CISCO CCNA1

CCNA Routing and Switching: Introduction to Networks

# HOOFDSTUK 7

# IP Addressing

DE HOGESCHOOL
MET HET NETWERK

Hogeschool PXL – Elfde-Liniestraat 24 – B-3500 Hasselt
www.pxl.be - www.pxl.be/facebook

# CCNA1 - Overzicht

- OSI model en de belangrijkste (LAN) protocollen.
- Data Flow in een LAN
  (verklaring volgens het OSI model).
- **IP** en subnetting.
- Het toepassen en onderzoeken van bovenstaande 3 in Packettrace oefeningen.

# Situering hoofdstuk 7

In hoofdstuk 7 worden IP adressen in detail besproken.
Opdat je IP adressen goed kan begrijpen is het belangrijk dat je Binair kan tellen.  Je moet omzettingen van 0 tot 255 vlot kunnen, alvorens je dit hoofdstuk kan begrijpen.

**Doelstellingen:**

- Ken de opbouw van een IPv4 adres en een subnetmask
- IP adresseringen kunnen ontleden
- Begrijpen en berekenen van het netwerkadres, broadcast adres, subnetmask, prefix, IP range en het aantal geldige IP adressen.
- Het verschil kennen tussen private en public adressen.
- Toekennen van IP adressering aan netwerk devices
- Het verschil kunnen uitleggen tussen public en private IP adressen
- Fouten in ip adressering kunnen troubleshooten (Packettrace oefening)
- Verschillen tussen unicast, multicast & broadcast benoemen
- Classe netwerken kennen en het verschil met classless netwerken
- Het nut van een subnet / prefix begrijpen en toepassen
- IPv4 en IPv6 kunnen onderscheiden
- Basis kennis van IPv6 (noodzaak, types, notatie, structuur, verkorte schrijfwijze)
- De verschillende manier om connectiviteit te testen kennen en kunnen toepassen. (7.3.2)

# Situering hoofdstuk 7

**Activity & PT:**

- 7.1.2.4 ANDing to derermine the network address
- 7.1.4.8 Public or private IPv4 addresses
- 7.2.1.3 IPv4 Issues and solutions
- 7.2.2.4 Practicing IPv6 address representations7
- 7.2.3.5 Identiy types of IPv6 addresses
- 7.1.3.8 PT investigate Unicast, Broadcast and multicast traffic
- 7.2.4.9 PT Configuring IPv6 addressing
- 7.3.2.4 PT Verifying IPv4 and IPv6 addressing
- 7.3.2.6 PT Pinging and tracing to test the path
- 7.3.2.9 PT Troubleshooting IPv4 and IPv6 addressing

**Leertip:**

Studeer aandachtig de theorie van IPv4 en IPv6. Dit heb je nodig om subnetten (Chapter 8) te begrijpen. Leg de focus of de verschillende activities. De PT oefening 7.3.2.9 geeft een praktische samenvatting van het hoofdstuk.

Cisco Networking Academy
Mind Wide Open

# Chapter 7:

# Explore the Network

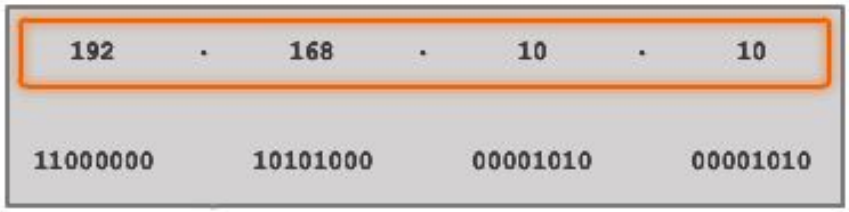
Introduction to Networks v5.1

# Chapter Outline


# Topic 7.1.1:
# Binary and Decimal Conversion

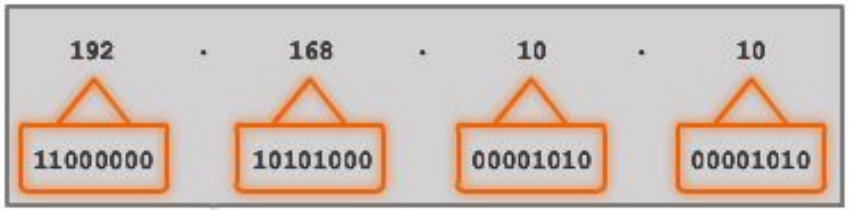
# 7.1.1.1 IPv4 Addresses

Dotted Decimal Address



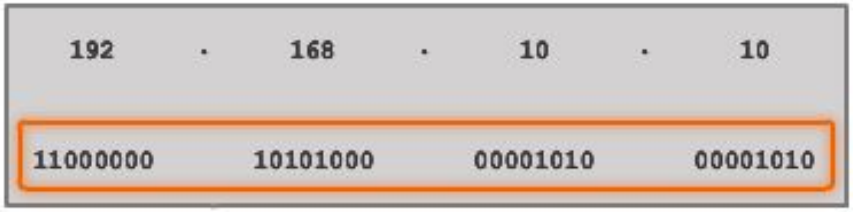

192.168.10.10 is an IP address that is assigned to a computer.

Octets




This address is made up of four different octets.

32-Bit Address

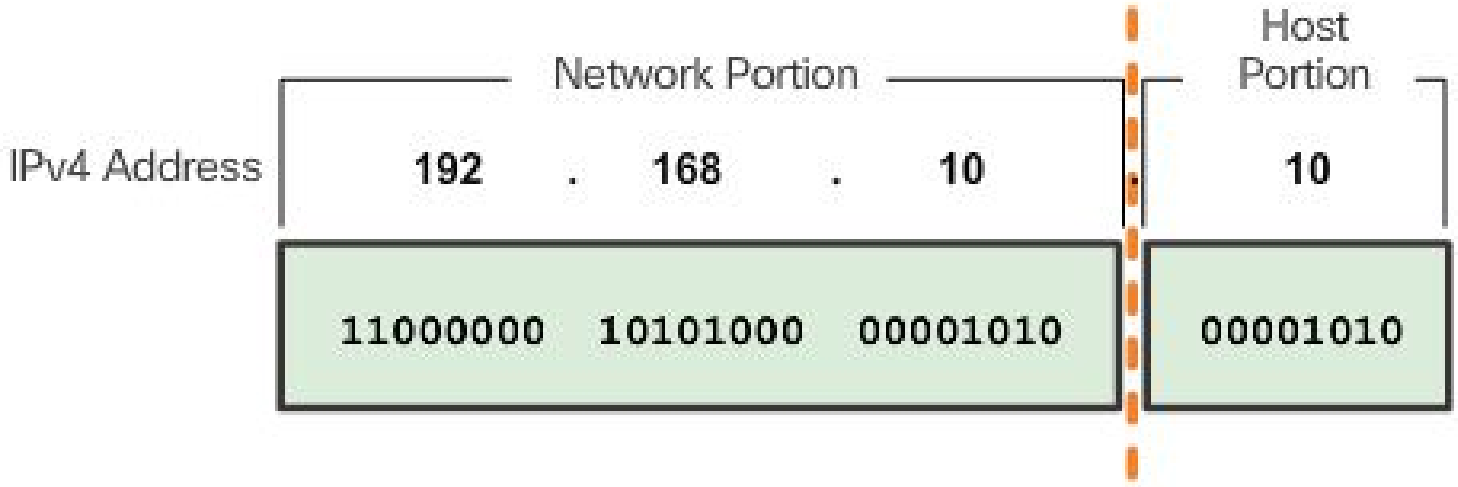



The computer stores the address as the entire 32-bit data stream.

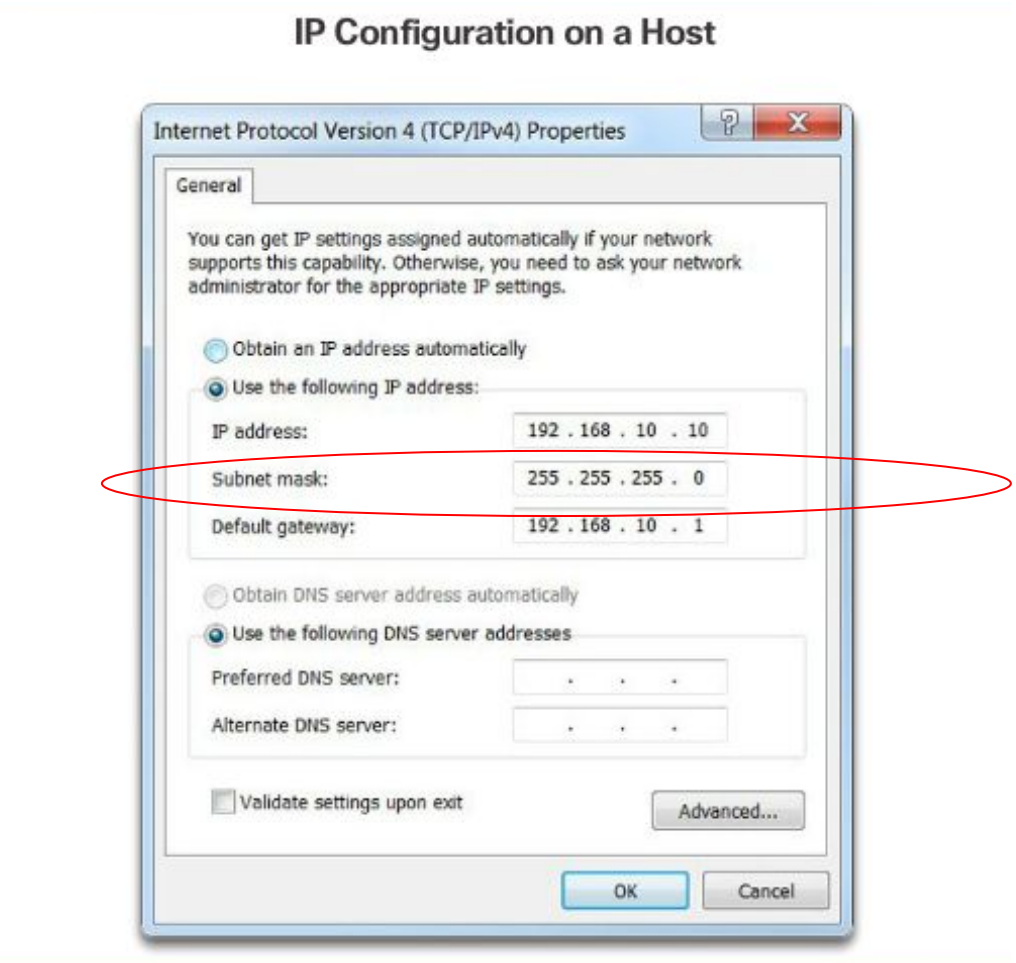
# Topic 7.1.2:
# IPv4 Address Structure

# 7.1.2.1 Network and Host Portions

One portion of the 32 bit IPv4 address identifies the network, and another portion identifies the host.

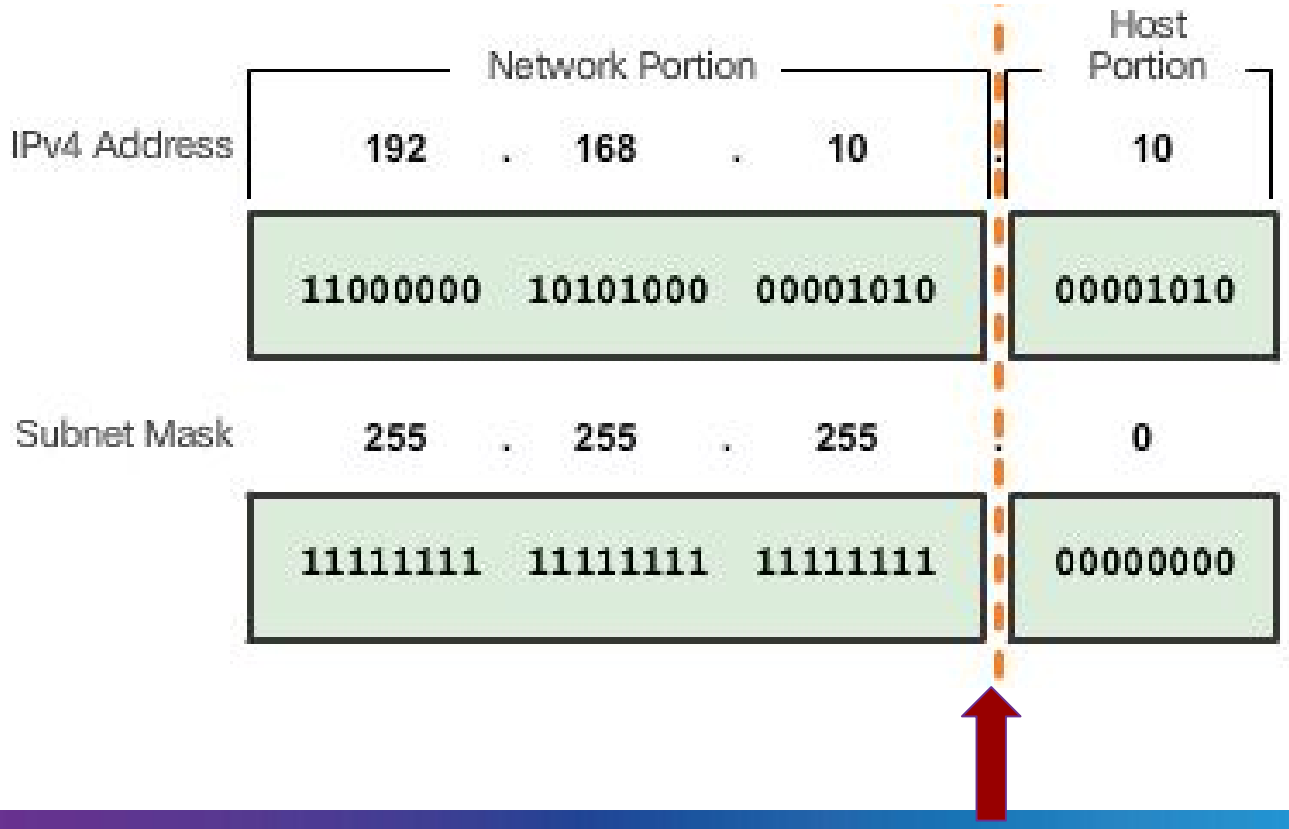


# 7.1.2.2 The Subnet Mask



# 7.1.2.2 The Subnet Mask (cont.)

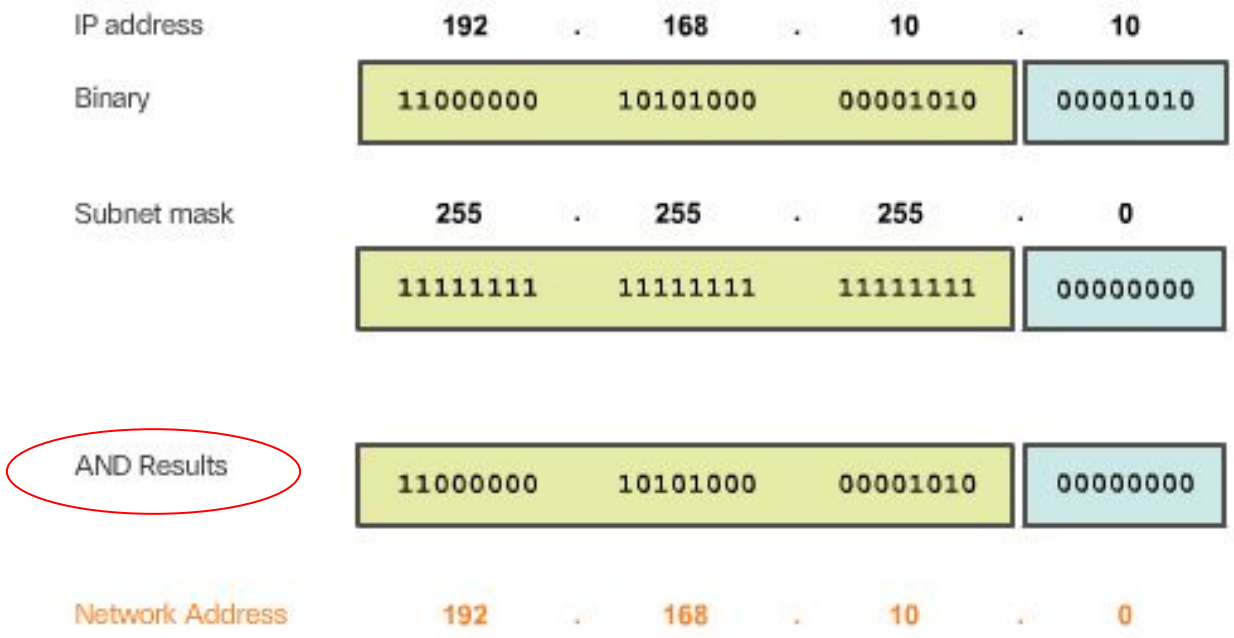
- Comparing the IP Address and the Subnet Mask
- The 1s in the subnet mask identify the network portion while the 0s identify the host portion.



# 7.1.2.3 ANDing

1 AND 1 = 1
0 AND 1 = 0
0 AND 0 = 0
1 AND 0 = 0

- Logical AND is the comparison of two bits.
- ANDing between the IP address and the subnet mask yields the network address.



# 7.1.2.4 Activity – ANDing to Determine the Network Address

**Activity – ANDing to Determine the Network Address**

Use the ANDing process to determine the Network Address (in binary and decimal formats).

| | | | | |
|---|---|---|---|---|
| Host Address | 10 | 115 | 134 | 194 |
| Subnet Mask | 255 | 255 | 248 | 0 |
| Host Address in binary | 00001010 | 01110011 | 10000110 | 11000010 |
| Subnet Mask in binary | 11111111 | 11111111 | 11111000 | 00000000 |
| Network Address in binary | | | | |
| Network Address in decimal | | | | |

Check Reset New Number

# 7.1.2.4 Activity – ANDing to Determine the Network Address

**Activity – ANDing to Determine the Network Address**

Use the ANDing process to determine the Network Address (in binary and decimal formats).

Correct

The binary and decimal versions of the network address are correct! Please click New Number to continue.

| | | | | |
|---|---|---|---|---|
| Host Address | 10 | 115 | 134 | 194 |
| Subnet Mask | 255 | 255 | 248 | 0 |
| Host Address in binary | 00001010 | 01110011 | 10000110 | 11000010 |
| Subnet Mask in binary | 11111111 | 11111111 | 11111000 | 00000000 |
| Network Address in binary | **00001010** | **01110011** | **10000000** | **00000000** |
| Network Address in decimal | **10** | **115** | **128** | **0** |

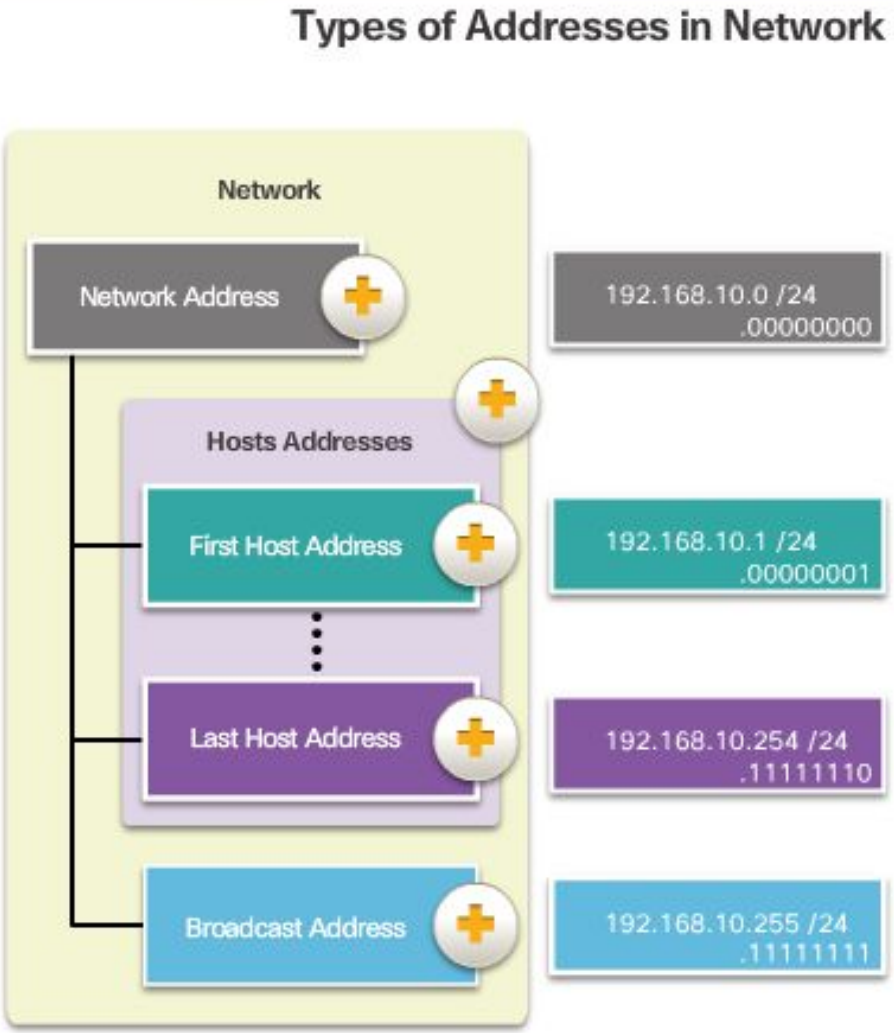
Check Reset New Number

# 7.1.2.5 The Prefix Length

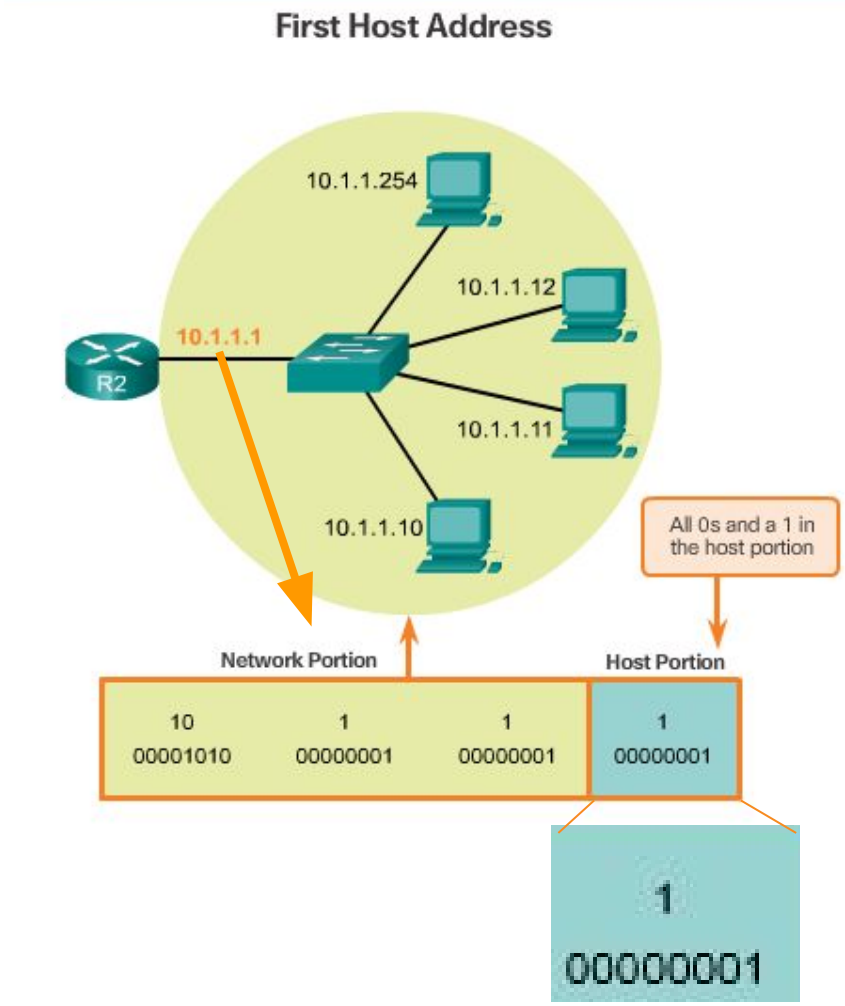
- Shorthand method of identifying a subnet mask.
- It is the number of bits set to 1 in the subnet mask.
- Written in “slash notation”, a “/” followed by the number of bits set to 1.

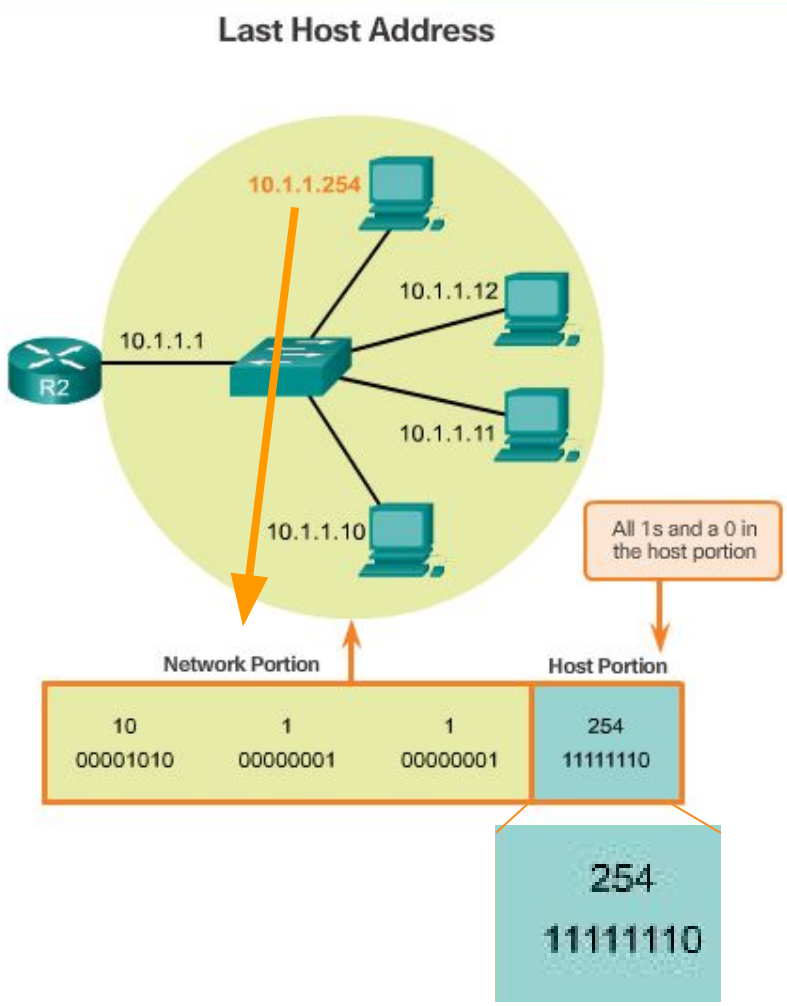
| Subnet Mask | 32-bit Address | Prefix Length |
|---|---|---|
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | /8 |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | /16 |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

# 7.1.2.6 Network, Host, and Broadcast Addresses

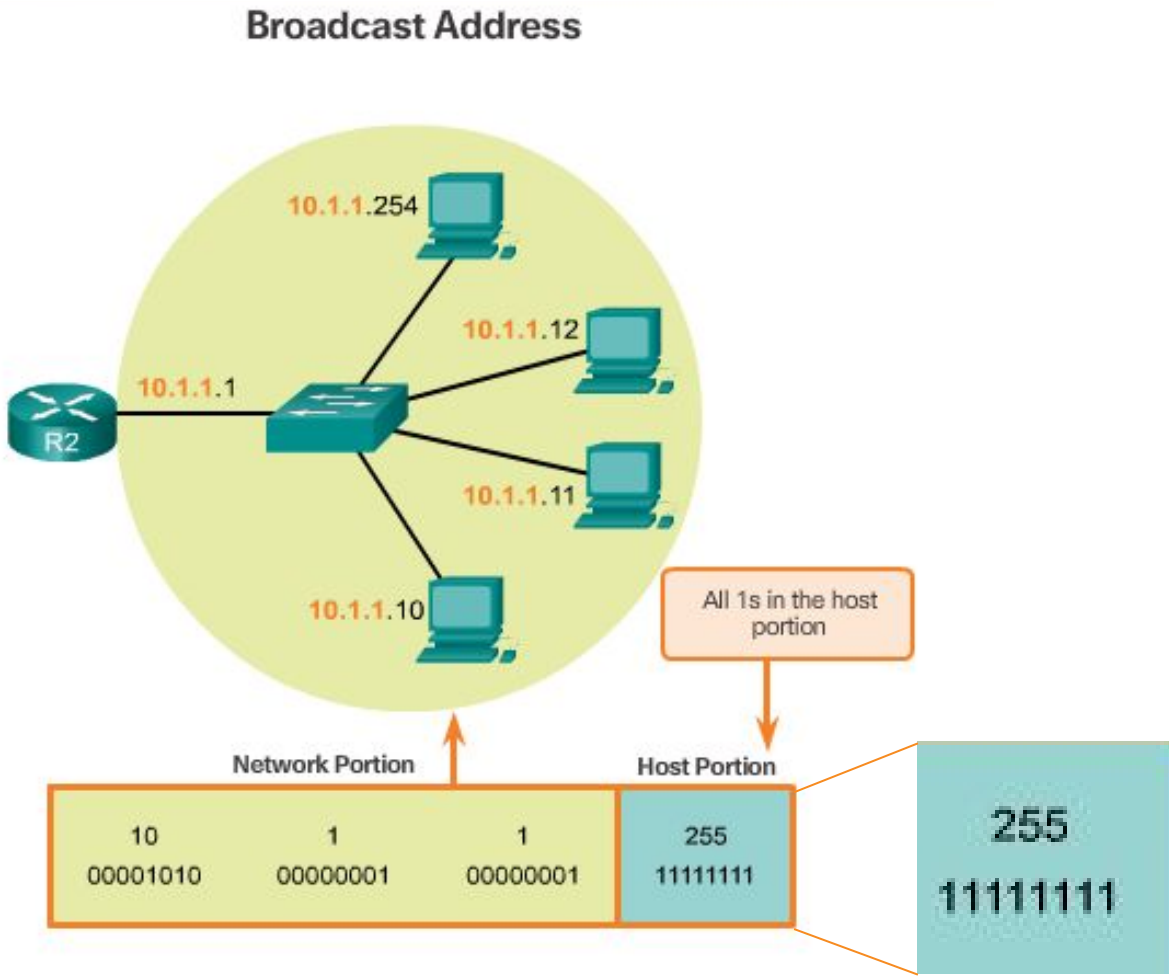


# 7.1.2.6 Network, Host, and Broadcast Addresses (cont.)



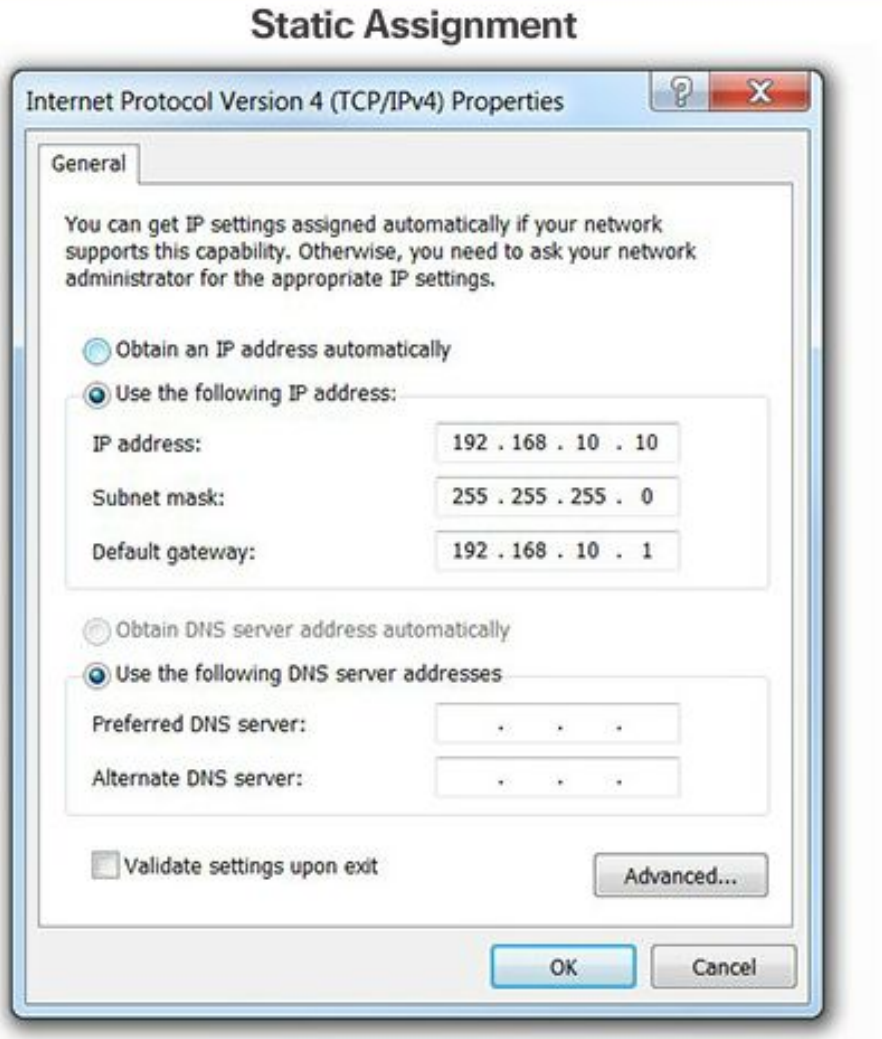
# 7.1.2.6 Network, Host, and Broadcast Addresses (cont.)



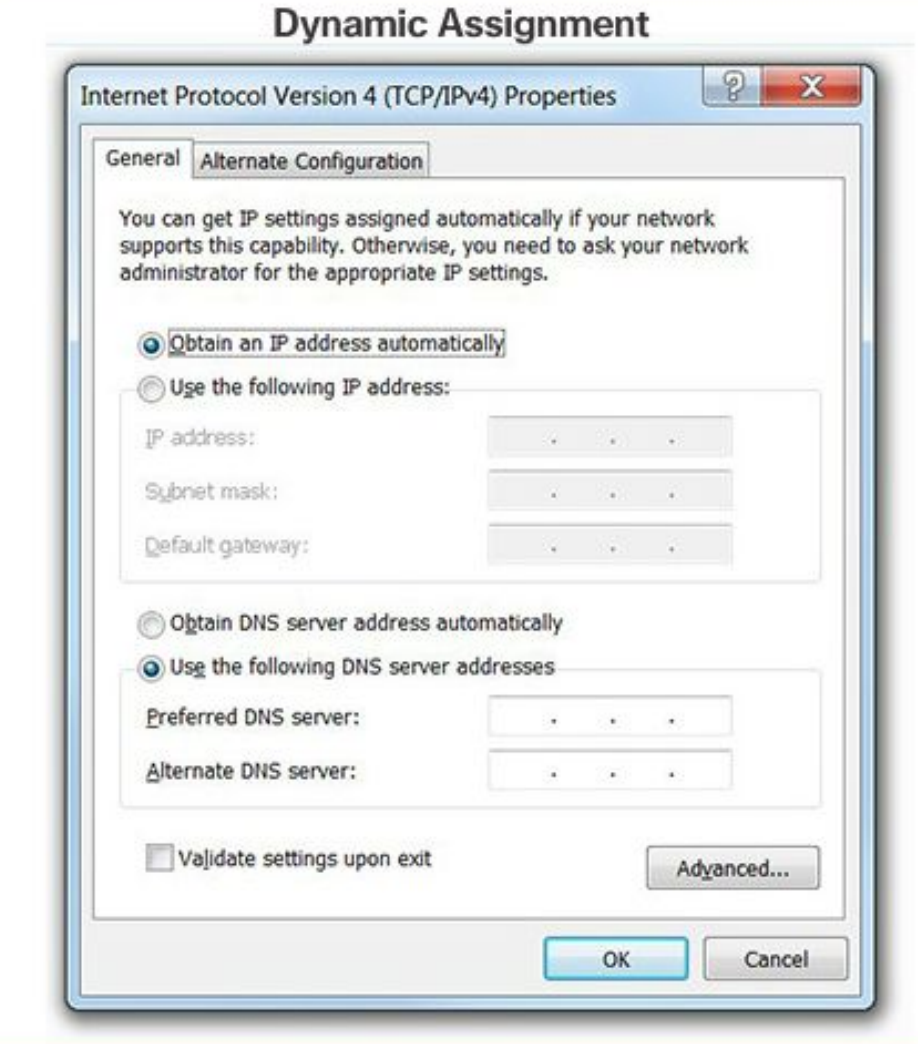

See VIDEO DEMONSTRATION

# Topic 7.1.3:
# IPv4 Unicast, Broadcast, and Multicast

# 7.1.3.1 Static IPv4 Address Assignment to a Host

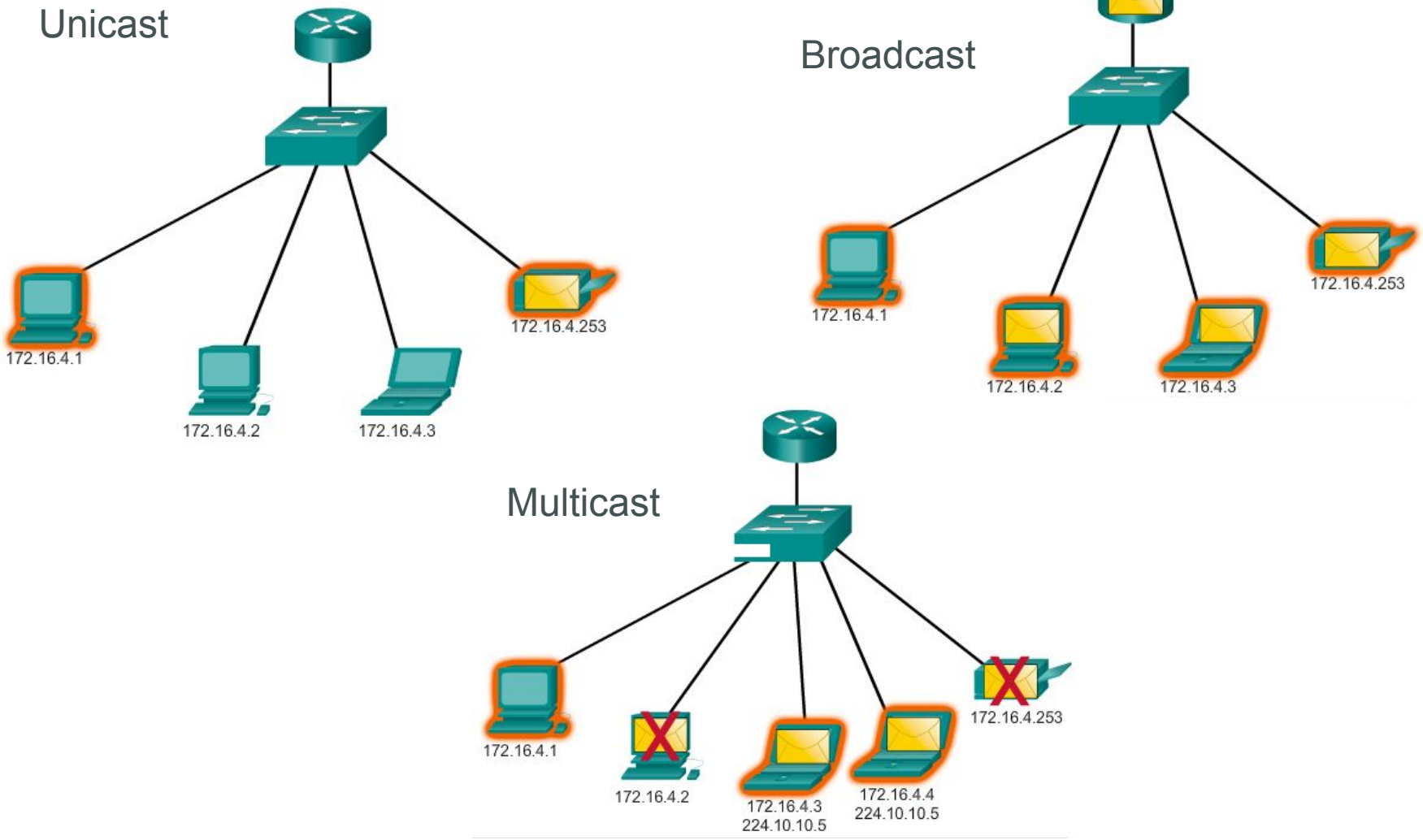


# 7.1.3.1 Dynamic IPv4 Address Assignment to a Host



see animation online

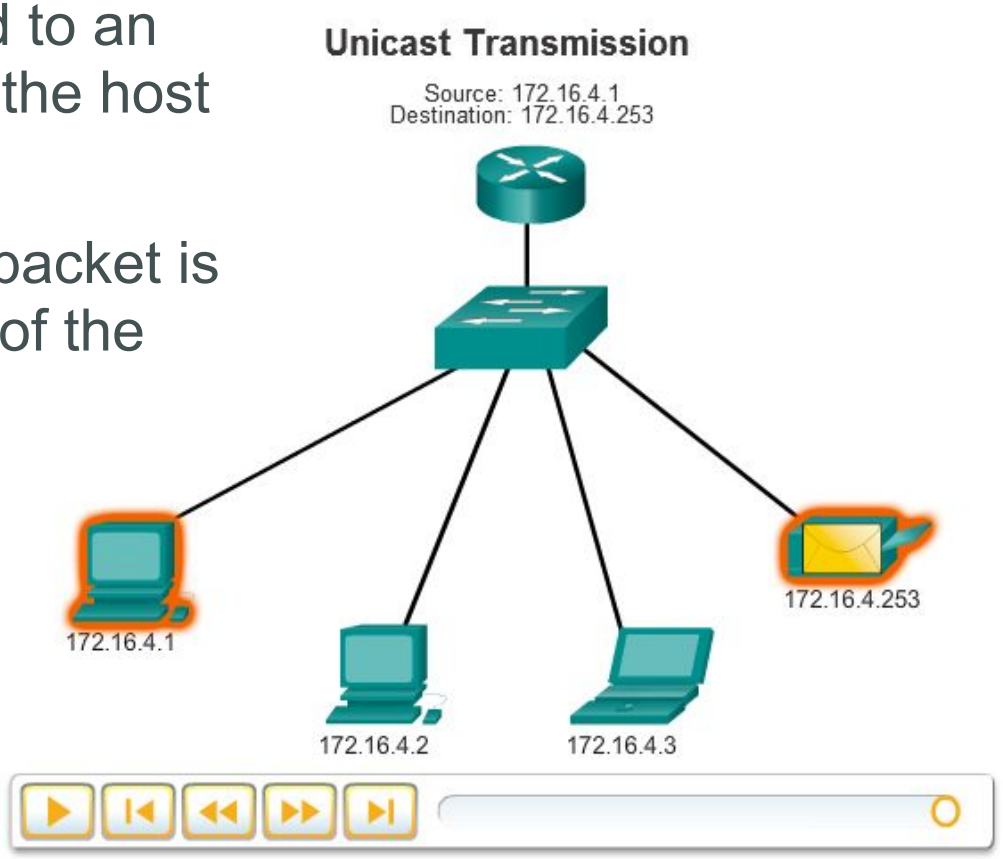
# 7.1.3.3 IPv4 Communication



see animation online

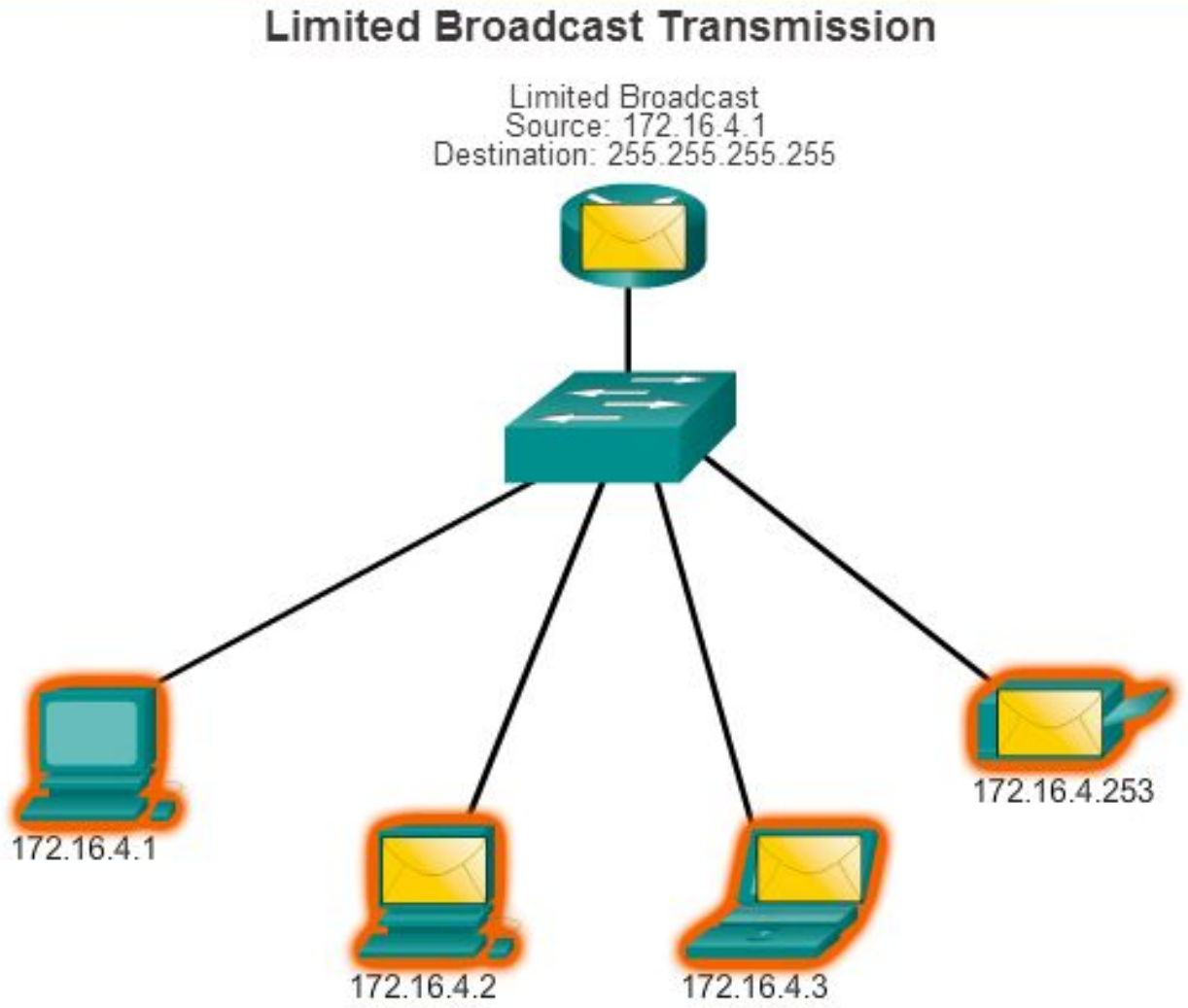
# 7.1.3.4 Unicast Transmission

- Unicast communication is used for normal host-to-host communication.
- The unicast address applied to an end device is referred to as the host address.
- The source address of any packet is always the unicast address of the originating host.



see animation online

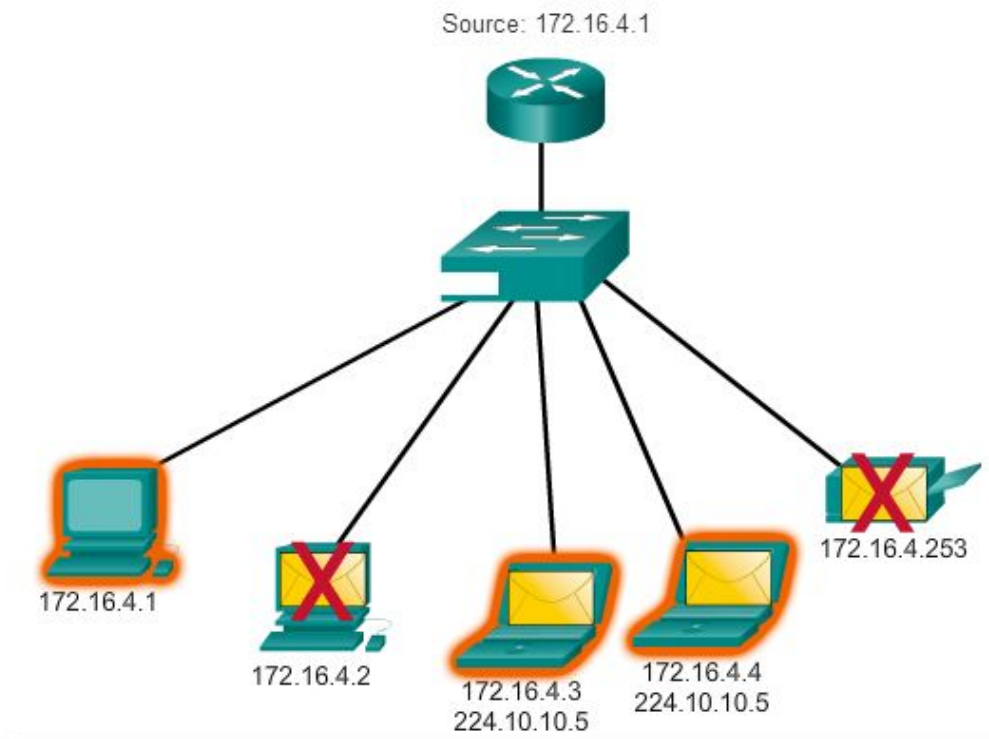
# 7.1.3.5 Broadcast Transmission



see animation online

# 7.1.3.6 Multicast Transmission

- A host sends a single packet to a selected set of hosts that subscribe to a multicast group.
- The 224.0.0.0 to 239.255.255.255 range of addresses are reserved for multicast.

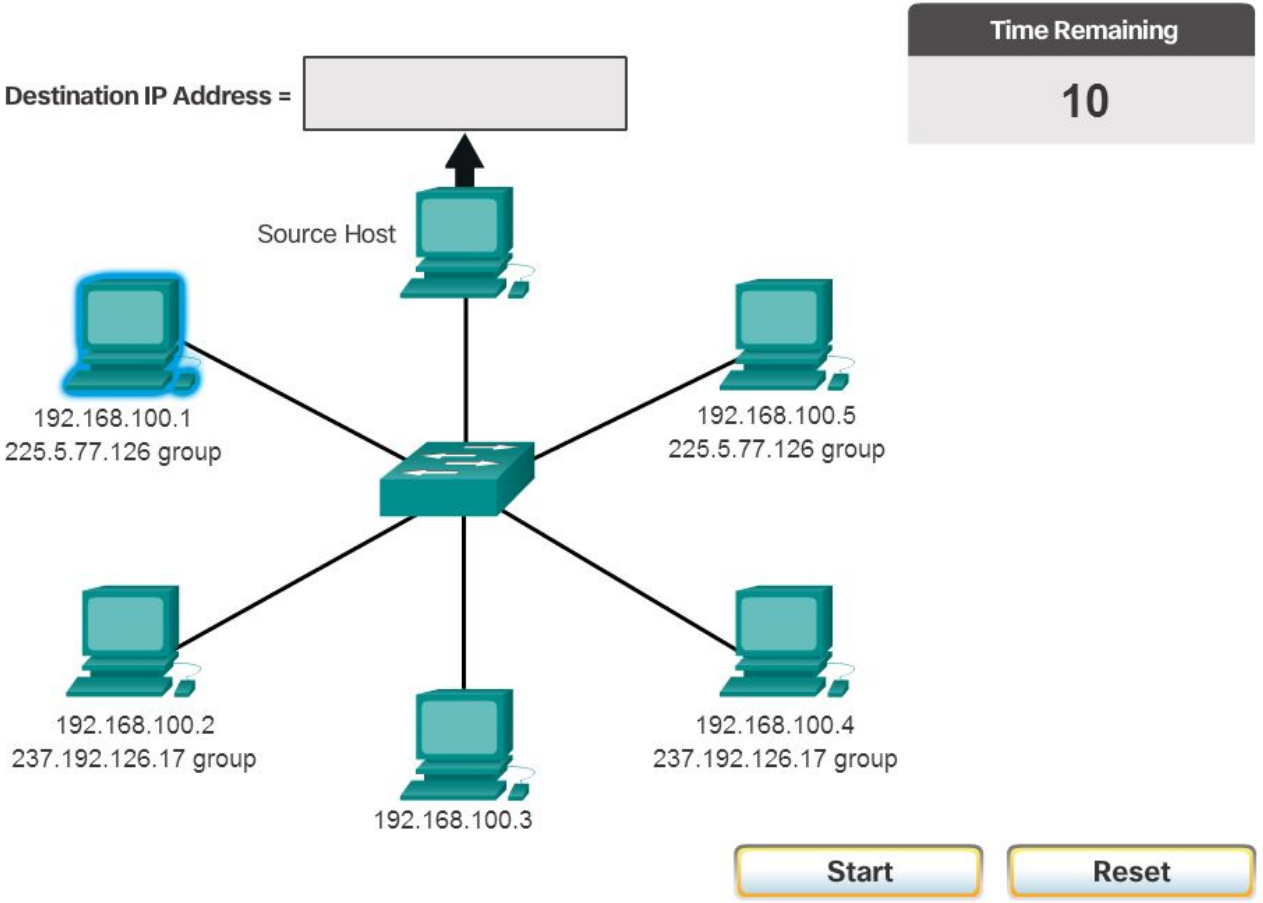


# 7.1.3.7 Activity - Unicast, Broadcast, or Multicast

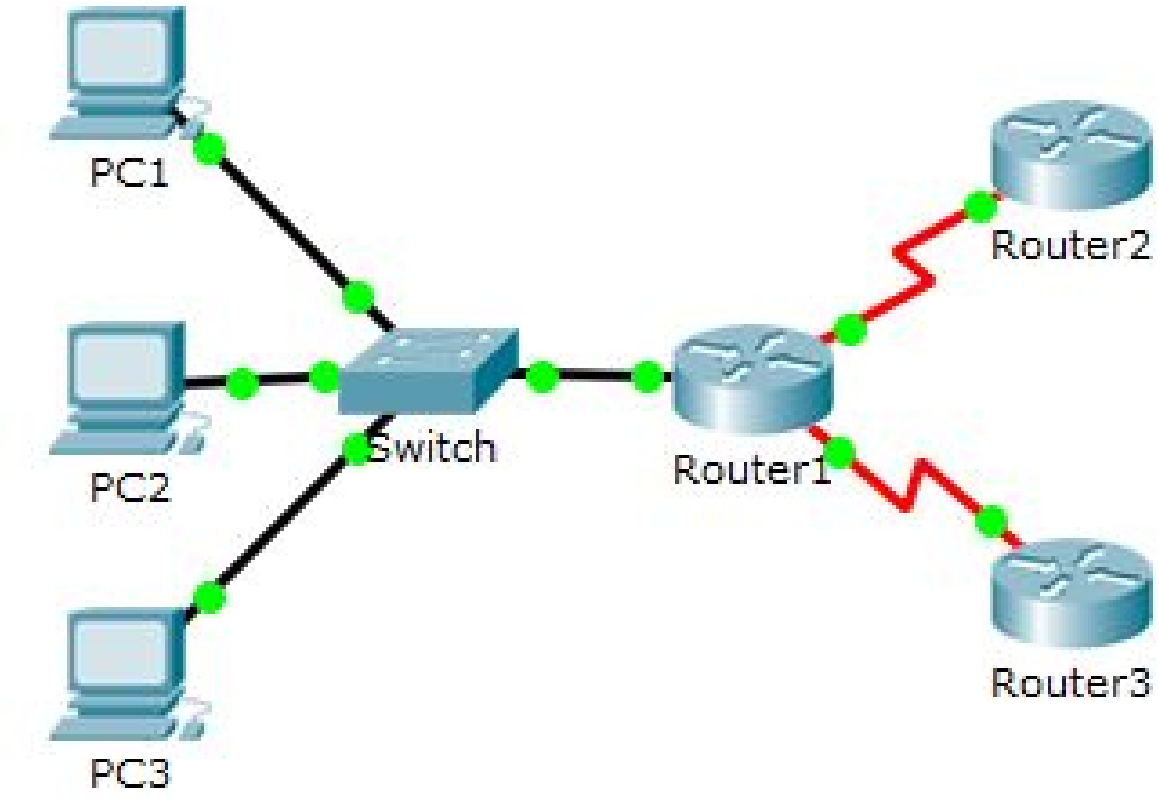
**Activity – Unicast, Broadcast, or Multicast?**

Click **Start** to view the Destination IP Address. Next, click the host(s) which will receive a packet based on the address type (Unicast, Broadcast or Multicast).

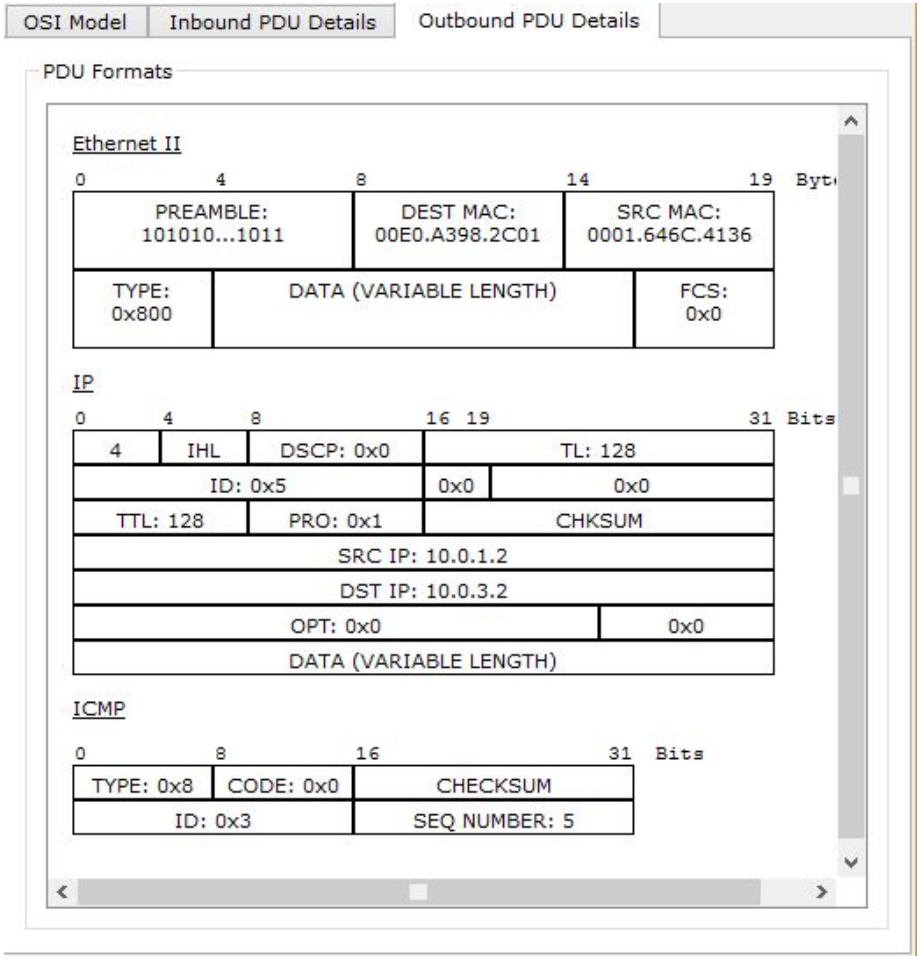
This is a timed activity.

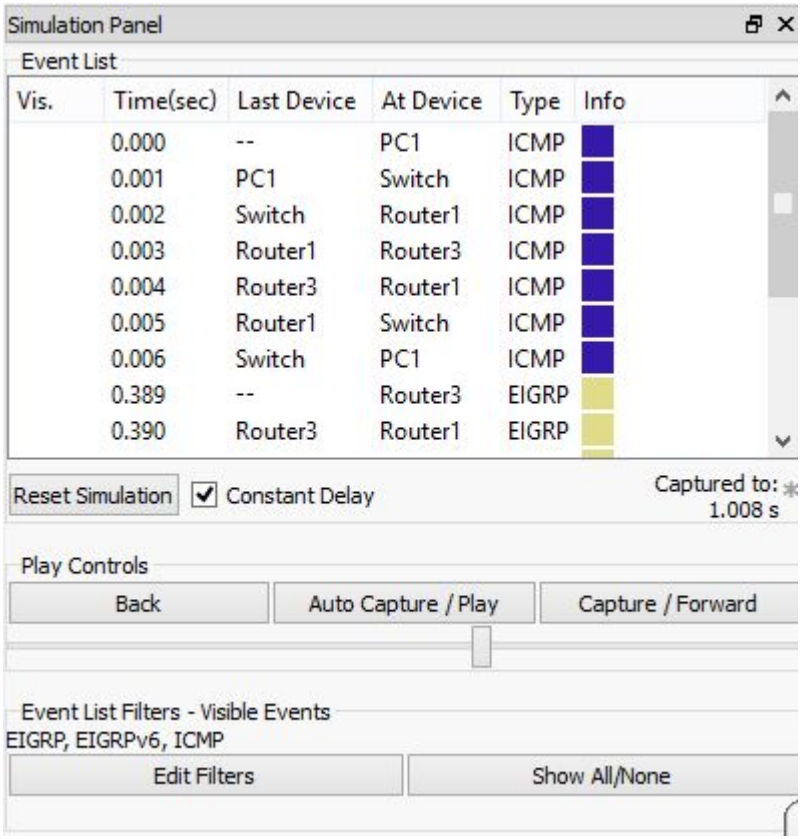


# 7.1.3.8 PT- Investigate Unicast, Broadcast, and Multicast



# 7.1.3.8 Packet Tracer - Investigate Unicast, Broadcast



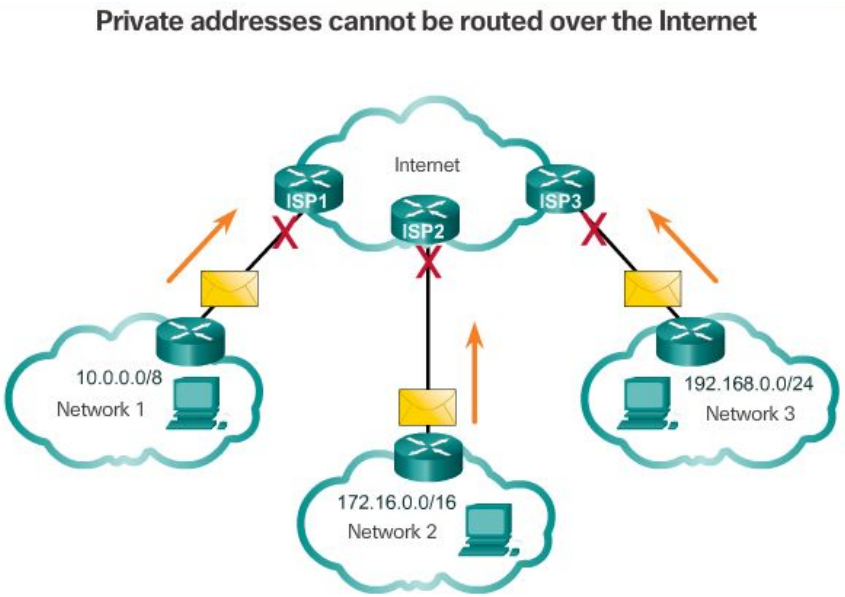



# Topic 7.1.4:
# Types of IPv4 Addresses

# 7.1.4.1 Public and Private IPv4 Addresses

## Private Addresses:

- 10.0.0.0/8 or 10.0.0.0 to10.255.255.255
- 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255
- 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255



# 7.1.4.2 Activity – Pass or Block IPv4 Addresses

**Activity**

Decide to Pass or Block each IP address depending on whether it is Public (the Internet) or Private (small local network).

Click Start to begin and click on either Pass or Block.

| Points |
| --- |
| 5 |


Start Reset

# 7.1.4.3 Special Use IPv4 Addresses

- Loopback addresses
  127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254
- Link-Local addresses or Automatic Private IP Addressing (APIPA) addresses
  169.254.0.0 /16 or
  169.254.0.1 to 169.254.255.254
- TEST-NET addresses
  192.0.2.0/24 or 192.0.2.1
  to 192.0.2.254

**Pinging the Loopback Interface**

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\NetAcad> 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\NetAcad> ping 127.1.1.1

Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>
```

# 7.1.4.6 Legacy Classful Addressing

| Class A Specifics | |
|---|---|
| Address block | 0.0.0.0 – 127.0.0.0* |
| Default Subnet Mask | /8 (255.0.0.0) |
| Maximum Number of Networks | 128 |
| Number of Host per Network | 16,777,214 |
| High order bit | 0xxxxxxx.___.___.___ |

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

| Class B Specifics | |
|---|---|
| Address block | 128.0.0.0 – 191.255.0.0 |
| Default Subnet Mask | /16 (255.255.0.0) |
| Maximum Number of Networks | 16,384 |
| Number of Host per Network | 65,534 |
| High order bit | 10xxxxxx.___.___.___ |

| Class C Specifics | |
|---|---|
| Address block | 192.0.0.0 – 223.255.255.0 |
| Default Subnet Mask | /24 (255.255.255.0) |
| Maximum Number of Networks | 2,097,152 |
| Number of Host per Network | 254 |
| High order bit | 110xxxxx.___.___.___ |

# 7.1.4.6 Classless Addressing

- Formal name is Classless Inter-Domain Routing (CIDR, pronounced “cider”).
- Created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address.

# 7.1.4.8 Activity - Public or Private IPv4 addresses

**Activity – Public or Private IPv4 Address**

Drag each IP address to the correct category: Public or Private.

172.16.35.2
192.168.3.5
192.0.3.15
64.104.0.22
209.165.201.30
192.168.11.5
172.16.30.30
10.55.3.168

Public

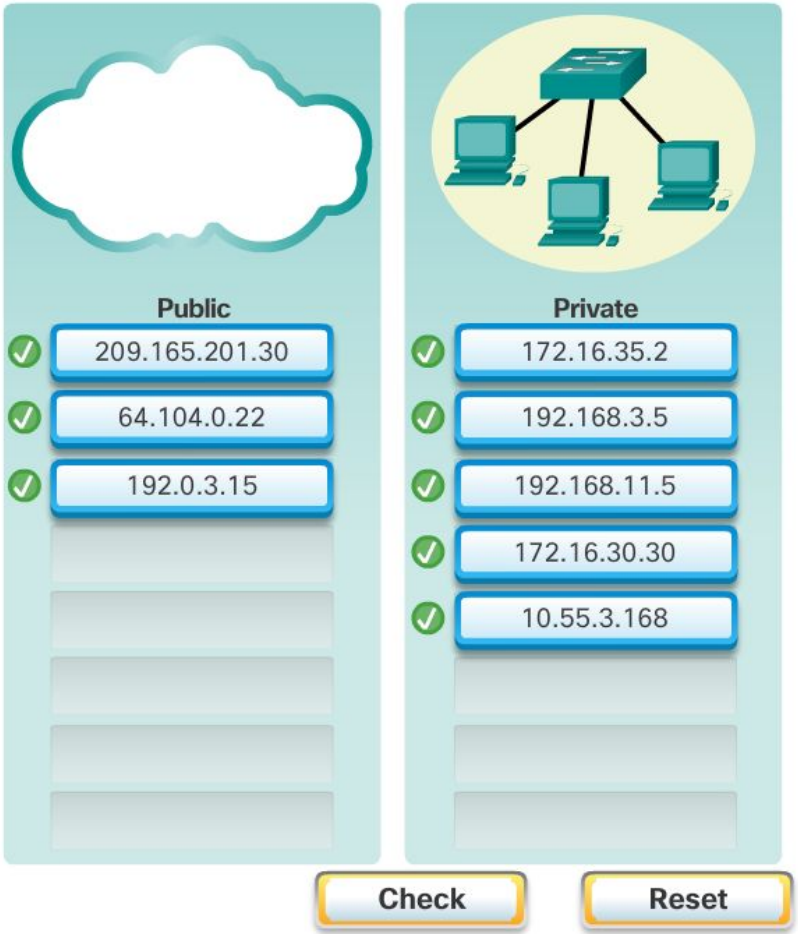
Private

Check Reset

# 7.1.4.8 Activity - Public or Private IPv4 addresses

**Activity – Public or Private IPv4 Address**

Drag each IP address to the correct category: Public or Private.




Correct

You have correctly identified all the IP addresses.

# Section 7.2: IPv6 Addresses

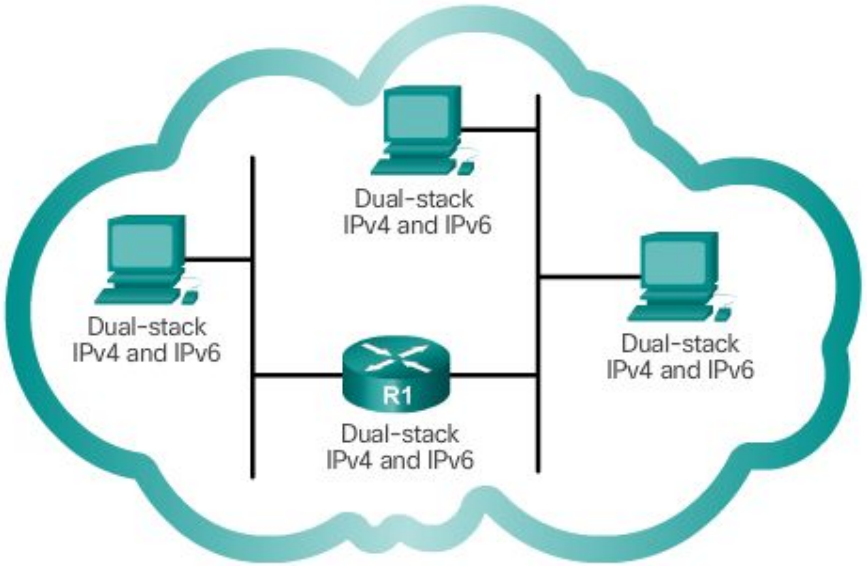
Upon completion of this section, you should be able to:

- Explain the need for IPv6 addressing.
- Describe the representation of an IPv6 address.
- Describe types of IPv6 network addresses.
- Configure global unicast addresses.
- Describe multicast addresses.

# Topic 7.2.1: IPv4 issues

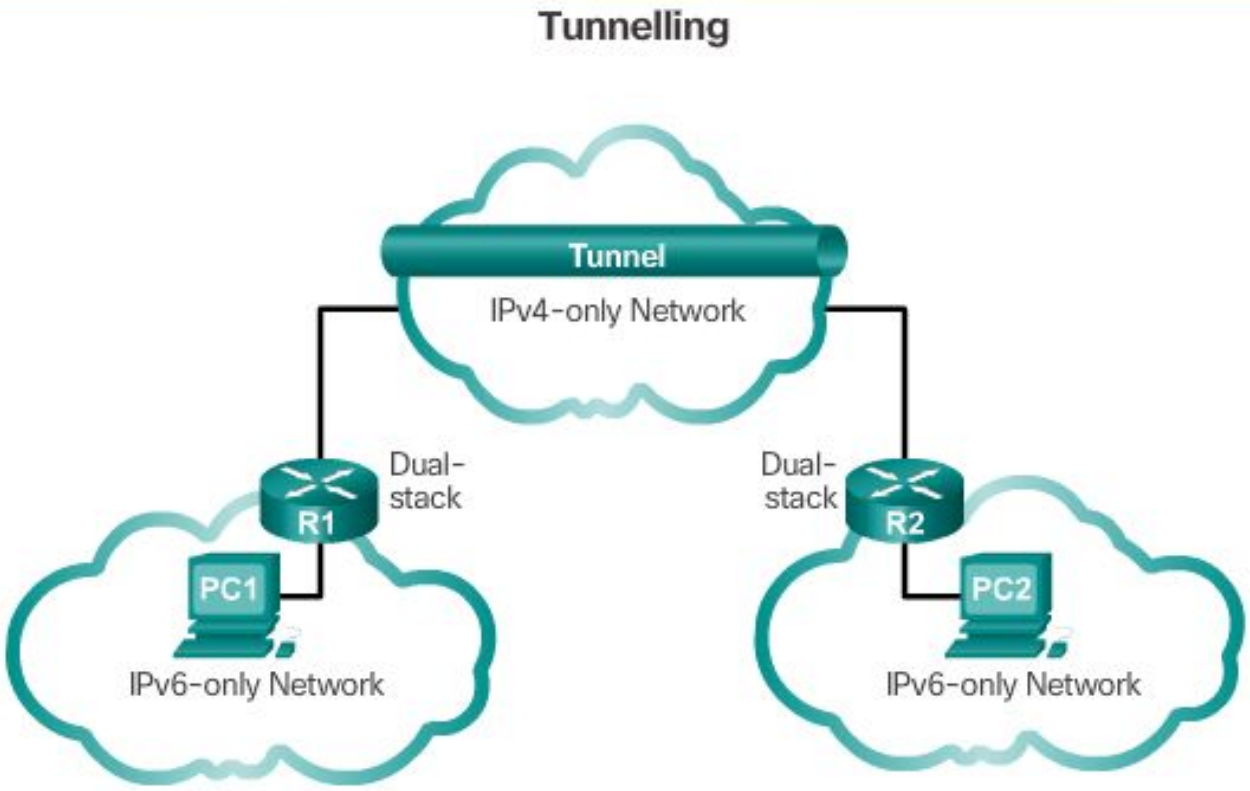
# 7.2.1.2 IPv4 and IPv6 Coexistence

- The migration techniques can be divided into three categories: Dual Stack, Tunneling, and Translation.
- **Dual-stack:** allows IPv4 and IPv6 to coexist on the same network. Devices run both IPv4 and IPv6 protocol stacks simultaneously.



# 7.2.1.2 IPv4 and IPv6 Coexistence (cont.)

- **Tunneling:** is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.



# 7.2.1.2 IPv4 and IPv6 Coexistence (cont.)

- **Translation**: Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet, and vice versa.

# 7.2.1.3 Activity - IPv4 Issues and Solutions

**Activity – IPv4 and IPv6 Terms and Descriptions**

Drag the IPv4 and IPv6 terms to the field next to the appropriate description.

- Dual Stack
- IPv4
- Tunneling
- IPv6
- Translation

| Term | Description |
|---|---|
| | 128-bit address/340 undecillion addresses. |
| | 32-bit address/4.3 billion addresses. |
| | Transports an IPv6 packet over IPv4 networks. |
| | Uses NAT64 to convert between IPv6 and IPv4. |
| | Allows IPv4 and IPv6 to coexist on the same network segment. |

Check Reset

# 7.2.1.3 Activity - IPv4 Issues and Solutions

**Activity – IPv4 and IPv6 Terms and Descriptions**

Drag the IPv4 and IPv6 terms to the field next to the appropriate description.

Correct

You have successfully matched the IPv4 and IPv6 terms to their descriptions.

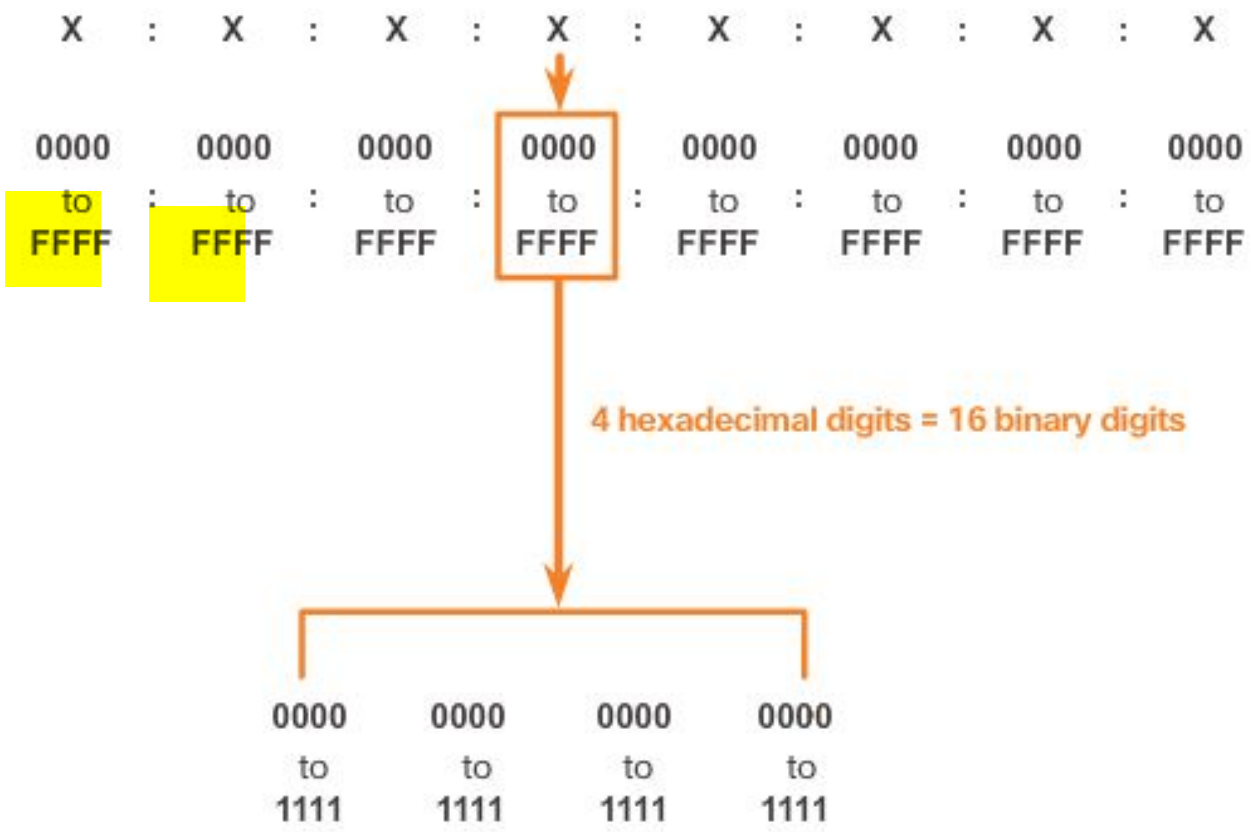
| Term | Description |
|---|---|
| IPv6 | 128-bit address/340 undecillion addresses. |
| IPv4 | 32-bit address/4.3 billion addresses. |
| Tunneling | Transports an IPv6 packet over IPv4 networks. |
| Translation | Uses NAT64 to convert between IPv6 and IPv4. |
| Dual Stack | Allows IPv4 and IPv6 to coexist on the same network segment. |

Check Reset

# Topic 7.2.2:
# IPv6 Address Structure

# 7.2.2.1 IPv6 Address Representation

## Hextets – 4 Hexadecimal digits = 16 binary digits



# 7.2.2.1 IPv6 Address Representation (cont.)

**Preferred Format Examples**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2001 | 0DB8 | 0000 | 1111 | 0000 | 0000 | 0000 | 0200 |
| 2001 | 0DB8 | 0000 | 00A3 | ABCD | 0000 | 0000 | 1234 |
| 2001 | 0DB8 | 000A | 0001 | 0000 | 0000 | 0000 | 0100 |
| 2001 | 0DB8 | AAAA | 0001 | 0000 | 0000 | 0000 | 0200 |
| FE80 | 0000 | 0000 | 0000 | 0123 | 4567 | 89AB | CDEF |
| FE80 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0001 |
| FF02 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0001 |
| FF02 | 0000 | 0000 | 0000 | 0000 | 0001 | FF00 | 0200 |
| 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0001 |
| 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 | 0000 |

# 7.2.2.2 Rule 1 – Omit Leading 0's

Example 1

| | |
|---|---|
| Preferred | 2001:0DB8:0000:1111:0000:0000:0000:0200 |
| No leading 0s | 2001: DB8: 0:1111: 0: 0: 0: 200 |

Example 2

| | |
|---|---|
| Preferred | 2001:0DB8:0000:A300:ABCD:0000:0000:1234 |
| No leading 0s | 2001: DB8: 0:A300:ABCD: 0: 0:1234 |

Example 3

| | |
|---|---|
| Preferred | FF02:0000:0000:0000:0000:0001:FF00:0200 |
| No leading 0s | FF02: 0: 0: 0: 0: 1:FF00: 200 |

# 7.2.2.3 Rule 2 – Omit All 0 Segments

Example 1

| | |
|---|---|
| Preferred | 2001:0DB8:0000:1111:0000:0000:0000:0200 |
| No leading 0s | 2001: DB8: 0:1111: 0: 0: 0: 200 |
| Compressed | 2001:DB8:0:1111::200 |

Example 2

| | |
|---|---|
| Preferred | 2001:0DB8:0000:0000:ABCD:0000:0000:0100 |
| No leading 0s | 2001: DB8: 0: 0:ABCD: 0: 0: 100 |
| Compressed | 2001:DB8::ABCD:0:0:100 |
| or | |
| Compressed | 2001:DB8:0:0:ABCD::100 |

Only one :: may be used.

# 7.2.2.3 Rule 2 – Omit All 0 Segments (cont.)

Example 3

| | |
|---|---|
| Preferred | FF02:0000:0000:0000:0000:0000:0000:0001 |
| No leading 0s | FF02: 0: 0: 0: 0: 0: 0: 1 |
| Compressed | FF02::1 |

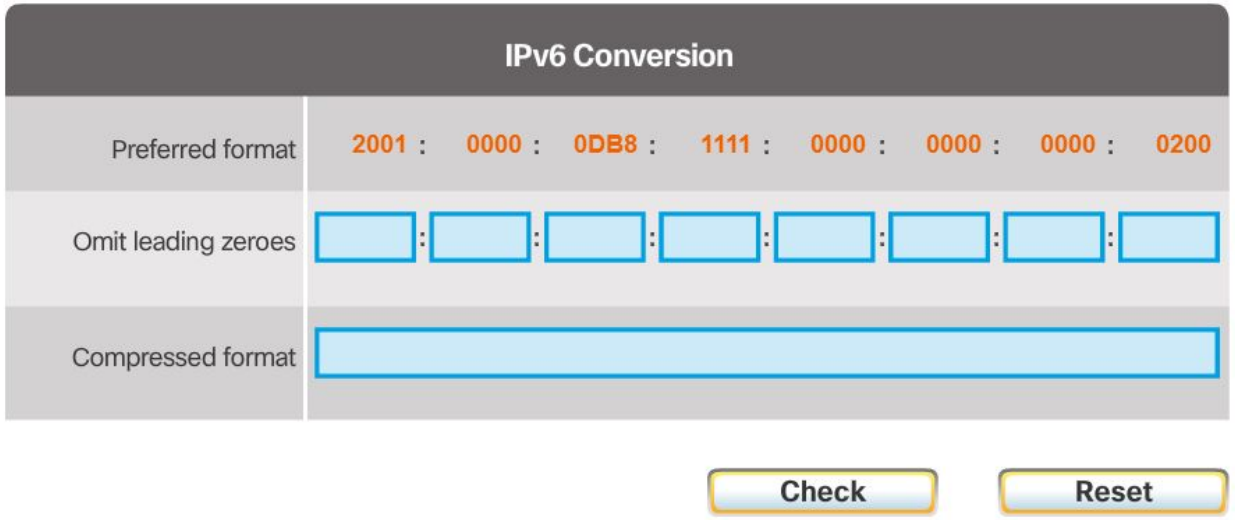
Example 4

| | |
|---|---|
| Preferred | 0000:0000:0000:0000:0000:0000:0000:0000 |
| No leading 0s | 0: 0: 0: 0: 0: 0: 0: 0 |
| Compressed | :: |

# 7.2.2.4 Activity – IPv6 Address Representations

**Activity – Practicing IPv6 Address Representations**

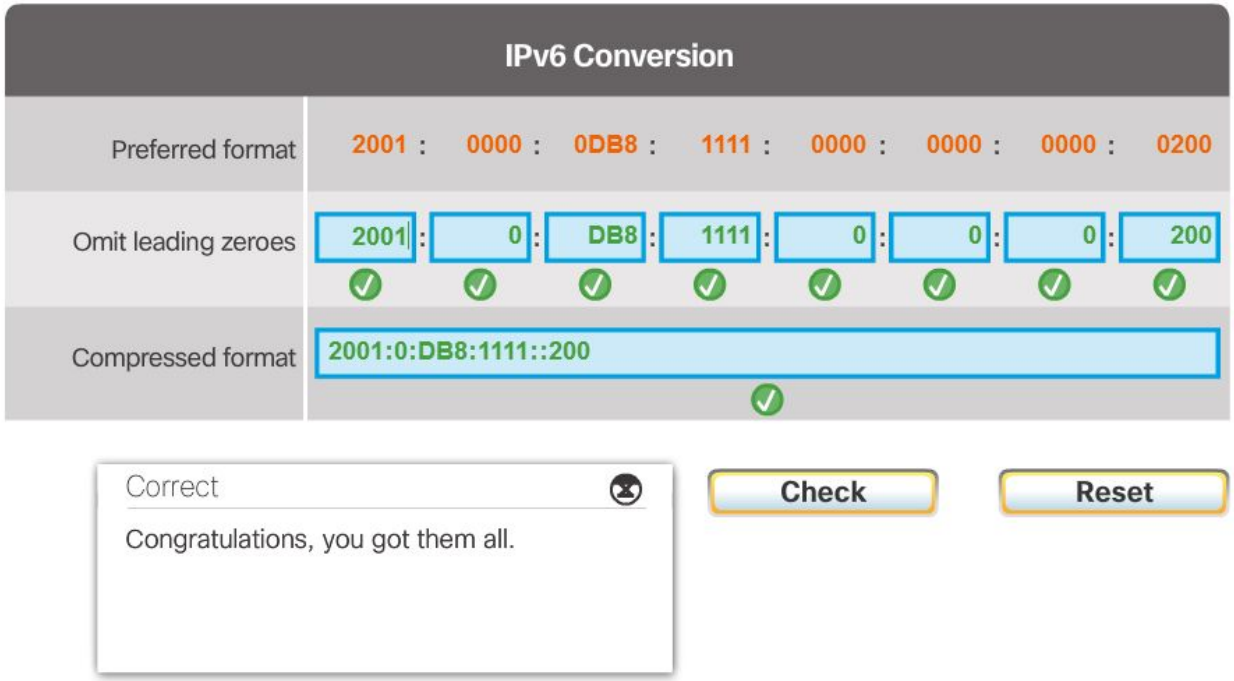
Convert the IPv6 addresses into short (omit the leading zeroes) and compressed forms. Use the numbers at the bottom of the page to continue this activity.



# 7.2.2.4 Activity – IPv6 Address Representations

**Activity - Practicing IPv6 Address Representations**

Convert the IPv6 addresses into short (omit the leading zeroes) and compressed forms. Use the numbers at the bottom of the page to continue this activity.



# Topic 7.2.3:
# Types of IPv6 Addresses

# 7.2.3.1 IPv6 Address Types

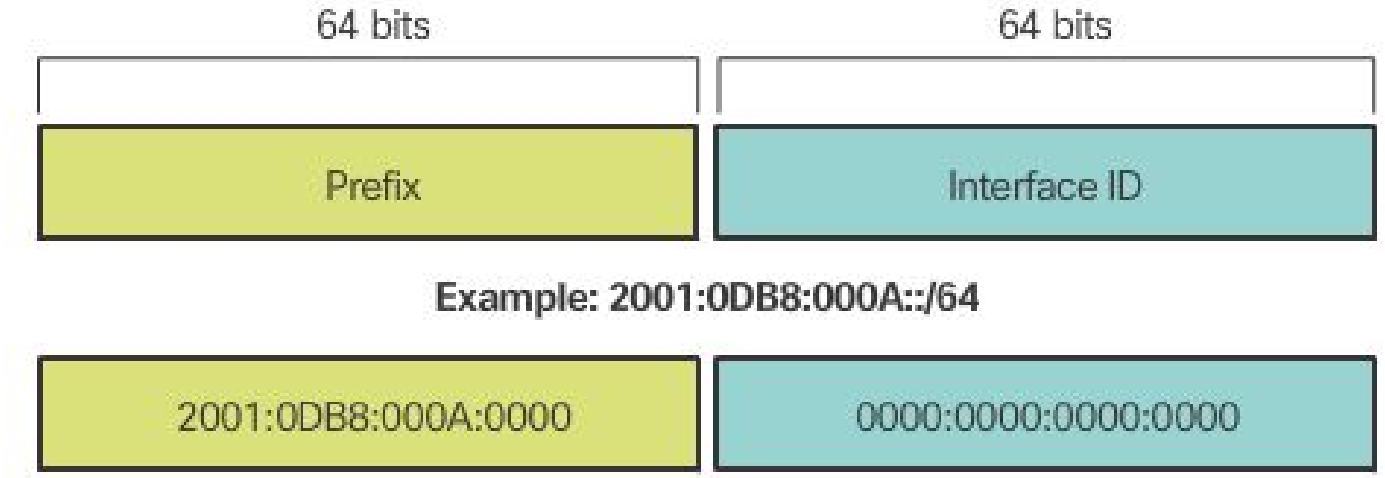
There are three types of IPv6 addresses:

- Unicast
- Multicast
- Anycast  (beyond the scope of this course)

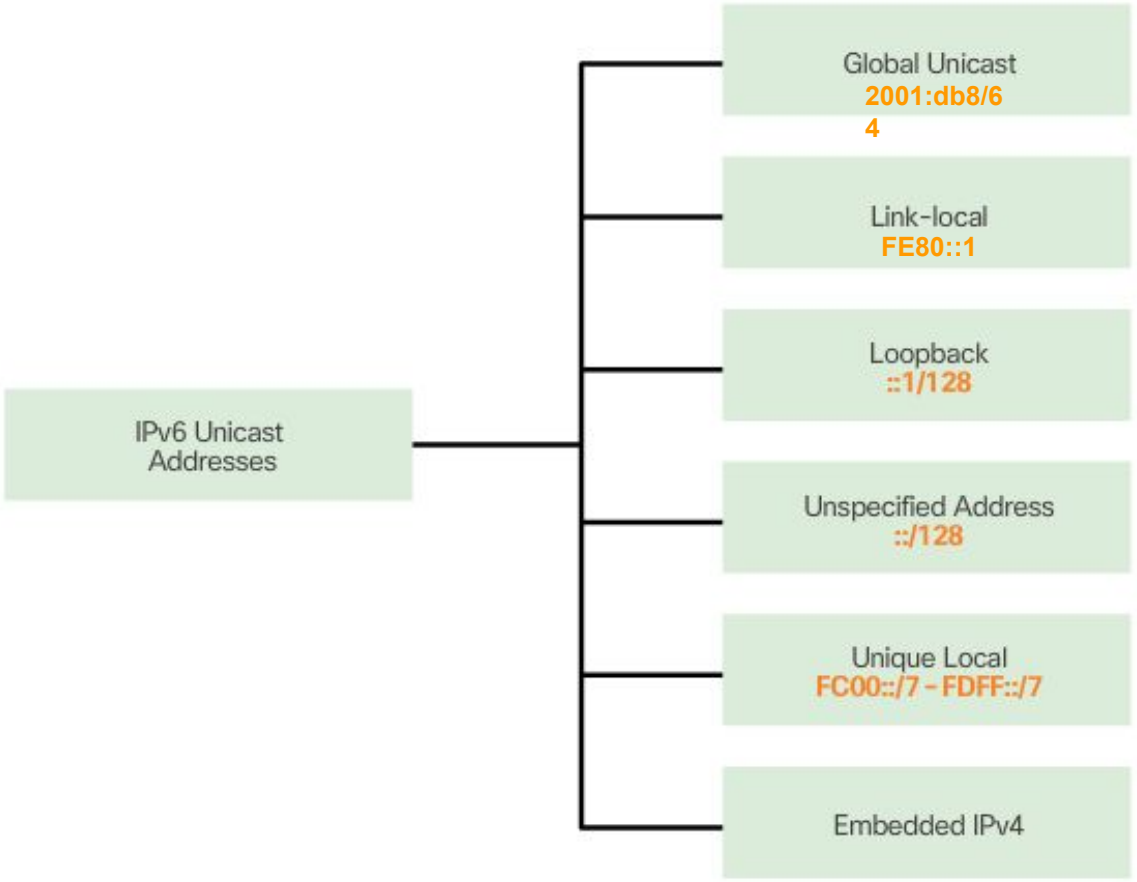
**Note: IPv6 does not have broadcast addresses.**

# 7.2.3.2 IPv6 Prefix Length

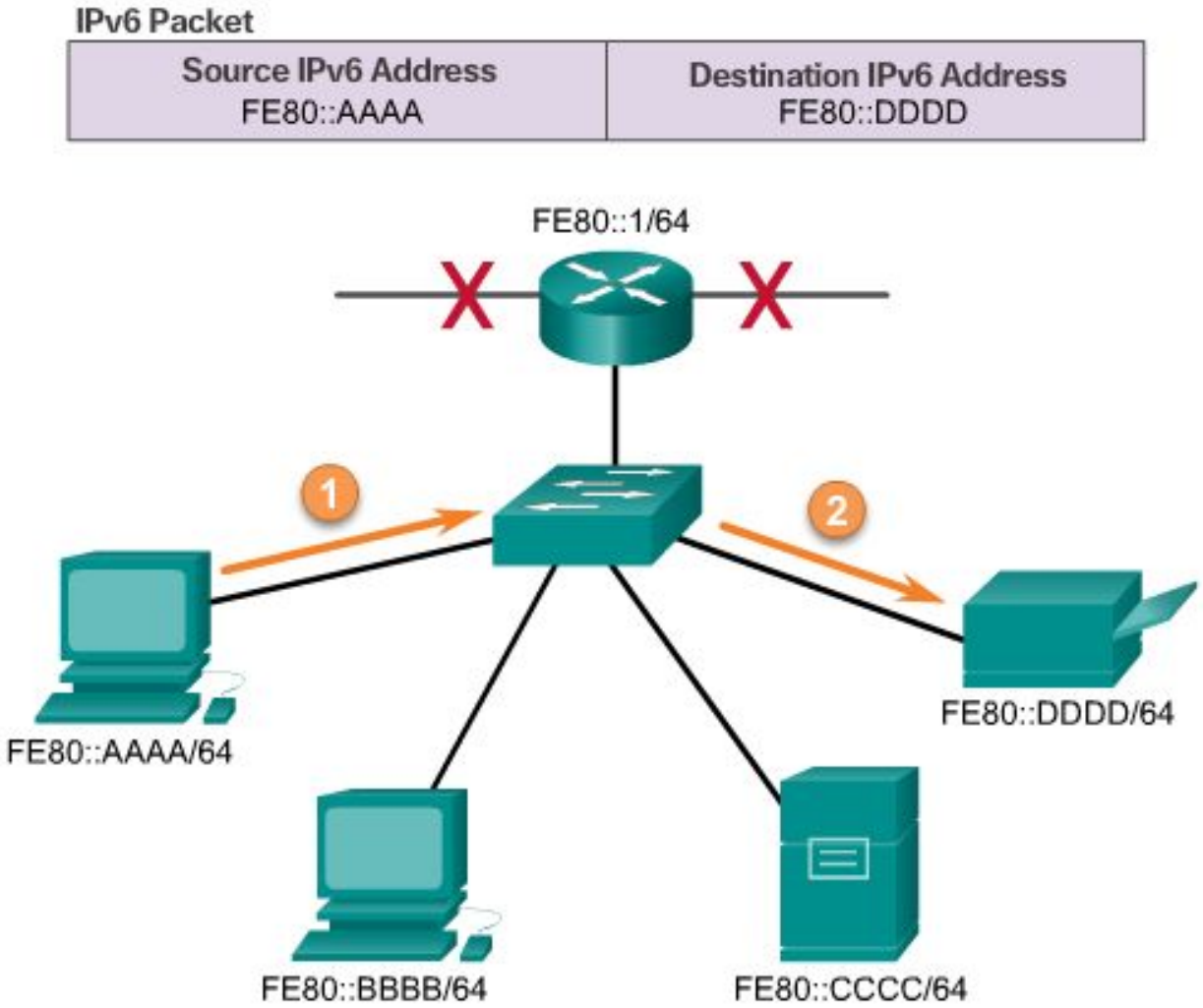
- IPv6 does not use the dotted-decimal subnet mask notation.
- Prefix length indicates the network portion of an IPv6 address using the following format:
  - IPv6 address /prefix length
  - Prefix length can range from 0 to 128
  - Typical prefix length is /64



# 7.2.3.3 IPv6 Unicast Addresses

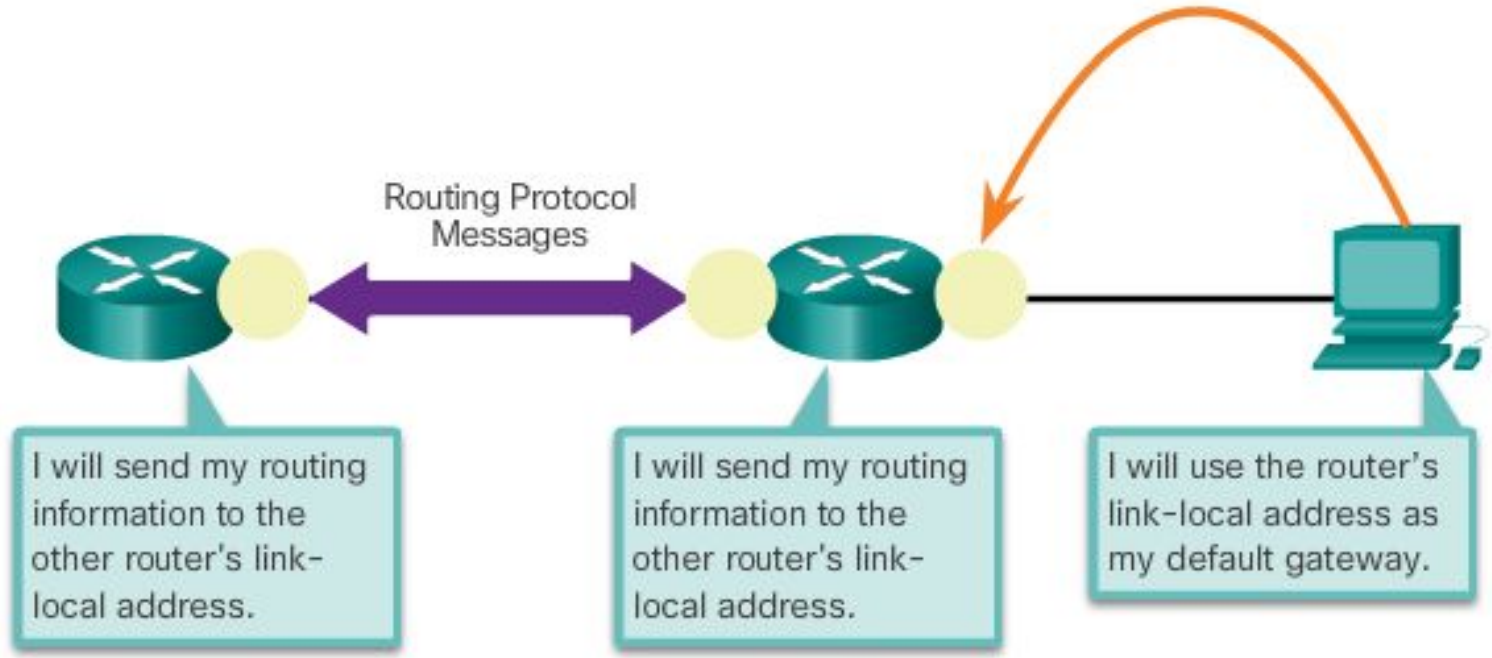


# 7.2.3.4 IPv6 Link-Local Unicast Addresses



# 7.2.3.4 IPv6 Link-Local Unicast Addresses (cont.)

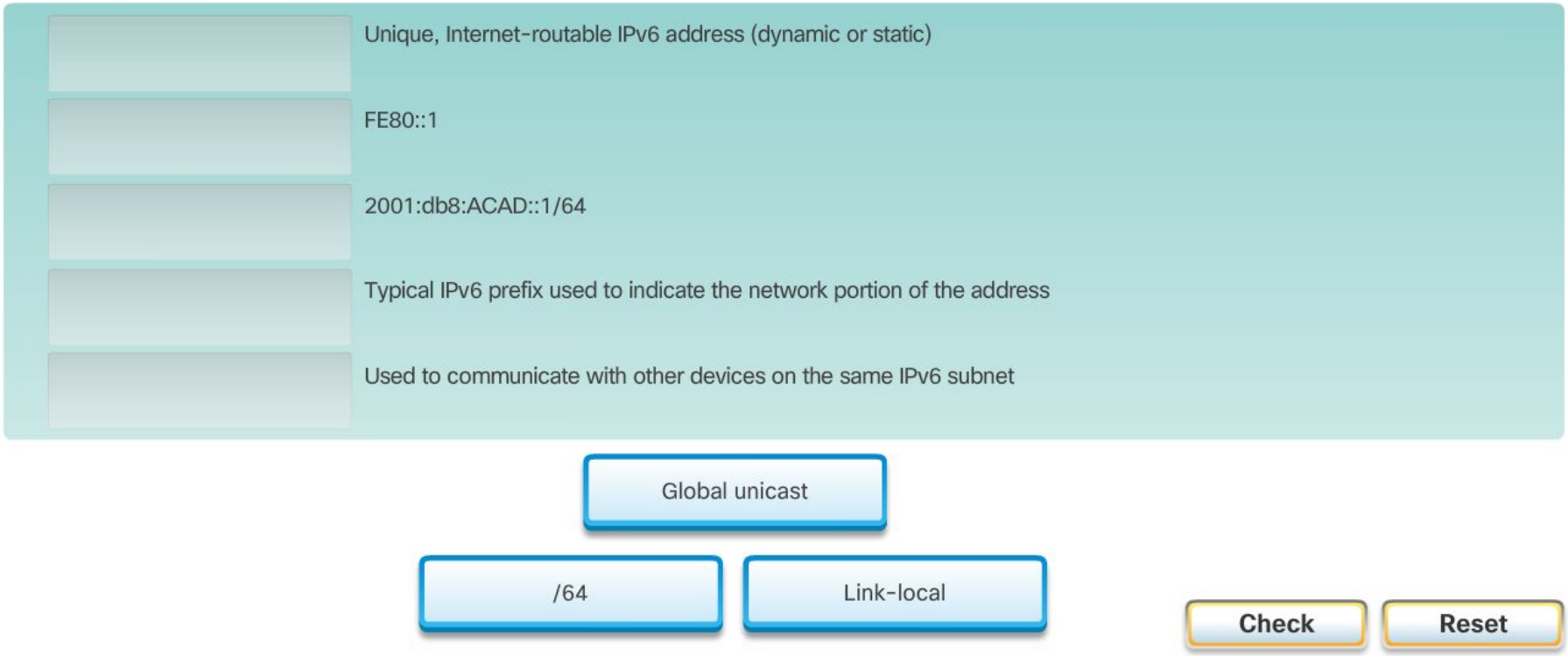
Uses of an IPv6 Link-local address



# 7.2.3.5 Activity – Identify Types of IPv6 Addresses

**Activity - Identify Types of IPv6 Addresses**

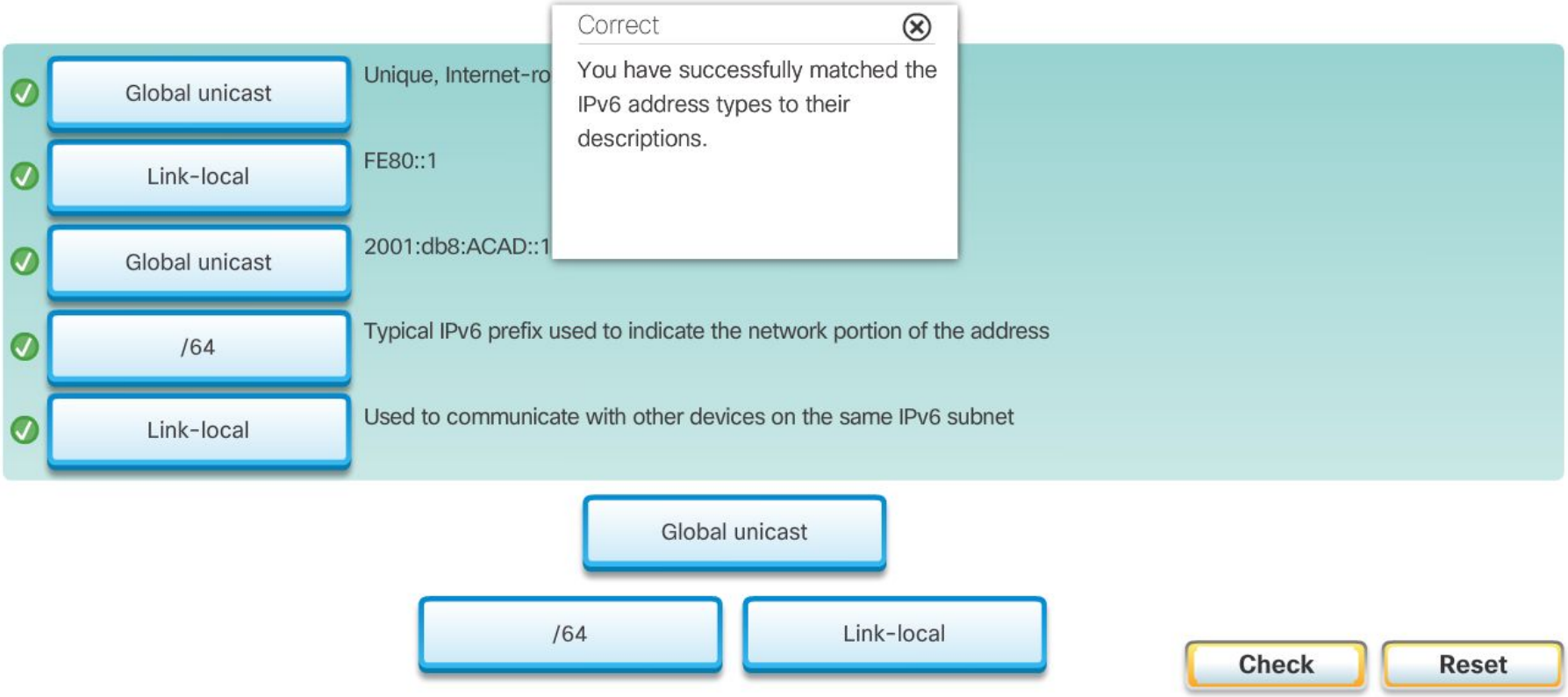
Drag the IPv6 address type to the most appropriate description.



# 7.2.3.5 Activity – Identify Types of IPv6 Addresses

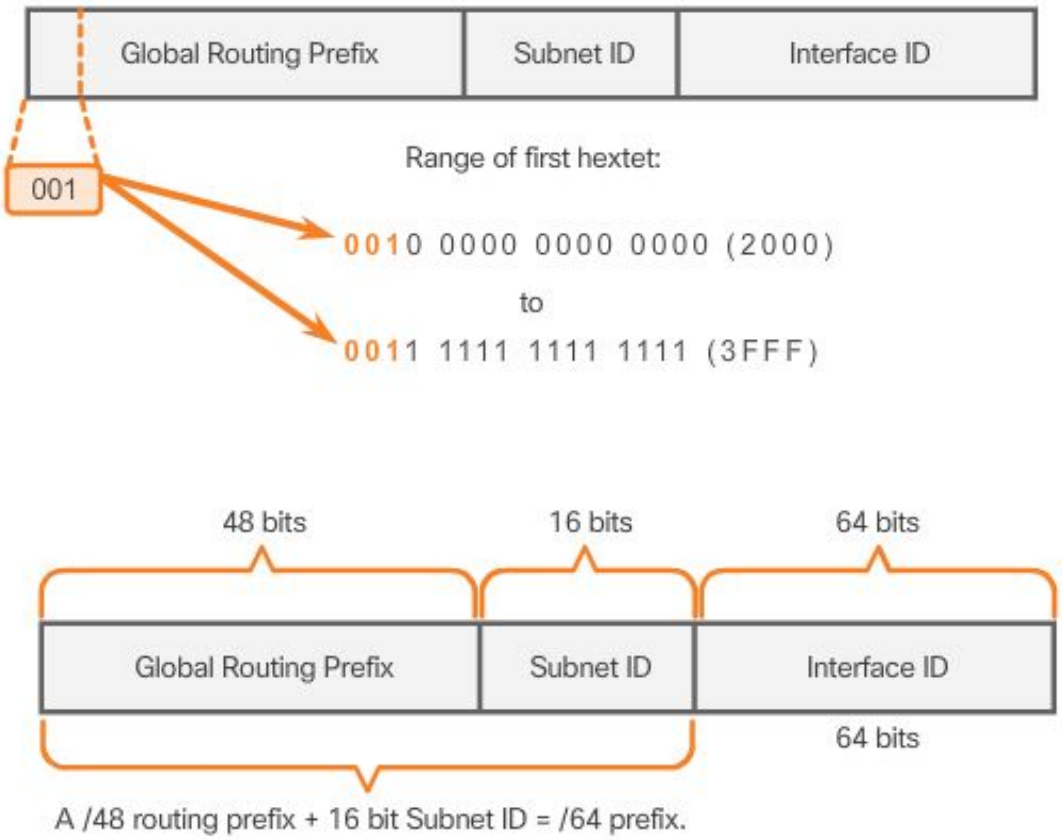
**Activity - Identify Types of IPv6 Addresses**

Drag the IPv6 address type to the most appropriate description.



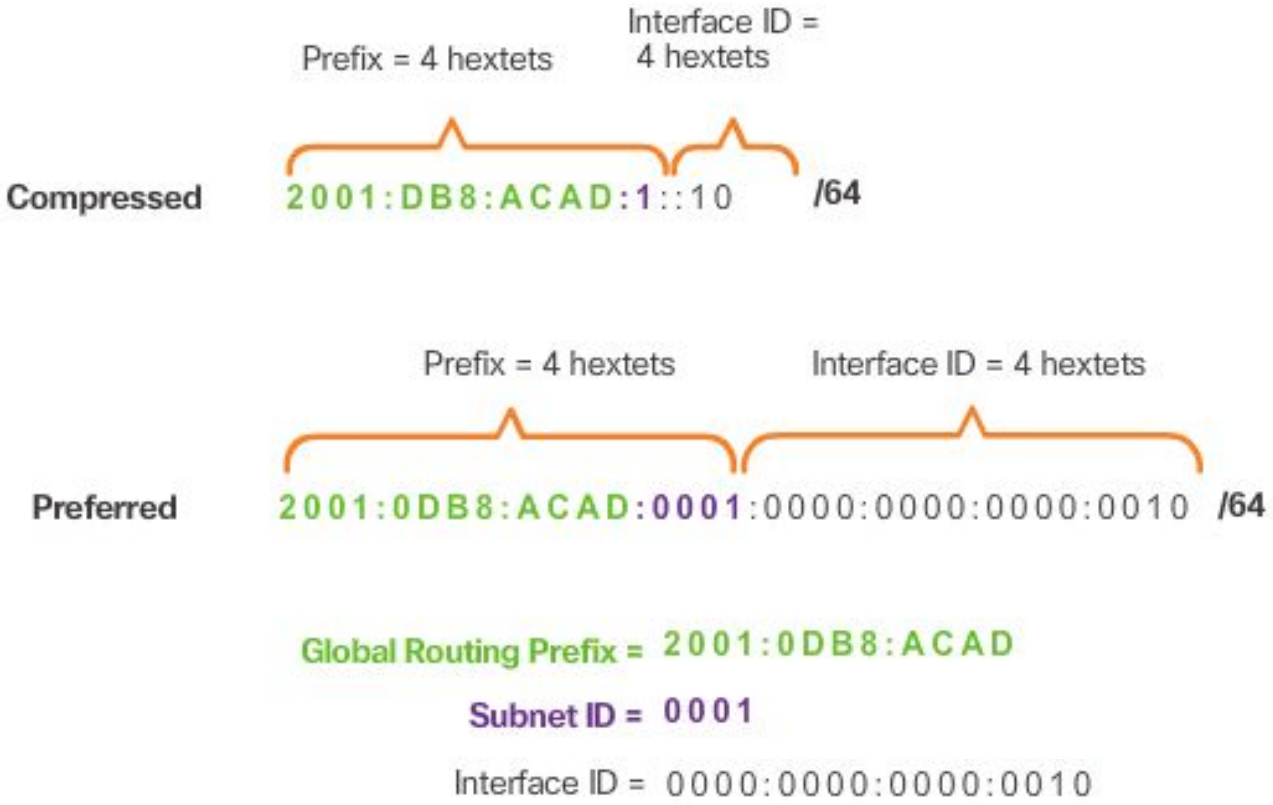
# Topic 7.2.4:
# IPv6 Unicast Addresses

# 7.2.4.1 Structure of an IPv6 Global Unicast Address

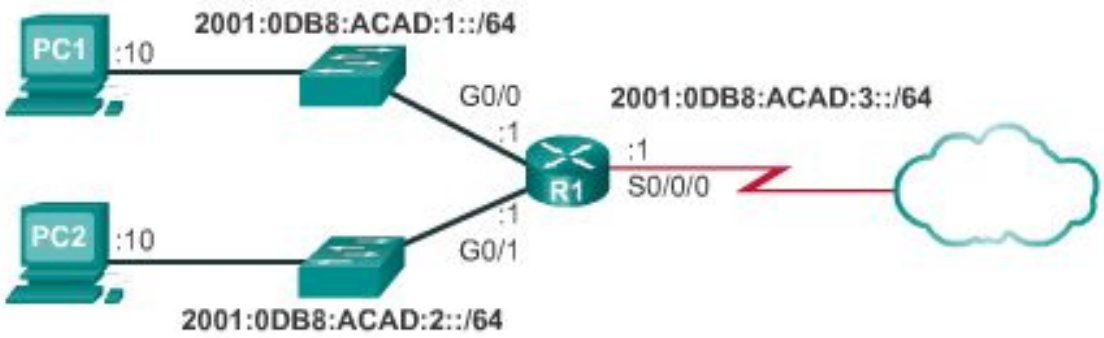


# 7.2.4.1 Structure of an IPv6 Global Unicast Address (cont.)

## Reading a Global Unicast Address

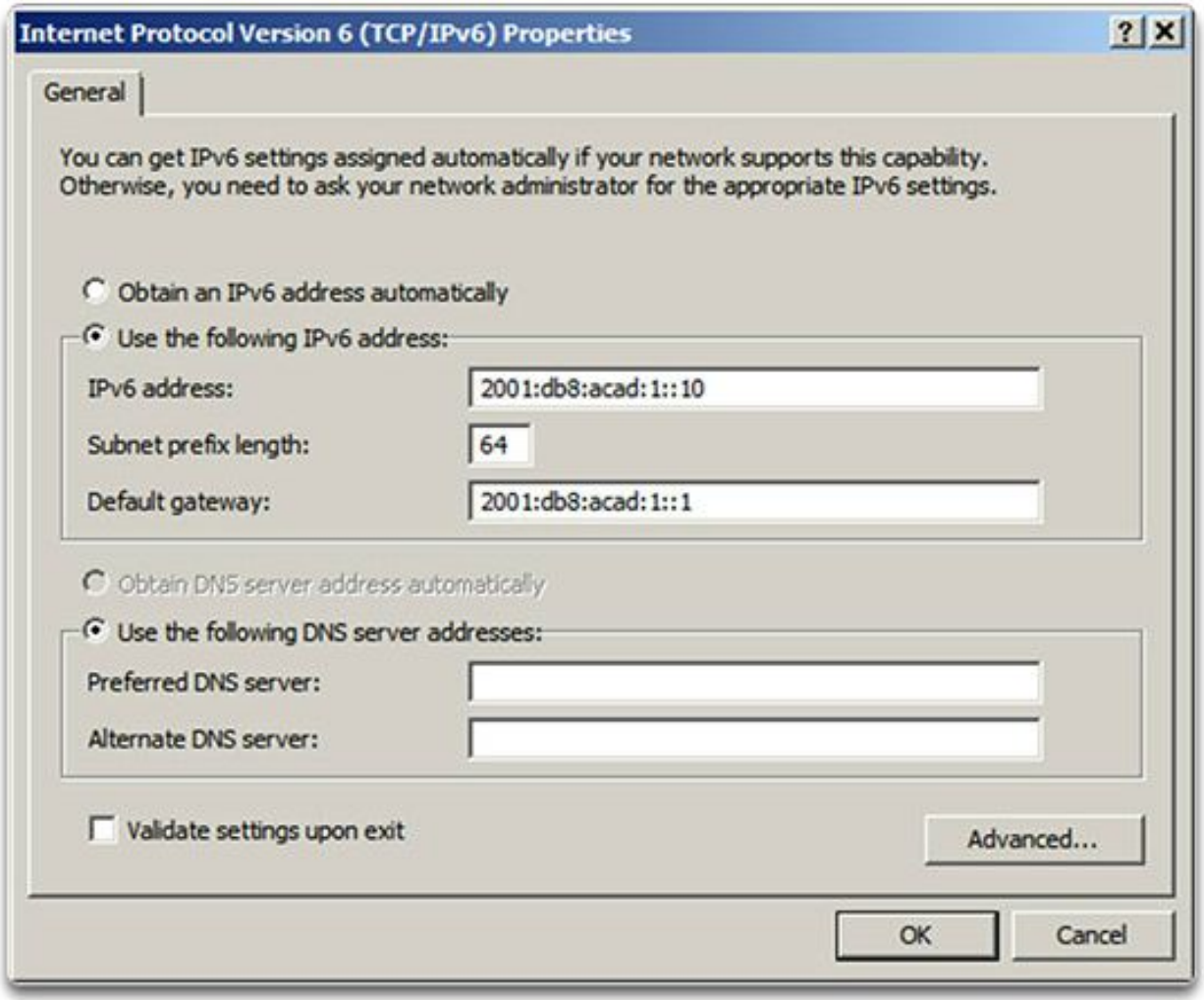


# 7.2.4.2 Static Configuration of a Global Unicast Address



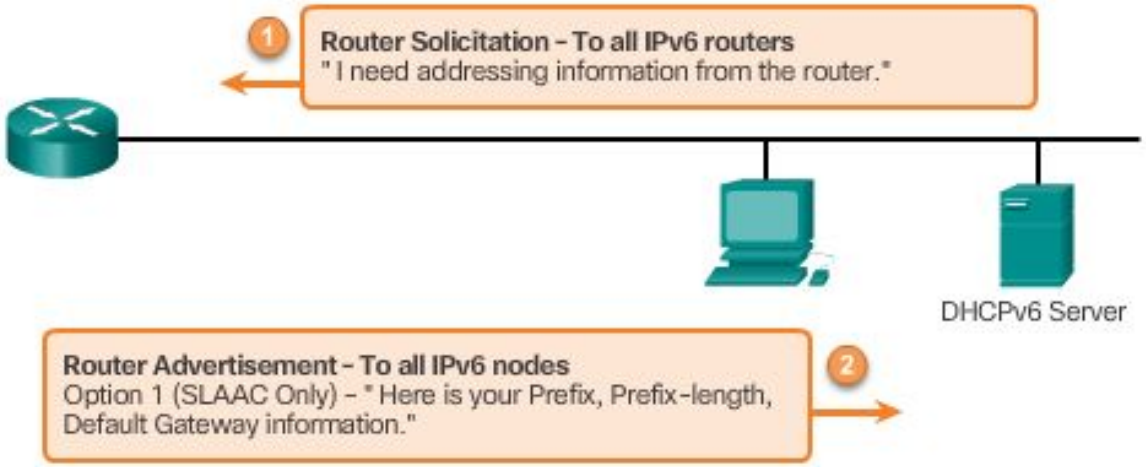

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```

# 7.2.4.2 Static Configuration of a Global Unicast Address (cont.



# 7.2.4.3 Dynamic Configuration - SLAAC

## Router Solicitation and Router Advertisement Messages



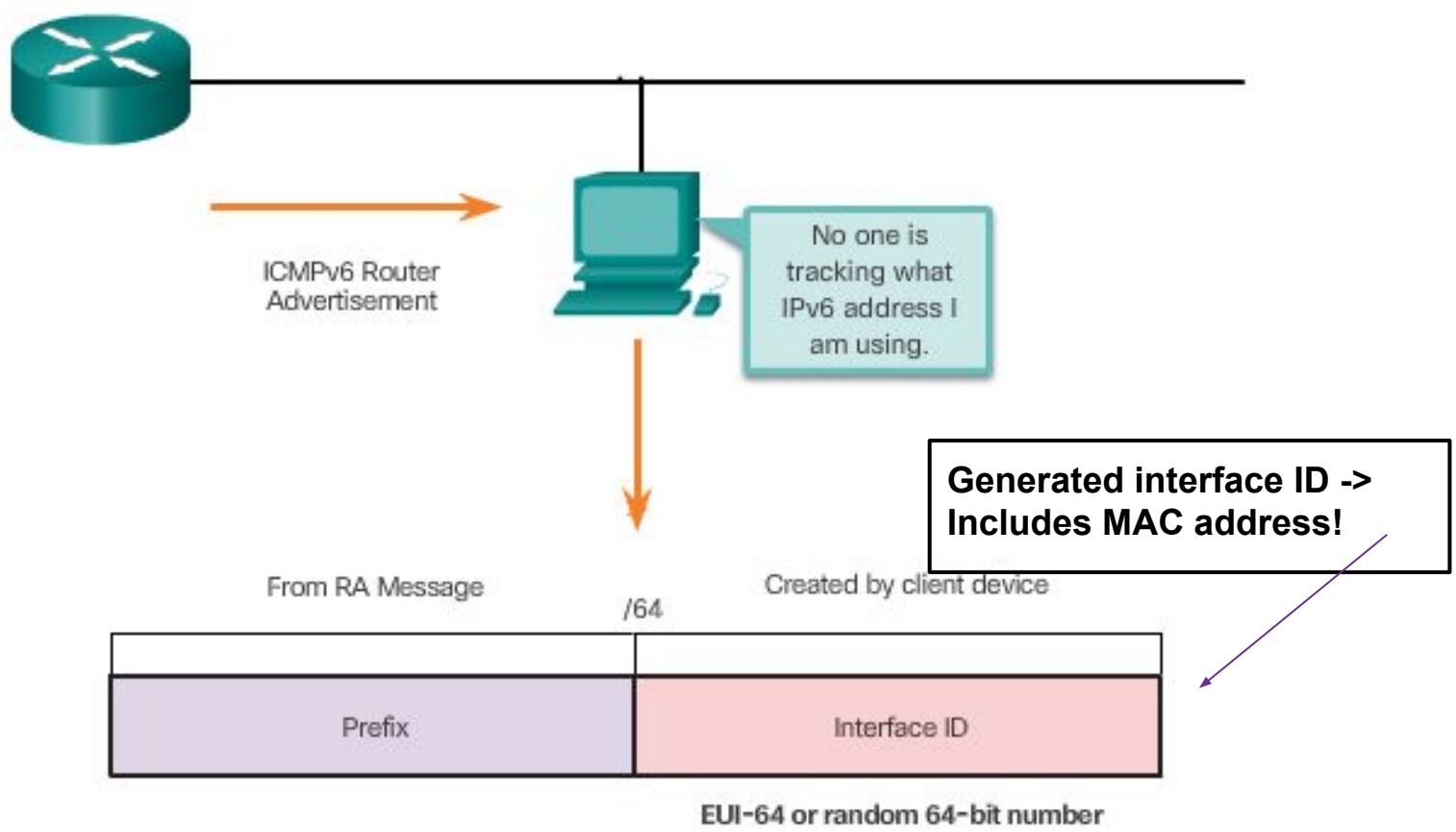

Router Advertisement Options

Option 1 (SLAAC Only) – " I'm everything you need (Prefix, Prefix-length, Default Gateway)"

Option 2 (SLAAC and DHCPv6) – " Here is my information but you need to get other information such as DNS addresses from a DHCPv6 server."

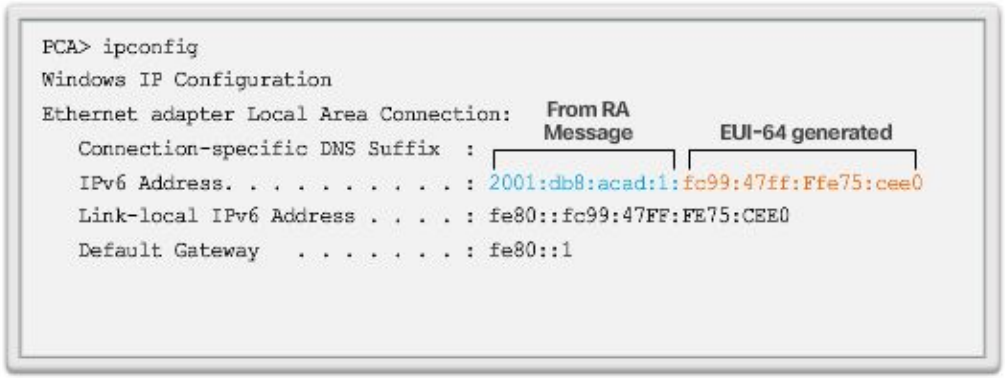
Option 3 (DHCPv6 Only) – " I can't help you. Ask a DHCPv6 server for all your

# 7.2.4.5 EUI-64 Process and Randomly Generated

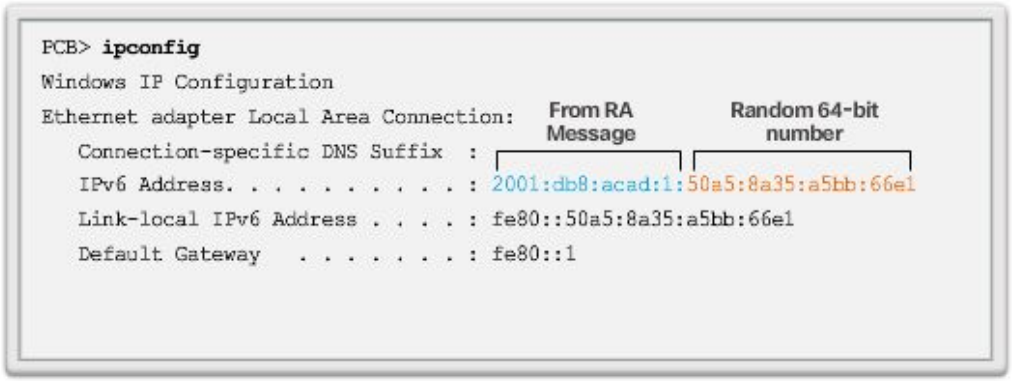


# 7.2.4.5 EUI-64 Process and Randomly Generated

## EUI-64 Process




## Randomly Generated Interface ID



# 7.2.4.6 Dynamic Link-Local Addresses

## Dynamically Created Link-Local Addresses

**EUI-64 generated Interface ID**

```
PCA> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
   Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
   Default Gateway . . . . . . . . . : fe80::1
```

**Random 64-bit generated Interface ID**

```
PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
```

# 7.2.4.6 Dynamic Link-Local Addresses (cont.)

Router's EUI-64 Generated Link-Local Address

```
R1# show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<Output Omitted>

R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

Link-local addresses using EUI-64

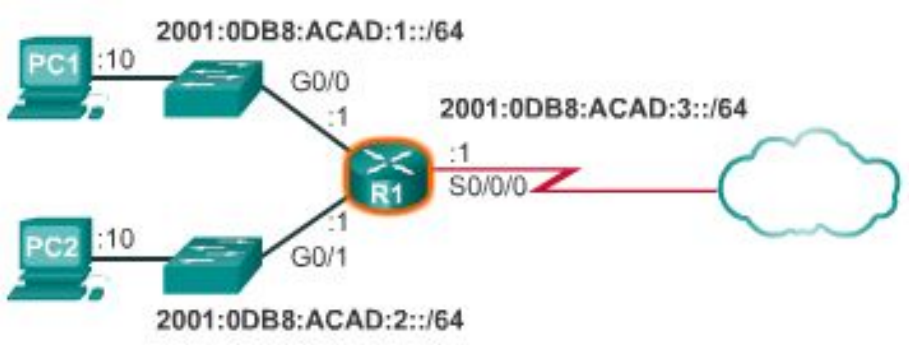
# 7.2.4.7 Static Link-Local Addresses

## Configuring Link-local Addresses on R1

```
Router(config-if)#

ipv6 address link-local-address link-local
```

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

# 7.2.4.8 Verifying IPv6 Address Configuration



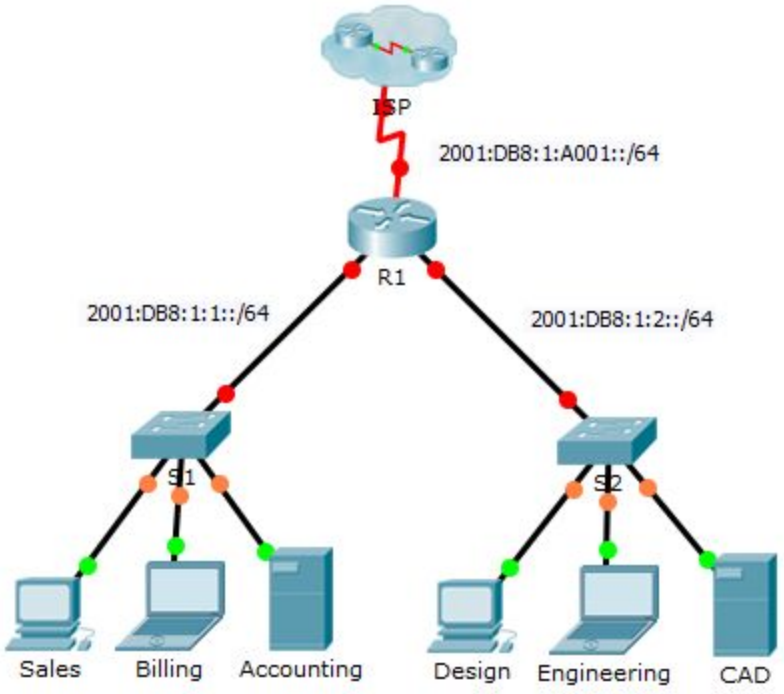

```
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

# 7.2.4.8 Verifying IPv6 Address Configuration (cont.)

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static

<output omitted>

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
R1#
```

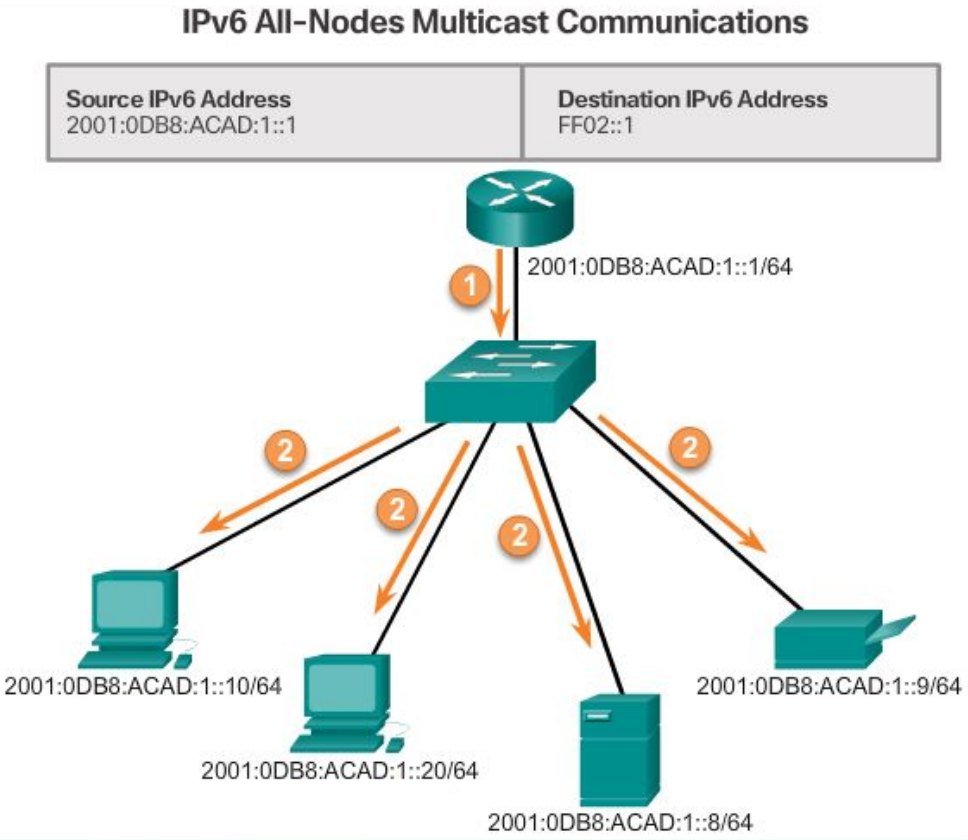
# 7.2.4.9 Packet Tracer - Configuring IPv6 Addressing



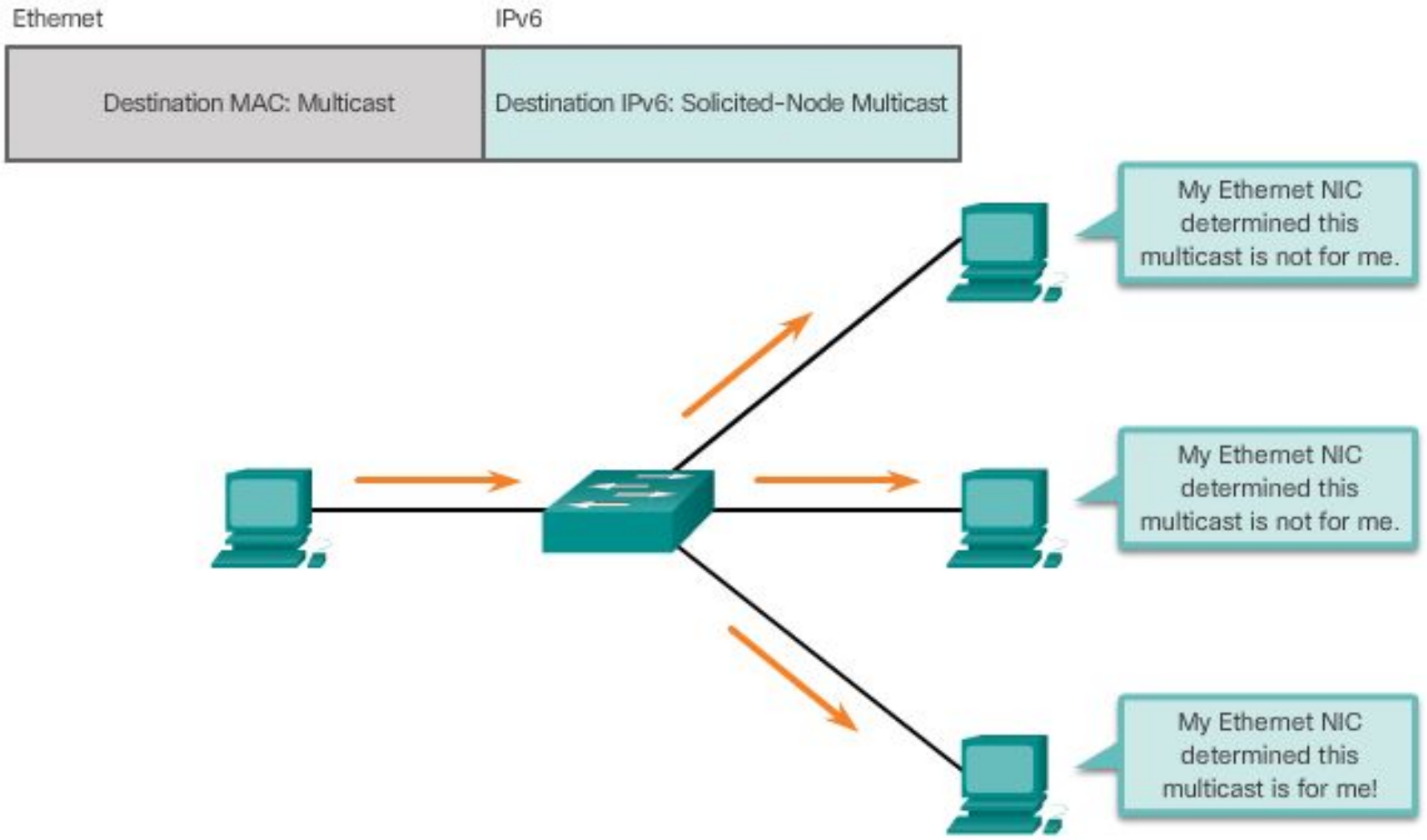
# Topic 7.2.5:
# IPv6 Multicast Addresses

# 7.2.5.1 Assigned IPv6 Multicast Addresses

- IPv6 multicast addresses have the prefix FF00::/8.
- There are two types of IPv6 multicast addresses:
  - Assigned multicast
  - Solicited node multicast



# 7.2.5.2 Solicited-Node IPv6 Multicast Addresses



# Section 7.3: Connectivity Verification

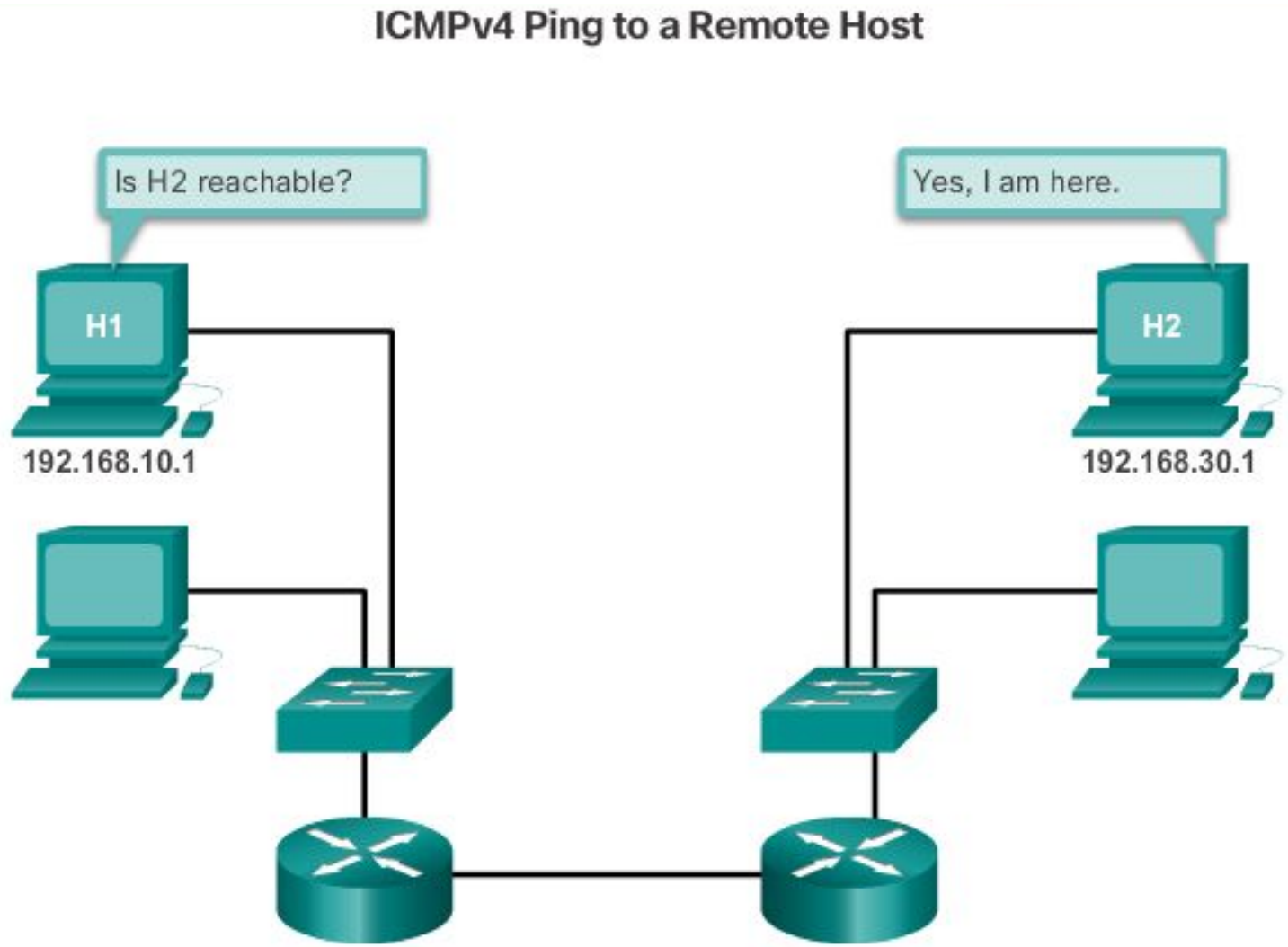
Upon completion of this section, you should be able to:

- Explain how ICMP is used to test network connectivity.
- Use ping and traceroute utilities to test network connectivity.

# Topic 7.3.1: ICMP

# 7.3.1.1 ICMPv4 and ICMPv6

see animation online

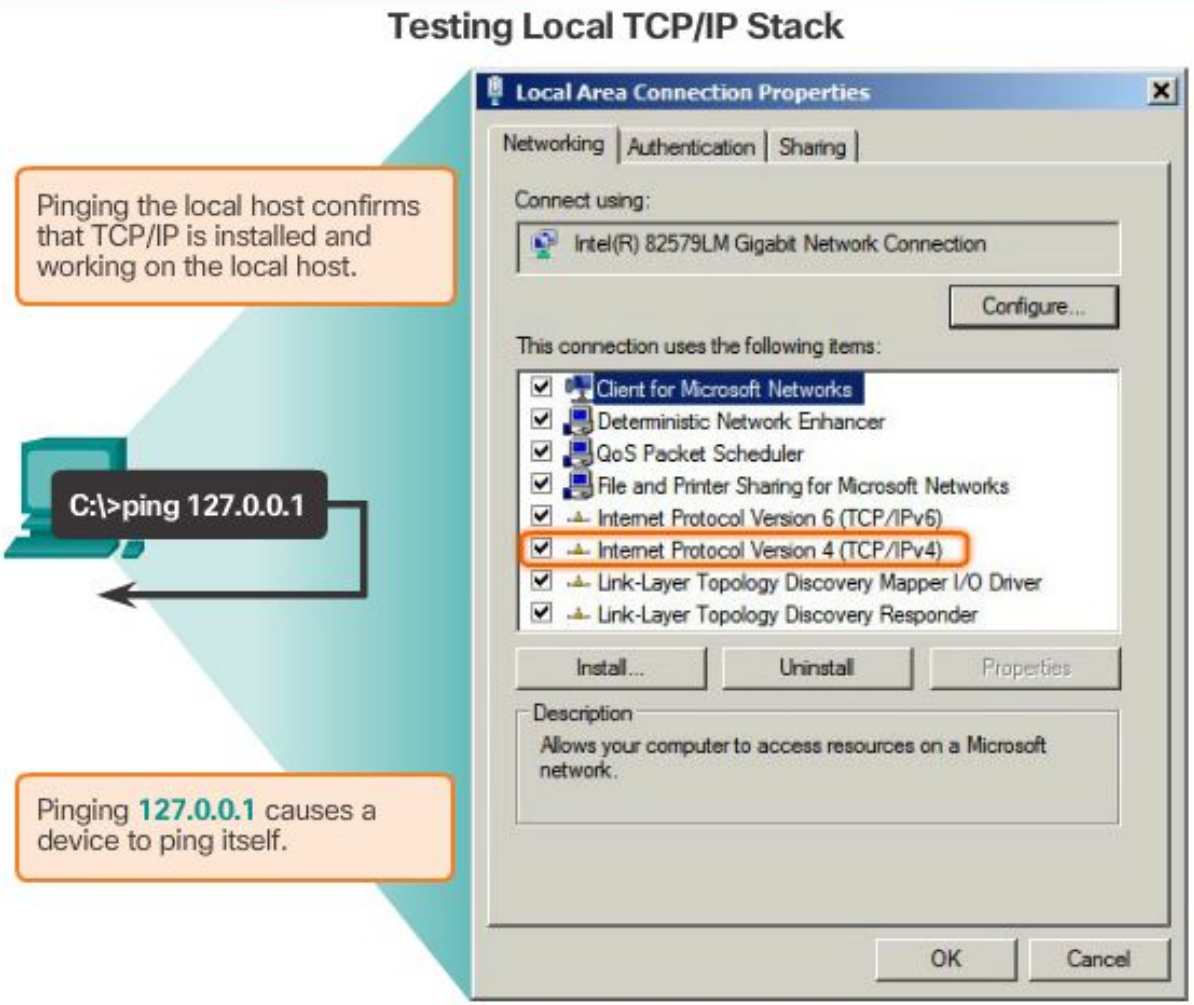


# 7.3.1.1 ICMPv4 and ICMPv6 (cont.)

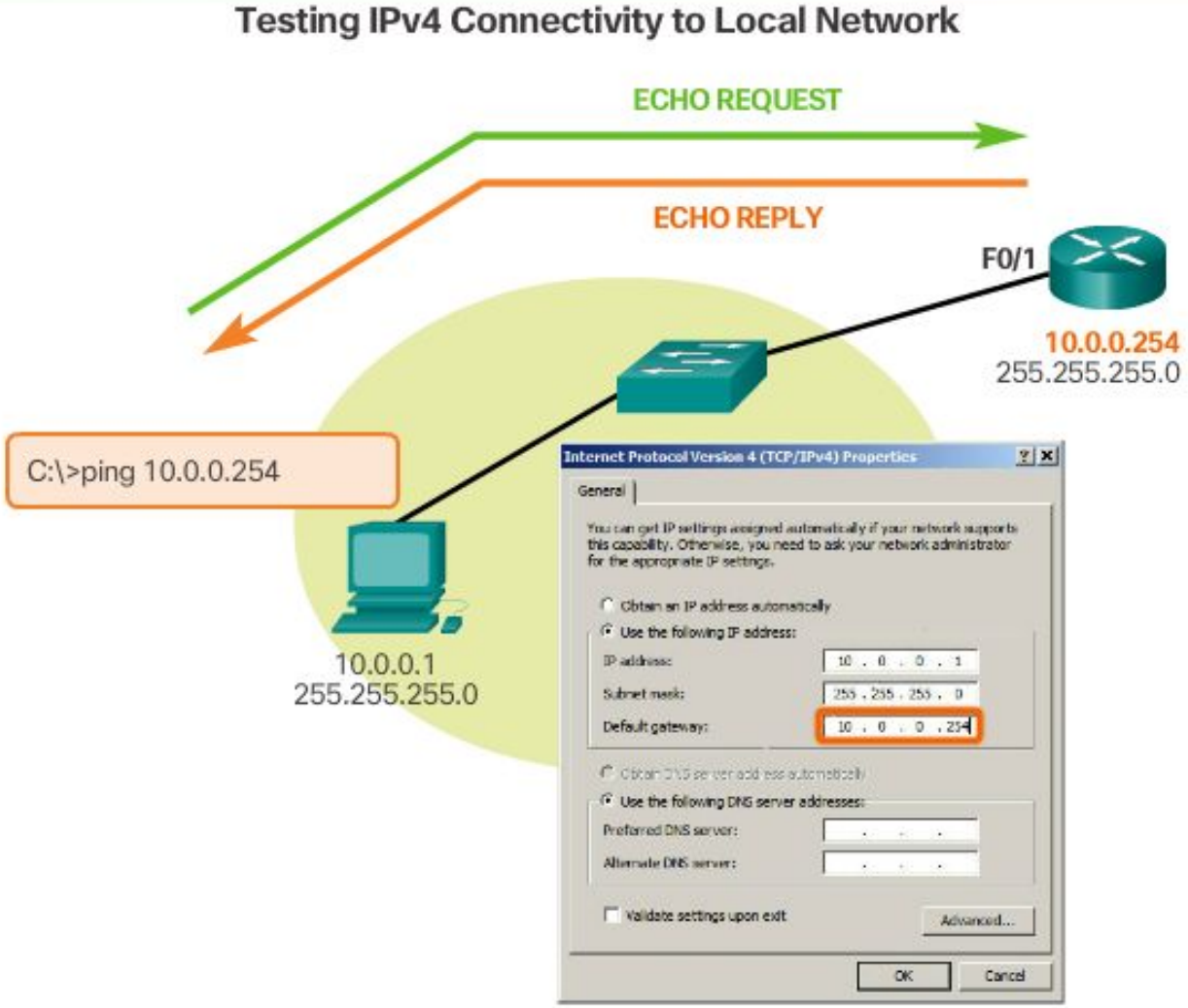
- ICMP messages common to both ICMPv4 and ICMPv6 include:
  - Host confirmation
  - Destination or service unreachable
  - Time exceeded
  - Route redirection
- Although IP is not a reliable protocol, the TCP/IP suite provides for messages to be sent in the event of certain errors. They are sent using the services of ICMP.

# Topic 7.3.2:
# Testing and Verification

# 7.3.2.1 Ping - Testing the Local Stack

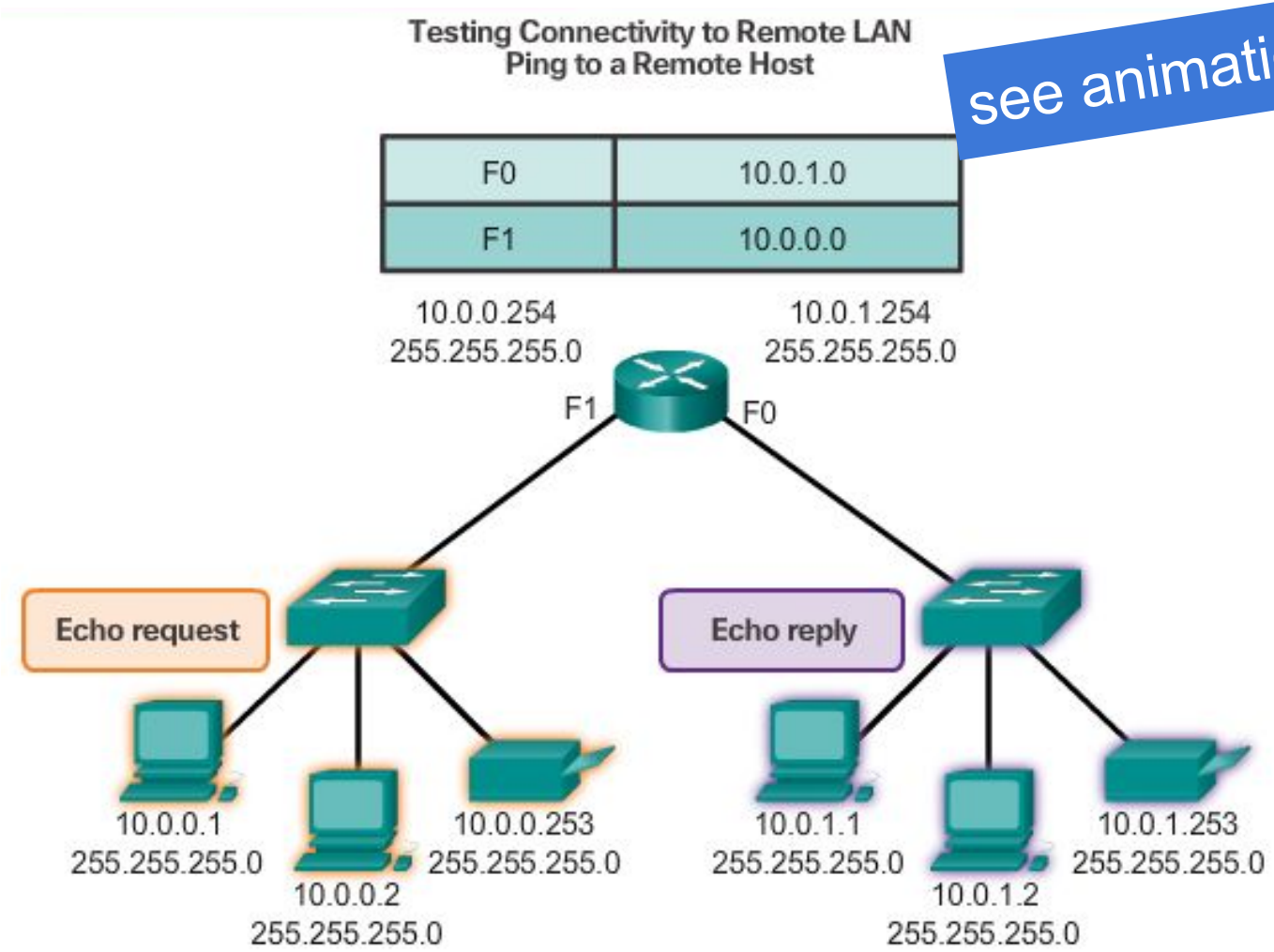


# 7.3.2.2 Ping – Testing Connectivity to the Local LAN

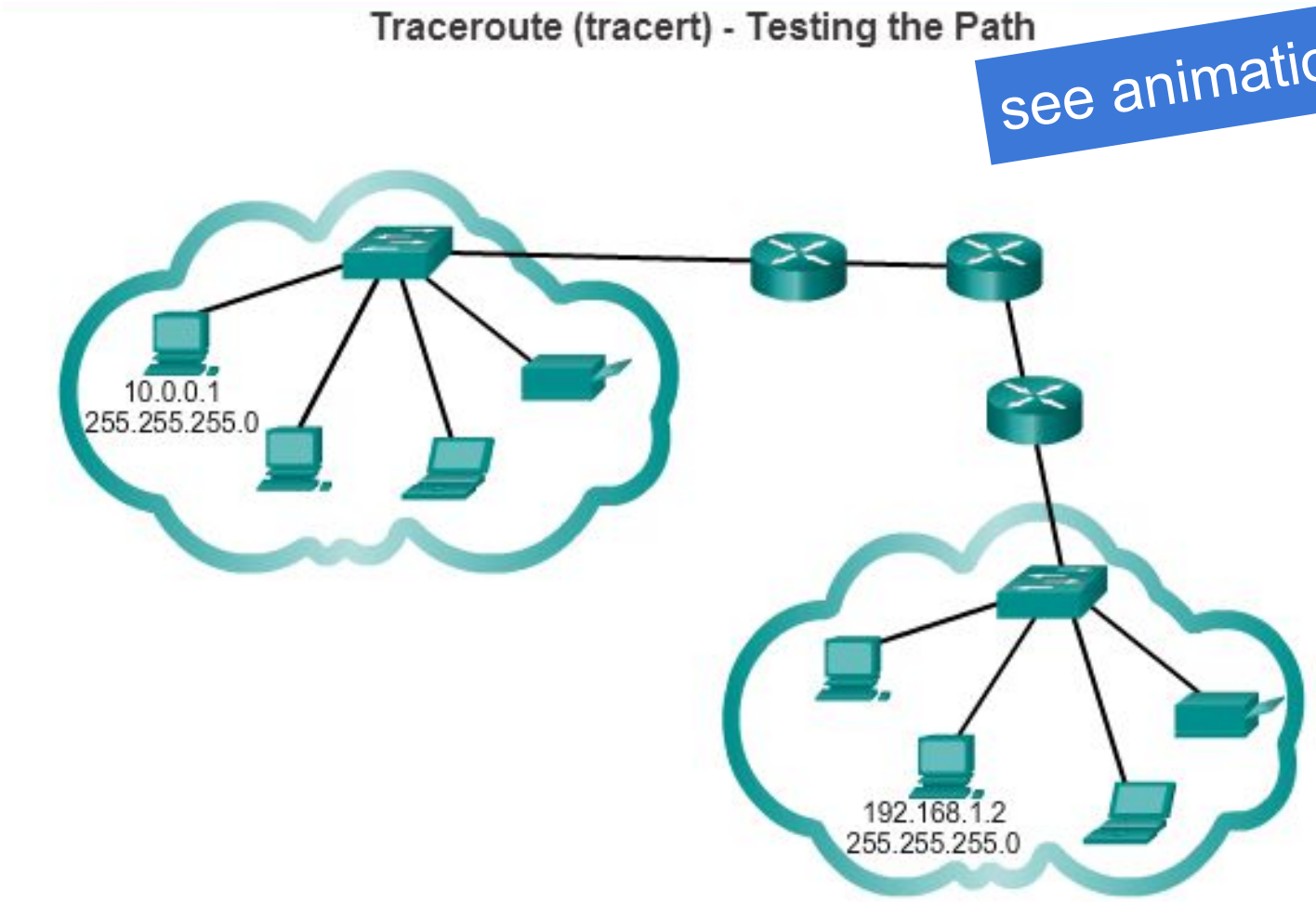


# 7.3.2.3 Ping – Testing Connectivity to Remote

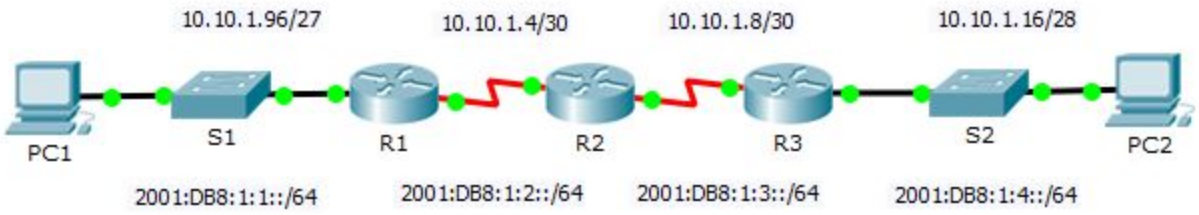
see animation online



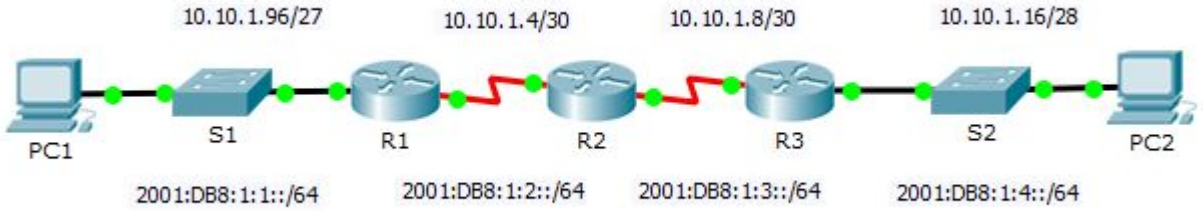
# 7.3.2.4 Traceroute – Testing the Path



# 7.3.2.5 PT – Verifying IPv4 and IPv6 Addressing



# 7.3.2.5 PT– Verifying IPv4 and IPv6 Addressing

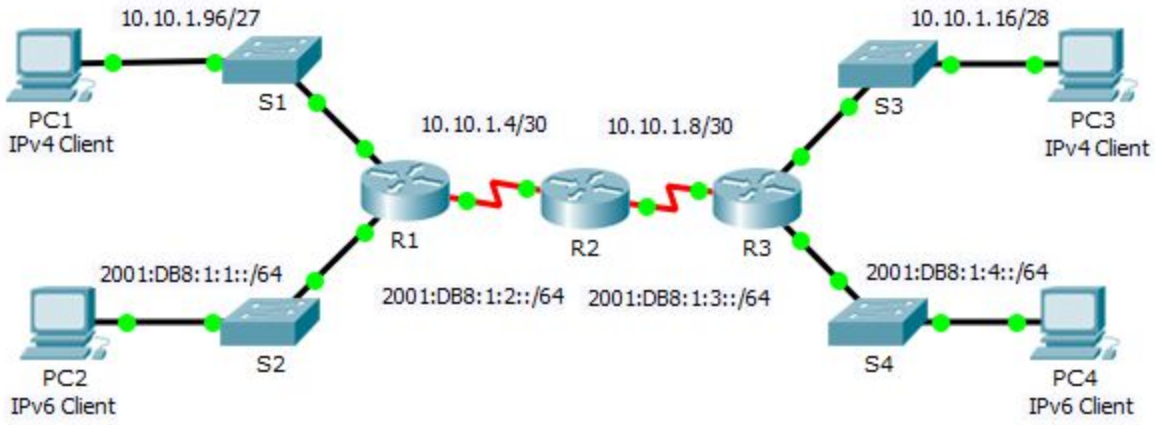



**Command Prompt**

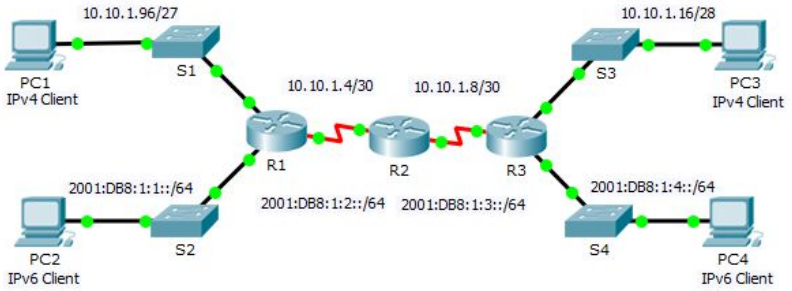
```
Packet Tracer PC Command Line 1.0
PC>ping 10.10.1.20

Pinging 10.10.1.20 with 32 bytes of data:

Request timed out.
Reply from 10.10.1.20: bytes=32 time=6ms TTL=125
Reply from 10.10.1.20: bytes=32 time=3ms TTL=125
Reply from 10.10.1.20: bytes=32 time=5ms TTL=125

Ping statistics for 10.10.1.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

```
PC>ping 2001:DB8:1:4::A

Pinging 2001:DB8:1:4::A with 32 bytes of data:

Reply from 2001:DB8:1:4::A: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=9ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=4ms TTL=125
Reply from 2001:DB8:1:4::A: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:4::A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

# 7.3.2.6 PT – Pinging and Tracing to Test the Path



# 7.3.2.6 PT – Pinging and Tracing to Test the Path

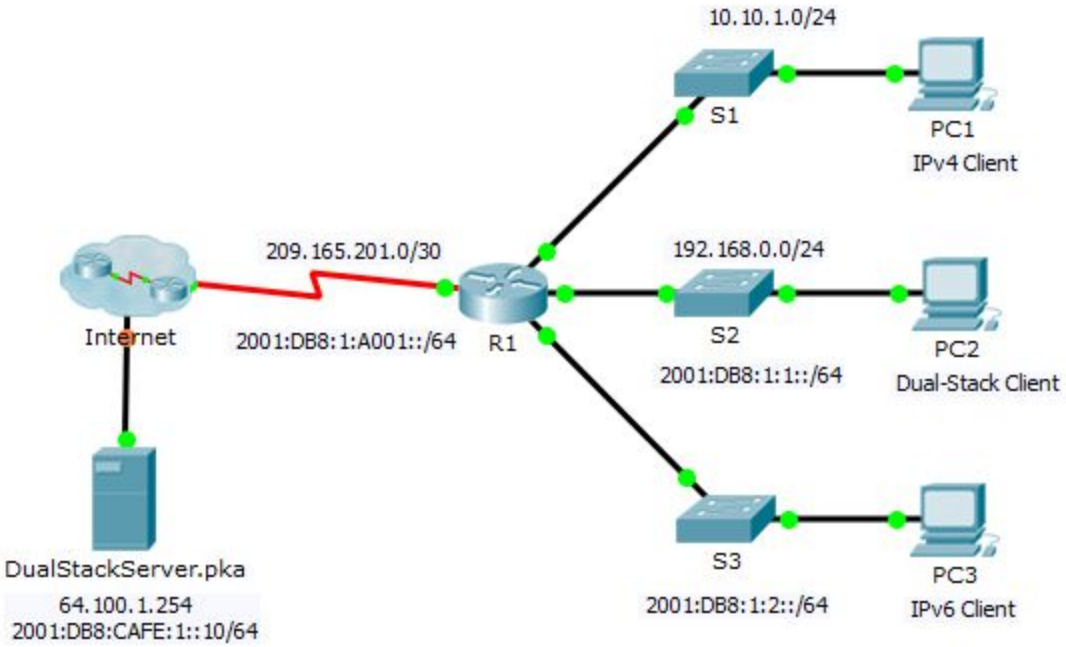



```
PC>tracert 10.10.1.18

Tracing route to 10.10.1.18 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.10.1.97
  2    0 ms      *         0 ms      10.10.1.97
  3    *         0 ms      *         Request timed out.
  4    0 ms      *         0 ms      10.10.1.97
  5    *         0 ms      *         Request timed out.
  6    0 ms
```

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     unassigned      YES unset  up                    up

GigabitEthernet0/1     10.10.1.97      YES manual up                    up

Serial0/0/0            unassigned      YES unset  administratively down down

Serial0/0/1            10.10.1.6       YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
```

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.10.1.4/30 is directly connected, Serial0/0/1
L       10.10.1.6/32 is directly connected, Serial0/0/1
C       10.10.1.96/27 is directly connected, GigabitEthernet0/1
L       10.10.1.97/32 is directly connected, GigabitEthernet0/1
```

# 7.3.2.9 PT–Troubleshooting IPv4 and IPv6 Addressing



# 7.3.2.9 PT – Troubleshooting IPv4 and IPv6 Addressing

| Help Desk Ticket | |
|---|---|
| **Client Identifier:** PC1 | |
| **Issue:** Unable to access the dualstackserver.pka web page. | |
| **Detailed information about the issue** | |
| **Test:** Does the computer have an IP address using **ipconfig**? | Yes |
| **Test:** Can the computer contact its gateway using **ping**? | Yes |
| **Test:** Can the computer contact the server using **tracert**? | Yes |
| **Test:** Can the computer contact the server using **nslookup**? | No |
| **Resolution:** Escalate to Level 2 support. | |

```
PC>ping 10.10.1.1

Pinging 10.10.1.1 with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time=0ms TTL=255
Reply from 10.10.1.1: bytes=32 time=0ms TTL=255
Reply from 10.10.1.1: bytes=32 time=0ms TTL=255
Reply from 10.10.1.1: bytes=32 time=0ms TTL=255
```

```
PC>tracert 64.100.1.254

Tracing route to 64.100.1.254 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.10.1.1
  2    0 ms      0 ms      1 ms      209.165.201.1
  3    *         0 ms      3 ms      64.100.1.254

Trace complete.
```

```
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....................: 0060.47CA.4DEE
   Link-local IPv6 Address.....: FE80::260:47FF:FECA:4DEE
   IP Address.....................: 10.10.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.....................: 10.10.1.1
   DNS Servers.....................: 64.100.1.1
   DHCP Servers.....................: 0.0.0.0
   DHCPv6 Client DUID.....: 00-01-00-01-BE-1B-A8-A0-00
```

```
PC>nslookup DualStackServer.pka

Server: [64.100.1.1]
Address:  64.100.1.1
DNS request timed out.
          timeout was 15000 milli seconds.
DNS request timed out.
          timeout was 15000 milli seconds.
```

# Section 7.4: Summary

Chapter Objectives:

- Explain the use of IPv4 addresses to provide connectivity in a small to medium-sized business network.
- Configure IPv6 addresses to provide connectivity in small to medium-sized business networks.
- Use common testing utilities to verify network connectivity.

# Thank you.

Cisco Networking Academy

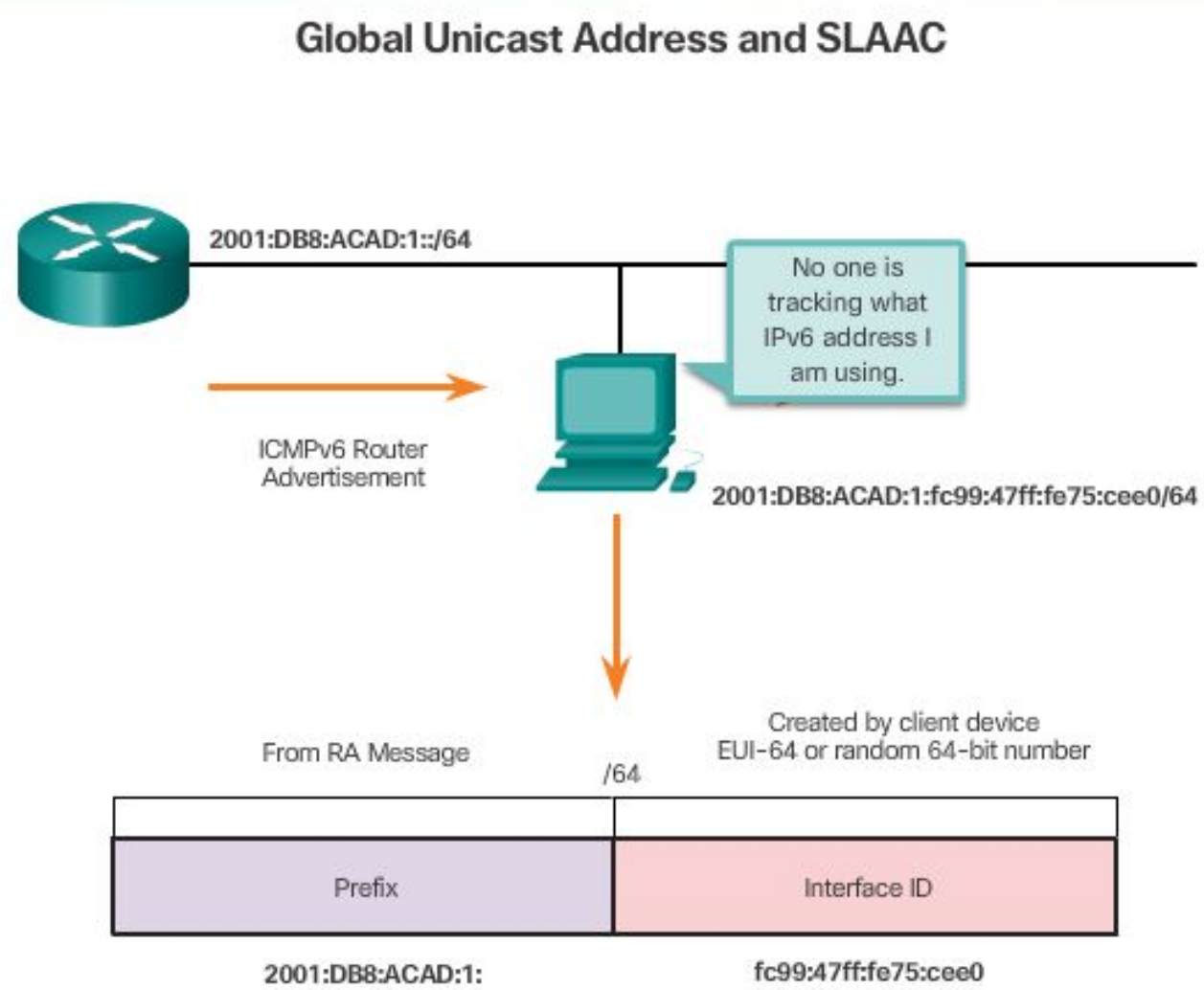
Mind Wide Open

# Thank you.

Cisco Networking Academy

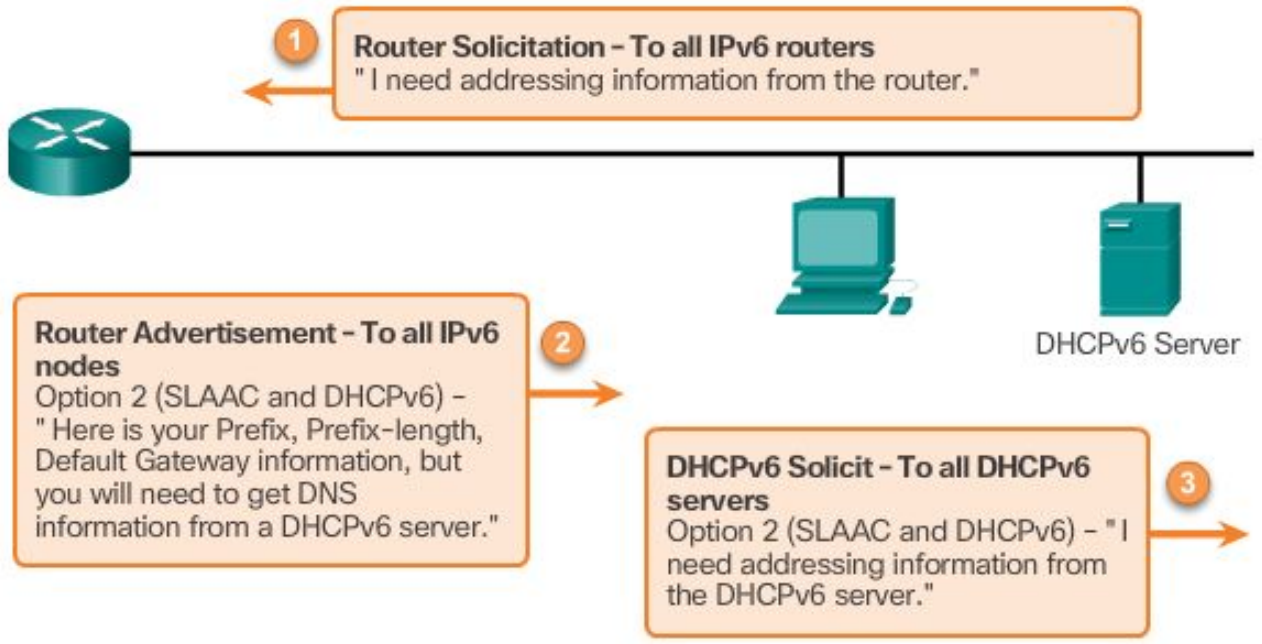
Mind Wide Open

# 7.2.4.3 Dynamic Configuration – SLAAC (cont.)



# 7.2.4.4 Dynamic Configuration – DHCPv6

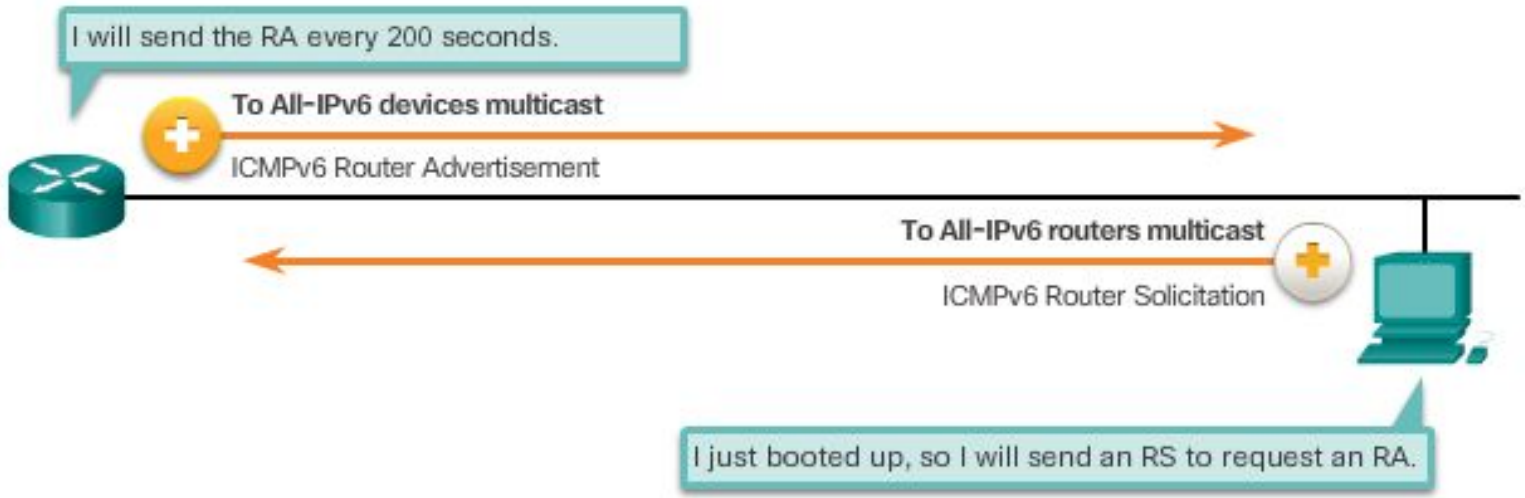
## Router Solicitation and Router Advertisement Messages




**Note:** An RA with option 3 (DHCPv6 Only) enabled will require the client to obtain all information from the DHCPv6 server except the default gateway address. The default gateway address is the RA's source IPv6 address.

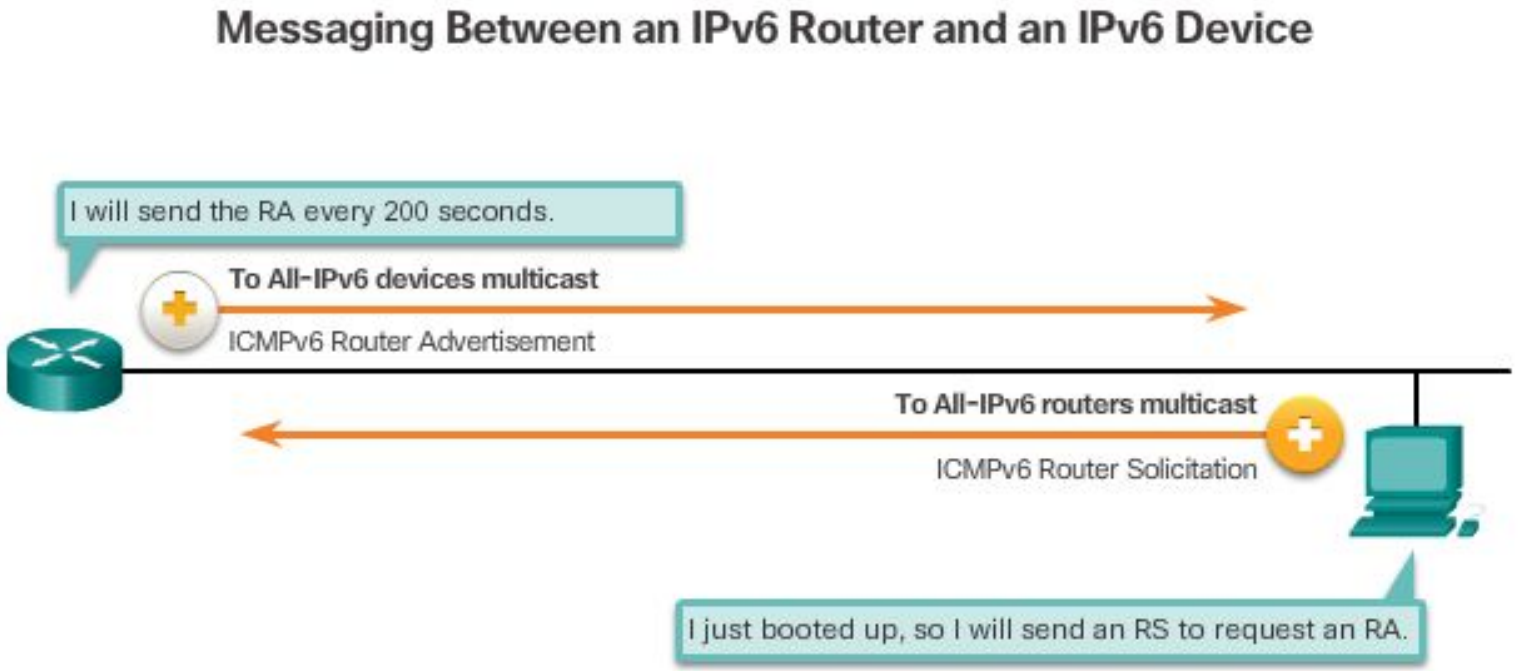
# 7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages

## Messaging Between an IPv6 Router and an IPv6 Device



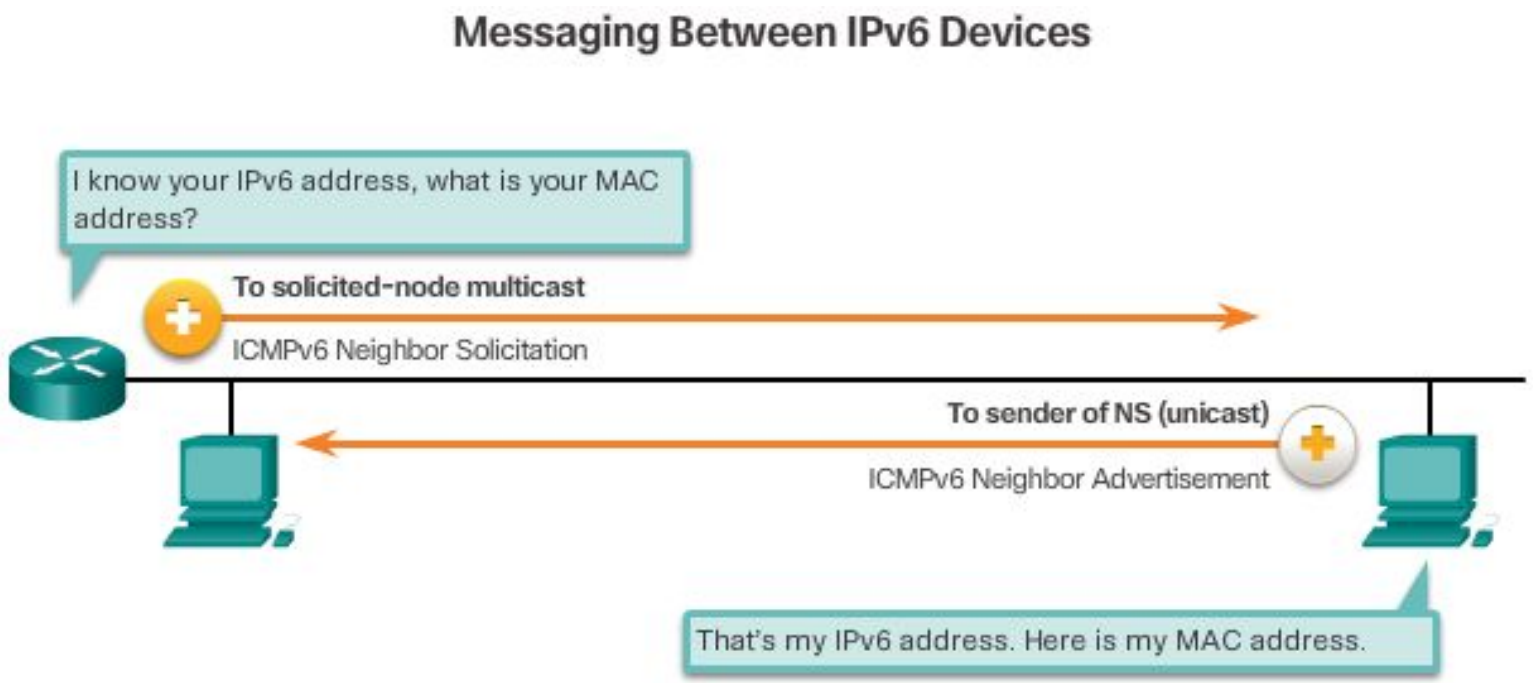

RA messages are sent by routers to provide addressing information to hosts using SLAAC. The RA message can include addressing information for the host such as the prefix, prefix length, DNS address and domain name. A router will send an RA message periodically or in response to an RS message. A host using SLAAC will set its default gateway to the link-local address of the router that sent the RA.

# 7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages



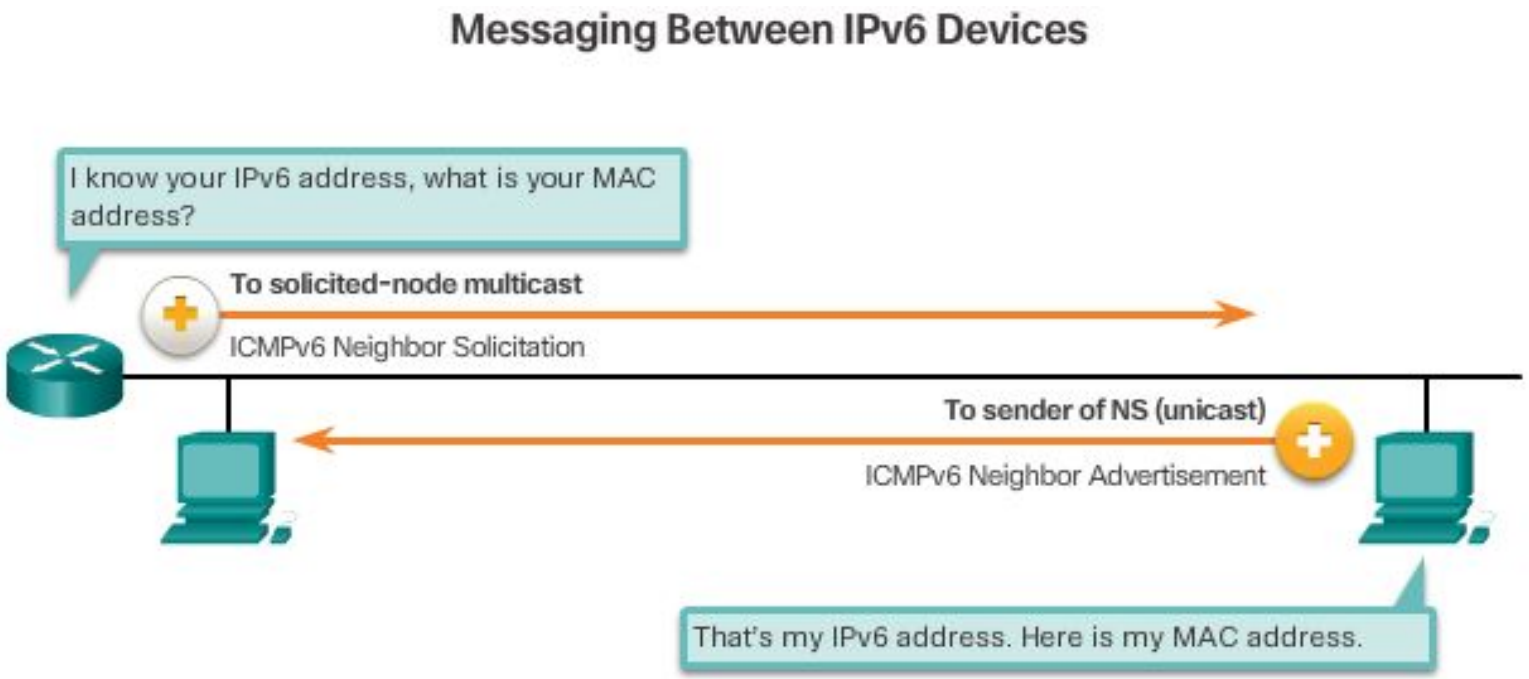

When a host is configured to obtain its addressing information automatically using Stateless Address Autoconfiguration (SLAAC), the host will send an RS message to the router requesting an RA message.

# 7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages (cont.)




NS messages are sent when a device knows the IPv6 address of a device but does not its MAC address. This is equivalent to an ARP Request for IPv4.

# 7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages (cont.)




NA mesages are sent in response to an NS message and matches the target IPv6 address in the NS. The NA message includes the device's Ethernet MAC address. This is equivalent to an ARP Reply for IPv4.

# 7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages (cont.)