Fundamentals of Telecommunications Networks

ECP 602

Eng. Rasha Samir

Electronics and Electrical Communications Dept.
Cairo University

IP Addressing

Lecture Objectives

Upon completion of this lecture, 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.

Lecture Overview

Introduction
IPv4 Network Addresses
Network Address Translation for IPv4
IPv6 Network Addresses
Connectivity Verification
Summary

IPv4 Network Addresses

IPv4 Address Structure

Binary Notation

- Binary notation refers to the fact that computers communicate in 1s and 0s
- Positional notation - converting binary to decimal requires an understanding of the mathematical basis of a numbering system

Positional Notation

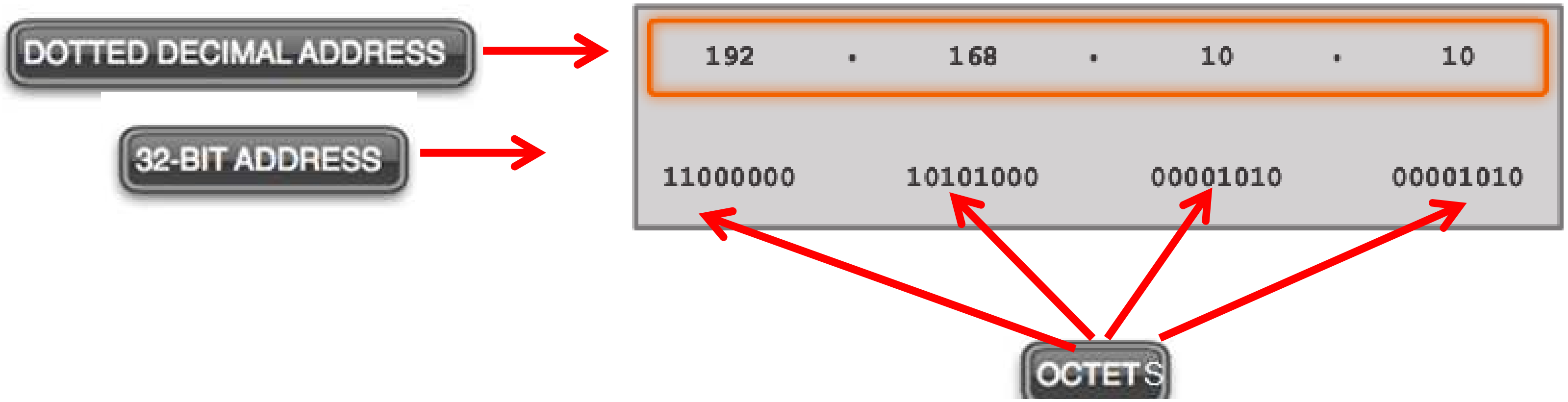
192

	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

IPv4 Address Structure

Binary Number System



Radix	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Octet Bit Values	128	64	32	16	8	4	2	1
Binary Address	1	1	0	0	0	0	0	0
Binary Bit Values	128	64	0	0	0	0	0	0

Add the binary bit values. 128 + 64 = 192

Converting a Binary Address to Decimal

Practice

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	0	0	0	0

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

Converting a Binary Address to Decimal

Practice

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	1	0	0	0	0

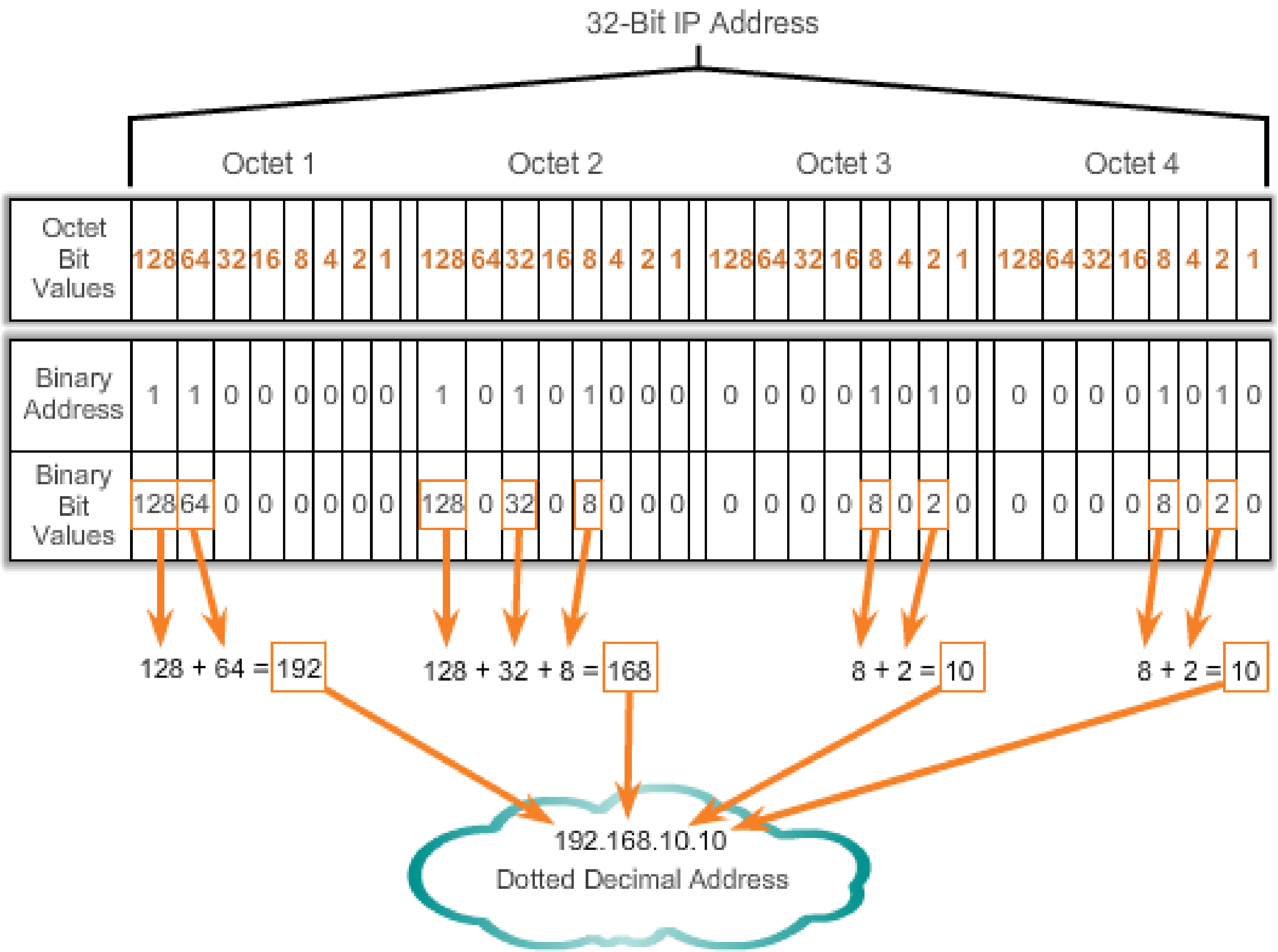
Answer = 176

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

Answer = 255

IPv4 Address Structure

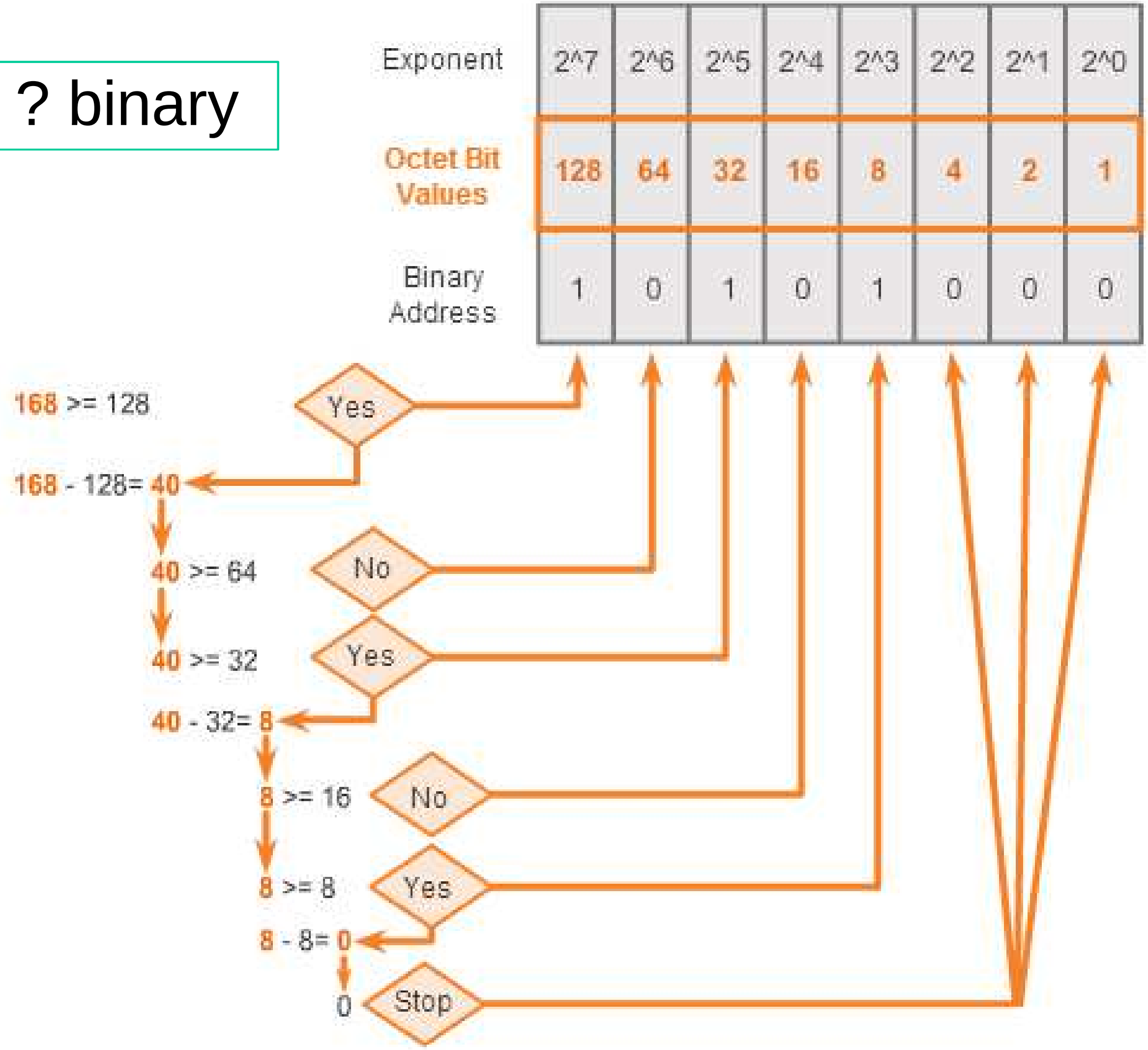
Converting a Binary Address to Decimal



IPv4 Address Structure

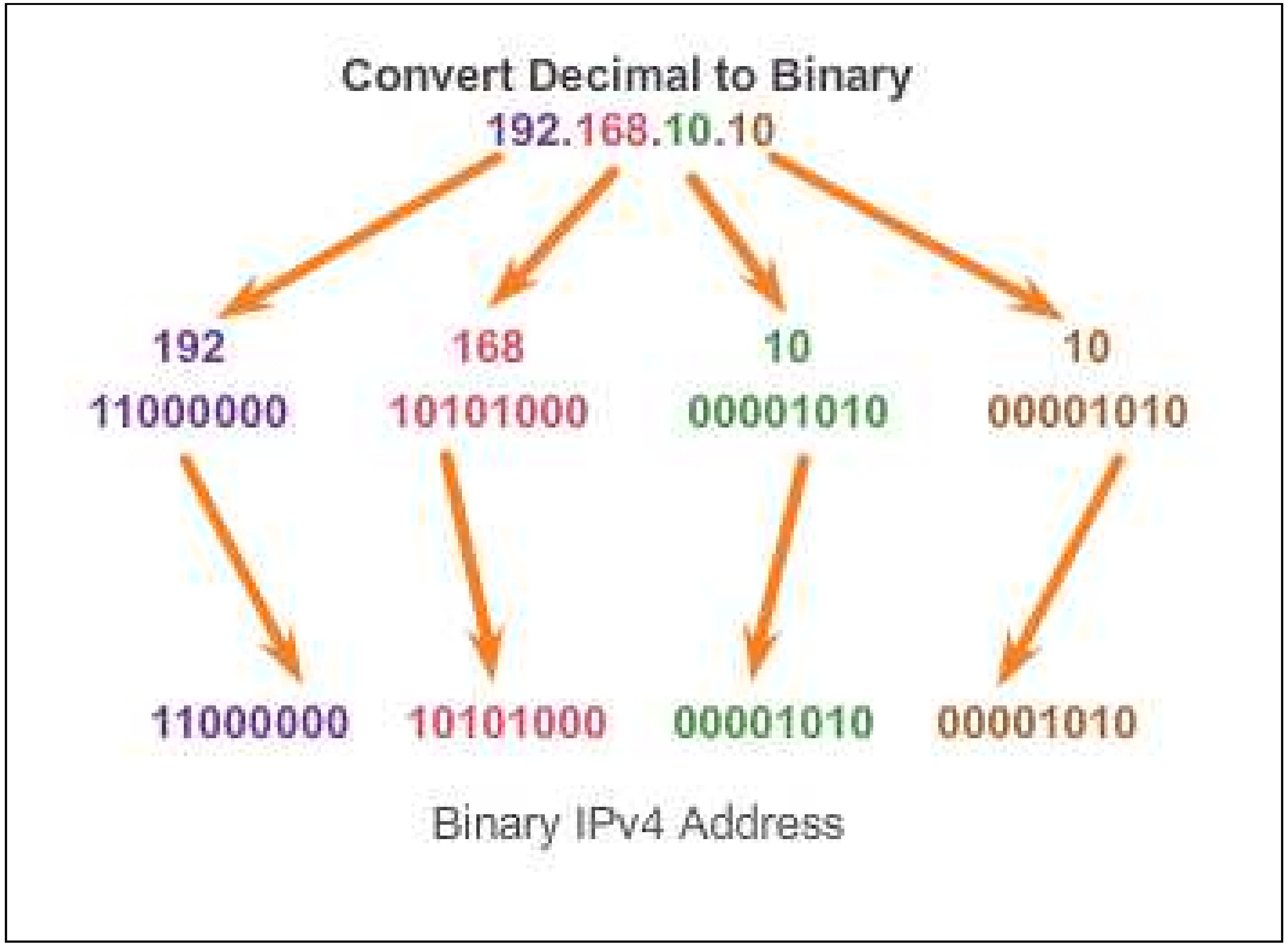
Converting from Decimal to Binary

168 = ? binary



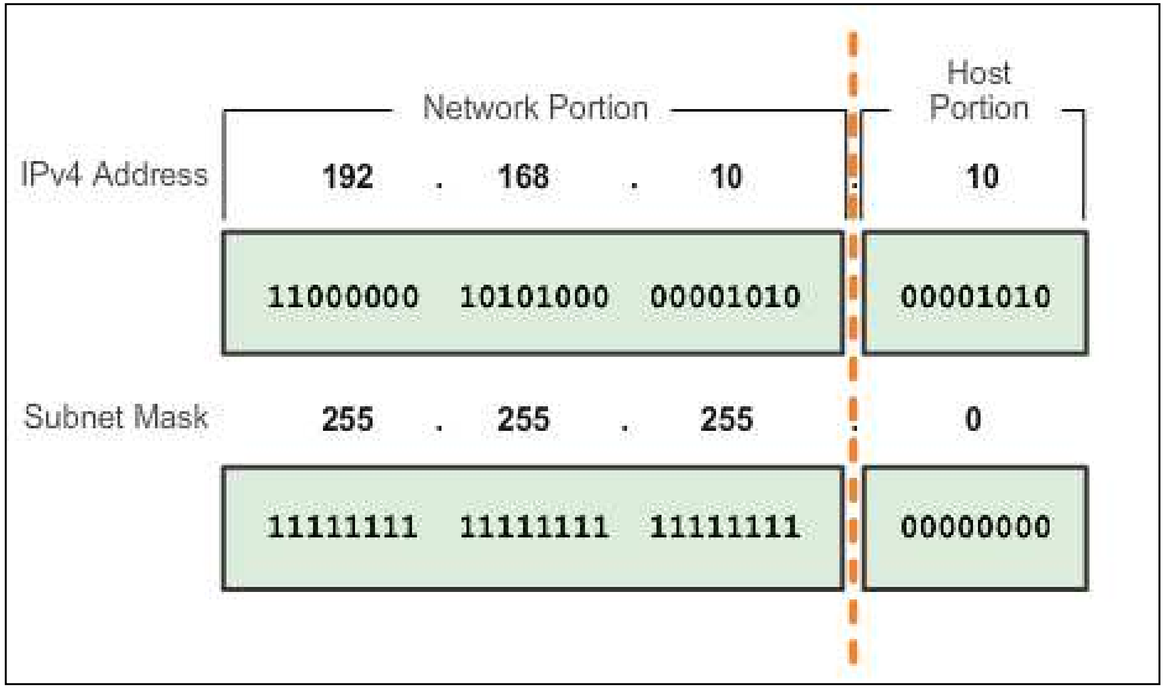
IPv4 Address Structure

Converting from Decimal to Binary (Cont.)



Network Portion and Host Portion of an IPv4 Address

- To define the network and host portions of an address, a devices use a separate 32-bit pattern called a subnet mask
- The subnet mask does not actually contain the network or host portion of an IPv4 address, it just says where to look for these portions in a given IPv4 address



IPv4 Subnet Mask

Network Portion and Host Portion of an IPv4 Address (cont.)

Valid Subnet Masks

Subnet Value	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

(Bit Value)

IPv4 Subnet Mask

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		

Network Address	**10.1.1.0/25**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.126	10.1.1.01111110
Broadcast Address	10.1.1.127	10.1.1.01111111
Number of hosts: 2^7 – 2 = 126 hosts		

Network Address	**10.1.1.0/26**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.62	10.1.1.00111110
Broadcast Address	10.1.1.63	10.1.1.00111111
Number of hosts: 2^6 – 2 = 62 hosts		

IPv4 Subnet Mask

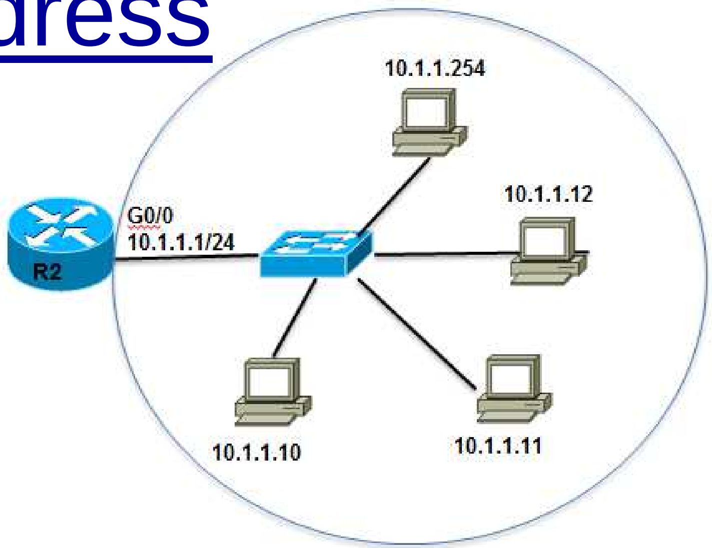
Examining the Prefix Length (cont.)

	Dotted Decimal	Significant bits shown in binary
Network Address	**10.1.1.0/27**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.30	10.1.1.00011110
Broadcast Address	10.1.1.31	10.1.1.00011111
Number of hosts: 2^5 – 2 = 30 hosts		

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		

IPv4 Subnet Mask

IPv4 Network, Host, and Broadcast Address

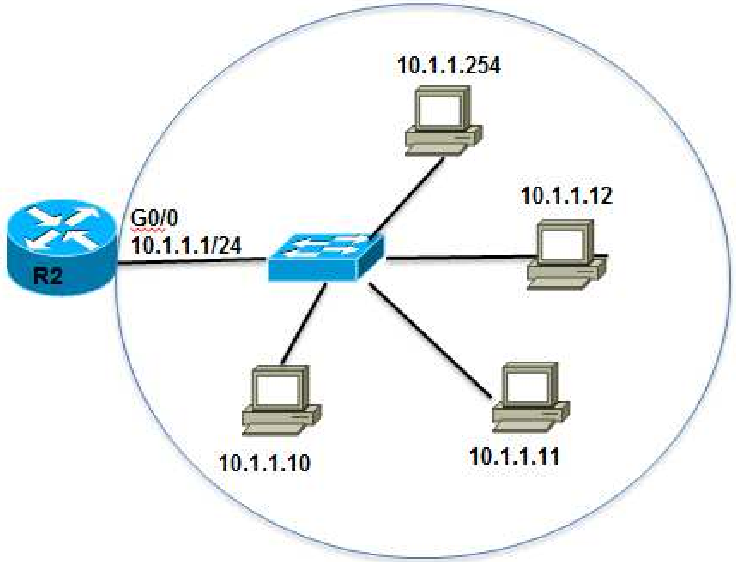


10.1.1.0/24

Network Portion			Host Portion	
10	1	1	0	
00001010	00000001	00000001	00000000	All 0s – NETWORK ADDRESS
10	1	1	10	
00001010	00000001	00000001	00001010	0s and 1s in host portion
10	1	1	255	
00001010	00000001	00000001	11111111	All 1s – BROADCAST ADDRESS

IPv4 Subnet Mask

First Host and Last Host Addresses



10.1.1.0/24

Network Portion			Host Portion	
10	1	1	1	FIRST HOST
00001010	00000001	00000001	00000001	All 0s and a 1 in the host portion
10	1	1	254	LAST HOST
00001010	00000001	00000001	11111110	All 1s and a 0 in the host portion

IPv4 Subnet Mask

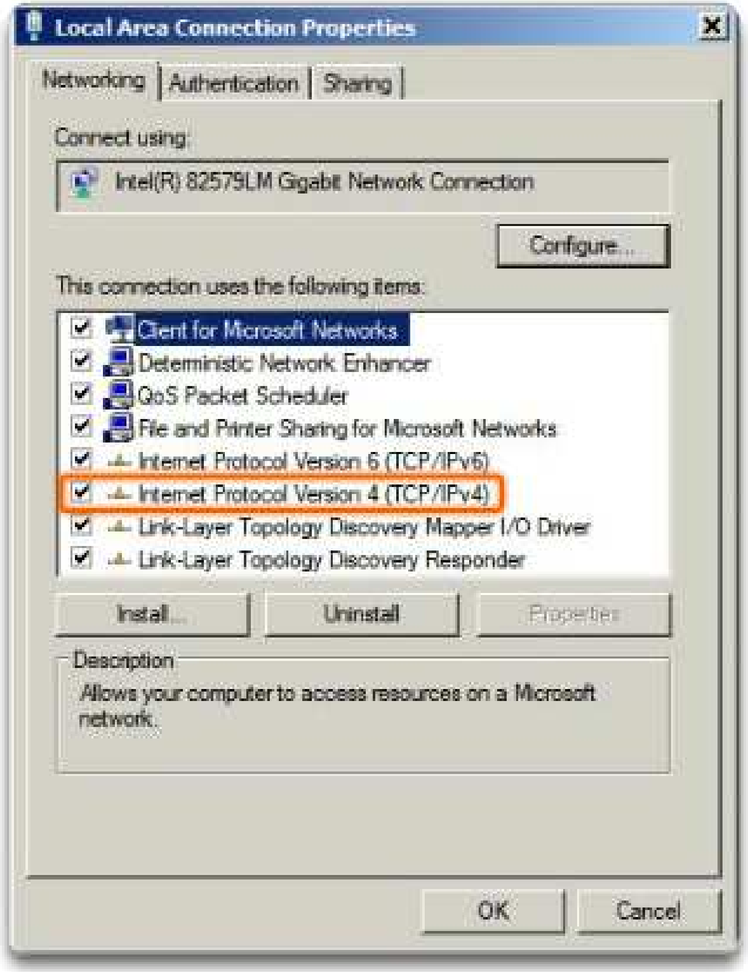
Bitwise AND Operation

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

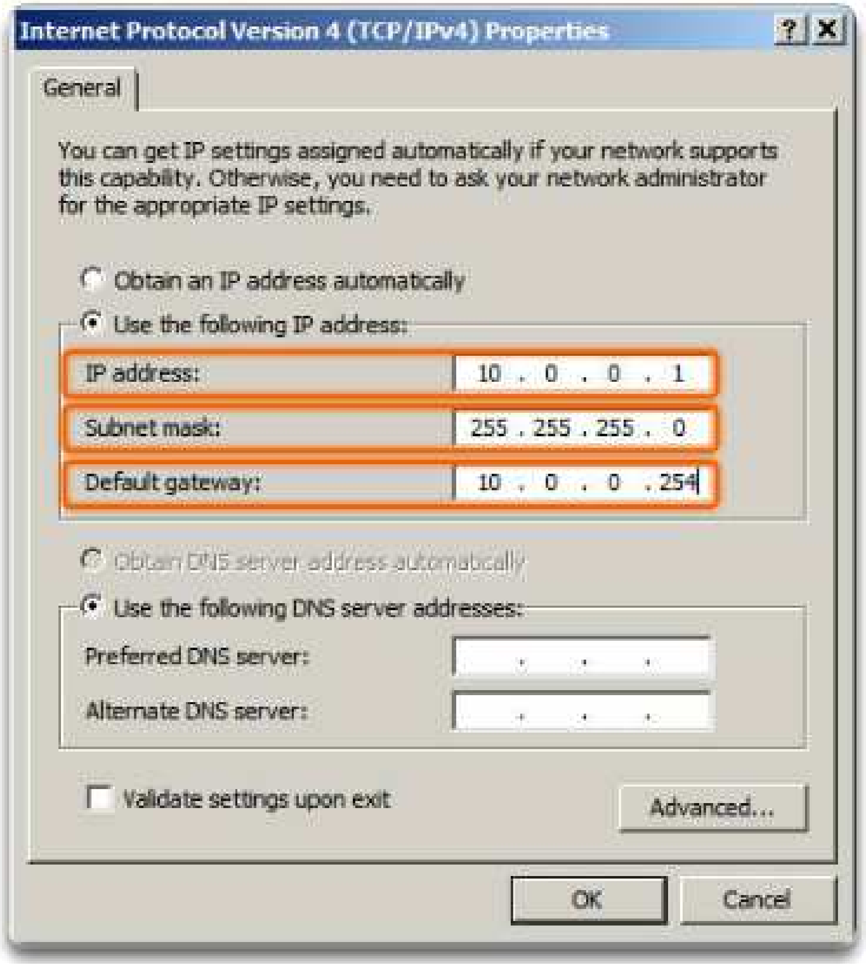
IPv4 Address	192 .	168 .	10 .	10
	11000000	10101000	00001010	00001010
Subnet Mask	255 .	255 .	255 .	0
	11111111	11111111	11111111	00000000
Network Address	192 .	168 .	10 .	0
	11000000	10101000	00001010	00000000

Assigning a Static IPv4 Address to a Host

LAN Interface Properties

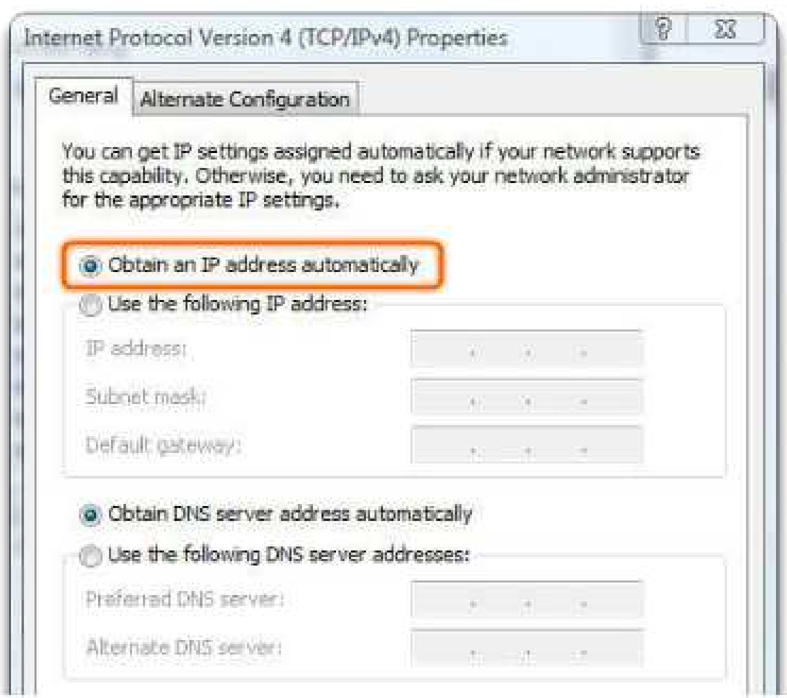


Configuring a Static IPv4 Address



IPv4 Unicast, Broadcast, and Multicast

Assigning a Dynamic IPv4 Address to a Host



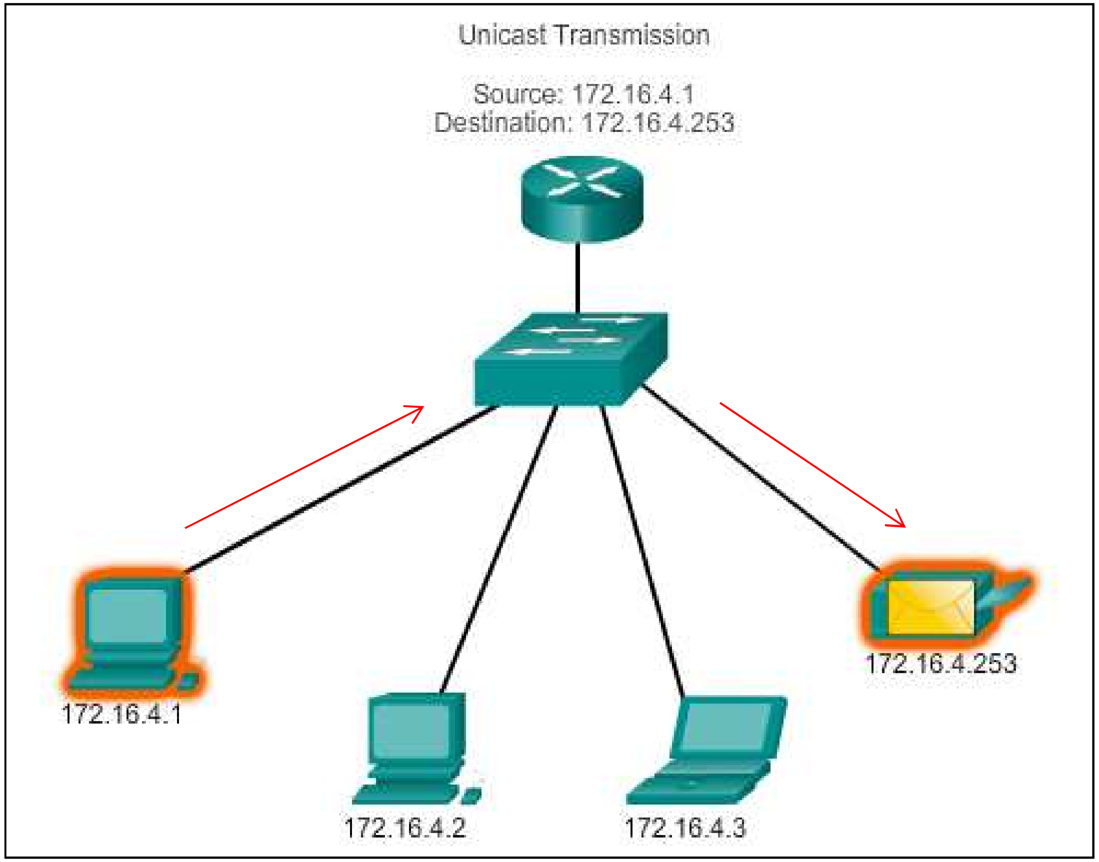
DHCP – The preferred method of assigning IPv4 addresses to hosts on large networks because it reduces the burden on network support staff and virtually eliminates entry errors.

IPv4 Unicast, Broadcast, and Multicast

Unicast Transmission

In an IPv4 network, the hosts can communicate one of three different ways: **Unicast**, Broadcast, and Multicast

#1 Unicast – the process of sending a packet from one host to an individual host.



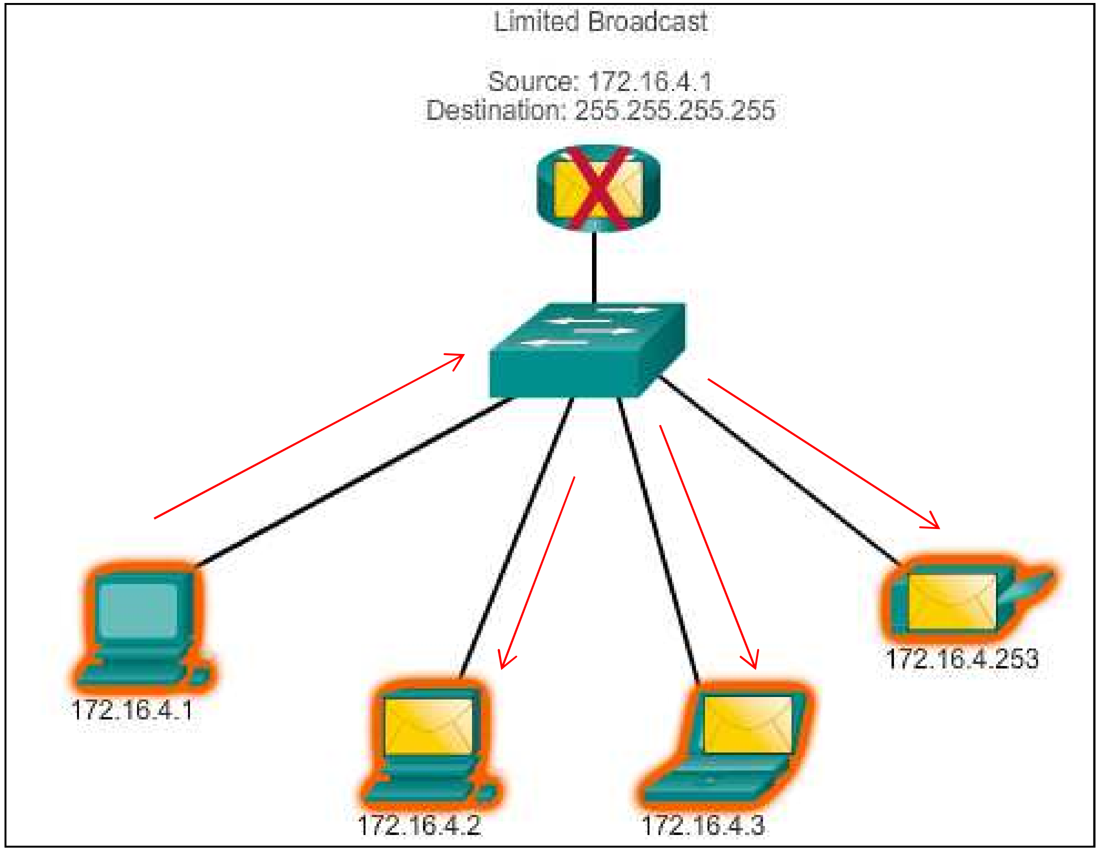
Broadcast Transmission

In an IPv4 network, the hosts can communicate one of three different ways: Unicast, **Broadcast**, and Multicast.

#2 Broadcast – the process of sending a packet from one host to all hosts in the network.

NOTE: Routers do not forward a limited broadcast!

Directed broadcast
- Destination 172.16.4.255
- Hosts within the 172.16.4.0/24 network



Multicast Transmission

In an IPv4 network, the hosts can communicate one of three different ways: Unicast, Broadcast, and **Multicast.**

#3 Multicast – The process of sending a packet from one host to a selected group of hosts, possibly in different networks.

- Reduces traffic
- Reserved for addressing multicast groups – 224.0.0.0 to 239.255.255.255.
- Link local – 224.0.0.0 to 224.0.0.255 (Example: routing information exchanged by routing protocols)
- Globally scoped addresses – 224.0.1.0 to 238.255.255.255 (Example: 224.0.1.1 has been reserved for Network Time Protocol)

Public and Private IPv4 Addresses

Private address blocks are:

- Hosts that do not require access to the Internet can use private addresses
  - 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)

Shared address space addresses:

- Not globally routable
- Intended only for use in service provider networks
- Address block is 100.64.0.0/10

Special Use IPv4 Addresses

- **Network and Broadcast addresses** – within each network the first and last addresses cannot be assigned to hosts
- **Loopback address** – 127.0.0.1 a special address that hosts use to direct traffic to themselves (addresses 127.0.0.0 to 127.255.255.255 are reserved)
- **Link-Local address** – 169.254.0.0 to 169.254.255.255 (169.254.0.0/16) addresses can be automatically assigned to the local host
- **TEST-NET addresses** – 192.0.2.0 to 192.0.2.255 (192.0.2.0/24) set aside for teaching and learning purposes, used in documentation and network examples
- **Experimental addresses** – 240.0.0.0 to 255.255.255.254 are listed as reserved

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	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

Legacy Classful Addressing (cont.)

Classless Addressing

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

Types of IPv4 Address

Assignment of IP Addresses

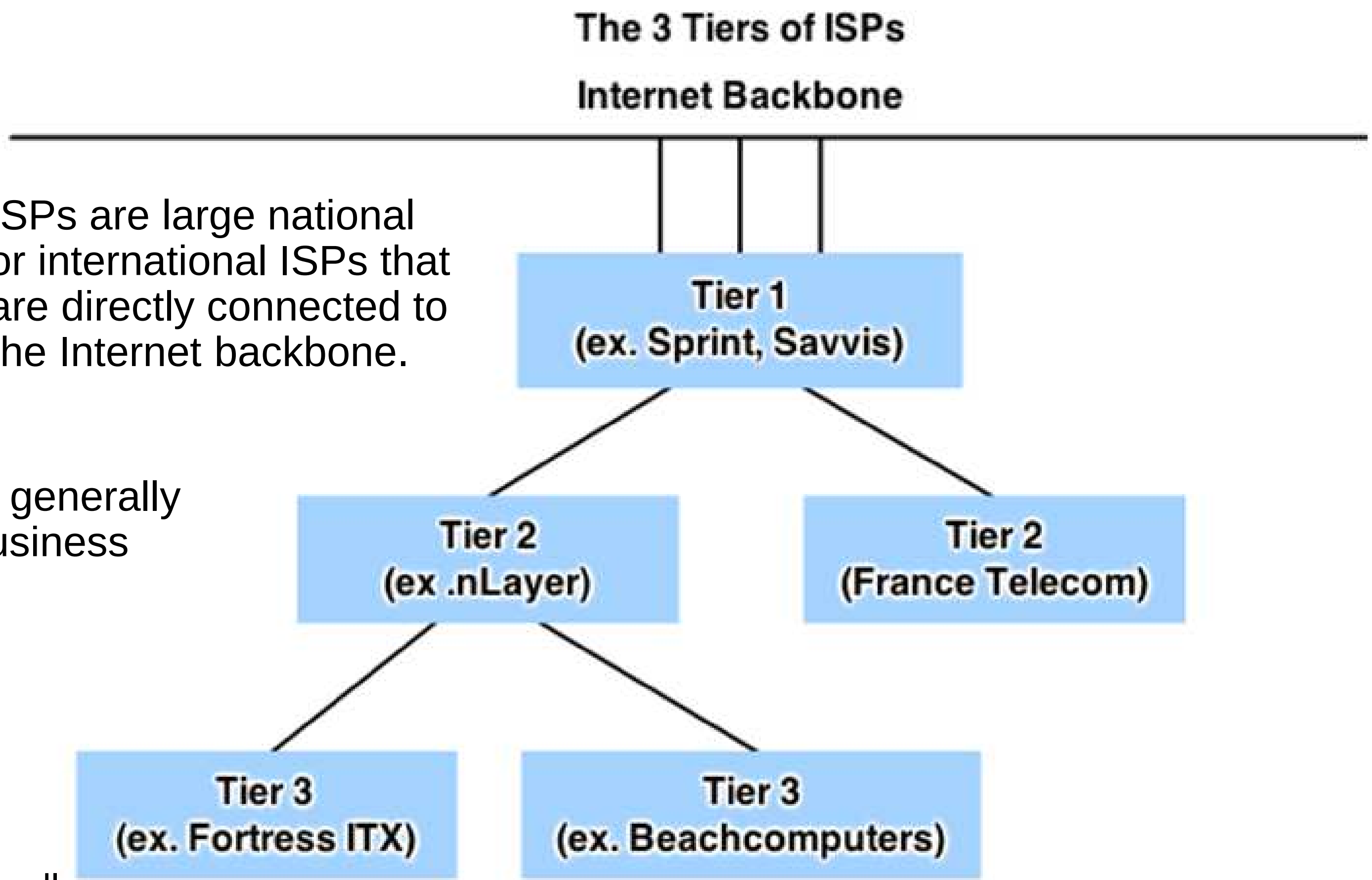
Regional Internet Registries (RIRs)

Types of IPv4 Address

Assignment of IP Addresses (Cont.)

ISPs are large national or international ISPs that are directly connected to the Internet backbone.

Tier 2 ISPs generally focus on business customers.



Tier 3 ISPs often bundle Internet connectivity as a part of network and computer service contracts for their customers.

Tier 3 ISPs purchase their Internet service from Tier 2 ISPs.

Network Address Translation for IPv4

NAT Characteristics

IPv4 Private Address Space

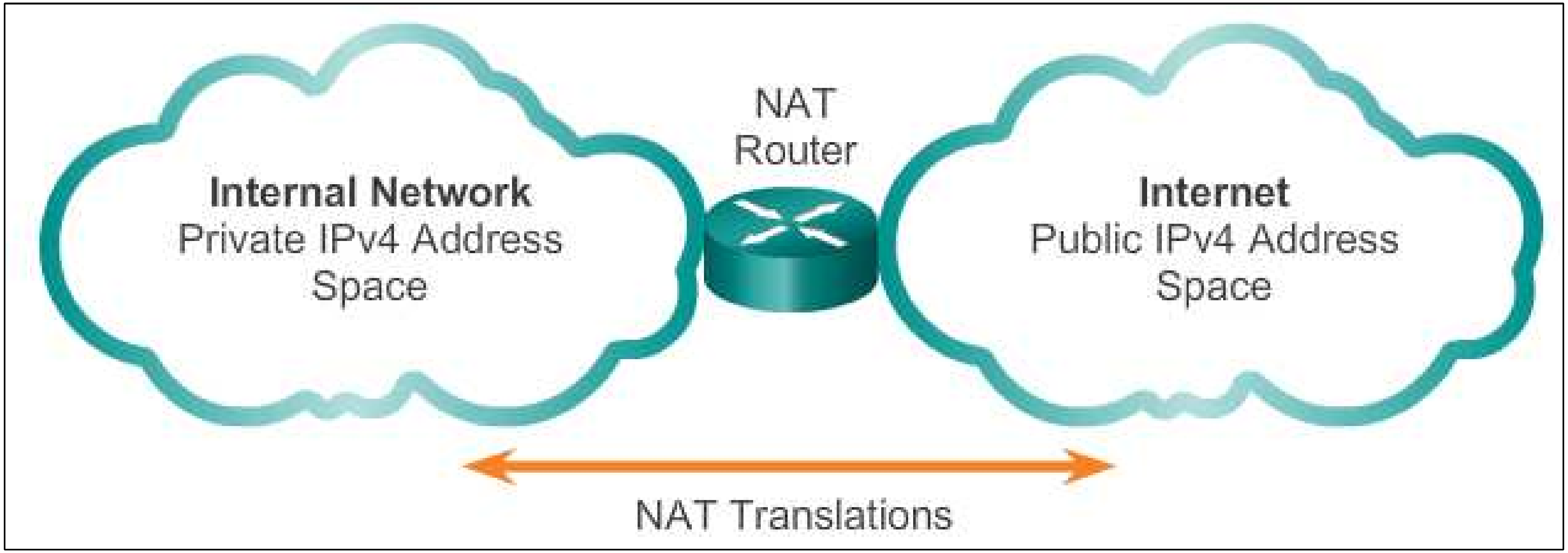
- IPv4 address space is not big enough to uniquely address all the devices that must be connected to the Internet.
- Network private addresses are described in RFC 1918 and are to designed to be used within an organization or site only.
- Private addresses are not routed by Internet routers while public addresses are.
- Private addresses can alleviate IPv4 scarcity, but because they aren't routed by Internet devices, they first need to be translated.
- NAT is process used to perform such translation.

NAT Characteristics

IPv4 Private Address Space

Private Internet addresses are defined in RFC 1918:

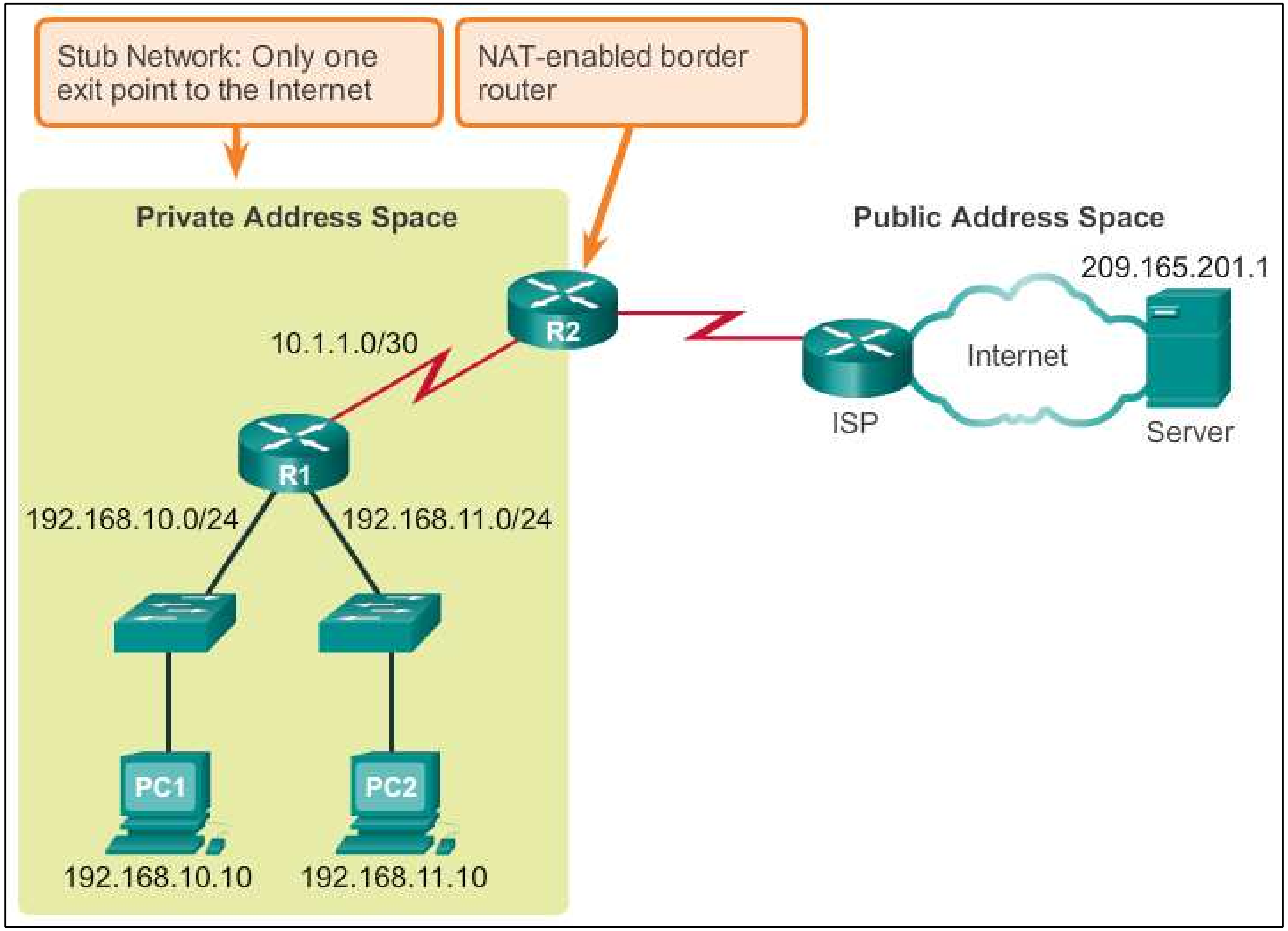
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16



NAT Characteristics
What is NAT?

- NAT is a process used to translate network addresses.
- NAT's primary use is to conserve public IPv4 addresses.
- NAT is usually implemented at border network devices, such as firewalls or routers.
- NAT allows the networks to use private addresses internally, only translating to public addresses when needed.
- Devices within the organization can be assigned private addresses and operate with locally unique addresses.
- When traffic must be sent or received to or from other organizations or the Internet, the border router translates the addresses to a public and globally unique address.

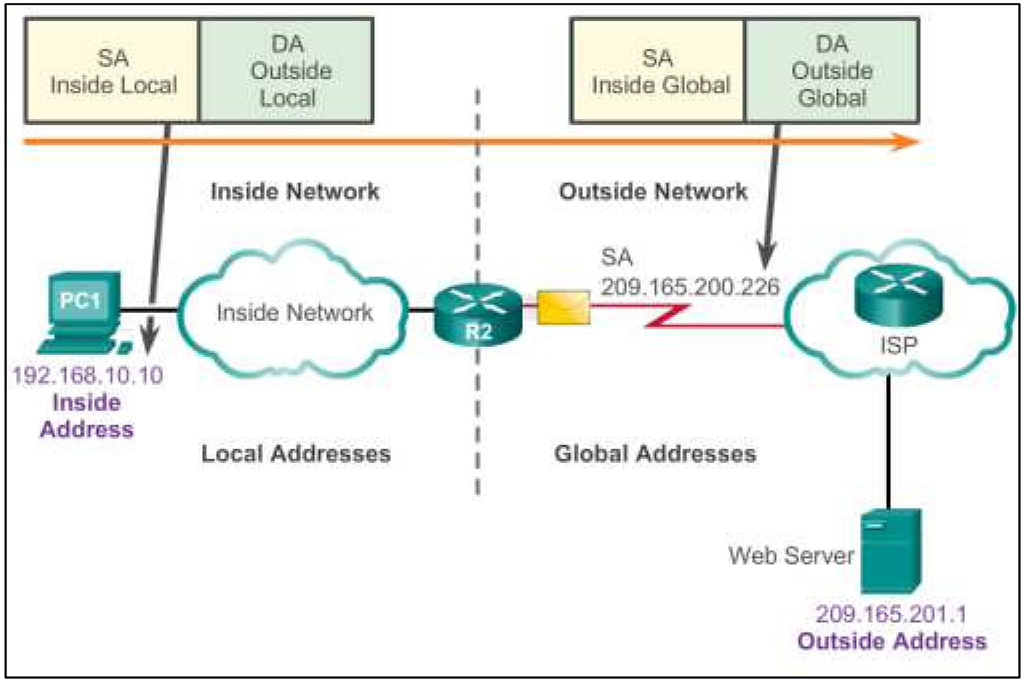
NAT Characteristics
What is NAT? (cont.)



NAT Characteristics

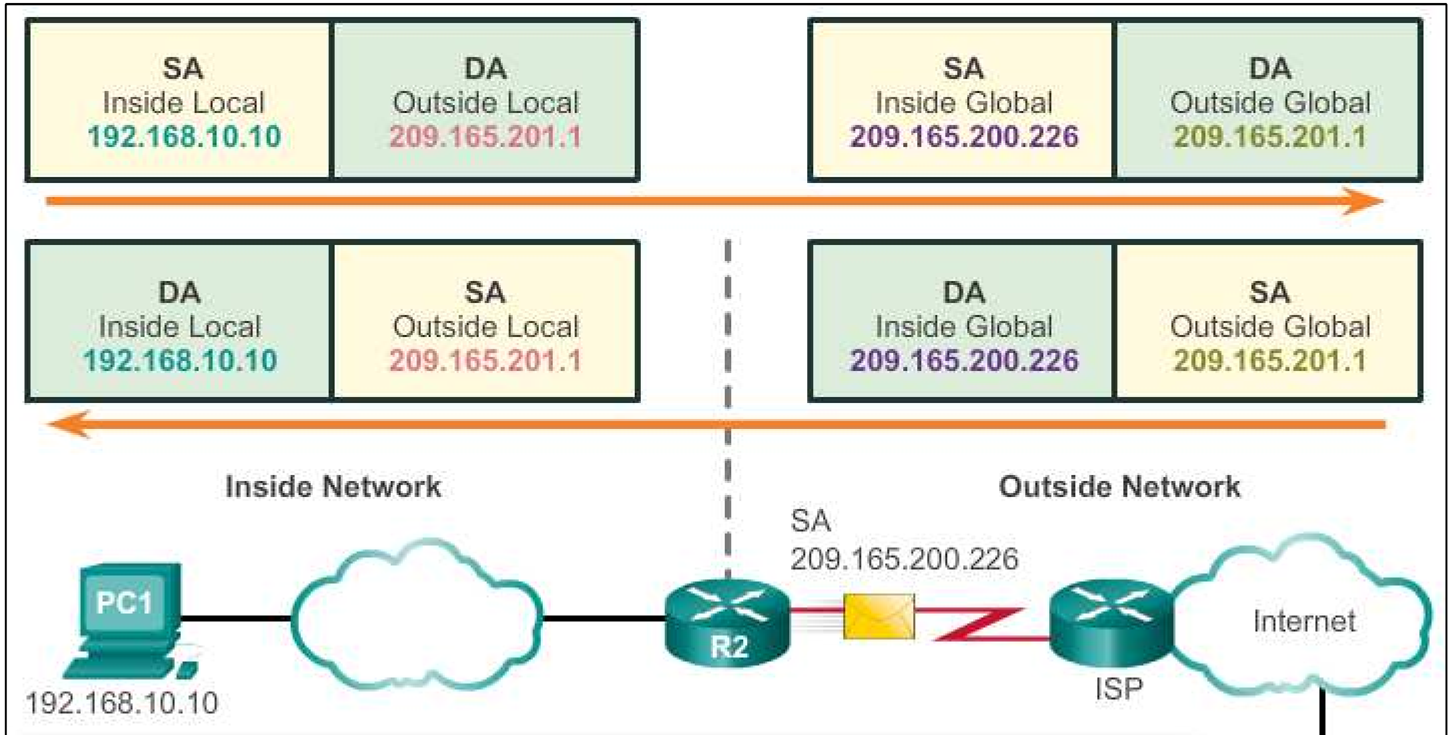
NAT Terminology

- Inside network is the set of devices using private addresses
- Outside network refers to all other networks
- NAT includes four types of addresses:
    - Inside local address
    - Inside global address
    - Outside local address
    - Outside global address



NAT Characteristics

NAT Terminology (cont.)



R2 NAT Table

PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

Types of NAT

Static NAT

- Static NAT uses a one-to-one mapping of local and global addresses.
- These mappings are configured by the network administrator and remain constant.
- Static NAT is particularly useful when servers hosted in the inside network must be accessible from the outside network.
- A network administrator can SSH to a server in the inside network by pointing the SSH client to the proper inside global address.

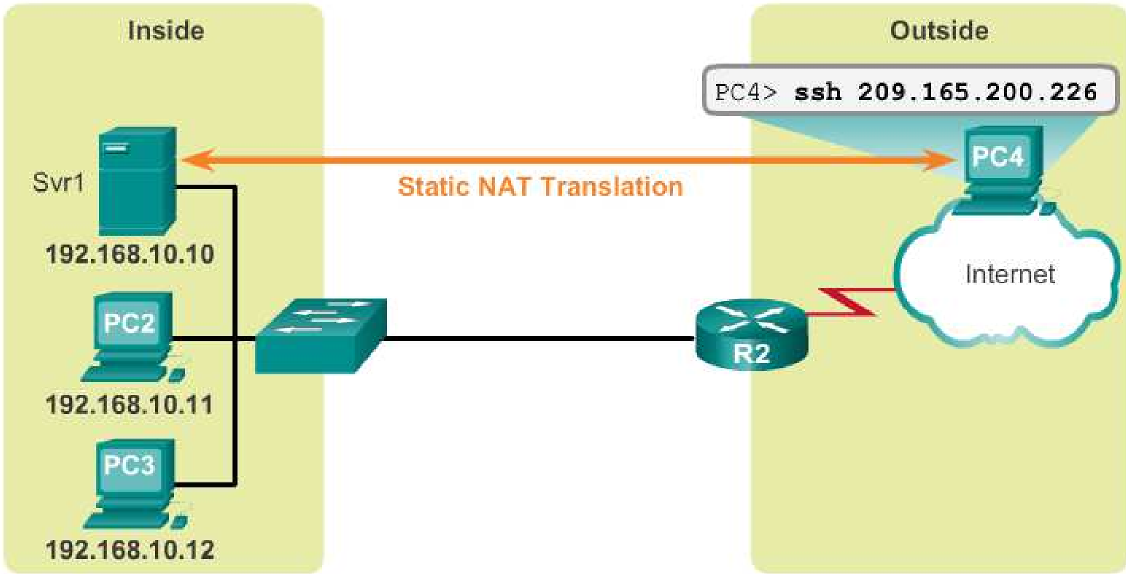
Types of NAT

Static NAT (cont.)

Static NAT

Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



Types of NAT

Dynamic NAT

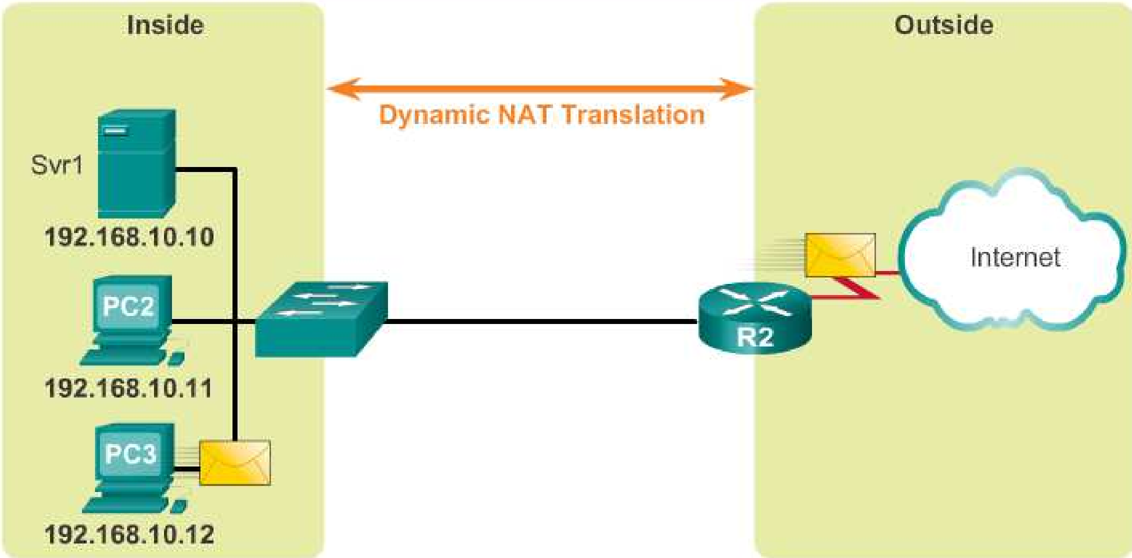
- Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis.
- When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool.
- Dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

Dynamic NAT (cont.)

Dynamic NAT

IPv4 NAT Pool

Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230



Types of NAT

Port Address Translation

- Port Address Translation (PAT) maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.
- PAT uses the pair source port and source IP address to keep track of what traffic belongs to what internal client.
- PAT is also known as NAT overload.
- By also using the port number, PAT forwards the response packets to the correct internal device.
- The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session.

Comparing NAT and PAT

- NAT translates IPv4 addresses on a 1:1 basis between private IPv4 addresses and public IPv4 addresses.
- PAT modifies both the address and the port number.
- NAT forwards incoming packets to their inside destination by referring to the incoming source IPv4 address provided by the host on the public network.
- With PAT, there is generally only one or a very few publicly exposed IPv4 addresses.
- PAT is able to translate protocols that do not use port numbers, such as ICMP; each one of these protocols is supported differently by PAT.

Benefits of NAT

- Conserves the legally registered addressing scheme
- Increases the flexibility of connections to the public network
- Provides consistency for internal network addressing schemes
- Provides network security

Benefits of NAT

Disadvantages of NAT

- Performance is degraded
- End-to-end functionality is degraded
- End-to-end IP traceability is lost
- Tunneling is more complicated
- Initiating TCP connections can be disrupted

IPv6 Network Addresses

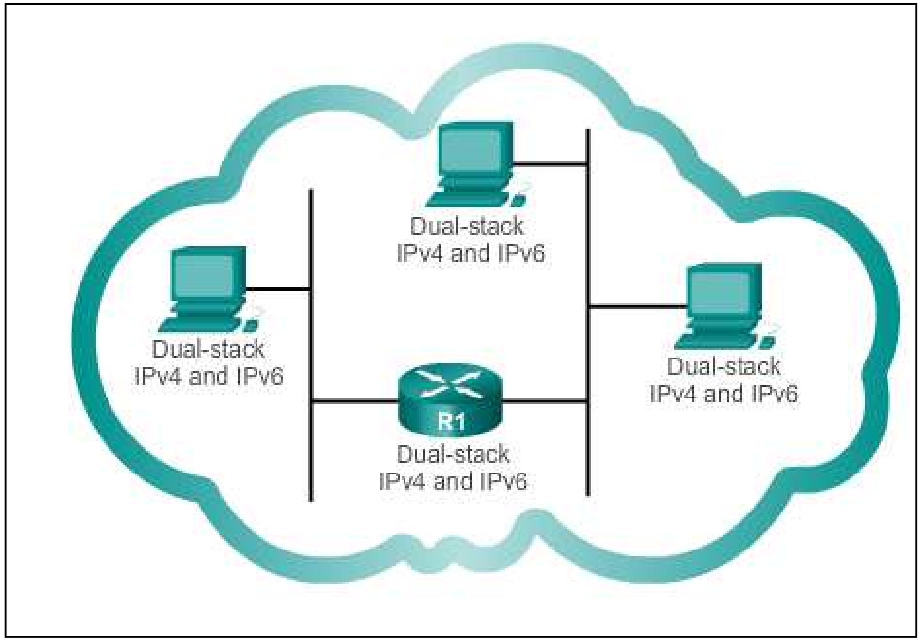
The Need for IPv6

- IPv6 is designed to be the successor to IPv4.
- Depletion of IPv4 address space has been the motivating factor for moving to IPv6.
- Projections show that all five RIRs will run out of IPv4 addresses between 2015 and 2020.
- With an increasing Internet population, a limited IPv4 address space, issues with NAT and an Internet of things, the time has come to begin the transition to IPv6!
- IPv4 has a theoretical maximum of 4.3 billion addresses, plus private addresses in combination with NAT.
- IPv6 larger 128-bit address space provides for 340 undecillion addresses.
- IPv6 fixes the limitations of IPv4 and includes additional enhancements, such as ICMPv6.

IPv4 and IPv6 Coexistence

The migration techniques can be divided into three categories: Dual-stack, Tunnelling, and Translation.

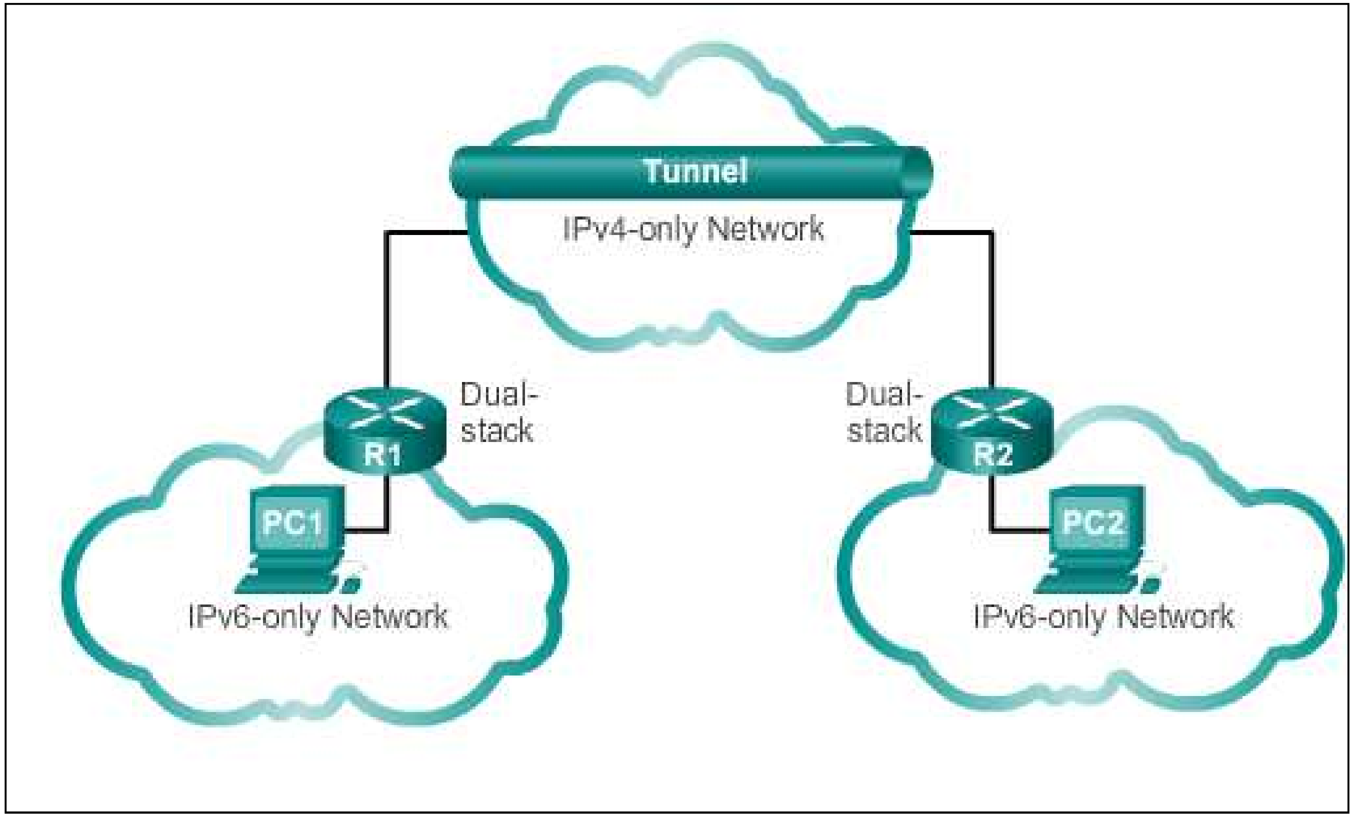
Dual-stack



Dual-stack: Allows IPv4 and IPv6 to coexist on the same network. Devices run both IPv4 and IPv6 protocol stacks simultaneously.

IPv4 and IPv6 Coexistence (cont.)

Tunnelling

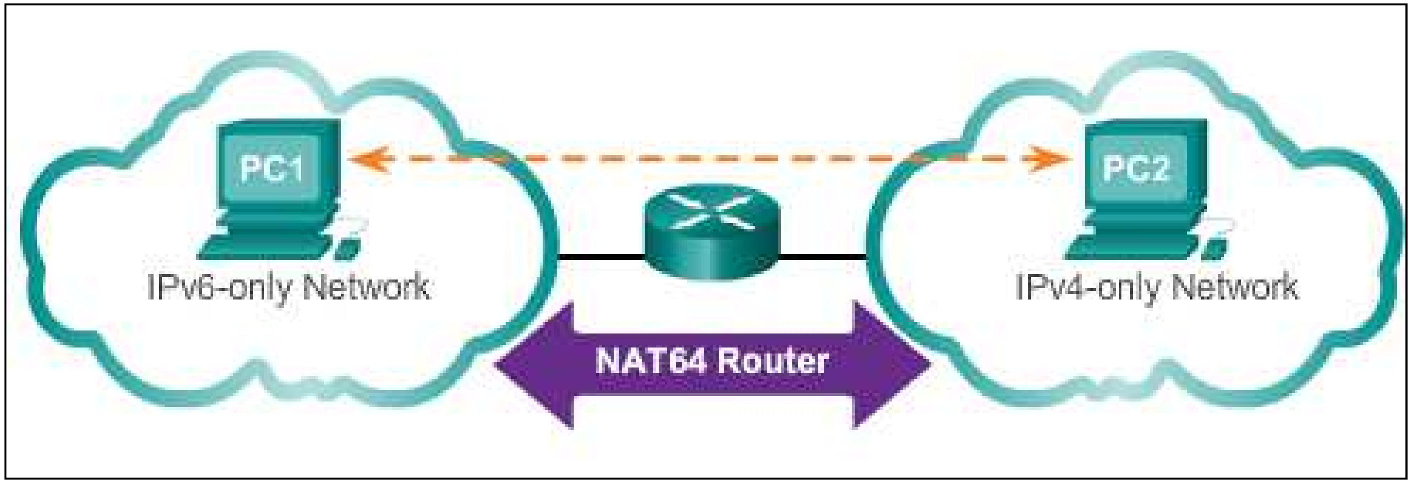


Tunnelling: A method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.

IPv4 Issues

IPv4 and IPv6 Coexistence (cont.)

Translation



Translation: The 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.

Hexadecimal Number System

- Hexadecimal is a base sixteen system.
- Base 16 numbering system uses the numbers 0 to 9 and the letters A to F.
- Four bits (half of a byte) can be represented with a single hexadecimal value.

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 Number System (cont.)

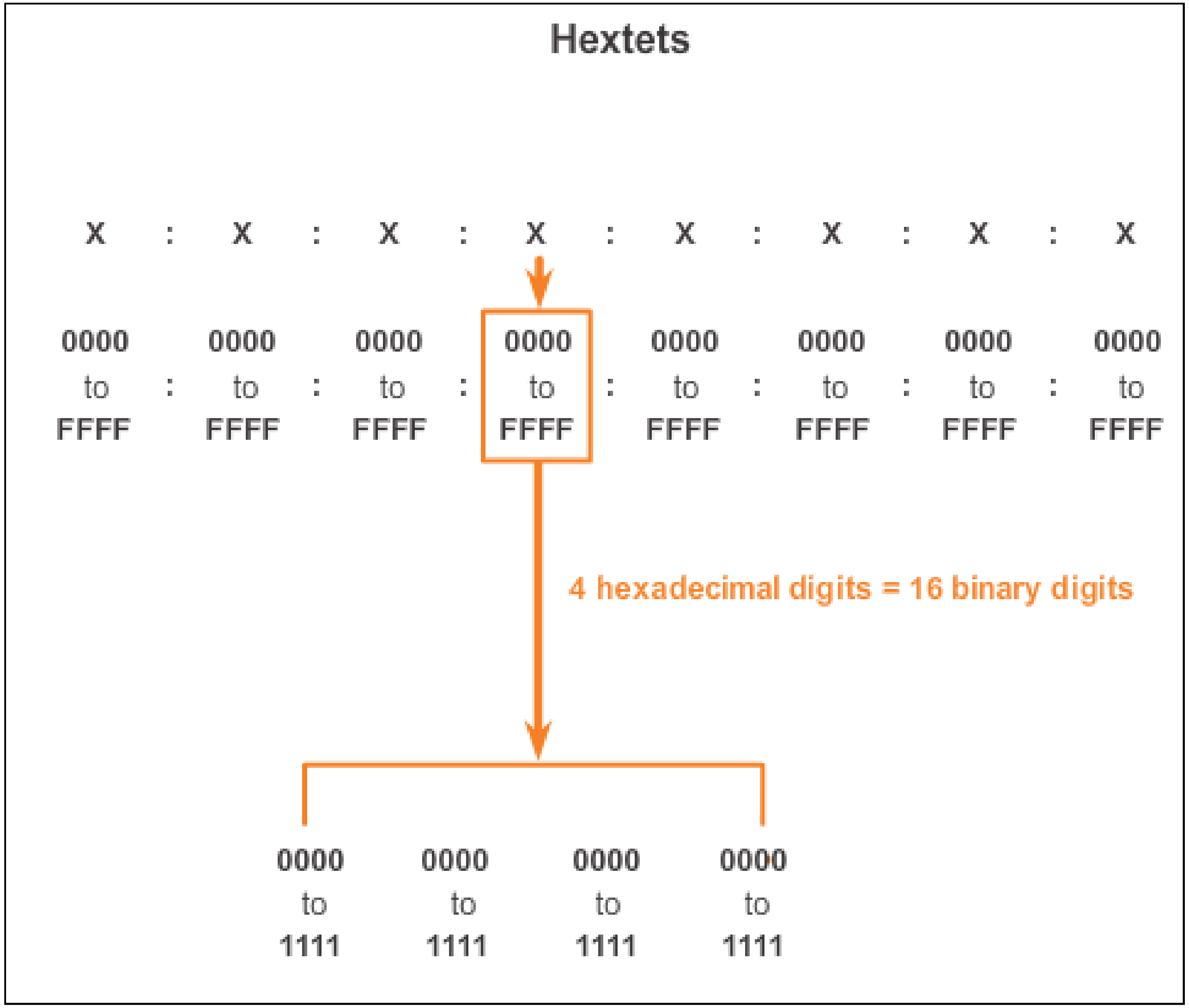
Look at the binary bit patterns that match the decimal and hexadecimal values

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

IPv6 Address Representation

- 128 bits in length and written as a string of hexadecimal values
- In IPv6, 4 bits represents a single hexadecimal digit, 32 hexadecimal value = IPv6 address
  - **2001:0DB8:0000:1111:0000:0000:0000:0200**
  - **FE80:0000:0000:0000:0123:4567:89AB:CDEF**
- Hextet used to refer to a segment of 16 bits or four hexadecimals
- Can be written in either lowercase or uppercase

IPv6 Address Representation (cont.)



Rule 1- Omitting Leading 0s

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

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

Rule 2 - Omitting All 0 Segments

- A double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0's.
- Double colon (::) can only be used once within an address otherwise the address will be ambiguous.
- Known as the *compressed format.*
- Incorrect address - 2001:0DB8::ABCD::1234.

Rule 2 - Omitting All 0 Segments (cont.)

Example #1

Preferred	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Omit 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

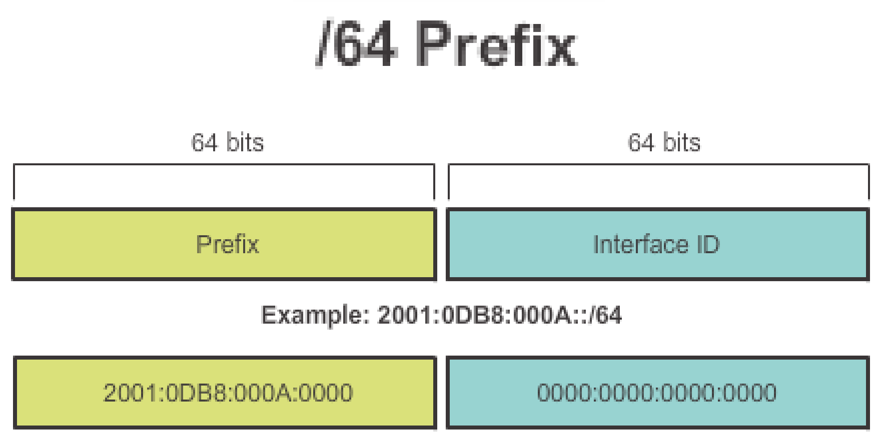
Only one :: may be used.

Example #2

Preferred	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Omit leading 0s	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compressed	FE80::123:4567:89AB:CDEF

IPv6 Prefix Length

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



IPv6 Address Types

There are three types of IPv6 addresses:

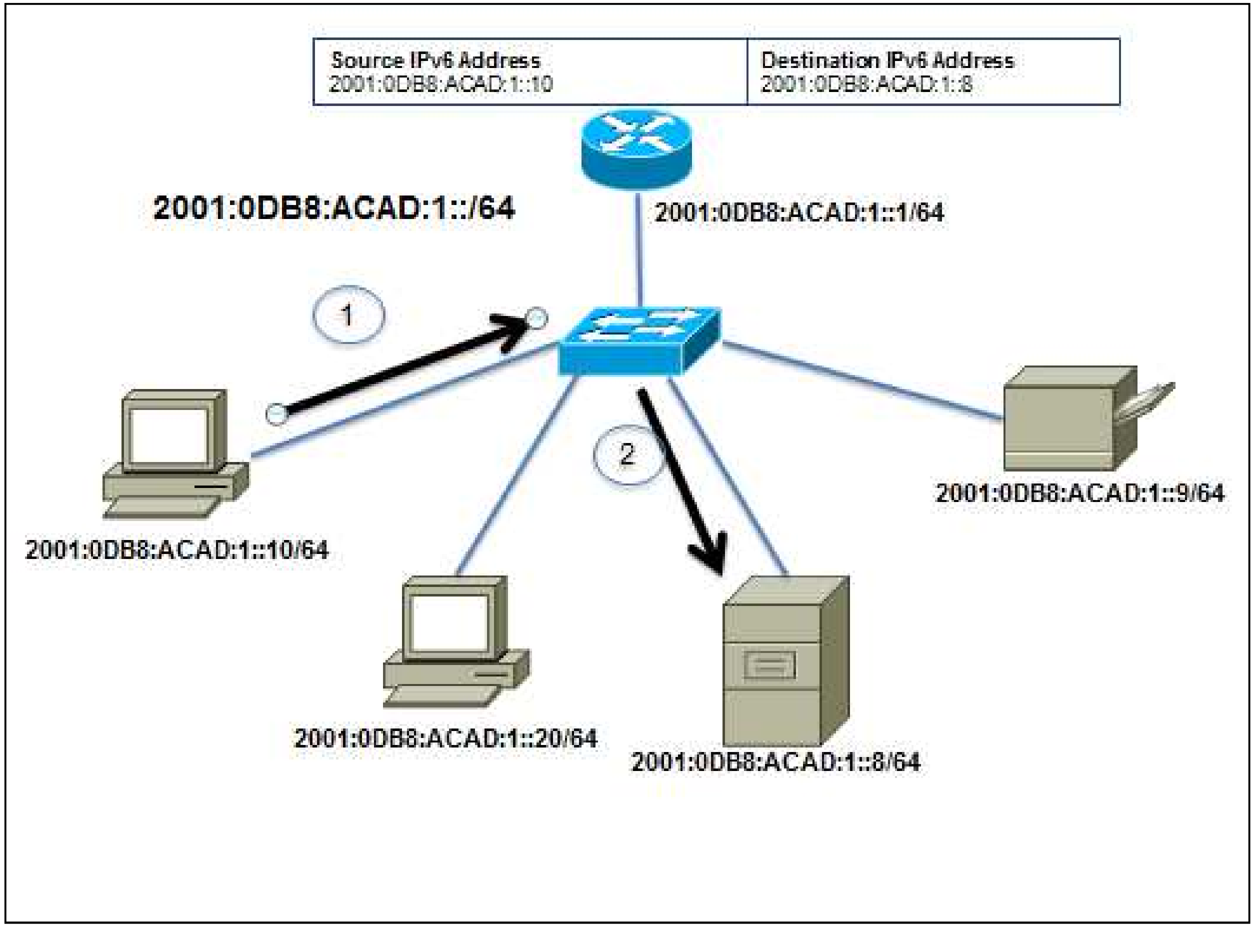
- Unicast
- Multicast
- Anycast.

Note: IPv6 does not have broadcast addresses.

IPv6 Unicast Addresses

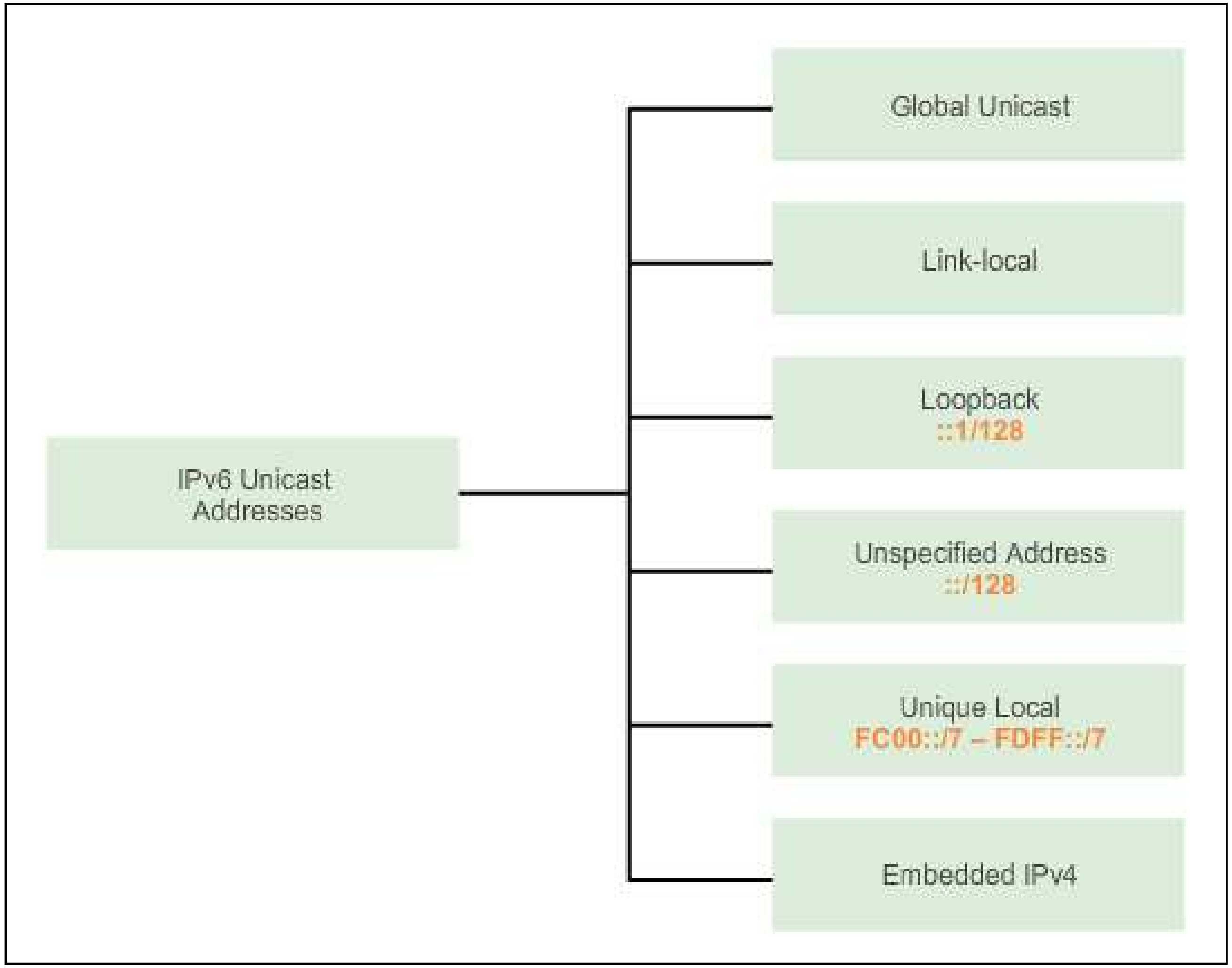
Unicast

- 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.



Types of IPv6 Addresses

IPv6 Unicast Addresses (cont.)



IPv6 Unicast Addresses (cont.)

Global Unicast

- Similar to a public IPv4 address
- Globally unique
- Internet routable addresses
- Can be configured statically or assigned dynamically

Link-local

- Used to communicate with other devices on the same local link
- Confined to a single link; not routable beyond the link

IPv6 Unicast Addresses (cont.)

Loopback

- Used by a host to send a packet to itself and cannot be assigned to a physical interface.
- Ping an IPv6 loopback address to test the configuration of TCP/IP on the local host.
- All-0s except for the last bit, represented as ::1/128 or just ::1.

Unspecified Address

- All-0's address represented as ::/128 or just ::
- Cannot be assigned to an interface and is only used as a source address.
- An unspecified address is used as a source address when the device does not yet have a permanent IPv6 address or when the source of the packet is irrelevant to the destination.

IPv6 Unicast Addresses (cont.)

Unique Local

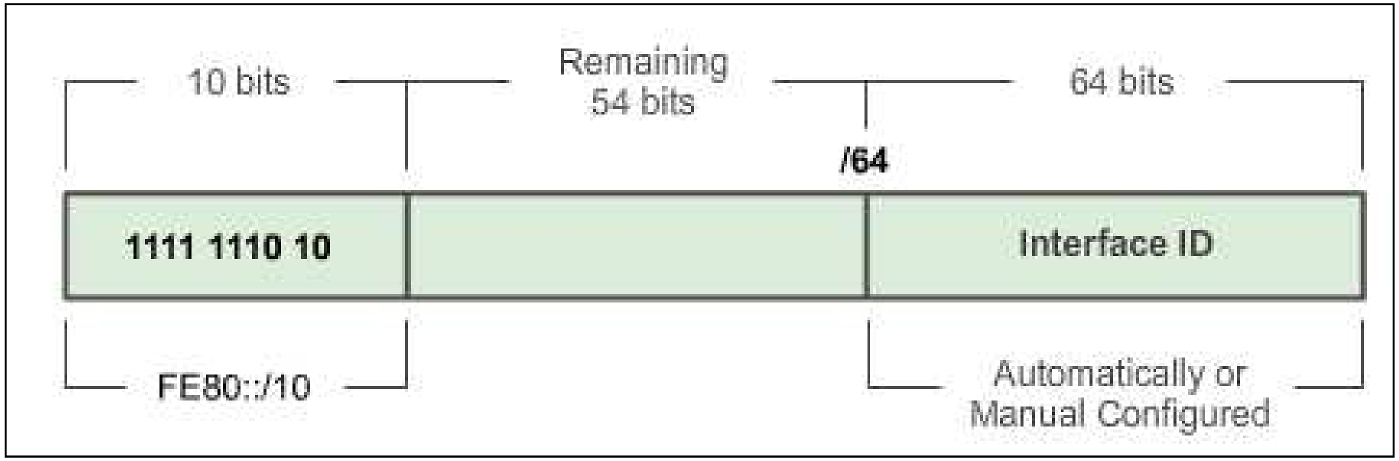
- Similar to private addresses for IPv4.
- Used for local addressing within a site or between a limited number of sites.
- In the range of FC00::/7 to FDFF::/7.

IPv4 Embedded (not covered in this course)

- Used to help transition from IPv4 to IPv6.

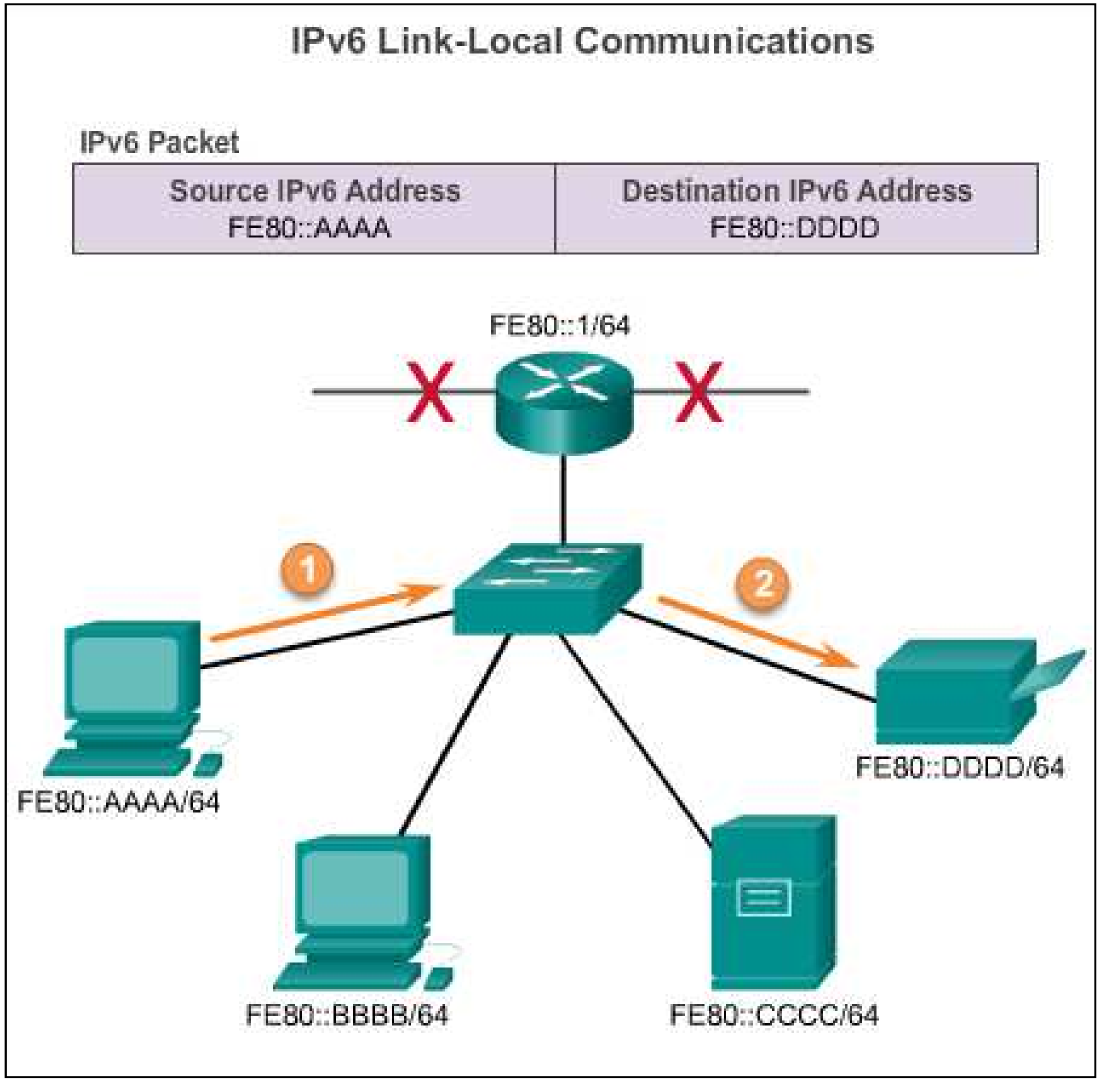
IPv6 Link-Local Unicast Addresses

- Every IPv6-enabled network interface is REQUIRED to have a link-local address
- Enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet)
- FE80::/10 range, first 10 bits are 1111 1110 10xx xxxx
- 1111 1110 1000 0000 (FE80) - 1111 1110 1011 1111 (FEBF)



IPv6 Link-Local Unicast Addresses (cont.)

Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.

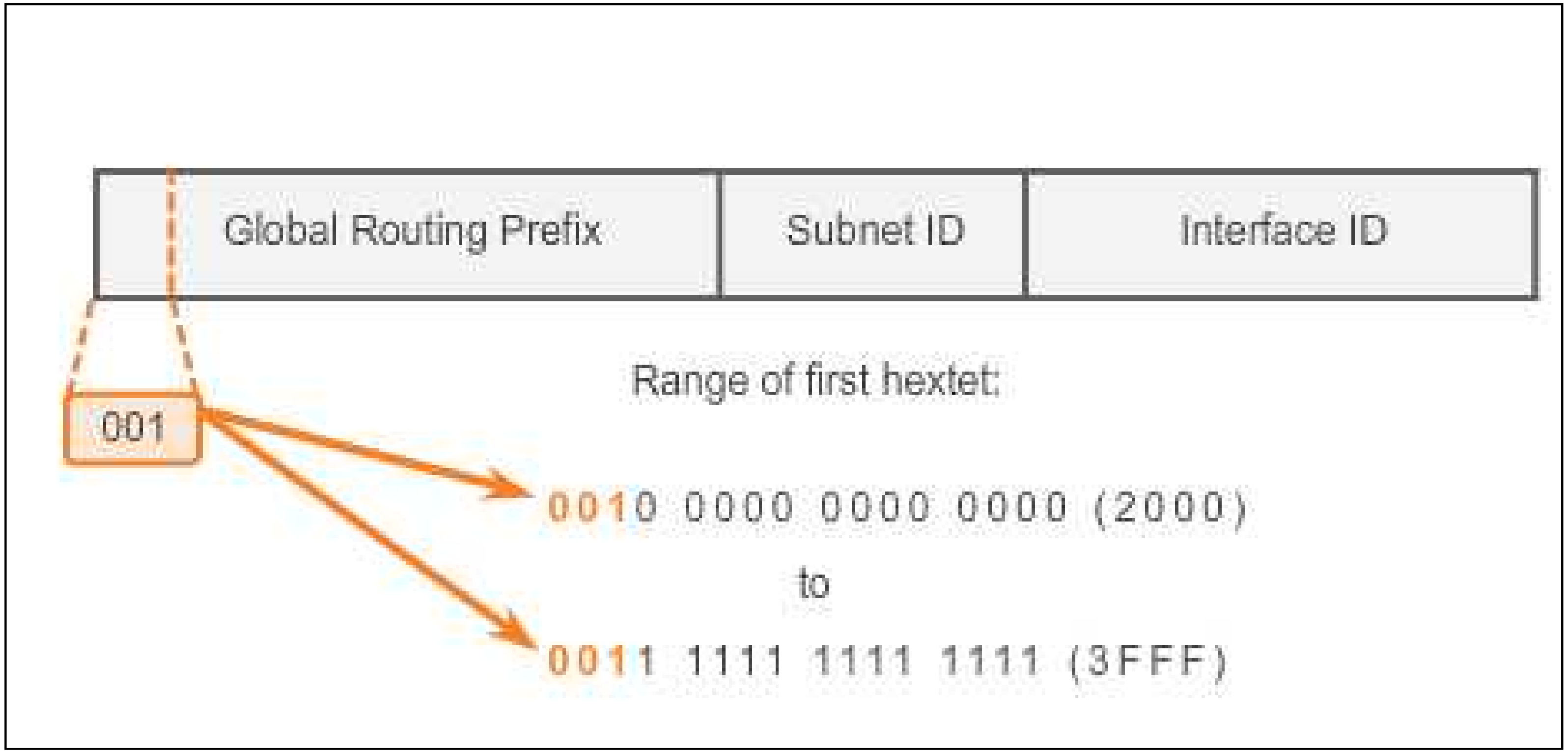


Structure of an IPv6 Global Unicast Address

- IPv6 global unicast addresses are globally unique and routable on the IPv6 Internet
- Equivalent to public IPv4 addresses
- ICANN allocates IPv6 address blocks to the five RIRs

Structure of an IPv6 Global Unicast Address (cont.)

Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned



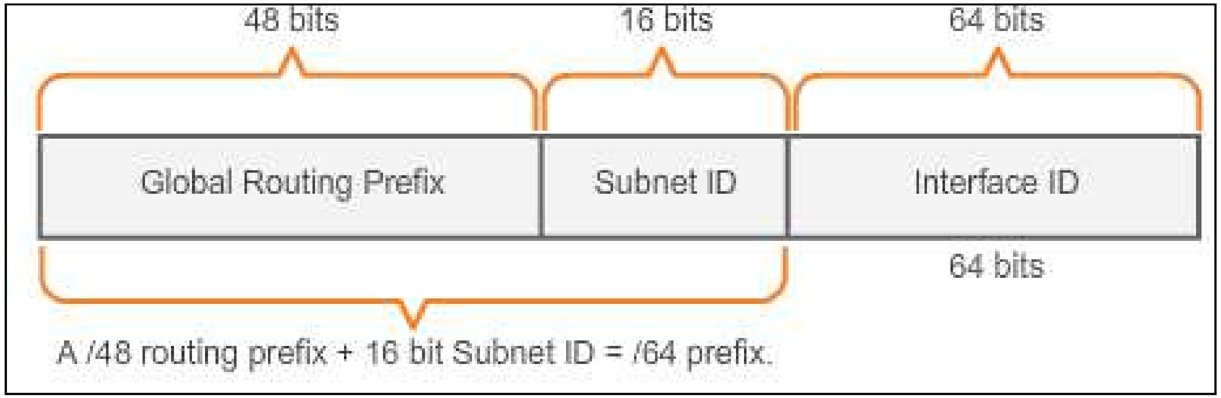
IPv6 Unicast Addresses

Structure of an IPv6 Global Unicast Address (cont.)

A global unicast address has three parts: Global Routing Prefix, Subnet ID, and Interface ID.

- **Global Routing Prefix** is the prefix or network portion of the address assigned by the provider, such as an ISP, to a customer or site, currently, RIR's assign a /48 global routing prefix to customers.
- 2001:0DB8:ACAD::/48 has a prefix that indicates that the first 48 bits (2001:0DB8:ACAD) is the prefix or network portion.

IPv6 /48 Global Routing Prefix

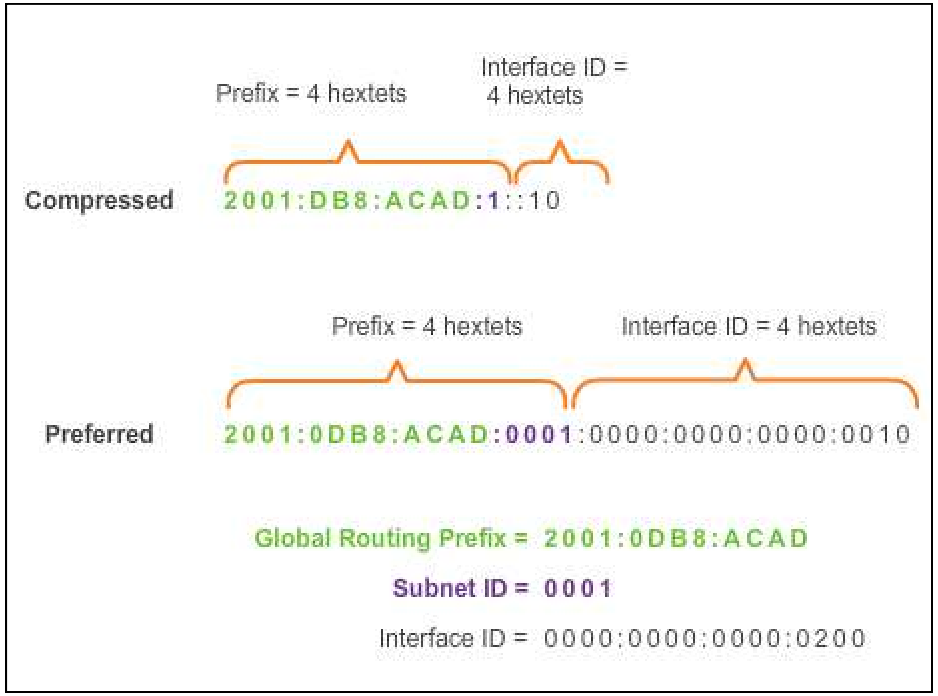


IPv6 Unicast Addresses

Structure of an IPv6 Global Unicast Address (cont.)

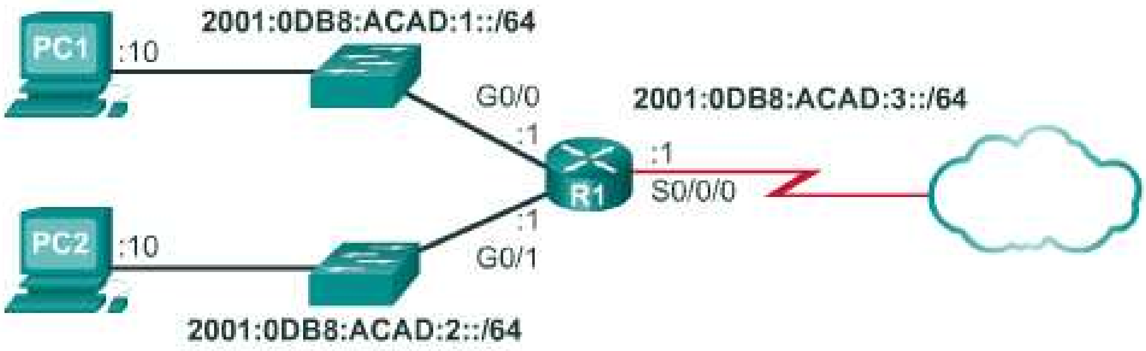
- **Subnet ID** is used by an organization to identify subnets within its site
- **Interface ID**
  - Equivalent to the host portion of an IPv4 address.
  - Used because a single host may have multiple interfaces, each having one or more IPv6 addresses.

Reading a Global Unicast Address



IPv6 Unicast Addresses

Static Configuration of a Global Unicast Address

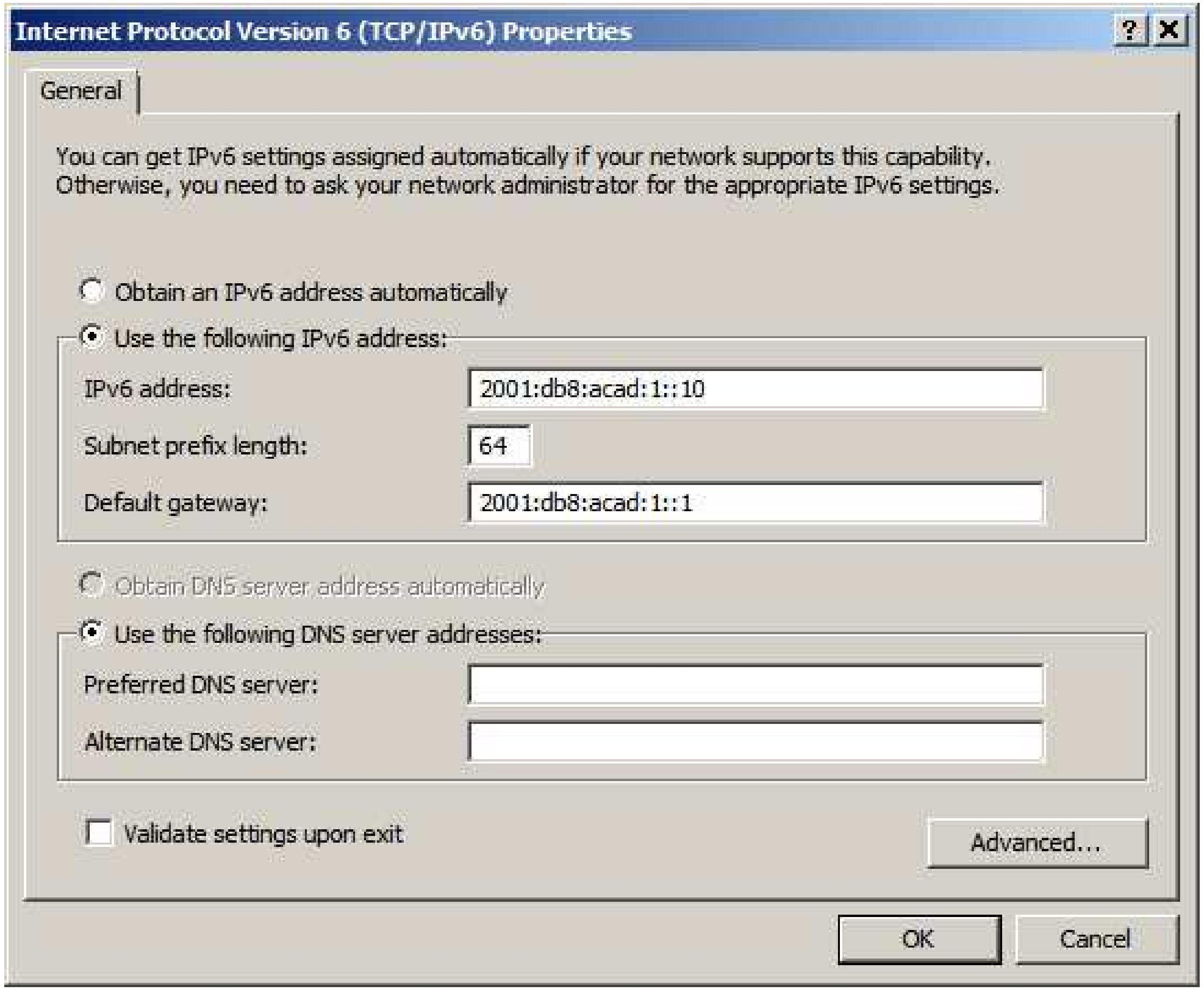



```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial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

IPv6 Unicast Addresses

Static Configuration of an IPv6 Global Unicast Address (cont.)

Windows IPv6 Setup



Dynamic Configuration of a Global Unicast Address using SLAAC

Stateless Address Autoconfiguraton (SLAAC)

- A method that allows a device to obtain its prefix, prefix length and default gateway from an IPv6 router
- No DHCPv6 server needed
- Rely on ICMPv6 Router Advertisement (RA) messages

IPv6 routers

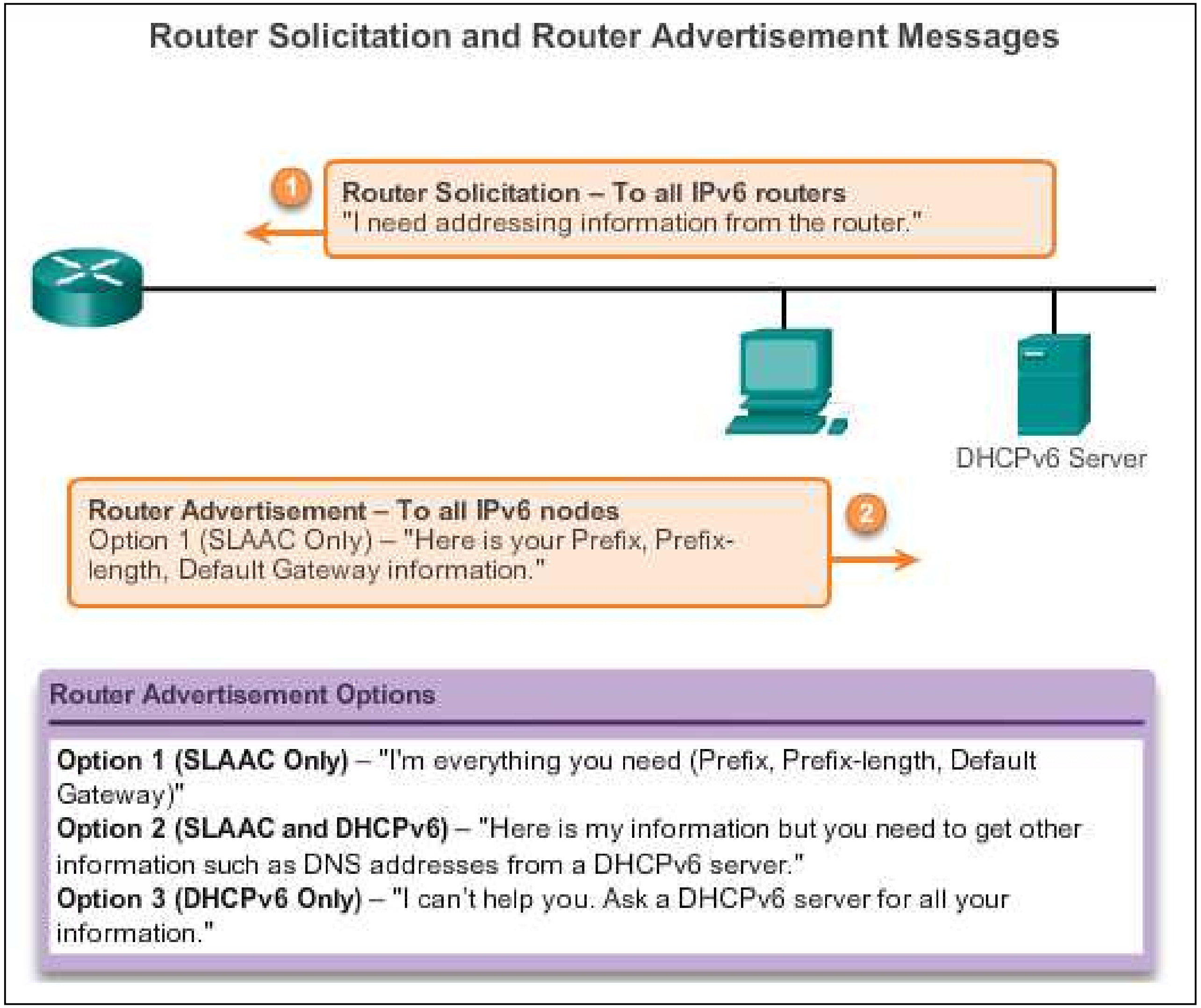
- Forwards IPv6 packets between networks
- Can be configured with static routes or a dynamic IPv6 routing protocol
- Sends ICMPv6 RA messages

Dynamic Configuration of a Global Unicast Address using SLAAC (cont.)

- The **`IPv6 unicast-routing`** command enables IPv6 routing.
- RA message can contain one of the following three options:
  - SLAAC Only – Uses the information contained in the RA message.
  - SLAAC and DHCPv6 – Uses the information contained in the RA message and get other information from the DHCPv6 server, stateless DHCPv6 (for example, DNS).
  - DHCPv6 only – The device should not use the information in the RA, stateful DHCPv6.
- Routers send ICMPv6 RA messages using the link-local address as the source IPv6 address

IPv6 Unicast Addresses

Dynamic Configuration of a Global Unicast Address using SLAAC (cont.)



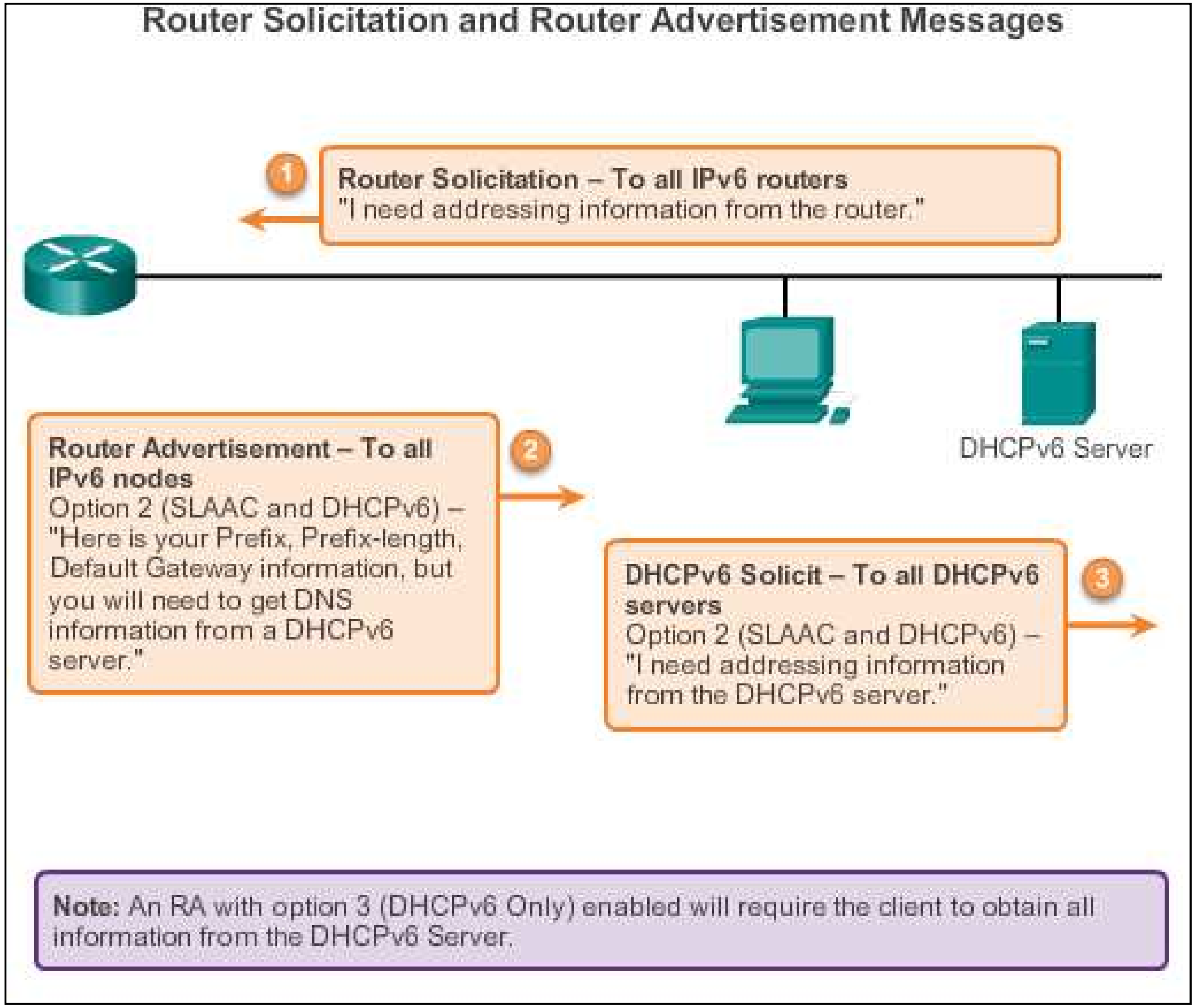
Dynamic Configuration of a Global Unicast Address using DHCPv6 (cont.)

Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

- Similar to IPv4
- Automatically receives 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.
- Device may receive all or some of its IPv6 addressing information from a DHCPv6 server depending upon whether option 2 (SLAAC and DHCPv6) or option 3 (DHCPv6 only) is specified in the ICMPv6 RA message.
- Host may choose to ignore whatever is in the router's RA message and obtain its IPv6 address and other information directly from a DHCPv6 server.

IPv6 Unicast Addresses

Dynamic Configuration of a Global Unicast Address using DHCPv6 (cont.)



EUI-64 Process or Randomly Generated

EUI-64 Process

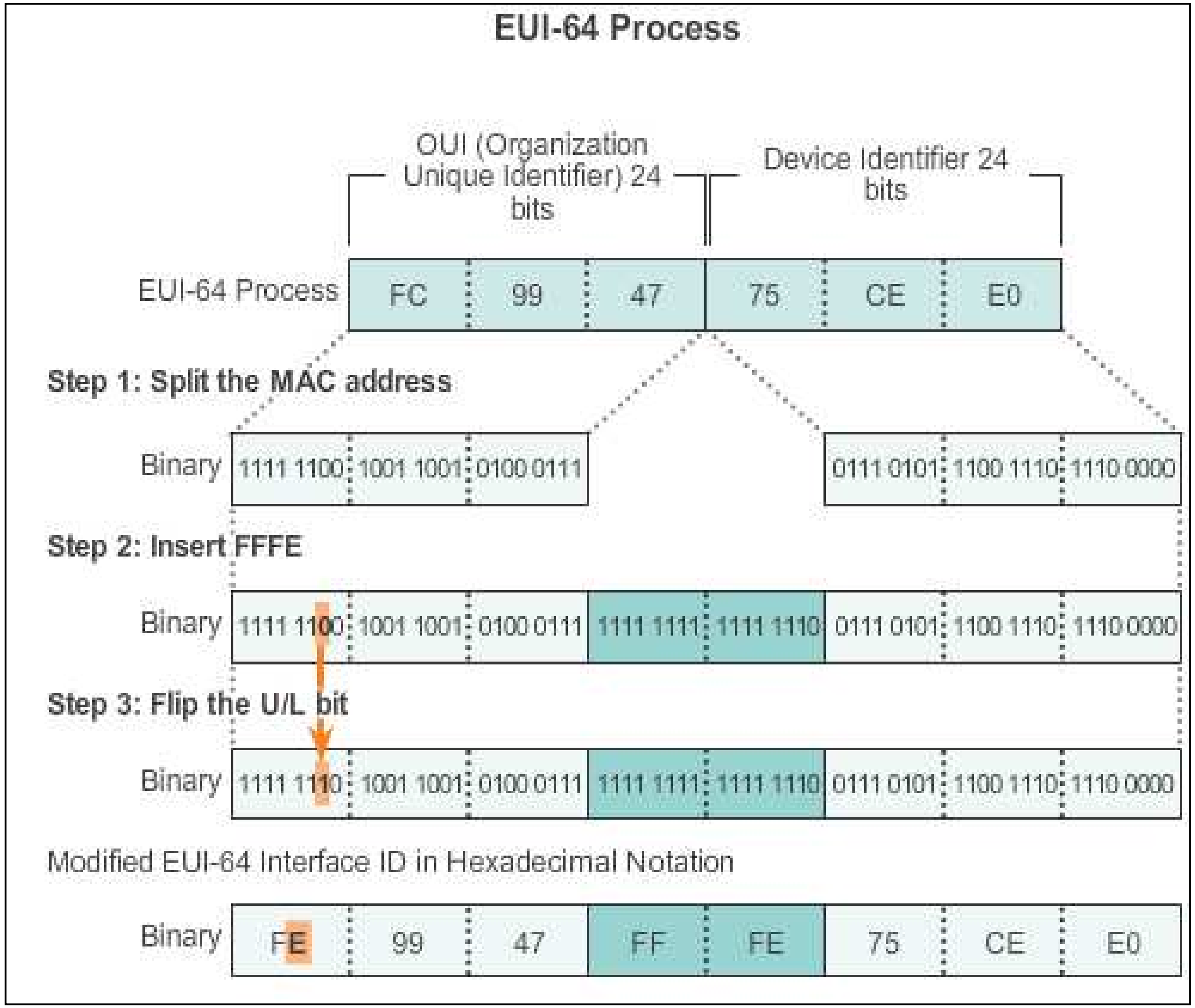
- Uses a client's 48-bit Ethernet MAC address and inserts another 16 bits in the middle of the 46-bit MAC address to create a 64-bit Interface ID.
- Advantage is that the Ethernet MAC address can be used to determine the interface; is easily tracked.

EUI-64 Interface ID is represented in binary and comprises three parts:

- 24-bit OUI from the client MAC address, but the 7^{th} bit (the Universally/Locally bit) is reversed (0 becomes a 1).
- Inserted as a 16-bit value FFFE.
- 24-bit device identifier from the client MAC address.

IPv6 Unicast Addresses

EUI-64 Process or Randomly Generated (cont.)



EUI-64 Process or Randomly Generated (cont.)

```
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

EUI-64 Process or Randomly Generated (cont.)

Randomly Generated Interface IDs

- Depending upon the operating system, a device can use a randomly generated Interface ID instead of using the MAC address and the EUI-64 process.
- 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.

IPv6 Unicast Addresses

Dynamic Link-local Addresses

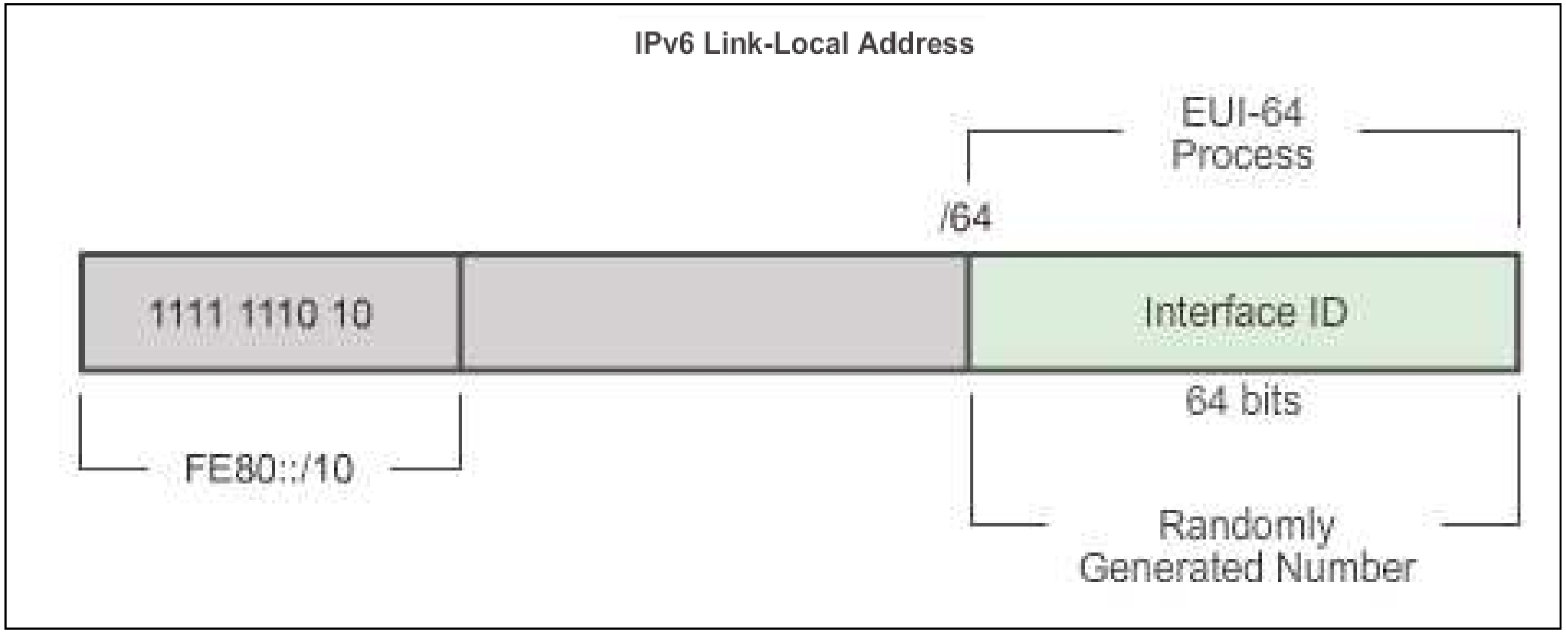
Link-Local Address

- After a global unicast address is assigned to an interface, an IPv6-enabled device automatically generates its link-local address.
- Must have a link-local address that enables a device to communicate with other IPv6-enabled devices on the same subnet.
- 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.

Dynamic Link-local Addresses (cont.)

Dynamically Assigned

The link-local address is dynamically created using the FE80::/10 prefix and the Interface ID.



Static Link-local Addresses

Configuring 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 (cont.)

Configuring Link-local

```
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#
```

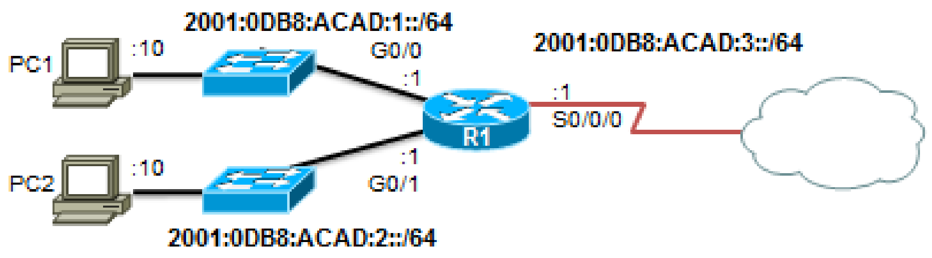
Statically configured link-local addresses

IPv6 Global Unicast Addresses

Verifying IPv6 Address Configuration

Each interface has two IPv6 addresses -

1. global unicast address that was configured
2. one that begins with FE80 is automatically added as a link-local unicast address




```
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 (cont.)

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

<output omitted>

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

Assigned IPv6 Multicast Addresses

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

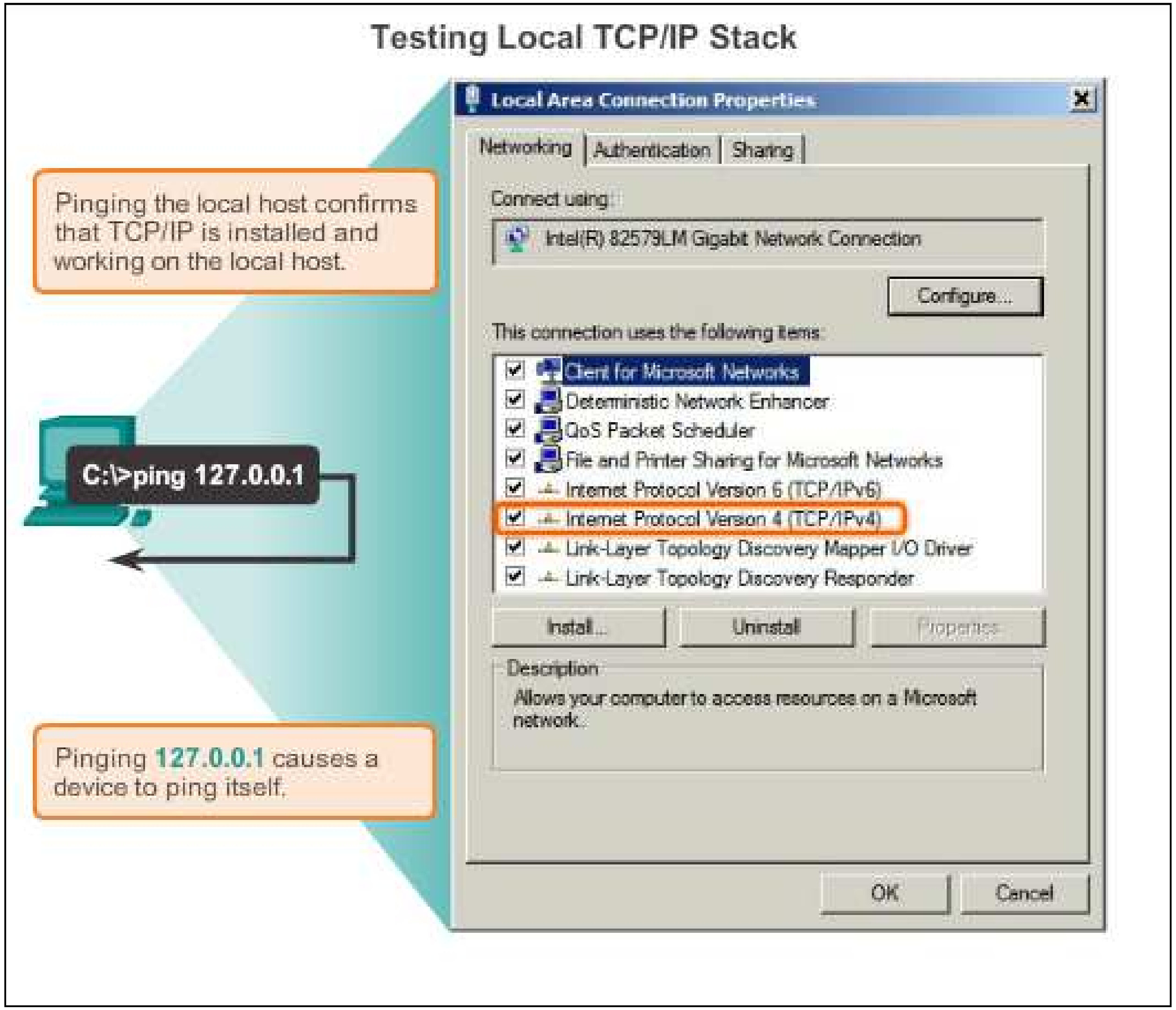
Assigned IPv6 Multicast Addresses (cont.)

Two common IPv6 assigned multicast groups include:

- **FF02::1 All-nodes multicast group** –
  - All IPv6-enabled devices join
  - Same effect as an IPv4 broadcast address
- **FF02::2 All-routers multicast group**
  - All IPv6 routers join
  - A router becomes a member of this group when it is enabled as an IPv6 router with the **`ipv6 unicast-routing`** global configuration mode command.
  - A packet sent to this group is received and processed by all IPv6 routers on the link or network.

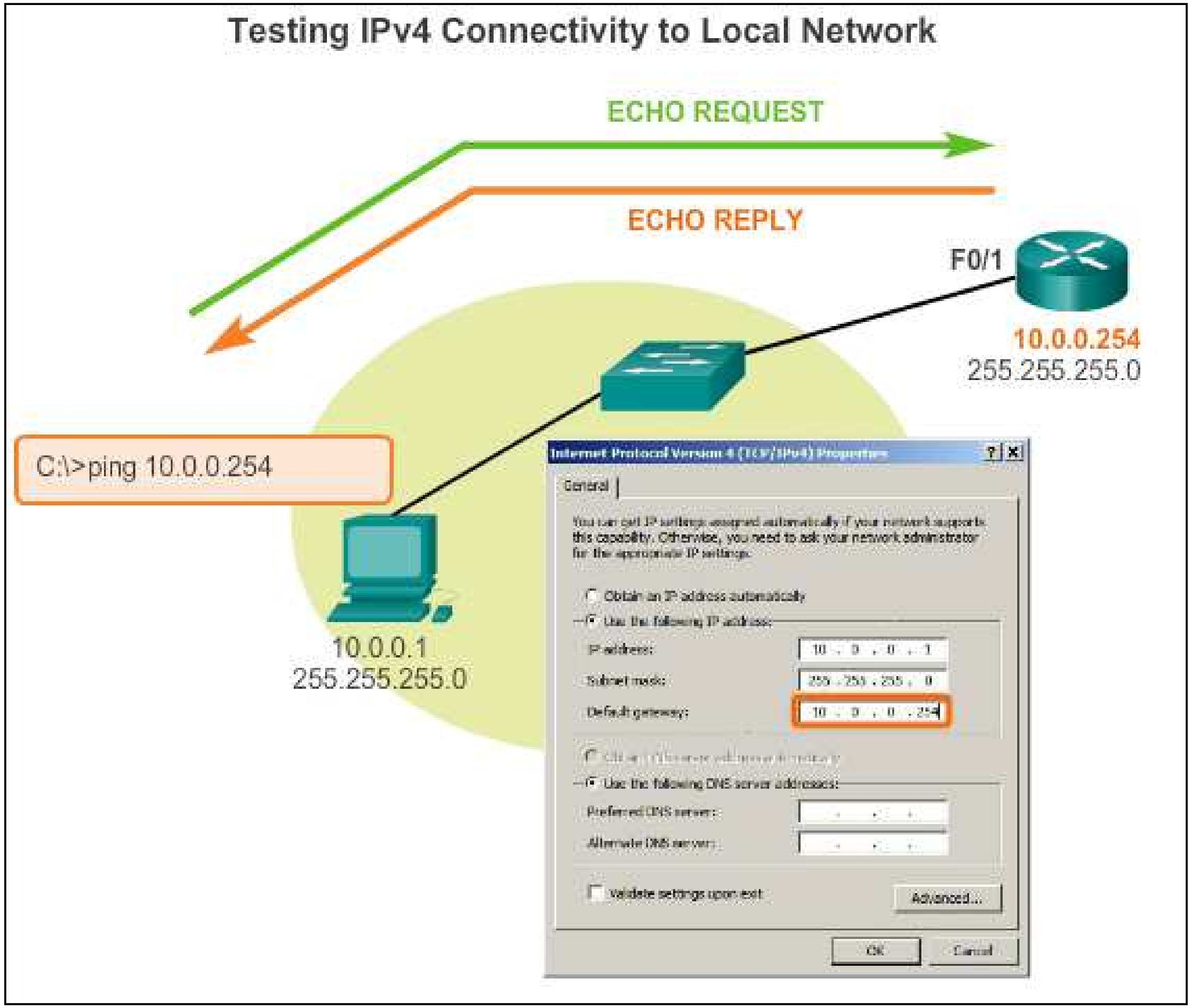
Connectivity Verification

Ping – Testing the Local Stack

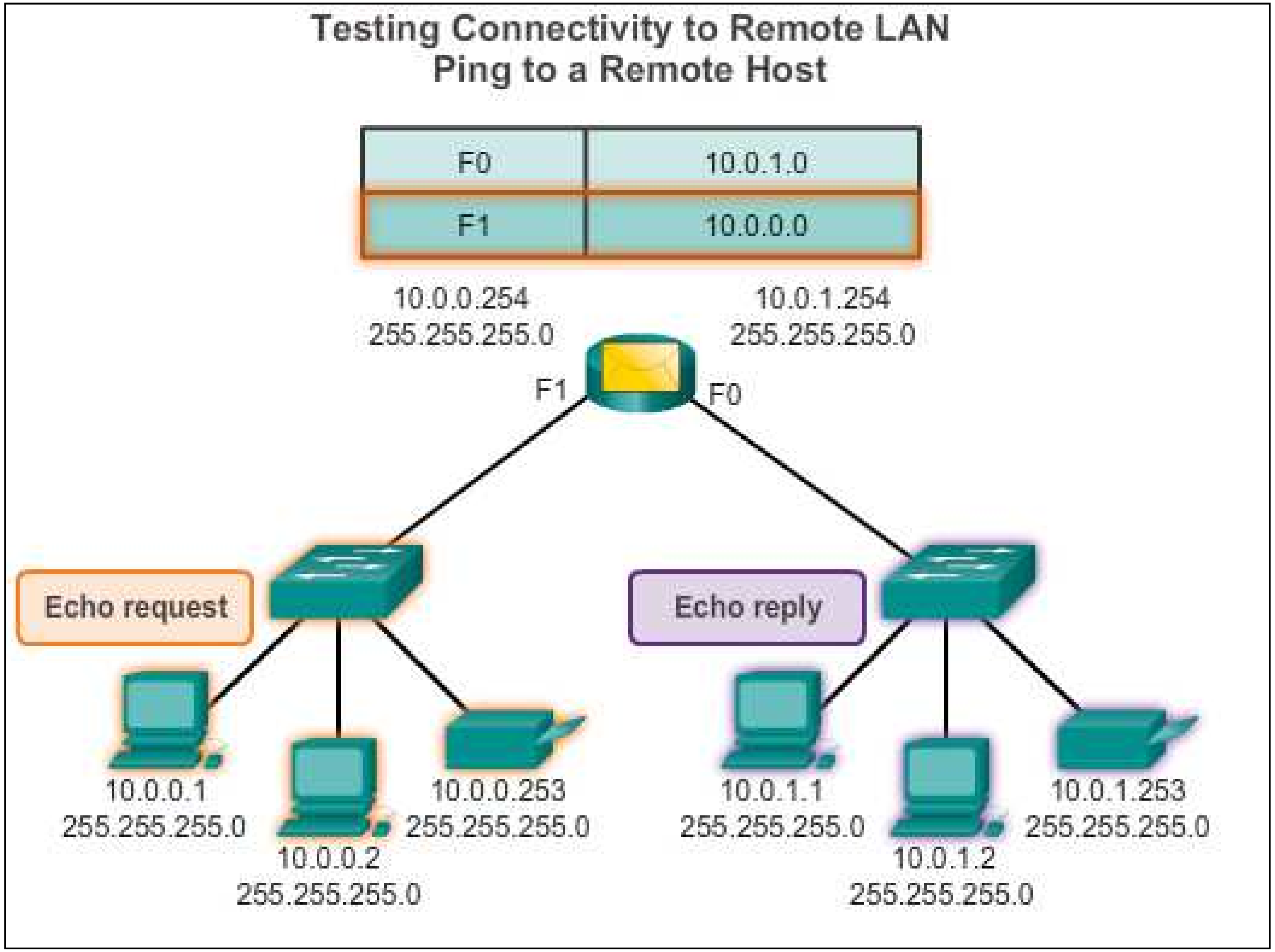


Testing and Verification

Ping – Testing Connectivity to the Local LAN



Ping – Testing Connectivity to Remote



Traceroute – Testing the Path

Traceroute

- Generates a list of hops that were successfully reached along the path.
- Provides important verification and troubleshooting information.
- If the data reaches the destination, then the trace lists the interface of every router in the path between the hosts.
- If the data fails at some hop along the way, the address of the last router that responded to the trace can provide an indication of where the problem or security restrictions are found.
- Provides round-trip time for each hop along the path and indicates if a hop fails to respond.

Summary

Summary

In this lecture, you learned that:

- 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.
- The subnet mask or prefix is used to determine the network portion of an IP address. Once implemented, an IP network needs to be tested to verify its connectivity and operational performance.
- DHCP enables the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information.

Summary (cont.)

- IPv4 hosts can communicate one of three different ways: unicast, broadcast, and multicast.
- The private IPv4 address blocks are: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.
- The depletion of IPv4 address space is the motivating factor for moving to IPv6.
- Each IPv6 address has 128 bits verses the 32 bits in an IPv4 address.
- The prefix length is used to indicate the network portion of an IPv6 address using the following format: IPv6 address/prefix length.

Summary (cont.)

- There are three types of IPv6 addresses: unicast, multicast, and anycast.
- 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.
- IPv6 link-local addresses are in the FE80::/10 range.
- ICMP is available for both IPv4 and IPv6.