::2 (R1)	0	64
64.100.0.1 (ISP)	0	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)	0	126

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
```

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

```
C:\Users\User1> ping –t 209.165.200.226
```

To illustrate the results when a host is unreachable, shut down the GigabitEthernet 0/0/1 interface on the ISP router.

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. 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.

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?

Type your answers here.

"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?

Type your answers here.

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, shut down the GigabitEthernet 0/0/1 interface on the ISP router.

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:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.U.U.U.U.U.
U.U.............!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
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
```

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
```

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
```

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
```

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

R1# traceroute 2001:db8:acad:200::226
```

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

S1# traceroute 2001:db8:acad:200::226
```

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.

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.

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.

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.

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.

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

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?

Router issues, misconfigurations, firewalls, down interfaces, powered-off equipment

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?

Pinging the non-existent address will result in a "Request timed out" message or periods. Either message means that host did not receive a response from the host that is getting pinged. If when pinging a valid host and the message is received, check to see if any devices are down first, if that is not the issue, then check the configuration.

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?

The message displayed is "Destination host unreachable" and it means that there is no route to the destination within 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?

The TTL value on a Windows host is 128 while the TTL value for a Cisco host is 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?

The hop limit on a Windows host is 128 while the hop limit for a Cisco host is 64.

Router and Switch Interface Summary Table

Router / Switch 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)
2960	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3560	Fast Ethernet 0/1 (F0/1)	Fast Ethernet 0/2 (F0/2)	n/a	n/a
3650	Gigabit Ethernet 1/0/1 (G1/0/1)	Gigabit Ethernet 1/0/2 (G1/0/2)	n/a	n/a
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.