Module 13: ICMP

Introduction of Networks v7.0
(ITN)

Module Objectives

Module Title: ICMP

Module Objective: Use various tools to test network connectivity.

Topic Title	Topic Objective
ICMP Messages	Explain how ICMP is used to test network connectivity.
Ping and Traceroute Testing	Use ping and traceroute utilities to test network connectivity.

13.1 ICMP Messages

ICMPv4 and ICMPv6 Messages

- Internet Control Message Protocol (ICMP) provides feedback about issues related to the processing of IP packets under certain conditions.

- ICMPv4 is the messaging protocol for IPv4. ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.

- The ICMP messages common to both ICMPv4 and ICMPv6 include:

  - Host reachability

  - Destination or Service Unreachable
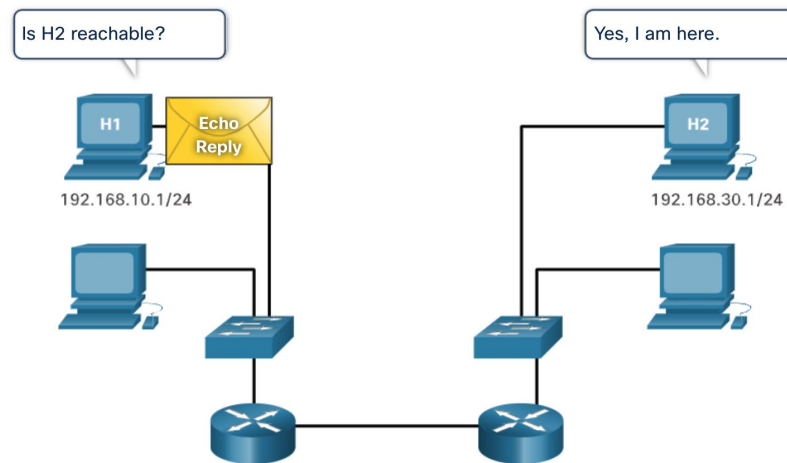
  - Time exceeded

Note: ICMPv4 messages are not required and are often not allowed within a network for security reasons.

Host Reachability

ICMP Echo Message can be used to test the reachability of a host on an IP network.

In the example:

- The local host sends an ICMP Echo Request to a host.
- If the host is available, the destination host responds with an Echo Reply.

ICMPv6 Messages

ICMPv6 has new features and improved functionality not found in ICMPv4, including four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).

Messaging between an IPv6 router and an IPv6 device, including dynamic address allocation are as follows:

- Router Solicitation (RS) message
- Router Advertisement (RA) message

Messaging between IPv6 devices, including duplicate address detection and address resolution are as follows:

- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

Note: ICMPv6 ND also includes the redirect message, which has a similar function to the redirect message used in ICMPv4.

13.2 Ping and Traceroute Tests

Ping – Test Connectivity

- The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.

- If a reply is not received within the timeout, ping provides a message indicating that a response was not received.

- It is common for the first ping to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```
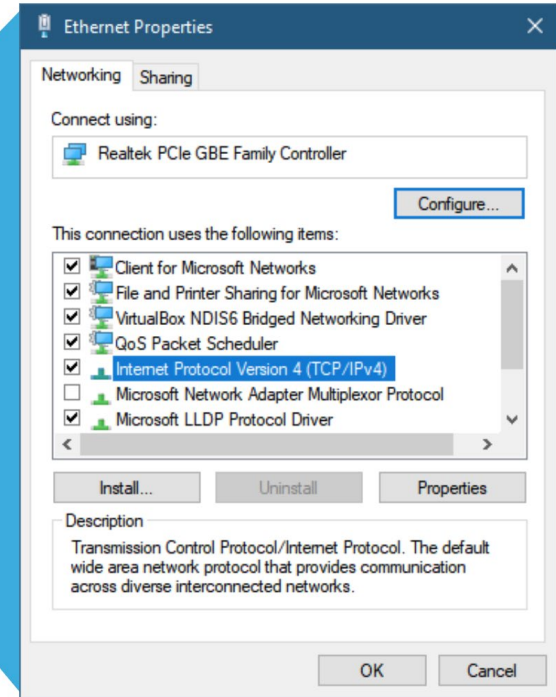
Ping the Loopback

Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, **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.

Ping the Default Gateway

The **ping** command can be used to test the ability of a host to communicate on the local network.

The default gateway address is most often used because the router is normally always operational.

- 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.

- 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 known to be operational.
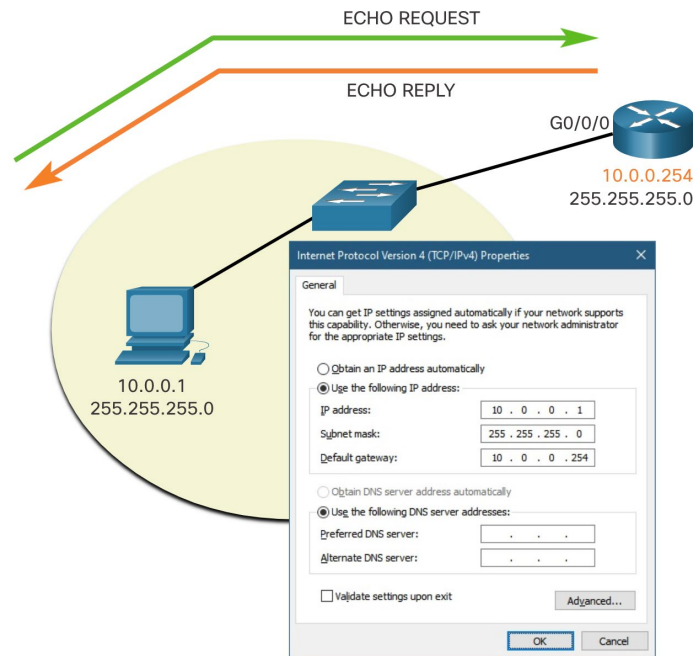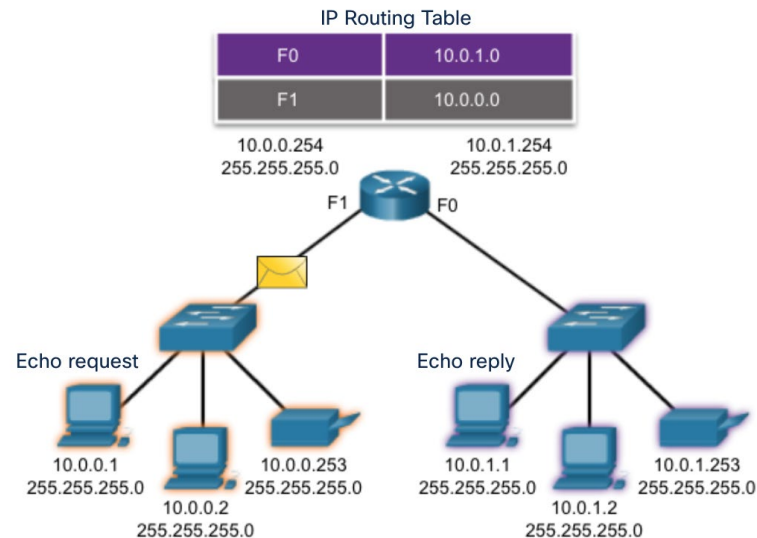
Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork.

A local host can ping a host on a remote network. A successful **ping** across the internetwork confirms communication on the local network.

Note: Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a **ping** response could be due to security restrictions.

IP Routing Table

F0	10.0.1.0
F1	10.0.0.0

10.0.0.254
255.255.255.0

10.0.1.254
255.255.255.0

F1   F0

Echo request

Echo reply

10.0.0.1
255.255.255.0

10.0.0.253
255.255.255.0

10.0.0.2
255.255.255.0

10.0.1.1
255.255.255.0

10.0.1.253
255.255.255.0

10.0.1.2
255.255.255.0

CISCO

Traceroute – Test the Path

- Traceroute (**tracert**) is a utility that is used to test the path between two hosts and provide a list of hops that were successfully reached along that path.

- Traceroute provides round-trip time for each hop along the path and indicates if a hop fails to respond. 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.

Traceroute – Test the Path (Cont.)

- The first message sent from traceroute will have a TTL field value of 1. This causes the TTL to time out at the first router. This router then responds with a ICMPv4 Time Exceeded message.

- 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, or it is incremented to a predefined maximum.

**Traceroute
192.168.1.2
(TTL = 4)**