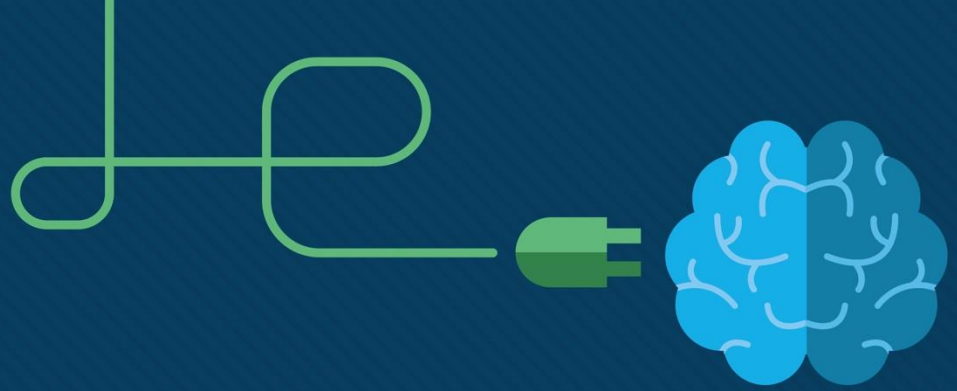


Module 13: ICMP (Internet Control Message Protocol)

CCNA1

Introduction to Networks v7.0
(ITN)

Gökhan AKIN - CCIE
gokhan@agyoneticileri.org

Ozan BÜK - CCIE
ozan@agyoneticileri.org

Module Objectives

Module Title: ICMP

Module Objective: Use various tools to test network connectivity.

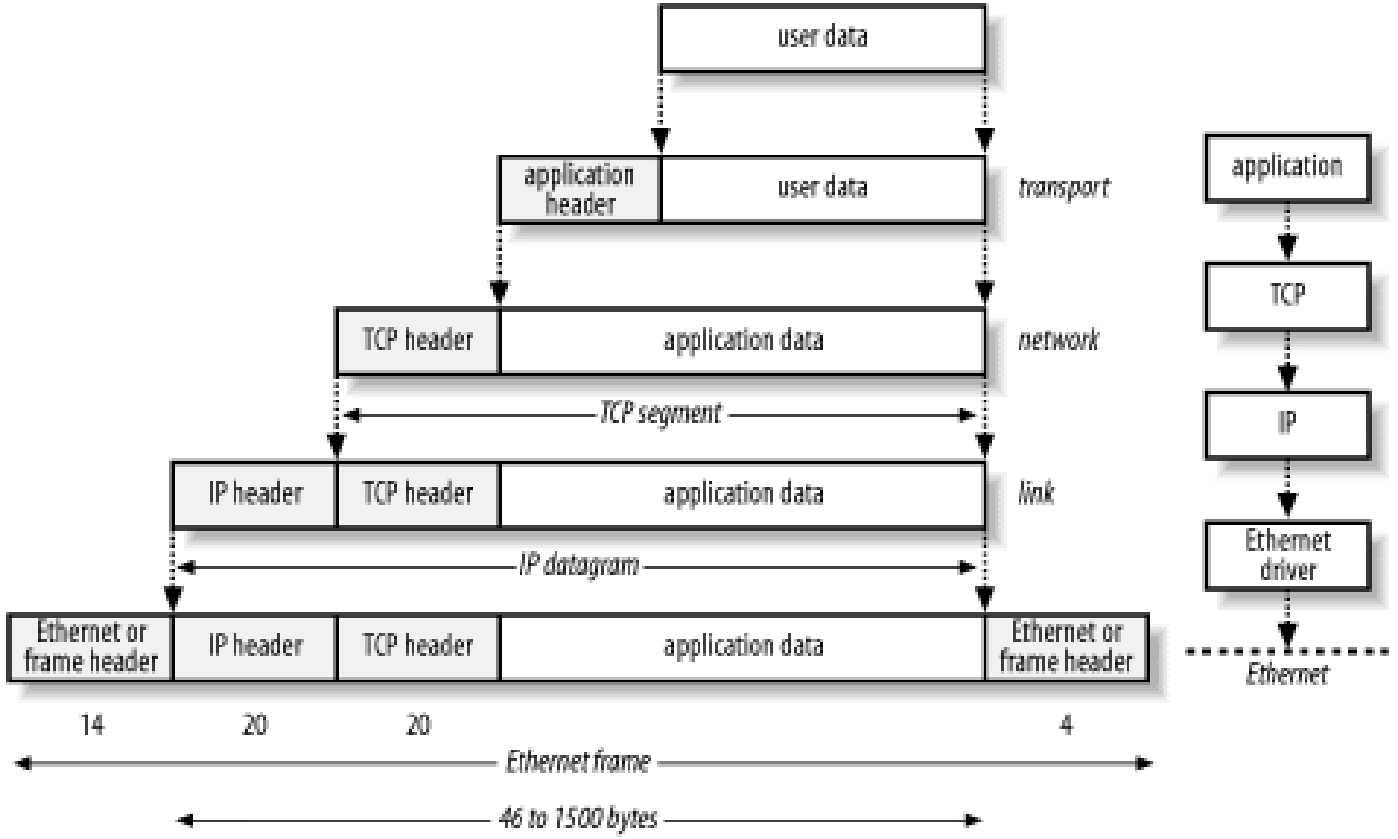
Topic Title	Topic Objective
ICMP Messages	Explain how ICMP is used to test network connectivity.
Ping and Traceroute Testing	Use ping and traceroute utilities to test network connectivity.

13.1 ICMP Messages

ICMPv4 and ICMPv6 Messages

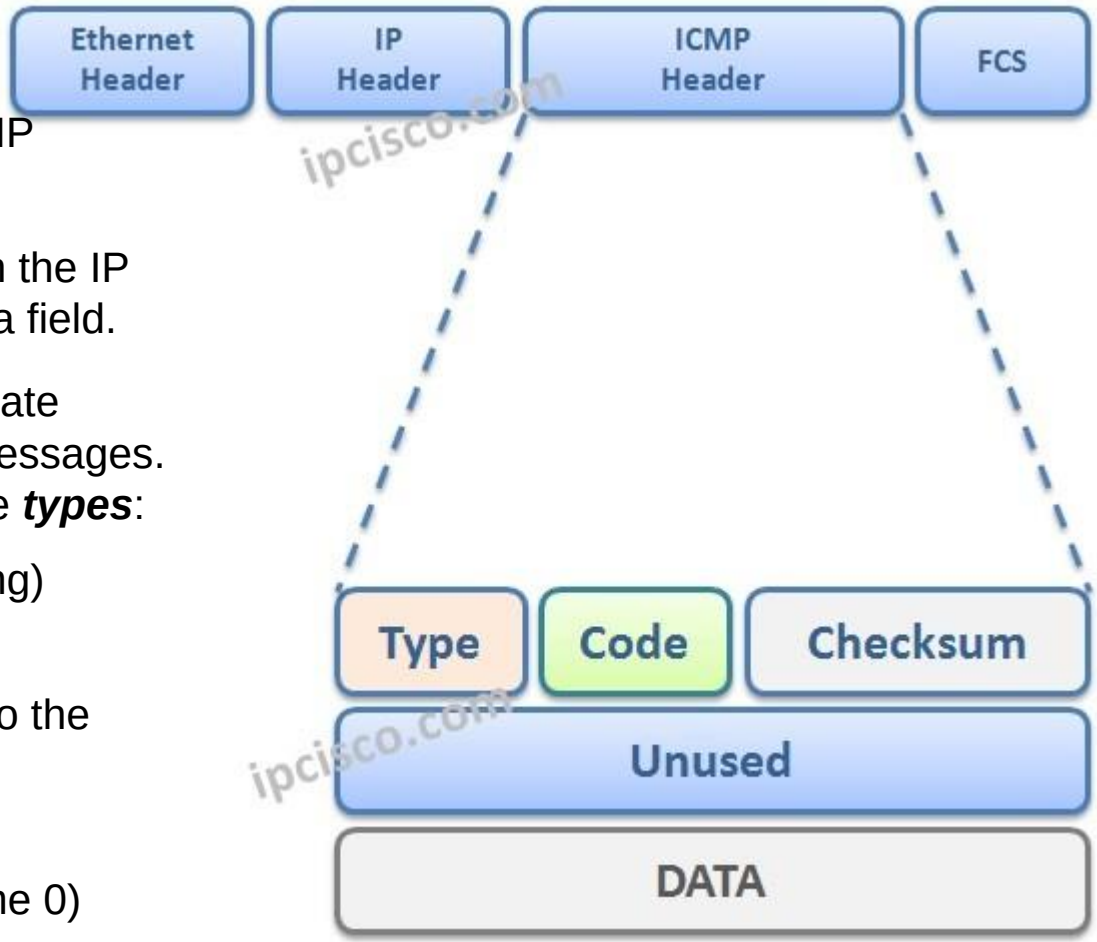
- **Internet Control Message Protocol (ICMP)** provides feedback about issues related to the processing of IP packets under certain conditions.
- ICMPv4 is the messaging protocol for IPv4. ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.
- The ICMP messages common to both ICMPv4 and ICMPv6 include:
  - **Host reachability**
  - **Destination or Service Unreachable**
  - **Time exceeded (TTL değeri sıfırlandı)**

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



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 ***types***:
  - **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)



ICMP Type-Code values

Type	Code	Description
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation needed and DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect datagram for the Network
	1	Redirect datagram for the host
	2	Redirect datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Use to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem	0	Pointer indicates error
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

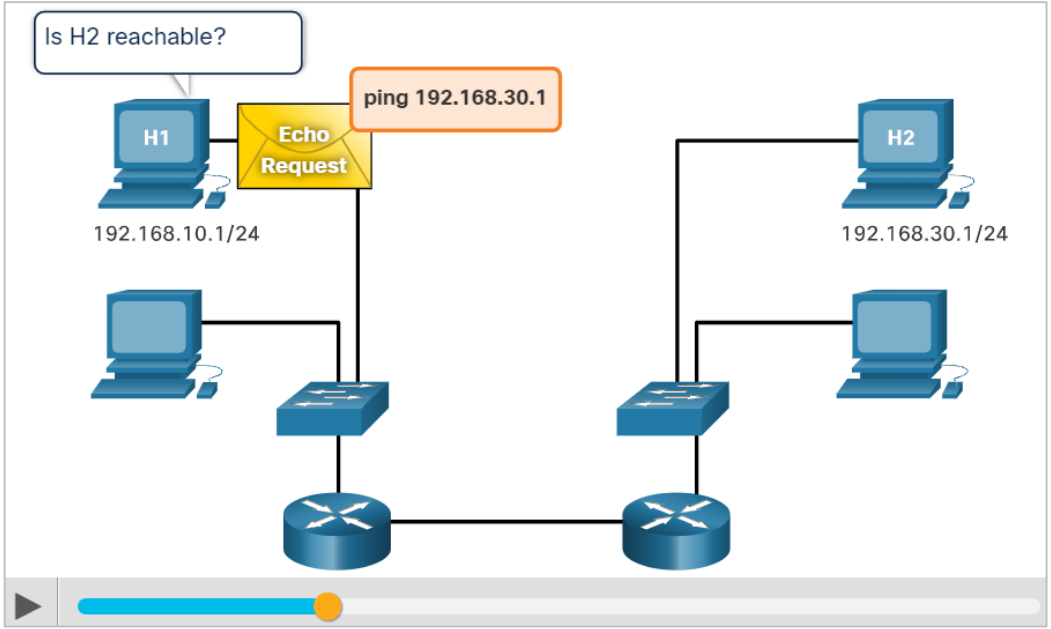
Host Reachability

Host Confirmation

echo req. (Type 8)

echo reply (Type 0)

- 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.



Destination or Service Unreachable (ICMP Type 3)

- 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.

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.

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:

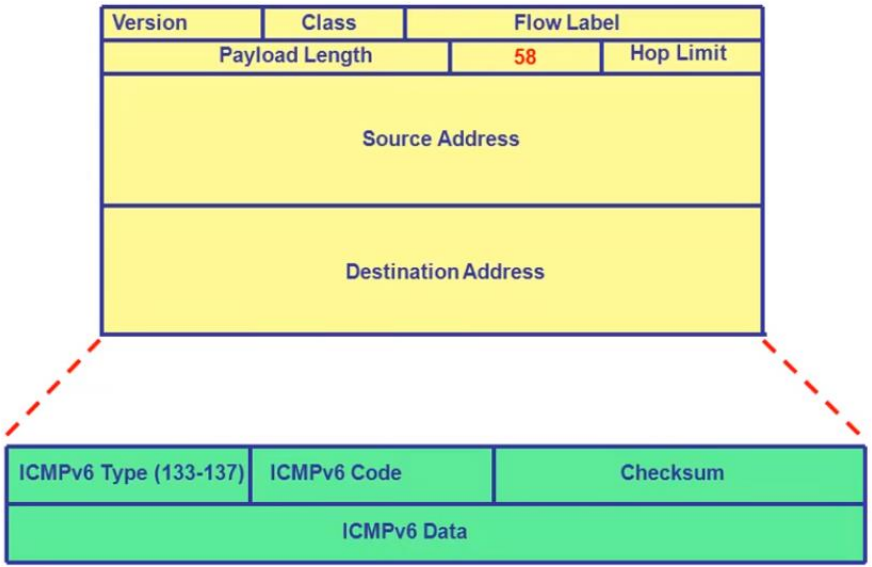
- **Neighbor Solicitation (NS) message**
- **Neighbor Advertisement (NA) message**

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

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).

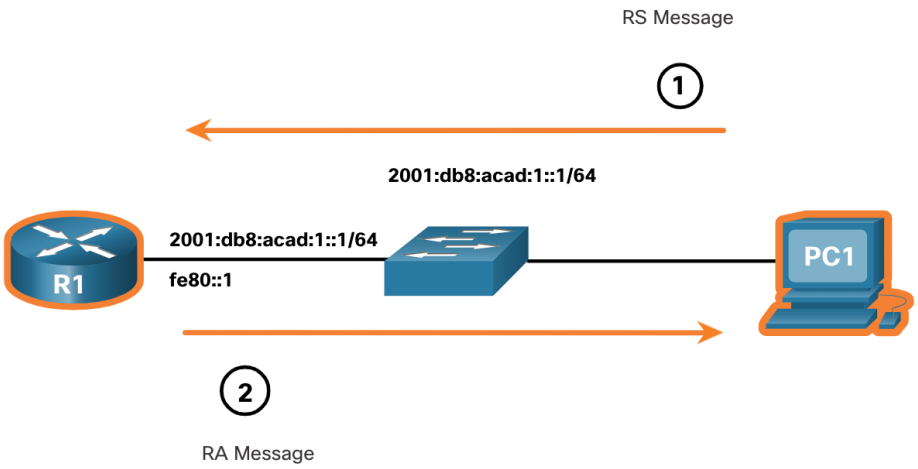
Neighbor Discovery using ICMPv6



- Router Solicitation
  - Type 133
  - Host requests routers to send Router Advertisement immediately
- Router Advertisement
  - Type 134
  - Contains one or more prefixes
  - Prefixes have lifetime
  - Stateless or stateful autoconfiguration to be used
- Neighbor Solicitation
  - Type 135
  - Used by node to get Link-layer address of neighbor
- Neighbor Advertisement
  - Type 136
  - Response to a Neighbor Solicitation

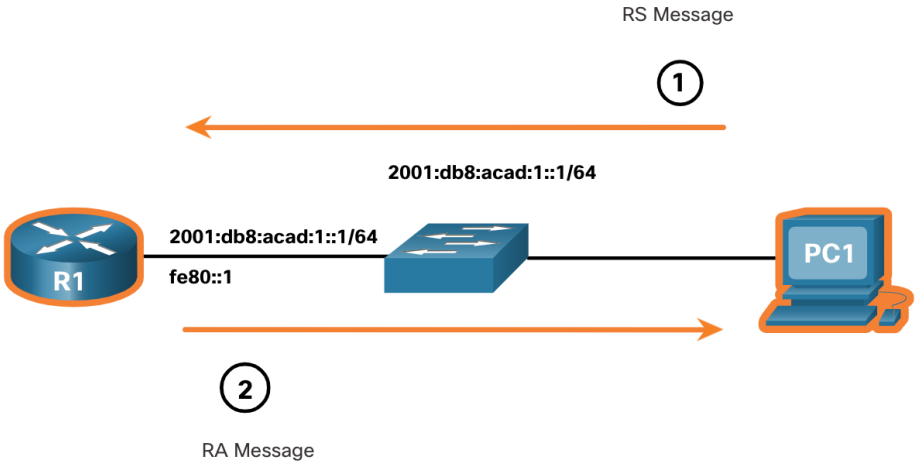
ICMPv6 Messages (Cont.)

- 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.



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."

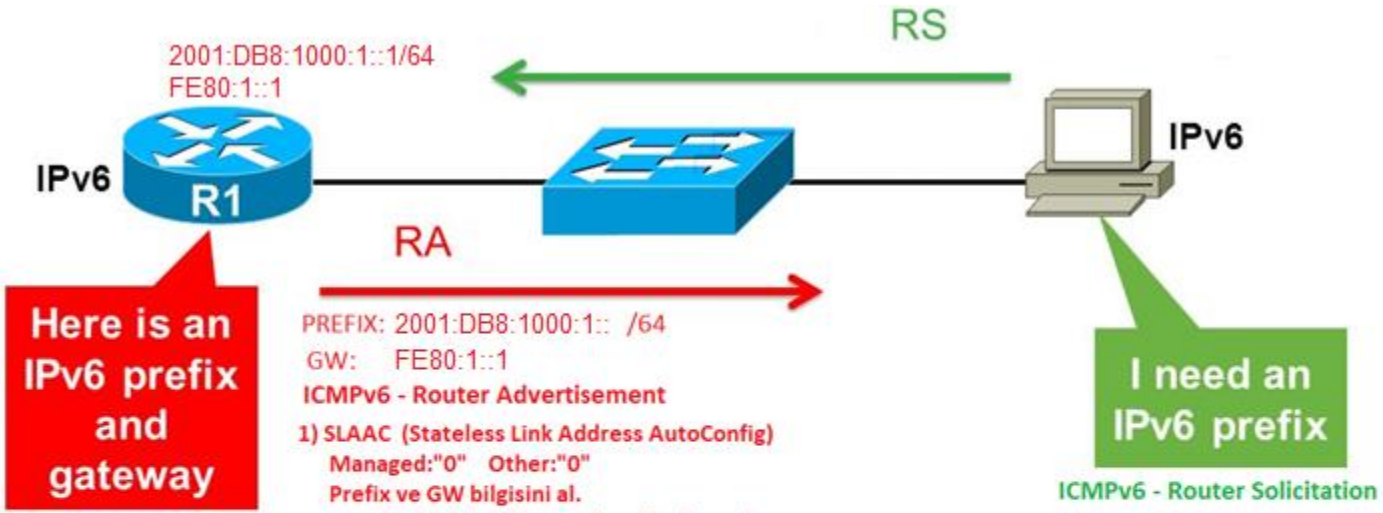


SLAAC
IPv6 adreslerini aşağıdaki bilgileri kullanarak kendin türet:

Managed:0 Other:0
PREFIX: 2001:db8:acad:1::/64
Router LLA (gateway): FE80::1

IPv6 Global Unicast Adresini Dinamik Yapılandırma

ICMPv6 Router Solicitation (RS)
ICMPv6 Router Advertisement (RA)



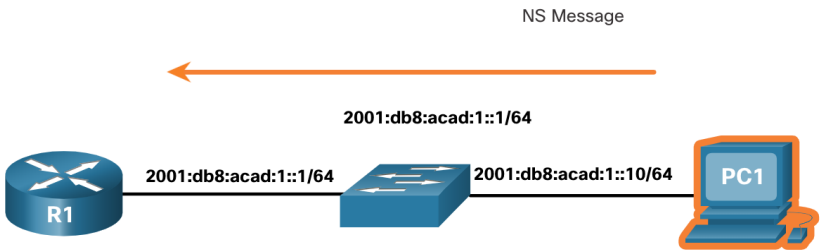
1) SLAAC (Stateless Link Address AutoConfig)
   Managed:"0" Other:"0"
   Prefix ve GW bilgisini al.
   InterfaceID (Host Kısmını kendin oluştur)
   DNS'i statik ver.

2) SLAAC + DHCP
   Managed:"0" Other:"1"
   Prefix ve GW bilgisini al.
   InterfaceID (Host Kısmını kendin oluştur)
   DNS gibi diğer bilgileri DHCP sunucusuna sor.

3) Stateful DHCP (Stateful: DHCP sunucusu kime ne IP adresi verdiğinin kaydını tutuyor)
   Managed:"1" Other:"0"
   Herşeyi DHCP Sunucusuna sor. (Ben IPv6 adresi vermiyorum)

ICMPv6 Messages (Cont.)

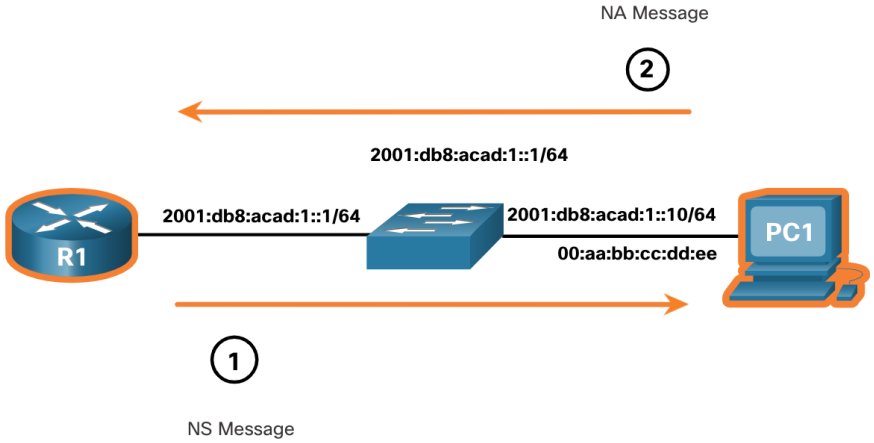
- A device assigned a global IPv6 unicast or link-local unicast address, may perform **duplicate address detection (DAD)** to ensure that the IPv6 address is unique.
- To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address.
- If 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.

ICMPv6 Messages (Cont.)

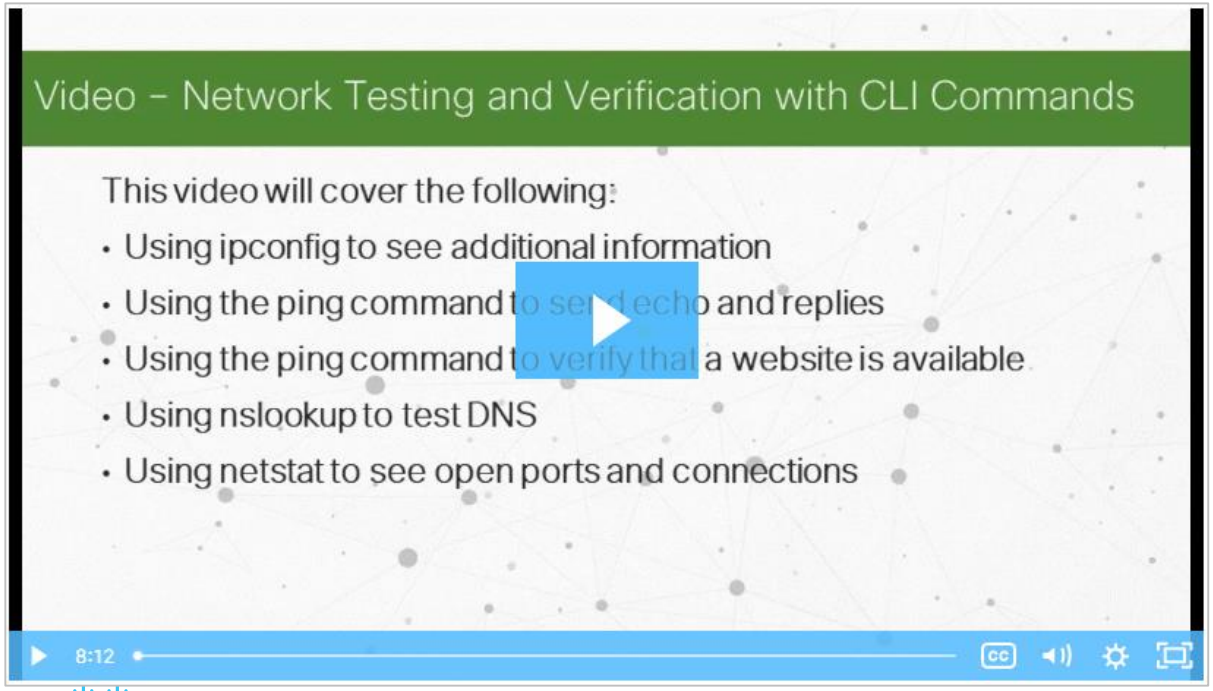
- **To determine the MAC address for the destination, the device will send an NS message to the solicited node address.**
- The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address.
-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



13.2 Ping and Traceroute Tests

Video - Network Testing and Verification with Windows CLI Commands

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



ipconfig /all

ping 192.168.1.1
ping www.cisco.com
nslookup www.cisco.com

netstat /?
netstat -b -n

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. «*Request timed out.*»

```
C:\>ping 208.67.220.220

Pinging 208.67.220.220 with 32 bytes of data:
Reply from 208.67.220.220: bytes=32 time=14ms TTL=56
Reply from 208.67.220.220: bytes=32 time=17ms TTL=56
Reply from 208.67.220.220: bytes=32 time=13ms TTL=56
Reply from 208.67.220.220: bytes=32 time=11ms TTL=56

Ping statistics for 208.67.220.220:
    Packets: Sent = 4, Received = 4,Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 17ms, Average = 13ms
```

```
C:\>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [104.66.32.105] with 32 bytes of data:
Reply from 104.66.32.105: bytes=32 time=5ms TTL=55
Reply from 104.66.32.105: bytes=32 time=6ms TTL=55
Reply from 104.66.32.105: bytes=32 time=5ms TTL=55
Reply from 104.66.32.105: bytes=32 time=5ms TTL=55

Ping statistics for 104.66.32.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

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 is2 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
```

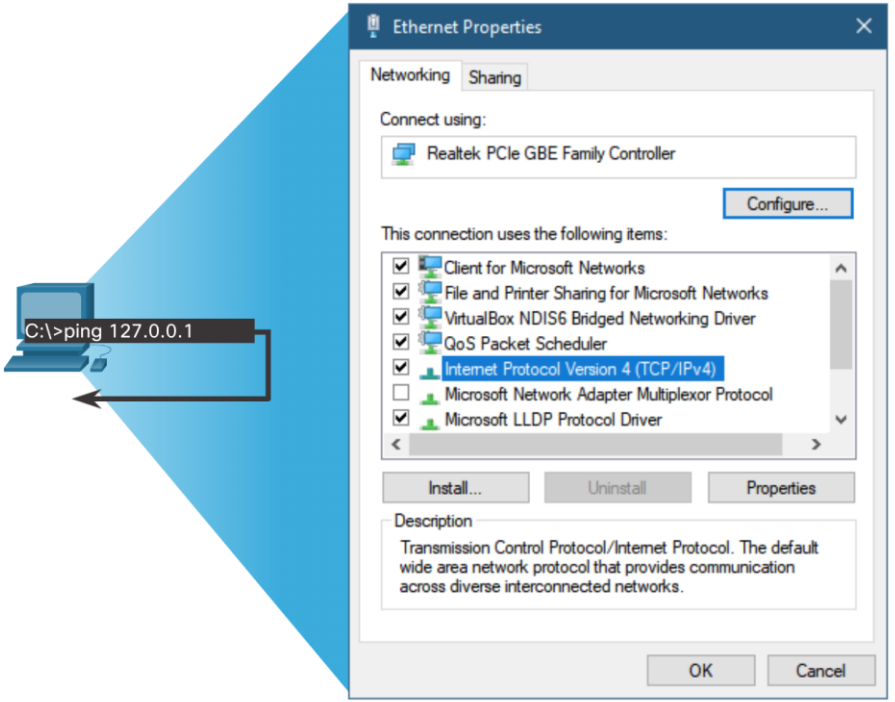
Ping – Test Connectivity (Contd.)

- 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 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.
- 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.

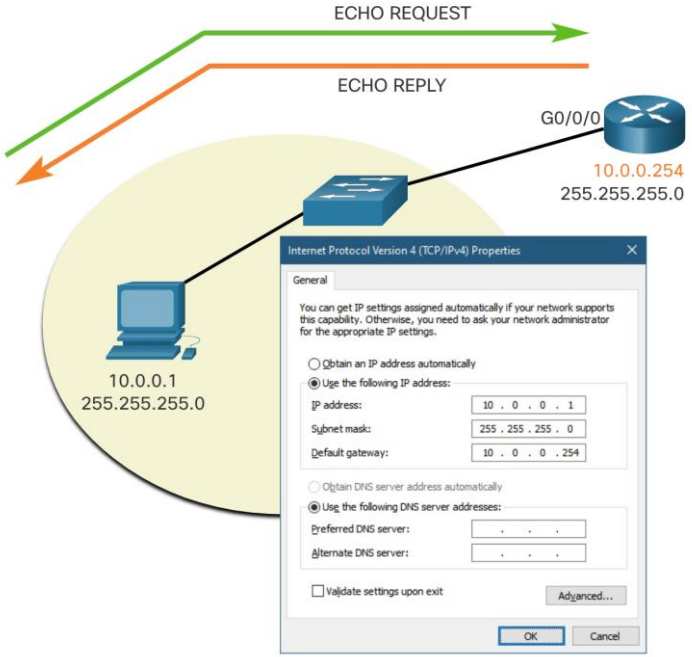


Ping the Default Gateway

The **ping** 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.

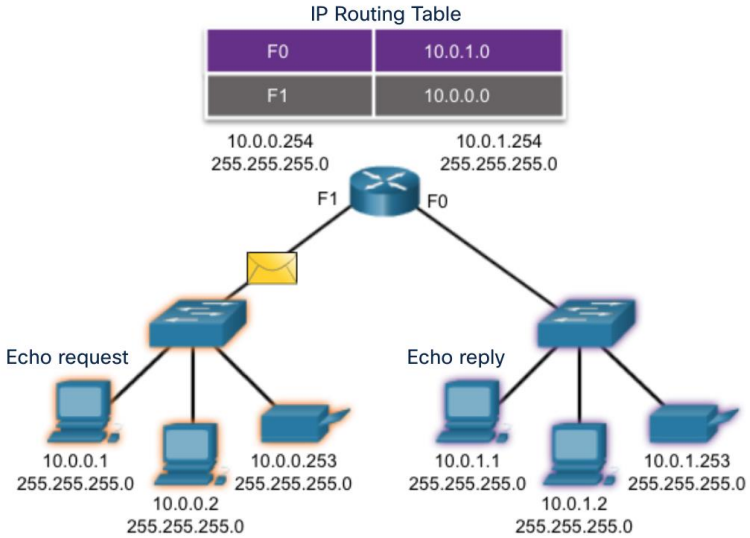


Ping a Remote Host

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.



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.

```
Select C:\Windows\system32\cmd.exe
C:\>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1     7 ms     5 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    12 ms    10 ms    10 ms  172.25.34.29
  4    14 ms    15 ms    14 ms  10.59.10.109
  5    20 ms    14 ms    13 ms  10.34.8.154
  6    15 ms    19 ms    13 ms  10.34.8.150
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10    65 ms    67 ms    67 ms  72.14.212.96
 11    70 ms    68 ms    68 ms  216.239.62.49
 12    70 ms    72 ms    79 ms  209.85.142.65
 13    64 ms    69 ms    68 ms  8.8.8.8

Trace complete.
```

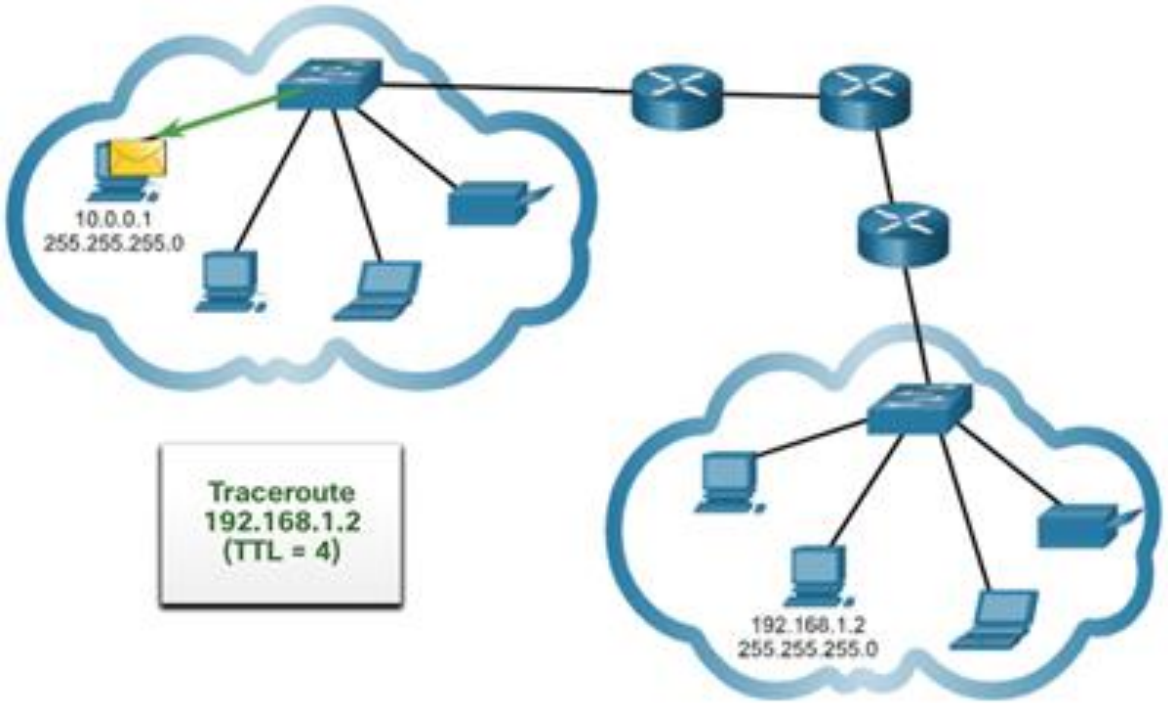
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2     1 msec     0 msec     0 msec
  2   192.168.20.2     2 msec     1 msec     0 msec
  3   192.168.30.2     1 msec     0 msec     0 msec
  4   192.168.40.2     0 msec     0 msec     0 msec
```

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.

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 ou at the first router. This router then responds with a ICMPv4 Time Exceeded message.
- Traceroute then progressively increments the TTL field (2, 3, 4...) each sequence of messages. This provides the trace with the address 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.



13.3 Module Practice and Quiz

What did I learn in this module?

- The purpose of ICMP 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.
- 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 (used by IPv4 and IPv6) uses ICMP echo request and echo reply messages to test connectivity between hosts
- Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host.
- Traceroute (tracert) generates a list of hops that were successfully reached along the path.


CISCO