Data Communication Network
DAY - 1

Mrs.Akshita.S.Chanchlani
akshita.chanchlani@sunbeaminfo.com

DCN DAY -1 Contents

- Few Network Terminologies
- Need of Network
- Network Criteria's
- Transmission Media
- Switching
- Multiplexing
- Network Classification (LAN, MAN, WAN)
- ARP
- Network Classification by Component Role
- Network Physical Structure
  - Types of Connection
  - Physical Topology
- Network Devices

Few Terminologies

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

Components of Data communication

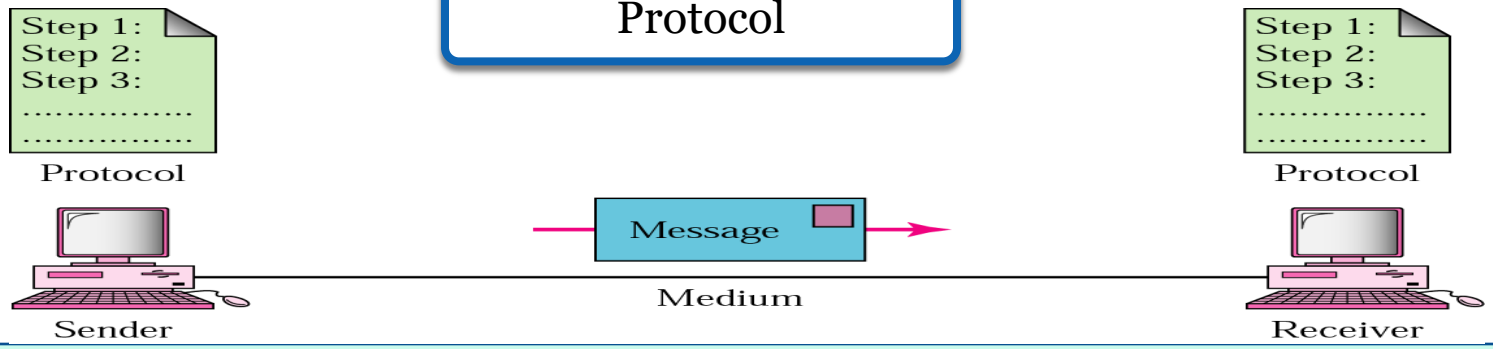
- Message
- Sender
- Receiver
- Transmission Medium
- Protocol

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

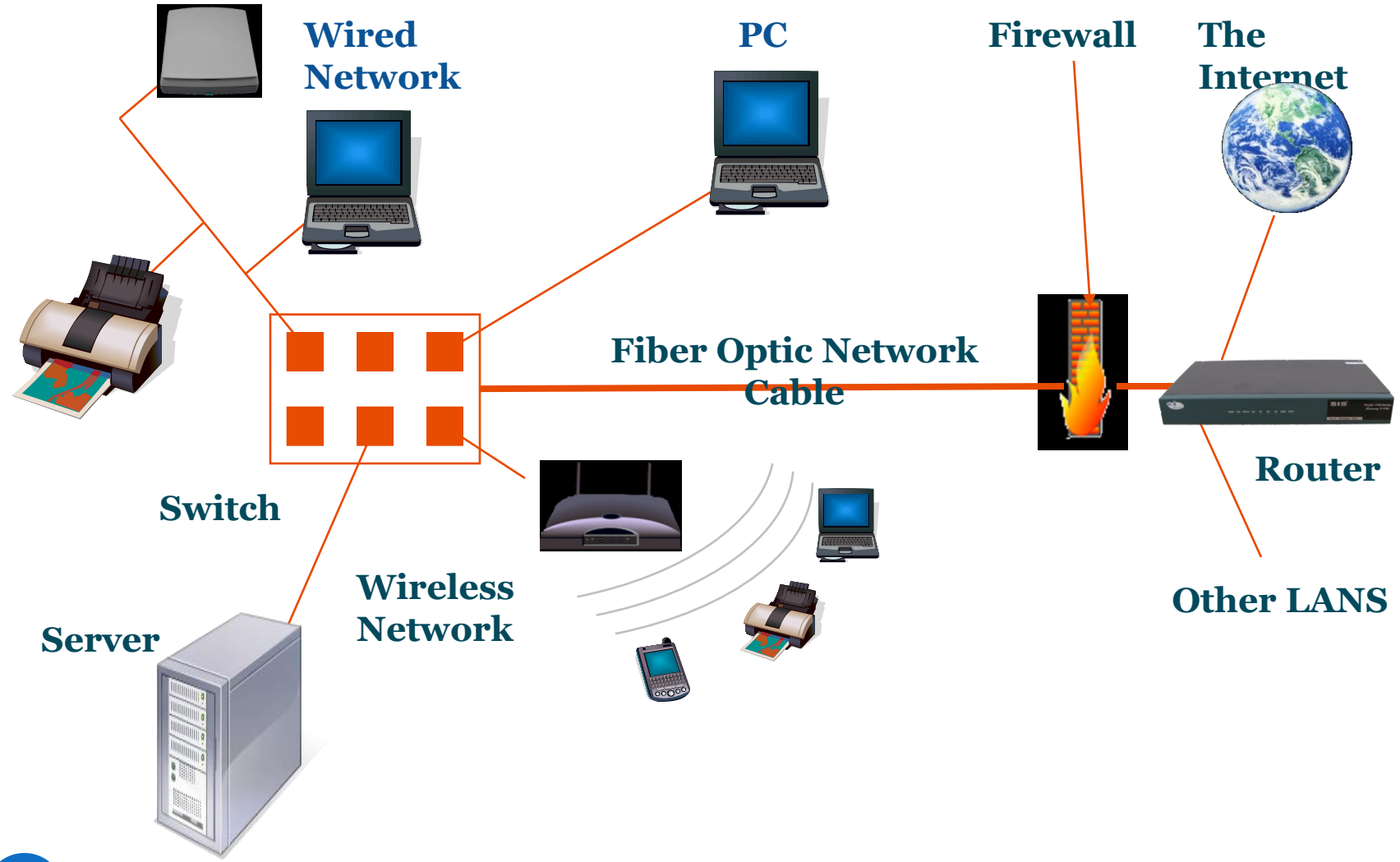


The effectiveness of a data communications system depends on four fundamental characteristics:
Delivery, Accuracy , Timeliness , Jitter

Need of Network/ Applications of Network

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

Network Diagram



Network Criteria

Performance

- depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
- Measured in terms of Delay and Throughput

Reliability

- is measured by the frequency of failure, the time it takes a link to recover from a failure
- Measured in terms of availability/robustness

Security

- Data protection against corruption/loss of data due to:
  - Errors
  - Malicious users

Basic Concepts in a Data Communication System

Bandwidth

- Amount of data that can be transferred from one point to another in a certain time period

Attenuation

- Loss of power in a signal as it travels from the sending device to the receiving device

Broadband

- Multiple pieces of data, sent simultaneously to increase the transmission rate

Protocols

- Rules that govern data communication
  - Error detection, message length, and transmission speed

Network Types

wired

- cable
  - co-axial , CAT (TP) : category cable also called as Twisted Pairs cable
- Types: UTP : Unshielded and STP: Shielded
  - Version:
    - cat 1
    - cat 2 : 1Mbps
    - cat 3 : 10Mbps
    - cat 4 : 16Mbps
    - cat 5 : 100Mbps
    - cat 5e: 125Mbps
    - cat 6 : 1000Mbps ~ 1Gbps
    - cat 6a: 1000Mbps ~ 1Gbps
    - cat 7 : 10000Mbps ~ 10Gbps
    - Fiber Optics :+10Gbps

Topology

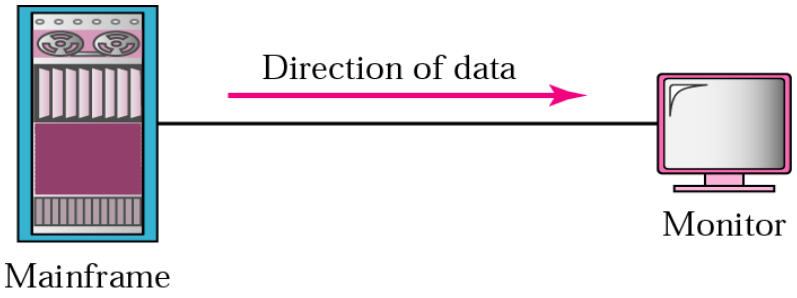
- Bus , Ring, Mesh , Star

Types

- LAN , MAN , WAN

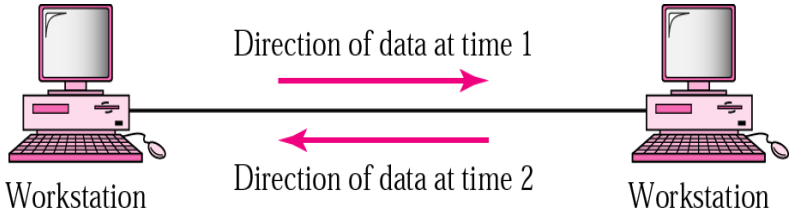
Media (Transmission Medium)

Transmission Modes / Data Flow Direction



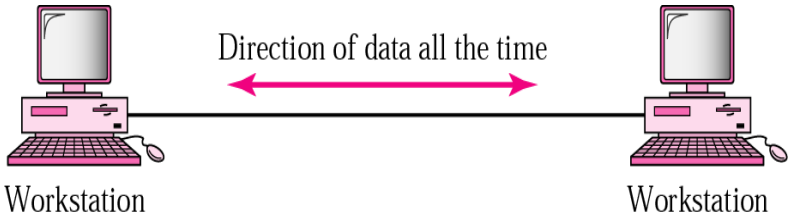
Simplex Mode

- 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.

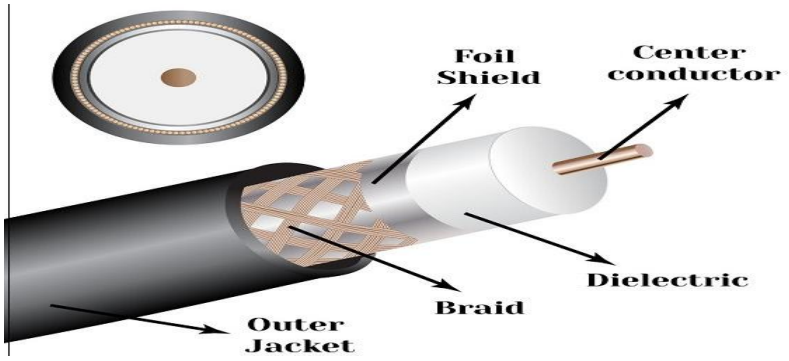
Unguided

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

Twisted Pair (maximum length of 100 meters)

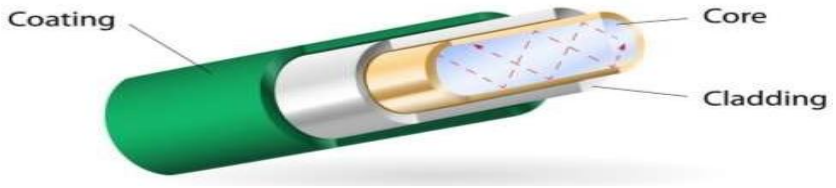
- Most common wires used for transmitting signals
- To reduce this electromagnetic interference, pair of copper wires are twisted together.
- Shielding twisted pair cable
  - To counter the tendency of twisted pair cables to pick up noise signals, wires are shielded .
  - Such twisted pairs are called **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**.
- Light Emitting Diodes (LEDs) or Laser Diodes (LDs) emit light waves at the **source**, which is read by a **detector** at the other end.
- 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**

Merits:

- Signals carrying data can travel long distances without weakening
- Immune to electromagnetic interference , Suitable for industrial and noisy areas

Demerits:

- Optical fiber cables are expensive
- Sophisticated technology required for manufacturing, installing and maintaining optical fiber cables

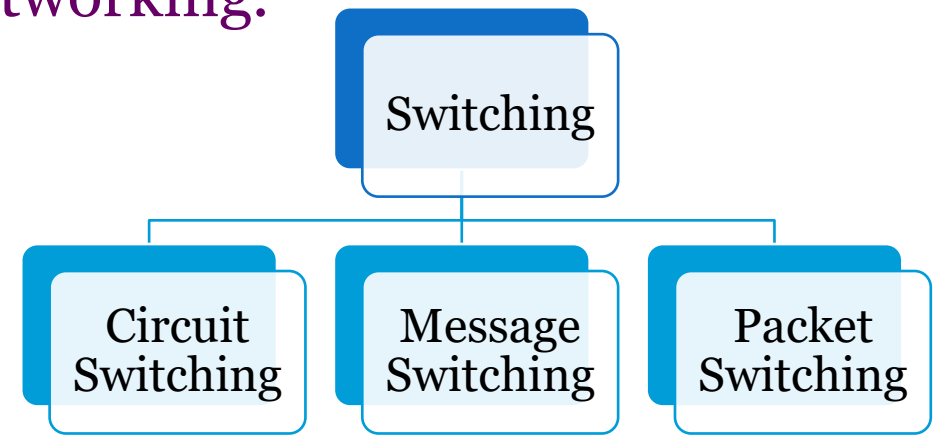
Infrared and Radio Waves

- Infrared:
  - Low frequency infrared waves are used for very short distance communication like TV remote, wireless speakers, automatic doors, hand held devices etc.
- Radio Waves:
  - Transmission of data using radio frequencies is called **radio-wave transmission**.
  - Radio stations transmit radio waves using **transmitters**, which are received by the receiver installed in our devices.
  - Both transmitters and receivers use antennas to radiate or capture radio signals.
  - These radio frequencies can also be used for **direct voice communication** within the **allocated range**.

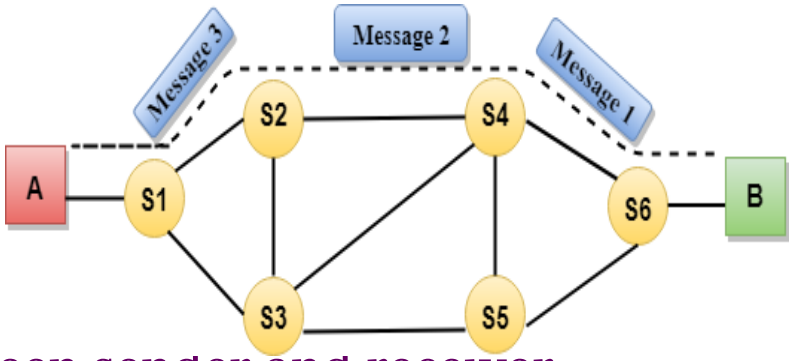
Switching

Switching

- In large networks, there can be multiple paths from sender to receiver.
- The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.
- The mechanism for exchange of information between different computer networks and network segments is called switching in Networking.

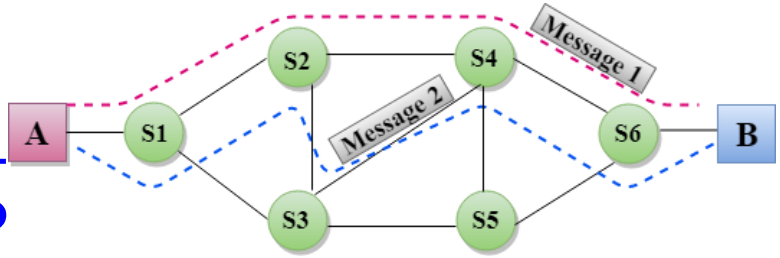


Circuit Switching



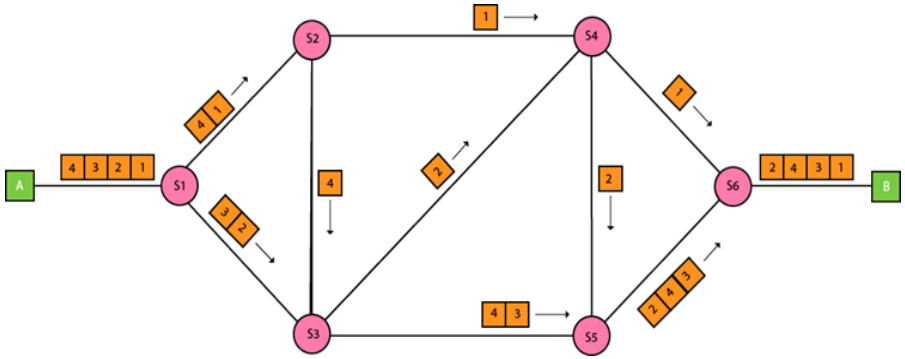
- Establishes a dedicated path between sender and receiver.
- once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Operates in a similar way as the telephone works.
- when any user wants to send the data a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Three Phases:
  - Circuit Establishment
  - Data Transfer
  - Circuit Disconnect

Message Switching



- There is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message.
- provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- they can provide the most efficient routes.
- Uses a method of **store and forward network**

Packet Switching



- Message is divided in packets , packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent

Multiplexing

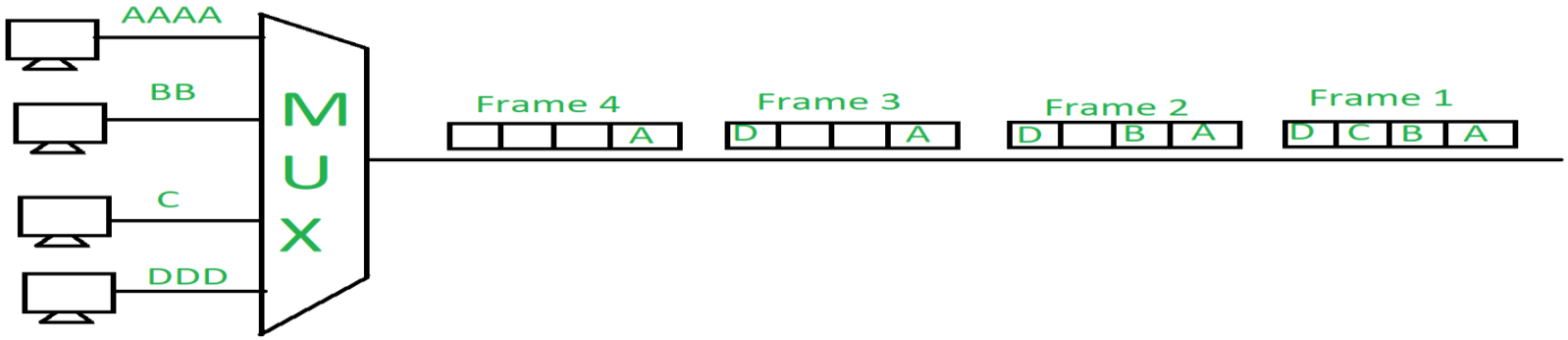
Multiplexing

- A communication channel such as an optical fiber or coaxial cable can carry only one signal at any moment in time. **Wastage of Bandwidth**
- Multiplexing is the process of combining multiple signals into one, in such a manner that each individual signal can be retrieved at the destination.
- **Multiplexing** is used in the cases where the signals of lower bandwidth and the transmitting media is having higher bandwidth.
- Methods of Multiplexing;
  - FDM (Frequency Division Multiplexing)
  - TDM (Time Division Multiplexing)

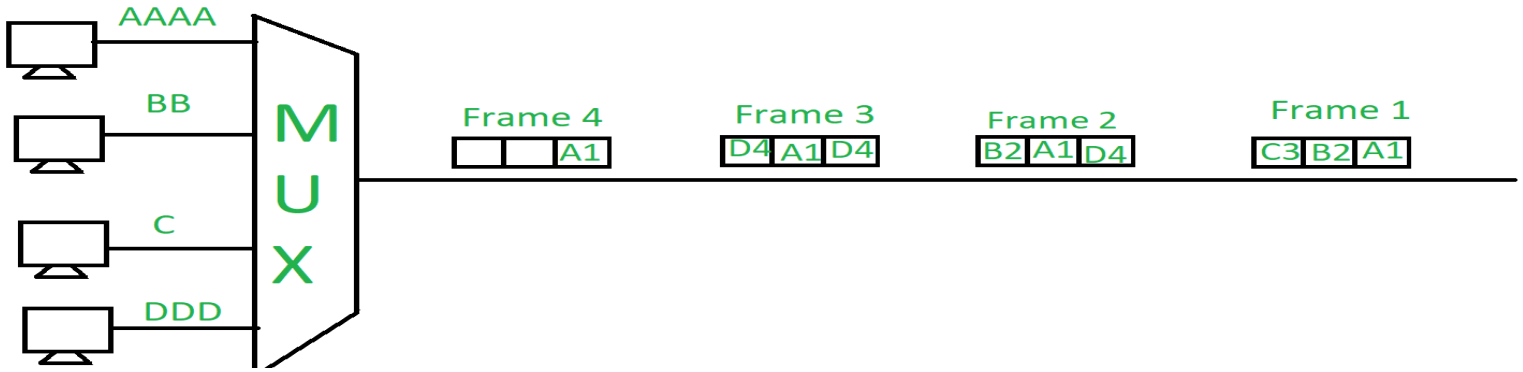
Time Division Multiplexing (TDM)

- data transmission rate of media is greater than that of the source, and each signal is allotted a definite amount of time.
- Time division multiplexing all the signals operate with same frequency at different times.

Synchronous TDM

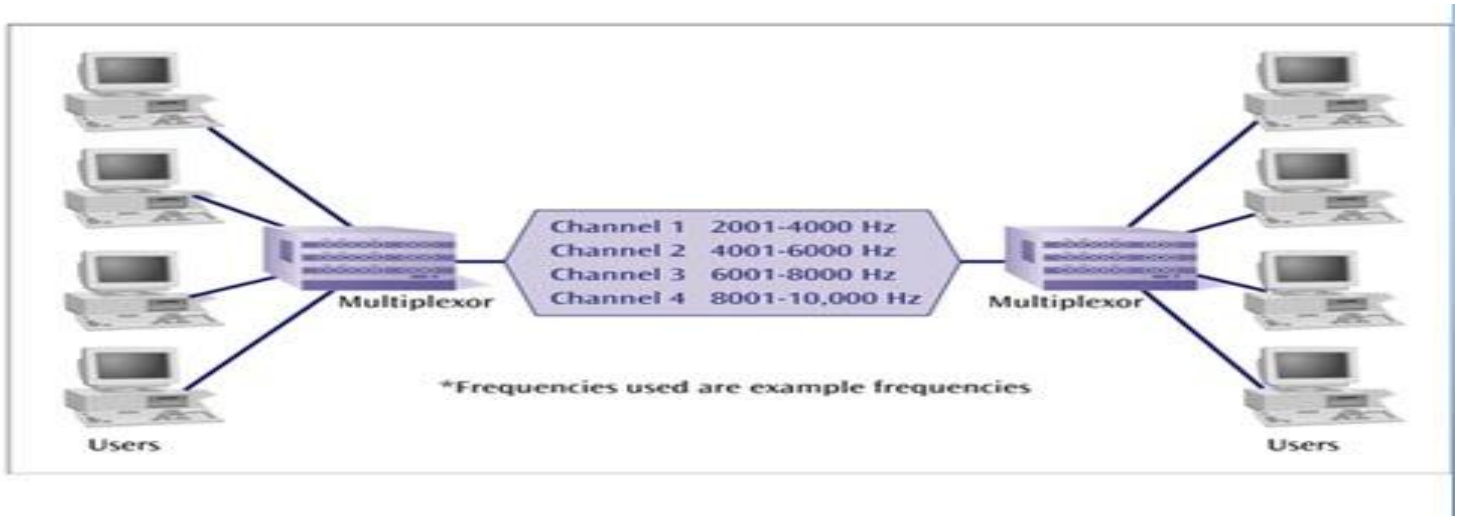


Asynchronous (or statistical) TDM



Frequency Division Multiplexing (FDM)

- Number of signals are transmitted at the same time, and each source transfers its signals in the allotted frequency range
- The frequency spectrum is divided into several logical channels, in which every user feels that they posses a particular bandwidth.
- To avoid interference between two successive channels **Guard bands** are used.



TDM VS FDM

	TDM (Time Division Multiplexing.)	FDM(Frequency Division Multiplexing)
1	TDM works with digital signals as well as analog signals.	While FDM works with only analog signals.
2	TDM has low conflict.	While it has high conflict.
3	TDM is efficient.	While it is inefficient.
4	In TDM, time sharing takes place.	While in this, frequency sharing takes place.
5	Here synchronization pulse is necessary.	Here Guard band is necessary.
6	sharing of the time through utilizing time slots for the signals	involves the distribution of the frequencies, where the channel is divided into various bandwidth ranges (channels)
7	Framing bits (Sync Pulses) are used in TDM at the start of a frame in order to enable synchronization	FDM uses Guard bands to separate the signals and prevent its overlapping

Network Classification

Network Classification

Classification by network geography

- according to the geographical boundaries spanned by the network itself
- LAN, WAN, MAN ,PAN, SAN(Major two are LAN and WAN)

Classification by component roles

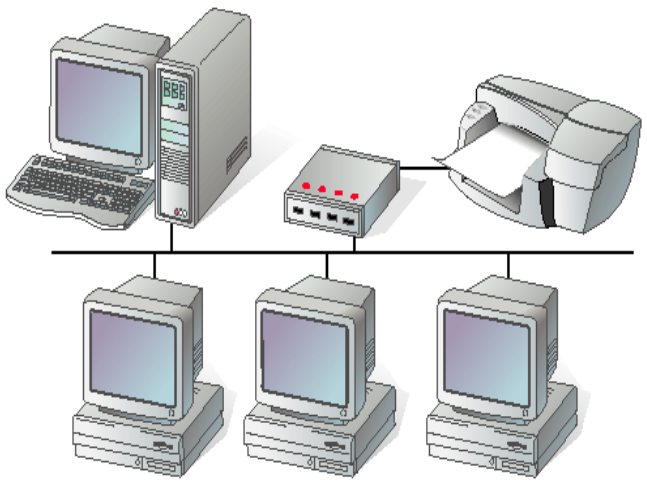
- according to the roles that the networked computers play in the network's operation
- Peer-to-peer, server-based, and client-based .

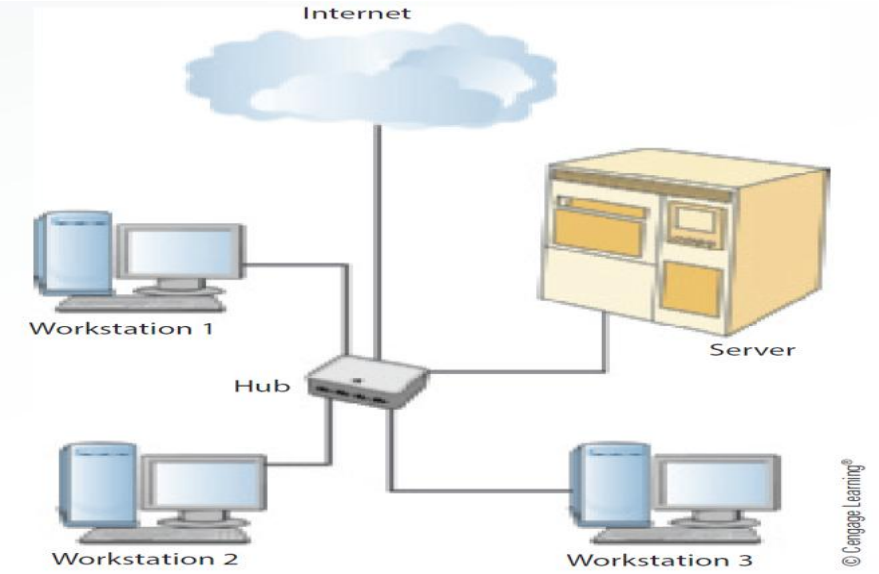
Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

LAN (Local Area Network)

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)

Wired Network Designing

TOKEN RING

Token Ring

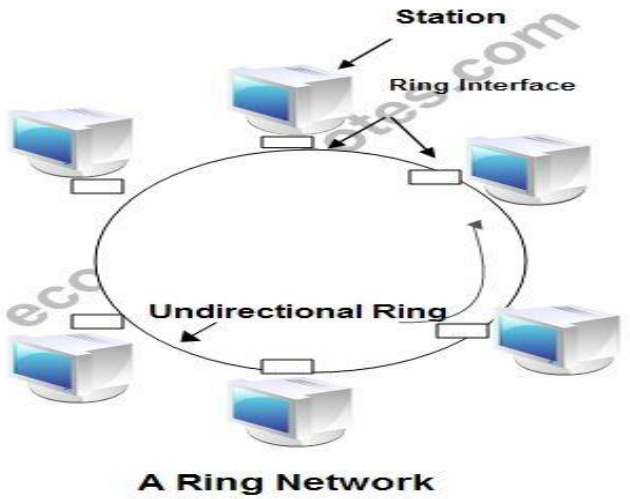
- The token ring LAN process is delineated by the following sequence of events:
  - A token continually circulates inside the toke ring LAN
  - To transmit a message, a node inserts a message and destination address inside an empty token.
  - The token is examined by each successive node.
  - The destination 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

Token Ring Working

- It maintains one or more common data frames that continuously circulate through the network.
- All connected devices on the network share these frames as follows:
  - A frame (packet) arrives at the next device in the ring sequence.
  - That device checks whether the frame contains a message addressed to it.
    - If so, the device removes the message from the frame.
    - If not, the frame is empty (this is called a token frame).
  - The device holding the frame decides whether to send a message.
    - If so, it inserts message data into the token frame and issues it back to the LAN.
    - If not, the device releases the token frame for the next device in sequence to pick up.

How Token Ring Compares to Ethernet

- devices within a token ring network can have the exact same MAC address
- Here are some more differences:
  - Cabling for token ring networks is more expensive than Ethernet.
  - Token ring network cards and ports are more expensive.
  - Token ring networks can be configured so that certain nodes have more priority than others.
  - Token ring networks use tokens to avoid collisions. Ethernet networks (especially when hubs are used) are more prone to collisions.

Wired Network Designing

ETHERNET

Ethernet

Transfer speed 10 Mbps, 100 Mbps, or above

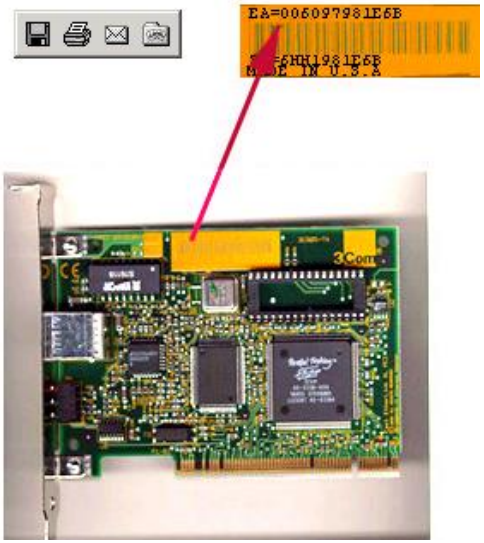
- Ethernet is the dominant cabling and low level data delivery technology used in Local Area Networks (LAN's).
- It was developed by Xerox corp. along with DEC and Intel.
- **Features:**
  1. Ethernet Addresses are 6 bytes(48 bits) long.
  2. Ethernet supports networks built with twisted pair, thin and 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 left 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. • 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.

How to determine the type of destination addresses

- To find the type of the address, we need to look at the **second hexadecimal digit** from the left. If it is **even**, the address is **unicast.** If it is **odd**, the address is **multicast**.
- ***Define the type of the following destination addresses:***

a) *4A:30:10:21:10:1A*

b) *47:20:1B:2E:08:EE*

c) *FF:FF:FF:FF:FF:FF*

Solution:

a) *This is a unicast address because A in binary is 1010.*

b) *This is a multicast address because 7 in binary is 0111.*

c) *This is a broadcast address because all digits are F's.*

Collision

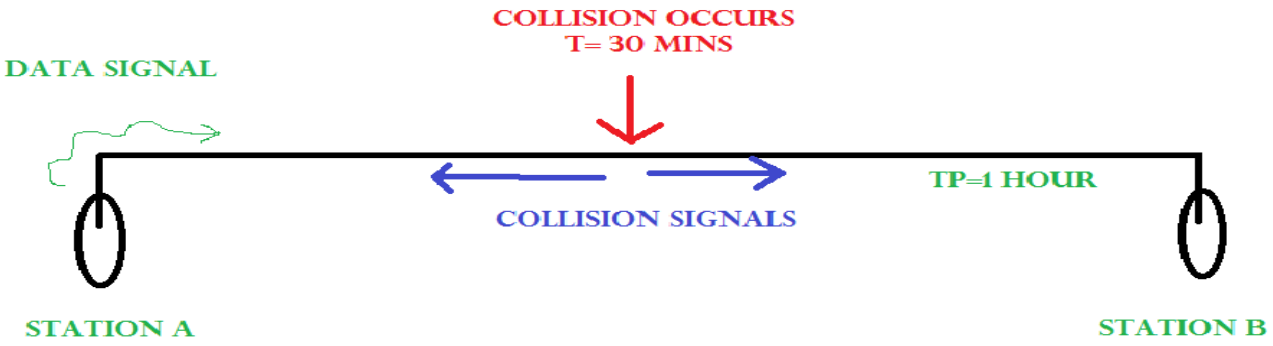
- The collision occurs when the sending device does not receive a clear response back within the allotted time.
- Two devices on the same Ethernet network attempting to transmit data at exactly the same time.
- The network detects the "collision" of the two transmitted packets and discards them both.
- **Ethernet uses Carrier Sense Multiple Access/ Collision Detect (CSMA/CD) as its method of allowing devices to "take turns" using the signal carrier line.**

Ethernet's MAC Algorithm- **CSMA/CD**

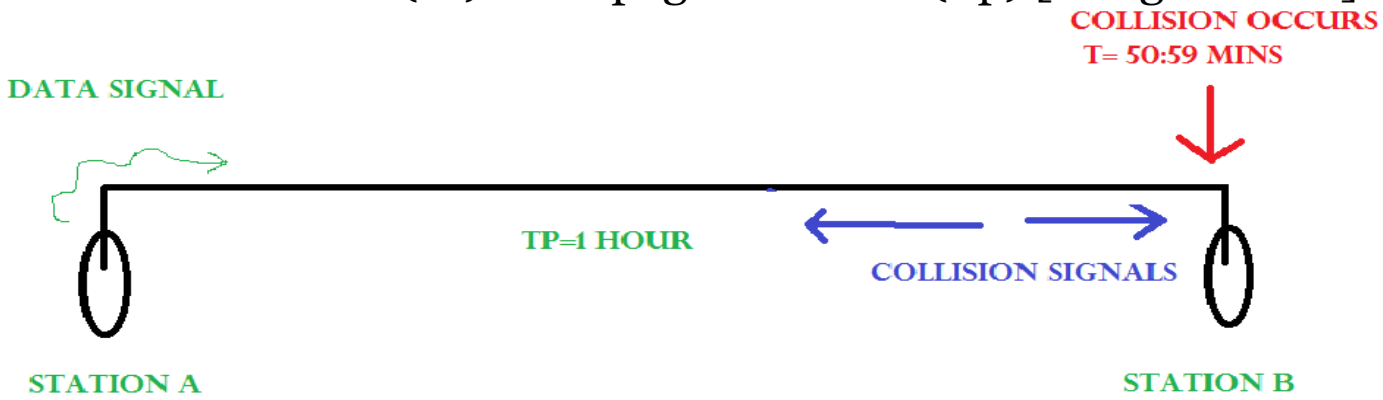
- Ethernet uses CSMA/CD – listens to line before/during sending.
- It decides which station will transmit when so that data reaches the destination without corruption.
- If line is idle (no carrier sensed) (Check If transmission link is idle)
  - send packet immediately
  - Transmit anytime
  - upper bound message size of 1500 bytes
- If line is busy (carrier sensed)
  - wait until idle and transmit packet immediately
    - called *1-persistent* sending
- If collision detected
  - Send 4 bytes JAM
  - Back off for a random period
  - Stop sending and jam signal
  - Try again later

CS - Carrier Sense (Is someone already talking?)
MA - Multiple Access (I hear what you hear!)
CD - Collision Detection (Hey, we're both talking!)

CSMA/CD



Scenario 1 : Detection of collision :
Transmission time (Tt) > Propagation Time (Tp) [Rough bound]

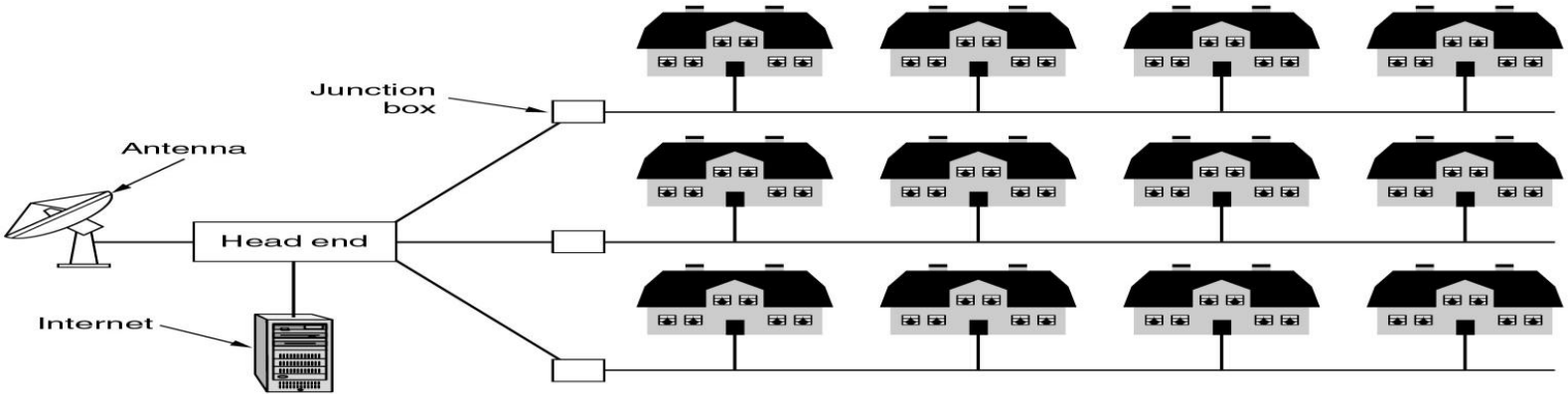


Scenario 2 : Detection of collision :
Transmission time (Tt) >> 2* Propagation Time (Tp) [Tighter bound]

MAN (Metropolitan area network)

MAN

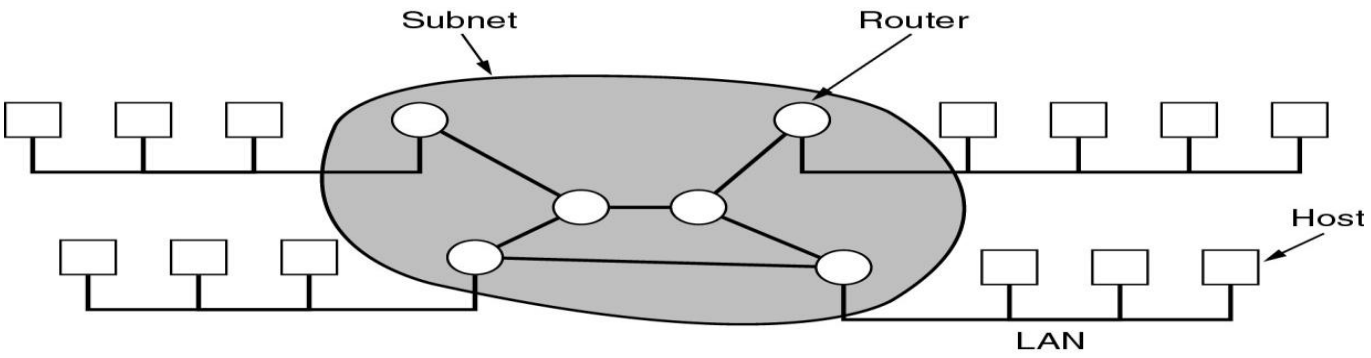
- A MAN spans the distance of a typical metropolitan city.
- The cost of installation and operation is higher.
- MANs use high-speed connections such as fiber optics to achieve higher speeds.
- Provide connectivity over areas such as a city, a campus
- More than 100m , Designed to handle data communication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



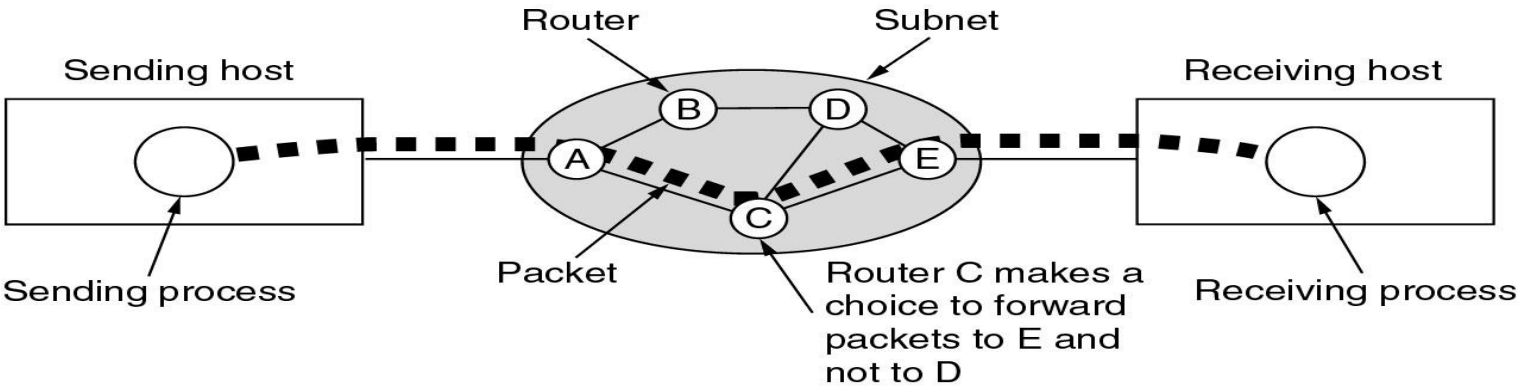
WAN (Wide Area Network)

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



WAN Cont...



A stream of packets from sender to receiver. (virtual- circuit)

- If we connect two machines using cable then its a LAN.
- If media belong to me , media can be cable/wireless/ wired **LAN.**
  - e.g. 2 phones connected via wire.
- If media belong to third party that can be called as **WAN.**
  - e.g. 2 phones/pc's connected by telephone lines of their party provider.

Other Types of Networks

Other Types of Network

- CAN (Campus Area Network)
  - Eg. Sunbeam
- PAN
  - Personal Area Network
    - Laptop connected to Bluetooth, speaker, camera , mic etc
    - made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building.
  - Private Area Network
    - E.g. One m/c in India (One IP) is connected to other machine in US (Other IP) are connected via Internet / VPN(Virtual Private Network)
- SAN
  - Server Area Network/ System Area Network
    - designed to provide high-speed connection in server-to-server applications (cluster environments)
    - Bank Branches and their transactions are done at centralized Bank server
  - Storage Area Network
    - That connects shared pools of storage devices to several servers, they don't rely on a LAN or WAN.
    - One instance of server is created and kept at each location
    - Google Drive data (google.co.in/ google.com/google.jp etc)
- GAN(Global Area Network)
  - network composed of different interconnected networks that cover an unlimited geographical area.
  - used to support mobile number of arbitrary number of wireless LAN (LAN), satellite coverage areas, etc.

Address Resolution Protocol (ARP)

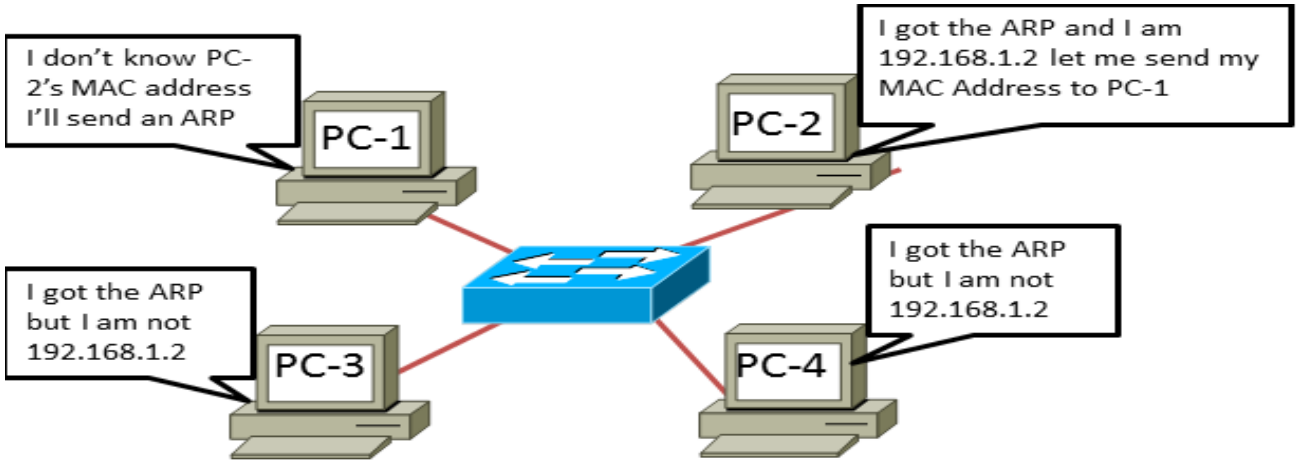
ARP

- 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

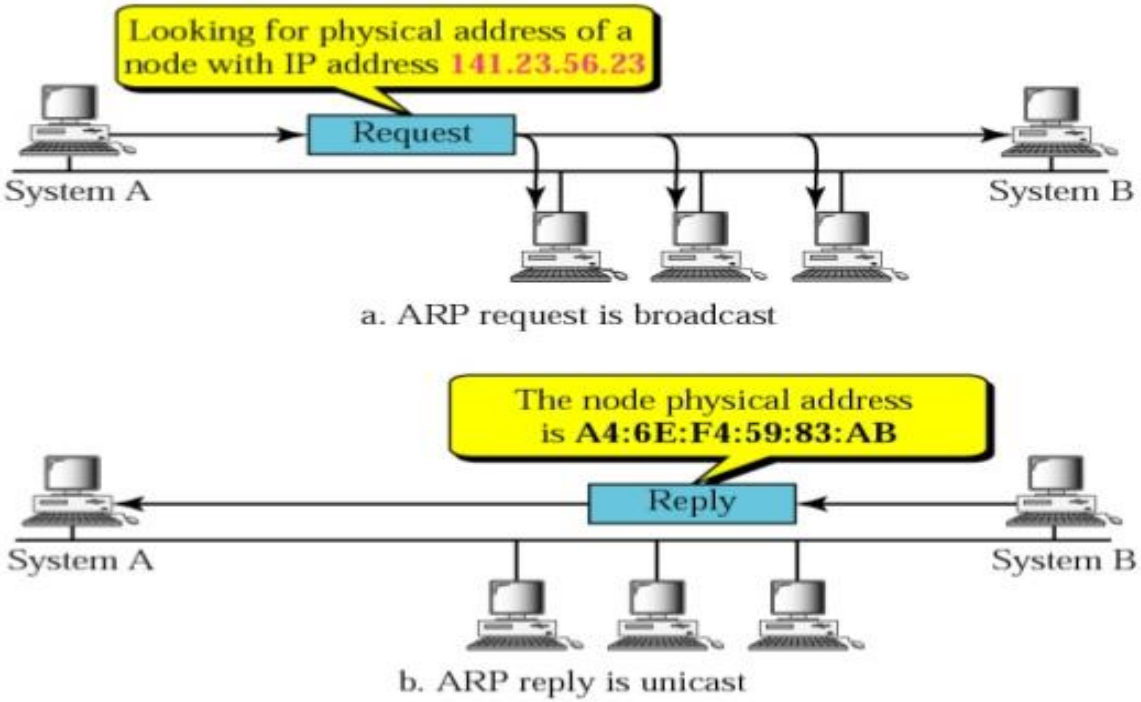
ARP

- 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



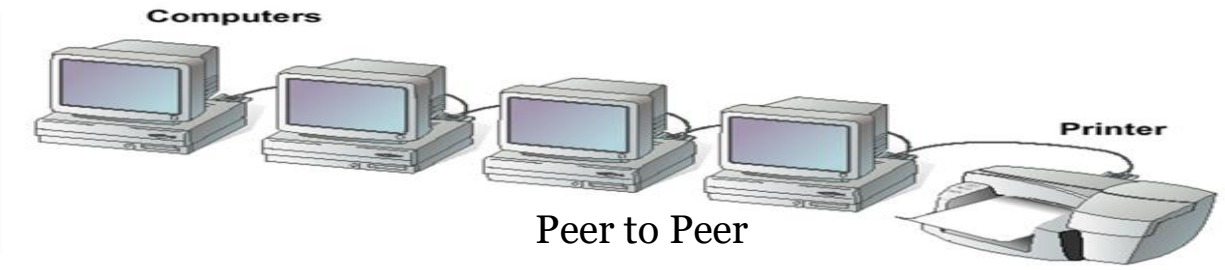
ARP Operation



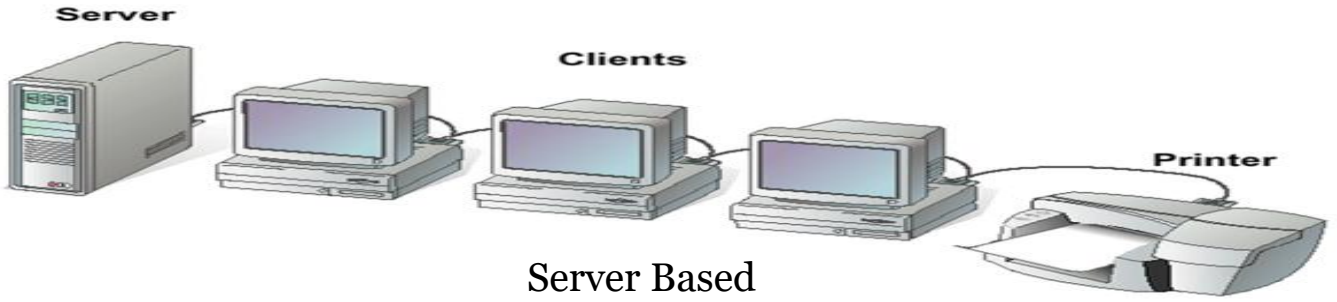
ARP Cache Times : Means the time till that Machine ‘A’ should store the machine ‘B’ ‘s MAC address in its memory for data transmission.

Network Classification by Component Roles

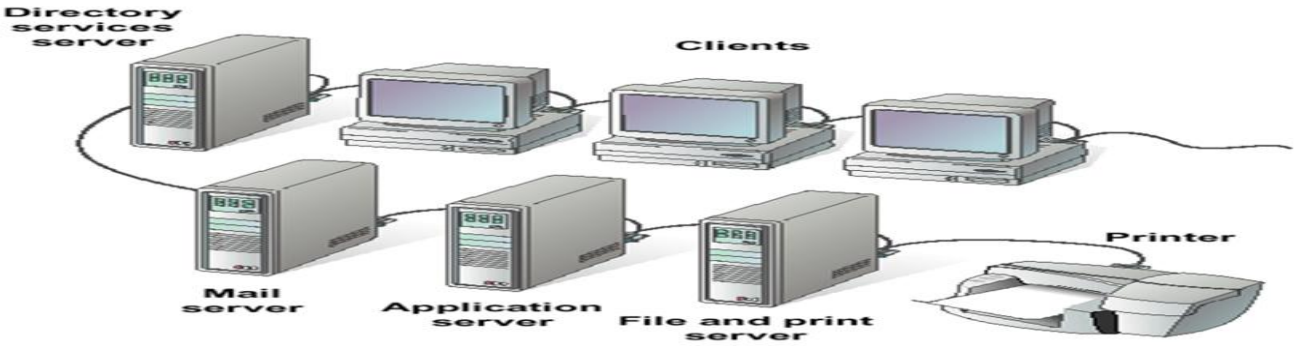
Network Classification by Component Roles



Peer to Peer



Server Based



Client Based

Network Physical Structure

Physical Structure

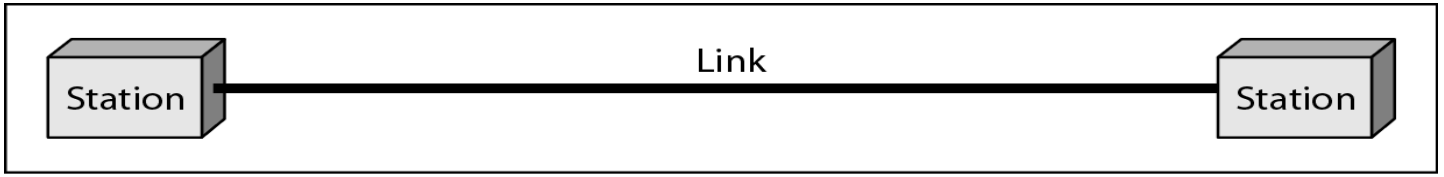
Type of Connection

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

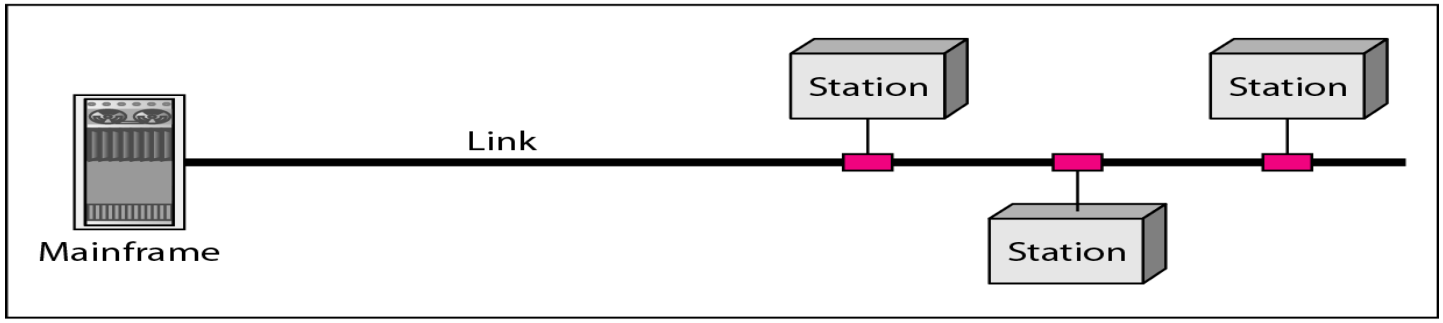
Physical Topology

- 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



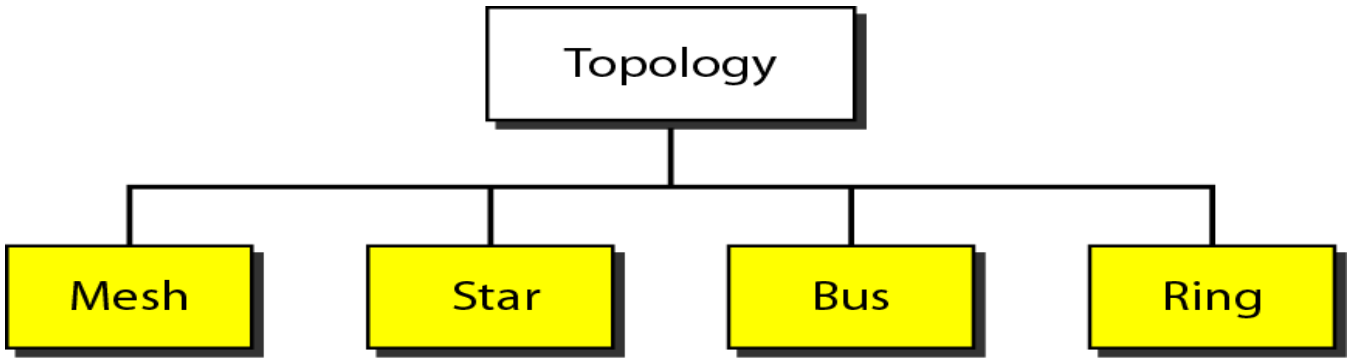
a. Point-to-point



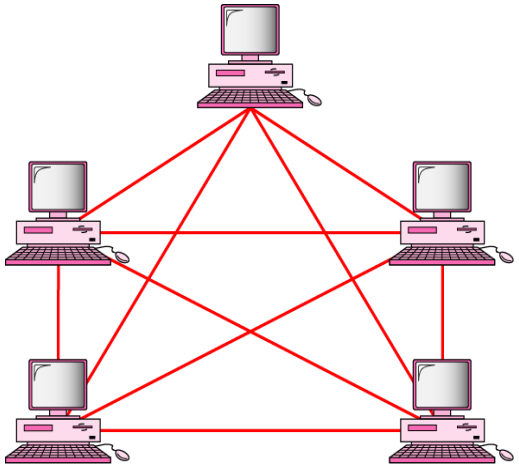
b. Multipoint

Physical Topology

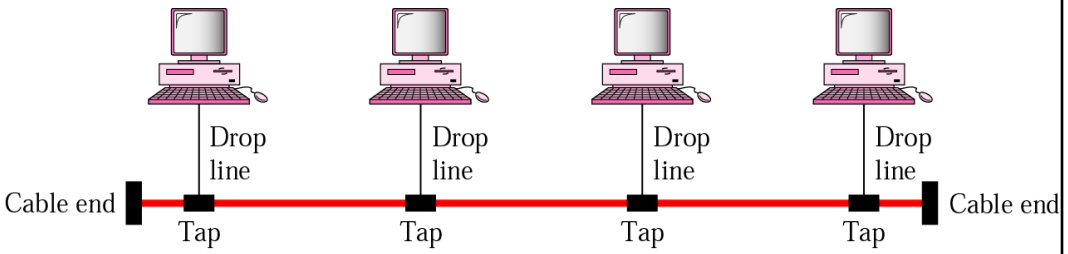
- Topology defines the way hosts are connected to the network
- The network topology defines the way in which computers, printers, and other devices are connected.
- A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



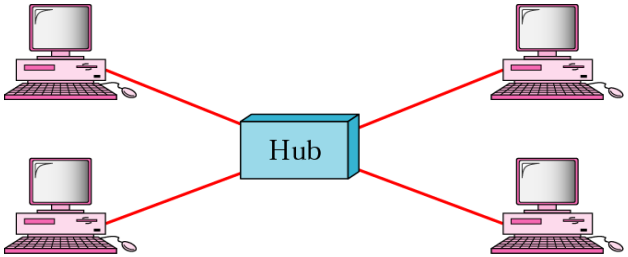
Network Topology



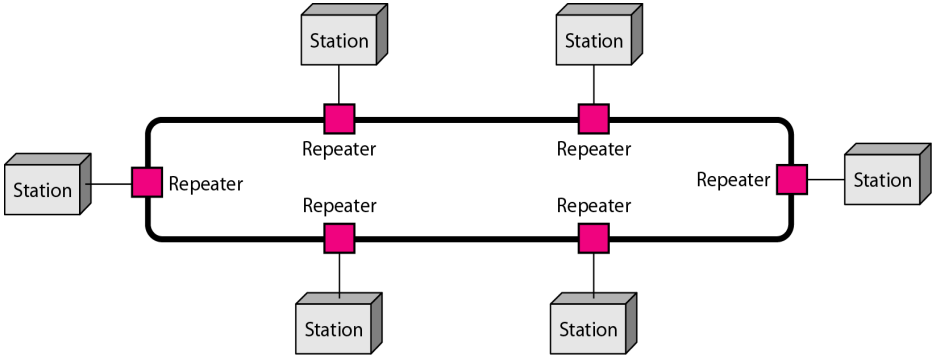
mesh



bus



star



ring

Mesh

- Every device has a **dedicated point-to-point link to every other device.**
- connects all devices (nodes) to each other for redundancy and fault tolerance.
- Number of connections= n(n-1) where n= the number of devices.
- Example:Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star

- Each device has a dedicated point-to-point link only to a **central controller, usually called a hub.**
- The controller acts as an exchange.
- The star topology is the most commonly used architecture in Ethernet LANs.

Bus

- A bus topology is multipoint.
- One long cable acts as a backbone to link all the devices in a network
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core

Ring

- Each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.
- The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.
- No host required as each computer manages its own connectivity
- Transmission is in one direction
- Needs less cable than star topology

Hierarchical Organization of the Internet

National Internet Service Providers

- backbone networks created and maintained by specialized companies.
- Some national ISP networks are also connected to one another by private switching stations called peering points.

Regional Internet Service Providers

- Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs.

Local Internet Service Providers

- direct service to the end users
- a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network.
- Each of these local ISPs can be connected to a regional or national service provider.

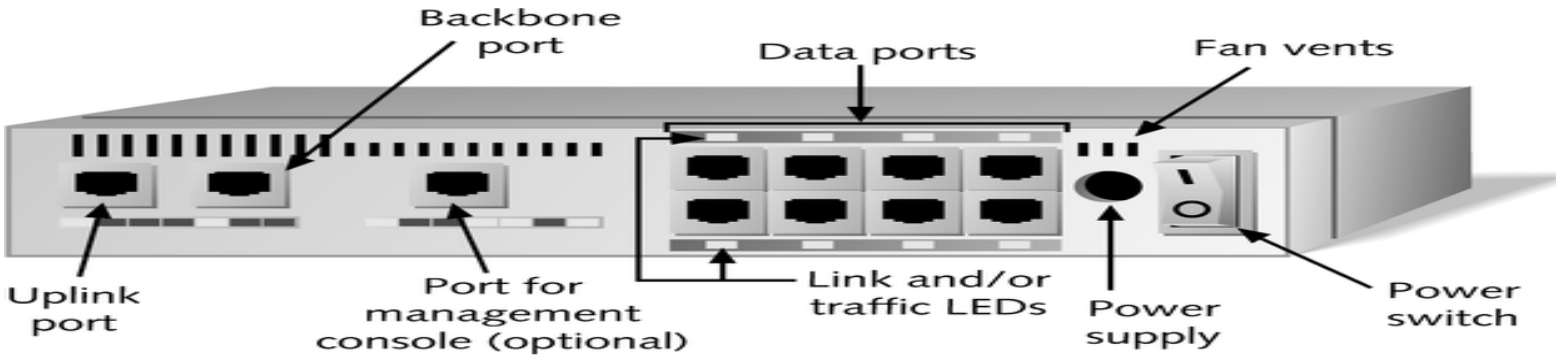
Network Devices / Internetworking Devices

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

- Common connection point for devices in a network.
- Hub is Multiport repeater containing multiple ports to interconnect multiple devices
- Hubs regenerate and retime network signals
- They cannot filter network traffic and they cannot determine best path
- Hubs are devices commonly used to connect segments of a LAN.
- 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



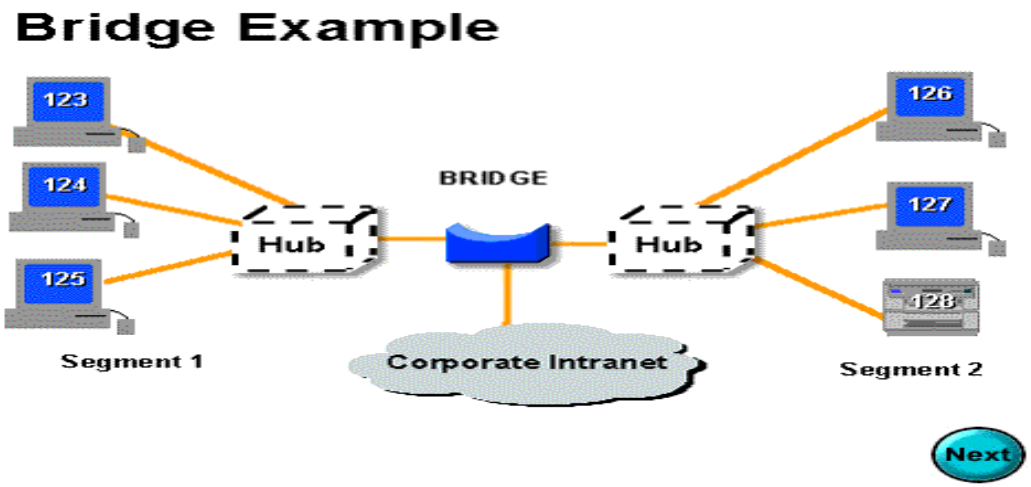
Repeaters

- **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.
- Disadvantages:
  - It can't filter network traffic.
  - Data gets passed along by a repeater to all other LAN segments of a network regardless of whether it needs to go there or not.

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.
- **Can interpret address information**
- Allow different nodes of a network to communicate directly with each other.
- 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.

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

- Routers are another type of internetworking device.
- 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.

How Gateways Work

- All networks have a boundary that limits communication to devices that are directly connected to it.
- Due to this, 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.
- The gateway is implemented at the edge of a network and manages all data that is directed internally or externally from that network.
- When one network wants to communicate with another, the data packet is passed to the gateway and then routed to the destination through the most efficient path.
- Gateways are basically protocol converters, facilitating compatibility between two protocols and operating on any layer of the open systems interconnection (OSI) model.

General Network Design Process

General Network Design Process

- In general ,the network design problems consists of the following 3 general elements:

1. **Environmental given:** Includes the locations of hosts, servers, terminals and other nodes
2. **Performance constraints:** Consists of network reliability, traffic throughput and host/client computer speeds
3. **Internetworking variables:** Includes the network topology, line capacities, and packet flow assignments

Thank You