



# Ch 7: IP Addressing



*Computer Networks Course*

*BY*

*Dr. Essam Halim Houssein*

Cisco | Networking Academy®  
Mind Wide Open™

A large, dark blue arrow pointing to the right, which serves as a background for the chapter title. To the left of the arrow's tail are two vertical blue bars of different heights.

# Chapter 7: IP Addressing

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

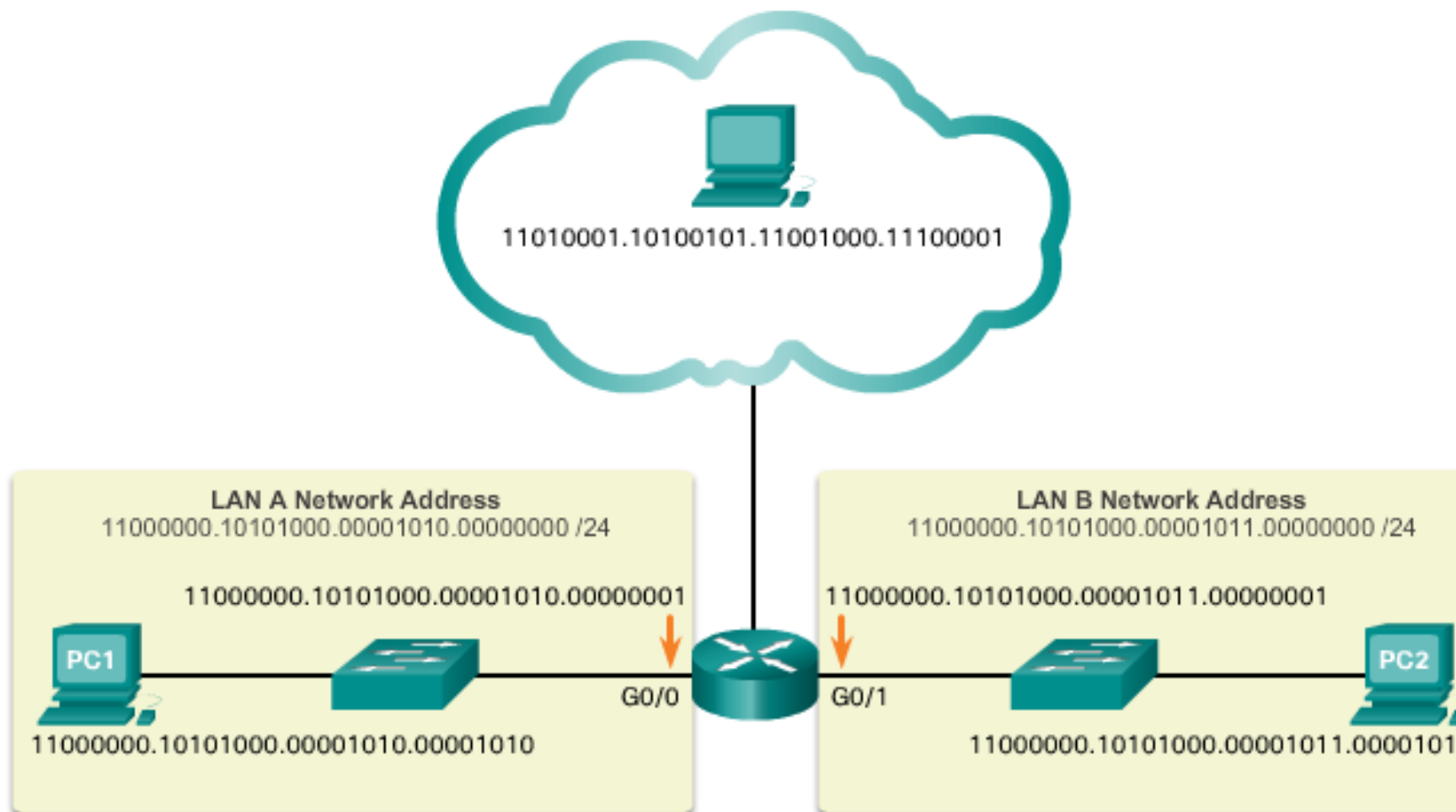
Designing, implementing and managing an effective IP addressing plan ensures that networks can operate effectively and efficiently.

## IPv4 Addresses

**Binary** is important for us to understand because hosts, servers, and network devices use binary addressing. Specifically, they use binary IPv4 addresses, to identify each other.

**Each address consists of a string of 32 bits, divided into four sections called *octets*.** Each octet contains 8 bits (or 1 byte) separated with a dot. For example, PC1 is assigned IPv4 address 11000000.10101000.00001010.00001010. Its default gateway address would be that of R1 Gigabit Ethernet interface 11000000.10101000.00001010.00000001.

## IPv4 Addresses Expressed in Binary



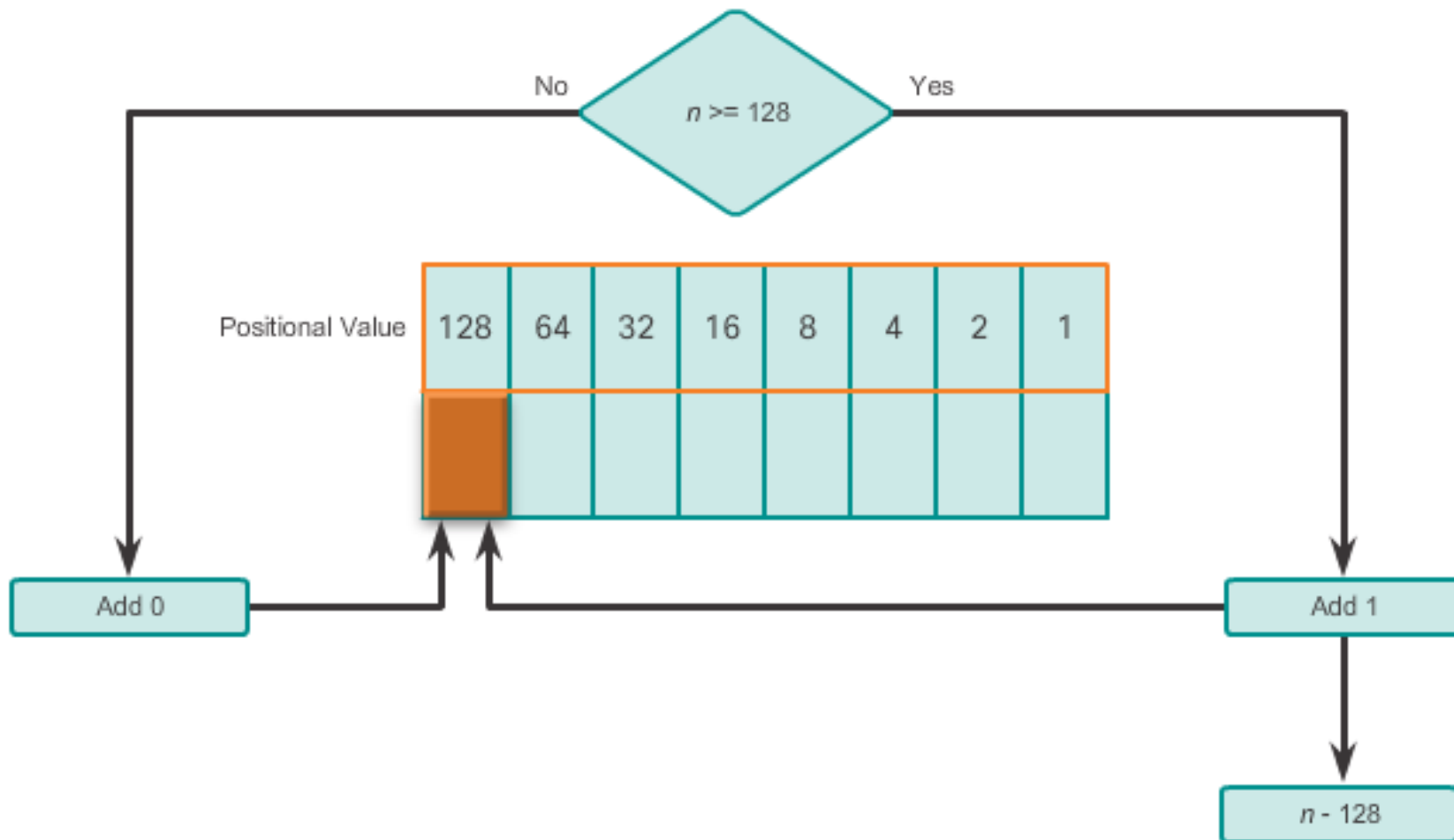
## Converting the First Octet to Decimal

11000000.10101000.00001011.00001010

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

192.\_\_\_\_.\_\_\_\_.\_\_\_\_  
Dotted Decimal Notation

Is the Decimal  $n$  Greater Than or Equal To 128?



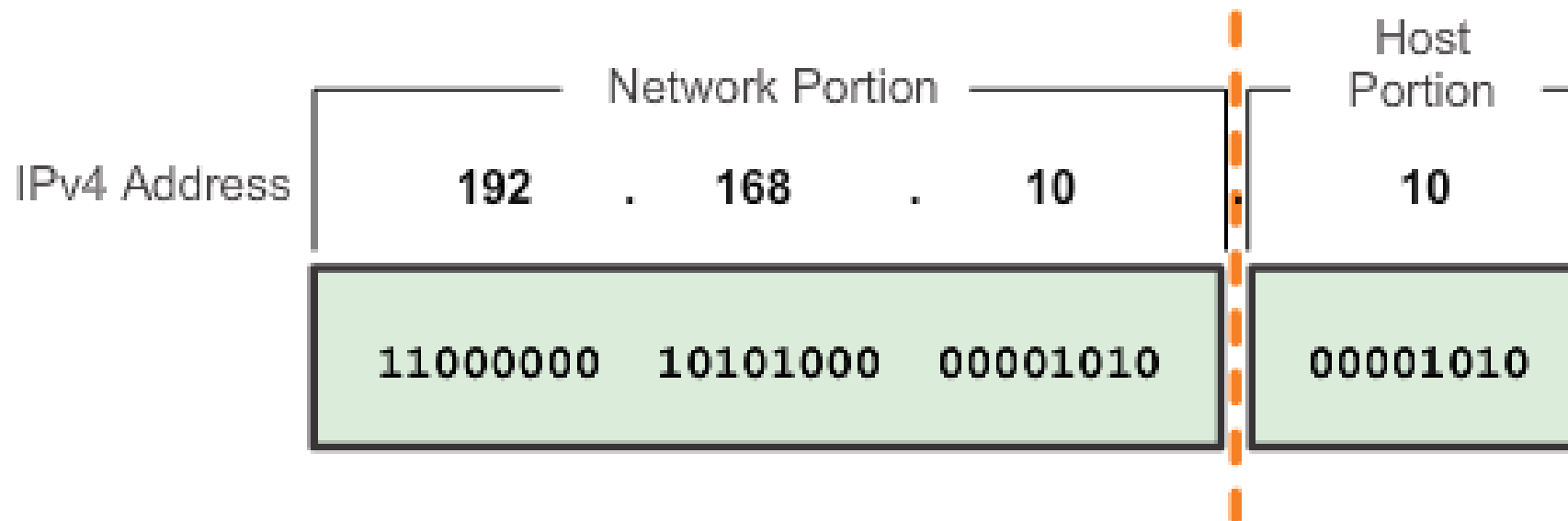
## Network and Host Portions

An IPv4 address is a hierarchical address that is made up of a network portion and a host portion. When determining the network portion versus the host portion, it is necessary to look at the 32-bit stream. Within the 32-bit stream, a portion of the bits identify the network, and a portion of the bits identify the host.

The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network.

But how do hosts know which portion of the 32-bits identifies the network and which identifies the host? That is the job of the **subnet mask**.





## The Subnet Mask

**Three dotted decimal IPv4 addresses** must be configured when assigning an IPv4 configuration to host:

**IPv4 address** – Unique IPv4 address of the host

**Subnet mask**- Used to identify the network/host portion of the IPv4 address

**Default gateway** – Identifies the local gateway (i.e. local router interface IPv4 address) to reach remote networks

When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address where the device belongs.

The dotted decimal address and the 32-bit subnet mask. **Notice how the subnet mask is essentially a sequence of 1 bits followed by a sequence of 0 bits.**

To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right. **The 1s in the subnet mask identify the network portion while the 0s identify the host portion.**

The actual process used to identify the network portion and host portion is called **ANDing**.

## Comparing the IP address and Subnet Mask

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

## Resulting Network Address

IP address	192	.	168	.	10	.	10
Binary	11000000 10101000 00001010						00001010
Subnet mask	255	.	255	.	255	.	0
	11111111 11111111 11111111						00000000
AND Results	11000000 10101000 00001010						00000000
Network Address	192	.	168	.	10	.	0

## The Prefix Length

The prefix length is the number of bits set to 1 in the subnet mask. It is written in “slash notation”, which is a “/” followed by the number of bits set to 1.

For example, the first column lists various subnet masks that can be used with a host address. The second column displays the converted 32-bit binary address. The last column displays the resulting prefix length.

## Comparing the Subnet Mask and Prefix Length

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

## Public and Private IPv4 Addresses

Public IPv4 addresses are addresses which are globally routed between ISP (Internet Service Provider) routers. However, not all available IPv4 addresses can be used on the Internet. There are blocks of addresses called *private addresses* that are used by most organizations to assign IPv4 addresses to internal hosts.

Private IPv4 addresses are not unique and can be used by an internal network.

Specifically, the private address blocks are:

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

**172.16.0.0 /12**   or **172.16.0.0**      to **172.31.255.255**

**192.168.0.0 /16** or **192.168.0.0**      to **192.168.255.255**

It is important to know that addresses within these address blocks are not allowed on the Internet and must be filtered (discarded) by Internet routers.



## Special User IPv4 Addresses

There are certain addresses such as the network address and broadcast address that cannot be assigned to hosts. There are also special addresses that can be assigned to hosts, but with restrictions on how those hosts can interact within the network.

**Loopback addresses (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254)** – More commonly identified as only 127.0.0.1, these are special addresses used by a host to direct traffic to itself. For example, it can be used on a host to test if the TCP/IP configuration is operational. Notice how the 127.0.0.1 loopback address replies to the ping command. Also note how any address within this block will loop back to the local host, such as shown with the second ping in the figure.

**Link-Local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254)** – More commonly known as the Automatic Private IP Addressing (APIPA) addresses, they are used by a Windows DHCP client to self-configure in the event that there are no DHCP servers available. Useful in a peer-to-peer connection.

**TEST-NET addresses (192.0.2.0/24 or 192.0.2.0 to 192.0.2.255)** – These addresses are set aside for teaching and learning purposes and can be used in documentation and network examples.

# classful addressing

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

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

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

## Classless Addressing

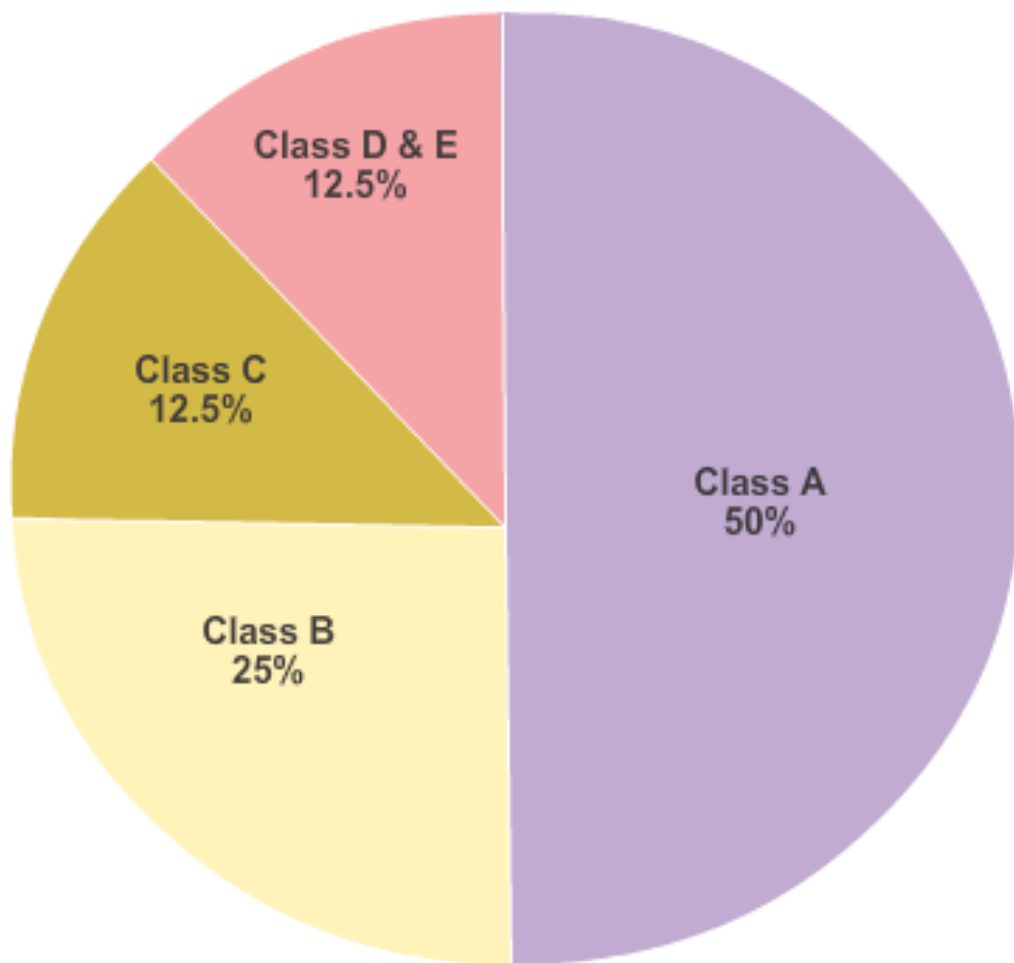
The problem is that this wasted a great deal of addresses and exhausted the availability of IPv4 addresses.

The system in use today is referred to as *classless addressing*. The formal name is Classless Inter-Domain Routing (CIDR, pronounced “cider”).

The IETF knew that CIDR was only a temporary solution and that a new IP protocol would have to be developed to accommodate the rapid growth in the number of Internet users. In 1994, the IETF began its work to find a successor to IPv4, which eventually became IPv6.

**So who manages and assigns these IP addresses?**

## Summary of Classful Addressing



### Class A

Total Networks: 128  
Total Hosts/Net: 16,777,214

### Class B

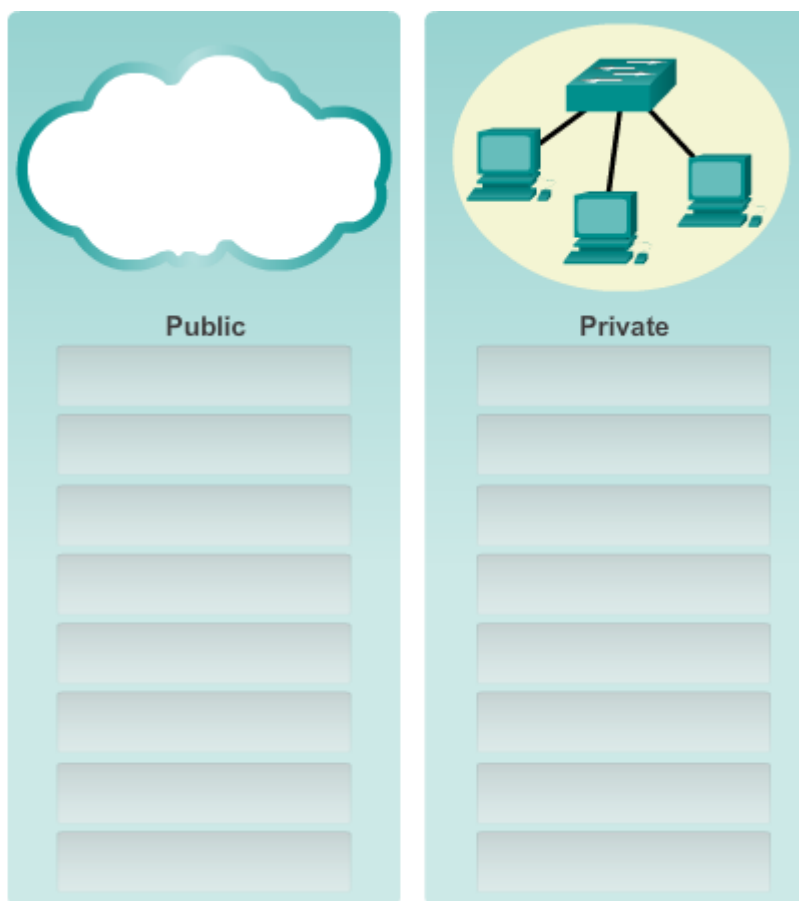
Total Networks: 16,384  
Total Hosts/Net: 65,534


### Class C

Total Networks: 2,097,152  
Total Hosts/Net: 254

# Activity (1)


- 117.22.10.10
- 198.172.17.7
- 200.0.0.1
- 192.255.255.255
- 172.16.255.255
- 127.255.255.255
- 172.16.5.9
- 192.168.33.33





**Public**

- ✓
- ✓
- ✓
- ✓
- ✓
- 
- 
- 



**Private**

- ✓
- ✓
- ✓
- 
- 
- 
-

## The Need for IPv6

IPv6 has a larger 128-bit address space, providing for 340 undecillion addresses. (That is the number 340, followed by 36 zeroes.) However, IPv6 is more than just larger addresses. When the IETF began its development of a successor to IPv4, it used this opportunity to fix the limitations of IPv4 and include additional enhancements.

### Need for IPv6

The depletion of IPv4 address space has been the motivating factor for moving to IPv6. IPv4 has a theoretical maximum of 4.3 billion addresses. Private addresses in combination with Network Address Translation (NAT) have been instrumental in slowing the depletion of IPv4 address space. However, NAT breaks many applications and has limitations that severely impede peer-to-peer communications.

### Internet of Everything

The Internet of today is significantly different than the Internet of past decades. The Internet of today is more than email, web pages, and file transfer between computers. The evolving Internet is becoming an **Internet of things**. No longer will the only devices accessing the Internet be computers, tablets, and smartphones. The sensor-equipped, Internet-ready devices of tomorrow will include everything from automobiles and biomedical devices, to household appliances and natural ecosystems.



## IPv4 and IPv6 Coexistence

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

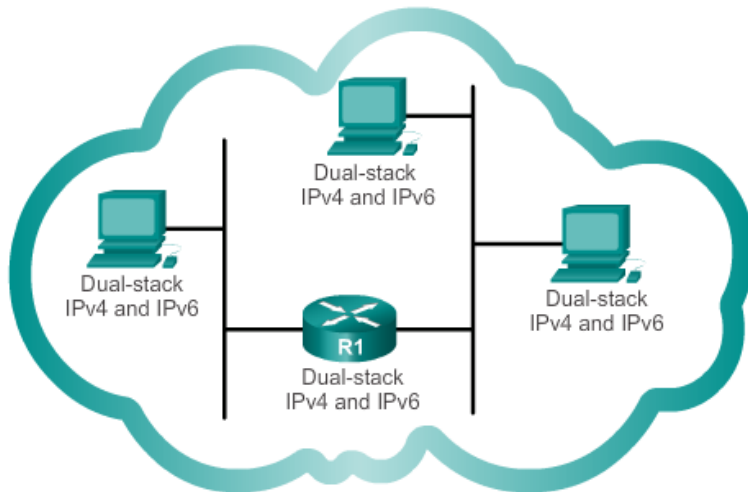
**Dual Stack** – dual stack allows IPv4 and IPv6 to coexist on the same network segment. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously.

**Tunneling** – tunneling 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.

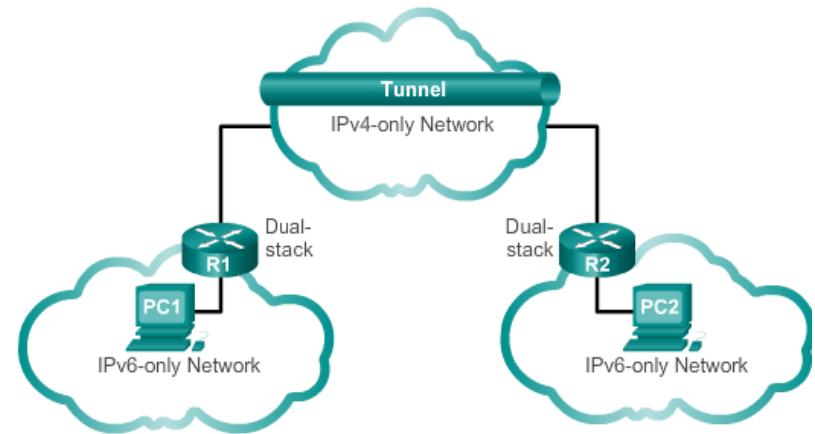
**Translation** – Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet and vice versa.



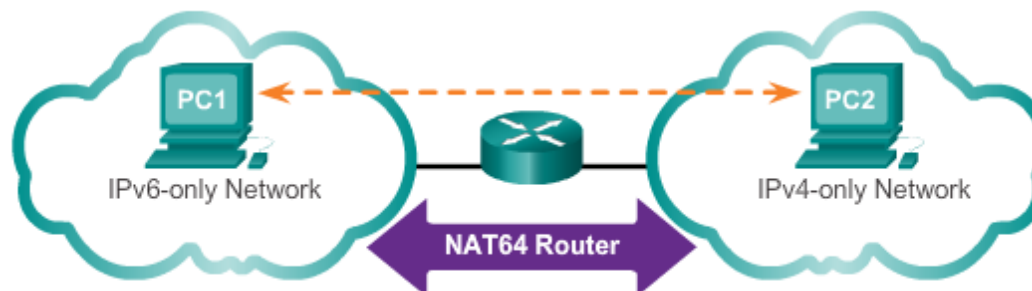
## Dual-Stack



## Tunneling



## Translation



## Pv6 Address Representation

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

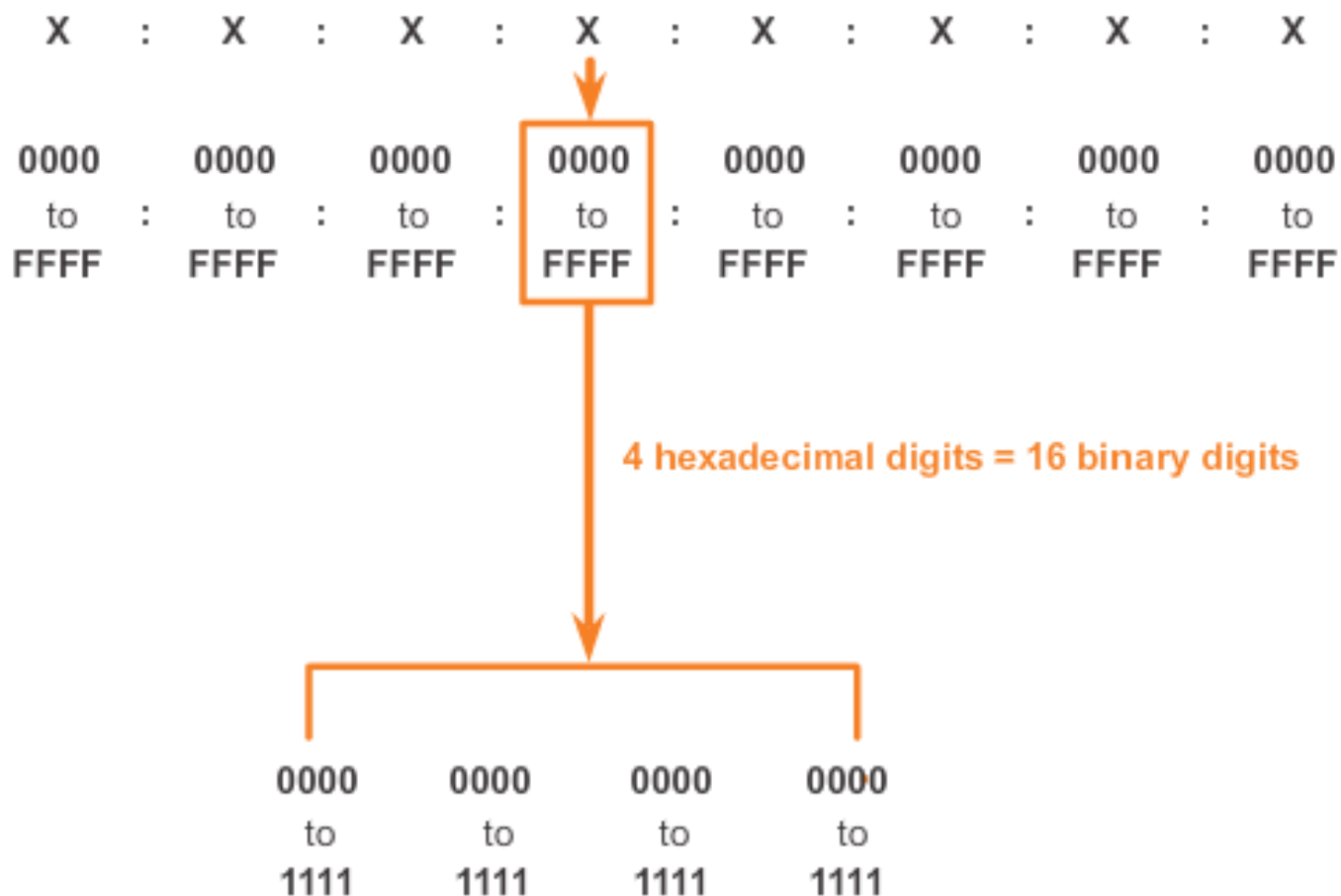
### Preferred Format

As shown in Figure 1, the preferred format for writing an IPv6 address is `x:x:x:x:x:x:x:x`, with each “x” consisting of four hexadecimal values. When referring to 8 bits of an IPv4 address we use the term octet. In IPv6, a hextet is the unofficial term used to refer to a segment of 16 bits or four hexadecimal values. Each “x” is a single hextet, 16 bits or four hexadecimal digits.

Preferred format means the IPv6 address is written using all 32 hexadecimal digits. It does not necessarily mean it is the ideal method for representing the IPv6 address. In the following pages, we will see two rules to help reduce the number of digits needed to represent an IPv6 address.

Figure 2 is a review of the relationship between decimal, binary and hexadecimal. Figure 3 has examples of IPv6 addresses in the preferred format.

## Hextets



## Hexadecimal Numbering

Decimal and Binary equivalents of 0 to F Hexadecimal

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

## 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

## Rule 1 – Omit Leading 0s

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

01AB can be represented as 1AB

09F0 can be represented as 9F0

0A00 can be represented as A00

00AB can be represented as AB

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

The Figures, show several examples of how omitting leading 0s can be used to reduce the size of an IPv6 address. For each example, the preferred format is shown. Notice how omitting the leading 0s in most examples results in a smaller address representation.

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

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

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

## Rule 2 – Omit All 0 Segments

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

**Incorrect address:**

2001:0DB8::ABCD::1234

Possible expansions of ambiguous compressed addresses:

2001:0DB8::ABCD:0000:0000:1234

2001:0DB8::ABCD:0000:0000:0000:1234

2001:0DB8:0000:ABCD::1234

2001:0DB8:0000:0000:ABCD::1234



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

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

Only one :: may be used.

Preferred

FF02:0000:0000:0000:0000:0000:0000:0001

No leading 0s

FF02: 0: 0: 0: 0: 0: 0: 1

Compressed

FF02::1

Preferred

0000:0000:0000:0000:0000:0000:0000:0001

No leading 0s

0: 0: 0: 0: 0: 0: 0: 1

Compressed

::1

## IPv6 Prefix Length

Recall that the prefix, or network portion, of an IPv4 address, can be identified by a **dotted-decimal subnet mask or prefix length** (slash notation). For example, an IPv4 address of 192.168.1.10 with dotted-decimal subnet mask 255.255.255.0 is equivalent to 192.168.1.10/24.

**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.

## /64 Prefix

64 bits

64 bits

Prefix

Interface ID

**Example: 2001:DB8:A::/64**

2001:0DB8:000A:0000

0000:0000:0000:0000

## IPv6 Unicast Addresses

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

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

### Global unicast

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

### Link-local unicast

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

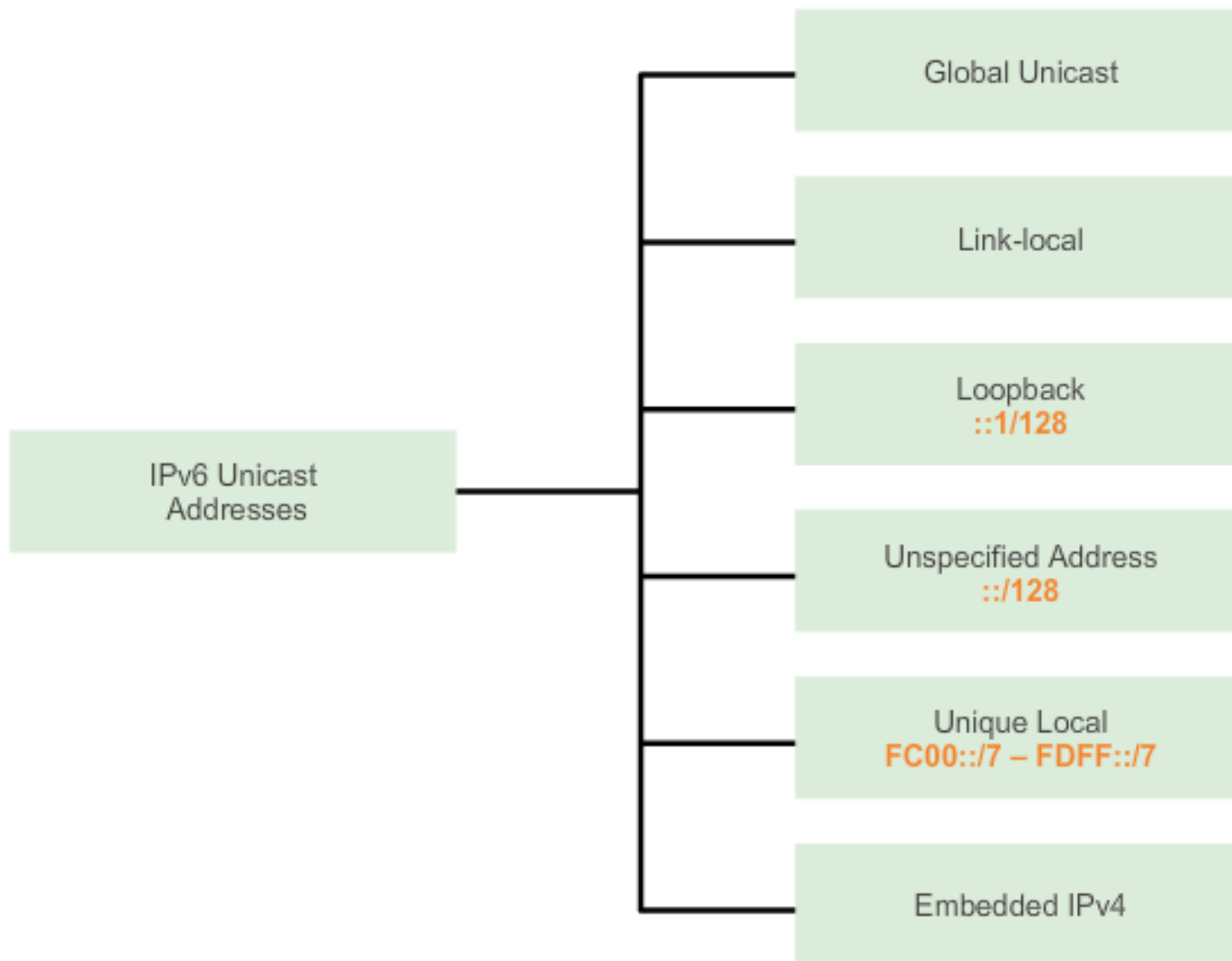
## Unique local

Another type of unicast address is the **unique local unicast address**.

IPv6 unique local addresses have some similarity to RFC 1918 **private addresses for IPv4**, but there are significant differences. Unique local addresses are used for local addressing within a site or between a limited number of sites. These addresses should not be **routable** in the global IPv6 and should not be translated to a global IPv6 address.

Unique local addresses are in the range of FC00::/7 to FDFF::/7.

Unique local addresses can be used for devices that will never need or have access from another network.



## Structure of an IPv6 Global Unicast Address

IPv6 global unicast addresses are globally unique and routable on the IPv6 Internet. These addresses are equivalent to public IPv4 addresses. Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned. This is only 1/8th of the total available IPv6 address space, excluding only a very small portion for other types of unicast and multicast addresses.

Note: The 2001:0DB8::/32 address has been reserved for documentation purposes, including use in examples.

### A global unicast address has three parts:

1. Global routing prefix
2. Subnet ID
3. Interface ID

### Global Routing Prefix

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

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

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



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

### Subnet ID

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

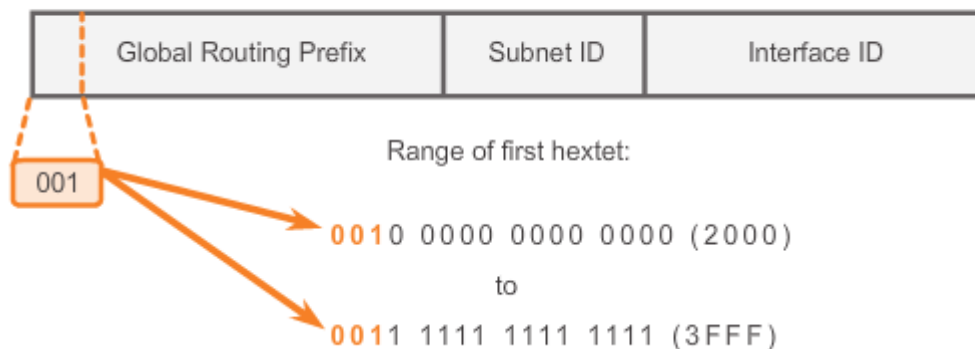
### Interface ID

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

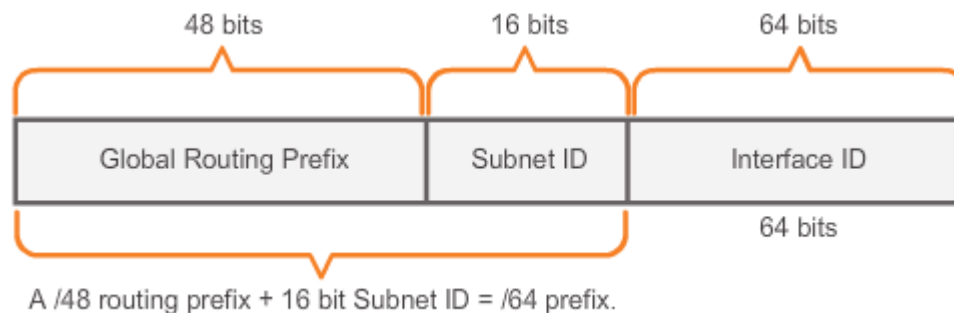
**Note:** Unlike IPv4, in IPv6, the all-0s and all-1s host addresses can be assigned to a device. The all-1s address can be used due to the fact that broadcast addresses are not used within IPv6. The all-0s address can also be used, but is reserved as a Subnet-Router **anycast** address, and should be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

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

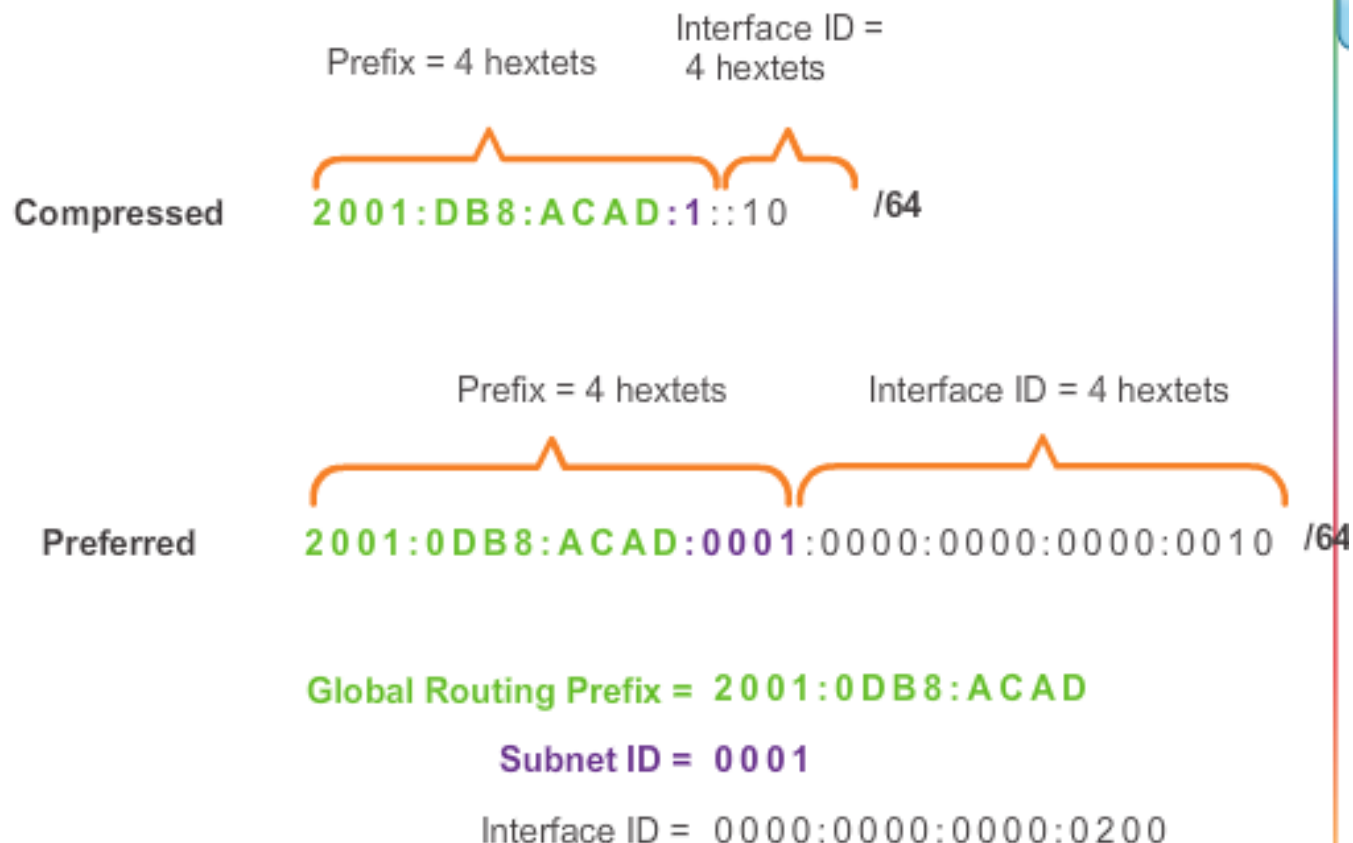
## IPv6 Global Unicast Address



## IPv6 /48 Global Routing Prefix



## Reading a Global Unicast Address



## Dynamic Link-Local Addresses

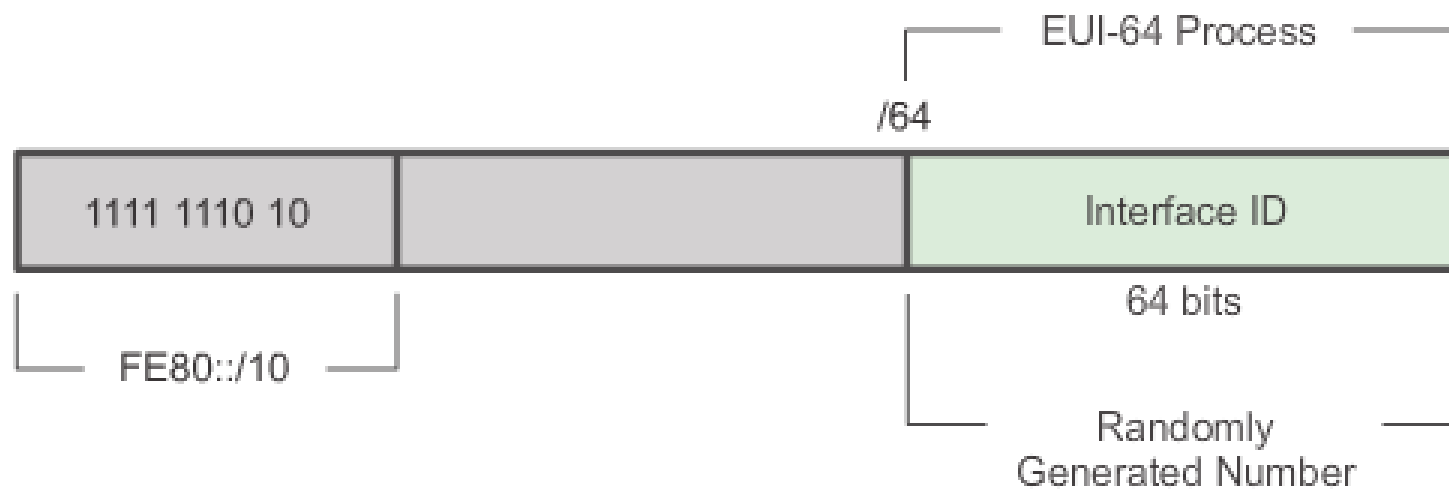
All IPv6 devices must have an IPv6 link-local address. A link-local address can be established dynamically or configured manually as a static link-local address.

Figure 1 shows the link-local address is dynamically created using the FE80::/10 prefix and the Interface ID using the EUI-64 process or a randomly generated 64-bit number. Operating systems will typically use the same method for both a SLAAC created global unicast address and a dynamically assigned link-local address, as shown in Figure 2.

Cisco routers automatically create an IPv6 link-local address whenever a global unicast address is assigned to the interface. By default, Cisco IOS routers use EUI-64 to generate the Interface ID for all link-local address on IPv6 interfaces. For serial interfaces, the router will use the MAC address of an Ethernet interface. Recall that a link-local address must be unique only on that link or network. However, a drawback to using the dynamically assigned link-local address is its length, which makes it challenging to identify and remember assigned addresses. Figure 3 displays the MAC address on router R1's GigabitEthernet 0/0 interface. This address is used to dynamically create the link-local address on the same interface.

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

## IPv6 Link-Local Address



## ICMPv4 and ICMPv6

Although IP is not a reliable protocol, the TCP/IP suite does provide for messages to be sent in the event of certain errors. These messages are sent using the services of ICMP. The purpose of these messages is to provide feedback about issues related to the processing of IP packets under certain conditions, not to make IP reliable. ICMP messages are not required and are often not allowed within a network for security reasons.

ICMP is available for both IPv4 and IPv6. ICMPv4 is the messaging protocol for IPv4. ICMPv6 provides these same services for IPv6 but includes additional functionality. In this course, the term ICMP will be used when referring to both ICMPv4 and ICMPv6.

The types of ICMP messages and the reasons why they are sent, are extensive. We will discuss some of the more common messages.

**ICMP messages common to both ICMPv4 and ICMPv6 include:**

1. **Host confirmation**
2. **Destination or Service Unreachable**
3. **Time exceeded**
4. **Route redirection**

### Host Confirmation

An ICMP Echo Message can be used to determine if a host is operational. The local host sends an ICMP Echo Request to a host. If the host is available, the destination host responds with an Echo Reply. In the figure, click the Play button to see an animation of the ICMP Echo Request/Echo Reply. This use of the ICMP Echo messages is the basis of the ping utility.

## Destination or Service Unreachable

When a host or gateway receives a packet that it cannot deliver, it can use an ICMP Destination Unreachable message to notify the source that the destination or service is unreachable. The message will include a code that indicates why the packet could not be delivered.

Some of the Destination Unreachable codes for ICMPv4 are:

- 0 - Net unreachable
- 1 - Host unreachable
- 2 - Protocol unreachable
- 3 - Port unreachable

**Note:** ICMPv6 has similar but slightly different codes for Destination Unreachable messages.

## Time Exceeded

An ICMPv4 Time Exceeded message is used by a router to indicate that a packet cannot be forwarded because the Time to Live (TTL) field of the packet was decremented to 0. If a router receives a packet and decrements the TTL field in the IPv4 packet to zero, it discards the packet and sends a Time Exceeded message to the source host.

ICMPv6 also sends a Time Exceeded message if the router cannot forward an IPv6 packet because the packet has expired. IPv6 does not have a TTL field; it uses the hop limit field to determine if the packet has expired.



## ICMPv6 Router Solicitation and Router Advertisement Messages

The informational and error messages found in ICMPv6 are very similar to the control and error messages implemented by ICMPv4. However, ICMPv6 has new features and improved functionality not found in ICMPv4. ICMPv6 messages are encapsulated in IPv6.

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

Messaging between an IPv6 router and an IPv6 device:

1. **Router Solicitation (RS) message**
2. **Router Advertisement (RA) message**
3. **Messaging between IPv6 devices:**
4. **Neighbor Solicitation message**
5. **Neighbor Advertisement message**

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

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



## Address Resolution

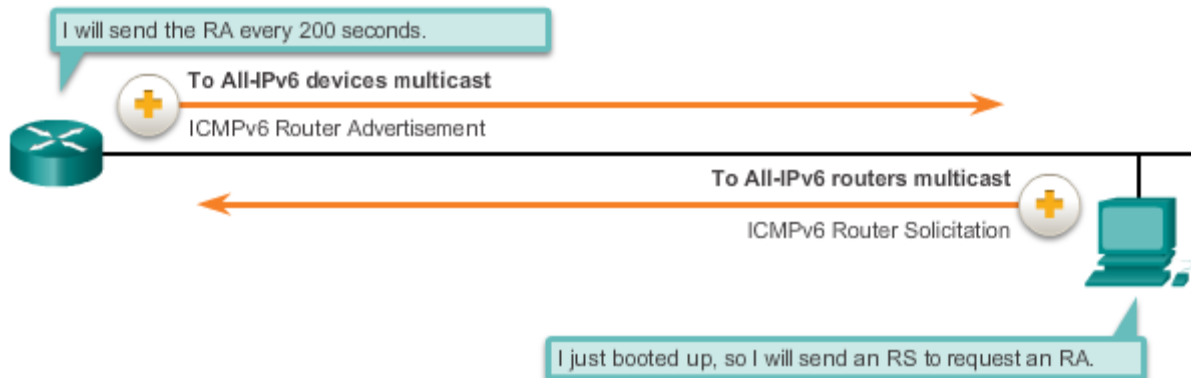
Address resolution is used when a device on the LAN knows the IPv6 unicast address of a destination but does not know its Ethernet MAC address. To determine the MAC address for the destination, the device will send an NS message to the solicited node address. The message will include the known (targeted) IPv6 address. The device that has the targeted IPv6 address will respond with an NA message containing its Ethernet MAC address. Figure 2 shows two PCs exchanging NS and NA messages. Click each message for more information.

## Duplicate Address Detection

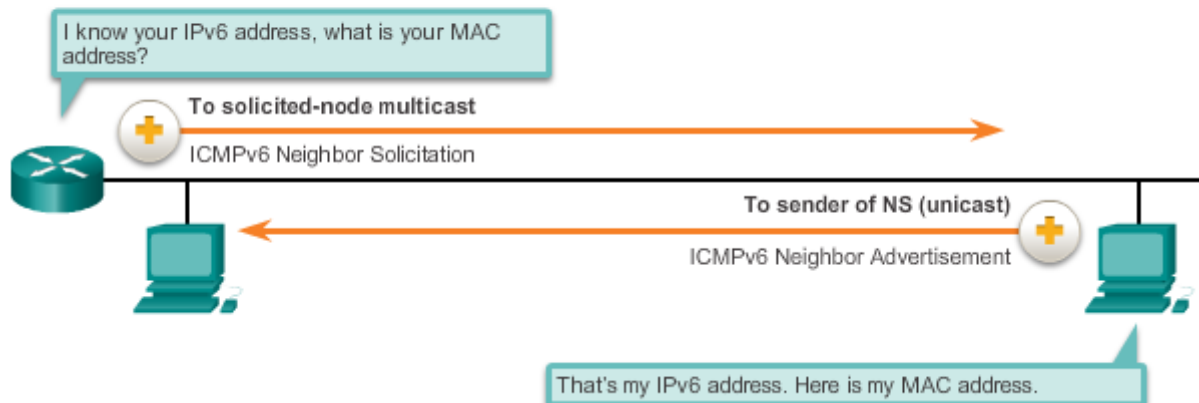
When a device is assigned a global unicast or link-local unicast address, it is recommended that DAD is performed on the address to ensure that it is unique. To check the uniqueness of an address, the device will send an NS message with its own IPv6 address as the targeted IPv6 address, shown in Figure 3. If another device on the network has this address, it will respond with an NA message. This NA message will notify the sending device that the address is in use. If a corresponding NA message is not returned within a certain period of time, the unicast address is unique and acceptable for use.

**Note:** DAD is not required, but RFC 4861 recommends that DAD is performed on unicast addresses.

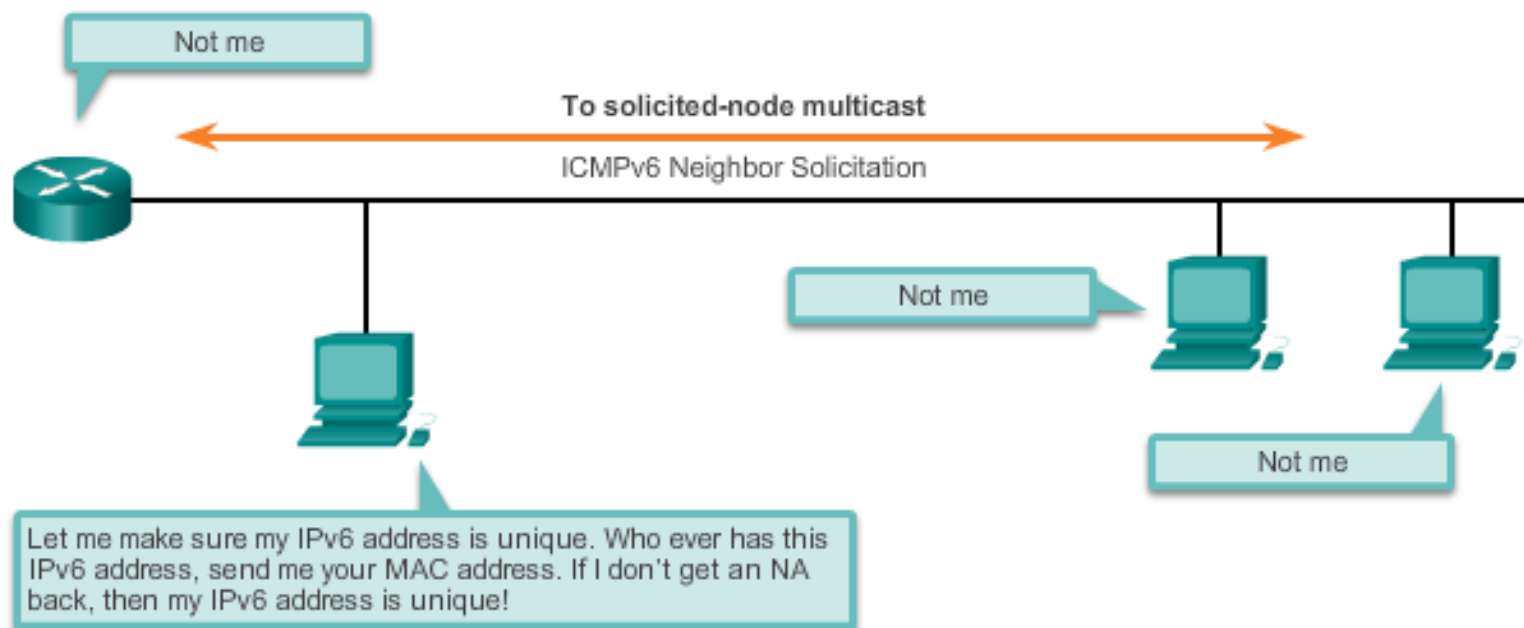
## Messaging Between an IPv6 Router and an IPv6 Device



## Messaging Between IPv6 Devices



## Duplicate Address Detection (DAD)



## Summary

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across the network. To accomplish this end-to-end transport, the network layer uses four basic processes: IP addressing for end devices, encapsulation, routing, and de-encapsulation.

The Internet is largely based on IPv4, which is still the most widely-used network layer protocol. An IPv4 packet contains the IP header and the payload. However, IPv4 has a limited number of unique public IP addresses available. This led to the development of IP version 6 (IPv6). The IPv6 simplified header offers several advantages over IPv4, including better routing efficiency, simplified extension headers, and capability for per-flow processing. Plus, IPv6 addresses are based on 128-bit hierarchical addressing as opposed to IPv4 with 32 bits. This dramatically increases the number of available IP addresses.

In addition to hierarchical addressing, the network layer is also responsible for routing.

Hosts require a local routing table to ensure that packets are directed to the correct destination network. The local table of a host typically contains the direct connection, the local network route, and the local default route. The local default route is the route to the default gateway.

The default gateway is the IP address of a router interface connected to the local network. When a host needs to forward a packet to a destination address that is not on the same network as the host, the packet is sent to the default gateway for further processing.

When a router, such as the default gateway, receives a packet, it examines the destination IP address to determine the destination network. The routing table of a router stores information about directly-connected routes and remote routes to IP networks. If the router has an entry in its routing table for the destination network, the router forwards the packet. If no routing entry exists, the router may forward the packet to its own default route if one is configured, or it will drop the packet.

Routing table entries can be configured manually on each router to provide static routing, or the routers may communicate route information dynamically between each other using a routing protocol.

In order for routers to be reachable, the router interface must be configured. To enable a specific interface, enter interface configuration mode using the **interface** *type-and-number* global configuration mode command.

