Cisco Networking Academy

CCNA R&S: Introduction to Networks

Chapter 8:

IP Addressing

Frank Schneemann

8.0.1.1 Introduction

Upon completion of this chapter you will be able to:

- Describe the structure of an IPv4 address.
- Describe the purpose of the subnet mask.
- Compare the characteristics and uses of the unicast, broadcast, and multicast IPv4 addresses.
- Compare the use of public address space and private address space.
- 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.
- Describe the role of ICMP in an IP network. (Include IPv4 and IPv6.)
- Use ping and traceroute utilities to test network connectivity.

8.0.1.2 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?

If nature, traffic, transportation, networking, and space exploration depend on digital information sharing, how will that information be identified from source to destination?

In this activity, you will begin to think about not only what will be identified in the IoE world, but how everything will be addressed in the same world!

8.1.1.1 Binary Notation

Characters	ASCII Bit Translation
A	01000001

Positional Notation

192

	Hundreds	Tens	Ones
Radix	10	10	10
Exponent	2	1	0
Positional Value	100	10	1
Numerical Identifier	1	9	2
Numerical Value	1*100=100	9*10=90	2*1=2

100+90+2

- Binary Representation
- American Standard Code for Information Interchange (ASCII).
- Decimal system

8.1.1.1 Binary Notation

Keyboard	Binary Codes
A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000

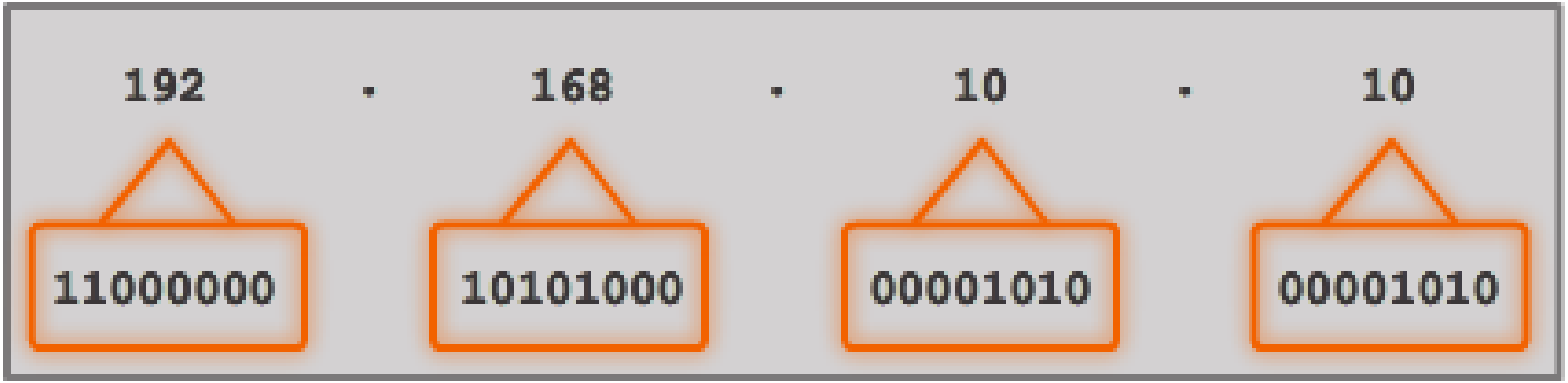
128	64	32	16	8	4	2	1

The Letter A

0	1	0	0	0	0	0	1

8.1.1.2 Binary Number System

128	64	32	16	8	2	1	0

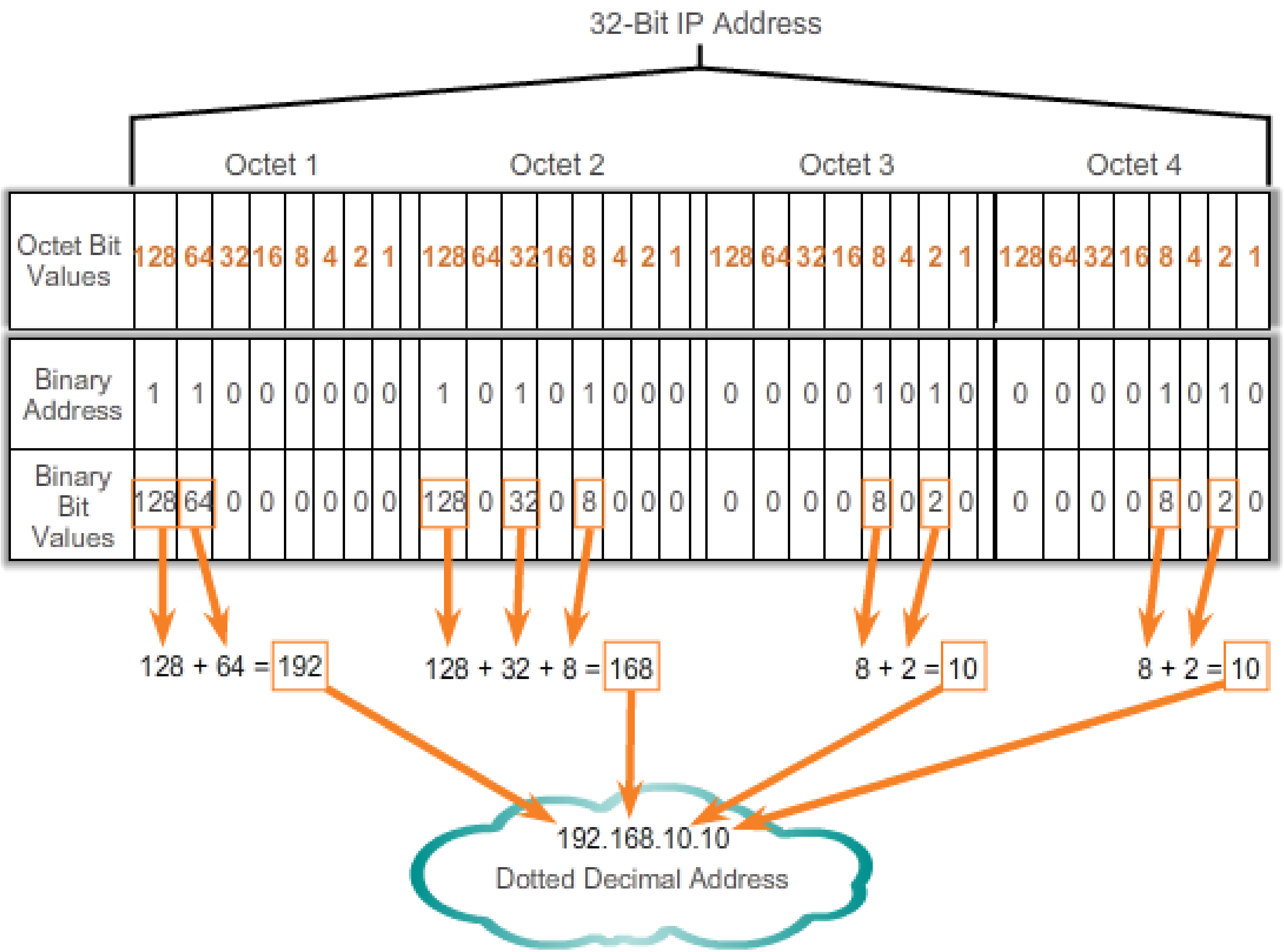


This address is made up of four different octets.

Dotted Decimal Notation

Binary	11001000		01110010		00000110		00110011
Decimal	200	.	114	.	6	.	51
	number	dot	number	dot	number	dot	number

8.1.1.3 Converting a Binary Address to Decimal



Binary to Decimal Conversion

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

1	**1**	**0**	**0**	**0**	**0**	**0**	**0**

1	**0**	**0**	**1**	**1**	**0**	**0**	**1**

1	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Decimal - Binary - Hexadecimal Table

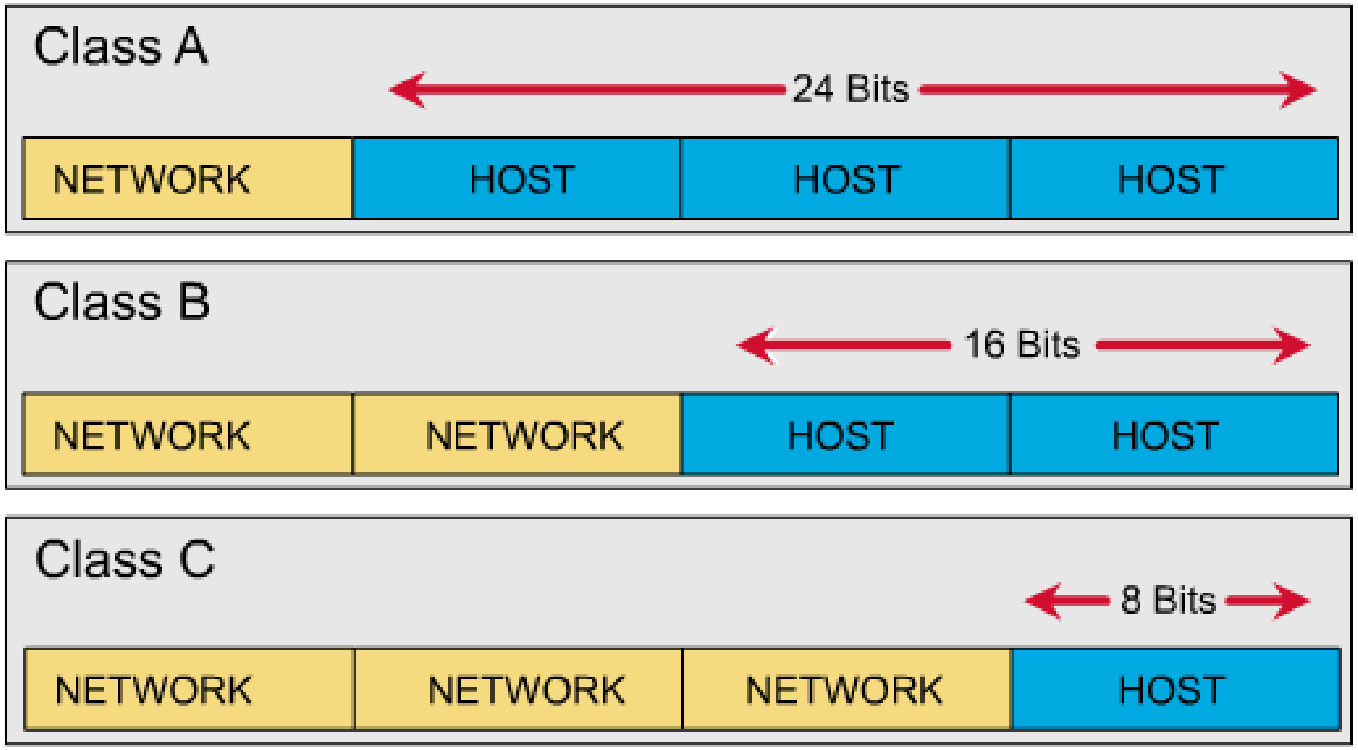
Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

Address Classes

Cls	1st Octet Decimal Range	1st Octet High Order Bits	Network / Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (usable addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 (2^7 – 2)	16,777,214 (2^{24} – 2)
B	128 – 191	1 0	N.N.H.H	255.255.0.0	16,382 (2^{14} - 2)	65,534 (2^{16} – 2)
C	192 – 223	1 1 0	N.N.N.H	255.255.255.0	2,097,150 (2^{21} – 2)	254 (2^8 – 2)
D	224 – 239	1 1 1 0	Reserved for Multicasting			
E	240 – 254	1 1 1 1 0	Experimental, used for research			

IP Address Classes

IP Address Classes



Class "C" is the final commercial class of addresses. With eight bits for the host address, only two hundred fifty four hosts are allowed. Most smaller organizations use a class "C" or several class "C" addresses. As you'll see later, two addresses are always reserved: one for the network, and one for the broadcast address.

IP First Octet Address Ranges

High Order Bits	Octet in Decimal	Address Class
0	0 - 127	A
10	128 - 191	B
110	192 - 223	C

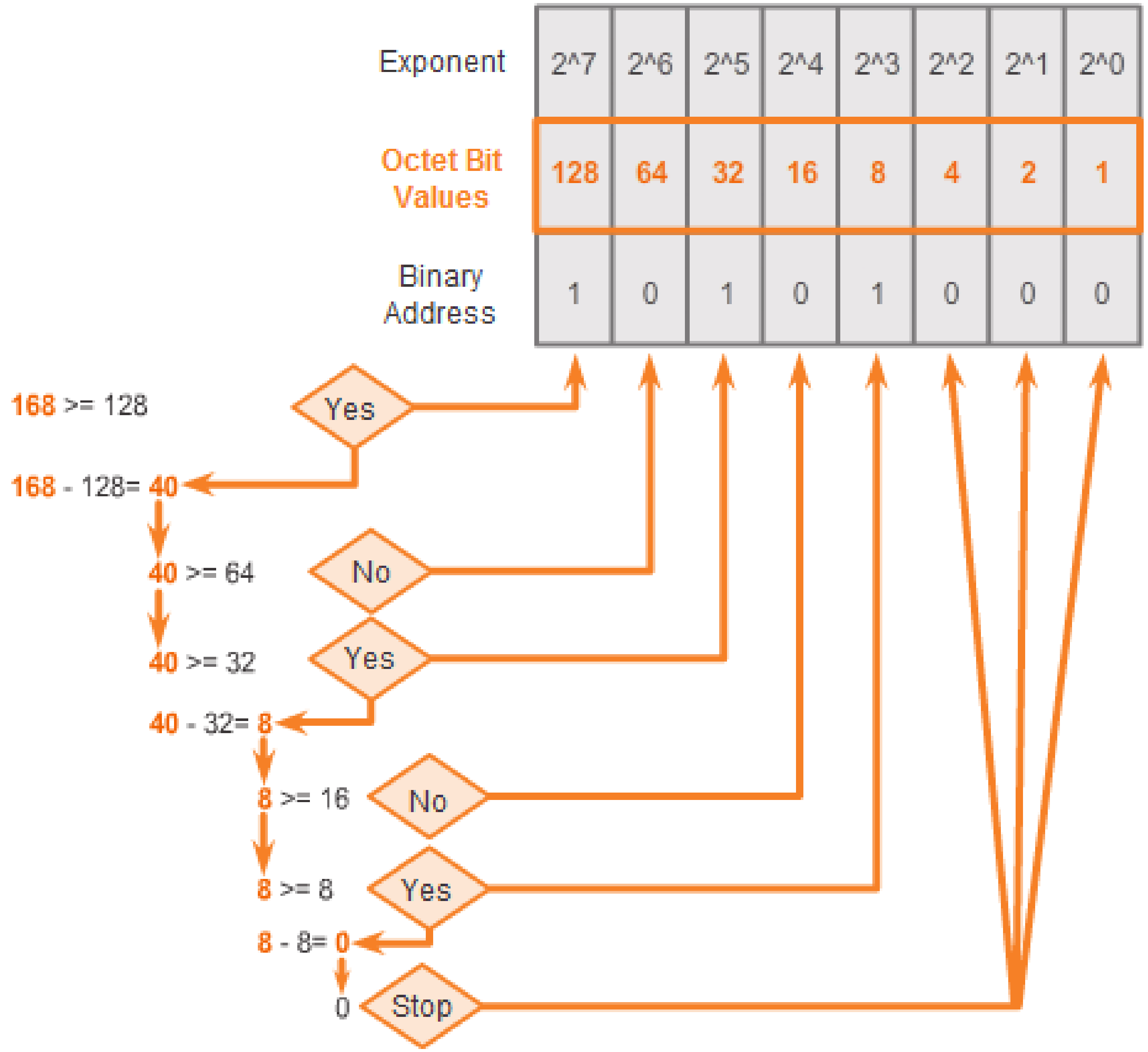
8.1.1.4 Activity - Binary to Decimal Conversions

Enter decimal answer here

Decimal value	113							
Radix	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**	**1**	**1**	**1**	**0**	**0**	**0**	**1**

Binary number

8.1.1.5 Converting from Decimal to Binary

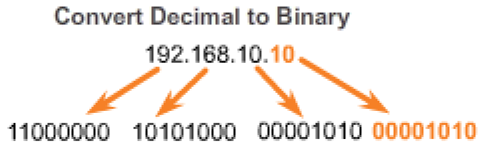


8.1.1.5 Converting from Decimal to Binary

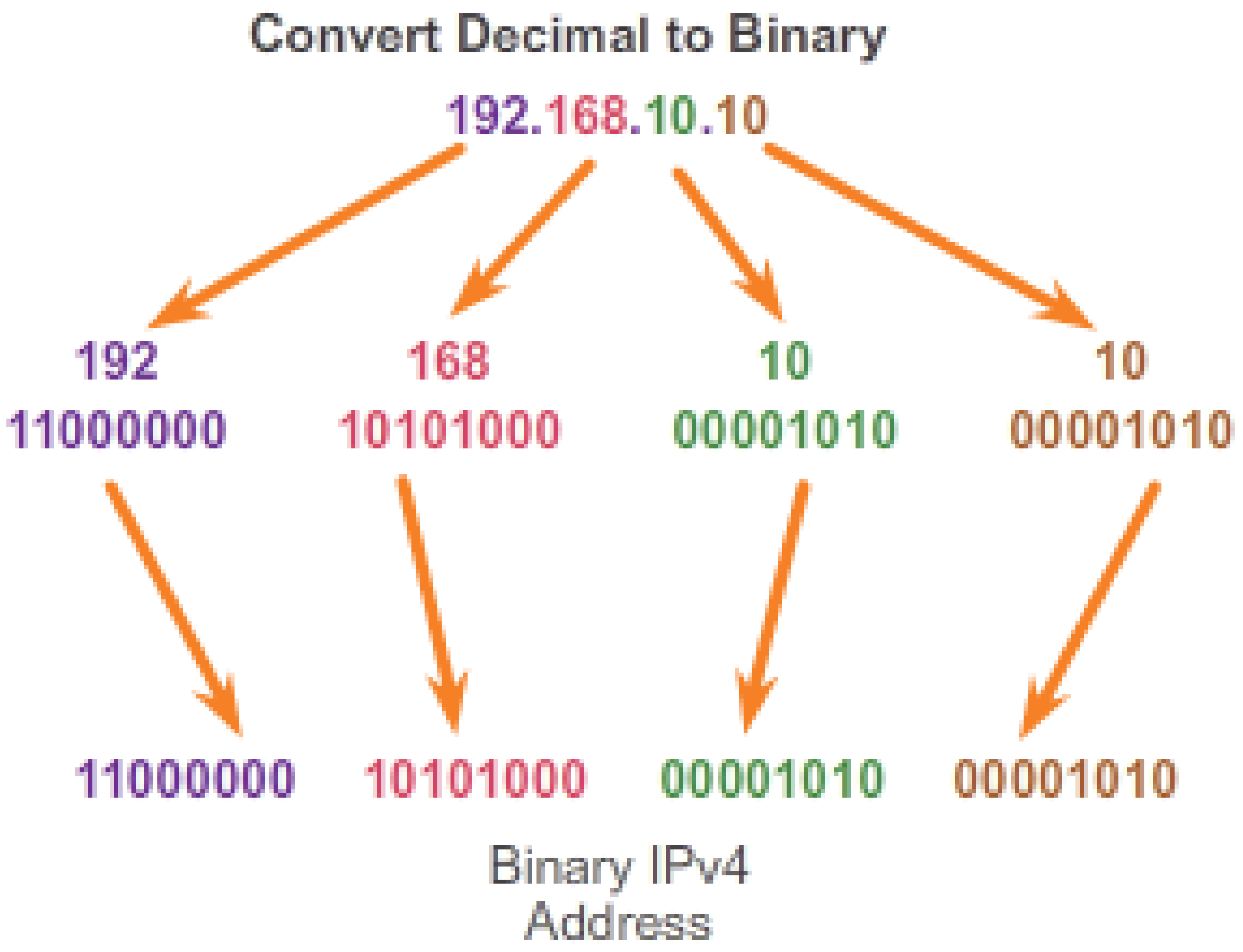
128	64	32	16	8	4	2	1

Number	Divide	Result	Remainder
192	**/ 2 =**	96	0
96	**/ 2 =**	48	0
48	**/ 2 =**	24	0
24	**/ 2 =**	12	0
12	**/ 2 =**	6	0
6	**/ 2 =**	3	0
3	**/ 2 =**	1	1
1	**/ 2 =**	0	1

8.1.1.5 Converting from Decimal to Binary



	128	64	32	16	8	4	2	1
10 < 128, place a 0 in the 128 position do not subtract	0	0	0	0	1	0	1	0
10 < 64, place a 0 in the 64 position do not subtract	0	0	0	0	1	0	1	0
10 < 32, place a 0 in the 32 position do not subtract	0	0	0	0	1	0	1	0
10 < 16, place a 0 in the 16 position do not subtract	0	0	0	0	1	0	1	0
10 > 8, place a 1 in the 8 position subtract 8	0	0	0	0	1	0	1	0
2 < 4, place a 0 in the 4 position do not subtract	0	0	0	0	1	0	1	0
2 = 2, place a 1 in the 2 position -2 subtract 2	0	0	0	0	1	0	1	0
0 place a 0 in all remaining positions								
All done. Result	0	0	0	0	1	0	1	0



8.1.1.7 Activity - Decimal to Binary Conversion Activity

Decimal value	104							
Radix	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	1	1	0	1	0	0	0

8.1.1.8 Activity - Binary Game

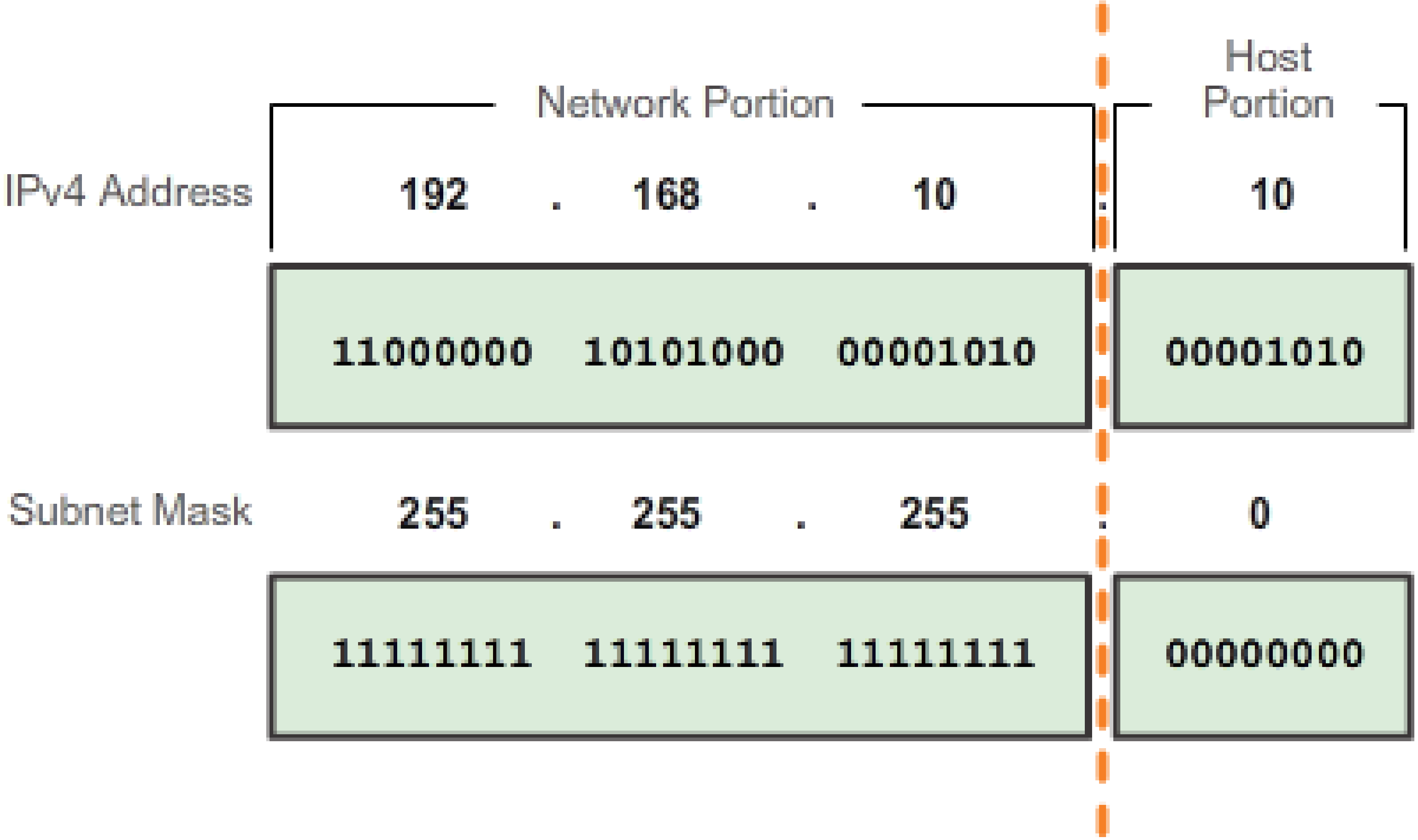
Binary Game

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

8.1.2.1 Network Portion and Host Portion of an IPv4 Address



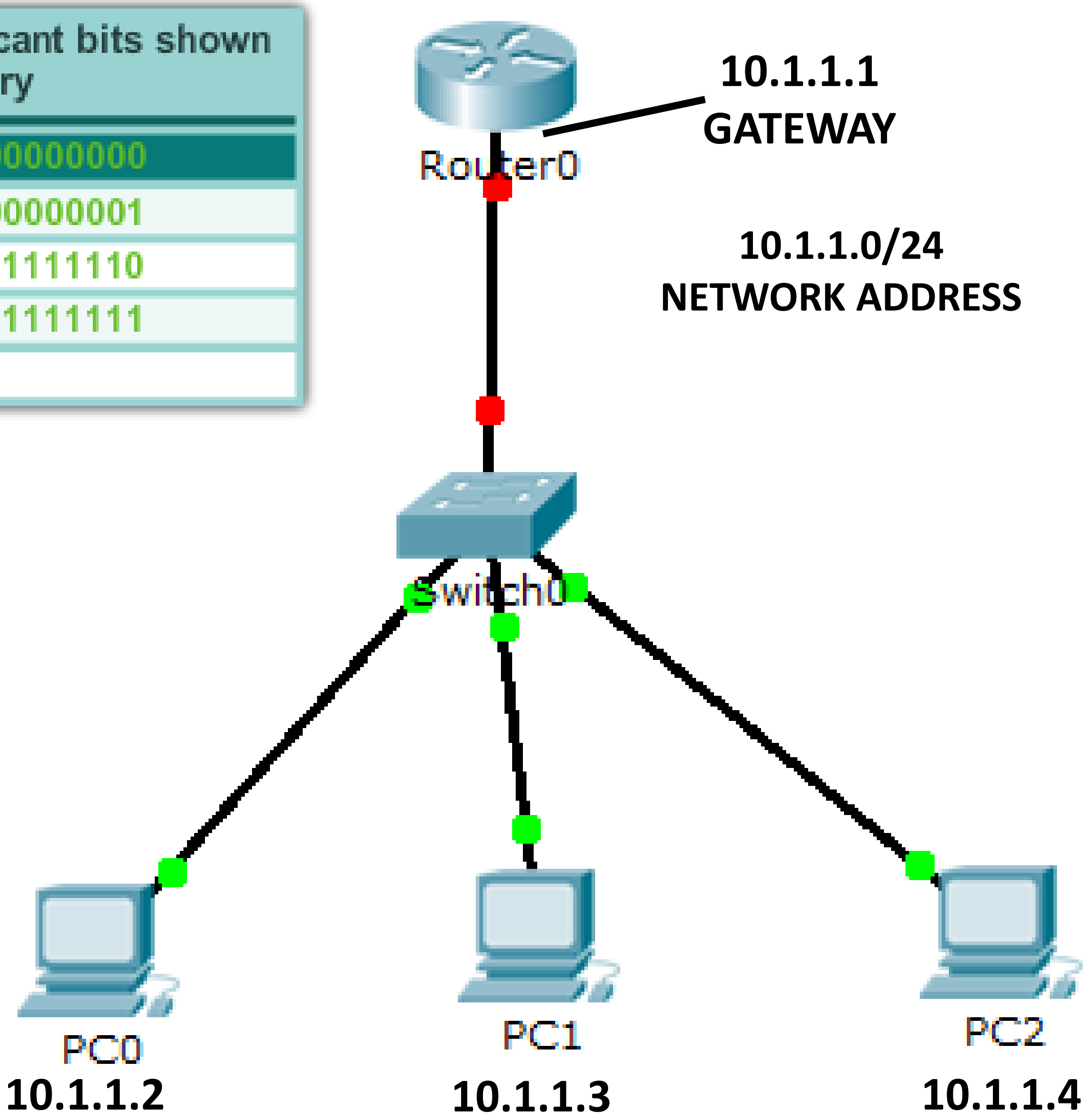
8.1.2.2 Examining the Prefix Length

	Dotted Decimal	Significant bits shown in binary
Network Address	**10.1.1.0/24**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.254	10.1.1.11111110
Broadcast Address	10.1.1.255	10.1.1.11111111
Number of hosts: 2^8 – 2 = 254 hosts		

255.255.255.0 – SUBNET MASK

11111111.11111111.11111111.00000000

10.1.1.0 – NETWORK ADDR
10.1.1.1 – HOST
10.1.1.2 – HOST
10.1.1.3 – HOST
10.1.1.4 – HOST
10.1.1.5 – 10.1.1.254 HOST
10.1.1.255 – BROADCAST ADDR



8.1.2.2 Examining the Prefix Length

Network Address	10.1.1.0/28	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.14	10.1.1.00001110
Broadcast Address	10.1.1.15	10.1.1.00001111
Number of hosts: 2^4 – 2 = 14 hosts		

255.255.255.240 – SUBNET MASK

11111111.11111111.11111111.11110000

10.1.1.0 – NETWORK ADDR

10.1.1.1 – HOST

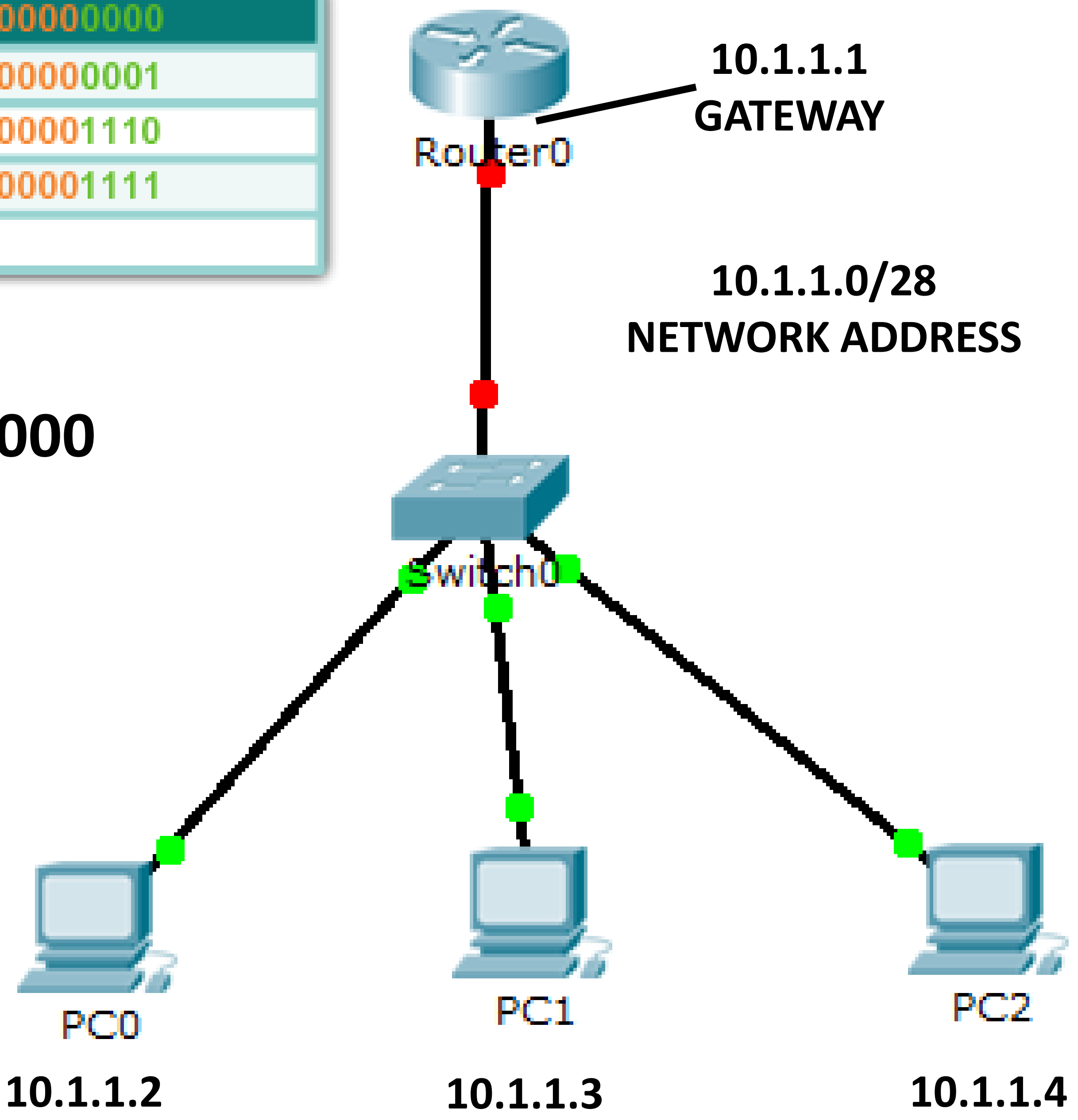
10.1.1.2 – HOST

10.1.1.3 – HOST

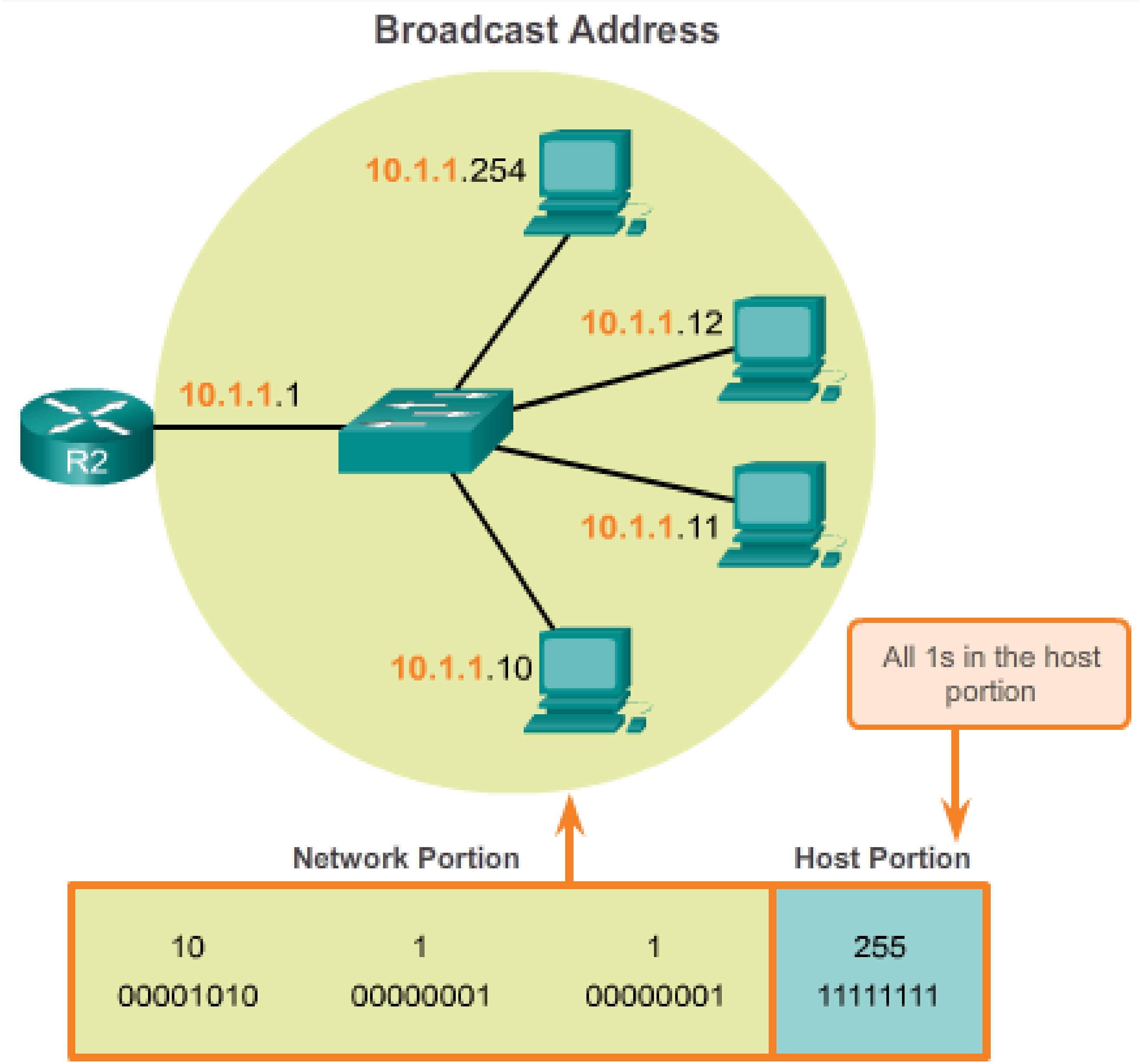
10.1.1.4 – HOST

10.1.1.5 – 10.1.1.14 HOST

10.1.1.15 – BROADCAST ADDR



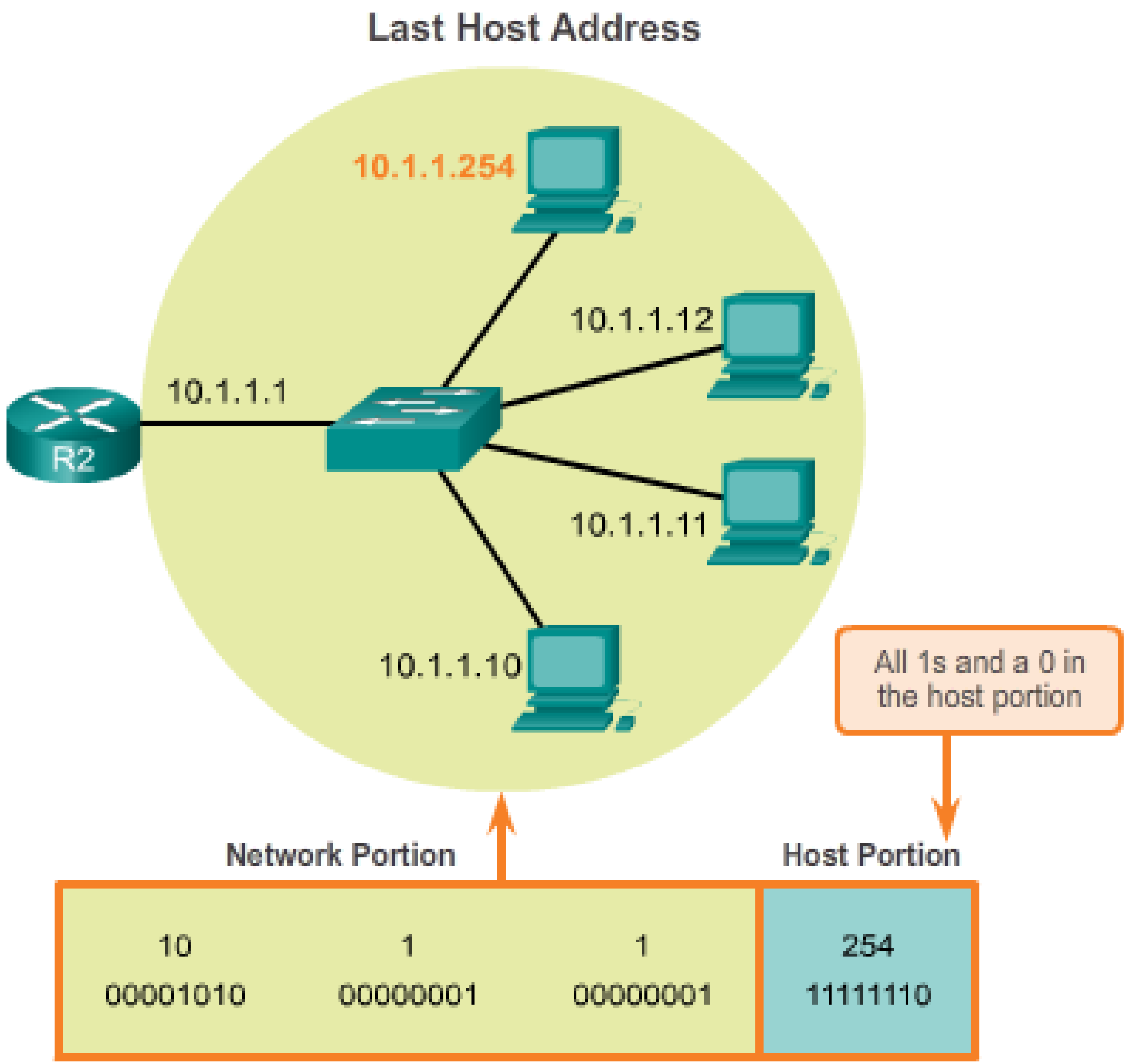
8.1.2.3 IPv4 Network, Host and Broadcast Addresses



There are three types of addresses within the address range of each IPv4 network:

- Network address
- Host addresses
- Broadcast address

8.1.2.4 First Host and Last Host Addresses



8.1.2.5 Bitwise AND Operation

1 AND 0 = 0

IPv4 Address

11000000	10101000	00001010	00001010

Subnet Mask

11111111	11111111	11111111	00000000

Network Address

11000000	10101000	00001010	00000000

8.1.2.6 Importance of ANDing

IPv4 Address	192	168	10	10
	11000000	10101000	00001010	00001010
Subnet Mask	255	255	255	0
	11111111	11111111	11111111	00000000
Network Address	192	168	10	0
	11000000	10101000	00001010	00000000

Routers need to know what the Network Address is

Address
172.16.20.35
10101100.00010000.00010100.00100011

Subnet mask
255.255.255.224
11111111.11111111.11111111.11100000
or
172.16.20.35/27

IP Address

202	19	196	100
1 1 0 0 1 0 1 0	**0 0 0 1 0 0 1 1**	**1 1 0 0 0 1 0 0**	**0 1 1 0 0 1 0 0**

IP Address & Subnet Mask

202	19	196	100
1 1 0 0 1 0 1 0	0 0 0 1 0 0 1 1	1 1 0 0 0 1 0 0	0 1 1 0 0 1 0 0

255	255	255	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0

IP Address & Subnet Mask used to extract Network Address

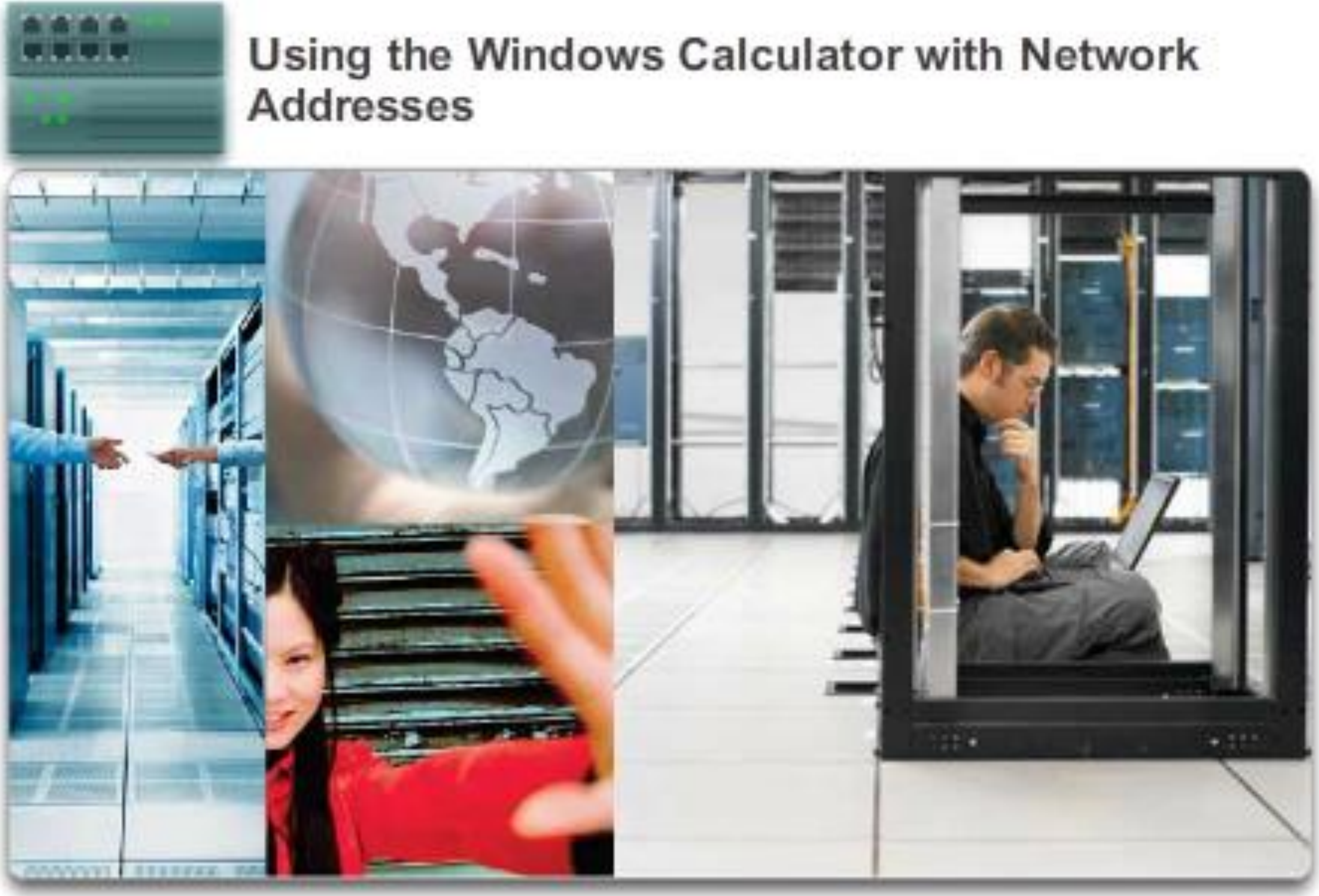
202	19	196	100
1 1 0 0 1 0 1 0	0 0 0 1 0 0 1 1	1 1 0 0 0 1 0 0	0 1 1 0 0 1 0 0

255	255	255	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0

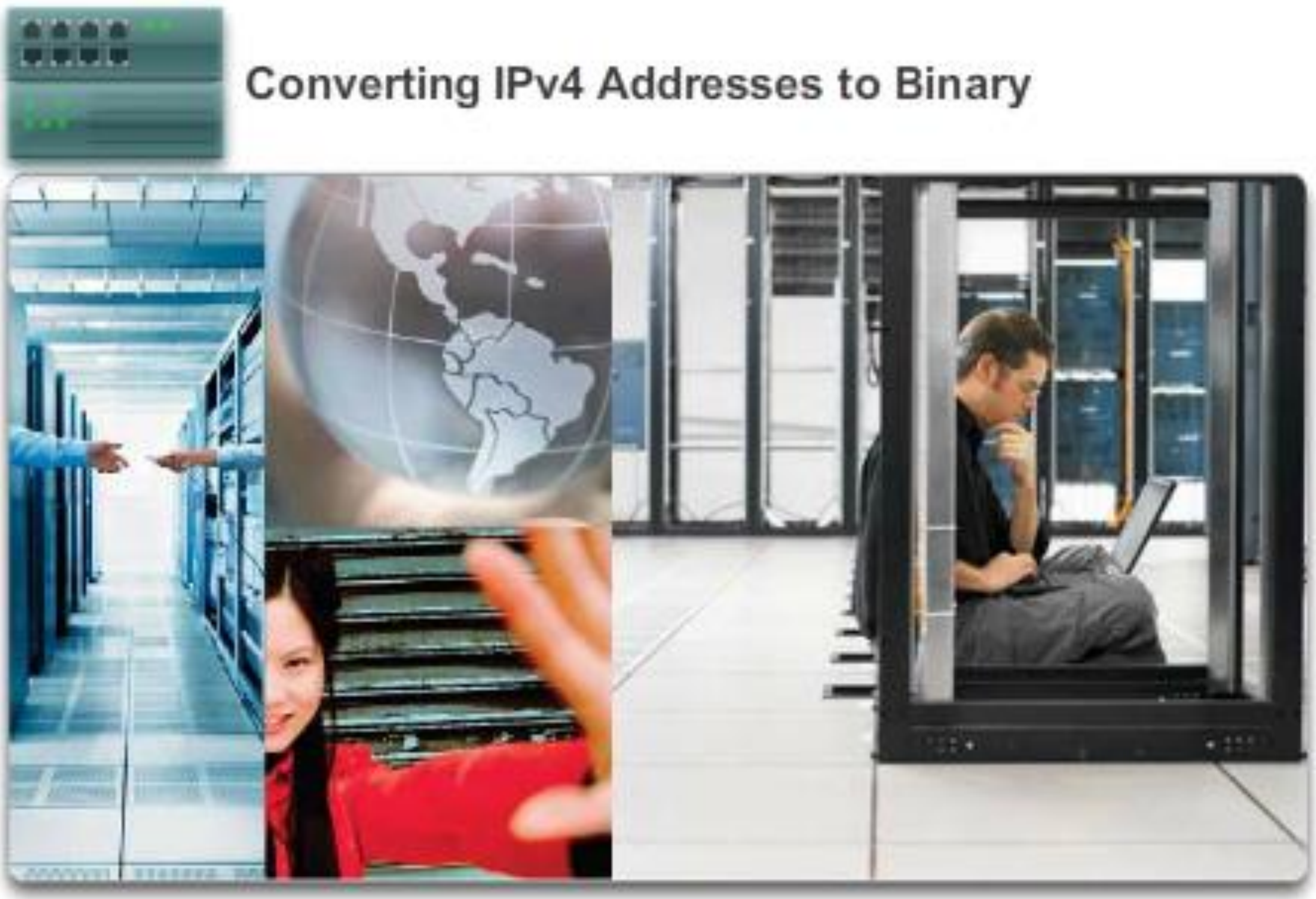
202	19	196	0
1 1 0 0 1 0 1 0	0 0 0 1 0 0 1 1	1 1 0 0 0 1 0 0	0 0 0 0 0 0 0 0

202	19	196	100
1 1 0 0 1 0 1 0	0 0 0 1 0 0 1 1	1 1 0 0 0 1 0 0	0 1 1 0 0 1 0 0
255	255	255	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0
202	19	196	0
1 1 0 0 1 0 1 0	0 0 0 1 0 0 1 1	1 1 0 0 0 1 0 0	0 0 0 0 0 0 0 0

IPv4 Network Addresses



8.1.2.8 Lab - Converting IPv4 Addresses to Binary

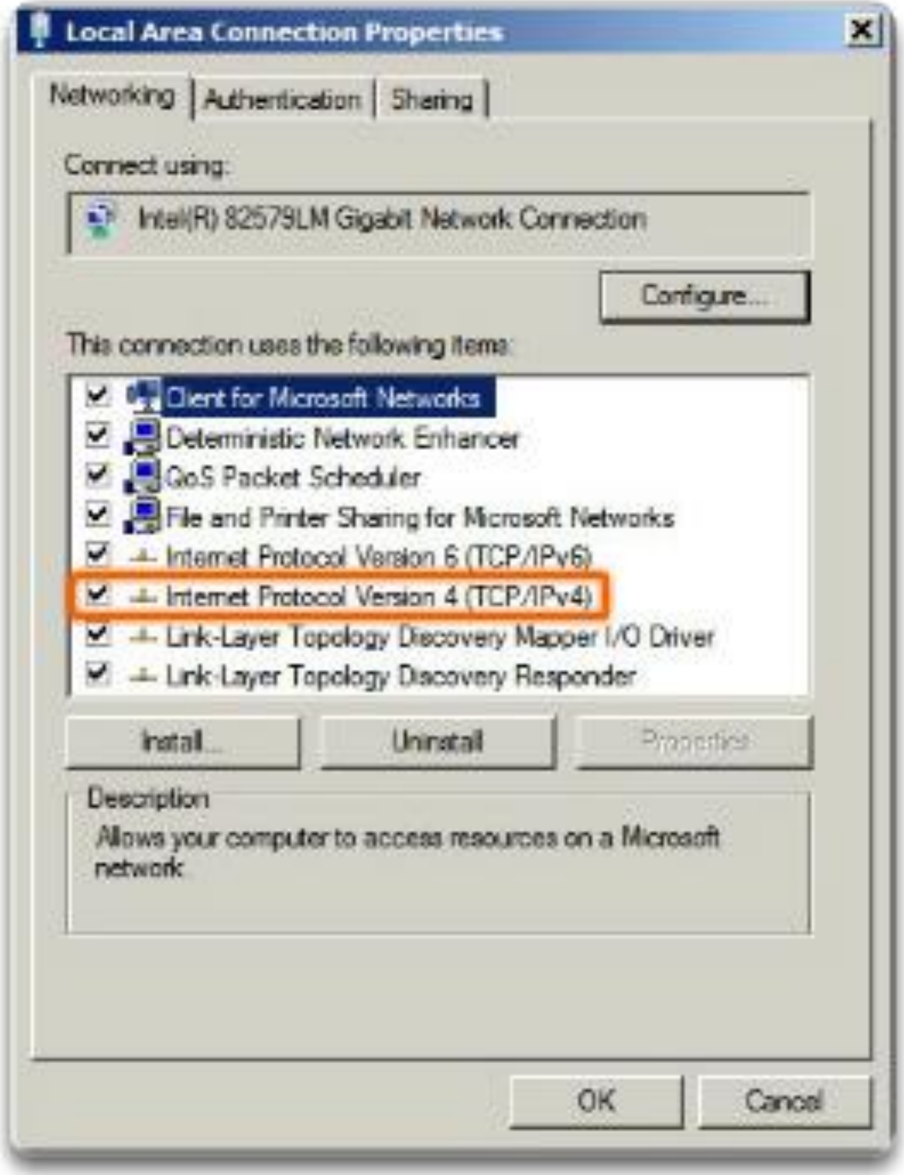


8.1.2.9 Activity - ANDing to Determine the Network Address

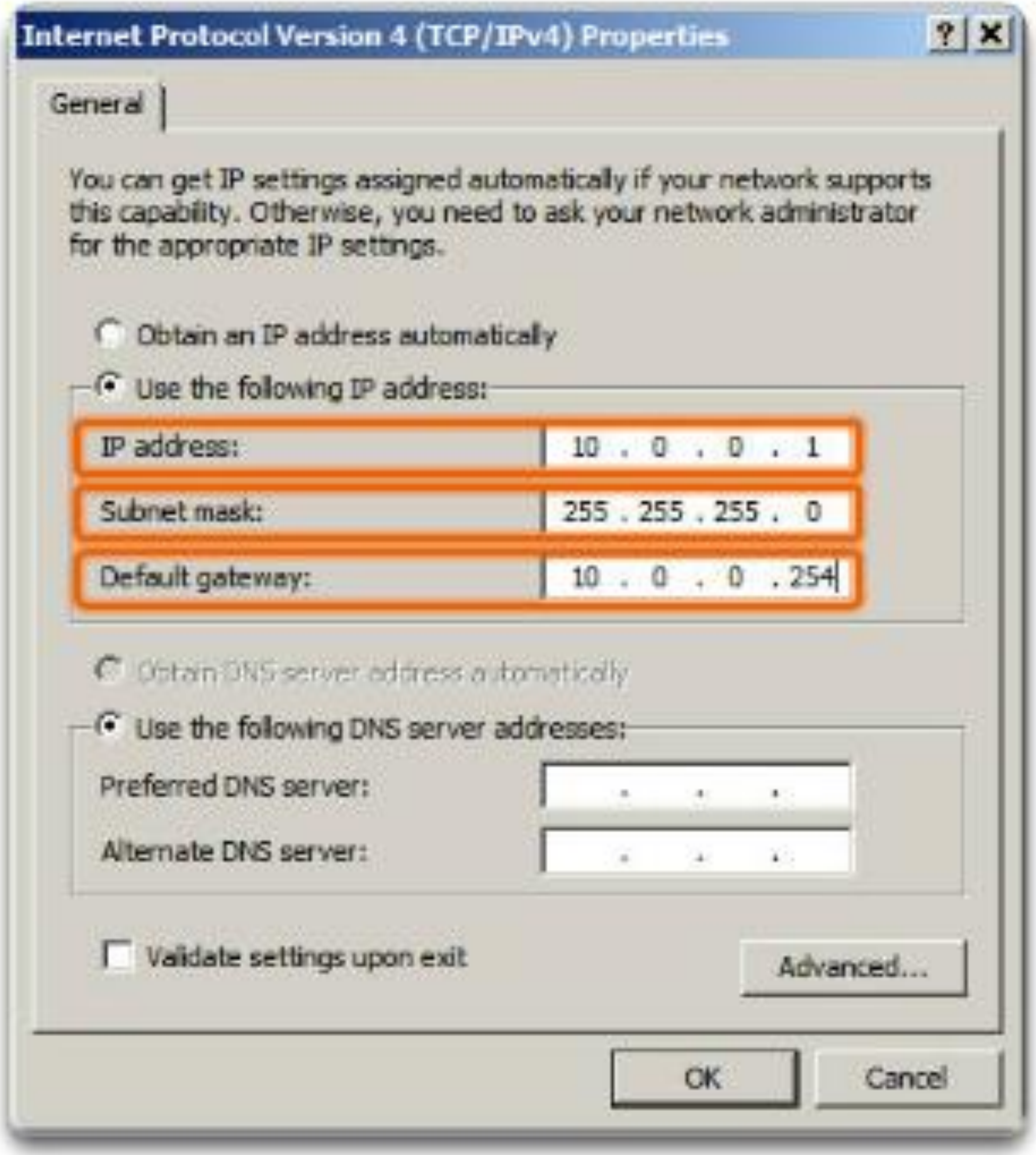
Host Address	10	171	174	234
Subnet Mask	255	255	224	0
Host Address in binary	00001010	10101011	10101110	11101010
Subnet Mask in binary	11111111	11111111	11100000	00000000
Network Address in binary	**00001010**	**10101011**	**10100000**	**00000000**
Network Address in decimal	**10**	**171**	**160**	**0**

8.1.3.1 Assigning a Static IPv4 Address to a Host

LAN Interface Properties

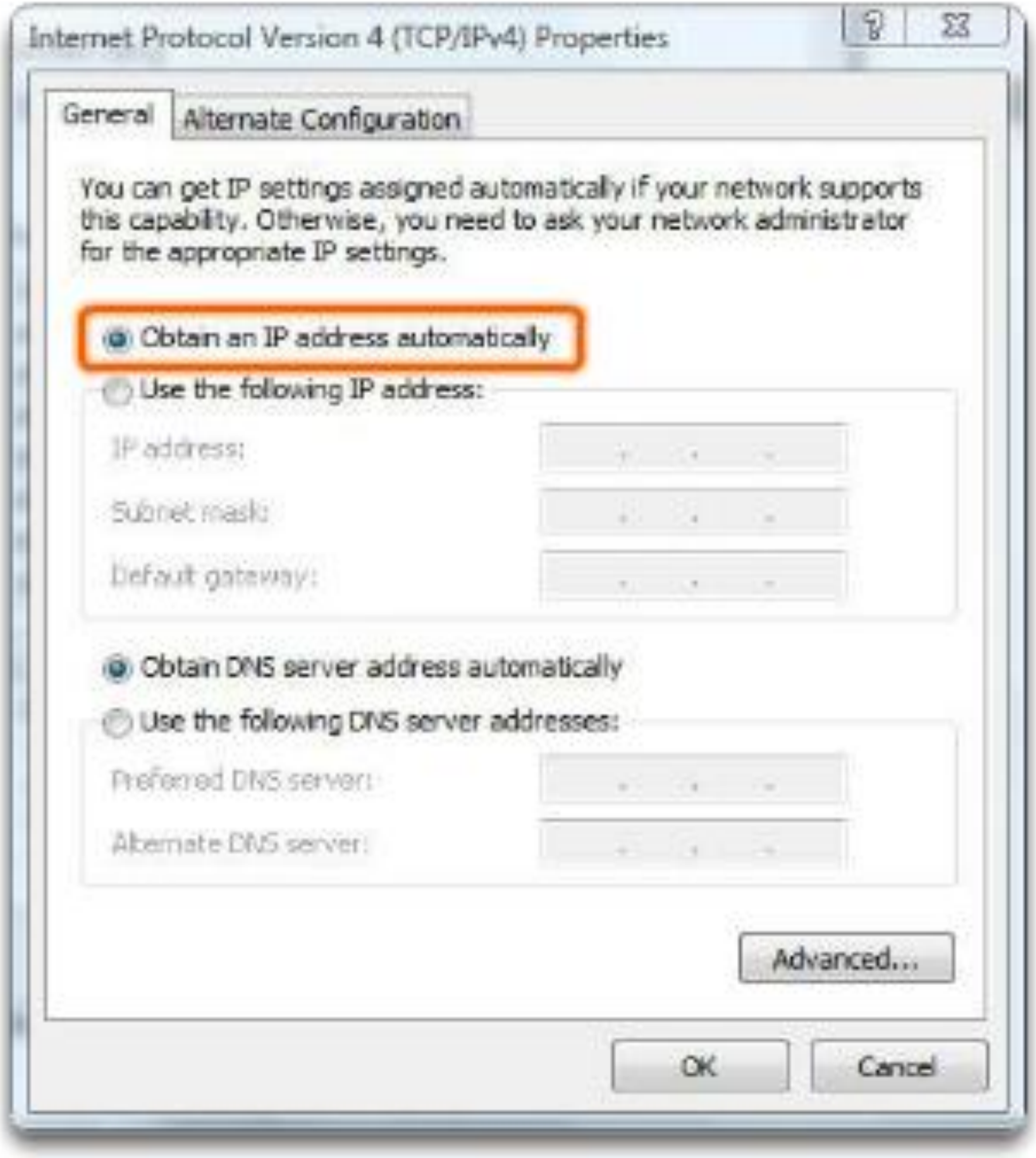


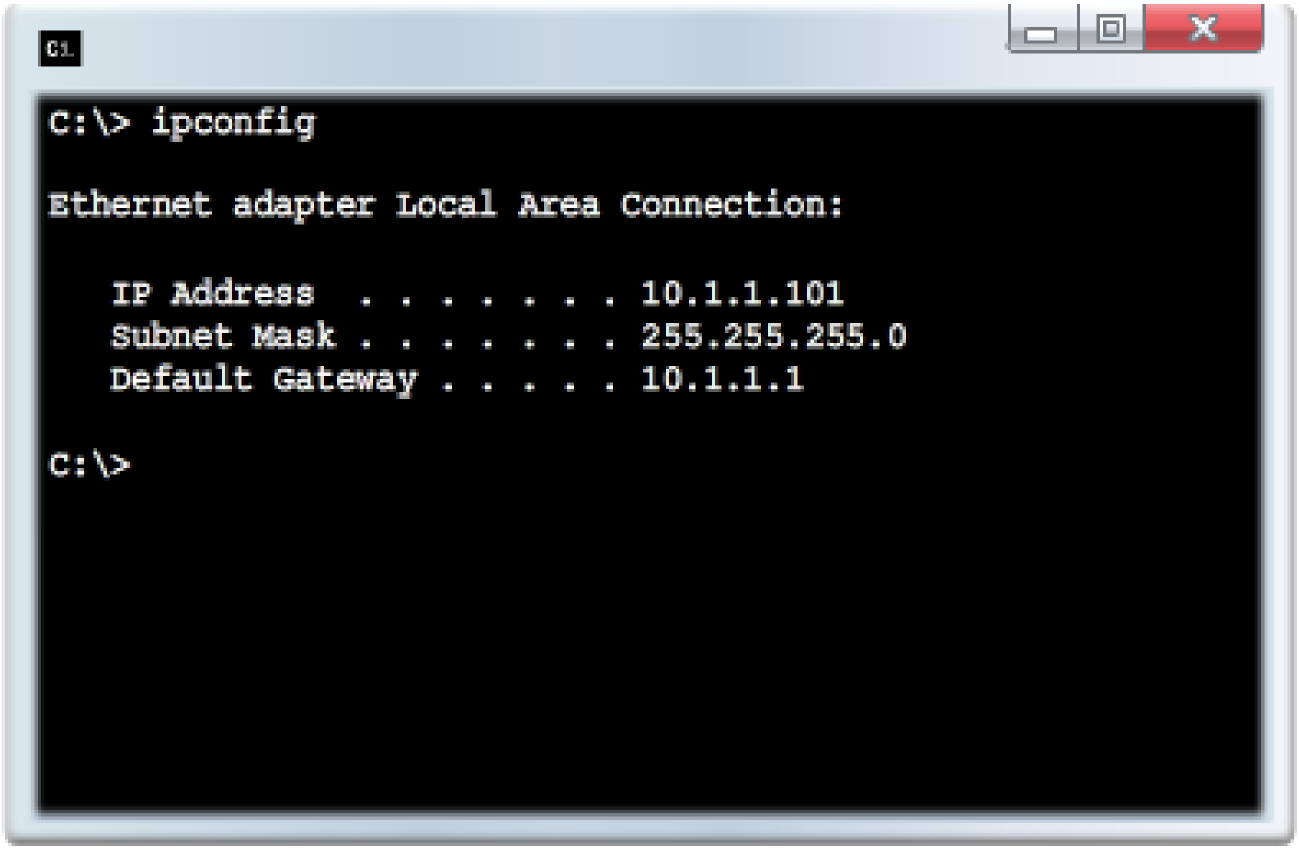
Configuring a Static IPv4 Address

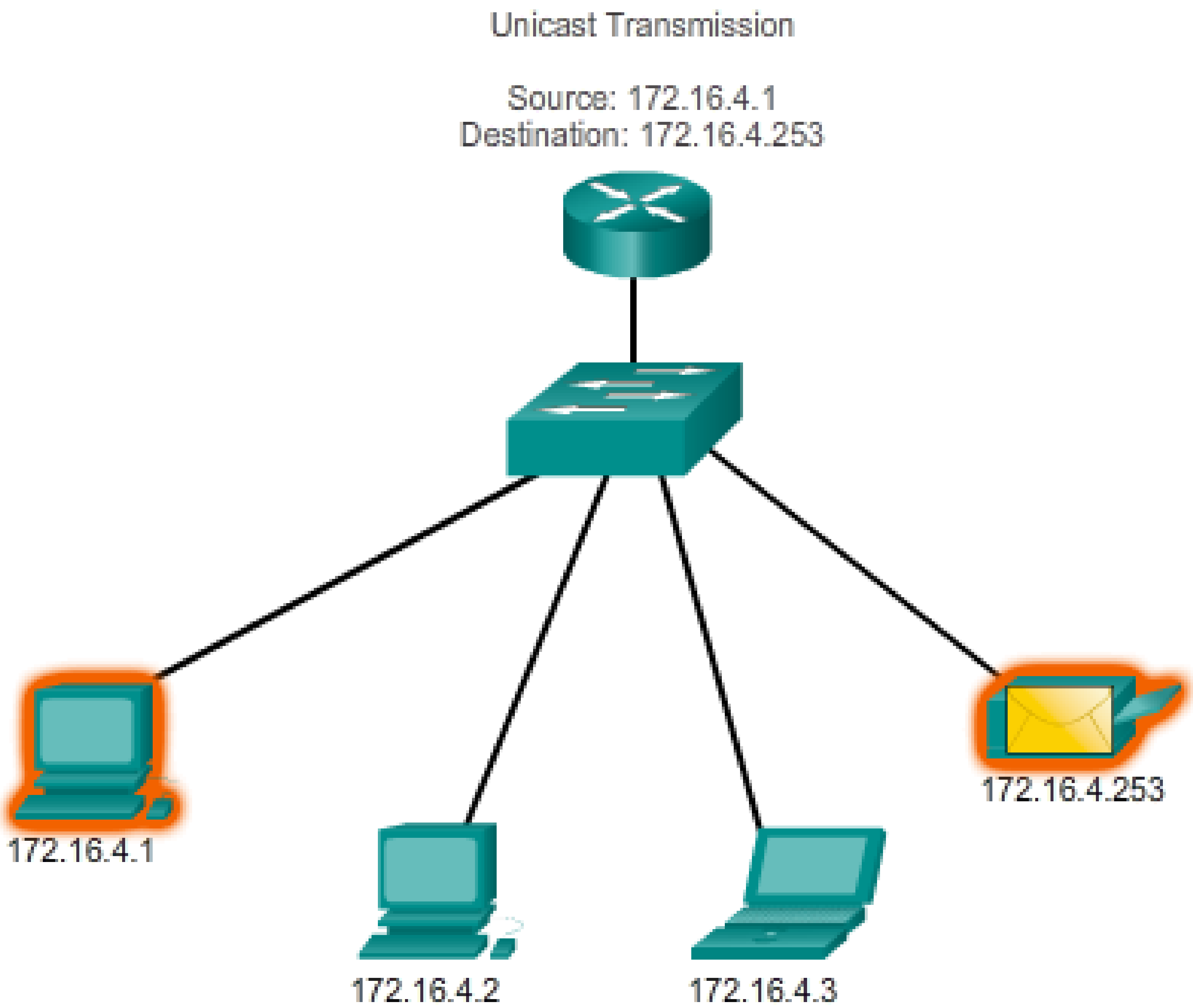


8.1.3.2 Assigning a Dynamic IPv4 Address to a Host

Assigning a Dynamic IPv4 Address



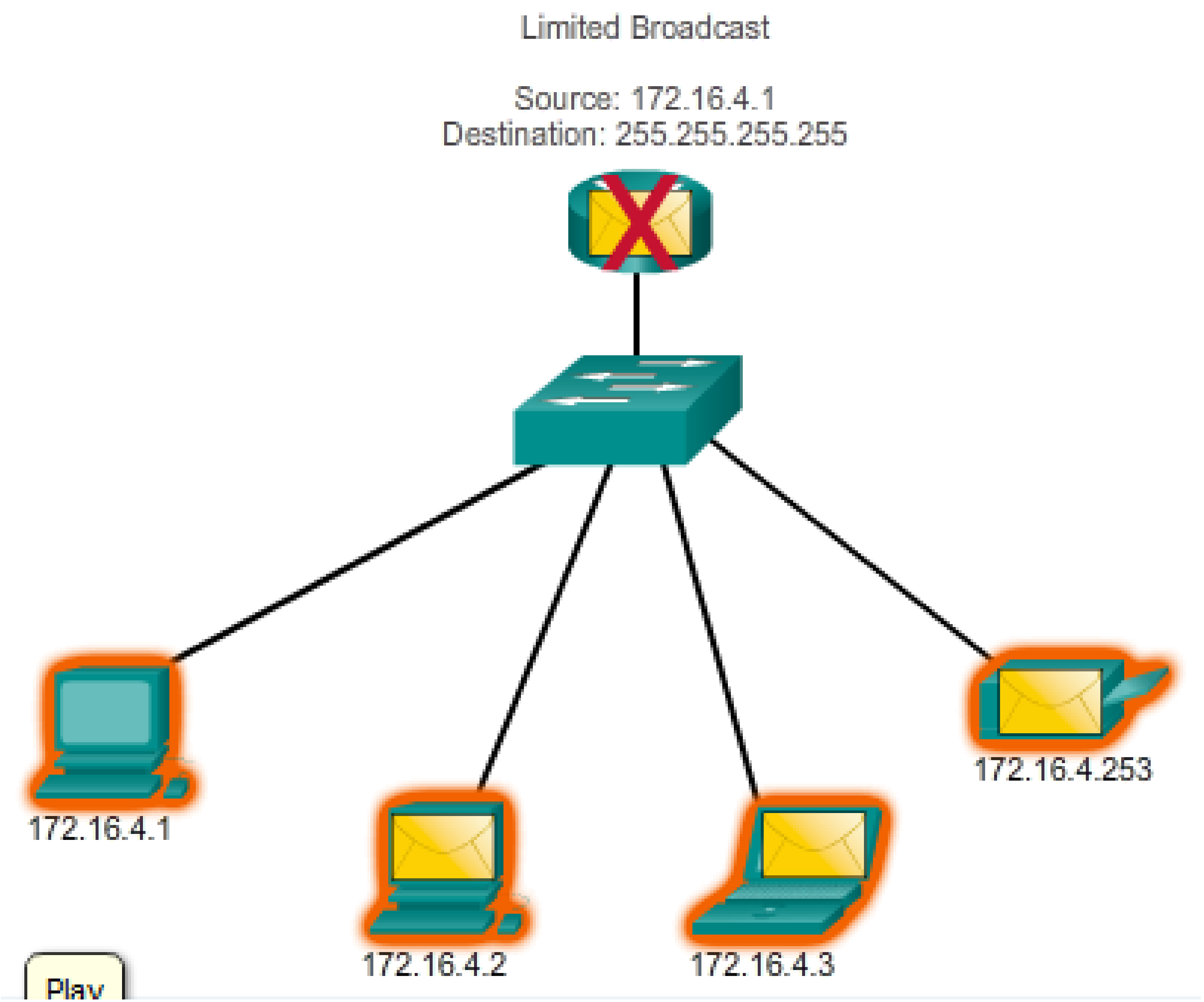




In an IPv4 network, the hosts can communicate one of three ways:

- Unicast - The process of sending a packet from one host to an individual host
- Broadcast - The process of sending a packet from one host to all hosts in the network
- Multicast - The process of sending a packet from one host to a selected group of hosts, possibly in different networks

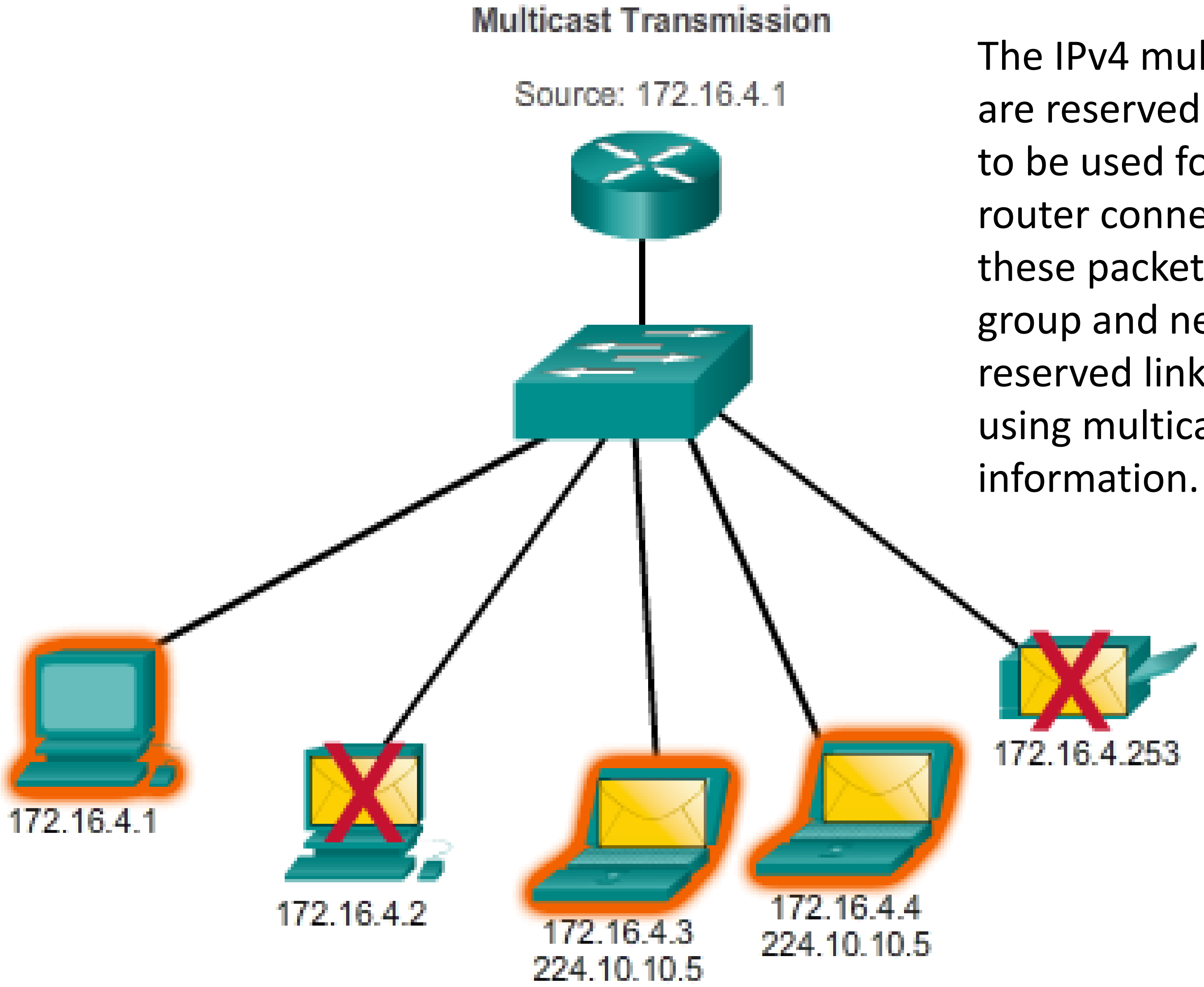
8.1.3.4 Broadcast Transmission



A directed broadcast is sent to all hosts on a specific network

The limited broadcast is used for communication that is limited to the hosts on the local network.

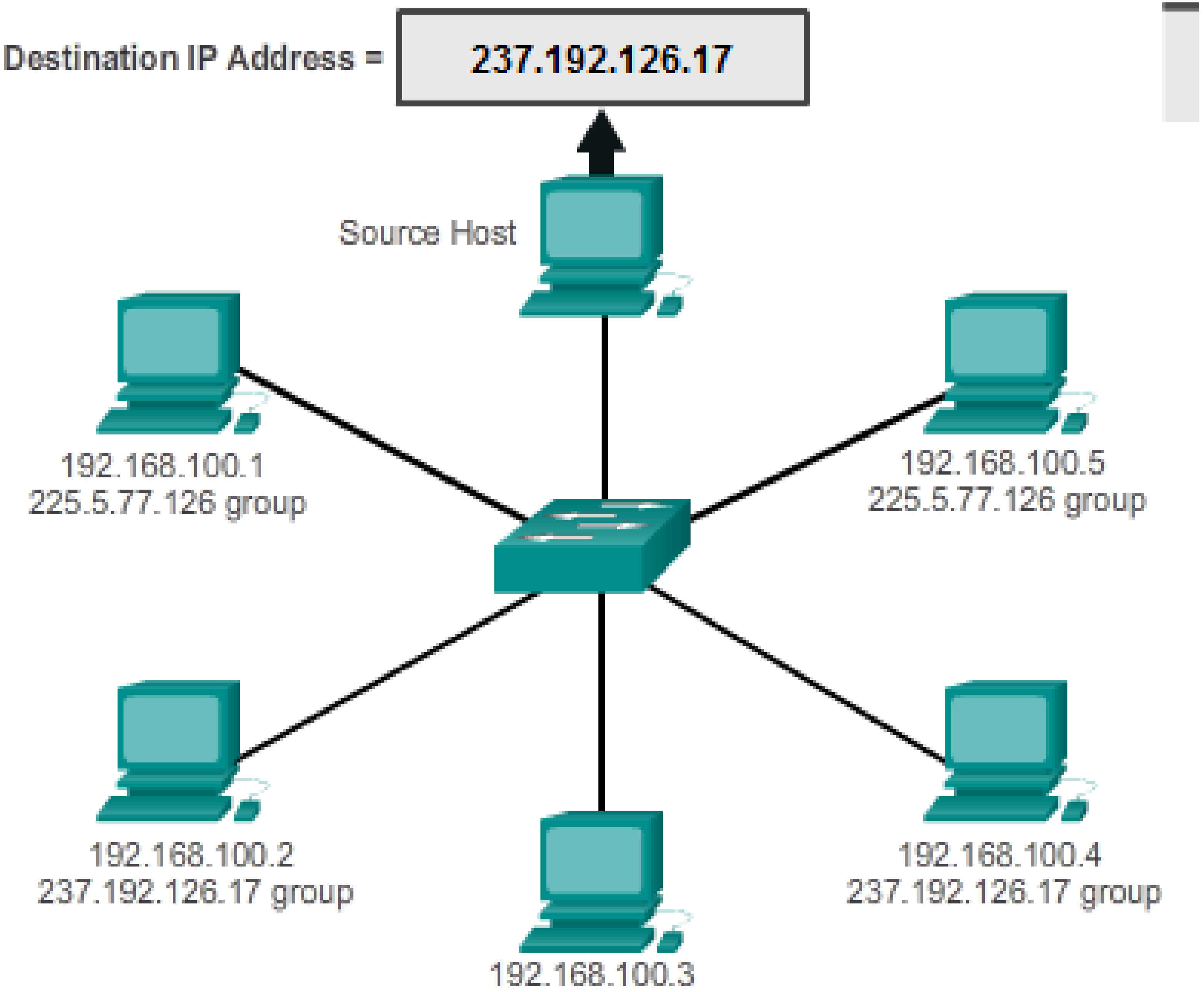
8.1.3.5 Multicast Transmission



The IPv4 multicast addresses 224.0.0.0 to 224.0.0.255 are reserved link local addresses. 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 link-local multicast group and never forwards them further. A typical use of reserved link-local addresses is in routing protocols using multicast transmission to exchange routing information.

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address and packets addressed to its uniquely allocated unicast address.

8.1.3.6 Activity - Unicast, Broadcast, or Multicast



8.1.3.7 Activity - Calculate the Network, Broadcast and Host Addresses

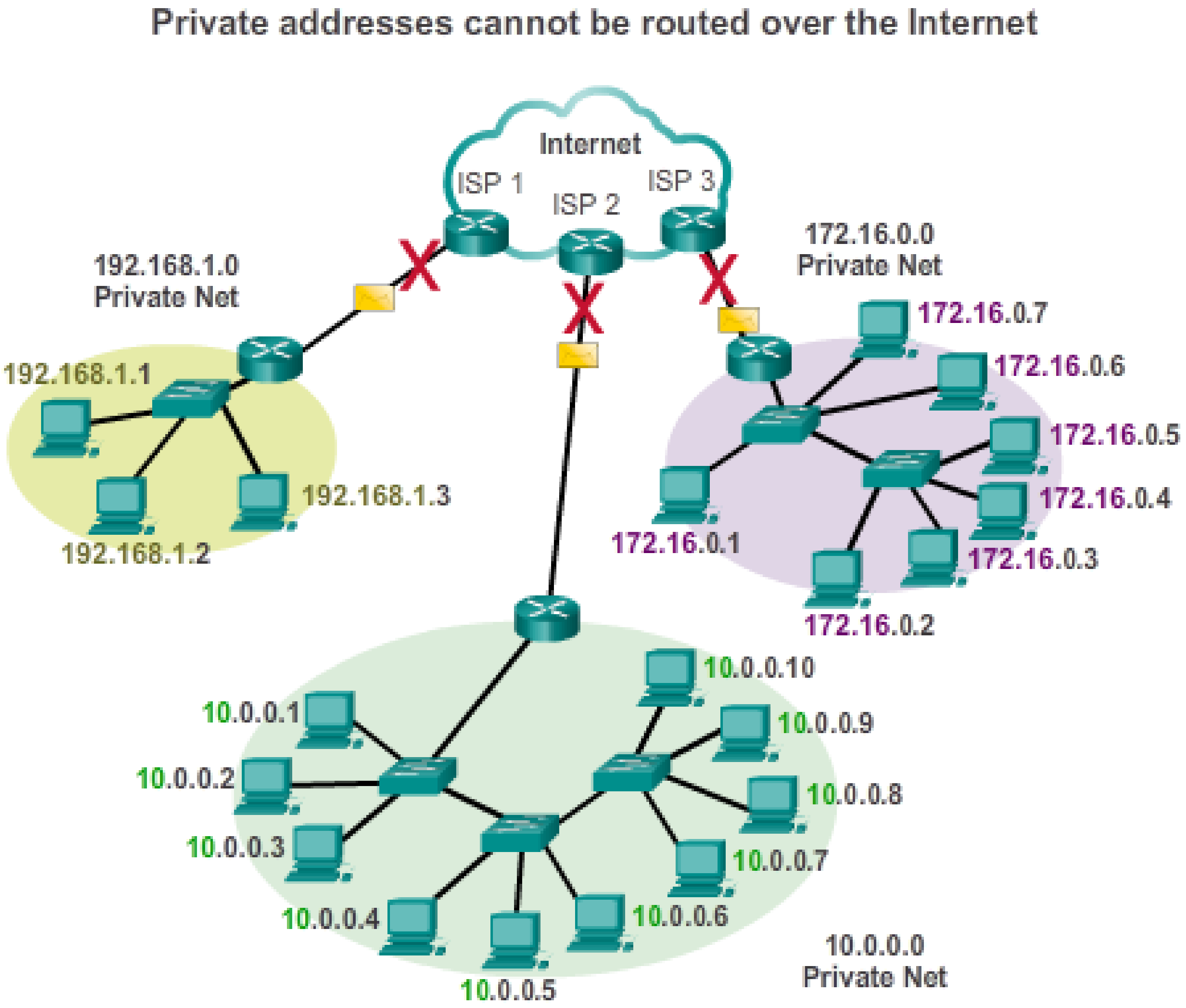
Given address/prefix of 175.217.98.235/24

Type of Address	Enter Last octet of network prefix in binary	Enter LAST octet in decimal	Enter full address in decimal
Network	00000000	0	175.217.98.0
Broadcast	11111111	255	175.217.98.255
First Usable Host Address	00000001	1	175.217.98.1
Last Usable Host Address	11111110	254	175.217.98.254

Check | Reset | New Values | Show Me

8.1.3.8 Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic

8.1.4.1 Public and Private IPv4 Addresses



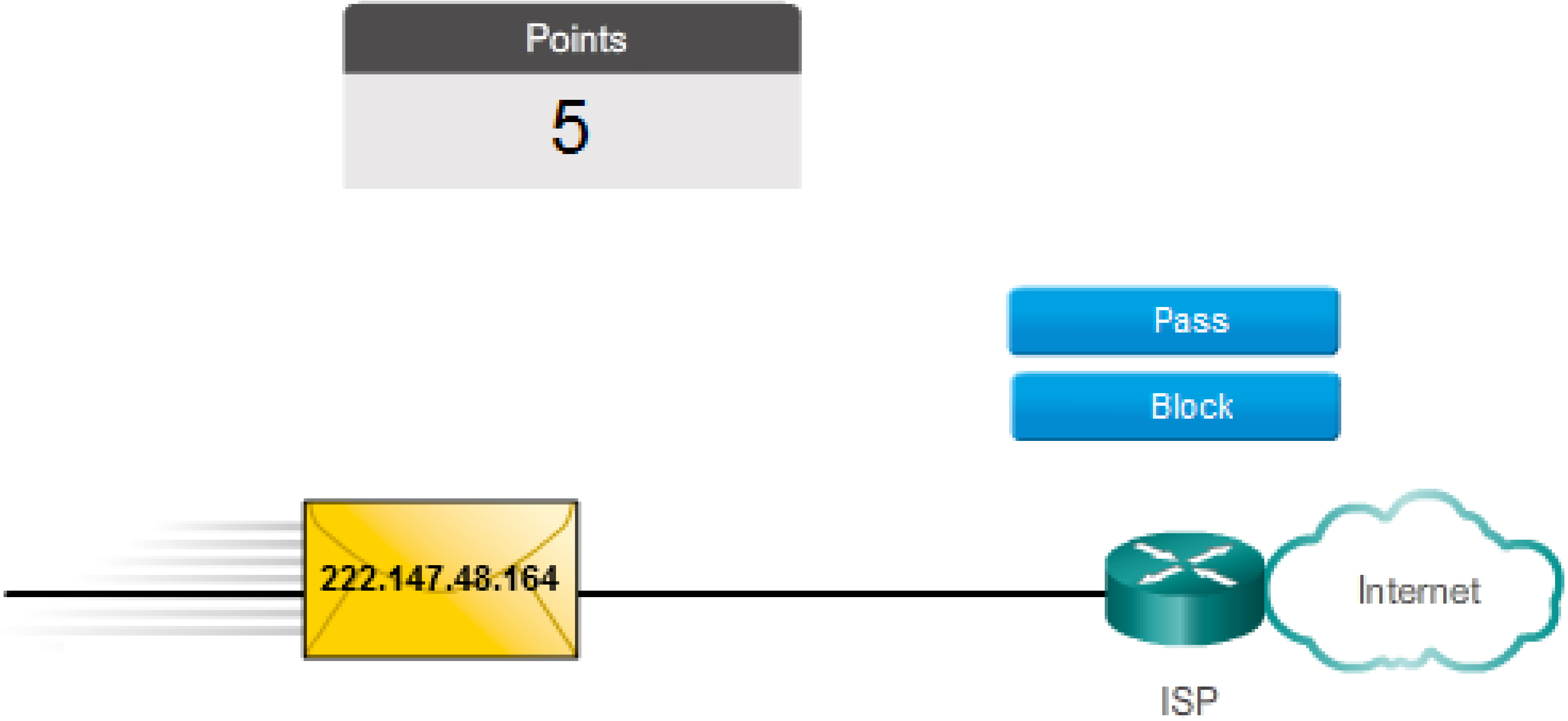
The private address blocks are:

10.0.0.0 to 10.255.255.255
(10.0.0.0/8)

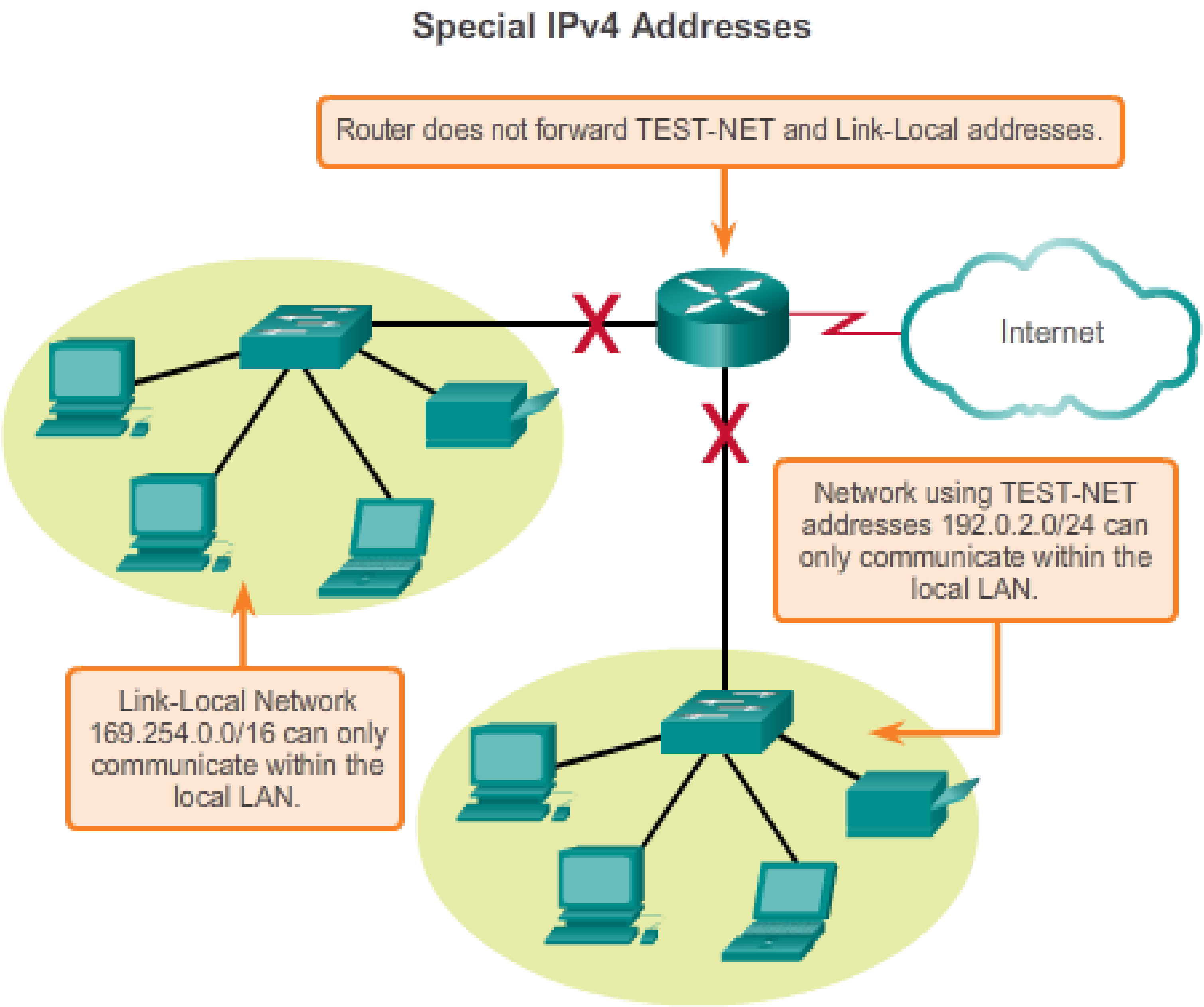
172.16.0.0 to 172.31.255.255
(172.16.0.0/12)

192.168.0.0 to 192.168.255.255
(192.168.0.0/16)

8.1.4.2 Activity - Pass or Block IPv4 Addresses



8.1.4.3 Special Use IPv4 Addresses



Network and Broadcast Addresses

- **Loopback**
- **Link-Local Addresses**
- **TEST-NET Addresses**
- **Experimental Addresses**

8.1.4.4 Legacy Classful Addressing

IP Address Classes

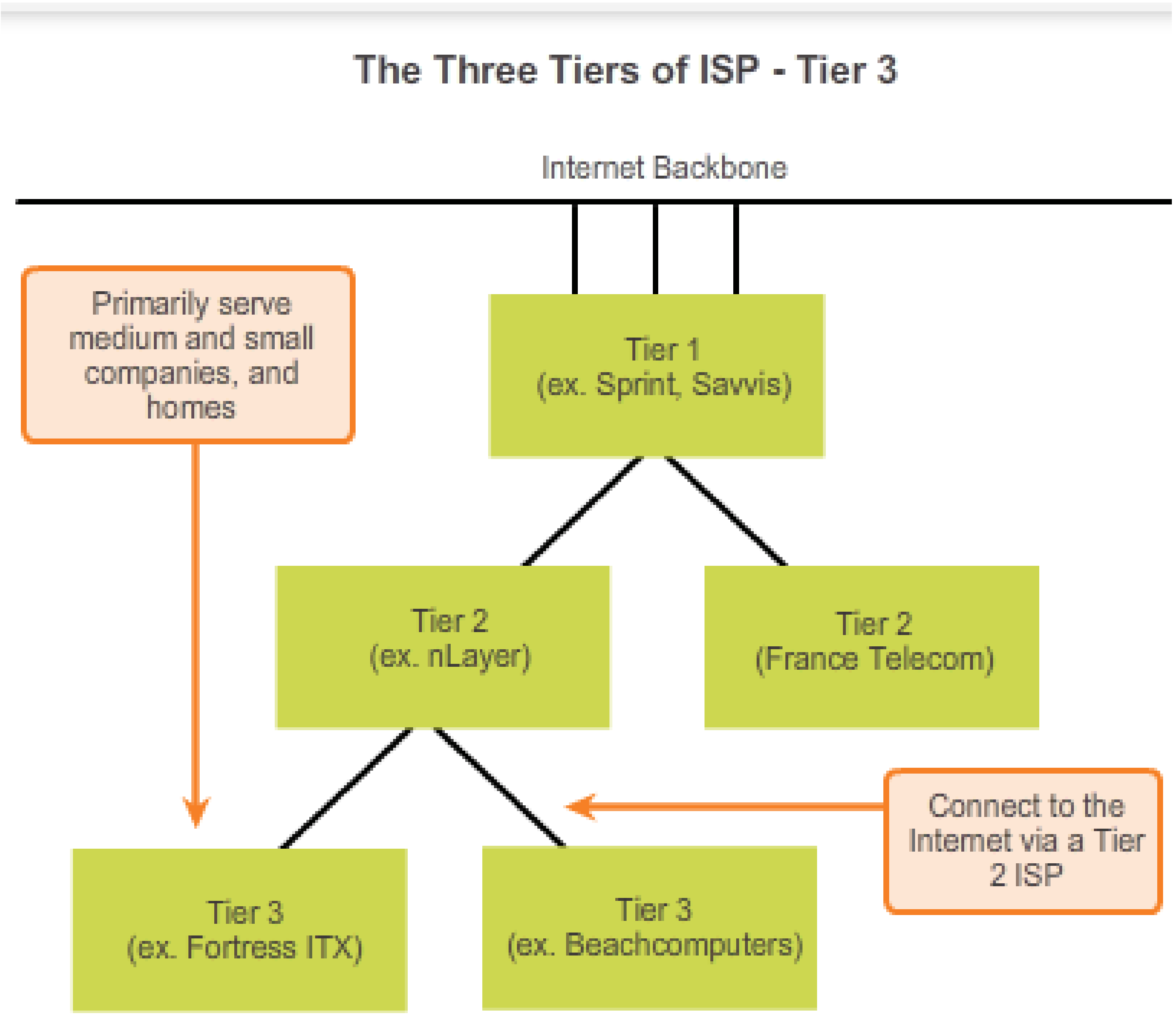
Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network (N) and Host (H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,152 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

Note: All zeros (0) and all ones (1) are invalid hosts addresses.

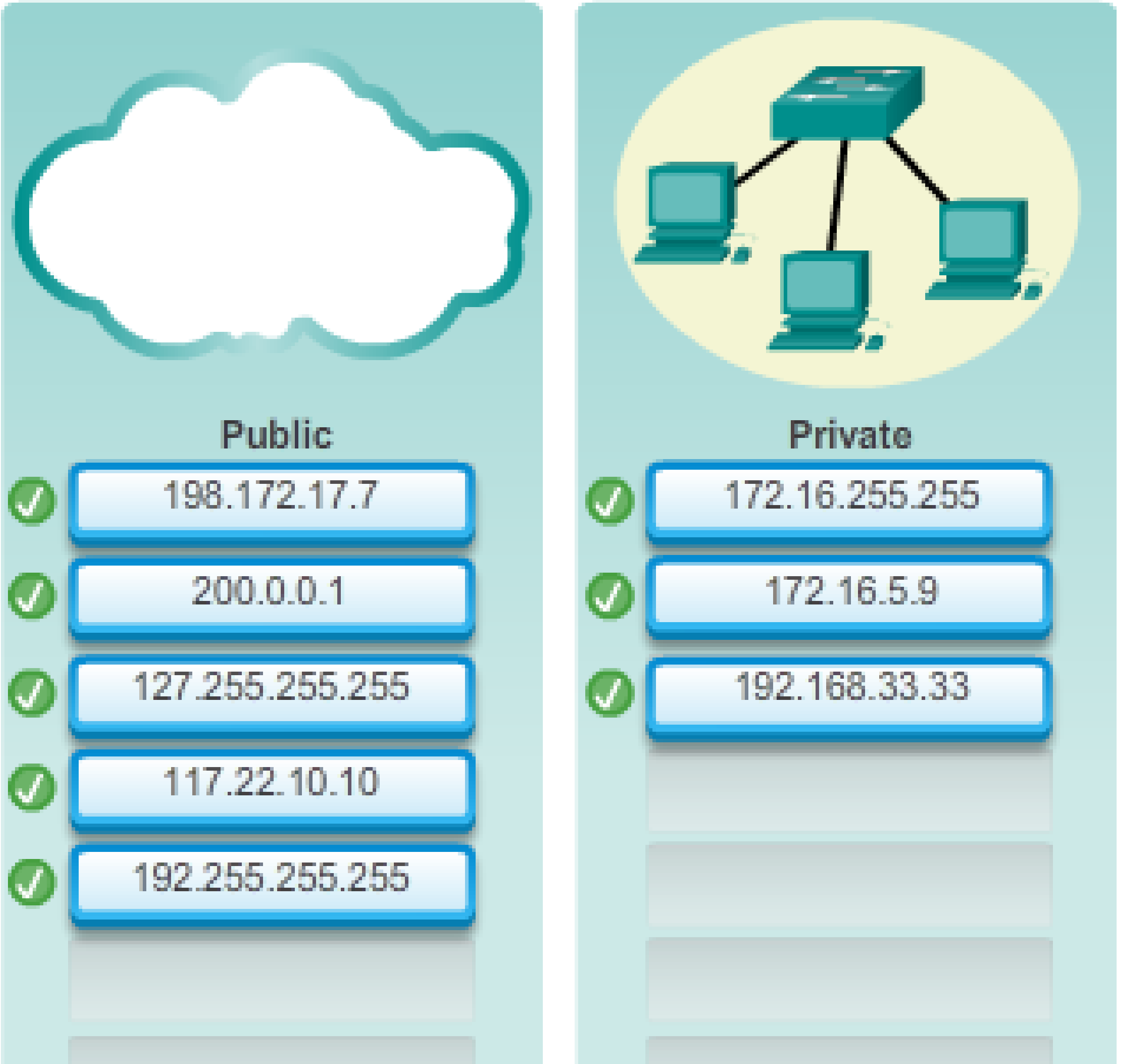
8.1.4.5 Assignment of IP Addresses

Assignment of IP Addresses

8.1.4.6 Assignment of IP Addresses (Cont.)



8.1.4.7 Activity - Public or Private IPv4 Addresses



8.1.4.8 Lab - Identifying IPv4 Addresses

Hex Lab

Base 16 (Hexadecimal) System

Place Value	____ ____ ____ ____ 4096's 256's 16's 1's
$Base^{Exponent}$	$16^3 = 4096$ $16^2 = 256$ $16^1 = 16$ $16^0 = 1$
Number of Symbols	16
Symbols	0, 1, 2, 3, 4, 5, 6, 7, 8, 9 A(=10), B(=11), C(=12), D(=13), E(=14), F(=15)
Rationale	Useful for computer engineering and programming purposes.

Decimal - Binary - Hexadecimal Table

Decimal	Binary	Hexadecimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

Binary and Hexadecimal System

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

Only need 4 Hex positions:

4096 256 16 1

Converting Binary to Hexadecimal

Converting Binary Number to Hexadecimal Number

10010010001011111011111011100100 1

Converts to:

0001 0010 0100 0101 1111 0111 1101 1100 1001

Converts to:

1 2 4 5 F 7 D C 9

So:

100100100010111110111110111001001 binary

= 1245F7DC9 hexadecimal

Converting Hexadecimal Number to Binary Number

0x2102

Converts to:

2	1	0	2
0010	0001	0000	0010

So:

2102 hexadecimal converts to: 0010 0001 0000 0010 binary

Convert hex 3F4B to a Decimal

(Work right to left)

3*	4096	=12288
F*	256	=3840
4*	16	=64
B*	1	=11
		=16203

Example:

4F6A =

(4 x 16^3)

+ (F[15] x 16^2)

+ (6 x 16^1)

+ (A[10] x 16^0)

= 20330 (decimal)

____ ____ ____ ____

4096's 256's 16's 1's

$16^3 = 4096$

$16^2 = 256$

$16^1 = 16$

$16^0 = 1$

Convert the decimal number 24032 to hex.

24032/16= 1502, with a remainder of 0

1502/16=93, with a remainder of 14 or E

93/16=5, with a remainder of 13 or D

5/16=0, with a remainder of 5

By collecting all the remainders backward, you have the hex number 5DE0.

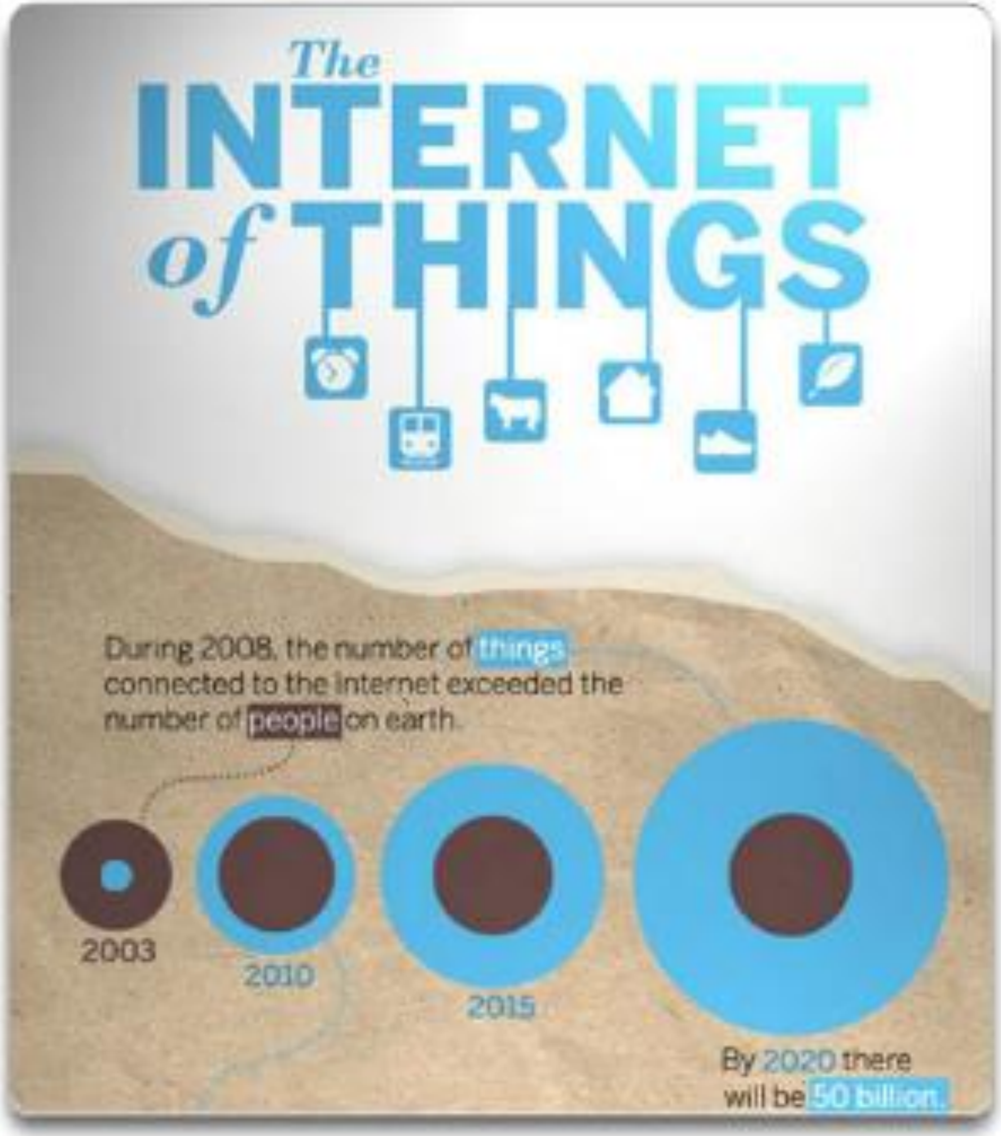
Dec	Bin	Hex
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	01
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

$15*16^1$ =240
$15*16^0$ =15

= 255

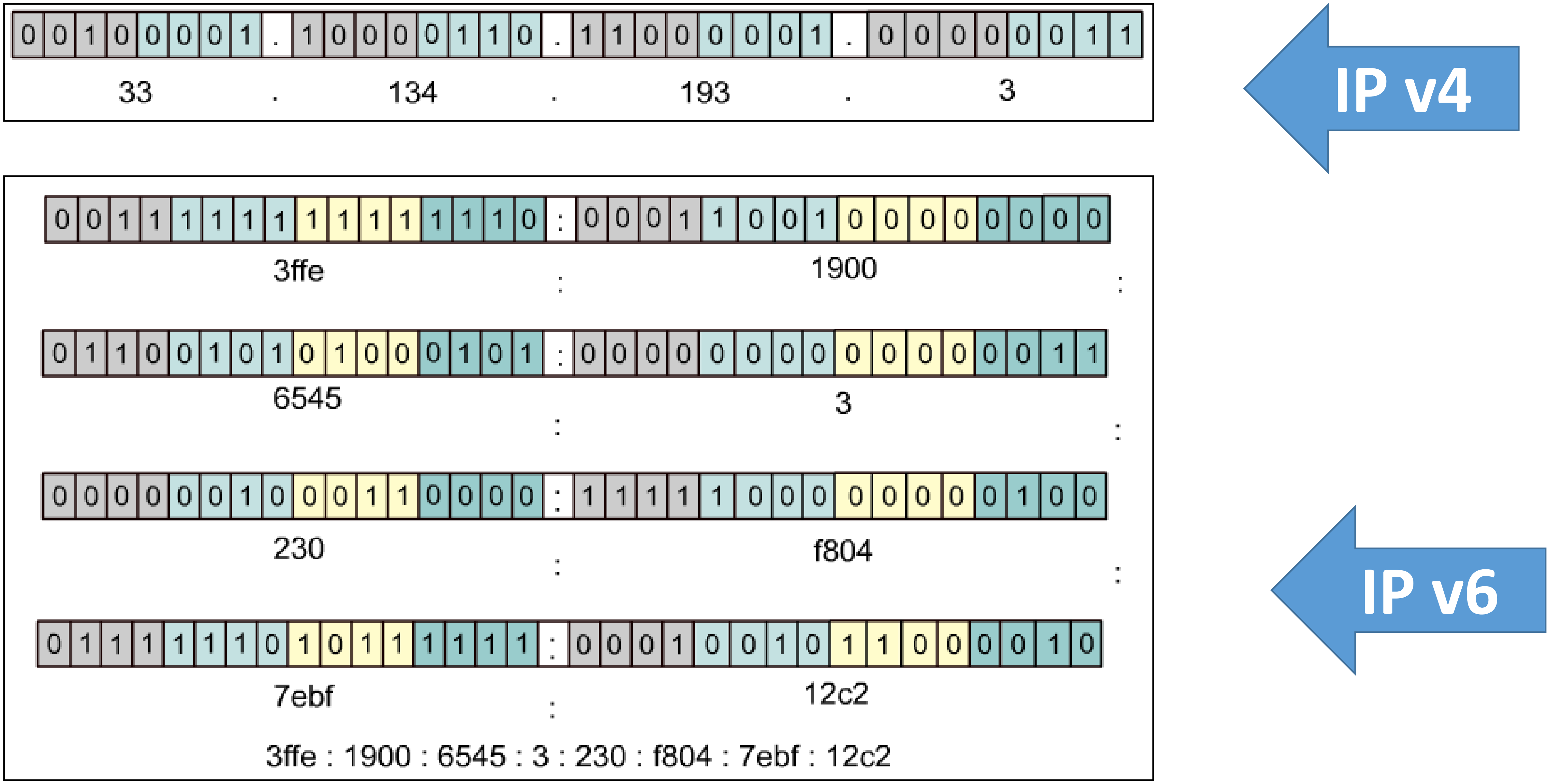
IPv6

8.2.1.1 The Need for IPv6

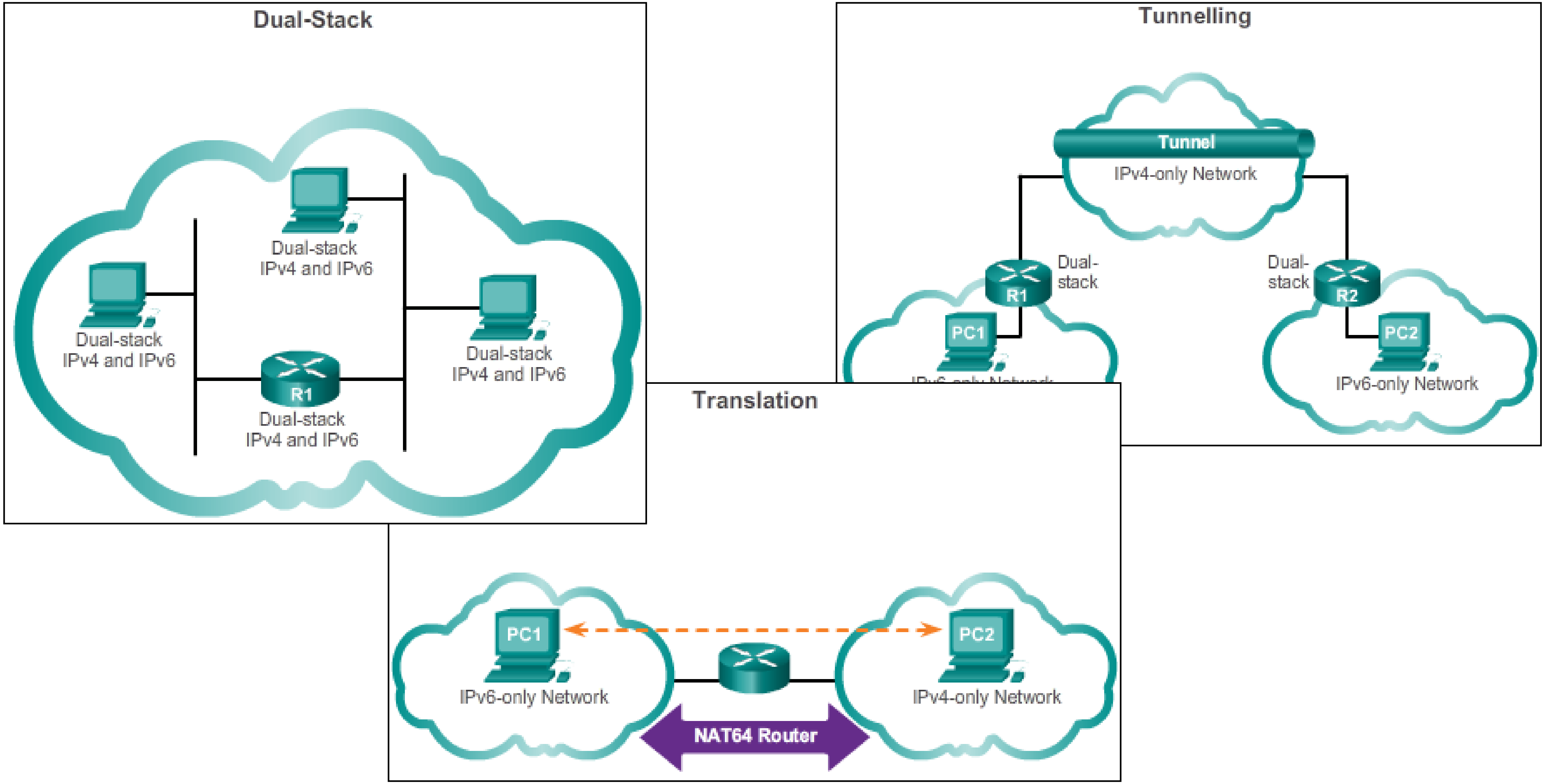


To view this infographic in its entirety, go to:
http://share.cisco.com/internet-of-things.html

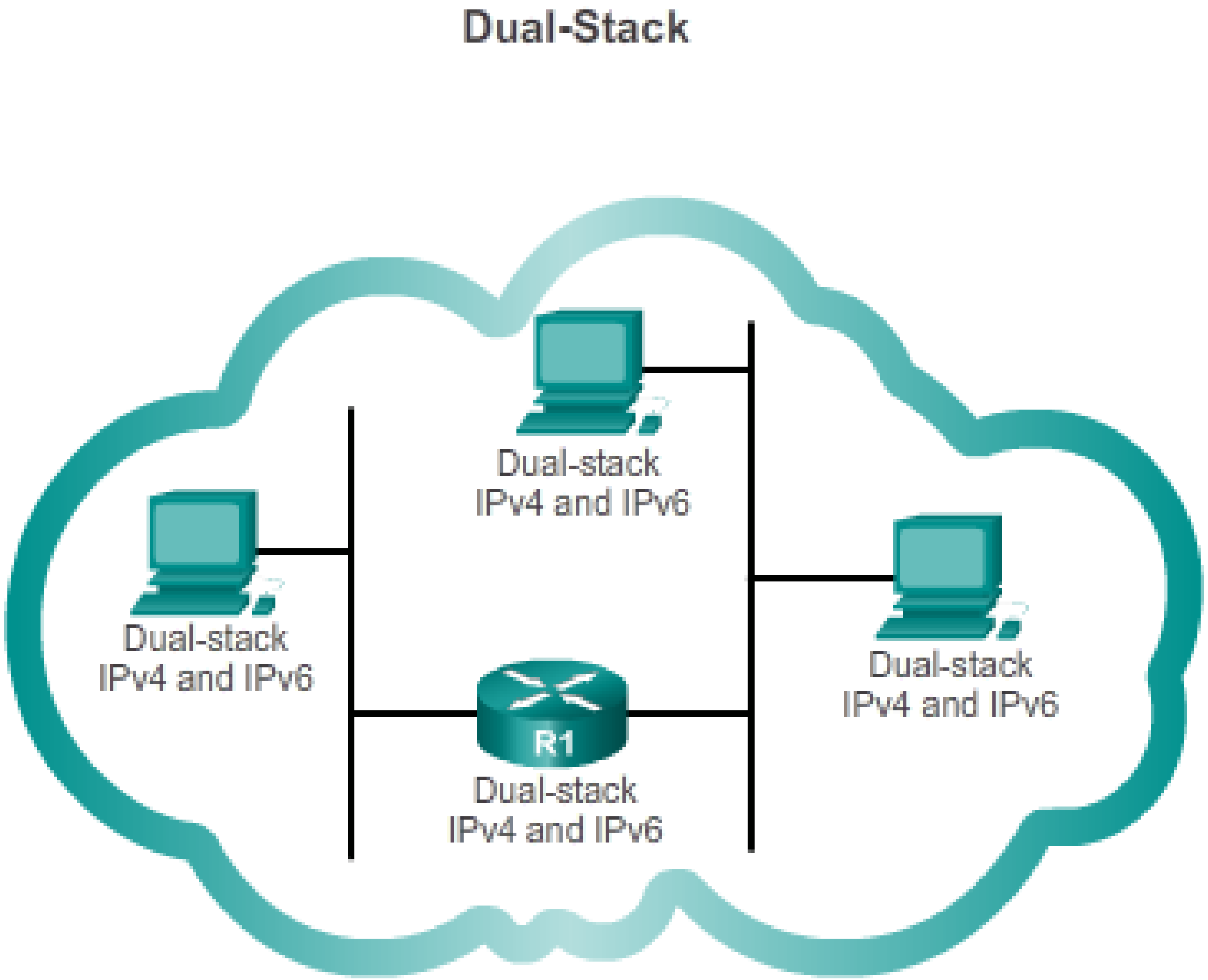
8.2.1.1 The Need for IPv6



8.2.1.2 IPv4 and IPv6 Coexistence

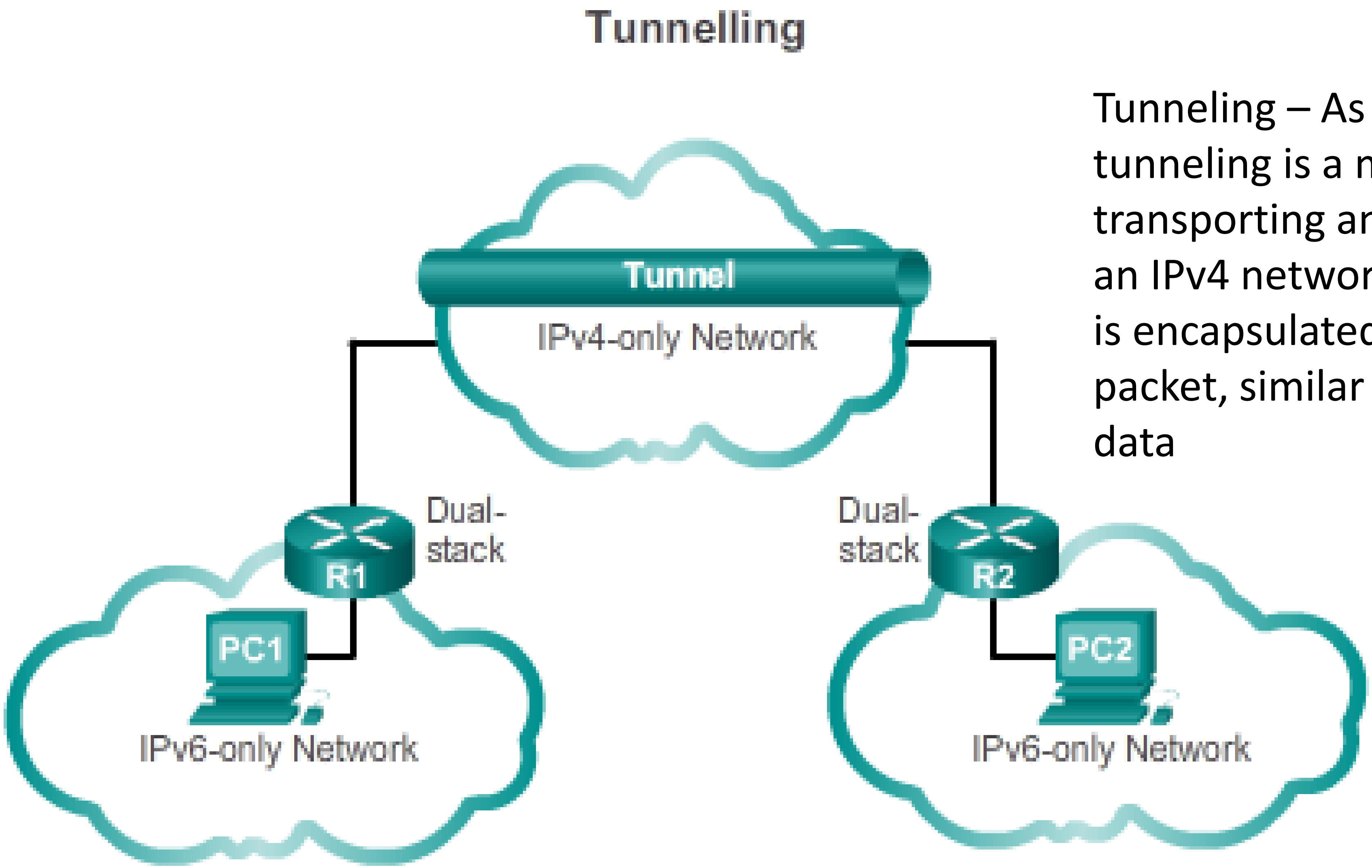


8.2.1.2 IPv4 and IPv6 Coexistence



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

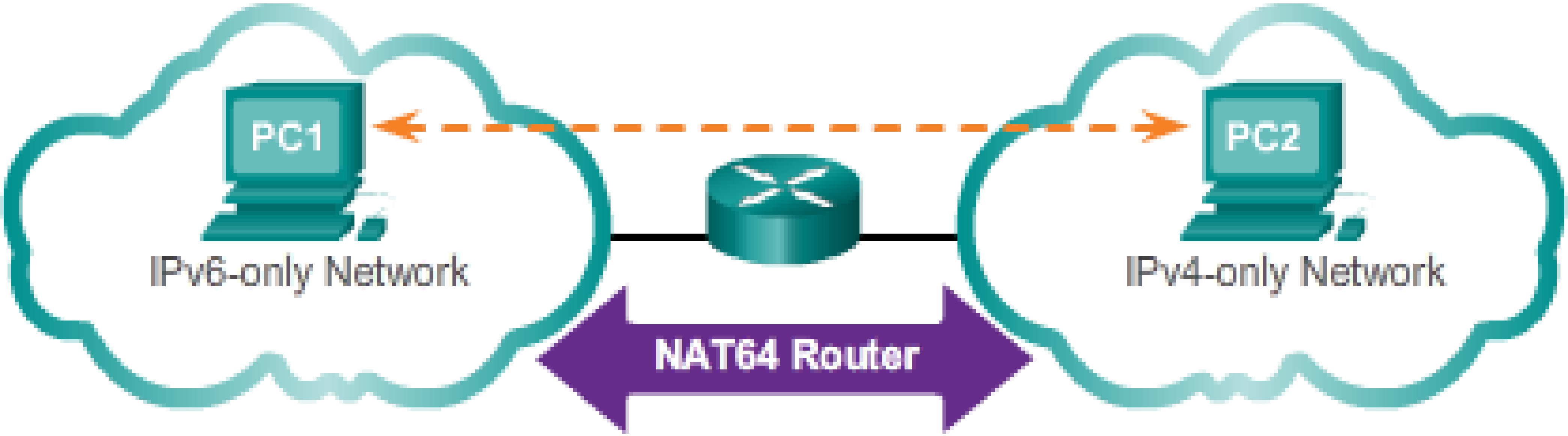
8.2.1.2 IPv4 and IPv6 Coexistence



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.



8.2.1.3 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	Allows NAT to be used in both IPv6 and IPv4 networks.
Dual Stack	Allows IPv4 and IPv6 to coexist on the same network.

8.2.2.1 Hexadecimal Number System

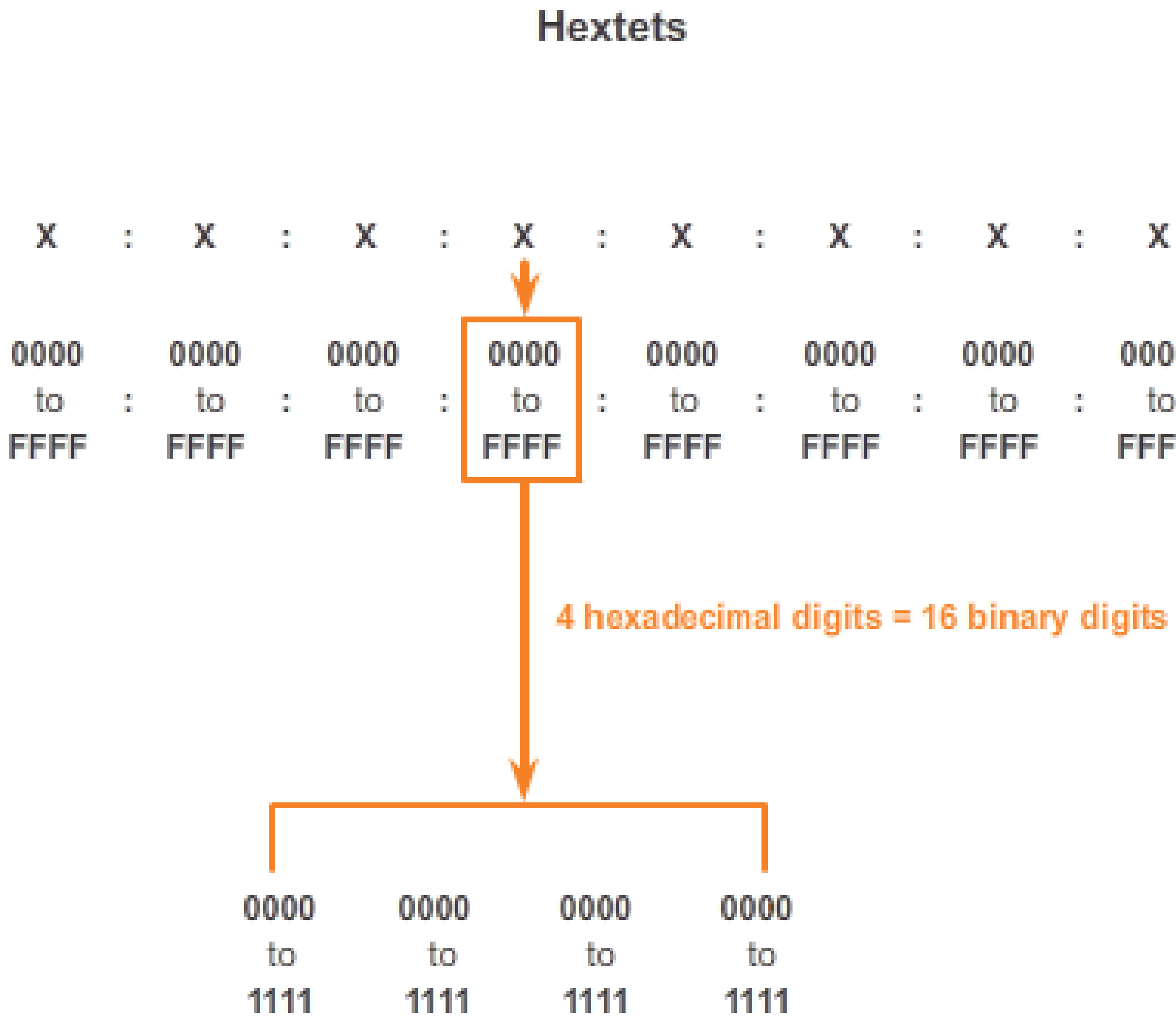
Representing Hexadecimal Values

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

Hexadecimal Conversions of Binary Octets

Hexadecimal	Decimal	Binary
00	0	0000 0000
01	1	0000 0001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
0A	10	0000 1010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	1000 0000
C0	192	1100 0000
CA	202	1100 1010
F0	240	1111 0000
FF	255	1111 1111

8.2.2.2 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.

IPv6 addresses are not case sensitive and can be written in either lowercase or uppercase.

8.2.2.2 IPv6 Address Representation

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

8.2.2.3 Rule 1 - Omitting Leading 0s

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

The first rule to help reduce the notation of IPv6 addresses is any leading 0s (zeros) in any 16-bit section or hextet can be omitted. 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”.

8.2.2.4 Rule 2 - Omitting All 0 Segments

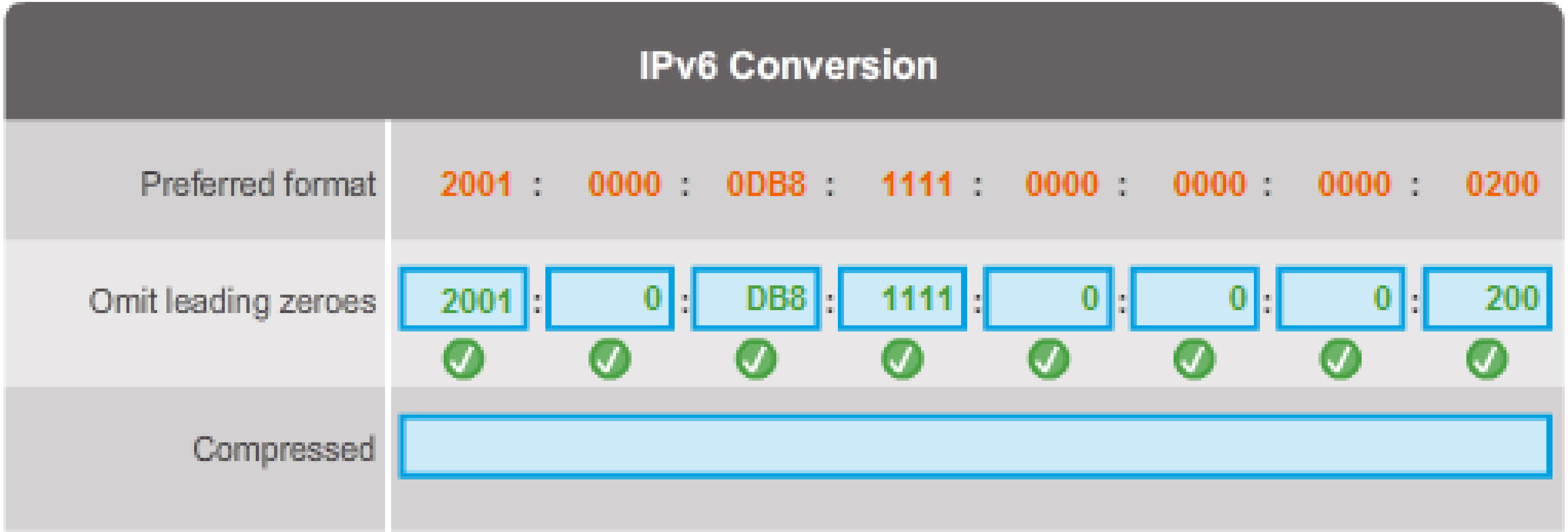
Preferred	FF02:0000:0000:0000:0000:0001:FF00:0200
No leading 0s	FF02: 0: 0: 0: 0: 1:FF00: 200
Compressed	FF02::1:FF00:200

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

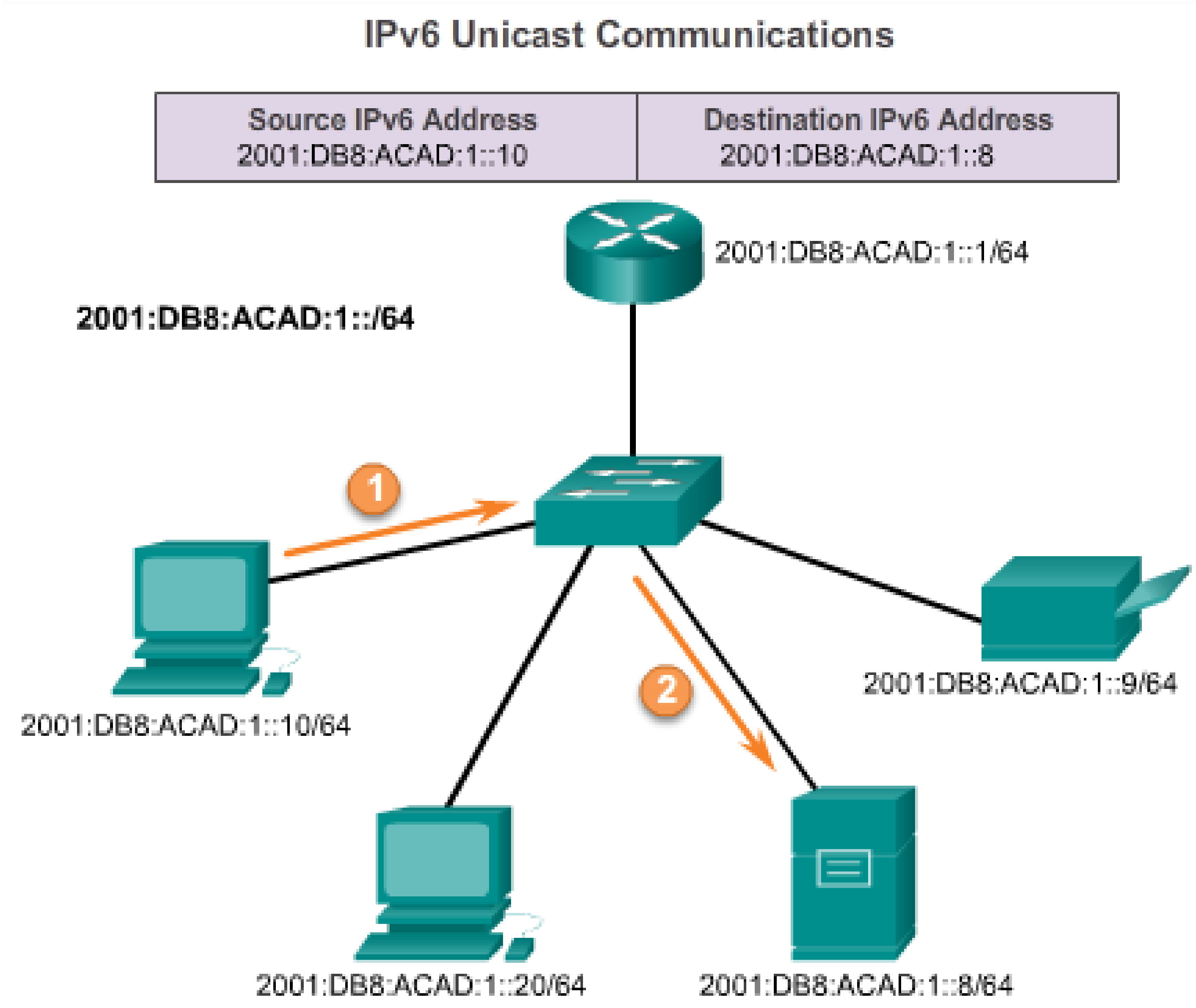
The second rule to help reduce the notation of IPv6 addresses is that a double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s.

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.

8.2.2.5 Activity - Practicing IPv6 Address Representations



8.2.3.1 IPv6 Address Types

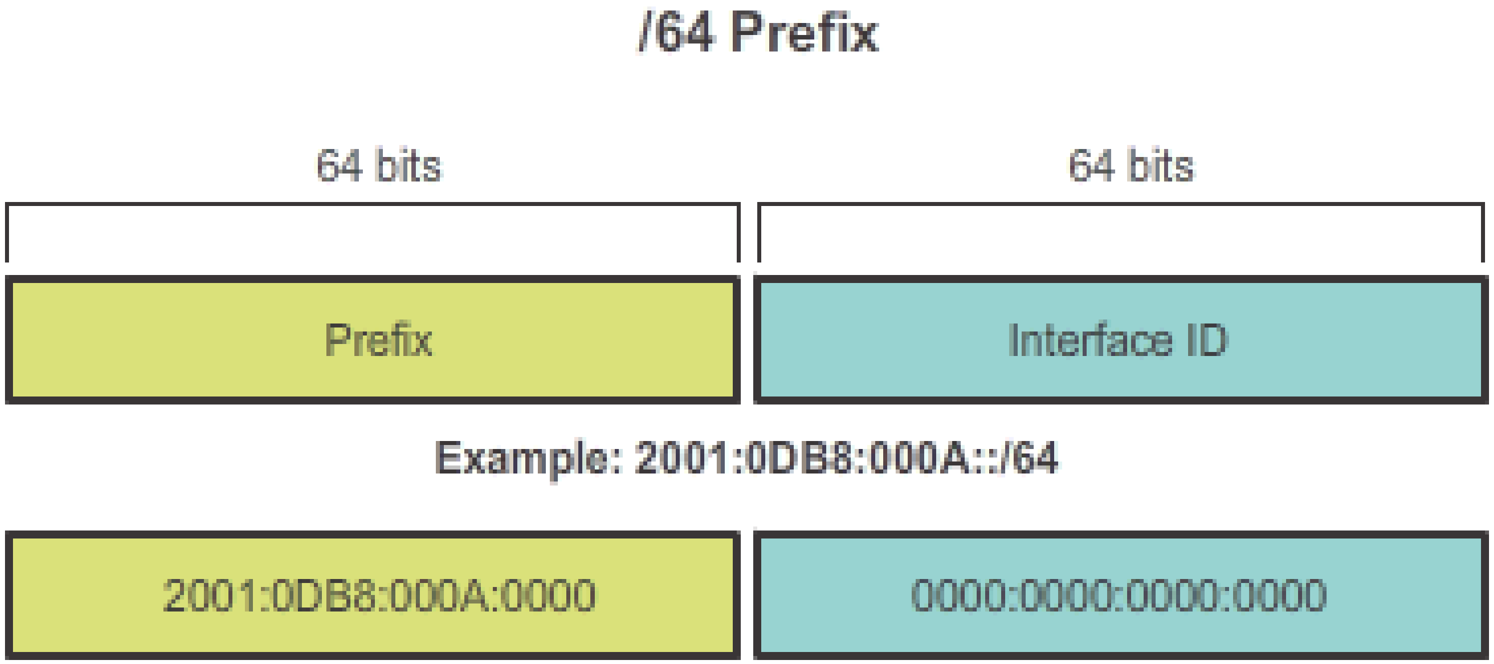


There are three types of IPv6 addresses:

- **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.

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

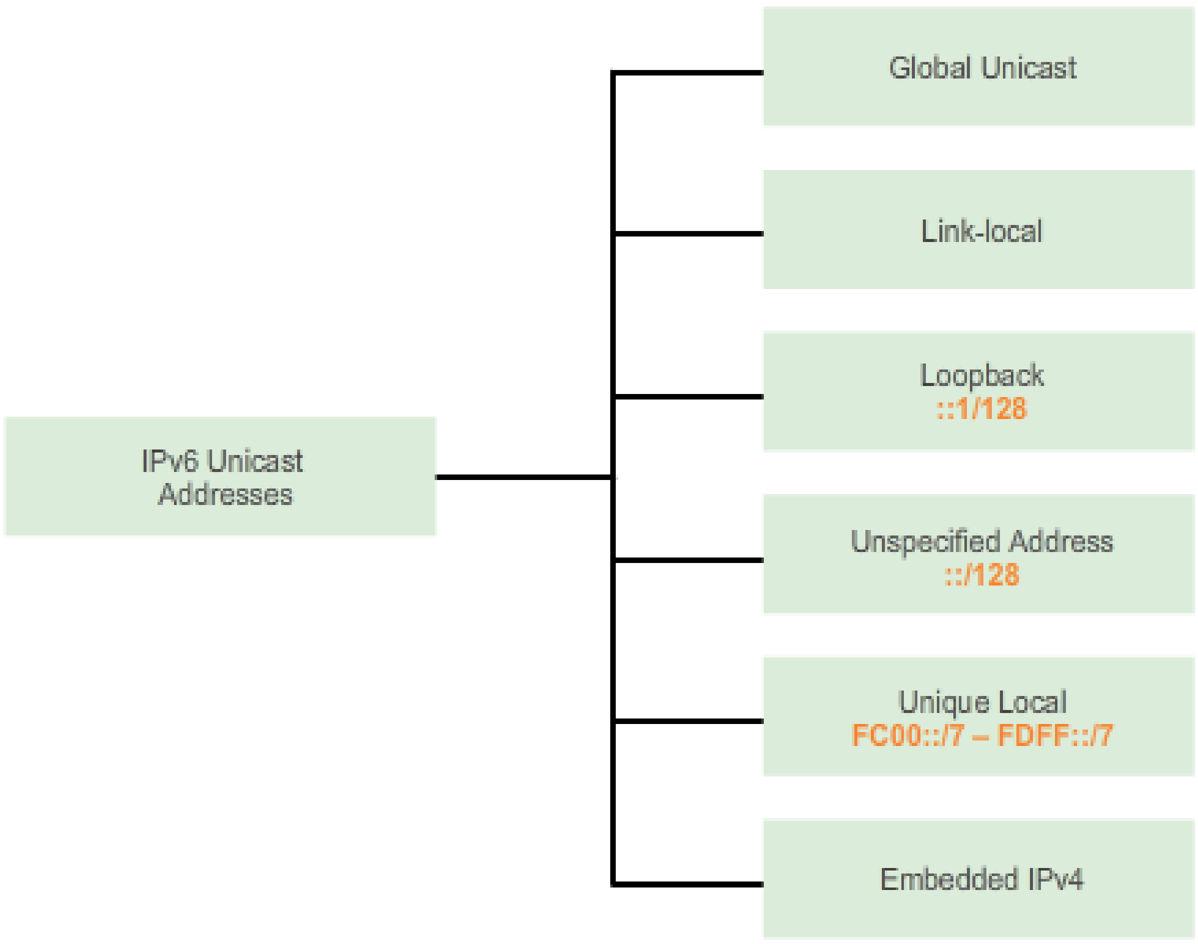
8.2.3.2 IPv6 Prefix Length



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.

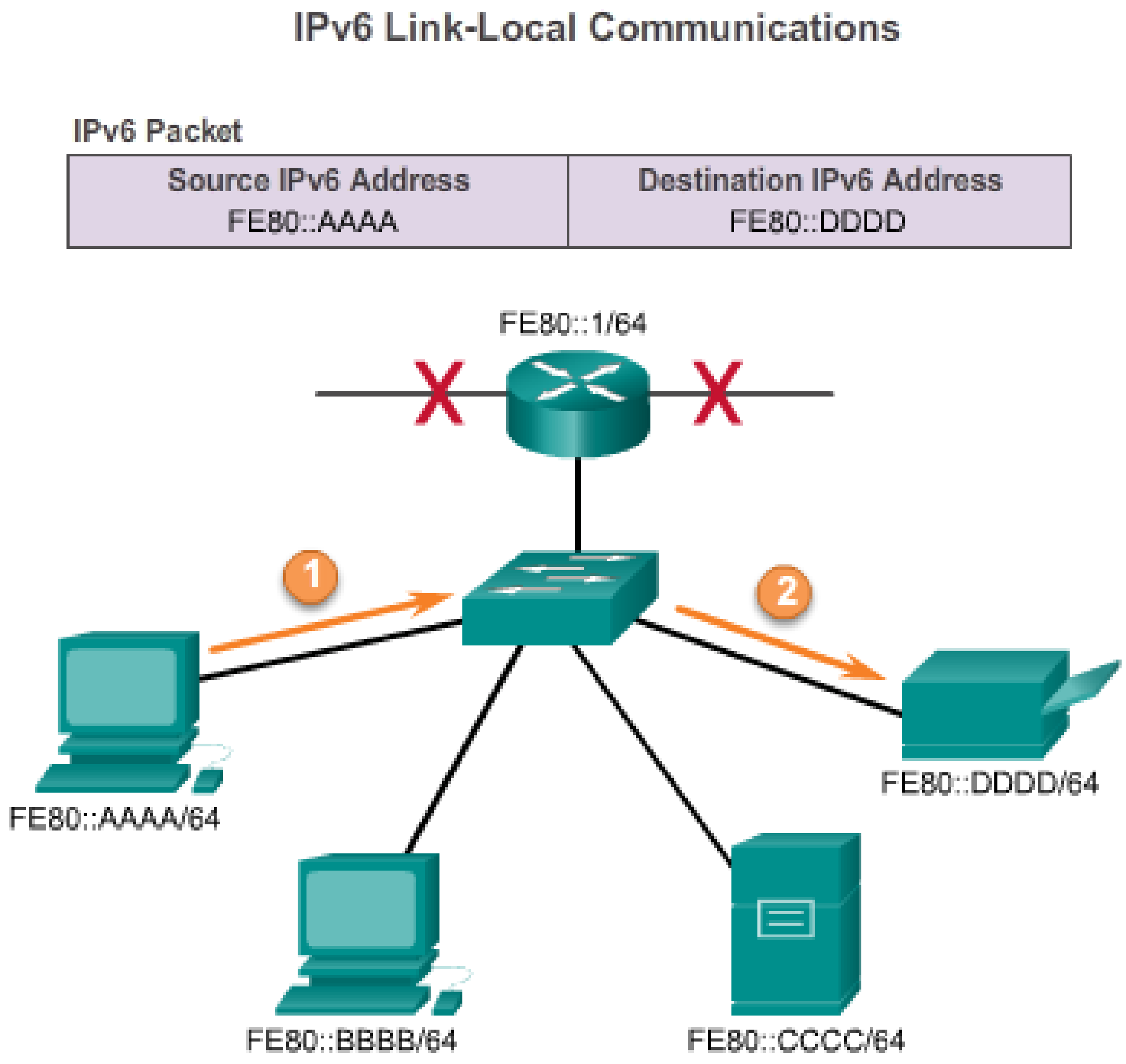
The prefix length can range from 0 to 128. A typical IPv6 prefix length for LANs and most other types of networks is /64. This means the prefix or network portion of the address is 64 bits in length, leaving another 64 bits for the interface ID (host portion) of the address.

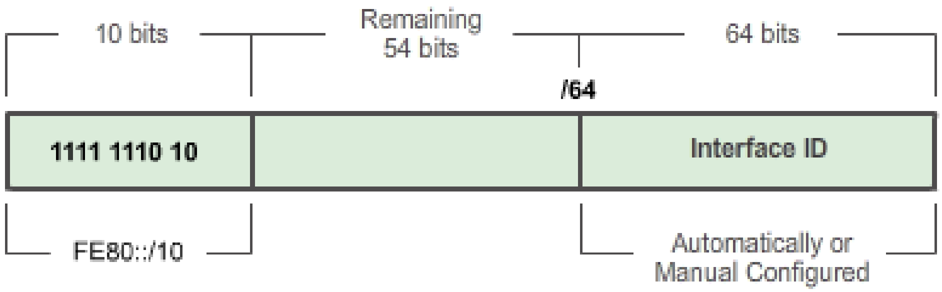
8.2.3.3 IPv6 Unicast Addresses



- A **global unicast** address is similar to a public IPv4 address. These are globally unique, Internet routable addresses
- **Link-local** addresses are used to communicate with other devices on the same local link.
- The **IPv6 loopback** address is all-0s except for the last bit, represented as ::1/128 or just ::1 in the compressed format.
- An **unspecified address is an all-0s address represented** in the compressed format as ::/128 or just :: in the compressed format. It cannot be assigned to an interface and is only be used as a source address in an IPv6 packet
- **Unique local addresses** are used for local addressing within a site or between a limited number of sites
- **the IPv4 embedded address**. These addresses are used to help transition from IPv4 to IPv6. IPv4 embedded addresses are beyond the scope of this course.

8.2.3.4 IPv6 Link-Local Unicast Addresses





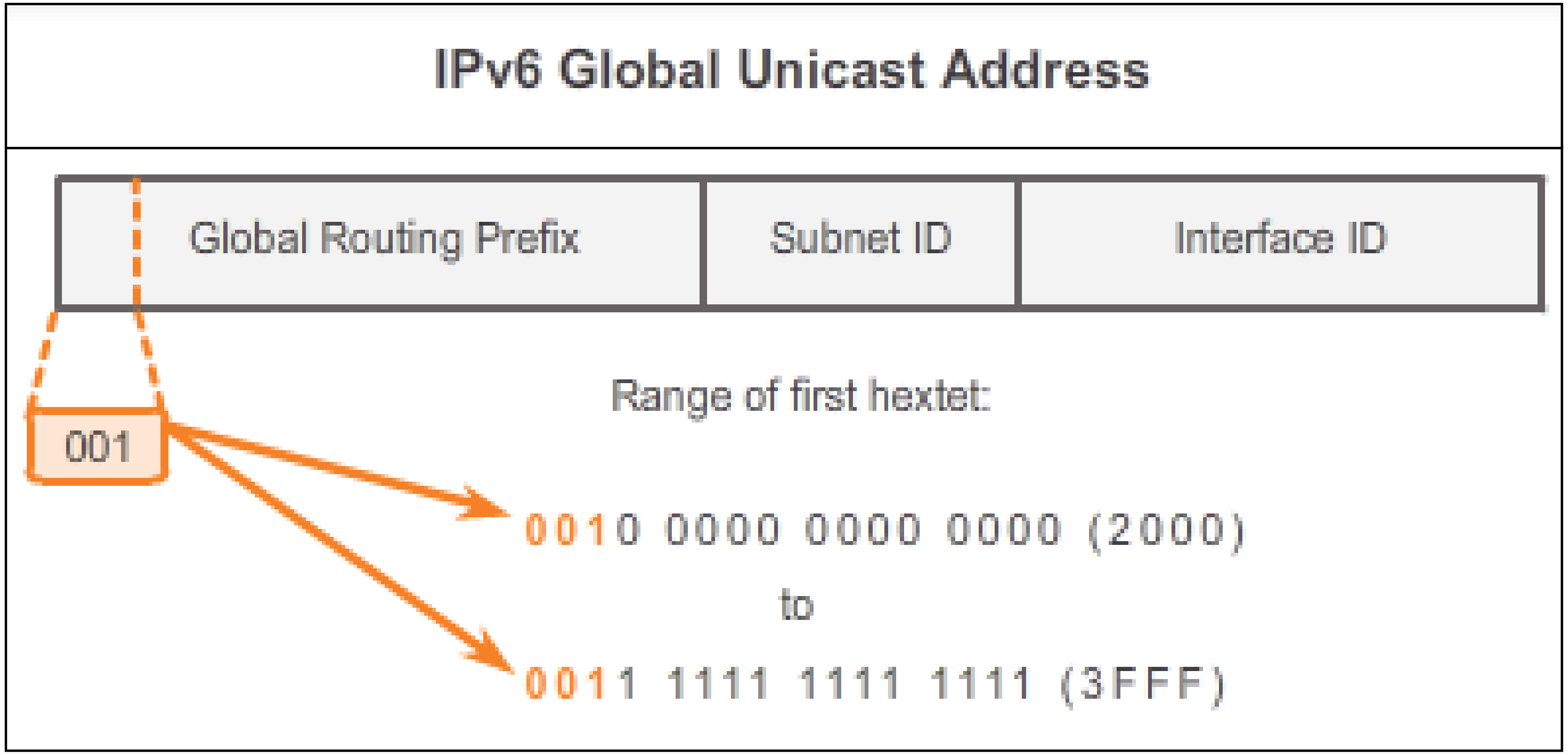
An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.

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).

8.2.3.5 Activity - Identify Types of IPv6 Addresses

Global unicast	Unique, Internet-routable IPv6 address (dynamic or static)
Loopback	IPv6 address represented as ::1 (compressed format)
Unspecified	IPv6 address represented as :: (compressed format) – cannot be assigned to an interface
/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

8.2.4.1 Structure of an IPv6 Global Unicast Address



A global unicast address has three parts:

- Global routing prefix
- Subnet ID
- Interface ID

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.

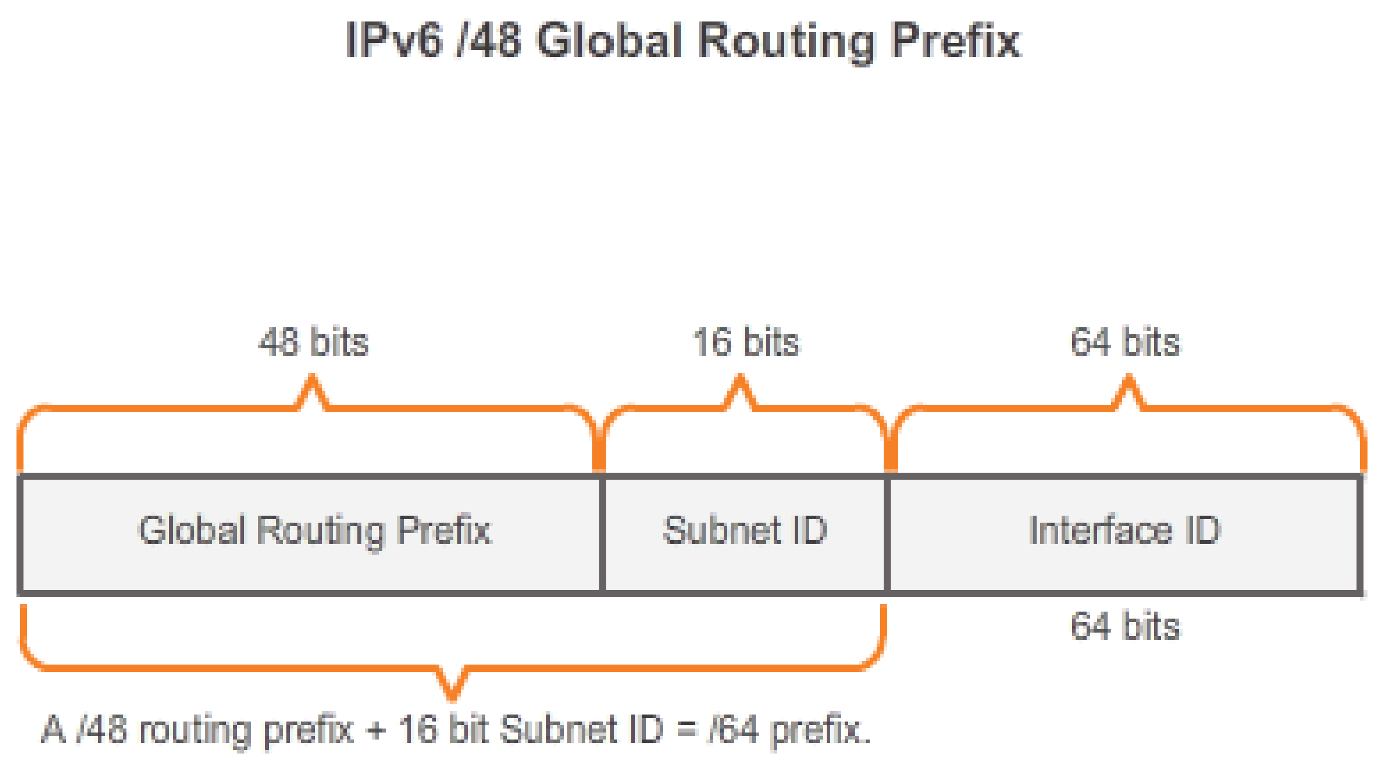
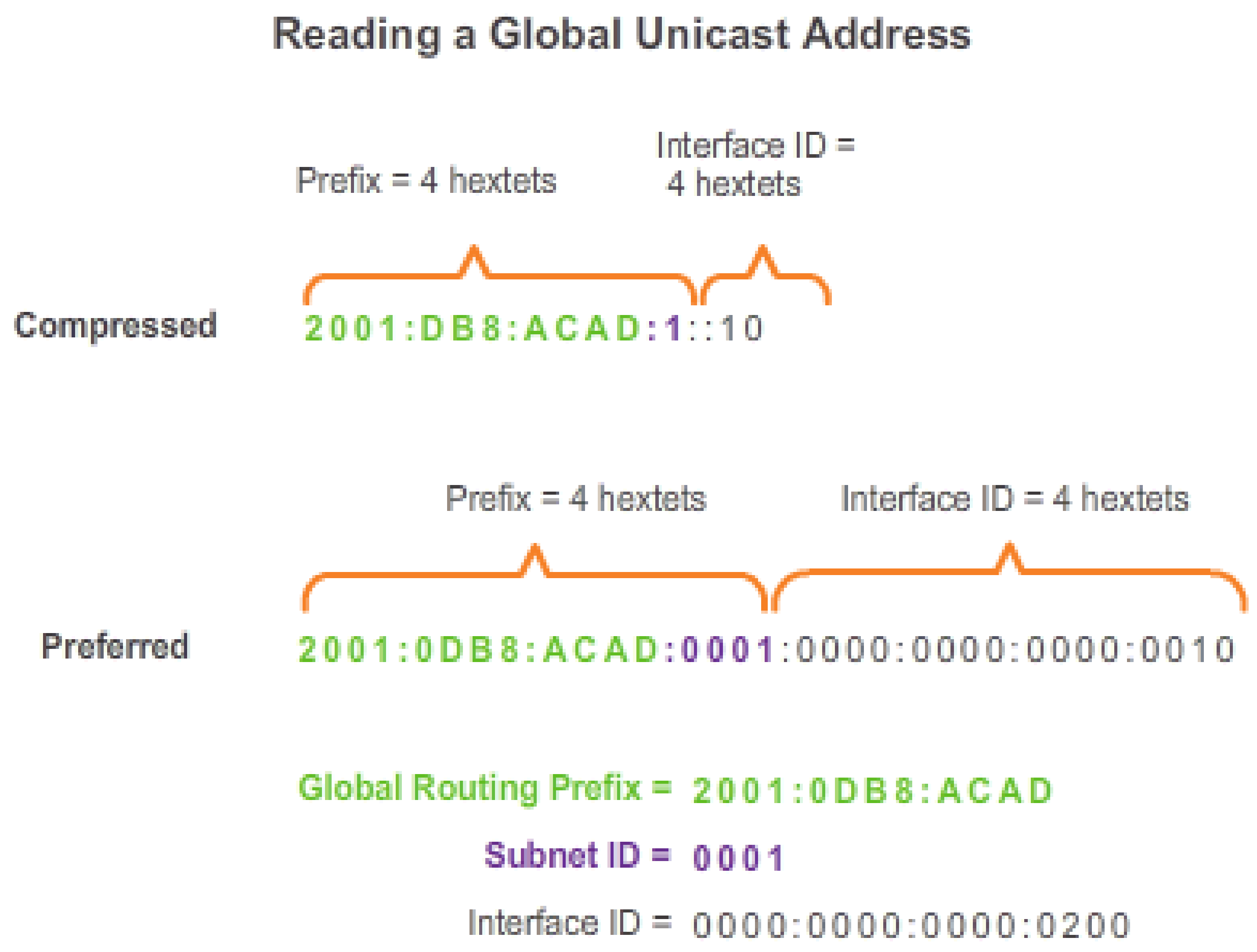


Figure 2 shows the structure of a global unicast address using a /48 global routing prefix. /48 prefixes are the most common **global routing prefixes** assigned and will be used in most of the examples throughout this course.

The **Subnet ID** is used by an organization to identify subnets within its site.

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.

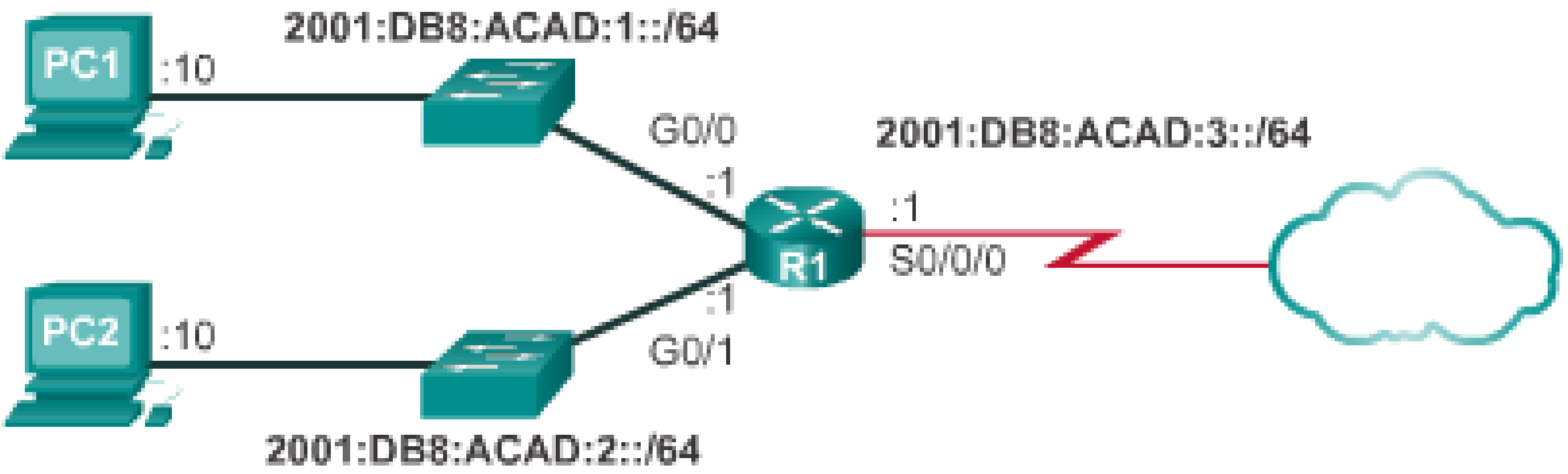
8.2.4.1 Structure of an IPv6 Global Unicast Address



An easy way to read most IPv6 addresses is to count the number of hextets.

As shown in Figure 3, in a /64 global unicast address the first four hextets are for the network portion of the address, with the fourth hextet indicating the Subnet ID. The remaining four hextets are for the Interface ID.

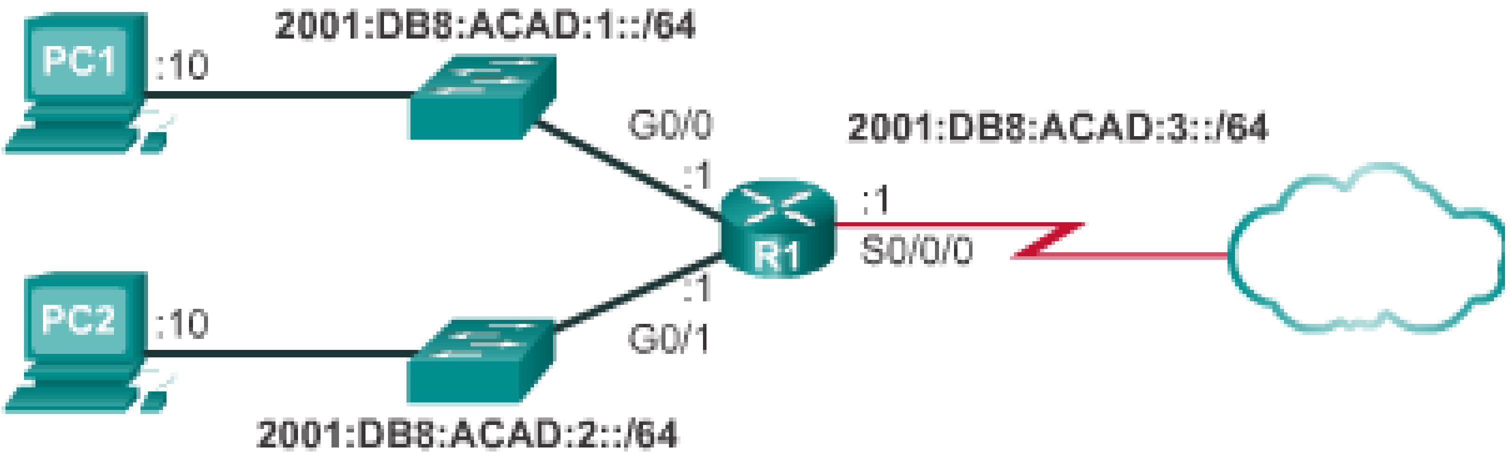
Configuring IPv6 on a Router



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.

8.2.4.2 Static Configuration of a Global Unicast Address

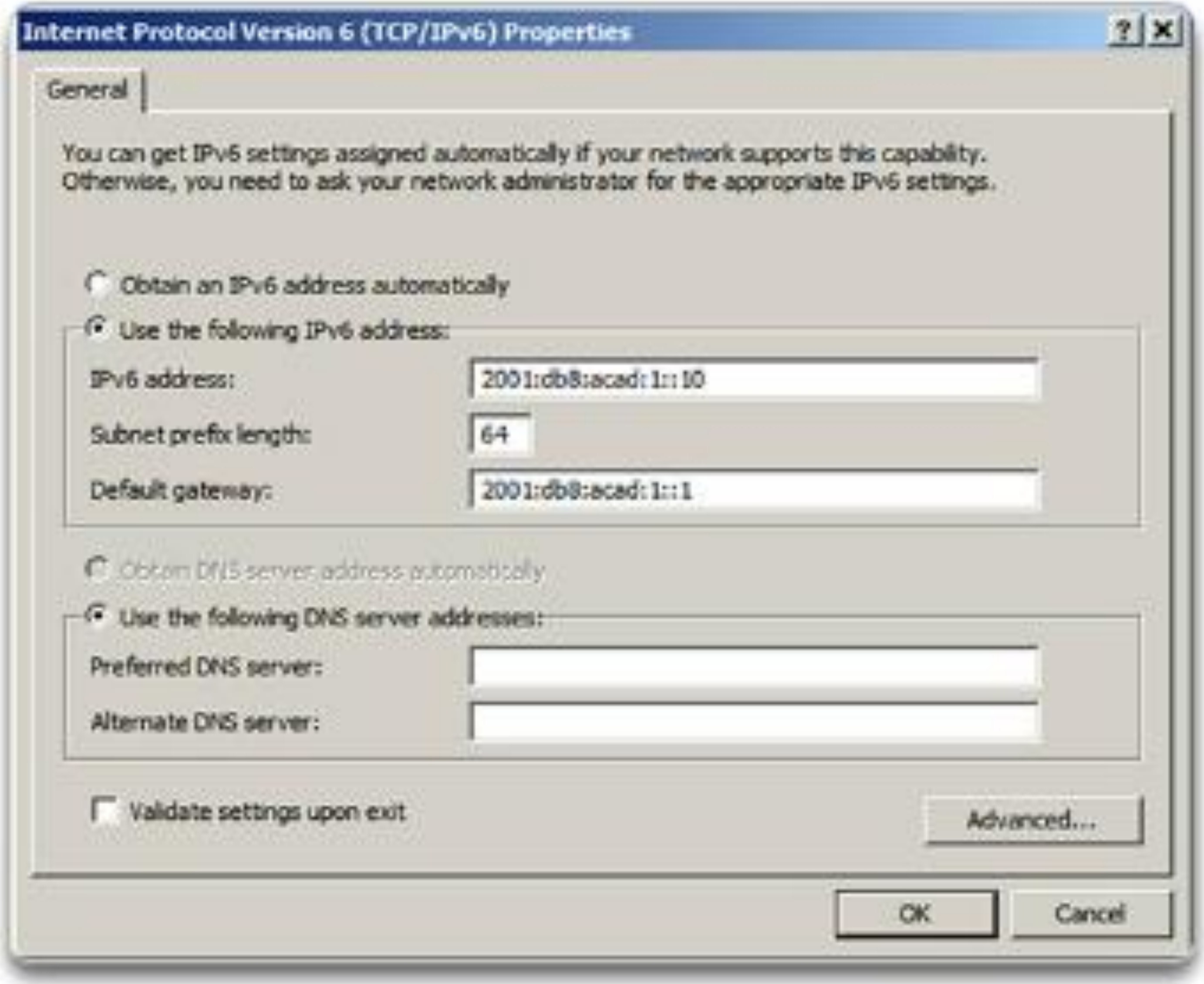



```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial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

As shown in Figure 2, the commands required to configure the IPv6 global unicast address on the GigabitEthernet 0/0 interface of R1 would be:

- Router(config)#interface GigabitEthernet 0/0
- Router(config-if)#ipv6 address 2001:db8:acad:1::1/64
- Router(config-if)#no shutdown

8.2.4.2 Static Configuration of a Global Unicast Address



Host Configuration

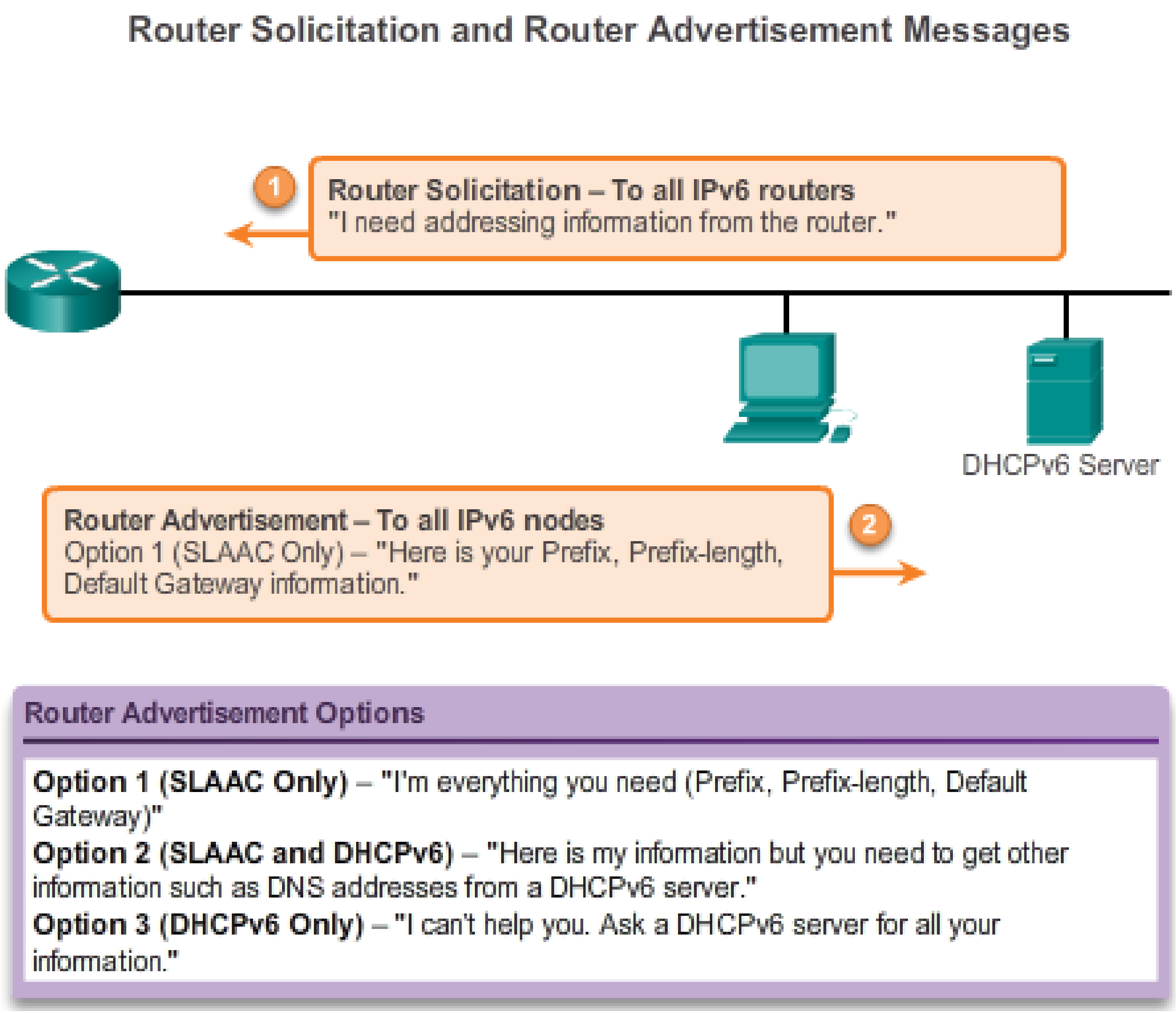
Manually configuring the IPv6 address on a host is similar to configuring an IPv4 address

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

Two ways a device can obtain an IPv6 global unicast address automatically:
Stateless Address Autoconfiguration (SLAAC) or DHCPv6

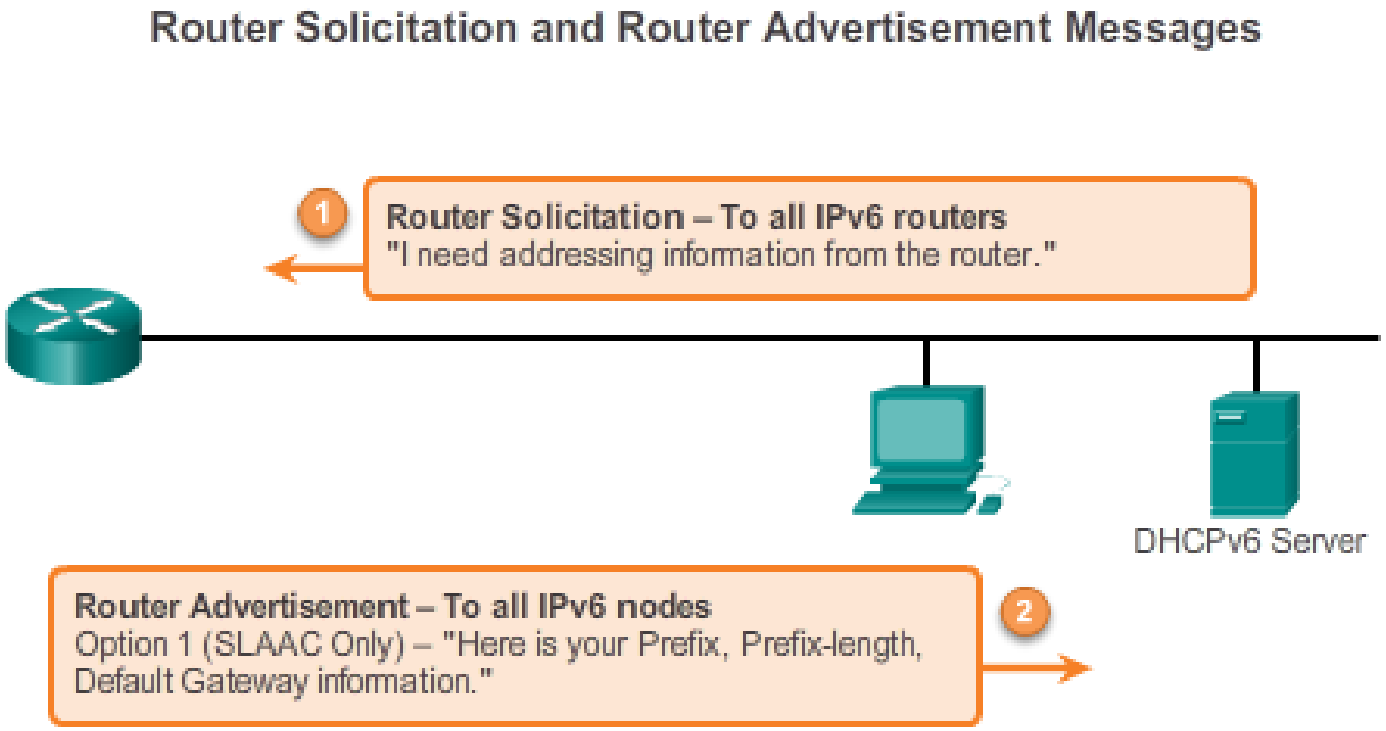
8.2.4.3 Dynamic Configuration of a Global Unicast Address using SLAAC



Stateless Address Autoconfiguration (SLAAC) is a method that allows a device to obtain its prefix, prefix length, and default gateway address 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 Router Advertisement (RA) messages to all IPv6-enabled devices on the network. By default, Cisco routers send out RA messages every 200 seconds to the IPv6 all-nodes multicast group address.

8.2.4.3 Dynamic Configuration of a Global Unicast Address using SLAAC



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."

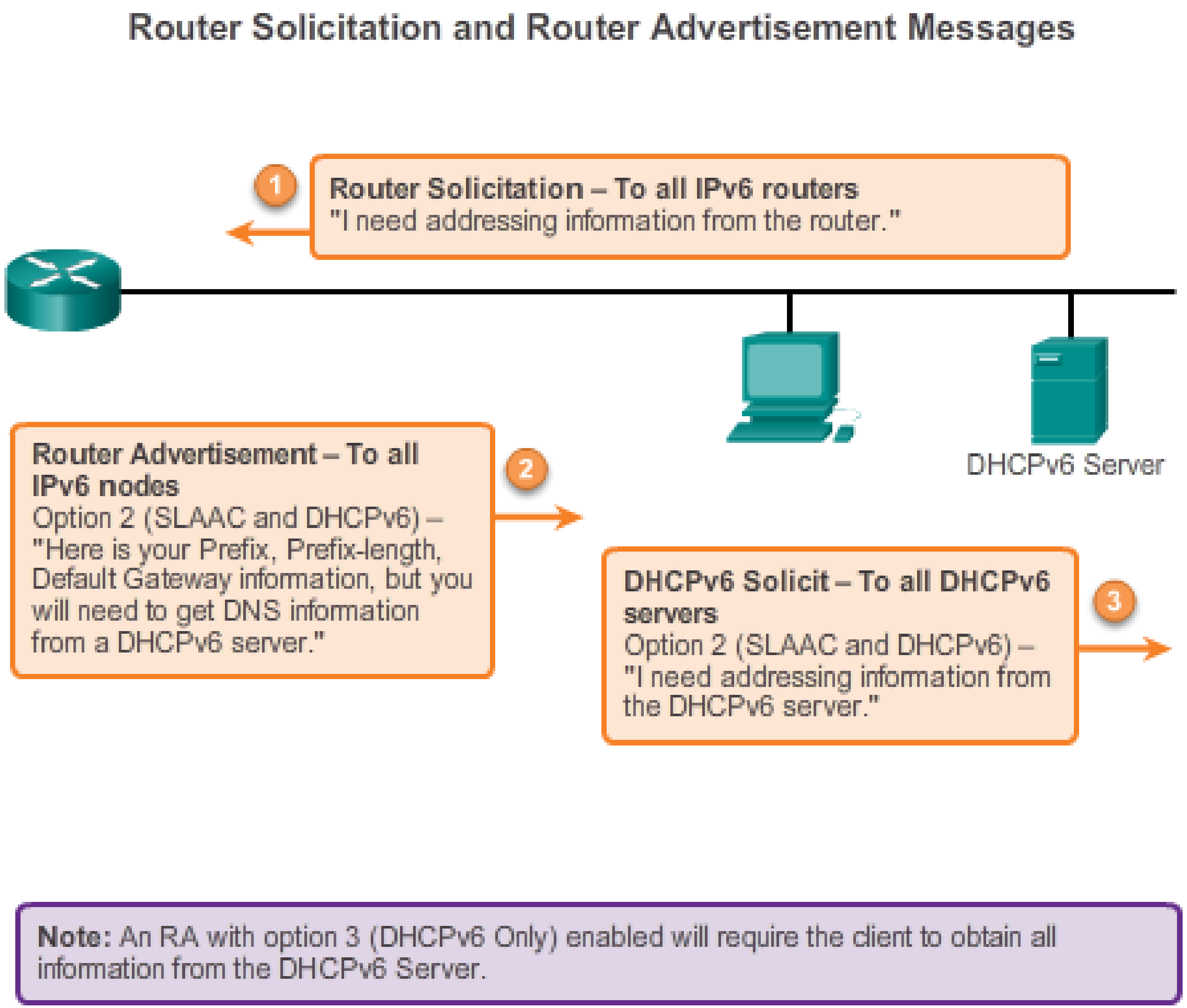
Even though an interface on a Cisco router can be configured with an IPv6 address, this does not make it an "IPv6 router". An IPv6 router is a router that:

1. Forwards IPv6 packets between networks
2. Can be configured with static IPv6 routes or a dynamic IPv6 routing protocol
3. Sends ICMPv6 RA messages

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: Cisco routers are enabled as IPv4 routers by default.

8.2.4.4 Dynamic Configuration of a Global Unicast Address using DHCPv6



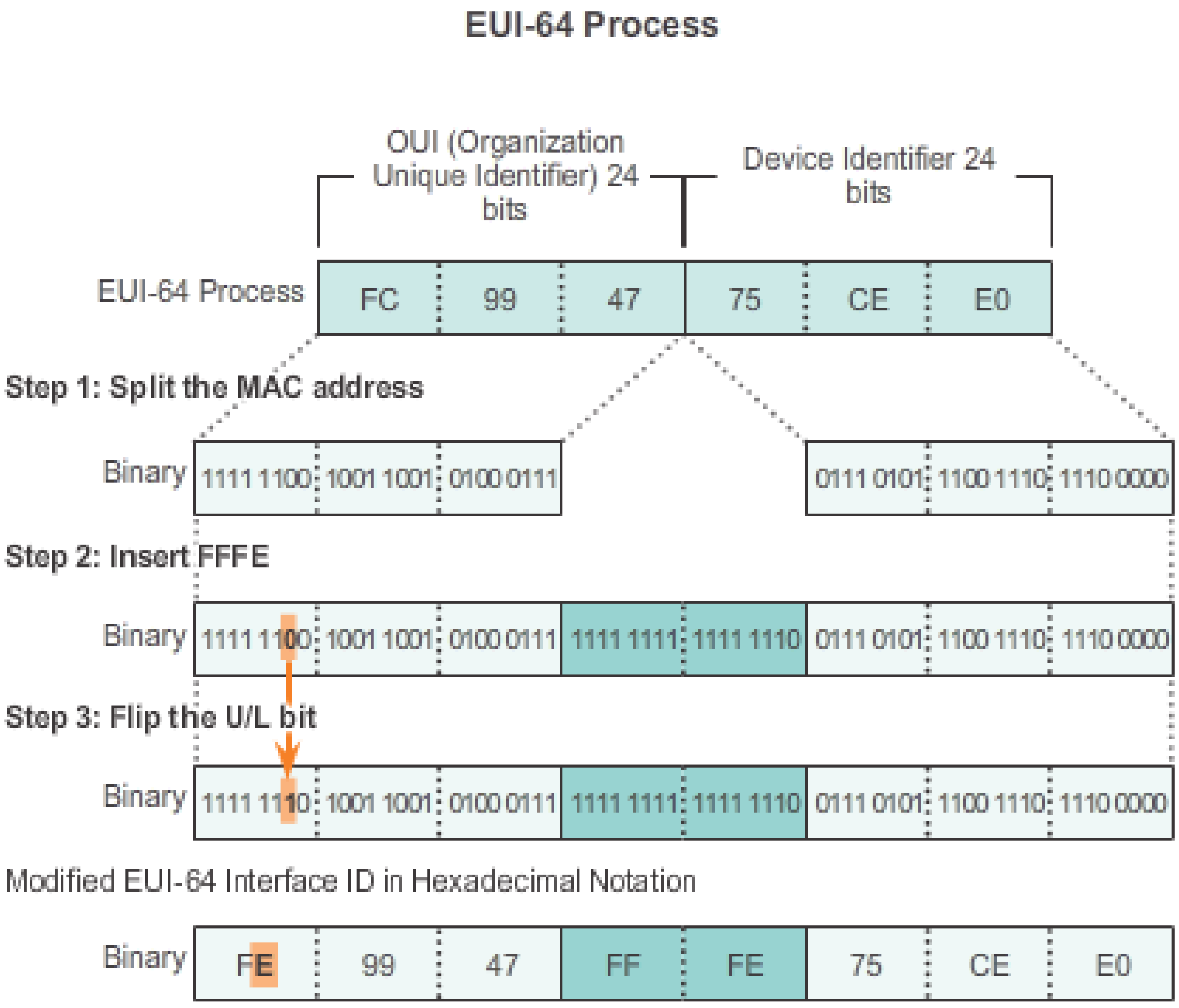
DHCPv6

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is similar to DHCP for IPv4. A device can automatically receive its addressing information including a global unicast address, prefix length, default gateway address and the addresses of DNS servers using the services of a DHCPv6 server.

A device may receive all or some of its IPv6 addressing information from a DHCPv6 server

Before deploying IPv6 devices in a network it is a good idea to first verify whether the host observes the options within the router's ICMPv6 RA message.
A device may obtain its IPv6 global unicast address dynamically

8.2.4.5 EUI-64 Process or Randomly Generated



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.

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

8.2.4.5 EUI-64 Process or Randomly Generated

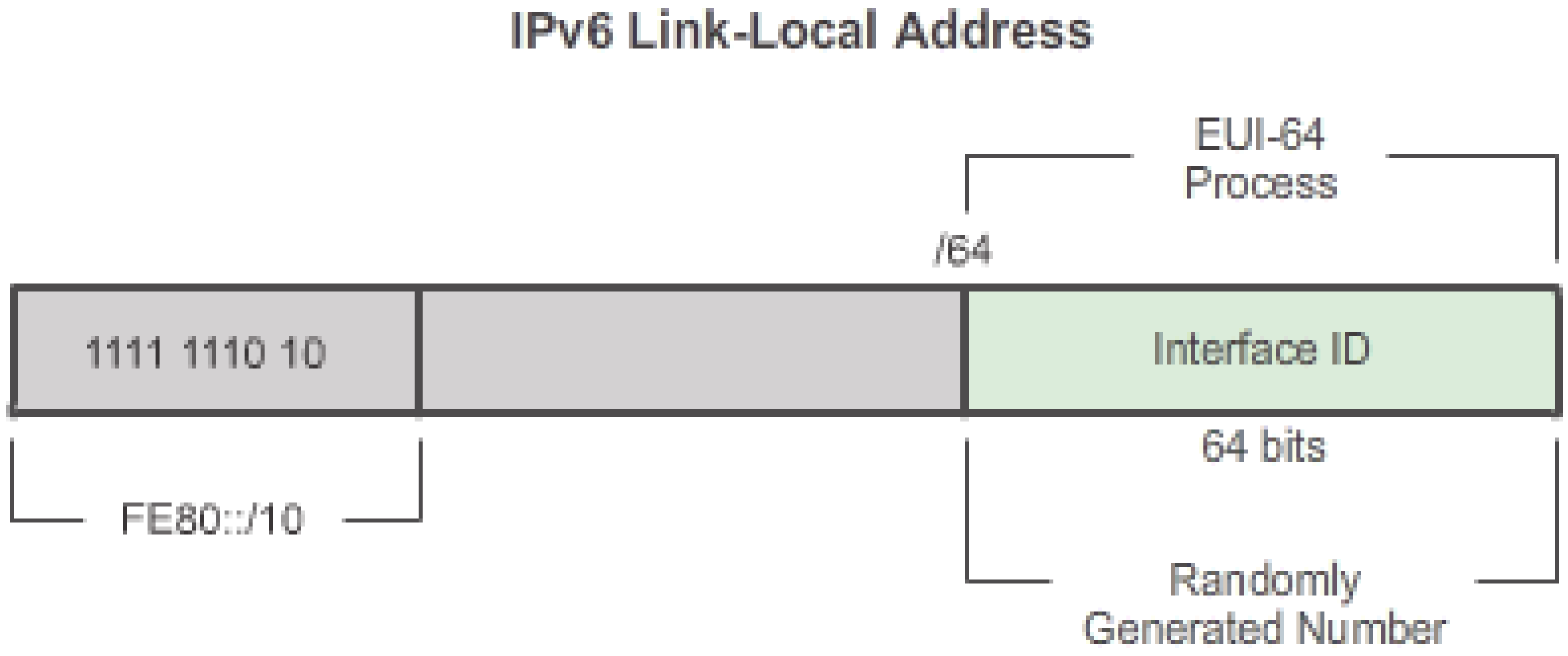
```
R1#show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<Output Omitted>

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

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.

8.2.4.6 Dynamic Link-local Addresses



IPv6 link-local addresses are used for a variety of purposes including:

- A host uses the link-local address of the local router for its default gateway IPv6 address.
- Routers exchange dynamic routing protocol messages using link-local addresses.
- Routers' routing tables use the link-local address to identify the next-hop router when forwarding IPv6 packets.

A link-local address can be established dynamically or configured manually as a static link-local address

By default, Cisco IOS routers use EUI-64 to generate the Interface ID for all link-local address on IPv6 interfaces

8.2.4.7 Static Link-Local Addresses

Configuring Link-local Addresses on R1

```
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)#
```

Configuring Link-local Addresses on R1

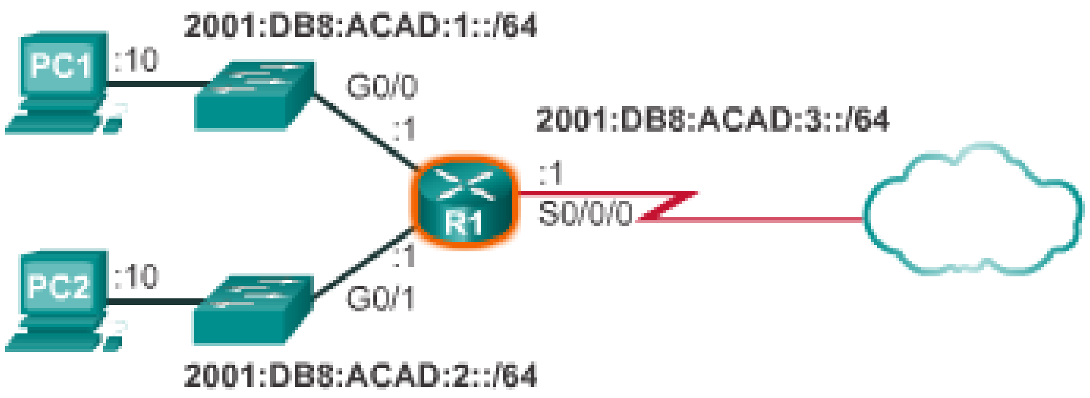
```
R1#show ipv6 interface brief
GigabitEthernet0/0        [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
GigabitEthernet0/1        [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
Serial0/0/0               [up/up]
    FE80::1
    2001:DB8:ACAD:3::1
Serial0/0/1               [administratively down/down]
    unassigned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

Statically configured 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 an additional parameter:

8.2.4.8 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#
```

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. Recall that the link-local address is automatically added to the interface when a global unicast address is assigned.

8.2.4.8 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#
```

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

8.2.4.8 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.

```
Router# 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
```

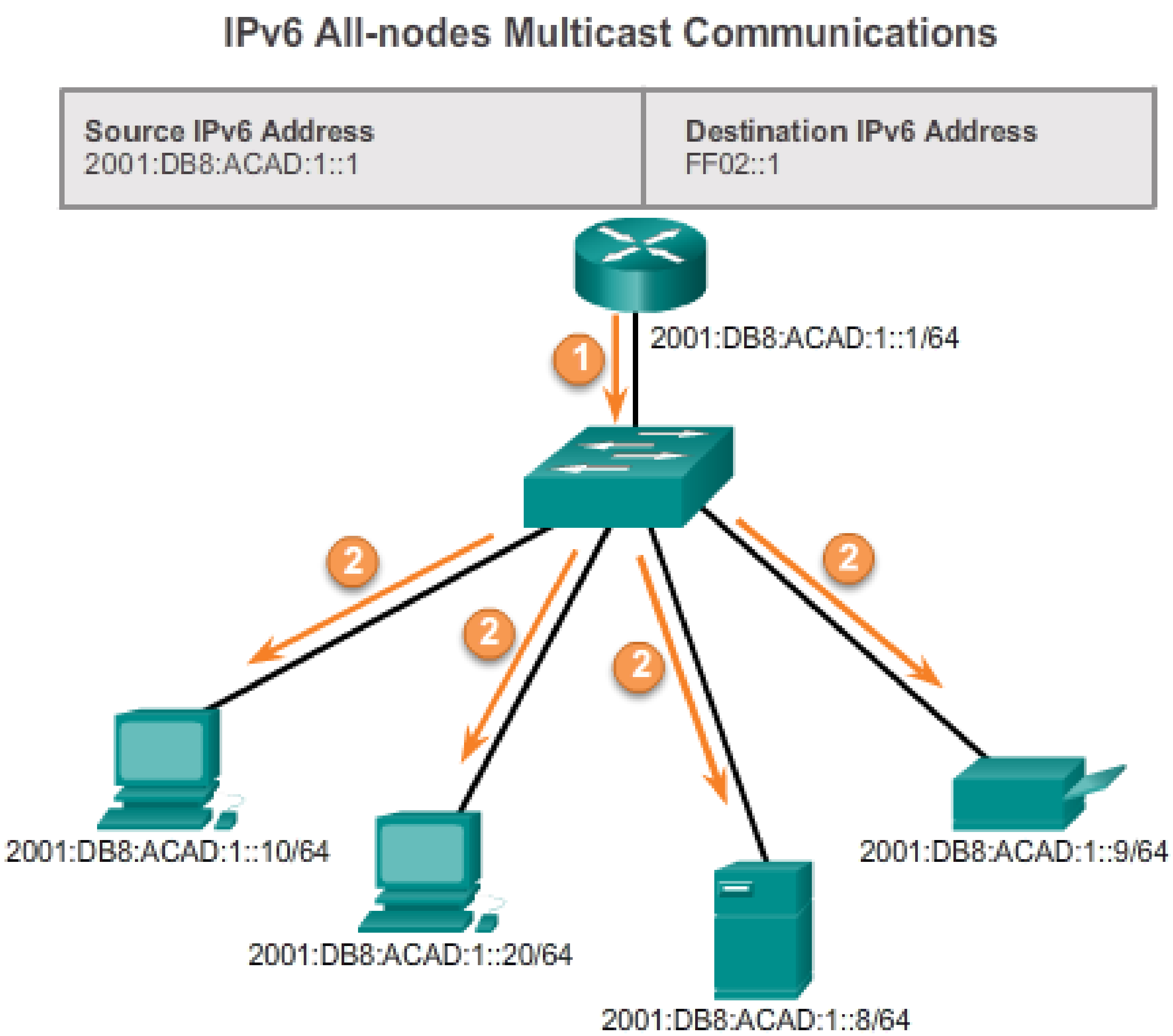
Enter the show command that will display the IPv6 routing table.

```
Router# |
```

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.

8.2.5.1 Assigned IPv6 Multicast Addresses



There are two types of IPv6 multicast addresses:

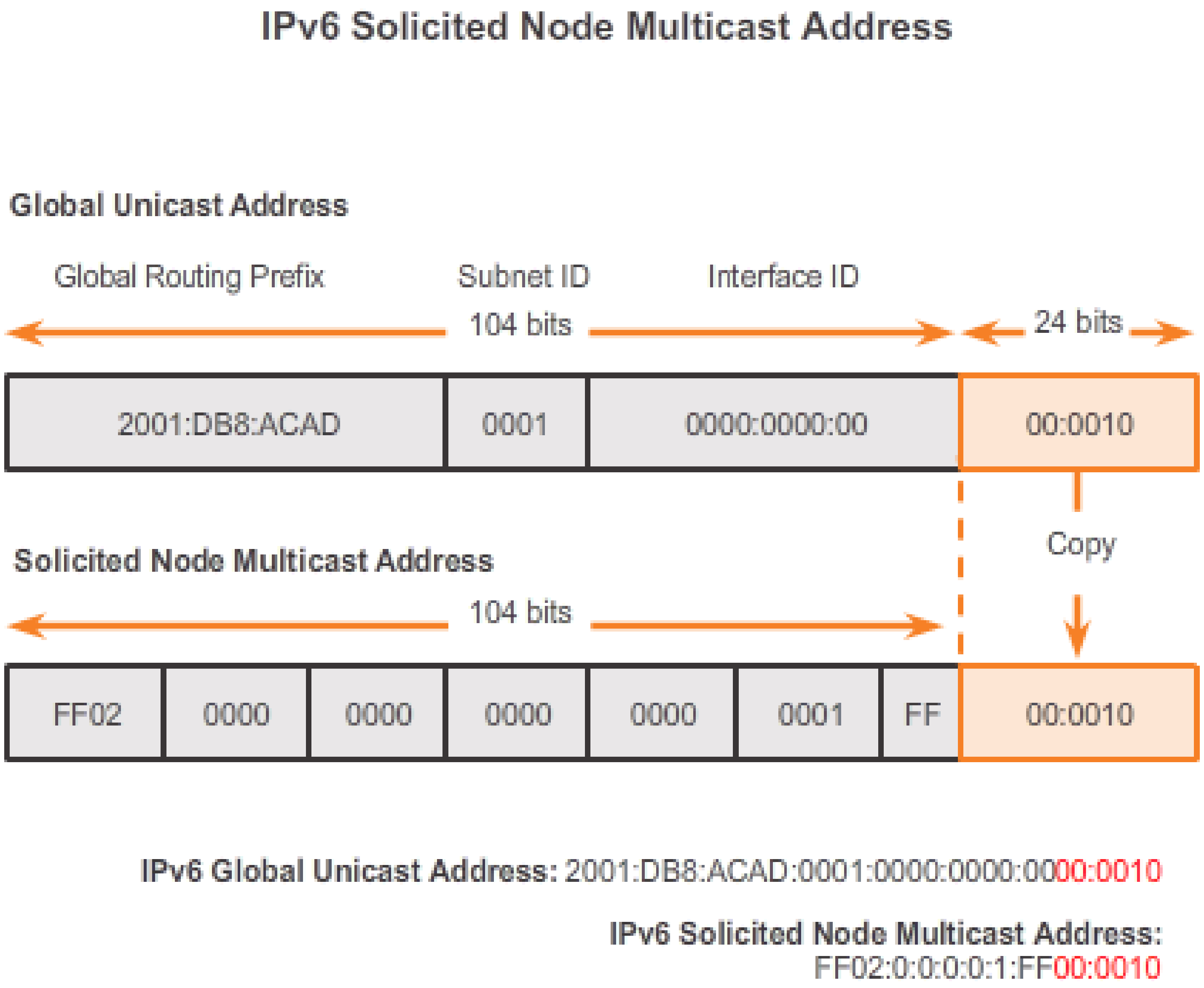
1. Assigned multicast
2. Solicited node multicast

Assigned multicast addresses are reserved multicast addresses for predefined groups of devices.

An assigned multicast address is a **single address used to reach a group of devices running a common protocol or service**. Assigned multicast addresses are used in context with specific protocols such as DHCPv6.

IPv6-enabled devices send ICMPv6 Router Solicitation (RS) messages to the all-routers multicast address. The RS message requests an RA message from the IPv6 router to assist the device in its address configuration.

8.2.5.2 Solicited-Node IPv6 Multicast Addresses



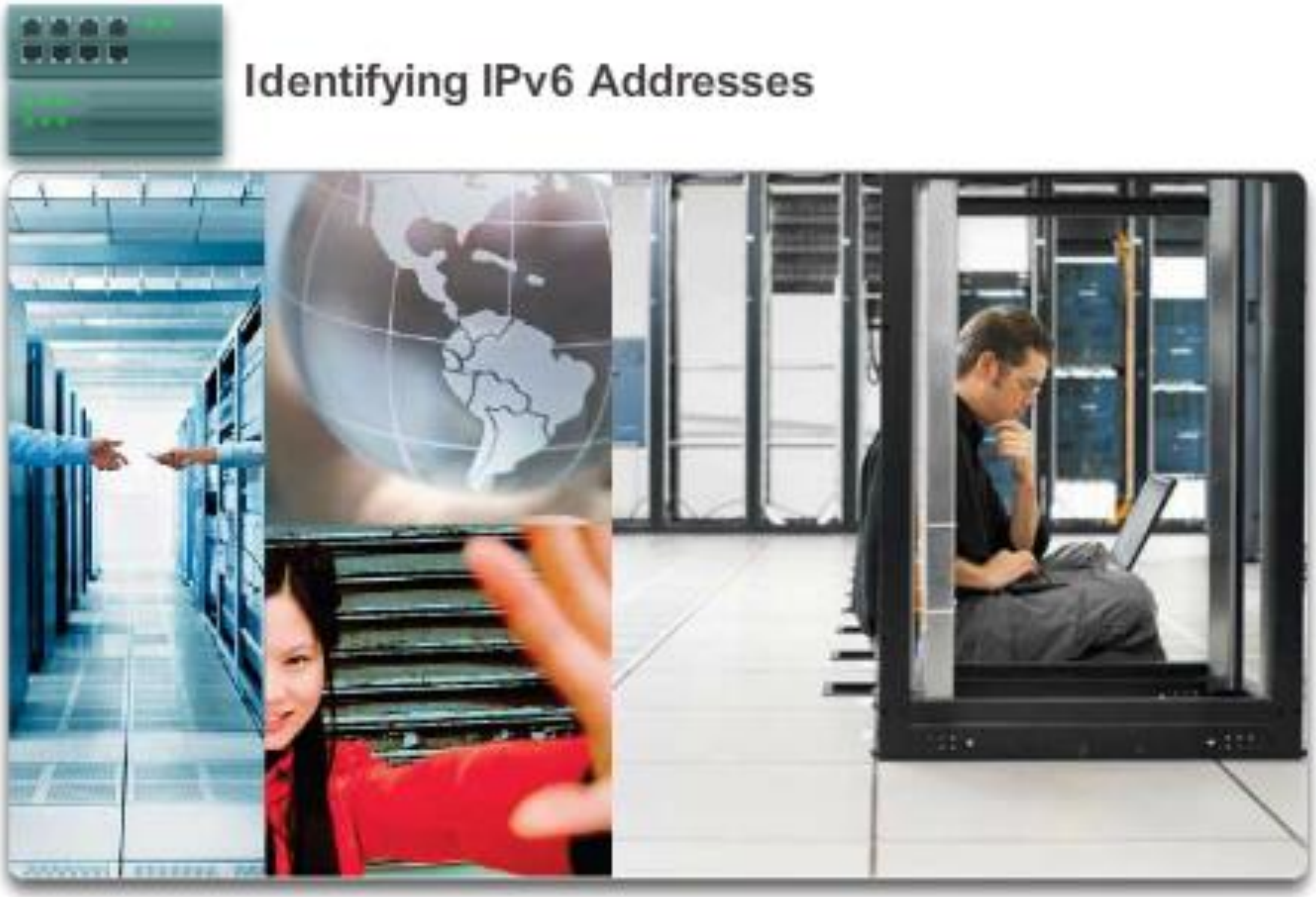
A solicited-node multicast is similar to the all-nodes multicast address. Recall that the all-nodes multicast address is essentially the same thing as an IPv4 broadcast. All devices on the network must process traffic sent to the all-nodes address. To reduce the number of devices that must process traffic, use a solicited-node multicast address.

A solicited-node multicast address is an address that matches only the last 24 bits of the IPv6 global unicast address of a device. The only devices that need to process these packets are those devices that have these same 24 bits in the least significant, far right portion of their Interface ID

8.2.5.3 Packet Tracer - Configuring IPv6 Addressing

In this activity, you will practice configuring IPv6 addresses on a router, servers, and clients. You will also practice verifying your IPv6 addressing implementation.

8.2.5.4 Lab - Identifying IPv6 Addresses



In this lab, you will complete the following objectives:

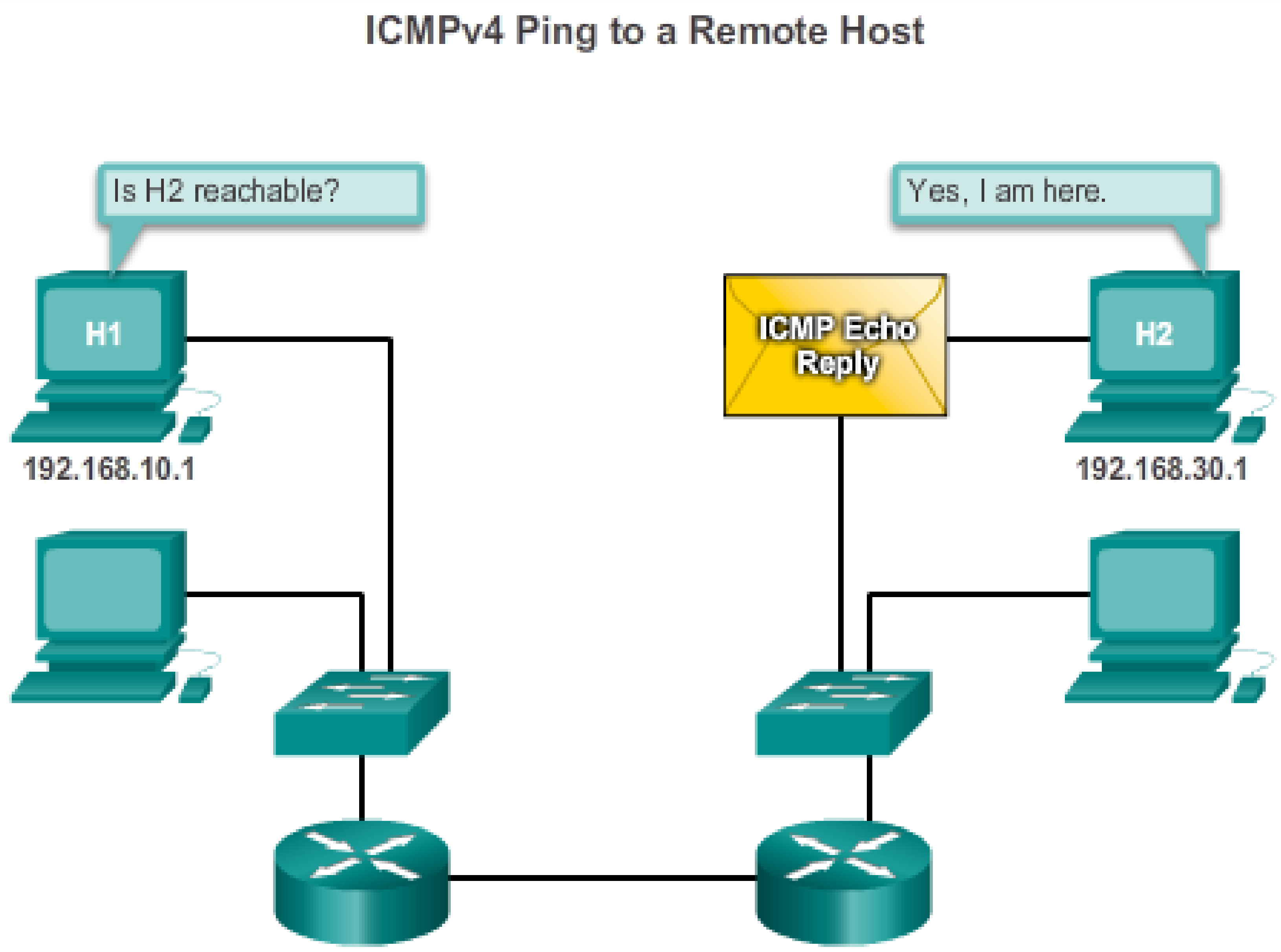
- Part 1: Identify the Different Types of IPv6 Addresses
- Part 2: Examine a Host IPv6 Network Interface and Address
- Part 3: Practice IPv6 Address Abbreviation
- Part 4: Identify the Hierarchy of the IPv6 Global Unicast Address Network Prefix

8.2.5.5 Lab - Configuring IPv6 Addresses on Network Devices

In this lab, you will complete the following objectives:

- Part 1: Set Up Topology and Configure Basic Router and Switch Settings
- Part 2: Configure IPv6 Addresses Manually
- Part 3: Verify End-to-End Connectivity

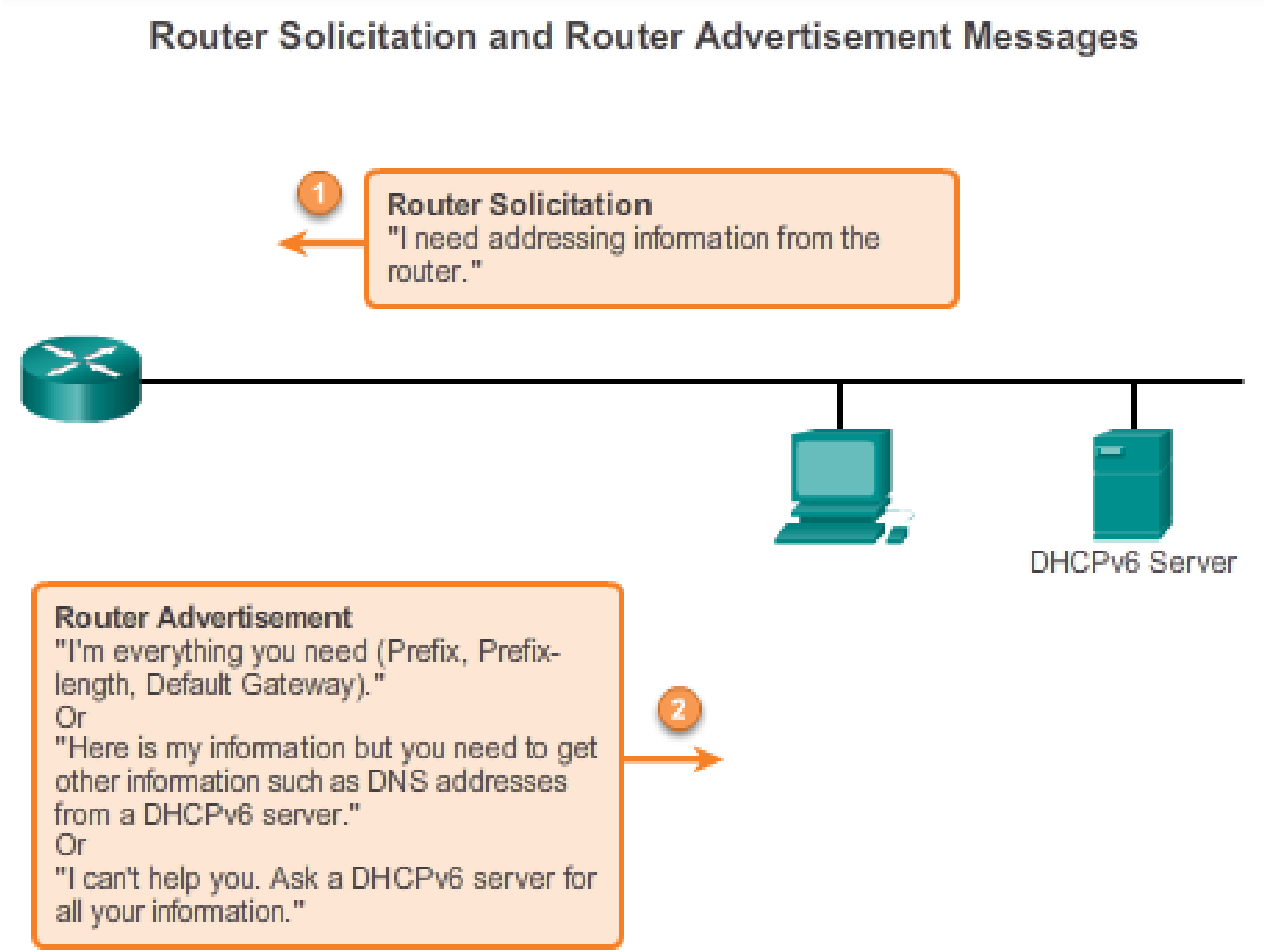
8.3.1.1 ICMPv4 and ICMPv6 Messages



ICMP messages common to both ICMPv4 and ICMPv6 include:

- Host confirmation
- Destination or Service Unreachable
- Time exceeded
- Route redirection

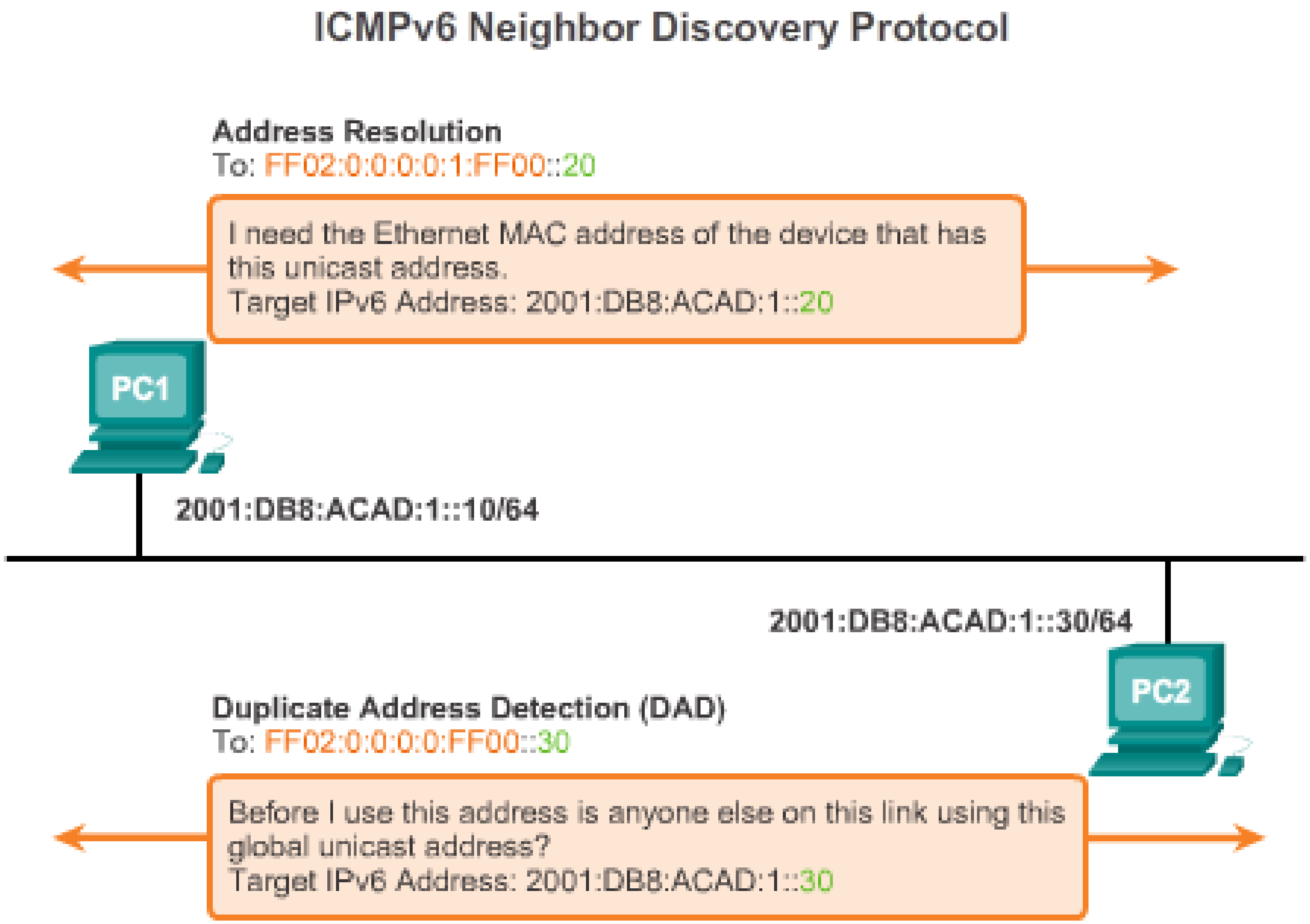
8.3.1.2 ICMPv6 Router Solicitation and Router Advertisement Messages



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

- Router Solicitation message
- Router Advertisement message
- Neighbor Solicitation message
- Neighbor Advertisement message

8.3.1.3 ICMPv6 Neighbor Solicitation and Neighbor Advertisement Messages

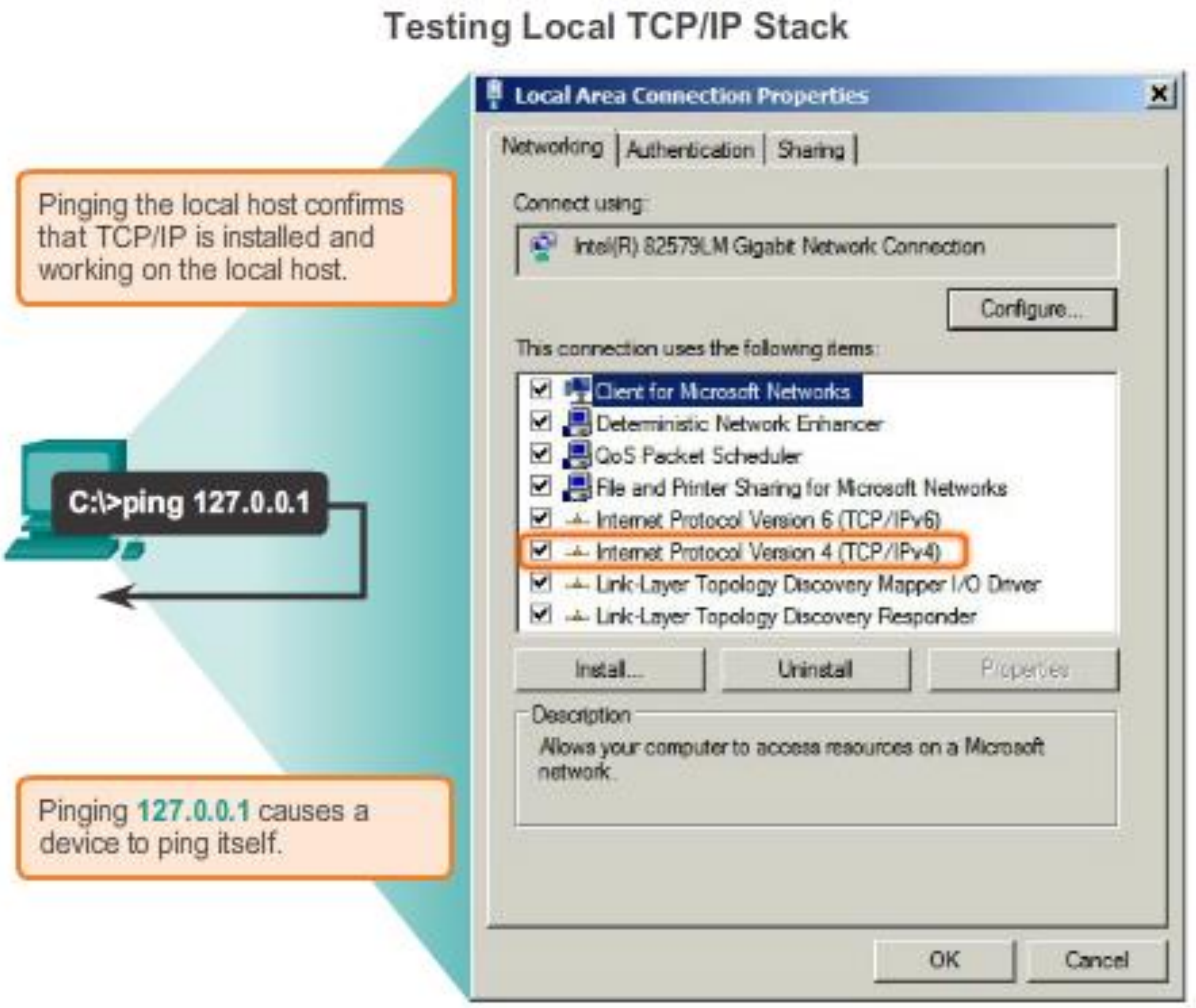


ICMPv6 Neighbor Discovery Protocol includes two additional message types, Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

Neighbor Solicitation and Neighbor Advertisement messages are used for:

- Address resolution
- Duplicate Address Detection (DAD)

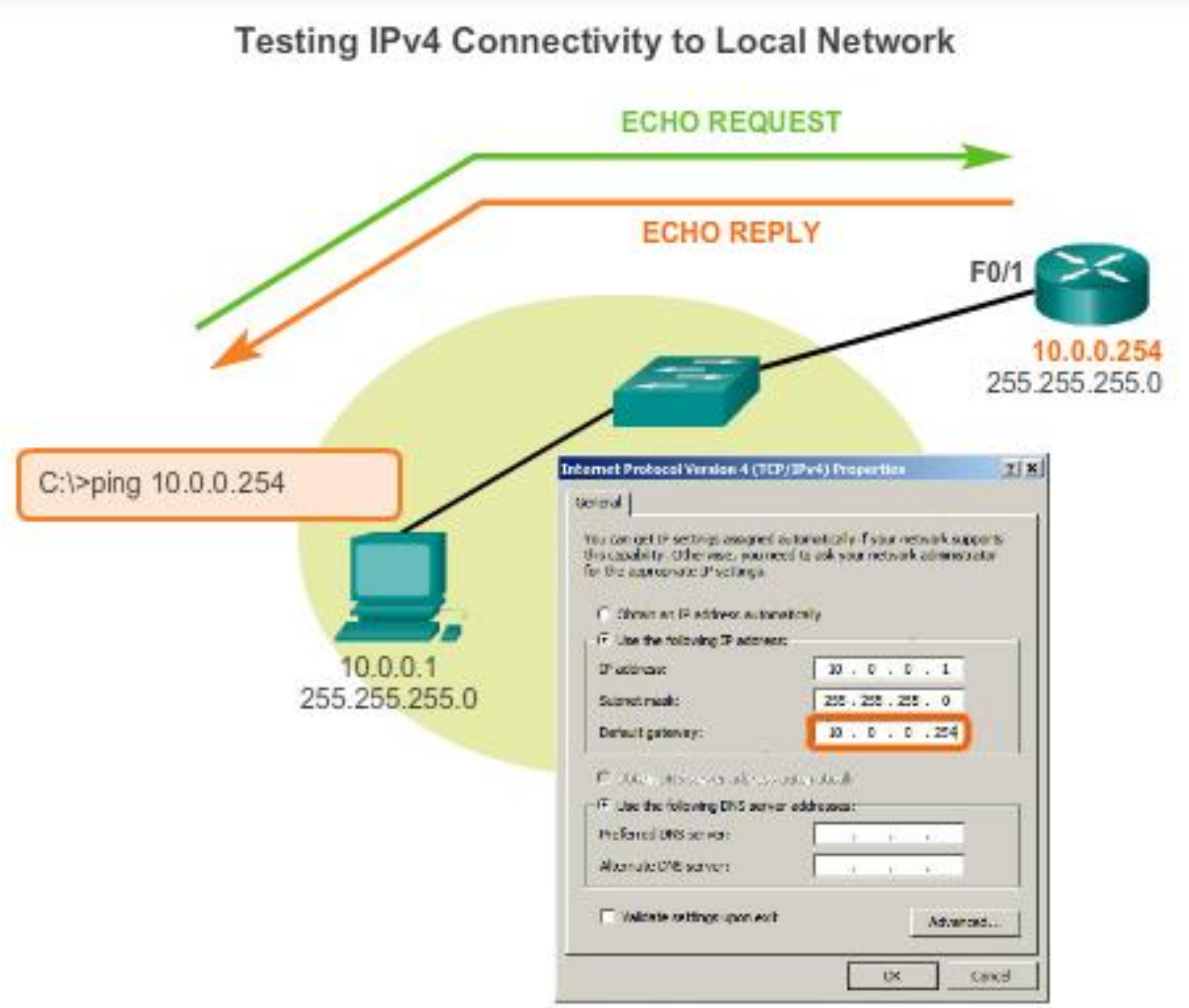
8.3.2.1 Ping - Testing the Local Stack



Ping is a testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts. Ping works with both IPv4 and IPv6 hosts.

There are some special testing and verification cases for which we can use ping. One case is for testing the internal configuration of IPv4 or IPv6 on the local host. To perform this test, we ping the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6). Testing the IPv4 loopback is shown in the figure.

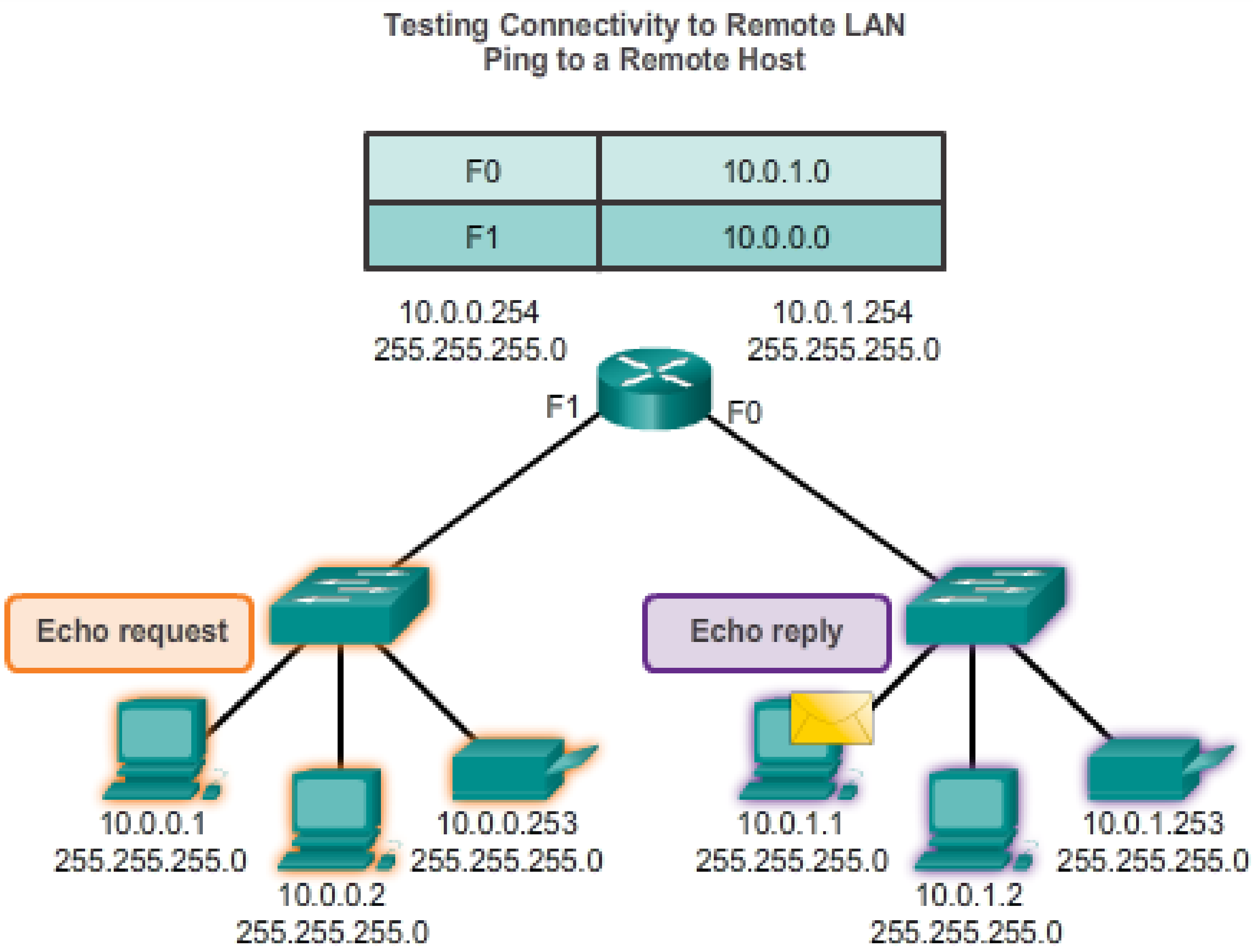
8.3.2.2 Ping - Testing Connectivity to the Local LAN



You can also use ping to test the ability of a host to communicate on the local network. This is generally done by pinging the IP address of the gateway of the host. A ping to the gateway indicates that the host and the router interface serving as the gateway are both operational on the local network.

For this test, the gateway address is most often used, because the router is normally always operational. If the gateway address does not respond, a ping can be sent to the IP address of another host on the local network that is known to be operational.

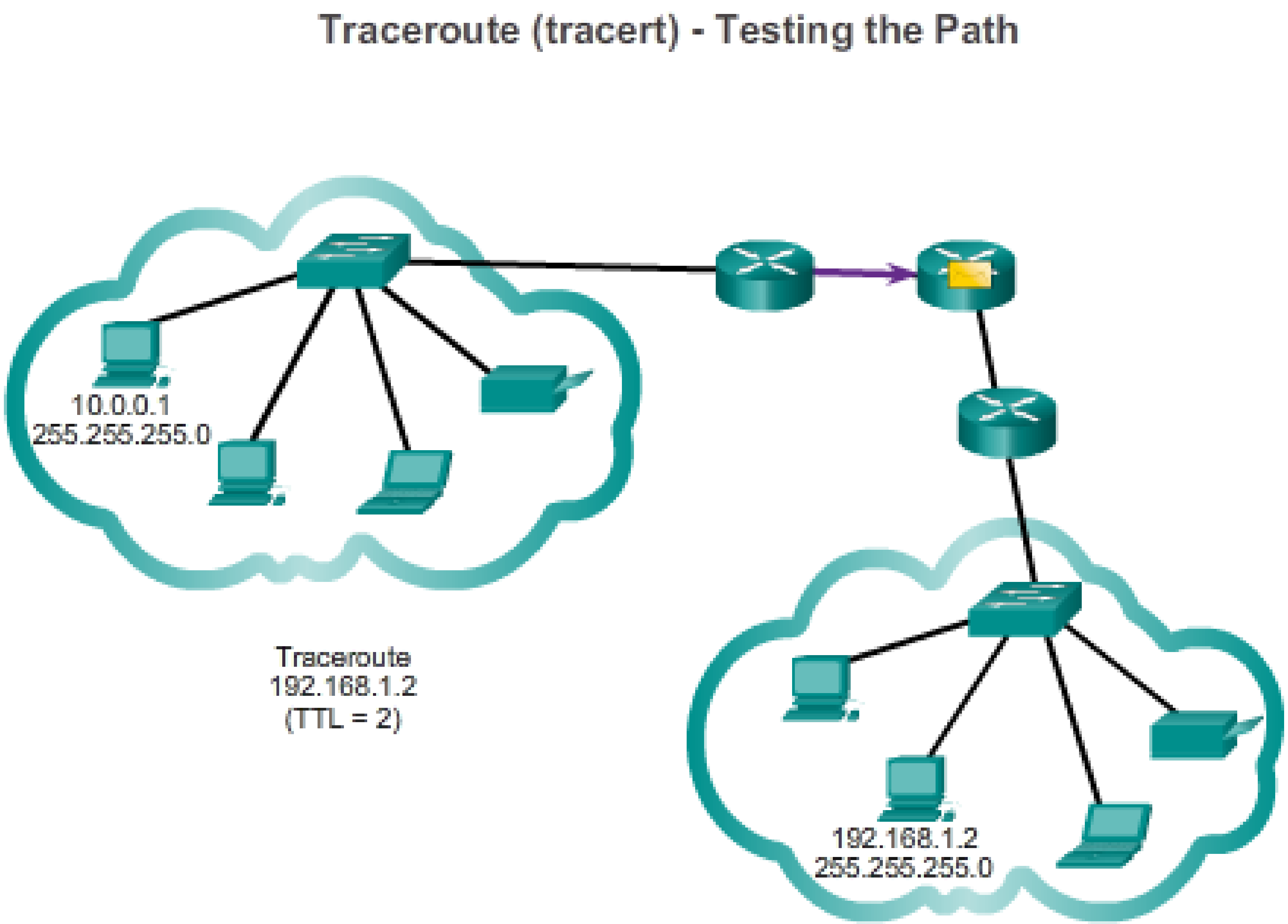
8.3.2.3 Ping - Testing Connectivity to Remote



Ping can also be used to test the ability of a local host to communicate across an internetwork. The local host can ping an operational IPv4 host of a remote network, as shown in the figure.

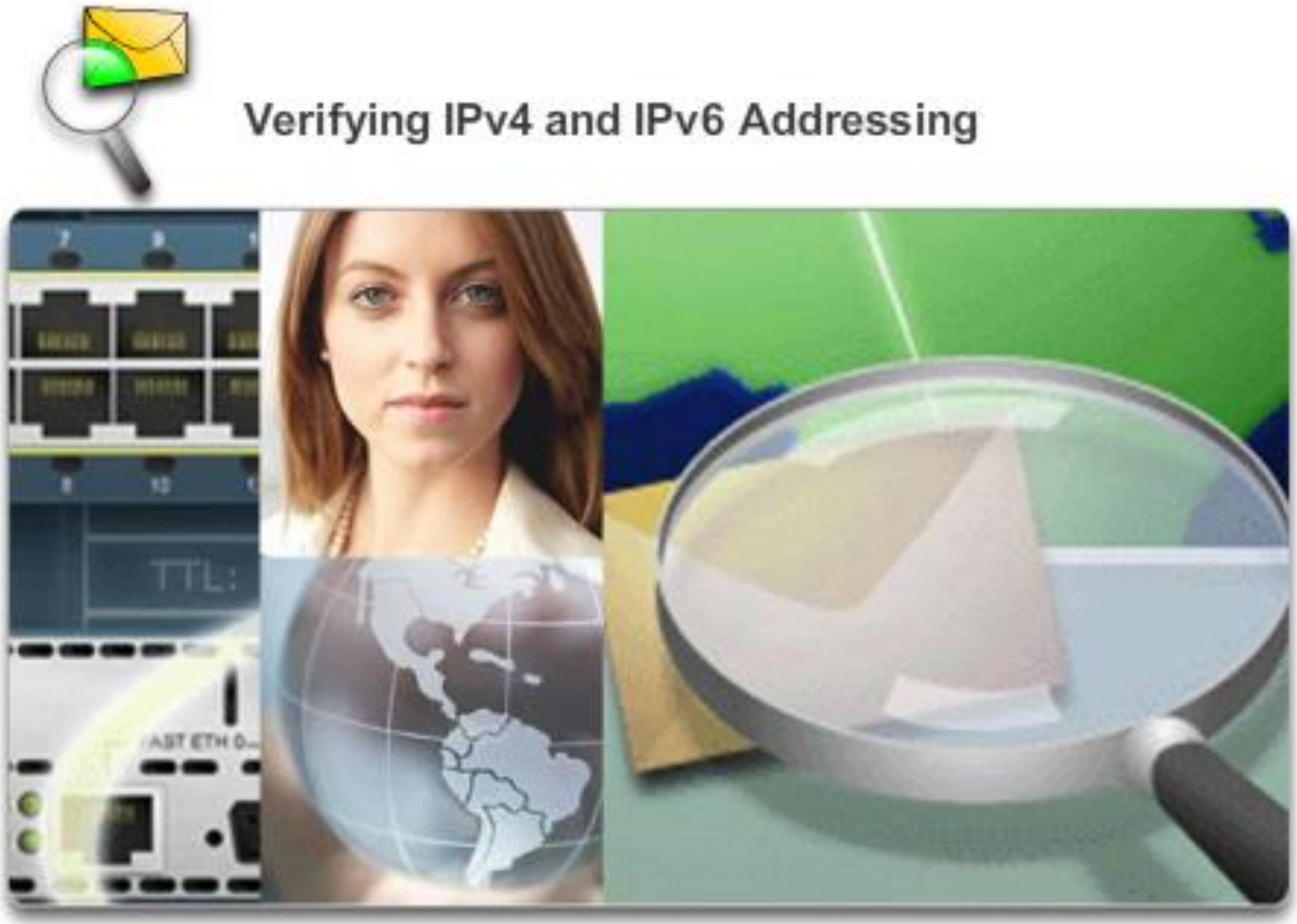
If this ping is successful, the operation of a large piece of the internetwork can be verified. A successful ping across the internetwork confirms communication on the local network, the operation of the router serving as our gateway, and the operation of all other routers that might be in the path between the local network and the network of the remote host.

8.3.2.4 Traceroute - Testing the Path



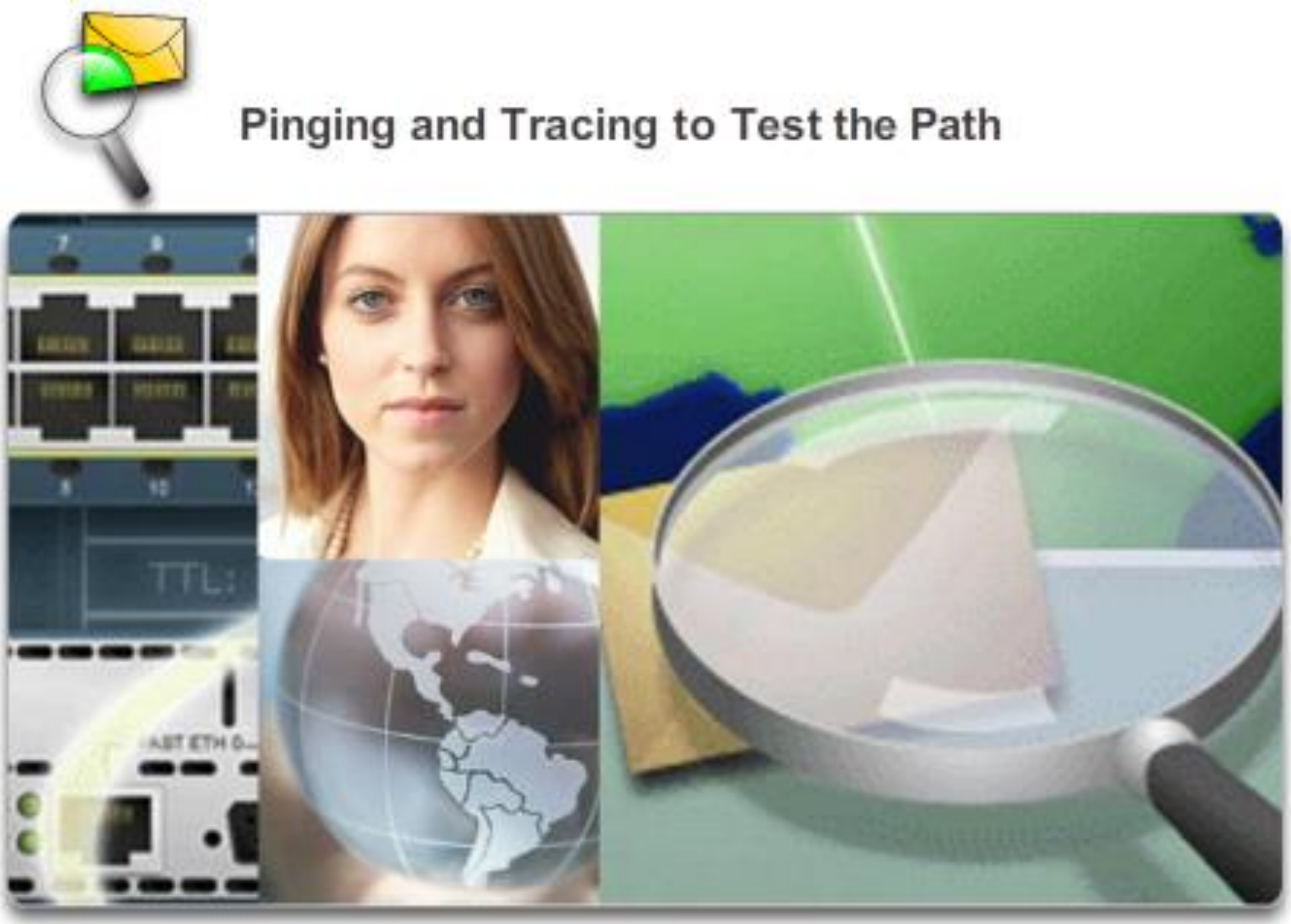
Using traceroute provides round trip time for each hop along the path and indicates if a hop fails to respond. The round trip time is the time a packet takes to reach the remote host and for the response from the host to return. An asterisk (*) is used to indicate a lost or unreplied packet.
This information can be used to locate a problematic router in the path. If the display shows high response times or data losses from a particular hop, this is an indication that the resources of the router or its connections may be stressed.

8.3.2.5 Packet Tracer - Verifying IPv4 and IPv6 Addressing



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

8.3.2.6 Packet Tracer - Pinging and Tracing to Test the Path



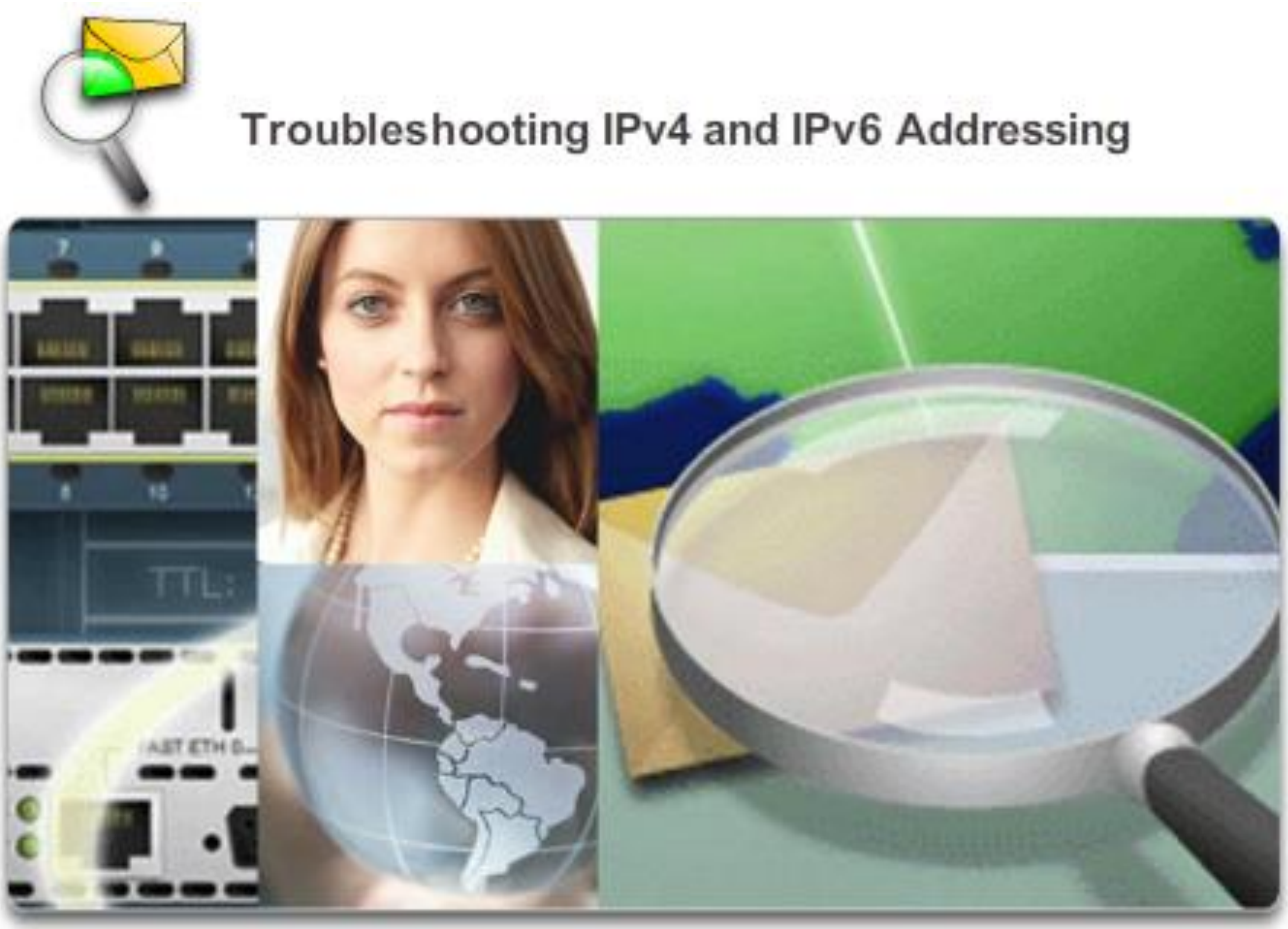
There are connectivity issues in this activity. In addition to gathering and documenting information about the network, you will locate the problems and implement acceptable solutions to restore connectivity

8.3.2.7 Lab - Testing Network Connectivity with Ping and Traceroute

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Use Ping Command for Basic Network Testing
- Part 3: Use Tracert and Traceroute Commands for Basic Network Testing
- Part 4: Troubleshoot the Topology

8.3.2.8 Packet Tracer - Troubleshooting IPv4 and IPv6 Addressing



You are a network technician working for a company that has decided to migrate from IPv4 to IPv6. In the interim, they must support both protocols (dual stack). Three co-workers have called the help desk with problems and have received limited assistance. The help desk has escalated the matter to you, a Level 2 support technician.

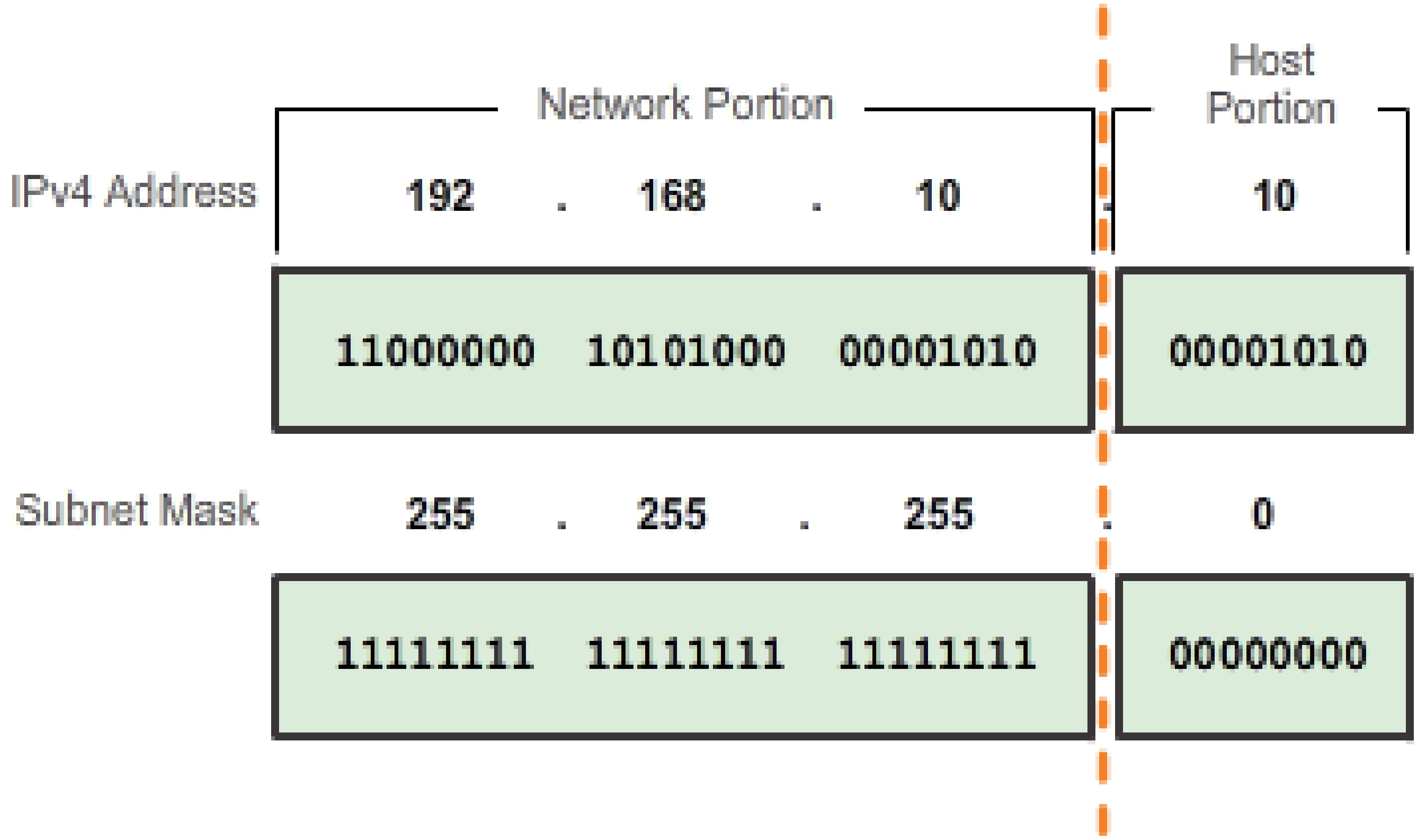
8.4.1.1 Class Activity - The Internet of Everything…Naturally!

Designing, implementing and managing an effective IP addressing plan ensures an effective and efficient network!

8.4.1.2 Packet Tracer – Skills Integration Challenge

Your company has won a contract to set up a small network for a restaurant owner. There are two restaurants near each other, and they all share one connection. The equipment and cabling is installed and the network administrator has designed the implementation plan. You job is implement the rest of the addressing scheme according to the abbreviated Addressing Table and verify connectivity.

8.4.1.3 Summary



IP addresses are hierarchical with network, subnetwork, and host portions. An IP address can represent a complete network, a specific host, or the broadcast address of the network.

Thanks for your attention!!

CISCO SYSTEMS