Computer Networking

By Amul Batra

Course Content

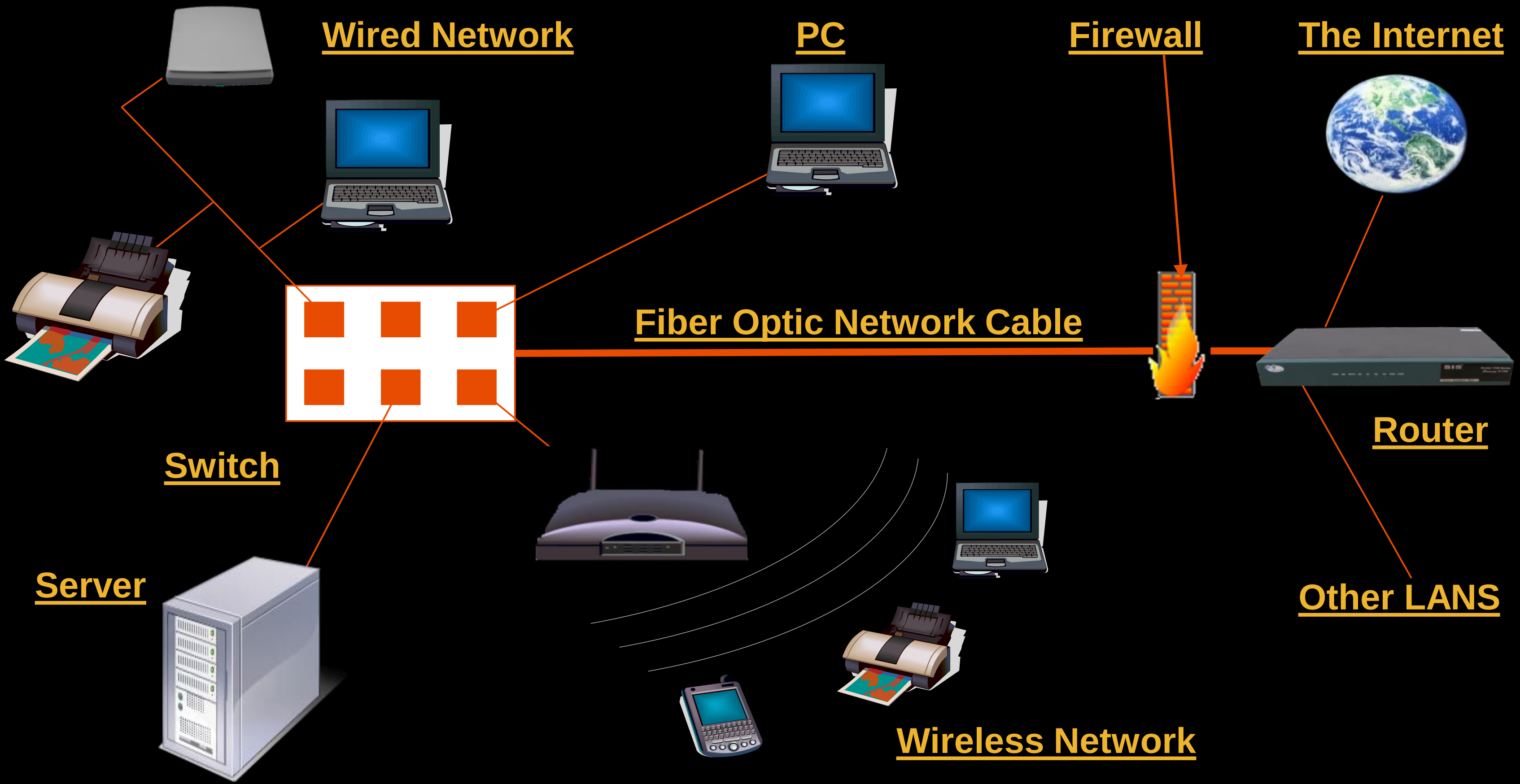
- Networks: Basic concepts
- Uses of networks in sharing of resources, Backups
- Common types of networks; LAN/WAN/Internet, Server based networks, client server model, P2P
- Network media
- Wireless networks.
- Threats to networks
- The internet world
- Cloud and Cloud Computing

The Computer Network

- A **computer network** is a group of computers/devices(Nodes) that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.
- The nodes of a computer network may include personal computers, servers, networking hardware, or other specialised or general-purpose hosts.
- The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless technologies.
- A communication protocol is a set of rules for exchanging information over a network.

The Network Diagram

(Click on the Words Below and Learn More About Each Component)



The Advantages/Uses of Network

Simultaneous Access

- ➢ There are moments in any business when several workers may need to use the same data at the same time.

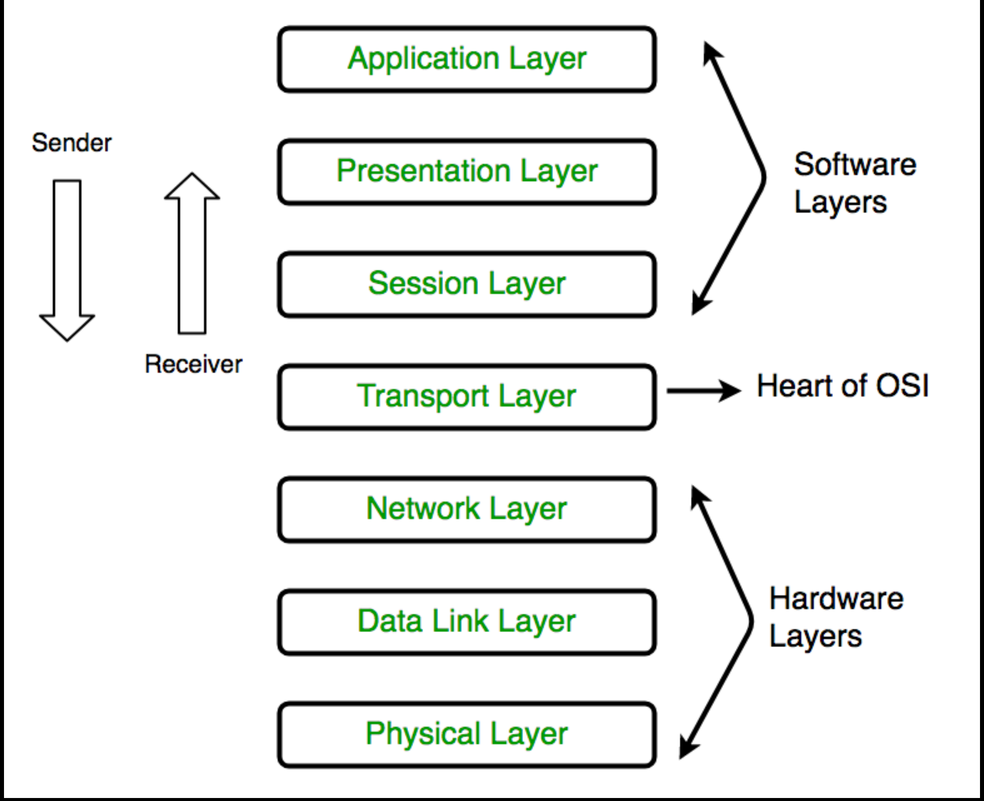
Shared Peripheral Devices

Personal Communications

- ➢ Videoconferencing
- ➢ Voice over Internet Protocol (VoIP):-VoIP transmits the sound of voice over a computer network using the Internet Protocol (IP) rather than sending the signal over traditional phone wires

Easier Data Backup

OSI MODEL



Sender

Receiver

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Software Layers

Heart of OSI

Hardware Layers

Physical Layer (Layer 1)

Responsible for the actual physical connection between the devices.

Functions of the physical layer are as follows:

Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.

Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

Hub, Repeater, Modem, Cables are Physical Layer devices

Data Link Layer (DLL) (Layer 2)

Responsible for node-to-node error-free delivery of the message.
Data Link Layer is divided into two sub layers:

Logical Link Control (LLC): controls the synchronization, flow control, and error-checking functions

Media Access Control (MAC): responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel.

Devices: Switch & Bridge are Data Link Layer devices

DL LAYER

The functions of the Data Link layer are :

Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

Physical addressing: After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.

Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames. Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.

Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

TRANSPORT LAYER

The functions of the Transport layer are:
The data in the transport layer is referred to as Segments
Devices of transport layer are Gateways and Firewalls

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the **End to End Delivery of the complete message**. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

TRANSPORT LAYER

At sender’s side: Transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Note: The sender needs to know the port number associated with the receiver’s application. Generally, this destination port number is configured, either by default or manually.

For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

TRANSPORT LAYER

At receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are as follows:

Segmentation and Reassembly: This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.

Service Point Addressing: In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

TRANSPORT LAYER

The services provided by the transport layer :

A. Connection-Oriented Service: It is a three-phase process that includes – Connection Establishment – Data Transfer – Termination / disconnection In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

B. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices.

Connection-oriented service is more reliable than connectionless Service.

** Data in the Transport Layer is called as Segments.*

*** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*

Transport Layer is called as Heart of OSI model.

NETWORK LAYER

Main Function is packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
Devices: Router and Layer 3 Switch. The sender & receiver's IP addresses are placed in the header by the network layer.

The functions of the Data Link layer are :
Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
Logical Addressing: In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

* Segment in Network layer is referred to as Packet.

SESSION LAYER

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.

The functions of the Data Link layer are :

Session establishment, maintenance, and termination: The layer allows the two processes to establish, use and terminate a connection.

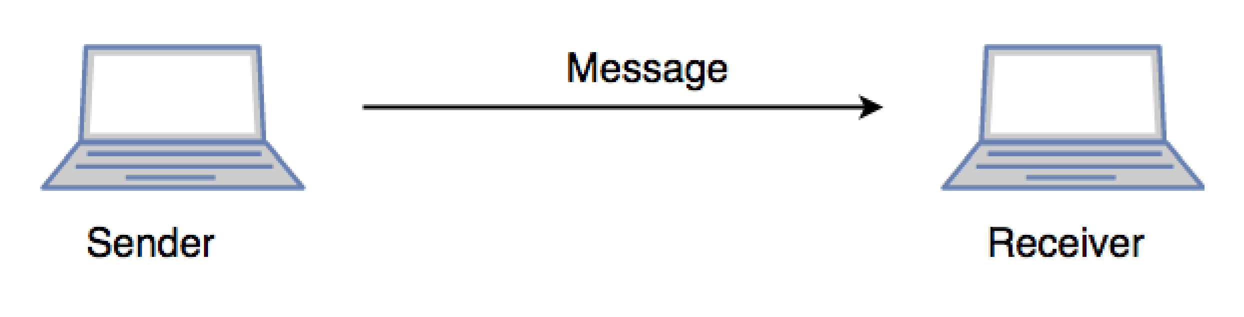
Synchronization: This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

SESSION LAYER

Scenario:

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0's and 1's) so that it can be transmitted.



PRESENTATION LAYER

The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network..

The functions of the Data Link layer are :

Translation: For example, ASCII to EBCDIC.

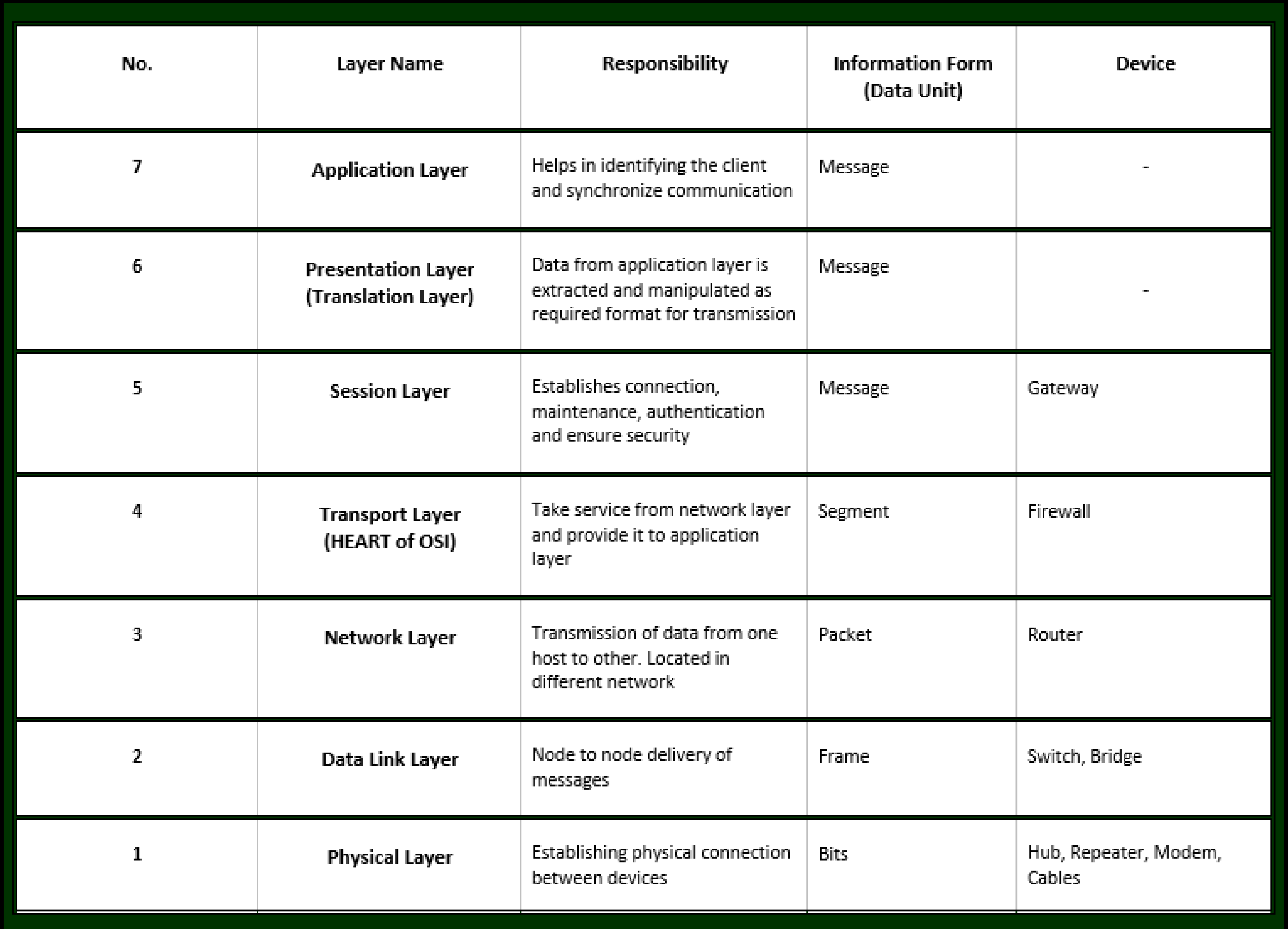
Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

Compression: Reduces the number of bits that need to be transmitted on the network.

APPLICATION LAYER

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Example: Application – Browsers, Skype Messenger, etc. **Application Layer is also called Desktop Layer.

OSI MODEL



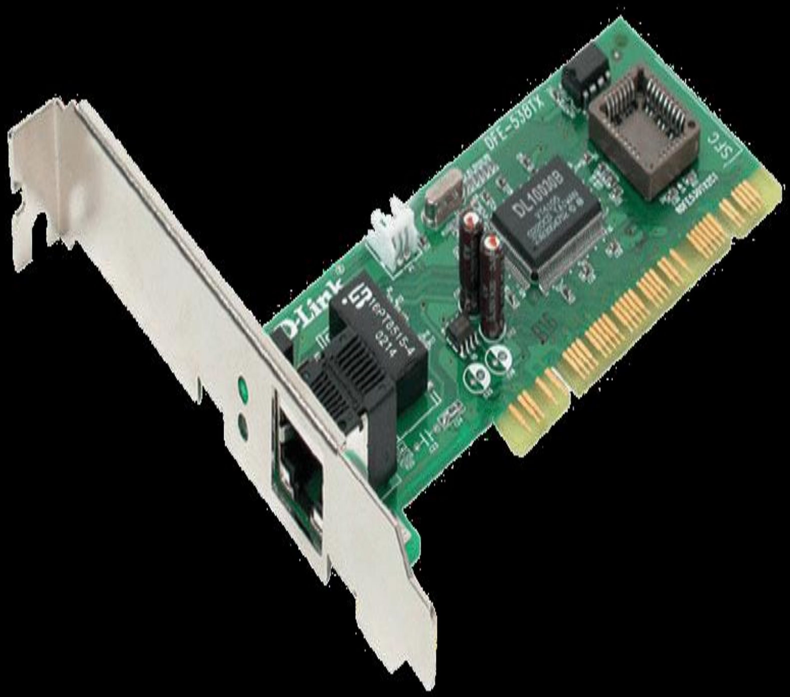
No.	Layer Name	Responsibility	Information Form (Data Unit)	Device
7	**Application Layer**	Helps in identifying the client and synchronize communication	Message	-
6	**Presentation Layer (Translation Layer)**	Data from application layer is extracted and manipulated as required format for transmission	Message	-
5	**Session Layer**	Establishes connection, maintenance, authentication and ensure security	Message	Gateway
4	**Transport Layer (HEART of OSI)**	Take service from network layer and provide it to application layer	Segment	Firewall
3	**Network Layer**	Transmission of data from one host to other. Located in different network	Packet	Router
2	**Data Link Layer**	Node to node delivery of messages	Frame	Switch, Bridge
1	**Physical Layer**	Establishing physical connection between devices	Bits	Hub, Repeater, Modem, Cables

The Networking Devices(Nodes)

1. NIC Card
2. Repeater
3. Hub
4. Switch
5. Bridge
6. Router
7. Gateway
8. Firewall

1. Network Interface Card

- NIC is used to physically connect host devices to the network media.
- A NIC is a printed circuit board that fits into the expansion slot of a bus on a computer motherboard.
- It can also be a peripheral device. NICs are sometimes called network adapters.
- Each NIC is identified by a unique code called a Media Access Control (MAC) address.
- This address is used to control data communication for the host on the network.

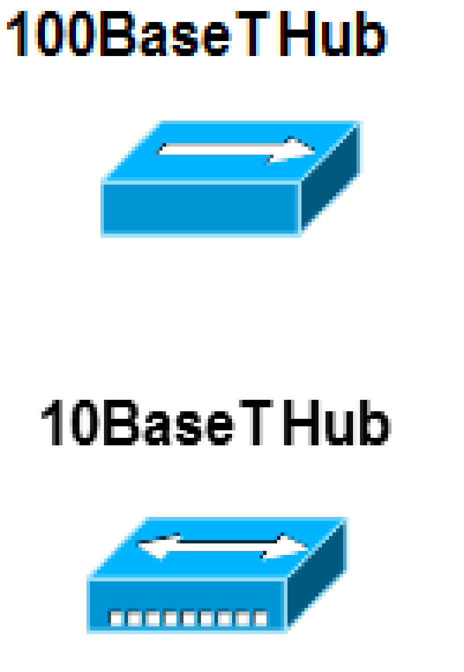


2. Repeaters

- A repeater is a network device used to regenerate a signal.
- Repeaters regenerate analog or digital signals that are distorted by transmission loss due to attenuation.
- A repeater does not make an intelligent decision concerning forwarding packets

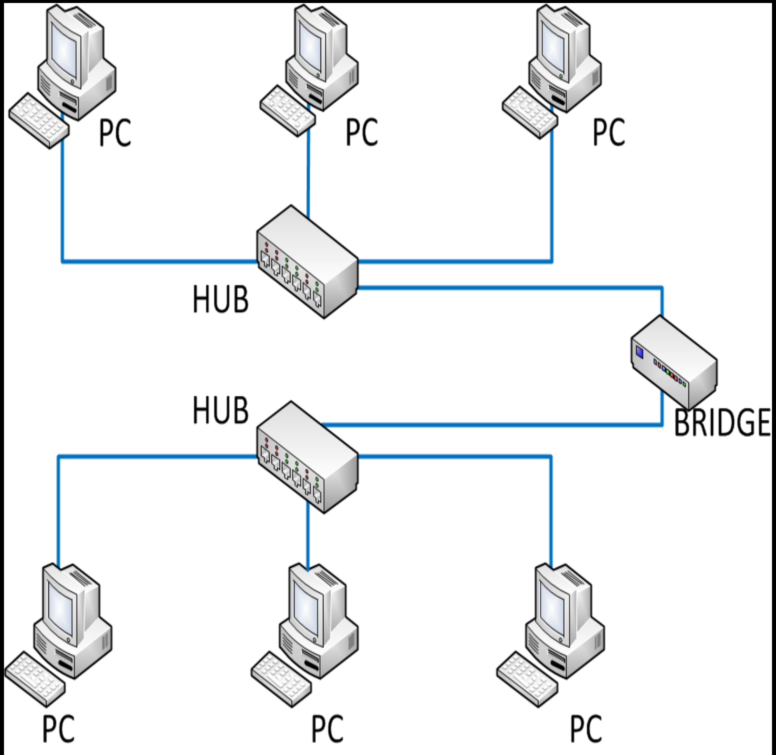
3. Hubs

- Hubs concentrate on connections.
- In other words, they take a group of hosts and allow the network to see them as a single unit. This is done passively, without any other effect on the data transmission.
- Active hubs concentrate hosts and also regenerate signals.



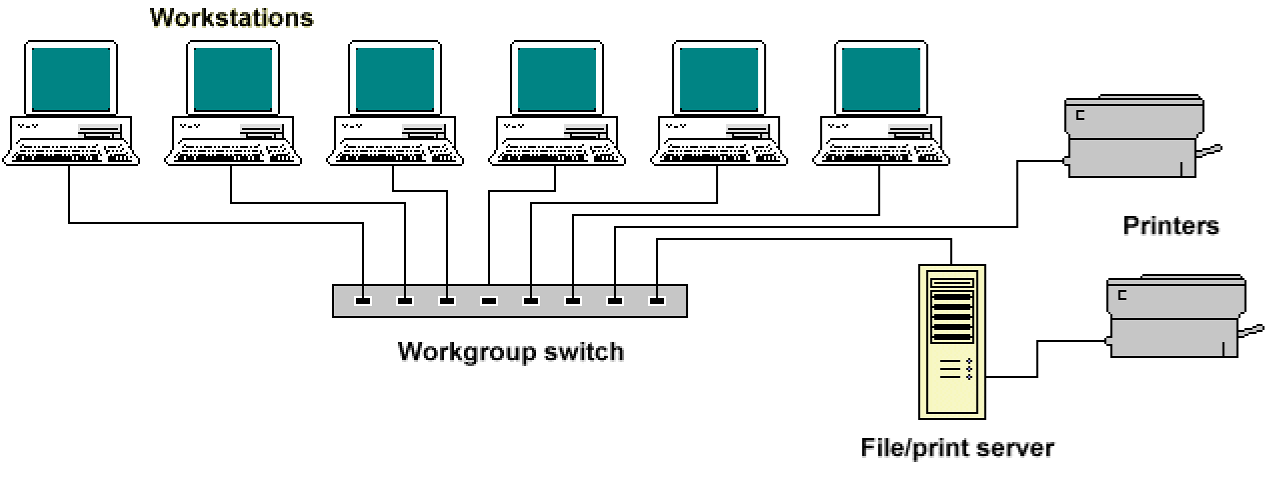
4. Bridges

- Bridges convert network data formats and perform basic data transmission management.
- Bridges provide connections between LANs.
- They also check data to determine if it should cross the bridge. This makes each part of the network more efficient



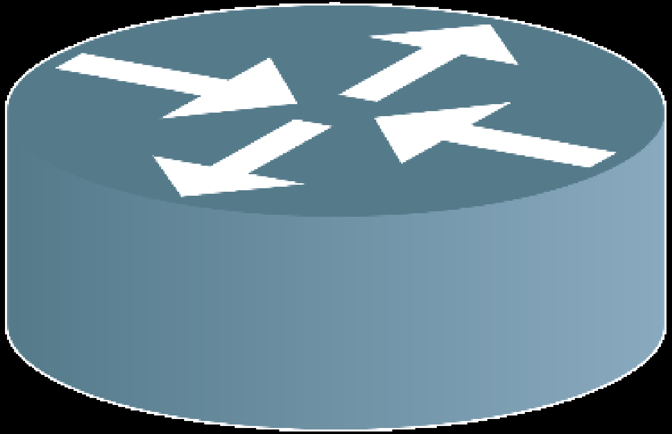
5. Switches

- Switches add more intelligence to data transfer management.
- They can determine if data should remain on a LAN and transfer data only to the connection that needs it.
- Another difference between a bridge and switch is that a switch does not convert data transmission formats



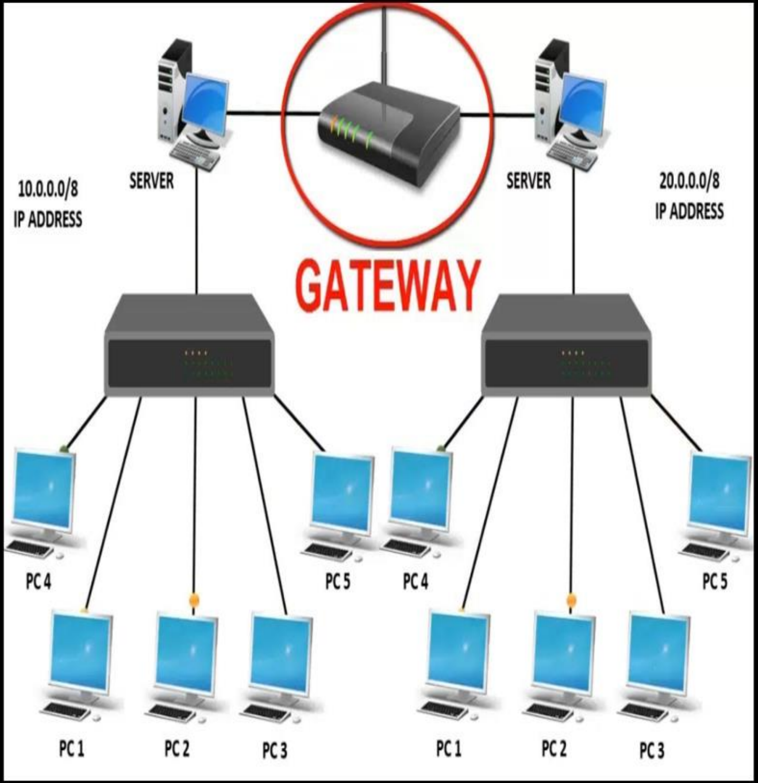
6. Routers

- Routers have all the capabilities listed above.
- Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers.
- They can also connect to a WAN, which allows them to connect LANs that are separated by great distances.



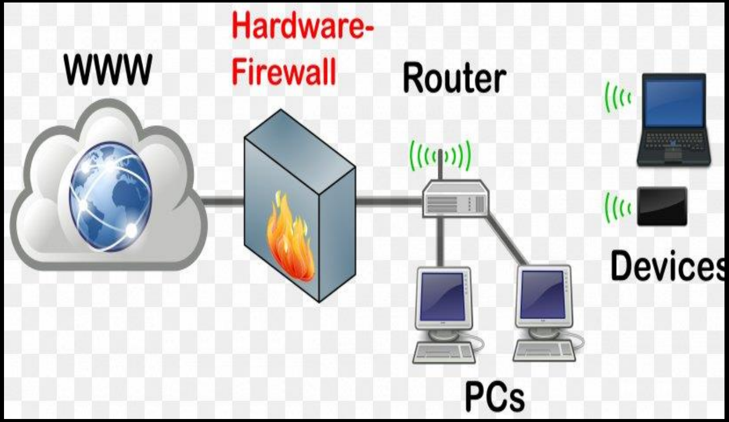
7. Gateway

- A **gateway** is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
- Gateways are distinct from routers or switches in that they communicate using more than one protocol to connect a bunch of networks



8. Firewall

- A firewall is a network device or software for controlling network security and access rules.
- Firewalls are inserted in connections between secure internal networks and potentially insecure external networks such as the Internet.
- Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones.
- The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.



Network Media

The **function of the media is to carry a flow of information through a** LAN**.**

A. Wired Media:- widely adopted *family* that uses copper and fiber media in <u>local area network</u> (LAN) technology are collectively known as <u>Ethernet</u>

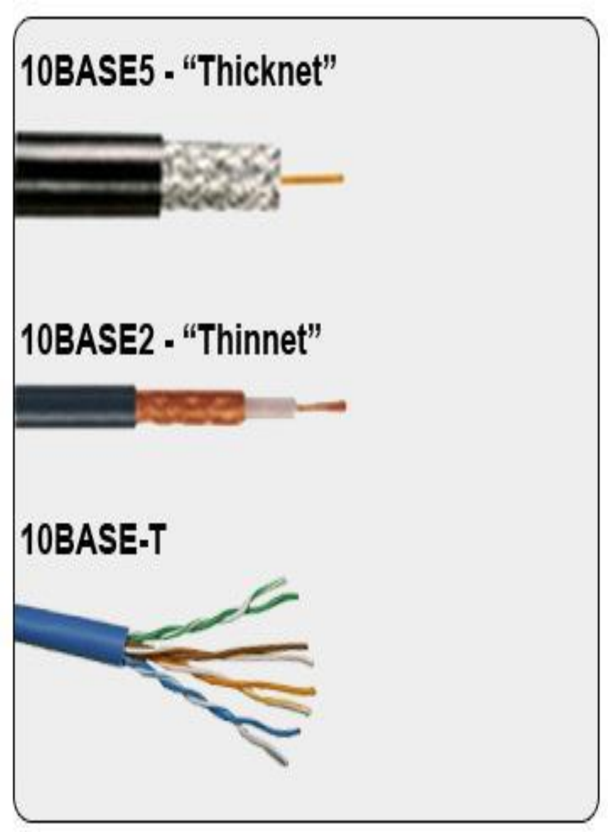
   1. Copper Cable
      a. Coaxial Cables
      b. Shielded Twisted Pair(STP)
      c. Unshielded Twisted Pair

   2. Fibre Optic Cable

B. Wireless Media:- use the atmosphere, or space, as the medium.

1. Copper Cable

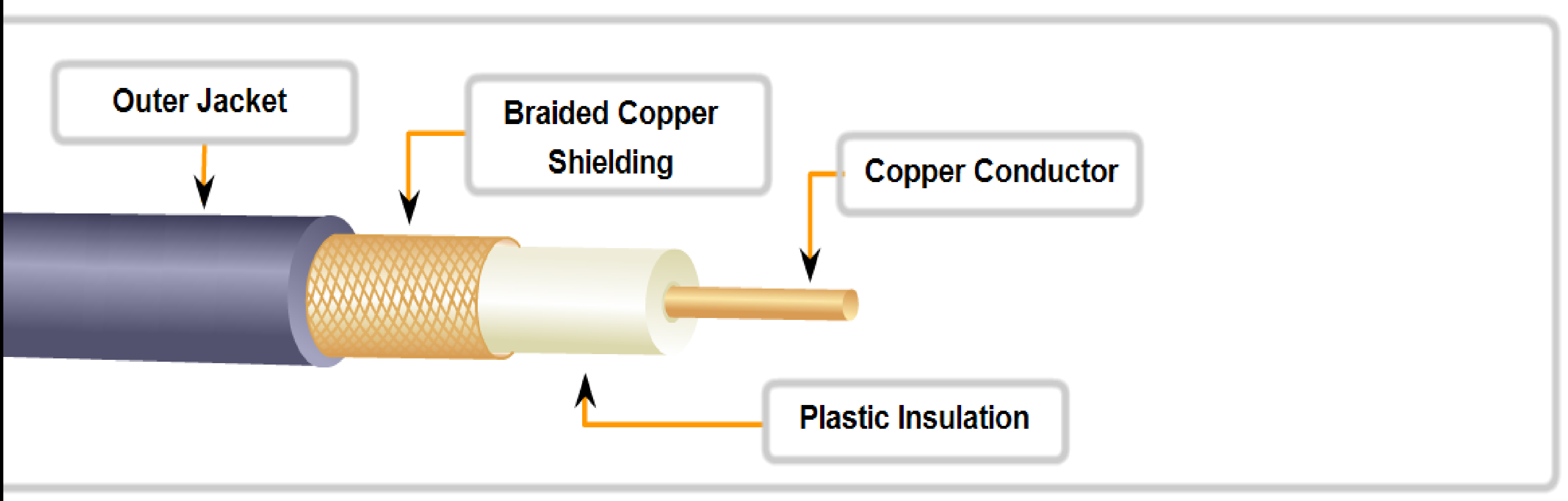
- The most common, easiest, quickest, and cheapest form of network media to install.
- The disadvantage of sending data over copper wire is that the further the signal travels, the weaker it becomes.



a. Coaxial Cable

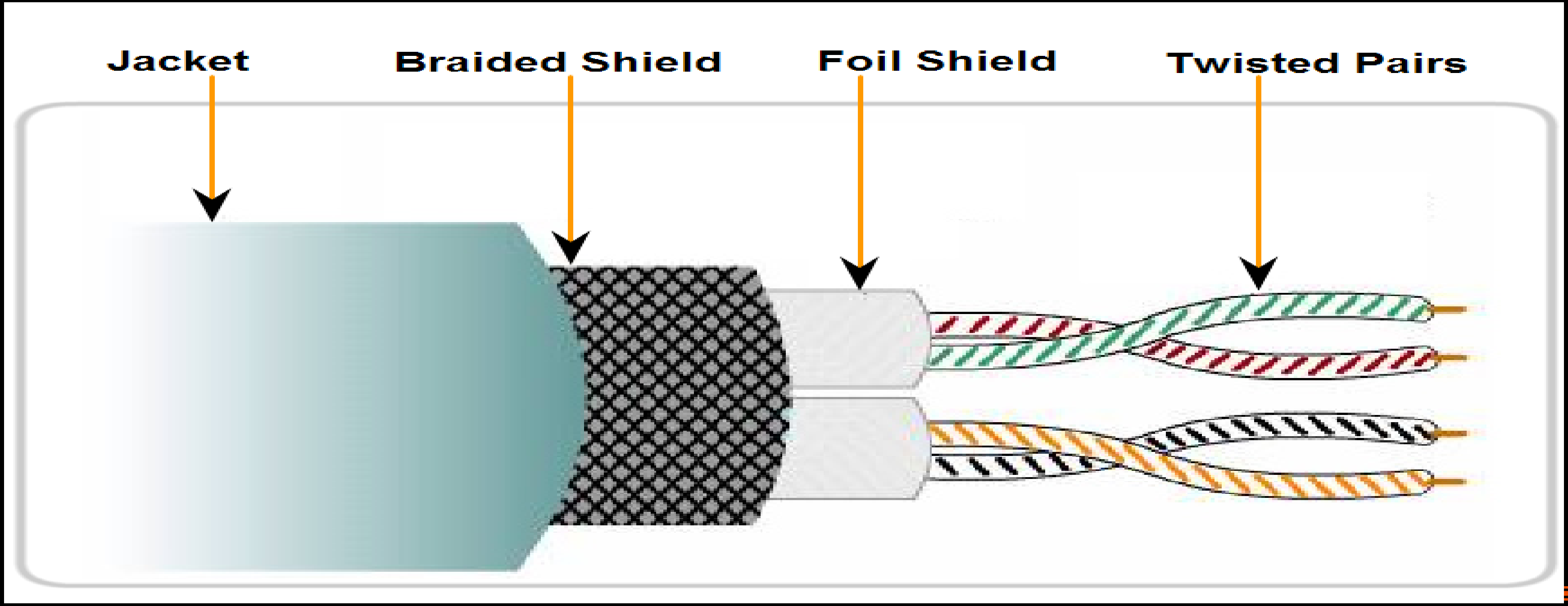
➢ It can be run longer distances than Twisted pair Cables.

- Speed: 10-100Mbps
- Cost: Inexpensive
- Media and connector size: Medium
- Maximum cable length: 500m



b. Shielded Twisted Pair(STP)

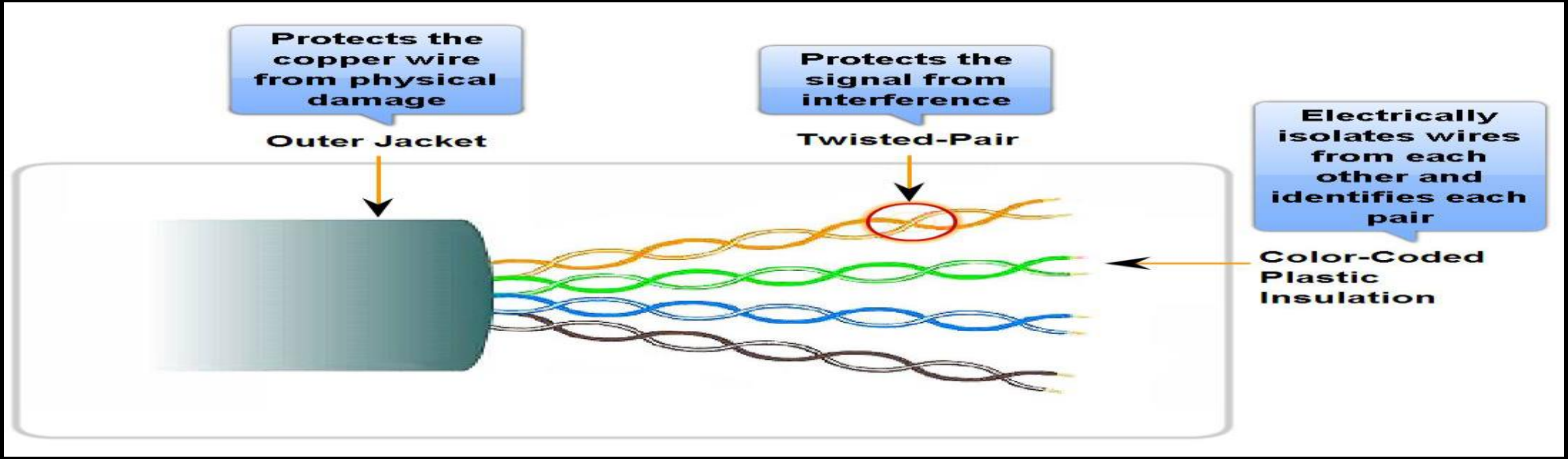
- Speed: 0-100Mbps
- Cost: Moderate
- Media and connector size: Medium to large
- Maximum cable length: 100m



c. Unshielded Twisted Pair

- UTP is a four-pair wire medium used in a variety of networks.
- Each of the eight copper wires in the UTP cable is covered by insulating material

Speed: 10-100-1000 Mbps*
Cost: Least Expensive
Media and connector size: Small
Maximum cable length: 100m * (Depending on the quality/category of cable)


Protects the copper wire from physical damage
Outer Jacket
Protects the signal from interference
Twisted-Pair
Electrically isolates wires from each other and identifies each pair
Color-Coded Plastic Insulation

UTP Implementation

- EIA/TIA specifies an RJ-45 connector for UTP cable.
- The letters RJ stand for registered jack.

Fiber Optic Cable

- Glass fiber carrying light pulses, each pulse a bit.
- Based on the Total Internal Reflection of Light.
- High-speed point-to-point transmission 10-100’s Gbps
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise

Communication Protocols

Internet Protocol Suite

- ➢ Also called TCP/IP, is the foundation of all modern networking.
- ➢ It defines the addressing, identification, and routing specifications for IPv4 and for IPv6.
- ➢ It is the defining set of protocols for the Internet.

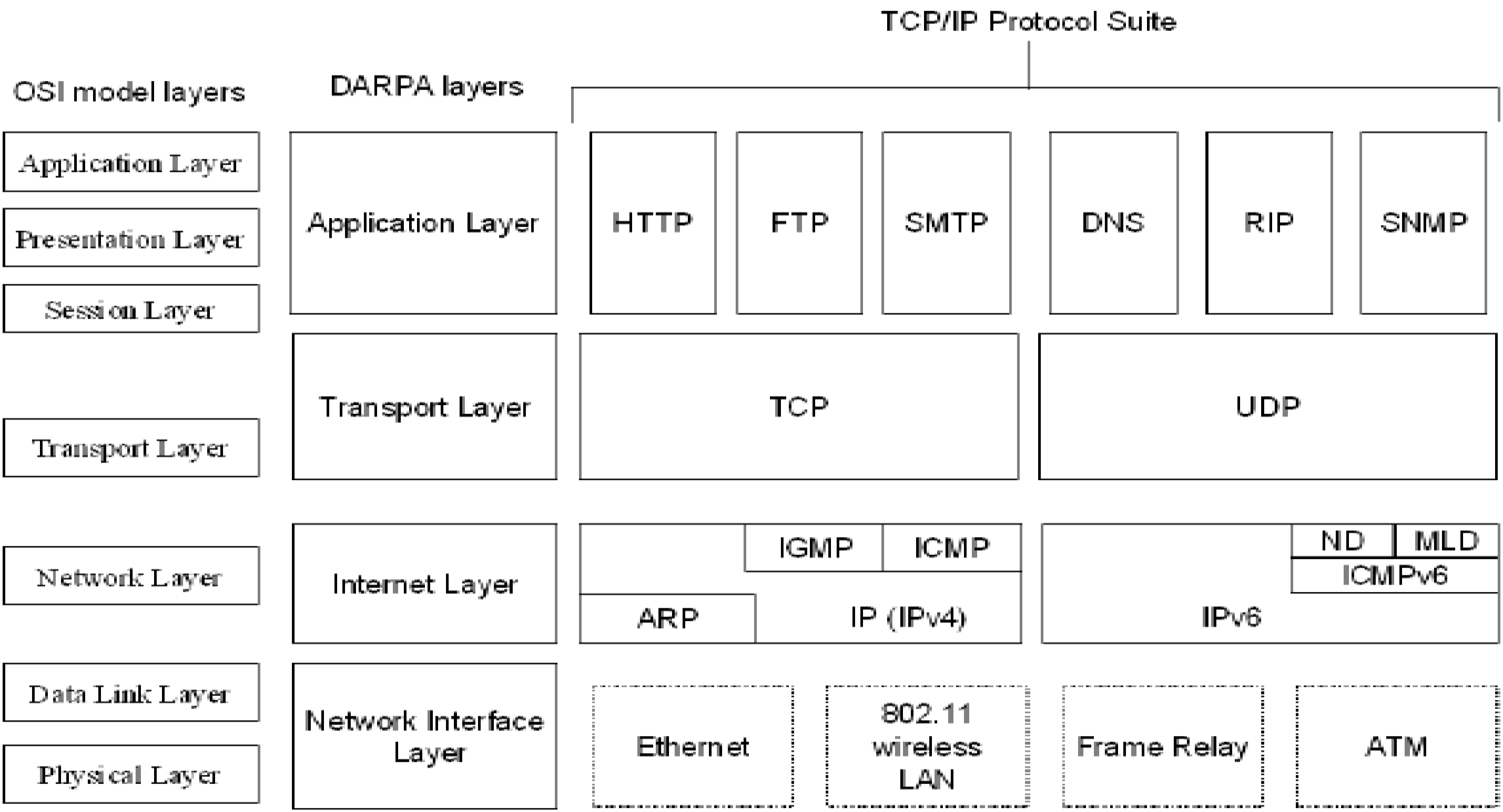
IEEE 802

- ➢ It is a family of IEEE standards dealing with local area networks and metropolitan area networks.
- ➢ They operate mostly at levels 1 and 2 of the OSI model.

Ethernet

- ➢ It is a family of protocols used in wired LANs, described by a set of standards together called IEEE 802.3

TCP/IP Protocol Suite



TCP/IP Protocol Suite

OSI model layers

DARPA layers

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Application Layer

Transport Layer

Internet Layer

Network Interface Layer

HTTP

FTP

SMTP

DNS

RIP

SNMP

TCP

UDP

IGMP

ICMP

ARP

IP (IPv4)

ND

MLD

ICMPv6

IPv6

Ethernet

802.11 wireless LAN

Frame Relay

ATM

Communication Protocols

Wireless LAN

- It is standardized by IEEE 802.11 and shares many properties with wired Ethernet.

SONET/SDH

- Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical Fibre using lasers.

Asynchronous Transfer Mode(ATM)

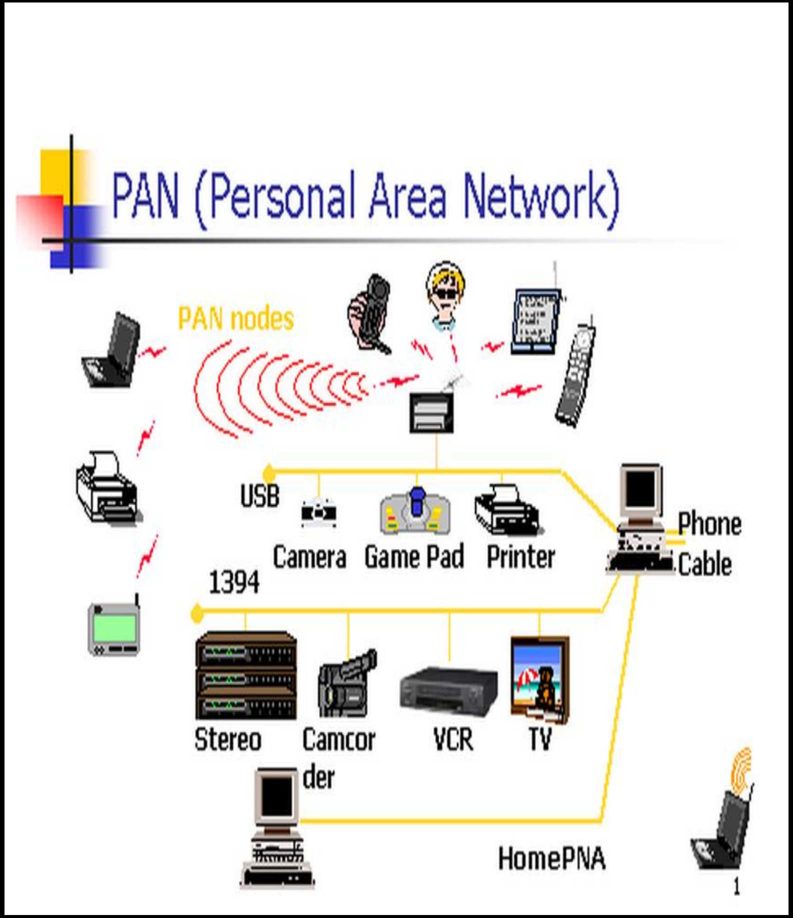
- It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells.
- Good choice for a network that handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video.

Types of Networks

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Campus Area Network (CAN)
4. Metropolitan Area Network (MAN)
5. Wide Area Network (WAN)
6. Storage-Area Network (SAN)
7. Virtual Private Network (VPN)
8. Client Server Network
9. Peer to Peer Network (P2P)

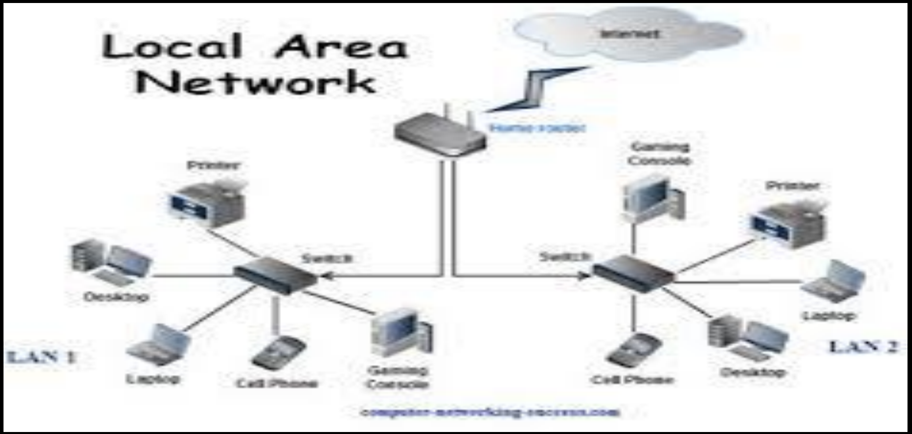
1. Personal Area Network

1. Personal Area Network (PAN) is a computer network used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants.
2. **Also Known as HAN (Home Area Network)**
3. PANs can be used for communication amongst the personal devices themselves (interpersonal communication), or for connecting to a higher level network and the Internet (an uplink) where one "master" device takes up the role as internet router.



2. Local Area Network

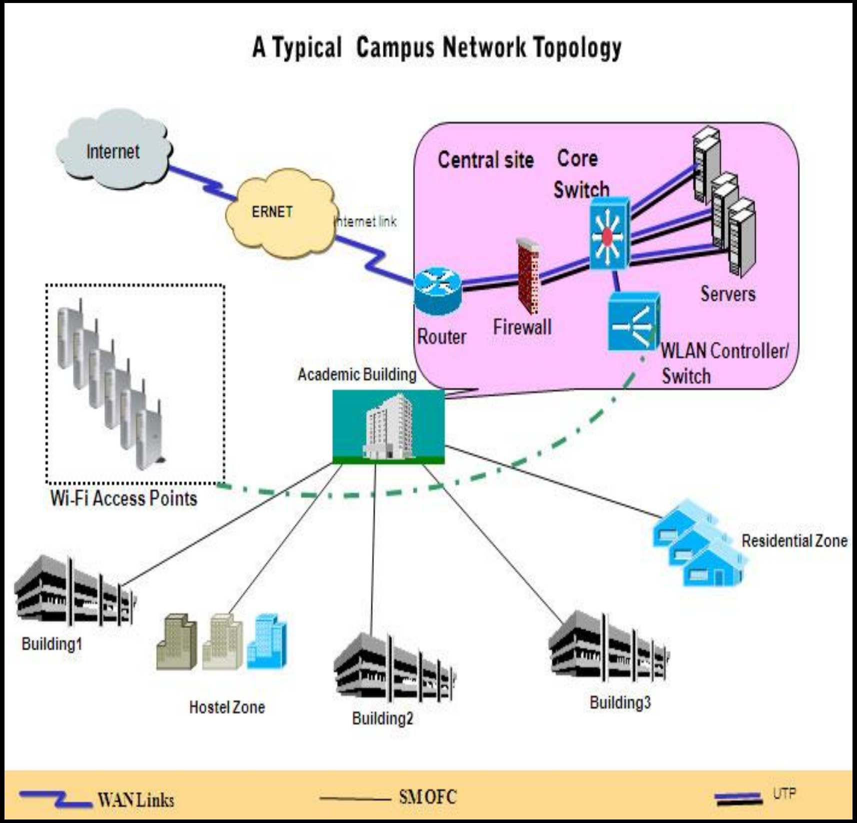
- Xerox Corporation worked in collaboration with DEC and Intel to create Ethernet, which is the most pervasive LAN architecture used today.
- Ethernet has evolved and has seen significant improvements in regard to speed and efficiency.



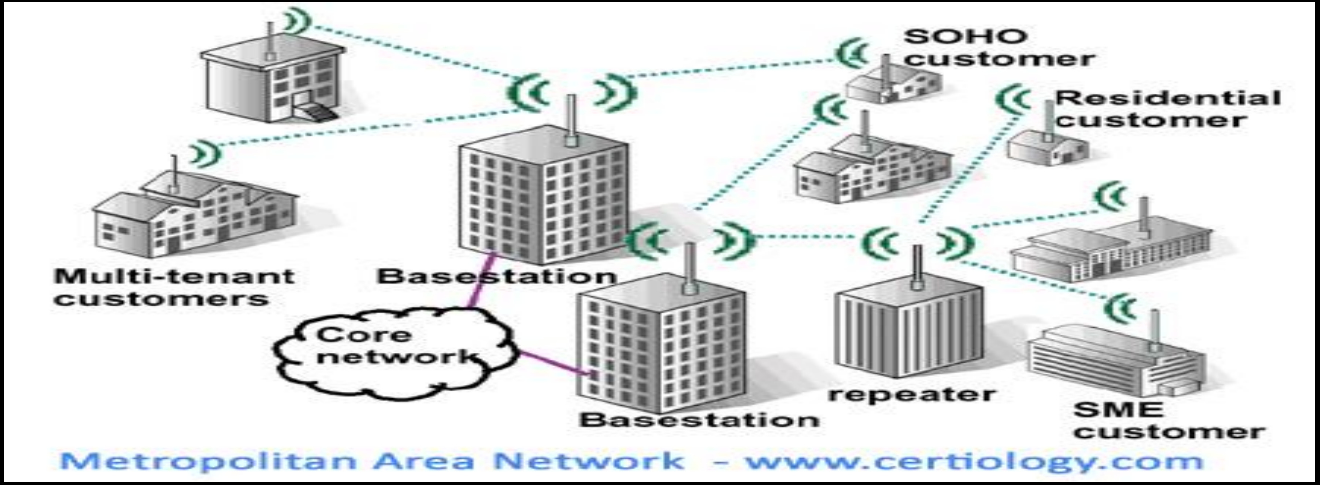
- An upside of a LAN is fast data transfer with data speed that can reach up to 10Gbps.
- Other significant LAN technologies are Fiber Distributed Data Interface (FDDI) and token ring.

3. Campus Area Network

- Larger than LANs, but smaller than metropolitan area networks these types of networks are typically seen in universities, large K-12 school districts or small businesses.
- They can be spread across several buildings that are fairly close to each other so users can share resources



4. Metropolitan Area Network



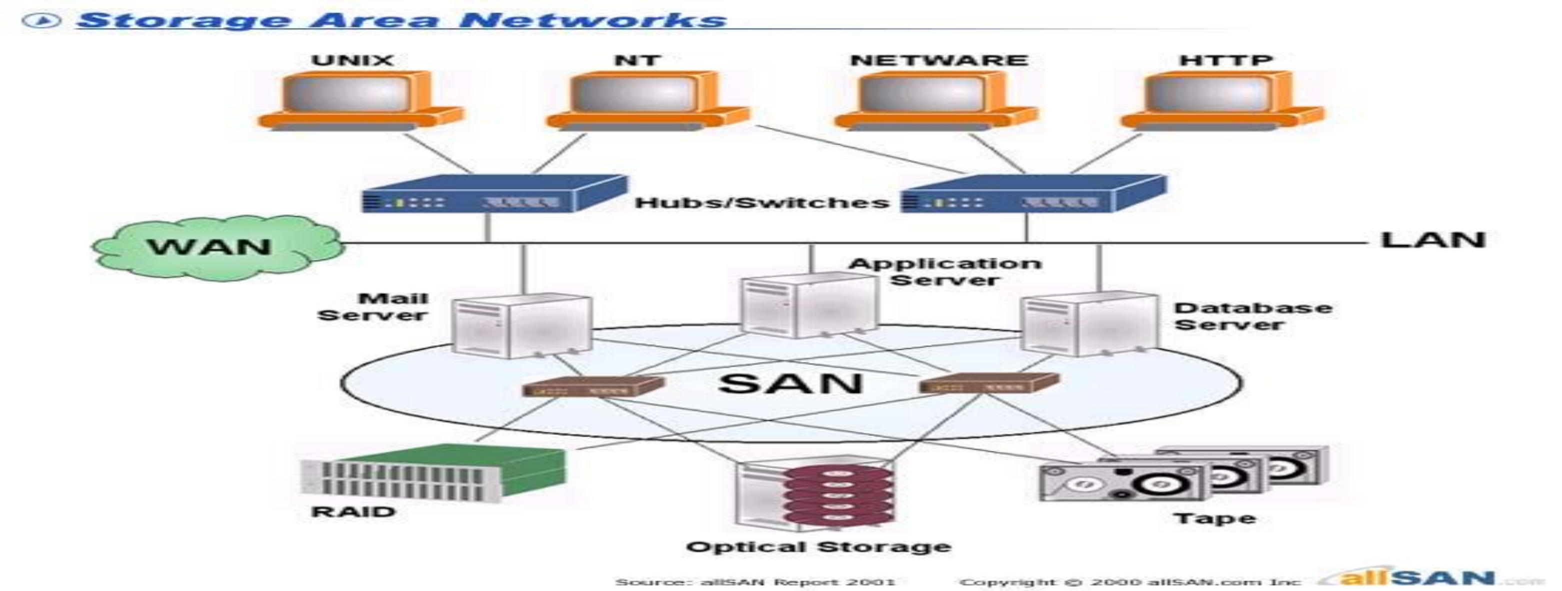
1. A MAN is larger than a LAN but smaller than or equal in size to a WAN.
2. The size range anywhere from 5 to 50km in diameter.
3. MANs are typically owned and managed by a single entity.
4. This could be an ISP or telecommunications company that sells its services to end-users in that metropolitan area.
5. For all intents and purposes, a MAN has the same characteristics as a WAN with distance constraints.

5. Wide Area Network

- A Wide Area Network exist over a large area
- Data travels through telephone or cable lines
- Usually requires a Modem
- The world’s largest Wide Area Network in the Internet

6. Storage Area Network

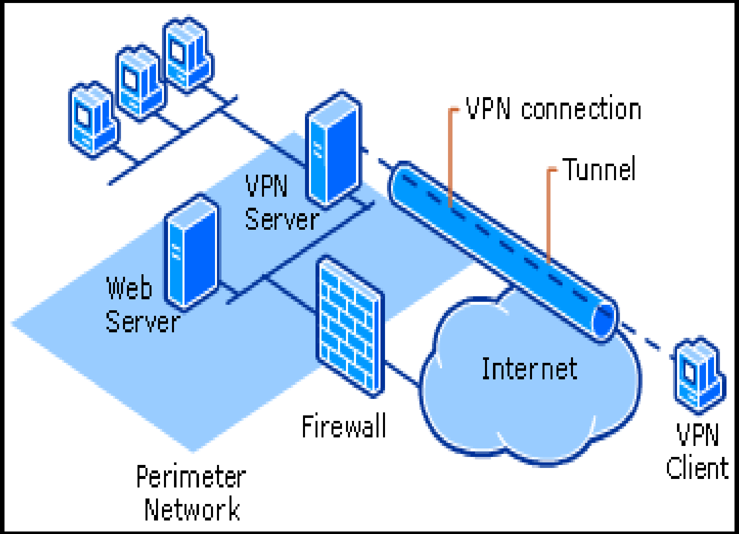
- SAN may be referred to as a Sub network or special purpose network.
- Its special purpose is to allow users on a larger network to connect various data storage devices with clusters of data servers.
- SANs can be accessed in the same fashion as a drive attached to a server.



Source: allSAN Report 2001 Copyright © 2000 allSAN.com Inc

7. Virtual Private Network

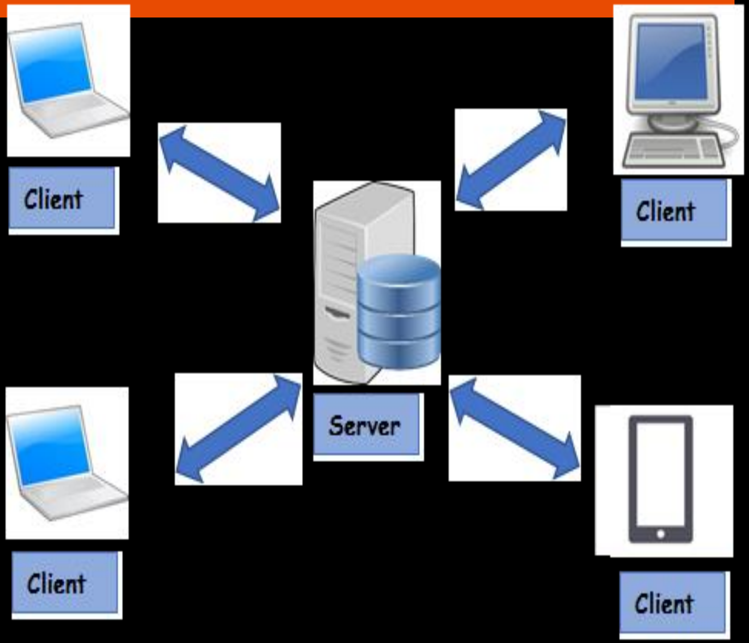
- VPN is a private network that can access public networks remotely. VPN uses encryption and security protocols to retain privacy while it accesses outside resources.
- When employed on a network, VPN enables an end user to create a virtual tunnel to a remote location. Typically, telecommuters use VPN to log in to their company networks from home.



- ***Authentication*** is provided to validate the identities of the two peers.
- ***Confidentiality*** provides encryption of the data to keep it private from prying eyes.
- ***Integrity*** is used to ensure that the data sent between the two devices or sites has not been tampered with.

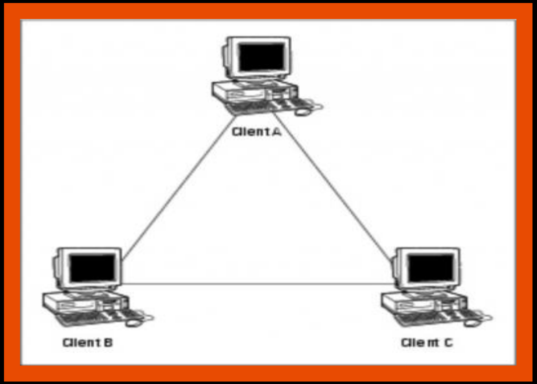
8. Client/Server Network

- In a client/server arrangement, network services are located on a dedicated computer called a server.
- The server responds to the requests of clients.
- The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services.



- Most network operating systems adopt the form of a client/server relationship.
- Typically, desktop computers function as clients, and one or more computers with additional processing power, memory, and specialized software function as servers.

9. Peer to Peer Network



- Usually very small networks
- Each workstation has equivalent capabilities and responsibilities
- Does not require a switch or a hub.
- These types of networks do not perform well under heavy data loads.

Network Topologies

Network topology defines the structure of the network.

A. **Physical topology**:- It define the actual layout of the wire or media.

   1. Bus
   2. Ring
   3. Star
   4. Tree(Hierarchical)
   5. Mesh

B. **Logical topology:-** It defines how the hosts access the media to send data.

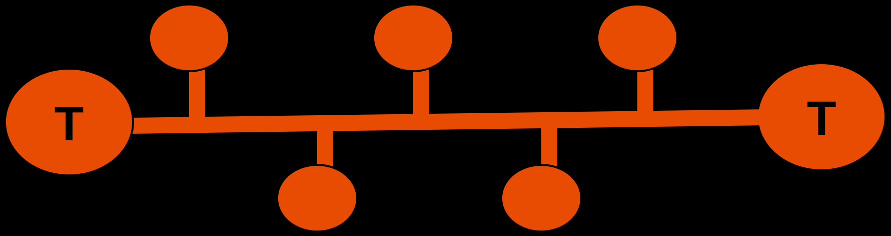
   1. Broadcast
   2. Token passing

C. **Hybrid Topology**

1. Bus Topology

All devices are connected to a central cable, called bus or backbone.

There are terminators at each end of the bus that stops the signal and keeps it from traveling backwards.



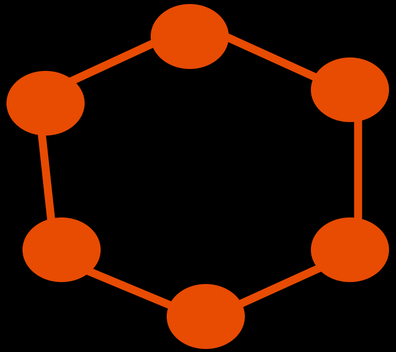
Advantages:

1. There is no central controller.
2. Control resides in each station
3. The less interconnecting wire is required.
4. Ease of installation.
5. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths

Disadvantages:

1. It is possible that more than one station may attempt transmission simultaneously (collision or contention).
2. Difficult reconfiguration and fault isolation.
3. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.
4. The damaged area reflects signals in the direction of origin, creating noise in both directions

2. Ring Topology



- **All devices are connected to one another in the shape of a closed loop.**
- **Each device is connected directly to two other devices, one on either side of it.**

Advantages:

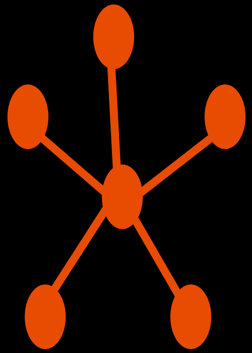
1. Avoids the collisions that are possible in the bus topology.
2. Each pair of stations has a point-to-point connection.
3. A signal is passed along the ring in one direction, from device to another, until it reaches its destination.
4. Each device incorporates a repeater.
5. Relatively easy to install and reconfigure.
6. Fault isolation is simplified.

Disadvantages:

1. A break in the ring (such as station disabled) can disable the entire network.
2. Unidirectional traffic.

3. Star Topology

- All devices are connected to a central hub.
- Nodes communicate across the network by passing data through the hub or switch.



Advantages:

1. Easy to install and reconfigure.

2. Robustness, if one link fails; only that link is affected. All other links remain active.

3. Easy fault identification and isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:

1. The devices are not linked to each other.

2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.

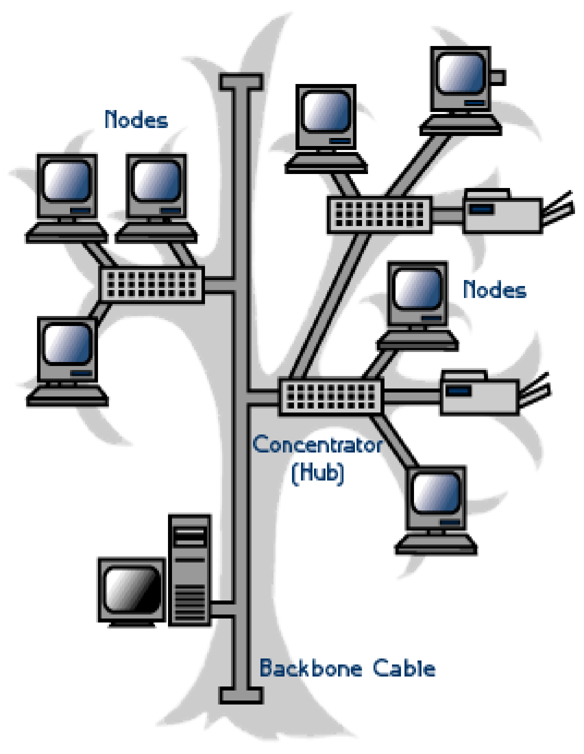
4. Tree/Hierarchical Topology

Advantages:

1. It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
2. It allows the network to isolate and prioritize communications from different computers.

Disadvantages:

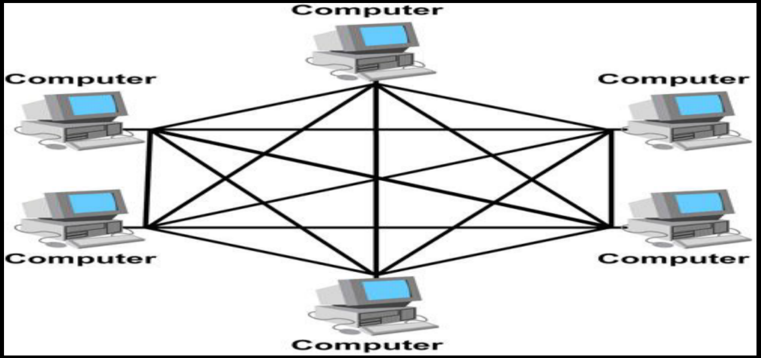
1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.
3. The addition of secondary hubs brings two further advantages.



6. Mesh Topology

Each host has its connections to all other hosts. Mesh topology is implemented to provide as much protection as possible from interruption of service.

1. A nuclear power plant might use a mesh topology in the networked control systems.
2. Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.



Advantages:
1. The use of dedicated links guarantees that each connection can carry its data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. It is robust, if one link becomes unusable, it does not incapacitate (affect) the entire system.
3. Privacy and Security (every message sent travels along a dedicated line; only the intended recipient sees it).
4. Point-to-point links make fault identification and fault isolation easy.

Disadvantages:
1. A large amount of cabling required.
2. A large amount of I/O ports required.
3. Installation and reconfiguration are difficult.
4. The sheer bulk of the wiring can be greater than the available space (in the walls, ceiling, or floors) can accommodate.
5. The hardware required to connect each link (I/O ports and cables) can be prohibitively expensive.

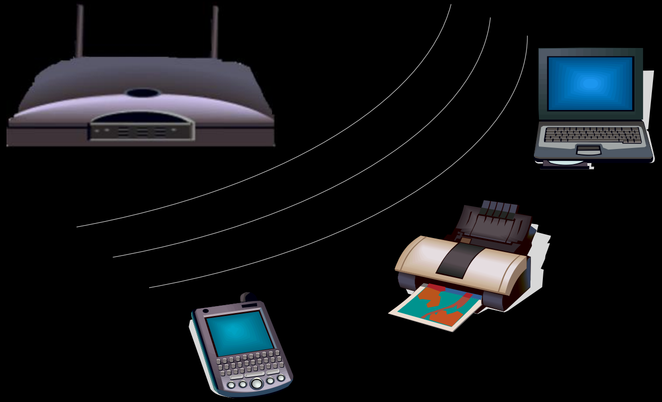
Wireless Networks

Wireless network is a type of computer network that uses wireless data connections for connecting network nodes.

Example

Bluetooth

Wi-Fi

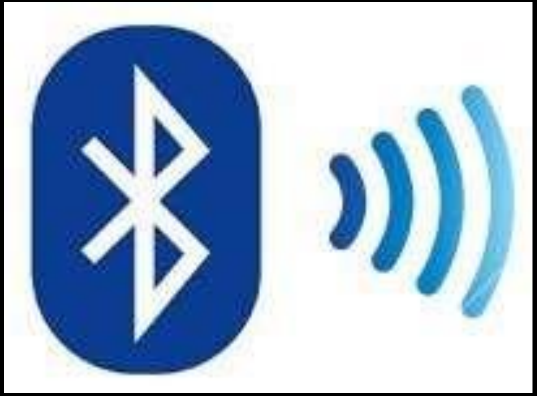


Bluetooth

- **Bluetooth** is a short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances.

- It is using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz.

- The IEEE standardized Bluetooth as **IEEE 802.15.1**, but no longer maintains the standard.



Wi-Fi

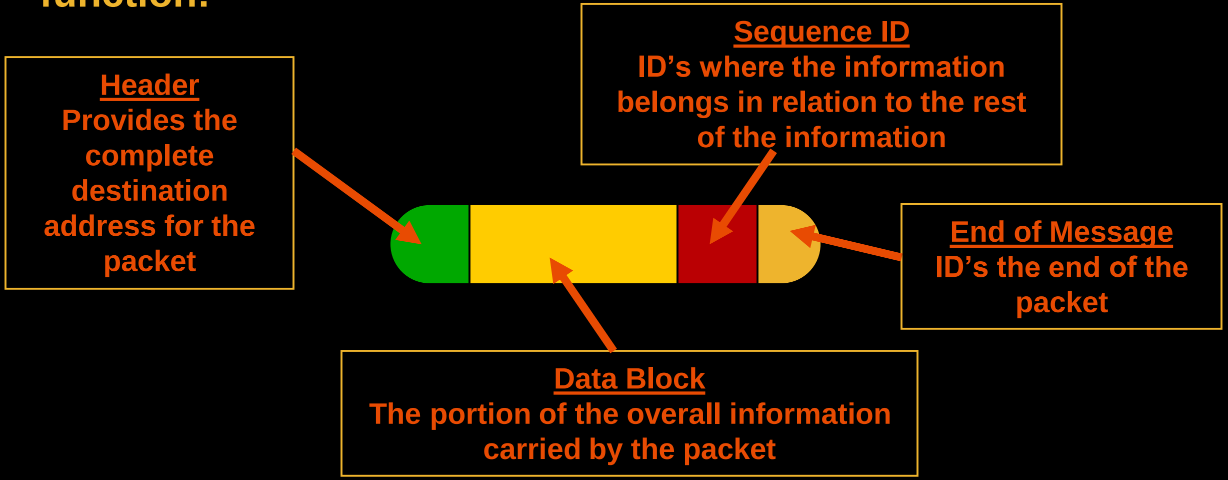
- Wi-Fi Stands for Wireless Fidelity.
- **Wi-Fi**, is a Local Area Wireless technology.
- Wi-Fi networks use radio technologies to transmit and receive data at high speed.
- It is based on the IEEE 802.11 family of standards.
- **Access point:** The access point is a wireless LAN transceiver or " base station" that can connect one or many wireless devices simultaneously to the internet

The Internet

The simplest definition of the Internet is that it's a network of computer networks

How Information Travel Through the Internet

A page on the Internet—whether it's full of words, images or both—doesn't come to you in one shipment. It's translated into digital information, chopped into 1500 byte pieces called PACKETS, and sent to you like a puzzle that needs to be reassembled. Each part of the packet has a specific function:



Header
Provides the complete destination address for the packet

Sequence ID
ID's where the information belongs in relation to the rest of the information

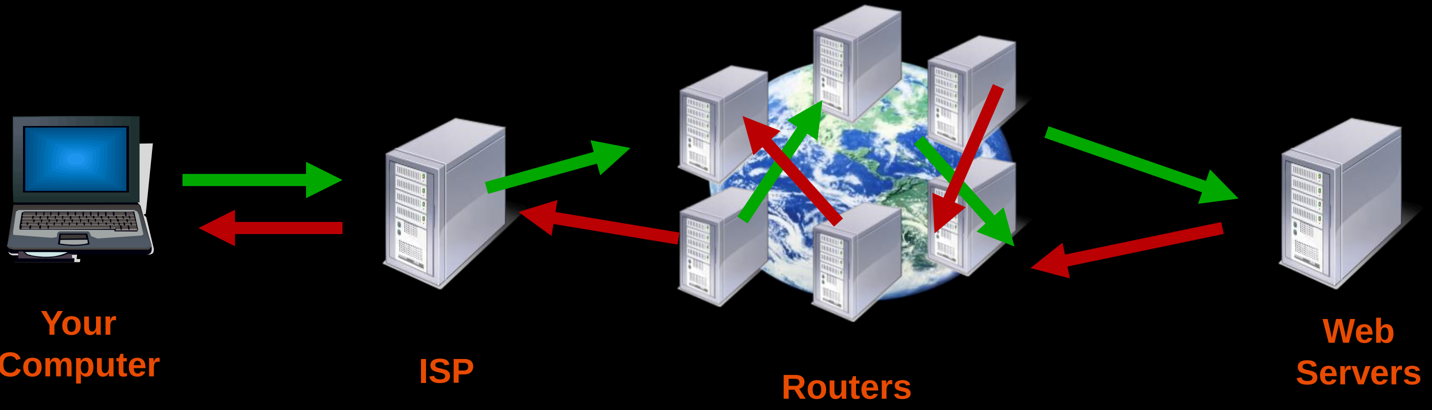
End of Message
ID's the end of the packet

Data Block
The portion of the overall information carried by the packet

The Internet

How Information Travel Through the Internet

When you connect to a Web site through an ISP and start exchanging information, there isn't a fixed connection between your computer and the Web server computer hosting the Web site. Instead, information is exchanged using the best possible path at that particular time. Special computers called routers determine these paths, avoiding slow links and favoring fast ones.



What are Malware, Viruses, Spyware, and Cookies?

Malware: Malware" is short for malicious software

A program which is designed to damage your computer it may be a virus, worm or Trojan.

Virus: Malware that replicate itself to harm your computer

Spyware: A programme installed with or without your permission to steal your data

Worms: Replicates to use resources

Adware: Show adds based on user search criteria

Trojan: Destructive programme hidden behind a genuine programme

Ransomware: Demands money

Cookies: Store users information for fast processing.

How to handle: Best solution is ------------

Data security and cryptography