# Data Communication Network
# DAY – 1

**Mrs.Akshita.S.Chanchlani**

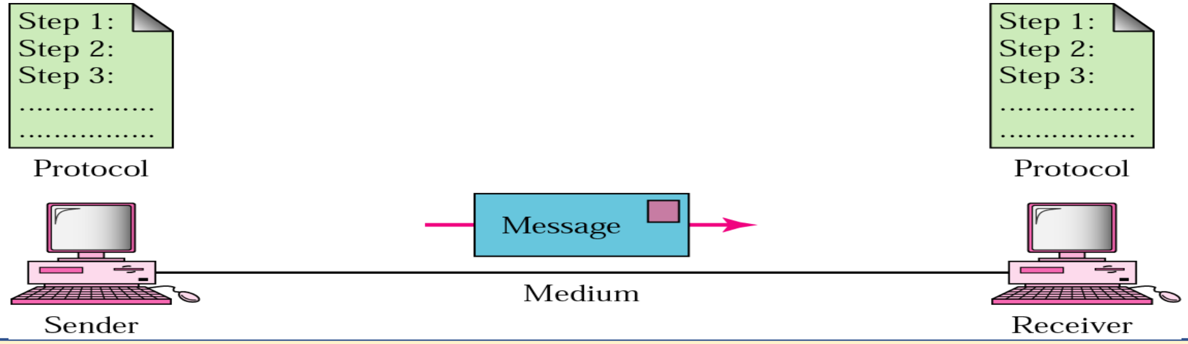
**akshita.chanchlani@sunbeaminfo.com**

# Network Terminologies

•connecting multiple devices (computers) together to share the information group of devices/machines/IP addresses/hosts.

- **Data**
- **Communication**
- **Network**
- **Computer Network**

**Components of Data communication**



## *Node*

- any device connected to the network(a computer, a printer etc)

## *Network Interface Card (NIC)*

- is the circuit board that is used to connect computers to the network.
- In most cases, this is an *Ethernet* card plugged in a computer’s motherboard

**The effectiveness of a data communications system depends on four fundamental characteristics**:
Delivery, Accuracy , Timeliness , Jitter

# Need of Network/ Applications of Network

- **Information Sharing**
- **Enhance communication**
- **Share resources**
- **Facilitate centralized management**
- **Remote computing**

# Network Types

## Wired

### Medium

- Wire / Cable

### Cable Types

- co-axial
  - transfers the data in the form of electrical signals
- CAT Cable / Twisted Pair Cable (STP/UTP)
  - transfers the data in the form of electrical signals
- Fiber Optics
  - transfers the data in the form of light
  - Minimum 10gbps

### Types

- LAN , MAN , WAN

cat1 : - [it was used only for telephony network]

cat2 : 1 mbps

cat3 : 10 mbps

cat4 : 16 mbps

cat5 : 100 mbps

cat5e: 125 mbps

cat6 : 1000 mbps ~ 1 gbps

cat7 : 10000 mbps ~ 10 gbps

cat8 : 25000 mbps ~ 25 gbps

## Wireless

### Medium

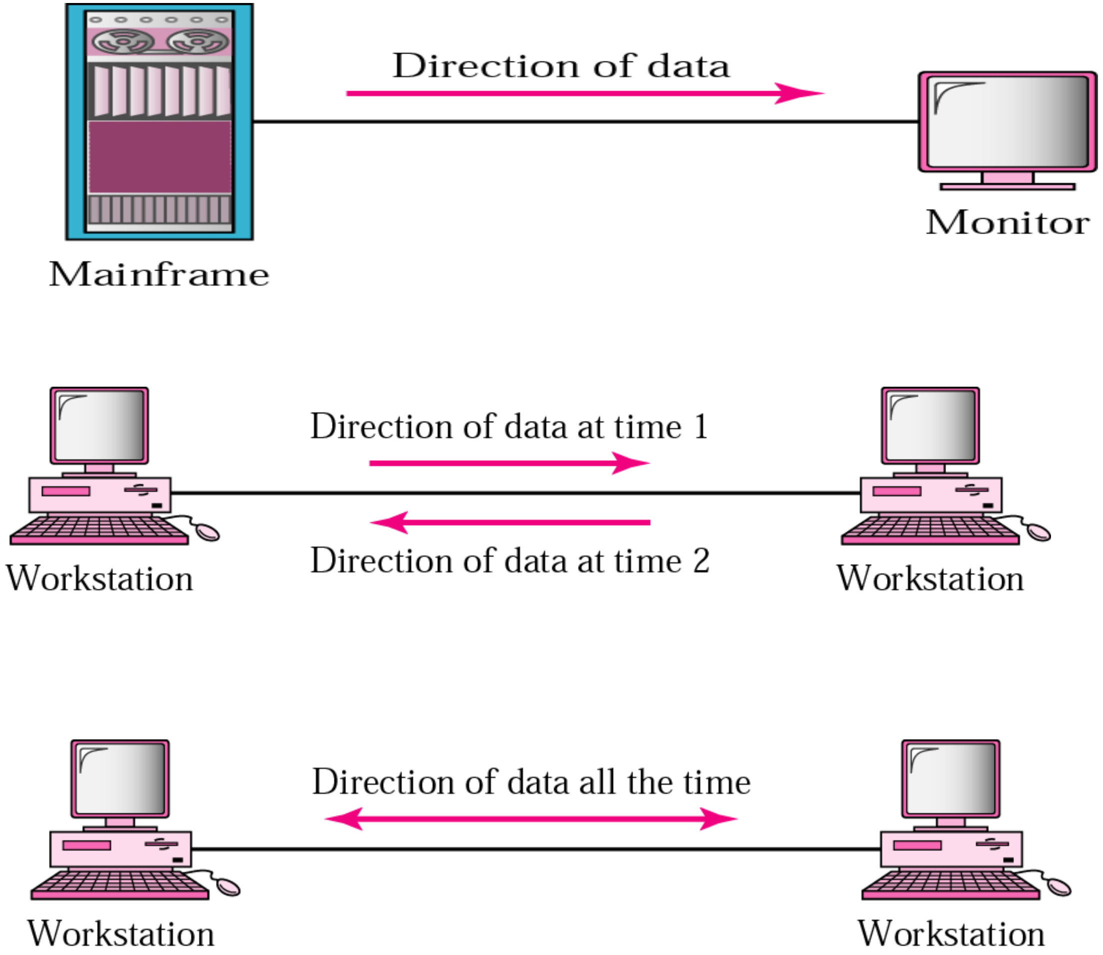
- Air (EM Waves)

### Cable Types

- PAN
- WLAN
- WAN (GSM)

# Media (Transmission Medium)

# Transmission Modes / Data Flow Direction


Direction of data
Mainframe
Monitor
Direction of data at time 1
Direction of data at time 2
Workstation
Workstation
Direction of data all the time
Workstation
Workstation

### Simplex Mode

- Example: Keyboard and traditional monitors.

### Half-Duplex Mode

- each station can both transmit and receive, but not at the same time.
- Example: Walkie- talkie

### Full-Duplex Mode

- Example: Telephone Network there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

# Transmission Medium

- For any networking to be effective, raw stream of data is to be transmitted from one device to other over some medium.
- Various transmission media can be used for transfer of data.

**Types of Transmission Medium**

## Guided

- Transmitted data travels through cabling system that has a fixed path.
- For example, copper wires, fibre optic wires, etc.

## Unguided

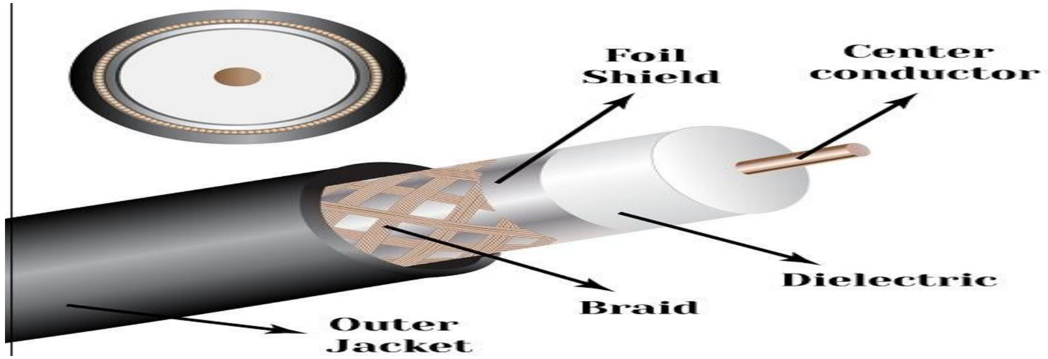
- Transmitted data travels through free space in form of electromagnetic signal.
- For example, radio waves, lasers, etc

# Twisted Pair  (maximum length of 100 meters)

- Most common wires used for transmitting signals
- To reduce this electromagnetic interference, pair of copper wires are twisted together.
- Shielding twisted pair cable
  - To counter the tendency of twisted pair cables to pick up noise signals, wires are shielded .
  - Such twisted pairs are called **shielded twisted pair (STP) cables**.
- The wires that are not shielded but simply bundled together in a protective sheath are called **unshielded twisted pair (UTP) cables**.

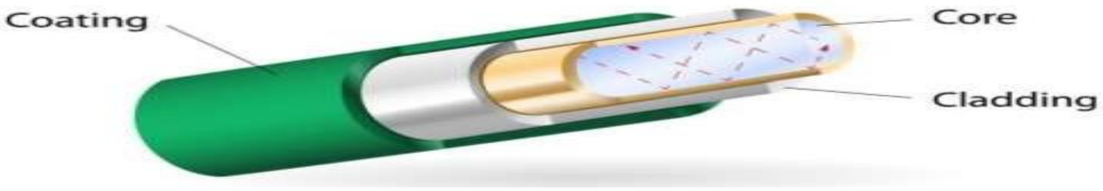
# Coaxial Cable

- Coaxial cables are widely used for **cable TV** connections and **LANs**.
- **Coaxial cables** are copper cables with better **shielding** than twisted pair cables.
- Transmitted signals may travel **longer distances** at higher speeds.
  - e.g. 1 to 2 Gbps for 1 Km cable
- Can be used for both analog and digital signals
- Inexpensive as compared to fiber optic cables
- Easy to install and maintain



# Optical Fiber

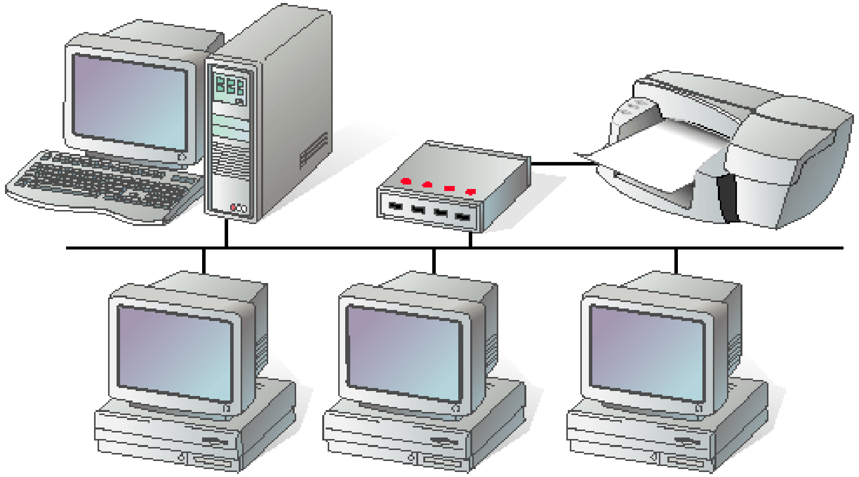
- Thin glass or plastic threads used to transmit data **using light waves** are called **optical fiber**.
- Signals carrying data can travel long distances without weakening
- Immune to electromagnetic interference , Suitable for industrial and noisy areas
- Three Layers:
  - **Core** made of high quality **silica glass** or **plastic**
  - **Cladding** made of high quality **silica glass** or **plastic**, with a lower refractive index than the core
  - Protective outer covering called **buffer**



# Network Classification

# LAN (Local Area Network) : Wired Network

- Network in small geographical Area (Room, Building or a Campus)
- **Short distances (100 meters)**
- **Designed to provide local interconnectivity**
- LAN’s can either be made wired or wireless. Twisted pair, coax or fiber optic cable can be used in wired LAN’s
- a network that is used for communicating among computer devices, usually within an office building or home.



# Basic systems people use to set up wired networks

## An **Ethernet** system

- uses either a twisted copper-pair or coaxial-based transport system.
- The most commonly used cable for Ethernet is a **category 5 unshielded twisted pair (UTP)** cable

## A **phone line**

- simply uses existing phone wiring found in most homes

## **Broadband** systems

- provide cable Internet and use the same type of coaxial cable that gives us cable television

# Wired Network Designing

## Token Ring (Not used)

- Its copy write by IBM.
- It is a data link technology for local area networks (LANs) in which devices are connected in a star or ring topology.
- It was designed by only IBM PCs with 4mbps they increased upto 16mbps.

## Ethernet (Used World wide /Now a days)

- It belongs to IEEE
- Its autonomous
  - 10mbps (Ethernet),
  - 100mbps (fast Ethernet)
  - 1Gbps (Gigabit Ethernet)
  - 10gbps (10 gig Ethernet)
  - 100gbps (100 gig Ethernet)
  - LRE (Long Range Ethernet)

# Token Ring

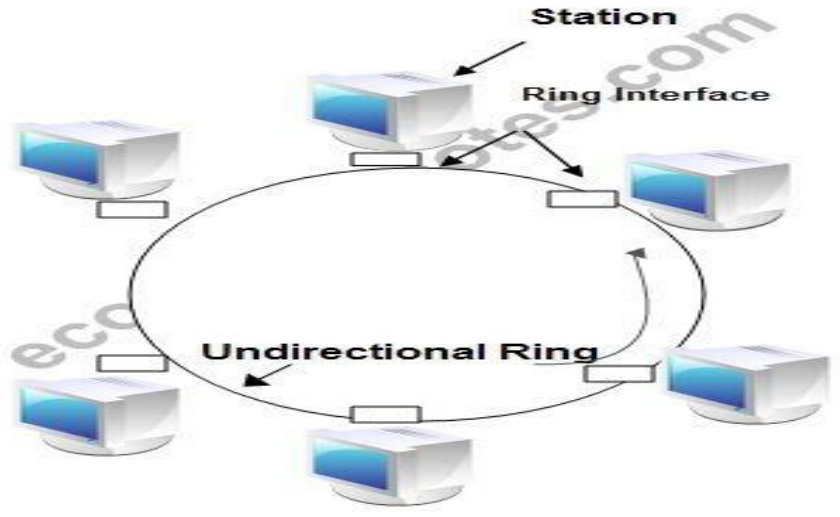
- The token ring LAN process is delineated by the following sequence of events:
  - A token continually circulates inside the toke ring LAN
  - To transmit a message, a node inserts a message and destination address inside an empty token.
  - The token is examined by each successive node.
    The destination node copies the message data and returns the token to the source with the source address and a data receipt message.
  - The source receives the returned token, verifies copied and received data and empties the token.
  - The empty token now changes to circulation mode, and the process continues.

Listen Mode

- The input bits are simply copied to output with a delay of 1-bit time.

Transmit Mode

- The connection between input and output is broken by the interface so that is can insert its own data



A Ring Network

# **Ethernet** Transfer speed 10 Mbps, 100 Mbps, or above

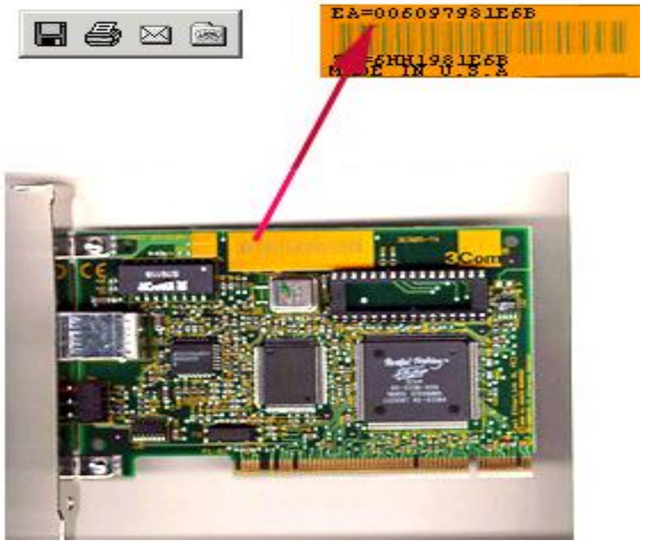
- Ethernet is the dominant cabling and low level data delivery technology used in Local Area Networks (LAN’s).
- It was developed by Xerox corp. along with DEC and Intel.
- **Features:**
  1. Ethernet Addresses are 6 bytes( 48 bits) long.
  2. Ethernet supports networks built with twisted pair, thin and thick coaxial and fiber optic cabling.
  3. To prevent the loss of data, when two or more devices attempt to send packets at the same time, Ethernet detects collisions.

# Ethernet Address/ MAC Address

***Example: 47:20:1B:2E:08:EE***

- First three bytes from <u>left</u> specify the vendor.
- the last 24 bit should be created uniquely by the company

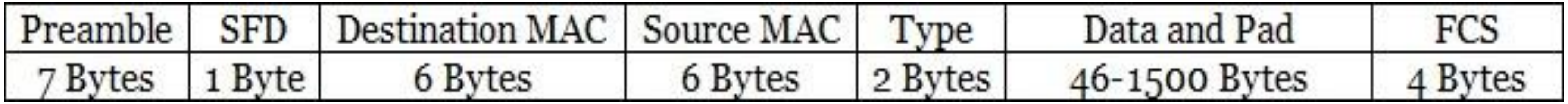
| | |
|---|---|
| Cisco | 00-00-0C |
| Dell | 20-47-47 |
| Sun | 08-00-20 |
| IBM | 08-00-5A |
| Nokia | 00-40-43 |



**Ipconfig/all : Ethernet adapter Ethernet(Physical Address)**

**A network interface card (NIC) / Ethernet Card is a piece of computer hardware designed to allow computers to communicate over a computer network.**

# Ethernet Frame Format/MAC Frame

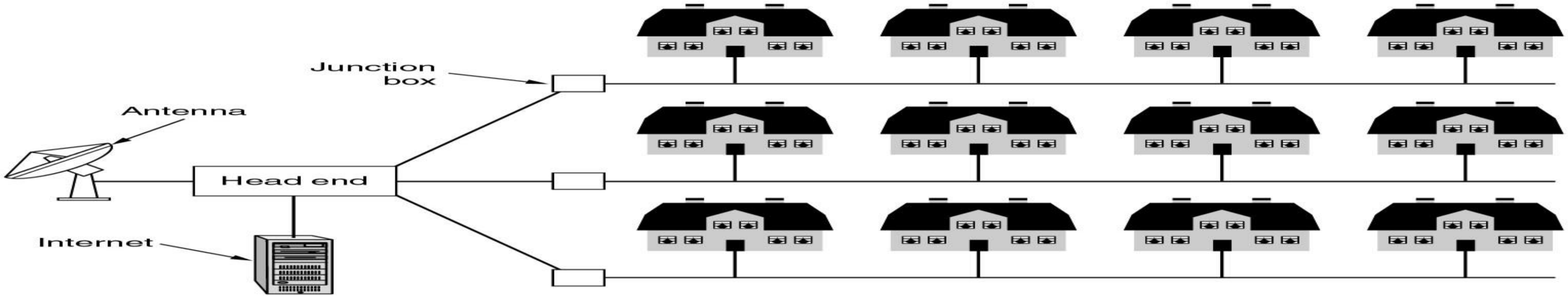


| Preamble | SFD | Destination MAC | Source MAC | Type | Data and Pad | FCS |
|---|---|---|---|---|---|---|
| 7 Bytes | 1 Byte | 6 Bytes | 6 Bytes | 2 Bytes | 46-1500 Bytes | 4 Bytes |

| | |
|---|---|
| **Preamble** | • informs the receiving system that a frame is starting and enables synchronization. In IEEE 802.3, eighth byte is start of frame (10101011) |
| **SFD (Start Frame Delimiter)** | • signifies that the Destination MAC Address field begins with the next byte. |
| **Destination MAC** | • identifies the receiving system. |
| **Source MAC** | • identifies the sending system. |
| **Type** | • defines the type of protocol inside the frame, for example IPv4 or IPv6. |
| **Data and Pad** | • contains the payload data.<br>• Padding data is added to meet the minimum length requirement for this field (46 bytes). |
| **FCS (Frame Check Sequence)** | • contains a 32-bit Cyclic Redundancy Check (CRC) which allows detection of corrupted data. |

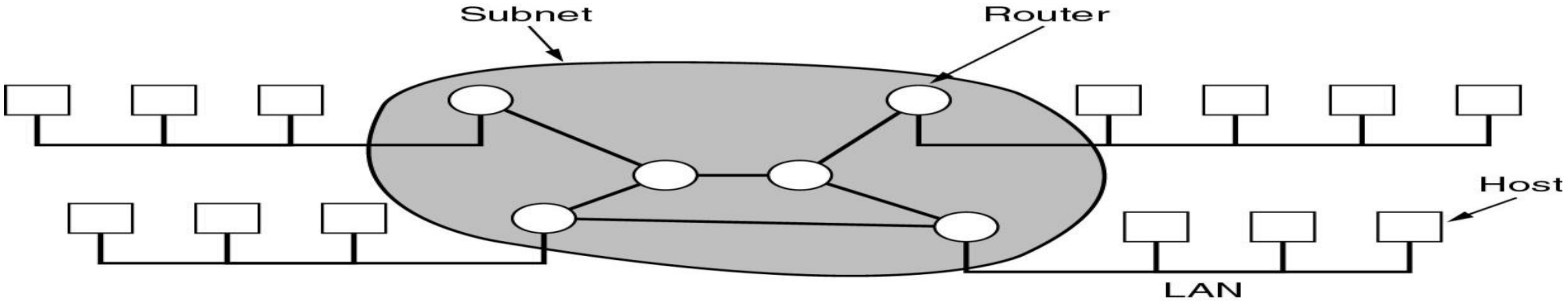
# MAN

- A MAN spans the distance of a typical metropolitan city.
- The cost of installation and operation is higher.
- MANs use high-speed connections such as fiber optics to achieve higher speeds.
- Provide connectivity over areas such as a city, a campus
- More than 100m , Designed to handle data communication for multiple organizations in a city and nearby cities as well
- e.g. cable television network



# WAN

- Network spread geographically (Country or across Globe)
- WANs consist of two distinct components:
  - transmission lines (copper, fiber, microwave) and switches (electronics, optics)
  - Store-and-forward or packet-switched subnet
- WANs span a larger area than a single city.
- These use long distance telecommunication networks for connection, thereby increasing the cost.
- The Internet is a good example of a WAN.
- More than 1000m long distance, Provide connectivity over large areas



# Address Resolution Protocol (ARP)

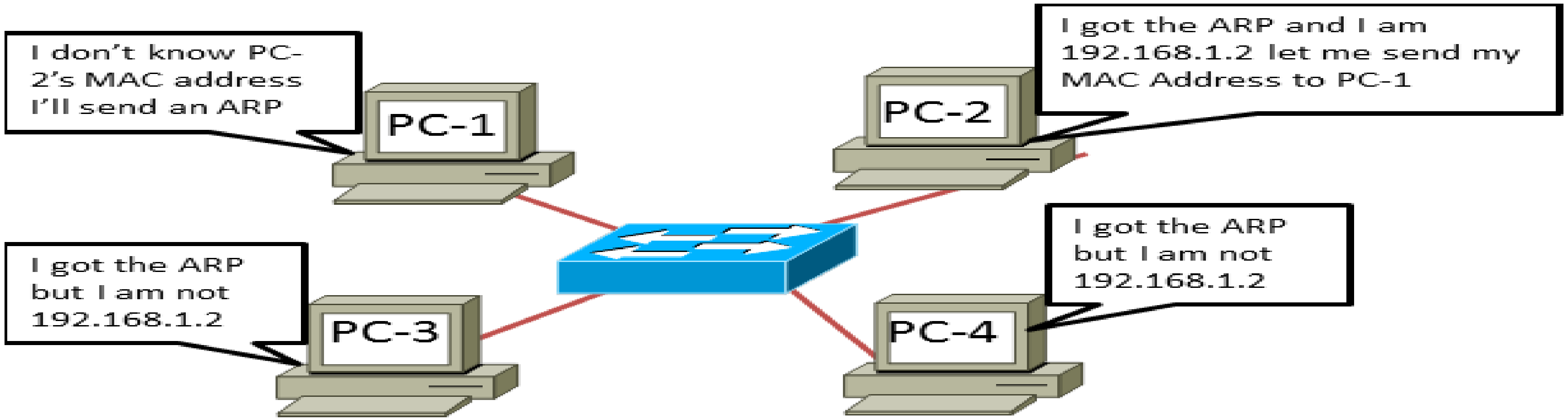
# ARP

- Address resolution refers to the process of finding an address of a computer in a network.
- The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer.
- The address resolution procedure is completed when the client receives a response from the server containing the required address.
- The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa

# ARP

- Step1 : ARP Broadcast
  - Note: Broadcast is received by everyone and processed by everyone.
- Step 2: ARP Reply
- Step 3 : Actual Data Transfer

- Router creates an ARP Request message to be sent to all hosts on the subnet.
- Address resolution protocol message asks “Who has specified IP address ?”
- Passes ARP request to data link layer process for delivery


I don’t know PC-2’s MAC address I’ll send an ARP
PC-1
I got the ARP and I am 192.168.1.2 let me send my MAC Address to PC-1
PC-2
I got the ARP but I am not 192.168.1.2
PC-3
I got the ARP but I am not 192.168.1.2
PC-4

# Network Physical Structure

# Physical Structure

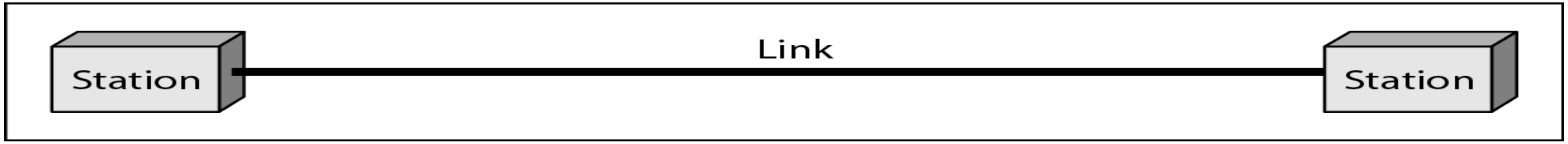
## Type of Connection

- Point to Point - single transmitter and receiver
- Multipoint - multiple recipients of single transmission

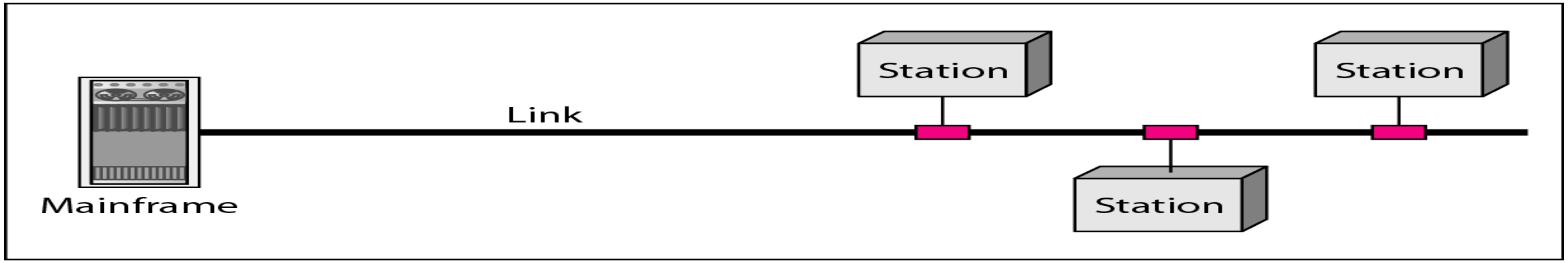
## Physical Topology

- Connection of devices
- Refers to the way in which a network is laid out physically
- The geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- **Type of transmission** - unicast, mulitcast, broadcast

# Types of Connection



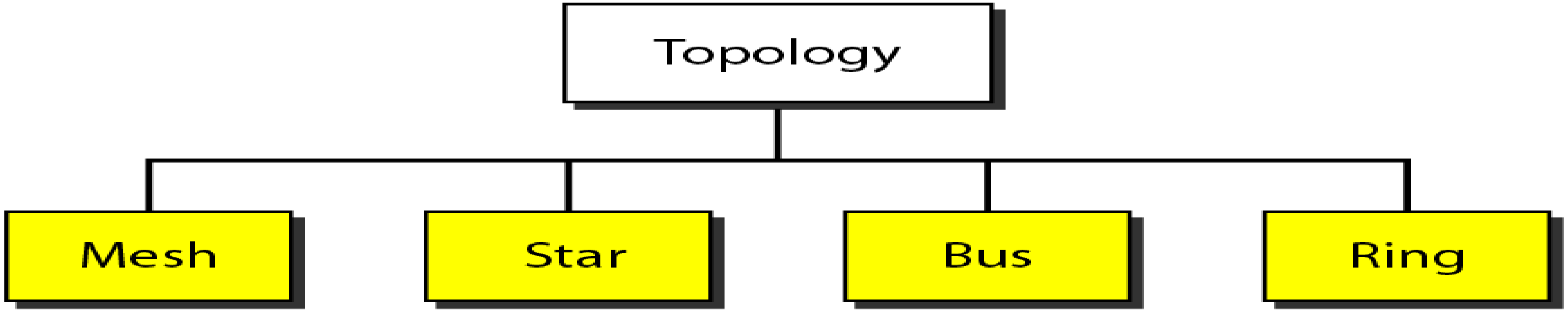
a. Point-to-point



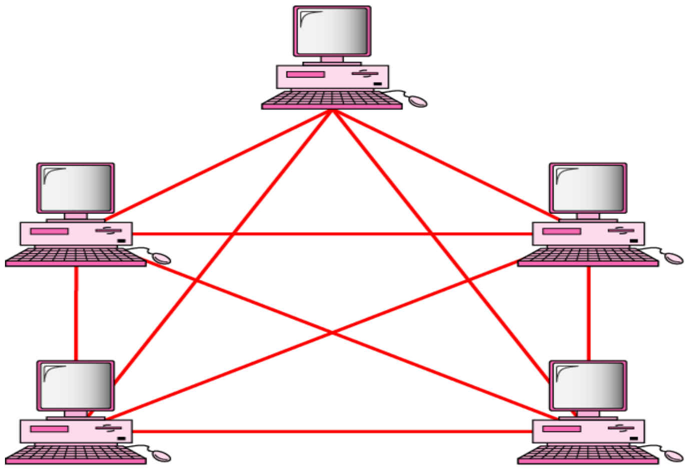
b. Multipoint

# Physical Topology

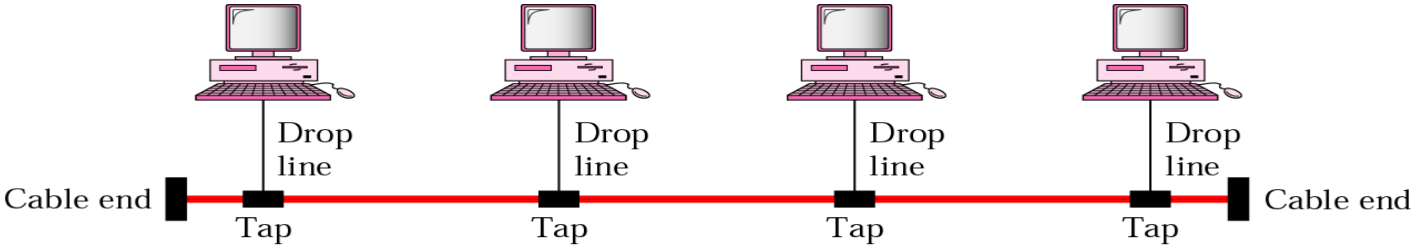
- Topology defines the way hosts are connected to the network
- The network topology defines the way in which computers, printers, and other devices are connected.
- A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



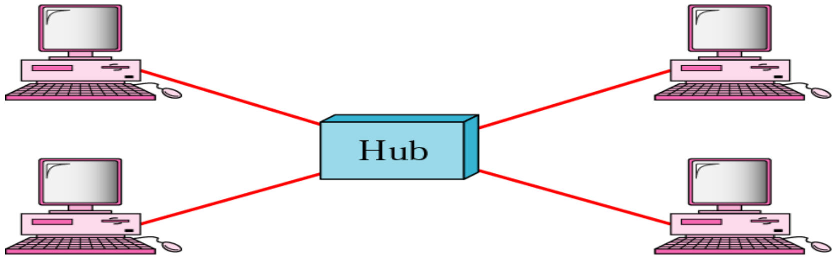
# Network Topology



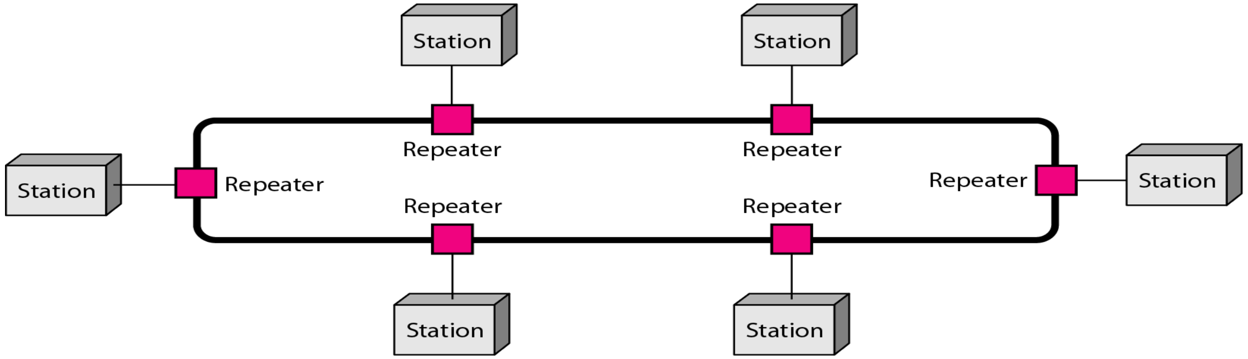
mesh



bus



star



ring

# Network Devices / Internetworking Devices

# Internetworking Devices

- Internetworking devices are products used to connect networks.
- As computer networks grow in size and complexity, so the internetworking devices used to connect them.
  - Hubs
  - Repeaters
  - Bridges
  - Switches
  - Routers
  - Gateways

# Hubs

- Hub is used to build a LAN.
- Common connection point for devices in a network.
- It is non intelligent device.
- It does not understand the addressing.
- Hub is Multiport repeater containing multiple ports to interconnect multiple devices
- Hubs regenerate and retime network signals (increases traffic and collision)
- They cannot filter network traffic and they cannot determine best path
- The hub contains multiple ports.
- When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
  - does not concern about the address
  - concerns with only electrical signals
  - increases the traffic, as they broadcast data to all
  - increases the collision

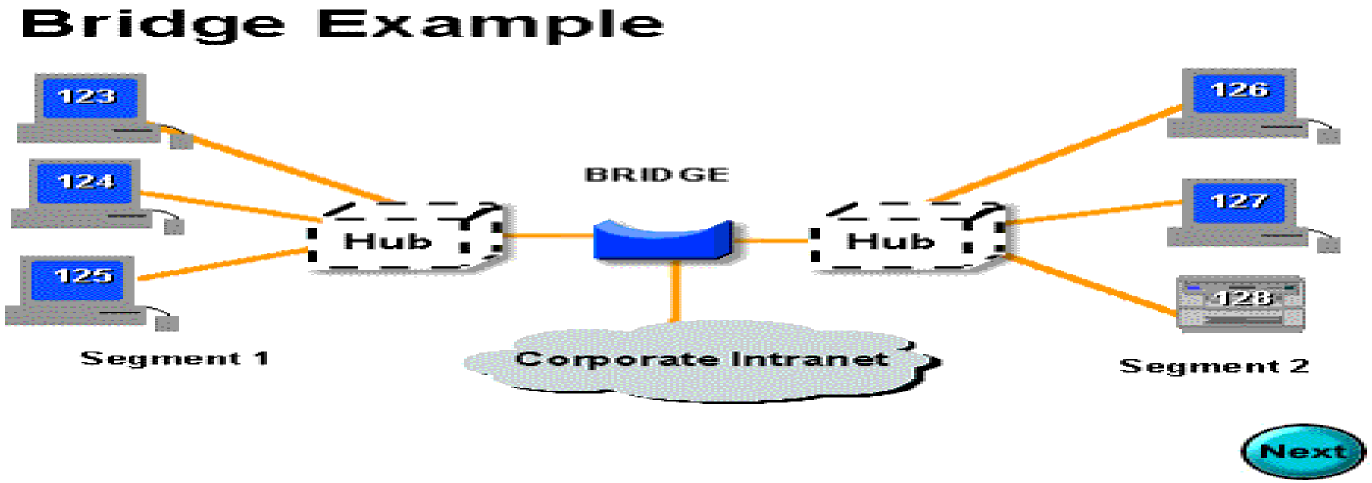
# Repeaters

- **Repeaters or hubs work at the OSI physical layer to regenerate the network's signal and resend them to other segments.**
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- The longer the cable length, the weaker and more deteriorated the signals become as they pass along the networking media.
- Repeaters can be installed along the way to ensure that data packets reach destination.

One way to solve the problems of too much traffic on a network and too many collisions is to use an internetworking device **called a bridge.**

# Bridges : Operates at Data Link Layer

- A bridge eliminates unnecessary traffic and minimizes the chances of collisions occurring on a network by dividing it into segments .
- Device that connects and passes packets between two network segments.
- More intelligent than hub- As they analyze incoming packets and forwards (or drops) based on addressing information.(Routing Table is Build to record segment number of address)
- Bridges work best where traffic from one segment of a network to other segments is not too great.



However, when traffic between network segments becomes too heavy, the bridge can become a bottleneck and actually slow down communication.

# Switches (Multiport Bridges)

- **Switches operate at the Data Link layer (layer 2) of the OSI model**
- A switch is a device that is used to segment networks into sub networks called subnets. (Used to build LAN)
- **Can interpret address information**
- Uses Addressing Scheme knows as MAC Addressing.
- Switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately
- Switch conserves network bandwidth and offers generally better performance than a hub.
- **Switch may Broadcase , unicast or Multicast .**

**Learning the MAC Addresses and forwarding to the respective machine is switching.**

- Switches have
  - ASIC (Application Specific IC)
  - OS is hardcoded in microprocessor
  - So switches are hardware based.
  - Ports are unlimited

- Bridges have
  - OS is separated
  - So bridges are not used
  - Bridges are software based.
  - Limited Ports (16)

# Routers

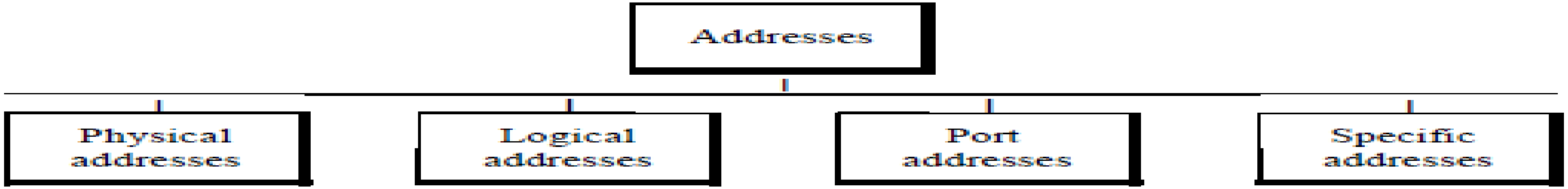
- Used to build WAN
- Router connect multiple networks and route the packets.
- Uses IP Address to identify every machine uniquely.
- Routers are used to connect two or more networks. For routing to be successful, each network must have a unique network number
- Routers have the ability to make intelligent decisions as to the best path for delivery of data on the network.
- **They use the "logical address" of packets and routing tables to determine the best path for data delivery.**
- To determine the **best path**, routers communicate with each other through **routing protocols**
- The four most common routing protocols:
  - RIP (Routing Information Protocol) for IP
  - OSPF (Open Shortest Path First) for IP
  - EIGRP (Enhanced Interior Gateway Routing Protocol) for IP, IPX, and AppleTalk
  - BGP (Border Gateway Protocol) for IP

# Gateways

- Device that connects dissimilar networks.
- Operates at the highest level of abstraction.
- Expands the functionality of routers by performing data translation and protocol conversion.
- Establishes an intelligent connection between a local network and external networks with completely different structures.
- Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.
- If a network wants to communicate with devices, nodes or networks outside of that boundary, they require the functionality of a gateway.
- A gateway is often characterized as being the combination of a router and a modem.

# Addressing

# Addressing



## Physical Address/ Link Address

- For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

## Logical Address

- logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.

## Port Address

- computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).

## Specific Addresses

- Examples include the e-mail address and any Universal Resource Locator (URL)

# MAC Address / Physical Address/ Ethernet Address

- used on data link layer
- used to identify every NIC uniquely
- is burnt into the ROM part of NIC once written the MAC address can not be changed
- also known as  read only address
- to find the MAC address of NIC
  - windows: ipconfig /all
  - linux/macOS: ifconfig
- e.g.   78 : 4f : 43 : 90 : 13 : d0
- size: 6 bytes = 8 x 6 = 48 bits
- Group of first three bytes(78 : 4f : 43)  represent's manufacturer ID and last 3  bytes (90 : 13 : d0 ) represents NIC's unique address.
- to find the manufacturer, please visit https://hwaddress.com/

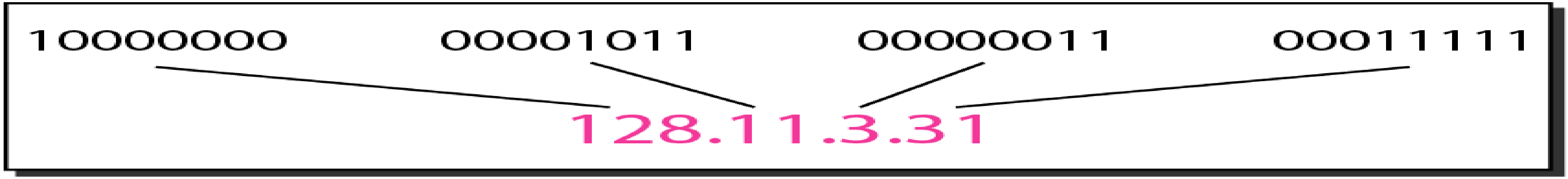
# IP Address / Logical Address

- IP address to mean a logical address in the network layer of the TCP/IP protocol suite.
- Identify a machine / device uniquely.
- Size = 4 bytes = 32 bits
- to find the IP address of Machine
  - windows: ipconfig
  - linux/macOS: ifconfig
- IP Versions:
  - IPV4 (32 bits address length)
  - IPV6 (128 bits address length)
- IP addresses are made up of four sets of numbers called **“Octets”.**
- Types
  - Private : used to identify a machine on the LAN and can not be used to connect to internet
  - Public : used to connect to the internet
- e.g.
  - decimal: 192.168.1.6
  - binary : 11000000.10101000.00000001.00000110

# IP Addressing Types

- Classful : IP Address is split into 5 classes
- Classless

- IPv4 uses 32-bit addresses, which means that the address space is $2^{32}$ or4,294,967,296 (more than 4 billion)
- **There are two prevalent notations to show an IPv4 address:**
  - binary notation
  - dotted decimal notation

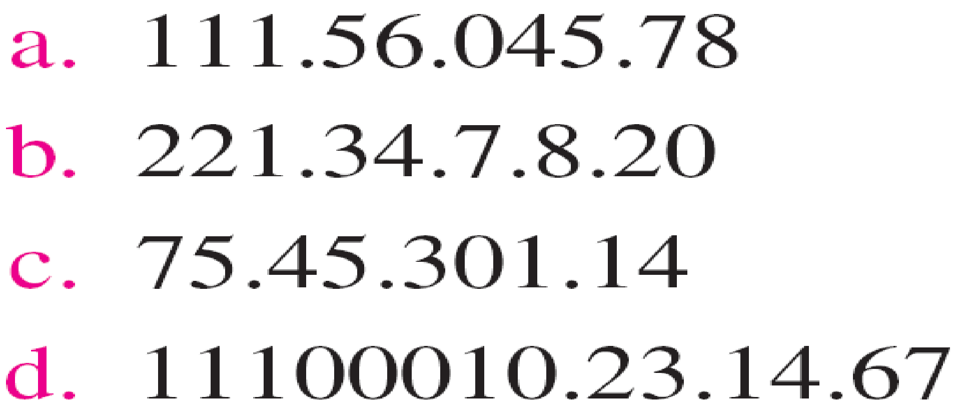


10000000 00001011 00000011 00011111

128.11.3.31

# Example

- *Find the error, if any, in the following IPv4 addresses.*



a. 111.56.045.78

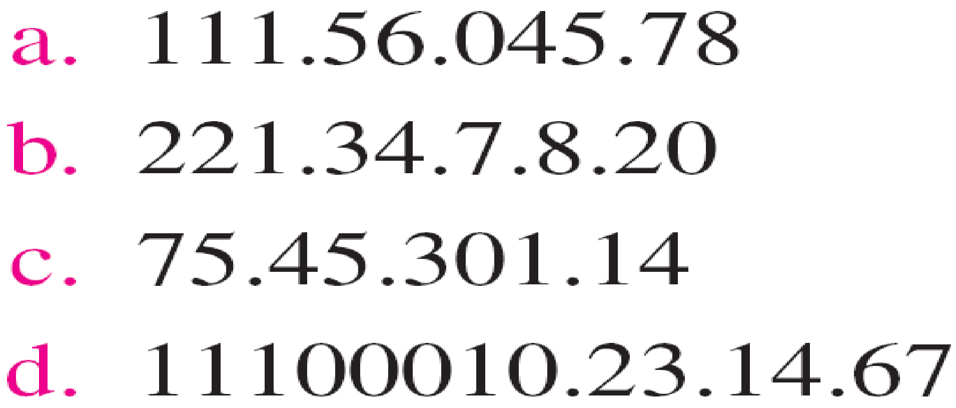
b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

# Example

- *Find the error, if any, in the following IPv4 addresses.*

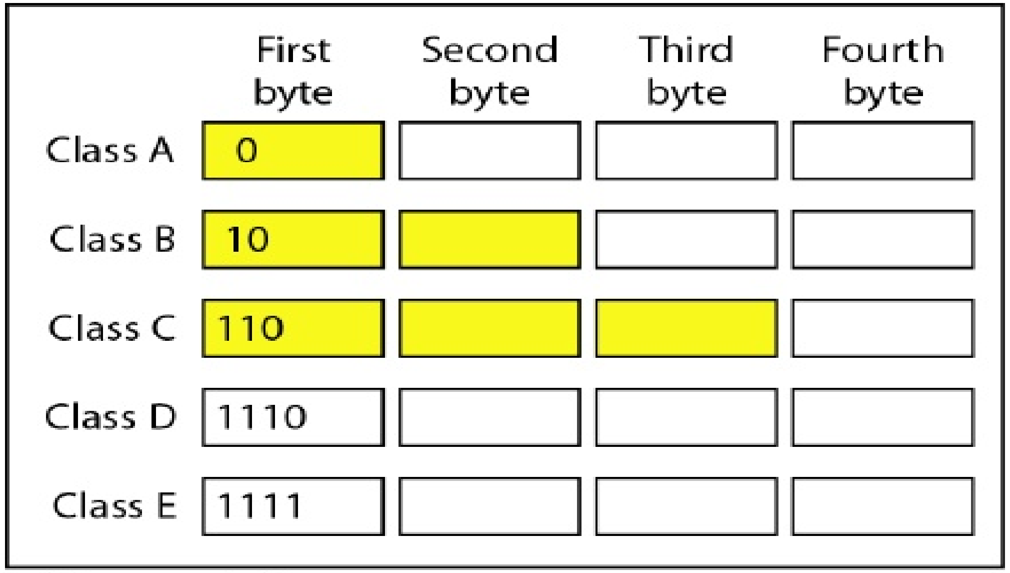


a. 111.56.045.78
b. 221.34.7.8.20
c. 75.45.301.14
d. 11100010.23.14.67

***Solution***
*a. There must be no leading zero (045).*
*b. There can be no more than four numbers.*
*c. Each number needs to be less than or equal to 255.*
*d. A mixture of binary notation and dotted-decimal notation is not allowed.*

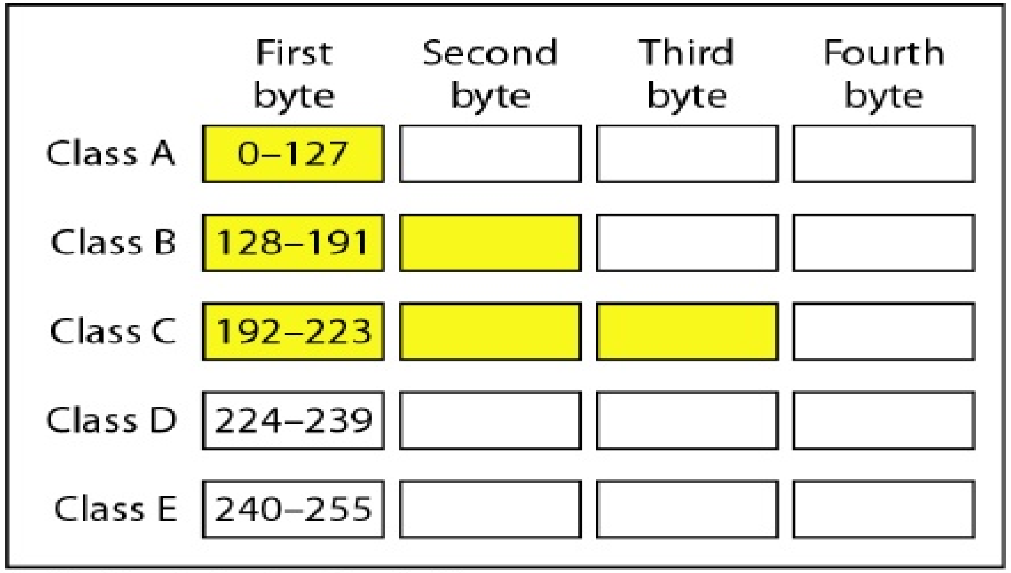
# Classful Addressing

- IP is 32 bit means $2^{32}$ IP Addresses. (more than 4 billion , so many IP Addresses)
- We need to distribute those that's why we have classes.
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.



| | First byte | Second byte | Third byte | Fourth byte |
|---|---|---|---|---|
| Class A | 0 | | | |
| Class B | 10 | ▨ | | |
| Class C | 110 | ▨ | ▨ | |
| Class D | 1110 | | | |
| Class E | 1111 | | | |

a. Binary notation



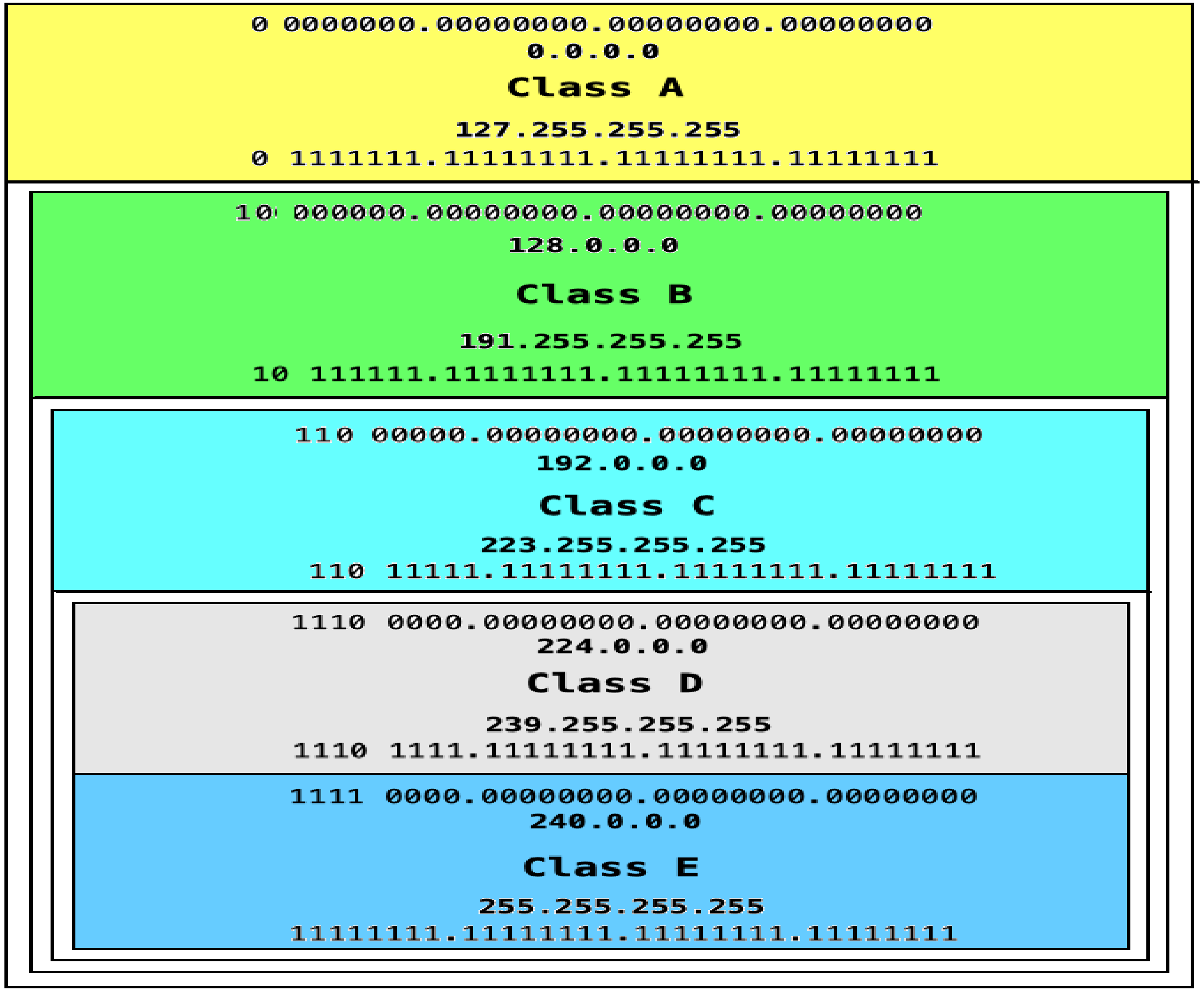
| | First byte | Second byte | Third byte | Fourth byte |
|---|---|---|---|---|
| Class A | 0–127 | | | |
| Class B | 128–191 | ▨ | | |
| Class C | 192–223 | ▨ | ▨ | |
| Class D | 224–239 | | | |
| Class E | 240–255 | | | |

b. Dotted-decimal notation

# How range of IP Address is defined

| $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ | | |
|---|---|---|---|---|---|---|---|---|---|
| **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** | | **Range** |
| 0 | x | x | x | x | x | x | x | Class A | 0-127 |
| 1 | 0 | x | x | x | x | x | x | Class B | 128-191 |
| 1 | 1 | 0 | x | x | x | x | x | Class C | 192-223 |
| 1 | 1 | 1 | 0 | x | x | x | x | Class D | 224-239 |
| 1 | 1 | 1 | 1 | x | x | x | x | Class E | 240-255 |

# IP Classful Addressing



0 0000000.00000000.00000000.00000000
0.0.0.0
Class A
127.255.255.255
0 1111111.11111111.11111111.11111111

10 000000.00000000.00000000.00000000
128.0.0.0
Class B
191.255.255.255
10 111111.11111111.11111111.11111111

110 00000.00000000.00000000.00000000
192.0.0.0
Class C
223.255.255.255
110 11111.11111111.11111111.11111111

1110 0000.00000000.00000000.00000000
224.0.0.0
Class D
239.255.255.255
1110 1111.11111111.11111111.11111111

1111 0000.00000000.00000000.00000000
240.0.0.0
Class E
255.255.255.255
11111111.11111111.11111111.11111111

– IP addresses starting with 0
– 0.0.0.0 – 127.255.255.255

– IP addresses starting with 10
– 128.0.0.0 – 191.255.255.255

– IP addresses starting with 110
– 192.0.0.0 – 223.255.255.255

– IP addresses starting with 1110
– 224.0.0.0 – 239.255.255.255

– IP addresses starting with 1111
– 240.0.0.0 – 255.255.255.255

# Example

- Find the class of each address.

1. 00000001 00001011 00001011 11101111
2. 11000001 10000011 00011011 11111111
3. 14.23.120.8
4. 252.5.15.111

# Example

- Find the class of each address.

1. 00000001 00001011 00001011 11101111
2. 11000001 10000011 00011011 11111111
3. 14.23.120.8
4. 252.5.15.111

Solution

1. The first bit is O. This is a class A address.
2. The first 2 bits are 1; the third bit is O. This is a class C address.
3. The first byte is 14 (between 0 and 127); the class is A.
4. The first byte is 252 (between 240 and 255); the class is E.

# Points to be noted

- Any IP Address start with 127, That is : 127.x.x.x means its **a loop back series** that is used for **self testing**.
- E.g. Ping 127.0.0.1 (ping to yourself)
- That is 127.0.0.1 is **Universal IP** ,
- We can not configure **universal IP**. Its by default configured.
- PING ( Packet Internet Groper ) is a tool used to troubleshoot networking issues .

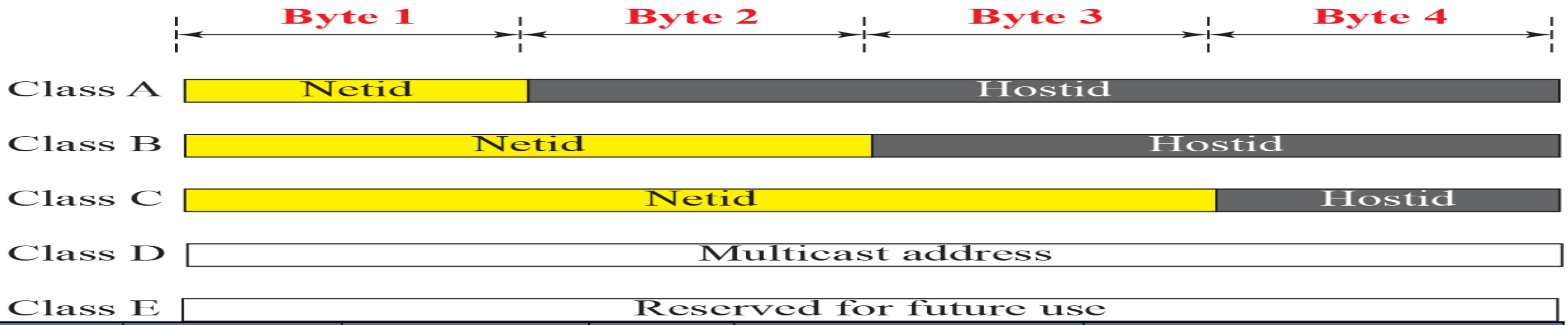
**IANA(Inter Associated Number Association) manages private IP's.**

## Regular Private IP Addresses

| Address Class | Reserved Private IP Addresses |
|---|---|
| Class A | 10.0.0.0 - 10.255.255.255 |
| Class B | 172.16.0.0 - 172.31.255.255 |
| Class C | 192.168.0.0 - 192.168.255.255 |

**Private network will have private IP's means devices that we connect to our router will get private IP addresses provided by IANA.**

# Netid and hostid of A, B, and C Classes



| Class | Network bits | Networks | Host bits | Hosts Per Network | Suitable for |
|---|---|---|---|---|---|
| Class A | 8 | $2^8$=256 | 24 | $2^{24}$ - $2^*$ =16,777,214 maximum hosts | For large organizations like Apple/Google/MS/Amazon |
| Class B | 16 | $2^{16}$=65536 | 16 | $2^{16}$ - $2^*$ = 65,534 maximum hosts | for medium scaled organizations like Sunbeam |
| Class C | 24 | $2^{24}$=16million | 8 | $2^8$ - $2^*$ = 254 maximum hosts | for small organizations/home network |

** Subtracting the network and broadcast address*

# Example: What is the type of the given IP address

1. 11.34.56.66
2. 10.46.34.67
3. 156.46.36.46
4. 172.20.34.56
5. 172.45.66.77
6. 192.168.2.5
7. 192.169.34.6

# Example (Solution ): What is the type of the given IP address

1. 11.34.56.66 : public
2. 10.46.34.67 : private
3. 156.46.36.46 : public
4. 172.20.34.56 : private
5. 172.45.66.77 : public
6. 192.168.2.5 : private
7. 192.169.34.6 : public

# Example : which class needs to be used for following number of Devices?

1. 200 devices
2. 3000 devices
3. 50000 devices
4. 200000 devices

# Example (Solution ) : which class needs to be used for following number of Devices?

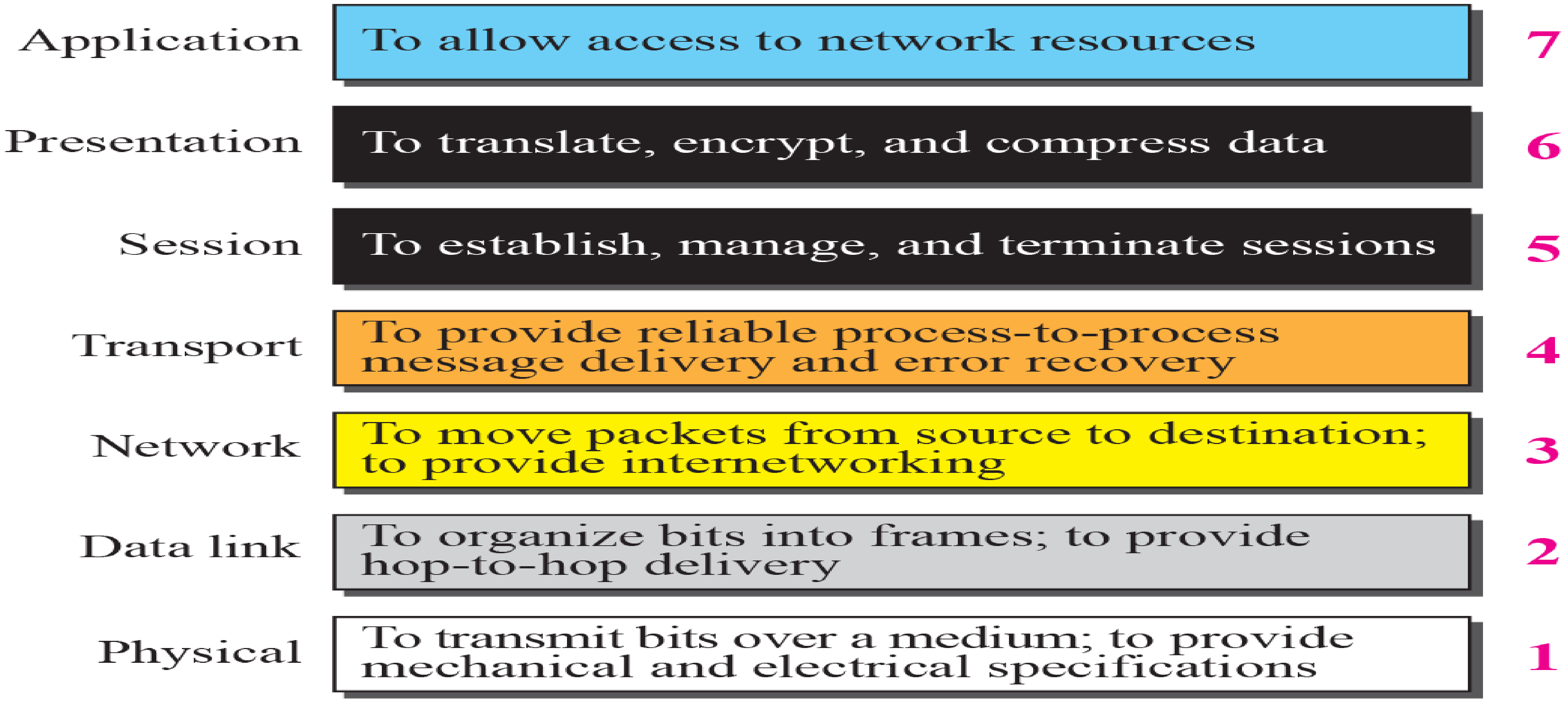
1. 200 devices : class C
2. 3000 devices : class B
3. 50000 devices : class B
4. 200000 devices : class A

# OSI Model

# OSI Model & Layers

- Established in 1947, **the International Standards Organization (ISO)** is a multinational body dedicated to worldwide agreement on international standards.
- We can not see standard but we can represent them.
- An ISO standard that covers all aspects of network communications is the **Open Systems Interconnection (OSI)** model.
- OSI model is now considered the primary Architectural model for inter-computer communications.
- **Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.**

# OSI Layers



| | | |
|---|---|---|
| Application | To allow access to network resources | 7 |
| Presentation | To translate, encrypt, and compress data | 6 |
| Session | To establish, manage, and terminate sessions | 5 |
| Transport | To provide reliable process-to-process message delivery and error recovery | 4 |
| Network | To move packets from source to destination; to provide internetworking | 3 |
| Data link | To organize bits into frames; to provide hop-to-hop delivery | 2 |
| Physical | To transmit bits over a medium; to provide mechanical and electrical specifications | 1 |

# Application Layer

- Interacts with application programs and is the highest level of OSI model.
- contains management functions to support distributed applications.
- enables the user, whether human or software, to access the network
- Examples : browser , applications such as file transfer, electronic mail, remote login etc.
- Protocols
  - http [80]: hyper text transfer protocol
  - https [443]: secure hyper text transfer protocol
  - ftp [20/21]: file transfer protocol
  - Smtp (25) : simple mail transfer protocol
  - Pop3 (110) : post office protocol
  - telnet(23)  : used to connect to the remote machine
  - ssh [22]: secure shell
  - dns ( 53) : domain name service  (used to get the IP address from the domain name)

# Presentation Layer

### Translation

- On sender side : translates from ASCII to EBDIC (Extended Binary Coded Decimal Interchange Code)
- On receiver side: translates from EBDIC to ASCII

### Encryption/Decryption

- Plain Text to Cipher Text
- Algorithms : RSA, SHA

### Compression / Decompression

- Sender Side : Compression
- Receiver Side : Decompression

### Data Representation [Content-type] (Used to Decide Common File Formats)

- For text ( plain: text/plain , html: text/html , json: application/json , xml: text/xml)
- For image ( bmp: image/bmp , png: image/png, jpg: image/jpg , jpeg: image/jpeg)
- For audio & Video (wave: audio/wav, mp3: audio/mp3, mp4: video/mp4, fllv: video/flv

# Session Layer

- **To start/manage/terminate the session.**
  - how to start, control and end conversations (called sessions) between applications.
  - log-on or password validation is also handled by this layer.
- **The session layer is the network *dialog controller.***
  - mechanism for controlling the dialogue between the two end systems and synchronization.
  - Allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization**
  - Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.
  - It establishes, maintains, and synchronizes the interaction among communicating systems.
- **Protocols**
  - SIP: session initiation protocol
  - NetBIOS : Network Basic Input Output Service
  - RPC: Remote Procedure Call

# Transport Layer

- Most Important Layer of OSI
- Responsible **for process-to-process/ End to End delivery** of the entire message.
- Provide a reliable mechanism for the **exchange of data between two processes** in different computers.
- Segment
  - smaller part of session PDU
  - every segment contains sequence number
  - every segment contains checksum for error checking
  - Segment contains:
    - **data** (from the session layer PDU)
    - **sequence number** : used for re-assembling the segments on the receiver machine
    - **checksum :** used to check if the data is not damaged

# Transport Layer Protocol

## TCP

- Transmission Control Protocol (Reliable)
- connection oriented protocol
  - connection will kept alive till the data transfer in progress
- flow control, error checking and sequencing
- slower than UDP
- E.g. Email (no data loss)

## UDP

- User Datagram Protocol (Unreliable)
- Connection Less Protocol
- does not provide error checking/ flow control
- Faster than TCP because no ACK only sending of data packets
- E.g: Online Games, Streaming

# Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- Segment Contains :
- data
  - source IP address
  - destination IP address
- **Network Layer Responsibilities:**
  - Logical Addressing : The network layer translates the logical addresses into physical addresses
  - Routing : sending the data across the network
  - Internetworking : provides the logical connection between different types of networks
  - Fragmentation : breaking the packets into the smallest individual data units that travel through different networks.
  - **Protocols :**
  - IP : internet protocol
  - IPx : internetwork packet exchange
  - ICMP : Internet Control Messaging Protocol
  - NAT : Network Address Translation
  - ARP : Address Resolution Protocol
  - PPP: Point to Point Protocol
- **Device** : Router

# Data Link Layer

- Data link layer attempts to provide reliable communication over the physical layer interface.
- **<u>DATA LINK Layer Responsibilities :</u>**
  - **Framing:**
    - Breaks the outgoing data into frames and reassemble the received frames.
    - every frame contains ( Source MAC address and Destination MAC address)
  - **Physical Addressing:**
    - uses MAC address to identify every NIC uniquely
  - **Flow Control:**
    - A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
  - **Error Control:**
    - Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
  - **Access Control:**
    - Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.
- **Protocols**
  - ARP(Address Resolution Protocol) : getting physical address from logical address
  - RARP: Reverse Address Resolution Protocol
- **Device :** Switch

# Physical Layer

- Provides physical interface for transmission of information.
- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication. Characteristics like voltage levels, timing of voltage changes, physical data rates, etc.
- send data in the form of 1's and 0's.
- senders and receivers clock must be synchronized.
- **Transmission mode:**
  - Defines direction of transmission  simplex, half duplex  and full duplex
- **Devices:**
  - NIC , Cables , hubs , repeaters , connectors

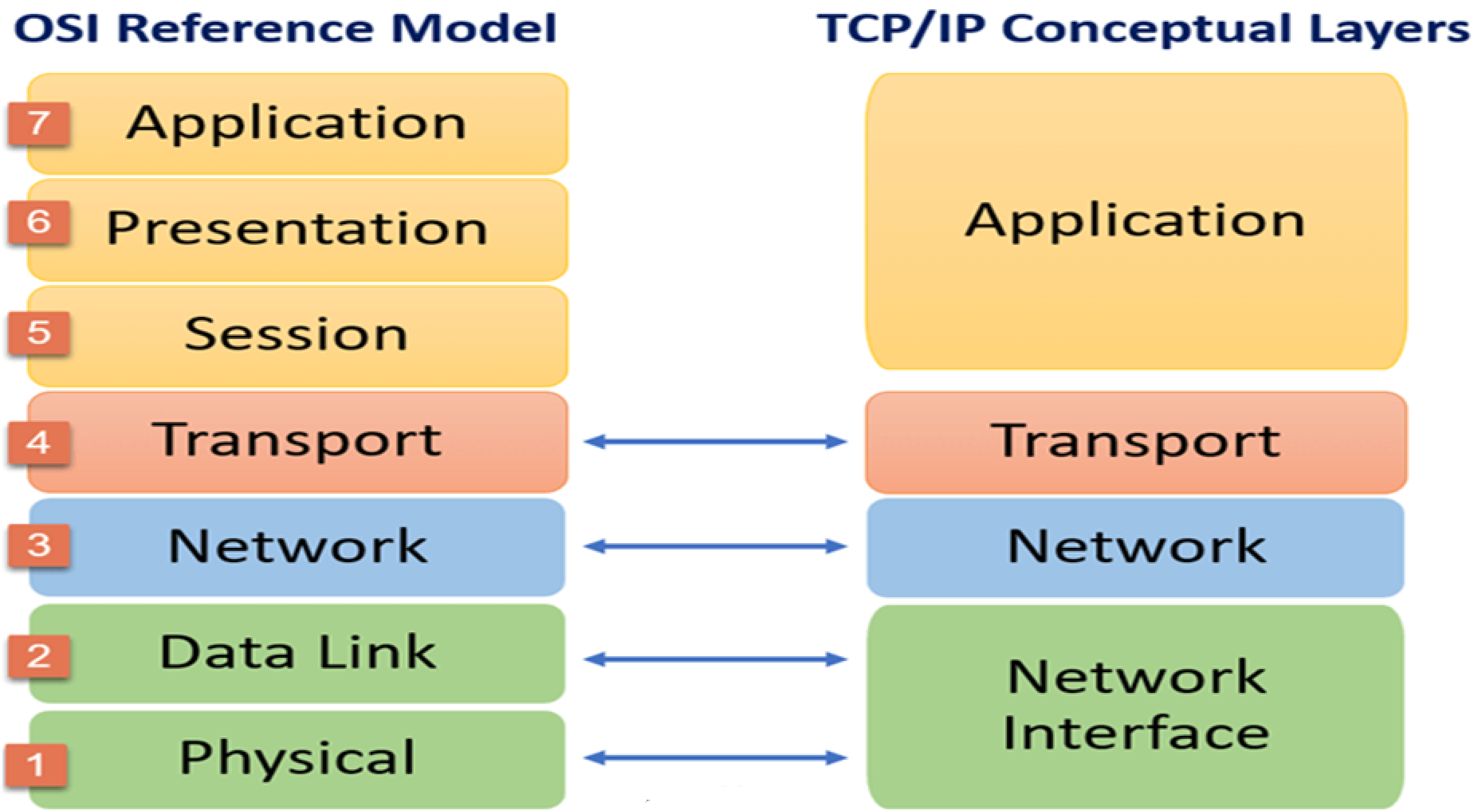
# 7 Layers of OSI Model

| | |
|---|---|
| **Application**<br>**(PDU : Data)** | • End user Layer<br>• HTTP, FTP, IRC, SSH, DNS |
| **Presentation**<br>**(PDU : Data)** | • Syntax Layer<br>• SSL, SSH, IMAP, FTP, MPEG, JPEG |
| **Session**<br>**(PDU : Data)** | • Synch and Send to port<br>• API's, Sockets |
| **Transport**<br>**(PDU : Segment)** | • End to end Connections<br>• TCP , UDP |
| **Network**<br>**(PDU : Packet)** | • Packets<br>• IP, ICMP, IPSec, IGMP |
| **Data Link**<br>**(PDU : Frame)** | • Frames<br>• Ethernet, PPP. Switch, Bridge |
| **Physical**<br>**(PDU : Bits)** | • Physical Structure<br>• Coax, Fiber, Wireless, Hubs, Repeaters |

# OSI and TCP/IP Model

- OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.
- OSI model distinguishes the three concepts, namely, services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three.
- OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
- In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.
- The OSI has seven layers while the TCP/IP has four layers.

# OSI and TCP/IP Model



# Thank You