

Addressing is a critical function of network layer protocols. Addressing enables data communication between hosts, regardless of whether the hosts are on the same network, or on different networks. Both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) provide hierarchical addressing for packets that carry data.

7.0.1.2 Class Activity – The Internet of Everything (IoE)

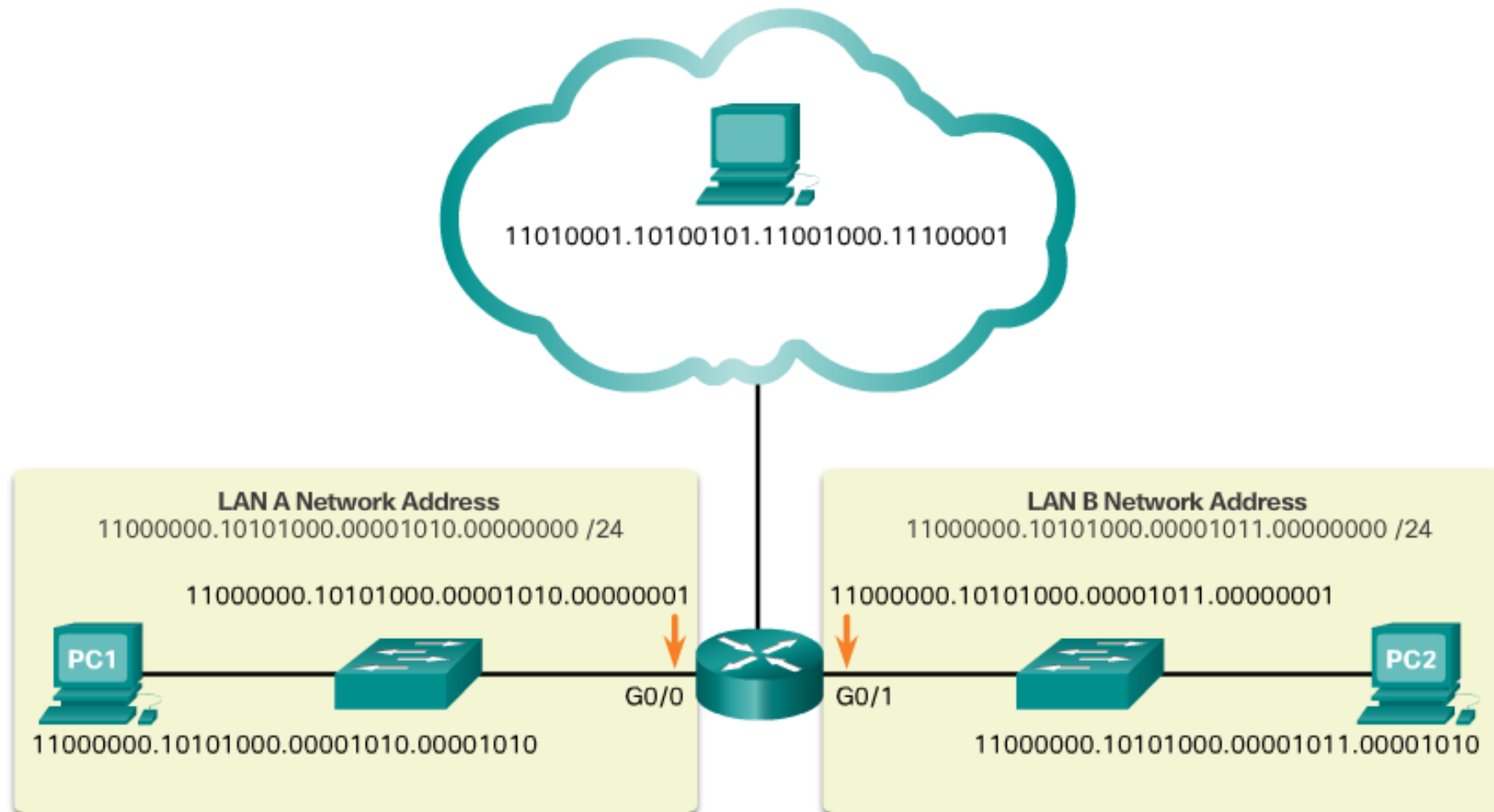


“Today, more than 99% of our world remains unconnected. Tomorrow, we connect everything.”

How will the IoE use IP addressing services for network communication?

7.1.1.1 IPv4 Addresses

IPv4 Addresses Expressed in Binary

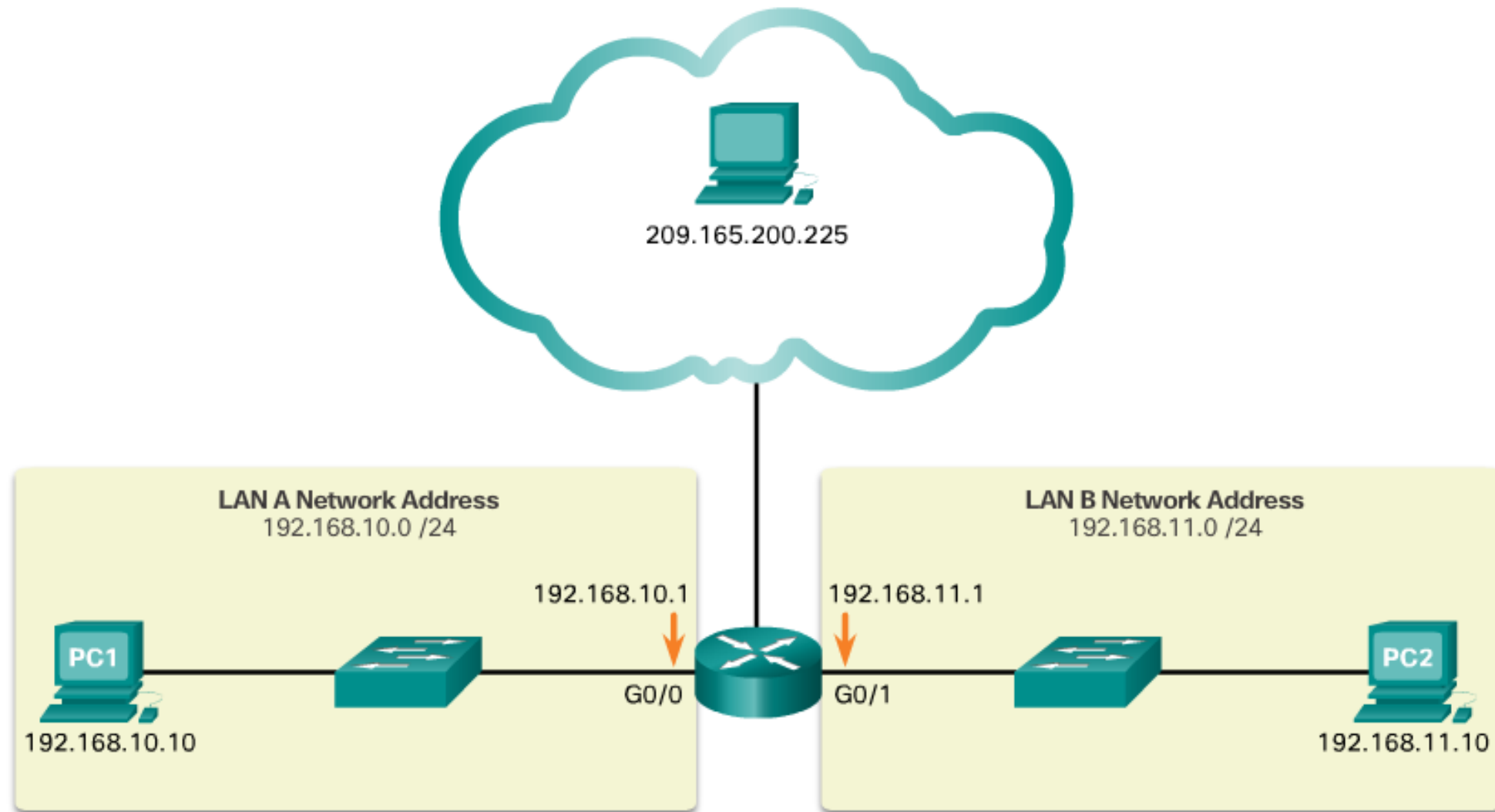


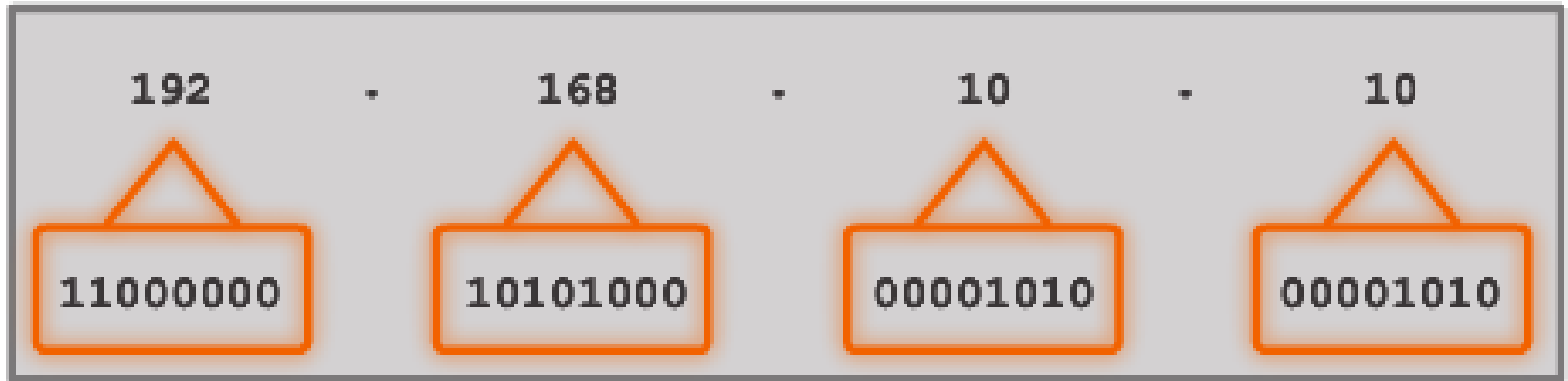
Each address consists of a string of 32 bits, divided into four sections called *octets*.

Each octet contains 8 bits (or 1 byte) separated with a dot. For example, PC1 in the figure is assigned IPv4 address `11000000.10101000.00001010.00000001`.

Its default gateway address would be that of R1 Gigabit Ethernet interface `11000000.10101000.00001011.00000001`.

IPv4 Addresses Expressed in Dotted Decimal





This address is made up of four different octets.

7.1.1.2 Video Demonstration – Converting Between Binary and Decimal Numbering Systems



7.1.1.3 Positional Notation

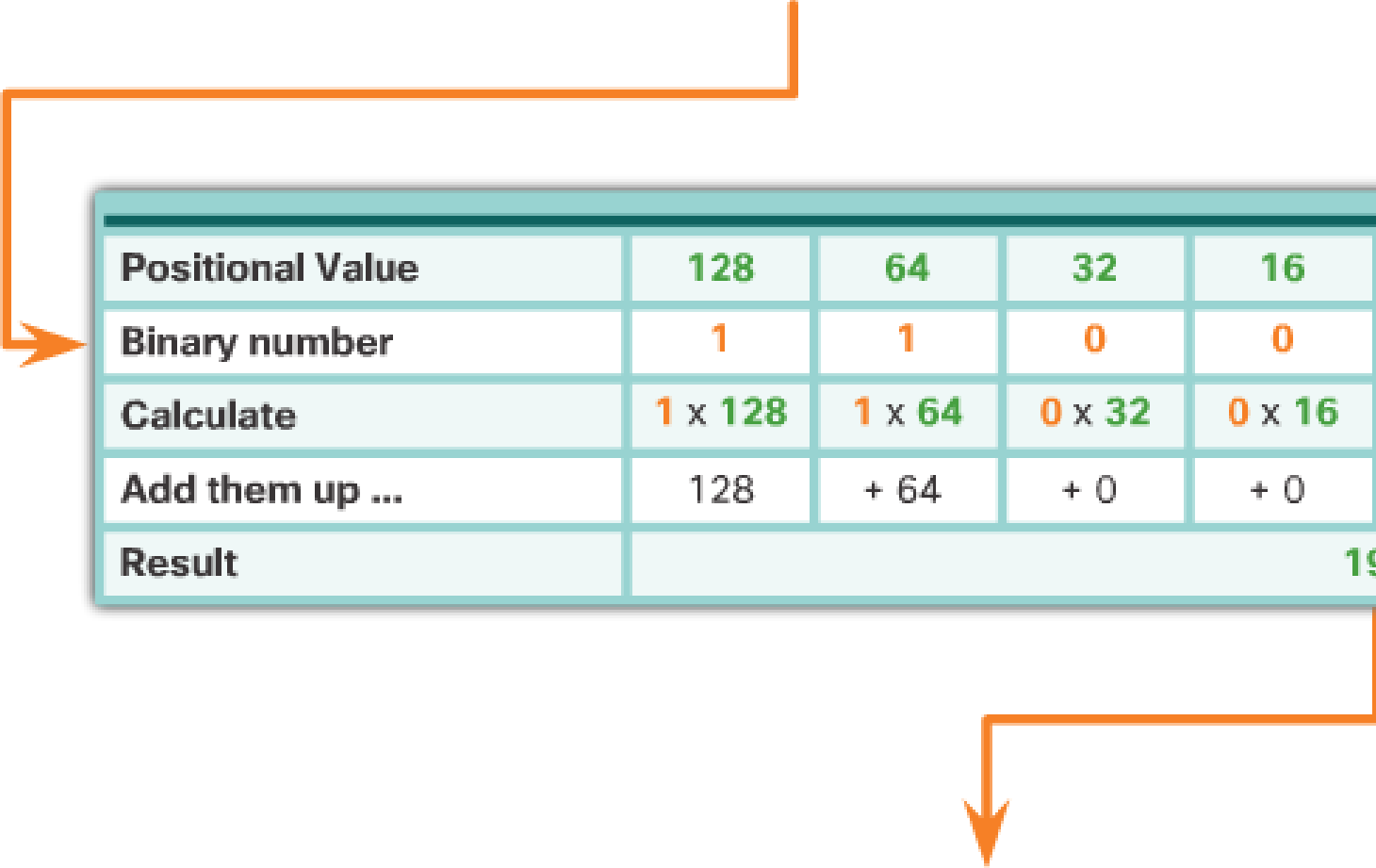
Radix	10	10	10	10
Position in #	3	2	1	0
Calculate	(10^3)	(10^2)	(10^1)	(10^0)
Positional Value	1000	100	10	1

Radix

The first row identifies the number base or radix. The decimal notation system is based on 10, therefore the radix is 10.

7.1.1.4 Binary to Decimal Conversion

11000000.10101000.00001011.00001010



Positional Value	128	64	32	16	8	4	2	1
Binary number	1	1	0	0	0	0	0	0
Calculate	1 x 128	1 x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	0 x 1
Add them up ...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Result	192							

192.____.____.____
Dotted Decimal Notation

7.1.1.5 Activity – Binary to Decimal Conversion

Enter decimal answer here

Decimal value

13

Base

2

2

2

2

2

2

2

2

Exponent

7

6

5

4

3

2

1

0

Position

128

64

32

16

8

4

2

1

Bit

0

0

0

0

1

1

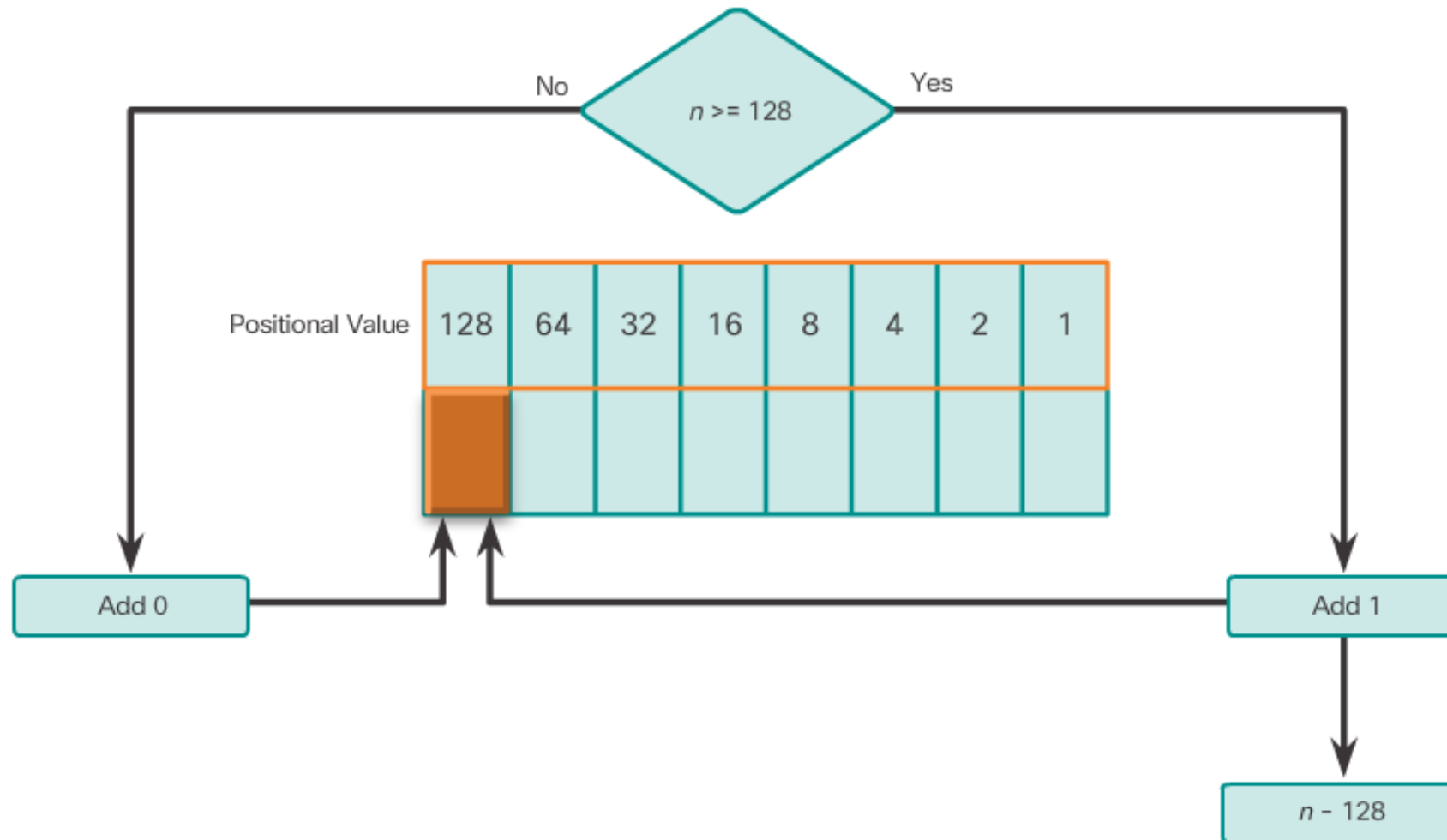
0

1

Binary number

7.1.1.6 Decimal to Binary Conversion

Is the Decimal n Greater Than or Equal To 128?



Decimal to Binary Conversion

It is also necessary to understand how to convert a dotted decimal IPv4 address to binary. A useful tool is the binary positional value table. The following illustrates how to use the table to convert decimal to binary:

7.1.1.7 Decimal to Binary Conversion Examples

$$11 = 00001011$$

Example: 192.168.10.11

Positional Value	128	64	32	16	8	4	2	1
	0	0	0	0	1	0	1	1

11000000 . 10101000 . 00001010 . 00001011

Decimal to Binary Conversion Examples

To help understand the process, consider the IP address 192.168.11.10. Using the previously explained process, start with the binary positional value table and the first decimal number 192.

Decimal value	37							
Base	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Position	128	64	32	16	8	4	2	1
Bit	0	0	1	0	0	1	0	1



Binary Game

A fun way to learn binary numbers for networking.

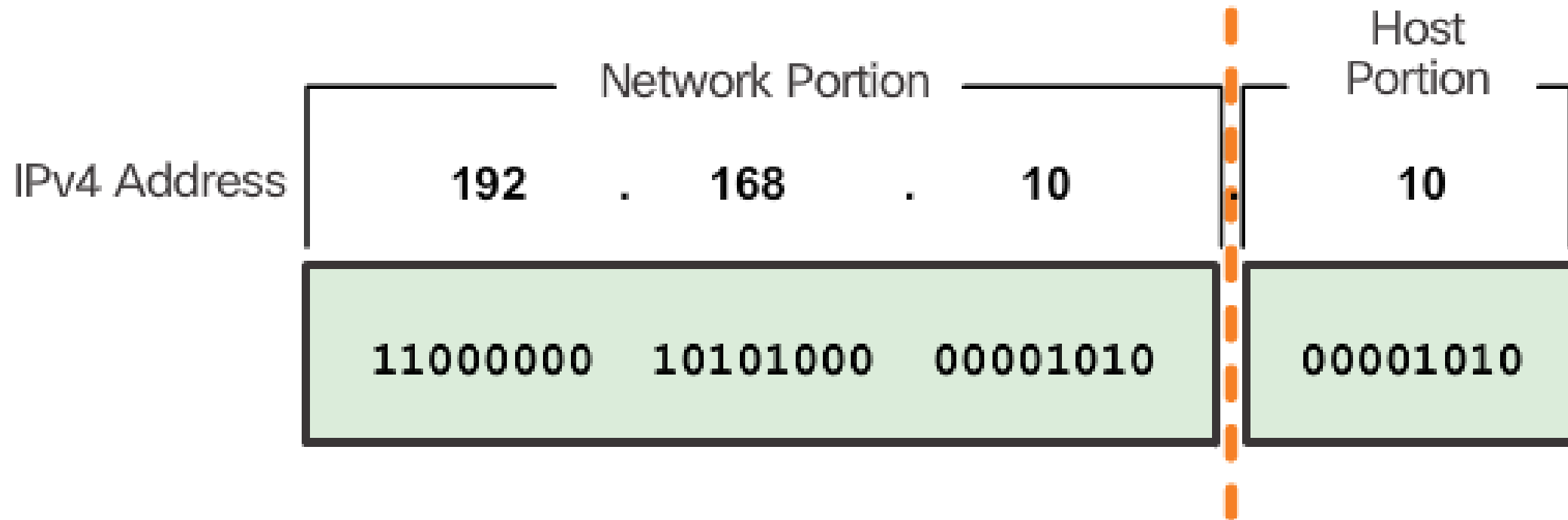
Game Link:

<https://learningnetwork.cisco.com/docs/DOC-1803>

(You will need to log in to cisco.com to use this link. It will be necessary to create an account if you do not already have one.)

Mobile Download:

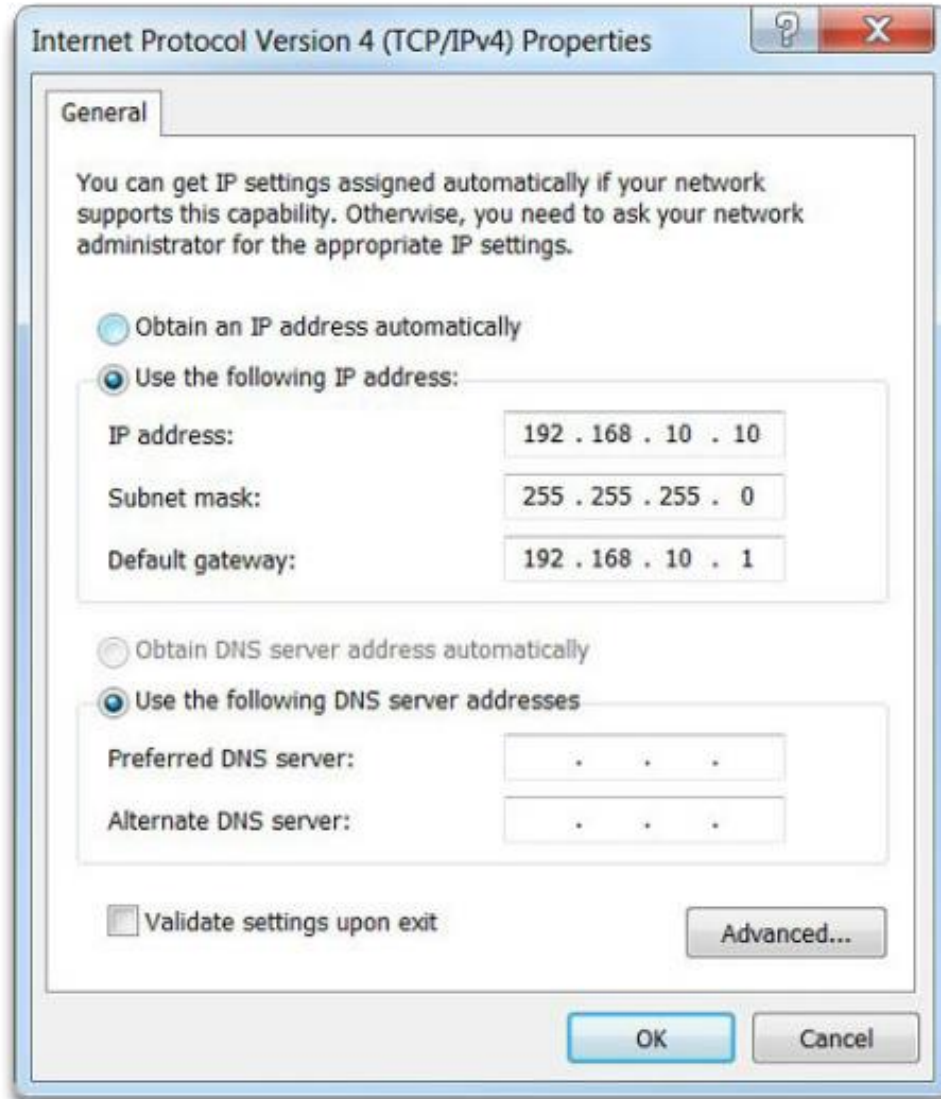
<https://learningnetwork.cisco.com/docs/DOC-11119>



172.16.8.4

10.15.15.1

IP Configuration on a Host



The Subnet Mask

As shown in Figure 1, three dotted decimal IPv4 addresses must be configured when assigning an IPv4 configuration to host:

- **IPv4 address** – Unique IPv4 address of the host
- **Subnet mask**- Used to identify the network/host portion of the IPv4 address
- **Default gateway** – Identifies the local gateway (i.e. local router interface IPv4 address) to reach remote networks

Resulting Network Address

IP address

192 . 168 . 10 . 10

Binary

11000000 10101000 00001010 00001010

Subnet mask

255 . 255 . 255 . 0

11111111 11111111 11111111 00000000

AND Results

11000000 10101000 00001010 00000000

Network Address

192 . 168 . 10 . 0

7.1.2.4 Activity – ANDing to Determine the Network Address

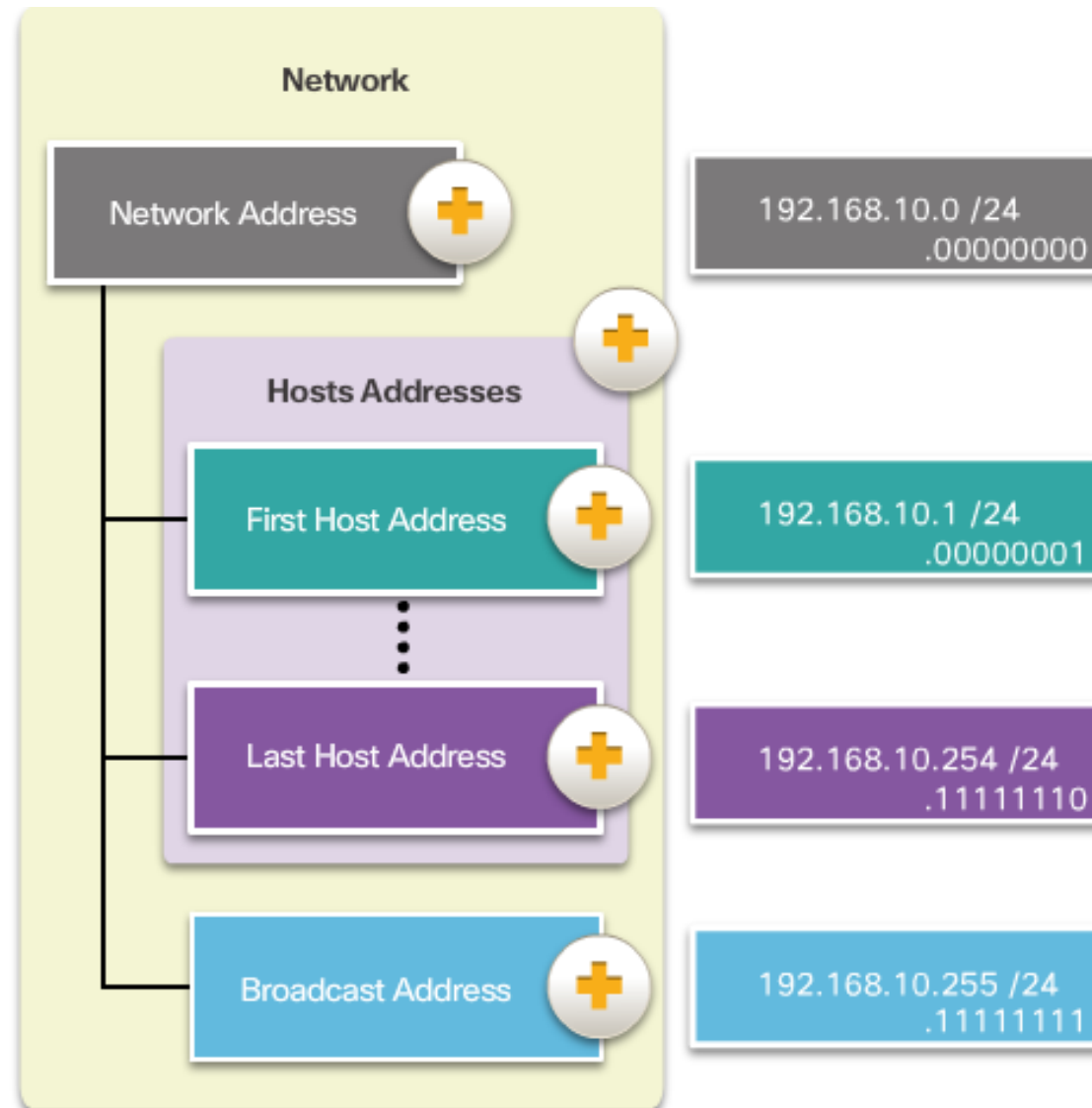
Host Address	10	123	182	171
Subnet Mask	255	255	255	192
Host Address in binary	00001010	01111011	10110110	10101011
Subnet Mask in binary	11111111	11111111	11111111	11000000
Network Address in binary	00001010	01111011	10110110	10000000
Network Address in decimal	10	123	182	128

Comparing the Subnet Mask and Prefix Length

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

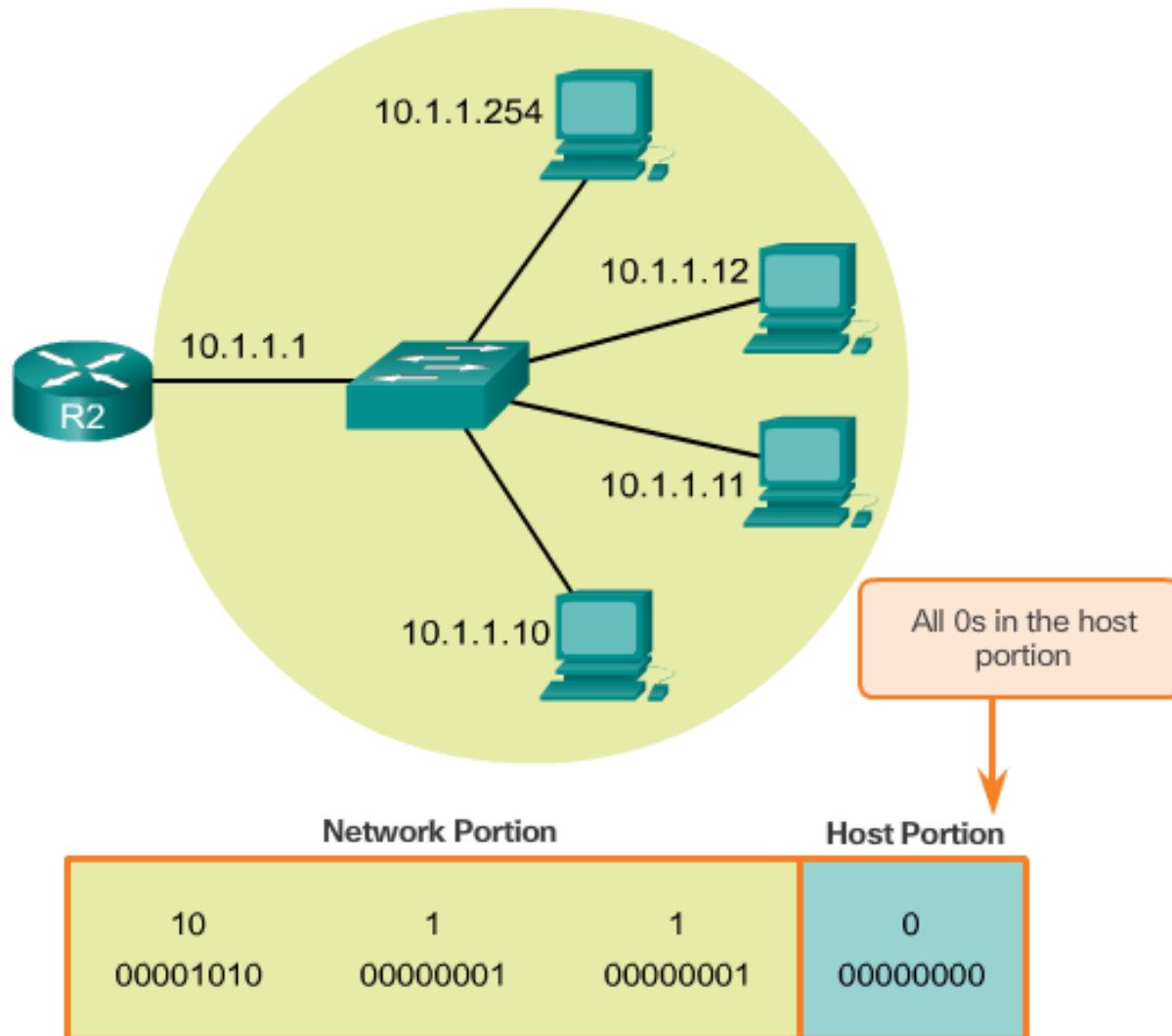
7.1.2.6 Network, Host, and Broadcast Addresses

Types of Addresses in Network 192.168.10.0 /24

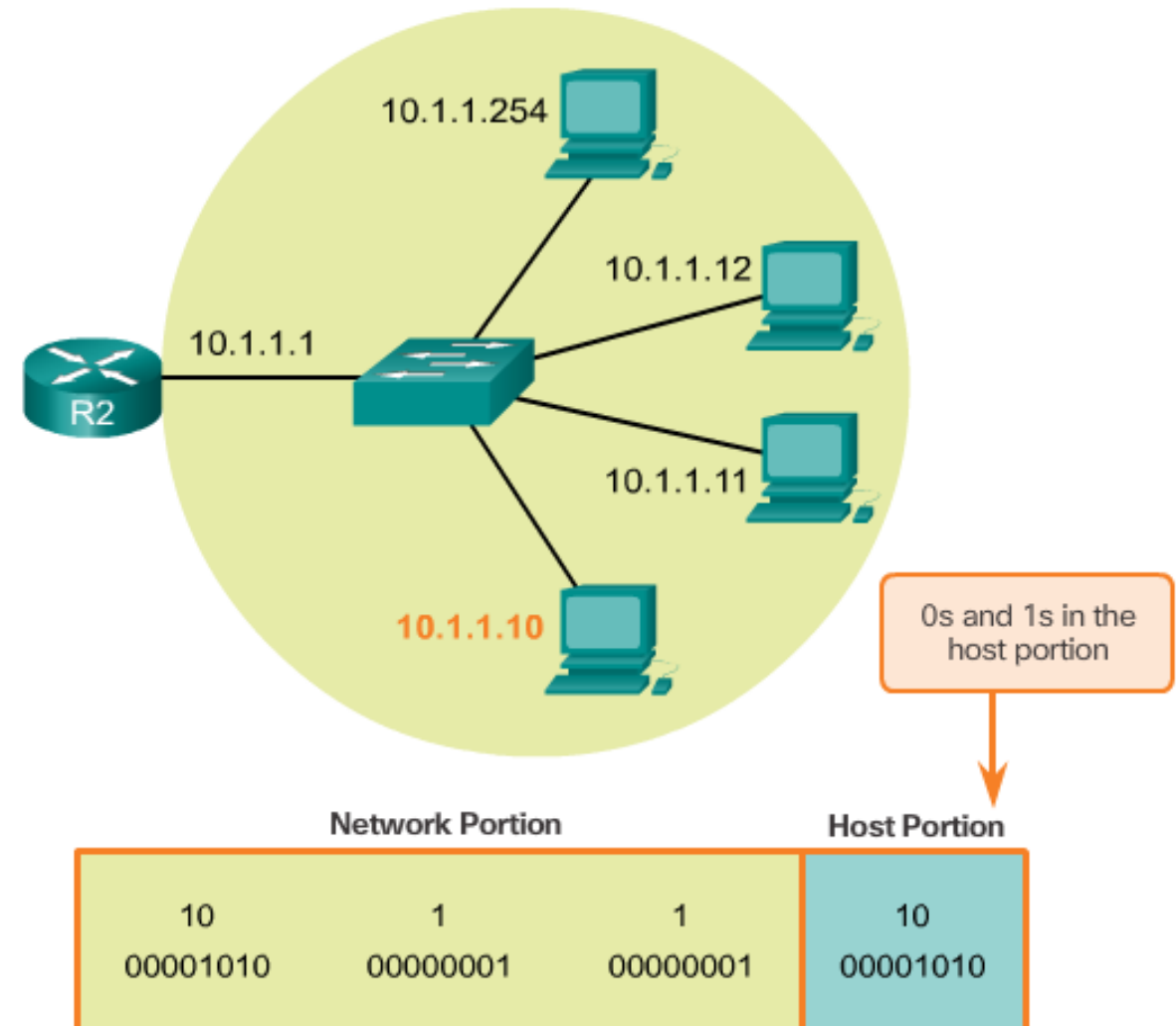


7.1.2.6 Network, Host, and Broadcast Addresses

Network Address

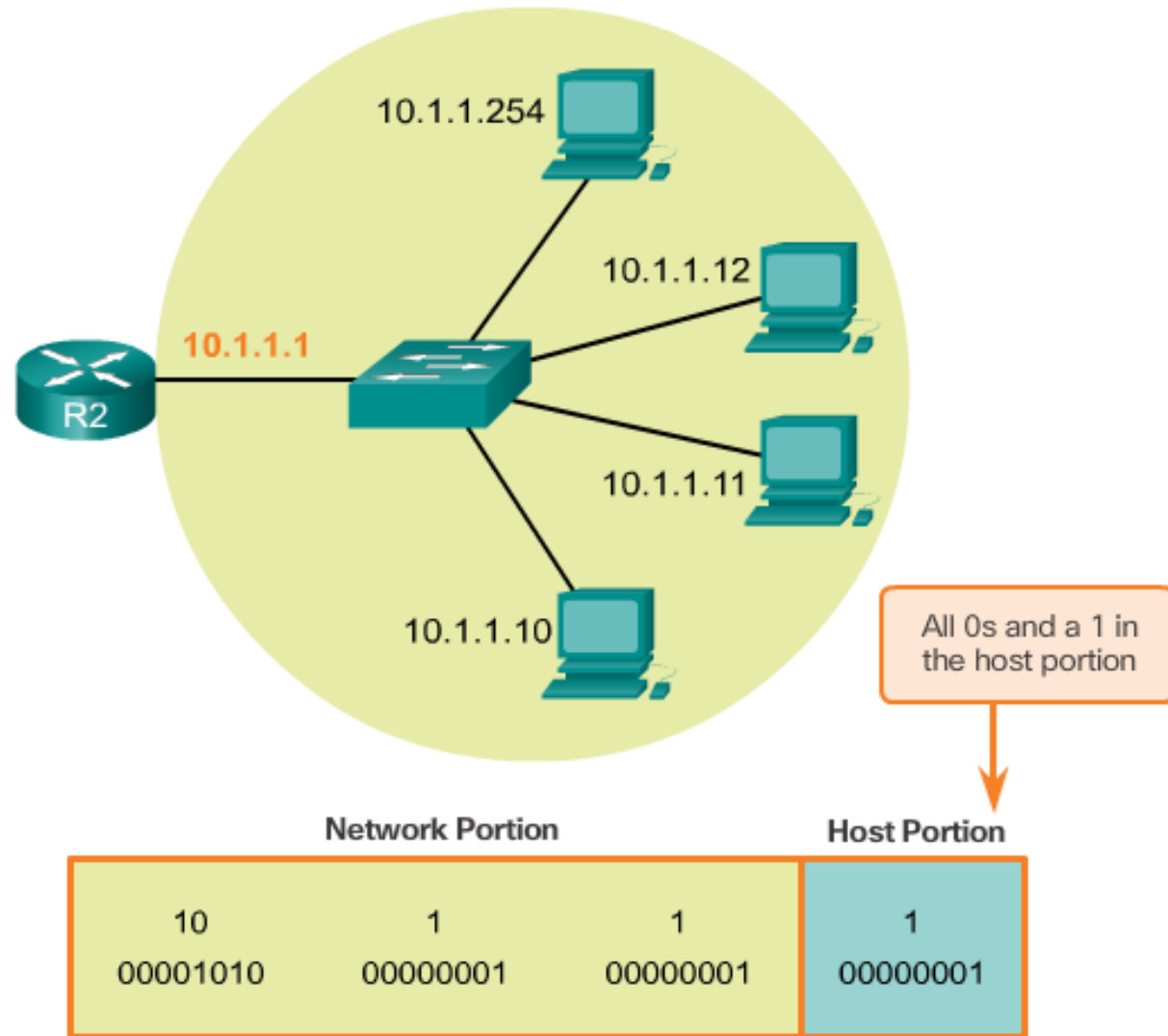


Host Address

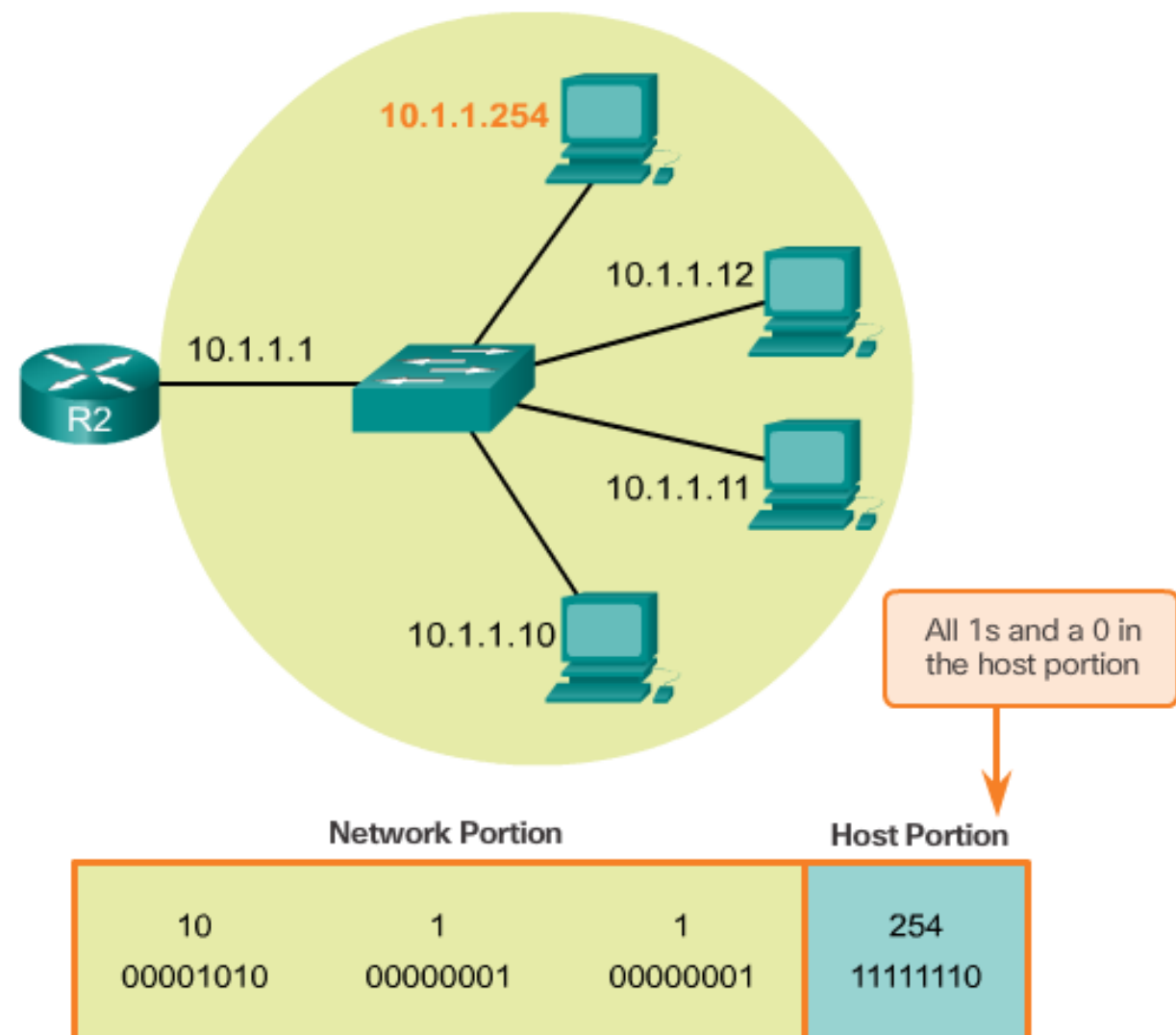


7.1.2.6 Network, Host, and Broadcast Addresses

First Host Address

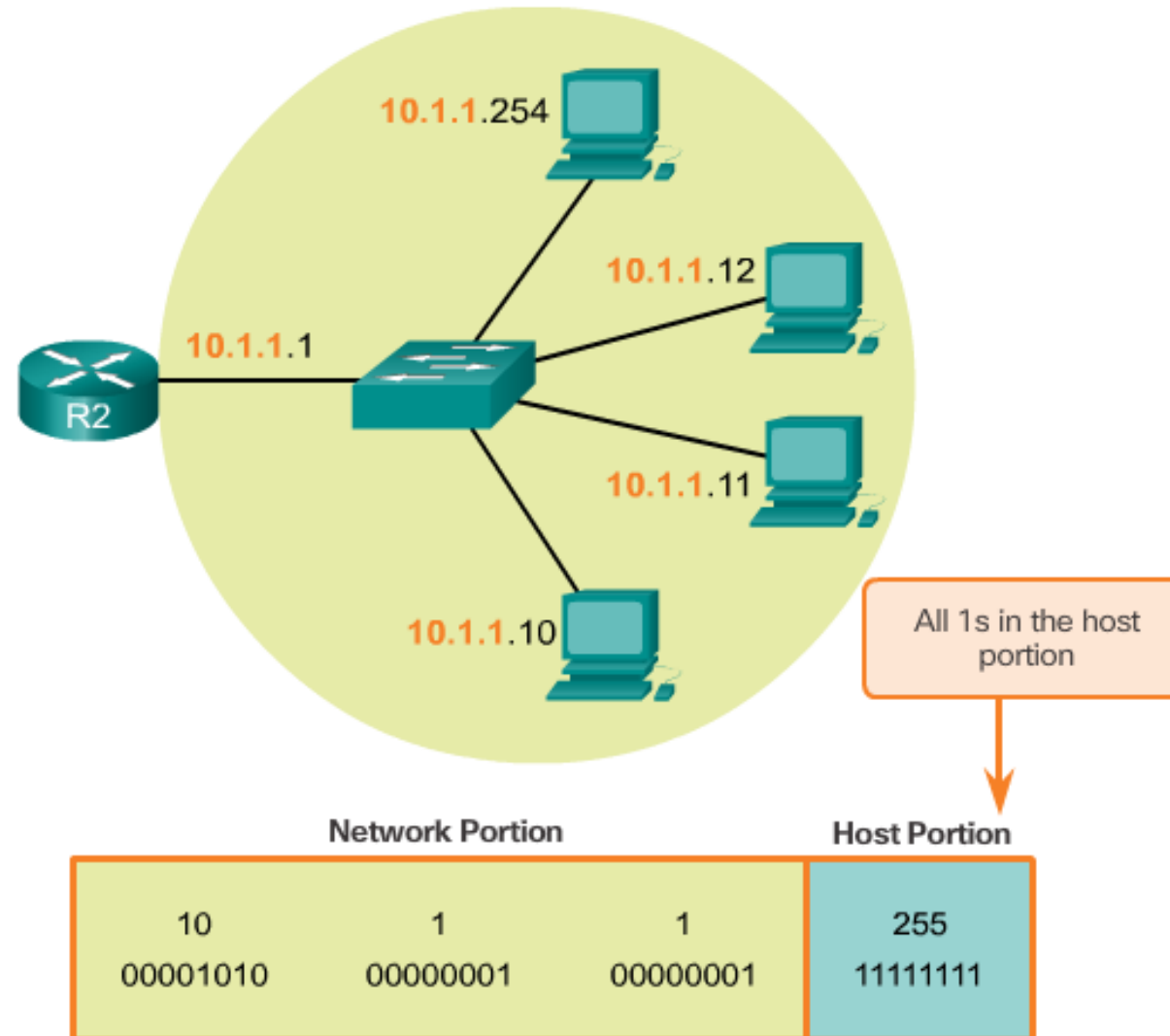


Last Host Address

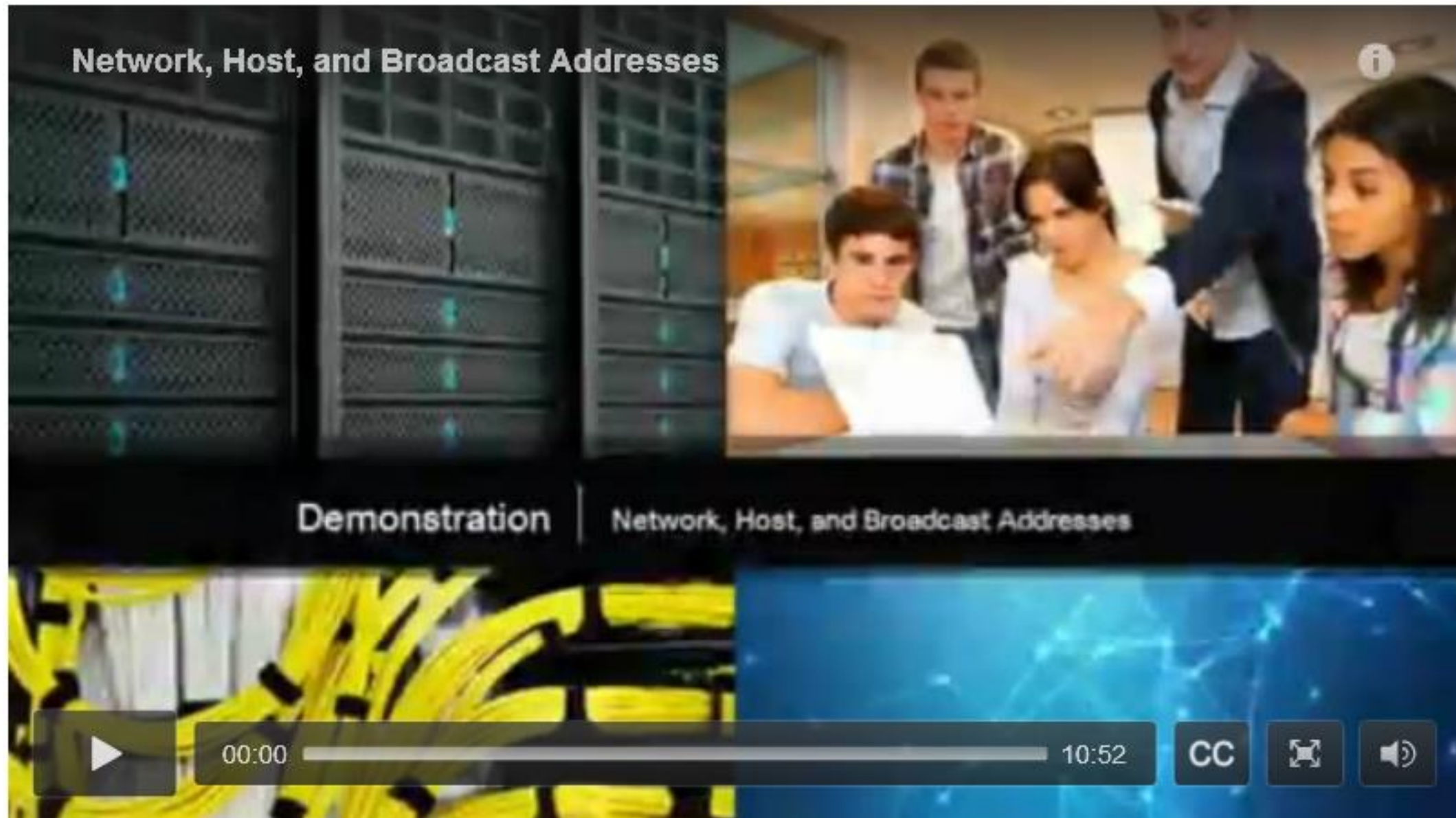


7.1.2.6 Network, Host, and Broadcast Addresses

Broadcast Address



7.1.2.7 Video Demonstration - Network, Host, and Broadcast Addresses



7.1.2.8 Lab – Using the Windows Calculator with Network Addresses



7.1.2.9 Lab – Converting IPv4 Addresses to Binary



7.1.3.1 Static IPv4 Address Assignment to a Host

Static Assignment

The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box with the 'General' tab selected. The text inside reads: 'You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.' Below this, there are two radio button options. The first is 'Obtain an IP address automatically' which is unselected. The second is 'Use the following IP address:' which is selected. Under this selection, there are three text boxes: 'IP address:' containing '192 . 168 . 10 . 10', 'Subnet mask:' containing '255 . 255 . 255 . 0', and 'Default gateway:' containing '192 . 168 . 10 . 1'. Below these, there are two more radio button options for DNS: 'Obtain DNS server address automatically' (unselected) and 'Use the following DNS server addresses' (selected). Under this, there are two text boxes: 'Preferred DNS server:' and 'Alternate DNS server:', both containing ' . . .'. At the bottom left, there is a checkbox 'Validate settings upon exit' which is unchecked. At the bottom right, there is an 'Advanced...' button. At the very bottom, there are 'OK' and 'Cancel' buttons.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 10 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Dynamic Assignment

The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' dialog box with the 'Alternate Configuration' tab selected. The text inside reads: 'You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.' Below this, there are two radio button options. The first is 'Obtain an IP address automatically' which is selected. The second is 'Use the following IP address:' which is unselected. Under this selection, there are three text boxes: 'IP address:', 'Subnet mask:', and 'Default gateway:', all containing ' . . .'. Below these, there are two more radio button options for DNS: 'Obtain DNS server address automatically' (selected) and 'Use the following DNS server addresses' (unselected). Under this, there are two text boxes: 'Preferred DNS server:' and 'Alternate DNS server:', both containing ' . . .'. At the bottom left, there is a checkbox 'Validate settings upon exit' which is unchecked. At the bottom right, there is an 'Advanced...' button. At the very bottom, there are 'OK' and 'Cancel' buttons.

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

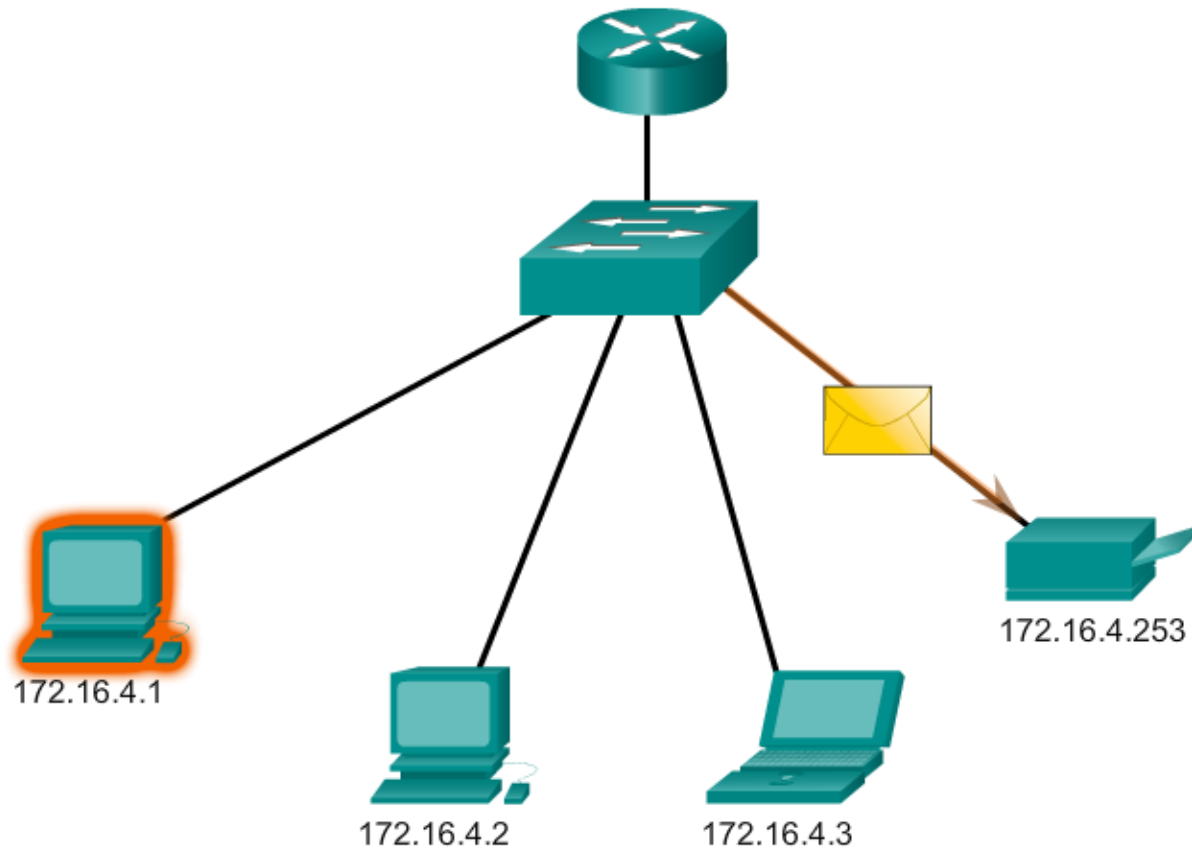
☐ Validate settings upon exit

Advanced...

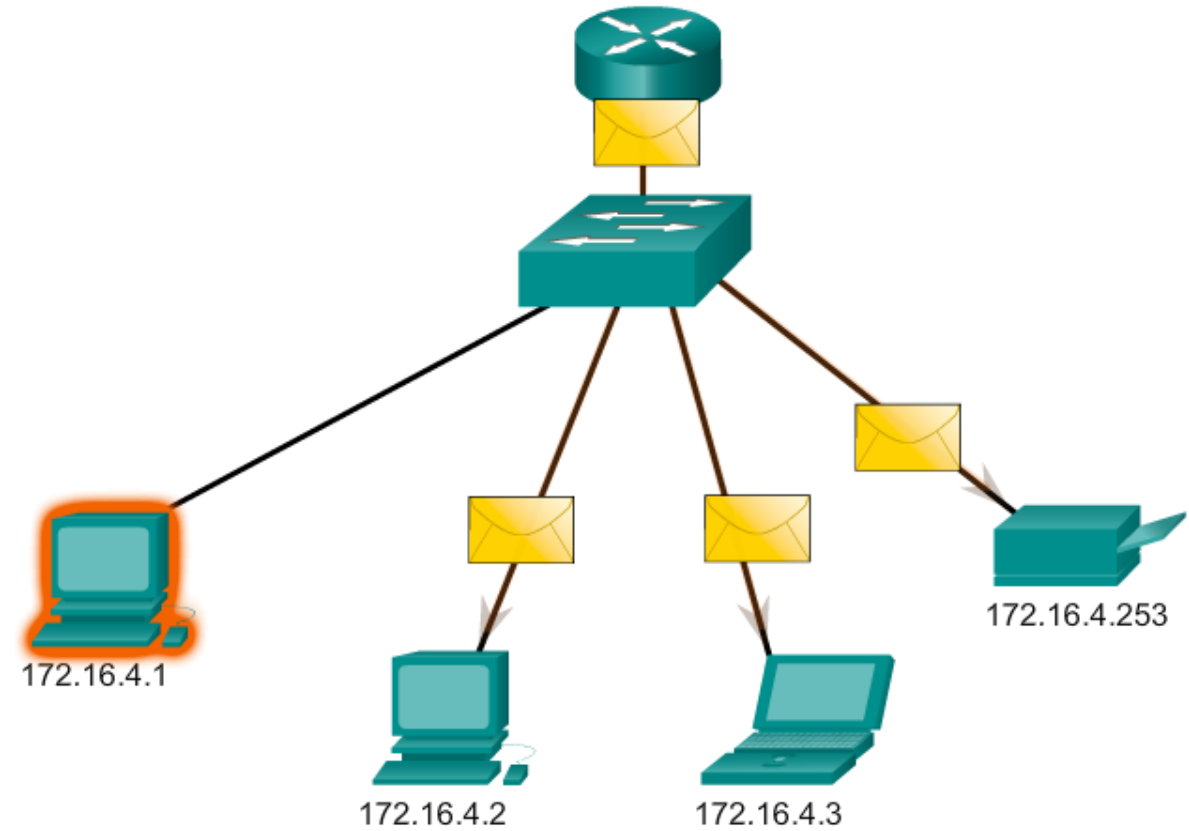
OK Cancel

7.1.3.3 IPv4 Communication

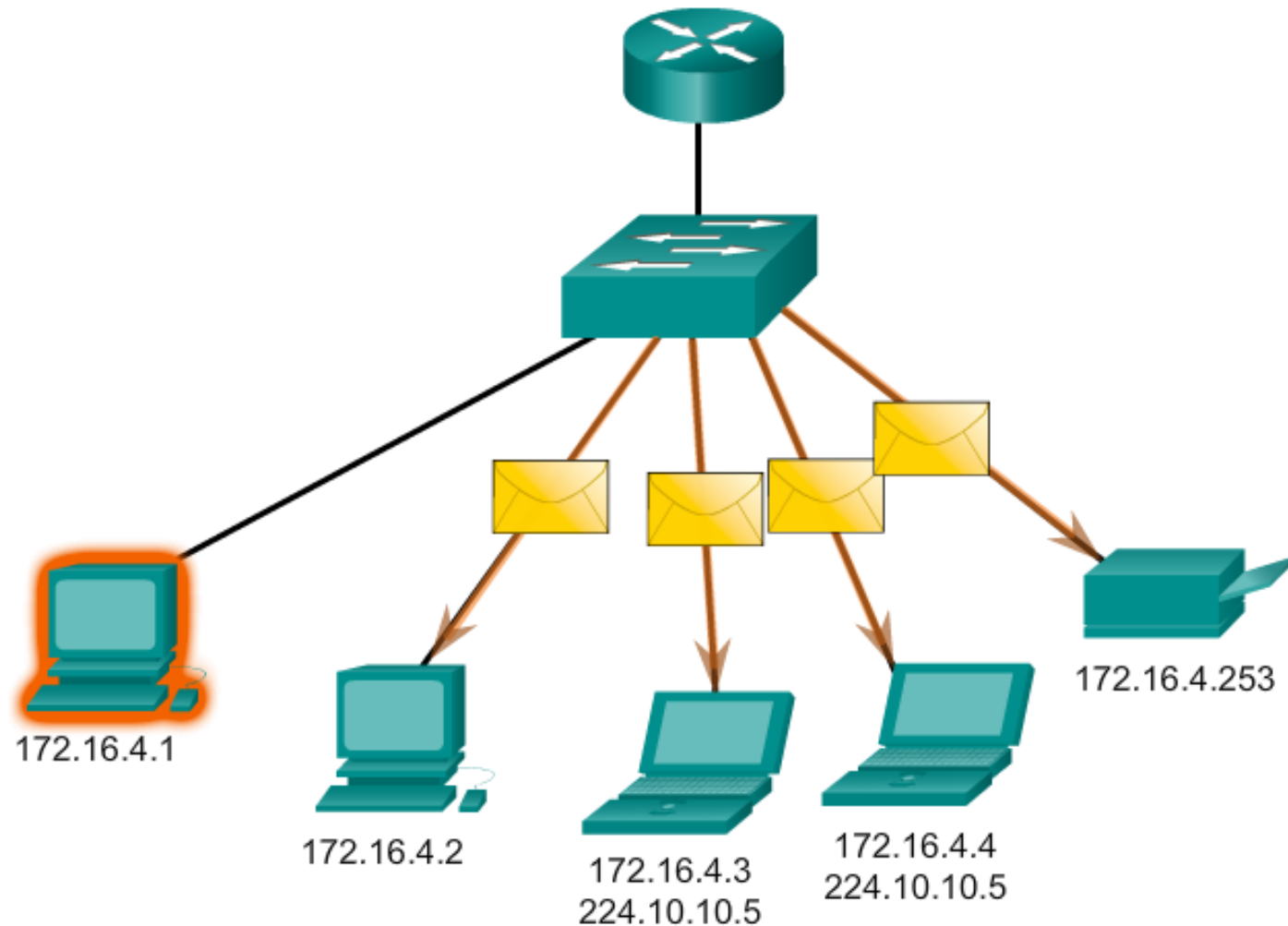
Unicast Communication



Broadcast Communication



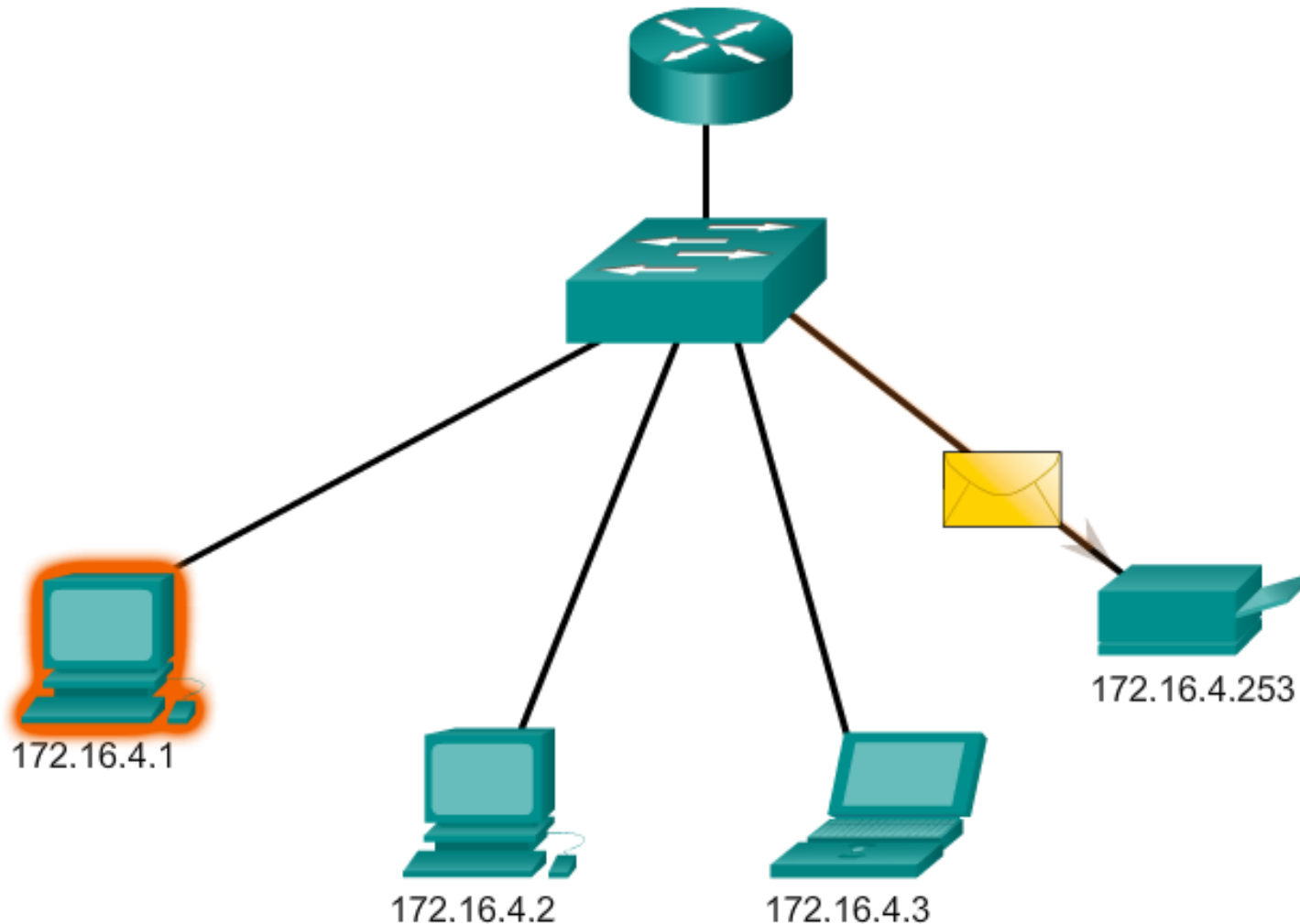
Multicast Communication



Multicast - The process of sending a packet from one host to a selected group of hosts, possibly in different networks, as shown in Figure 3

Unicast Transmission

Source: 172.16.4.1
Destination: 172.16.4.253

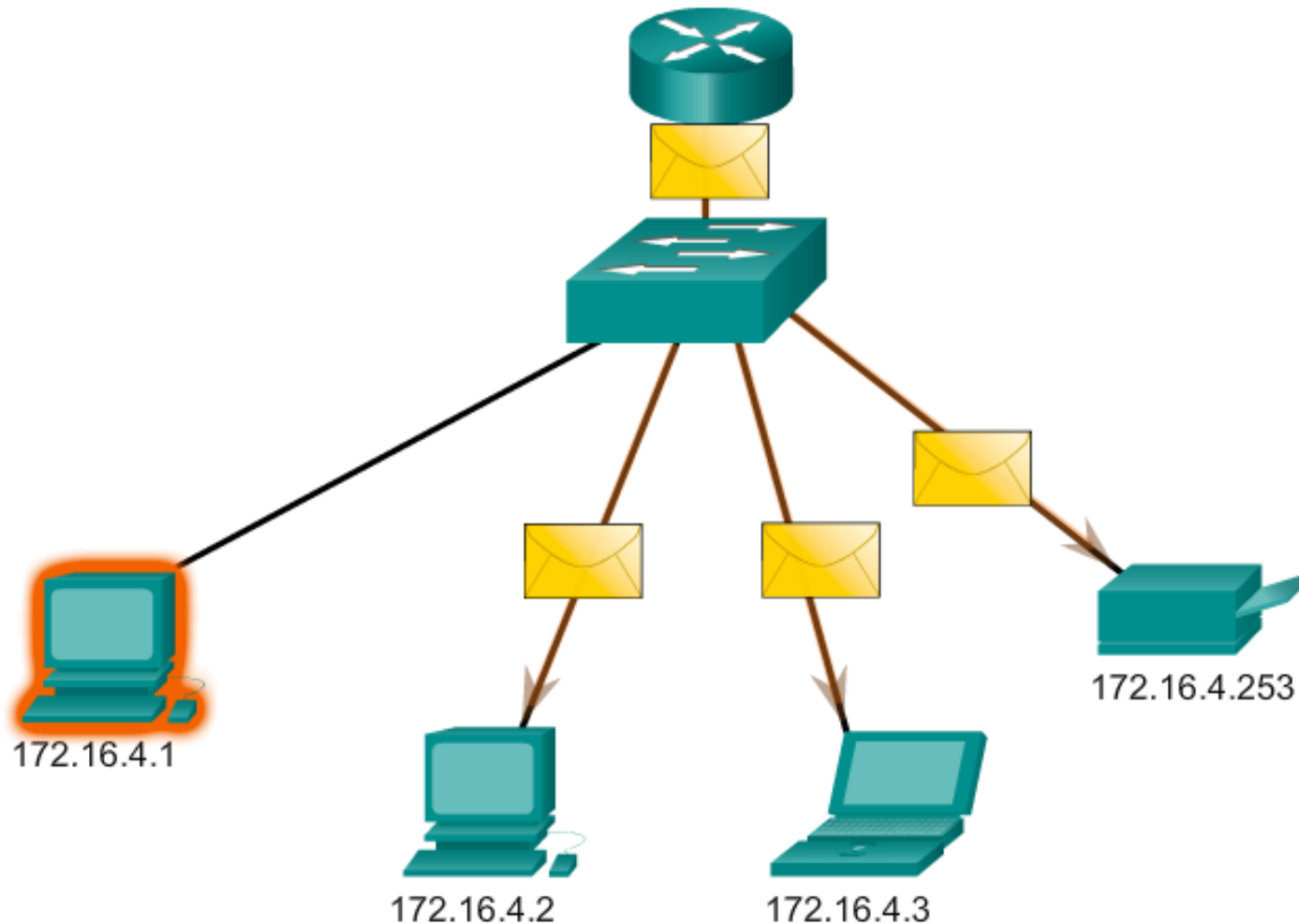


Unicast Transmission

Unicast communication is used for normal host-to-host communication in both a client/server and a peer-to-peer network. Unicast packets use the address of the destination device as the destination address and can be routed through an internetwork.

Limited Broadcast Transmission

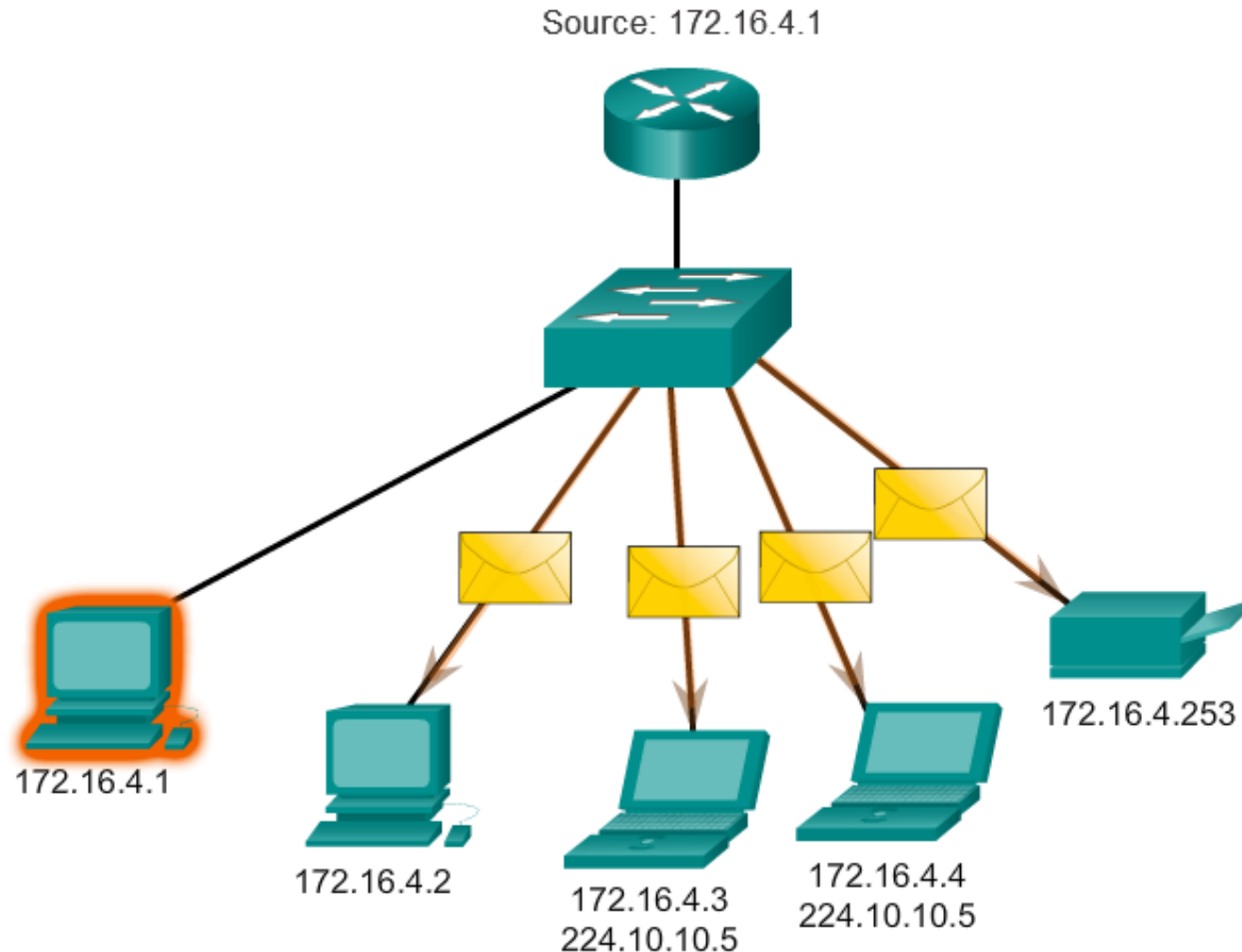
Limited Broadcast
Source: 172.16.4.1
Destination: 255.255.255.255



Broadcast Transmission

Broadcast traffic is used to send packets to all hosts in the network using the broadcast address for the network. With a broadcast, the packet contains a destination IPv4 address with all ones (1s) in the host portion. This means that all hosts on that local network (broadcast domain) will receive and look at the packet. Many network protocols, such as DHCP, use broadcasts. When a host receives a packet sent to the network broadcast address, the host processes the packet as it would a packet addressed to its unicast address.

Multicast Transmission

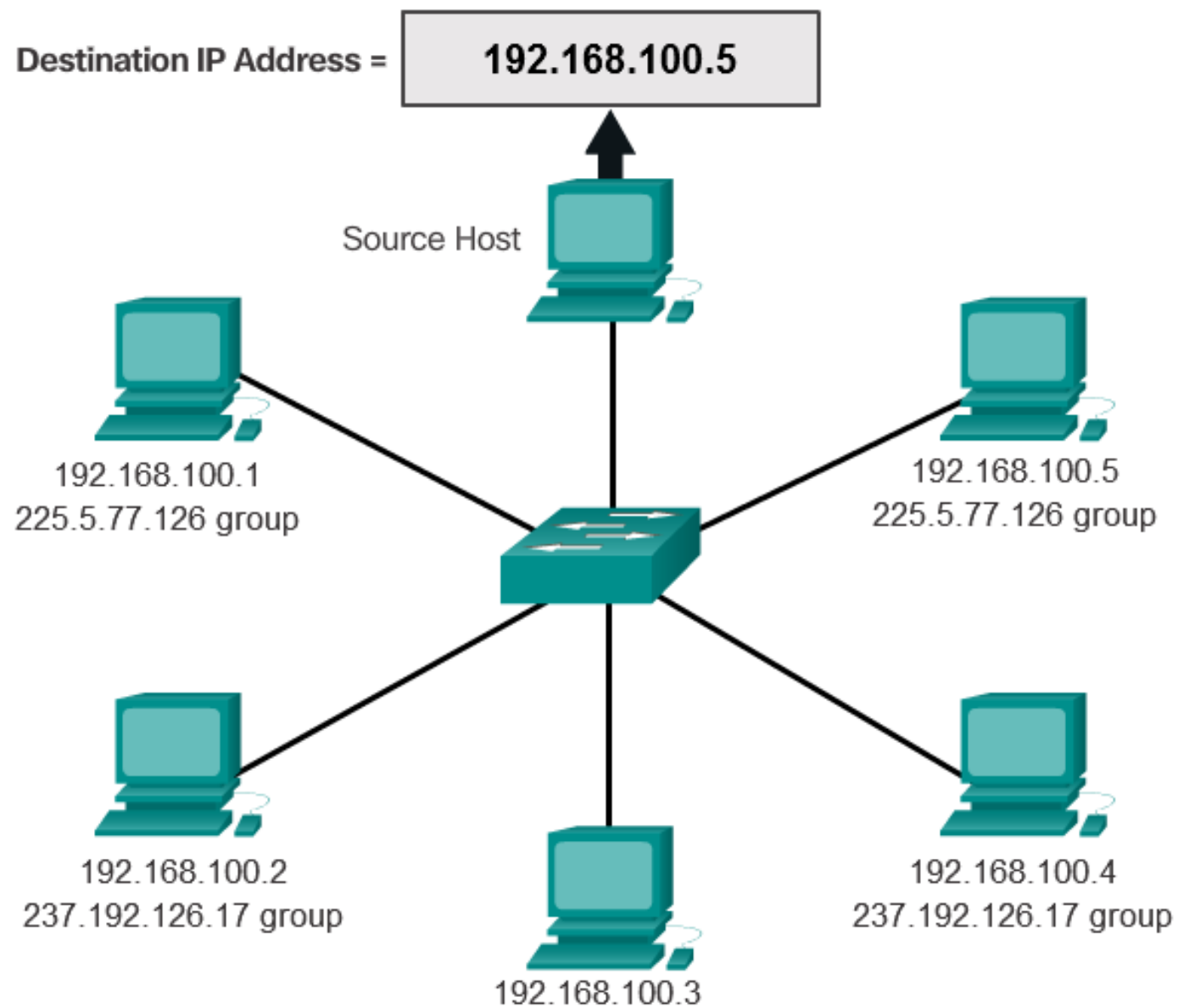


Multicast Transmission

Multicast transmission reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group.

IPv4 has reserved the 224.0.0.0 to 239.255.255.255 addresses as a multicast range. The IPv4 multicast addresses 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. These addresses are to be used for multicast groups on a local network. A router connected to the local network recognizes that these packets are addressed to a local network multicast group and never forwards them further

7.1.3.7 Activity – Unicast, Broadcast, or Multicast



7.1.3.8 Packet Tracer – Investigate Unicast, Broadcast, and Multicast Traffic

Cisco Networking Academy®
Mind Wide Open™

Cisco Packet Tracer

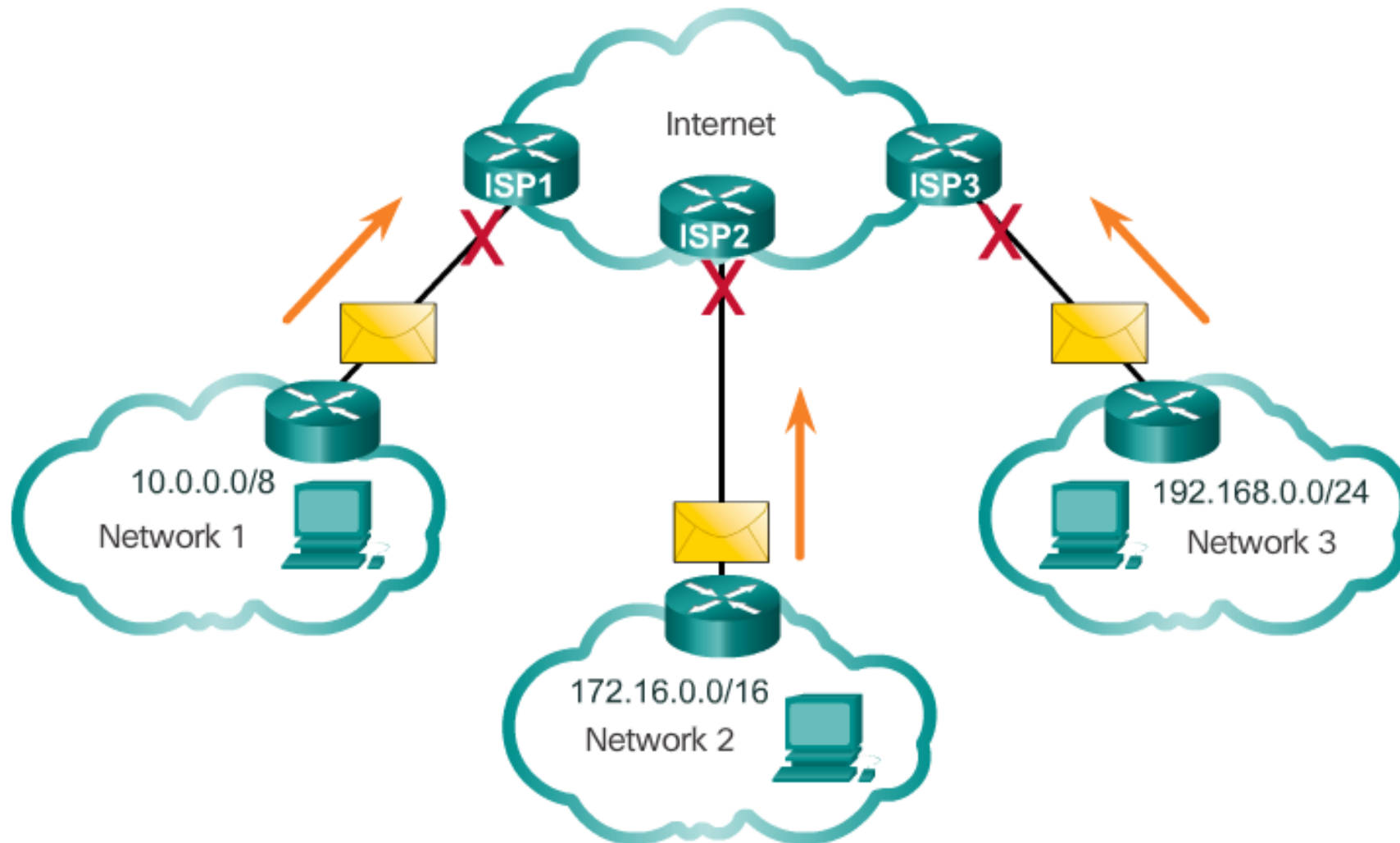
Packet Tracer | Investigate Unicast, Broadcast, and Multicast Traffic

2950T-24
SW-A

PC-PT C1 PC-PT C2 PC-PT C3 PC-PT C4 PC-PT D1 PC-PT D2

7.1.4.1 Public and Private IPv4 Addresses

Private addresses cannot be routed over the Internet



Specifically, the private address blocks are:

- **10.0.0.0 /8** or **10.0.0.0** to **10.255.255.255**
- **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



7.1.4.3 Special User IPv4 Addresses

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>
```

- **Loopback addresses (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254)** – More commonly identified as only 127.0.0.1, these are special addresses used by a host to direct traffic to itself.
- **Link-Local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254)** – More commonly known as the Automatic Private IP Addressing (APIPA) addresses, they are used by a Windows DHCP client to self-configure in the event that there are no DHCP servers available. Useful in a peer-to-peer connection.
- **TEST-NET addresses (192.0.2.0/24 or 192.0.2.0 to 192.0.2.255)** – These addresses are set aside for teaching and learning purposes and can be used in documentation and network examples.

7.1.4.4 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.____.____.____

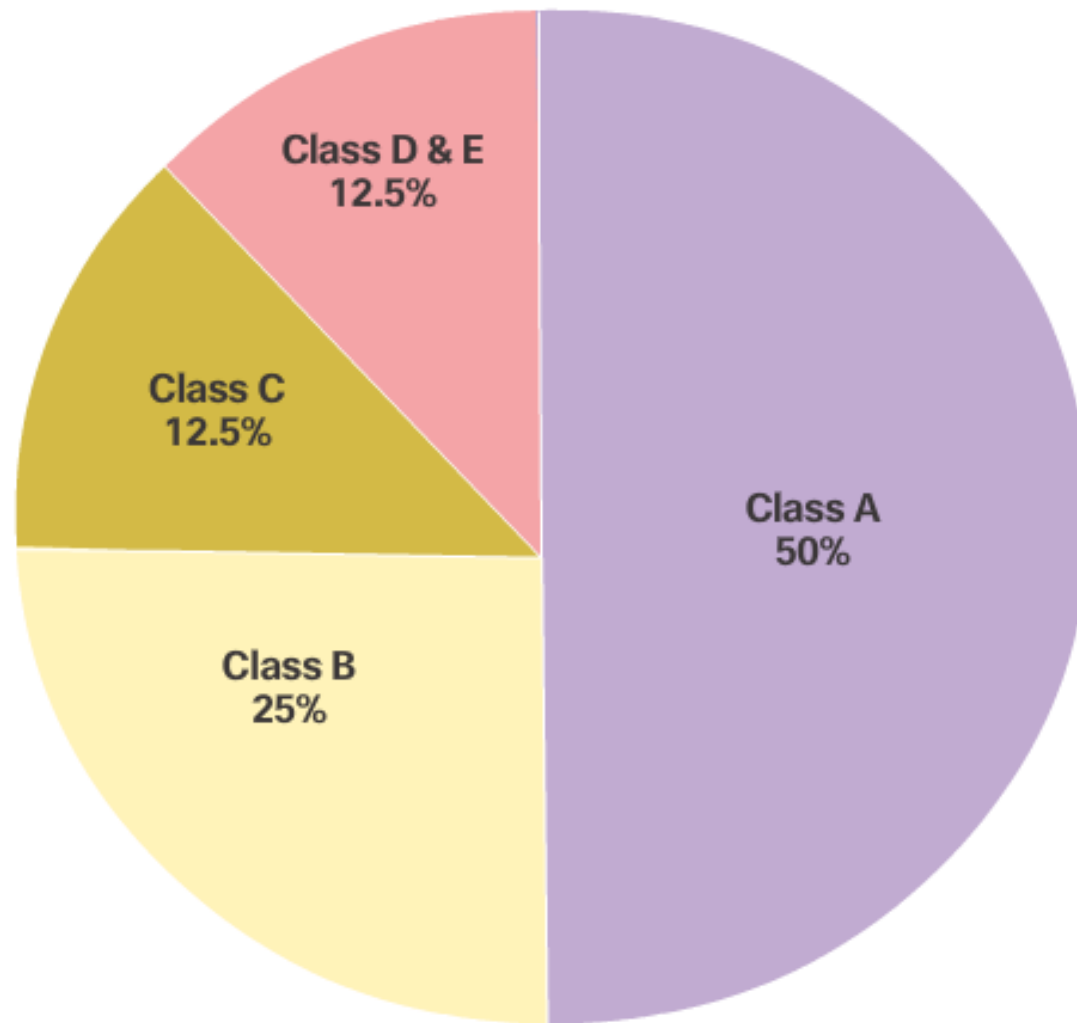
- **Class A (0.0.0.0/8 to 127.0.0.0/8)** – Designed to support extremely large networks with more than 16 million host addresses
Class B (128.0.0.0/16 – 191.255.0.0/16) – Designed to support the needs of moderate to large size networks with up to approximately 65,000 host addresses
Class C (192.0.0.0/24 – 223.255.255.0/24) – Designed to support small networks with a maximum of 254 hosts. It used a fixed /24 prefix with the first three octets to indicate the network and the remaining octet for the host addresses.

7.1.4.5 Video Demonstration - Classful IPv4 Addressing



7.1.4.6 Classless Addressing

Summary of Classful Addressing



Class A

Total Networks: 128

Total Hosts/Net: 16,777,214

Class B

Total Networks: 16,384

Total Hosts/Net: 65,534

Class C

Total Networks: 2,097,152

Total Hosts/Net: 254

Assignment of IP Addresses



Both IPv4 and IPv6 addresses are managed by the Internet Assigned Numbers Authority (IANA) (<http://www.iana.org>). The IANA manages and allocates blocks of IP addresses to the Regional Internet Registries (RIRs).

7.1.4.8 Activity – Public or Private IPv4 Addresses



Public



117.22.10.10



198.172.17.7



200.0.0.1



192.255.255.255



127.255.255.255



Private



172.16.255.255



172.16.5.9

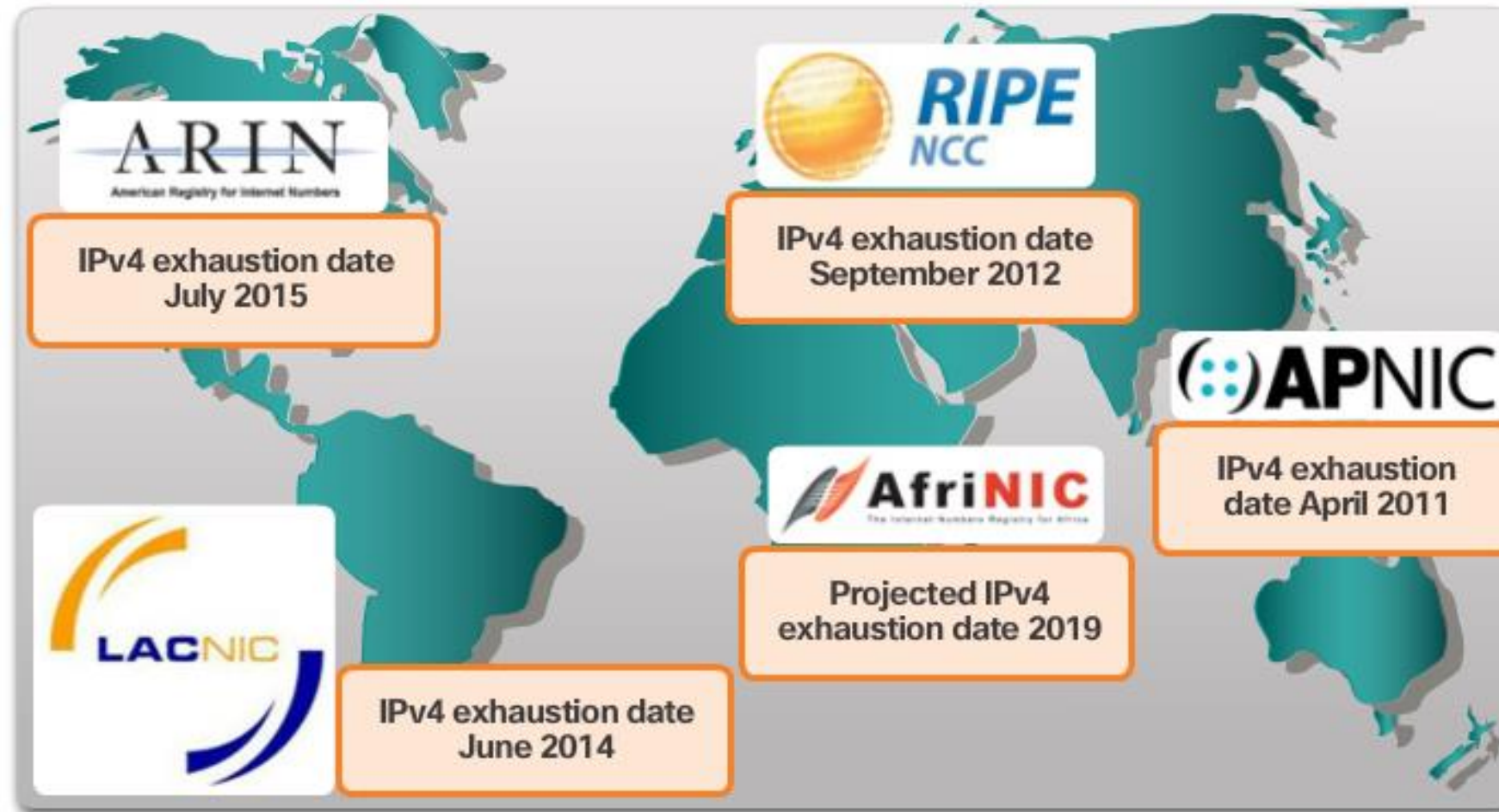


192.168.33.33

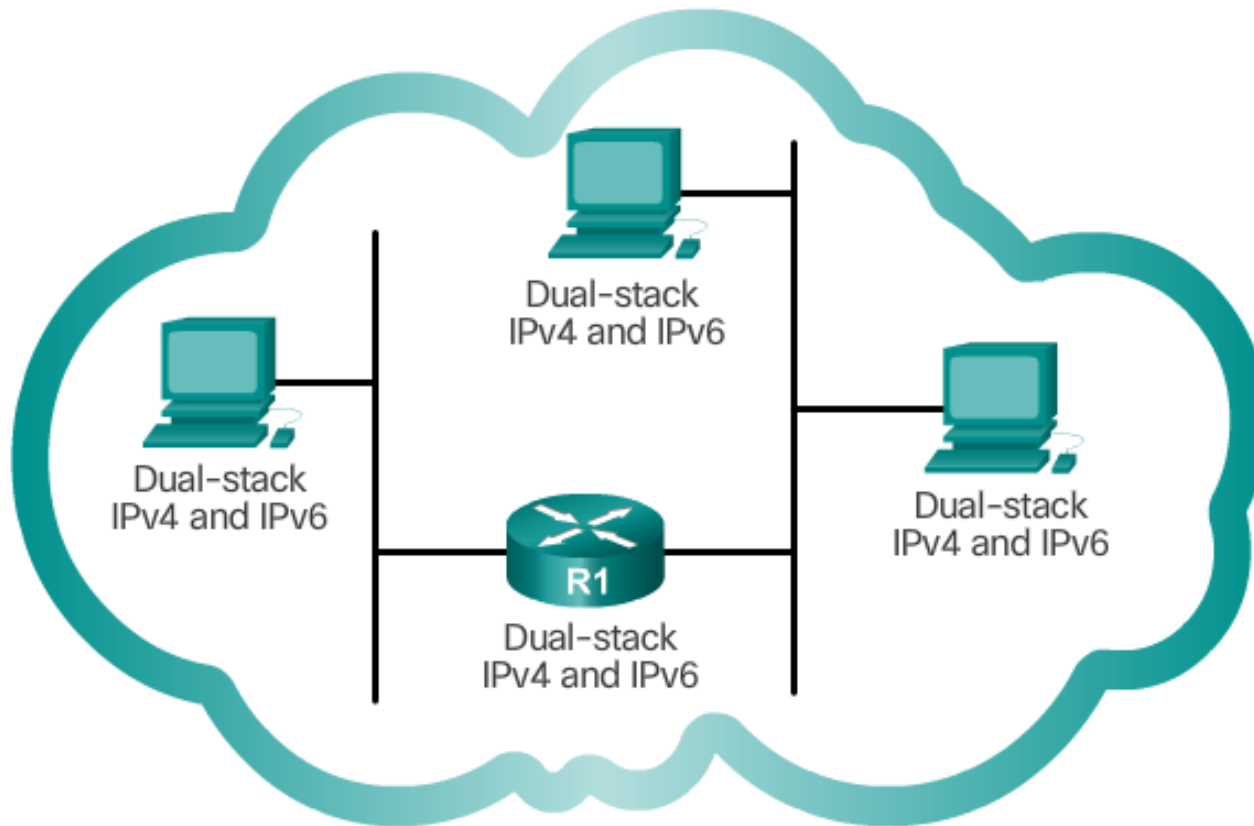
7.1.4.9 Lab – Identifying IPv4 Addresses



RIR IPv4 Exhaustion Dates



Dual-Stack

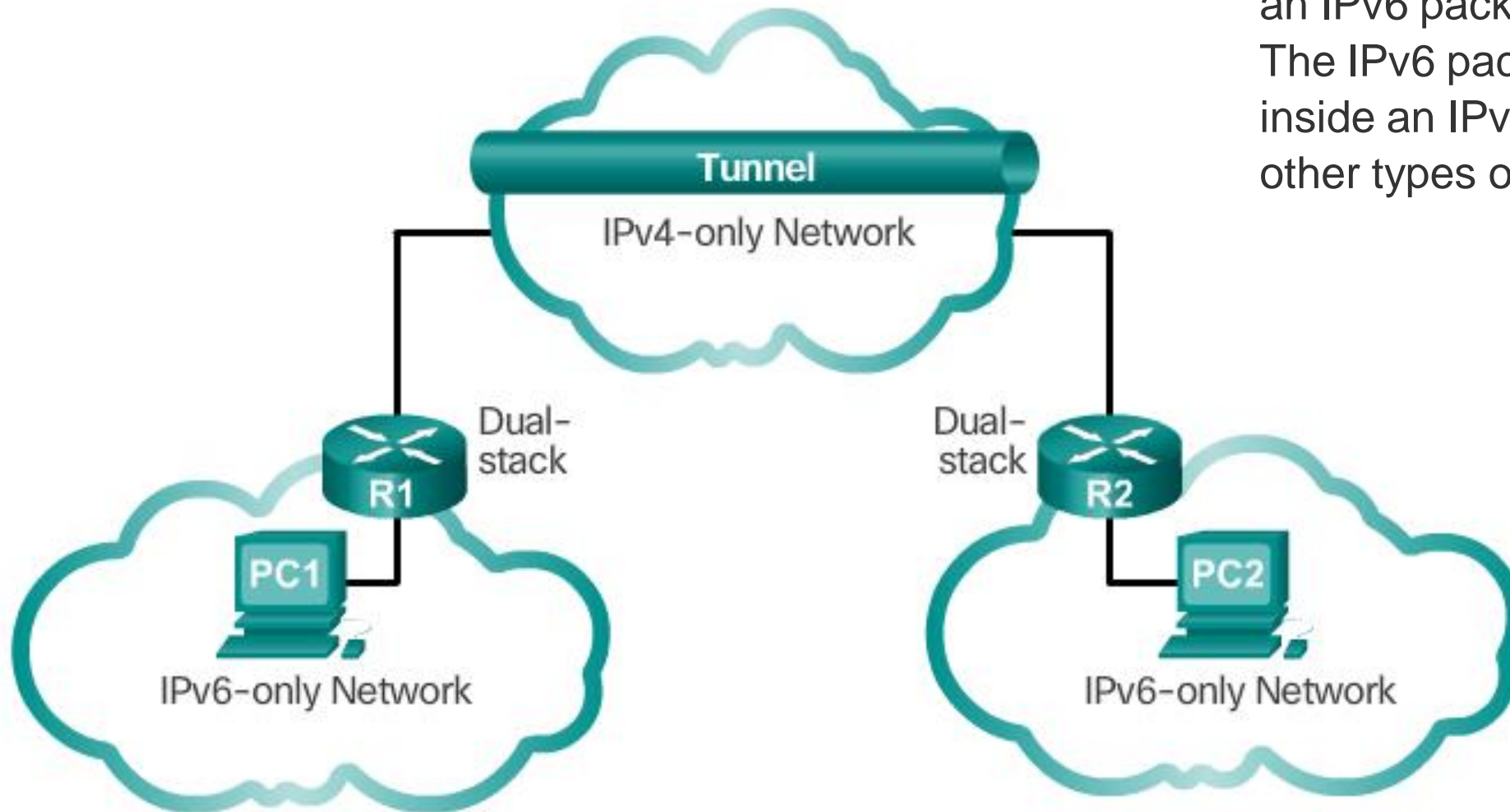


IPv4 and IPv6 Coexistence

There is not a single date to move to IPv6. For the foreseeable future, both IPv4 and IPv6 will coexist. The transition is expected to take years. The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. The migration techniques can be divided into three categories

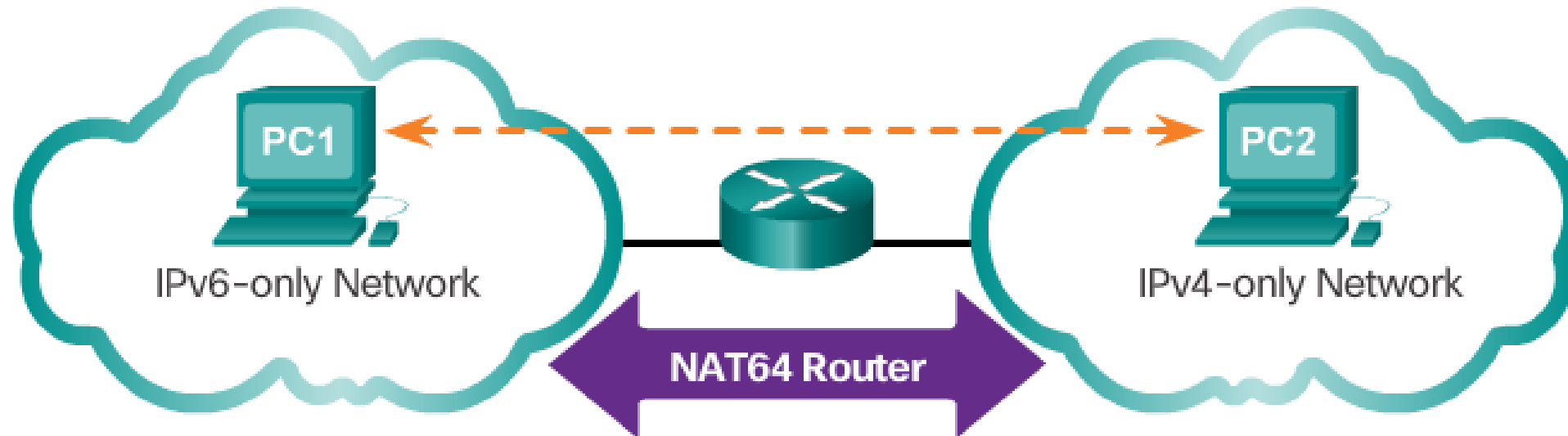
Dual Stack – As shown in Figure 1, dual stack allows IPv4 and IPv6 to coexist on the same network segment. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously

Tunneling



Tunneling – As shown in Figure 2, tunneling is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data.

Translation

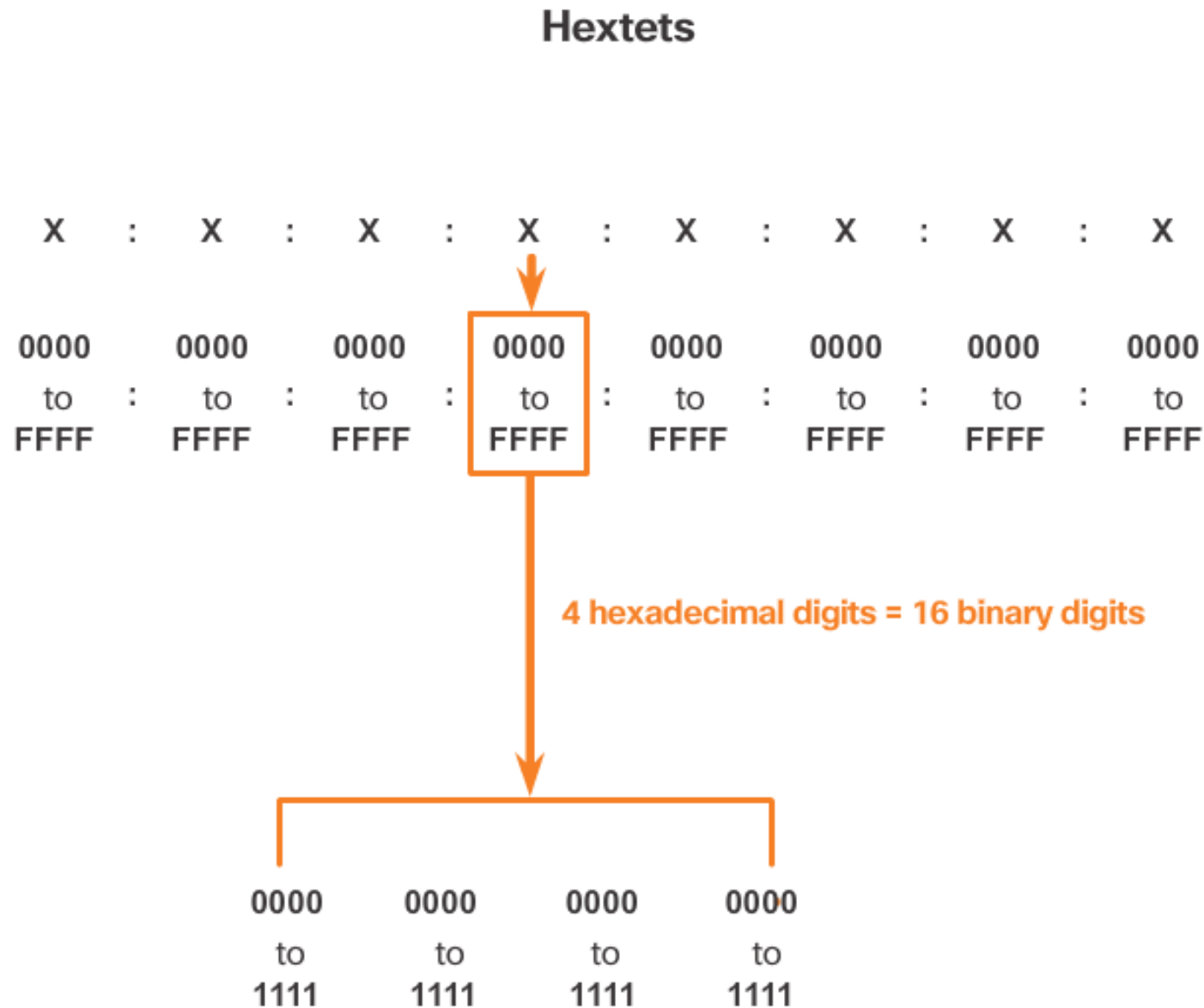


- **Translation** – As shown in Figure 3, Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet and vice versa.

7.2.1.3 Activity – IPv4 Issues and Solutions

	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.

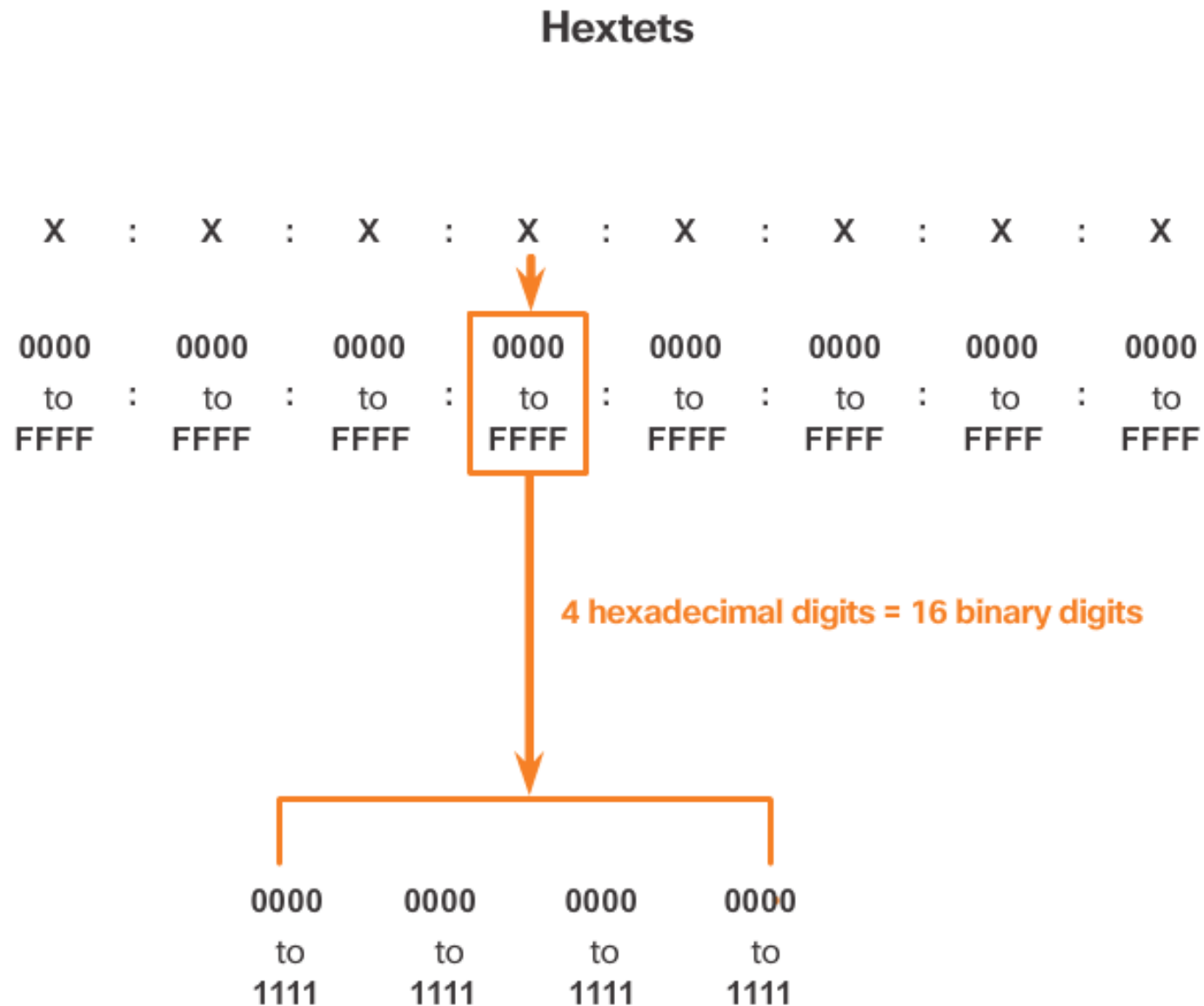
7.2.2.1 IPv6 Address Representation



IPv6 Address Representation

IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every 4 bits is represented by a single hexadecimal digit; for a total of 32 hexadecimal values, as shown in Figure 1. IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.

7.2.2.1 IPv6 Address Representation



The preferred format for writing an IPv6 address is `x:x:x:x:x:x:x:x`, with each “x” consisting of four hexadecimal values. When referring to 8 bits of an IPv4 address we use the term octet. In IPv6, a hextet is the unofficial term used to refer to a segment of 16 bits or four hexadecimal values. Each “x” is a single hextet, 16 bits or four hexadecimal digits.

7.2.2.1 IPv6 Address Representation

Hexadecimal Numbering

Decimal and Binary equivalents of 0 to F Hexadecimal

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Omitting Leading 0s

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

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

Preferred	2001:0DB8:000A:1000:0000:0000:0000:0100
No leading 0s	2001: DB8: A:1000: 0: 0: 0: 100

7.2.2.2 Rule 1 – Omit Leading 0s

Preferred	FE80:0000:0000:0000:0123:4567:89AB:CDEF
No leading 0s	FE80: 0: 0: 0: 123:4567:89AB:CDEF

Preferred	FF02:0000:0000:0000:0000:0000:0000:0001
No leading 0s	FF02: 0: 0: 0: 0: 0: 0: 1

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

7.2.2.2 Rule 1 – Omit Leading 0s

Preferred	0000:0000:0000:0000:0000:0000:0000:0001
No leading 0s	0: 0: 0: 0: 0: 0: 0: 1

Preferred	0000:0000:0000:0000:0000:0000:0000:0000
No leading 0s	0: 0: 0: 0: 0: 0: 0: 0

Rule 1 – Omit Leading 0s

The first rule to help reduce the notation of IPv6 addresses is to omit any leading 0s (zeros) in any 16-bit section or hextet. For example:

- 01AB can be represented as 1AB
- 09F0 can be represented as 9F0
- 0A00 can be represented as A00
- 00AB can be represented as AB

This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous. For example, the hextet “ABC” could be either “0ABC” or “ABC0”, but these do not represent the same value.

7.2.2.3 Rule 2 – Omit All 0 Segments

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

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.

Rule 2 – Omit All 0 Segments

The second rule to help reduce the notation of IPv6 addresses is that a double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hexets) consisting of all 0s.

The double colon (::) can only be used once within an address, otherwise there would be more than one possible resulting address. When used with the omitting leading 0s technique, the notation of IPv6 address can often be greatly reduced. This is commonly known as the compressed format.

7.2.2.3 Rule 2 – Omit All 0 Segments

Preferred	FE80:0000:0000:0000:0123:4567:89AB:CDEF
No leading 0s	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compressed	FE80::123:4567:89AB:CDEF

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

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

7.2.2.3 Rule 2 – Omit All 0 Segments

Preferred	0000:0000:0000:0000:0000:0000:0000:0001
No leading 0s	0: 0: 0: 0: 0: 0: 0: 1
Compressed	::1

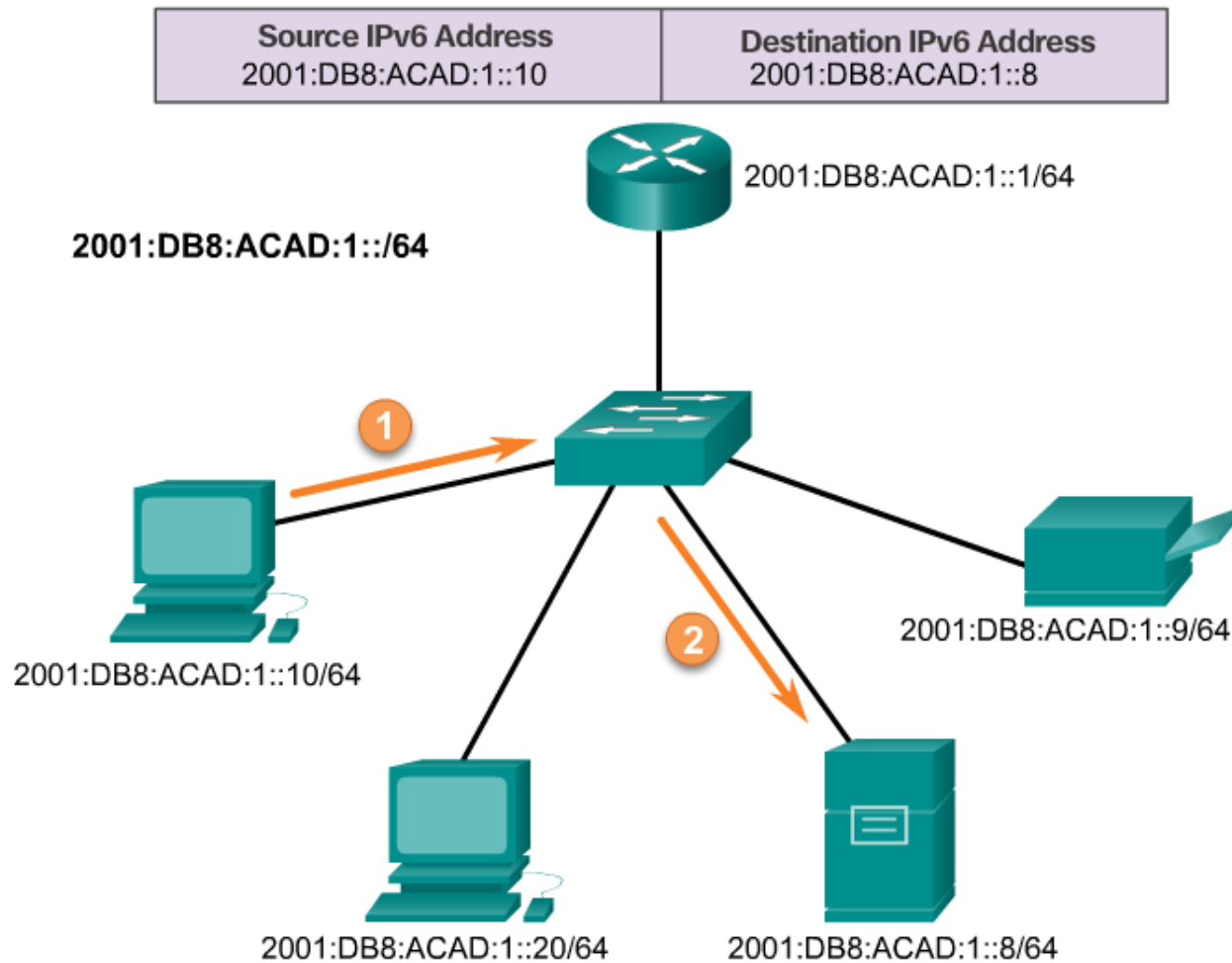
Preferred	0000:0000:0000:0000:0000:0000:0000:0000
No leading 0s	0: 0: 0: 0: 0: 0: 0: 0
Compressed	::

7.2.2.4 Activity – Practicing IPv6 Address Representations

IPv6 Conversion	
Preferred format	2001 : 0000 : 0DB8 : 1111 : 0000 : 0000 : 0000 : 0200
Omit leading zeroes	<div> <div>2001</div> <div>0</div> <div>DB8</div> <div>1111</div> <div>0</div> <div>0</div> <div>0</div> <div>200</div> </div> <div> <div>✓</div> <div>✓</div> <div>✓</div> <div>✓</div> <div>✓</div> <div>✓</div> <div>✓</div> <div>✓</div> </div>
Compressed format	<div>2001:0:DB8:1111::200</div> <div>✓</div>

7.2.3.1 IPv6 Address Types

IPv6 Unicast Communications



Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

IPv6 Address Types

There are three types of IPv6 addresses:

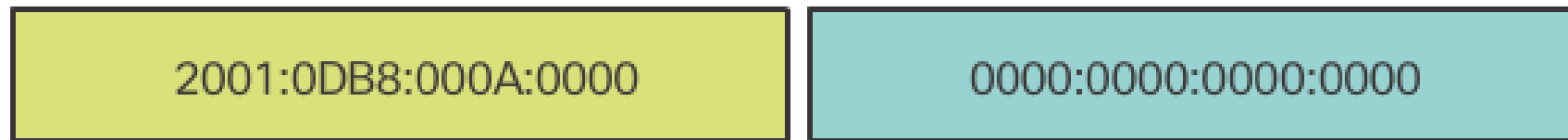
- **Unicast** - An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. As shown in the figure, a source IPv6 address must be a unicast address.
- **Multicast** - An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.
- **Anycast** - An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address. Anycast addresses are beyond the scope of this course.

7.2.3.2 IPv6 Prefix Length

/64 Prefix



Example: 2001:DB8:A::/64



IPv6 uses the prefix length to represent the prefix portion of the address. IPv6 does not use the dotted-decimal subnet mask notation. The prefix length is used to indicate the network portion of an IPv6 address using the IPv6 address/prefix length.

The prefix length can range from 0 to 128. A typical IPv6 prefix length for LANs and most other types of networks is /64. This means the prefix or network portion of the address is 64 bits in length, leaving another 64 bits for the interface ID (host portion) of the address.

7.2.3.3 IPv6 Unicast Addresses

IPv6 Unicast Addresses

An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. A packet sent to a unicast address is received by the interface that is assigned that address. Similar to IPv4, a source IPv6 address must be a unicast address. The destination IPv6 address can be either a unicast or a multicast address.

The most common types of IPv6 unicast addresses are global unicast addresses (GUA) and link-local unicast addresses.

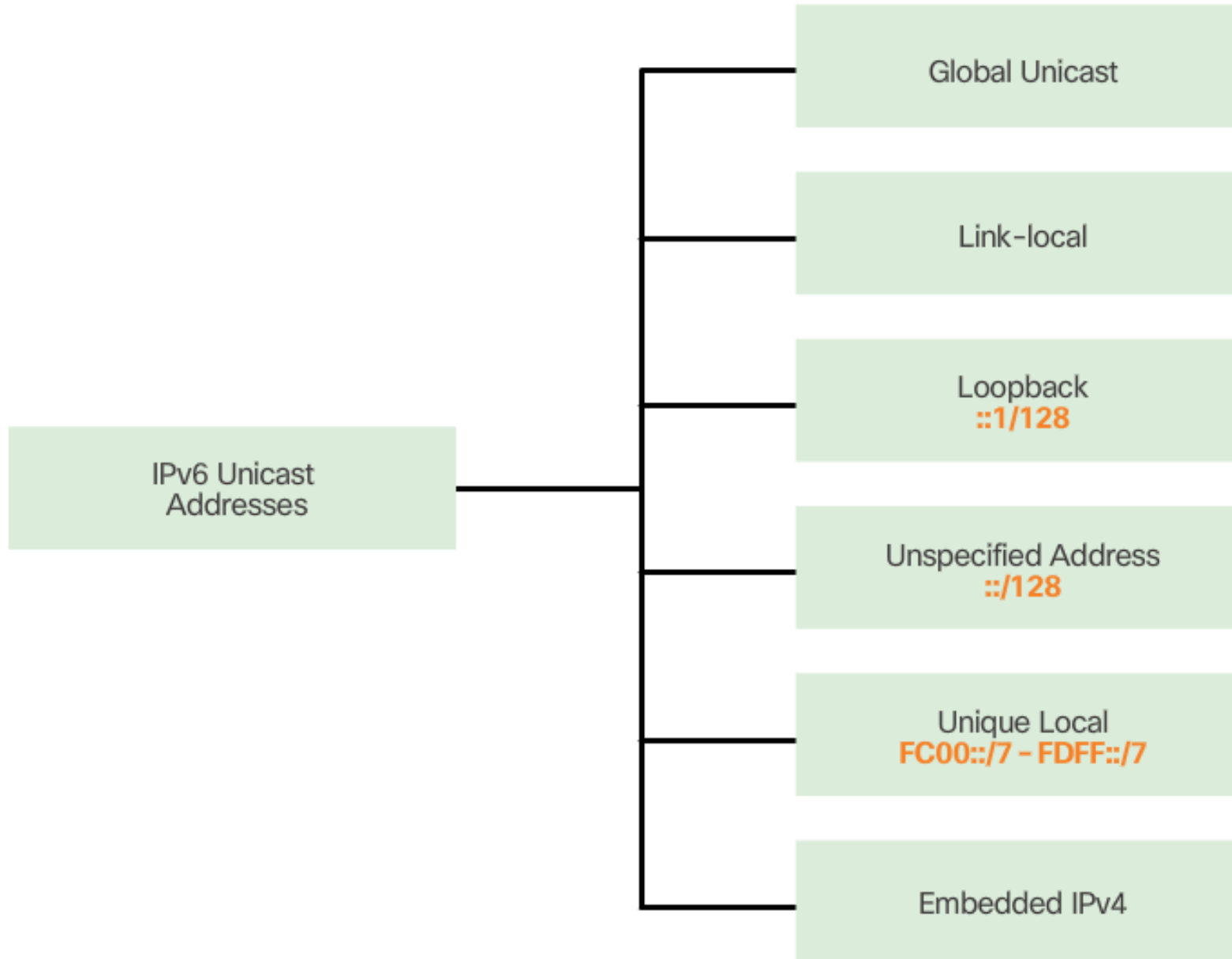
Global unicast

A global unicast address is similar to a public IPv4 address. These are globally unique, Internet routable addresses. Global unicast addresses can be configured statically or assigned dynamically.

Link-local

Link-local addresses are used to communicate with other devices on the same local link. **With IPv6, the term link refers to a subnet.** Link-local addresses are confined to a single link. Their uniqueness must only be confirmed on that link because they are not routable beyond the link. In other words, routers will not forward packets with a link-local source or destination address.

7.2.3.3 IPv6 Unicast Addresses



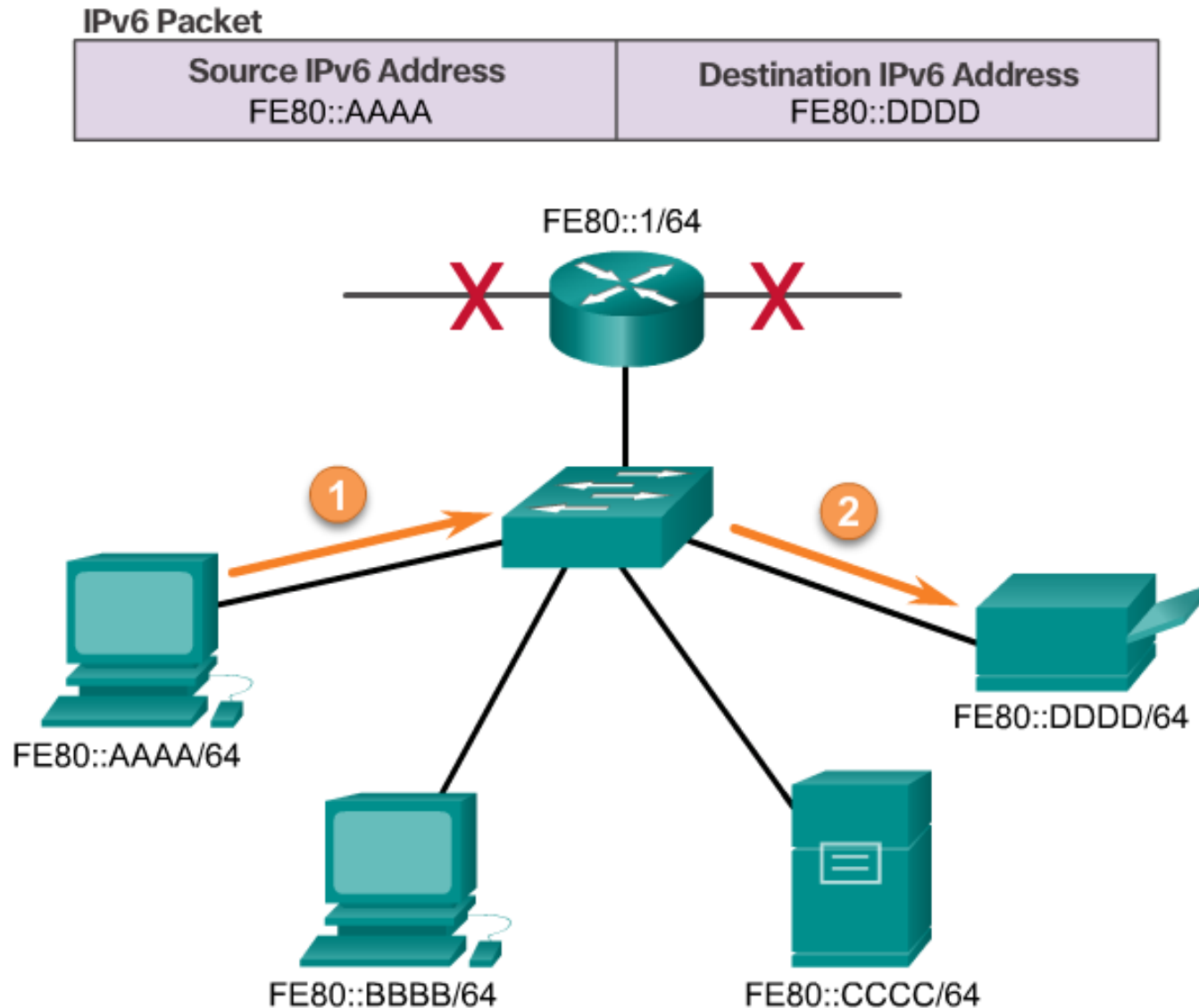
Unique local

Another type of unicast address is the unique local unicast address. IPv6 unique local addresses have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences.

Unique local addresses are used for local addressing within a site or between a limited number of sites. These addresses should not be routable in the global IPv6 and should not be translated to a global IPv6 address. Unique local addresses are in the range of FC00::/7 to FDFF::/7.

7.2.3.4 IPv6 Link-Local Unicast Addresses

IPv6 Link-Local Communications



An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination link-local address cannot be routed beyond the link from which the packet originated.

The global unicast address is not a requirement. However, every IPv6-enabled network interface is required to have a link-local address.

Figure 1 shows an example of communication using IPv6 link-local addresses.

7.2.3.4 IPv6 Link-Local Unicast Addresses

Uses of an IPv6 Link-Local Address

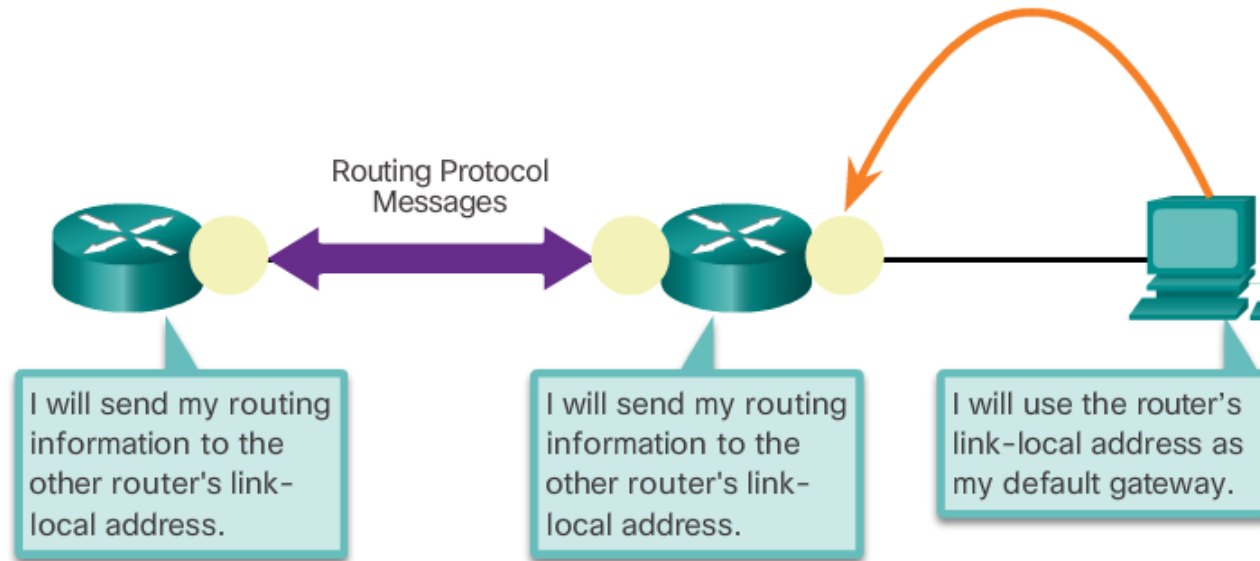


Figure 2 shows some of the uses for IPv6 link-local addresses.

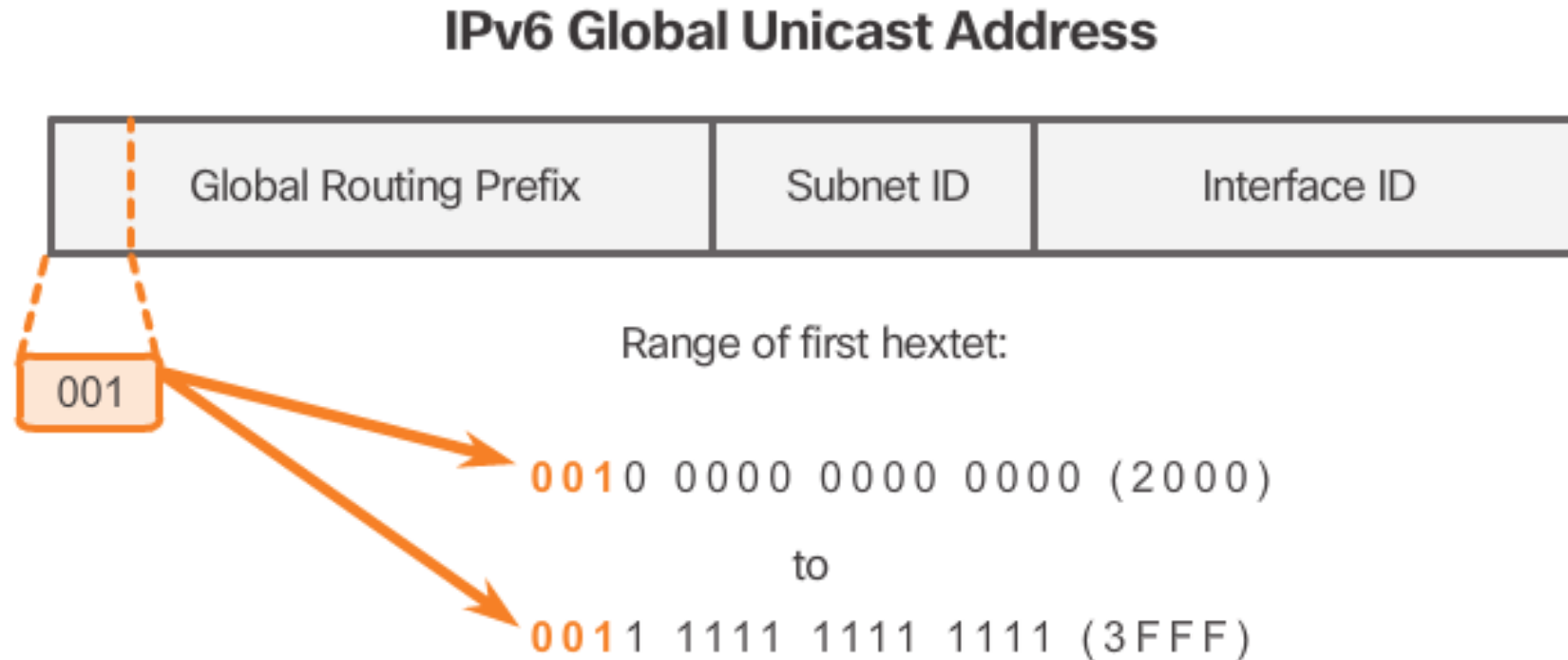
If a link-local address is not configured manually on an interface, the device will automatically create its own without communicating with a DHCP server. IPv6-enabled hosts create an IPv6 link-local address even if the device has not been assigned a global unicast IPv6 address. This allows IPv6-enabled devices to communicate with other IPv6-enabled devices on the same subnet. This includes communication with the default gateway (router).

IPv6 link-local addresses are in the FE80::/10 range. The /10 indicates that the first 10 bits are 1111 1110 10xx xxxx. The first hextet has a range of 1111 1110 1000 0000 (FE80) to 1111 1110 1011 1111 (FEBF).

7.2.3.5 Activity – Identify Types of IPv6 Addresses

✓	Global unicast	Unique, Internet-routable IPv6 address (dynamic or static)
✓	Link-local	FE80::1
✓	Global unicast	2001:db8:ACAD::1/64
✓	/64	Typical IPv6 prefix used to indicate the network portion of the address
✓	Link-local	Used to communicate with other devices on the same IPv6 subnet

7.2.4.1 Structure of an IPv6 Global Unicast Address



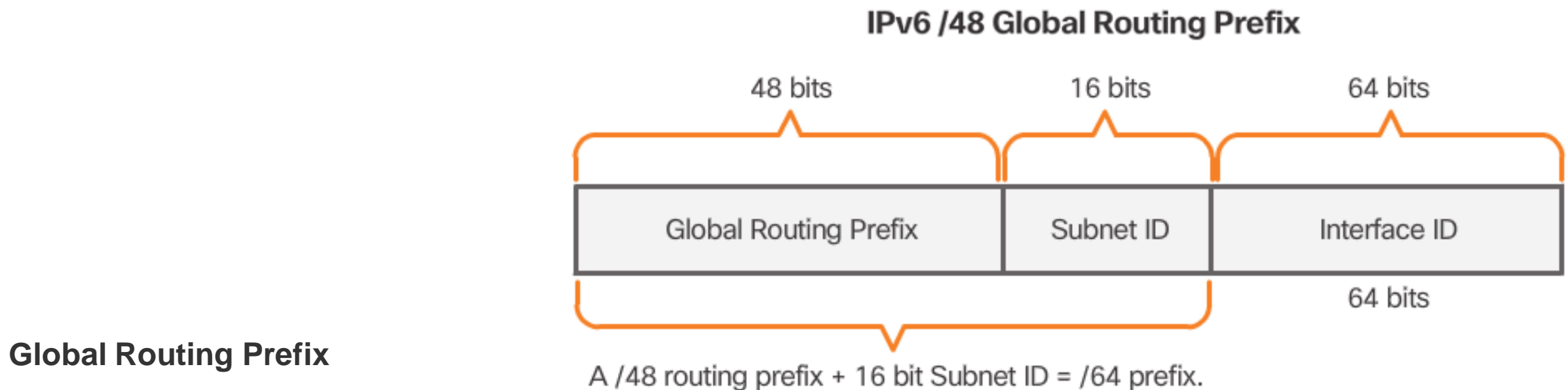
A global unicast address has three parts:

- Global routing prefix
- Subnet ID
- Interface ID

Structure of an IPv6 Global Unicast Address

IPv6 global unicast addresses are globally unique and routable on the IPv6 Internet. These addresses are equivalent to public IPv4 addresses. The Internet Committee for Assigned Names and Numbers (ICANN), the operator for IANA, allocates IPv6 address blocks to the five RIRs. Currently, only global unicast addresses with the first three bits of 001 or 2000:: are being assigned. This is only 1/8th of the total available IPv6 address space, excluding only a very small portion for other types of unicast and multicast addresses.

7.2.4.1 Structure of an IPv6 Global Unicast Address



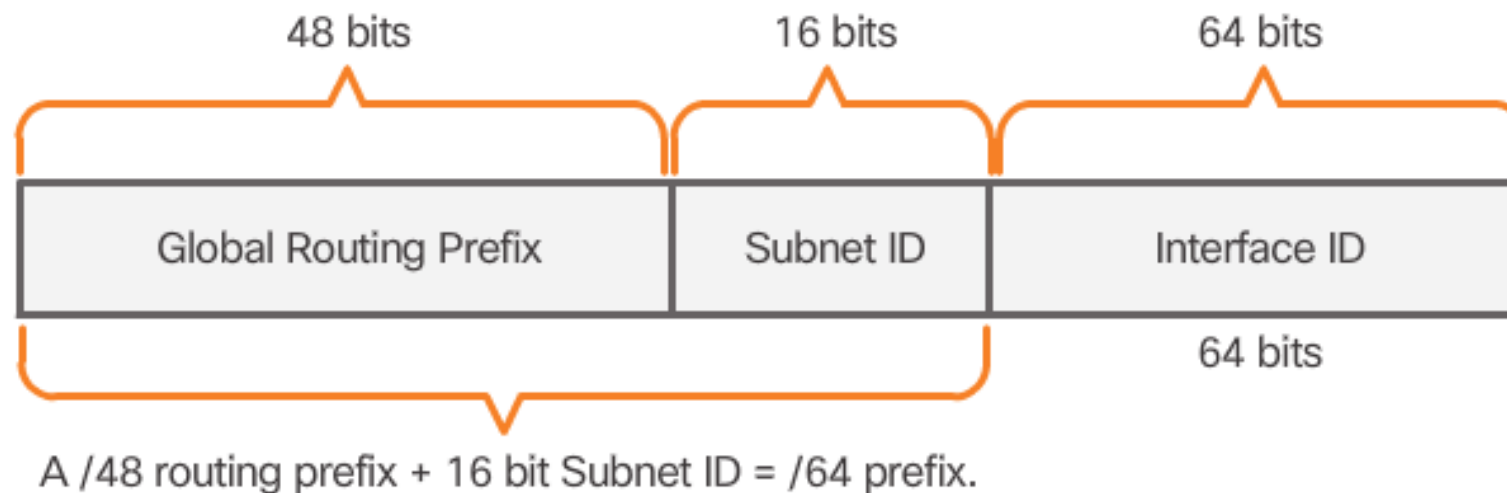
Global Routing Prefix

The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider, such as an ISP, to a customer or site. Typically, RIRs assign a /48 global routing prefix to customers. This can include everyone from enterprise business networks to individual households.

Figure 2 shows the structure of a global unicast address using a /48 global routing prefix. /48 prefixes are the most common global routing prefixes assigned and will be used in most of the examples throughout this course.

For example, the IPv6 address 2001:0DB8:ACAD::/48 has a prefix that indicates that the first 48 bits (3 hextets) (2001:0DB8:ACAD) is the prefix or network portion of the address. The double colon (::) prior to the /48 prefix length means the rest of the address contains all 0s.

7.2.4.1 Structure of an IPv6 Global Unicast Address



The size of the global routing prefix determines the size of the subnet ID.

Subnet ID

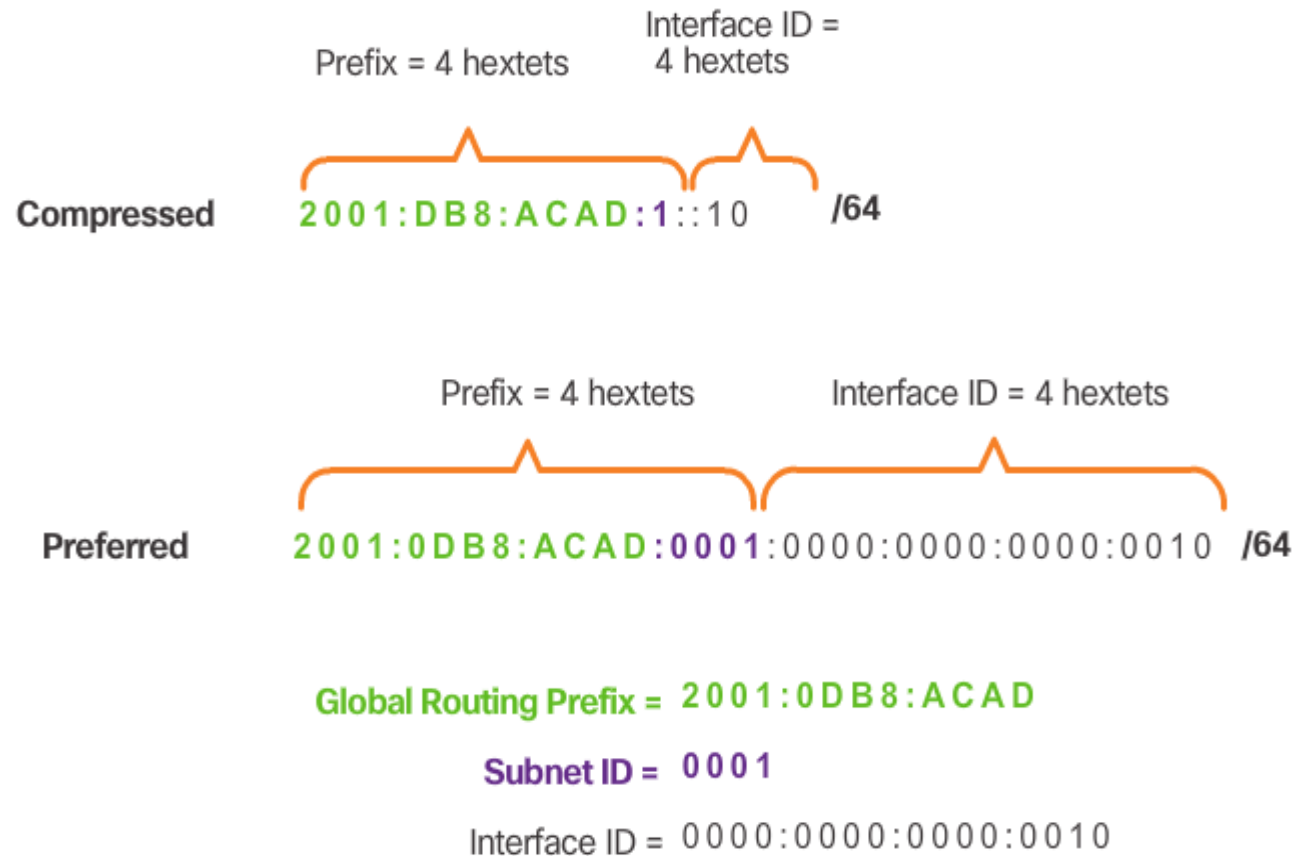
The Subnet ID is used by an organization to identify subnets within its site. The larger the subnet ID, the more subnets available.

Interface ID

The IPv6 Interface ID is equivalent to the host portion of an IPv4 address. The term Interface ID is used because a single host may have multiple interfaces, each having one or more IPv6 addresses. It is highly recommended that in most cases /64 subnets should be used. In other words a 64-bit interface ID as shown in Figure 2.

7.2.4.1 Structure of an IPv6 Global Unicast Address

Reading a Global Unicast Address

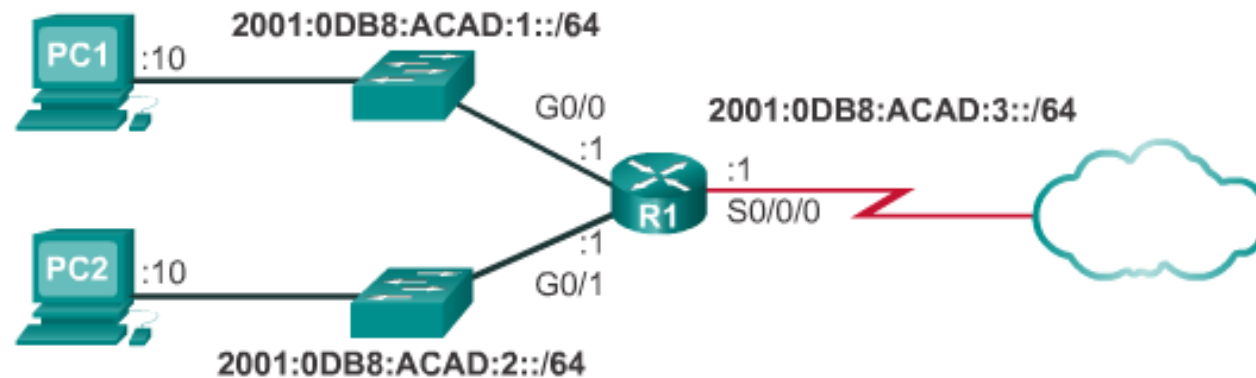


Note: Unlike IPv4, in IPv6, the all-0s and all-1s host addresses can be assigned to a device. The all-1s address can be used due to the fact that broadcast addresses are not used within IPv6. The all-0s address can also be used, but is reserved as a Subnet-Router anycast address, and should be assigned only to routers.

An easy way to read most IPv6 addresses is to count the number of hexets. As shown in Figure 3, in a /64 global unicast address the first four hexets are for the network portion of the address, with the fourth hexet indicating the Subnet ID. The remaining four hexets are for the Interface ID.

7.2.4.2 Static Configuration of a Global Unicast Address

Configuring IPv6 on a Router



```
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
```

Router Configuration

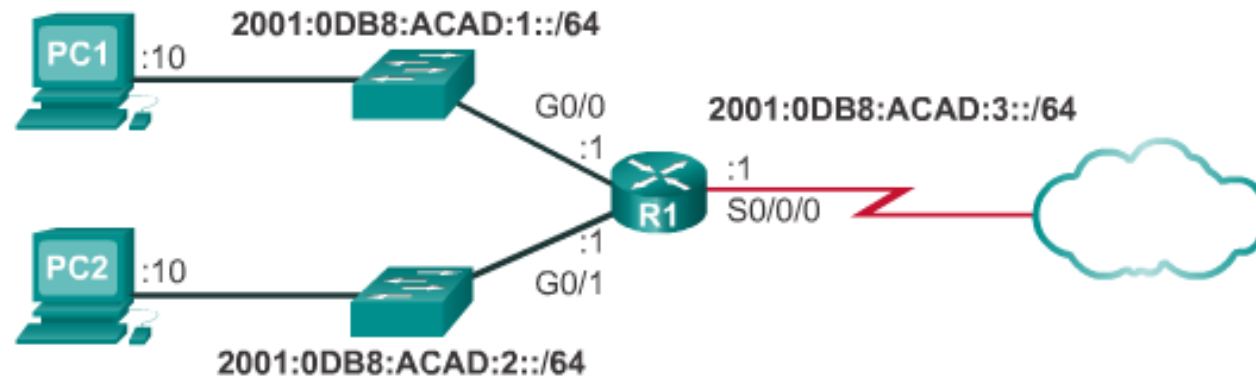
Most IPv6 configuration and verification commands in the Cisco IOS are similar to their IPv4 counterparts. In many cases, the only difference is the use of **ipv6** in place of **ip** within the commands.

The command to configure an IPv6 global unicast address on an interface is **ipv6 address ipv6-address/prefix-length**.

Notice that there is not a space between *ipv6-address* and *prefix-length*.

7.2.4.2 Static Configuration of a Global Unicast Address

Configuring IPv6 on a Router



```
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
```

The example configuration uses the topology shown in Figure 1 and these IPv6 subnets:

- 2001:0DB8:ACAD:0001:/64 (or 2001:DB8:ACAD:1::/64)
- 2001:0DB8:ACAD:0002:/64 (or 2001:DB8:ACAD:2::/64)
- 2001:0DB8:ACAD:0003:/64 (or 2001:DB8:ACAD:3::/64)

Figure 1 also shows the commands required to configure the IPv6 global unicast address on the GigabitEthernet 0/0, GigabitEthernet 0/1, and Serial 0/0/0 interface of R1.

7.2.4.2 Static Configuration of a Global Unicast Address

Host Configuration

Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address.

As shown in Figure 2, the default gateway address configured for PC1 is 2001:DB8:ACAD:1::1. This is the global unicast address of the R1 GigabitEthernet interface on the same network. Alternatively, the default gateway address can be configured to match the link-local address of the GigabitEthernet interface. Either configuration will work.

Use the Syntax Checker in Figure 3 to configure the IPv6 global unicast address.

Just as with IPv4, configuring static addresses on clients does not scale to larger environments. For this reason, most network administrators in an IPv6 network will enable dynamic assignment of IPv6 addresses.

There are two ways in which a device can obtain an IPv6 global unicast address automatically:

- Stateless Address Autoconfiguration (SLAAC)
- DHCPv6

Note: When DHCPv6 or SLAAC is used, the local router's link-local address will automatically be specified as the default gateway address.

7.2.4.2 Static Configuration of a Global Unicast Address

The image shows a Windows XP-style dialog box titled "Internet Protocol Version 6 (TCP/IPv6) Properties". It has a "General" tab selected. The dialog contains instructions about automatic vs. manual configuration. Under the "Use the following IPv6 address:" section, the "IPv6 address" field is set to "2001:db8:acad:1::10", the "Subnet prefix length" is "64", and the "Default gateway" is "2001:db8:acad:1::1". The "Obtain DNS server address automatically" option is disabled. Under the "Use the following DNS server addresses:" section, the "Preferred DNS server" and "Alternate DNS server" fields are empty. At the bottom, there is a checkbox for "Validate settings upon exit" which is unchecked, an "Advanced..." button, and "OK" and "Cancel" buttons.

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address: 2001:db8:acad:1::10

Subnet prefix length: 64

Default gateway: 2001:db8:acad:1::1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

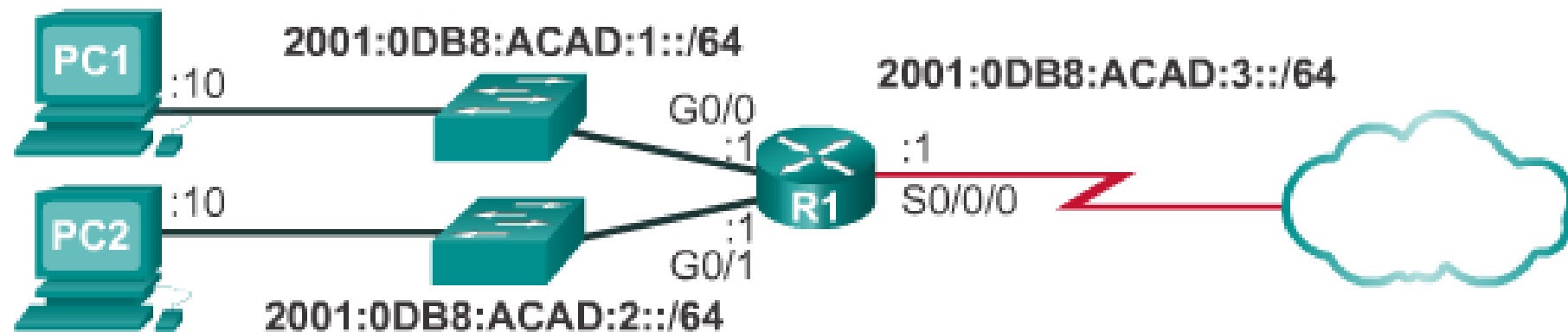
Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

7.2.4.2 Static Configuration of a Global Unicast Address

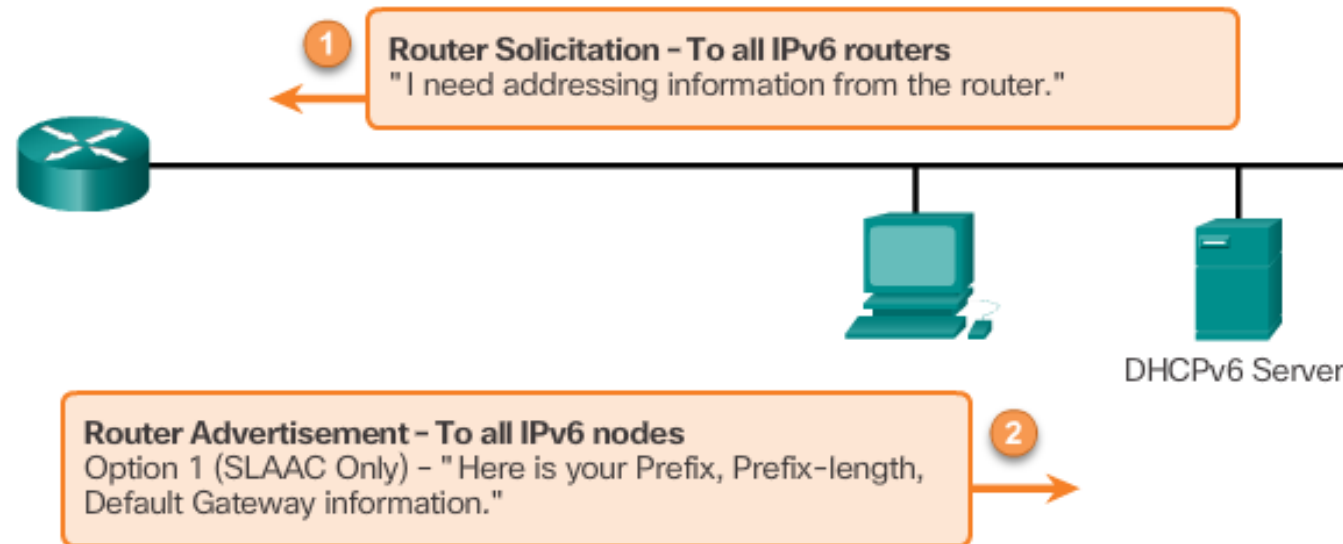


Configure and activate the following interfaces:

- GigabitEthernet 0/0 - 2001:db8:acad:1::1/64
- GigabitEthernet 0/1 - 2001:db8:acad:2::1/64
- Serial 0/0/0 - 2001:db8:acad:3::1/64

```
R1 (config) #
```

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 information."

Dynamic Configuration - SLAAC

Stateless Address Autoconfiguration (SLAAC) is a method that allows a device to obtain its prefix, prefix length, default gateway address, and other information from an *IPv6 router* without the use of a DHCPv6 server. Using SLAAC, devices rely on the local router's ICMPv6 Router Advertisement (RA) messages to obtain the necessary information.

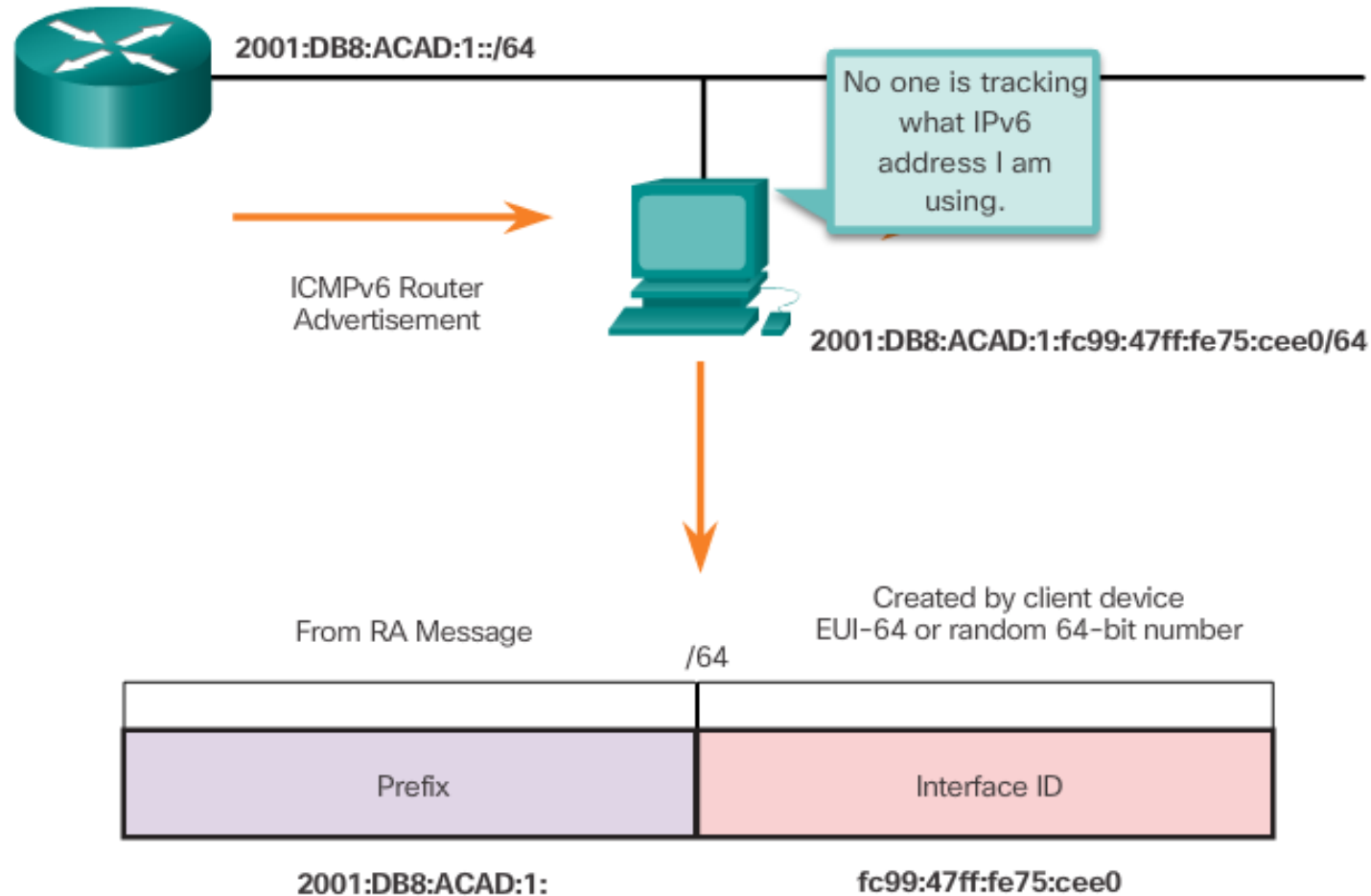
IPv6 routers periodically send out ICMPv6 RA messages, every 200 seconds, to all IPv6-enabled devices on the network. An RA message will also be sent in response to a host sending an ICMPv6 Router Solicitation (RS) message.

IPv6 routing is not enabled by default. To enable a router as an IPv6 router, the **ipv6 unicast-routing** global configuration command must be used.

Note: IPv6 addresses can be configured on a router without it being an IPv6 router.

7.2.4.3 Dynamic Configuration - SLAAC

Global Unicast Address and SLAAC



7.2.4.3 Dynamic Configuration - SLAAC

The ICMPv6 RA message is a suggestion to a device on how to obtain an IPv6 global unicast address. The ultimate decision is up to the device's operating system. The ICMPv6 RA message includes:

- **Network prefix and prefix length** – Tells the device which network it belongs to.
- **Default gateway address** – This is an IPv6 link-local address, the source IPv6 address of the RA message.
- **DNS addresses and domain name** – Addresses of DNS servers and a domain name.

As shown in Figure 1, there are three options for RA messages:

- Option 1: SLAAC
- Option 2: SLAAC with a stateless DHCPv6 server
- Option 3: Stateful DHCPv6 (no SLAAC)

RA Option 1: SLAAC

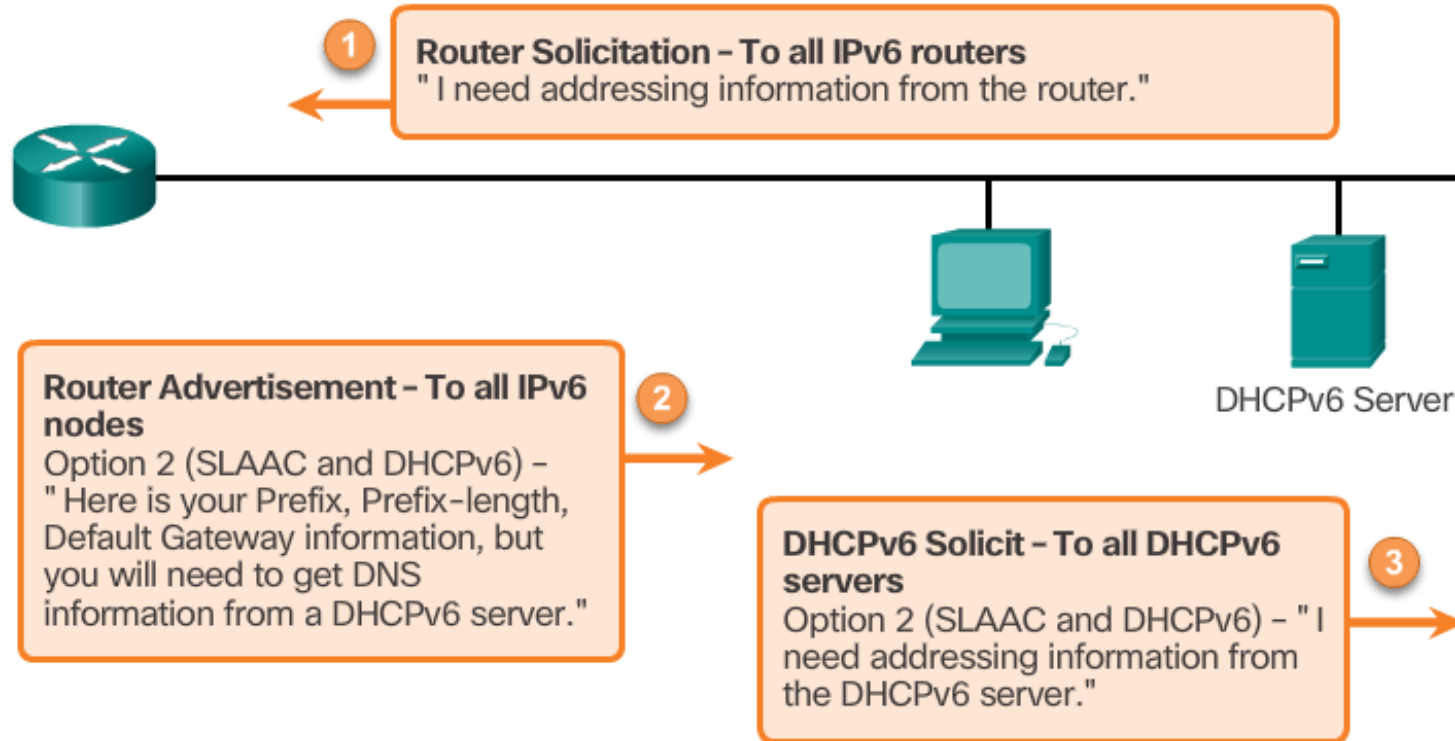
By default, the RA message suggests that the receiving device use the information in the RA message to create its own IPv6 global unicast address and for all other information. The services of a DHCPv6 server are not required.

SLAAC is stateless, which means there is no central server (for example, a stateful DHCPv6 server) allocating global unicast addresses and keeping a list of devices and their addresses. With SLAAC, the client device uses the information in the RA message to create its own global unicast address. As shown in Figure 2, the two parts of the address are created as follows:

- **Prefix** – Received in the RA message
- **Interface ID** – Uses the EUI-64 process or by generating a random 64-bit number

7.2.4.4 Dynamic Configuration – DHCPv6

Router Solicitation and Router Advertisement Messages

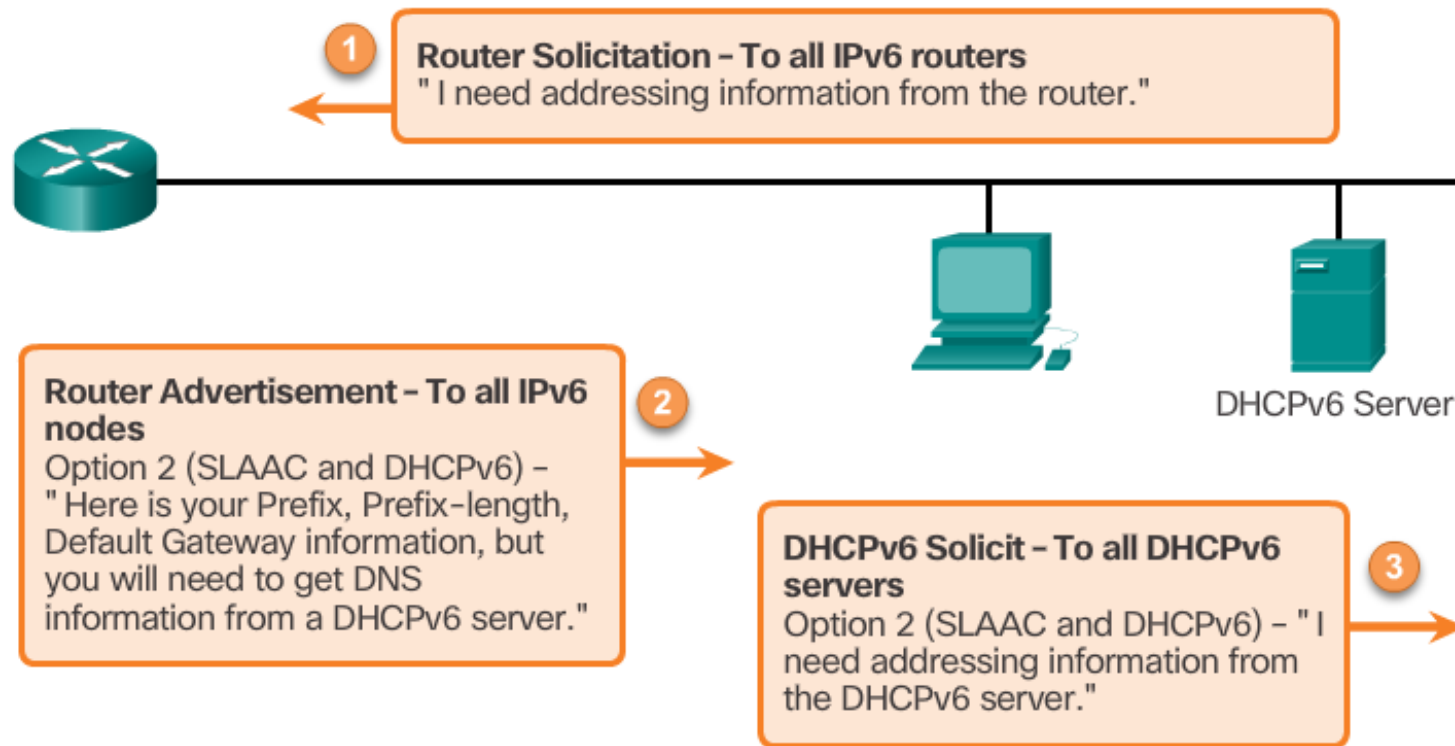


Dynamic Configuration – DHCPv6

By default, the RA message is option 1, SLAAC only. The router's interface can be configured to send a router advertisement using SLAAC and stateless DHCPv6, or stateful DHCPv6 only.

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.

7.2.4.4 Dynamic Configuration – DHCPv6



RA Option 2: SLAAC and Stateless DHCPv6

With this option, the RA message suggests devices use:

- SLAAC to create its own IPv6 global unicast address
- The router's link-local address, the RA's source IPv6 address for the default gateway address.
- A stateless DHCPv6 server to obtain other information such as a DNS server address and a domain name..

A stateless DHCPv6 server distributes DNS server addresses and domain names. It does not allocate global unicast addresses

RA Option 3: Stateful DHCPv6

Stateful DHCPv6 is similar to DHCP for IPv4. A device can automatically receive its addressing information including a global unicast address, prefix length, and the addresses of DNS servers using the services of a stateful DHCPv6 server.

With this option the RA message suggests devices use:

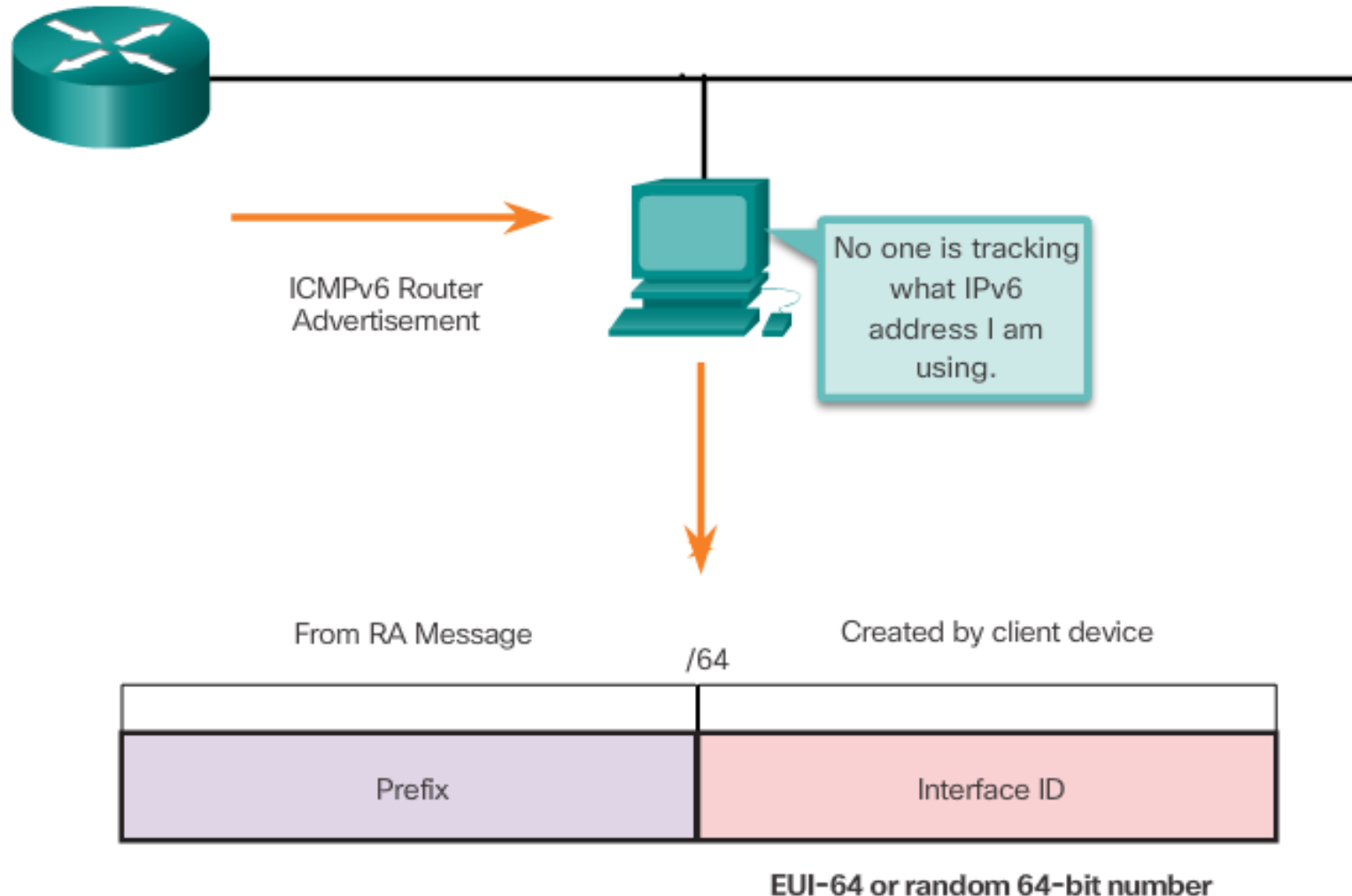
- The router's link-local address, the RA's source IPv6 address for the default gateway address.
- A stateful DHCPv6 server to obtain a global unicast address, DNS server address, domain name and all other information.

A stateful DHCPv6 server allocates and maintains a list of which device receives which IPv6 address. DHCP for IPv4 is stateful.

Note: The default gateway address can only be obtained dynamically from the RA message. The stateless or stateful DHCPv6 server does not provide the default gateway address.

7.2.4.5 EUI-64 Process and Randomly Generated

EUI-64 Process



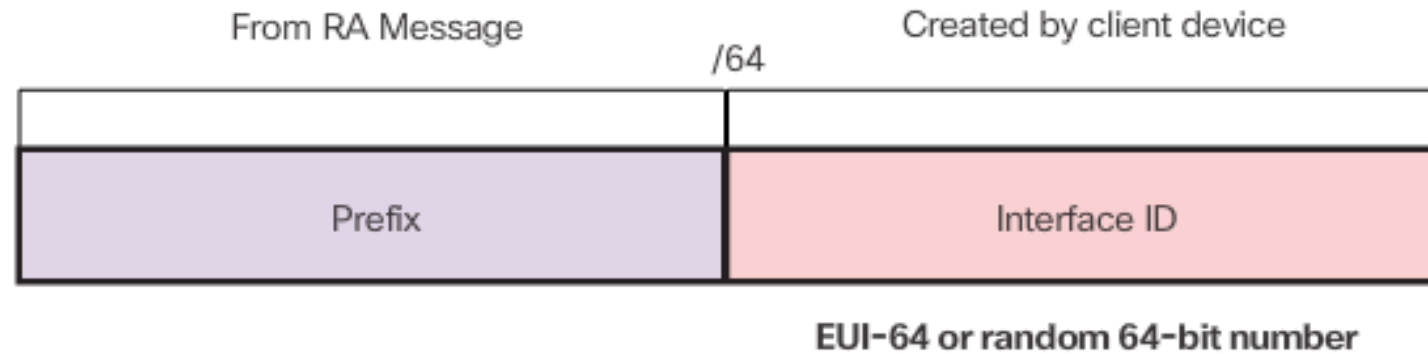
EUI-64 Process and Randomly Generated

When the RA message is either SLAAC or SLAAC with stateless DHCPv6, the client must generate its own Interface ID.

The client knows the prefix portion of the address from the RA message but must create its own Interface ID.

The Interface ID can be created using the EUI-64 process or a randomly generated 64-bit number, as shown in Figure 1.

7.2.4.5 EUI-64 Process and Randomly Generated



EUI-64 Process

IEEE defined the Extended Unique Identifier (EUI) or modified EUI-64 process. This process uses a client's 48-bit Ethernet MAC address, and inserts another 16 bits in the middle of the 48-bit MAC address to create a 64-bit Interface ID.

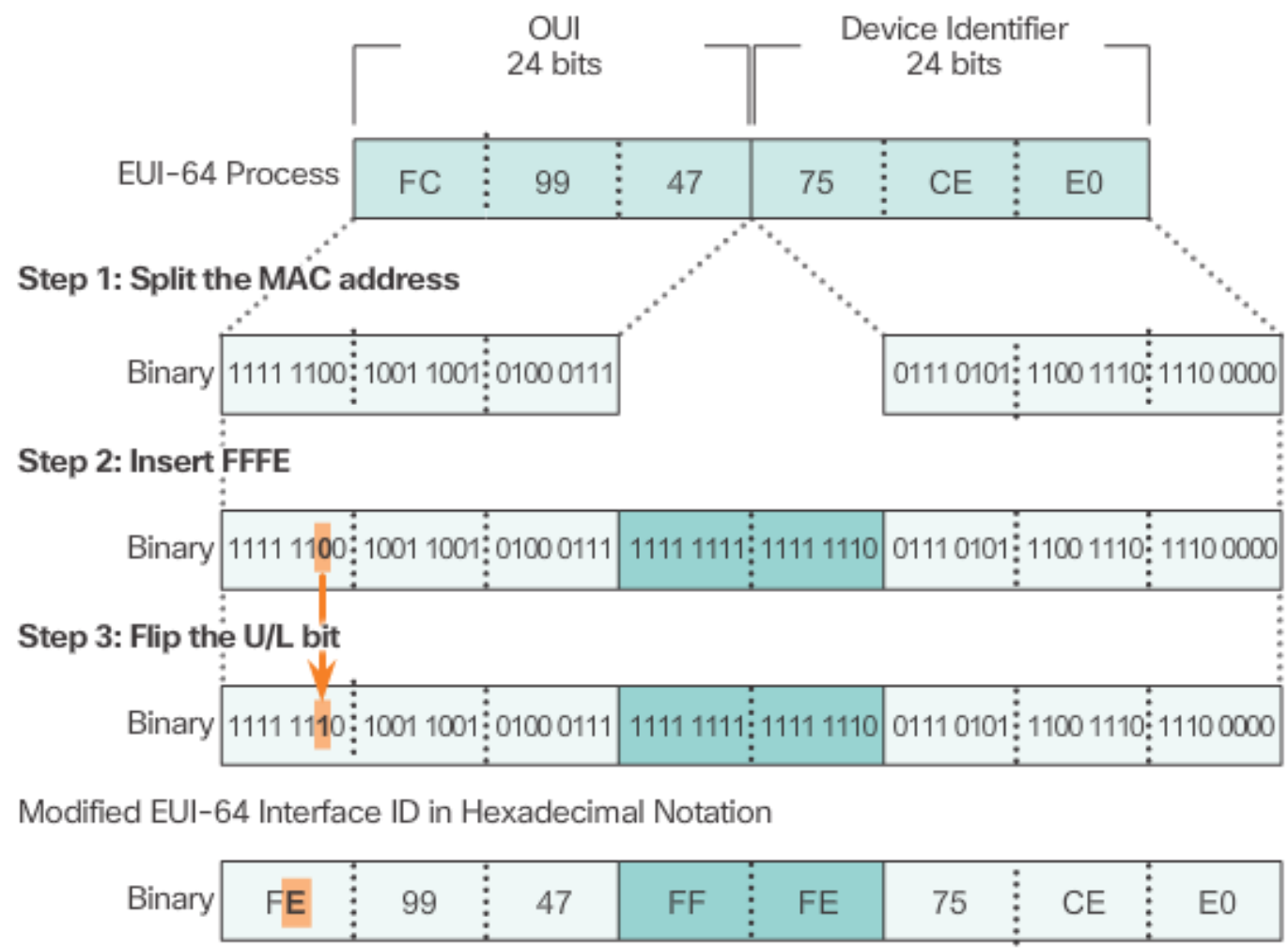
Ethernet MAC addresses are usually represented in hexadecimal and are made up of two parts:

- **Organizationally Unique Identifier (OUI)** – **Device Identifier** –

An EUI-64 Interface ID is represented in binary and is made up of three parts:

- 24-bit OUI from the client MAC address, but the 7th bit (the Universally/Locally (U/L) bit) is reversed. This means that if the 7th bit is a 0, it becomes a 1, and vice versa.
- The inserted 16-bit value FFFE (in hexadecimal)
- 24-bit Device Identifier from the client MAC address

EUI-64 Process



The EUI-64 process is using R1's GigabitEthernet MAC address of FC99:4775:CEE0.

Step 1: Divide the MAC address between the OUI and device identifier.

Step 2: Insert the hexadecimal value FFFE, which in binary is: 1111 1111 1111 1110.

Step 3: Convert the first 2 hexadecimal values of the OUI to binary and flip the U/L bit (bit 7). In this example, the 0 in bit 7 is changed to a 1.

The result is an EUI-64 generated Interface ID of FE99:47FF:FE75:CEE0.

Note: The use of the U/L bit, and the reasons for reversing its value, are discussed in RFC 5342.

7.2.4.5 EUI-64 Process and Randomly Generated

```
PCA> ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

**From RA
Message**

EUI-64 generated

```
Connection-specific DNS Suffix  : 
IPv6 Address. . . . . : 2001:db8:acad:1:fc99:47ff:Ffe75:cee0
Link-local IPv6 Address . . . . : fe80::fc99:47FF:FE75:CEE0
Default Gateway . . . . . : fe80::1
```

Figure 3 shows PCA's IPv6 global unicast address dynamically created using SLAAC and the EUI-64 process. An easy way to identify that an address was more than likely created using EUI-64 is the FFFE located in the middle of the Interface ID, as shown in Figure 3.

The advantage of EUI-64 is the Ethernet MAC address can be used to determine the Interface ID. It also allows network administrators to easily track an IPv6 address to an end-device using the unique MAC address. However, this has caused privacy concerns among many users. They are concerned that their packets can be traced to the actual physical computer. Due to these concerns, a randomly generated Interface ID may be used instead.

7.2.4.5 EUI-64 Process and Randomly Generated

```
PCB> ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

From RA
Message

Random 64-bit
number

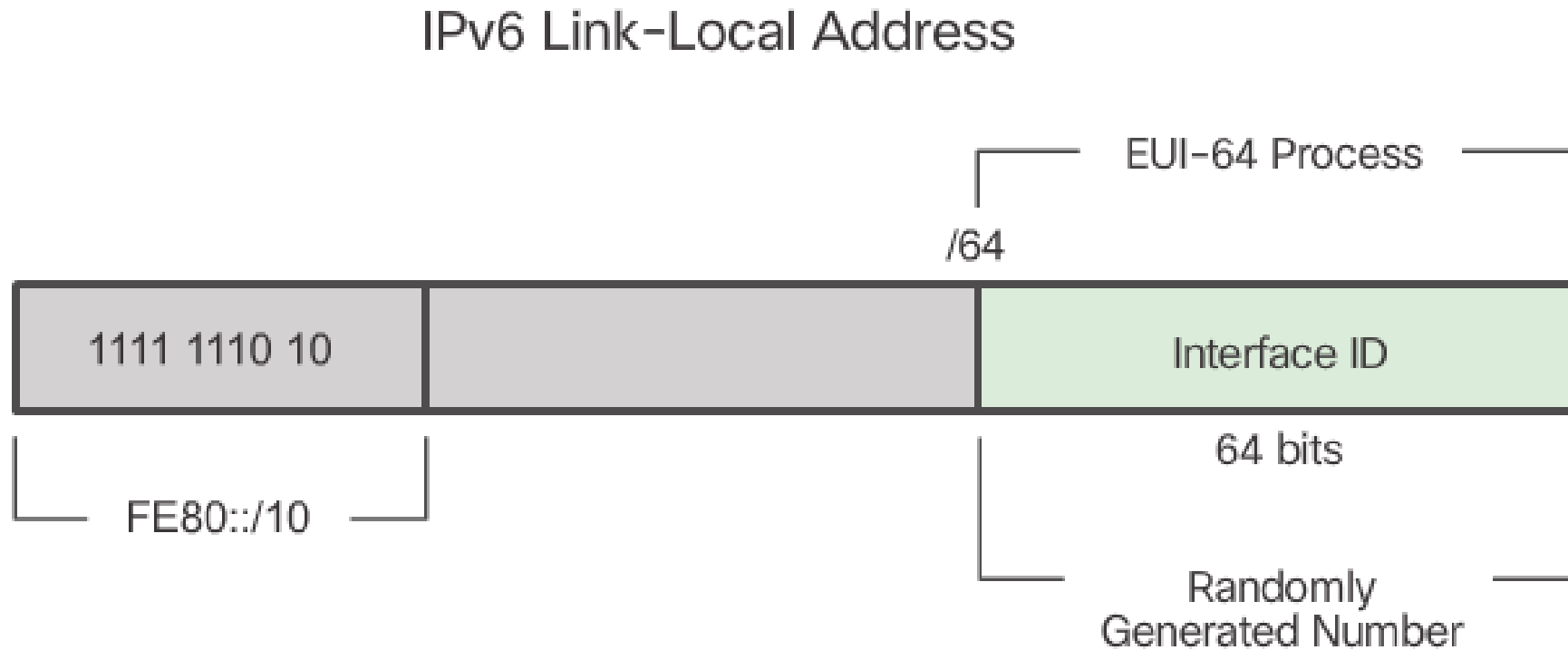
```
Connection-specific DNS Suffix  : 
IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . : fe80::1
```

Randomly Generated Interface IDs

Depending upon the operating system, a device may use a randomly generated Interface ID instead of using the MAC address and the EUI-64 process. For example, beginning with Windows Vista, Windows uses a randomly generated Interface ID instead of one created with EUI-64. Windows XP and previous Windows operating systems used EUI-64.

After the Interface ID is established, either through the EUI-64 process or through random generation, it can be combined with an IPv6 prefix in the RA message to create a global unicast address, as shown in Figure 4.

To ensure the uniqueness of any IPv6 unicast address, the client may use a process known as Duplicate Address Detection (DAD)



Dynamic Link-Local Addresses

All IPv6 devices must have an IPv6 link-local address. A link-local address can be established dynamically or configured manually as a static link-local address.

Figure 1 shows the link-local address is dynamically created using the FE80::/10 prefix and the Interface ID using the EUI-64 process or a randomly generated 64-bit number

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
```

Operating systems will typically use the same method for both a SLAAC created global unicast address and a dynamically assigned link-local address, as shown in Figure 2.

Cisco routers automatically create an IPv6 link-local address whenever a global unicast address is assigned to the interface. By default, Cisco IOS routers use EUI-64 to generate the Interface ID for all link-local address on IPv6 interfaces. For serial interfaces, the router will use the MAC address of an Ethernet interface. Recall that a link-local address must be unique only on that link or network. However, a drawback to using the dynamically assigned link-local address is its length, which makes it challenging to identify and remember assigned addresses

7.2.4.6 Dynamic Link-Local Addresses

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#
```

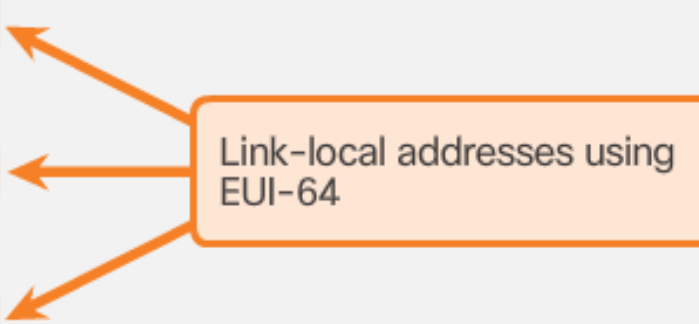


Figure 3 displays the MAC address on router R1's GigabitEthernet 0/0 interface. This address is used to dynamically create the link-local address on the same interface.

To make it easier to recognize and remember these addresses on routers, it is common to statically configure IPv6 link-local addresses on routers.

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) #
```

Static Link-Local Addresses

Configuring the link-local address manually provides the ability to create an address that is recognizable and easier to remember.

Link-local addresses can be configured manually using the same interface command used to create IPv6 global unicast addresses but with the additional **link-local** parameter. When an address begins with this hextet within the range of FE80 to FEBF, the link-local parameter must follow the address.

Configuring Link-local Addresses on R1

```
Router(config-if) #
```

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

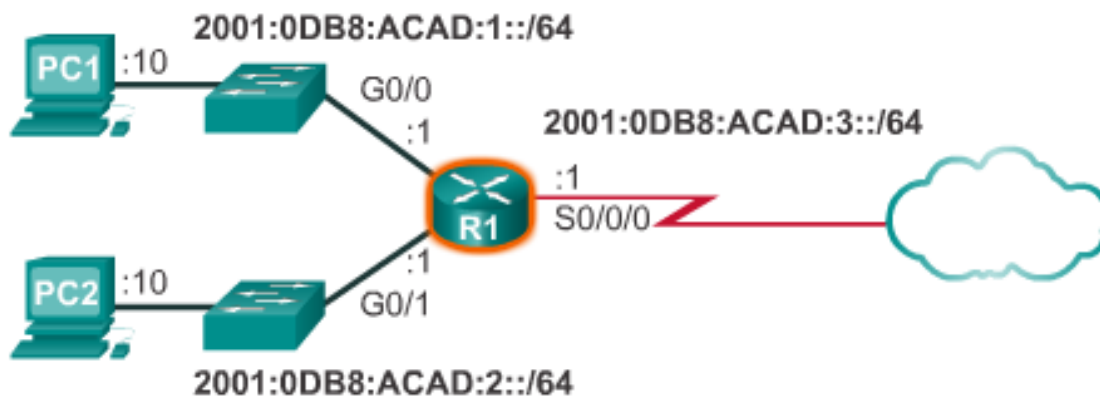
```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
    link-local    Use link-local address

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)#
```

The figure shows the configuration of a link-local address using the **ipv6 address** interface command. The link-local address FE80::1 is used to make it easily recognizable as belonging to router R1. The same IPv6 link-local address is configured on all of R1's interfaces. FE80::1 can be configured on each link because it only has to be unique on that link.

Similar to R1, router R2 would be configured with FE80::2 as the IPv6 link-local address on all of its interfaces.

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#
```

Verifying IPv6 Address Configuration

The **show interface** command displays the MAC address of the Ethernet interfaces. EUI-64 uses this MAC address to generate the Interface ID for the link-local address. Additionally, the **show ipv6 interface brief** command displays abbreviated output for each of the interfaces. The **[up/up]** output on the same line as the interface indicates the Layer 1/Layer 2 interface state. This is the same as the **Status** and **Protocol** columns in the equivalent IPv4 command.

Notice that each interface has two IPv6 addresses. The second address for each interface is the global unicast address that was configured. The first address, the one that begins with FE80, is the link-local unicast address for the interface.

7.2.4.8 Verifying IPv6 Address Configuration

```
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#
```

As shown in Figure 2, the **show ipv6 route** command can be used to verify that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table. The **show ipv6 route** command will only display IPv6 networks, not IPv4 networks.

Within the route table, a **C** next to a route indicates that this is a directly connected network. When the router interface is configured with a global unicast address and is in the “up/up” state, the IPv6 prefix and prefix length is added to the IPv6 routing table as a connected route.

The IPv6 global unicast address configured on the interface is also installed in the routing table as a local route. The local route has a /128 prefix. Local routes are used by the routing table to efficiently process packets with a destination address of the router’s interface address.

7.2.4.8 Verifying IPv6 Address Configuration

```
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#
```

Verifying IPv6 Address Configuration

```
Enter the show command that will display a brief summary of the IPv6 interface status.
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
Enter the show command that will display the IPv6 routing table.
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, a - Application
```

The **ping** command for IPv6 is identical to the command used with IPv4, except that an IPv6 address is used. As shown in Figure 3, the command is used to verify Layer 3 connectivity between R1 and PC1. When pinging a link-local address from a router, Cisco IOS will prompt the user for the exit interface. Because the destination link-local address can be on one or more of its links or networks, the router needs to know which interface to send the ping to.

Use the Syntax Checker in Figure 4 to verify IPv6 address configuration.

7.2.4.9 Packet Tracer – Configuring IPv6 Addressing

Cisco Networking Academy®
Mind Wide Open™

Cisco Packet Tracer

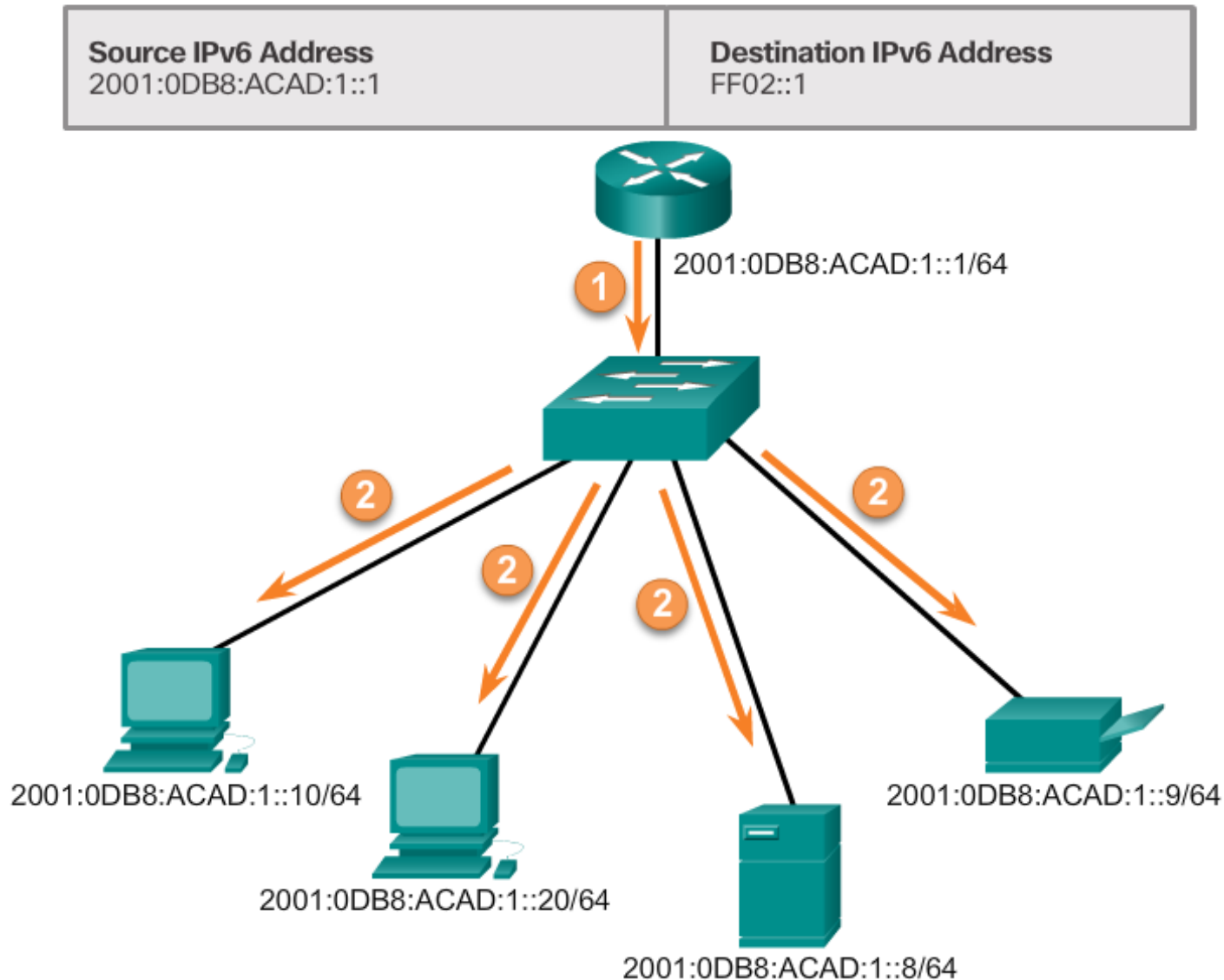
Packet Tracer | Configuring IPv6 Addressing



The image displays the Cisco Packet Tracer interface. The top section features the Cisco Networking Academy logo and the title 'Cisco Packet Tracer'. Below this is a banner with a grid of small icons and a magnifying glass icon. The main area is divided into two panels. The left panel shows a video of two students, a woman and a man, looking at a computer screen. The right panel displays a network diagram. The diagram shows a central switch labeled 'SW-A' with IP address '192.168.1.24'. It is connected to five PCs labeled 'PC-PT C1', 'PC-PT C2', 'PC-PT C3', 'PC-PT C4', and 'PC-PT D1'. The background of the right panel is a blue globe with binary code and network lines.

7.2.5.1 Assigned IPv6 Multicast Addresses

IPv6 All-Nodes Multicast Communications



Assigned IPv6 Multicast Addresses

IPv6 multicast addresses are similar to IPv4 multicast addresses. Recall that a multicast address is used to send a single packet to one or more destinations (multicast group). IPv6 multicast addresses have the prefix FF00::/8.

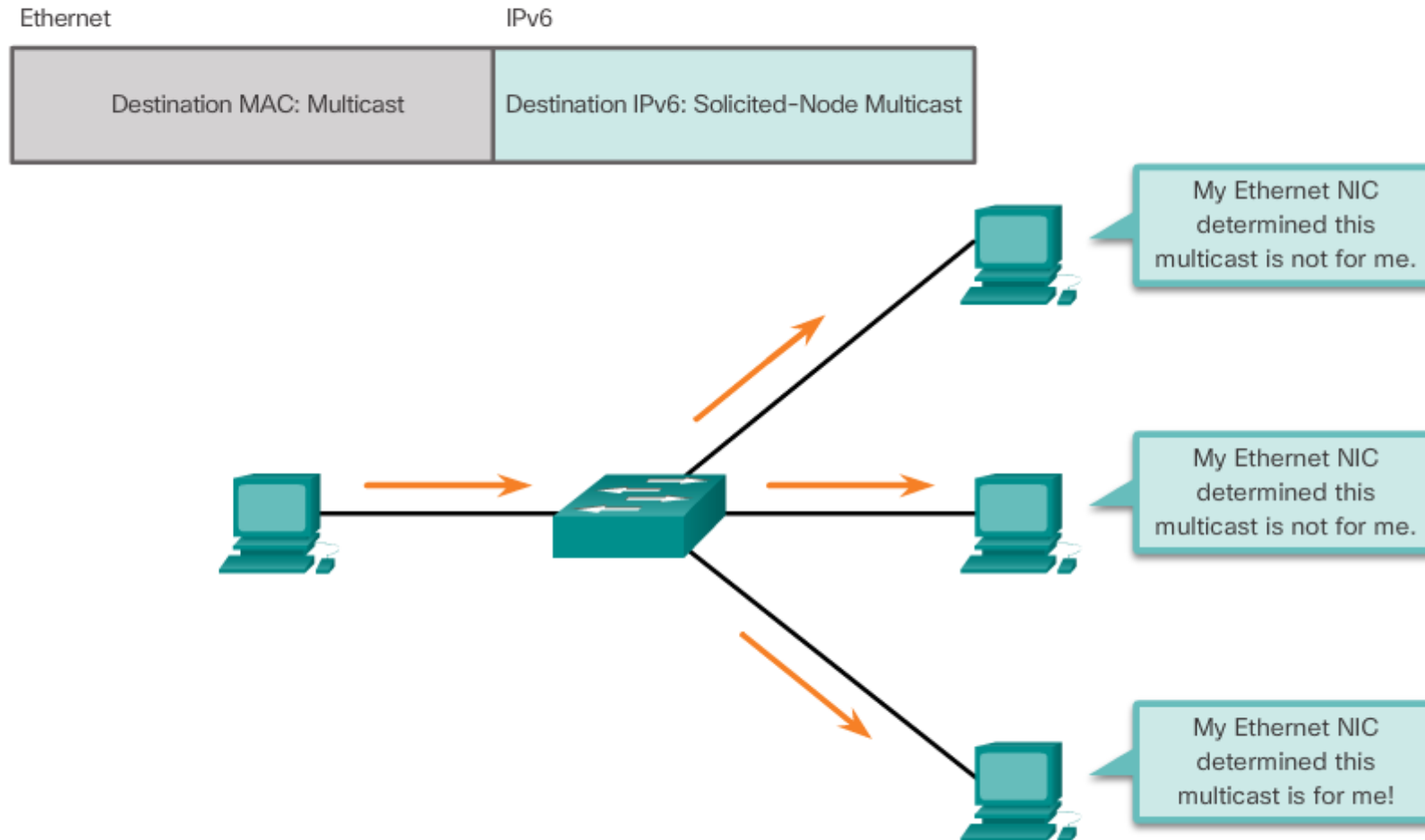
Note: Multicast addresses can only be destination addresses and not source addresses.

There are two types of IPv6 multicast addresses:

- Assigned multicast
- Solicited node multicast

7.2.5.2 Solicited-Node IPv6 Multicast Addresses

IPv6 Solicited-Node Multicast Address



Solicited-Node IPv6 Multicast Addresses

A solicited-node multicast address is similar to the all-nodes multicast address. The advantage of a solicited-node multicast address is that it is mapped to a special Ethernet multicast address. This allows the Ethernet NIC to filter the frame by examining the destination MAC address without sending it to the IPv6 process to see if the device is the intended target of the IPv6 packet.

Refer to the Chapter Appendix for more information on the solicited-node multicast address.

7.2.5.3 Lab – Identifying IPv6 Addresses

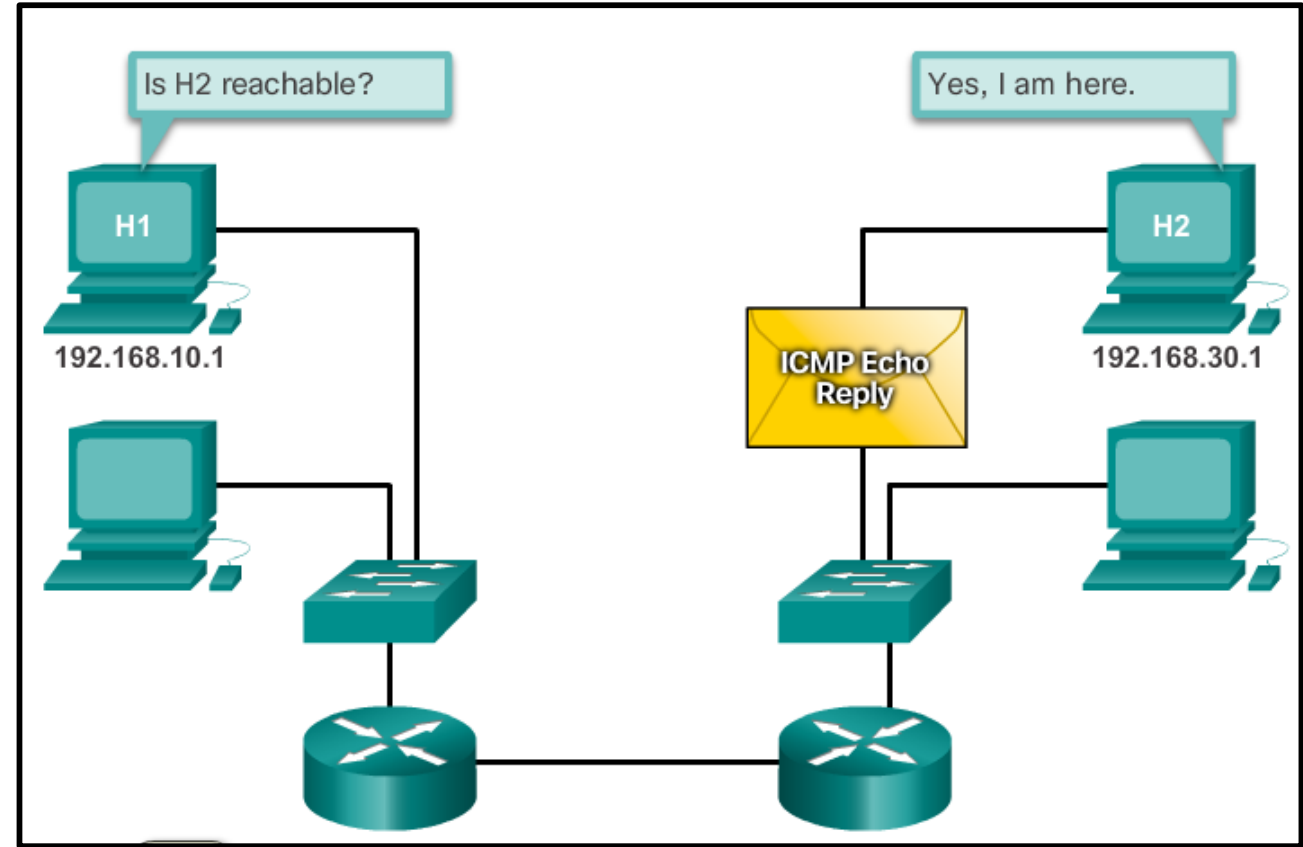
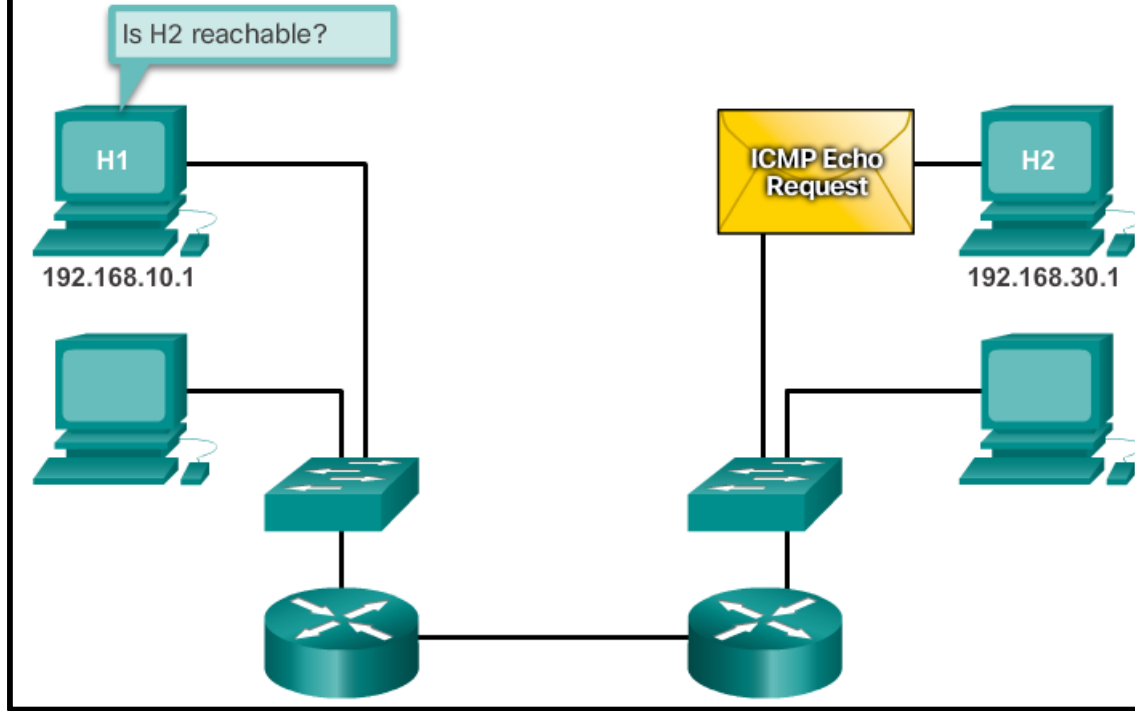


7.2.5.4 Lab – Configuring IPv6 Addresses on Network Devices



7.3.1.1 ICMPv4 and ICMPv6

ICMPv4 Ping to a Remote Host

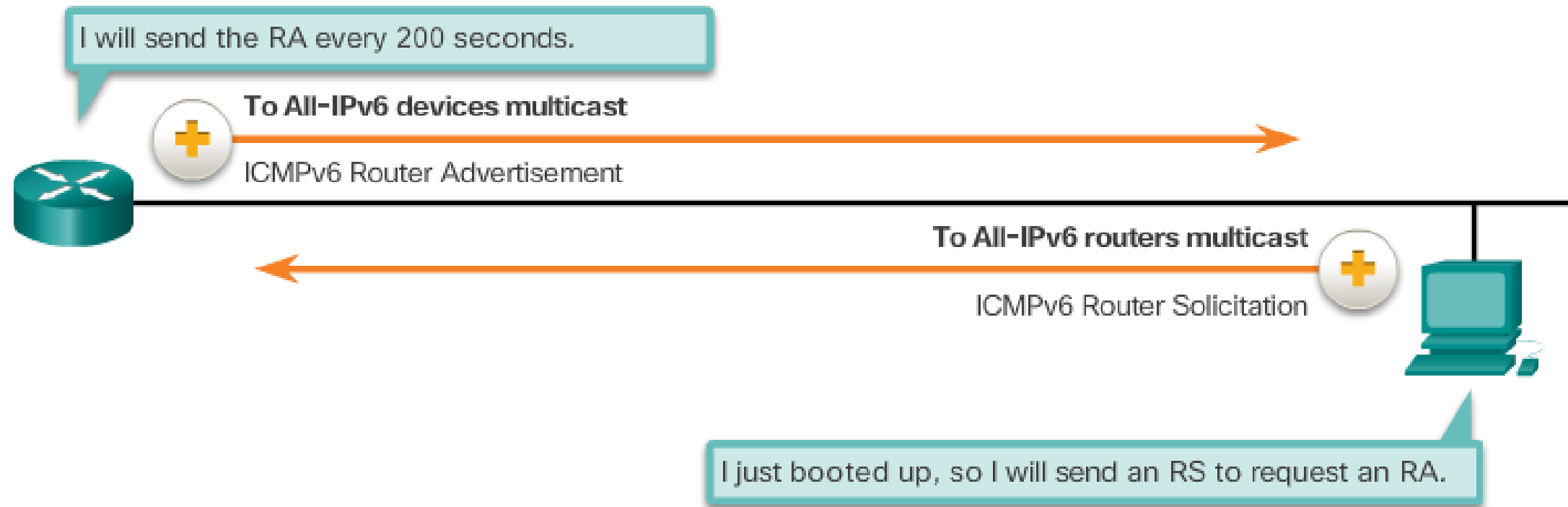


ICMPv4 and ICMPv6

Although IP is not a reliable protocol, the TCP/IP suite does provide for messages to be sent in the event of certain errors. 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.

7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages

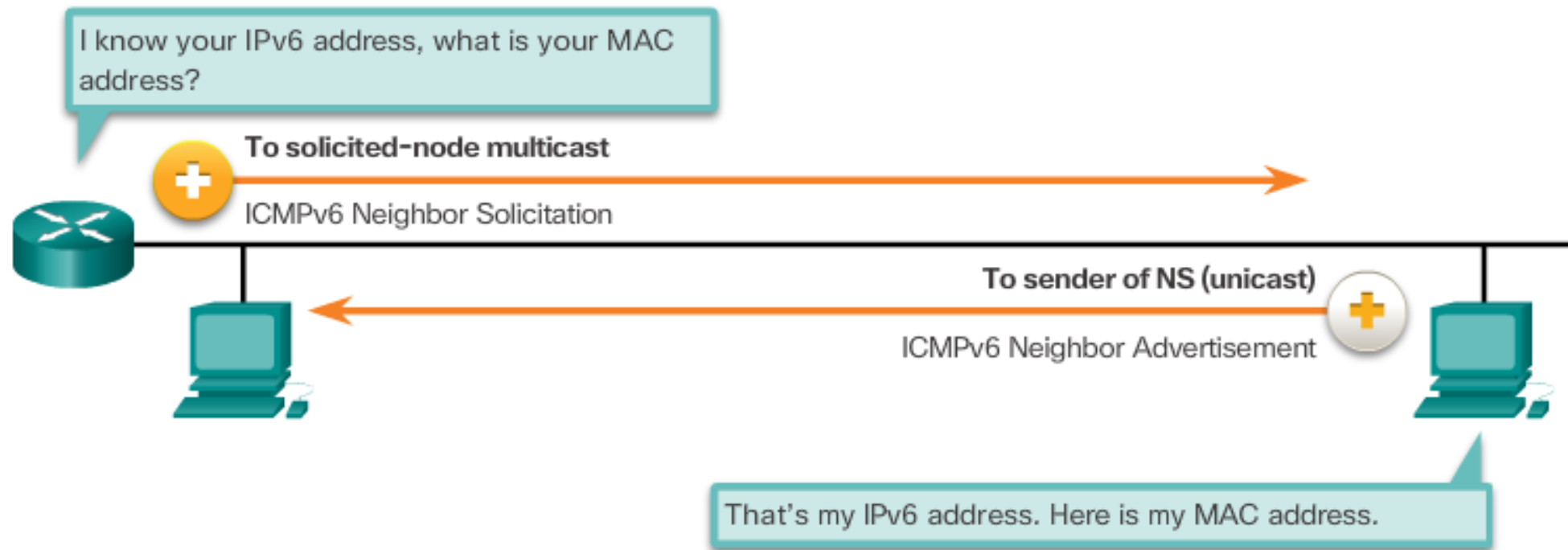
Messaging Between an IPv6 Router and an IPv6 Device



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.

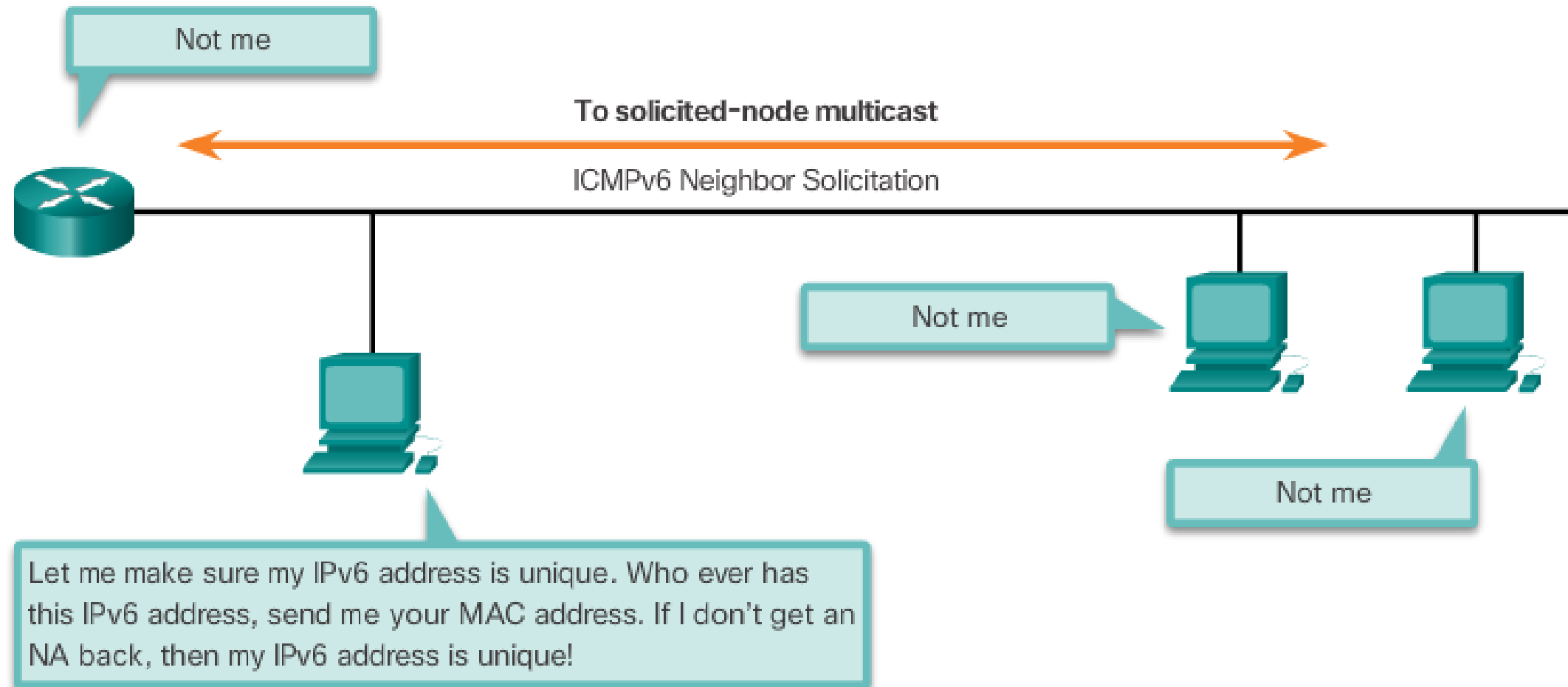
7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages

Messaging Between IPv6 Devices



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.

Duplicate Address Detection (DAD)



7.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages

ICMPv6 includes four new protocols as part of the Neighbor Discovery Protocol (ND or NDP).

Messaging between an IPv6 router and an IPv6 device:

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

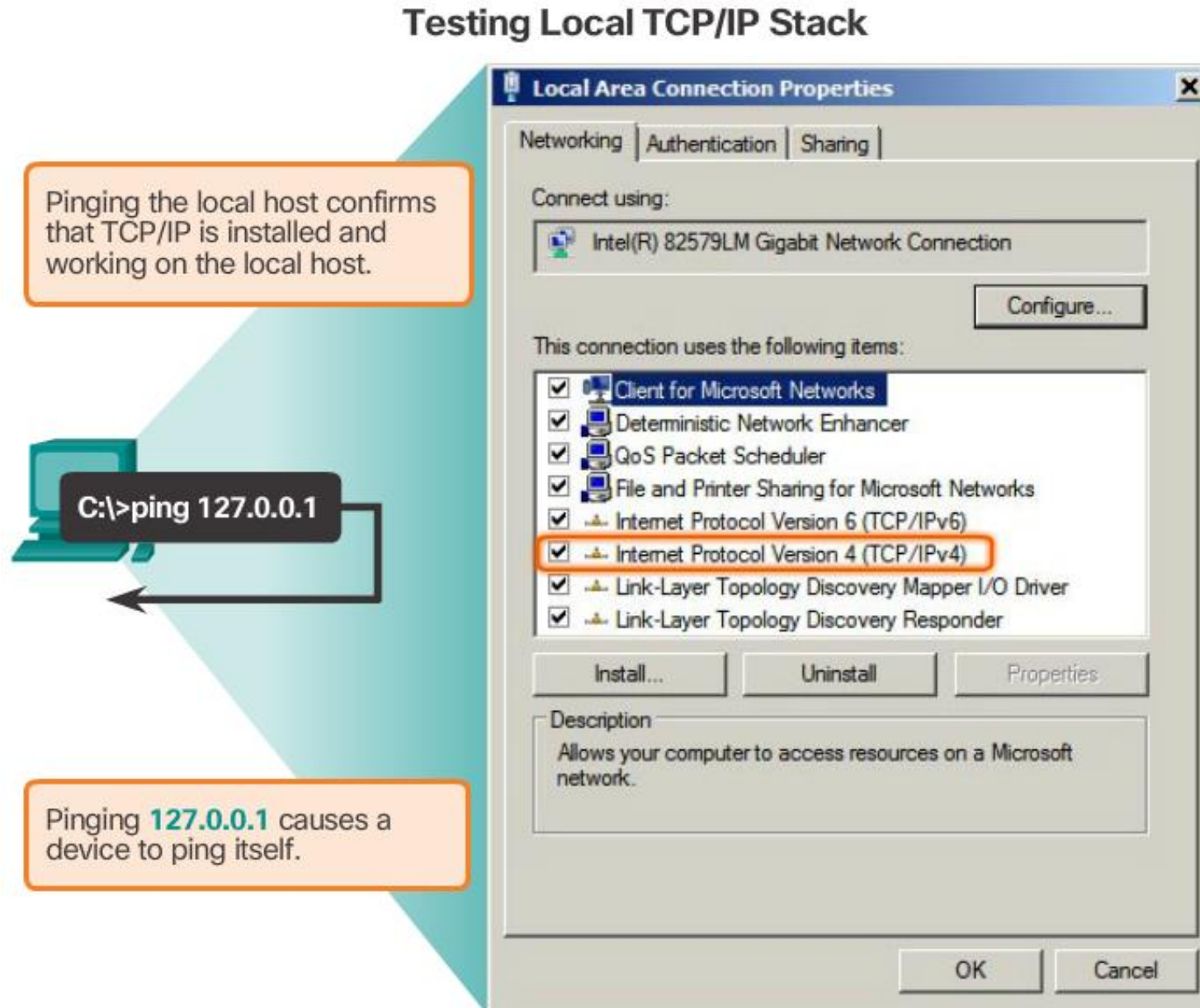
Messaging between IPv6 devices:

- Neighbor Solicitation message
- Neighbor Advertisement message

Figure 1 shows an example of a PC and router exchanging Solicitation and Router Advertisement messages. Click each message for more information.

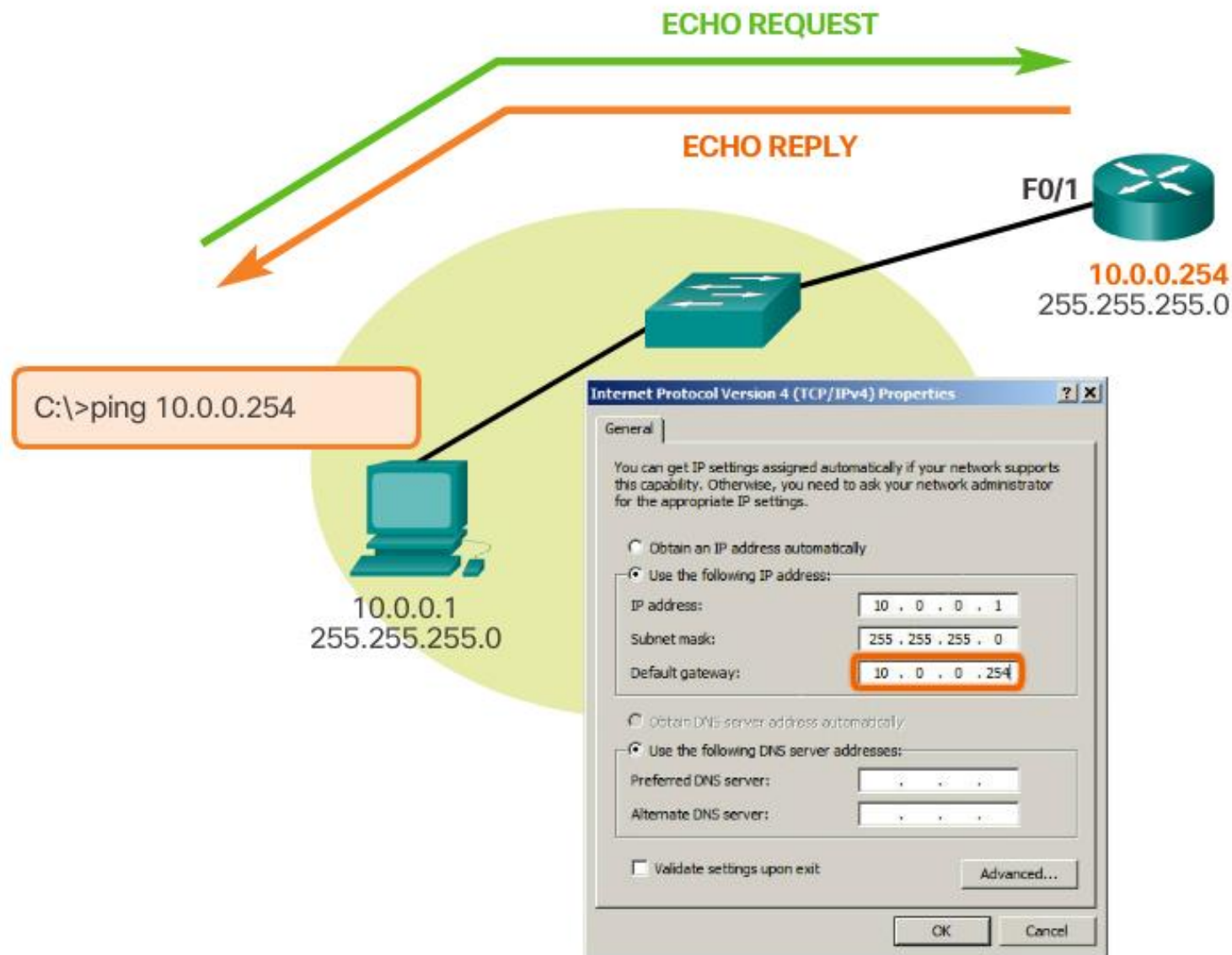
Neighbor Solicitation and Neighbor Advertisement messages are used for Address resolution and Duplicate Address Detection (DAD).

7.3.2.1 Ping - Testing the Local Stack

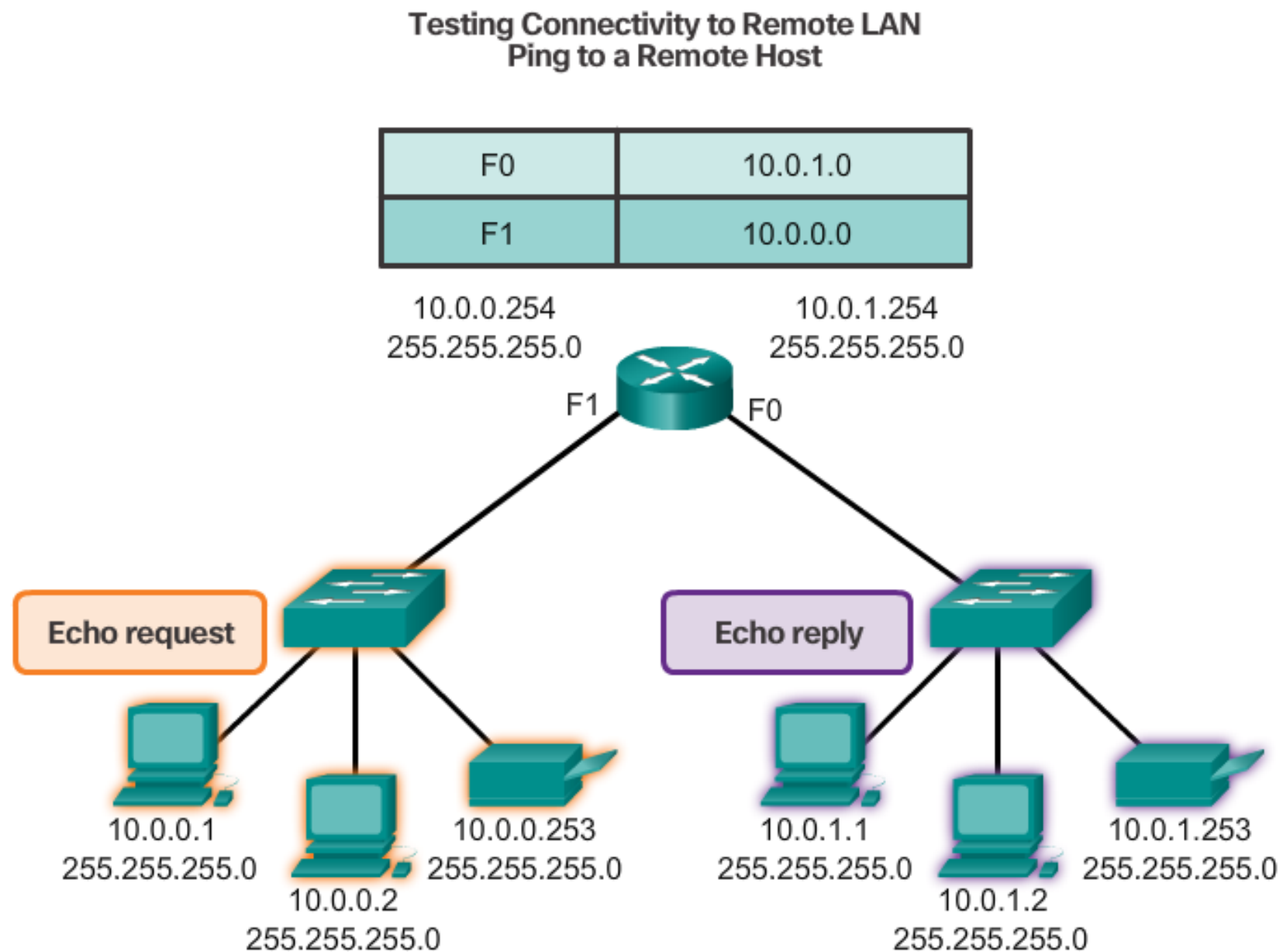


7.3.2.2 Ping – Testing Connectivity to the Local LAN

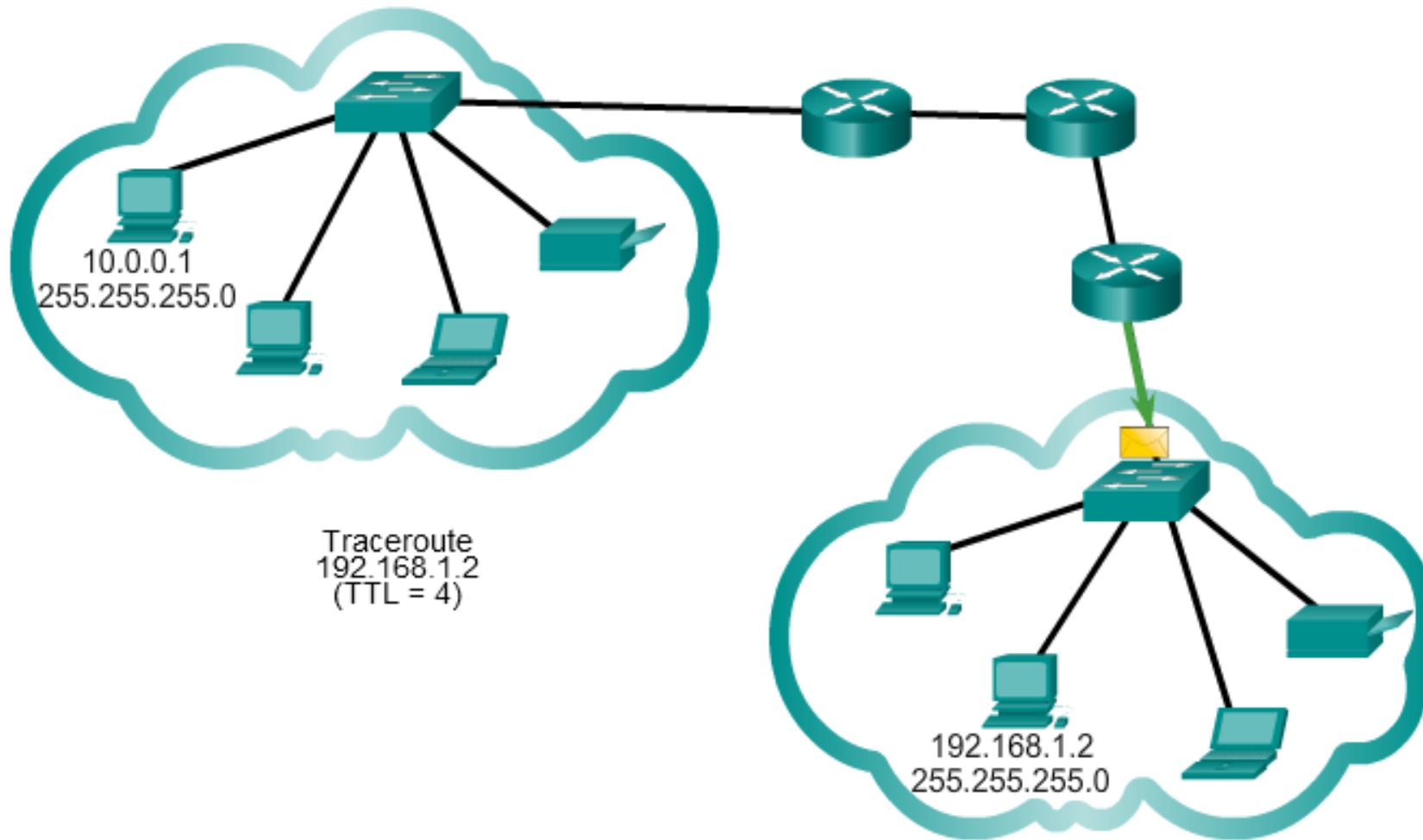
Testing IPv4 Connectivity to Local Network



7.3.2.3 Ping – Testing Connectivity to Remote



Traceroute (tracert) - Testing the Path



7.3.2.5 Packet Tracer – Verifying IPv4 and IPv6 Addressing

Cisco Networking Academy®
Mind Wide Open™

Cisco Packet Tracer

Packet Tracer | Verifying IPv4 and IPv6 Addressing

The image is a composite graphic for a Cisco Packet Tracer presentation. It features the Cisco Networking Academy logo and the text 'Cisco Packet Tracer' in the top left. Below this is a banner with six diverse people. The top right shows a world map with glowing network nodes and binary code. The bottom left is a photo of a woman and a man looking at a computer. The bottom right is a network diagram showing a central switch labeled '2950T-24 SW-A' connected to six PCs labeled 'PC-PT C1' through 'PC-PT D2'.

7.3.2.6 Packet Tracer – Pinging and Tracing to Test the Path

Cisco Networking Academy®
Mind Wide Open™

Cisco Packet Tracer



The image displays the Cisco Packet Tracer software interface. The top section features the Cisco Networking Academy logo and the title "Cisco Packet Tracer". Below this is a banner with a world map and binary code. The main area is divided into two sections: "Packet Tracer" on the left and "Pinging and Tracing to Test the Path" on the right. The "Packet Tracer" section shows a video of two people working on a computer. The "Pinging and Tracing to Test the Path" section displays a network diagram with a central switch labeled "2950T-24 SW-A" connected to six PCs labeled "PC-PT C1", "PC-PT C2", "PC-PT C3", "PC-PT C4", "PC-PT D1", and "PC-PT D2".

Packet Tracer | Pinging and Tracing to Test the Path

2950T-24 SW-A

PC-PT C1, PC-PT C2, PC-PT C3, PC-PT C4, PC-PT D1, PC-PT D2

7.3.2.7 Lab – Testing Network Connectivity with Ping and Traceroute



7.3.2.8 Lab – Mapping the Internet



7.3.2.9 Packet Tracer – Troubleshooting IPv4 and IPv6 Addressing

Cisco Networking Academy®
Mind Wide Open™

Cisco Packet Tracer



Packet Tracer | Troubleshooting IPv4 and IPv6 Addressing



```
graph TD; SW_A[2950T-24 SW-A] --- C1[PC-PT C1]; SW_A --- C2[PC-PT C2]; SW_A --- C3[PC-PT C3]; SW_A --- C4[PC-PT C4]; SW_A --- D1[PC-PT D1]; SW_A --- D2[PC-PT D2];
```


7.4.1.2 Packet Tracer – Skills Integration Challenge

Cisco Networking Academy®
Mind Wide Open™

Cisco Packet Tracer



The banner features a collage of images: a world map with glowing network connections, a row of diverse people, a magnifying glass over a grid, and a network diagram. The network diagram shows a central switch labeled '2950T-24 SW-A' connected to six PCs labeled 'PC-PT C1' through 'PC-PT D2'. The PCs are arranged in two groups of three, with dashed lines indicating a connection between the two groups.

Packet Tracer | Skills Integration Challenge

2950T-24
SW-A

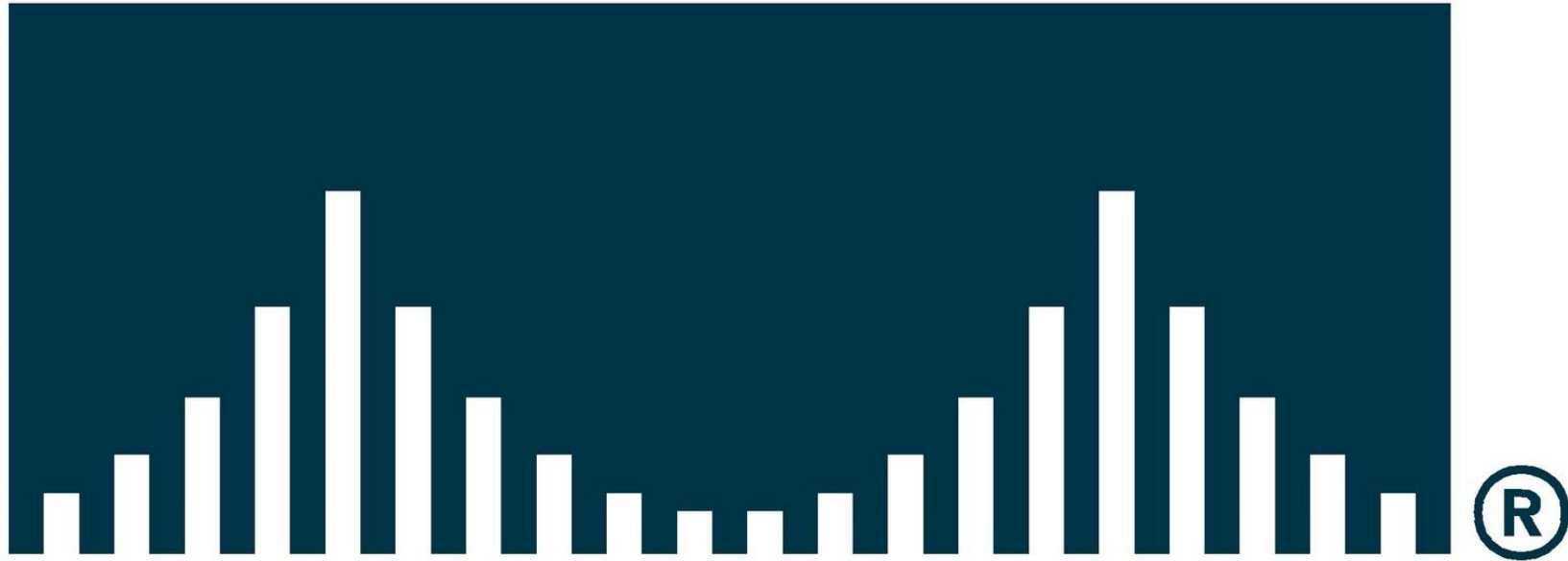
PC-PT C1 PC-PT C2 PC-PT C3 PC-PT C4 PC-PT D1 PC-PT D2



Summary | Chapter 7



CISCO SYSTEMS



Thank you for your attention!