Chapter 8: IP Addressing

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

8.1 IPv4 Network Addresses

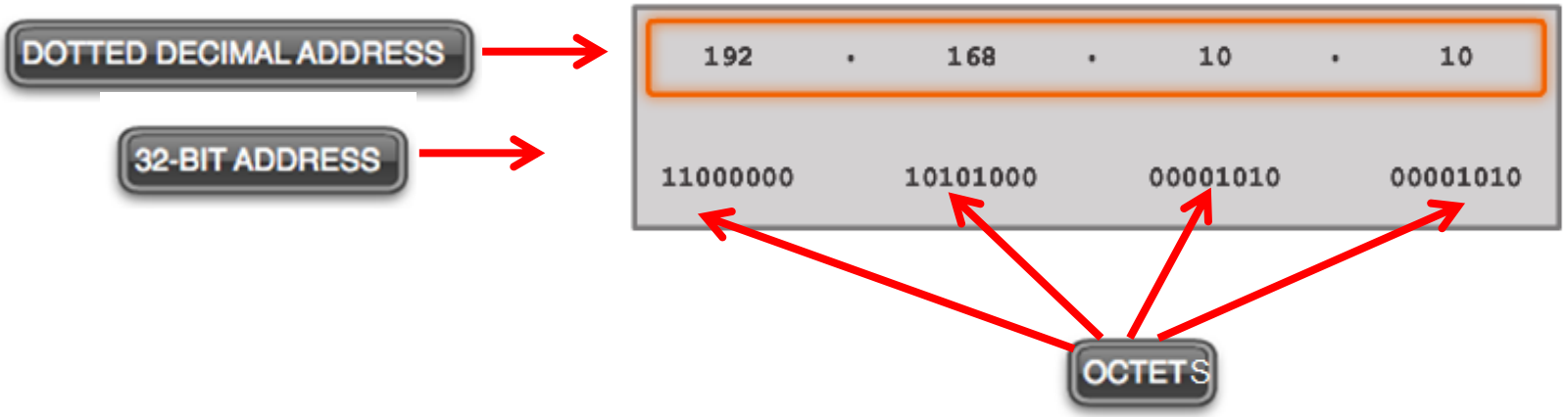
Cisco | Networking Academy®
Mind Wide Open™

IP Address and Address Space

- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- The IP address is the address of the connection, not the host or the router because if the device is moved to another network, the IP address may be changed.
- Address Space: An address space is the total number of addresses used by the protocol.
- If a protocol uses *b* bits to define an address, the address space is 2^b because each bit can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than four billion)

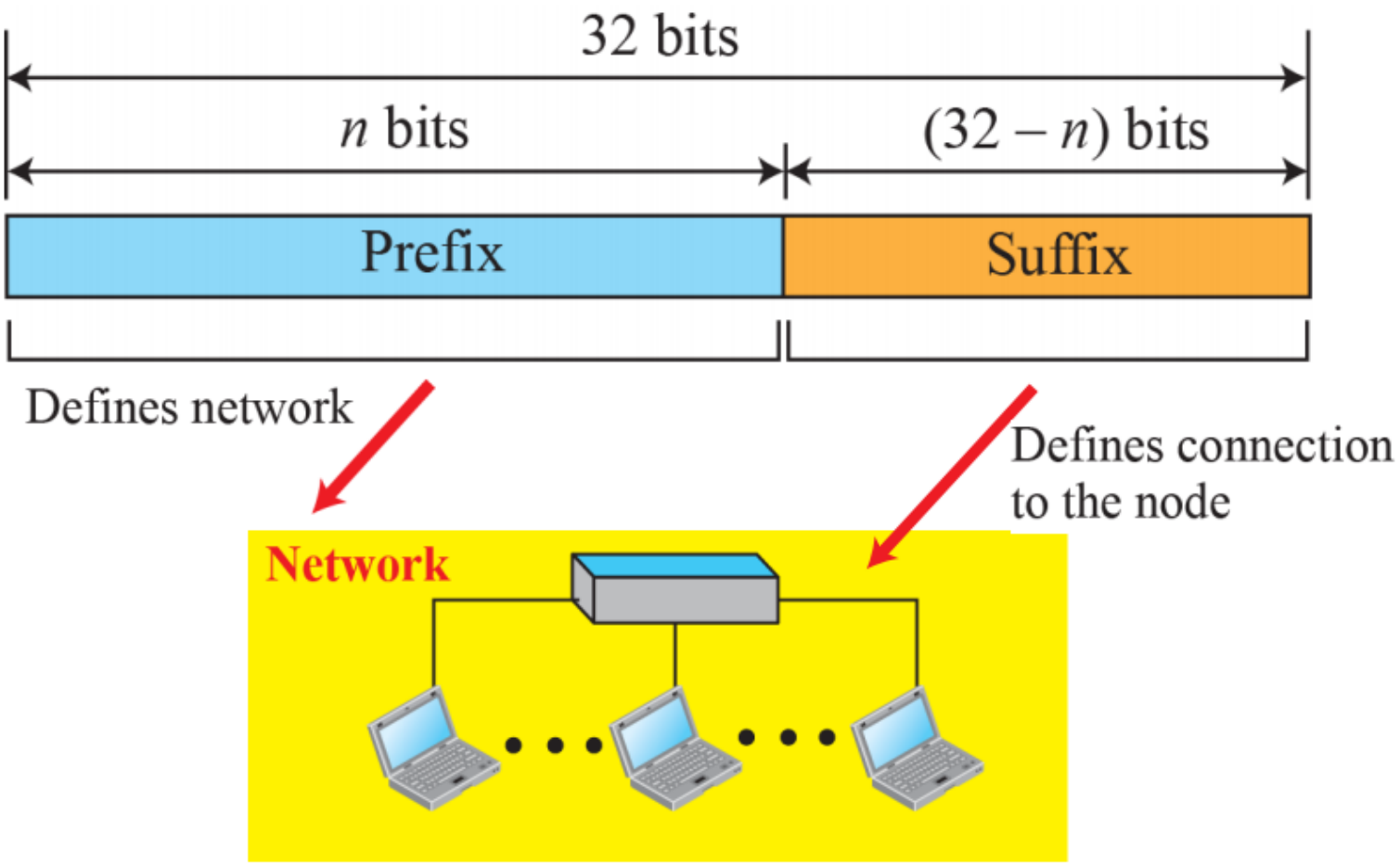
Binary Notation

- Binary notation refers to the fact that computers communicate in 1s and 0s
- For ease of use by people, binary patterns representing IPv4 addresses are expressed as dotted decimals.
- This is first accomplished by separating each byte (8 bits) of the 32-bit binary pattern, called an octet, with a dot.



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

IPv4 Subnet Mask
Hierarchy in Addressing

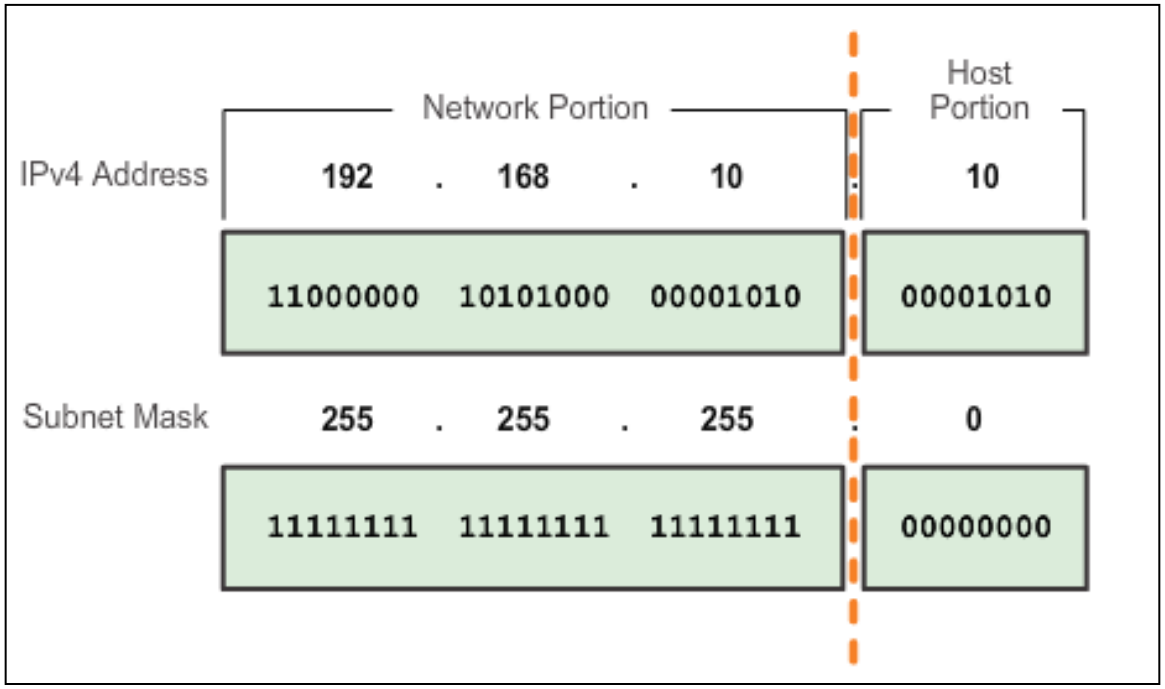


IPv4 Subnet Mask

Network Portion and Host Portion of an IPv4 Address

- To define the network and host portions of an address, a device uses 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

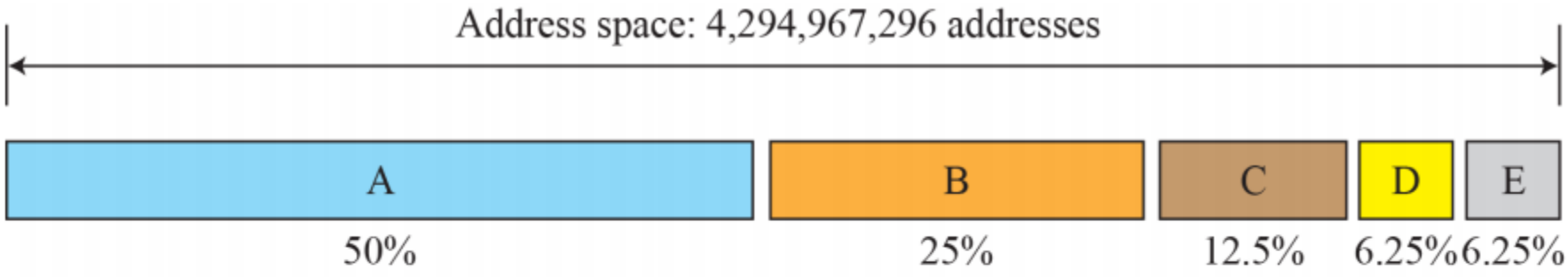


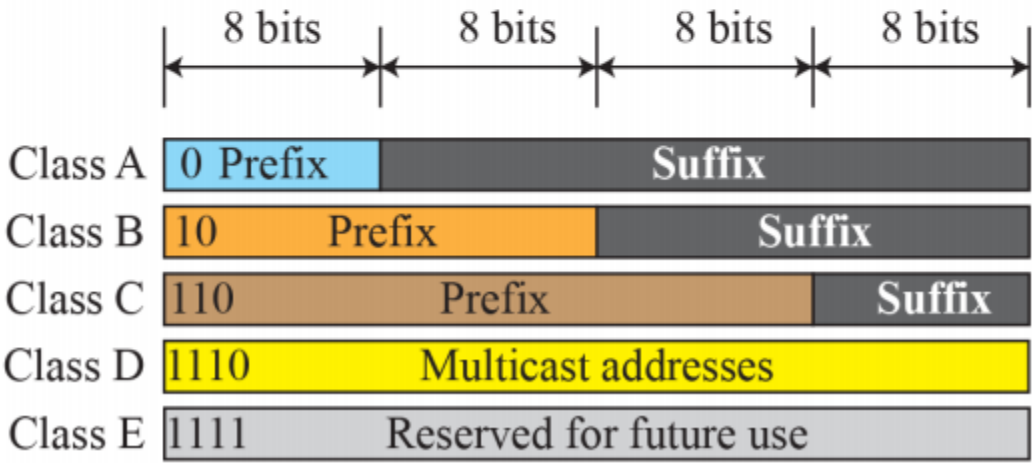
Classful Addressing

- The whole Address space was divided into five classes (Class A, B, C, D and E)
- The unicast address classes A, B, and C defined specifically-sized networks and specific address blocks for these networks.
- A company or organization was assigned an entire network from class A, class B, or class C address block.
- This use of address space is referred to as classful addressing.
- It also defined class D (multicast) and class E (experimental) addresses, as previously presented.

Types of IPv4 Address

occupation of the address space in Classful Addressing





Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

From Forouzan's book

Types of IPv4 Address

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)		

Classless Addressing

Limits to the Class-based System

- Not all organizations' requirements fit well into one of these three classes.
- Classful allocation of address space often wasted many addresses, which exhausted the availability of IPv4 addresses.
- For example, a company that had a network with 260 hosts would need to be given a class B address with more than 65,000 addresses.

Classless Addressing/Prefix length

- 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

Prefix Length

- The prefix length is another way of expressing the subnet mask.
- The prefix length is the number of bits set to 1 in the subnet mask.
- It is written in “slash notation”, a “/” followed by the number of bits set to1.
- For example, if the subnet mask is 255.255.255.0, there are 24 bits set to 1 in the binary version of the subnet mask, so the prefix length is 24 bits or /24.
- The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

Examining the Prefix Length

- Let's examine an example in Section 8.1.2.3.

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		

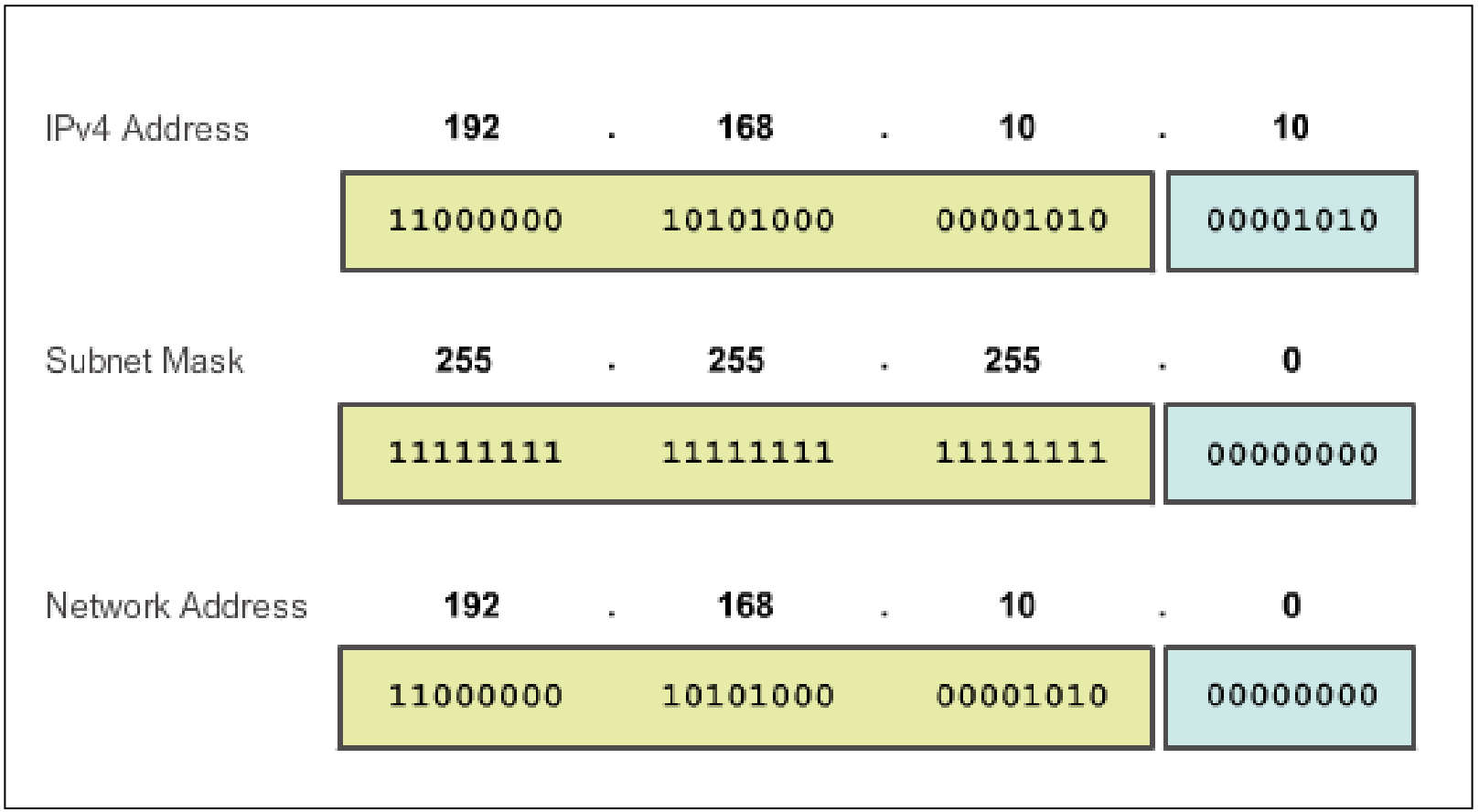
Examining the Prefix Length (cont.)

	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		

Bitwise AND Operation

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

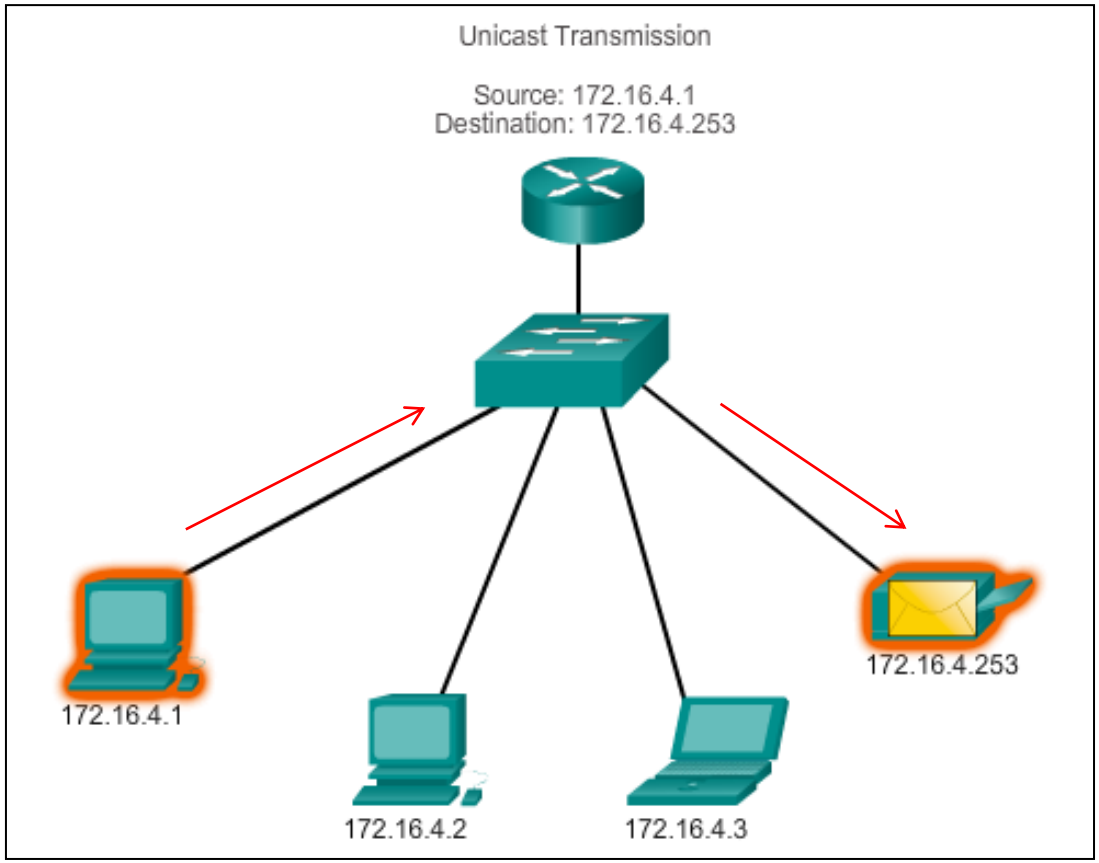


Unicast Transmission

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.

Let's see the animation (Section 8.1.3.3).



Broadcast Transmission

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

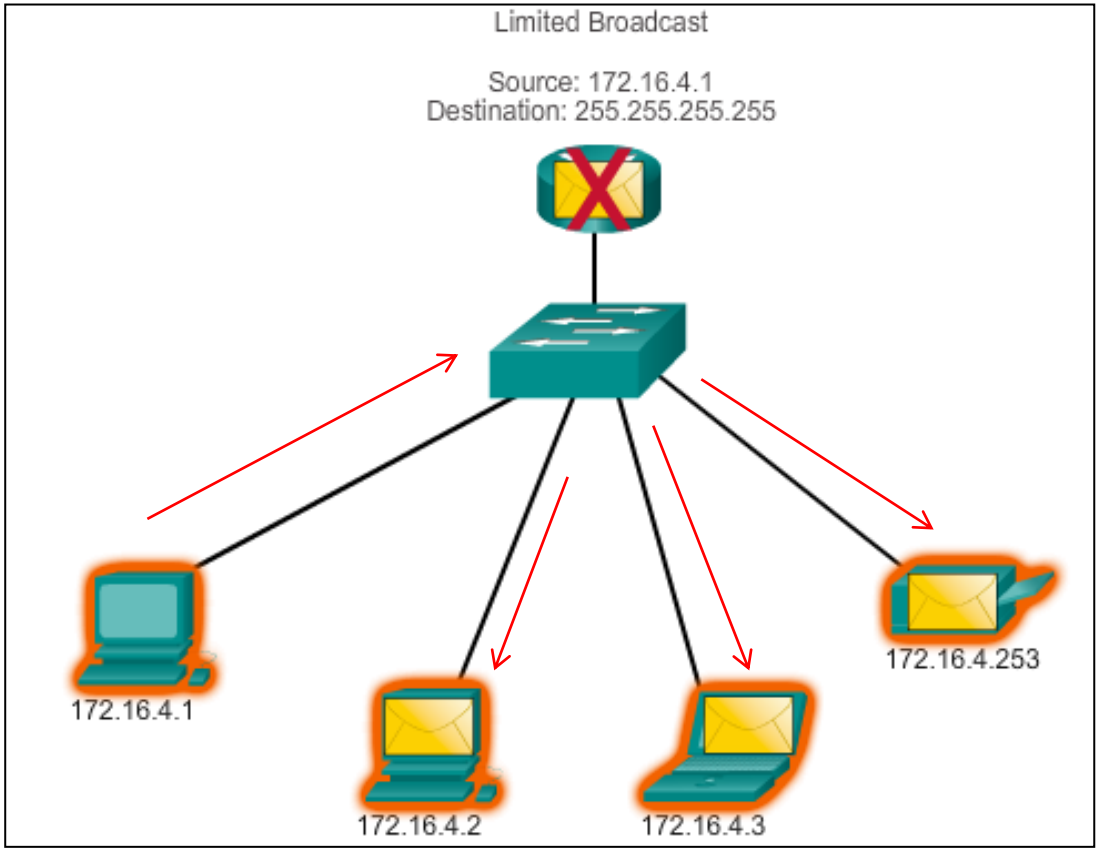
#2 Broadcast – the process of sending a packet from one host to all hosts in the network.

Directed broadcast

- Destination 172.16.4.255
- Hosts within the 172.16.4.0/24 network

Limited broadcast

- Destination 255.255.255.255
- **NOTE**: Routers do not forward a limited broadcast!



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
- Some examples: Video and audio broadcasts, Routing information exchange, Distribution of software, Remote gaming
- 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

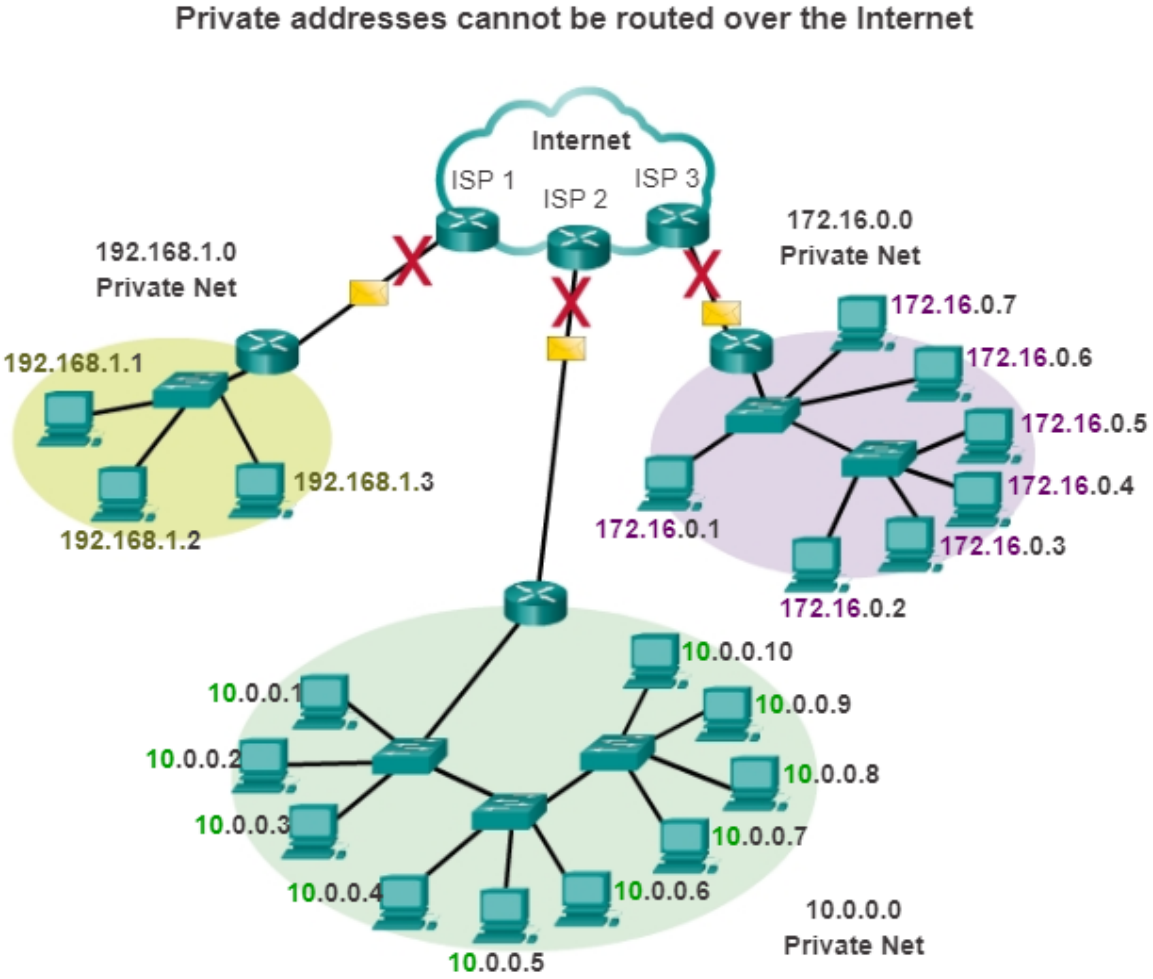
Private address blocks are:

- 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

Public and Private IPv4 Addresses



Public and Private IPv4 Addresses

Public address:

- **Public IP address** of a system is the IP address which is used to communicate outside the network.
- Public IP address is basically assigned by the ISP (Internet Service Provider).
- Besides private IP addresses, rest are public.

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 for future use. Currently using for research and experimental use.

8.2 IPv6 Network Addresses

Cisco | Networking Academy®
Mind Wide Open™

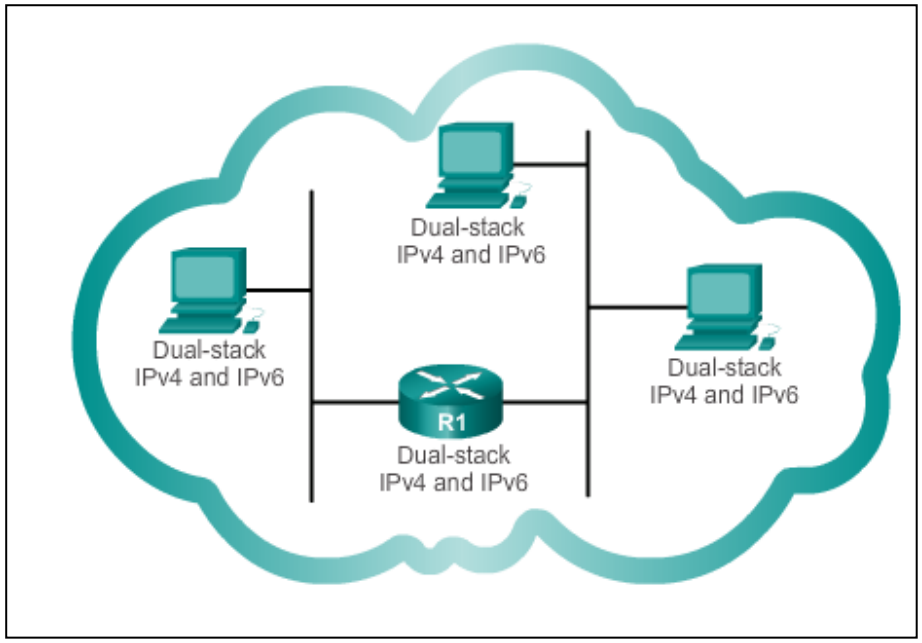
The Need for IPv6

- 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 IPv4 addresses will run out 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 (36 zeros) 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.

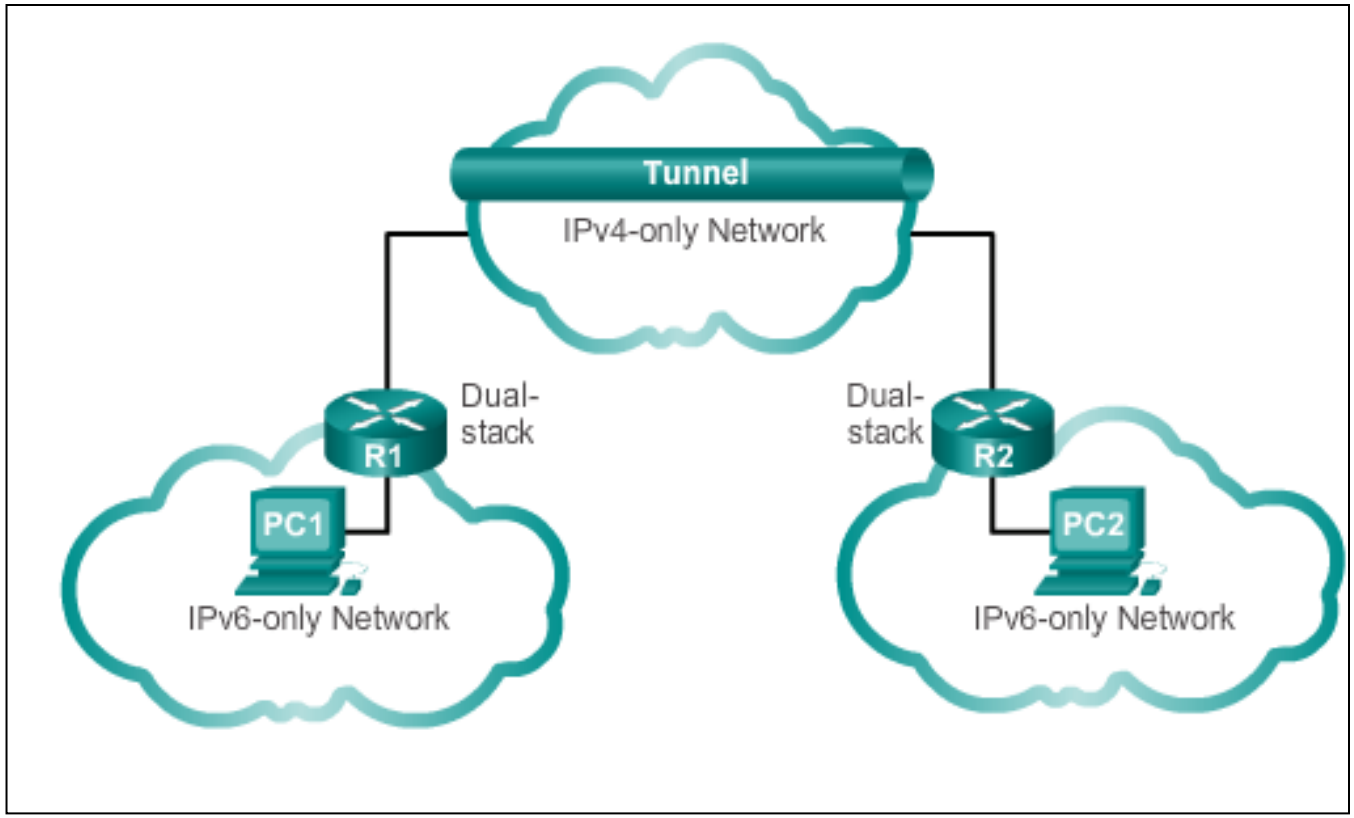
Dual-stack



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.)

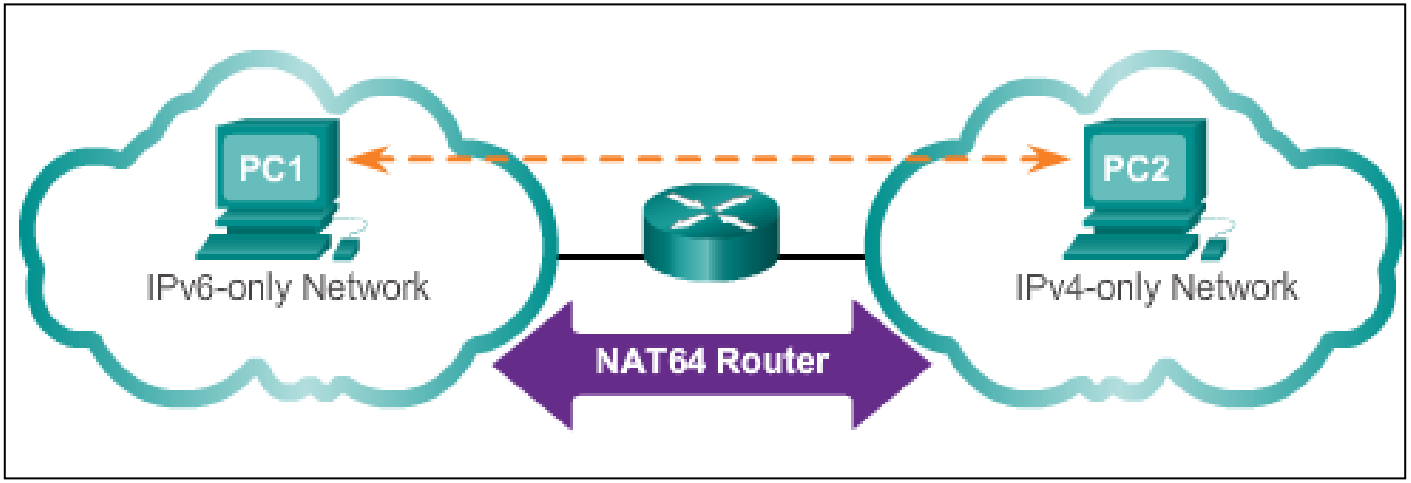
Tunnelling



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

IPv4 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

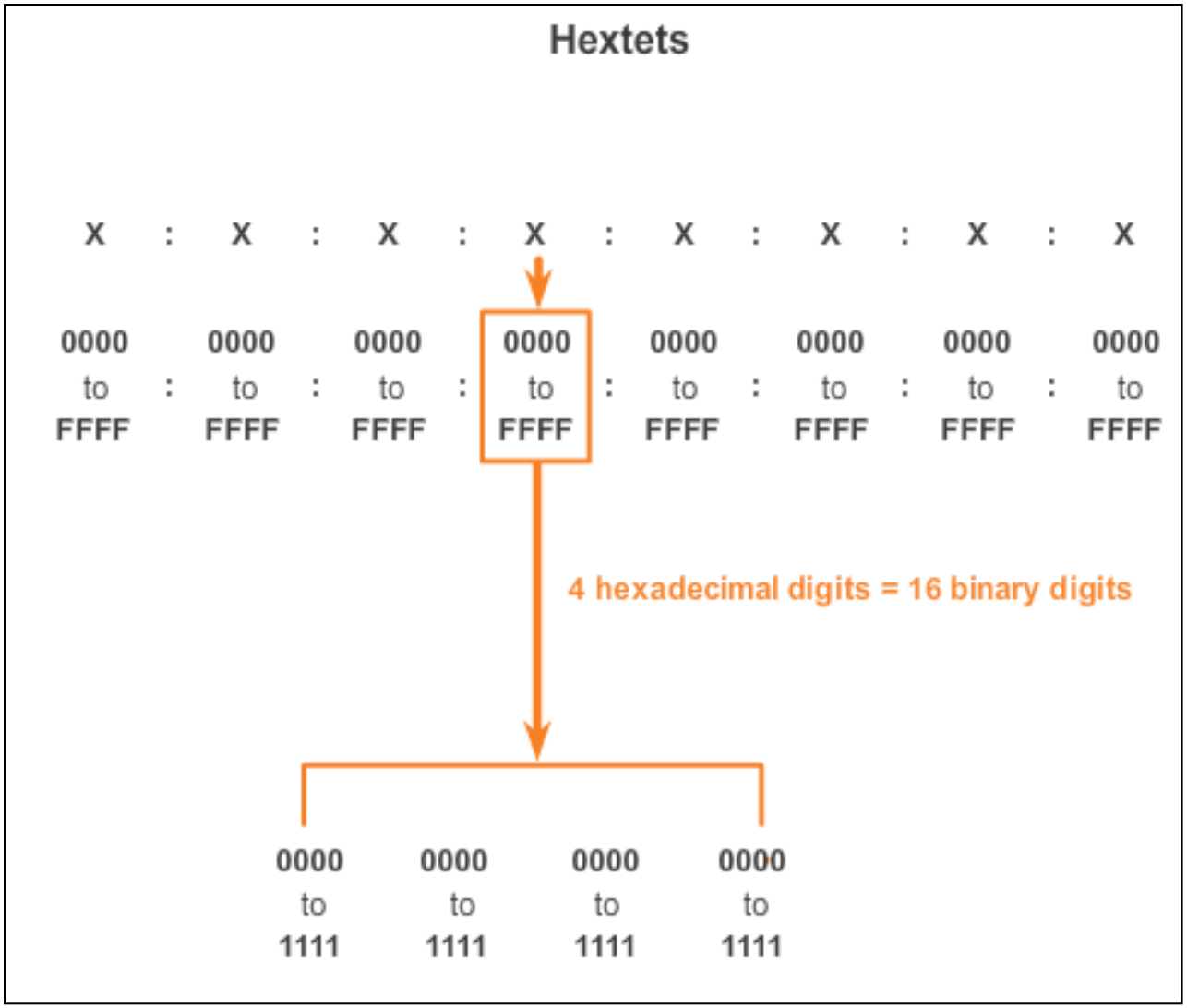
IPv6 Address Representation

- 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

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

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

Rule 2 - Omitting All 0 Segments (cont.)

Example #1

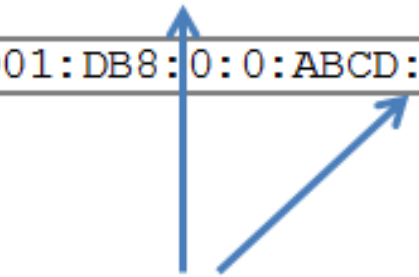
Preferred	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Omit leading 0s	2001: DB8: 0: 0:ABCD: 0: 0: 100
Compressed	2001:DB8::ABCD:0:0:100
OR	
Compressed	2001:DB8:0:0:ABCD::100

Only one **::** may be used.

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



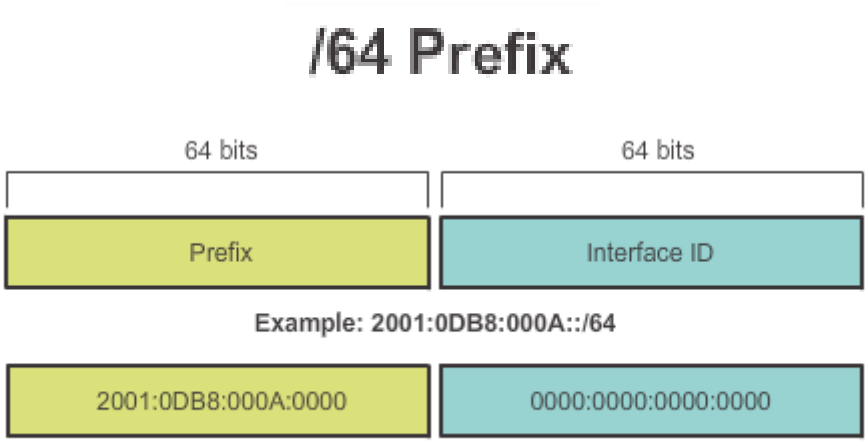
Only one **::** may be used.

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:

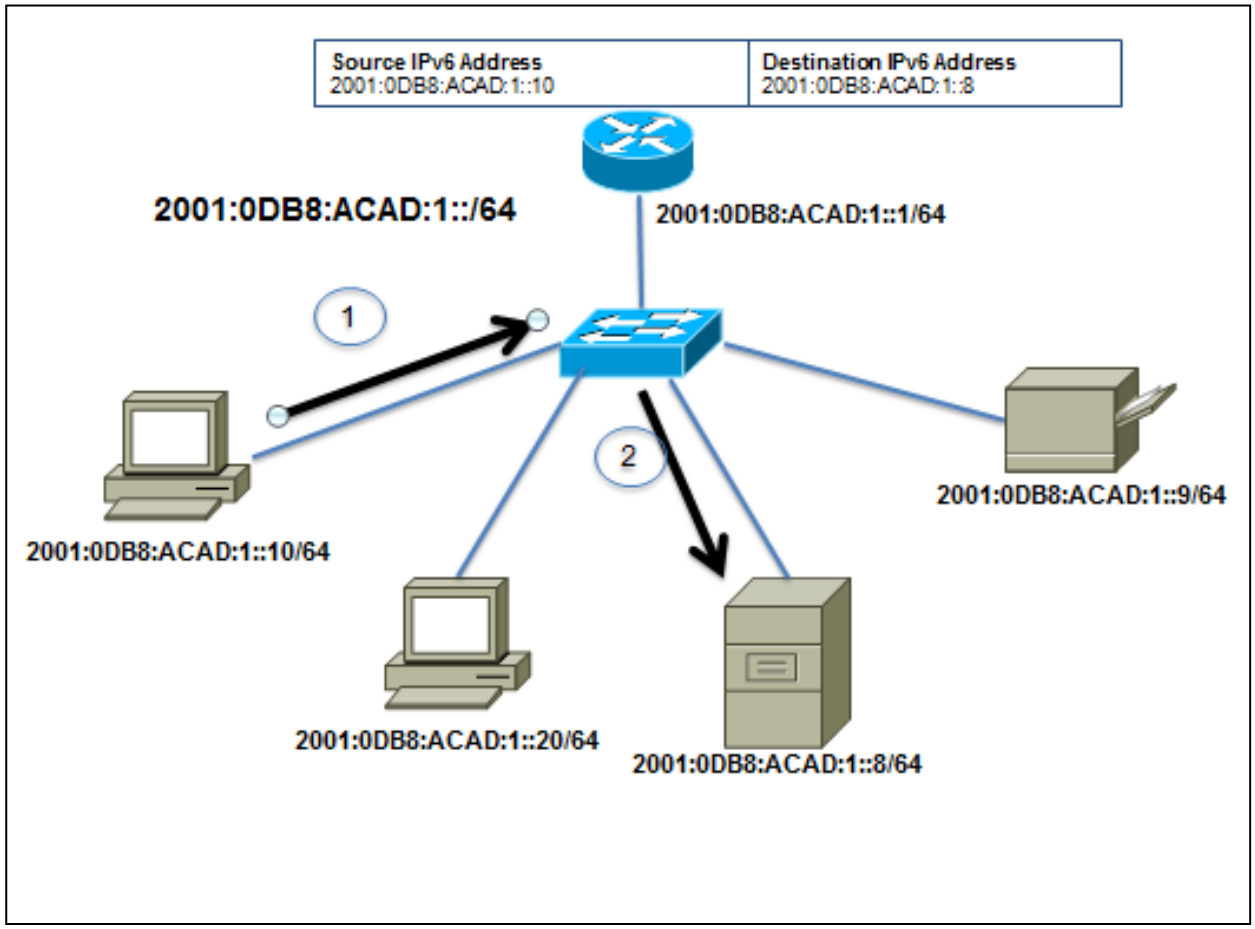
- Unicast
- Multicast
- Anycast (beyond the scope of the syllabus).

Note: IPv6 does not have broadcast addresses.

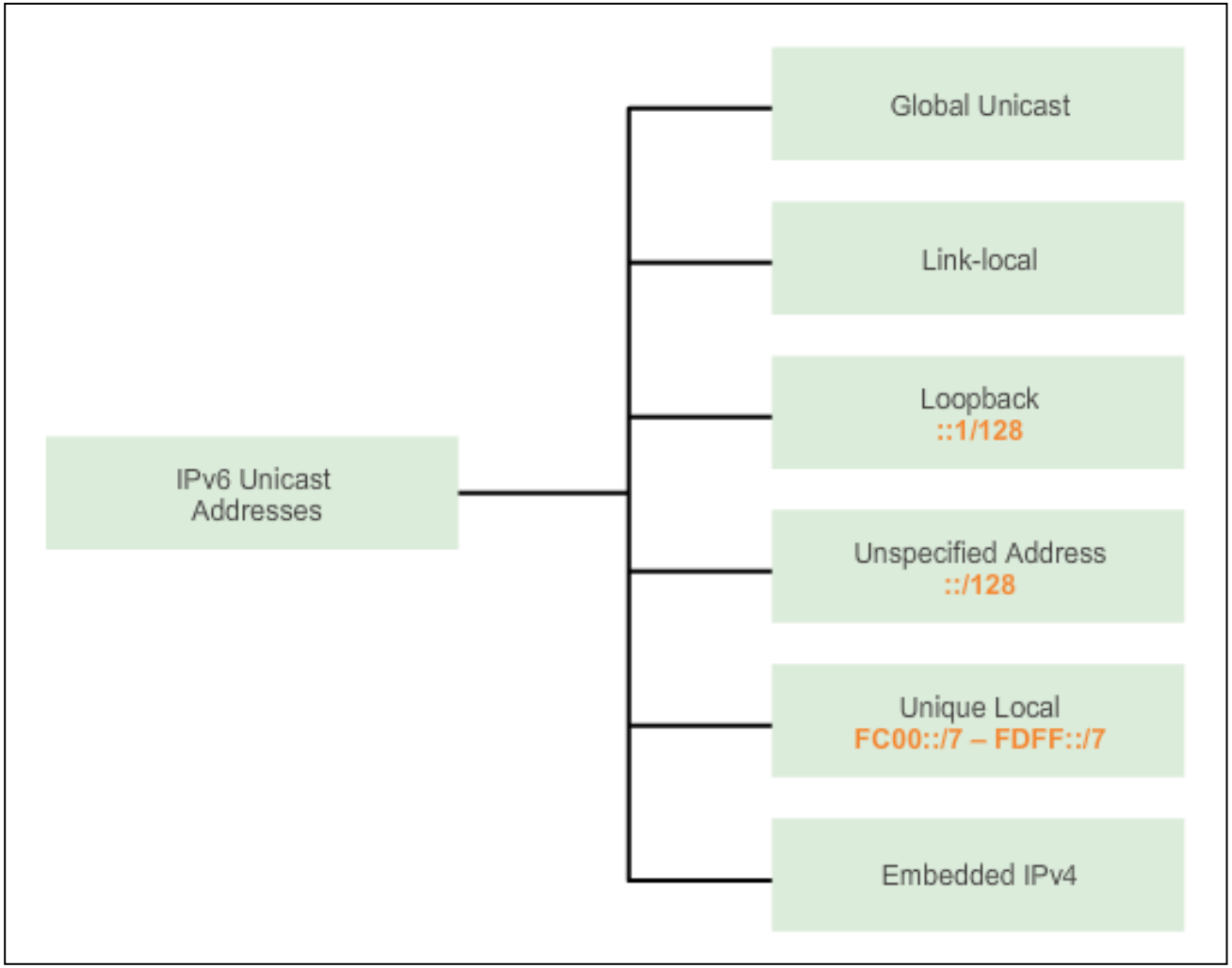
IPv6 Unicast Addresses

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.



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.)

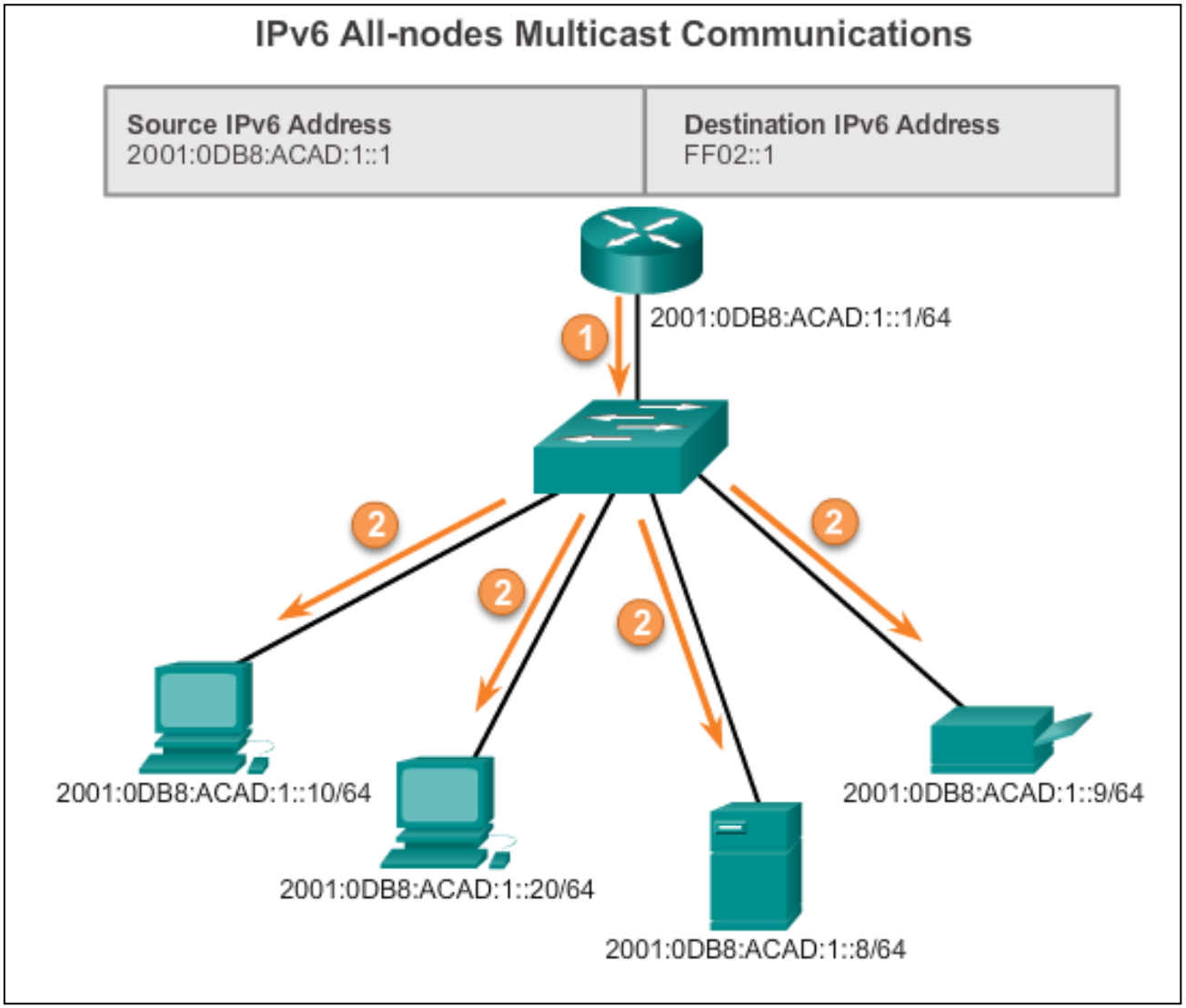
Unique Local

- 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.

Assigned IPv6 Multicast Addresses



ICMPv4 and ICMPv6 Messages

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

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
- **Router Solicitation and Router Advertisement Message** – Sent between hosts and routers.
- **Router Solicitation (RS) message** – RS messages are sent as an IPv6 all-routers multicast message.
- **Router Advertisement (RA) message** – RA messages are sent by routers to provide addressing information.