COMPUTER NETWORKS

MCA II SEMESTER

K.G.R.L. P.G COURSES

…JS

MCA-20201 COMPUTER NETWORKS

UNIT I

Introduction to Computer Networks: Introduction, Network Hardware, Network Software, Reference Models, Data Communication Services & Network Examples, Internet Based Applications.

DataCommunications: Transmission Media, Wireless Transmission, Multiplexing, Switching, Transmission in ISDN, Broad Band ISDN, ATM Networks

UNIT II

Data Link Control, Error Detection & Correction, Sliding Window Protocols, LANs & MANs: IEEE Standards for LANs & MANs-IEEE Standards 802.2, 802.3, 802.4, 802.5, 802.6, High Speed LANs.

Design Issues in Networks: Routing Algorithms, Congestion Control Algorithms, Network Layer in the Internet, IP Protocol, IP Address, Subnets, and Internetworking

UNIT III

Internet Transport Protocols: Transport Service, Elements of Transport Protocols, TCP and UDP Protocols, Quality of Service Model, Best Effort Model, Network Performance Issues. Over View of DNS, SNMP, Electronic Mail, FTP, TFTP, BOOTP, HTTP Protocols, World Wide Web, Firewalls.

UNIT IV

Network Devices: Over View of Repeaters, Bridges, Routers, Gateways, Multiprotocol Routers, Brouters, Hubs, Switches, Modems, Channel Service Unit CSU, Data Service Units DSU, NIC, Wireless Access Points, Transceivers, Firewalls, Proxies.

Overview of Cellular Networks, Ad-hoc Networks, Mobile Ad-hoc Networks, Sensor Networks

UNIT I

Introduction to Computer Networks: Introduction, Network Hardware, Network Software, Reference Models, Data Communication Services & Network Examples, Internet Based Applications.

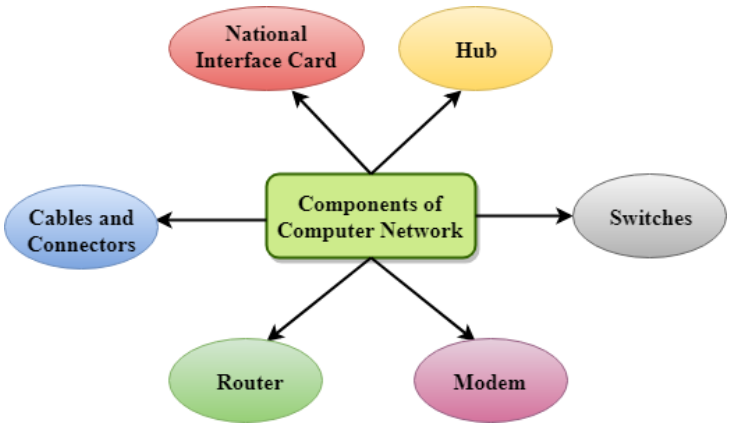
DataCommunications: Transmission Media, Wireless Transmission, Multiplexing, Switching, Transmission in ISDN, Broad Band ISDN, ATM Networks

Introduction to Computer Networks

Introduction:

- **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the sharing of resources among various devices.
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.

Components Of Computer Network:--



Major components of a computer network are:

NIC(Network interface card):NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

- **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.

- **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

Hub: Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.

Switches: Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

Cables and connectors: Cable is a transmission media that transmits the communication signals. **There are three types of cables:**

- **Twisted pair cable:** It is a high-speed cable that transmits the data over **1Gbps** or more.
- **Coaxial cable:** Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.
- **Fibre optic cable:** Fibre optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

Router: Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

Modem: Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard. A modem is a separate part on the PC slot found on the motherboard.

Uses Of Computer Network:--

- **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.

- **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

*****

Network Hardware:

The basic computer hardware components that are needed to set up a network are as follows −

Network Cables: Network cables are the transmission media to transfer data from one device to another. A commonly used network cable is category 5 cable with RJ – 45 connector, as shown in the image below:

Routers:A router is a connecting device that transfers data packets between different computer networks. Typically, they are used to connect a PC or an organization's LAN to a broadband internet connection. They contain RJ-45 ports so that computers and other devices can connect with them using network cables.

Repeaters, Hubs, and Switches:

Repeaters, hubs and switches connect network devices together so that they can function as a single segment.

A repeater receives a signal and regenerates it before re-transmitting so that it can travel longer distances.

A hub is a multiport repeater having several input/output ports, so that input at any port is available at every other port.

A switch receives data from a port, uses packet switching to resolve the destination device and then forwards the data to the particular destination, rather than broadcasting it as a hub.

Bridges:A bridge connects two separate Ethernet network segments. It forwards packets from the source network to the destined network.

Gateways:A gateway connects entirely different networks that work upon different protocols. It is the entry and the exit point of a network and controls access to other networks.

Network Interface Cards:NIC is a component of the computer to connect it to a network. Network cards are of two types: Internal network cards and external network cards.

*****

Network Software:

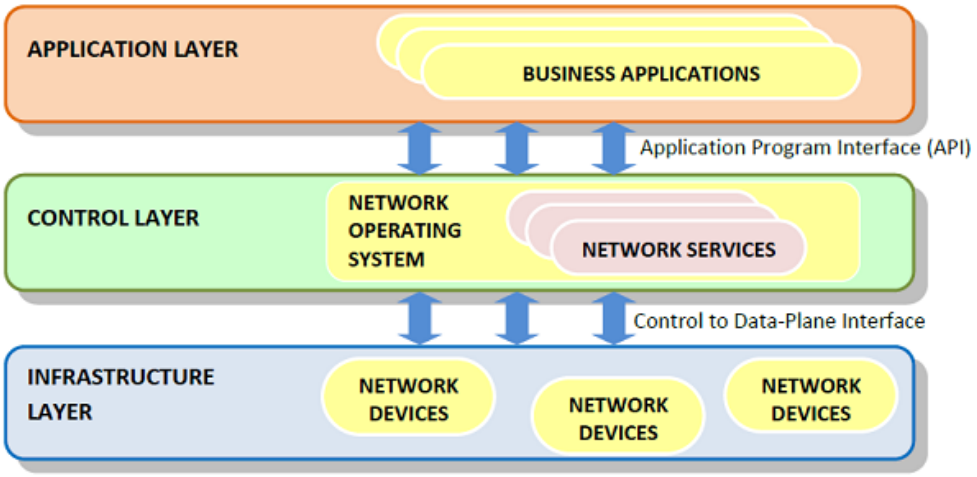
Network software encompasses a broad range of software used for design, implementation, and operation and monitoring of computer networks. Traditional networks were hardware based with software embedded. With the advent of Software – Defined Networking (SDN), software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

Functions of Network Software:

- Helps to set up and install computer networks
- Enables users to have access to network resources in a seamless manner
- Allows administrations to add or remove users from the network
- Helps to define locations of data storage and allows users to access that data
- Helps administrators and security system to protect the network from data breaches, unauthorized access and attacks on a network
- Enables network virtualizations

SDN Framework:

The Software Defined Networking framework has three layers as depicted in the following diagram −

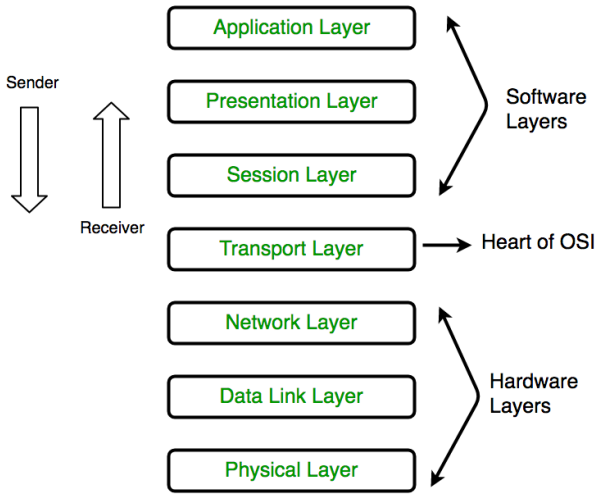


- **APPLICATION LAYER** − SDN applications reside in the Application Layer. The applications convey their needs for resources and services to the control layer through APIs.
- **CONTROL LAYER** − The Network Control Software, bundled into the Network Operating System, lies in this layer. It provides an abstract view of the underlying network infrastructure. It receives the requirements of the SDN applications and relays them to the network components.
- **INFRASTRUCTURE LAYER** − Also called the Data Plane Layer, this layer contains the actual network components. The network devices reside in this layer that shows their network capabilities through the Control to data-Plane Interface.

*****

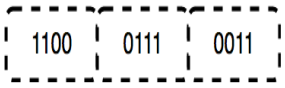
Reference Models:

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) : The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer

contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

a) **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
b) **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
c) **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
d) **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

2. Data Link Layer (DLL) (Layer 2) : The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :
a) Logical Link Control (LLC)
b) Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the data Link layer are :

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

b) **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
c) **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
d) **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
e) **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

3. Network Layer (Layer 3) : Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.

The functions of the Network layer are :

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

* Segment in Network layer is referred as **Packet**.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) : Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

• At sender's side:

Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.
Note: The sender need to know the port number associated with the receiver's application.

Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

• At receiver's side:

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.
The functions of the transport layer are :

A. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
B. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

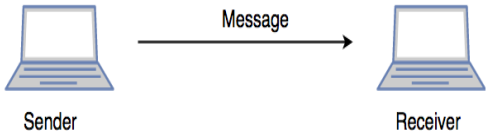
a) **Connection Oriented Service:** It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
b) **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

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

5. Session Layer (Layer 5) : This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
The functions of the session layer are :

a) **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
b) **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
c) **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

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



6. Presentation Layer (Layer 6) : Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

a) **Translation :** For example, ASCII to EBCDIC.
b) **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used forencrypting as well as decrypting data.
c) **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) : At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Ex: Application – Browsers, Skype Messenger etc.
**Application Layer is also called as Desktop Layer.

The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model.

*****

Data Communication Services & Network Examples:

Data Communication Services:

Data Communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum also. For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs.

Data Communication System Components :

There are mainly five components of a data communication system:

1. Message
2. Sender
3. Receiver
4. Transmission Medium
5. Set of rules (Protocol)

All above mentioned elements are described below:

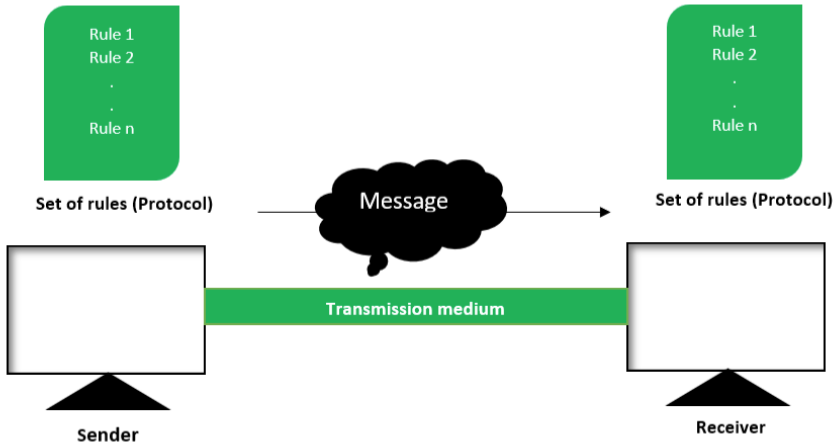


Figure – Components of Data Communication System

1. **Message :**This is most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.
2. **Sender :**To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.
3. **Receiver :**It is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.
4. **Transmission Medium:**In entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

5. **Set of rules (Protocol) :**To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus the protocol is necessary for data communication to take place.

A typical example of a data communication system is sending an e-mail. The user which send email act as sender, message is data which user wants to send, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send and receive email.

*

Network Examples:

A computer network is a cluster of computers over a shared communication path that work for the purpose of sharing resources from one computer to another, provided by or located on the network nodes.

Some of the uses of computer networks are the following:

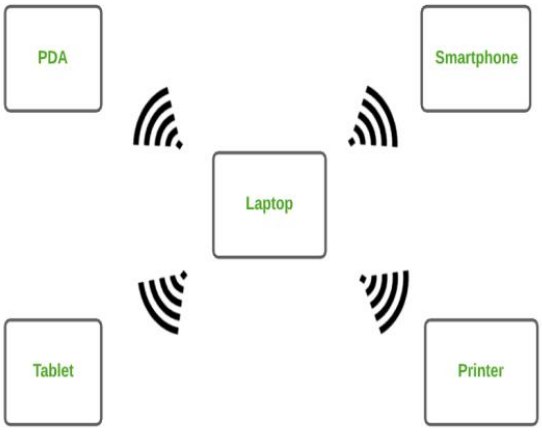
- Communicating using email, video, instant messaging, etc.
- Sharing devices such as printers, scanners, etc.
- Sharing files
- Sharing software and operating programs on remote systems
- Allowing network users to easily access and maintain information

Types of Computer Networks

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Wide Area Network (WAN)
4. Wireless Local Area Network (WLAN)
5. Campus Area Network (CAN)
6. Metropolitan Area Network (MAN)
7. Storage Area Network (SAN)
8. System-Area Network (SAN)
9. Passive Optical Local Area Network (POLAN)
10. Enterprise Private Network (EPN)
11. Virtual Private Network

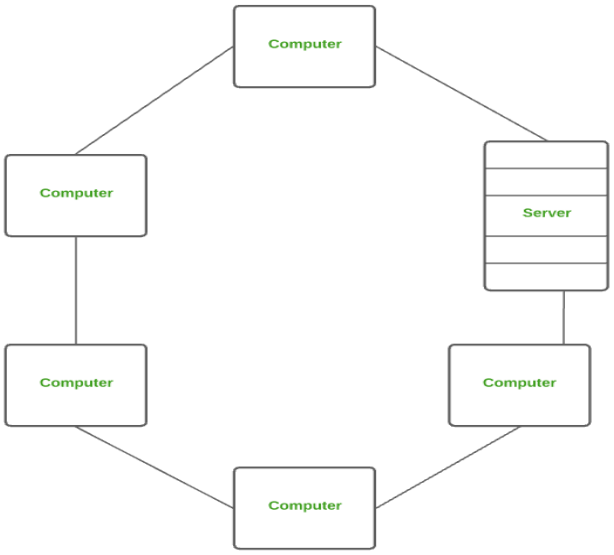
These are explained as following below.

1. Personal Area Network (PAN) :PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centred only to an individual's work space. PAN offers a network range of 10 meters from a person to the device providing communication.
Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.



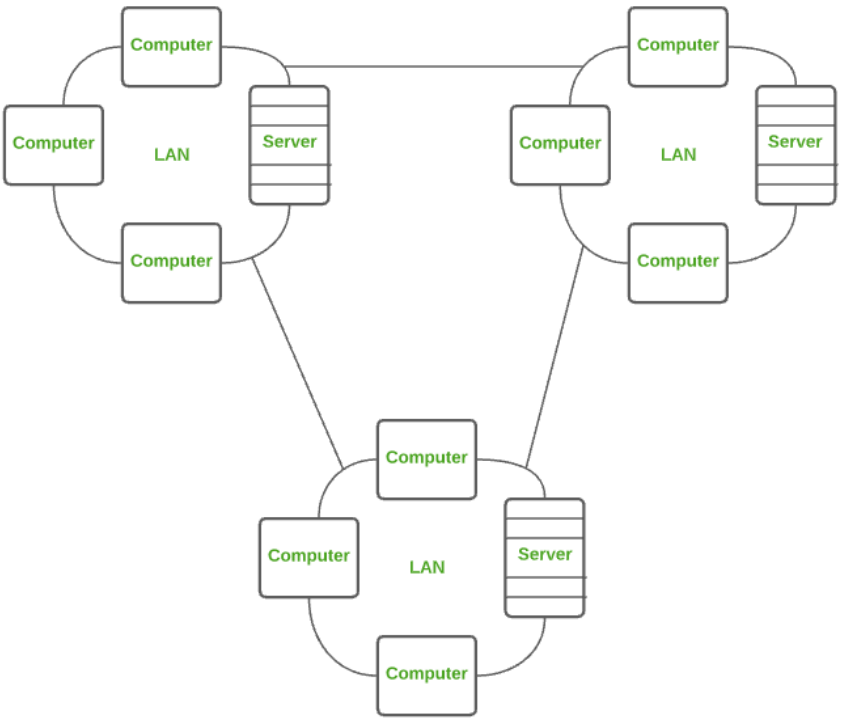
2. Local Area Network (LAN) : LAN is the most frequently used network. A LAN is a computer network that connects computers together through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi.

Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

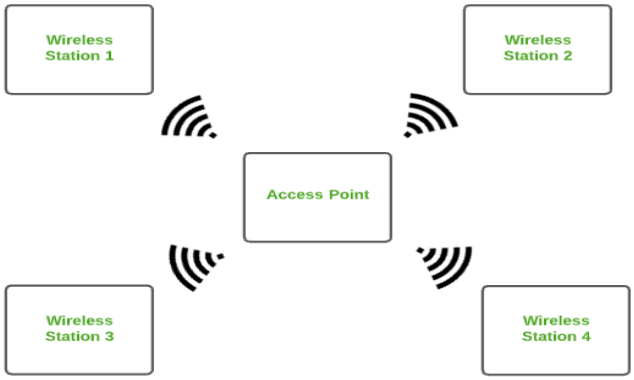


3. Wide Area Network (WAN) :WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other.

The most common example of WAN is the Internet.

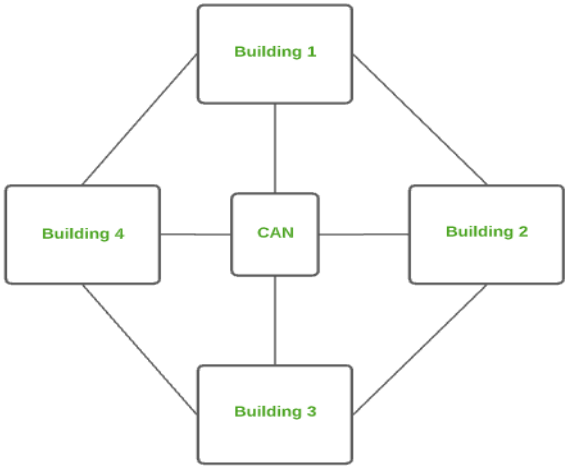


4.Wireless Local Area Network (WLAN) : WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices communicating over physical cables like in LAN, but allows devices to communicate wirelessly.
The most common example of WLAN is Wi-Fi.



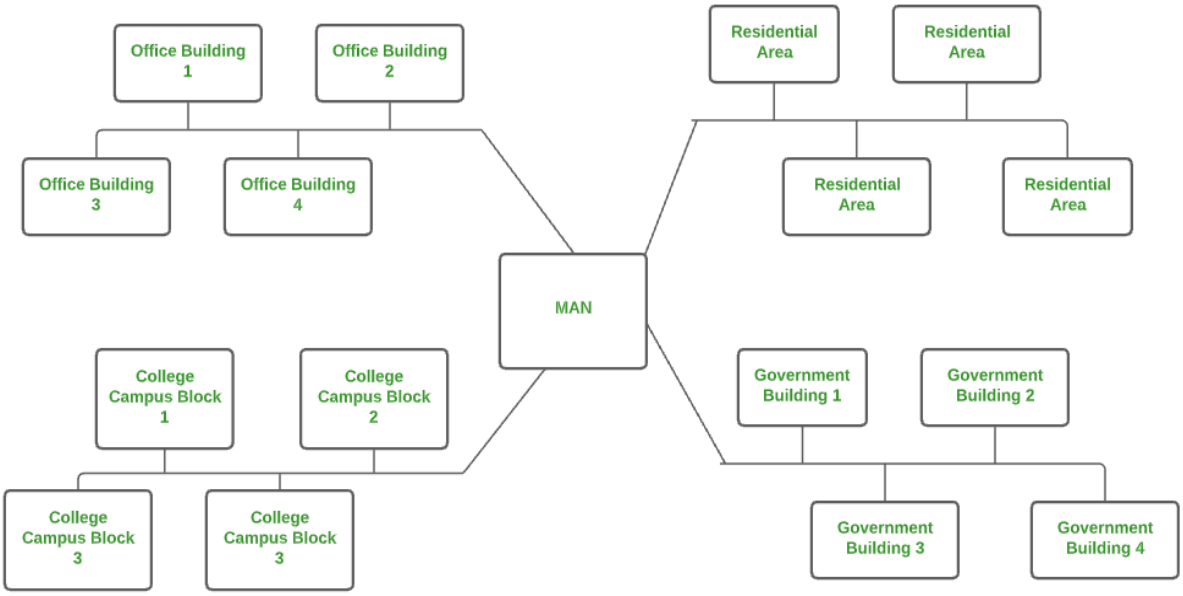
5. Campus Area Network (CAN) :CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network which is usually used in places like a school or college. This network covers a limited geographical area that is, it spreads across several buildings within the campus.

Examples of CAN are networks that cover schools, colleges, buildings, etc.

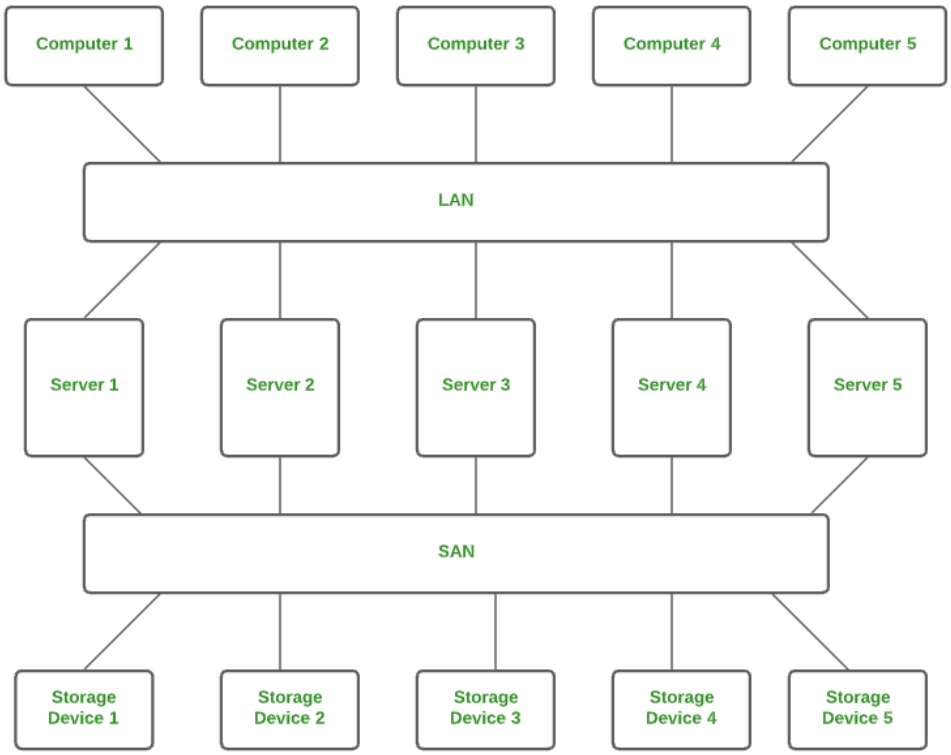


6. Metropolitan Area Network (MAN) : A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town or metropolitan area.

Examples of MAN are networking in towns, cities, a single large city, large area within multiple buildings, etc.

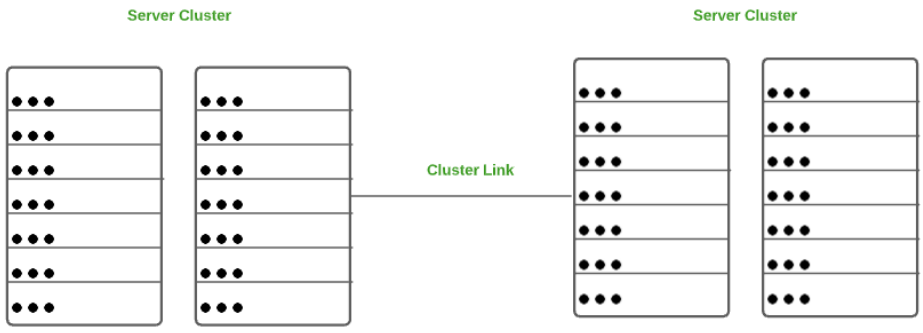


7. Storage Area Network (SAN) :SAN is a type of computer network that is high speed and connects groups of storage devices to several servers. This network does not depend on LAN or WAN.. Instead, a SAN moves the storage resources from the network to its own high-powered network. A SAN provides access to block-level data storage.
Examples of SAN are a network of disks accessed by a network of servers.

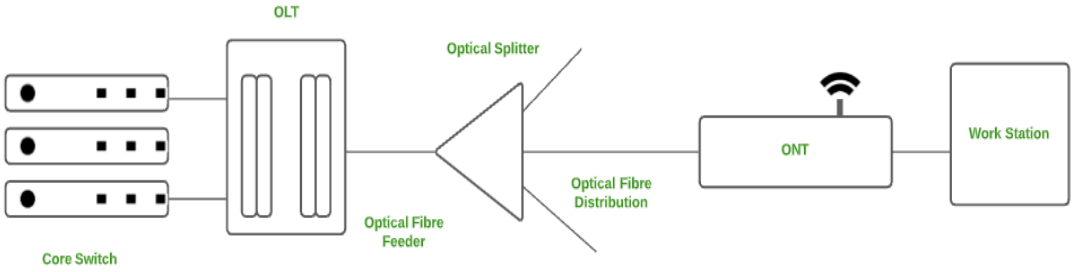


8. System Area Network (SAN) :A SAN is a type of computer network that connects a cluster of high performance computers. It is a connection-oriented and high bandwidth network. A SAN is a type of LAN that handles high amounts of information in large requests. This network is useful for processing applications that require high network performance.

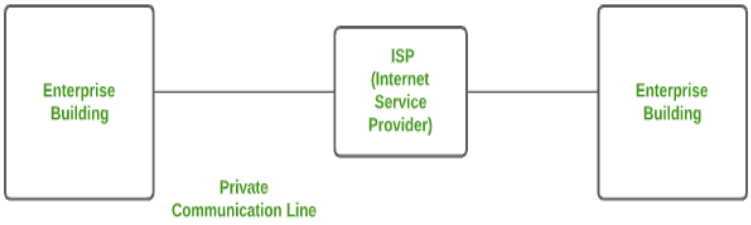
Microsoft SQL Server 2005 uses SAN through virtual interface adapter.



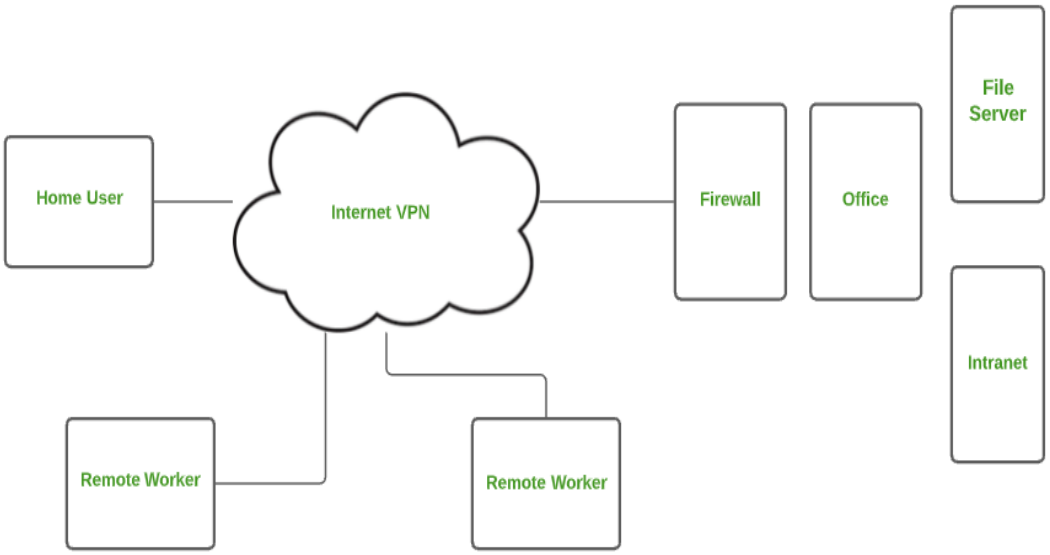
9. Passive Optical Local Area Network (POLAN) :A POLAN is a type of computer network which is an alternative to a LAN. POLAN uses optical splitters to split an optical signal from a single strand of single mode optical fibre to multiple signals to distribute users and devices. In short, POLAN is a point to multipoint LAN architecture.



10. Enterprise Private Network (EPN) :EPN is a type of computer network mostly used by businesses that want a secure connection over various locations to share computer resources.



11. Virtual Private Network (VPN) :A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point to point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you protected network connection.



*****

Internet Based Applications:

Here are the top 8 internet applications listed below

1.SmartHome: Smart Home has become the evolutionary ladder in residential and developing as common as smartphones. It is a special feature of Google and now deployed in many areas to make life convenient and user-friendly. The smart home is designed to save time, money and energy.

2.ElectronicDevices: Electronic devices like wearables are installed with different sensors and software, which gather data and information of the user where data is processed to give required info about the user. The devices mainly used to monitor fitness, entertainment, and health. They mostly work on ultra-low power and available in small sizes.

3.Automated Digital Technology: The automated digital technology has concentrated on the optimization of vehicles and their internal functions. the automated car is designed with special features that give a comfort zone to passengers with onboard sensors and internet establishment. Popular companies like Tesla, Apple, BMW, Google is yet to aboard their revolution in the automobile industry by installing excellent features.

4.Industrial Internet: The industrial internet is investing in industrial engineering with Artificial intelligence and data analytics to build brilliant machines. The important moto is to build smart machines that are accurate and compatible with a human. It holds vast potential with good quality and reliability. The applications are deployed for tracing the goods to be delivered, real-time data regarding retails and supplies that increase the efficiency of the business's supply chain and productivity.

5. Smart City:A smart city is another major implementation of the internet, which is employed for smart surveillance, water distribution, automatic transportation, environment monitoring. People are prone to pollution, improper supplies and shortage of sources, and the installation of traffic sensors solves irregular traffic flow, and the app is developed to report the municipal systems. Citizens can able to diagnose simple malfunctions in meter and can report to the

electricity system via electricity board applications or websites, and they can also find available slots for vehicle parking easily in sensor systems.

6.Smartphones: Smartphones are also used for retailers and customers to stay connected for their business transactions, even out of the store. They have using Beacon technology to help business people to provide smart service to the client. They can track the products and enhance the store dashboard and deliver premium order before the scheduled date, even in congested traffic areas.

7.SmartGrids: The idea applied in smart grids is to gather data in an automated way to analyze the attribute of electricity. Consumers to improve the efficiency and economics of usage. Smart grids can easily detect the power outage and shortage quickly and fix them shortly.

8.MajorApplication:Another major application of the internet is in healthcare as it is smart medical systems installed to diagnose and cure the disease at an earlier stage. Many machine learning algorithms are used in image processing and classification to detect the fetus's abnormalities before birth. The main aim applied in the medical field is to provide a healthier life for all by wearing connected devices. The gathered medical data of patients made the treatment easier, and a monitoring device is installed to track the sugar and blood pressure.

*****

Data Communications

Transmission Media:

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.

Some factors need to be considered for designing the transmission media:

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:

- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification Of Transmission Media:

1. Guided Transmission Media
2. UnGuided Transmission Media

1.GuidedMedia: 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.

Types of Twisted pair:

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.

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.

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.

2.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.

Microwaves:

Microwaves are of two types:

a) Terrestrial microwave
b) Satellite microwave communication.

a)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.

b)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.

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.

*****

Wireless Transmission:

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

A little part of electromagnetic spectrum can be used for wireless transmission.

Radio Transmission:

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike.Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back.The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers, over the earth's surface.

Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.

Microwave Transmission:

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.

Microwave antennas concentrate the waves making a beam of it. As shown in picture above, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwave transmission depends highly upon the weather conditions and the frequency it is using.

Infrared Transmission:

Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

Light Transmission:

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line.Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector needs to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.

Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles such as walls, rain, and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature, or variation in temperature in the path.

Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

*****

Multiplexing:

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

Concept of Multiplexing:

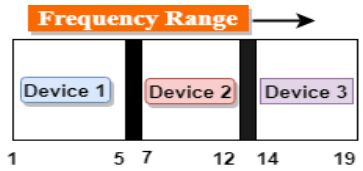
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Multiplexing Techniques:

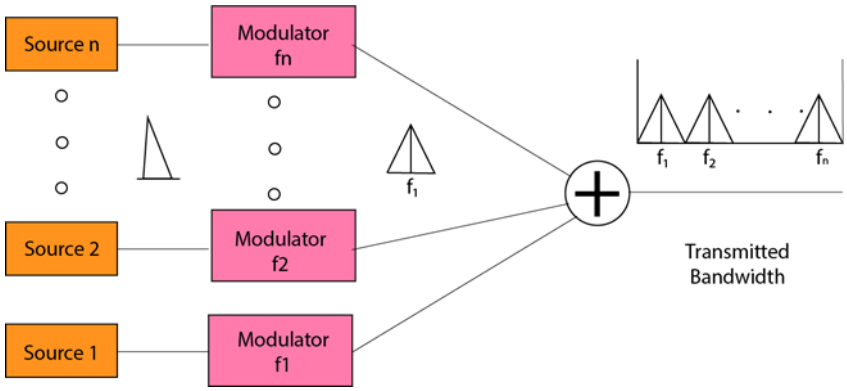
Multiplexing techniques can be classified as:

Frequency-division Multiplexing (FDM):

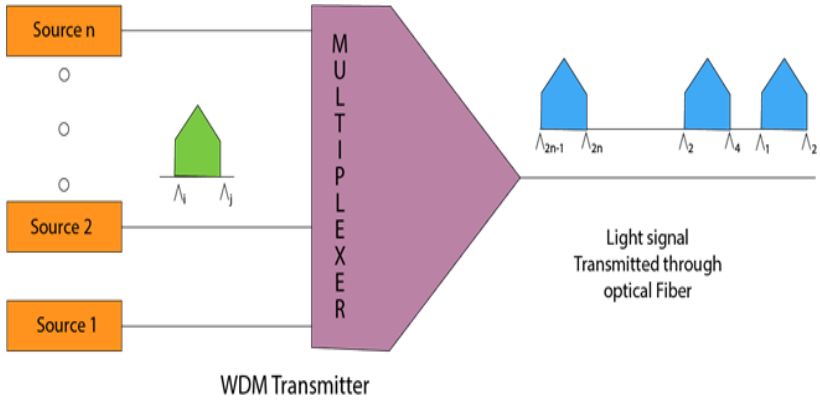
- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



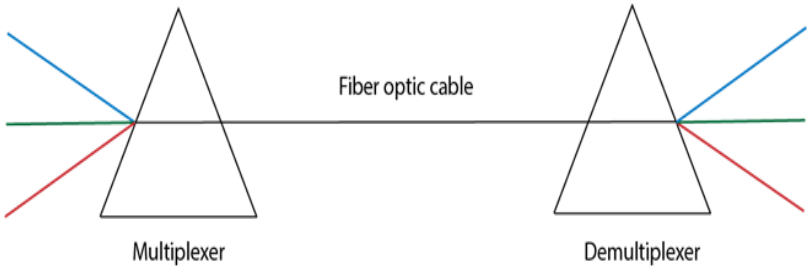
- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.



Wavelength Division Multiplexing (WDM):



- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing:

- It is a digital technique.

- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

1.Synchronous TDM
2.Asynchronous TDM

1.Synchronous TDM:

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.

2.Asynchronous TDM:

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to

send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.

- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

*****

Switching:

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.

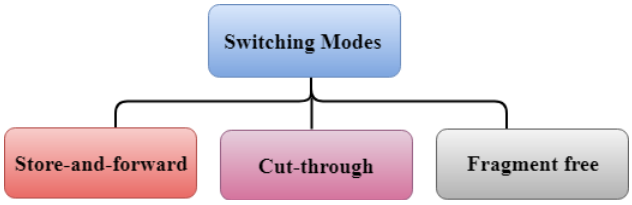
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Switching concept is developed because of the following reasons:

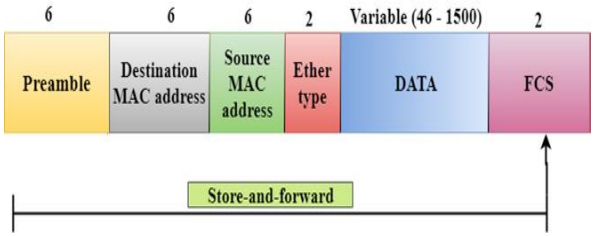
- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

There are three types of switching modes:

1.Store-and-forward
2.Cut-through
3.Fragment-free



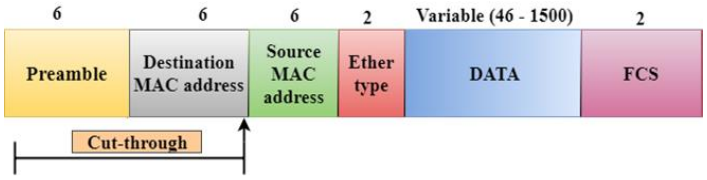
1.Store-and-forward:



- Store-and-forward is a technique in which the intermediate nodes store the received frame and then check for errors before forwarding the packets to the next node.

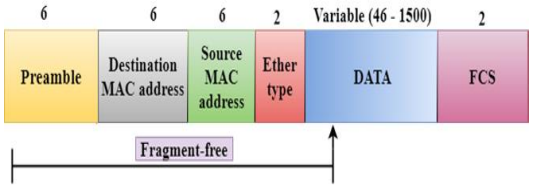
- The layer 2 switch waits until the entire frame has received. On receiving the entire frame, switch store the frame into the switch buffer memory. This process is known as **storing the frame**.
- When the frame is stored, then the frame is checked for the errors. If any error found, the message is discarded otherwise the message is forwarded to the next node. This process is known as **forwarding the frame**.
- CRC (Cyclic Redundancy Check) technique is implemented that uses a number of bits to check for the errors on the received frame.
- The store-and-forward technique ensures a high level of security as the destination network will not be affected by the corrupted frames.
- Store-and-forward switches are highly reliable as it does not forward the collided frames.

2.Cut-through Switching:



- Cut-through switching is a technique in which the switch forwards the packets after the destination address has been identified without waiting for the entire frame to be received.
- Once the frame is received, it checks the first six bytes of the frame following the preamble, the switch checks the destination in the switching table to determine the outgoing interface port, and forwards the frame to the destination.
- It has **low latency** rate as the switch does not wait for the entire frame to be received before sending the packets to the destination.
- It has no **error checking technique**. Therefore, the errors can be sent with or without errors to the receiver.
- A Cut-through switching technique has **low wait time** as it forwards the packets as soon as it identifies the destination MAC address.
- In this technique, collision is not detected, if frames have collided will also be forwarded.

3.Fragment-free Switching:



- A Fragment-free switching is an advanced technique of the Cut-through Switching.
- A Fragment-free switching is a technique that reads atleast 64 bytes of a frame before forwarding to the next node to provide the error-free transmission.
- It combines the speed of Cut-through Switching with the error checking functionality.
- This technique checks the 64 bytes of the ethernet frame where addressing information is available.
- A collision is detected within 64 bytes of the frame, the frames which are collided will not be forwarded further.

*****

Transmission in ISDN:

ISDN is a circuit-switched telephone network system, but it also provides access to packet switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. A greater data rate was achieved through channel bonding. Generally ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

ISDN Interfaces:

The following are the interfaces of ISDN:

1. **Basic Rate Interface (BRI):**There are two data-bearing channels (‘B’ channels) and one signaling channel (‘D’ channel) in BRI to initiate connections. The B channels operate at a maximum of 64 Kbps while the D channel operates at a maximum of 16 Kbps. The two channels are independent of each other. For example, one channel is used as a TCP/IP connection to a location while the other channel is used to send a fax to a remote location. In iSeries ISDN supports basic rate interface (BRl).
   The basic rate interface (BRl) specifies a digital pipe consisting two B channels of 64 Kbps each and one D channel of 16 Kbps. This equals a speed of 144 Kbps. In addition, the BRl service itself requires an operating overhead of 48 Kbps. Therefore a digital pipe of 192 Kbps is required.
2. **Primary Rate Interface (PRI):**Primary Rate Interface service consists of a D channel and either 23 or 30 B channels depending on the country you are in. PRI is not supported on the iSeries. A digital pipe with 23 B channels and one 64 Kbps D channel is present in the usual Primary Rate Interface (PRI). Twenty-three B channels of 64 Kbps each and one D channel of 64 Kbps equals 1.536 Mbps. The PRI service uses 8 Kbps of overhead also. Therefore PRI requires a digital pipe of 1.544 Mbps.

3. **Broadband-ISDN (B-ISDN):**Narrowband ISDN has been designed to operate over the current communications infrastructure, which is heavily dependent on the copper cable however B-ISDN relies mainly on the evolution of fiber optics. According to CCITT B-

ISDN is best described as 'a service requiring transmission channels capable of supporting rates greater than the primary rate.

ISDN Services:

ISDN provides a fully integrated digital service to users. These services fall into 3 categories- bearer services, teleservices and supplementary services.

1. **Bearer Services:**Transfer of information (voice, data and video) between users without the network manipulating the content of that information is provided by the bearer network. There is no need for the network to process the information and therefore does not change the content. Bearer services belong to the first three layers of the OSI model. They are well defined in the ISDN standard. They can be provided using circuit-switched, packet-switched, frame-switched, or cell-switched networks.
2. **Tele services:**In this the network may change or process the contents of the data. These services corresponds to layers 4-7 of the OSI model. Teleservices relay on the facilities of the bearer services and are designed to accommodate complex user needs. The user need not to be aware of the details of the process. Teleservices include telephony, teletex, telefax, videotex, telex and teleconferencing. Though the ISDN defines these services by name yet they have not yet become standards.
3. **Supplementary Service:**Additional functionality to the bearer services and teleservices are provided by supplementary services. Reverse charging, call waiting, and message handling are examples of supplementary services which are all familiar with today's telephone company services.

Principle of ISDN:

The ISDN works based on the standards defined by ITU-T (formerly CCITT). The Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. The various principles of ISDN as per ITU-T recommendation are:

- To support switched and non-switched applications
- To support voice and non-voice applications
- Reliance on 64-kbps connections
- Intelligence in the network
- Layered protocol architecture
- Variety of configurations

*****

Broad Band ISDN:

ISDN was first defined in the CCITT red book in 1988.The **Integrated Services of Digital Networking**, in short ISDN is a telephone network based infrastructure that allows the transmission of voice and data simultaneously at a high speed with greater efficiency. This is a circuit switched telephone network system, which also provides access to Packet switched networks.

The model of a practical ISDN is as shown below.

ISDN supports a variety of services. A few of them are listed below −

- Voice calls
- Facsimile
- Videotext
- Teletext
- Electronic Mail
- Database access
- Data transmission and voice
- Connection to internet
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer
- Audio and Video Conferencing
- Automatic alarm services to fire stations, police, medical etc.

Types of ISDN:

Among the types of several interfaces present, some of them contains channels such as the **B-Channels** or Bearer Channels that are used to transmit voice and data simultaneously; the **D-Channels** or Delta Channels that are used for signaling purpose to set up communication.

The ISDN has several kinds of access interfaces such as −

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)
- Narrowband ISDN
- Broadband ISDN

1.Basic Rate Interface (BRI): The Basic Rate Interface or Basic Rate Access, simply called the **ISDN BRI Connection** uses the existing telephone infrastructure. The BRI configuration provides **two data** or bearer channels at **64 Kbits/sec** speed and one control or delta channel at **16 Kbits/sec**. This is a standard rate.

The ISDN BRI interface is commonly used by smaller organizations or home users or within a local group, limiting a smaller area.

2.Primary Rate Interface (PRI): The Primary Rate Interface or Primary Rate Access, simply called the ISDN PRI connection is used by enterprises and offices. The PRI configuration is based on T-carrier or T1 in the US, Canada and Japan countries consisting of **23 data** or bearer channels and one control or delta channel, with 64kbps speed for a bandwidth of 1.544 M bits/sec. The PRI configuration is based on E-carrier or E1 in Europe, Australia and few Asian countries consisting of **30 data** or bearer channels and **two-control** or delta channel with 64kbps speed for a bandwidth of 2.048 M bits/sec.

The ISDN BRI interface is used by larger organizations or enterprises and for Internet Service Providers.

3.NarrowbandISDN: The Narrowband Integrated Services Digital Network is called the **N-ISDN**. This can be understood as a telecommunication that carries voice information in a narrow band of frequencies. This is actually an attempt to digitize the analog voice information. This uses 64kbps circuit switching.

The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

4.BroadbandISDN: The Broadband Integrated Services Digital Network is called the **B-ISDN**. This integrates the digital networking services and provides digital transmission over ordinary telephone wires, as well as over other media. The CCITT defined it as, "Qualifying a service or system requiring transmission channels capable of supporting rates greater than primary rates."

The broadband ISDN speed is around 2 MBPS to 1 GBPS and the transmission is related to ATM, i.e., Asynchronous Transfer Mode. The broadband ISDN communication is usually made using the fiber optic cables.

As the speed is greater than 1.544 Mbps, the communications based on this are called **Broadband Communications**. The broadband services provide a continuous flow of information, which is distributed from a central source to an unlimited number of authorized receivers connected to the network. Though a user can access this flow of information, he cannot control it.

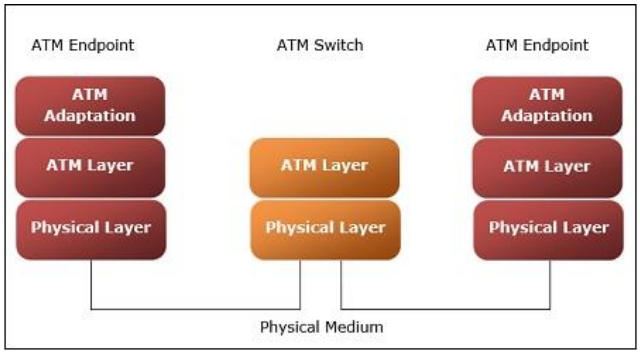
*****

ATM Networks:

ATM stands for Asynchronous Transfer Mode. It is a switching technique that uses time division multiplexing (TDM) for data communications.

ATM networks are connection oriented networks for cell relay that supports voice, video and data communications. It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.

The size of an ATM cell is 53 bytes: 5 byte header and 48 byte payload. There are two different cell formats - user-network interface (UNI) and network-network interface (NNI). The below image represents the Functional Reference Model of the Asynchronous Transfer Mode.



Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

ATM reference model comprises of three layers

- **Physical Layer** − This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.
- **ATM Layer** −This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
- **ATM Adaptation Layer (AAL)** −This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers − Convergence sub layer and Segmentation and Reassembly sub layer.
- **ATM endpoints** − It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.
- **ATM switch** −It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination.

*****

UNIT II

Data Link Control, Error Detection & Correction, Sliding Window Protocols, LANs & MANs: IEEE Standards for LANs & MANs-IEEE Standards 802.2, 802.3, 802.4, 802.5, 802.6, High Speed LANs.

Design Issues in Networks: Routing Algorithms, Congestion Control Algorithms, Network Layer in the Internet, IP Protocol, IP Address, Subnets, and Internetworking

Data Link Control:

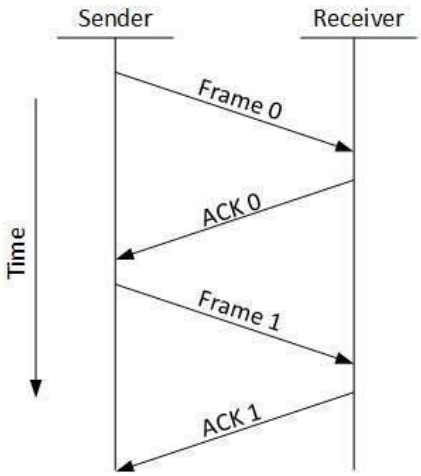
Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

1.Flow Control:

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

Stop and Wait: This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



Sliding Window: In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

2.ErrorControl: When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct

data-frame and sender does not know anything about any loss.In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

*****

Error Detection & Correction:

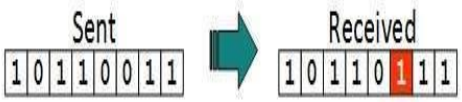
There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing.Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors:

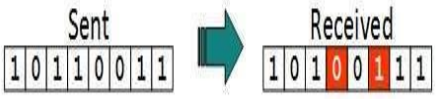
There may be three types of errors:

1.Single bit error:



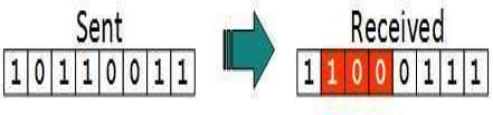
In a frame, there is only one bit, anywhere though, which is corrupt.

2.Multiple bits error:



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

3.Burst error:



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

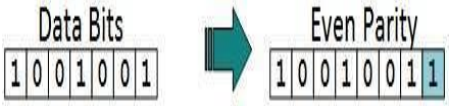
Error Detection:

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.

a.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.

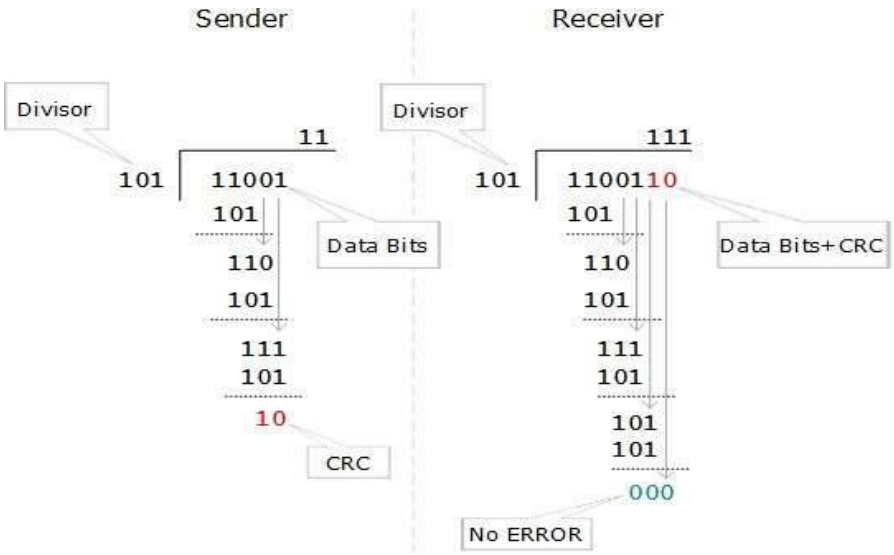


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

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 erroneous, then it is very hard for the receiver to detect the error.

b.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.

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

*****

Sliding Window Protocols:

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.

In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

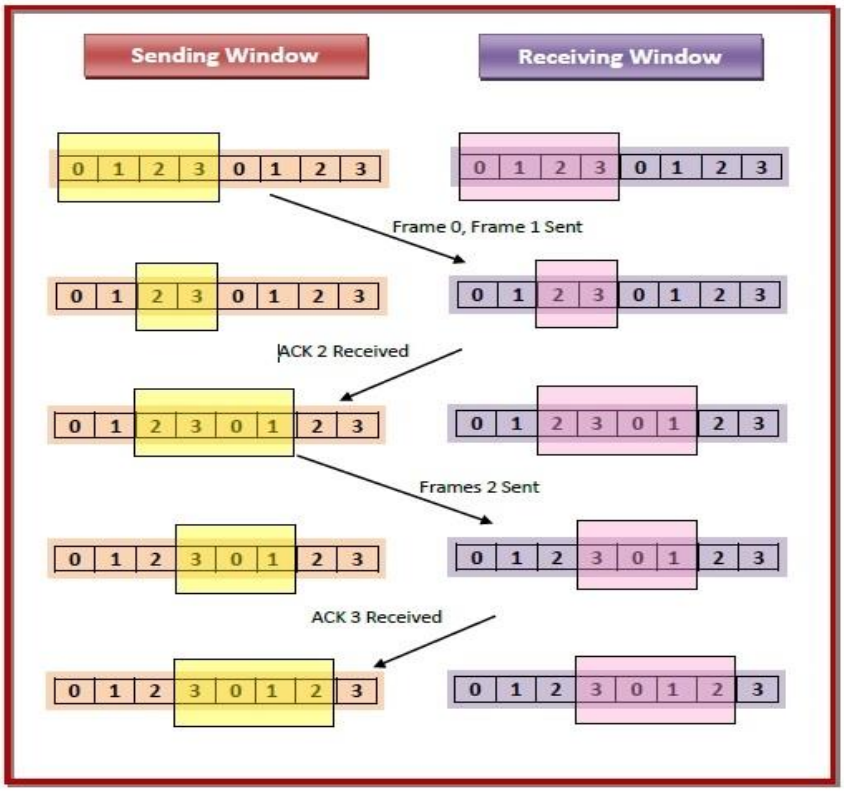
Working Principle: In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1. Consequently, the size of the sending window is 2^n-1. Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

Example:- Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.



Types of Sliding Window Protocols:

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories −

Go – Back – ***N*** **ARQ:**Go – Back – *N* ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

Selective Repeat ARQ: This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

*****

LANs & MANs:

IEEE Standards for LANs & MANs:

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN and WAN are the three major types of the network designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area; **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.

Local Area Network (LAN):

LAN or Local Area Network connects network devices in such a way that personal computer and workstations can share data, tools and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked are limited. By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters and Ethernet cables). LANs cover smaller geographical area (Size is limited to a few kilometers) and are privately owned. One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Metropolitan Area Network (MAN):

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN is moderate. Devices used for transmission of data through MAN are: Modem and Wire/Cable. Examples of a MAN are the part of the telephone company

network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

*****

IEEE Standards 802.2, 802.3, 802.4, 802.5, 802.6, High Speed LANs:

The Institute of Electrical and Electronics Engineers is a standards setting body. Each of their standards is numbered and a subset of the number is the actual standard. The 802 family of standards is ones developed for computer networking.

802.2 Logical Link Control:

The technical definition for 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers)."

802.2 "specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).

Basically, think of the 802.2 as the "translator" for the Data Link Layer. 802.2 is concerned with managing traffic over the physical network. It is responsible for flow and error control. The Data Link Layer wants to send some data over the network, 802.2 Logical Link Control helps make this possible. It also helps by identifying the line protocol, like NetBIOS, or Netware.

The LLC acts like a software bus allowing multiple higher layer protocols to access one or more lower layer networks. For example, if you have a server with multiple network interface cards, the LLC will forward packers from those upper layer protocols to the appropriate network interface. This allows the upper layer protocols to not need specific knowledge of the lower layer networks in use.

802.3 Ethernet:

Now that we have an overview of the OSI model, we can continue on these topics. I hope you have a clearer picture of the network model and where things fit on it.

802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.

Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can

be a minimum size of 72 bytes or a maximum of 1518 bytes.

The most common topology for Ethernet is the star topology.

802.4 Token Bus:

Token Bus (IEEE 802.4) is a standard for implementing token ring over the virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of the token bus is similar to Token Ring.

802.5 Token Ring:

As we mentioned earlier when discussing the ring topology, Token Ring was developed primarily by IBM. Token ring is designed to use the ring topology and utilizes a token to control the transmission of data on the network.

The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fibber.

Token ring can be run over a star topology as well as the ring topology.

There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fibber.

Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

802.6 DQDB:

IEEE 802.6 standard i.e. DQDB(Distributed Queue Dual Bus) is a MAN(Metropolitan Area Network) protocol. It can be defined as a high speed shared medium access control protocol that is used over a bus network. It has two unidirectional buses, for controlling purposes, where the bus can carry data, video, and voice over a network with bandwidth being allocated as per time slots. The advantage of using the paired bus is that it is used to tackles failure configuration. It can be extended up to 30 miles at 34-55 Mbps.

High Speed LANs:

- The most widely used high-speed LANs today are based on Ethernet and were developed by the IEEE 802.3 standards committee.
- To keep pace with the changing local networking needs of business, a number of approaches to high speed LAN design have become commercial products. The most important of these are:
- **Fast Ethernet and Gigabit Ethernet:** The extension of 10-Mbps CSMA/CD(Standard Ethernet) to higher speeds is a logical strategy because it tends to preserve the ivestment in existing systems.
- **Fibre Channel:** This standard provides a low-cost, easily scalable approach for achieving very high data rates in local areas.
- **High-speed wireless LANs:** Wireless LAN technology technology and standards have at last come of age, and high-speed standards and products are being introduced.

*****

Design Issues in Networks

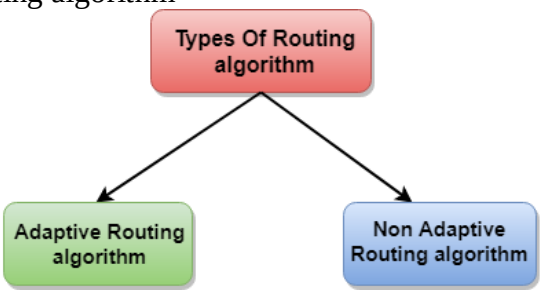
Routing Algorithms:

- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm:

The Routing algorithm is divided into two categories:

1.Adaptive Routing algorithm
2.Non-adaptive Routing algorithm



1.Adaptive Routing algorithm:

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link**

state algorithm is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

2.Non-Adaptive Routing algorithm:

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

*****

Congestion Control Algorithms:

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion

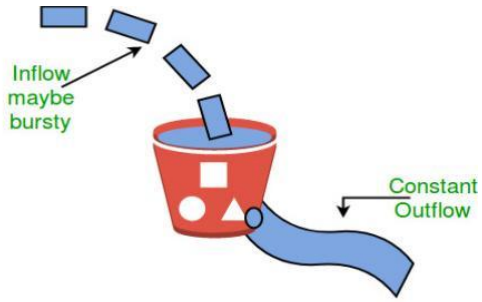
- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Congestion control algorithms:

1.Leaky Bucket Algorithm

Let us consider an example to understand

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following **steps** are involved in leaky bucket algorithm:

1. When host wants to send packet, packet is thrown into the bucket.
2. The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
3. Bursty traffic is converted to a uniform traffic by the leaky bucket.
4. In practice the bucket is a finite queue that outputs at a finite rate.

2.Token bucket Algorithm

Need of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. *f*
2. The bucket has a maximum capacity. *f*
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

*****

Network Layer in the Internet:

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

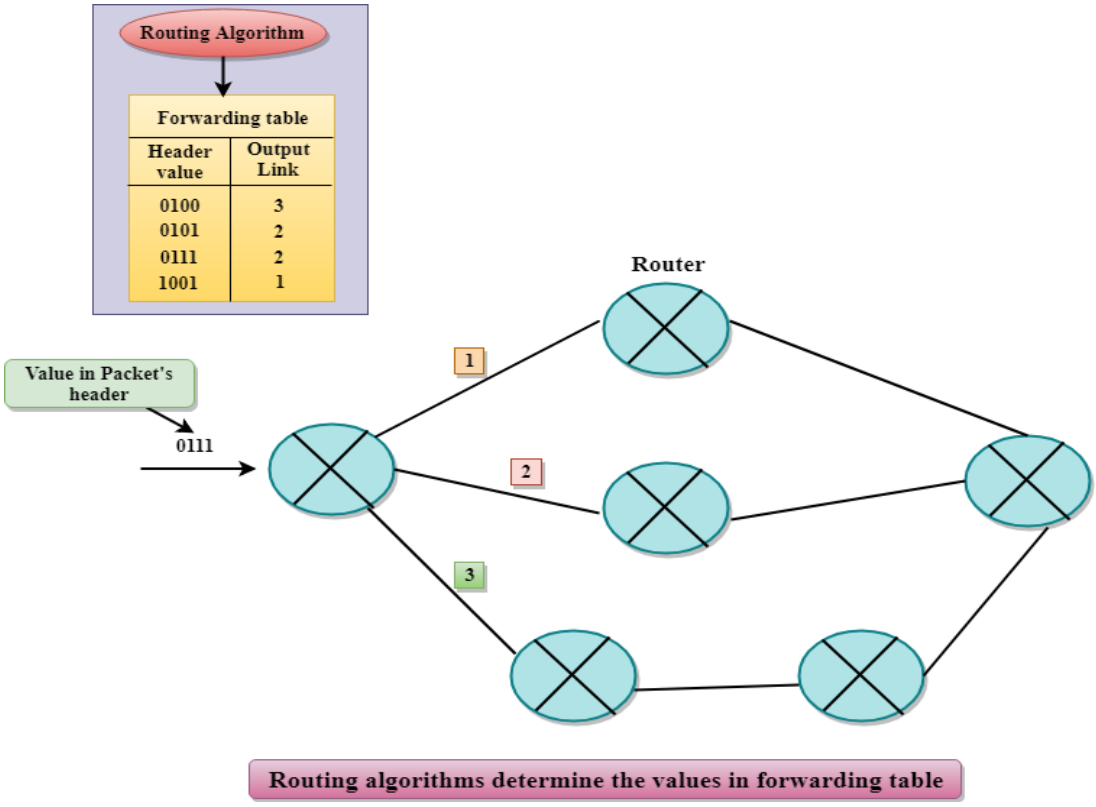
The main functions performed by the network layer are:

- **Routing:** When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
- **Logical Addressing:** The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
- **Internetworking:** This is the main role of the network layer that it provides the logical connection between different types of networks.
- **Fragmentation:** The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Forwarding & Routing:

In Network layer, a router is used to forward the packets. Every router has a forwarding table. A router forwards a packet by examining a packet's header field and then using the header field value to index into the forwarding table. The value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

For example, the router with a header field value of 0111 arrives at a router, and then router indexes this header value into the forwarding table that determines the output link interface is 2. The router forwards the packet to the interface 2. The routing algorithm determines the values that are inserted in the forwarding table. The routing algorithm can be centralized or decentralized.



Services Provided by the Network Layer

- **Guaranteed delivery:** This layer provides the service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** This service guarantees that the packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** This service ensures that the packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** This service ensures that the amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host. The network layer in the source host encrypts the payloads of datagrams being sent to the destination host. The network layer in the destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

*****

IP Protocol:

Here, IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.

The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.

History of Internet Protocol

The development of the protocol gets started in 1974 by **Bob Kahn and Vint Cerf**. It is used in conjunction with the Transmission Control Protocol (TCP), so they together named the TCP/IP.

The first major version of the internet protocol was IPv4, which was version 4. This protocol was officially declared in RFC 791 by the Internet Engineering Task Force (IETF) in 1981.

After IPv4, the second major version of the internet protocol was IPv6, which was version 6. It was officially declared by the IETF in 1998. The main reason behind the development of IPv6 was to replace IPv4. There is a big difference between IPv4 and IPv6 is that IPv4 uses 32 bits for addressing, while IPv6 uses 128 bits for addressing.

Function:

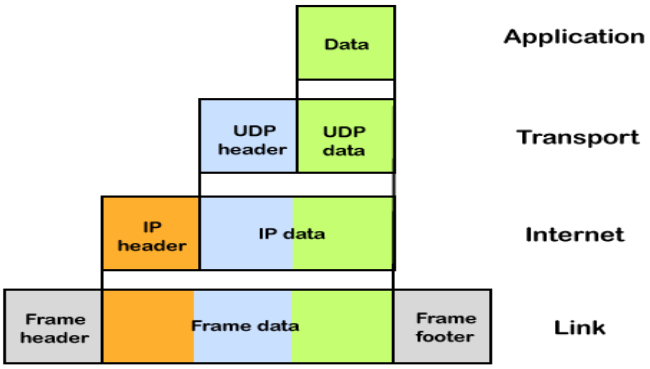
The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more IP networks. In order to achieve these functionalities, internet protocol provides two major things which are given below.

An internet protocol defines two things:

- Format of IP packet
- IP Addressing system

IP packet:

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.



An IP header contains lots of information about the IP packet which includes:

- Source IP address: The source is the one who is sending the data.
- Destination IP address: The destination is a host that receives the data from the sender.
- Header length
- Packet length
- TTL (Time to Live): The number of hops occurs before the packet gets discarded.
- Transport protocol: The transport protocol used by the internet protocol, either it can be TCP or UDP.

There is a total of 14 fields exist in the IP header, and one of them is optional.

Payload: Payload is the data that is to be transported.

*****

IP Address:

An IP address is the identifier that enables your device to send or receive data packets across the internet. It holds information related to your location and therefore making devices available for two-way communication. The internet requires a process to distinguish between different networks, routers, and websites. Therefore, IP addresses provide the mechanism of doing so, and it forms an indispensable part in the working of the internet. You will notice that most of the IP addresses are essentially numerical. Still, as the world is witnessing a colossal growth of network users, the network developers had to add letters and some addresses as internet usage grows.

An IP address is represented by a series of numbers segregated by periods(.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255.

IP addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN.

ICANN stands for Internet Corporation for Assigned Names and Numbers. It is a non-profit corporation founded in the US back in 1998 with an aim to manage Internet security and enable it to be available by all.

Types of IP addresses:

There are various classifications of IP addresses, and each category further contains some types.

Consumer IP addresses:

Every individual or firm with an active internet service system pursues two types of IP addresses, i.e., Private IP (Internet Protocol) addresses and public IP (Internet Protocol) addresses. The public and private correlate to the network area. Therefore, a private IP address is practiced inside a network, whereas the other (public IP address) is practiced outside a network.

1. Private IP addresses: All the devices that are linked with your internet network are allocated a private IP address. It holds computers, desktops, laptops, smartphones, tablets, or even Wi-Fi-enabled gadgets such as speakers, printers, or smart Televisions. With the expansion of IoT (internet of things), the demand for private IP addresses at individual homes is also seemingly growing. However, the router requires a method to identify these things distinctly. Therefore, your router produces unique private IP addresses that act as an identifier for every device using your internet network. Thus, differentiating them from one another on the network.

2. Public IP addresses: A public IP address or primary address represents the whole network of devices associated with it. Every device included within with your primary address contains their own private IP address. ISP is responsible to provide your public IP address to your router. Typically, ISPs contains the bulk stock of IP addresses that they dispense to their clients. Your public IP address is practiced by every device to identify your network that is residing outside your internet network.

Public IP addresses are further classified into two categories- dynamic and static.

- **Dynamic IPaddresses:** As the name suggests, Dynamic IP addresses change automatically and frequently. With this types of IP address, ISPs already purchase a bulk stock of IP addresses and allocate them in some order to their customers. Periodically, they re-allocate the IP addresses and place the used ones back into the IP addresses pool so they can be used later for another client. The foundation for this method is to make cost savings profits for the ISP.
- **Static IPaddresses:** In comparison to dynamic IP addresses, static addresses are constant in nature. The network assigns the IP address to the device only once and, it remains consistent. Though most firms or individuals do not prefer to have a static IP address, it is essential to have a static IP address for an organization that wants to host its network server. It protects websites and email addresses linked with it with a constant IP address.

Types of website IP addresses:

The following classification is segregated into the two types of website IP addresses i.e., shared and dedicated.

1. Shared IP addresses: Manystartups or individual website makers or various SME websites who don't want to invest initially in dedicated IP addresses can opt for shared hosting plans. Various web hosting providers are there in the market providing shared hosting services where two or more websites are hosted on the same server. Shared hosting is only feasible for websites that receive average traffic, the volumes are manageable, and the websites themselves are confined in terms of the webpages, etc.

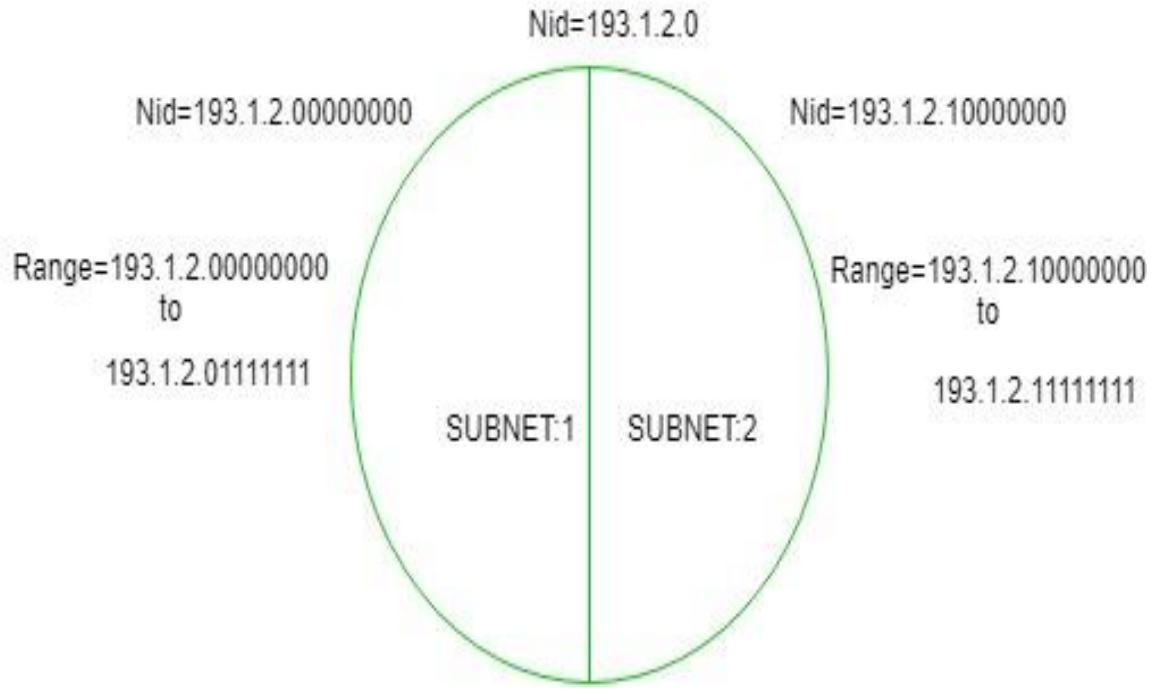
2. Dedicated IP addresses: Web hosting providers also provide the option to acquire a dedicated IP address. Undoubtedly dedicated IP addresses are more secure, and they permit the users to run their File Transfer Protocol (FTP) server. Therefore, it is easier to share and transfer data with many people within a business, and it also provides the option of anonymous FTP sharing. Another advantage of a dedicated IP addresses it the user can easily access the website using the IP address rather than typing the full domain name.

*****

Subnets and Internetworking:

When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting.so, maintenance is easier for smaller networks.

Now, let's talk about dividing a network into two parts:
so to divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

For Subnet-1:

The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.
Thus, the range of subnet-1:

193.1.2.0 to 193.1.2.127

For Subnet-2:

The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).
Thus, the range of subnet-2:

193.1.2.128 to 193.1.2.255

*****

UNIT III

Internet Transport Protocols: Transport Service, Elements of Transport Protocols, TCP and UDP Protocols, Quality of Service Model, Best Effort Model, Network Performance Issues. Over View of DNS, SNMP, Electronic Mail, FTP, TFTP, BOOTP, HTTP Protocols, World Wide Web, Firewalls.

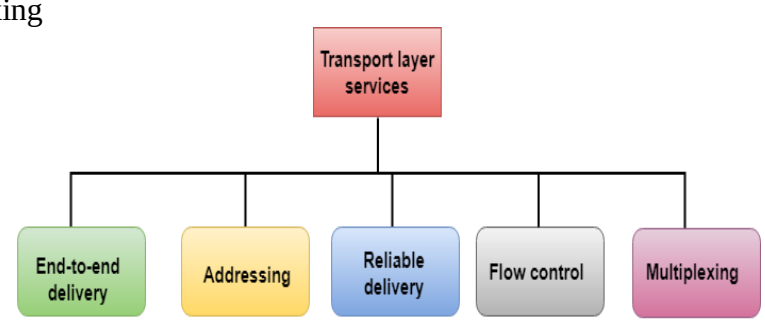
Internet Transport Protocols

Transport Service:

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

1.End-to-end delivery
2.Addressing
3.Reliable delivery
4.Flow control
5.Multiplexing



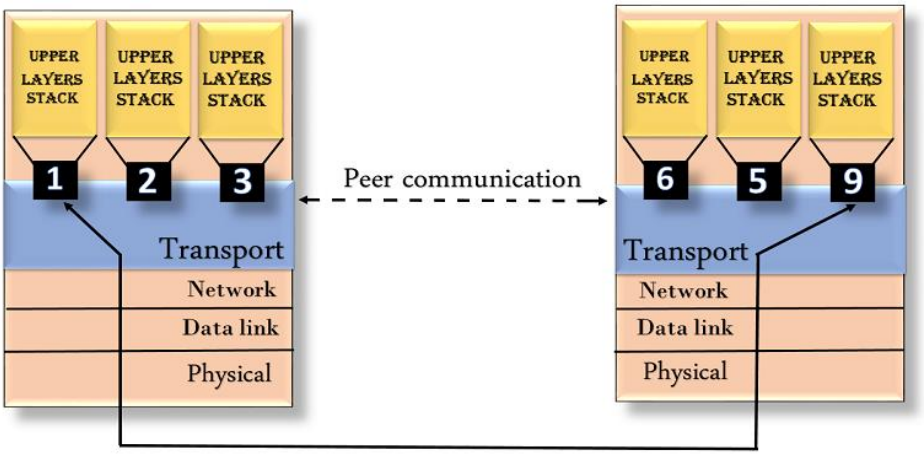
1.End-to-end delivery:

The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

2.Addressing:

- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.

- The transport layer protocols need to know which upper-layer protocols are communicating.

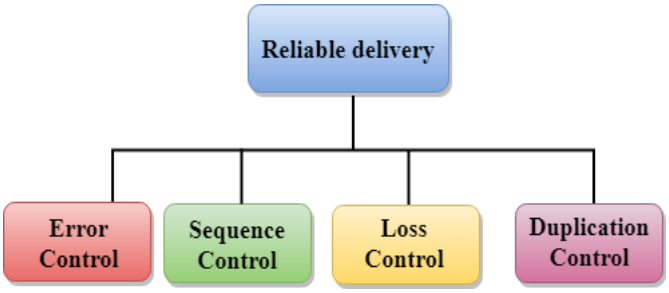


3.Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

The reliable delivery has four aspects:

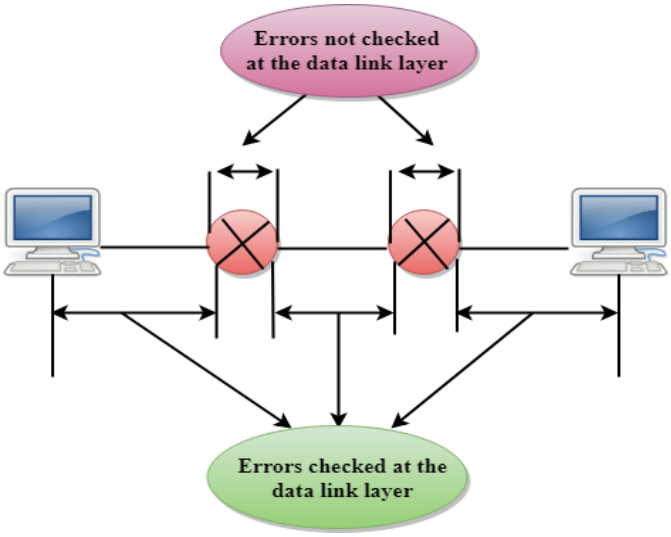
a)Error control
b)Sequence control
c)Loss control
d)Duplication control



a)Error Control:

- The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link.

Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.



b)Sequence Control:

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

c)Loss Control:

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

d)Duplication Control:

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

4.Flow Control:

Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so

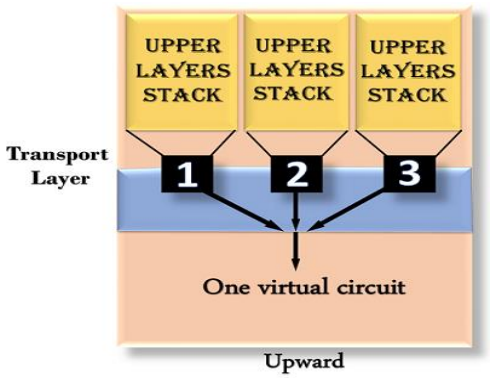
that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

5.Multiplexing:

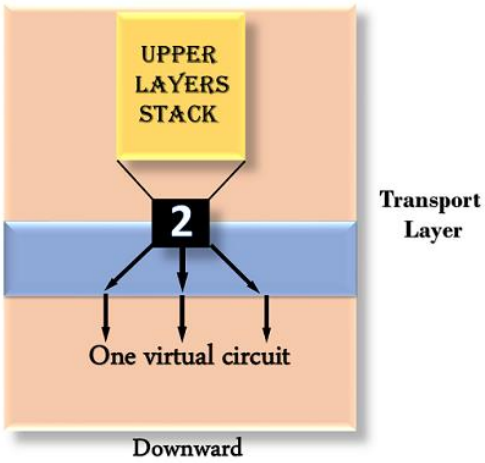
The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

a)Upward multiplexing: Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.



b)Downward multiplexing: Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.



*****

Elements of Transport Protocols:

To establish a reliable service between two machines on a network, transport protocols are implemented, which somehow resembles the data link protocols implemented at layer 2. The major difference lies in the fact that the data link layer uses a physical channel between two routers while the transport layer uses a subnet.

Following are the issues for implementing transport protocols−

Types of Service:

The transport layer also determines the type of service provided to the users from the session layer. An error-free point-to-point communication to deliver messages in the order in which they were transmitted is one of the key functions of the transport layer.

1.ErrorControl: Error detection and error recovery are an integral part of reliable service, and therefore they are necessary to perform error control mechanisms on an end-to-end basis. To control errors from lost or duplicate segments, the transport layer enables unique segment sequence numbers to the different packets of the message, creating virtual circuits, allowing only one virtual circuit per session.

2.FlowControl: The underlying rule of flow control is to maintain a synergy between a fast process and a slow process. The transport layer enables a fast process to keep pace with a slow one. Acknowledgements are sent back to manage end-to-end flow control. Go back N algorithms are used to request retransmission of packets starting with packet number N. Selective Repeat is used to request specific packets to be retransmitted.

3.Connection Establishment/Release: The transport layer creates and releases the connection across the network. This includes a naming mechanism so that a process on one machine can indicate with whom it wishes to communicate. The transport layer enables us to establish and delete connections across the network to multiplex several message streams onto one communication channel.

4.Multiplexing/De multiplexing: The transport layer establishes a separate network connection for each transport connection required by the session layer. To improve throughput, the transport layer establishes multiple network connections. When the issue of throughput is not important, it multiplexes several transport connections onto the same network connection, thus reducing the cost of establishing and maintaining the network connections.

When several connections are multiplexed, they call for demultiplexing at the receiving end. In the case of the transport layer, the communication takes place only between two processes and not between two machines. Hence, communication at the transport layer is also known as peer-to-peer or process-to-process communication.

5.Fragmentation and re-assembly: When the transport layer receives a large message from the session layer, it breaks the message into smaller units depending upon the requirement. This process is called fragmentation. Thereafter, it is passed to the network layer. Conversely, when the transport layer acts as the receiving process, it reorders the pieces of a message before reassembling them into a message.

6.Addressing: Transport Layer deals with addressing or labelling a frame. It also differentiates between a connection and a transaction. Connection identifiers are ports or sockets that label each frame, so the receiving device knows which process it has been sent from. This helps in keeping

track of multiple-message conversations. Ports or sockets address multiple conservations in the same location.

*****

TCP and UDP Protocols:

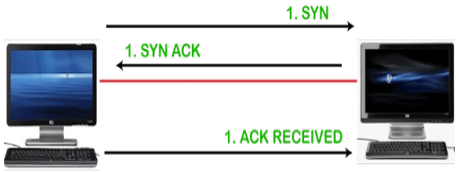
The TCP stands for **Transmission Control Protocol**. If we want the communication between two computers and communication should be good and reliable. For example, we want to view a web page, then we expect that nothing should be missing on the page, or we want to download a file, then we require a complete file, i.e., nothing should be missing either it could be a text or an image. This can only be possible due to the TCP. It is one of the most widely used protocols over the TCP/IP network.

Features of TCP:

1.Datadelivery:
TCP protocol ensures that the data is received correctly, no data is missing and in order. If TCP protocol is not used, then the incorrect data can be received or out of order. For example, if we try to view the web page or download a file without using TCP, then some data or images could be missing.

2.Protocol:
TCP is a connection-oriented protocol. Through the word **connection-oriented,** we understand that the computers first establish a connection and then do the communication. This is done by using a three-way handshake. In a **three-way handshake,** the first sender sends the SYN message to the receiver then the receiver sends back the SYN ACK message to confirm that the message has been received.

After receiving the **SYN ACK** message, the sender sends the acknowledgment message to the receiver. In this way, the connection is established between the computers. Once the connection is established, the data will be delivered. This protocol guarantees the data delivery means that if the data is not received then the TCP will resend the data.



Connection oriented protocol

UDP:

The UDP stands for **User Datagram Protocol**. Its working is similar to the TCP as it is also used for sending and receiving the message. The main difference is that UDP is a connectionless protocol. Here, connectionless means that no connection establishes prior to communication.

It also does not guarantee the delivery of data packets. It does not even care whether the data has been received on the receiver's end or not, so it is also known as the "fire-and-forget" protocol. It is also known as the **"fire-and-forget"** protocol as it sends the data and does not care whether the

data is received or not. UDP is faster than TCP as it does not provide the assurance for the delivery of the packets.

Differences between the TCP and UDP:

1.Type of protocol:

Both the protocols, i.e., TCP and UDP, are the transport layer protocol. TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol. It means that TCP requires connection prior to the communication, but the UDP does not require any connection.

2.Reliability:

TCP is a reliable protocol as it provides assurance for the delivery of the data. It follows the acknowledgment mechanism. In this mechanism, the sender receives the acknowledgment from the receiver and checks whether the acknowledgment is positive or negative. If the ACK is positive means, the data has been received successfully. If ACK is negative, then TCP will resend the data. It also follows the flow and error control mechanism.

UDP is an unreliable protocol as it does not ensure the delivery of the data.

3.FlowControl:

TCP follows the flow control mechanism that ensures a large number of packets are not sent to the receiver at the same time, while UDP does not follow the flow control mechanism.

4.Ordering:

TCP uses ordering and sequencing techniques to ensure that the data packets are received in the same order in which they are sent. On the other hand, UDP does not follow any ordering and sequencing technique; i.e., data can be sent in any sequence.

5.Speed:

Since TCP establishes a connection between a sender and receiver, performs error checking, and also guarantees the delivery of data packets while UDP neither creates a connection nor it guarantees the delivery of data packets, so UDP is faster than TCP.

6.Flowofdata:

In TCP, data can flow in both directions means that it provides the full-duplex service. On the other hand, UDP is mainly suitable for the unidirectional flow of data.

*****

Quality of Service Model:

Quality-of-Service (QoS) refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions or traffic aggregates. Basic phenomenon for QoS means in terms of packet delay and losses of various kinds.

Need for QoS :

- Video and audio conferencing require bounded delay and loss rate.
- Video and audio streaming requires bounded packet loss rate, it may not be so sensitive to delay.
- Time-critical applications (real-time control) in which bounded delay is considered to be an important factor.
- Valuable applications should be provided better services than less valuable applications.

QoS Specification:

QoS requirements can be specified as:

1. Delay
2. Delay Variation(Jitter)
3. Throughput
4. Error Rate

There are two types of QoS Solutions:

1. **Stateless Solutions:**Routers maintain no fine grained state about traffic, one positive factor of it is that it is scalable and robust. But it has weak services as there is no guarantee about kind of delay or performance in a particular application which we have to encounter.

2. **Stateful Solutions:**Routers maintain per flow state as flow is very important in providing the Quality-of-Service i.e. providing powerful services such as guaranteed services and high resource utilization, provides protection and is much less scalable and robust.

*****

Best Effort Model:

The best-effort model means that no QoS policy is implemented. It is natural to wonder why this model was not called no-effort. Within this model, packets belonging to voice calls, e-mails, file transfers, and so on are treated as equally important; indeed, these packets are not even differentiated. The basic mail delivery by the post office is often used as an example for the best-effort model, because the post office treats all letters as equally important.

The best-effort model has some benefits as well as some drawbacks.Following
are the main benefits of this model:

- **Scalability—**The Internet is a best-effort network. The best-effort model has no scalability limit. The bandwidth of router interfaces dictates throughput efficiencies.
- **Ease**—The best-effort model requires no special QoS configuration, making it the easiest and quickest model to implement.
  The drawbacks of the best-effort model are as follows:

- **Lack of service guarantee:** The best-effort model makes no guarantees about packet delivery/loss, delay, or available bandwidth.
- **Lack of service differentiation**: The best-effort model does not differentiate packets that belong to applications that have different levels of importance from the business perspective.

*****

Network Performance Issues:

1. High CPU Usage:

CPU, or "Central Processing Unit", is the primary component of a computer that receives and processes instructions for operating systems and applications. With such a big job on its shoulders, the signs of high CPU usage on a network device are troubling for many of us.

As your network device continues to work harder to perform tasks, there is a greater chance that things can go wrong.

The most common cause of high CPU usage is when your network becomes bogged down by enormous amounts of traffic. CPU usage can increase drastically when processes require more time to execute or when a larger number of network packets are sent and received throughout your network.

2. High Bandwidth Usage:

Bandwidth refers to a network's capacity to transfer data between devices or the internet within a given span of time. Higher bandwidth allows data to be transferred at a faster rate and allows more devices to connect at once.

When someone or something on your network is monopolizing your bandwidth by downloading gigabytes worth of data, possibly by video, it creates a congestion in your network.

When there's congestion in your network due to high bandwidth usage, it leaves not enough bandwidth for other parts of your network — which is when you can start experiencing problems like slow download speed over the internet.

3. Poor Physical Connectivity:

It may seem obvious, but when the time comes to troubleshoot network problems, our instinct is often to think about the most complex cases first, when sometimes the problem is actually very simple.

Testing all your cables one by one in search of that one cable that may be damaged can be a nightmare. We don't always have the equipment to do it and changing the cables one by one is sometimes not an option. Nevertheless, when a cable or connector is defective, the interface of the network equipment to which it is connected will typically generate errors.

This is also the case outside of the LAN. A copper, cable, or fiber-optic cable can be damaged, which will likely reduce the amount of data that can go through it without packet loss.

4. Malfunctioning Devices:

Another common network performance problem is when devices or hardware are not functioning properly, perhaps because they have been misconfigured or disabled.

You need to pay attention to all the switches and devices on your network to ensure that they're always working as they should be and so you can react quickly if they aren't.

Long story short, all devices on your network need to be configured correctly in order for your network to function properly. Whenever you install or reconfigure a device, or upgrade equipment

firmware on your network, you need to test that device to ensure that it's been configured correctly. Many performance issues are caused by misconfigurations that can turn into major problems down the line.

5. DNS Problems:

DNS, which stands for Domain Name System, is basically a directory for the Internet (and every internet-connected device) that matches domain names with IP addresses. Every single website has its own IP address on the web, and computers can connect to other computers via the Internet and look up websites using their IP address.

DNS errors essentially happen because you're unable to connect to an IP address, signalling that you may have lost network or internet access. For example, your site can simultaneously appear online for you, but offline to your visitors.

The inability to access the internet or particular sites can have a very immediate and negative impact on your business. Just a few hours offline can cost your company or website in both revenue and reputation.

That's why it's important to find and fix DNS problems as soon as possible.

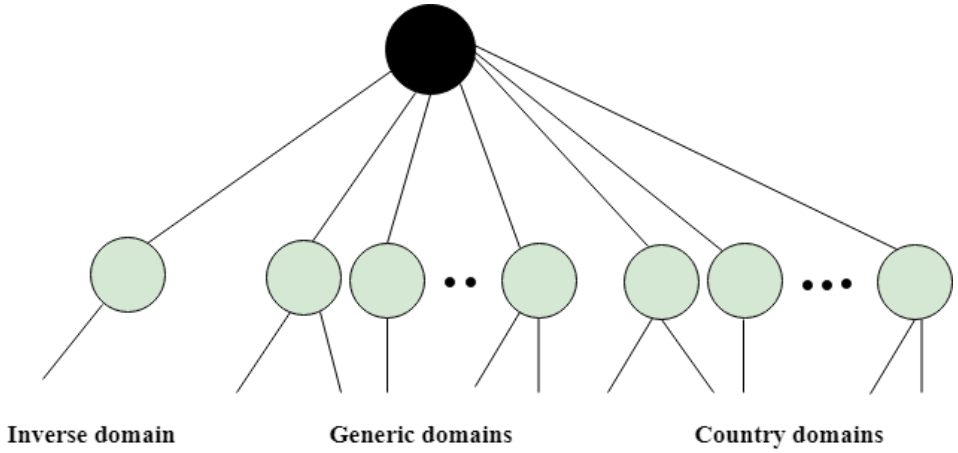
*****

Over View of 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.

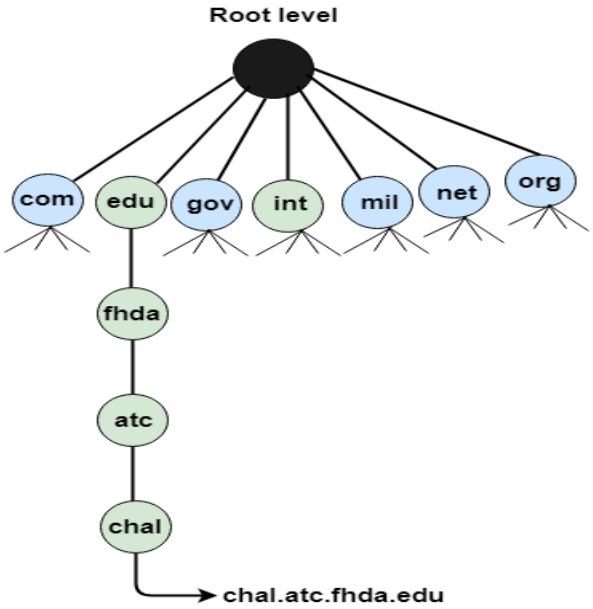


1.Generic Domains:

- 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
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers

org	Nonprofit Organizations
pro	Professional individual Organizations



2.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.

3.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.

*****

SNMP:

If an organization has 1000 of devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP):

SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.

SNMP components:

There are 3 components of SNMP:

1. **SNMP Manager:** It is a centralised system used to monitor network.It is also known as Network Management Station (NMS)
2. **SNMP agent:** It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
3. **Management Information Base:** MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.

SNMP messages:

Different variables are:

1. **GetRequest:**SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.

2. **GetNextRequest:**This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.

3. **GetBulkRequest:** This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.

4. **SetRequest:** It is used by SNMP manager to set the value of an object instance on the SNMP agent.

5. **Response:** It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.

6. **Trap:** These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.

7. **InformRequest:** It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.

SNMP security levels:

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv :**This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.

2. **authNopriv:** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.

3. **authPriv:** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

SNMP versions:

There are 3 versions of SNMP:

1. **SNMPv1:** It uses community strings for authentication and use UDP only.

2. **SNMPv2c:** It uses community strings for authentication. It uses UDP but can be configured to use TCP.

3. **SNMPv3:** It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy.This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

*****

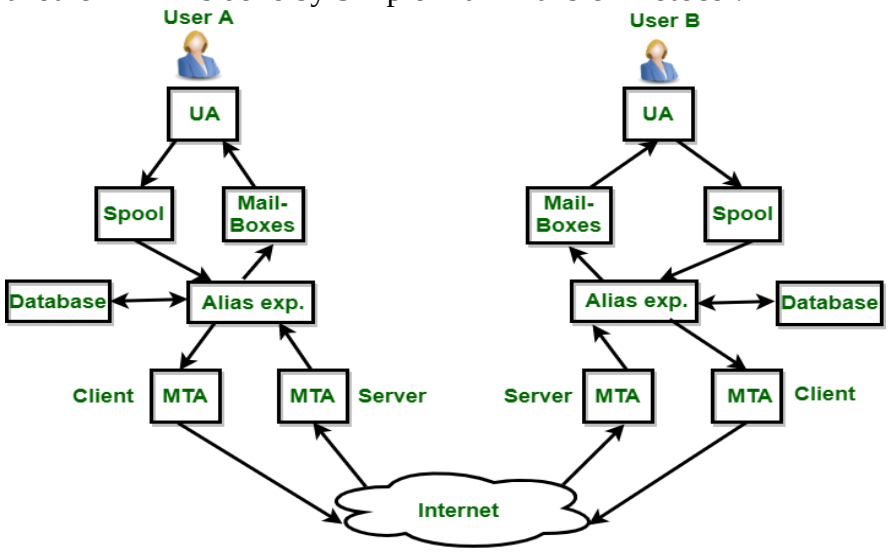
Electronic Mail:

Electronic Mail (e-mail) is one of most widely used services of Internet. This service allows an Internet user to send a message in formatted manner (mail) to the other Internet user in any part of world. Message in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called **sender** and person who receives mail is called **recipient**. It is just like postal mail service.

Components of E-Mail System :

The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained as following below.

1. **User Agent (UA):**The UA is normally a program which is used to send and receive mail. Sometimes, it is called as mail reader. It accepts variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.
2. **Message Transfer Agent (MTA):**MTA is actually responsible for transfer of mail from one system to another. To send a mail, a system must have client MTA and system MTA. It transfer mail to mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if destination mailbox is in another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.



3. **Mailbox :**It is a file on local hard drive to collect mails. Delivered mails are present in this file. The user can read it delete it according to his/her requirement. To use e-mail system each user must have a mailbox . Access to mailbox is only to owner of mailbox.
4. **Spool file :**This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from spool file for their delivery. E-mail allows one name, an **alias**, to represent several different e-mail addresses. It is known as **mailing list**, Whenever user have to sent a message, system checks recipients's name against alias database. If mailing list is present for defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for defined alias, there is no such mailing list is present, name itself becomes naming address and a single message is delivered to mail transfer entity.

Services provided by E-mail system :

1.Composition: The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.

2.Transfer: Transfer means sending procedure of mail i.e. from the sender to recipient.

3.Reporting: Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.

4.Displaying: It refers to present mail in form that is understand by the user.

5.Disposition: This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

*****

FTP:

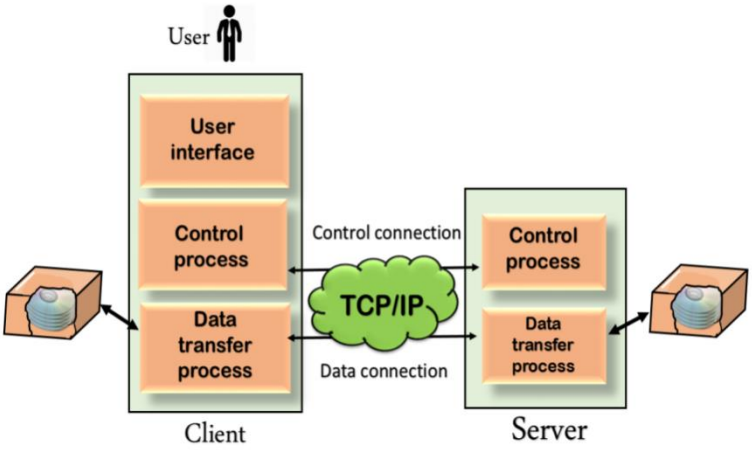
- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

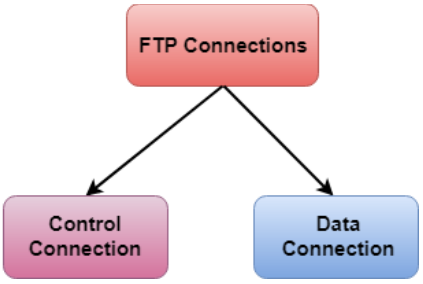
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP:



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



1.Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

2.Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients:

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

*****

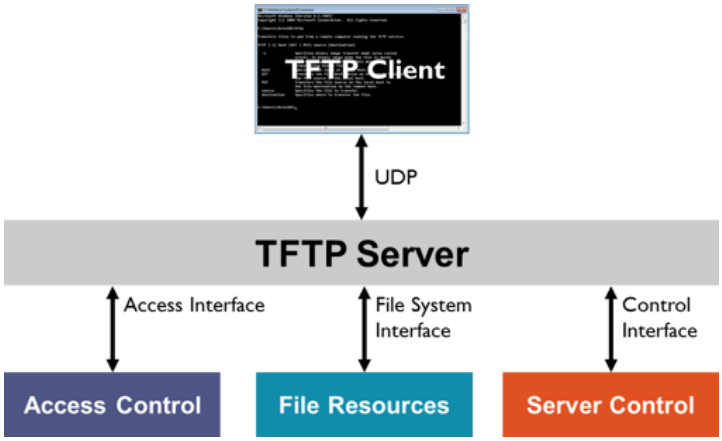
TFTP:

TFTP Server:-

TFTP Server is used for simple file transfer (typically for boot-loading remote devices).

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files. The TFTP protocol supports only file send and receive operations. File delete, move, and rename are not supported. Due to its limitations, TFTP is a complement to the regular FTP and not a replacement. It is only used when its simplicity is important, and its lack of features is acceptable. The most common application is bootstrapping, although it can be used for other purposes as well.

The TFTP Server can also be used to upload HTML pages onto the HTTP Server or to download log files to a remote PC. In this case, the File System Component must be used, and the HTTP Server must be properly configured.



1.Control Interface explains how to start/stop the TFTP Server and to manage built-in user accounts.

2.Access Interface shows how to filter out hosts, which are **not allowed** to connect to the TFTP Server.

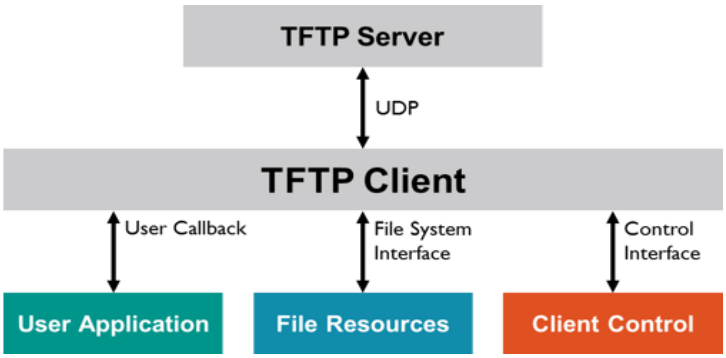
3.File System Interface gives you details about the functions that are used to read/write data on the TFTP server's storage device.

4.Configuration explains the configuration options of the TFTP server.

TFTP Client:-

TFTP Client is used to connect to a TFTP Server for simple file transfer.

A TFTP Client can exchange files with a **TFTP Server**. File delete, file move, and file rename are not impossible, because the TFTP protocol does not support these file operations in general.



1.Control Interface: explains how to start the TFTP Client.

2.User Callback: describes the operation of a TFTP client session and how an event notification is sent to the user application.

3.File System Interface: gives you details about the functions that are used to read/write data on the TFTP server's storage device.

4.Configuration: explains the configuration options of the TFTP client.

*****

BOOTP:

Bootstrap Protocol (BOOTP) provides a dynamic method for associating workstations with servers. It also provides a dynamic method for assigning workstation Internet Protocol (IP) addresses and initial program load (IPL) sources.

BOOTP is a TCP/IP protocol. It allows a client to find its IP address and the name of a load file from a server on the network. A client uses BOOTP to find this information without intervention from the user of the client.

The BOOTP server listens on the well-known BOOTP server port 67, which Dynamic Host Configuration Protocol (DHCP) also uses. Because of this, BOOTP and DHCP cannot operate at the same time on the same system. (DHCP is the preferred method for supporting BOOTP clients.) When the server receives a client request, it looks up the IP address for the client and returns a reply to that client. This reply contains both the IP address of the client and the name of the load file. The client then initiates a Trivial File Transfer Protocol (TFTP) request to the server for the load file.

1.PDF file for Bootstrap Protocol: You can view and print a PDF file of this information.

2.Configuring the BOOTP server: You can use two ways to configure the BOOTP server.

3.Changing BOOTP attributes: From the Change BOOTP Attributes (CHGBPA) display, you can specify the AUTOSTART attribute. This attribute determines whether the BOOTP server starts automatically when TCP/IP is started by the STRTCP command, or when the STRTCPSVR SERVER(*AUTOSTART) command is issued.

4.Working with the BOOTP table: From the Work with BOOTP Table display, you can add, change, remove, or display an entry in the BOOTP table.

*****

HTTP Protocols:

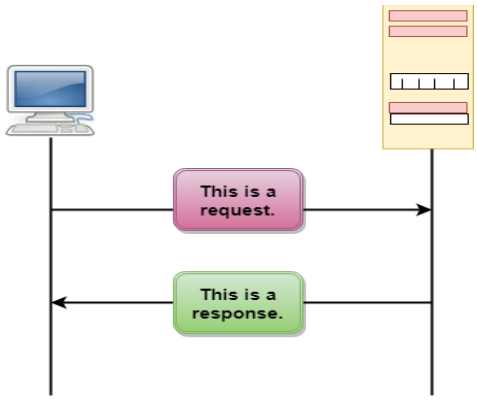
- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.

- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

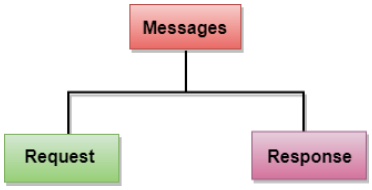
- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

HTTP Transactions:

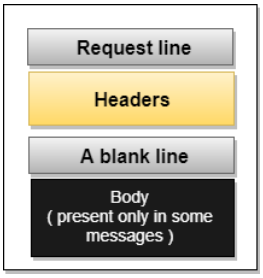


The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

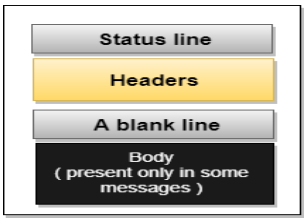
Messages:HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

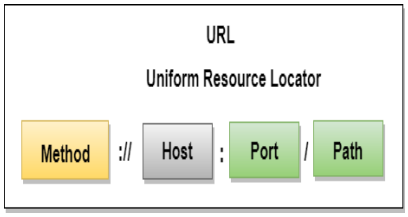


Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



Uniform Resource Locator (URL):

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.



- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

*****

World Wide Web:

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP. These links are electronic connections that link related pieces of information so that users can access the desired information quickly. Hypertext offers the advantage to select a word or phrase from text and thus to access other pages that provide additional information related to that word or phrase.

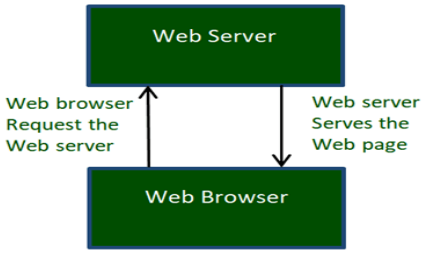
A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., *www.facebook.com*, *www.google.com*, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

Small websites store all of their WebPages on a single server, but big websites or organizations place their WebPages on different servers in different countries so that when users of a country search their site they could get the information quickly from the nearest server.

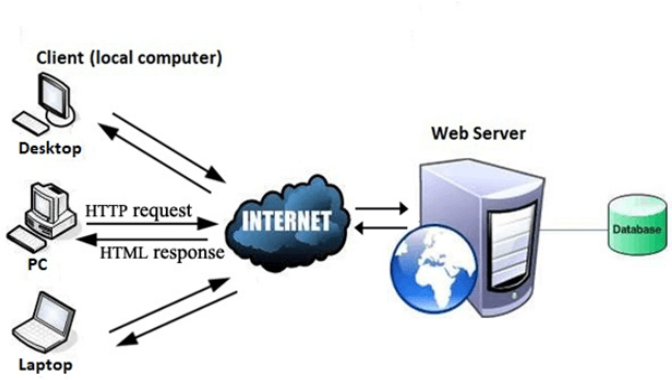
So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web.

World Wide Web Working:

Now, we have understood that WWW is a collection of websites connected to the internet so that people can search and share information. Now, let us understand how it works!



The Web works as per the internet's basic client-server format as shown in the following image. The servers store and transfer web pages or information to user's computers on the network when requested by the users. A web server is a software program which serves the web pages requested by web users using a browser. The computer of a user who requests documents from a server is known as a client. Browser, which is installed on the user' computer, allows users to view the retrieved documents.



All the websites are stored in web servers. Just as someone lives on rent in a house, a website occupies a space in a server and remains stored in it. The server hosts the website whenever a user requests its WebPages, and the website owner has to pay the hosting price for the same.

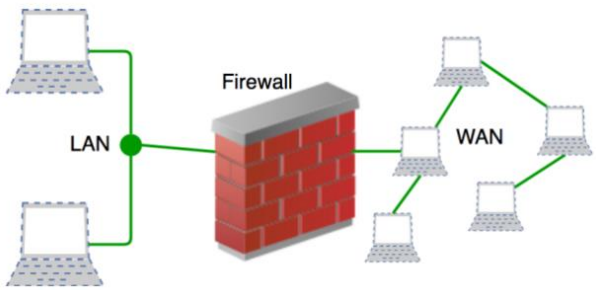
The moment you open the browser and type a URL in the address bar or search something on Google, the WWW starts working. There are three main technologies involved in transferring information (web pages) from servers to clients (computers of users). These technologies include Hypertext Markup Language (HTML), Hypertext Transfer Protocol (HTTP) and Web browsers.

*****

Firewalls:

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply
A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



History and Need for Firewall:

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.
But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.
Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Types of Firewall:

Firewalls are generally of two types: Host-based and Network-based.

1. **Host- based Firewalls:** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls:** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

*****

UNIT IV

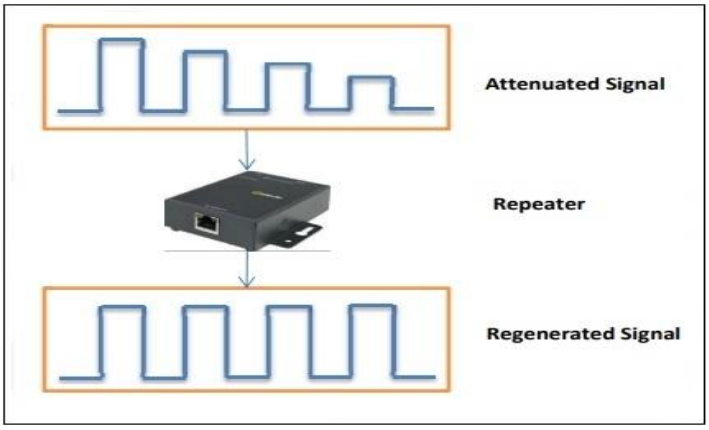
Network Devices: Over View of Repeaters, Bridges, Routers, Gateways, Multiprotocol Routers, Brouters, Hubs, Switches, Modems, Channel Service Unit CSU, Data Service Units DSU, NIC, Wireless Access Points, Transceivers, Firewalls, Proxies.

Overview of Cellular Networks, Ad-hoc Networks, Mobile Ad-hoc Networks, Sensor Networks

Network Devices

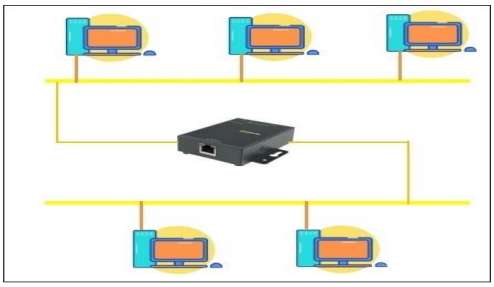
Over View of Repeaters:

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.So,repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN. This is shown in the following diagram −



Types of Repeaters: According to the types of signals that they regenerate, repeaters can be classified into two categories

- **AnalogRepeaters** : They can only amplify the analog signal.

- **Digital Repeaters** :They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types

- **Wired Repeaters**: They are used in wired LANs.
- **Wireless Repeaters**: They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories

- **Local Repeaters** : They connect LAN segments separated by small distance.
- **Remote Repeaters** : They connect LANs that are far from each other.

Advantages of Repeaters:

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- Repeaters don't require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

Disadvantages of Repeaters:

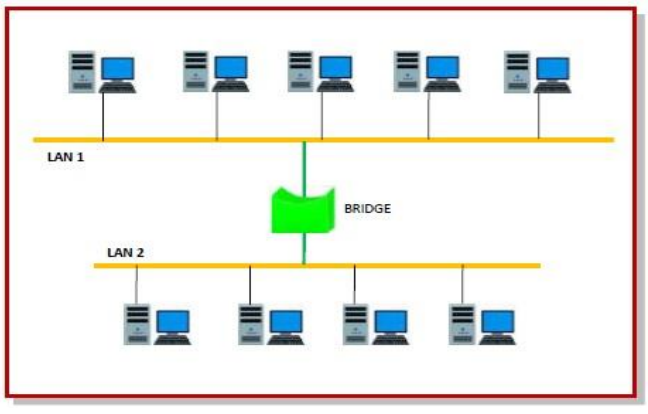
- Repeaters cannot connect dissimilar networks.
- They cannot differentiate between actual signal and noise.
- They cannot reduce network traffic or congestion.
- Most networks have limitations upon the number of repeaters that can be deployed.

*****

Bridges:

A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

The following diagram showsa bridges connecting two LANs:



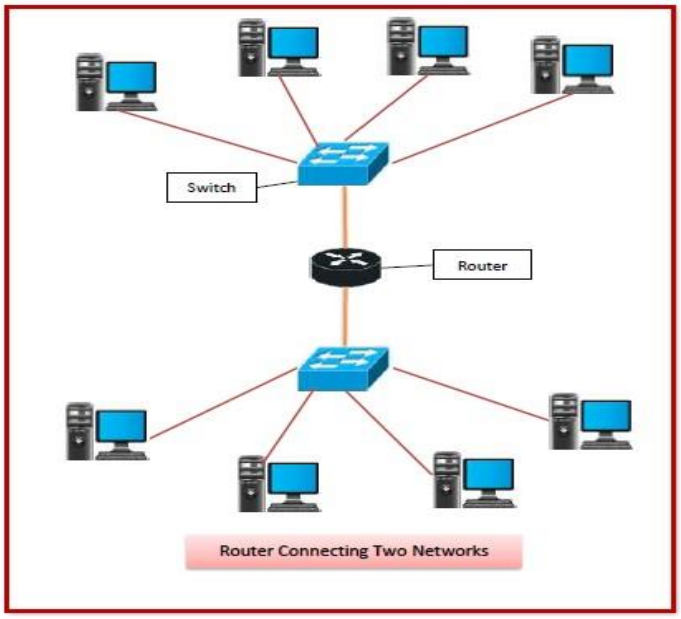
Uses of Bridge:

- Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
    - ✓ If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
    - ✓ If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
- By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
- In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
- In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
- Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
- Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
- A wireless bridge is used to connect wireless networks or networks having a wireless segment.

*****

Routers:

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



Features of Routers:

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs,bridges and switches.
- Routers are manufactured by some popular companies like −
    - ✓ Cisco
    - ✓ D-Link
    - ✓ HP

- ✓ 3Com
- ✓ Juniper
- ✓ Nortel

Routing Table: The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations. The router consults the routing table to determine the optimal route through which the data packets can be sent.

A routing table typically contains the following entities:

- IP addresses and subnet mask of the nodes in the network
- IP addresses of the routers in the network
- Interface information among the network devices and channels

Routing tables are of two types −

- **Static Routing Table** − Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.
- **Dynamic Routing Table** − Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of routers.

Types of Routers:

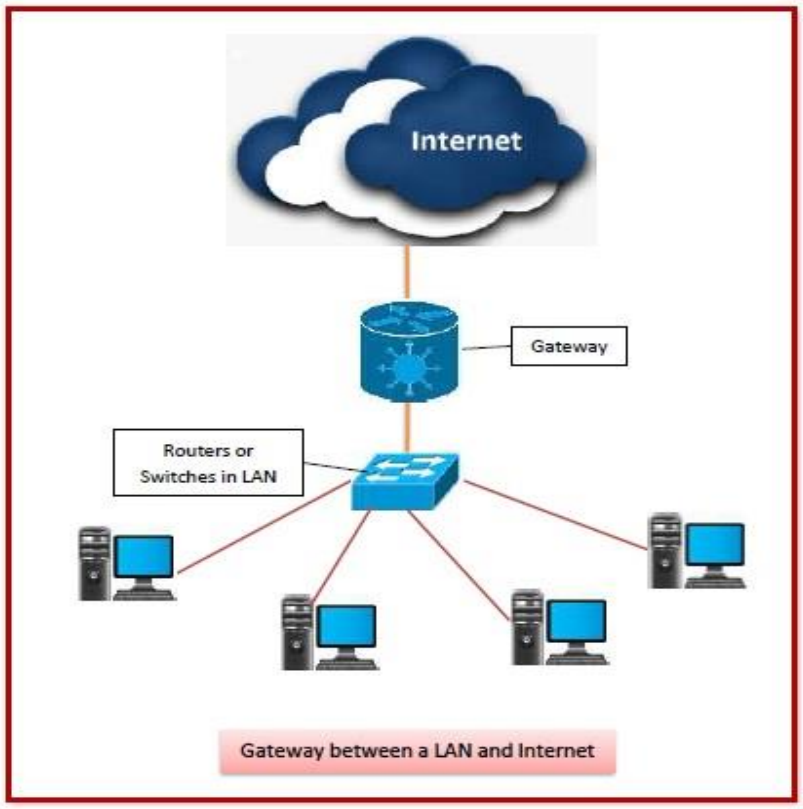
A variety of routers are available depending upon their usages. The main types of routers are −

- **Wireless Router:** They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
- **Broadband Routers:** They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- **Core Routers:** They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
- **Edge Routers:** They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.
- **Brouters:**Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

*****

Gateways:

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.



Features of Gateways:

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.

- It uses packet switching technique to transmit data across the networks.

Types of Gateways:

On basis of direction of data flow, gateways are broadly divided into two categories −

- **Unidirectional Gateways:** They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
- **Bidirectional Gateways:** They allow data to flow in both directions. They can be used as synchronization tools.

On basis of functionalities, there can be a variety of gateways, the prominent among them are as follows −

- **Network Gateway:** This is the most common type of gateway that provides as interface between two dissimilar networks operating with different protocols. Whenever the term gateway is mentioned without specifying the type, it indicates a network gateway.
- **Cloud Storage Gateway:** It is a network node or server that translates storage requests with different cloud storage service API calls, such as SOAP (Simple Object Access Protocol) or REST (REpresentational State Transfer).It facilitates integration of private cloud storage into applications without necessitating transfer of the applications into any public cloud, thus simplifying data communication.
- **Internet-To-Orbit Gateway (I2O):**It connects devices on the Internet to satellites and spacecraft orbiting the earth. Two prominent I2O gateways are Project HERMES and Global Educational Network for Satellite Operations (GENSO).
- **IoT Gateway:**IoT gateways assimilates sensor data from IoT (Internet of Things) devices in the field and translates between sensor protocols before sending it to the cloud network. They connect IoT devices, cloud network and user applications.
- **VoiP Trunk Gateway:**It facilitates data transmission between plain old telephone service (POTS) devices like landline phones and fax machines, with VoIP (voice over Internet Protocol) network.

*****

Multiprotocol Routers:

Multiprotocol Label Switching (MPLS) is a routing technique that augments speed and control of the network traffic by directing data from one node to the next node based on short path labels. Instead of being routed using long network addresses, the data packets are routed through path labels that identify virtual paths between the nodes rather than endpoints. MPLS speeds up traffic flows by avoiding complex lookups in the routing table at each node as in conventional routing algorithms.

MPLS is a scalable and protocol-independent routing technique. It works with Internet Protocol (IP), Ethernet, Frame Relay and Asynchronous Transport Mode (ATM). Despite the advent of newer technologies, it remains relevant due to its features like security, flexibility and traffic engineering.

Working Principle:

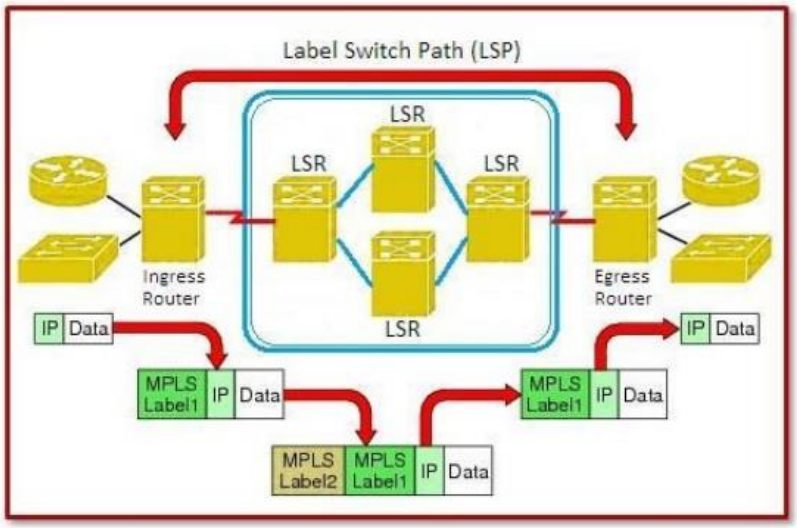
MPLS works by prefixing 32-bit labels with the MPLS header. The 32-bit label contains four fields −

- Label value field of 20-bits
- Traffic class field of 3-bits for QoS (quality of service)
- Bottom of stack flag of 1-bit (1 value denotes that the current label is the last one in the stack)
- TTL (time to live) field of 8-bits

When an IP packet enters the MPLS network, the 32-bit MPLS label is added by the ingress router, which is a label edge router (LER). LER decides the virtual path called label-switched path (LSP) that the packet will follow until it reaches its destination.

The subsequent label-switching routers (LSRs) along the LSP, forwards the packet based upon only the MPLS labels. They do not look beyond the MPLS label to the IP header.

When the packet reaches the egress router (also an LER), the MPLS labels are removed and the original IP packet is forwarded towards the final destination. The mechanism is depicted in the following diagram



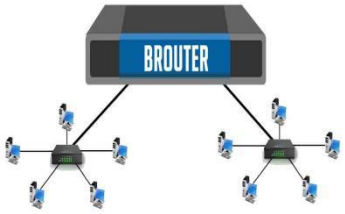
*****

Brouters:

A brouter is a networking device that functions both as a bridge and a router. It can forward data between networks (serving as a bridge), but can also route data to individual systems within a network (serving as a router).

Brouter is a network device, which operates as a combination of both bridge and router. In this single device, a user will get a function of both bridge and router, as it can send out data to create a connection or link as a bridge between networks, and can also route as a router the data to each system inside a network. It is aware of the processes for identified protocols to route particular

categories of packets, such as TCP/IP packets, and whichever additional packets it takes delivery of are sent out to perform a function of the bridge to further networks associated to the device.



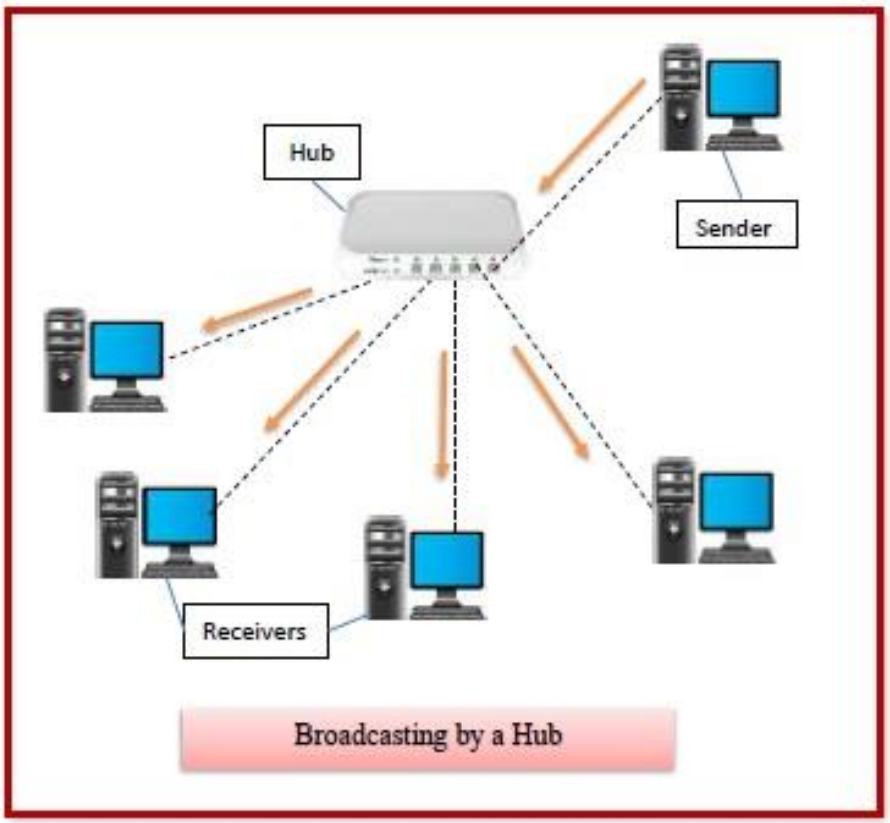
A **brouter** merges these two functions of bridge and router in the networking system by routing a number of inward bound data to the exact and approved individual systems, at the same time as sending out other data to another interrelated network.

*****

Hubs:

Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.



Features of Hubs:

- A hub operates in the physical layer of the OSI model.
- A hub cannot filter data. It is a non-intelligent network device that sends message to all ports.
- It primarily broadcasts messages. So, the collision domain of all nodes connected through the hub stays one.
- Transmission mode is half duplex.
- Collisions may occurs during setup of transmission when more than one computers place data simultaneously in the corresponding ports.
- Since they lack intelligence to compute best path for transmission of data packets, inefficiencies and wastage occur.
- They are passive devices, they don't have any software associated with it.
- They generally have fewer ports of 4/12.

Types of Hubs:

Initially, hubs were passive devices. However, with development of advanced technology, active hubs and intelligent hubs came into use.

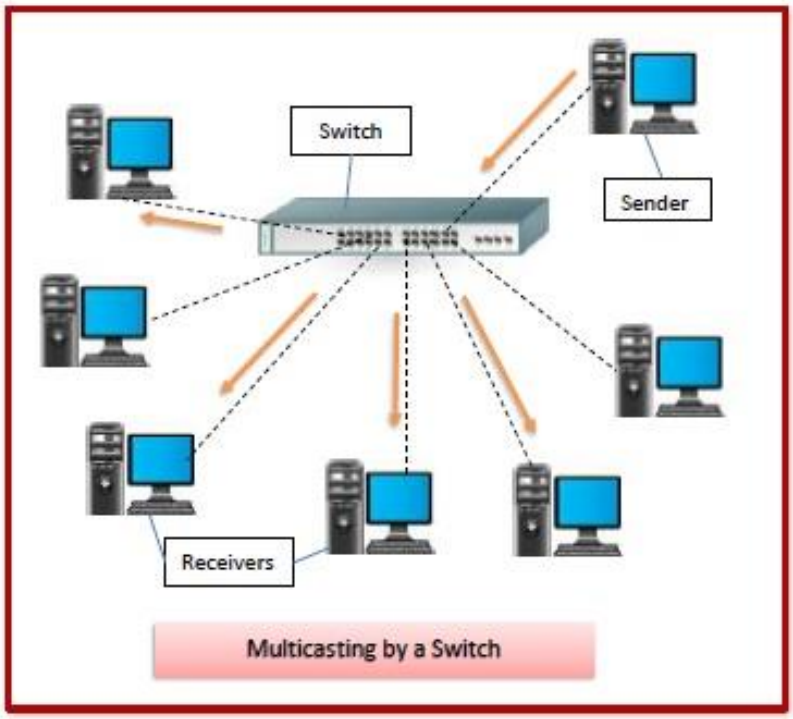
- **Passive Hubs** − Passive hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.
- **Active Hubs** − Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting centre. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.
- **Intelligent Hubs** − Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc.

*****

Switches:

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.



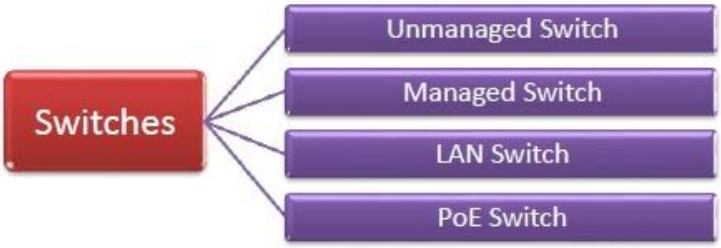
Features of Switches:

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.

- The number of ports is higher – 24/48.

Types of Switches:

There are variety of switches that can be broadly categorised into 4 types



- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoEGogabit Ethernets. PoEtechnology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections.

*****

Modems:

A modem is a box-type device that connects your home/office network directly to the internet. The router is also a box-type device that enables multiple computer systems (either wired or wireless) to simultaneously use the internet. Nowadays, both the devices are integrated and usually provided by the ISP(Internet Service Provider) when we take the new internet plan. But to get the internet connection for our home/office network, we need both modem and router either integrated or individual.

Although most of the time people get confused to identify both the devices, both devices have two different roles on a network that we will know on this topic. In this topic, we will understand the difference between the modem and router, but before understanding the main differences, we will first understand what Modem and Router are, their features, how they work, and what feature makes them different.

Types of Modem: The modem can be of various types based on data transmission and how it is installed. These types are given below:

1. External Modem:

- The external modem is connected outside the computer system using a serial cable.
- The installation is very easy, and it also provides a high data transmission rate.
- It is expensive but still used due to its high-speed data transmission in offices, mostly to avoid interruption in network connectivity.

2. Internal Modem:

- As its name suggests, the internal modem is installed over a PC's motherboard, termed as the internal modem.
- It looks similar to an electronic circuit and mounted into an expansion slot of the motherboard.
- The installation is complex, and its data transmission speed is also slow; hence it is used for the dedicated computer in homes/ or small spaces.

3. Wireless Modem:

- Wireless modems are connected to the computer systems without any cable, and most people use these modems for their personal use.
- These modems use radio frequencies to transmit the data through the air and also provides good transmission speed.

4. Dial-up Modem:

- Dial-up modem establishes the internet connection by connecting the ISP to the computer using the conventional telephone line.
- It uses a PSTN facility (Public Switched telephone network) and provides a transmission speed of **56kb/sec**.

5. Cable Modem:

- The cable modem is known as the broadband device as it allows the computer to communicate with ISP over a landline connection.
- It is connected with the landline connection using the coaxial cable and with the computer using the ethernet.

6. DSL Modem:

- DSL stands for **Digital Subscriber line** that allows the transmission of data over the normal telephone line.
- It provides a high data transmission speed, hence widely used in offices/homes.
- It can be used to connect to a computer or router to provide the internet connection through the ethernet port or USB port.
- The DSL modems are of two types:
    - **ADSL Modem**
    - **SDSL Modem**

7. Satellite Modem:

- Satellite modems are expensive modems and do not require any telephone connection for the internet.
- It uses satellite technology to send or receive the data.
- The speed of the modem is comparatively slower than DSL or cable Modem.

8. Half-duplex Modem:

- As the name suggests, it allows transmitting the data in one direction only at a time.
- It means if it is receiving the signal from one end, at that time, it will stop receiving the signal at another end. Once the transmission of one end is completed, then only the other end can transmit the data.

9. Full Duplex Modem:

- The full-duplex modems can transmit the data from both ends at the same time.
- It means it can receive the data from one end and the other end simultaneously without any interruption.

10. Four-wire Modem:

- It splits the pair of wires for incoming and outgoing data carriers.
- With this split, it can transmit the same frequency on both ends.

11. Two-wire Modem:

- It uses a pair of wires hence called two-wire modems. Only these two wires are used for incoming and outgoing carriers.

*****

Channel Service Unit CSU (OR) Data Service Units DSU:

CSU/DSU stands for Channel Service Unit/Data Service Unit, is a digital communications device that combines the functions of both a Channel Service Unit (CSU) and a Data Service Unit (DSU).

These devices lie between the telephone company network and the customer network at the demarcation point and are the local interfaces between the data terminal equipment (DTE) at the customer premises and the telco's digital communications line (such as a T1 line).

CSU/DSU working:

CSU/DSUs essentially function as the digital counterpart to analog modems. They are typically external units that look similar to an external modem, but they can also come in sizes that can be mounted in a rack. Unlike analog modems, CSU/DSUs do not perform signal conversion because the signal at both ends is already digital.

CSU/DSUs package digital data into a format suitable for the particular digital transmission line they are servicing, and buffer and rate-adapt digital signals going to and from the telephone company network. CSU/DSUs ensure that data frames are properly formed and timed for the telephone company network and provide a protective barrier to electrical disturbances that can harm customer premises equipment (CPE).

The customer's CSU/DSU then connects directly to the customer's router, and from there connects to the customer's network.

At the other end of the DDS line at the central office (CO), the telco has a similar CSU that interfaces with a multiplexer to feed into the carrier's backbone network.

*****

NIC:

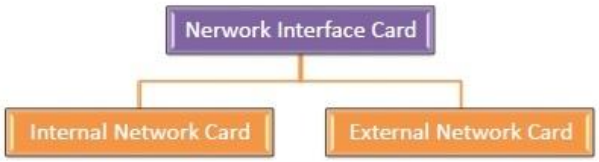
A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards

NIC cards are of two types −



Internal Network Cards: In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

External Network Cards: In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

*****

Wireless Access Points:

The **access point** (abbreviated AP or WAP (for **wireless access point**)), is a networking hardware device, such as a wireless router, that transmits and receives data (sometimes referred to as a transceiver) and also can serve as the bridge between the WAP device and a wired LAN (Local Area Network), which facilitates connectivity between nearby wireless clients. A WAP (also known as a hotspot) acts as a central transmitter and receiver of wireless radio signals.

For example, in the enterprise's wireless network, multiple workers can print documents from their PC that physically connected to the wireless network, with the help of a wireless printer that located at a central location in the office. The WAP device acts as a central hub for sending and receiving data via WLAN (Wireless Local Area Networks).

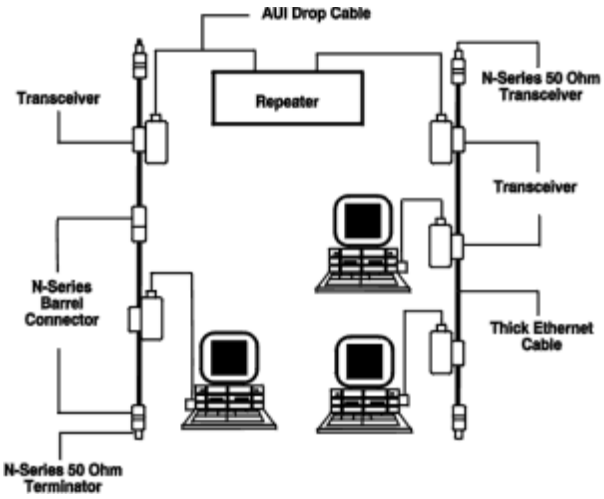
An access point is most commonly used in homes and office networks. A business may provide secure access points to you and co-worker to work anywhere in the office and remain connected to a central network; you are going through an access point, to access the internet without connecting to it using a cable. In most houses, the wireless access point (WAP) is a wireless router, which connected to a DSL or cable modem. The standards and frequencies are prescribed by IEEE, and all WAP devices use IEEE 802.11 standards.

*****

Transceivers:

Network transceivers connect network nodes and send and receive analog or digital signals. In Ethernet networks, they are called medium access units (MAU). Network transceivers apply signals onto a network wire and detect signals passing through the same wire. In local area networks (LAN), they may be used with networking repeaters, devices that regenerate or re-time signals to ensure that these signals are transmitted through all network segments.

This diagram describes the role of transmitter-receivers in a thick Ethernet network. Attachment unit interface (AUI) connections provide a path between each node's Ethernet interface and the MAU.



Types :

There are two basic types of network receivers: board and module.

- **Board-style** devices are network interface cards (NIC) that plug-in to a computer motherboard. They are more difficult to remove than chip-style devices, but also still classified as internal transmitter-receivers.
- **Modular** products are stand-alone devices. They are external network transmitter-receivers.

Specifications:

The Engineering360 SpecSearch database provides detailed information about network transceivers that use various network protocols (e.g., Ethernet, Token Ring). Industrial buyers should remember to specify the number of ports or channels through which the transceiver will connect to other devices. Additional product and performance specifications cover associated peripherals and the type of connection ports.

Features and Applications:

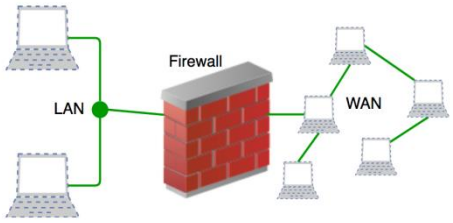
Network transceivers that use industrial protocols such as CANbus are used both in automotive and general industrial applications. Features for network transmitter-receivers include low-power management and fault protection.

*****

Firewalls:

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply
A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



History and Need for Firewall:

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.
But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

Types of Firewall:

Firewalls are generally of two types: Host-based and Network-based.

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

*****

Proxies:

Proxy server refers to a server that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources. There are different types of proxy servers available that are put into use according to the purpose of a request made by the clients to the servers. The basic purpose of Proxy servers is to protect the direct connection of Internet clients and internet resources. The proxy server also prevents the identification of the client's IP address when the client makes any request is made to any other servers.

- **Internet Client and Internet resources:** For internet clients, Proxy servers also act as a shield for an internal network against the request coming from a client to access the data stored on the server. It makes the original IP address of the node remains hidden while accessing data from that server.

- **Protects true host identity:** In this method, outgoing traffic appears to come from the proxy server rather than internet navigation. It must be configured to the specific application such as HTTPs or FTP. For example, organizations can use a proxy to observe the traffic of its employees to get the work efficiently done. It can also be used to keep a check on any kind of highly confidential data leakage. Some can also use it to increase their websites rank.

Types Of Proxy Server:

1. **Reverse Proxy Server:** The job of a reverse proxy server to listen to the request made by the client and redirect to the particular web server which is present on different servers.

2. **Web Proxy Server:** Web Proxy forwards the HTTP requests, only URL is passed instead of a path. The request is sent to particular the proxy server responds. Examples, Apache, HAP Proxy.

3. **Anonymous Proxy Server:** This type of proxy server does not make an original IP address instead these servers are detectable still provides rational anonymity to the client device.

4. **Highly Anonymity Proxy:** This proxy server does not allow the original IP address and it as a proxy server to be detected.

5. **Transparent Proxy:** This type of proxy server is unable to provide any anonymity to the client, instead, the original IP address can be easily detected using this proxy. But it is put into use to act as a cache for the websites. A transparent proxy when combined with gateway results in a proxy server where the connection requests are sent by the client then, then IP are redirected. Redirection will occurs without the client IP address configuration. HTTP headers present on the server-side can easily detect its redirection .

6. **CGI Proxy:** CGI proxy server developed to make the websites more accessible. It accepts the requests to target URLs using a web form and after processing its result will be returned to the web browser. It is less popular due to some privacy policies like VPNs but it still receives a lot of requests also. Its usage got reduced due to excessive traffic that can be caused to the website after passing the local filtration and thus leads to damage to the organization.

7. **Suffix Proxy:** Suffix proxy server basically appends the name of the proxy to the URL. This type of proxy doesn't preserve any higher level of anonymity. It is used for bypassing the web filters. It is easy to use and can be easily implemented but is used less due to the more number or web filter present in it.

8. **Distorting Proxy:** Proxy servers are preferred to generate an incorrect original IP address of clients once being detected as a proxy server. To maintain the confidentiality of the Client IP address HTTP headers are used.

9. **Tor Onion Proxy:** This server aims at online anonymity to the user's personal information. It is used to route the traffic through various networks present worldwide to arise difficulty in tracking the users' address and prevent the attack of any anonymous activities. It makes it difficult for any person who is trying to track the original address. In this type of routing, the information is encrypted in a multi-folds layer. At the destination, each layer is decrypted one by one to prevent the information to scramble and receive original content. This software is open-source and free of cost to use.

10. **12P Anonymous Proxy:** It uses encryption to hide all the communications at various levels. This encrypted data is then relayed through various network routers present at different locations and thus I2P is a fully distributed proxy. This software is free of cost and open source to use, It also resists the censorship.

11. **DNS Proxy:** DNS proxy take requests in the form of DNS queries and forward them to the Domain server where it can also be cached, moreover flow of request can also be redirected.

*****

Overview of Cellular Networks:

Cellular Network is formed of some cells, **cell** covers a geographical region, has a base station analogous to 802.11 AP which helps mobile users attach to network and there is an air-interface of physical and link layer protocol between mobile and base station. All these base stations are connected to Mobile Switching Center which connects cells to wide area net, manages call setup and handles mobility.

There is certain radio spectrum that is allocated to base station and to a particular region and that now needs to be shared. There are 2 techniques for sharing mobile-to-base station radio spectrum are:

1. **Combined FDMA/TDMA:**It divide spectrum in frequency channel and divide each channel into time slots.

2. **Code Division Multiple Access (CDMA):**It allows reuse of same spectrum over all cells. Net capacity improvement. Two frequency bands are used one of which is for forward channel (cell-site to subscriber) and one for reverse channel (sub to cell-site).

Need for Cellular Hierarchy:

Extending the coverage to the areas that are difficult to cover by a large cell. Increasing the

capacity of the network for those areas that have a higher density of users. Increasing number of wireless devices and the communication between them.

Cellular Hierarchy:

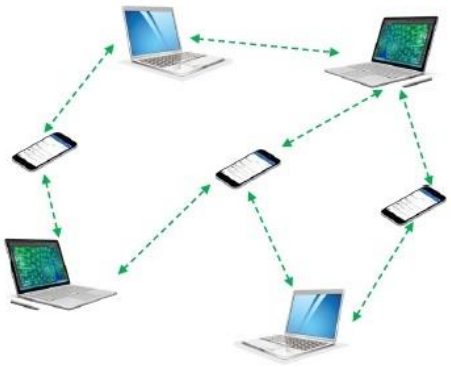
1. **Femtocells:**
   Smallest unit of the hierarchy, these cells need to cover only a few meters where all devices are in the physical range of the uses.
2. **Picocells:**
   Size of these networks is in the range of few tens of meters, e.g., WLANs.
3. **Microcells:**
   Cover a range of hundreds of meters e.g. in urban areas to support PCS which is another kind of mobile technology.
4. **Macro cells:**
   Cover areas in the order of several kilometers, e.g., cover metropolitan areas.
5. **Mega cells:**
   Cover nationwide areas with ranges of hundreds of kilometers, e.g., used with satellites.

*****

Ad-hoc Networks:

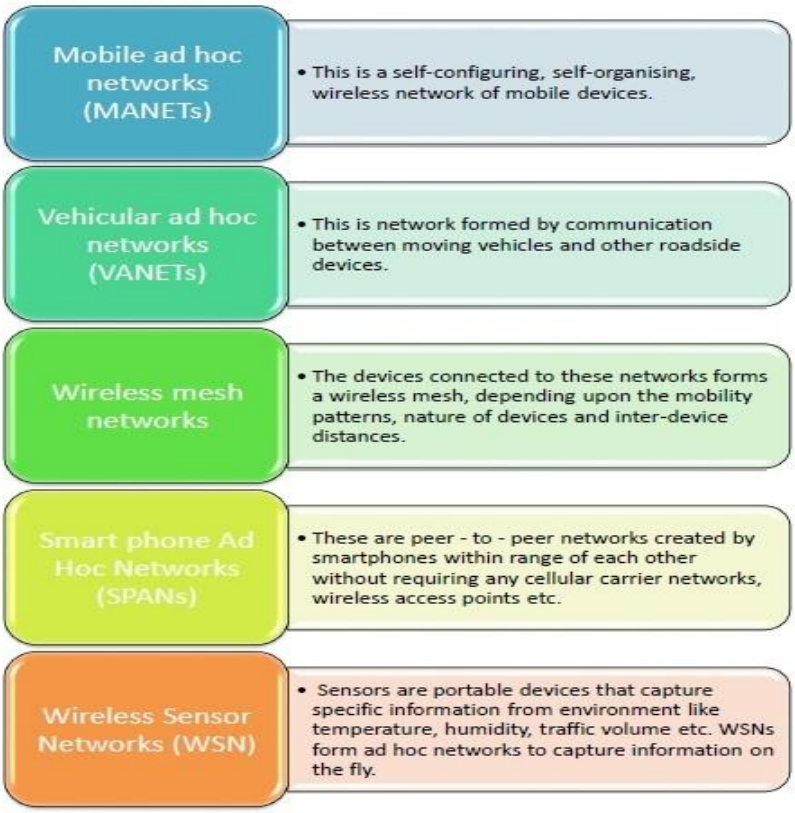
An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. The term ad hoc is a Latin word that literally means "for this," implying improvised or impromptu.

Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.



Classifications of Ad Hoc Networks:

Ad hoc networks can be classified into several types depending upon the nature of their applications. The most prominent ad hoc networks that are commonly incorporated are illustrated in the diagram below −



*****

Mobile Ad-hoc Networks:

- A MANET consists of a number of mobile devices that come together to form a network as needed, without any support from any existing internet infrastructure or any other kind of fixed stations.
- A MANET can be defined as an autonomous system of nodes or MSs(also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph.
- This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication between two mobile nodes relies on the wired backbone and fixed base stations.
- In a MANET, no such infrastructure exists and network topology may be changed dynamically in an unpredictable manner since nodes are free to move and each node has limiting transmitting power, restricting access to the node only in the neighboring range.
- MANETs are basically peer-to-peer, multi-hop wireless networks in which information packets are transmitted in a store and forward manner from a source to an arbitrary destination, via intermediate nodes.

Characteristics of MANET:

Some characteristics of adhoc network are as follows:

- **Dynamic topologies:** nodes are free to move arbitrarily; thus the network topology may be changed randomly and unpredictably and primarily consists of bidirectional links. In some cases where the transmission power of two nodes is different, a unidirectional link may exist.
- **Bandwidth-constrained and variable capacity links:** wireless links continue to have significantly lower capacity than infrastructure networks.
- **Energy-constrained operation:** some or all of the MSs in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes or devices, the most important system design optimization criteria may be energy conservation.
- **Limited physical security:** MANETs are generally more prone to physical security threats than wire line networks. The increased possibility of eavesdropping, spoofing, and denial of services (DoS) attacks should be considered carefully. To reduce security threats, many existing link security techniques are often applied within wireless networks.

Applications of MANET:

Some specific applications of ad hoc networks include industrial and commercial applications involving cooperative mobile data exchange. There are many existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks, with many of these networks consist of highly dynamic autonomous topology segments.

Advanced features of Mobile ad hoc networks, including data rates compatible with multimedia applications global roaming capability, and coordination with other network structures are enabling new applications.

- **Defense applications:** Many defense applications require on the fly communications set-up, and ad hoc/sensor networks are excellent candidates for use in battlefield management.
- **Crisis management applications:** These arise, for example, as a result of natural disasters in which the entire communication infrastructure is in disarray. Restoring communications quickly is essential.
- **Telemedicine:** The paramedic assisting the victim of a traffic accident in a remote location must access medical records (e.g. X-rays) and may need video conference assistance from a surgeon for an emergency intervention. In fact, the paramedic may need to instantaneously relay back to the hospital the victim's X-rays and other diagnostic tests from the site of the accident.

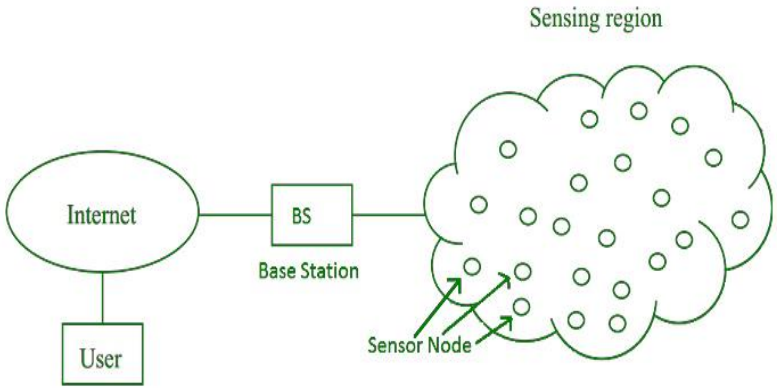
- **Tele-geoprocessing application:** The combination of GPS, GIS (Geographical Information Systems), and high-capacity wireless mobile systems enables a new type of application referred to as tele- geo processing.
- **Virtual Navigation:** A remote database contains the graphical representation of building, streets, and physical characteristics of a large metropolis. They may also "virtually" see the internal layout of buildings, including an emergency rescue plan, or find possible points of interest.
- **Education via the internet:** Educational opportunities available on the internet or remote areas because of the economic infeasibility of providing expensive last-mile wire line internet access in these areas to all subscribers.
- **Vehicular area network:** This a growing and very useful application of adhoc network in providing emergency services and other information. This is equally effective in both urban and rural setup. The basic and exchange necessary data that is beneficial in a given situation.

*****

Sensor Networks:

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.
Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:

1. Internet of Things (IOT)
2. Surveillance and Monitoring for security, threat detection
3. Environmental temperature, humidity, and air pressure
4. Noise Level of the surrounding
5. Medical applications like patient monitoring
6. Agriculture
7. Landslide Detection

Challenges of WSN:

1. Quality of Service
2. Security Issue
3. Energy Efficiency
4. Network Throughput
5. Performance
6. Ability to cope with node failure
7. Cross layer optimisation
8. Scalability to large scale of deployment

Components of WSN:

1. **Sensors:**
   Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.

2. **Radio Nodes:**
   It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.

3. **WLAN Access Point:**
   It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.

4. **Evaluation Software:**
   The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

THE-END