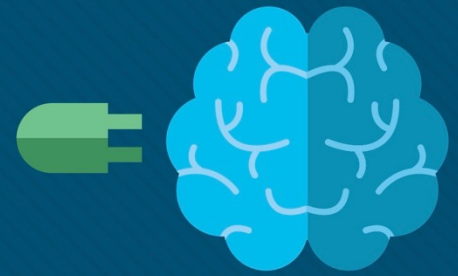


Chapter 3: Network Protocols and Services

Information Security

Dr. Ayman Aljarbouh

3.2 Ethernet and Internet Protocol (IP)

Module Objectives

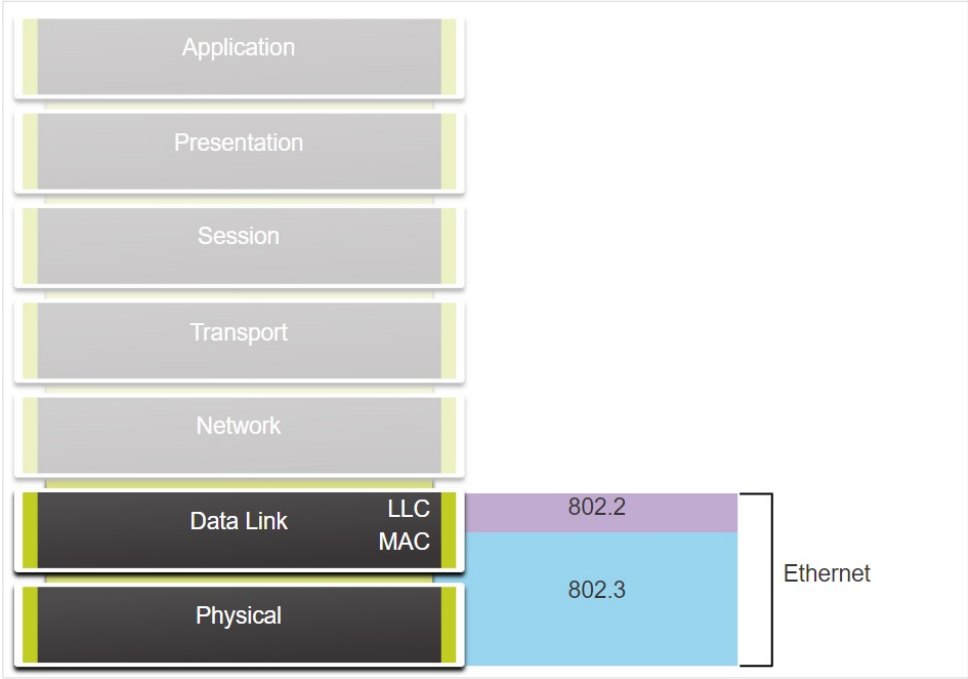
Module Title: Ethernet and Internet Protocol (IP)

Module Objective: Explain how the Ethernet and IP protocols support network communication.

Topic Title	Topic Objective
Ethernet	Explain how Ethernet supports network communication.
IPv4	Explain how the IPv4 protocol supports network communications.
IP Addressing Basics	Explain how IP addresses enable network communication.
Types of IPv4 Addresses	Explain the types of IPv4 addresses that enable network communication.
The Default Gateway	Explain how the default gateway enables network communication.
IPv6	Explain how the IPv6 protocol supports network communications.

The Ethernet Protocol

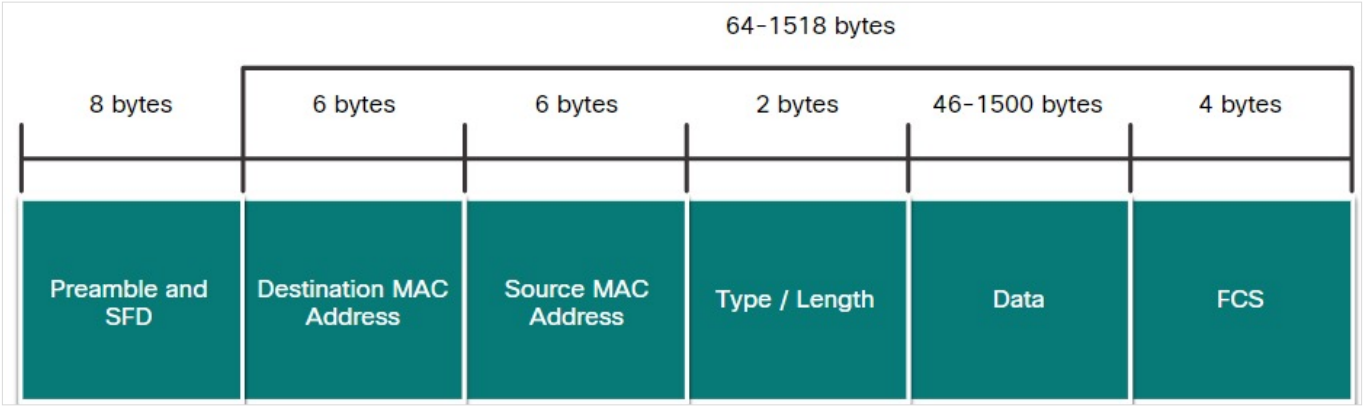
- Unlike wireless, Ethernet uses wired communications, including twisted pair, fiber-optic links, and coaxial cables.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.
- Ethernet supports data bandwidths from 10 Mbps to 100,000 Mbps (100 Gbps)
- Ethernet Sublayers
  - Logical Link Layer (LLC)
  - Media Access Control Layer (MAC)



Ethernet and the OSI Model

Ethernet Frame Fields

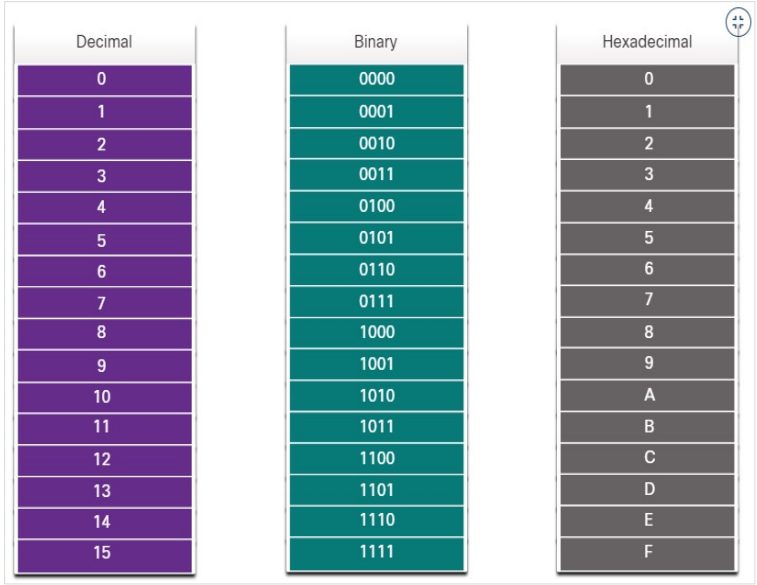
- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes. This includes all bytes from the destination MAC address field through the Frame Check Sequence (FCS) field.
- Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded by receiving stations. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.



Ethernet Frame Fields

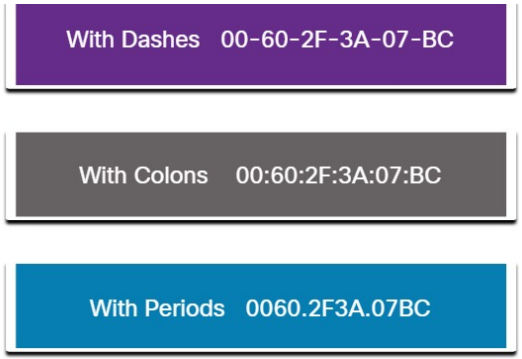
MAC Address Format

- An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits.
- Hexadecimal digits uses numbers 0 to 9 and the letters A to F.
- Hexadecimal is commonly used to represent binary data.
- All data that travels on the network is encapsulated in Ethernet frames.



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

Decimal and Binary Equivalents of 0 to F Hexadecimal



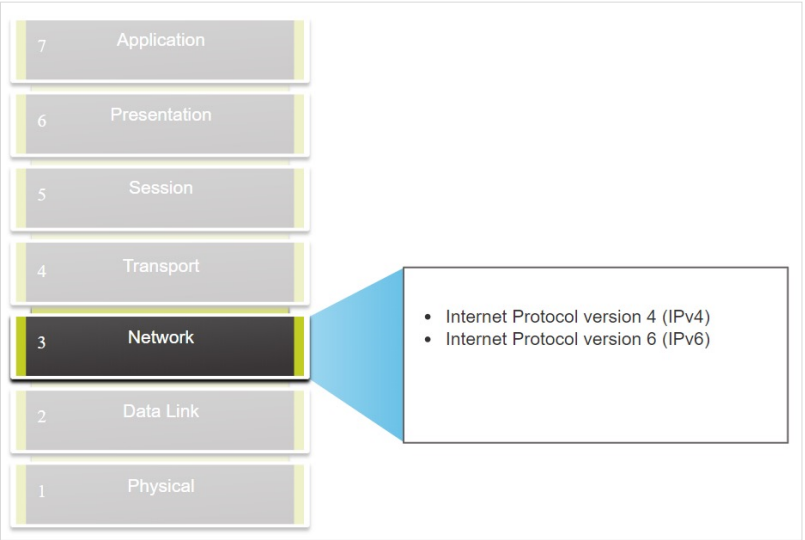
Different Representations of MAC Addresses

The Network Layer

- The network layer provides services to allow end devices to exchange data across networks.
- IPv4 and IPv6 are the principle network layer communication protocols.

Basic operations of network layer protocol:

- **Addressing end devices** - Configured with a unique IP address for identification
- **Encapsulation** - Encapsulates the Protocol Data Unit (PDU) from the transport layer into a packet.
- **Routing** - Select the best path and direct packets towards destination host.
- **De-encapsulation** – Performed by the destination host.



Network Layer Protocol

Characteristics of IP

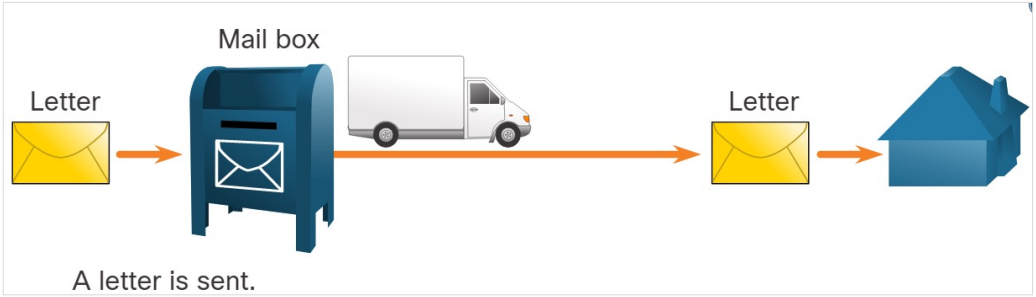
Characteristics of IP

- **Connectionless** – no dedicated end-to-end connection is created before data is sent.
- **Unreliable (Best Effort)** - IP protocol does not guarantee that all packets that are delivered are, in fact, received.
- **Media Independent** - IP operates independently of the media that carry the data at lower layers of the protocol stack.

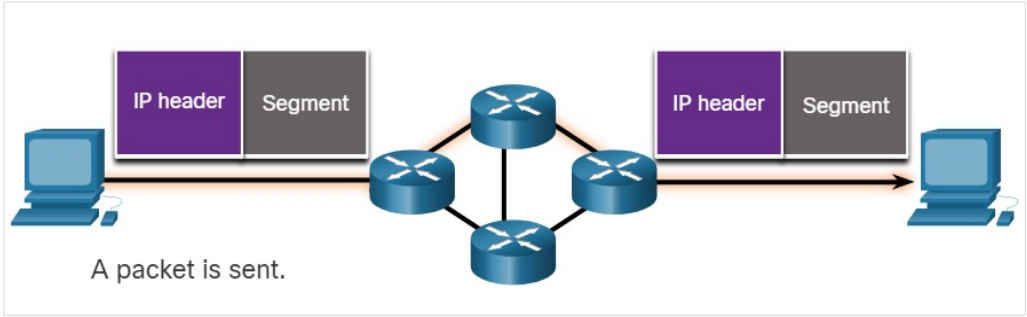
Characteristics of IP

Characteristics of IP

- **Connectionless** – no dedicated end-to-end connection is created before data is sent.
- **Unreliable (Best Effort)** - IP protocol does not guarantee that all packets that are delivered are, in fact, received.
- **Media Independent** - IP operates independently of the media that carry the data at lower layers of the protocol stack.



Connectionless - Analogy

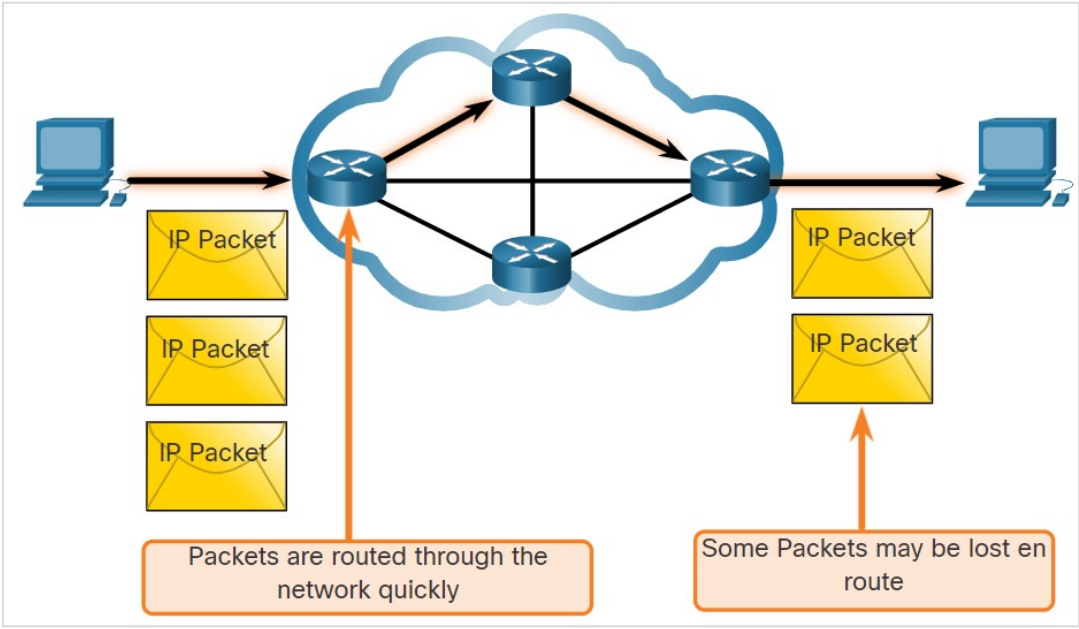


Connectionless - Network

Characteristics of IP

Characteristics of IP

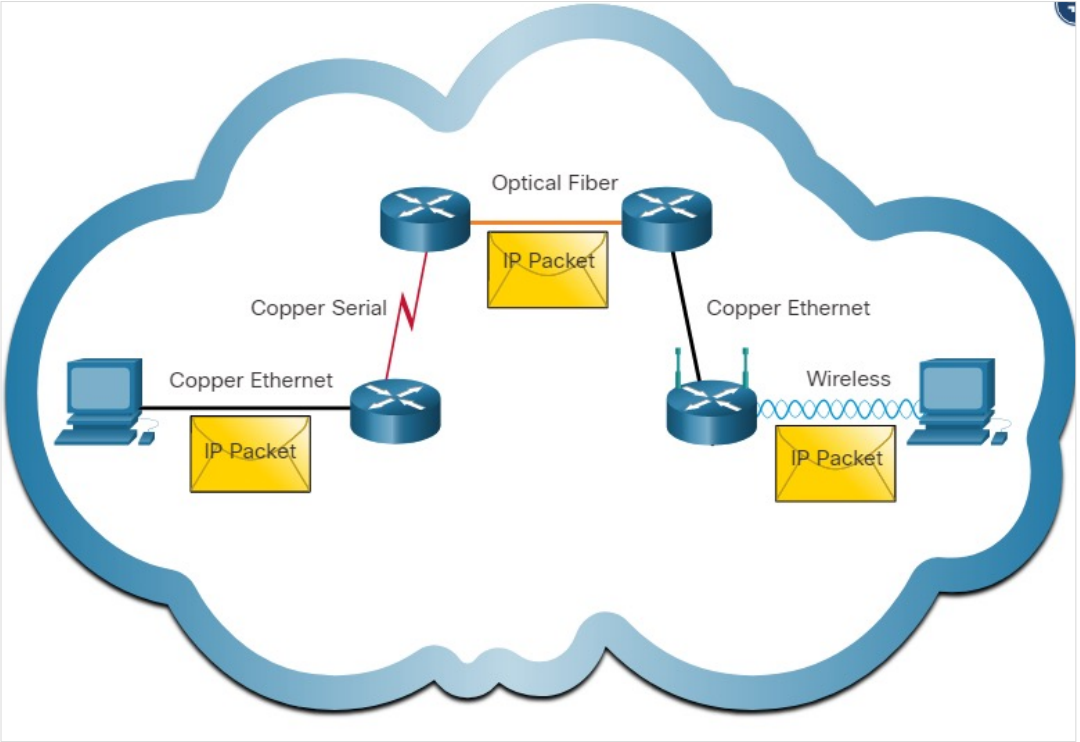
- **Connectionless** – no dedicated end-to-end connection is created before data is sent.
- **Unreliable (Best Effort)** - IP protocol does not guarantee that all packets that are delivered are, in fact, received.
- **Media Independent** - IP operates independently of the media that carry the data at lower layers of the protocol stack.



Characteristics of IP

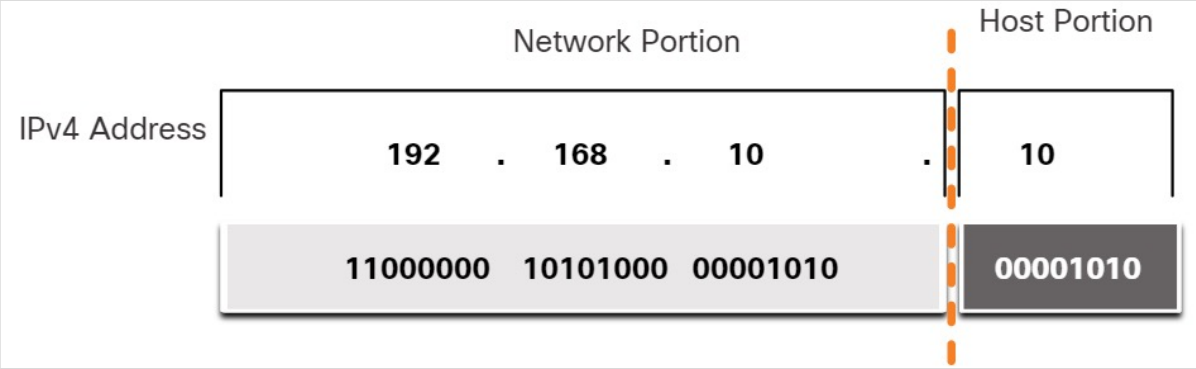
Characteristics of IP

- **Connectionless** – no dedicated end-to-end connection is created before data is sent.
- **Unreliable (Best Effort)** - IP protocol does not guarantee that all packets that are delivered are, in fact, received.
- **Media Independent** - IP operates independently of the media that carry the data at lower layers of the protocol stack.



Network and Host Portions

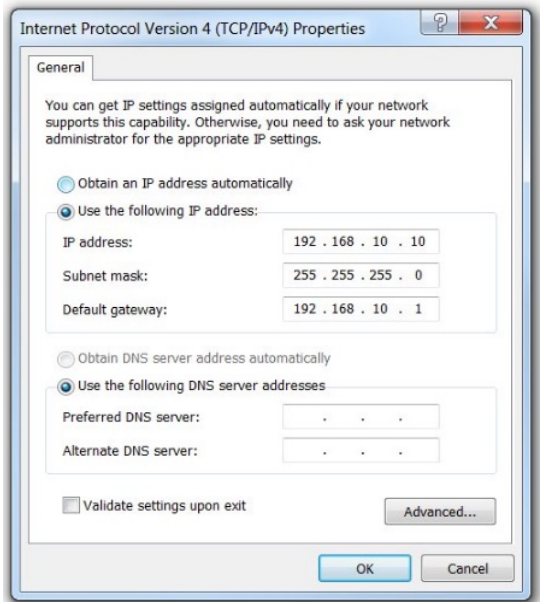
- An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.
- The bits within the network portion of the address must be identical for all devices that are in the same network.
- The bits within the host portion of the address must be unique to identify a specific host within a network.



The Subnet Mask

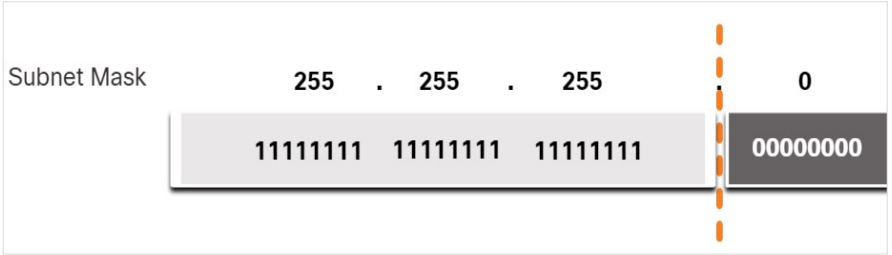
To assign IPv4 address to a host requires the following:

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



Subnet Mask

- When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address of the device.
- Subnet mask is a consecutive sequence of 1 bits followed by a consecutive sequence of 0 bits.



The Prefix Length

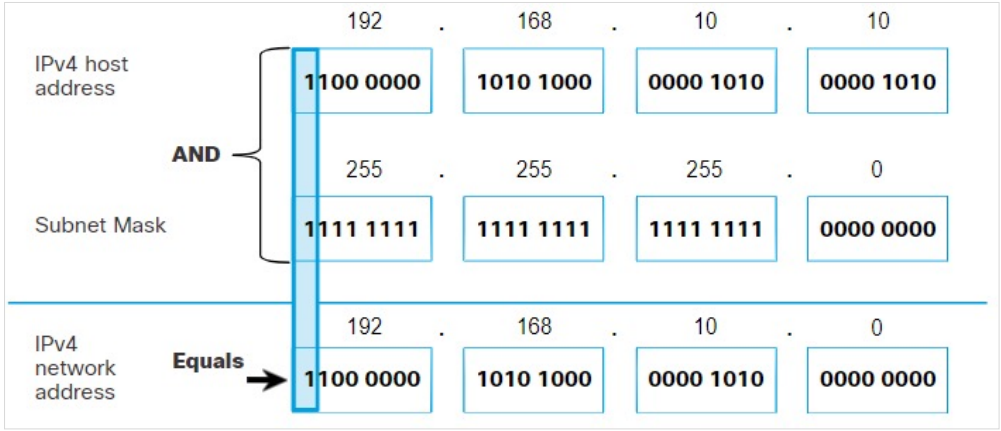
The prefix length is the number of bits set to 1 in the subnet mask. When representing an IPv4 address using a prefix length, the IPv4 address is written followed by the prefix length with no spaces. For example, 192.168.10.10 255.255.255.0 would be written as 192.168.10.10/24.

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

Determining the Network: Logical AND

- Consider a host with IPv4 address 192.168.10.10 and subnet mask of 255.255.255.0, as shown in the figure:

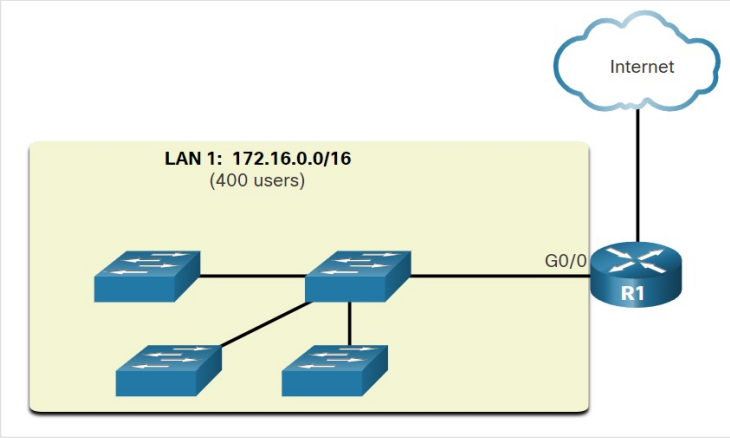
- **IPv4 host address (192.168.10.10)** - The IPv4 address of the host in dotted decimal and binary formats.
- **Subnet mask (255.255.255.0)** - The subnet mask of the host in dotted decimal and binary formats.
- **Network address (192.168.10.0)** - The logical AND operation between the IPv4 address and subnet mask results in an IPv4 network address shown in dotted decimal and binary formats.



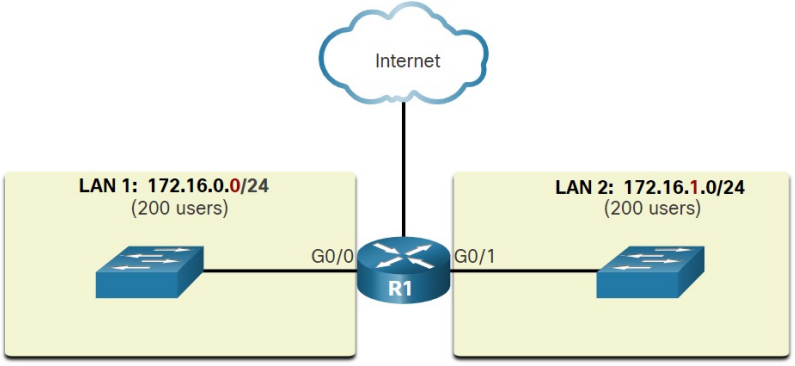
To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask.

Subnetting Broadcast Domains

- In the figure, LAN 1 connects 400 users that could each generate broadcast traffic, which can slow down network and device operations.
- The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting. These smaller network spaces are called subnets.
- Subnetting reduces the overall network traffic and improves network performance.



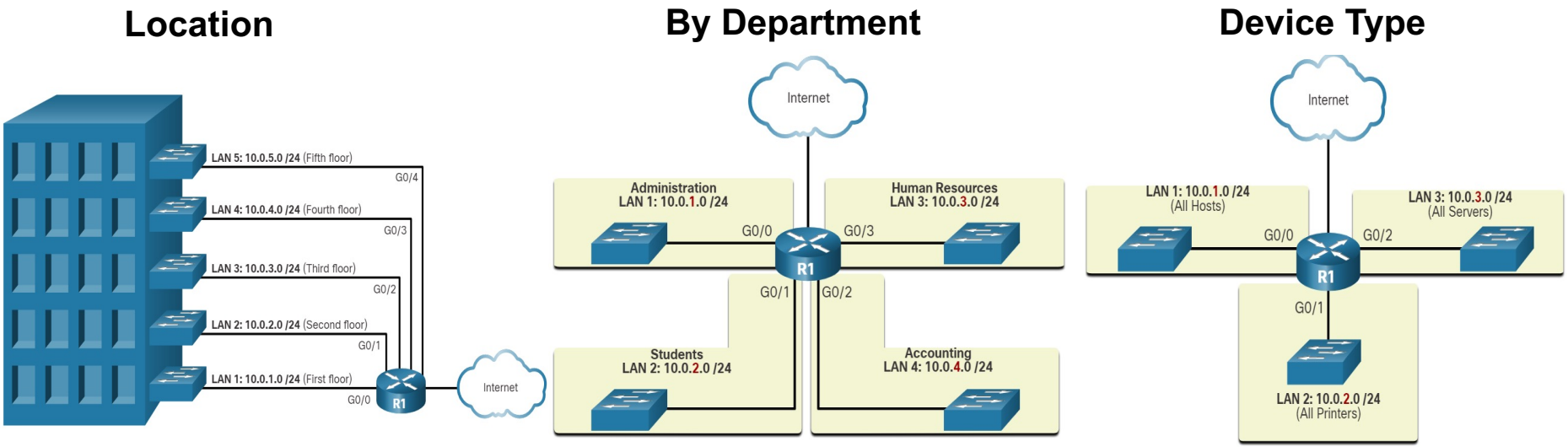
A Large Broadcast Domain



Communication between Networks

Subnetting Broadcast Domains (Contd.)

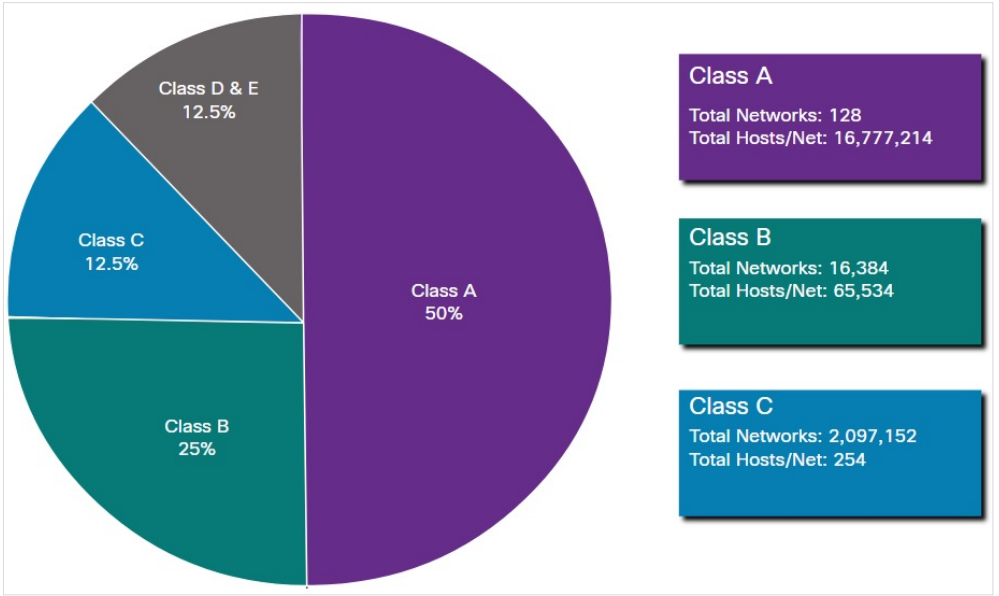
- Network administrators can group devices and services into subnets that may be determined by a variety of factors.



IPv4 Address Classes and Default Subnet Masks

Assigned Classes – A, B, C, D, and E

- **Class A** (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks.
- **Class B** (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support moderate to large networks.
- **Class C** (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks.
- **Class D** (224.0.0.0 to 239.0.0.0) – Multicast block.
- **Class E** (240.0.0.0 – 255.0.0.0) – Experimental address block.



Summary of Classful Addressing

Reserved Private Addresses

Private Addresses:

- 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 any internal network.

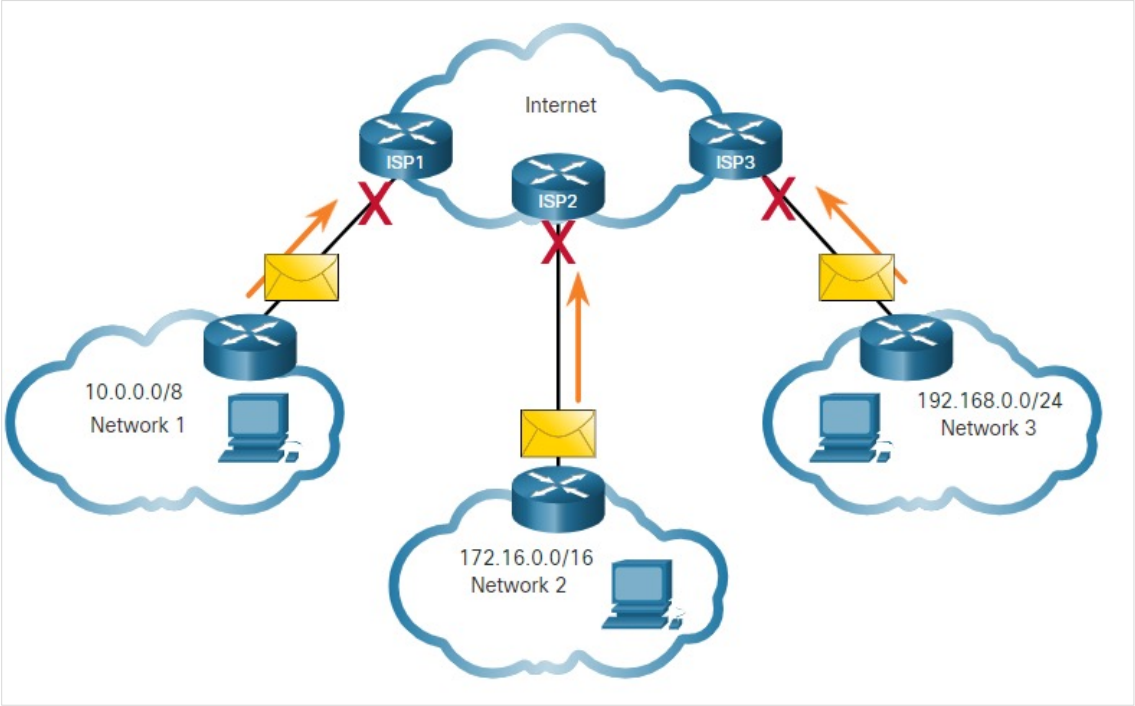
Private address blocks:

  - 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

- The addresses within these address blocks are not allowed on the internet and must be filtered by internet routers.

Reserved Private Addresses (Contd.)

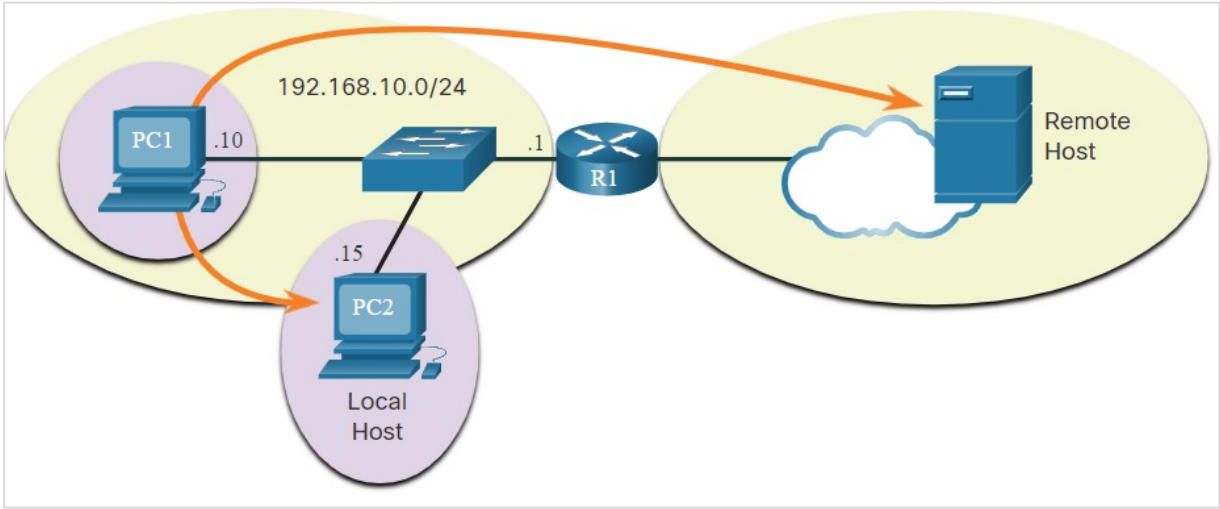
- In the figure, users in networks 1, 2, or 3 are sending packets to remote destinations. The ISP routers would see that the source IPv4 addresses in the packets are from private addresses and discard the packets.
- Most organizations use private IPv4 addresses for their internal hosts.



Private Addresses Cannot be Routed over the Internet

Host Forwarding Decision

- A host can send a packet to three types of destinations:
  - **Itself** - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1.
  - **Local host** - This is a host on the same local network.
  - **Remote host** - This is a host on a remote network. The hosts do not share the same network address.



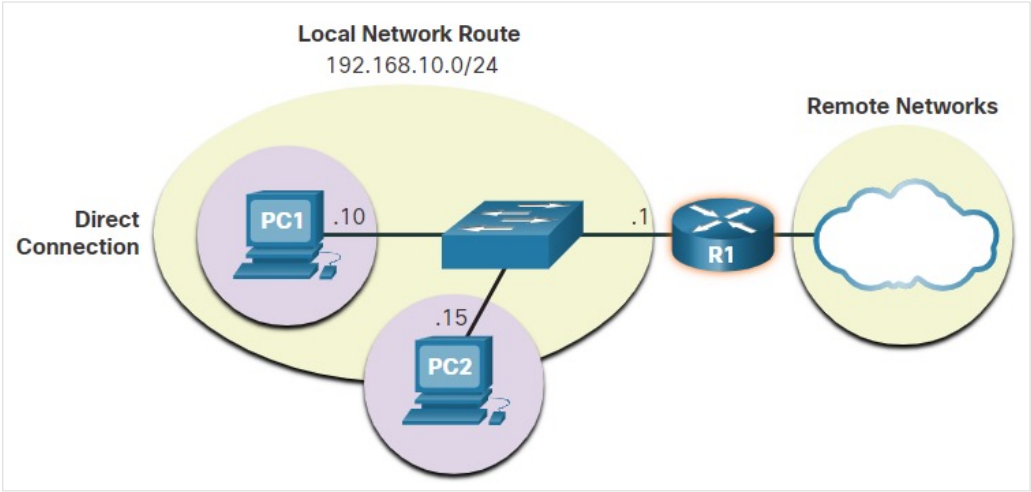
Default Gateway

- The default gateway is the network device that can route traffic to other networks.
- On a network, a default gateway is usually a router with these features:
  - It has a local IP address in the same address range as other hosts on the local network.
  - It can accept data into the local network and forward data out of the local network.
  - It routes traffic to other networks.
- A default gateway is required to send traffic outside the local network.
- Traffic cannot be forwarded outside the local network if there is no default gateway, or the default gateway address is not configured, or the default gateway is down.

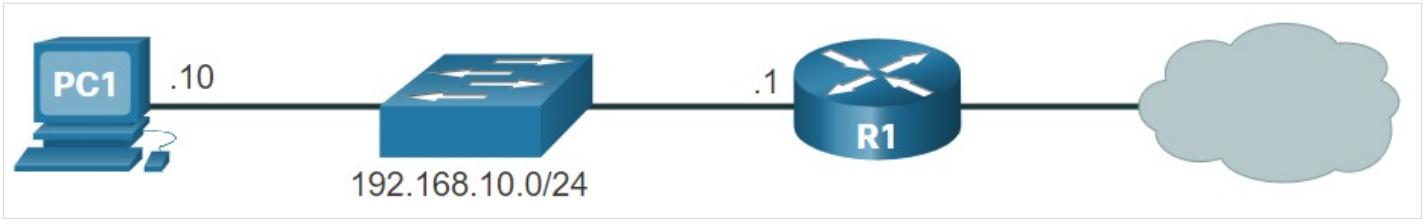
Using the Default Gateway

A host's routing table will typically include a default gateway.

- The host receives the IPv4 address of the default gateway.
- IP addressing information:
  - Configured manually.
  - Obtained automatically/dynamically using Dynamic Host Configuration Protocol (DHCP).
  - Placed in computer's routing table.



PC1 and PC2 are configured with the IPv4 address of 192.168.10.1 as the default gateway



Host Routing Tables

- Entering the **netstat -r** command displays three sections related to the current TCP/IP network connections:
  - Interface List
  - IPv4 Route Table
  - IPv6 Route Table

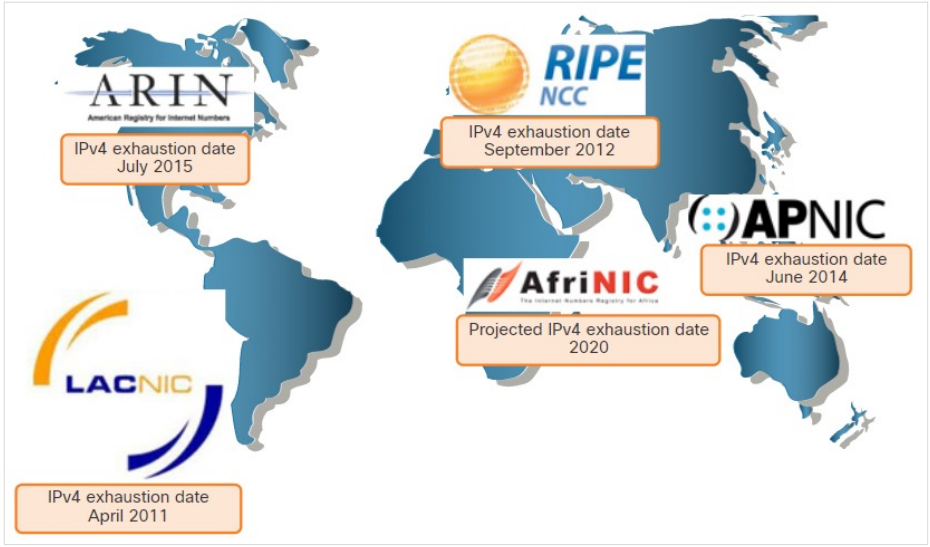

```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```

IPv4 Routing Table for PC1

Need for IPv6

- IPv6 is designed to be the successor to IPv4.
- IPv6 has a larger 128-bit address space, providing 340 undecillion possible addresses.
- Mobile providers have been leading the way with the transition to IPv6.
- Most top ISPs and content providers such as YouTube, Facebook, and Netflix, have also made the transition.
- Many companies like Microsoft, Facebook, and LinkedIn are transitioning to IPv6-only internally.
- The depletion of IPv4 address space has been the motivating factor for moving to IPv6.

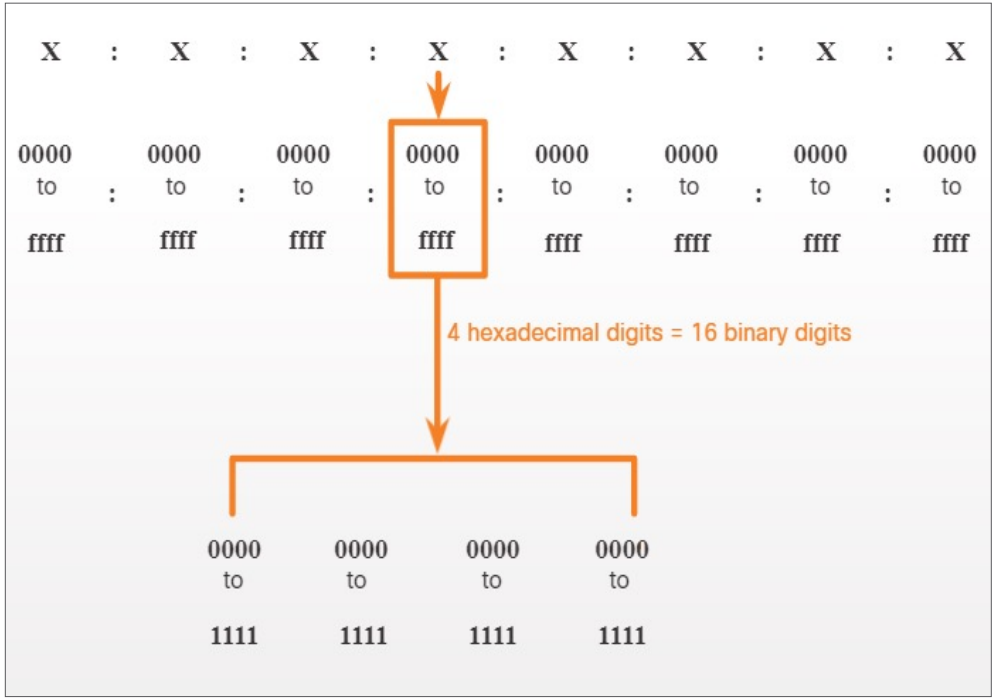


RIR IPv4 Exhaustion Dates

IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written as a string of hexadecimal values.
- Every four bits is represented by a single hexadecimal digit for a total of 32 hexadecimal values.
- IPv6 addresses are not case-sensitive.

```
2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a: 19ac
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0000
```



16-bit Segments or Hextets

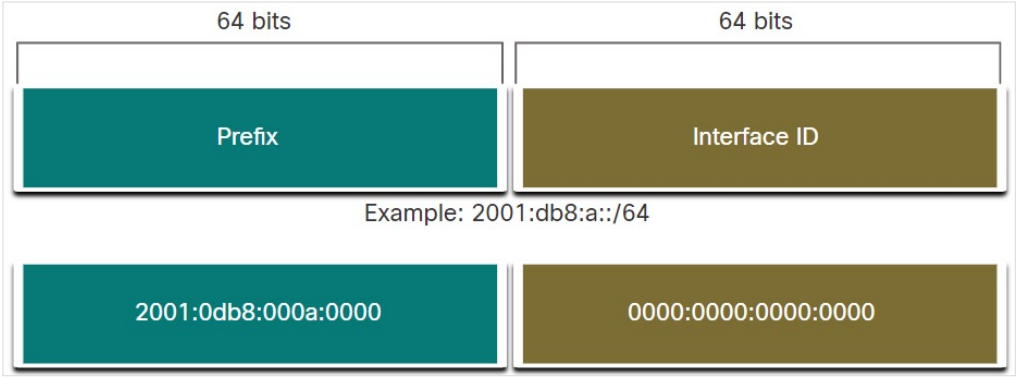
IPv6 Addressing Formats

- IPv6 Addresses:
  - 128 bit address space.
  - Can remove leading zeros.
  - Can leave out 1 “all zeros” segment.
  - Double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros

Type	Format
Fully expanded	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

IPv6 Prefix Length

- The prefix 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.
- In IPv4 the /24 is called the prefix, whereas in Pv6 it is called the prefix length.
- Similar to IPv4, the prefix length is represented in slash notation and is used to indicate the network portion of an IPv6 address. It can range from 0 to128.
- It is strongly recommended to use a 64-bit Interface ID for most networks.



New Terms and Commands

• subnet mask • subnetting • Internet Protocol (IP)	• Time to Live (TTL) • Media Access Control (MAC)

Lab 10 - Introduction to Wireshark

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education.

In this lab, you will use Wireshark to capture and analyze network traffic.