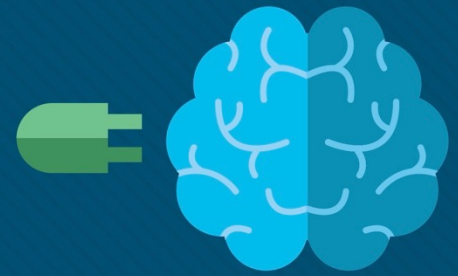


Chapter 3: Network Protocols and Services

Information Security

Dr. Ayman Aljarbouh

3.3 Connectivity Verification

Module Objectives

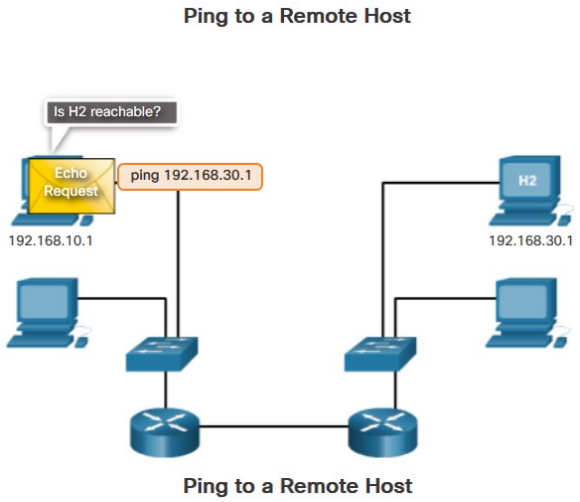
Module Title: Connectivity Verification

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.

ICMPv4 Messages

- Used to provide feedback and troubleshoot network problems.
- **Message types:**
  - **Host confirmation** – echo request and echo reply with the ping utility.
  - **Destination or service unreachable codes:**
    - **0** – net unreachable
    - **1** – host unreachable
    - **2** – protocol unreachable
    - **3** – port unreachable
  - **Time exceeded** – used by a router to indicate that a packet cannot be sent onward:
    - IPv4 is due to the time to live (TTL) field having a value of 0.
    - IPv6 does not have a TTL field, but has a hop limit field instead.



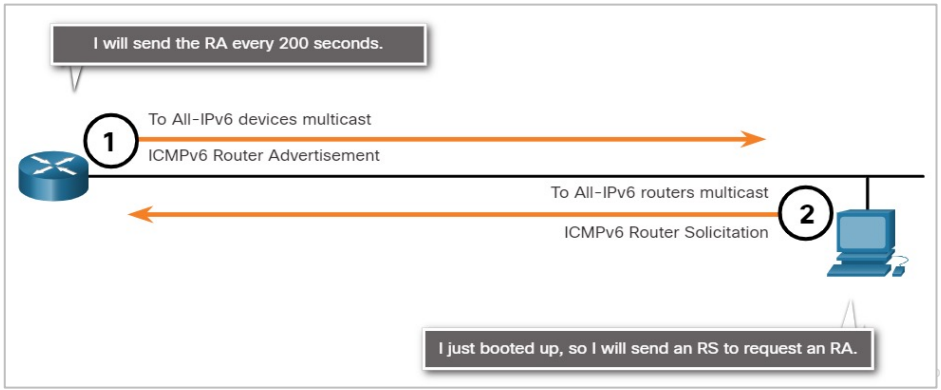
ICMPv6 RS and RA Messages

- 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

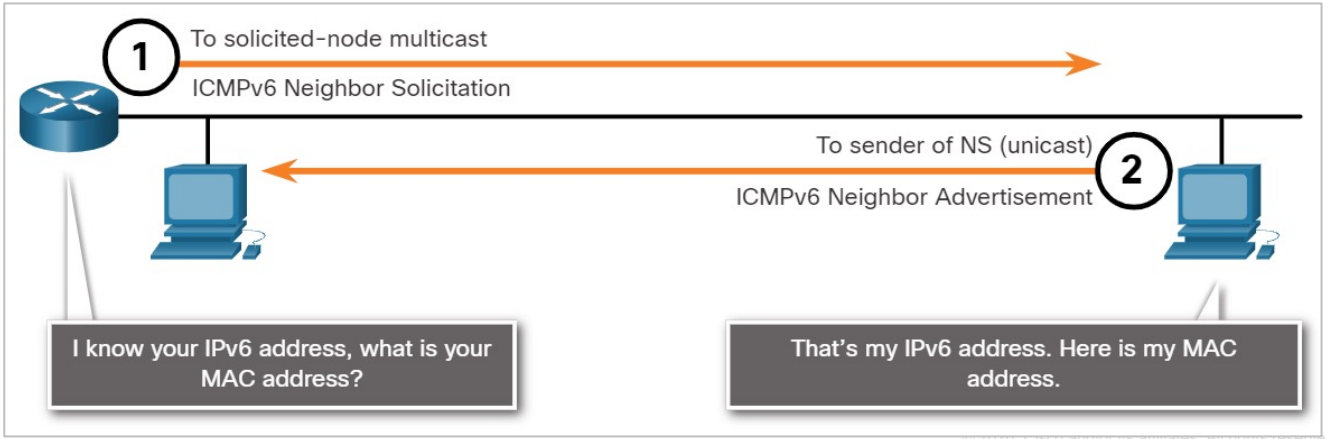
- RA messages are sent by routers to provide addressing information to hosts using Stateless Address Auto Configuration (SLAAC).
- A router will send an RA message periodically or in response to an RS message. A host using SLAAC will set its default gateway to the link-local address of the router that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

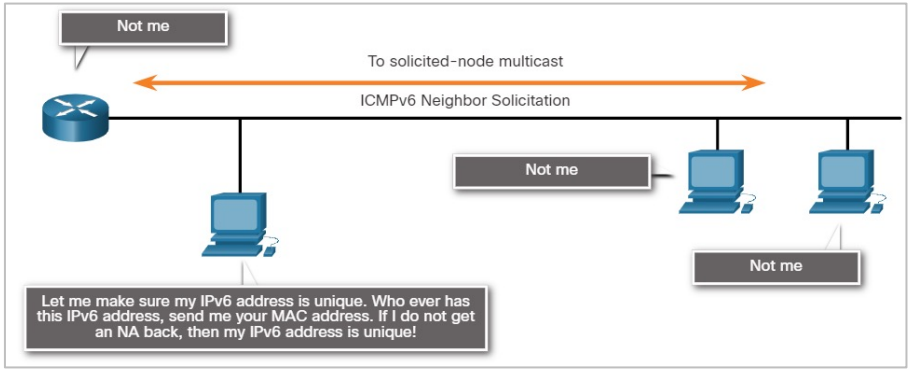
- NA messages are sent when a device knows the IPv6 address of a device but does not know its MAC address. This is equivalent to an ARP Request for IPv4.
- NA messages are sent in response to an NS message and match the target IPv6 address in the NS. The NA message includes the device's Ethernet MAC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

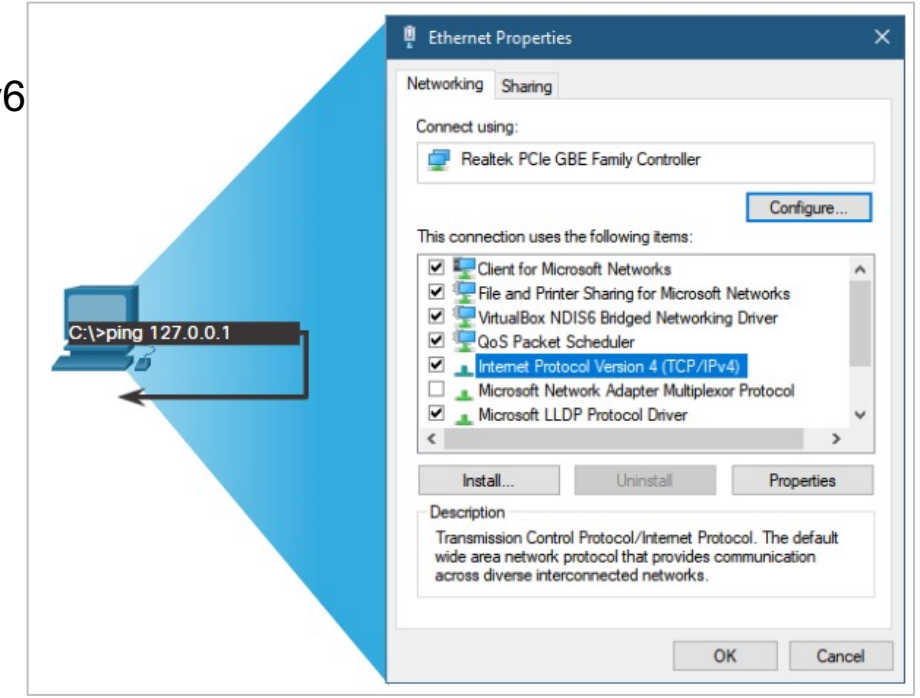


Ping – Test Connectivity

- 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.
- Type of connectivity tests performed with **ping** include the following:
  - Pinging the local loopback
  - Pinging the default gateway
  - Pinging the remote host

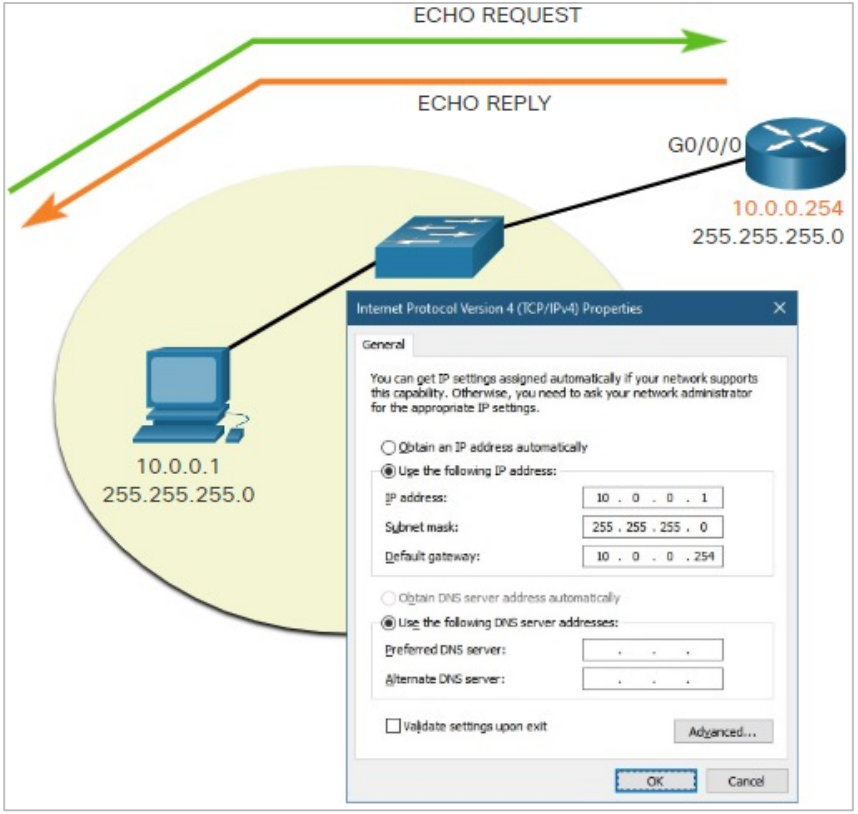
Ping the Loopback

- 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.
- 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.



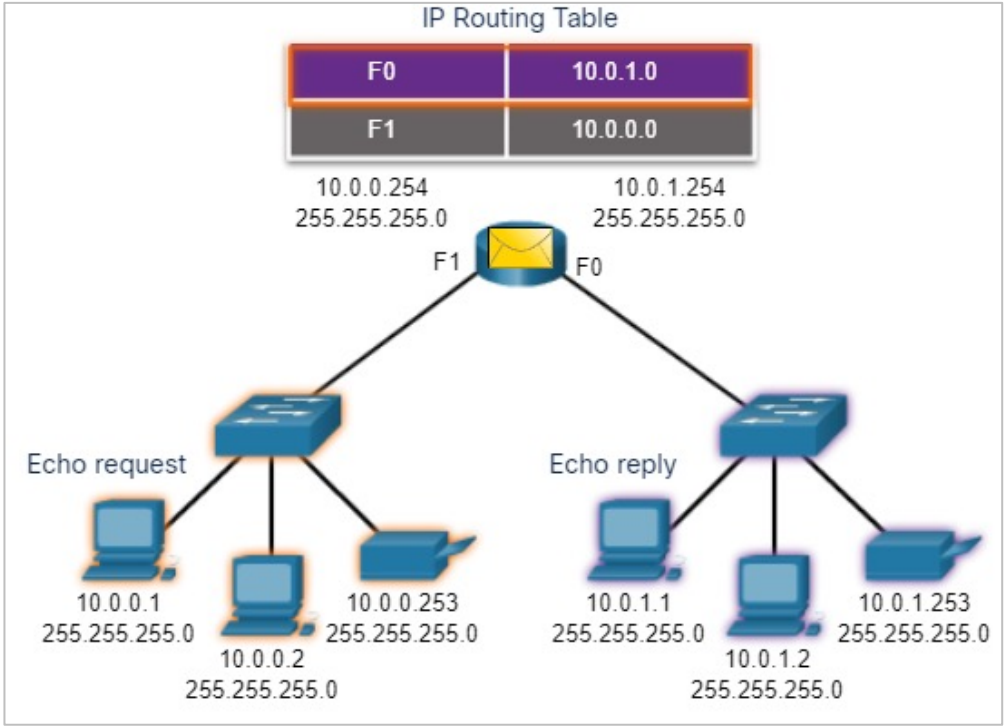
Ping the Default Gateway

- You can also use ping to test the ability of a host to communicate on the local network. This is generally done by pinging the IP address of the gateway of the host.
- A successful ping to the gateway indicates that the host and the router interface serving as the gateway are both operational on the local network.
- For this test, the gateway address is most often used because the router is normally always operational.



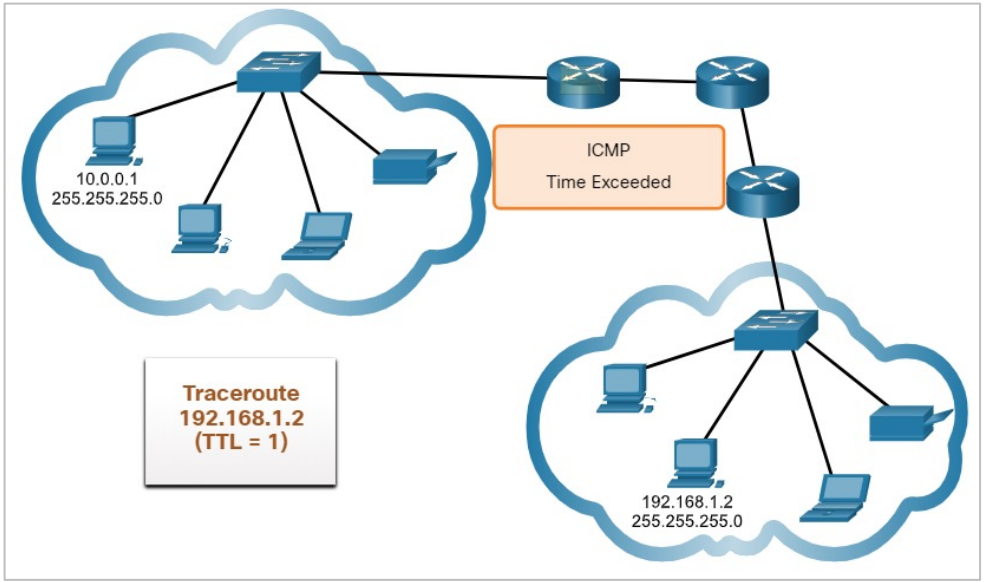
Ping a Remote Host

- 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.



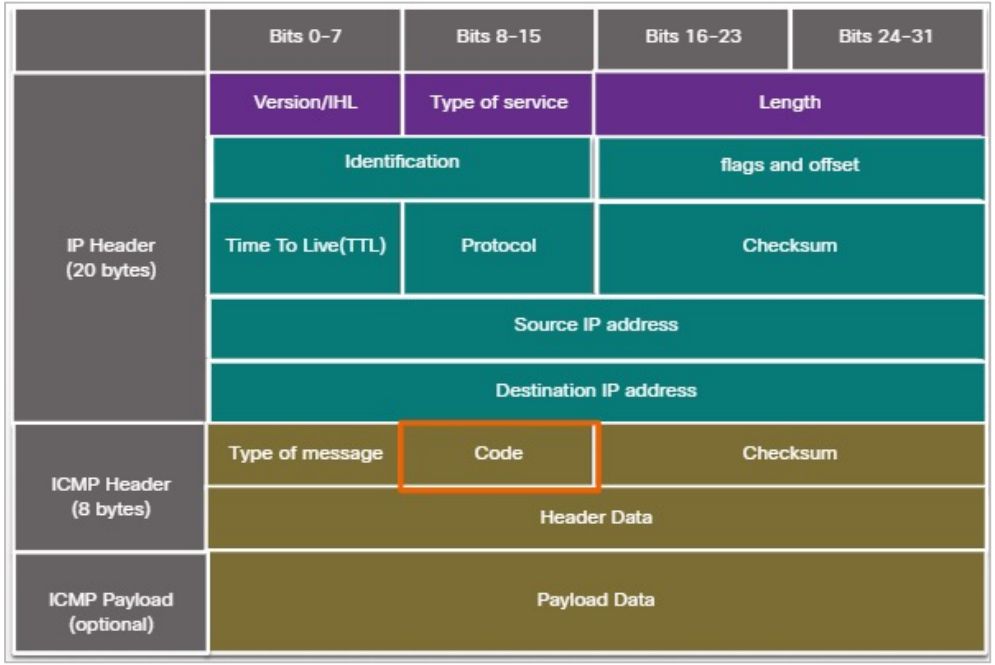
Traceroute - Test the Path

- Traceroute provides information about the details of devices between the hosts.
- Generates a list of hops that were successfully reached along the path:
  - **Round trip Time (RTT)** – time for each hop along path.
  - **IPv4 TTL and IPv6 Hop Limit** - Traceroute makes use of a 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.
- 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)



New Terms and Commands

• ICMP Echo Message • Time to Live (TTL) • Neighbor Discovery Protocol (ND or NDP) • Router Solicitation (RS) message • Router Advertisement (RA) message • Stateless Address Auto Configuration (SLAAC)	• Duplicate Address Detection (DAD) • Ping • Traceroute (tracert) • Round Trip Time (RTT) • Hop Limit

Lab 11 – Verify IPv4 and IPv6 Addressing

In this lab, you will do the following:

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