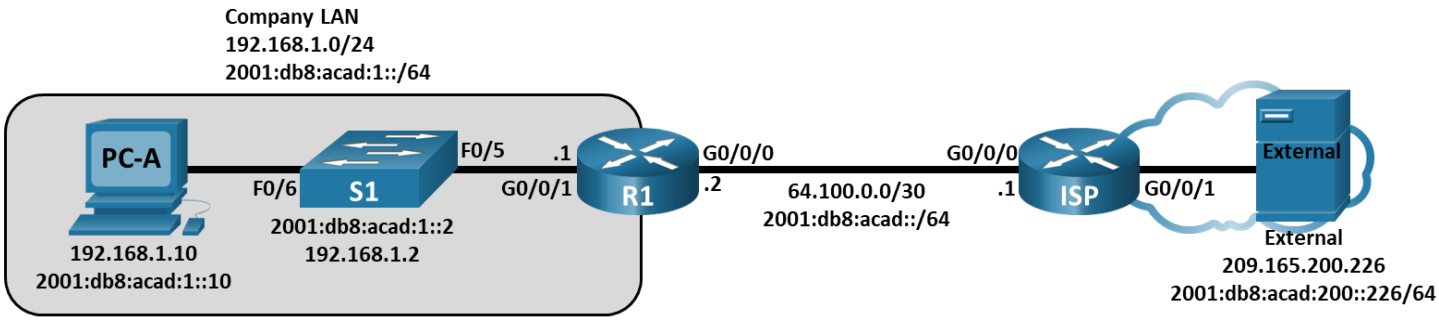
Packet Tracer - Use Ping and Traceroute to Test Network Connectivity - Physical Mode

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	
	G0/0/1	192.168.1.1 /24	
		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	
	G0/0/1	209.165.200.225 /27	
		2001:db8:acad:200::225 /64	
		fe80::225	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
		2001:db8:acad:1::2 /64	fe80::1
		fe80::2	
PC-A	NIC	2001:db8:acad:1::10 /64	fe80::1
		192.168.1.10 /24	192.168.1.1
External	NIC	209.165.200.226 /27	209.165.200.225

Device	Interface	IP Address / Prefix	Default Gateway
		2001:db8:acad:200::226 /64	fe80::225

Objectives

Part 1: Use Ping Command for Basic Network Testing

Part 2: Use Tracert and Traceroute Commands for Basic Network Testing

Part 3: Troubleshoot the Topology

Background / Scenario

Ping and traceroute are two tools that are critical when testing TCP/IP network connectivity. Ping is a network administration utility that is used to test the reachability of a device on an IP network. This utility also measures the time it takes for messages that are sent from the originating host to a destination host and back again.

The traceroute utility is a network diagnostic tool for displaying the path or route of a packet, and for measuring the transit delays of packets travelling over an IP network.

In this Packet Tracer Physical Mode (PTPM) activity, 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 activity for command exploration. The available options for the **ping** and **tracert** commands are limited in Packet Tracer. The necessary Cisco device configurations are provided in this activity.

Instructions

Part 1: Use the Ping Command for Basic Network Testing

In this part of the activity, 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. IPv4 packets use an 8 bit Time to Live (TTL). IPv6 packets use a Hop Limit header field value. The TTL and the Hop Limit specify the maximum number of Layer 3 hops that can be traversed on the path to their destination. Each host on a network will set the 8 bit value with a maximum value of 255.

Each time an IP packet arrives at a Layer 3 network device, this value is reduced by one before it is forwarded to the destination. If this value eventually reaches zero before reaching the destination, the IP packet is discarded.

You will examine the results of the **ping** command and the additional ping options that are available in Packet Tracer PCs and Cisco devices.

Step 1: Test network connectivity to R1 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. From **PC-A**, ping the default gateway using the IPv4 address (GigabitEthernet 0/0/1 interface of R1).

```
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 ICMP requests that have 32 bytes each, were sent. 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 destination.

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

```
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: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:1::1: bytes=32 time<1ms TTL=255

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 = 0ms, Maximum = 0ms, Average = 0ms
```

b. From **PC-A**, ping the addresses listed in the following table and record the average round trip time and IPv4 TTL, or IPv6 Hop Limit.

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
192.168.1.10		
2001:db8:acad:1::10		
192.168.1.1 (R1)		
2001:db8:acad:1::1 (R1)		
192.168.1.2 (S1)		
2001:db8:acad:1::2(S1)		
64.100.0.2 (R1)		
2001:db8:acad::2 (R1)		
64.100.0.1 (ISP)		
2001:db8:acad::1 (ISP)		
209.165.200.225 (ISP G0/0/1)		
2001:db8:acad:200::225 (ISP G0/0/1)		

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
209.165.200.226 (External)		
2001:db8:acad:200::226 (External)		

Step 2: Perform pings from S1 to External.

From **S1**, attempt to ping **ISP** and **External** using IPv4 and IPv6 addresses.

What are the ping results from S1 to ISP and External?

Part 2: 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 destination. The **traceroute** command uses the User Datagram Protocol (UDP) datagrams for tracing routes to the destination for Cisco devices and other Unix-like PCs.

In this part, you will examine the traceroute commands and determine the path that a packet travels to the destination. You will use the **tracert** command from the 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: From PC-A, use the tracert command to External.

a. At the command prompt of **PC-A**, type **tracert 209.165.200.226**.

```
C:\> tracert 209.165.200.226

Tracing route to 209.165.200.226 over a maximum of 30 hops:

  1    *      *       1 ms    192.168.1.1
  2    *      0 ms    0 ms    64.100.0.1
  3    0 ms   *       0 ms    64.100.0.1
  4    *      11 ms   *       Request timed out.
  5    0 ms   *       0 ms    64.100.0.1
Control-C
^C
C:\>
```

Note: You can stop the trace route by pressing **Ctrl-C**.

The **tracert** result indicates the path from PC-A to External is from PC-A to R1 to ISP and is unable to arrive at External. The tracert results indicate an issue at the ISP router.

b. Repeat the tracert command using the IPv6 address. At the command prompt, enter **tracert 2001:db8:acad:200::226**.

Step 2: From S1, use the traceroute command to External.

From **S1**, type **traceroute 209.165.200.226** or **traceroute 2001:db8:acad:200::226**.

Note: To stop the traceroute, press **Ctrl-Shift-6**.

```
S1# traceroute 209.165.200.226
```

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

Note: The available options are limited in Packet Tracer.

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 3: Correct the network connectivity issue at ISP.

Step 1: Access the network location where the connectivity issue is occurring.

From the previous steps, you had determined that there is an issue at the ISP router using the **ping** and **traceroute** commands. You have remote SSH access to all the network devices using username **admin** and password **class**.

a. From the terminal of **S1**, SSH into the ISP router using the G0/0/0 interface to correct the problem.

```
C:\> ssh -l admin 64.100.0.1
```

b. 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 that it is configured with an incorrect IP address.

c. Correct the issues you found. From the command prompt on **PC-A**, copy and paste the following configuration into the ISP router to correct the issue in the SSH session to the ISP router.

```
configure terminal
interface g0/0/1
 no ip address 192.168.8.1 255.255.255.0
 ip address 209.165.200.225 255.255.255.224
 no ipv6 address 2001:db8:acad:201::225/64
 ipv6 address 2001:db8:acad:200::225/64
 ipv6 address fe80::225 link-local
no shutdown
```

d. Exit the SSH session when finished.

Step 2: Verify end-to-end connectivity.

From the **PC-A** command prompt, use the **ping** and **tracert** commands to verify end-to-end connectivity to the external server at 209.165.200.226 and 2001:db8:acad:200::226.

Part 4: Use Extended Ping Commands

Step 1: Use extended ping commands on PC-A.

The default **ping** command sends four requests of 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. The **-t** option will continuously ping the target until stopped. Use **Ctrl+c** to stop the ping sequence.

```
C:\> ping –t 209.165.200.226
```

c. To illustrate the results when a host is unreachable, shut down the GigabitEthernet 0/0/1 interface on the ISP router. From switch S1, SSH to the ISP G0/0/0 interface. Use the password **class**.

```
S1# ssh -l admin 64.100.0.1
```

d. Use the **shutdown** command to disable the GigabitEthernet 0/0/1 interface on the ISP router. command.

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.

e. Re-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.

f. Press **Ctrl**+**c** to stop the ping command.

g. The above steps can be repeated for the IPv6 address to obtain an ICMP error message.

What ICMP error messages did you receive?

h. 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 2: 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 R1 and S1.

a. From **R1**, ping External on the external network using the IP address of 209.165.200.226.

```
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 R1 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 R1, you can ping Externalv4 on the external network using the hostname configured from R1.

```
R1# ping Externalv4
```

What is the IP address used?

c. In the privileged EXEC mode, there are more options available for the **ping** command. At the command line, 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 where there is a network issue. Start the **ping** command to 209.165.200.226 with a repeat count of 50000. Then, shut down the GigabitEthernet 0/0/1 interface on the ISP router.

From the SSH session to ISP on switch **S1**, disable the GigabitEthernet 0/0/1 interface on ISP.

e. From the SSH session, enable the GigabitEthernet 0/0/1 interface on ISP 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.

```
R1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]: 50000
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 PDU was received by R1. 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.

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

f. In the PT activity window, click **Check Results** to verify all the assessment items and connectivity tests are correct.

Reflection Questions

1. What could prevent ping or traceroute responses from reaching the originating device beside network connectivity issues?

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?

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?