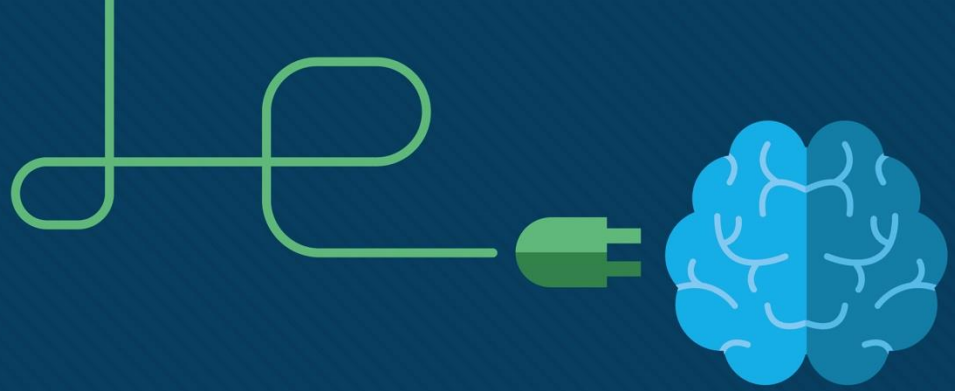
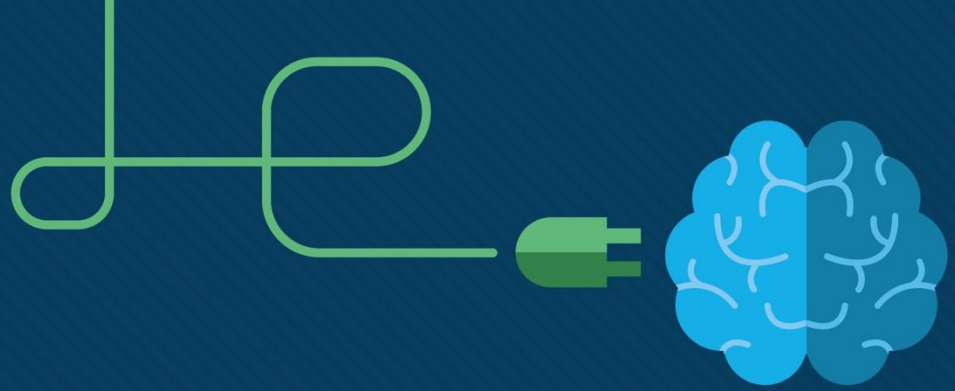


# Module 7: Connectivity Verification

## Instructor Materials

CyberOps Associate v1.0



# Module 7: Connectivity Verification

CyberOps Associate v1.0

# Module Objectives

**Module Title:** Connectivity Verification

**Module Objective:** Use ICMP connectivity verification tools

| Topic Title | Topic Objective |
|---|---|
| **ICMP** | Explain how ICMP is used to test network connectivity. |
| **Ping and Traceroute Utilities** | Use Windows tools, ping, and traceroute to verify network connectivity. |

# 7.1 ICMP

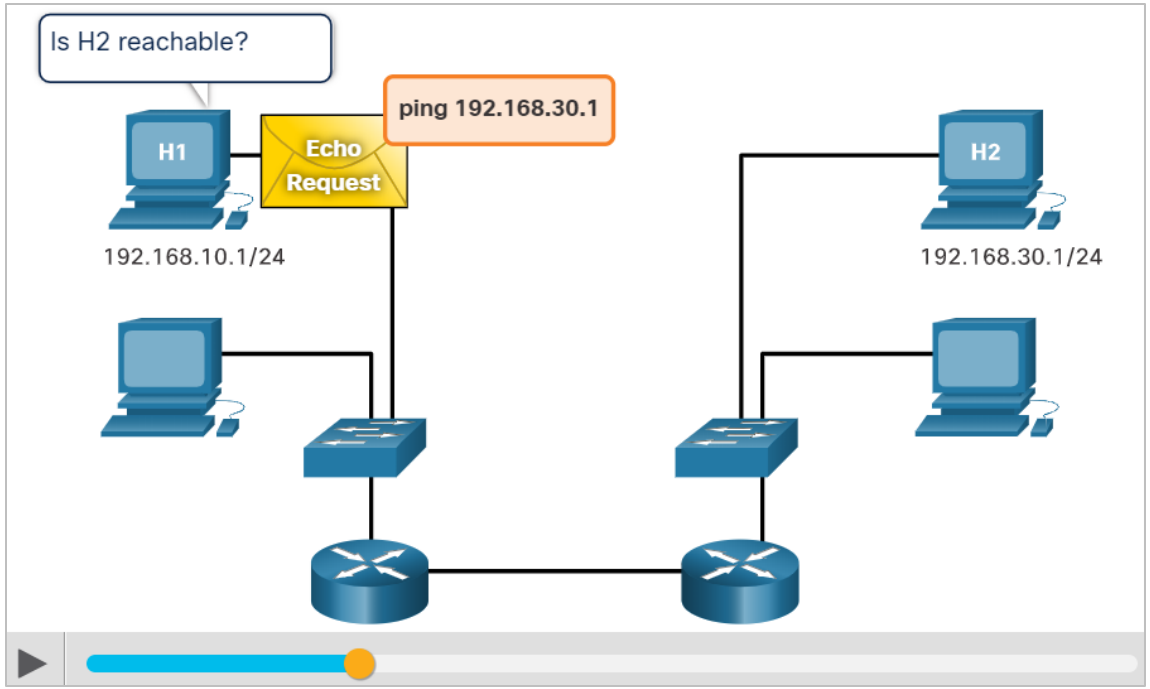
# ICMPv4 Messages

- The TCP/IP suite provide messages to be sent in the event of certain errors. These messages are sent using the services of ICMP.
- The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions.
- ICMP messages are not required and are often not allowed within a network for security reasons.
- ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides the same services for IPv6 but includes additional functionality.
- ICMP messages common to both ICMPv4 and ICMPv6 include host confirmation, destination or service unreachable, time exceeded and route redirection.

# ICMPv4 Messages (Contd.)

## Host Confirmation

- An ICMP Echo Message can be used to determine if a host is operational.
- The local host sends an ICMP Echo Request to a host. If the host is available, the destination host responds with an Echo Reply.
- This use of the ICMP Echo messages is the basis of the ping utility.



# ICMPv4 Messages (Contd.)

## Destination or Service Unreachable

- When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable.
- The message will include a code that indicates why the packet could not be delivered. The Destination Unreachable codes for ICMPv4 includes the following:
  - **0 -** Net unreachable
  - **1 -** Host unreachable
  - **2 -** Protocol unreachable
  - **3 -** Port unreachable

***Note:*** *ICMPv6 has slightly different codes for Destination Unreachable messages.*

# ICMPv4 Messages (Contd.)

## Time Exceeded

- An ICMPv4 Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the Time to Live (TTL) field of the packet was decremented to 0.
- If a router receives a packet and decrements the TTL field in the IPv4 packet to zero, it discards the packet and sends a Time Exceeded message to the source host.
- ICMPv6 also sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired.
- IPv6 does not have a TTL field. It uses the hop limit field to determine if the packet has expired.

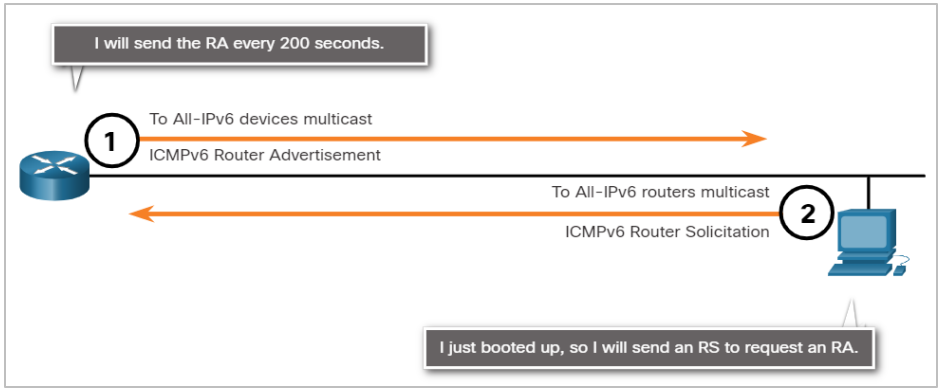
# ICMPv6 RS and RA Messages

- ICMPv6 has new features and improved functionality not found in ICMPv4. ICMPv6 messages are encapsulated in IPv6.
- It has four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).
- Messaging between an IPv6 router and an IPv6 device:
  - Router Solicitation (RS) message
  - Router Advertisement (RA) message
- Messaging between IPv6 devices:
  - Neighbor Solicitation (NS) message
  - Neighbor Advertisement (NA) message

# ICMPv6 RS and RA Messages (Contd.)

## Router Solicitation: Messaging Between an IPv6 Router and an IPv6 Device

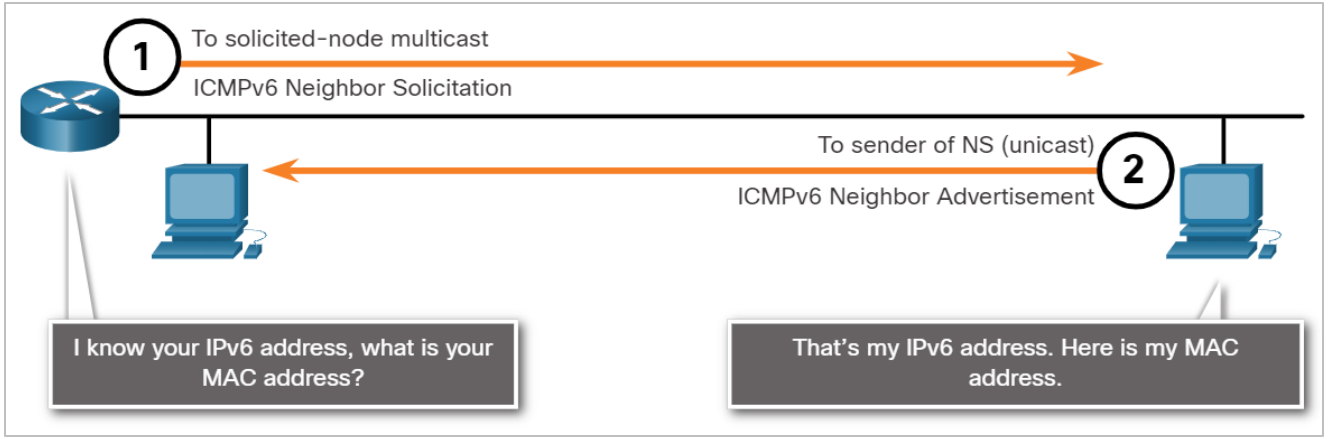
- RA messages are sent by routers to provide addressing information to hosts using Stateless Address Auto Configuration (SLAAC).
- A router will send an RA message periodically or in response to an RS message. A host using SLAAC will set its default gateway to the link-local address of the router that sent the RA.
- When a host is configured to obtain its addressing information automatically using SLAAC, the host will send an RS message to the router requesting an RA message.



# ICMPv6 RS and RA Messages (Contd.)

## Address Resolution: Messaging Between IPv6 Devices

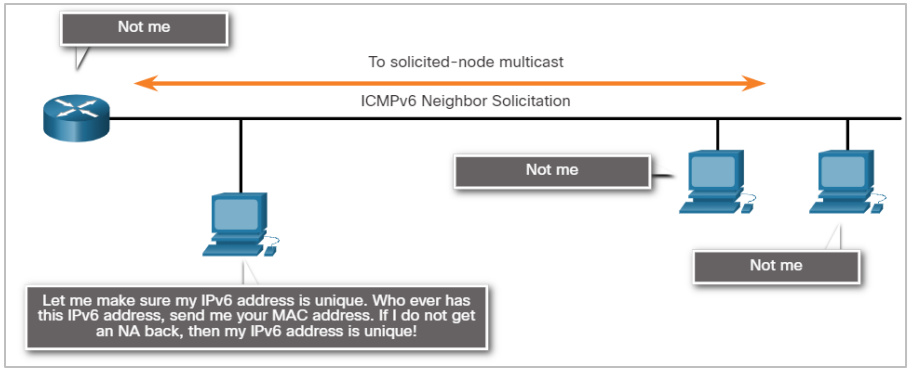
- NA messages are sent when a device knows the IPv6 address of a device but does not know its MAC address. This is equivalent to an ARP Request for IPv4.
- NA messages are sent in response to an NS message and match the target IPv6 address in the NS. The NA message includes the device's Ethernet MAC address. This is equivalent to an ARP Reply in IPv4.



# ICMPv6 RS and RA Messages (Contd.)

## Duplicate Address Detection (DAD)

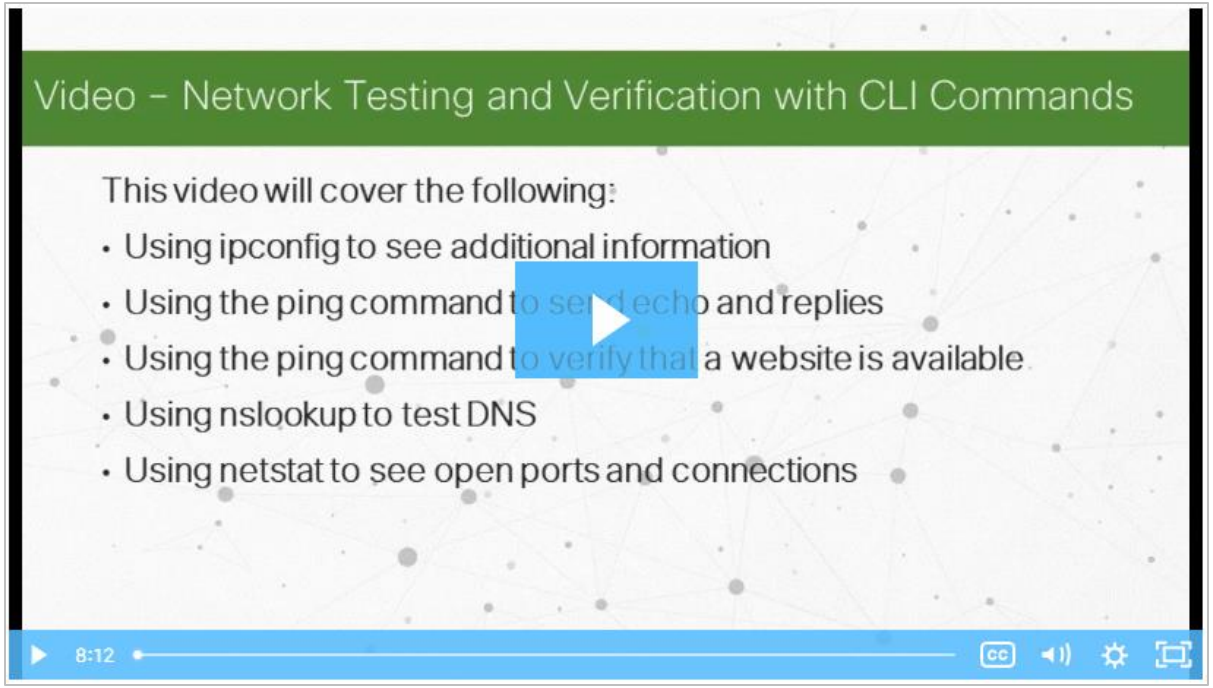
- When a device is assigned a global unicast or link-local unicast address, the DAD is performed on the address to ensure that it is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address.
- If another device on the network has this address, it will respond with an NA message which will notify the sending device that the address is in use. If a corresponding NA message is not returned within a certain period of time, the unicast address is unique and acceptable for use.



# 7.2 Ping and Traceroute Utilities

# Video - Network Testing and Verification with Windows CLI Commands

This video will demonstrate the Network Testing and Verification with Windows CLI Commands.



# Ping – Test Connectivity

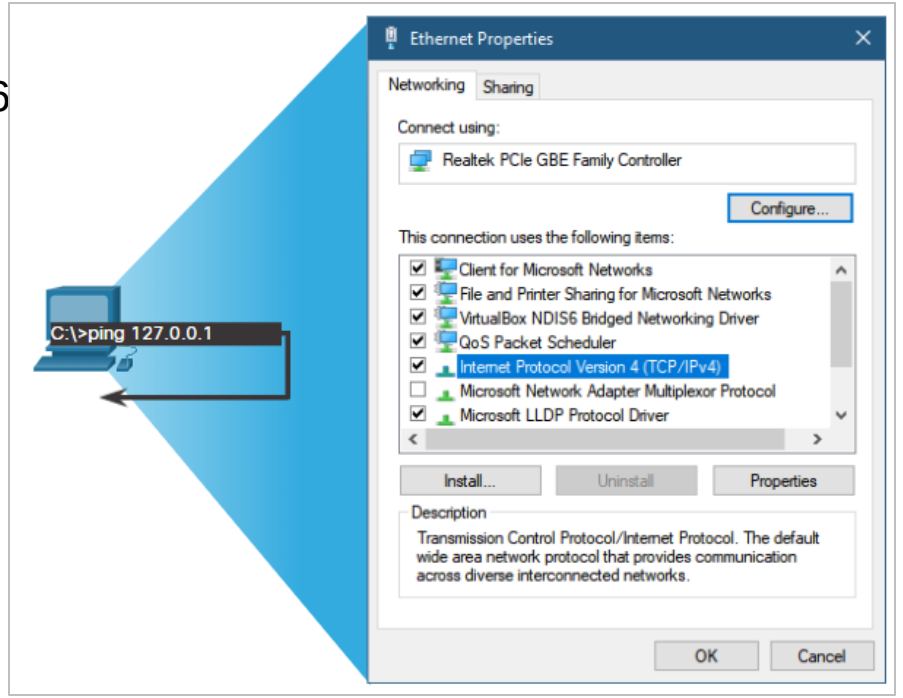
- Ping is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts.
- To test connectivity to another host on a network, an echo request is sent to the host address using the **ping** command. If the host at the specified address receives the echo request, it responds with an echo reply.
- As each echo reply is received, **ping** provides feedback on the time between when the request was sent and when the reply was received. This can be a measure of network performance.
- Ping has a timeout value for the reply. If a reply is not received within the timeout, ping provides a message indicating that a response was not received.

# Ping – Test Connectivity (Contd.)

- After all the requests are sent, the **ping** utility provides a summary that includes the success rate and average round-trip time to the destination.
- Type of connectivity tests performed with **ping** include the following:
  - Pinging the local loopback
  - Pinging the default gateway
  - Pinging the remote host

# Ping the Loopback

- Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host.
- To perform this test, **ping** the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).
- A response from 127.0.0.1 for IPv4, or ::1 for IPv6 indicates that IP is properly installed on the host. This response comes from the network layer.
- This response tests IP down through the network layer of IP.
- An error message indicates that TCP/IP is not operational on the host.
- Pinging the local host confirms that TCP/IP is installed and working on the local host.
- Pinging 127.0.0.1 causes a device to ping itself.

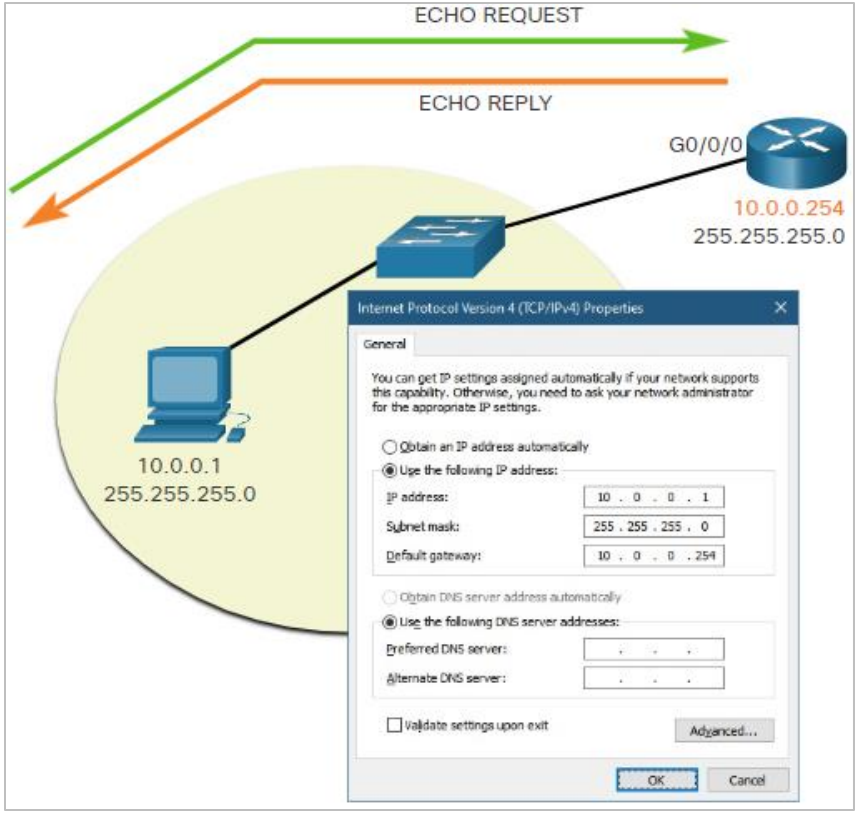


# Ping the Default Gateway

- The **ping** can be used to test the ability of a host to communicate on the local network. This is done by pinging the IP address of the default gateway of the host.
- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- For this test, the default gateway address is mostly used as the router is always operational. If the default gateway address does not respond, a **ping** can be sent to the IP address of another host on the local network that is operational.
- If either the default gateway or another host responds, then the local host can successfully communicate over the local network.
- If the default gateway does not respond but another host does, this could indicate a problem with the router interface serving as the default gateway.
- One possibility is that the wrong default gateway address been configured on the host or the router interface may be fully operational but have security applied to it.

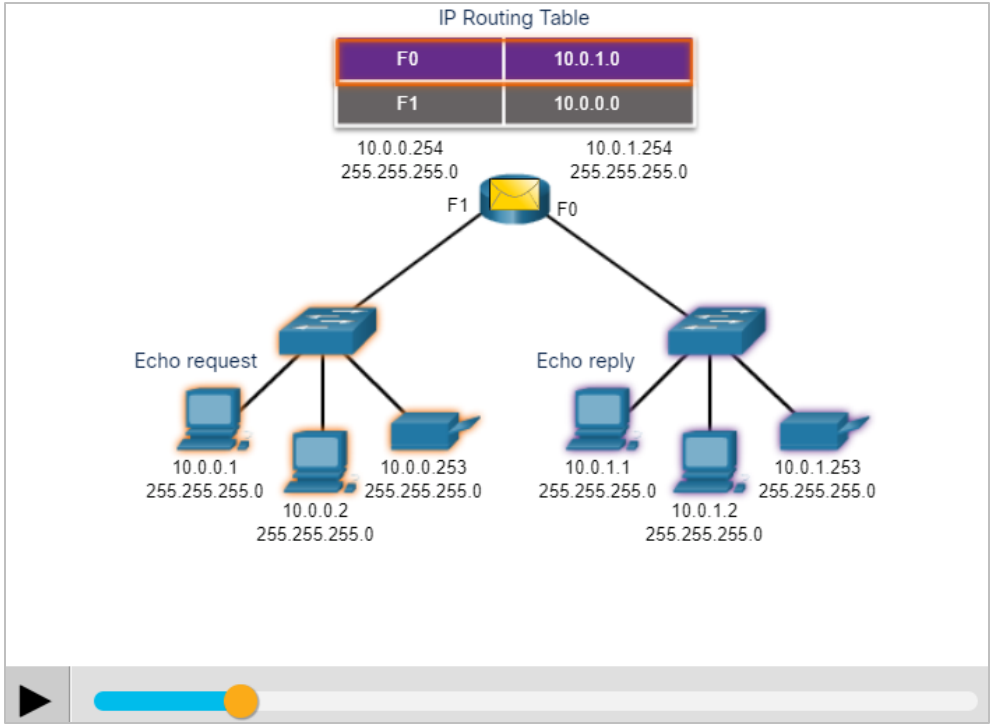
# Ping the Default Gateway (Contd.)

The host pings its default gateway, sending an ICMP echo request. The default gateway sends an echo reply confirming connectivity.



# Ping a Remote Host

- Ping can also be used to test the ability of a local host to communicate across an internetwork. The local host can ping an operational IPv4 host of a remote network.
- The router uses its IP routing table to forward the packets.
- If this ping is successful, the operation of a large piece of the internetwork and the functionality of the remote host can be verified.
- A successful **ping** across the network confirms communication on the local network, the operation of the router as the default gateway, and the operation of all other routers in the path between the local network and the network of the remote host.



# Traceroute - Test the Path

- Ping is used to test connectivity between two hosts but does not provide information about the details of devices between the hosts.
- Traceroute (**tracert**) is a utility that generates a list of hops that were successfully reached along the path. This list can provide important verification and troubleshooting information.
- If the data reaches the destination, then the trace lists the interface of every router in the path between the hosts.
- If the data fails at some hop along the way, the address of the last router that responded to the trace can provide an indication of where the problem or security restrictions are found.

# Traceroute - Test the Path (Contd.)

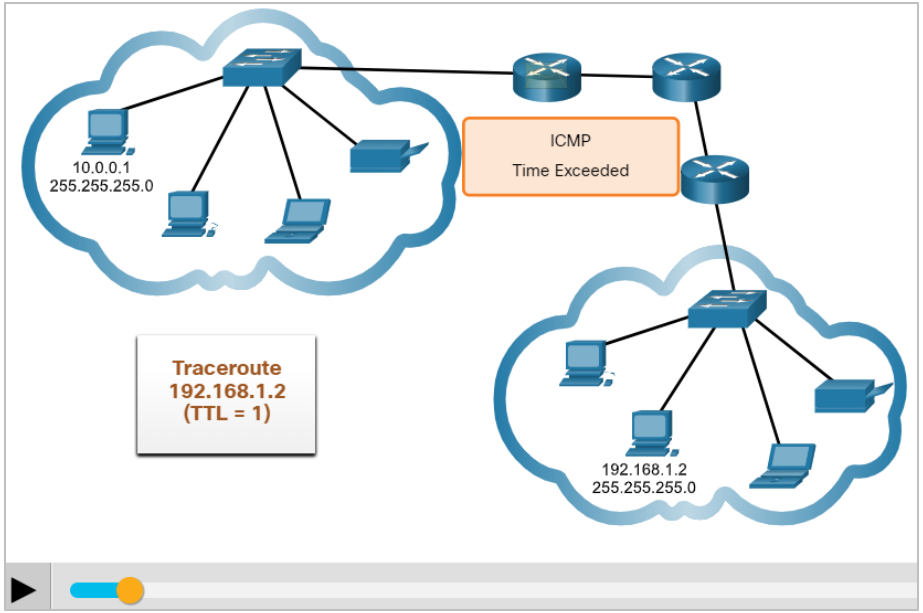
**Round Trip Time (RTT)**

- The traceroute provides a round-trip time for each hop along the path and indicates if a hop fails to respond.
- The round-trip time is the time a packet takes to reach the remote host and for the response from the host to return.
- An asterisk (*) is used to indicate a lost or unreplied packet.
- This information can be used to locate a problematic router in the path or may indicate that the router is configured not to reply.
- If the display shows high response times or data losses from a particular hop, this is an indication that the resources of the router or its connections may be overused.

# Traceroute - Test the Path (Contd.)

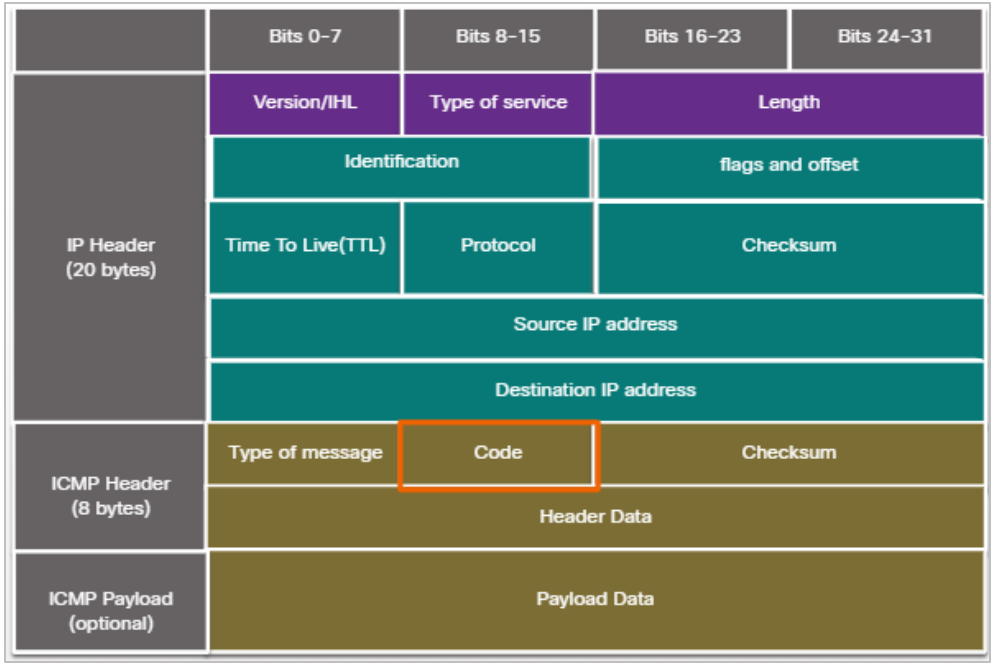
**IPv4 TTL and IPv6 Hop Limit:** Traceroute uses the function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.

- The first sequence of messages sent from traceroute have a TTL field value of 1 which causes the TTL to time out the IPv4 packet at the first router. This router then responds with an ICMPv4 Time Exceeded message. Traceroute now has the address of the first hop.
- Traceroute then progressively increments the TTL field (2, 3, 4...) for each sequence of messages. This provides the trace with the address of each hop as the packets time out further down the path. The TTL field continues to be increased until the destination is reached.
- After the final destination is reached, the host responds with either an ICMP Port Unreachable message or an ICMP Echo Reply message instead of the ICMP Time Exceeded message.



# ICMP Packet Format

- ICMP is encapsulated directly into IP packets.
- ICMP acts as a data payload within the IP packet. It has a special header data field.
- It uses message codes to differentiate between different types of ICMP messages. These are some common message codes:
  - **0 –** Echo reply (response to a ping)
  - **3 –** Destination Unreachable
  - **5 –** Redirect (use another route to the destination)
  - **8 –** Echo request (for ping)
  - **11 –** Time Exceeded (TTL became 0)



# Packet Tracer – Verify IPv4 and IPv6 Addressing

In this Packet Tracer, you will do the following:

- Verify IPv4 and IPv6 addressing configuration.
- Test connectivity with Ping and Tracert.

# 7.3 Connectivity Verification Summary

# What Did I Learn in this Module?

- The TCP/IP suite sends ICMP messages when IP packets encounter forwarding problems.
- ICMPv4 is the messaging protocol for IPv4, while ICMPv6 provides these same services for IPv6 and includes additional functionality.
- ICMP messages that are common to both ICMPv4 and ICMPv6 include host confirmation, destination or service unreachable, time exceeded, and route redirection.
- ICMPv6 includes the additional four ICMPv6 messages for the Neighbor Discovery Protocol (NDP).
- These messages are router solicitation (RS) and router advertisements (RA) messages that are sent between IPv6 routers and IPv6 hosts, and neighbor solicitation (NS) and neighbor advertisement (NA) messages that are sent between IPv6 devices.

# What Did I Learn in this Module? (Contd.)

- Ping is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts.
- Some of the types of connectivity tests that are performed with ping include pinging the local loopback, pinging the default gateway, and pinging a remote host.
- Traceroute (tracert) is a utility that generates a list of the router hops that were successfully reached along a path.
- Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in the IPv6 Layer 3 headers, along with the ICMP Time Exceeded message.
- ICMP is encapsulated directly into IP packets as the data payload. The ICMP data payload contains special header data fields.


CISCO