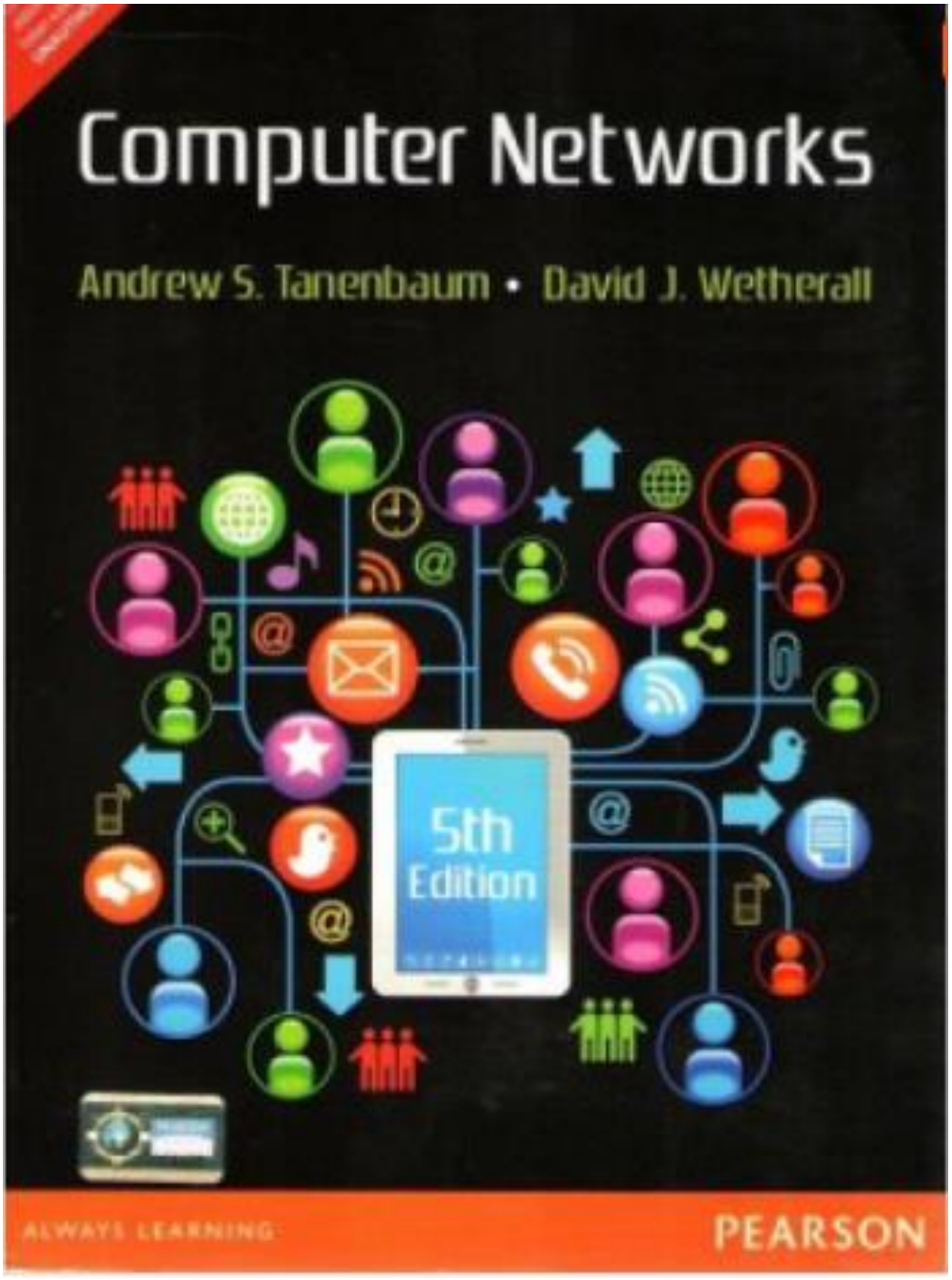
COMPUTER NETWORKS

16SCCCS6



STUDY MATERIAL PREPARED BY,

Prof. A. NARAYANAN., M.Sc., M.Phil.,
ASSISTANT OF COMPUTER SCIENCE,
SWAMI DAYANANDA COLLEGE OF ARTS & SCIENCE,
MANJAKKUDI.

COMPUTER NETWORKS

Objective: To understand the Design and Organization of Computer Networks

Unit I:

Overview and Physical Layer: Introduction: Data Communications - Networks - Network Types, Network Models: TCP/IP Protocol Suite- The OSI Model, Bandwidth utilization : Multiplexing- Spread Spectrum, Transmission Media: Guided Media-Unguided Media, Switching: Circuit Switched Network-Packet Switching-Structure of a switch.

Unit II:

DataLinkLayer: Error Deduction and Correction : Introduction- Cyclic codes Forward error correction, Data link Control: Data link layer protocols- Media Access Control: Random Access-Controlled Access, Wireless Networks: IEEE 802.11- Bluetooth-Cellular Telephone- Satellite network-Connection devices,

Unit III:

Network Layer Services : Packet Switching- Network layer performance- IPV4 Addresses-Internet Protocol-Routing Algorithms - IPV6 Addressing

Unit IV:

Transport Layer : Transport Layer Protocols- User Datagram Protocol - TCP:TCP Services TCP features - Windows in TCP - Flow Control - Error Control- TCP Congestion Control - TCP timers

Unit V:

Application Layers : Client Server Programming - Word Wide Web & HTTP - FTP - Email - DNS

Text Book:

1. Data Communications and Networking, Behrouz A Forouzan, Tata McGraw Hill, Fifth Edison, 2013
Reference Book: 1. Data Communications and Networks, Achyut Godbole and Atul Kahate, McGraw Hill Education, 2011 *

UNIT - I

What is Network?

- A system of interconnected computers and computerized peripherals such as printers is called computer network.
- This interconnection among computers facilitates information sharing among them.
- Computers may connect to each other by either wired or wireless media.

Applications of Communication & Computer Network

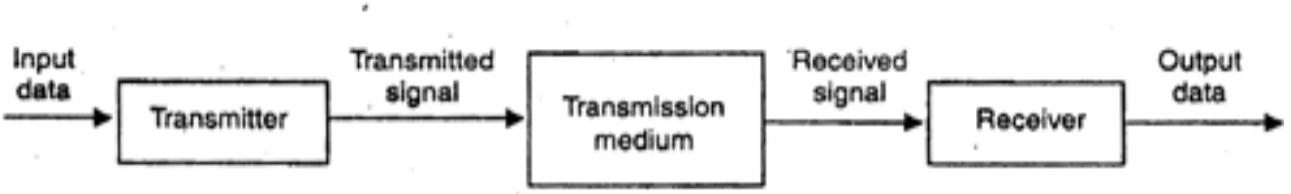
Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- Resource sharing such as printers and storage devices.
- Exchange of information by means of e-Mails and FTP.
- Information sharing by using Web or Internet.
- Interaction with other users using dynamic web pages.
- IP phones.
- Video conferences.
- Parallel computing.
- Instant messaging.

Data Communication - What is Data Communication?

Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.

The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.



Simple Data Communication System

Components of data communication system

A Communication system has following components:

1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

2. **Sender**: It is the device/computer that generates and sends that message.

3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.

4. **Medium**: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

A protocol performs the following functions:

1. **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

2. **Data routing**. Data routing defines the most efficient path between the source and destination.

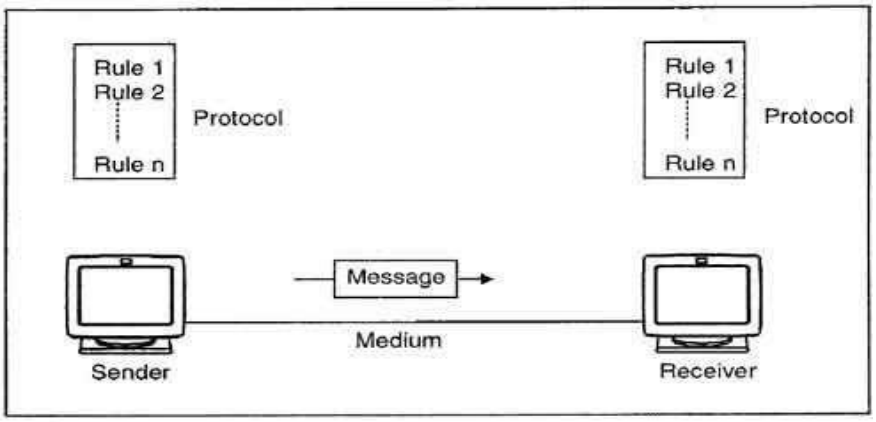
3. **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

7. **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.



8. **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. **Log information.** Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

The effectiveness depends on four fundamental characteristics of data communications

1. Delivery: The data must be deliver in correct order with correct destination.

2.Accuracy:The data must be deliver accurately.

3. Timeliness: The data must be deliver in a timely manner.late delivered Data useless.

4. Jitter: It is the uneven delay in the packet arrival time that cause uneven quality.

Difference between LAN, MAN and WAN.

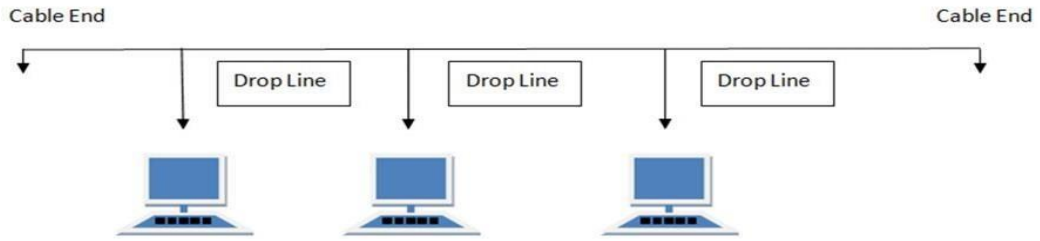
Parameter	LAN	MAN	WAN
Area covered	Covers small area. i.e. within building	Covers larger than LAN & smaller than WAN	Covers large area
Error rates	Lowest	Moderate	Highest
Transmission speed	High speed	Moderate speed	Low speed
Equipment cost	Inexpensive	Moderate expensive	Most expensive
Design & maintenance	Easy	Moderate	Difficult

Topologies (Network Topologies)

- Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.
- A Network Topology is the arrangement with which computer systems or network devices are connected to each other.

Types of network topologies :

- Bustopologyisanetworktypeinwhicheverycomputerandnetworkdeviceisconnectedto single cable.



Features:

- It transmits data only in one direction.
- Every device is connected to a single cable.

Advantages:

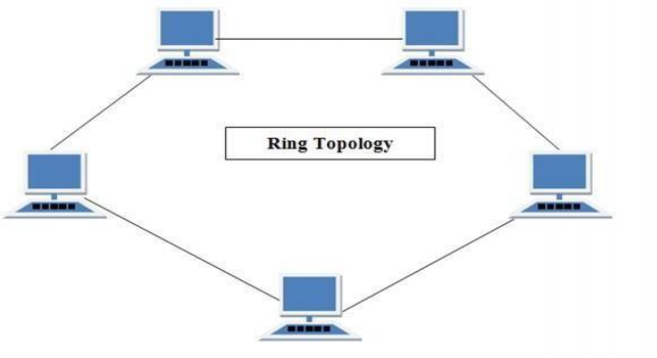
- It is cost effective (cheaper).
- Cable required is least compared to other network topology.
- Usedinsmallnetworks.
- It iseasytounderstand.
- Easy to expand joining two cables together.

Disadvantages:

- Cables fails then whole network fails.
- If networktrafficisheavyornodesaremoretheperformanceofthenetworkdecreases.
- Cable has a limited length.

Ring Topology

- It is called ring topology because it forms a ring as each computer is connected to another computer,withthelastoneconnectedtothefirst.Exactlytwoneighboursforeachdevice.



Features:

- A number of repeaters are used and the transmission is unidirectional.
- Date is transferred in a sequential manner that is bit by bit.

Advantages:

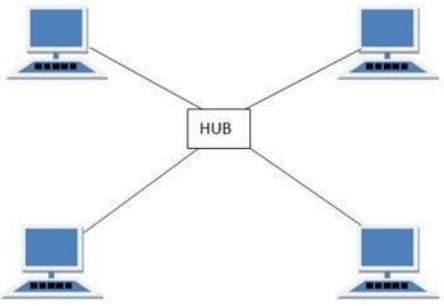
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand.

Disadvantages:

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

Star Topology

- In thistypeoftopologyallthecomputersareconnectedtoasinglehubthroughacable. This hubisthe central node and all othersnodes are connectedtothecentral node.



Features:

- Every node has its own dedicated connection to the hub.
- Acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fiber or coaxial cable.

Advantages:

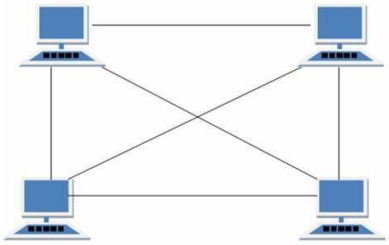
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy totroubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed rest of the nodes can work smoothly.

Disadvantages:

- Cost of installation is high.
- Expensive touse.
- Ifthehub isaffectedthenthewholenetworkisstoppedbecausealltheнodesdependonthe hub.
- Performance is based on the .

Mesh Topology

- It is a point-to-point connection to other nodes or devices.
- Traffic is carried only between two devices or nodes to which it is connected.



Features:

- Fully connected.
- Robust.
- Not flexible.

Advantages:

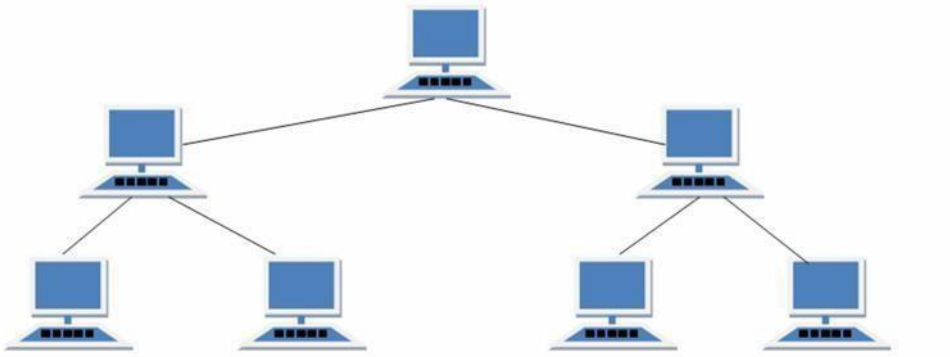
- Each connection can carry its own data load.
- It isrobust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages:

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

Tree Topology

- It has a root node and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical topology.
- It should at least have three levels to the hierarchy.



Features:

- Ideal if workstations are located in groups.

- Used in Wide Area Network.

Advantages:

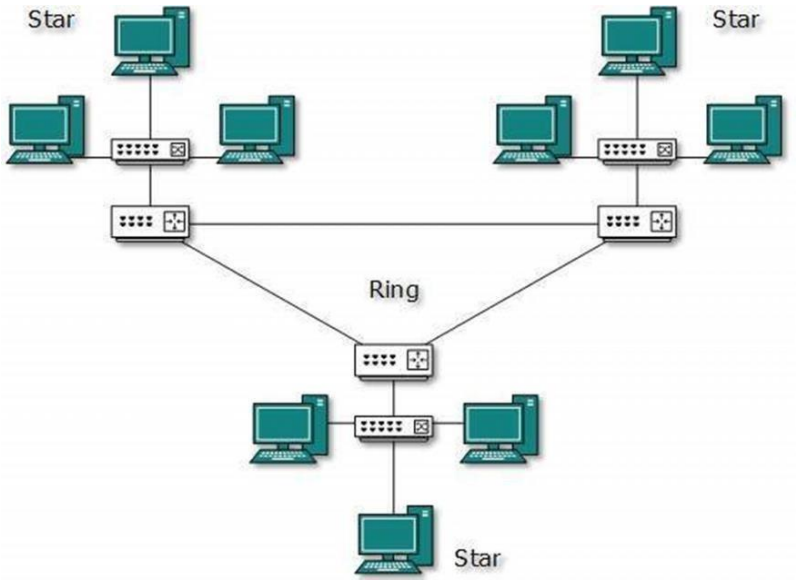
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages:

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails then network fails.

Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology.
- For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features:

- It is a combination of two or more topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages:

- Reliable as error detecting and trouble shooting is easy.
- Scalable as size can be increased easily.
- Flexible.

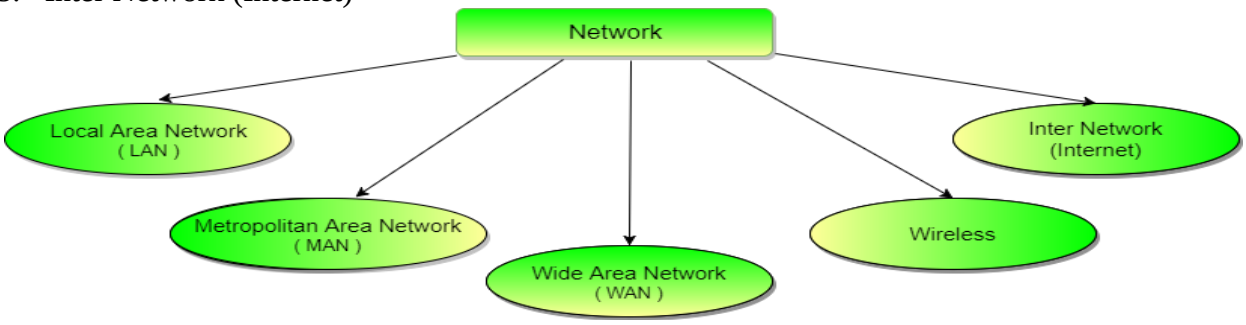
Disadvantages:

- Complex indesign.
- Costly.

Types of Communication Networks

Communication Networks can be of following 5 types:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Wireless
5. Inter Network (Internet)



Local Area Network (LAN)

- It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory.
- LANs are used widely as it is easy to design and to troubleshoot.
- Personal computers and workstations are connected to each other through LANs.
- We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.
- LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

Applications of LAN

- **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
- **Software Applications Sharing:** It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
- **Easy and Cheap Communication:** Data and messages can easily be transferred over networked computers.
- **Centralized Data:** The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
- **Data Security:** Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.
- **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

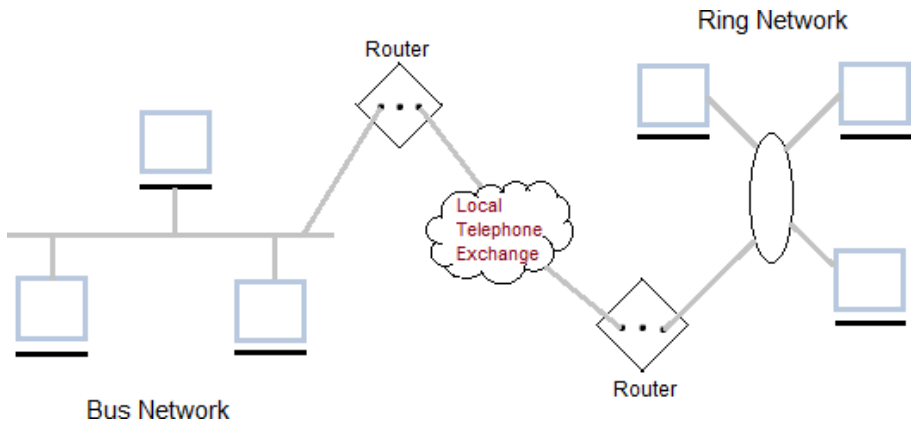
Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.

- **Privacy Violations:** The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.
- **Data Security Threat:** Unauthorised users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
- **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
- **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)

- It was developed in 1980s.It is basically a bigger version of LAN.
- It is also called MAN and uses the similar technology as LAN.
- It is designed to extend over the entire city. I
- t can be means to connecting a number of LANs into a larger network or it can be a single cable.
- It is mainly hold and operated by single private company or a public company.



Characteristics of MAN

- It generally covers towns and cities (50 km)
- Communication medium used for MAN are optical fibers, cables etc.
- Data rates adequate for distributed computing applications.

Advantages of MAN

- Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually encompasses several blocks of a city or an entire city.

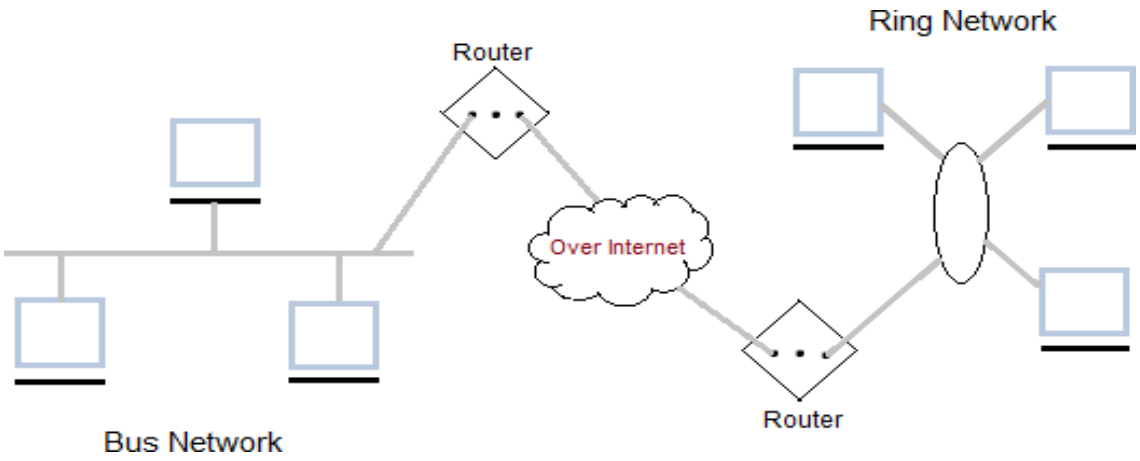
Disadvantages of MAN

- More cable required for a MAN connection from one place to another.

- It is difficult to make the system secure from hackers and industrial espionage(spying) graphical regions.

Wide Area Network (WAN)

- It is also called WAN. WAN can be private or it can be public leased network.
- It is used for the network that covers large distance such as cover states of a country. I
- t is not easy to design and maintain.
- Communication medium used by WAN are PSTN or Satellite links.
- WAN operates on low data rates.



Characteristics of WAN

- It generally covers large distances(states, countries, continents).
- Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages of WAN

- Covers a large geographical area so long distance business can connect on the one network.
- Shares software and resources with connecting workstations.
- Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them(called attachments).
- Expensive things(such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

Disadvantages of WAN

- Need a good firewall to restrict outsiders from entering and disrupting the network.

- Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
- Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.
- Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

Wireless Network

Digital wireless communication is not a new idea. Earlier, **Morse code** was used to implement wireless networks. Modern digital wireless systems have better performance, but the basic idea is the same.

Wireless Networks can be divided into three main categories:

1. **System interconnection, 2. Wireless LANs, 3. Wireless WANs**

System Interconnection

System interconnection is all about interconnecting the components of a computer using **short-range radio**. Some companies got together to design a short-range wireless network called **Bluetooth** to connect various components such as monitor, keyboard, mouse and printer, to the main unit, without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer by merely being brought within range.

In simplest form, system interconnection networks use the master-slave concept. The system unit is normally the **master**, talking to the mouse, keyboard, etc. as **slaves**.

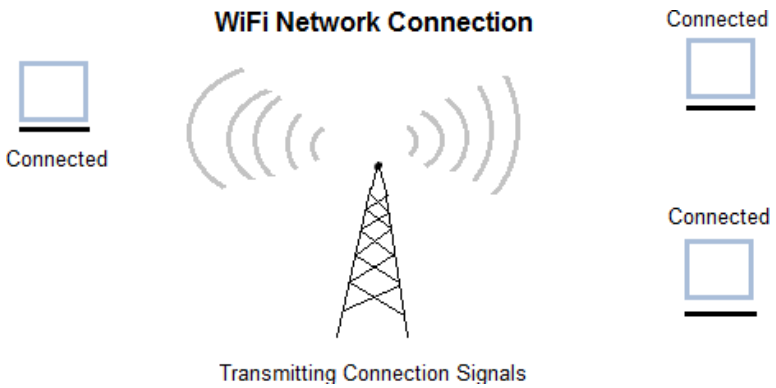
Wireless LANs

These are the systems in which every computer has a **radio modem** and **antenna** with which it can communicate with other systems. Wireless LANs are becoming increasingly common in small offices and homes, where installing **Ethernet** is considered too much trouble. There is a standard for wireless LANs called **IEEE 802.11**, which most systems implement and which is becoming very widespread.

Wireless WANs

The radio network used for cellular telephones is an example of a low-bandwidth wireless WAN. This system has already gone through three generations.

- The first generation was analog and for voice only.
- The second generation was digital and for voice only.
- The third generation is digital and is for both voice and data.



Inter Network

- Inter Network or Internet is a combination of two or more networks.

- Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.

Wide Area Networks (WAN)

Covers a very large geographical area such as a country, continent or even the whole world

Properties of WAN:

- Provide long distance communication of data or information
- Operating at lowDTRs
- Provide full time/ part time connectivity
- Connectdevicesseparatedoverwide, evenglobalareas.

Components of WAN:

- Router
- Communication Server

Modem Types of WANs:

- MAN (Metropolitan AreaNetwork)
- PAN (Public AccessNetwork)
- VAN(ValueAdded Network)
- VPN (Virtual PrivateNetwork)

Metropolitan Area Network (MAN):

- A network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN)
- Interconnection of networks in a city into a single larger network
- Interconnection of several LANs by bridging them with backbone lines
- Example: subscriber networks, TV service

Public Access Network (PAN):

- Could be accessed by public
- Examples: image services, web services

Value Added Network (VAN):

- Avalue-addednetwork(VAN) is aprivatenetworkprovider(sometimescalledaturnkey communications line) that is hired by a company to facilitate electronic data interchanges (EDI) or provides other network services.

Virtual Private Network (VPN):

- A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to theirorganization's network.
- Example: Research and development work
- Became popular as more employees worked in remote locations
- Employees can access the network(intranet) from remote locations
- The Internet isused as thebackbonefor VPNs(wearecreatingthisnetworkontopofinternet)

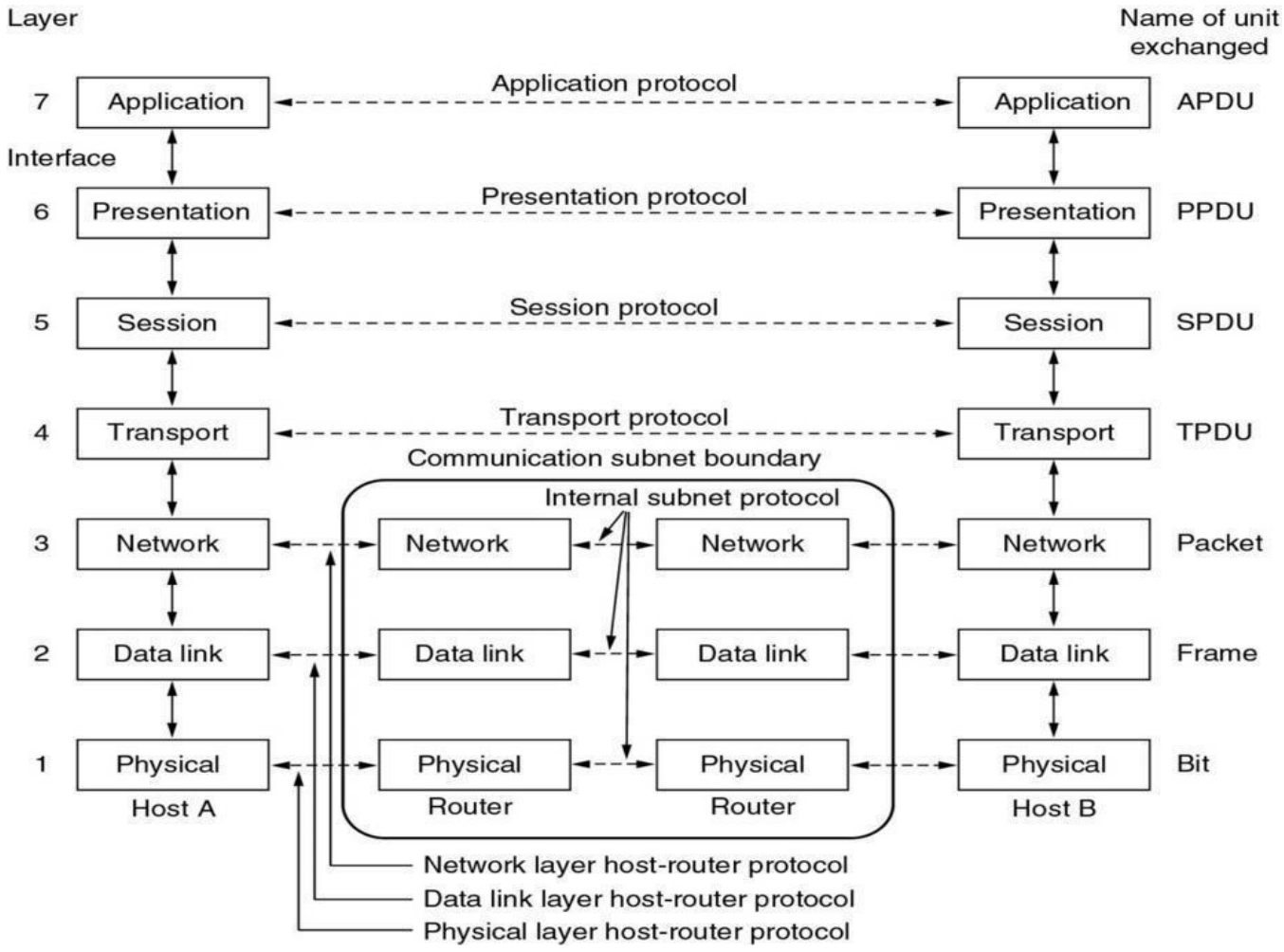
Protocols layers and their service model

OSI Layer Architecture

- OSImodel is basedonaproposaldevelopedbythe International Standards Organization(ISO) as afirststeptowardinternationalstandardizationoftheprotocolsusedinthevariouslayers.
- It was revised in 1995.
- The model is called the OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication withother systems.

The OSI model has seven layers.

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



Physical Layer

- Thephysicallayer, the lowestlayer of the OSImodel, is concerned with the transmissionand reception of the unstructured raw bit stream over a physical medium.
- It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:
- **Data encoding**: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization.
- **Transmission technique**: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signalling.
- **Physical medium transmission**: transmits bits as electrical or optical signals appropriate for the physical medium.

Data link Layer

- The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.
- To do this, the data link layer provides:
- **Link establishment and termination**: establishes and terminates the logical link between two nodes.
- **Frame traffic control**: tells the transmitting node to "back-off" (stop) when no frame buffers are available.
- **Frame sequencing**: transmits/receives frames sequentially.
- **Frame acknowledgment**: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate framereceipt.
- **Frame delimiting**: creates and recognizes frame boundaries.
- **Frame error checking**: checks received frames for integrity.
- **Media access management**: determines when the node "has the right" to use the physical medium.

Network Layer

- The network layer controls the operation of the subnet, deciding which physical path the data shouldtakebasedonnetworkconditions, priorityofservice, andotherfactors.
- To do this, the data link layer provides:
- **Routing**: routes frames among networks.
- **Subnet traffic control**: routers (network layer intermediate systems) can instruct a sending stationto "throttle back" its frametransmissionwhentherouter'sbufferfills up.
- **Frame fragmentation**: if it determines that a downstream router's maximum transmission unit (MTU) size is lessthan the frame size, a router can fragmenta frame for transmission and re-assembly at the destination station.
- **Logical-physical address mapping**: translates logical addresses or names, into physical addresses.
- **Subnet usage accounting**: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Transport Layer

- The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves (release) the higher layer protocols from any concern with the transfer of data between them and their peers.
- Thesizeandcomplexityofatransportprotocoldependsonthetypeofserviceitcangetfrom the networklayer. Forareliablenetworklayerwithvirtualcircuitcapability, aminimaltransport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive errordetection and recovery.
- The transport layer provides:
- **Message segmentation**: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the networklayer.Thetransportlayeratthedestination stationreassemblesthemessage.
- **Message acknowledgment**: provides reliable end-to-end message delivery with acknowledgments.
- **Message traffic control**: tells the transmitting station to "back-off" when no message buffers are available.
- Typically, thetransportlayer can acceptrelativelylargemessages, buttherearestrictmessage size limits imposed by the network (or lower) layer. Consequently, the transport layer must break upthemessagesintosmallerunits,orframes,prependingaheadertoeach frame.
- The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries.
- In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back togetherintherightorderbeforehandingthereceivedmessageuptothelayerabove.

Session Layer

- The session layerallows session establishmentbetween processes running on different stations. It provides:
- **Session establishment, maintenance and termination**: allows two application processes on differentmachinestoestablish, useandterminateaconnection, calledasession.
- **Session support**: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

Presentation Layer

- The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to theapplication layer at the receiving station.
- The presentation layer provides:
- **Character code translation**: for example, ASCII to EBCDIC.
- **Data conversion**: bit order, CR-CR/LF, integer-floating point, and so on.
- **Datacompression**: reducesthenumberofbitsthatneedtobetransmittedonthenetwork.
- **Dataencryption**: encryptdataforsecuritypurposes. Forexample, passwordencryption.

Application Layer

- The application layer serves as the window for users and application processes to access network services.
- This layer contains a variety of commonly needed functions:
    1. Resource sharing and device redirection
    2. Remote fileaccess
    3. Remote printeraccess
    4. Inter-process communication
    5. Network management
    6. Directory services
    7. Electronic messaging (such as mail)
    8. Network virtualterminals

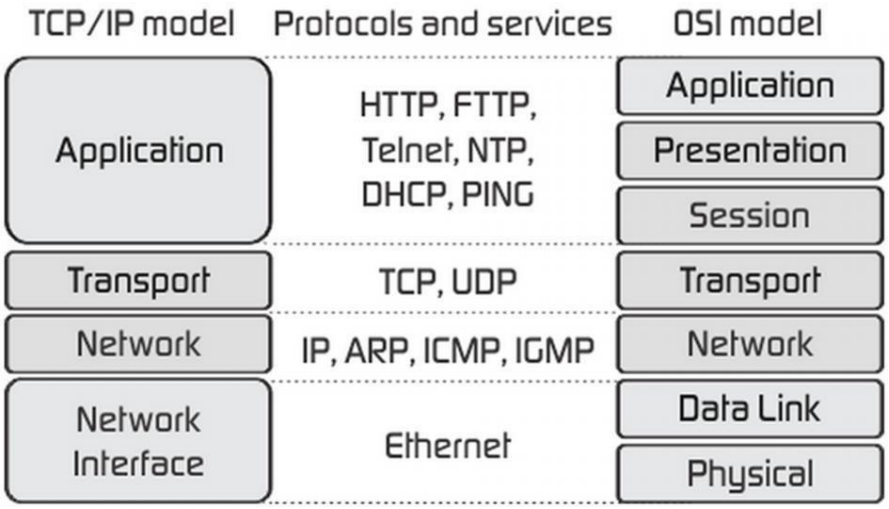
TCP/IP Reference Model (Internet Protocol Stack layers)

- Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide.
- TCP/IPeithercombinesseveralOSIlayersintoasinglelayer,ordoesnotusecertainlayersat all.
- TCP/IPisasetofprotocolsdevelopedto allowcooperating computers to share resourcesacross the network.

The TCP/IP model has five layers.

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Data LinkLayer
5. Physical Network
6.

Figure 16: TCP/IP Reference Model



- As we can see from the above figure, presentation and session layers are not there in TCP/IP model. Also note that the Network Access Layer in TCP/IP model combines the functionsof Data link Layer and Physical Layer.

Application Layer

- Application layer is the top most layer of four layer TCP/IP model.
- Application layer is present on the top of the Transport layer.
- Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.
- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP(Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Transport Layer

- The purpose of Transport layer is to permit devices on the source and destination hosts to carry on aconversation.
- Transportlayerdefinesthelevelofserviceandstatusoftheconnectionusedwhentransporting data.
- Thetransportlayerprovidestheend-to-enddatatransferbydeliveringdatafrom anapplication to its remote peer.
- The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
  - Reliable deliverydata
  - Duplicatedatasuppression
  - Congestion control
  - Flow control

Anothertransportlayer protocol is the User Datagram Protocol(UDP), whichprovides:

- Connectionless
- Unreliable
- Best-effort service

Network Layer (Internet Layer)

- The internet layer also called the network layer.
- Internetlayerpackdataintodatapacketsknown as IP datagrams, whichcontainsourceand destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.
- The InternetlayerisalsoresponsibleforroutingofIPdatagrams.
- InternetProtocol(IP)isthemostimportantprotocolinthislayer.
- It isaconnectionlessprotocolthatdoesnotassumereliabilityfromlowerlayers. IP doesnot provide reliability, flow control or error recovery.
- IP provides a routing function that attempts to deliver transmitted messages to their destination.
- These message units in an IP network are called an IP datagram.
- Example: IP, ICMP, IGMP, ARP, and RARP.

Network Interface Layer (Network Access Layer:

- Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signalled by hardware devices that interface directlywithanetworkmedium,suchascoaxialcable,opticalfiber,ortwistedpaircopperwire.
- The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

Difference between OSI and TCP / IP Model.

OSI(Open System Interconnection)	TCP/IP (Transmission Control Protocol/ Internet Protocol)
OSI provides layer functioning and also defines functions of all the layers.	TCP/IP model is more based on protocols and protocols are not flexible with other layers.
In OSImodelthetransportlayerguaranteesthe delivery of packets	In TCP/IP model the transport layer does not guarantees delivery of packets.
Follows horizontal approach	Follows vertical approach.
OSI model has a separate presentation layer	TCP/IPdoesn'thaveaseparatepresentationlayer
OSI is a general model.	TCP/IP model cannot be used in any other application.
Network layer of OSI model provide both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
OSImodelhasaproblemoffittingtheprotocolsin the model	TCP/IP model does not fit any protocol
ProtocolsarehiddeninOSImodelandareeasily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocolsveryclearlyandmakescleardistinction between them.	InTCP/IPitisnotclearlyseparateditsservices, interfaces andprotocols.
It has 7 layers	It has 4 layers

What is bandwidth?

Bandwidth is measured as the amount of data that can be transferred from one point to another within a network in a specific amount of time. Typically, bandwidth is expressed as a bitrate and measured in bits per second (bps).

The term bandwidth refers to the transmission capacity of a connection and is an important factor when determining the quality and speed of a network or the internet connection.

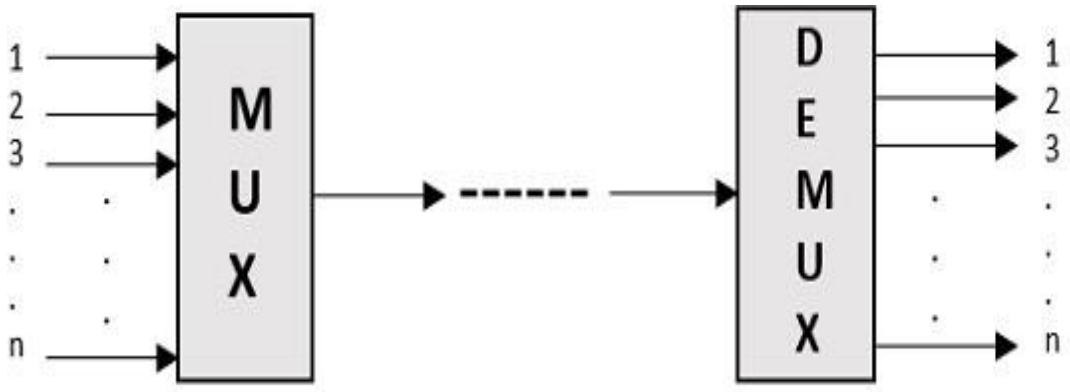
There are several different ways to measure bandwidth. Some measurements are used to calculate current data flow, while others measure maximum flow, typical flow, or what is considered to be good flow.

Bandwidth is also a key concept in several other technological fields. In signal processing, for example, it is used to describe the difference between the upper and lower frequencies in a transmission such as a radio signal and is typically measured in hertz (Hz).

Bandwidth can be compared to water flowing through a pipe. Bandwidth would be the rate at which water (data) flows through the pipe (connection) under various circumstances. Instead of bits per second, we might measure gallons per minute. The amount of water that possibly can flow through the pipe represents the maximum bandwidth, while the amount of water that is currently flowing through the pipe represents the current bandwidth.

Multiplexing

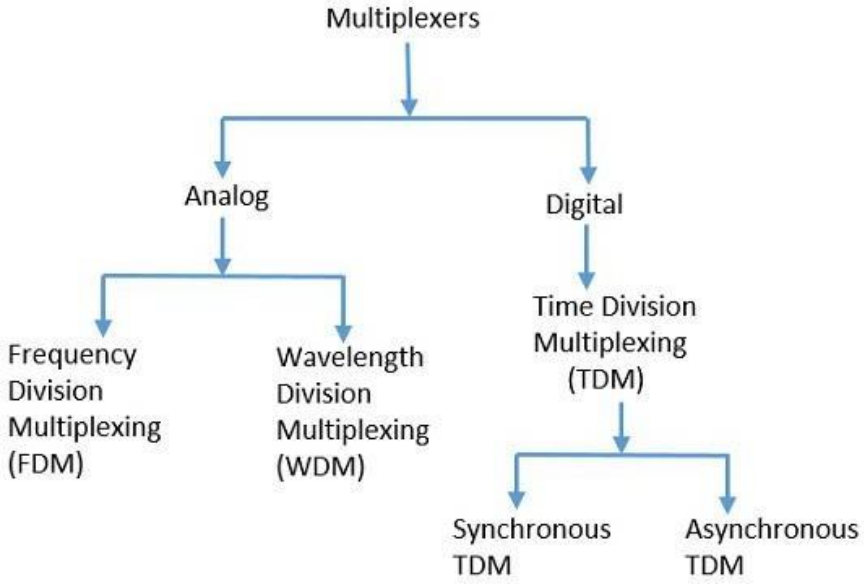
- **Multiplexing** is the process of combining multiple signals into one signal, over a shared medium.
  - The process is called as **analog multiplexing** if these signals are analog in nature.
  - If digital signals are multiplexed, it is called as **digital multiplexing**.
- Multiplexing was first developed in telephony. A number of signals were combined to send through a single cable.
- The process of multiplexing divides a communication channel into several number of logical channels, allotting each one for a different message signal or a data stream to be transferred.
- The device that does multiplexing, can be called as a **MUX**.
- The reverse process, i.e., extracting the number of channels from one, which is done at the receiver is called as **demultiplexing**. The device which does demultiplexing is called as **DEMUX**.
- The following figures illustrates the concept of MUX and DEMUX. Their primary use is in the field of communications.



Multiplexing and Demultiplexing

Types of Multiplexers

There are mainly two types of multiplexers, namely analog and digital. They are further divided into FDM, WDM, and TDM. The following figure gives a detailed idea about this classification.



There are many types of multiplexing techniques. Of them all, we have the main types with general classification, mentioned in the above figure. Let us take a look at them individually.

Analog Multiplexing

The analog multiplexing techniques involve signals which are analog in nature. The analog signals are multiplexed according to their frequency (FDM) or wavelength (WDM).

Frequency Division Multiplexing

In analog multiplexing, the most used technique is **Frequency Division Multiplexing (FDM)**. This technique uses various frequencies to combine streams of data, for sending them on a communication medium, as a single signal.

Example − A traditional television transmitter, which sends a number of channels through a single cable uses FDM.

Wavelength Division Multiplexing

Wavelength Division multiplexing (WDM) is an analog technique, in which many data streams of different wavelengths are transmitted in the light spectrum. If the wavelength increases, the frequency of the signal decreases. A prism which can turn different wavelengths into a single line, can be used at the output of MUX and input of DEMUX.

Example − Optical fiber Communications use the WDM technique, to merge different wavelengths into a single light for the communication.

Digital Multiplexing

The term digital represents the discrete bits of information. Hence, the available data is in the form of frames or packets, which are discrete.

Time Division Multiplexing (TDM)

In TDM, the time frame is divided into slots. This technique is used to transmit a signal over a single communication channel, by allotting one slot for each message.

Of all the types of TDM, the main ones are Synchronous and Asynchronous TDM.

Synchronous TDM

In Synchronous TDM, the input is connected to a frame. If there are 'n' number of connections, then the frame is divided into 'n' time slots. One slot is allocated for each input line.

In this technique, the sampling rate is common for all signals and hence the same clock input is given. The MUX allocates the **same slot** to each device at all times.

Asynchronous TDM

In Asynchronous TDM, the sampling rate is different for each of the signals and a common clock is not required. If the allotted device, for a time slot transmits nothing and sits idle, then that slot is **allotted to another** device, unlike synchronous.

This type of TDM is used in Asynchronous transfer mode networks.

Demultiplexer

- Demultiplexers are used to connect a single source to multiple destinations.
- This process is the reverse of multiplexing. As mentioned previously, it is used mostly at the receivers. DEMUX has many applications.
- It is used in receivers in the communication systems. It is used in arithmetic and logical unit in computers to supply power and to pass on communication, etc.
- Demultiplexers are used as serial to parallel converters.
- The serial data is given as input to DEMUX at regular interval and a counter is attached to it to control the output of the demultiplexer.
- Both the multiplexers and demultiplexers play an important role in communication systems, both at the transmitter and receiver sections.

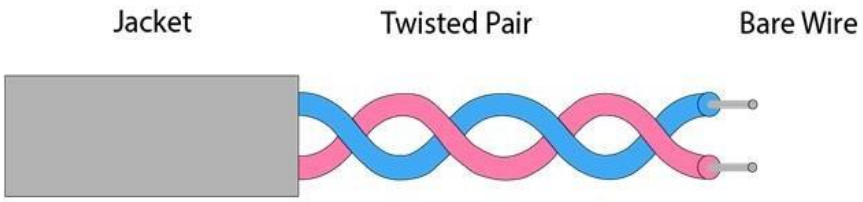
Guided Media

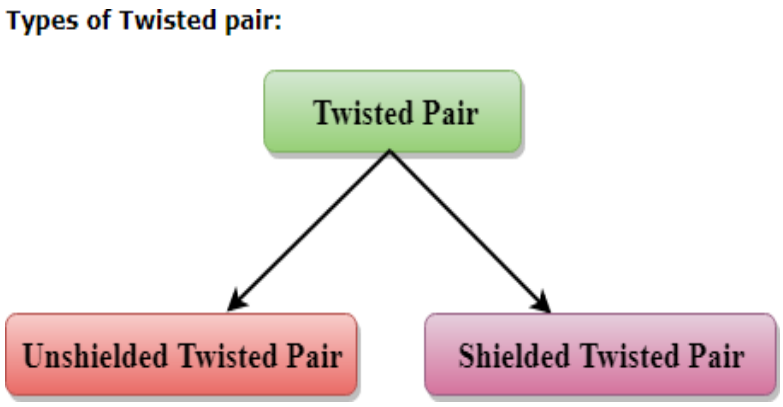
It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types of Guided media:

Twisted pair:

- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
- The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.





Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

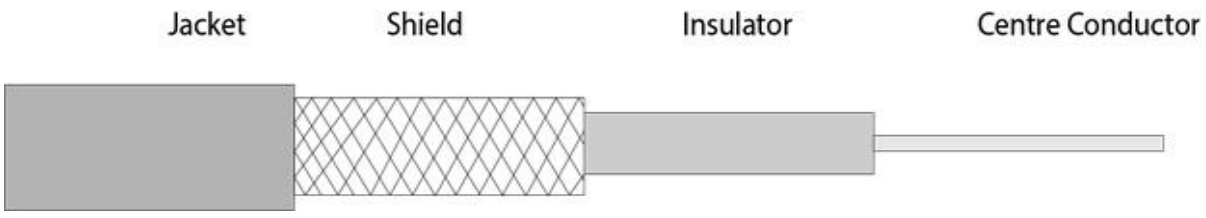
- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

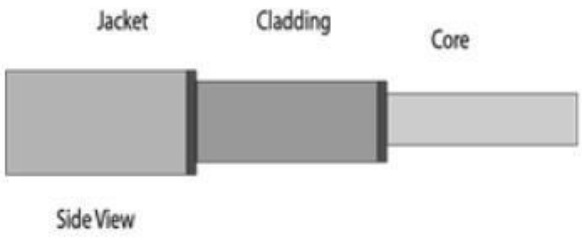
Disadvantages Of Coaxial cable:

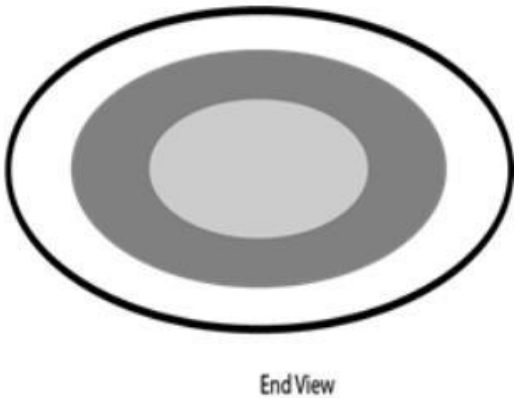
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:





Basic elements of Fibre optic cable:

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.

- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

Unguided Transmission

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.

Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves

Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Switching

- **Circuit Switched Networks** − Circuit switched networks are connection-oriented networks. Here, a dedicated route is established between the source and the destination and the entire message is transferred through it.
- **Packet Switched Networks** − Packet switched networks are connectionless networks. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination.

Difference between Circuit Switching and Packet Switching

CIRCUIT SWITCHING	PACKET SWITCHING
In circuit switching there are 3 phases. i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place .
In circuit switching, each data unit know the entire path address which is provided by the source	In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.
In Circuit switching, data is processed at source system only	In Packet switching, data is processed at all intermediate node including source system.
Delay between data units in circuit switching is uniform.	Delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources are more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source	Transmission of the data is done not only by the source, but also by the intermediate routers
Congestion can occur during connection establishment time, there might be a case will requesting for channel the channel is already occupied.	Congestion can occur during data transfer phase, large number of packets comes in no time

What is switching?

Switching is the most important mechanism which exchanges the information between different networks or different computer(s). Switching is the way which directs data or any digital information towards your network till the end point.

There are three type of switching techniques available: **Circuit Switching, Packet Switching and Message Switching**. Circuit and Packet Switching are the most popular among these three.

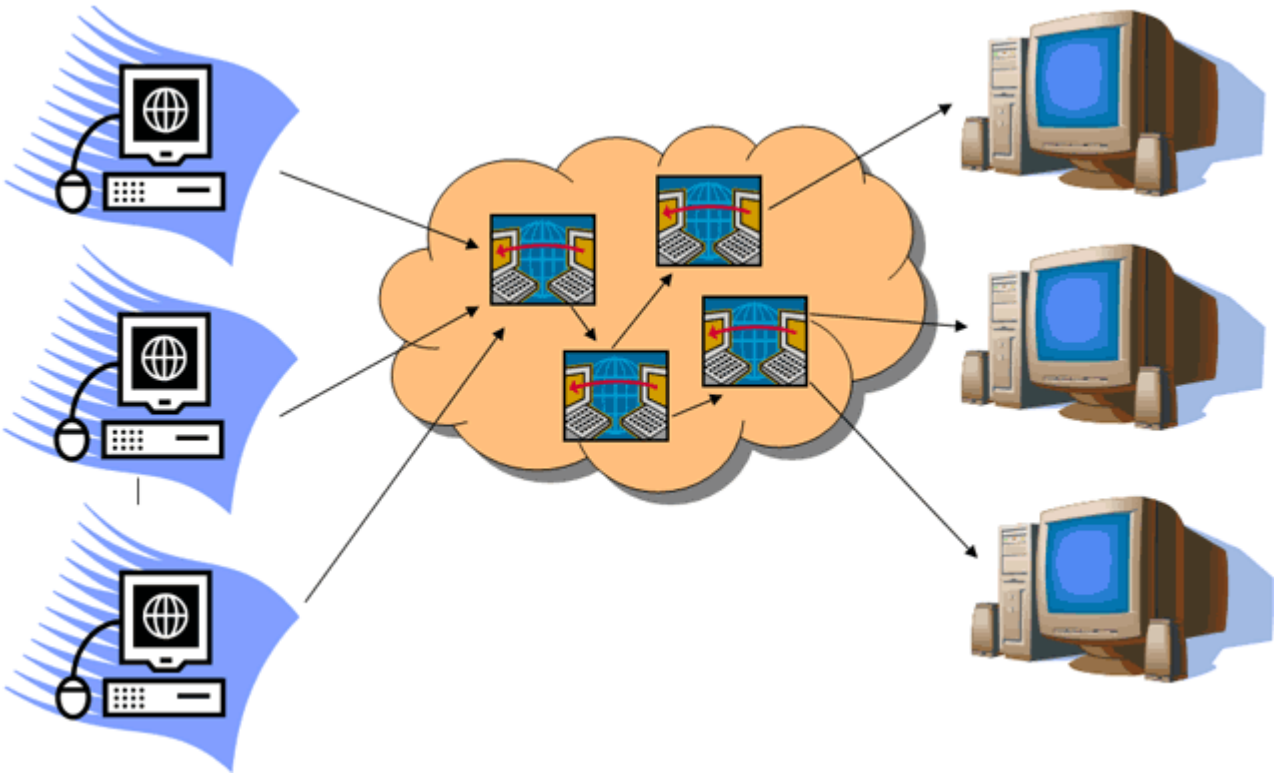
Circuit Switching

Circuit switching is a switching method where an end-to-end path is created between two stations within a network before starting the data transfer.

Circuit switching has three phases: Circuit establishment, Transferring the data and circuit disconnect.

Circuit switching method has a fixed data rate and both the subscribers need to operate at this fixed rate. Circuit switching is the simplest method of data communication where **dedicated physical connections are established between two individual senders and receiver**. To create these dedicated connections, a set of switches are connected by physical links.

In the below image, three computers on the left side are connected with three desktops PCs on the right side with physical links, depending on the four circuit switchers. If the circuit switching is not used, they need to be connected with point-to-point connections, where many number of dedicated lines are required, which will not only increase the connection cost but also increase the complexity of the system.



The routing decision, in the case of circuit switching, is made when the routing path is being established in the network. After the dedicated routing path is established the data continuously submitted to the receiver destination. The connection is maintained until the end of the conversation.

Three Phases in Circuit switching Communication

The start to the end communication in Circuit Switching is done using this formation-

During the Setup phase, in the circuit switching network, a dedicated routing or connection path is established between the sender and the receiver. The circuit switching happens in the physical layers.

Data transfer only happens after the setup phase is completed and only when a physical, dedicated path is established. No addressing method is involved in this phase.

Circuit disconnect phase, when sender or receiver needs to disconnect the path, a disconnect signal is sent to all involved switches to release the resource and break the connection.

A Circuit switch creates a temporary connection between an input link with an output link. There are various types of switches available with multiple inputs and output lines.

Generally, Circuit Switching is used in Telephone Lines.

Advantages of Circuit Switching

Circuit Switching Method provides large advantages in specific cases. The Advantages are as follows-

1. The data rate is fixed and dedicated because the connection is established using dedicated physical connection or circuits.
2. As there are dedicated transmission routing paths involved, it is a good choice for continuous transmission over a long duration.

Disadvantages of Circuit Switching

Other than the Advantages, Circuit switching also have some disadvantages.

1. Whether the communication channel is free or busy, the dedicated channel could not be used for other data transmission.
2. It requires more bandwidth, and continuous transmission offers wastage of bandwidth when there is a silence period.
3. It is highly inefficient when utilizing the system resource. We cannot use the resource for other connection as it is allocated for the entire conversation.

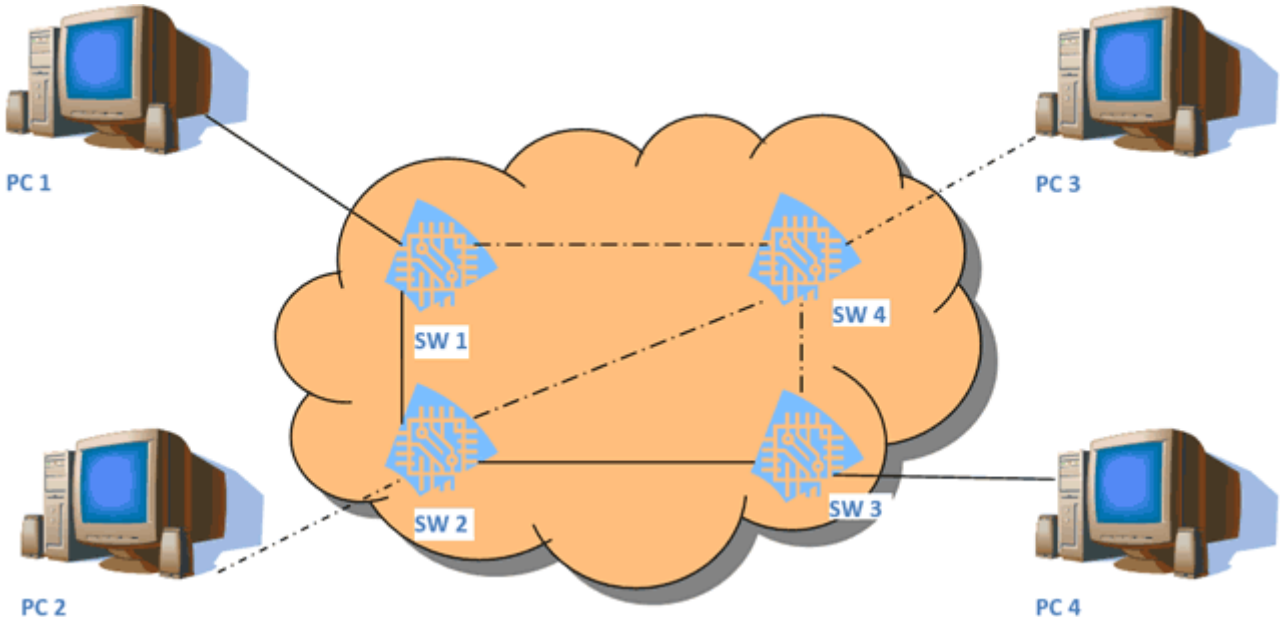
Packet Switching

- **Packet switching** is a method of data transfer where the data is broken into small pieces of variable lengths and then transmitted to the network line. Broken pieces of data are called as **packets**.
- After receiving those broken data or packets, all are reassembled at the destination and thus making a complete file. Due to this method, the data gets transferred fast and in an efficient manner

- This method use Store and Forward techniques. So each hop will store the packet first and then forward the packets to the next host destination.
- Each packet contains control information, source address and destination address. Due to this packets can use any route or paths in an existing network.

VC Based Packet Switching

- VC based package switching is a mode of packet switching where a logical path or virtual circuit connection is done between sender and receiver. **VC stands for Virtual Circuit**.
- In this mode of packet switching operation, a predefined route is created and all packets will follow the predefined paths.
- All routers or switches which are involved in the logical connection are provided a unique Virtual Circuit ID to uniquely identify the virtual connections.
- It also **has the same three-phase protocol used in circuit switching, Setup Phase, Data Transfer Phase and Tear down Phase**.



In the above image, 4 PCs are connected with a 4 switch network and the **data flow will be packet switching in Virtual circuit mode**. As we can see switches are connected with each other and share the communications path with each other. Now in the virtual circuit, a predefined route needs to be established. If we want to transfer data from PC1 to the PC 4 the path will be directed from the SW1 to SW2 to SW3 and then finally at PC4. This route is predefined and All SW1, SW2, SW3 are provided with a unique ID to identify the data paths, so the data is bound by the paths and could not choose another route.

Advantages of Packet Switching

Packet switching offers advantages over the circuit switching. Packet switching network is designed to overcome the drawbacks of Circuit Switching method.

1. Efficient in terms of Bandwidth.
2. Transmission delay is minimum
3. Missing packets can be detected by the destination.
4. Cost-effective implementation.

Disadvantages of Packet Switching

Packet switching also encounters few drawbacks.

1. Packet switching does not follow any particular order to transmit the packet one by one.
2. Packet missing occurs in large data transmission.
3. Each packet needs to be encoded with sequence numbers, Receiver and Senders address, and other information.
4. Routing is complex in the nodes as packets can follow multiple paths.

Data Link Layer

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.

Following services are provided by the Data Link Layer:

- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Error Detection in Computer Networks

Error

A condition when the receiver’s information does not match with the sender’s information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

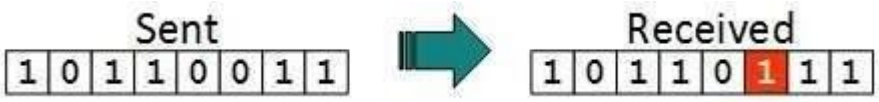
Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)
Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.
Some popular techniques for error detection are:
1. Simple Parity check
2. Two-dimensional Parity check
3. Checksum
4. Cyclic redundancy check

Types of Errors

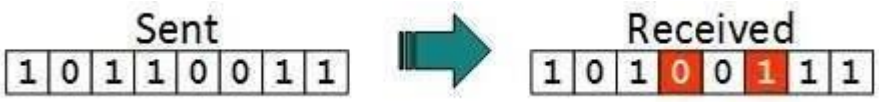
There may be three types of errors:

- **Single bit error**



In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**

Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

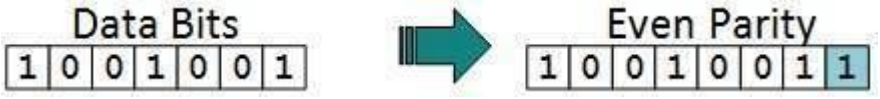
Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

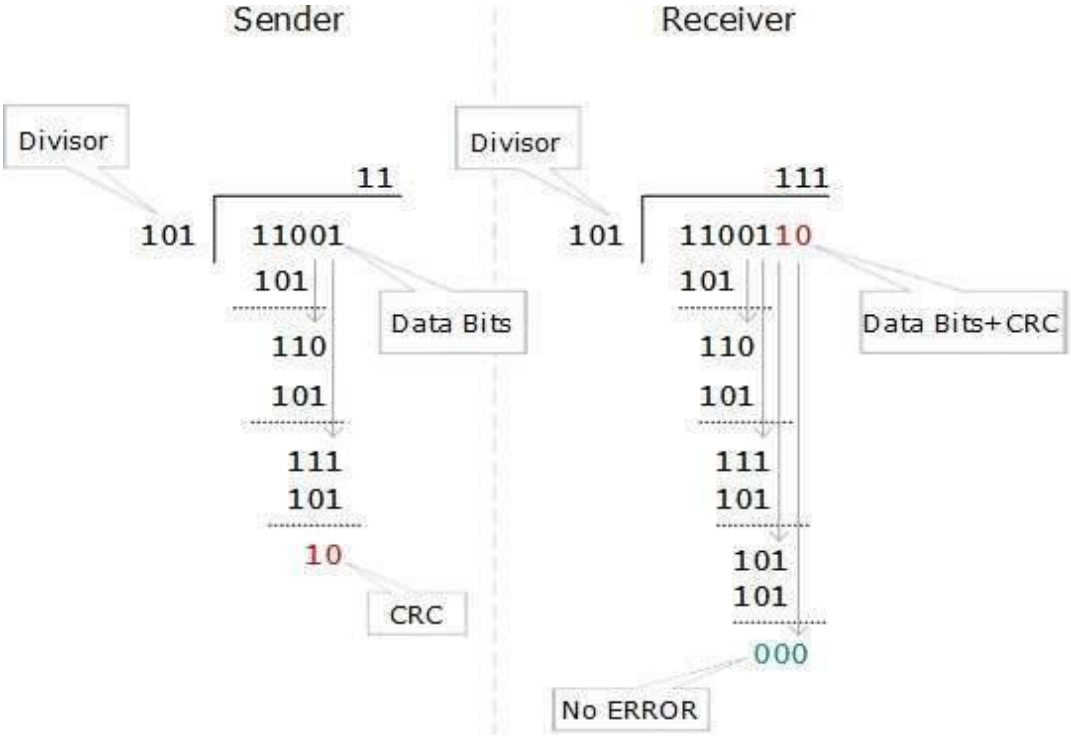


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erro neous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

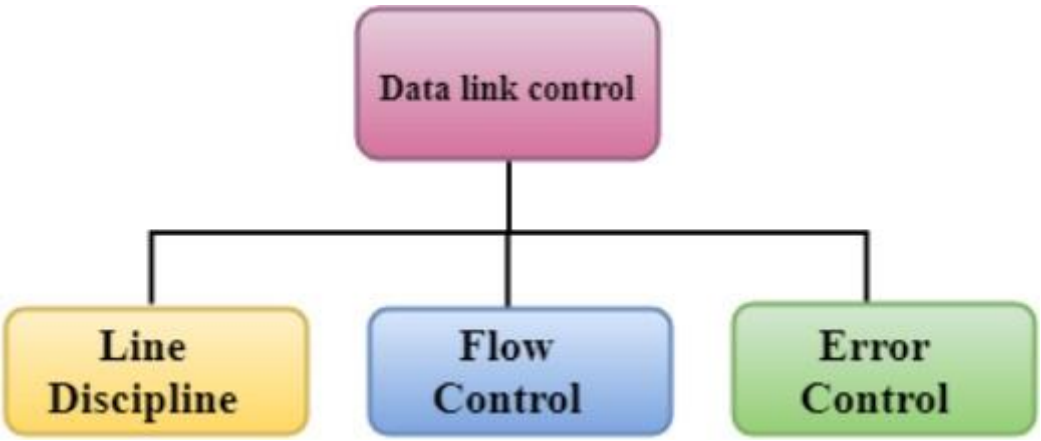
$$2^r >= m+r+1$$

Data Link Controls

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control



Line Discipline

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- ENQ/ACK
- Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.

END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

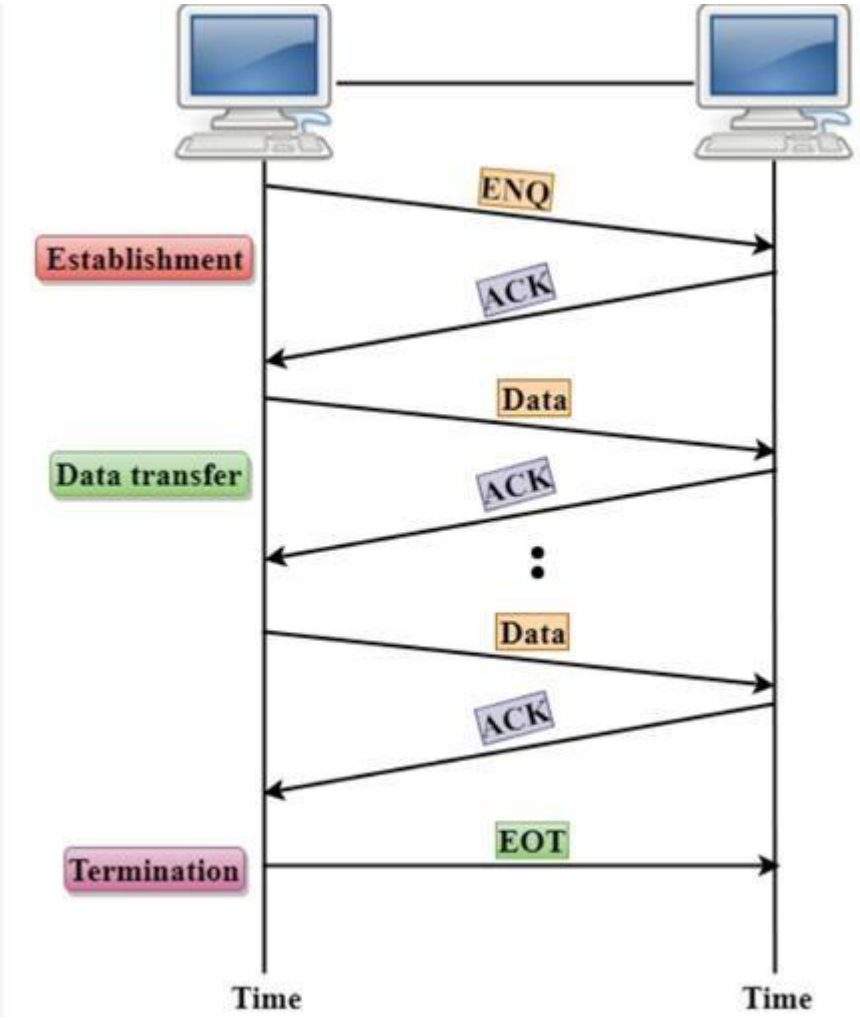
Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

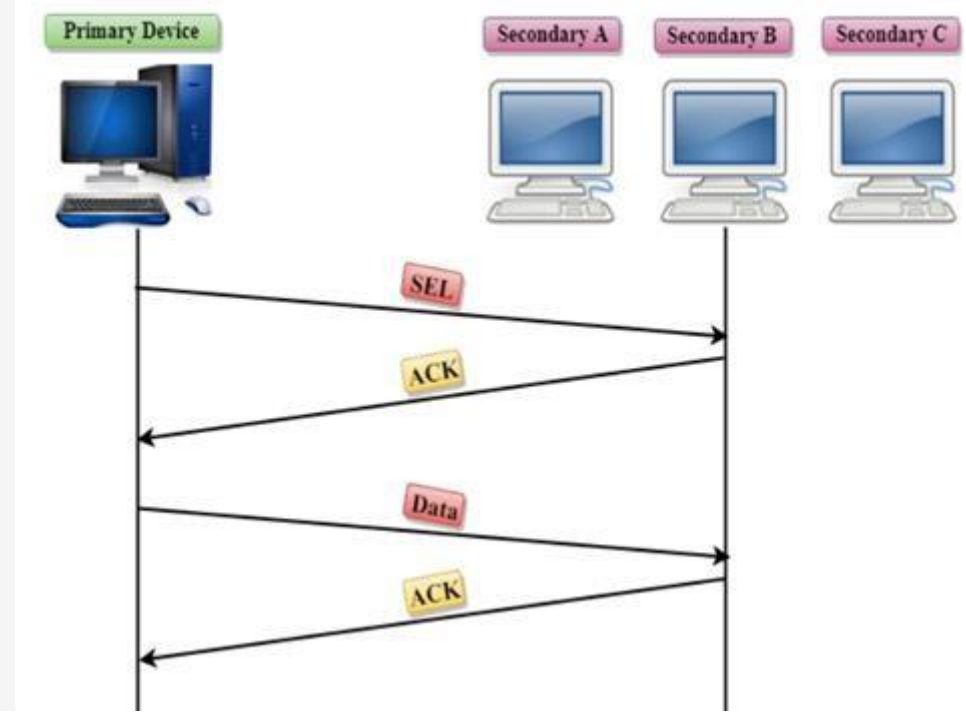
The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

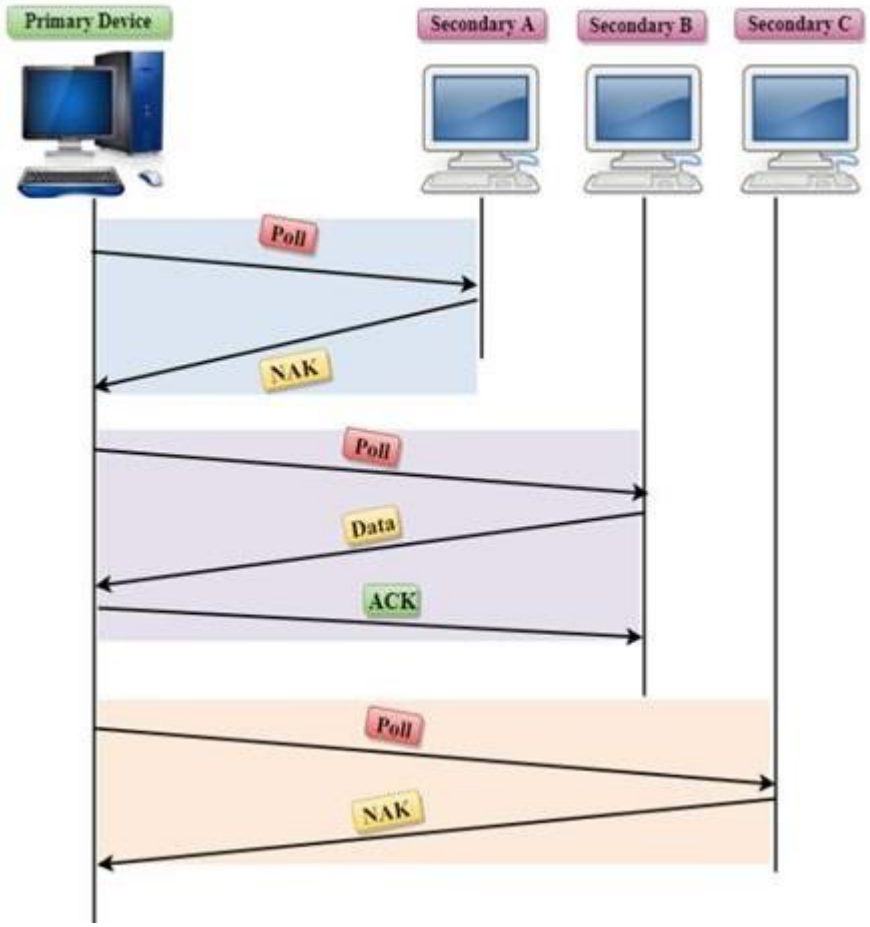
Select

- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

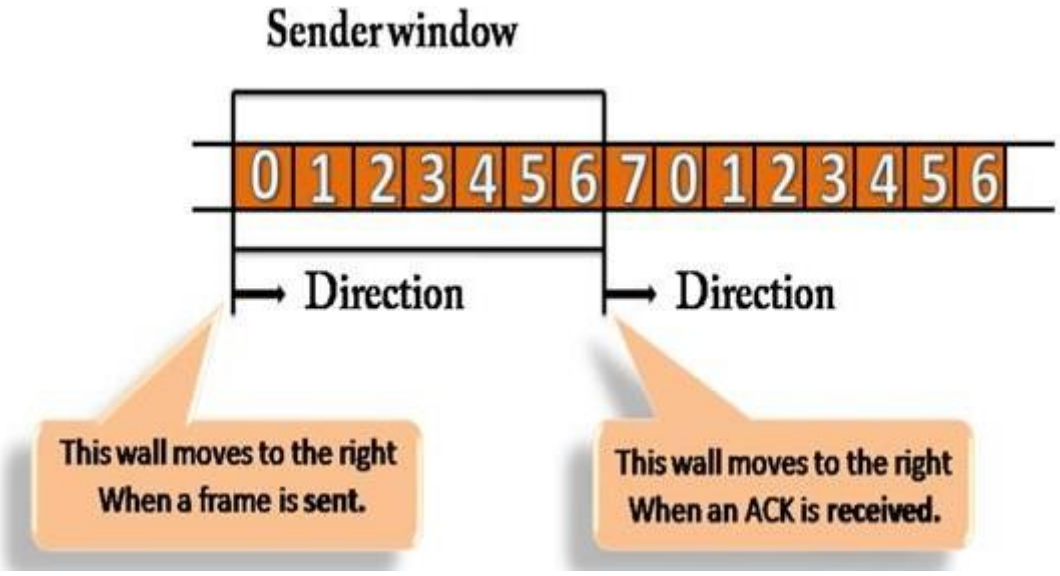
Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

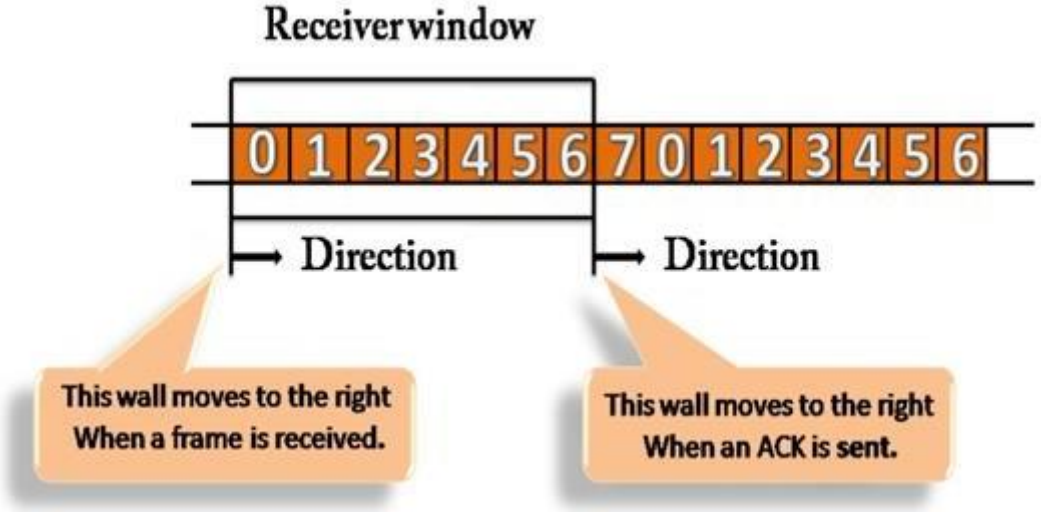
Sender Window

- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).



Receiver Window

- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.



Error Control

Error Control is a technique of error detection and retransmission.

Categories of Error Control:

Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

SlidingWindow ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

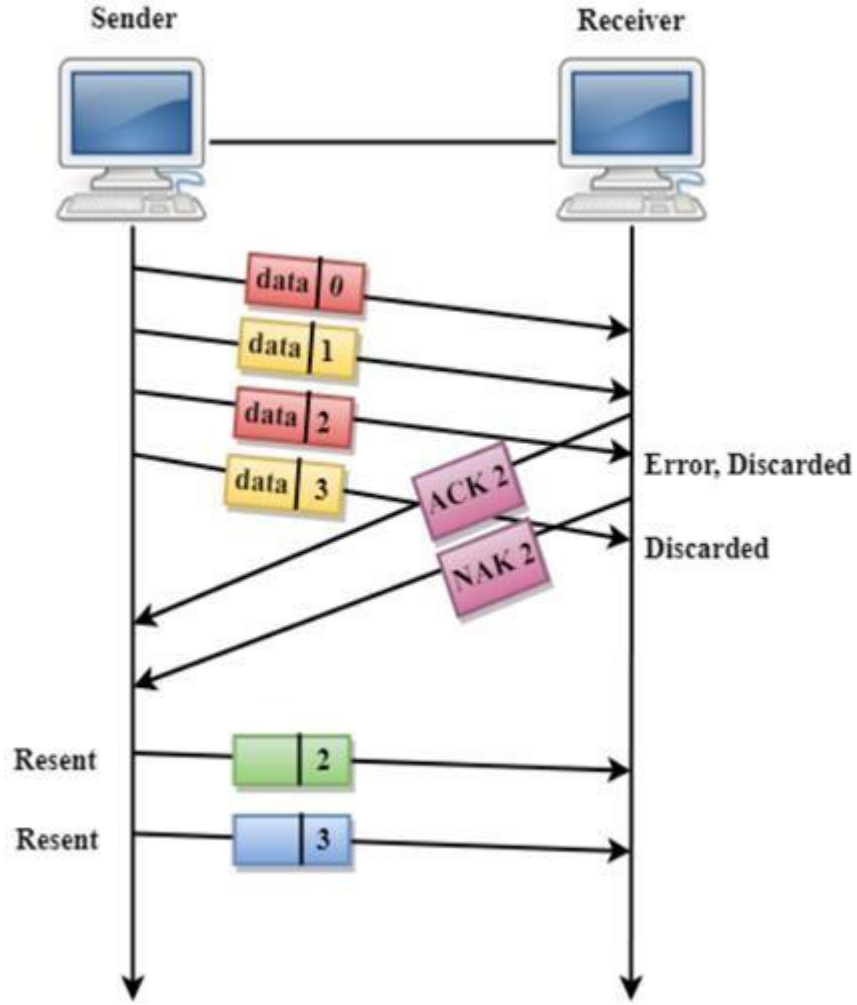
- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame.



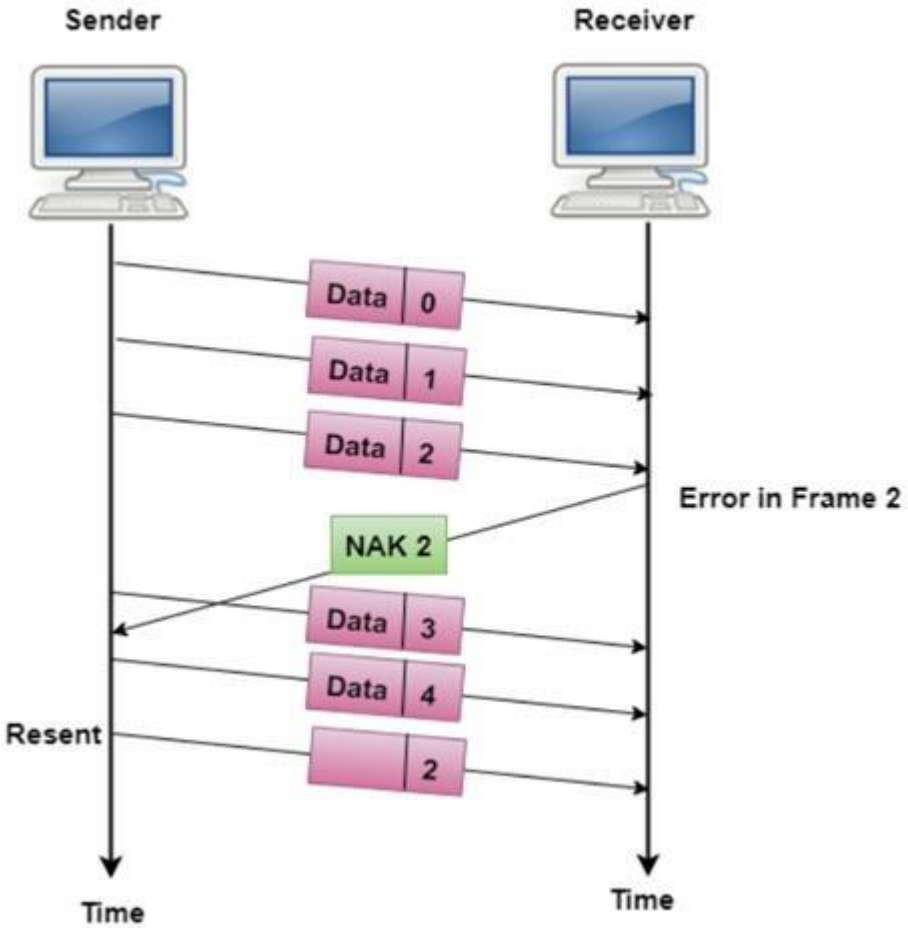
In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.
- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.

- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



Common Data Link Protocols

- **Synchronous Data Link Protocol (SDLC)** − SDLC was developed by IBM in the 1970s as part of Systems Network Architecture. It was used to connect remote devices to mainframe computers. It ascertained that data units arrive correctly and with right flow from one network point to the next.
- **High Level Data Link Protocol (HDLC)** − HDLC is based upon SDLC and provides both unreliable service and reliable service. It is a bit – oriented protocol that is applicable for both point – to – point and multipoint communications.
- **Serial Line Interface Protocol (SLIP)** − This is a simple protocol for transmitting data units between an Internet service provider (ISP) and home user over a dial-up link. It does not provide error detection / correction facilities.
- **Point - to - Point Protocol (PPP)** − This is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte – oriented protocol that is widely used in broadband communications having heavy loads and high speeds.
- **Link Control Protocol (LCP)** − It one of PPP protocols that is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Network Control Protocol (NCP)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there.

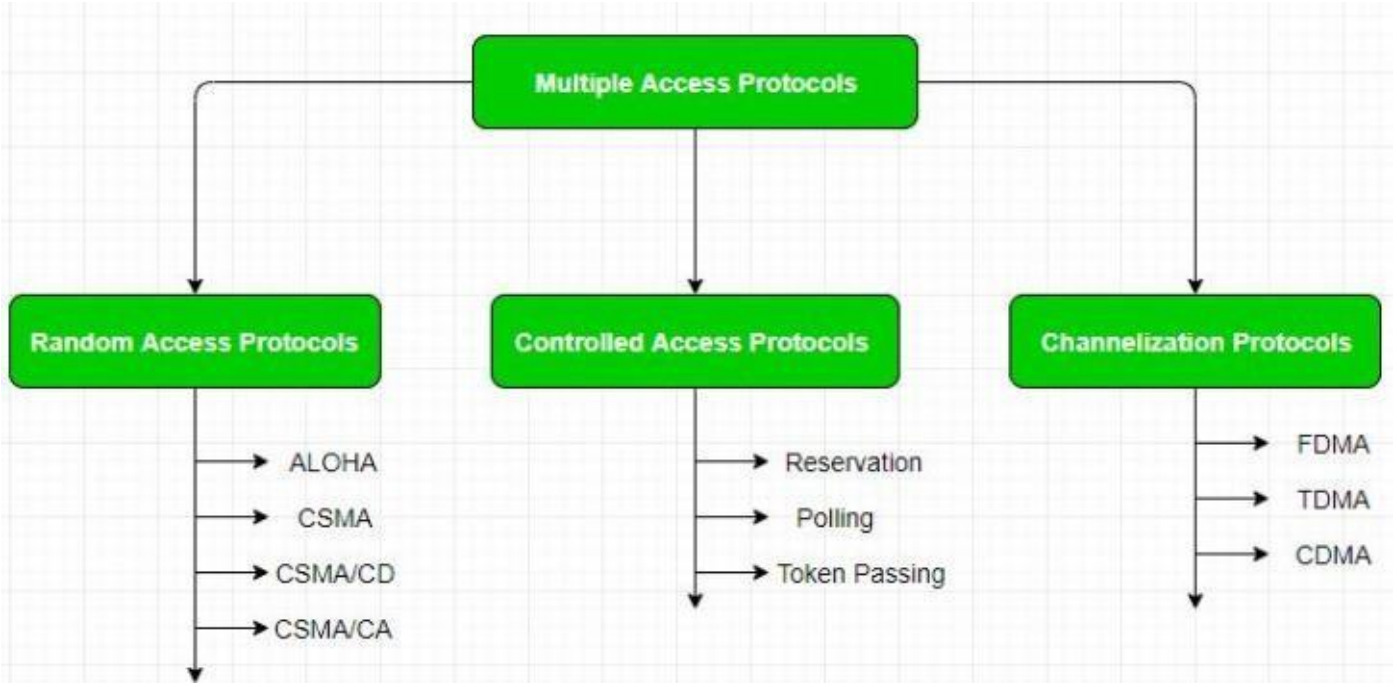
Multiple Access Protocols in Computer Network

The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

- Data Link Control
- Multiple Access Control

Data Link control –
The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control. For Data link control refer to – Stop and Wait ARQ

Multiple Access Control –
If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.
Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as –



1. Random Access Protocol: In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

(a) ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

(b) CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes-

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c) CSMA/CD – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer – Efficiency of CSMA/CD

(d) CSMA/CA – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.
CSMA/CA avoids collision by:

1. **Interframe space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access:

In this, the data is sent by that station which is approved by all other stations. For further details refer – Controlled Access Protocols

3. Channelization:

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no to bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
  For more details refer – Circuit Switching
- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly data from different stations can be transmitted simultaneously in

Wireless Communication - Overview

Wireless communication involves the transmission of information over a distance without the help of wires, cables or any other forms of electrical conductors.

Wireless communication is a broad term that incorporates all procedures and forms of connecting and communicating between two or more devices using a wireless signal through wireless communication technologies and devices.

Features of Wireless Communication

The evolution of wireless technology has brought many advancements with its effective features.

- The transmitted distance can be anywhere between a few meters (for example, a television's remote control) and thousands of kilometers (for example, radio communication).
- Wireless communication can be used for cellular telephony, wireless access to the internet, wireless home networking, and so on.
- Other examples of applications of radio wireless technology include GPS units, garage door openers, wireless computer mice, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones.

Cellular Wireless Networks

Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc. The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems. Cellular networks use lower power, shorter range and more transmitters for data transmission.

Features of Cellular Systems

Wireless Cellular Systems solves the problem of spectral congestion and increases user capacity. The features of cellular systems are as follows −

- Offer very high capacity in a limited spectrum.
- Reuse of radio channel in different cells.
- Enable a fixed number of channels to serve an arbitrarily large number of users by reusing the channel throughout the coverage region.
- Communication is always between mobile and base station (not directly between mobiles).
- Each cellular base station is allocated a group of radio channels within a small geographic area called a cell.
- Neighboring cells are assigned different channel groups.
- By limiting the coverage area to within the boundary of the cell, the channel groups may be reused to cover different cells.
- Keep interference levels within tolerable limits.
- Frequency reuse or frequency planning.
- Organization of Wireless Cellular Network.

Cellular network is organized into multiple low power transmitters each 100w or less.

Shape of Cells

The coverage area of cellular networks are divided into **cells**, each cell having its own antenna for transmitting the signals. Each cell has its own frequencies. Data communication in cellular networks is served by its base station transmitter, receiver and its control unit.

The shape of cells can be either square or hexagon −

Square

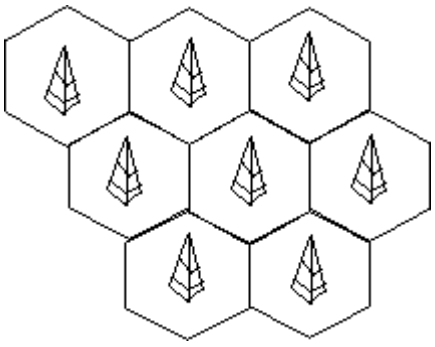
A square cell has four neighbors at distance **d** and four at distance Root **2 d**

- Better if all adjacent antennas equidistant
- Simplifies choosing and switching to new antenna

Hexagon

A hexagon cell shape is highly recommended for its easy coverage and calculations. It offers the following advantages −

- Provides equidistant antennas
- Distance from center to vertex equals length of side



Frequency Reuse

Frequency reusing is the concept of using the same radio frequencies within a given area, that are separated by considerable distance, with minimal interference, to establish communication.

Frequency reuse offers the following benefits −

- Allows communications within cell on a given frequency
- Limits escaping power to adjacent cells
- Allows re-use of frequencies in nearby cells
- Uses same frequency for multiple conversations
- 10 to 50 frequencies per cell

For example, when **N** cells are using the same number of frequencies and **K** be the total number of frequencies used in systems. Then each **cell frequency** is calculated by using the formulae **K/N**.

In Advanced Mobile Phone Services (AMPS) when K = 395 and N = 7, then frequencies per cell on an average will be 395/7 = 56. Here, **cell frequency** is 56.

Propagation Losses

Antenna and Wave propagation plays a vital role in wireless communication networks. An antenna is an electrical conductor or a system of conductors that radiates/collects (transmits or receives) electromagnetic energy into/from space. An idealized isotropic antenna radiates equally in all directions.

Propagation Mechanisms

Wireless transmissions propagate in three modes. They are −

- Ground-wave propagation
- Sky-wave propagation
- Line-of-sight propagation

Ground wave propagation follows the contour of the earth, while **sky wave propagation** uses reflection by both earth and ionosphere.

Line of sight propagation requires the transmitting and receiving antennas to be within the line of sight of each other. Depending upon the frequency of the underlying signal, the particular mode of propagation is followed.

Examples of ground wave and sky wave communication are **AM radio** and **international broadcasts** such as BBC. Above 30 MHz, neither ground wave nor sky wave propagation operates and the communication is through line of sight.

Transmission Limitations

In this section, we will discuss the various limitations that affect electromagnetic wave transmissions. Let us start with attenuation.

Attenuation

The strength of signal falls with distance over transmission medium. The extent of attenuation is a function of distance, transmission medium, as well as the frequency of the underlying transmission.

Distortion

Since signals at different frequencies attenuate to different extents, a signal comprising of components over a range of frequencies gets distorted, i.e., the shape of the received signal changes.

A standard method of resolving this problem (and recovering the original shape) is to amplify higher frequencies and thus equalize attenuation over a band of frequencies.

Dispersion

Dispersion is the phenomenon of spreading of a burst of electromagnetic energy during propagation. Bursts of data sent in rapid succession tend to merge due to dispersion.

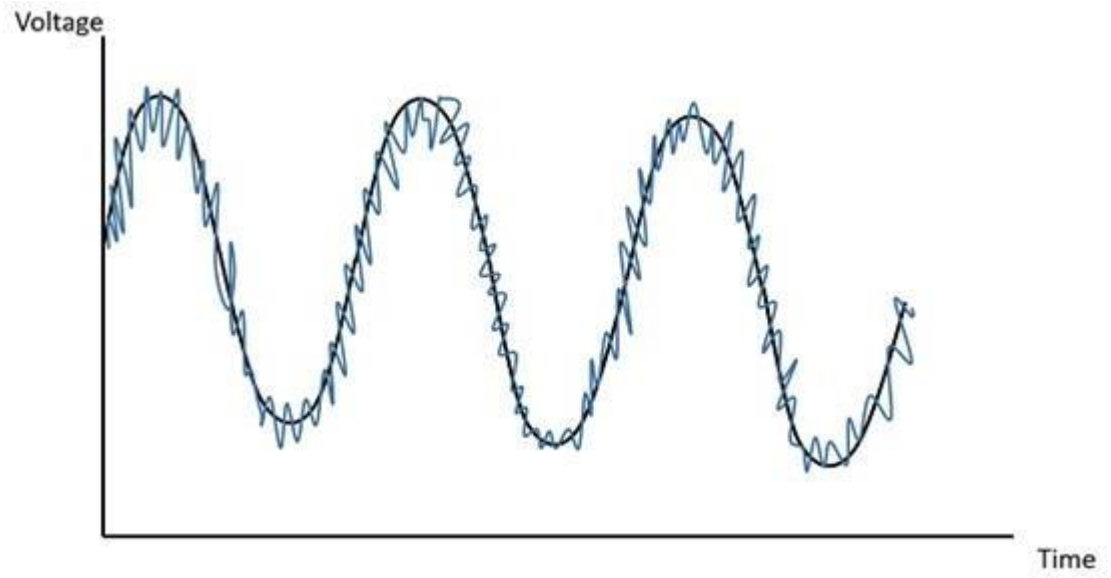
Noise

The most pervasive form of noise is thermal noise, which is often modeled using an additive Gaussian model. Thermal noise is due to thermal agitation of electrons and is uniformly distributed across the frequency spectrum.

Other forms of noise include −

- **Inter modulation noise** (caused by signals produced at frequencies that are sums or differences of carrier frequencies)
- **Crosstalk** (interference between two signals)
- **Impulse noise** (irregular pulses of high energy caused by external electromagnetic disturbances).

While an impulse noise may not have a significant impact on analog data, it has a noticeable effect on digital data, causing **burst errors**.



The above figure clearly illustrates how the noise signal overlaps the original signal and tries to change its characteristics.

Fading

Fading refers to the variation of the signal strength with respect to time/distance and is widely prevalent in wireless transmissions. The most common causes of fading in the wireless environment are multipath propagation and mobility (of objects as well as the communicating devices).

Multipath propagation

In wireless media, signals propagate using three principles, which are reflection, scattering, and diffraction.

- **Reflection** occurs when the signal encounters a large solid surface, whose size is much larger than the wavelength of the signal, e.g., a solid wall.
- **Diffraction** occurs when the signal encounters an edge or a corner, whose size is larger than the wavelength of the signal, e.g., an edge of a wall.
- **Scattering** occurs when the signal encounters small objects of size smaller than the wavelength of the signal.

One consequence of multipath propagation is that multiple copies of a signal propagation along multiple different paths, arrive at any point at different times. So the signal received at a point is not only affected by the **inherent noise, distortion, attenuation**, and **dispersion** in the channel but also the **interaction of signals** propagated along multiple paths.

Delay spread

Suppose we transmit a probing pulse from a location and measure the received signal at the recipient location as a function of time. The signal power of the received signal spreads over time due to multipath propagation.

The delay spread is determined by the density function of the resulting spread of the delay over time. **Average delay spread** and **root mean square delay spread** are the two parameters that can be calculated.

Doppler spread

This is a measure of **spectral broadening** caused by the rate of change of the mobile radio channel. It is caused by either relative motion between the mobile and base station or by the movement of objects in the channel.

When the velocity of the mobile is high, the Doppler spread is high, and the resulting channel variations are faster than that of the baseband signal, this is referred to as **fast fading**. When channel variations are slower than the baseband signal variations, then the resulting fading is referred to as **slow fading**.

Wireless Communication - Bluetooth

Bluetooth wireless technology is a short range communications technology intended to replace the cables connecting portable unit and maintaining high levels of security. Bluetooth technology is based on **Ad-hoc technology** also known as **Ad-hoc Pico nets**, which is a local area network with a very limited coverage.

History of Bluetooth

WLAN technology enables device connectivity to infrastructure based services through a wireless carrier provider. The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of **Personal Area Networks (PANs)**.

- Ericsson's Bluetooth project in 1994 defines the standard for PANs to enable communication between mobile phones using low power and low cost radio interfaces.
- In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a defacto standard for PANs.

- IEEE has approved a Bluetooth based standard named IEEE 802.15.1 for Wireless Personal Area Networks (WPANs). IEEE standard covers MAC and Physical layer applications.

Bluetooth specification details the entire protocol stack. Bluetooth employs Radio Frequency (RF) for communication. It makes use of **frequency modulation** to generate radio waves in the **ISM** band.

Symbol of Bluetooth

An example of a Bluetooth device

The usage of Bluetooth has widely increased for its special features.

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.
- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.
- Bluetooth offers interactive conference by establishing an adhoc network of laptops.
- Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

Piconets and Scatternets

Bluetooth enabled electronic devices connect and communicate wirelessly through shortrange devices known as **Piconets**. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave the specification allows a mechanism for **master** and **slave** to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.

When more than two Bluetooth devices communicate with one another, this is called a **PICONET**. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the **master**.

The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme which is shown below.

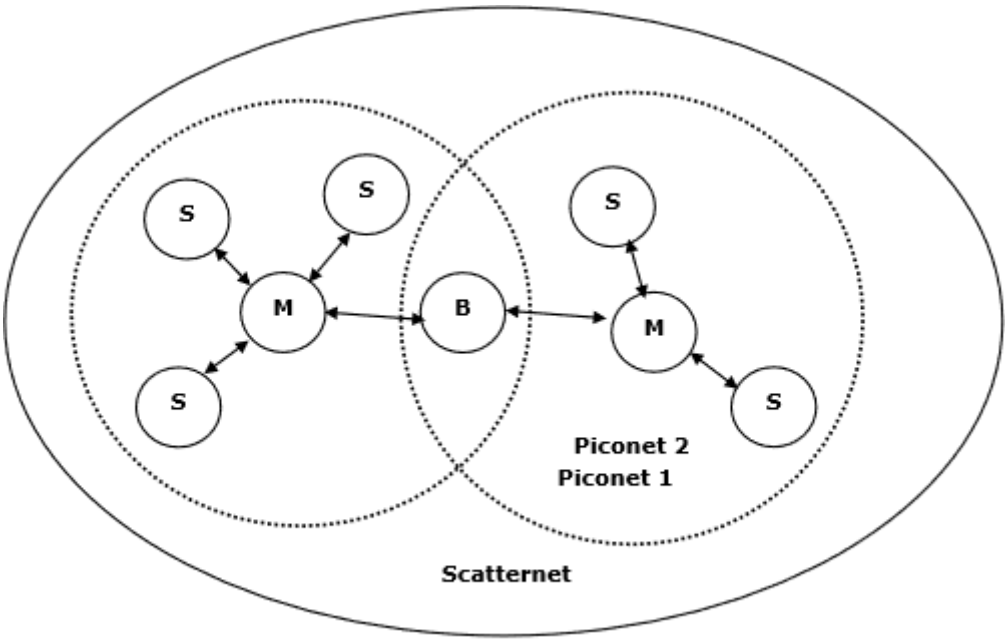


Figure: Piconets and Scatternets

The features of Piconets are as follows −

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique **48-bit address** of master.
- Each device can communicate simultaneously with up to seven other devices within a single Piconet.
- Each device can communicate with several piconets simultaneously.
- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.
- There is no direct connection between the slaves and all the connections are essentially master-to-slave or slave-to-master.
- Slaves are allowed to transmit once these have been polled by the master.
- Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
- A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.
- It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.
- Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as **Scatternet**.

Spectrum

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ, using a spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. the GHZ ISM band is available and unlicensed in most countries.

Range

Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Data rate

Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

Wireless - Advantages

Wireless communication involves transfer of information without any physical connection between two or more points. Because of this absence of any 'physical infrastructure', wireless communication has certain advantages. This would often include collapsing distance or space.

Wireless communication has several advantages; the most important ones are discussed below −

Cost effectiveness

Wired communication entails the use of connection wires. In wireless networks, communication does not require elaborate physical infrastructure or maintenance practices. Hence the cost is reduced.

Example − Any company providing wireless communication services does not incur a lot of costs, and as a result, it is able to charge cheaply with regard to its customer fees.

Flexibility

Wireless communication enables people to communicate regardless of their location. It is not necessary to be in an office or some telephone booth in order to pass and receive messages.

Miners in the outback can rely on satellite phones to call their loved ones, and thus, help improve their general welfare by keeping them in touch with the people who mean the most to them.

Convenience

Wireless communication devices like mobile phones are quite simple and therefore allow anyone to use them, wherever they may be. There is no need to physically connect anything in order to receive or pass messages.

Example − Wireless communications services can also be seen in Internet technologies such as Wi-Fi. With no network cables hampering movement, we can now connect with almost anyone, anywhere, anytime.

Speed

Improvements can also be seen in speed. The network connectivity or the accessibility were much improved in accuracy and speed.

Example − A wireless remote can operate a system faster than a wired one. The wireless control of a machine can easily stop its working if something goes wrong, whereas direct operation can’t act so fast.

Accessibility

The wireless technology helps easy accessibility as the remote areas where ground lines can’t be properly laid, are being easily connected to the network.

Example − In rural regions, online education is now possible. Educators no longer need to travel to far-flung areas to teach their lessons. Thanks to live streaming of their educational modules.

Constant connectivity

Constant connectivity also ensures that people can respond to emergencies relatively quickly.

Example − A wireless mobile can ensure you a constant connectivity though you move from place to place or while you travel, whereas a wired land line can't.

Forward Error Correction (FEC)

Forward error correction (FEC) is an error correction technique to detect and correct a limited number of errors in transmitted data without the need for retransmission.

In this method, the sender sends a redundant error-correcting code along with the data frame. The receiver performs necessary checks based upon the additional redundant bits. If it finds that the data is free from errors, it executes error-correcting code that generates the actual frame. It then removes the redundant bits before passing the message to the upper layers.

Advantages and Disadvantages

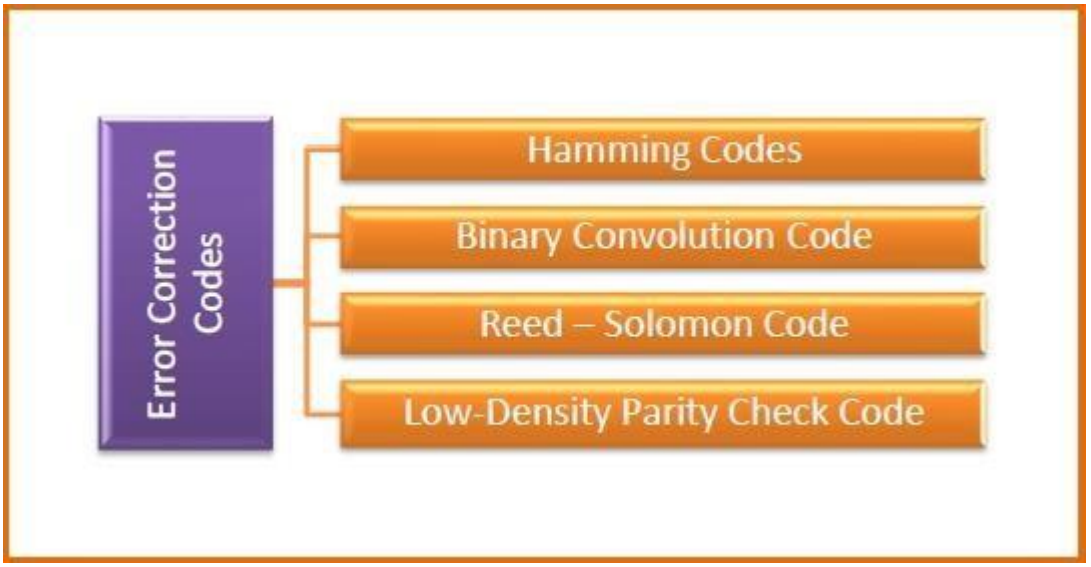
- Because FEC does not require handshaking between the source and the destination, it can be used for broadcasting of data to many destinations simultaneously from a single source.
- Another advantage is that FEC saves bandwidth required for retransmission. So, it is used in real time systems.
- Its main limitation is that if there are too many errors, the frames need to be retransmitted.

Error Correction Codes for FEC

Error correcting codes for forward error corrections can be broadly categorized into two types, namely, block codes and convolution codes.

- **Block codes** − The message is divided into fixed-sized blocks of bits to which redundant bits are added for error correction.
- **Convolutional codes** − The message comprises of data streams of arbitrary length and parity symbols are generated by the sliding application of a Boolean function to the data stream.

There are four popularly used error correction codes.



- **Hamming Codes** − It is a block code that is capable of detecting up to two simultaneous bit errors and correcting single-bit errors.
- **Binary Convolution Code** − Here, an encoder processes an input sequence of bits of arbitrary length and generates a sequence of output bits.
- **Reed - Solomon Code** − They are block codes that are capable of correcting burst errors in the received data block.
- **Low-Density Parity Check Code** − It is a block code specified by a parity-check matrix containing a low density of 1s. They are suitable for large block sizes in very noisy channels.

UNIT - III

Packet Switching

- **Packet switching** is a method of transferring the data to a network in form of packets.
- In order to transfer the file fast and efficient manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**.
- At the destination, all these small-parts (packets) has to be reassembled, belonging to the same file. A packet composes of payload and various control information.
- No pre-setup or reservation of resources is needed.
- Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first store that packet then forward.
- This technique is very beneficial because packets may get discarded at any hop due to some reason.
- More than one path is possible between a pair of source and destination. Each packet contains Source and destination address using which they independently travel through the network.
- In other words, packets belonging to the same file may or may not travel through the same path.

- If there is congestion at some path, packets are allowed to choose different path possible over existing network.
- Packet-Switched networks were designed to overcome the weaknesses of Circuit-Switched networks since circuit-switched networks were not very effective for small messages.

Advantage of Packet Switching over Circuit Switching :

- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as destination can detect the missing packet.
- More fault tolerant because packets may follow different path in case any link is down, Unlike Circuit Switching.
- Cost effective and comparatively cheaper to implement.

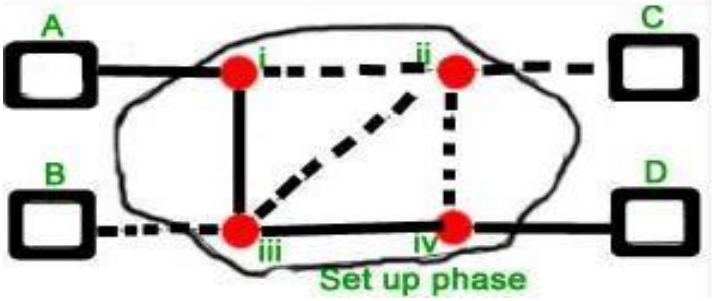
Disadvantage of Packet Switching over Circuit Switching :

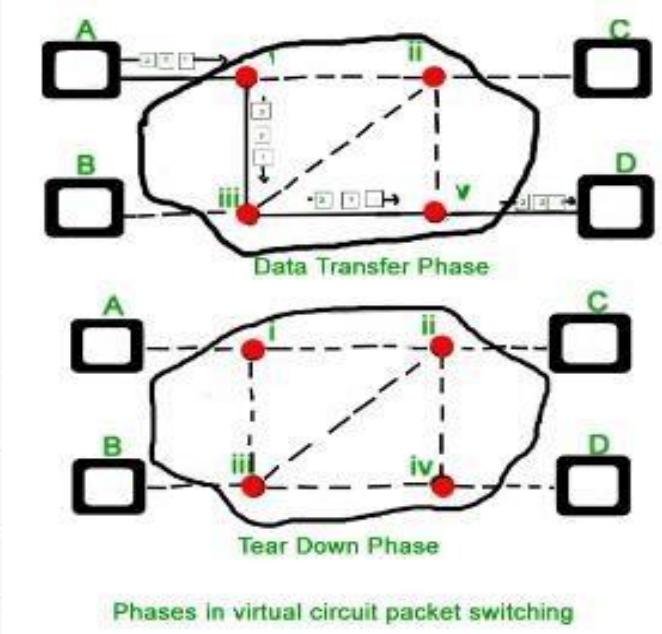
- Packet Switching don't give packets in order, whereas Circuit Switching provides ordered delivery of packets because all the packets follow the same path.
- Since the packets are unordered, we need to provide sequence numbers to each packet.
- Complexity is more at each node because of the facility to follow multiple path.
- Transmission delay is more because of rerouting.
- Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.

Modes of Packet Switching :

1. **Connection-oriented Packet Switching (Virtual Circuit) :-** Before starting the transmission, it establishes a logical path or virtual connection using signalling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence number. Overall, three phases takes place here- Setup, data transfer and tear down phase.

   All address information is only transferred during setup phase. Once the route to destination is discovered, entry is added to switching table of each intermediate node. During data transfer, packet header (local header) may contain information such as length, timestamp, sequence number etc. Connection-oriented switching is very useful in switched WAN. Some popular protocols which use Virtual Circuit Switching approach are X.25, Frame-Relay, ATM and MPLS(Multi-Protocol Label Switching).

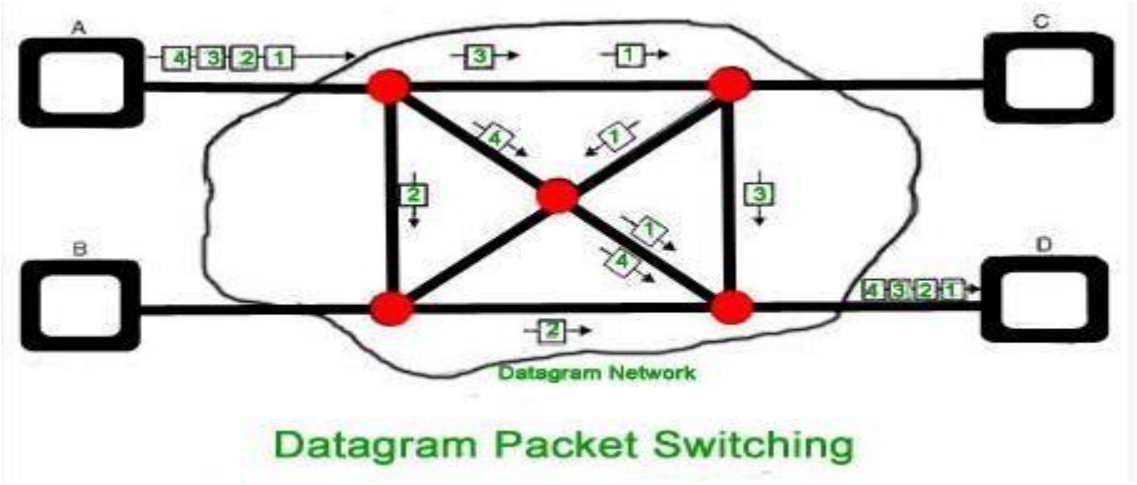




Phases in virtual circuit packet switching

2. **Connectionless Packet Switching (Datagram) :-** Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.
   Packet delivery is not guaranteed in connectionless packet switching, so the reliable delivery must be provided by end systems using additional protocols.

Network



Datagram Packet Switching

Performance

- **Network performance** without the use of specially designed processes and tools, will eat into a company's productivity, and as well as incur financial losses for every minute of downtime.
- Network demands increase every day, and that makes it very important for measurements to be carried out properly.
- The qualitative and quantitative aspects of a network need to be captured in each measurement procedure, so that all needed data are generated for use, in case of any occurrence of network performance problems.
- A challenge that was commonly faced while trying to determine network performance was the lack of a real-time provision that enables the instant detection of problems in transmission, routing, network paths, servers, bandwidth, etc.

- This meant that IT professionals had to conduct network measurement half blind until they stumble upon the problems halfway.
- Most of the times, data gathered is never complete, as slight errors in latency or packet loss might not be detected, thus leading to technical oversights that can lead to IT crisis in the long run.

Measurement by Metrics

- Some of the common metrics used to measure network performance include latency, packet loss indicators, jitter, retransmission, bandwidth, and throughput.

Latency

- Latency can be used to measure network delays, focusing on the time spent in the successful transfer of packets or a packet of data from one point to another within a network.
- A network that is working perfectly should have zero or near-zero latency.
- The measurement of latency is given in Milliseconds and is determined or compared to the speed of light, which is at 186,000 Miles/sec.
- To be able to measure the latency of a network, you will have to take into account

- The physical distance between the points in question
- The fastest route between the ends; and
- The delays which might have been caused by hardware and applications processing the data transmission

Packet loss

Packet loss refers to the number of packets that were successfully sent out from one point in a network, but never got to their destination.

- To be able to measure this, the focus will have to be laid on capturing data traffic on the points involved – both the sender and the receiver – and subsequently determining the number of packets that didn't get to their destination.
- This provides a measure for determining network performance, as the lost packets are expressed as a percentage of the total number of sent packets.
- Often, more than 3% of packet loss implies that the network is not performing optimally.

Retransmission

- Packet loss refers to the number of packets that were successfully sent out from one point in a network, but never got to their destination.
- To be able to measure this, the focus will have to be laid on capturing data traffic on the points involved – both the sender and the receiver – and subsequently determining the number of packets that didn't get to their destination.
- This provides a measure for determining network performance, as the lost packets are expressed as a percentage of the total number of sent packets.
- Often, more than 3% of packet loss implies that the network is not performing optimally.

Bandwidth and throughput

- These two work hand in hand in measuring network performance.
- Bandwidth refers to the number of data that can be transmitted from one point to another in a network, within a given time. Throughput,

- on the other hand, is the number of data that actually got transmitted from one point to another within the given time.
- A network performance measurement is created when the throughput is analyzed against the bandwidth.
- A throughput that is significantly lower than the bandwidth indicates a poor network performance.

Jitter

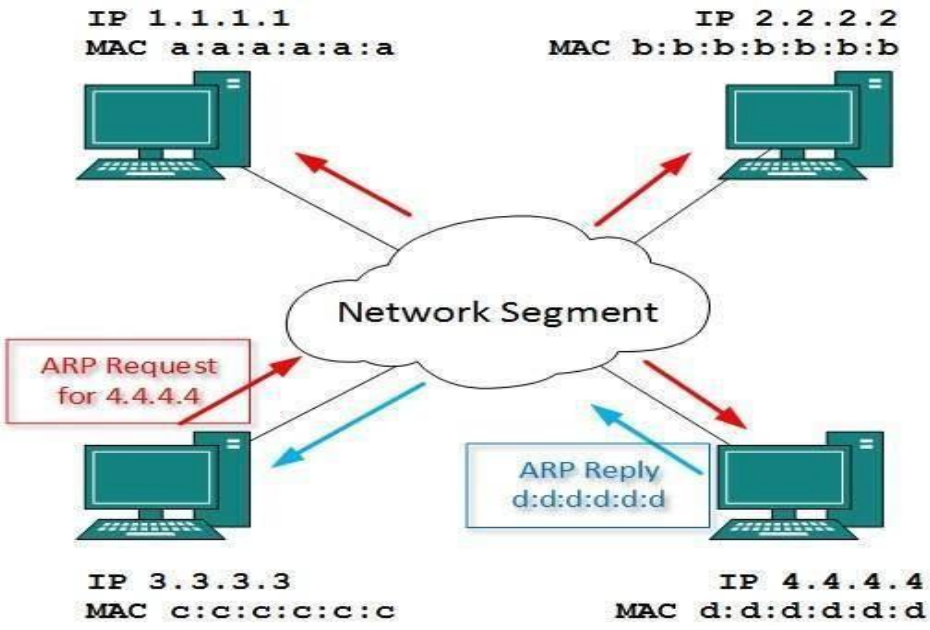
- The measurement of jitter can be detected while making use of the network for VoIP applications,
- By determining the closeness of the VoIP audio or video to real physical interaction.
- Otherwise, it is identified as a manifestation of uneven or increased latency or the disruption that occurs during the flow of data packets across the network.

Network Layer Protocols

- Every computer in a network has an IP address by which it can be uniquely identified and addressed.
- An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts.
- A computer can have one IP at one instance of time and another IP at some different time.

Address Resolution Protocol(ARP)

- While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network.
- A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.
- On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes.
- This way, for Layer-2 communication to take place, a mapping between the two is required.



- To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking,
- ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.
- Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol.
- This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.
- Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol (ICMP)

- ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol.
- After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.
- Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP.
- ICMP contains dozens of diagnostic and error reporting messages.
- ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts.
- When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for host addressing
- **Class B** - it uses first two octets for network addresses and last two for host addressing
- **Class C** - it uses first three octets for network addresses and last one for host addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

Internet Protocol Version 6 (IPv6)

- Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6.
- IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.
- IPv6 has introduced Anycast addressing but has removed the concept of broadcasting.
- IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet.
- This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers.
- This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.
- IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.
- IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6.
- There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4.

These are:

- Dual stack implementation
- Tunneling
- NAT-PT

Routing Algorithms

- **Routing** is process of establishing the routes that data packets must follow to reach the destination.
- In this process, a routing table table is created which contains information regarding routes which data packets follow.
- Various routing algorithm are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach destination efficiently.

Classification of Routing Algorithms:

The routing algorithms can be classified as follows:

1. Adaptive Algorithms –

- These are the algorithms which change their routing decisions whenever network topology or traffic load changes.
- The changes in routing decisions are reflected in the topology as well as traffic of the network.
- Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes.
- Optimization parameters are distance, number of hops and estimated transit time.

Further these are classified as follows:

- **(a) Isolated –** In this method each, node makes its routing decisions using the information it has without seeking information from other nodes. The sending nodes doesn't have information about status of particular link.
- **(b) Centralized –** In this method, a centralized node has entire information about the network and makes all the routing decisions
- **(c) Distributed –** In this method, the node receives information fro its neighbors and then takes the decision about routing the packets.

2. Non-Adaptive Algorithms –

- These are the algorithms which do not change their routing decisions once they have been selected.
- This is also known as static routing as route to be taken is computed in advance and downloaded to routers when router is booted.

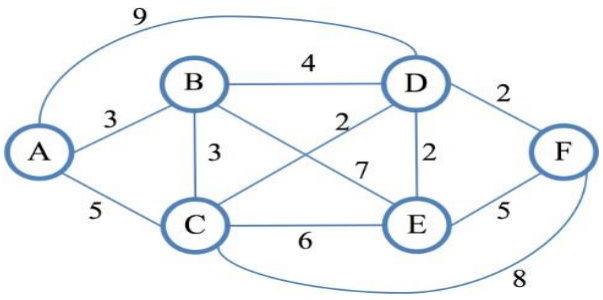
Further these are classified as follows:

- **(a) Flooding –** This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count and spanning tree.
- **(b) Random walk –** In this method, packets are sent host by host or node by node to one of its neighbors randomly. This is highly robust method which is usually implemented by sending packets onto the link which is least queued.

Routing Algorithms

Shortest Path Routing:

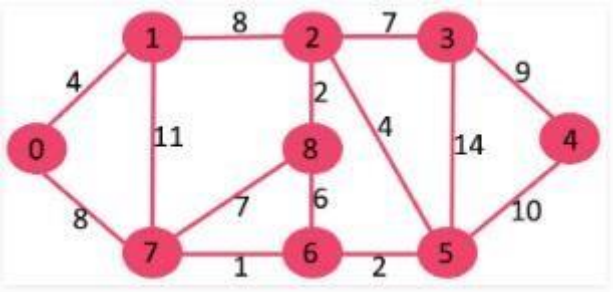
- Links between routers have a cost associated with them. In general, it could be a function of distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, router processing speed, etc.
- The shortest path algorithm just finds the least expensive path through the network, based on the cost function.
- Examples: Dijkstra's algorithm.



Dijkstra algorithm:

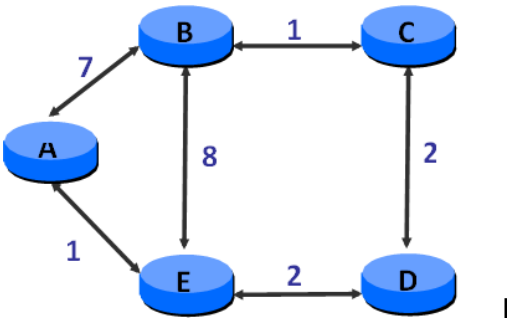
- Each node is labeled (in parentheses) with its distance from the source node along the best known path.
- Initially, no paths are known, so all nodes are labeled with infinity.
- As the algorithm proceeds and paths are found, the labels may change, reflecting better paths.

- A label may be either **tentative or permanent**. Initially, all labels are tentative.
- When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed.



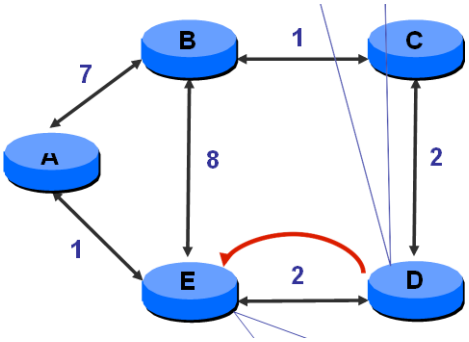
Distance Vector Routing:

- In this routing scheme, each router periodically shares its knowledge about the entire network with its neighbours.
- Each router has a table with information about the network. These tables are updated by exchanging information with the immediate neighbours.
- It is also known as **Belman-Ford** or Ford-Fulkerson Algorithm.
- It is used in the original ARPANET, and in the Internet as RIP.
- Neighbouring nodes in the subnet exchange their tables periodically to update each other on the state of the subnet (which makes this a dynamic algorithm). If a neighbour claims to have a path to a node which is shorter than your path, you start using that neighbour as the route to that node.
- Distance vector protocols (a vector contains both distance and direction), such as RIP, determine the path to remote networks using hop count as the metric. A hop count is defined as the number of times a packet needs to pass through a router to reach a remote destination.
- For IP RIP, the maximum hop is 15. A hop count of 16 indicates an unreachable network. Two versions of RIP exist version 1 and version 2.
- IGRP is another example of a distance vector protocol with a higher hop count of 255 hops.
- Periodic updates are sent at a set interval. For IP RIP, this interval is 30 seconds.
- Updates are sent to the broadcast address 255.255.255.255. Only devices running routing algorithms listen to these updates.
- When an update is sent, the entire routing table is sent.



Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	∞	2	0

Info at node	Distance to Node				
	A	**B**	**C**	**D**	**E**
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	**4**	2	0



Link State Routing:

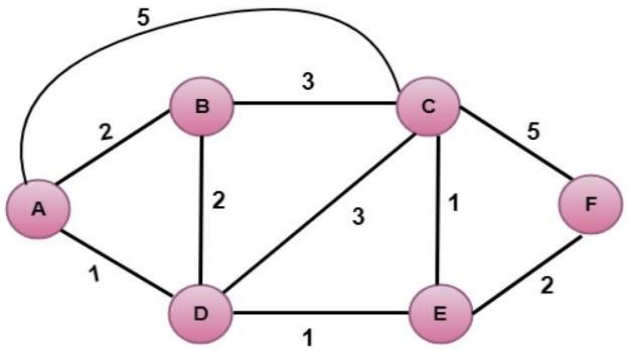
- The following sequence of steps can be executed in the Link State Routing.
- The basis of this advertising is a short packed called a Link State Packet (LSP).
- OSPF (Open shortest path first) and IS-IS are examples of Link state routing.
- Link State Packet(LSP) contains the following information:

    1. The ID of the node that created the LSP;
    2. A list of directly connected neighbours of that node, with the cost of the link to each one;
    3. A sequence number;
    4. A time to live(TTL) for this packet.

- When a router floods the network with information about its neighbourhood, it is said to be advertising.
    1. Discover your neighbours
    2. Measure delay to your neighbours
    3. Bundle all the information about your neighbours together
    4. Send this information to all other routers in the subnet
    5. Compute the shortest path to every router with the information you receive
    6. Each router finds out its own shortest paths to the other routers by using **Dijkstra's algorithm**.

- In link-state routing, each router shares its knowledge of its neighbourhood with all routers in the network.
- Link-state protocols implement an algorithm called the shortest path first (SPF, also known as Dijkstra's Algorithm) to determine the path to a remote destination.
- There is no hop-count limit. (For an IP datagram, the maximum time to live ensures that loops are avoided.)
- Only when changes occur, It sends all summary information every 30 minutes by default. Only devices running routing algorithms listen to these updates. Updates are sent to a multicast address.
- Updates are faster and convergence times are reduced. Higher CPU and memory requirements to maintain link-state databases.
- Link-state protocols maintain three separate tables:

    - **Neighbor table:** It contains a list of all neighbors, and the interface each neighbor is connected off of. Neighbors are formed by sending Hello packets.
    - **Topology table (Link- State table):** It contains a map of all links within an area, including



each link's status.

- **Routing table:** It contains the best routes to each particular destination.

Flooding Algorithm:

- Flooding is the static routing algorithm. In this algorithm, every incoming packet is sent on all outgoing lines except the line on which it has arrived.
- One major problem of this algorithm is that it generates a large number of duplicate packets on the network.
- To prevent from looping forever, each router decrements a hop count contained in the packet header.
- As soon as the hop counts decrements to zero, the router discards the packet.

Characteristics –

- All possible routes between Source and Destination is tried. A packet will always get through if path exists
- As all routes are tried, there will be atleast one route which is the shortest
- All nodes directly or indirectly connected are visited

Limitations –

- Flooding generates vast number of duplicate pakects
- Suitable damping mechanism must be used

Hop-Count –

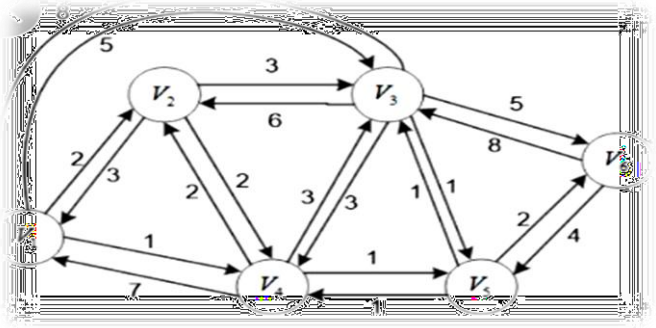
- A hop counter may be contained in the packet header which is decremented at each hop. with the packet being discarded when the counter becomes zero
- The sender initializes the hop counter. If no estimate is known, it is set to the full diameter of the subnet.
- Keep track of the packets which are responsible for flooding using a sequence number. Avoid sending them out a second time.

Advantages of Flooding :

- Highly Robust, emergency or immediate messages can be sent (eg military applications)
- Set up route in virtual circuit
- Flooding always chooses the shortest path
- Broadcast messages to all the nodes

- Several measures are takes to stop the duplication of packets. These are:
- 1. One solution is to include a hop counter in the header of each packet. This counter is decremented at each hop along the path. When this counter reaches zero the packet is discarded. Ideally, the hop counter should become zero at the destination hop, indicating that there are no more intermediate hops and destination is reached. This requires the knowledge of exact number of hops from a source to destination.
- 2. Another technique is to keep the track of the packed that have been flooded, to avoid sending them a second time. For this, the source router put a sequence number in each packet it receives from its hosts. Each router then needs a list per source router telling which sequence numbers originating at that source have already been seen. If an incoming packet is on the list, it is not flooded.

- 3. Another solution is to use **selective flooding.** In selective flooding the routers do not send every incoming packet out on every output line. Instead packet is sent only on those lines which are approximately going in the right direction.



Flow-Based Routing Algorithm:

- It is a non-adaptive routing algorithm.
- It takes into account both the topology and the load in this routing algorithm;
- We can estimate the flow between all pairs of routers.
- From the known average amount of traffic and the average length of a packet, you can compute the mean packet delays using queuing theory.
- Flow-based routing then seeks to find a routing table to minimize the average packet delay through the subnet.
- Given the line capacity and the flow, we can determine the delay. It needs to use the formula for delay time T.

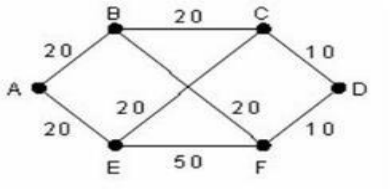
$$T = \frac{1}{\mu c - \lambda}$$

- Where, μ = Mean number of arrivals in packet/sec, 1/μ = The mean packet size in the bits, and c = Line capacity (bits/s).

- **Mean delay at each line T= 1/(μC -λ)**

  μC line capacity packet/sec

  λ traffic packet/sec



A subnet with link capacities given in kbps

Destination

Source	A	B	C	D	E	F
A		9 AB	4 ABC	1 ABFD	7 AE	4 AEF
B	9 BA		8 BC	3 BFD	2 BFE	4 BF
C	4 CBA	8 CB		3 CD	3 CE	2 CEF
D	1 DFBA	3 DFB	3 DC		3 DCE	4 DF
E	7 EA	2 EFB	3 EC	3 ECD		5 EF
F	4 FEA	4 FB	2 FEC	4 FD	5 FE	

The traffic in packets/sec and routing table

The Optimality Principal: This simple states that if router J is on the optimal path form router I to router k, then the optimal path from J to K also falls along this same path.

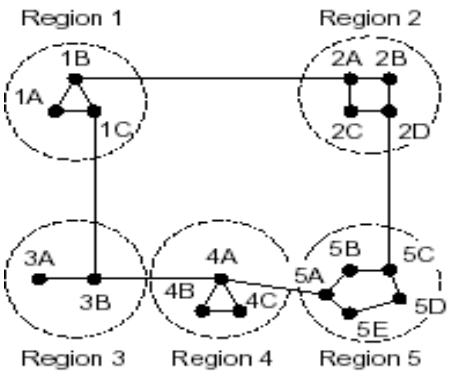
The routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.

For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.

- The full routing table for router 1A has 17 entries, as shown in (b).
- When routing is done hierarchically, as in (c), there are entries for all the local routers as before,but all other regions have been condensed into a single router,
- so all traffic for region 2 goes via the 1B -2A line, but the rest of the remote traffic goes via the
- 1C -3B line.
- Hierarchical routing has reduced the table from 17 to 7 entries.

Unfortunately, these gains in space are not free. There is apenalty to be paid, and this penalty is in the form of increased path length. For example, the best route from 1A to 5C is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.

Hieratical Routing



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Broadcast Routing

- Sending a packet to all destinations simultaneously is called **broadcasting**.
- The source simply sends a distinct packet to each destination. Not only is the method wasteful of bandwidth, but it also requires the source to have a complete list of all destinations.

Flooding.

- The problem with flooding as a broadcast technique is that it generates too many packets and consumes too much bandwidth.

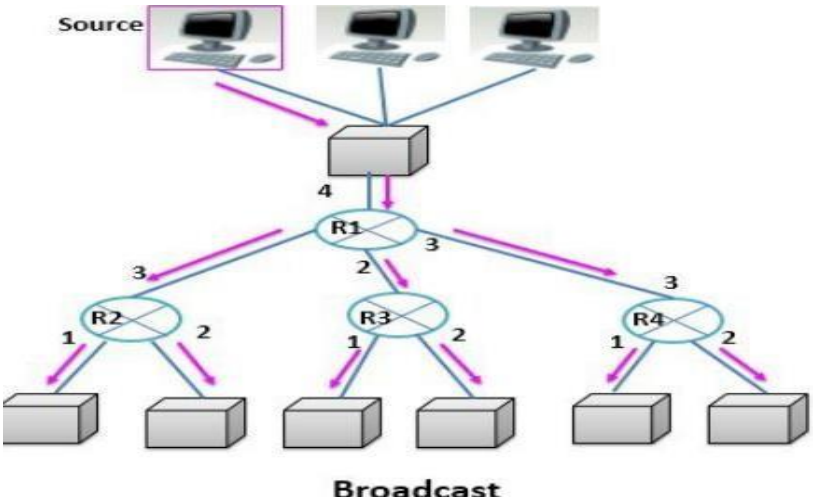
Multi-destination routing.

- If this method is used, each packet contains either a list of destinations or a bit map indicating the
- When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed. (An output line is needed if it is the best route to at least one of the destinations.)
- The router generates a new copy of the packet for each output line to be used and includes in each packet only those destinations that are to use the line. In effect, the destination set is partitioned among the output lines.
- After a sufficient number of hops, each packet will carry only one destination and can be treated as a normal packet.
- A fourth broadcast algorithm makes explicit use of the sink tree for the router initiating the broadcast—or any other convenient spanning tree for that matter.
- A **spanning tree** is a subset of the subnet that includes all the routers but contains no loops.
- If each router knows which of its lines belong to the spanning tree, it can copy an incoming broadcast packet onto all the spanning tree lines except the one it arrived on.

Reverse path forwarding.

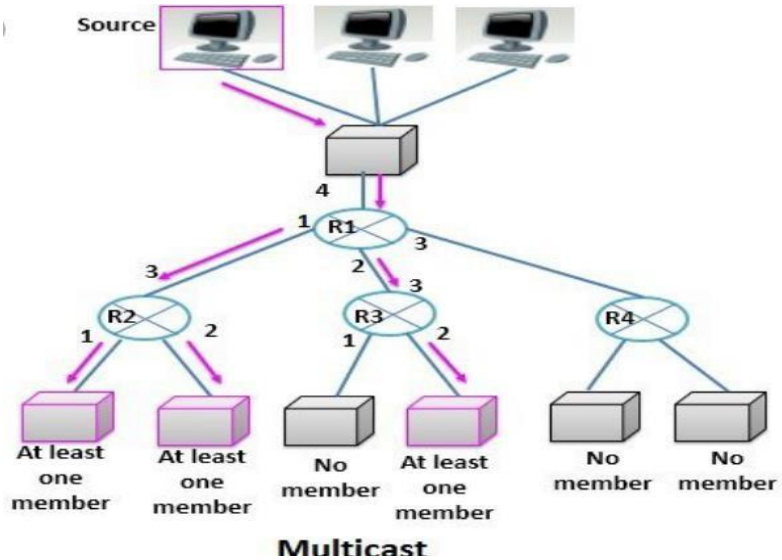
- When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast.
- If so, there is an excellent chance that the broadcast packet itself followed the best route from the router and is therefore the first copy to arrive at the router.
- This being the case, the router forwards copies of it onto all lines except the one it arrived on. If, however, the broadcast packet arrived on a line other than the preferred one for reaching the

source, the packet is discarded as a likely duplicate.



Multicast Routing

- Sending messages to well-defined groups that are numerically large in size, but small compared to the network as a whole is called **multicasting**. To do multicasting, group management is required, but that is not concern of routers. What is of concern is that when a process joins a group, it informs its host of this fact. It is important that routers know which of their hosts belong to which group. Either hosts must inform their routers about changes in group membership, or routers must query their hosts periodically.
- To do multicast routing, each router computes a spanning tree covering all other routers in the subnet. When a process sends a multicast packet to a group, the first router examines its spanning tree ad prunes it, removing all lines that do not lead to hosts that are members of the group.



- The simplest way of pruning the panning tree is under Link State routing when each router is aware of the complete subnet topology, including which hosts belong to which groups.

Then the spanning tree can be pruned by staring at the end to each path and working toward the root, removing all routers that do not belong the group in question.

- A different pruning strategy is followed with distance vector routing, reverse path forwarding algorithm. Whenever a router with no hosts interested in a particular group and no connections to other routers receives a multicast message for that group, it responds with a PRUNE message, telling the sender not to send it any more multicasts for that group. When a router with no group members among its own hosts has received such messages on all its lines, it, too, can respond with a PRUINE message. In this way, the subnet is recursively pruned.
- One potential disadvantage of this algorithm is that it scales poorly to large networks.
- An alternative design uses **core-base trees.** Here a single spanning tree per group is computed, with the root (the core) near the middle of the group. To send a multicast message, a host sends it to the core, which then does the multicast along the spanning tree. Although this tree will not be optimal for all sources, the reduction in storage costs from m trees to one tree per group is a major saving.

Internet Protocols

Transmission Control Protocol (TCP)

- TCP is a connection oriented protocol and offers end-to-end packet delivery.
- It acts as back bone for connection.

It exhibits the following key features:

- Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.
- TCP is a reliable and connection oriented protocol.
- TCP offers:
  - ✓ Stream Data Transfer.
  - ✓ Reliability.
  - ✓ Efficient Flow Control
  - ✓ Full-duplex operation.
  - ✓ Multiplexing.
- TCP offers connection oriented end-to-end packet delivery.

- TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect to receive.
- It retransmits the bytes not acknowledged with in specified time period.

TCP Services

TCP offers following services to the processes at the application layer:

Stream Deliver Service

TCP protocol is stream oriented because it allows the sending process to send data as stream of bytes and the receiving process to obtain data as stream of bytes.

Sending and Receiving Buffers

It may not be possible for sending and receiving process to produce and obtain data at same speed, therefore, TCP needs buffers for storage at sending and receiving ends.

Bytes and Segments

The Transmission Control Protocol (TCP), at transport layer groups the bytes into a packet. This packet is called segment. Before transmission of these packets, these segments are encapsulated into an IP datagram.

Full Duplex Service

Transmitting the data in duplex mode means flow of data in both the directions at the same time.

Connection Oriented Service

TCP offers connection oriented service in the following manner:

1. TCP of process-1 informs TCP of process – 2 and gets its approval.
2. TCP of process – 1 and TCP of process – 2 and exchange data in both the two directions.
3. After completing the data exchange, when buffers on both sides are empty, the two TCP's destroy their buffers.

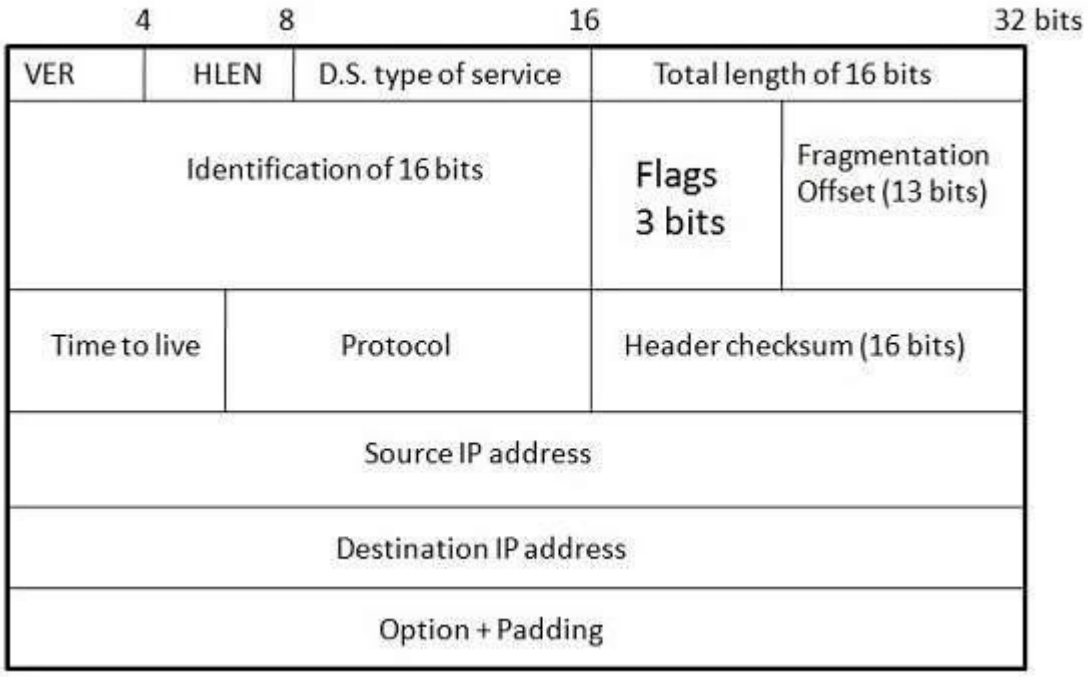
Reliable Service

For sake of reliability, TCP uses acknowledgement mechanism.

Internet Protocol (IP)

- Internet Protocol is **connectionless** and **unreliable** protocol.
- It ensures no guarantee of successfully transmission of data.
- In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Internet protocol transmits the data in form of a datagram as shown in the following diagram:



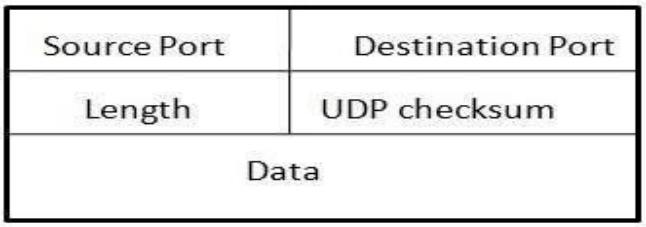
Points to remember:

- The length of datagram is variable.
- The Datagram is divided into two parts: **header** and **data.**
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.

User Datagram Protocol (UDP)

- UDP is connectionless and unreliable protocol.
- It doesn't require making a connection with the host to exchange data.
- Since UDP is unreliable protocol, there is no mechanism for ensuring that data sent is received.
- UDP transmits the data in form of a datagram.

The UDP datagram consists of five parts as shown in the following diagram:



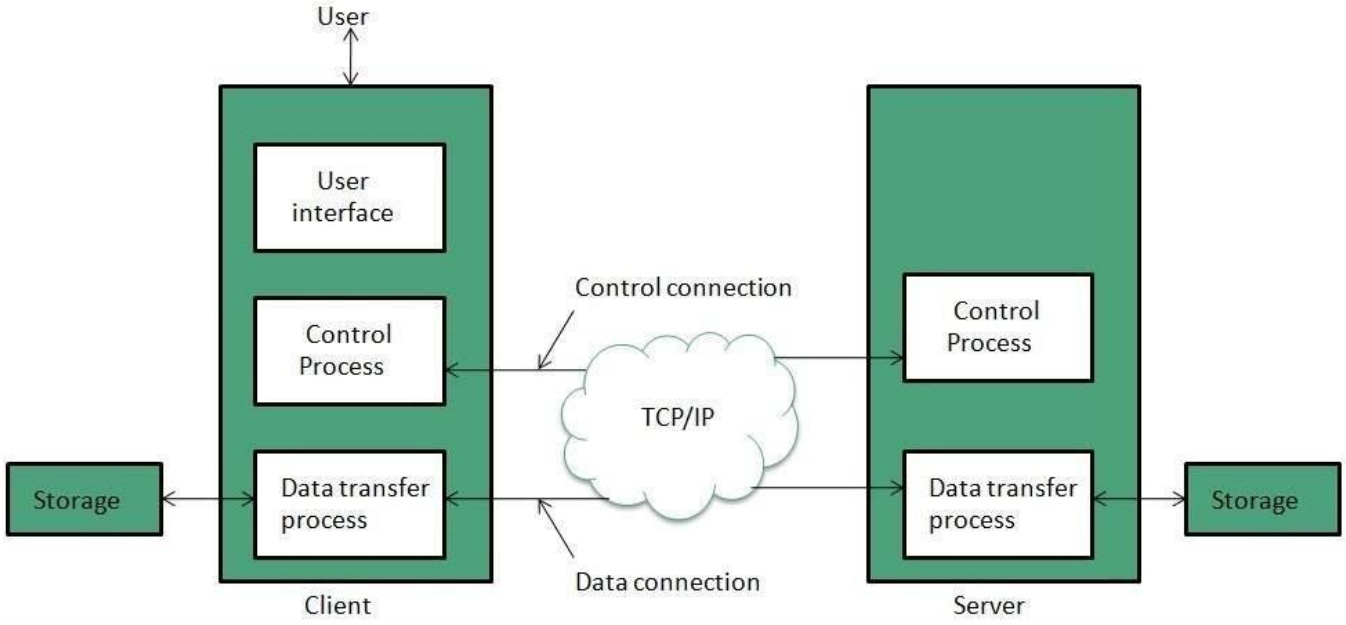
Points to remember:

- UDP is used by the application that typically transmit small amount of data at one time.
- UDP provides protocol port used i.e. UDP message contains both source and destination port number, that makes it possible for UDP software at the destination to deliver the message to correct application program.

File Transfer Protocol (FTP)

FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:

- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- **Control connection** is made between **control processes** while **Data Connection** is made between<="" b="">
- FTP uses **port 21** for the control connection and **Port 20** for the data connection.



Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol is also used to transfer the files but it transfers the files without authentication. Unlike FTP, TFTP does not separate control and data information. Since there is no authentication exists, TFTP lacks in security features therefore it is not recommended to use TFTP.

Key points

- TFTP makes use of UDP for data transport. Each TFTP message is carried in separate UDP datagram.
- The first two bytes of a TFTP message specify the type of message.
- The TFTP session is initiated when a TFTP client sends a request to upload or download a file.
- The request is sent from an ephemeral UDP port to the **UDP port 69** of an TFTP server.

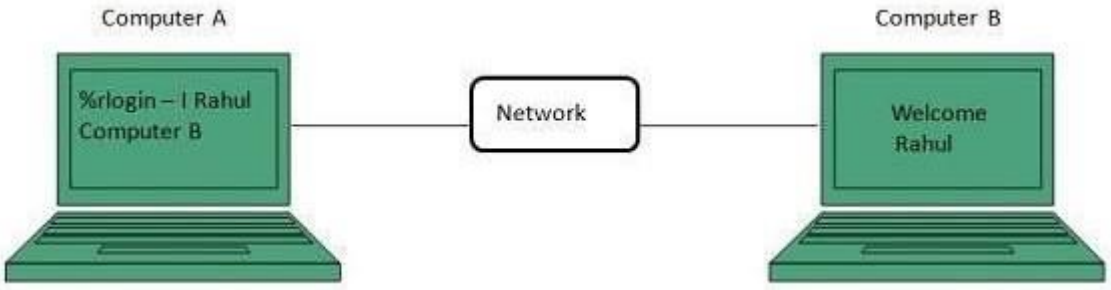
Difference between FTP and TFTP

S.N.	Parameter	FTP	TFTP

1	Operation	Transferring Files	Transferring Files
2	Authentication	Yes	No
3	Protocol	TCP	UDP
4	Ports	21 – Control, 20 – Data	Port 3214, 69, 4012
5	Control and Data	Separated	Separated
6	Data Transfer	Reliable	Unreliable

Telnet

Telnet is a protocol used to log in to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.



Hyper Text Transfer Protocol (HTTP)

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

HTTP Request

HTTP request comprises of lines which contains:

- Request line
- Header Fields
- Message body

Key Points

- The first line i.e. the **Request line** specifies the request method i.e. **Get** or **Post.**
- The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

HTTP Response

Like HTTP request, HTTP response also has certain structure. HTTP response contains:

- Status line
- Headers

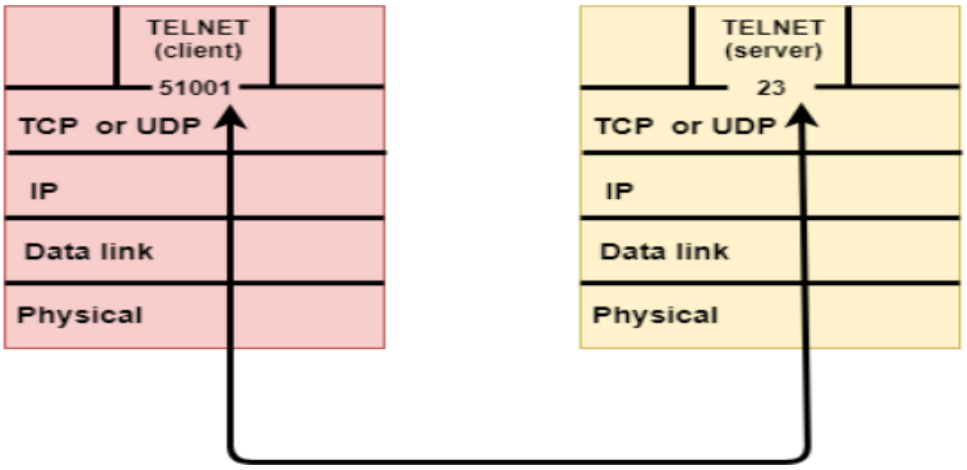
- Message body

STATIC ROUTING	DYNAMIC ROUTING
In static routing routes are user defined.	In dynamic routing, routes are updated according to topology.
Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
Static routing provides high or more security.	Dynamic routing provides less security.
Static routing is manual.	Dynamic routing is automated.
Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
In static routing, additional resources are not required.	In dynamic routing, additional resources are required.

UNIT - IV

Transport Layer protocols

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- Each port is defined by a positive integer address, and it is of 16 bits.



UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP

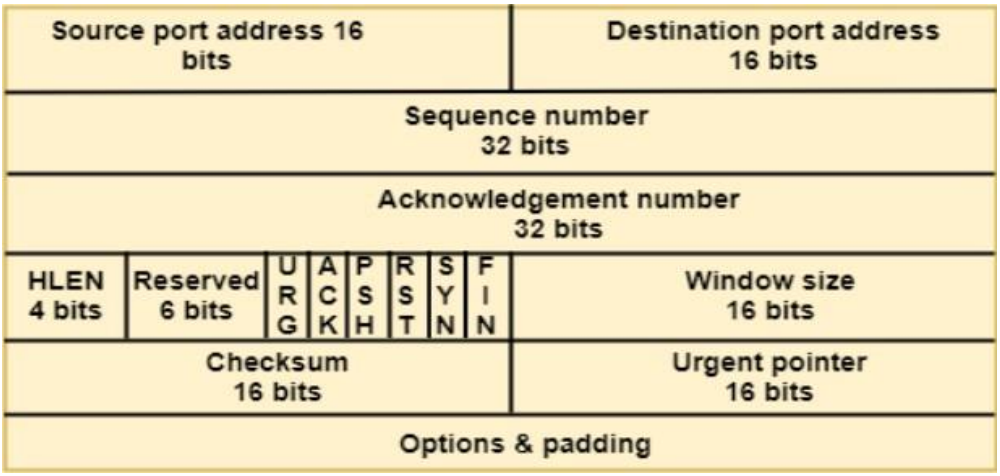
- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:

- Establish a connection between two TCPs.
- Data is exchanged in both the directions.
- The Connection is terminated.

TCP Segment Format



- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.

- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.

  - **Window Size:** The window is a 16-bit field that defines the size of the window.
  - **Checksum:** The checksum is a 16-bit field used in error detection.
  - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
  - **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

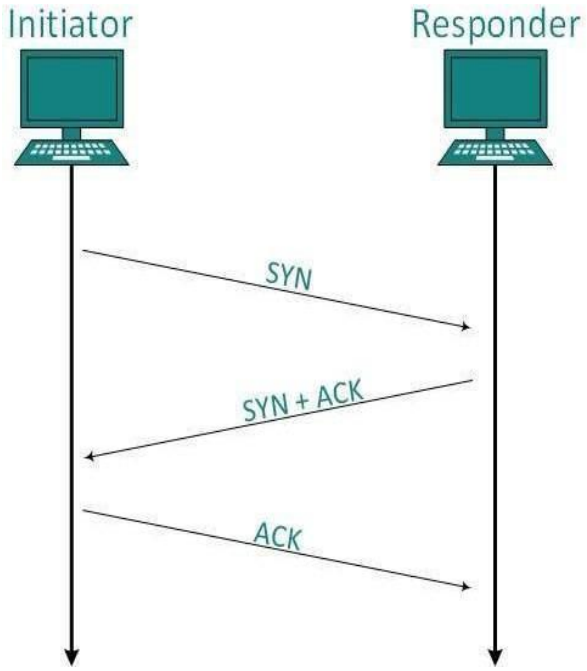
Addressing

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

Bandwidth Management

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

Error Control &and Flow Control

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

Congestion Control

When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

Timer Management

TCP uses different types of timer to control and management various tasks:

Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

Persist timer:

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds (4 minutes).

Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

UNIT - V

Application Layer

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.

The Application layer includes the following functions:

- **Identifying communication partners:** The application layer identifies the availability of communication partners for an application with data to transmit.
- **Determining resource availability:** The application layer determines whether sufficient network resources are available for the requested communication.
- **Synchronizing communication:** All the communications occur between the applications requires cooperation which is managed by an application layer.

Services of Application Layers

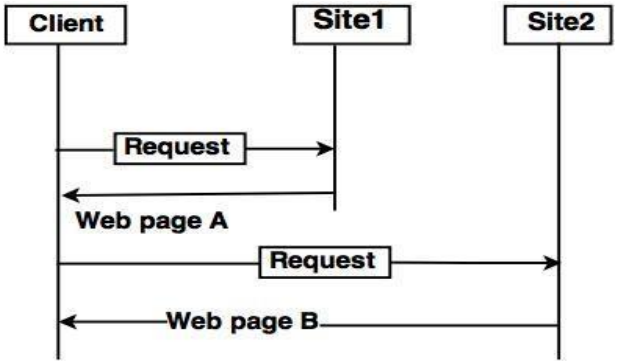
- **Network Virtual terminal:** An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allows the user to log on.
- **File Transfer, Access, and Management (FTAM):** An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.
- **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
- **Mail Services:** An application layer provides Email forwarding and storage.

- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.

World Wide Web in Computer Network

Introduction to World Wide Web

- The World Wide Web (WWW) is a collection of documents and other web resources which are identified by URLs, interlinked by hypertext links, and can be accessed and searched by browsers via the Internet.
- World Wide Web is also called the Web and it was invented by Tim Berners-Lee in 1989.
- Website is a collection of web pages belonging to a particular organization.
- The pages can be retrieved and viewed by using browser.



Architecture of WWW

Let us go through the scenario shown in above fig.

- The client wants to see some information that belongs to site 1.
- It sends a request through its browser to the server at site 2.
- The server at site 1 finds the document and sends it to the client.

Client (Browser):

- Web browser is a program, which is used to communicate with web server on the Internet.
- Each browser consists of three parts: a controller, client protocol and interpreter.
- The controller receives input from input device and use the programs to access the documents.
- After accessing the document, the controller uses one of the interpreters to display the document on the screen.

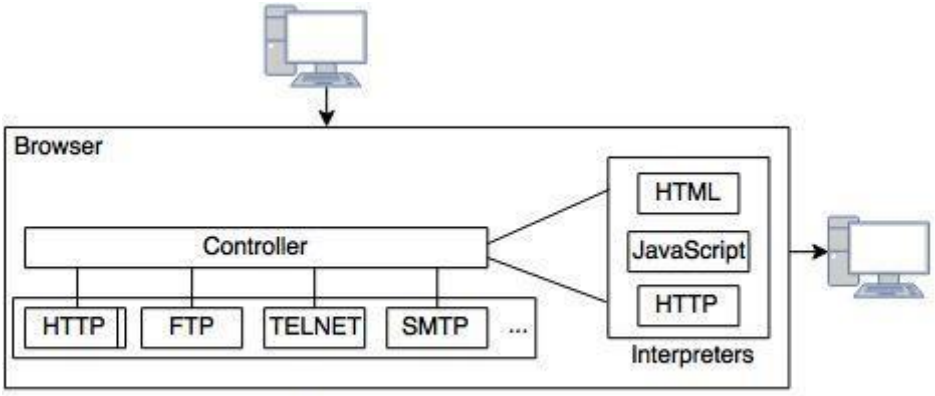


Fig: CIlient (Browser)

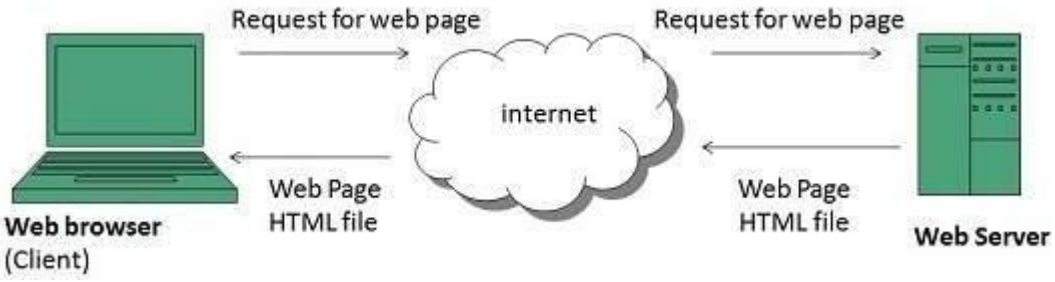
Server:

- A computer which is available for the network resources and provides service to the other computer on request is known as server.
- The web pages are stored at the server.
- Server accepts a TCP connection from a client browser.
- It gets the name of the file required.
- Server gets the stored file. Returns the file to the client and releases the top connection.

WWW Operation

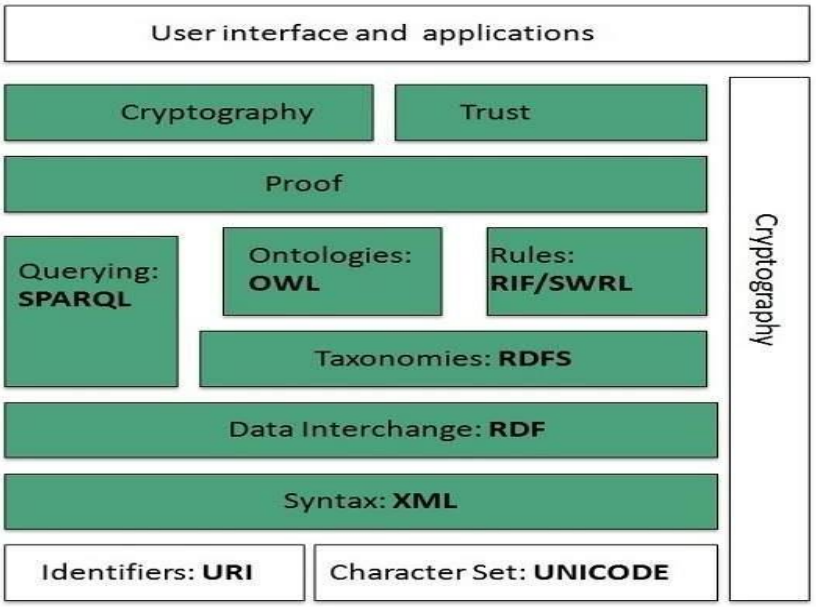
WWW works on client- server approach. Following steps explains how the web works:

1. User enters the URL (say, **http://www.tutorialspoint.com**) of the web page in the address bar of web browser.
2. Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.
3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.
4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.
5. Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.



WWW Architecture

WWW architecture is divided into several layers as shown in the following diagram:



Identifiers and Character Set

Uniform Resource Identifier (URI) is used to uniquely identify resources on the web and **UNICODE** makes it possible to built web pages that can be read and write in human languages.

Syntax

XML (Extensible Markup Language) helps to define common syntax in semantic web.

Data Interchange

Resource Description Framework (RDF) framework helps in defining core representation of data for web. RDF represents data about resource in graph form.

Taxonomies

RDF Schema (RDFS) allows more standardized description of **taxonomies** and other **ontological** constructs.

Ontologies

Web Ontology Language (OWL) offers more constructs over RDFS. It comes in following three versions:

- OWL Lite for taxonomies and simple constraints.
- OWL DL for full description logic support.
- OWL for more syntactic freedom of RDF

Rules

RIF and **SWRL** offers rules beyond the constructs that are available from **RDFs** and **OWL.** Simple Protocol and **RDF Query Language (SPARQL)** is SQL like language used for querying RDF data and OWL Ontologies.

Proof

All semantic and rules that are executed at layers below Proof and their result will be used to prove deductions.

Cryptography

Cryptography means such as digital signature for verification of the origin of sources is used.

User Interface and Applications

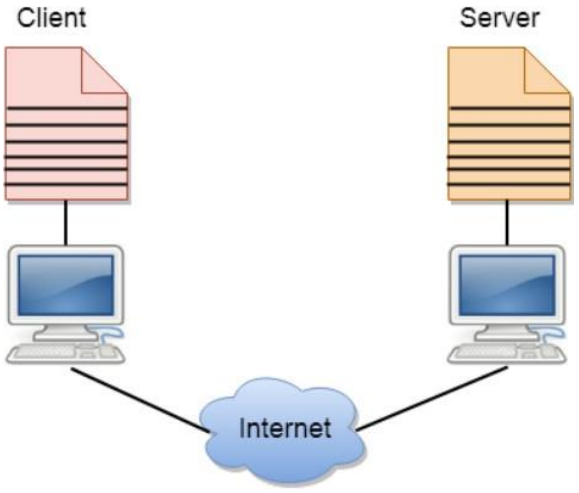
On the top of layer **User interface and Applications** layer is built for user interaction.

Uniform Resource Locater (URL)

- The URL is a standard for specifying any kind of information on the Internet.
- The URL consists of four parts: protocol, host computer, port and path.
- The protocol is the client or server program which is used to retrieve the document or file. The protocol can be ftp or http.
- The host is the name of computer on which the information is located.
- The URL can optionally contain the port number and it is separated from the host name by a colon.
- Path is the pathname of the file where the file is stored.

Client and Server model

- A client and server networking model is a model in which computers such as servers provide the network services to the other computers such as clients to perform a user based tasks. This model is known as client-server networking model.
- The application programs using the client-server model should follow the given below strategies:



- An application program is known as a client program, running on the local machine that requests for a service from an application program known as a server program, running on the remote machine.

- A client program runs only when it requests for a service from the server while the server program runs all time as it does not know when its service is required.
- A server provides a service for many clients not just for a single client. Therefore, we can say that client-server follows the many-to-one relationship. Many clients can use the service of one server.
- Services are required frequently, and many users have a specific client-server application program.

Client

A client is a program that runs on the local machine requesting service from the server. A client program is a finite program means that the service started by the user and terminates when the service is completed.

Server

A server is a program that runs on the remote machine providing services to the clients. When the client requests for a service, then the server opens the door for the incoming requests, but it never initiates the service.

A server program is an infinite program means that when it starts, it runs infinitely unless the problem arises. The server waits for the incoming requests from the clients. When the request arrives at the server, then it responds to the request.

Advantages of Client-server networks:

- **Centralized:** Centralized back-up is possible in client-server networks, i.e., all the data is stored in a server.
- **Security:** These networks are more secure as all the shared resources are centrally administered.
- **Performance:** The use of the dedicated server increases the speed of sharing resources. This increases the performance of the overall system.
- **Scalability:** We can increase the number of clients and servers separately, i.e., the new element can be added, or we can add a new node in a network at any time.

Disadvantages of Client-Server network:

- **Traffic Congestion** is a big problem in Client/Server networks. When a large number of clients send requests to the same server may cause the problem of Traffic congestion.

Application Protocols

. Application layer protocols can be broadly divided into two categories:

- Protocols which are used by users.For email for example, eMail.
- Protocols which help and support protocols used by users.For example DNS.

Few of Application layer protocols are described below:

Domain Name System

- The Domain Name System (DNS) works on Client Server model.
- It uses UDP protocol for transport layer communication.

- DNS uses hierarchical domain based naming scheme.
- The DNS server is configured with Fully Qualified Domain Names (FQDN) and email addresses mapped with their respective Internet Protocol addresses.

Simple Mail Transfer Protocol

- The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another.
- This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available.
- When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.
- Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side).
- Client software uses Internet Message Access Protocol (IMAP) or POP protocols to receive emails.

File Transfer Protocol

- The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network.
- FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client.
- FTP uses out-of-band controlling i.e. FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21.
- The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file.
- After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

Post Office Protocol (POP)

- The Post Office Protocol version 3 (POP 3) is a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server.
- When a client needs to retrieve mails from server, it opens a connection with the server on TCP port 110. User can then access his mails and download them to the local computer.
- POP3 works in two modes. The most common mode the delete mode, is to delete the emails from remote server after they are downloaded to local machines.
- The second mode, the keep mode, does not delete the email from mail server and gives the user an option to access mails later on mail server.

Hyper Text Transfer Protocol (HTTP)

- The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents.
- HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.
- To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

HTTP versions

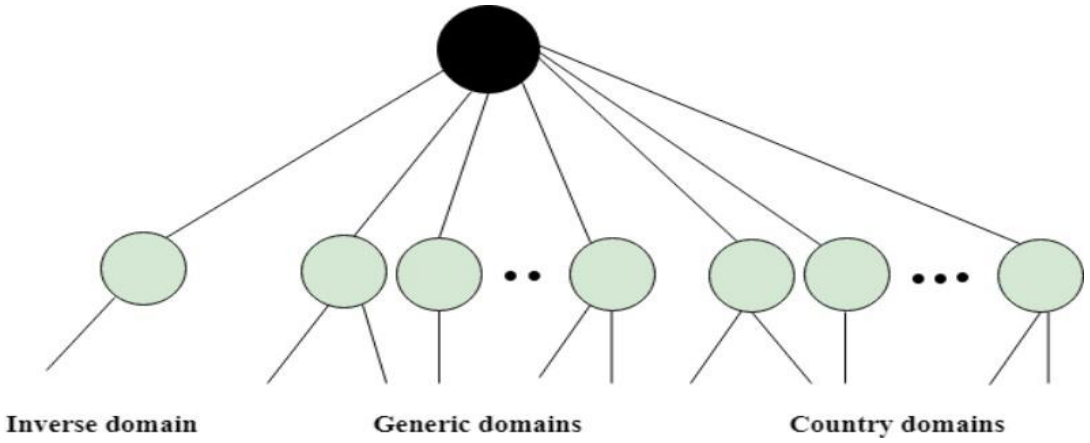
- HTTP 1.0 uses non persistent HTTP. At most one object can be sent over a single TCP connection.
- HTTP 1.1 uses persistent HTTP. In this version, multiple objects can be sent over a single TCP connection.

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

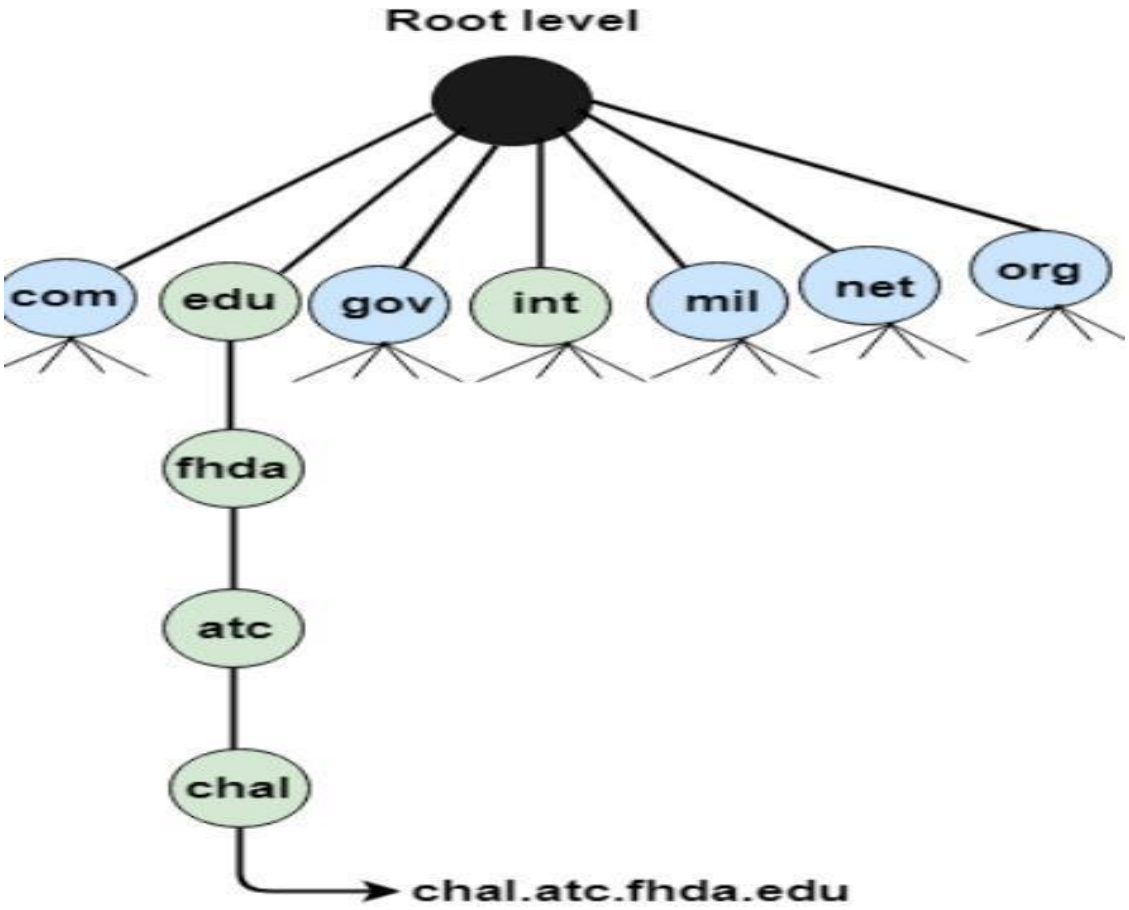
DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
net	Network Support centers
org	Nonprofit Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

- The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients.
- To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname.