**Computer Networks**

**Problem-solving session: Use Ping and Traceroute to Test Network Connectivity**

**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

**Background**

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 1:** The switch Cisco Catalyst 2960 and the router Cisco 4321 are employed in this work.

**Note 2:** 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

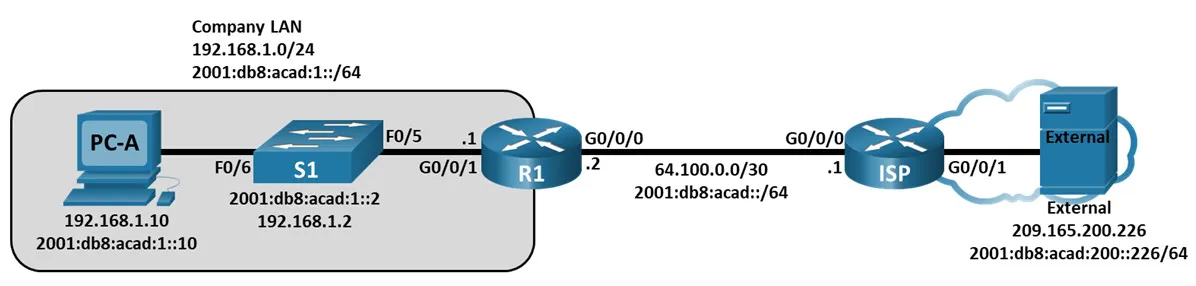
Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

S1# configure terminal

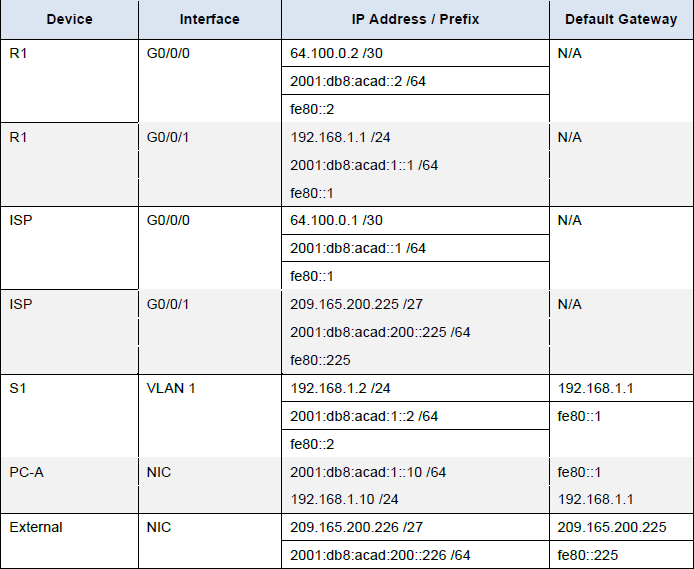
S1(config)# **sdm prefer dual-ipv4-and-ipv6 default**

S1(config)# end

S1# reload



Address table:



**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 then reload the devices.

**Step 3:** On the computer PC-A and the server External,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

ip route 0.0.0.0 0.0.0.0 64.100.0.2

ipv6 route ::/0 2001:db8:acad::2

**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

ipv6 host Externalv6 2001:db8:acad:200::226

ip host ISPv4 64.100.0.1

ipv6 host ISPv6 2001:db8:acad::1

ip host PC-Av4 192.168.1.10

ipv6 host PC-Av6 2001:db8:acad:1::10

ip host R1v4 64.100.0.2

ipv6 host R1v6 2001:db8:acad::2

ip host S1v4 192.168.1.2

ipv6 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.

| **Destination** | **Average Round Trip Time (ms)** |
| --- | --- |
| 192.168.1.10 | 9 |
| 2001:db8:acad:1::10 | 4 |
| 192.168.1.1 (R1) | 0 |
| 2001:db8:acad:1::1 (R1) | 0 |
| 192.168.1.2 (S1) | 0 |
| 2001:db8:acad:1::2(S1) | 504 |
| 64.100.0.2 (R1) | 2 |
| 2001:DB8:ACAD::2 (R1) | 0 |
| 64.100.0.1 (ISP) | 0 |
| 2001:DB8:ACAD::1 (ISP) | 5 |
| 209.165.200.225 (ISP G0/0/1) | unreachable |
| 2001:DB8:ACAD:200::225 (ISP G0/0/1) | unreachable |
| 209.165.200.226 (External) | 0 |
| 2001:DB8:ACAD:200::226 (External) | 0 |

**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.

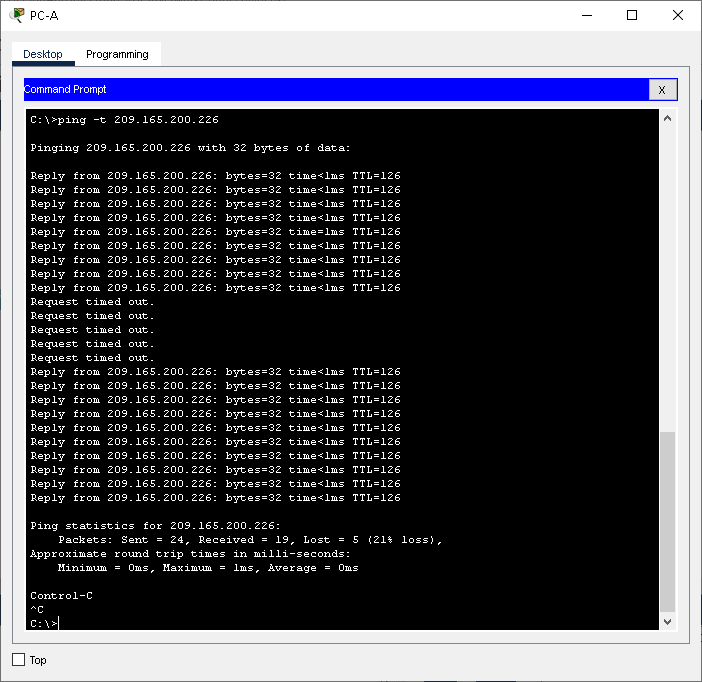
C:\Users\User1> ping -t 209.165.200.226

To illustrate the results when a host is unreachable, disconnect the cable between the ISP router and External, or 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. 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.

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



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

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.

R1# ping Externalv4

What is the IP address used?

Ans: 209.165.200.226

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

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 10000. 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:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

<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** result indicates the that 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

**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

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