CCNA 1 v7.0 Curriculum: Module 13 – ICMP

itexamanswers.net/ccna-1-v7-0-curriculum-module-13-icmp.html

April 1, 2020

13.0. Introduction

13.0.1. Why should I take this module?

Welcome to ICMP!

Imagine that you have an intricate model train set. Your tracks and trains are all connected and powered up and ready to go. You throw the switch. The train goes halfway around the track and stops. You know right away that the problem is most likely located where the train has stopped, so you look there first. It is not as easy to visualize this with a network. Fortunately, there are tools to help you locate problem areas in your network, AND they work with both IPv4 and IPv6 networks! You will be happy to know that this module has a couple Packet Tracer activities to help you practice using these tools, so let's get testing!

13.0.2. What will I learn in this module?

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

13.1.1. ICMPv4 and ICMPv6 Messages

In this topic, you will learn about the different types of Internet Control Message Protocols (ICMPs), and the tools that are used to send them.

Although IP is only a best-effort protocol, the TCP/IP suite does provide for error messages and informational messages when communicating with another IP device. 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, not to make IP reliable. ICMP messages are not required and are often not allowed within a network for security reasons.

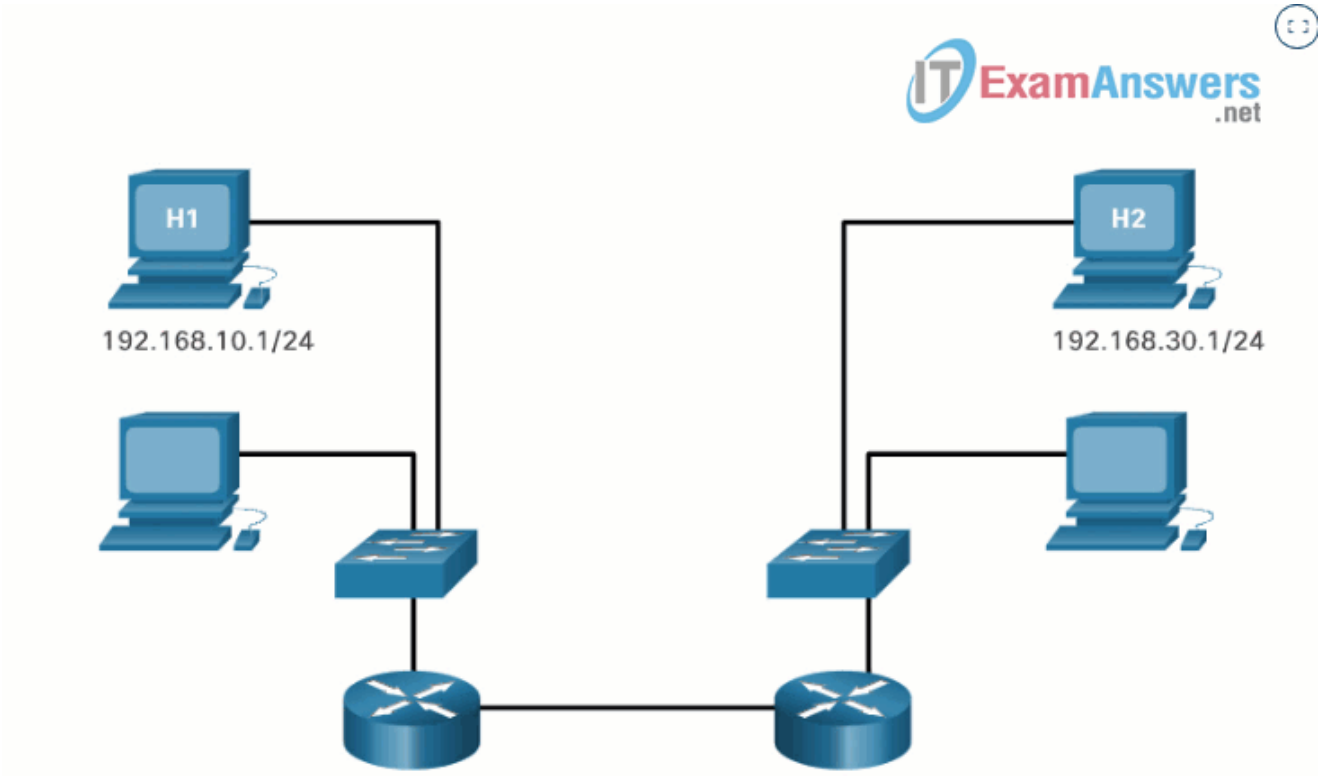
ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides these same services for IPv6 but includes additional functionality. In this course, the term ICMP will be used when referring to both ICMPv4 and ICMPv6.

The types of ICMP messages, and the reasons why they are sent, are extensive. The ICMP messages common to both ICMPv4 and ICMPv6 and discussed in this module include:

- Host reachability
- Destination or Service Unreachable
- Time exceeded

13.1.2. Host Reachability

An ICMP Echo Message can be used to test the reachability of a host on an IP network. The local host sends an ICMP Echo Request to a host. If the host is available, the destination host responds with an Echo Reply. In the figure, click the Play button to see an animation of the ICMP Echo Request/Echo Reply. This use of the ICMP Echo messages is the basis of the **ping** utility.



13.1.3. 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.

Some of the Destination Unreachable codes for ICMPv4 are as follows:

0 – Net unreachable
1 – Host unreachable
2 – Protocol unreachable
3 – Port unreachable

Some of the Destination Unreachable codes for ICMPv6 are as follows:

0 – No route to destination
1 – Communication with the destination is administratively prohibited (e.g., firewall)
2 – Beyond scope of the source address
3 – Address unreachable
4 – Port unreachable

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

13.1.4. 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. Instead of the IPv4 TTL field, ICMPv6 uses the IPv6 Hop Limit field to determine if the packet has expired.

Note: Time Exceeded messages are used by the **traceroute** tool.

13.1.5. ICMPv6 Messages

The informational and error messages found in ICMPv6 are very similar to the control and error messages implemented by ICMPv4. However, ICMPv6 has new features and improved functionality not found in ICMPv4. ICMPv6 messages are encapsulated in IPv6.

ICMPv6 includes 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:

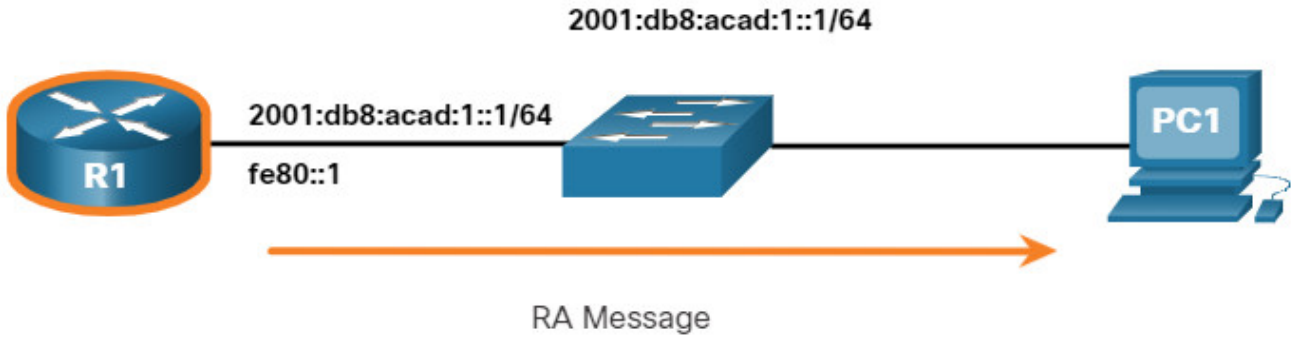
- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

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

Click each for an illustration and explanation of ICMPv6 messages.

- RA Message
- RS Message
- NS Message
- NA Message

RA messages are sent by IPv6-enabled routers every 200 seconds to provide addressing information to IPv6-enabled hosts. The RA message can include addressing information for the host such as the prefix, prefix length, DNS address, and domain name. A host using Stateless Address Autoconfiguration (SLAAC) will set its default gateway to the link-local address of the router that sent the RA.



R1 sends an RA message, “Hi all IPv6-enabled devices. I’m R1 and you can use SLAAC to create an IPv6 global unicast address. The prefix is 2001:db8:acad:1::/64. By the way, use my link-local address fe80::1 as your default gateway."

13.2. Ping and Traceroute Tests

13.2.1. Ping – Test Connectivity

In the previous topic, you were introduced to the **ping** and traceroute **(tracert)** tools. In this topic, you will learn about the situations in which each tool is used, and how to use them. 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. This may indicate that there is a problem, but could also indicate that security features blocking ping messages have been enabled on the network. 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.

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.

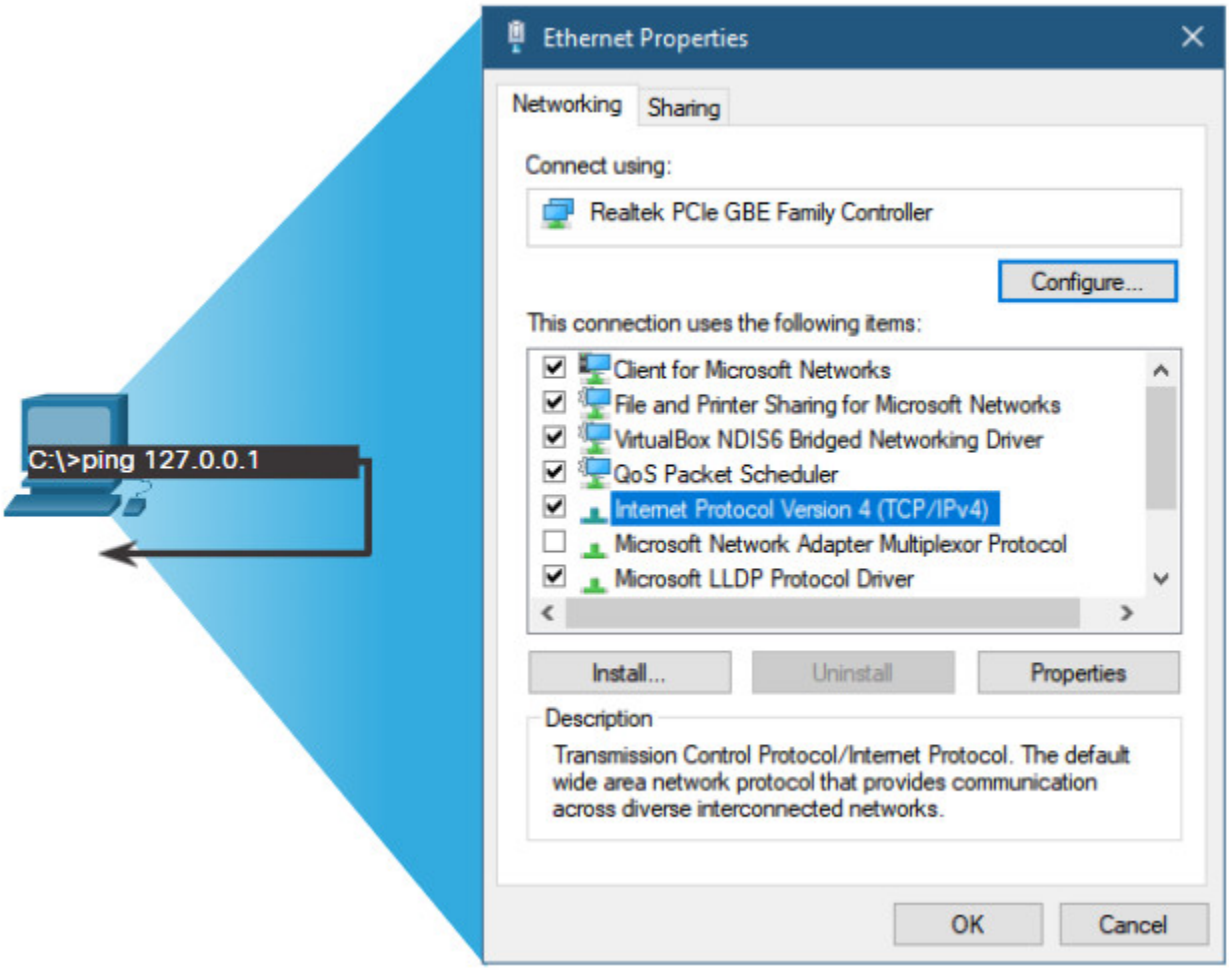
Type of connectivity tests performed with **ping** include the following:

- Pinging the local loopback
- Pinging the default gateway
- Pinging the remote host

13.2.2. 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 is not, however, an indication that the addresses, masks, or gateways are properly configured. Nor does it indicate anything about the status of the lower layer of the network stack. This simply 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.

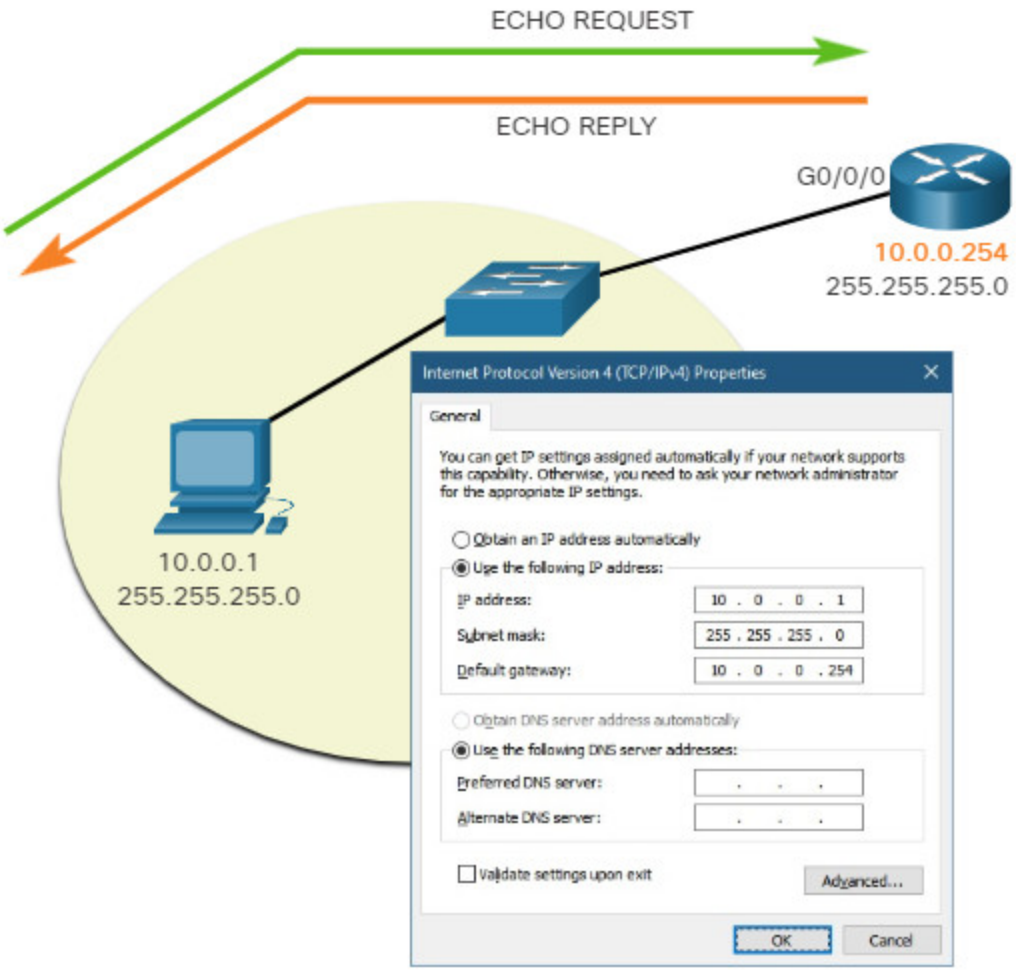
13.2.3. Ping the Default Gateway

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 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 most often used because the router is normally 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 known to be 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 has been configured on the host. Another possibility is that the router interface may be fully operational but have security applied to it that prevents it from processing or responding to ping requests.



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

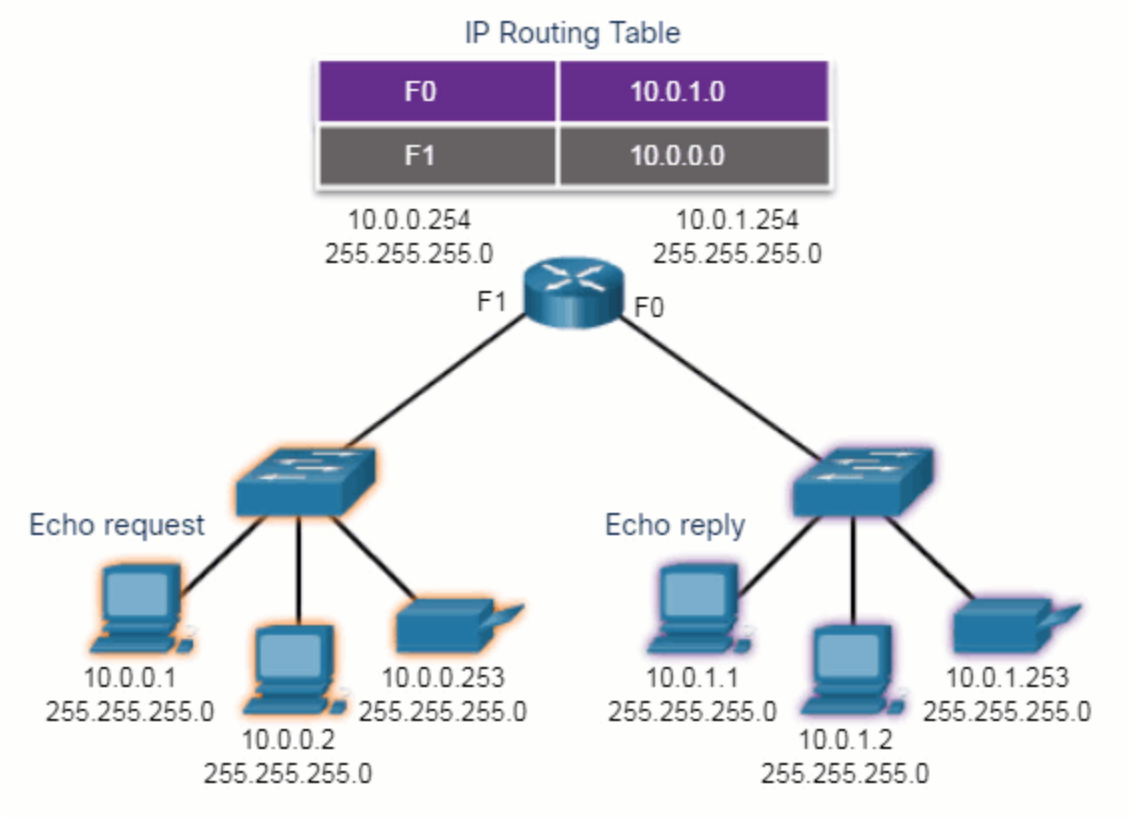
13.2.4. Ping a Remote Host

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, as shown in the figure. 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 can be verified. A successful **ping** across the internetwork confirms communication on the local network, the operation of the router serving as the default gateway, and the operation of all other routers that might be in the path between the local network and the network of the remote host.

Additionally, the functionality of the remote host can be verified. If the remote host could not communicate outside of its local network, it would not have responded.

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



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

13.2.5. 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.

Round Trip Time (RTT)

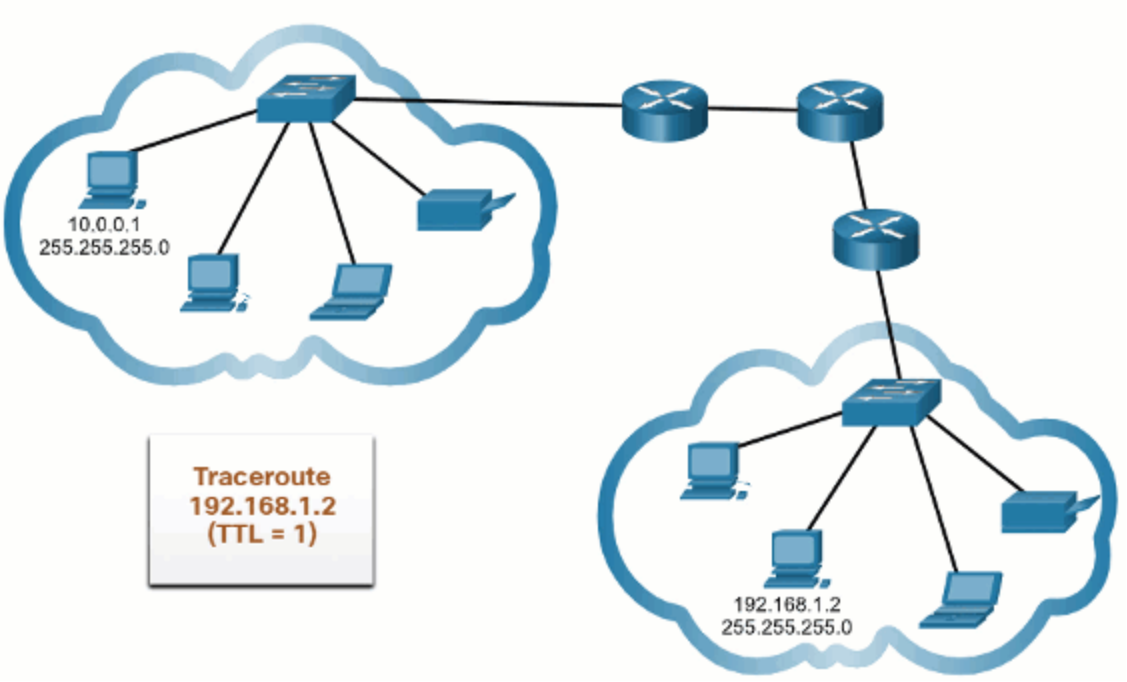
Using traceroute provides round-trip time for each hop along the path and indicates if a hop fails to respond. The round-trip time is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (*) is used to indicate a lost or unreplied packet.

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 stressed.

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.

The animation in the figure to see how traceroute takes advantage of TTL.



13.2.6. Packet Tracer – Verify IPv4 and IPv6 Addressing

IPv4 and IPv6 can coexist on the same network. From the command prompt of a PC, there are some differences in the way commands are issued and in the way output is displayed.

13.2.6 Packet Tracer – Verify IPv4 and IPv6 Addressing

13.2.7. Packet Tracer – Use Ping and Traceroute to Test Network Connectivity

There are connectivity issues in this activity. In addition to gathering and documenting information about the network, you will locate the problems and implement acceptable solutions to restore connectivity.

13.2.7 Packet Tracer – Use Ping and Traceroute to Test Network Connectivity

13.3. Module Practice and Quiz

13.3.1. Packet Tracer – Use ICMP to Test and Correct Network Connectivity

In this lab you will use ICMP to test network connectivity and locate network problems. You will also correct simple configuration issues and restore connectivity to the network.

Use ICMP to locate connectivity issues.

Configure network devices to correct connectivity issues.

13.3.1 Packet Tracer – Use ICMP to Test and Correct Network Connectivity

13.3.2. Lab – Use Ping and Traceroute to Test Network Connectivity

Skills Practice Opportunity
You have the opportunity to practice the following skills:

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
Part 4: Troubleshoot the Topology

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer – Physical Mode (PTPM)

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

Lab Equipment

13.3.2 Lab – Use Ping and Traceroute to Test Network Connectivity

13.3.3. What did I learn in this module?

ICMP Messages

The TCP/IP suite provides for error messages and informational messages when communicating with another IP device. These messages are sent using ICMP. The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions. The ICMP messages common to both ICMPv4 and ICMPv6 are: Host reachability, Destination or Service Unreachable, and Time exceeded. An ICMP Echo Message tests the reachability of a host on an IP network. 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 is the basis of the ping utility. When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source. The message will include a code that indicates why the packet could not be delivered. 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 zero. If a router receives a packet and decrements the TTL field to zero, it discards the packet and sends a Time Exceeded message to the source host. ICMPv6 also sends a Time Exceeded in this situation. ICMPv6 uses the IPv6 hop limit field to determine if the packet has expired. Time Exceeded messages are used by the traceroute tool. The messages between an IPv6 router and an IPv6 device including dynamic address allocation include RS and RA. The messages between IPv6 devices include the redirect (similar to IPv4), NS and NA.

Ping and Traceroute Testing

Ping (used by IPv4 and IPv6) 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. 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. Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. Ping the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6). Use ping to test the ability of a host to communicate on the local network, 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. 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. Traceroute (tracert) generates a list of hops that were successfully reached along the path. This list provides 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. The round-trip time is the time a packet

takes to reach the remote host and for the response from the host to return. 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.

13.3.4 Module Quiz – ICMP

Download Slide Powerpoint (PPT)

CCNA 1 v7.0 Curriculum: Module 13 - ICMP.pptx

1 file(s) 39.96 MB

Download

Tags:ccna 1 v7 modules