



ICMP

Dmytro Zubov, PhD

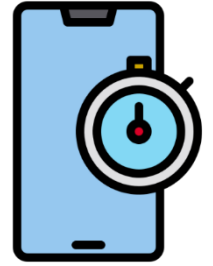
dmytro.zubov@ucentralasia.org



Naryn, 11:52am, October 20, 2022



Lessons learnt last time



- IPv4 Issues: Explain the need for IPv6 addressing
- IPv6 Address Representation: Explain how IPv6 addresses are represented
- IPv6 Address Types: Compare types of IPv6 network addresses
- GUA and LLA Static Configuration: Explain how to Configure static global unicast and link-local IPv6 network addresses
- Dynamic Addressing for IPv6 GUAs: Explain how to configure global unicast addresses dynamically
- VLSM (Variable Length Subnet Mask): IPv6 example

What we gonna discuss today?



- ICMP Messages: Explain how ICMP is used to test network connectivity
- Ping and Traceroute Testing: Use ping and traceroute utilities to test network connectivity

ICMP Messages

A decorative blue wavy line that spans across the upper portion of the slide, starting from the left edge and ending on the right, with a slight dip in the middle.

- ICMP Messages

ICMP Messages



- ICMPv4 and ICMPv6 Messages

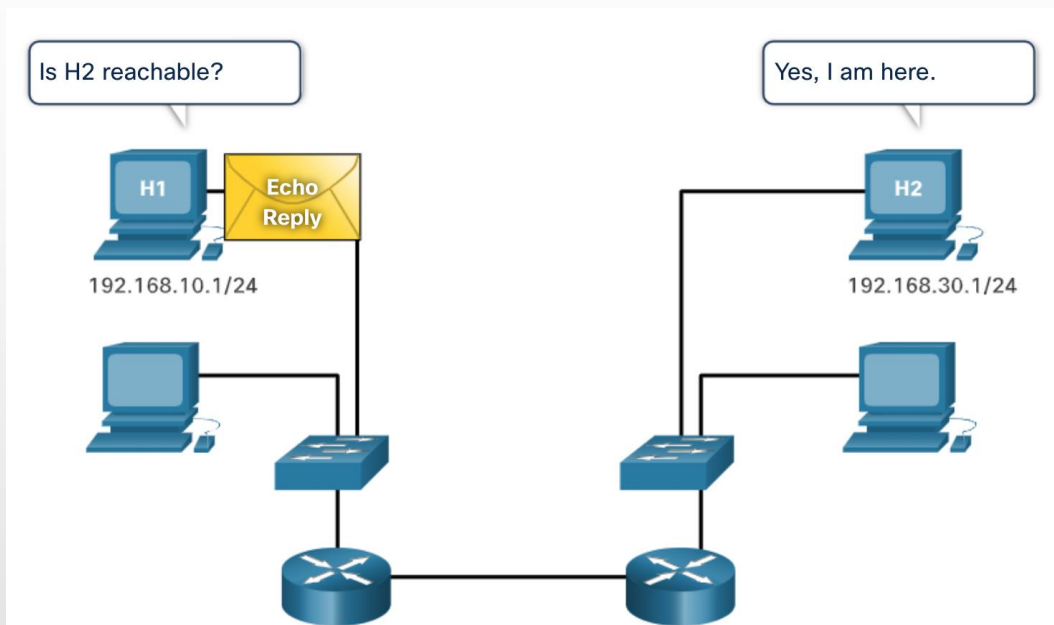
- Internet Control Message Protocol (ICMP) provides feedback about issues related to the processing of IP packets under certain conditions
- ICMPv4 is the messaging protocol for IPv4. ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.
- The ICMP messages common to both ICMPv4 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. Why? 😊

ICMP Messages

- Host Reachability

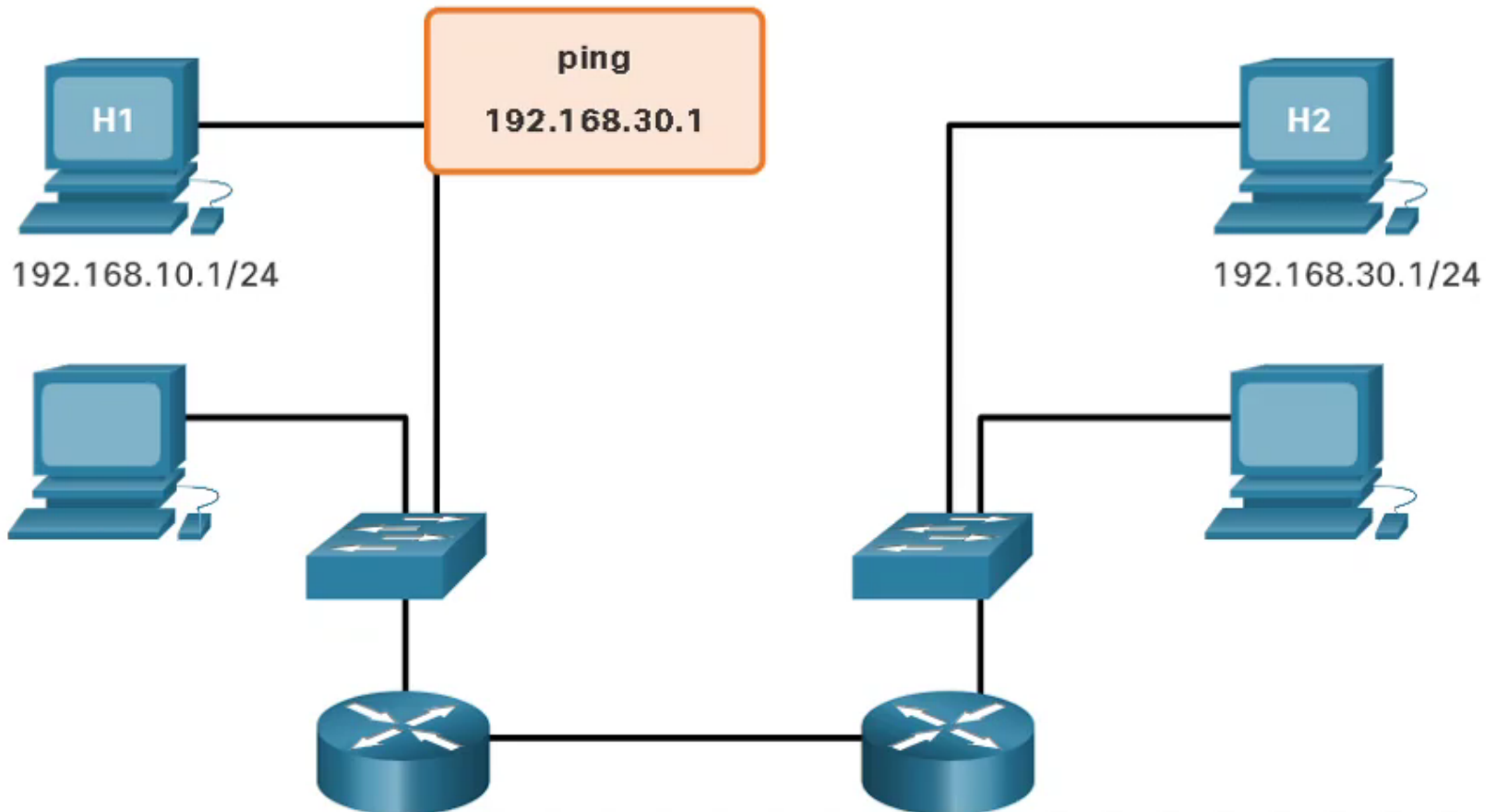
- ICMP Echo Message can be used to test the reachability of a host on an IP network
- In the example:
 - The local host sends an ICMP Echo Request to a host
 - If the host is available, the destination host responds with an Echo Reply



ICMP Messages

- Host Reachability (cont.)

Is H2 reachable?



ICMP Messages



- Destination or Service Unreachable

- An ICMP Destination Unreachable message can be used to notify the source that a destination or service is unreachable
- The ICMP message will include a code indicating why the packet could not be delivered

A few Destination Unreachable codes for ICMPv4 are as follows:

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

A few 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.

ICMP Messages

- Time Exceeded

- When the Time to Live (TTL) field in a packet is decremented to 0, an ICMPv4 Time Exceeded message will be sent to the source host
- ICMPv6 also sends a Time Exceeded message. Instead of the IPv4 TTL field, ICMPv6 uses the IPv6 Hop Limit field to determine if the packet has expired

```
Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
Reply from 192.168.1.1: TTL expired in transit.  
  
Ping statistics for 8.8.8.8:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

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

ICMP Messages



- 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:

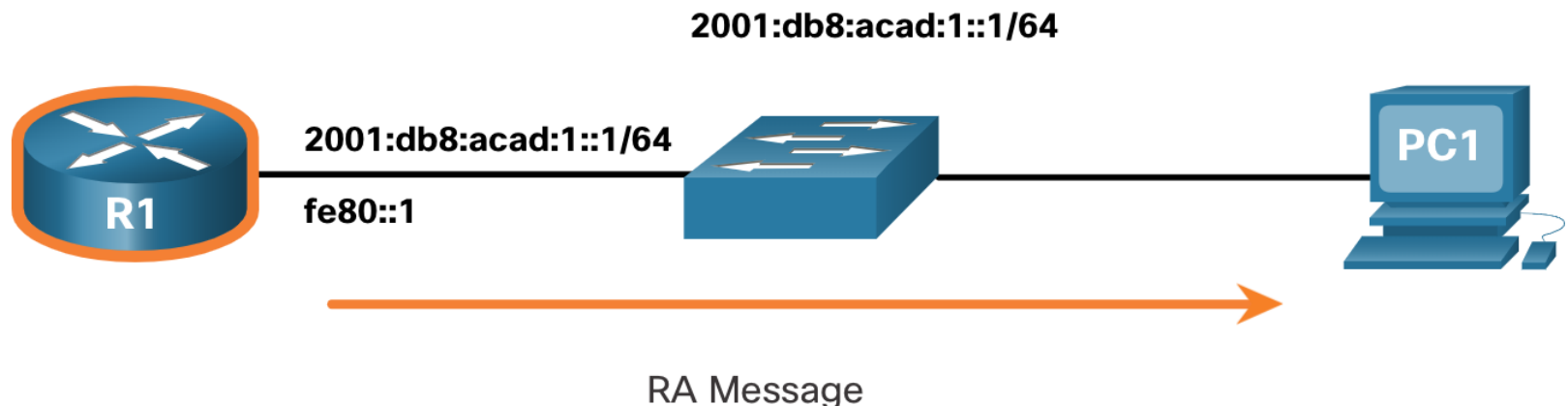
- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

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

ICMP Messages

- ICMPv6 Messages (Cont.)

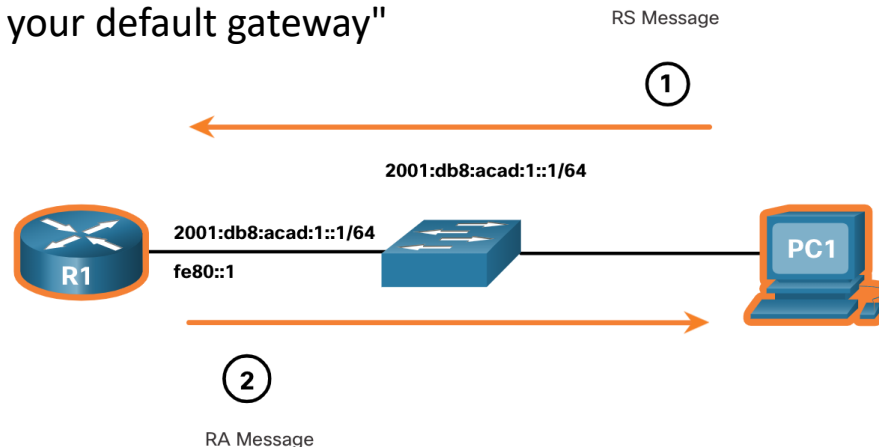
- RA messages are sent by IPv6-enabled routers every 200 seconds to provide addressing information to IPv6-enabled hosts
- RA message can include addressing information for the host such as the prefix, prefix length, DNS address, and domain name
- A host using Stateless Address Autoconfiguration (SLAAC)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



ICMP Messages

• ICMPv6 Messages (Cont.)

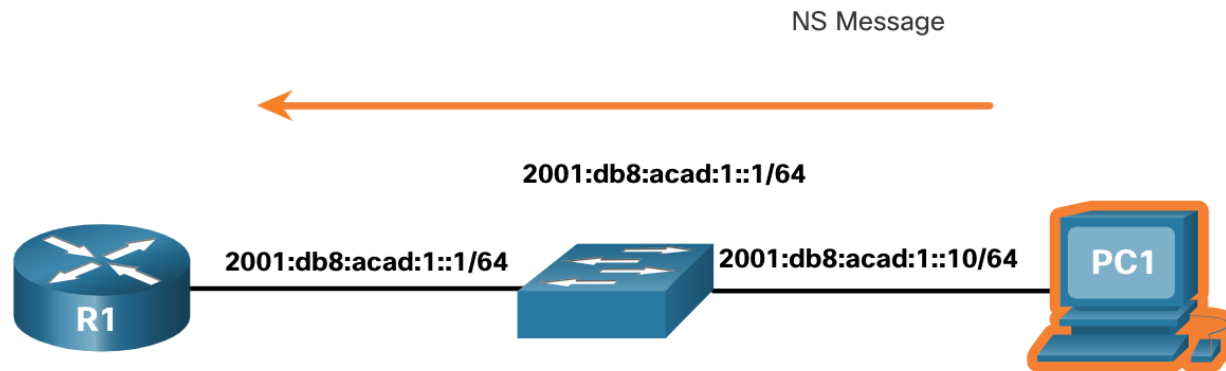
- An IPv6-enabled router will also send out an RA message in response to an RS message
- In the figure, PC1 sends a RS message to determine how to receive its IPv6 address information dynamically
 - R1 replies to the RS with an RA message
 - PC1 sends an RS message, "Hi, I just booted up. Is there an IPv6 router on the network? I need to know how to get my IPv6 address information dynamically"
 - R1 replies with 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"



ICMP Messages

- ICMPv6 Messages (Cont.)

- A device assigned a global IPv6 unicast or link-local unicast address, may perform duplicate address detection (DAD) to ensure that the IPv6 address is unique
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address
- If another device on the network has this address, it will respond with an NA message notifying to the sending device that the address is in use

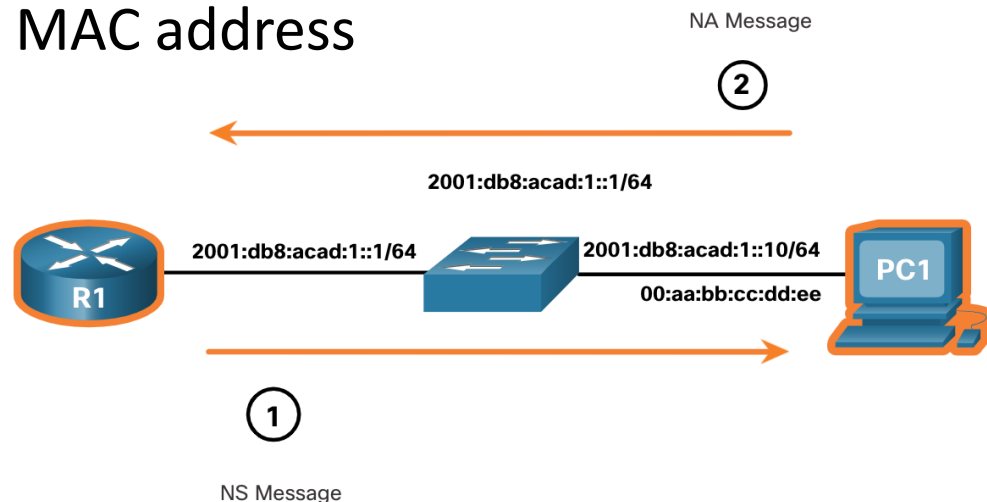


Note: DAD is not required, but RFC 4861 recommends that DAD is performed on unicast addresses.

ICMP Messages

- ICMPv6 Messages (Cont.)

- To determine the MAC address for the destination, the device will send an NS message to the solicited node address
- The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address.
- In the figure, R1 sends a NS message to 2001:db8:acad:1::10 asking for its MAC address



Ping and Traceroute Tests

A decorative blue wavy line that spans across the top of the slide, below the title.

- Ping and Traceroute Tests

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

Ping and Traceroute Tests



- Ping – Test Connectivity (cont.)

```
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
```

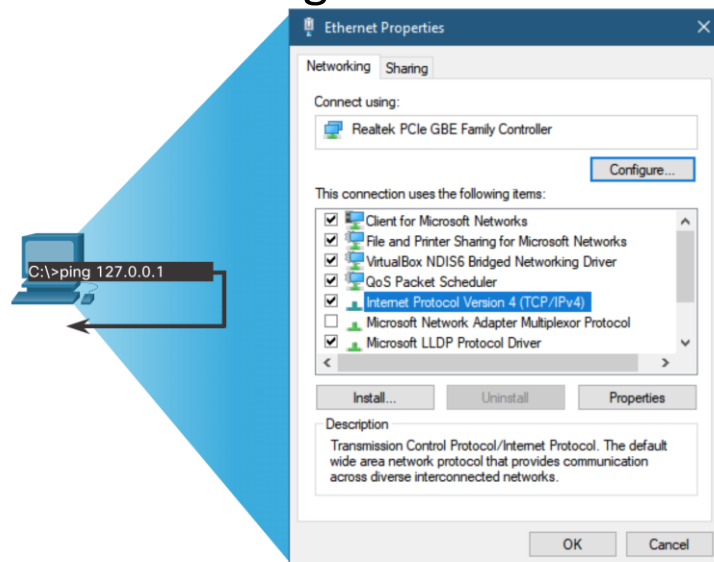
```
R1#ping 2001:db8:acad:1::2  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Ping and Traceroute Tests

- 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



```
C:\Users\DZUBOV>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\DZUBOV>ping ::1

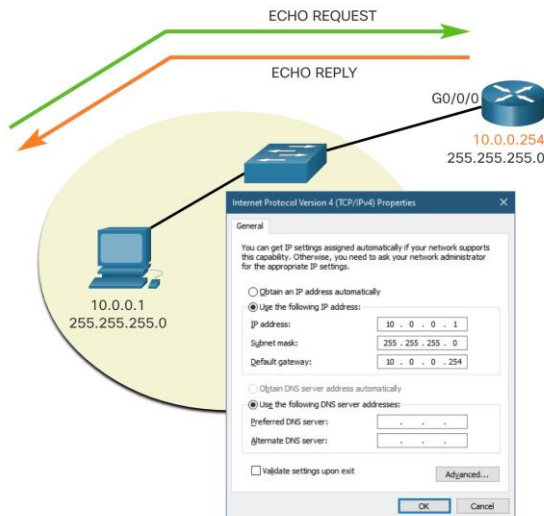
Pinging ::1 with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping and Traceroute Tests

- 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



```
C:\Users\DZUBOV>ping 192.168.0.1
```

```
Pinging 192.168.0.1 with 32 bytes of data:  
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
```

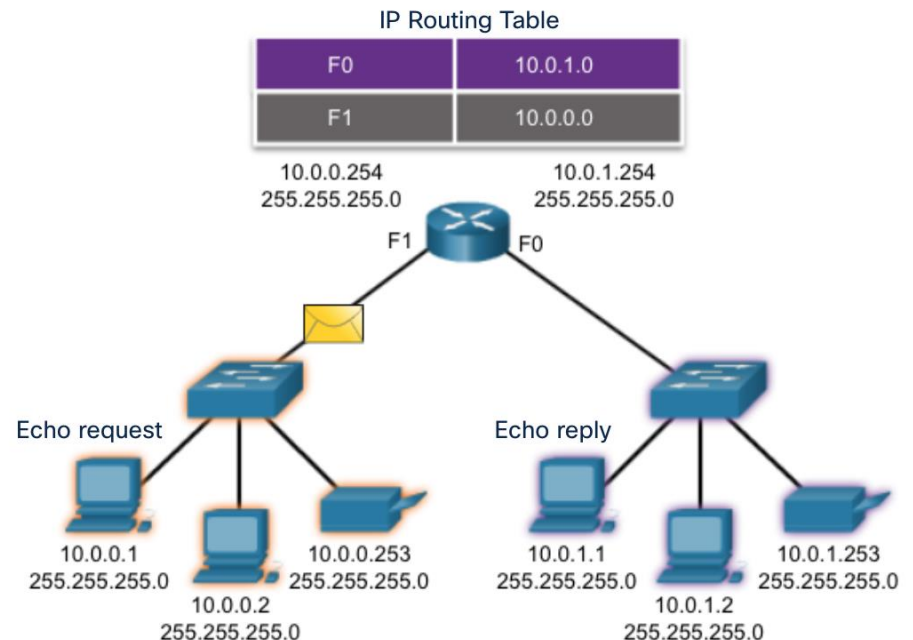
```
Ping statistics for 192.168.0.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping and Traceroute Tests

- Ping a Remote Host

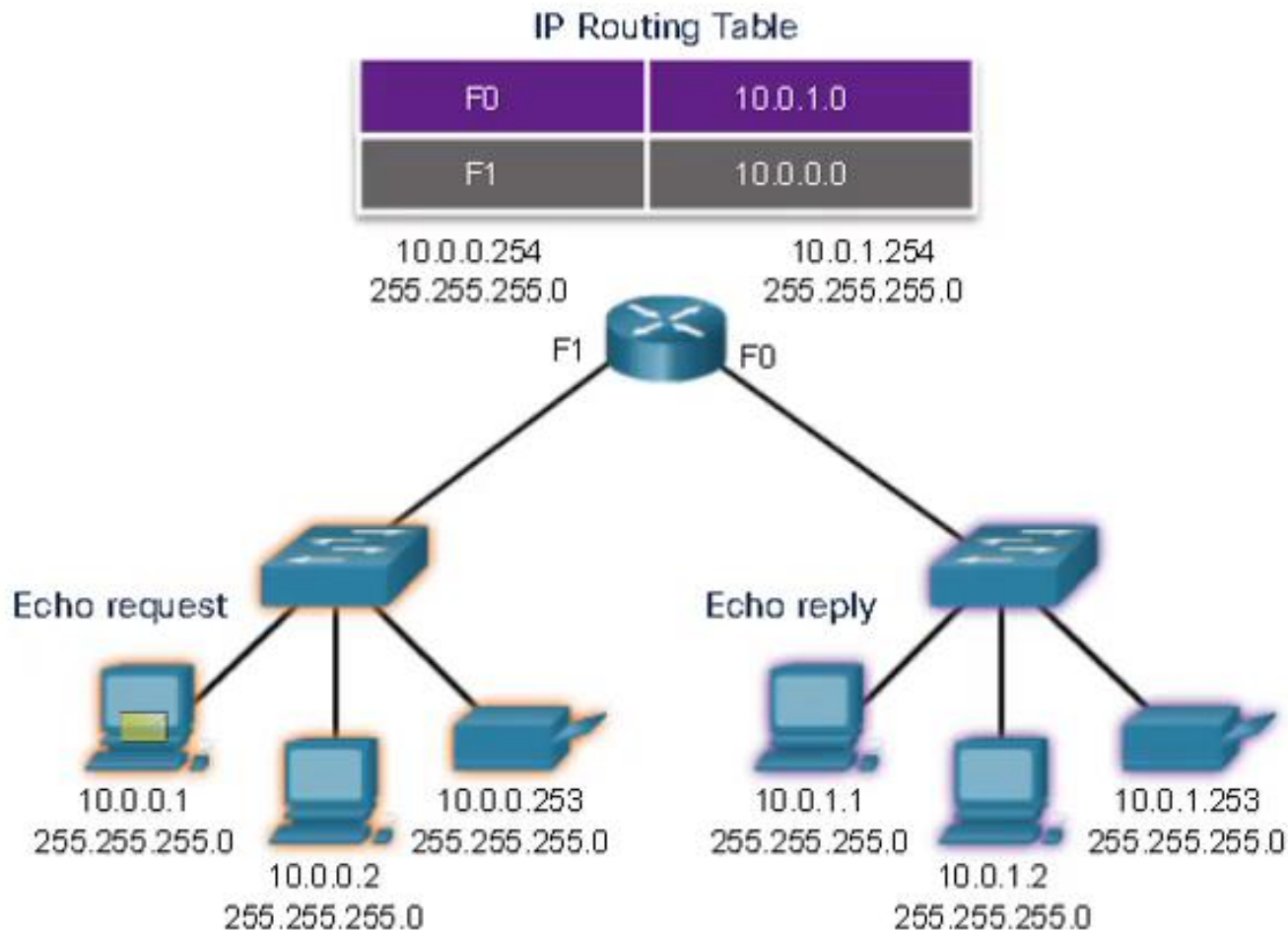
- Ping can also be used to test the ability of a local host to communicate across an internetwork
- A local host can ping a host on a remote network. A successful **ping** across the internetwork confirms communication on the local network.

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.



Ping and Traceroute Tests

- Ping a Remote Host (cont.)



Ping and Traceroute Tests

- Traceroute – Test the Path

- Traceroute (**tracert** on Windows, **traceroute** on Linux) 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.

Note: 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.

```
C:\Users\DZUBOV>tracert www.google.com

Tracing route to www.google.com [74.125.205.106]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.0.1
  1  <1 ms    <1 ms    <1 ms    212-42-101-45.elcat.kg [212.42.101.45]
  2  9 ms     9 ms     9 ms     asr.elcat.kg [212.42.96.250]
  3  10 ms    9 ms     9 ms     m2x.elcat.kg [94.143.195.159]
  4  9 ms     9 ms     9 ms     mx-bish-new.elcat.kg [94.143.195.158]
  5  64 ms    64 ms    64 ms    google-m9-local.elcat.kg [212.42.98.201]
  6  65 ms    65 ms    65 ms    google-m9-remote.elcat.kg [212.42.98.202]
  7  65 ms    65 ms    65 ms    209.85.250.231
  8  65 ms    65 ms    65 ms    108.170.250.113
  9  83 ms    80 ms    87 ms    142.251.237.154
 10  80 ms    85 ms    110 ms   142.251.237.144
 11  83 ms    84 ms    83 ms    216.239.47.201
 12  *         *         *         Request timed out.
 13  *         *         *         Request timed out.
 14  *         *         *         Request timed out.
 15  *         *         *         Request timed out.
 16  *         *         *         Request timed out.
 17  *         *         *         Request timed out.
 18  *         *         *         Request timed out.
 19  *         *         *         Request timed out.
 20  *         *         *         Request timed out.
 21  *         *         *         Request timed out.
 22  81 ms    81 ms    81 ms    le-in-f106.1e100.net [74.125.205.106]

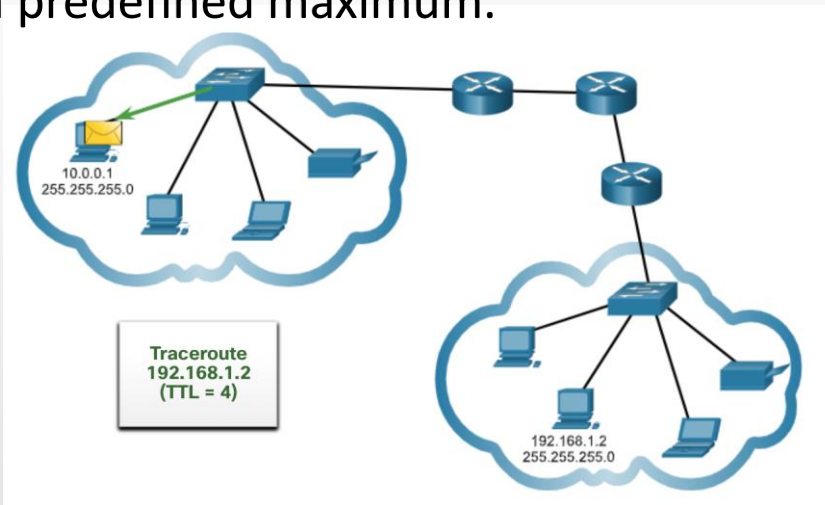
Trace complete.
```

```
C:\Users\DZUBOV>
```

Ping and Traceroute Tests

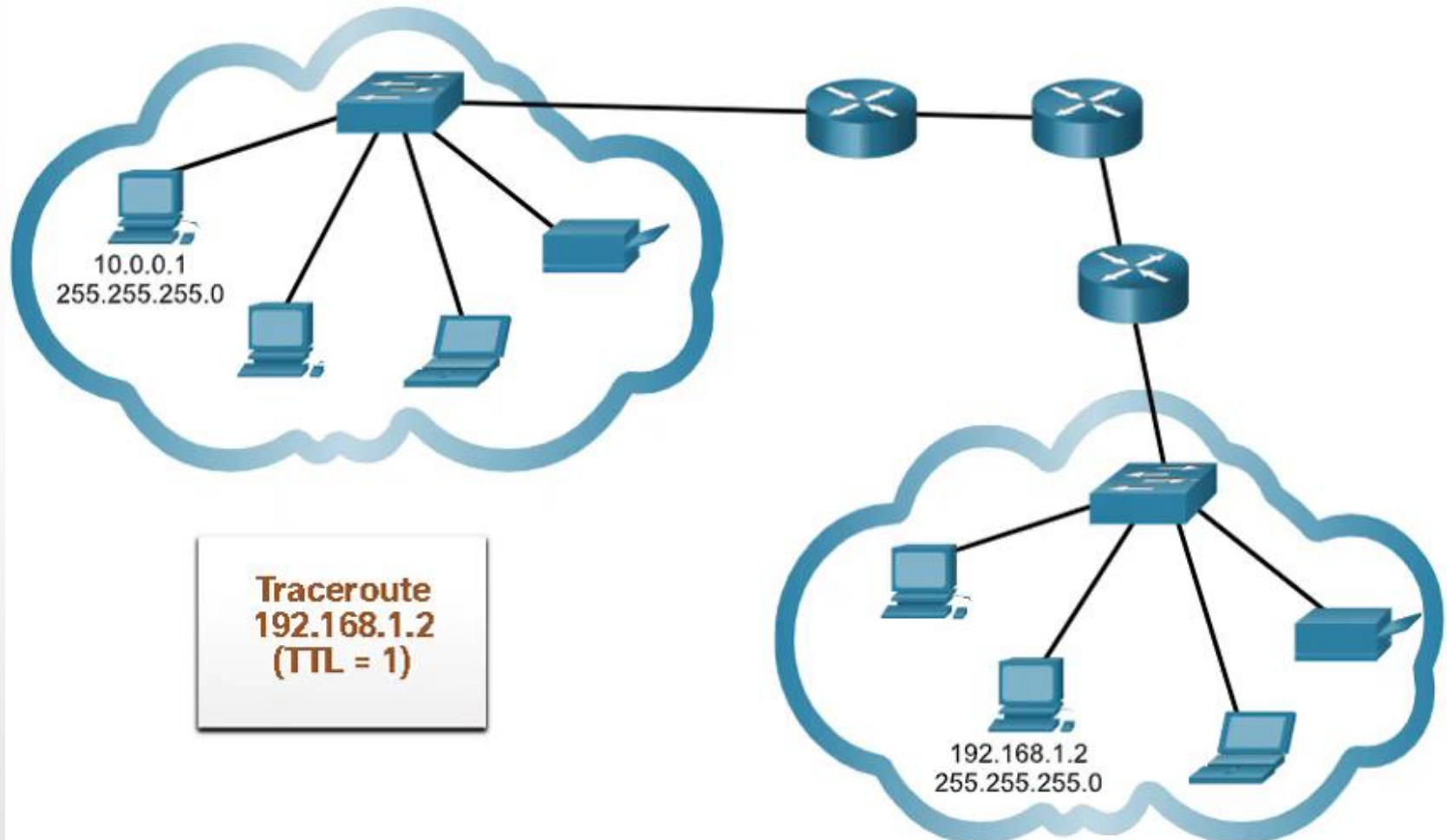
- Traceroute – Test the Path (Cont.)

- 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.



Ping and Traceroute Tests

- Traceroute – Test the Path (Cont.)



Do you have any
questions or
comments?



An abstract graphic consisting of multiple concentric, overlapping circular bands in shades of blue and grey, creating a sense of depth and motion. The bands are composed of various widths and colors, some appearing as solid lines and others as fragmented, pixelated segments.

Thank you
for your attention !

In this presentation:

- Some icons were downloaded from flaticon.com and iconscout.com