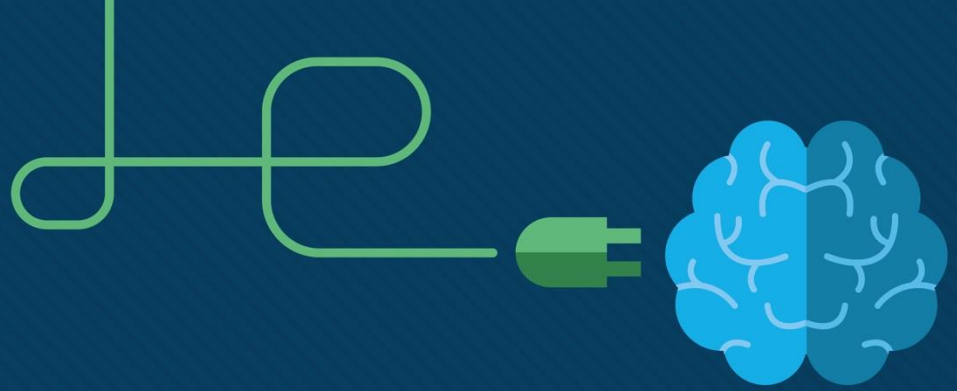
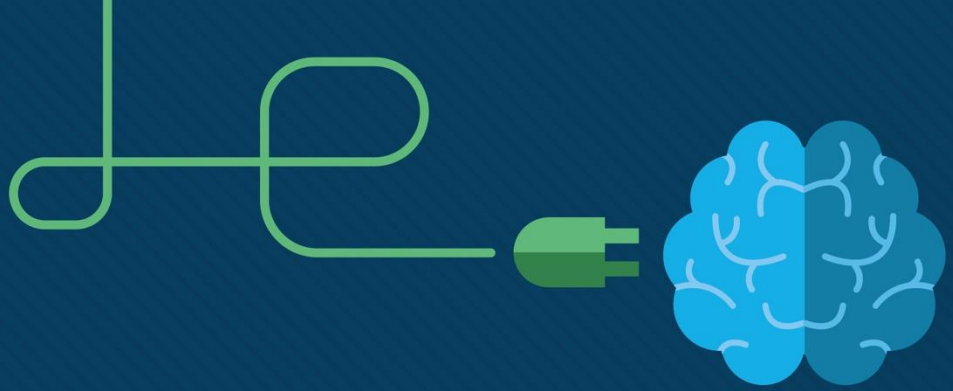


Module 6:Ethernet and Internet Protocol(IP)

Instructor Materials

CyberOps Associate v1.0



Module 6:Ethernet and Internet Protocol(IP)

CyberOps Associates v1.0

Module Objectives

Module Title: Ethernet and IP Protocol

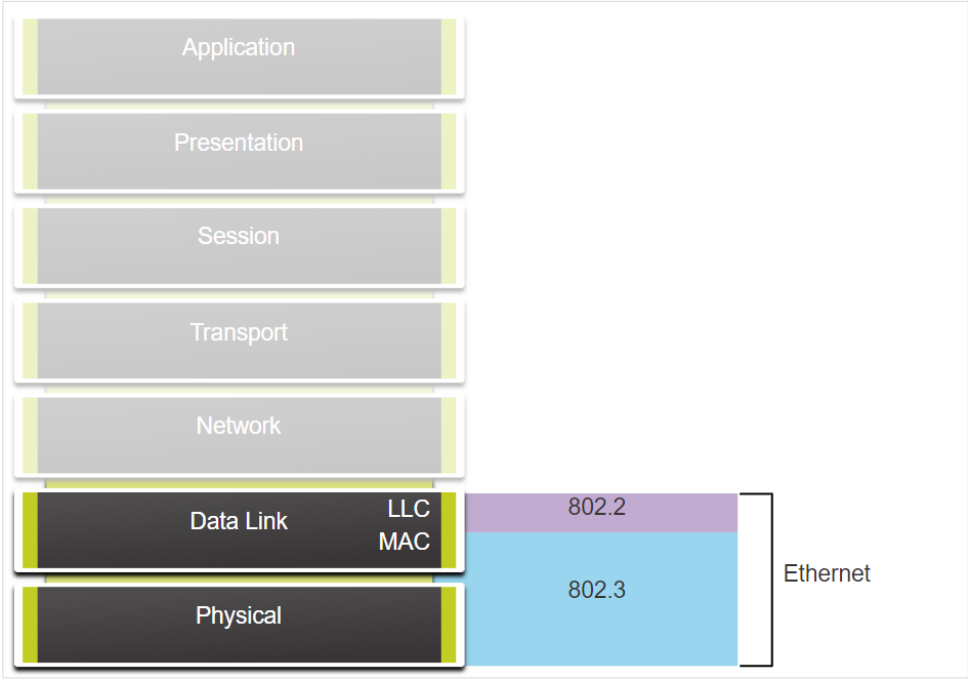
Module Objective: Explain how the Ethernet and IP protocols support network communication.

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.

6.1 Ethernet

Ethernet Encapsulation

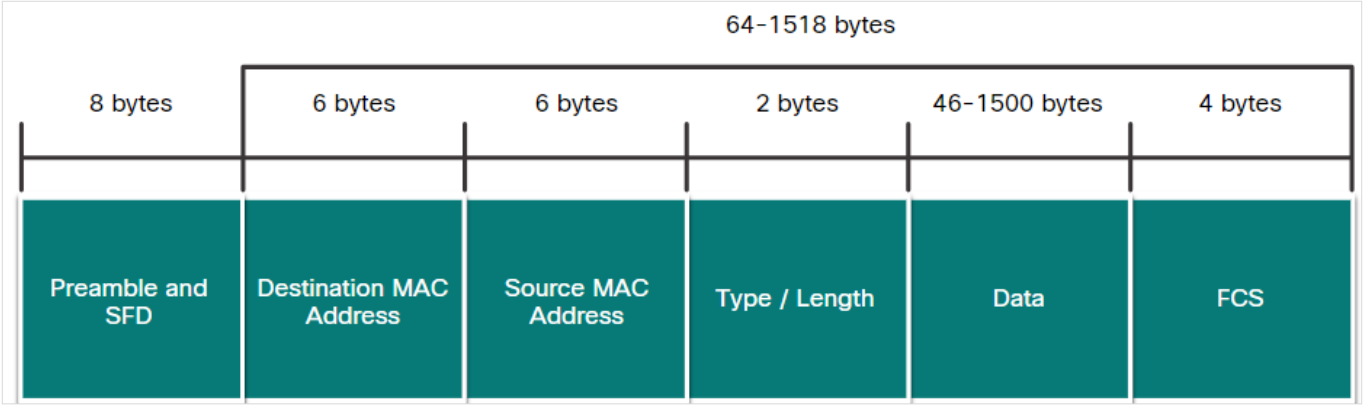
- Unlike wireless, Ethernet uses wired communications, including twisted pair, fiber-optic links, and coaxial cables.
- Ethernet operates in the data link layer and physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.
- Ethernet supports data bandwidths from 10 Mbps to 100,000 Mbps (100 Gbps)
- As seen in the figure, Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.



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

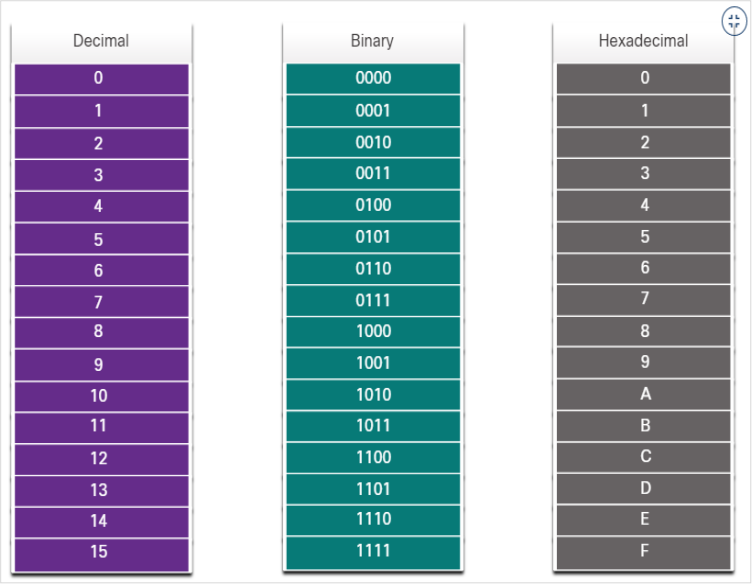
Ethernet Frame Fields

- The Ethernet fields and their description is as follows:

Field	Description
Preamble and Start Frame Delimiter	Used for synchronization between the sending and receiving devices.
Destination MAC Address	It is the identifier for the intended recipient. This address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device.
Source MAC Address	Identifies the originating NIC or interface of the frame.
Type / Length	Identifies the upper layer protocol encapsulated in the Ethernet frame.
Data Field	Contains the encapsulated data from a higher layer, an IPv4 packet.
Frame Check Sequence	Used to detect errors in a frame using Cyclic Redundancy Check (CRC).

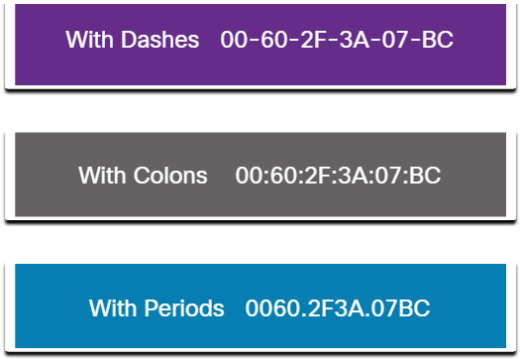
MAC Address Format

- 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

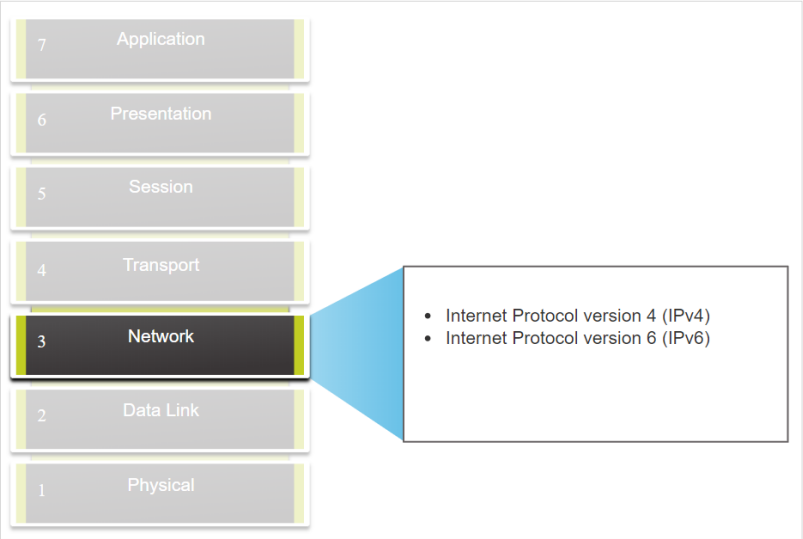
6.2 IPv4

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.
- Open Shortest Path First (OSPF) and Internet Control Message Protocol (ICMP) are other network layer 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.

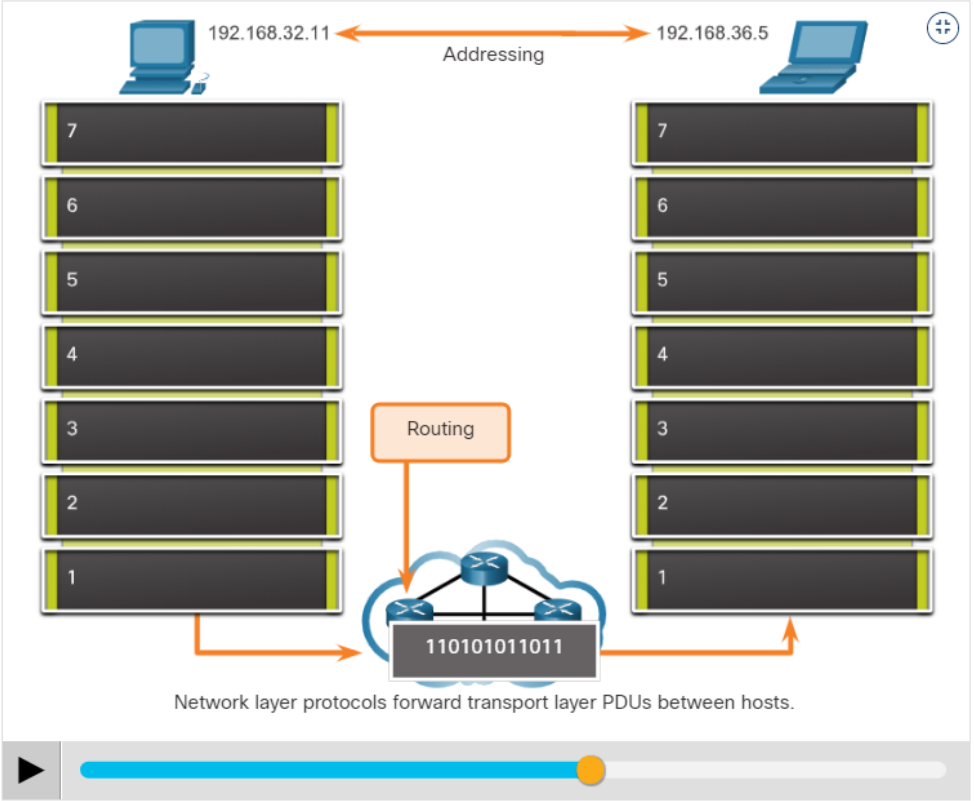


Network Layer Protocol

The Network Layer (Contd.)

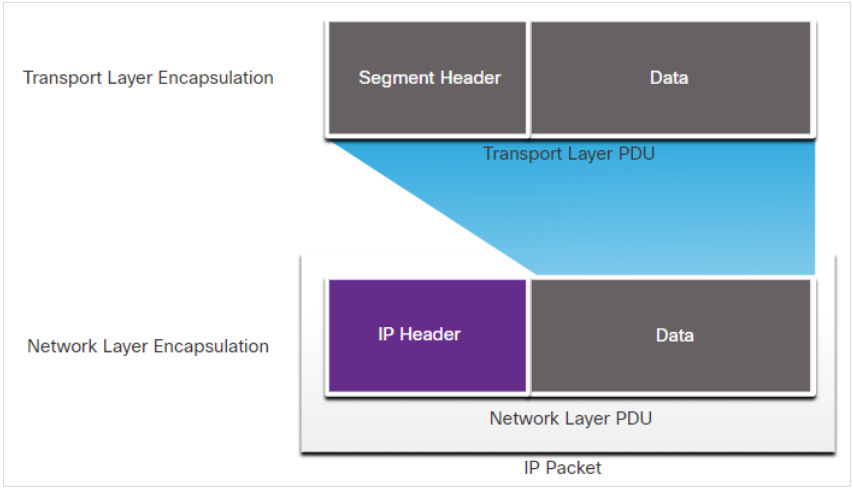
- Network layer communication protocols specify the packet structure and processing used to carry the data from one host to another host.
- Operating without regard to the data carried in each packet allows the network layer to carry packets for multiple types of communications between multiple hosts.

Click Play in the figure to view an animation that demonstrates the exchange of data.



IP Encapsulation

- IP encapsulates the transport layer segment or other data by adding an IP header.
- IP Header is used to deliver the packet to the destination host. It is examined by Layer 3 devices.
- The process of encapsulating data layer by layer enables the services at the different layers to develop and scale without affecting the other layers.
- IP addressing information remains the same from the time the packet leaves the source host until it arrives at the destination host, except when translated by the device performing Network Address Translation (NAT) for IPv4.
- The encapsulated transport layer PDU or other data, remains unchanged during the network layer processes.



Characteristics of IP

IP was designed as a protocol with low overhead.

IP provides the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.

The basic characteristics of IP are as follows**:**

- **Connectionless** - There is no connection with the destination established before sending data packets.
- **Best Effort** - IP is inherently unreliable because packet delivery is not guaranteed.
- **Media Independent** - Operation is independent of the medium (for example, copper, fiber-optic, or wireless) carrying the data.

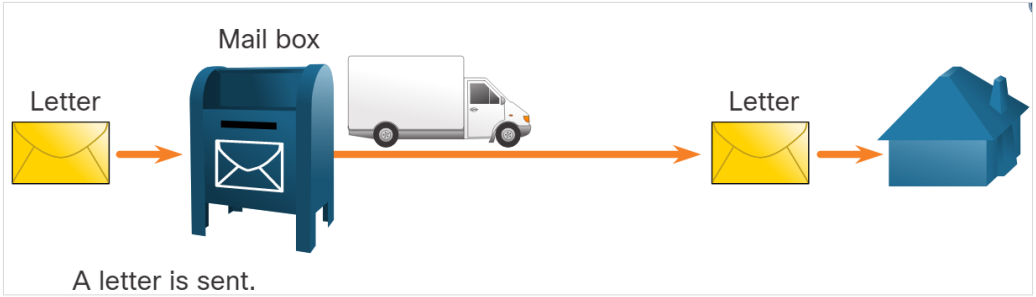
Connectionless

Connectionless - Analogy

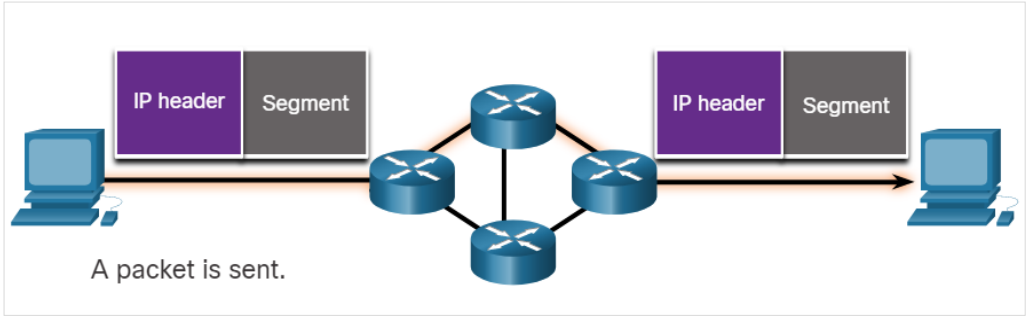
- There is no dedicated end-to-end connection created by IP before data is sent.
- Connectionless communication is conceptually similar to sending a letter to someone without notifying the recipient in advance.

Connectionless - Network

- IP requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded.



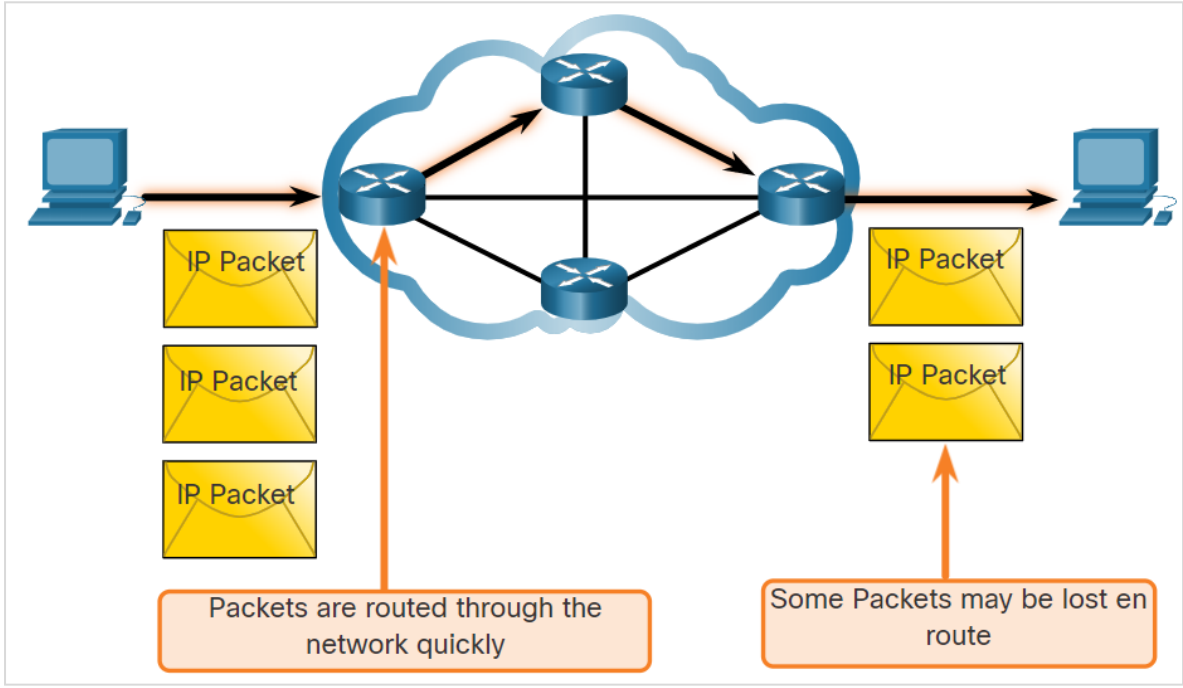
Connectionless - Analogy



Connectionless - Network

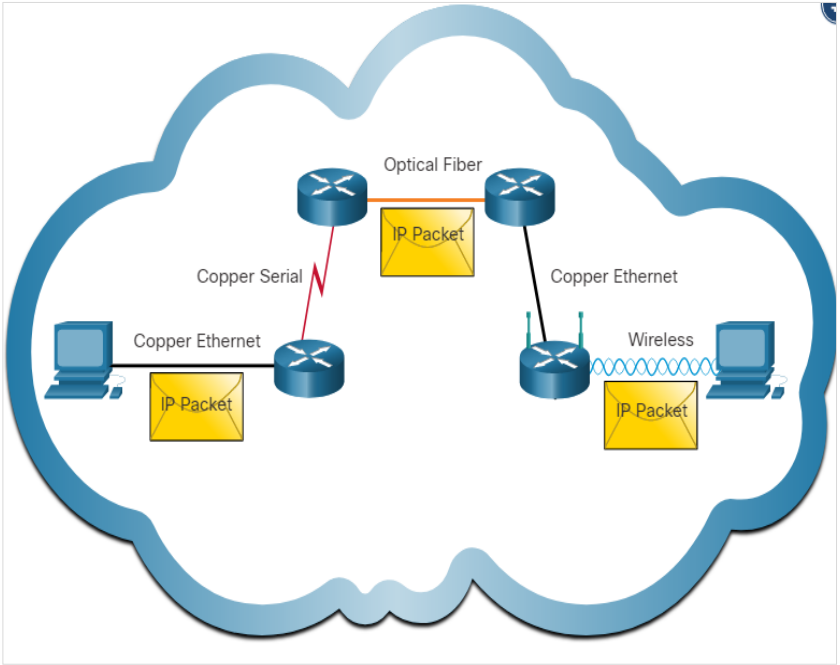
Best Effort

- As an unreliable network layer protocol, IP protocol does not guarantee that all the sent packets will be received.
- Other protocols manage the process of tracking packets and ensuring their delivery.
- The figure illustrates the unreliable or best-effort delivery characteristic of the IP protocol.



Media Independent

- IP operates independently of the media that carry the data at lower layers of the protocol stack.
- IP packets can be communicated as electronic signals over copper cable, as optical signals over fiber, or wirelessly as radio signals.
- The OSI data link layer is responsible for taking an IP packet and preparing it for transmission over the communications medium.
- The maximum size of the PDU that each medium can transport is referred to as the Maximum Transmission Unit (MTU).



- The data link layer passes the MTU value up to the network layer. Later, the network layer determines the size of the large packets.

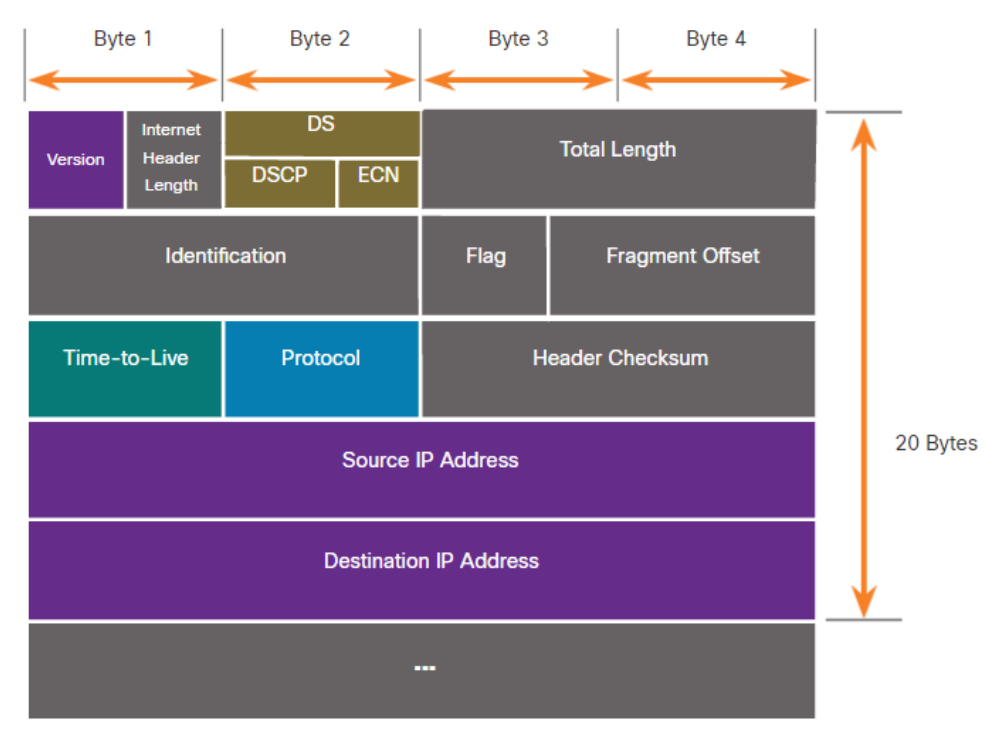
IPv4 Packet Header

- IPv4 is one of the primary network layer communication protocols.
- The IPv4 packet header is used to ensure that this packet is delivered to its next stop on the way to its destination end device.
- An IPv4 packet header consists of fields containing important information about the packet.
- These fields contain binary numbers which are examined by the Layer 3 process.

IPv4 Packet Header Fields

The significant fields in the IPv4 header include the following:

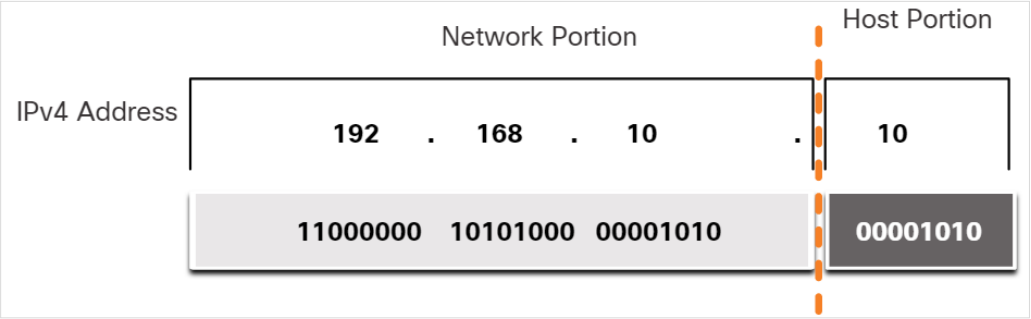
- Version
- Differentiated Services or DiffServ (DS)
- Header Checksum
- Time to Live (TTL)
- Protocol
- Source IPv4 Address
- Destination IPv4 Address



6.3 IP Addressing Basics

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.
- If two hosts have the same bit-pattern in the specified network portion of the 32-bit stream, then those two hosts will reside in the same network.

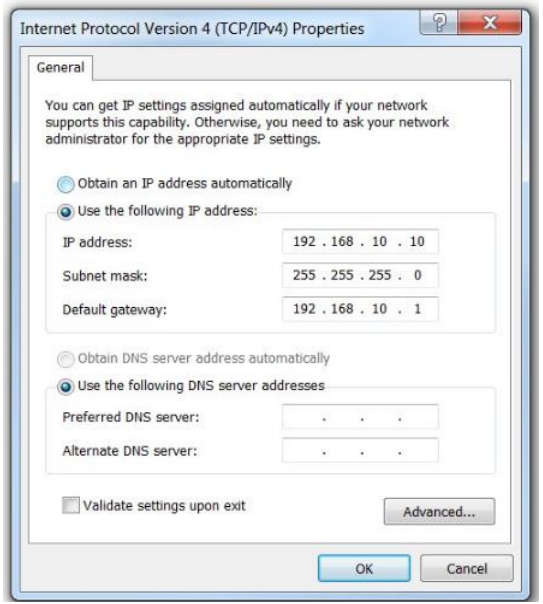


The Subnet Mask

To assign IPv4 address to a host requires the following:

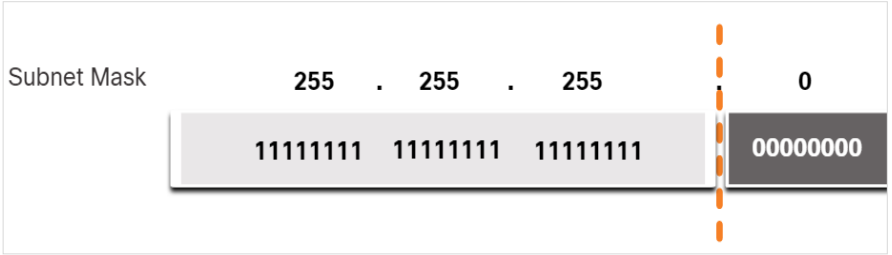
- **IPv4 address** - Unique IPv4 address of the host.
- **Subnet mask**- Used to identify the network/host portion.

Note: *A default gateway IPv4 address is required to reach remote networks and DNS server IPv4 addresses are required to translate domain names to IPv4 addresses.*



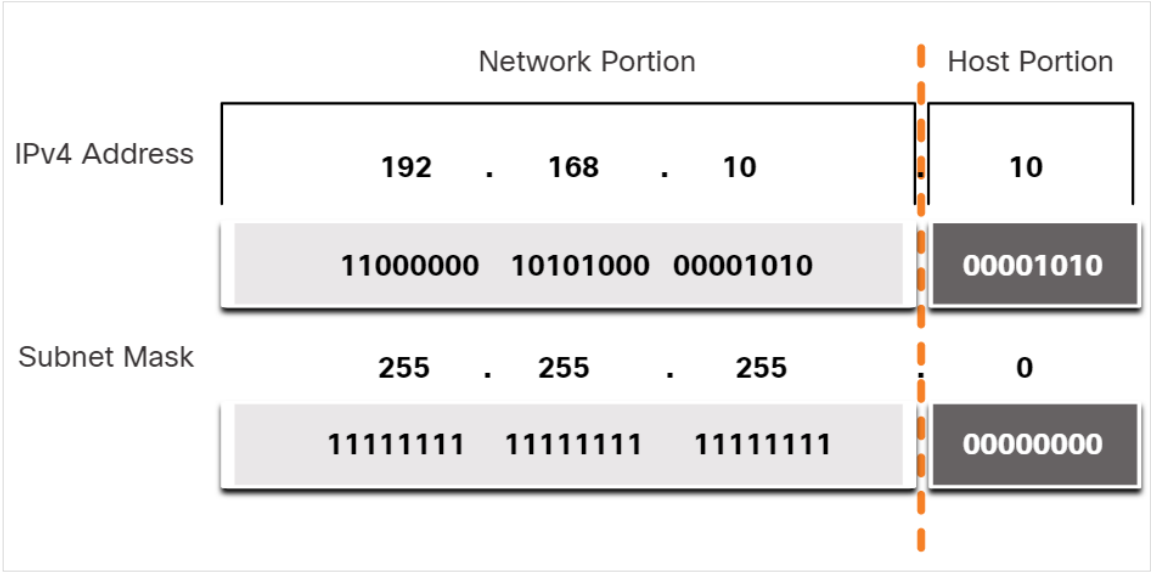
Subnet Mask

- 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 Subnet Mask (Contd.)

- 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 as shown in the figure.
- The subnet mask does not actually contain the network or host portion of an IPv4 address.
- The actual process used to identify the network portion and host portion is called ANDing.



Associating an IPv4 Address with its Subnet Mask

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 noted by a forward slash (/) followed by the number of bits set to 1.
- When representing an IPv4 address using a prefix length, the IPv4 address is written followed by the prefix length with no spaces.

Note: A network address is also referred to as a prefix or network prefix. Therefore, the prefix length is the number of 1 bits 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.

The Prefix Length (Contd.)

The first column lists the 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.

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

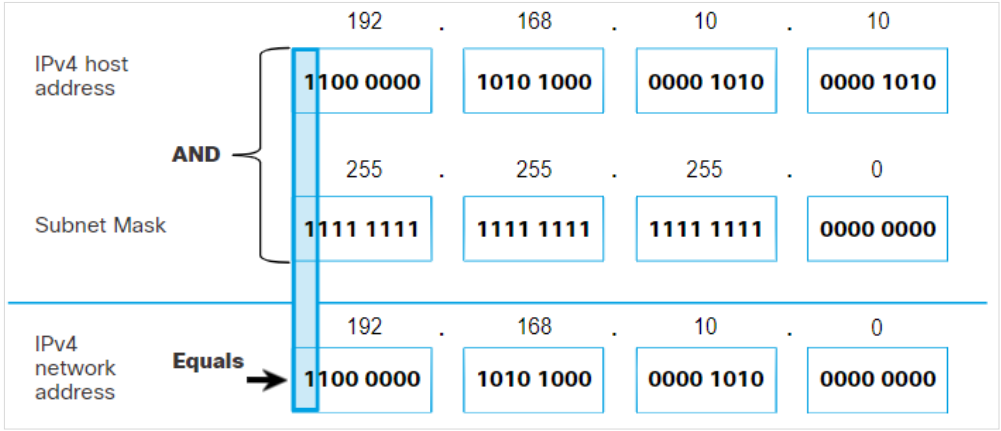
- A logical AND is one of three Boolean operations used in Boolean or digital logic.
- The AND operation is used in determining the network address.
- Logical AND is the comparison of two bits that produce the results as shown below
  - 1 AND 1 = 1
  - 0 AND 1 = 0
  - 1 AND 0 = 0
  - 0 AND 0 = 0
- To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask.

Note: *In digital logic, 1 represents True and 0 represents False. When using an AND operation, both input values must be True (1) for the result to be True (1).*

Determining the Network: Logical AND (Contd.)

- To illustrate how AND is used to discover a network address, 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.



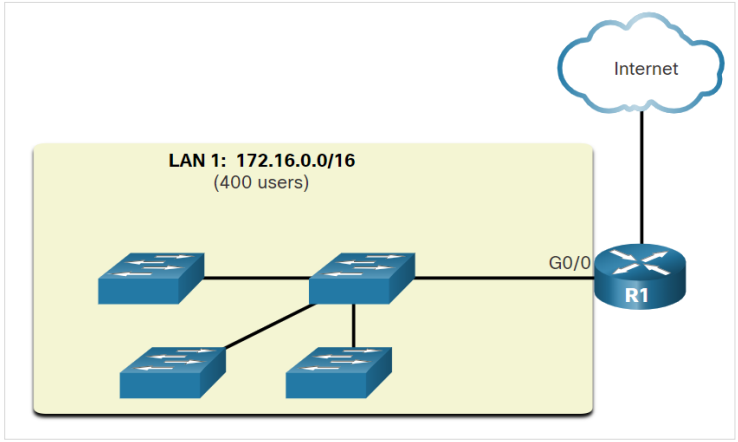
Video – Network, Host, and Broadcast Addresses

Watch the video to learn about Network, Host and Broadcast addresses.

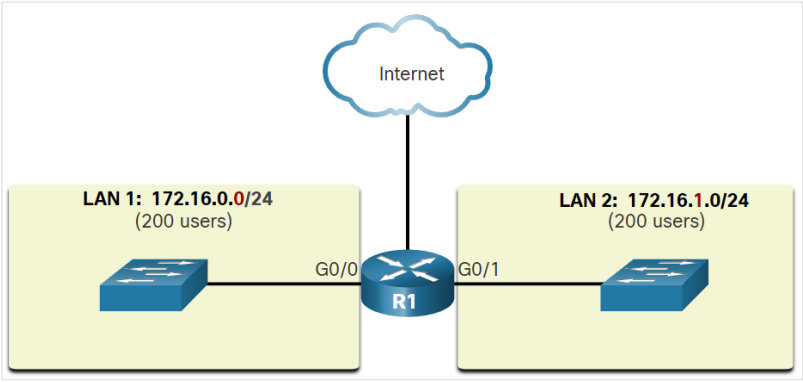
Subnetting Broadcast Domains

- 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.

Note: *The terms subnet and network are often used interchangeably. Most networks are a subnet of some larger address block.*



A Large Broadcast Domain

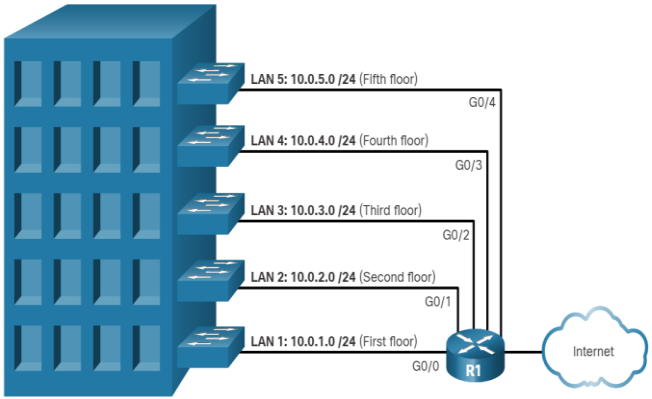


Communication between Networks

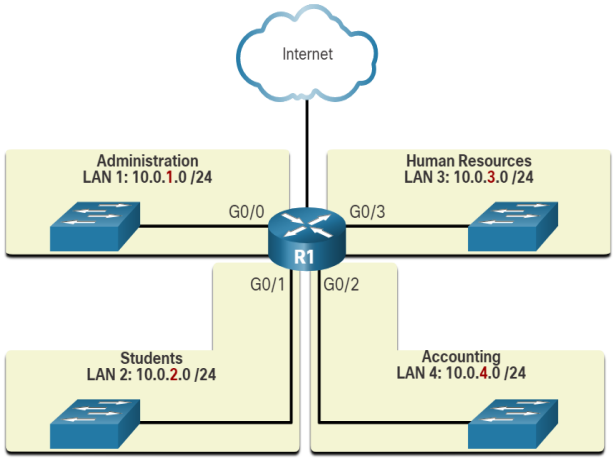
Subnetting Broadcast Domains (Contd.)

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

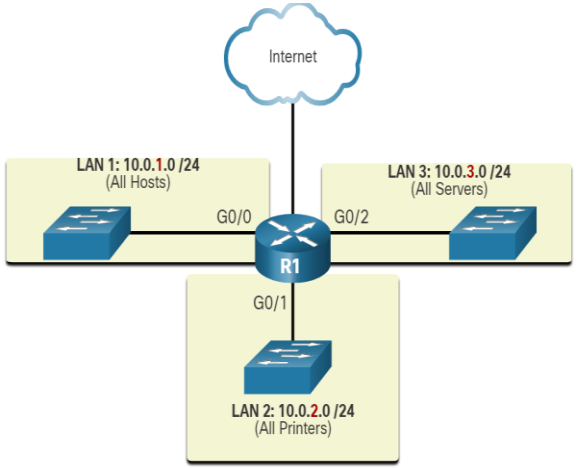
Location



By Department



Device Type



6.4 Types of IPv4 Addresses

IPv4 Address Classes and Default Subnet Masks

Address Classes

The IPv4 addresses were based on the following classes:

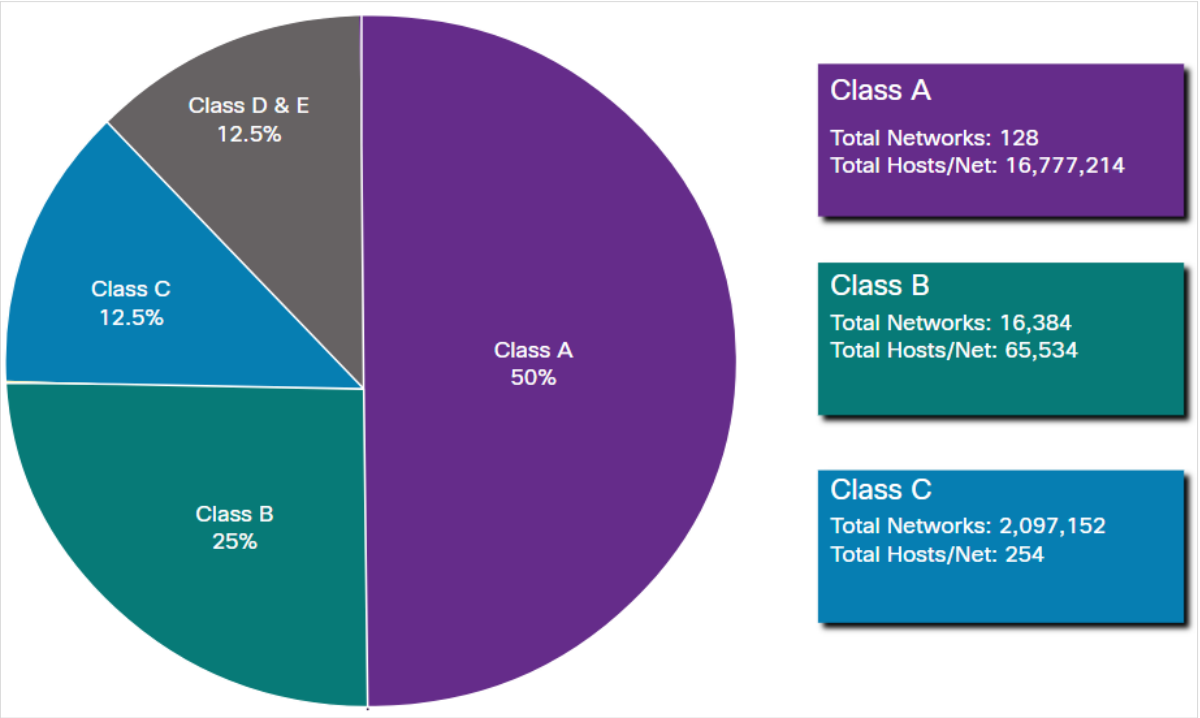
- **Class A** (0.0.0.0/8 to 127.0.0.0/8) – Designed to support extremely large networks with more than 16 million host addresses.
- **Class B** (128.0.0.0 /16 – 191.255.0.0 /16) – Designed to support moderate to large size networks with up to approximately 65,000 host addresses.
- **Class C** (192.0.0.0 /24 – 223.255.255.0 /24) – Designed to support small networks with a maximum of 254 hosts.

Note: *There is also a Class D multicast block consisting of 224.0.0.0 to 239.0.0.0 and a Class E experimental address block consisting of 240.0.0.0 – 255.0.0.0.*

IPv4 Address Classes and Default Subnet Masks (Contd.)

The classful system allocated :

- 50% of the available IPv4 addresses to 128 Class A networks
- 25% of the addresses to Class B
- Class C shared the remaining 25% with Class D and E.



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.

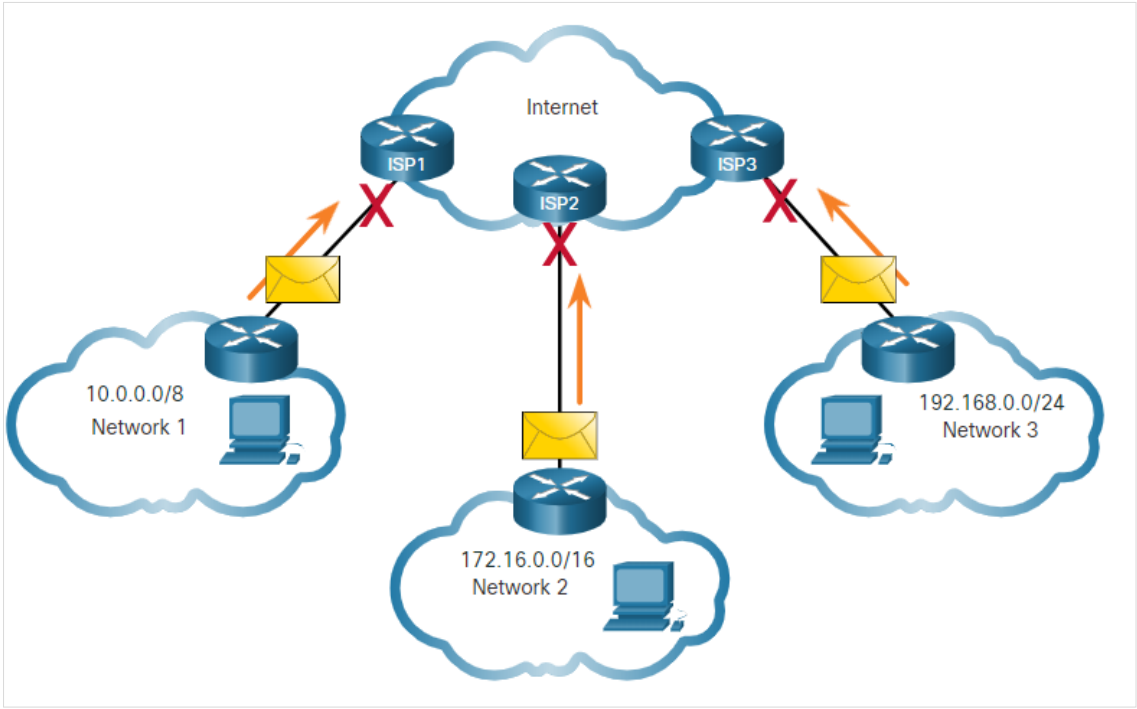
Private address blocks:

  - 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.
- Network Address Translation (NAT) is used to translate between private IPv4 and public IPv4 addresses.

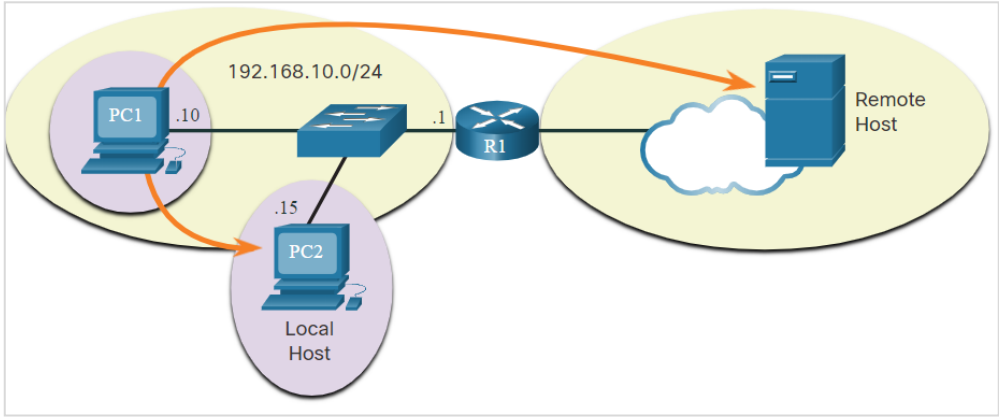


Private Addresses Cannot be Routed over the Internet

6.5 The Default Gateway

Host Forwarding Decision

- Another role of the network layer is to direct packets between hosts. A host can send a packet to: **Itself, Local host**, and **Remote host**.
- The figure illustrates PC1 connecting to a local host on the same network, and to a remote host located on another network.
- Whether a packet is destined for a local host or a remote host is determined by the source end device. The method of determination varies by IP version:
  - **In IPv4** - The source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to make this determination.
  - **In IPv6** - The local router advertises the local network address to all devices on the network.

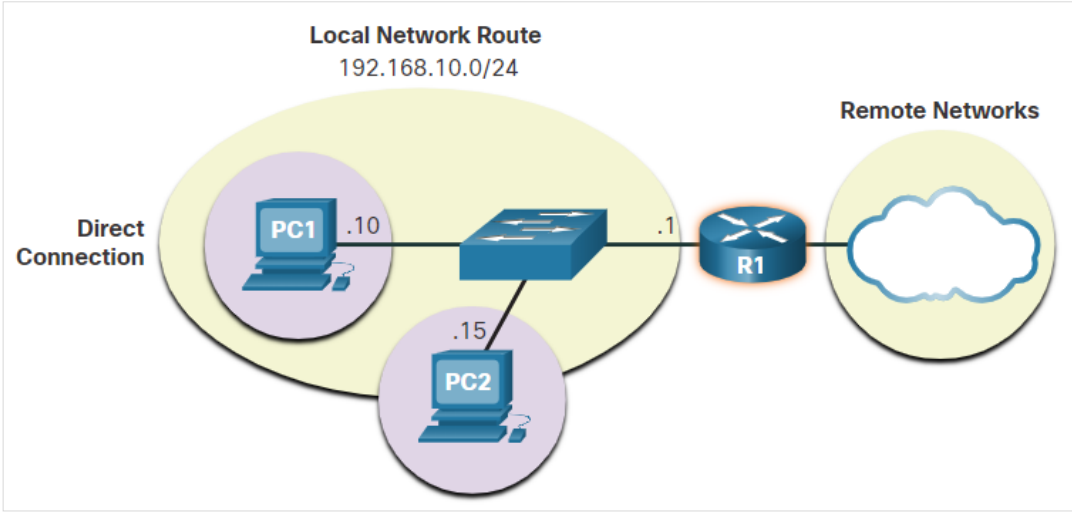


Default Gateway

- 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.

A Host Routes to the Default Gateway

- In IPv4, the host receives the IPv4 address of the default gateway either dynamically from Dynamic Host Configuration Protocol (DHCP) or configured manually.
- In IPv6, the router advertises the default gateway address or the host can be configured manually.
- Having a default gateway configured creates a default route in the routing table of the PC.
- A default route is the route or pathway your computer will take when it tries to contact a remote network.



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

Host Routing Tables

- On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table. Both commands generate the same output.
- The figure displays a sample topology and the output generated by the **netstat –r** command.

Host Routing Tables (Contd.)

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

Note: *The output only displays the IPv4 route table.*

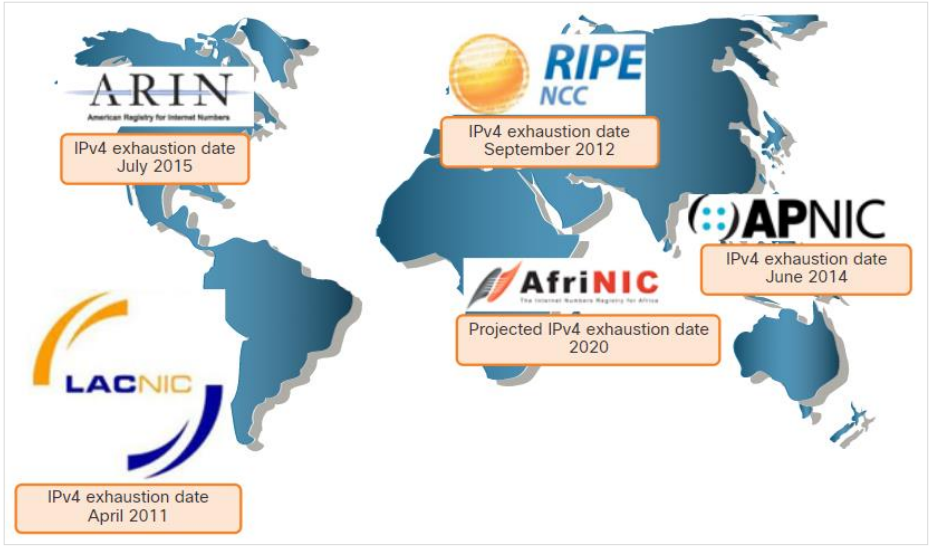
```
C:\Users\PC1> netstat -r

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

6.6 IPv6

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

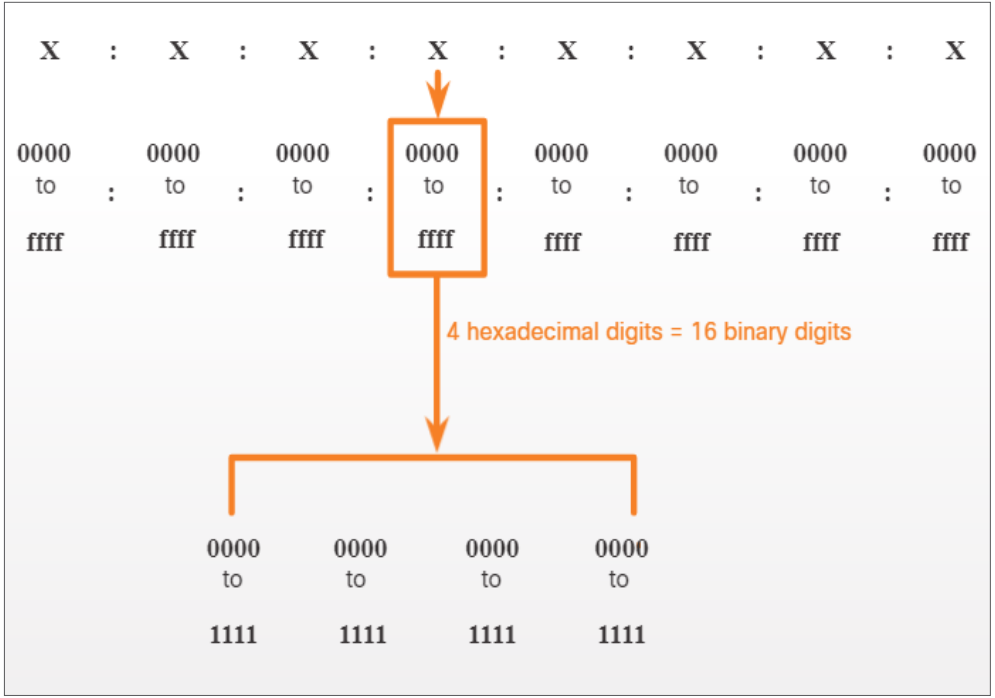
Need for IPv6 (Contd.)

Internet of Things

- The internet of today is more than email, web pages, and file transfers between computers.
- The evolving internet is becoming an Internet of Things (IoT).
- Computers, tablets, and smartphones will not be the only devices accessing the internet but there will also be sensor-equipped, internet-ready devices of tomorrow including everything from automobiles and biomedical devices, to household appliances and natural ecosystems.
- With an increasing internet population, a limited IPv4 address space, issues with NAT and the IoT, the time has come to begin the transition to IPv6.

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 and can be written in either lowercase or uppercase.



16-bit Segments or Hextets

IPv6 Addressing Formats (Contd.)

Preferred Format

- 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.
- Each “x” is a single hextet which is 16 bits or four hexadecimal digits.

Examples of IPv6 addresses in the preferred format

```
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
```

Rule 1 - Omit Leading Zeros

- **Rule 1:** Omit any leading 0s (zeros) in any hextet.
- The four examples of ways to omit leading zeros:
  - 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. 01ab. For example, refer to the below table.

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200
No leading 0s	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

Rule 2 - Double Colon

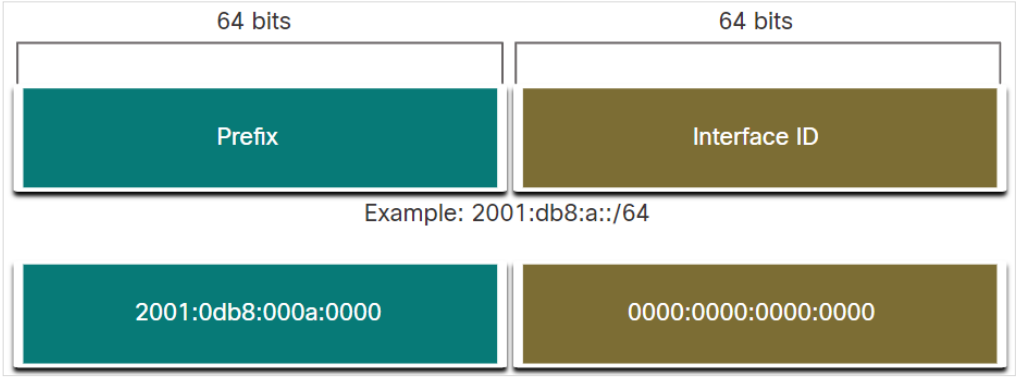
Rule 2: Double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.

- **Example:** 2001:db8:cafe:1:0:0:0:1 could be represented as 2001:db8:cafe:1::1.
- The double colon (::) is used in place of the three all-0 hextets (0:0:0).
- The double colon (::) can only be used once within an 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.
- **Example of incorrect use of the double colon:** 2001:db8::abcd::1234.

Type	Format
Preferred	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressed/spaces	2001 : db8 : 0 : 1111 : : 200
Compressed	2001:db8:0:1111::200

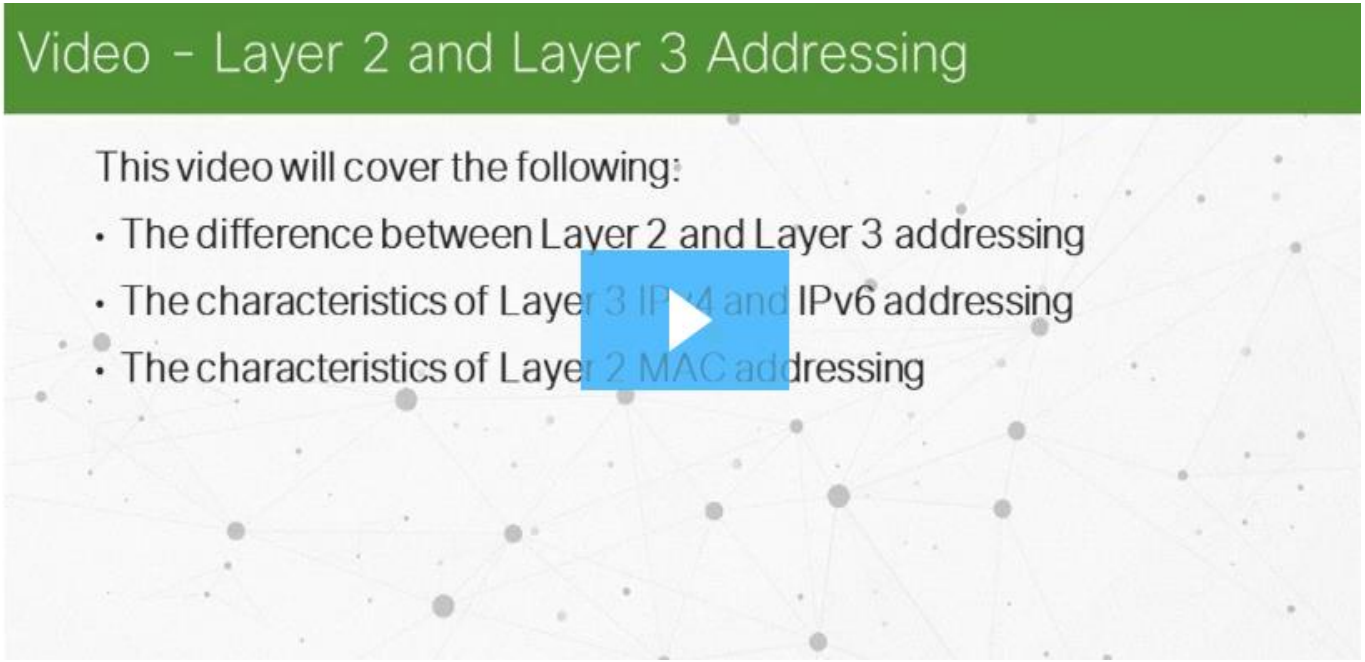
IPv6 Prefix Length

- 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.



Video – Layer 2 and Layer 3 Addressing

Watch the video to learn about Layer 2 and Layer 3 Addressing



6.7 Ethernet and IP Protocol Summary

What Did I Learn in this Module?

- Ethernet and wireless LANs (WLANs) are the two most popular LAN technologies. It operates at the physical and data link layers of the OSI model and are defined in the IEEE 802.2 and 802.3 standards.
- The MAC address can be represented using dashes, colons, or periods between the groups of digits.
- IP version 4 (IPv4) and IP version 6 (IPv6) are the principle network layer communication protocols.
- Network layer protocols perform four basic operations such as addressing end devices, encapsulation, routing, and de-encapsulation
- An IPv4 address is a 32-bit hierarchical address that identifies a network and a host on the network. An IPv6 address is a 128-bit hierarchical address.
- The prefix length is the number of bits that are set to 1 in the subnet mask. It is written in “slash notation”, which is noted by a forward slash (/) followed by the number of bits that are set to 1.

What Did I Learn in this Module?

- The process that is used to identify the network portion and host portion is called ANDing.
- Class A, Class B, and Class C are the different ranges of IP addresses.
- The router that is connected to the local network segment is referred to as the default gateway.
- On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table.
- There are two rules that help to reduce the number of digits that are needed to represent an IPv6 address.
- The prefix length can range from 0 to 128.


CISCO