Computer Network

IBPS SO (IT) Exam 2017

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

Characteristics of a Network-

A network is a group of systems that are connected to allow sharing of resources—such as files or printers—or sharing of services-such as an Internet connection .There are two aspects of setting up a network: the hardware used to connect the systems together and the software installed on the computers to allow them to communicate.

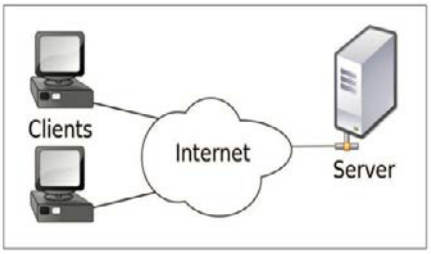
Components of Data Communication- A data communication system has five components**:**

1. **Message**: It is the actual information that is communicated. Format of information can be form of text, numbers, images, audio, and video.
2. **Sender**: It is a device that sends message. The sender can be computer, mobile phone, workstation etc.
3. **Receiver**: It is the device which receives message. It can be computer, mobile phone, workstation etc.
4. **Transmission Medium**: It is the physical path through which message travels from sender to receiver. It can be twisted-pair wire, coaxial cable, radio waves etc.
5. **Protocol**: It is the set of rules that controls data communication. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Workstations - The workstation also is known as a client, which is just a basic computer running a client operating system such as Windows XP or Linux. These users typically store their files on a central server so that they can share the files with other users on the network.

Hosts -The term host refers to any computer or device that is connected to a network and sends or receives information on that network. A host can be a server, a workstation, a printer with its own network card, or a device such as a router. We can summarize by saying that any system or device that is connected to the network is known as a host.

Server-



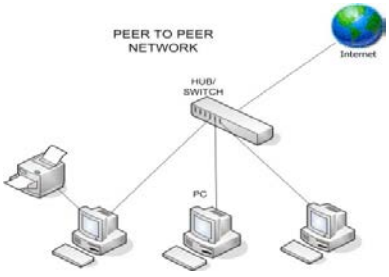
The server is a special computer that contains **more disk space and memory** than are found on client workstations. The server has special software installed that allows it to function as a server. This special software can provide file and print services (to allow sharing of files and printers), provide web pages to clients, or provide e-mail functionality to the company.

Types of Networks-

Organizations of different sizes, structures, and budgets need different types of networks. Networks can be divided into one of two categories: **peer-to-peer** and **server-based networks**.

1. **Peer-to-Peer Network**
2. **Server-Based Networks**

Peer-to-Peer Network-



A peer-to-peer network has no dedicated servers instead. A number of workstations are connected together for the purpose of sharing information or devices. When there is no dedicated server, all workstations are considered equal; any one of them can participate as the client or the server. Peer-to-peer networks are designed to satisfy the networking needs of home networks or of small companies

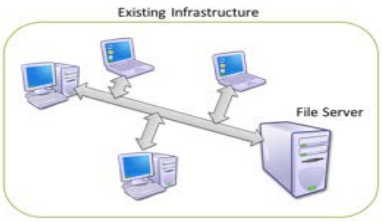
that do not want to spend a lot of money on a dedicated server but still want to have the Capability to share information or devices. For example, A small peer-to-peer network will allow these three computers to share the printer and the customer information with one another .The extra cost of a server was not incurred because the existing client systems were networked together to create the peer-to-peer network. **A big disadvantage of peer-to-peer networking is that you can't do your day-today administration in a single place.**

Server-Based Networks-

Usually after four or five systems have been networked, the need for a dedicated server to store all of the user accounts and data files becomes apparent—this is a server-based network. The advantage of a server-based network is that the data files that will be used by all of the users are stored on the one server. This will help you by giving you a central point to set up permissions on the data files, and it will give you a central point from which to back up all of the data in case data loss should occur. With a server-based network, the network server stores a list of users who may use network resources and usually holds the resources as well. The server in a server-based network may provide a number of different services. The services it will offer to the network usually are decided by the server's role. There are a number of different roles that a server could play on a network:

1. **File and print servers** **2. Application servers** **3. Web servers** **4. Directory servers**

1. File and print servers-:



File and print servers control, share printers and files among clients on the network. File and print servers were the original reason to have a network; a large number of users needed access to the same files, so the files were placed on a server, and all clients were connected to the server when they needed to work with the files.

2. Application servers-:

Application servers are servers that run some form of special program on the server. A good example of an application server is a server that runs the company's e-mail server. The e-mail server software is special software that can be run on a server operating system. Another example of software that would run on an application server is a database server product such as Microsoft SQL Server. A database server is a server that holds the company's core business data and typically gives this data to custom applications that run on the workstations. These are some applications that you might find on an application server:

A. Microsoft SQL Server **B. Oracle** **C. Microsoft Exchange Server** **D. IBM Lotus Domino**

3. Web servers-:

Web servers are servers that run the Hypertext Transfer Protocol (HTTP) and are designed to publish information on the Internet or the corporate intranet. Web servers are popular in today's businesses because **they host web applications (web sites)** for the organization. These web applications could be designed for internal use, or they could be used to publish information to the rest of the world on the Internet. Examples of web server software are Microsoft's Internet Information Services that runs on Windows or Apache web server software that runs on UNIX/Linux, Novell NetWare, and Windows.

4. Directory servers-

Directory servers **hold a list of the user accounts** that are allowed to log on to the network. This list of user accounts is stored in a database (known as the directory database) and can store information about these user accounts such as address, city, phone number, and fax number. A directory

service is designed to be a central database that can be used to store everything about such objects as users and printers.

Ethernet-:

Ethernet is a widely deployed LAN technology. This technology was invented by Bob Metcalfe and D.R. Boggs in the year 1970. It was standardized in IEEE 802.3 in 1980. Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data. Ethernet connector is network interface card equipped with **48-bits MAC address**. This helps other Ethernet devices to identify and communicate with remote devices in Ethernet. Traditional Ethernet uses 10BASE-T specifications. The number **10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet**. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5 twisted pair cable with RJ-5 connector. Ethernet follows Star topology with segment length up to 100 meters. All devices are connected to a hub/switch in a star fashion.

Fast-Ethernet-:

To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100MBPS. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 twisted pair cable. It uses CSMA/CD technique for wired media sharing among the Ethernet hosts and CSMA/CA (CA stands for Collision Avoidance) technique for wireless Ethernet LAN. Fast Ethernet on fiber is defined under 100BASE-FX standard which provides speed up to 100MBPS on fiber. Ethernet over fiber can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibers.

Ethernet vs Fast Ethernet

	Ethernet	Fast Ethernet
Speed	10 Mbps	100 Mbps
MAC	CSMA/CD	CSMA/CD
Network diameter	2.5 km	205 m
Topology	Bus, star	Star
Cable	Coax, UTP, Fiber	UTP, Fiber
Standard	802.3	802.3u
Cost	X	2X

Giga-Ethernet-:

After being introduced in 1995, Fast-Ethernet retained its high speed status only for three years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardizes Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.

Internet-: Internet is defined as an Information super Highway, to access information over the web. Internet can be defined in many ways as follows:

- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- Internet is accessible to every user all over the world.

Evolution: The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:

- The origin of Internet devised from the concept of **Advanced Research Project Agency Network (ARPANET).**

- **ARPANET** was developed by United States Department of Defense.
- Basic purpose of ARPANET was to provide communication among the various bodies of government.
- Initially, there were only four nodes, formally called **Hosts.**
- In 1972, the **ARPANET** spread over the globe with 23 nodes located at different countries and thus became known as **Internet.**
- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc.

Intranet - : Intranet is defined as private network of computers within an organization with its own server and firewall. Moreover we can define Intranet as:

- Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.
- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- Every computer in internet is identified by a unique IP address.
- Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.

Internet vs. Intranet: Apart from similarities there are some differences between the two. Following are the differences between Internet and Intranet:

Intranet	Internet
Localized Network.	Worldwide Network
Doesn't have access to Intranet	Have access to Internet.
More Expensive	Less Expensive
More Safe	Less Safe
More Reliability	Less Reliability

Extranet: Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.

Extranet vs. Intranet : The following table shows differences between Extranet and Intranet:

Extranet	Intranet
Internal network that can be accessed externally.	Internal network that cannot be accessed externally.
Extranet is extension of company's Intranet.	Only limited users of a company.
For limited external communication between customers, suppliers and business partners.	Only for communication within a company.

Internet Services allows us to access huge amount of information such as text, graphics, sound and software over the internet. Following diagram shows the four different categories of Internet Services.

IEEE Standards-:

The **Institute of Electrical and Electronics Engineers** Standards Association (IEEE-SA) is an organization within IEEE that develops global standards in a broad range of industries, including : power and energy, biomedical and health care, information technology and robotics, telecommunication and home automation, transportation, nanotechnology, information assurance, and many more.

- **IEEE 802.1**: Standards related to **network management**.
- **IEEE 802.2**: Standard for the **data link layer** in the OSI Reference Model.
- **IEEE 802.3**: Standard for the MAC layer for bus networks that use **CSMA/CD**. (Ethernet standard).
- **IEEE 802.4**: Standard for the **MAC layer for bus networks** that use a token-passing mechanism (token bus networks).
- **IEEE 802.5**: Standard for the **MAC layer for token-ring networks**.
- **IEEE 802.6**: Standard for Metropolitan Area Networks **(DQDB).**
- **IEEE 802.7** :Broadband LAN using Coaxial Cable disbanded
- **IEEE 802.8** :Fiber Optic TAG
- **IEEE 802.9** :Integrated Services LAN (ISLAN or iso Ethernet)
- **IEEE 802.10** :Interoperable LAN Securitydisbanded
- **IEEE 802.11**:Wireless LAN (WLAN) & Mesh (Wi-Fi certification)
- **IEEE 802.12**:100BaseVG
- **IEEE 802.13**:Unused ,Reserved for Fast Ethernet development
- **IEEE 802.14**:Cable modems
- **IEEE 802.15:**Wireless PAN

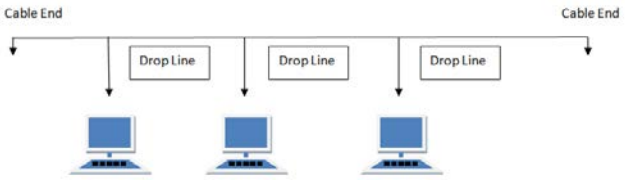
Network Topologies-:

A network topology is the physical layout of computers, cables, and other components on a network. There are a number of different network topologies, and a network may be built using multiple topologies. The different types of network layouts are

1. **Bus topology** **2.Star topology**
3. **Mesh topology** **4. Ring topology**
5. **Hybrid topology** **6. Wireless topology**

1. BUS Topology : Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

Advantages of Bus Topology:

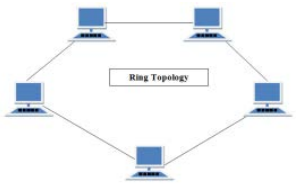


- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology:

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

2. RING Topology: It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



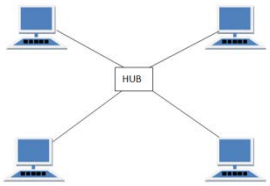
Advantages of Ring Topology:

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

Disadvantages of Ring Topology

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

3. STAR Topology: In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



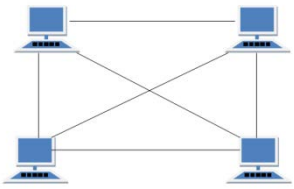
Advantages of Star Topology:

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

Disadvantages of Star Topology:

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity

4. MESH Topology: It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices. There are two techniques to transmit data over the Mesh topology, they are : 1. Routing 2. Flooding



Types of Mesh Topology

Partial Mesh Topology: In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.

Full Mesh Topology : Each and every nodes or devices are connected to each other.

Advantages of Mesh Topology

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

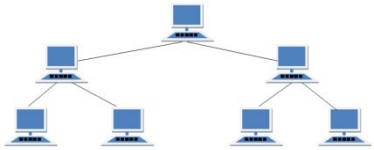
Disadvantages of Mesh Topology

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

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

Advantages of Tree Topology

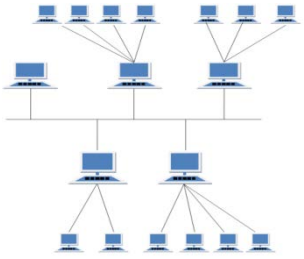
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.



Disadvantages of Tree Topology

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

5. HYBRID Topology: It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Advantages of Hybrid Topology

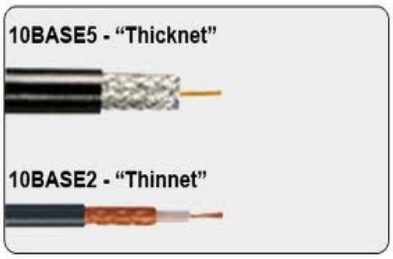
- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

Network Media and Connectors-:

Cabling is the medium for the transmission of data between hosts on the LANs. LANs can be connected together using a variety of cable types, such as unshielded twisted-pair, coax, or fiber. Each cable type has its own advantages and disadvantages, which you will examine in this section. There are three primary types of cable media that can be used to connect systems to a network—coaxial cable, twisted-pair cable, and fiber-optic cable. Transmission rates that can be supported on each of these physical media are measured in millions of bits per second, or megabits per second (Mbps).



Coaxial Cable-:

Coaxial, or coax, cable looks like the cable used to bring the cable TV signal to your television. One strand (a solid-core copper wire) runs down the middle of the cable. There are two types of coax cabling: **thinnet and thicknet.** The two differ in thickness and maximum cable distance that the signal can travel.

Twisted-Pair Cable-:

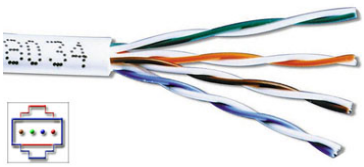
Coaxial cable is not as popular today as it was a few years ago; today the popularity contest has been dominated by twisted-pair cabling. Twisted-pair cabling gets its name by having four pairs of wires that are twisted to help reduce crosstalk or interference from outside electrical devices. (Crosstalk is interference from adjacent wires.) there are two forms of twisted-pair cabling—unshielded twisted-pair (UTP) and shielded twisted-pair (STP).

Fiber-Optic Cable-:

The third type of cabling that we want to discuss is fiber-optic cabling. Fiber-optic cabling is unlike coax and twisted-pair, because both of those types have a copper wire that carries the electrical signal. Fiber-optic cables use optical fibers that carry digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. There are two fibers per cable-one to transmit and one to receive. The core also can be an optical-quality clear plastic, and the cladding can be made up of gel that reflects signals back into the fiber to reduce signal loss. There are two types of fiber-optic cables: single-mode fiber (SMF) and multimode fiber (MMF).

Shielded twisted pair (STP)

Unshielded twisted pair (UTP)



1. Single-mode fiber Uses a single ray of light, known as a mode, to carry the transmission over long distances.

2. Multimode fiber Uses multiple rays of light (modes) simultaneously, with each ray of light running at a different reflection angle to carry the transmission over short distances

Cable	Max Distance	Transfer Rate	Connector Used
Thinnet	185 m	10 Mbps	BNC
Thicknet	500 m	10 Mbps	AUI

CAT 3 (UTP)	100 m	10 Mbps	RJ-45
CAT 5 (UTP)	100 m	100 Mbps	RJ-45
CAT 5e	100 m	1 Gbps	RJ-45
CAT 6	100 m	10 Gbps	RJ-45
Fiber	2 km	1+ Gbps	SC, ST

Network devices-:

Network devices are components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines. Devices used to setup a Local Area Network (LAN) are the most common types of network devices used by the public. A LAN requires a **hub**, **router**, **cabling** or **radio technology**, **network cards**, and if online access is desired, a high-speed **modem**. This is much less complicated than it might sound to someone new to networking.

Hub-:

- Hubs, also known as repeaters, are network devices that can operate on layer-1 (I.e. the physical layer) to connect network devices for communication.
- Hubs cannot process layer-2 or layer-3 traffic. Layer-2 deals with hardware addresses and layer-3 deals with logical (IP) addresses. So, hubs cannot process information based on MAC or IP addresses.
- Hubs cannot even process data based on whether it is a uni-cast, broadcast or multi-cast data.
- All that a hub does is that it transfers data to every port excluding the port from where data was generated.
- Hubs work only in half duplex mode I.e. a device connected to a hub can either send or receive data at a given time.
- If more than one device sends out data simultaneously then data collisions happen.
- In case of a collision, a hub rejects data from all the devices and signals them to send data again. Usually devices follow a random timer after which data is sent again to hub.
- Hubs are prone to collisions and as more and more devices are added to set up of multiple hubs, the chances of collisions will increase and hence the overall performance of network will go down.

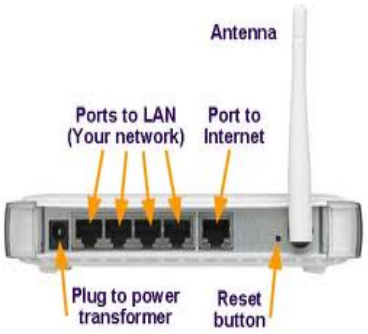
Switches

- Switches are network devices that operate **on layer-2 of OSI model** of communication.
- Switches are also known as intelligent hubs.
- Switches operate on hardware addresses to transfer data across devices connected to them.
- The reason switches are known as intelligent hubs is because they build address table in hardware to keep track of different hardware addresses and the port to which each hardware address is associated.

- The reason why they are compared to hubs because a switch, when started fresh, acts just like a hub. Suppose there are 3 devices connected to a switch. Let's call these devices as device A, device B and device C. Now, after a fresh start, if device A sends out a message to device B then just like a hub, switch will send it out to each port. But, it will store the hardware address and corresponding port in its hardware table. This means that whenever any other device will send any packet destined to device a then switch will act intelligently and send it to the correct port and not to all the ports. This way as more and more interaction takes place; the hardware table of switch grows and after a certain period of time switch becomes full blown intelligent version of a hub.

- Switches are often confused with bridges. Though both of them are mostly similar with major difference being that a switch forwards data at wire speed as it uses special hardware circuits known as ASICs.
- Switches, unlike hubs, support full duplex data transfer communication for each connected device.
- As layer 2 protocols headers have no information about network of data packet so switches cannot forward data based or networks and that is the reason switches cannot be used with large networks that are divided in sub networks.
- Switches can avoid loops through the use of spanning tree protocol.

Router -:

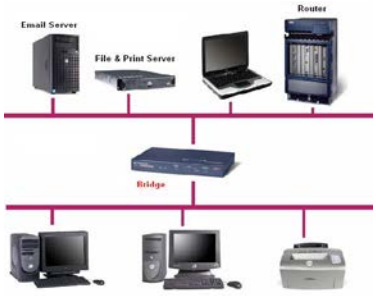


- Routers are the network devices that operate at Layer-3 of OSI model of communication.
- As layer-3 protocols have access to logical address (IP addresses) so routers have the capability to forward data across networks.
- Sometimes routers are also known as layer-3 switches.
- Routers are far more feature rich as compared to switches.
- Routers maintain routing table for data forwarding.
- Earlier, routing was slower as compared to switching. This was because of the fact that routing table lookup time was considerably high. The reason for this was that the complete packet was fetched into software buffers and then further operations were carried on it.
- Today, operations are done in hardware which has reduced the latency a lot and hence routers are not considered slower than switches today.
- Routers have lesser port densities as compared to switches.
- Routers are usually used as a forwarding network elements in Wide Area Networks.

Modem-:

A computer's digital signals must be converted to analog signals before they are transmitted over standard telephone lines. The communications devices that perform this conversion in a **modem**, sometimes called a ***dial-up modem***. The word, modem, is derived from the combination of the words, ***modulation,*** to change into an analog signal, and ***demodulation,*** to convert an analog signal into a digital signal. Both the sending and receiving ends o a standard telephone line (communications channel) must have a dial-up modem or data transmission to occur. For example, a dial-up modem connected to a sending computer converts the computer's digital signals into analog signals. The analog signals then can travel over a standard telephone line. At the receiving end, another dial-up modem converts the analog signals back into digital signals that a receiving computer can process.

Bridge-:



A bridge reads the outermost section of data on the data packet, to tell where the message is going. It reduces the traffic on other network segments, since it does not send all packets. Bridges can be programmed to reject packets from particular networks. Bridging occurs at the data link layer of the OSI model, which means the bridge cannot read IP address, but only the outermost hardware address of the packet. In our case the bridge can read the Ethernet data which gives the hardware address of the destination address, not the IP address. Bridges forward all broadcast messages. Only a special bridge called a translation bridge will allow two networks of different architectures to be connected. Bridges do not normally allow connection of networks with different architectures. The hardware address is also called the MAC (media access control) address. To determine the network segment a MAC address belongs to, bridges use one of the following

Transparent Bridging –: They build a table of addresses (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from. This type of bridge is used on Ethernet networks.

Source Route Bridging –:

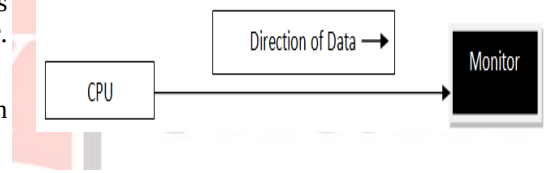
The source computer provides path information inside the packet. This is used on Token Ring networks. A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer o the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

Transmission Modes in Computer Networks: Transmission mode means transferring of data between two devices. It is also called communication mode. These modes direct the direction of flow of information. There are three types of transmission mode.
They are-:

- **Simplex Mode**
- **Half duplex Mode**
- **Full duplex Mode**

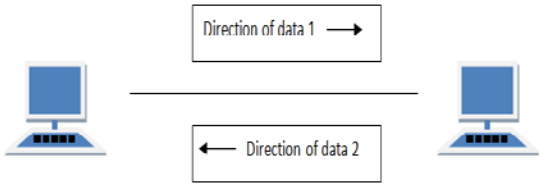
SIMPLEX Mode-: In this type of transmission mode data can be sent only through one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems.

Examples of simplex Mode is loudspeaker, television broadcasting, television and remote, keyboard and monitor etc.



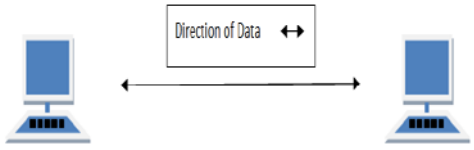
HALF DUPLEX Mode-: In half duplex system we can send data in both directions but it is done one at a time that is when the sender is sending the data then at that time we can't send the sender our message. The data is sent in one direction.

Example of half duplex is a **walkie- talkie** in which message is sent one at a time and messages are sent in both the directions.



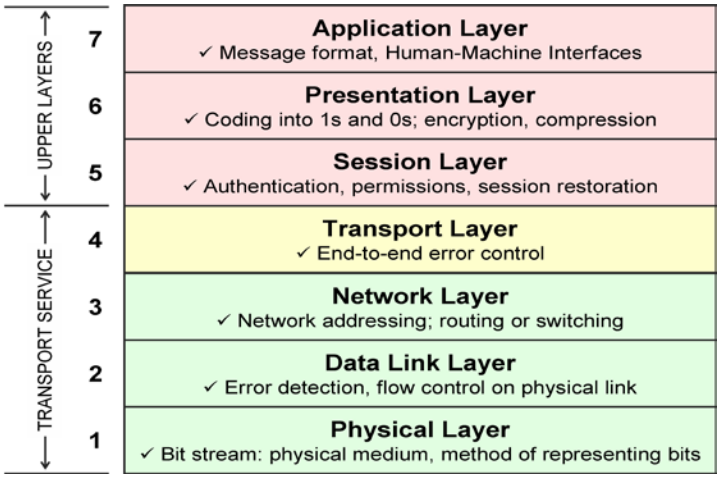
FULL DUPLEX Mode-: In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.

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



OSI (Open Systems Interconnection)

OSI (Open Systems Interconnection) is reference model for how messages should be transmitted between any two points in a telecommunication network. A reference model is a framework for understanding relationships. The purpose of the OSI reference model is to guide vendors and developers so that the digital communication products and software programs they create will interoperate. The OSI reference model defines seven layers of functions that take place at each end of a communication.



Layers of OSI

Layer 7-:

The application layer - This is the layer at which communication partners are identified, quality of service (QoS) is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. (This layer is not the application itself, although some applications may perform application layer functions.)

Layer 6-:

The presentation layer - This is a layer, usually part of an operating system (OS), that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly-arrived text).

Layer 5-:

The session layer - This layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end. It deals with session and connection coordination.

Layer 4-:

The transport layer - This layer manages the end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer.

Layer 3-:

The network layer - This layer handles the routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). The network layer does routing and forwarding.

Layer 2-:

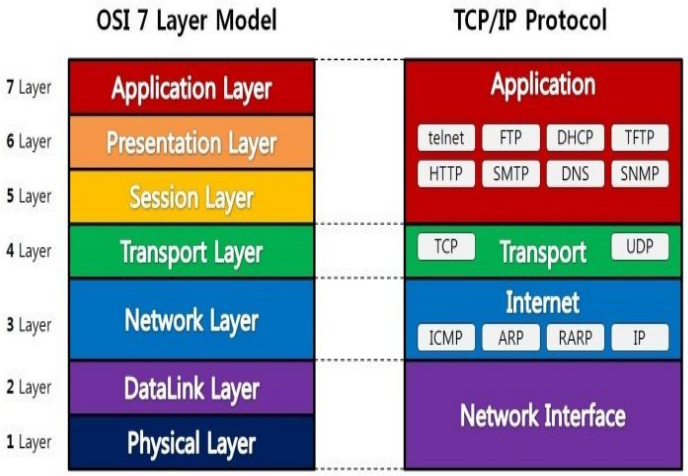
The data-link layer - This layer provides synchronization for the physical level and does bit-stuffing for strings of 1's in excess of 5. It furnishes transmission protocol knowledge and management. This layer has two sub layers, the Logical Link Control Layer and the Media Access Control Layer.

Layer 1-:

The physical layer - This layer conveys the bit stream through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier network.

TCP/IP Model

The Transmission Control Protocol / Internet Protocol (TCP/IP) was created by the **Department of Defense (DoD)** to make sure and protect data integrity, and also maintained communications in the time of disastrous war. However, if designed and deployed properly according to standard, a TCP/IP network can be a truly reliable and flexible one. Essentially, the Department of Defense (DoD) Model is a reduced version of the OSI Reference Model. The DoD model based on four layers:



Layer	Description	Protocols
4. Application	Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.	**HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP**, X Windows, other application protocols
3. Transport	Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data.	**TCP, UDP, RTP**
2. Internet	Packages data into IP datagram, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams.	**IP, ICMP, ARP, RARP**
1. Network interface/ Access	Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire.	Ethernet, **Token Ring**, **FDDI**, **X.25**, Frame Relay, RS-232, v.35

IP Address-:

Every machine on a network has a unique identifier. Most networks today, including all computers on the Internet, use the TCP/IP protocol as the standard for how to communicate on the network. In the TCP/IP protocol, **the unique identifier for a computer is called its IP address.**
There are two standards for IP addresses:-

1) IP Version 4 (IPv4) **2) IP Version 6 (IPv6)**

All computers with IP addresses have an IPv4 address, and many are starting to use the new IPv6 address system as well. Here's what these two address types mean:-

IPv4 uses 32 binary bits to create a single unique address on the network. An IPv4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number, also called an octet. For example: **216.27.61.137**.

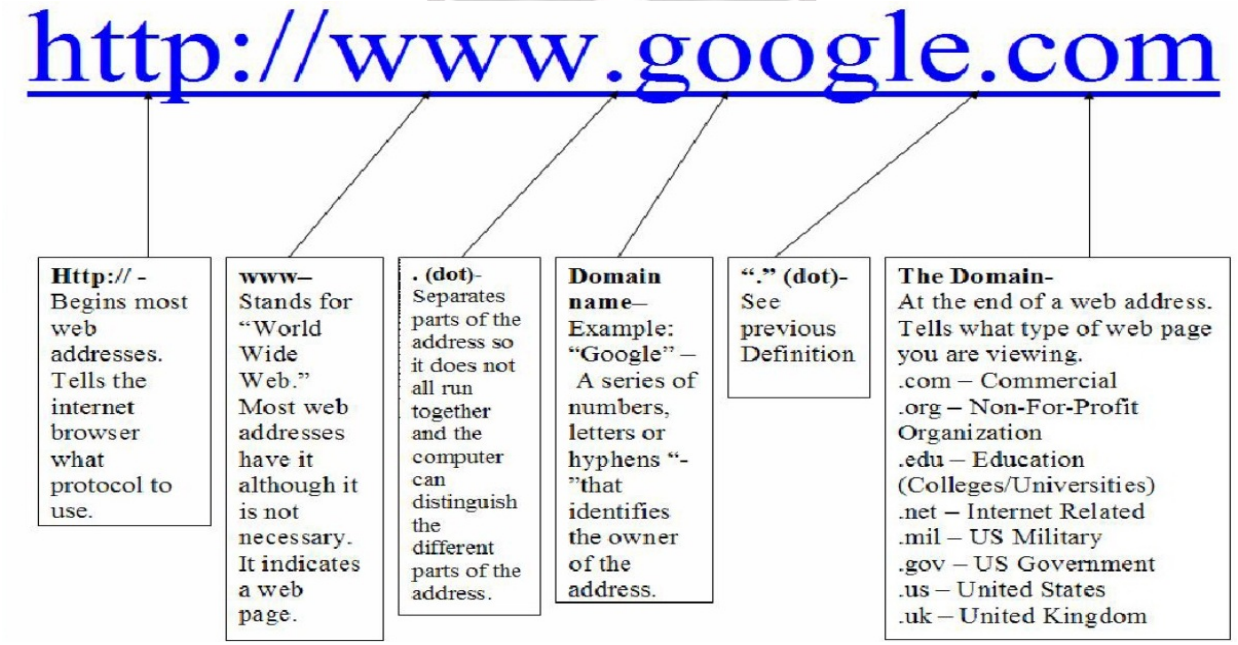
Class A - 0.0.0.0 - 127.255.255.255
Class B - 128.0.0.0 - 191.255.255.255
Class C - 192.0.0.0 - 223.255.255.255
Class D - 224.0.0.0 - 239.255.255.255
Class E - 240.0.0.0 - 247.255.255.255

IPv6 uses 128 binary bits to create a single unique address on the network. An IPv6 address is expressed by eight groups of hexadecimal (base-16) numbers separated by colons, as in **2001: cdba: 0000:0000:0000:0000:3257:9652** Groups of numbers that contain all zeros are often omitted to save space, leaving a colon separator to mark the gap (as in 2001:cdba::3257:9652).

At the dawn of IPv4 addressing, the Internet was not the large commercial sensation it is today, and most networks were private and closed off from other networks around the world. When the Internet exploded, having only 32 bits to identify a unique Internet address caused people to panic that we'd run out of IP addresses. Under IPv4, there are 232 possible combinations, which offer just under 4.3 billion unique addresses. IPv6 raised that to a panic-relieving 2128 possible addresses.

Web browser- :

A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online. Technically, a Web browser is a client program that uses HTTP to make requests of Web servers throughout the Internet on behalf of the browser user. Most browsers support e-mail and the File Transfer Protocol but a Web browser is not required for those Internet protocols and more specialized client programs are more popular. The first Web browser, called World Wide Web, was created in 1990. That browser's name was changed to Nexus to avoid confusion with the developing information space known as the World Wide Web. The first Web browser with a graphical user



interface was Mosaic, which appeared in 1993. Many of the user interface features in Mosaic went into Netscape Navigator. Microsoft followed with its Internet Explorer (IE).

Bandwidth -:

Bandwidth describes the rate at which data can be transferred to your computer from a website or internet service within a specific time. Therefore the amount of bandwidth you have (the bandwidth 'strength') determines the efficiency and speed of your internet activity – that is, when you open web pages, download files and so on. A useful analogy is a pipe with water running through it – the wider the pipe, the greater the volume of water that can flow through it. The same applies to bandwidth strength and the flow of the volume of data. Bandwidth is generally measured in 'bits per second' or sometimes 'bytes per second'.

Bookmark - :

When referring to the Internet or a browser, a bookmark or electronic bookmark is a method of saving a web page's address. For example, with most browsers pressing Ctrl + D will bookmark the page you are viewing.

Bounce - :

A description of what occurs when an e-mail message returns back to the sender as undeliverable. Some e-mail programs also have a **bounce** or **bounce back** feature built into them, which allows the user to bounce messages back to the sender causing the e-mail address to appear invalid.

Cyber Law-:

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law has been referred to as the Law of the Internet.

DNS-:

Domain Name System or Domain Name Service, a DNS is an Internet or other network server that helps to point domain names or the hostname to their associated IP address that was introduced by **Paul Mockapetris** and **Jon Postel** in1984. If a domain name is not found within the local database, the server may query other domain servers to obtain the address of a domain name. For example, when a user is accessing the ibtindia domain a user would enter the easy to remember domain: **ibtindia.com**. When entered that domain name is looked up on a Domain Name System to translate that name into an IP address that can be better understood by computer, e.g. 69.72.169.241. Using that IP address the computers can find the computer containing the **ibtindia** web page and forward that information to your computer.

Phishing-:

Pronounced like fishing, phishing is a term used to describe a malicious individual or group of individuals scamming users by sending e-mails or creating web pages that are designed to collect an individual's online bank, credit card, or other login information. Because these e-mails and web pages look like legitimate companies users trust them and enter their personal information.

Search engine-:

A search engine is a software program or script available through the Internet that searches documents and files for keywords and returns the results of any files containing those keywords. Today, there are thousands of different search engines available on the Internet, each with their own abilities and features. The first search engine ever developed is considered Archie, which was used to search for FTP files and the first text-based search engine is considered Veronica. Today, the most popular and well known search engine is Google.

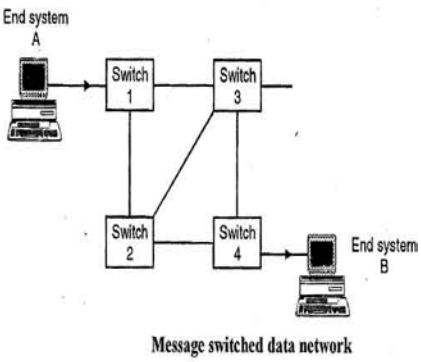
Firewall-:

A firewall is a software utility or hardware device that limits outside network access to a computer or local network by blocking or restricting network ports. Firewalls are a great step for helping prevent un-authorized access to a company or home network. The picture is an example of a hardware firewall, the ZyXEL ZyWALL a Unified Security Gateway with a Firewall and other security features. In addition to hardware firewalls like that shown above, basic hardware firewalls are also commonly found in most network routers and can be configured and setup through the router setup. Software firewalls are designed to protect the computer they are installed onto by blocking any unrestricted programs from sending and receiving information from the network or Internet. A good example of a software Firewall is the Windows Firewall that is included with Microsoft Windows.

Hacking-:

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian Laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information which is critical in nature.

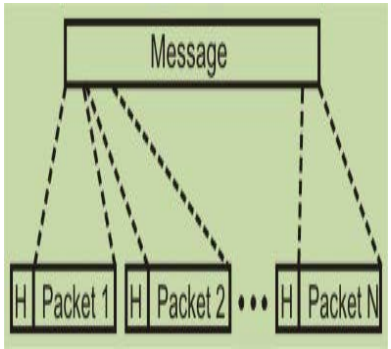
Message Switching-:



Message switched data network

In this switching method, a different strategy is used, where instead of establishing a dedicated physical line between the sender and the receiver, the message is sent to the nearest directly connected switching node. This node stores the message, checks for errors, selects the best available route and forwards the message to the next intermediate node. The line becomes free again for other messages, while the process is being continued in some other nodes. Due to the mode of action, this method is also known as **store-and-forward technology** where the message hops from node to node to its final destination. Each node stores the full message, checks for errors and forwards it. In this switching technique, more devices can share the network bandwidth, as compared with circuit switching technique. Temporary storage of message reduces traffic congestion to some extent. Higher priority can be given to urgent messages, so that the low priority messages are delayed while the urgent ones are forwarded faster. Through broadcast addresses one message can be sent to several users. Last of all, since the destination host need not be active when the message is sent, message switching techniques improve global communications.

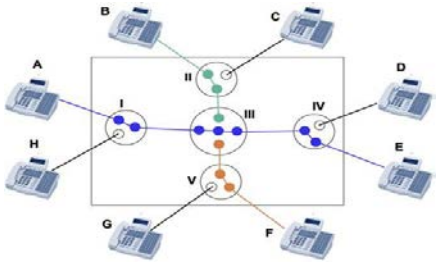
Packet Switching -:



The basic approach is not much different from message switching. It is also based on the same 'store-and-forward' approach. However, to overcome the limitations of message switching, messages are divided into subsets of equal length called packets. This approach was developed for long-distance data communication (1970) and it has evolved over time. In packet switching approach, data are transmitted in short packets (few Kbytes). A long message is broken up into a series of packets as shown in Fig. Every packet contains some control information in its header, which is required for routing and other purposes. Main difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing

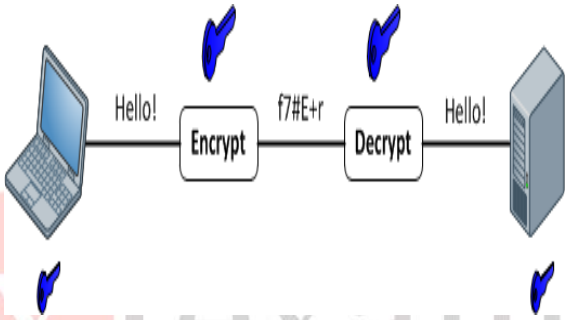
messages from the source to the destination. In Packet Switching, different messages (and even different packets) can pass through different routes, and when there is a "dead time" in the communication between the source and the destination, the lines can be used by other sources.

Circuit switching-:



A networking technology that provides a temporary, but dedicated, connection between two stations no matter how many switching devices the data are routed through. Circuit switching was originally developed for the analog-based telephone system in order to guarantee steady, consistent service for two people engaged in a phone conversation. Analog circuit switching Frequency Division Multiplexing **(FDM)** has given way to digital circuit switching Time Division Multiplexing **(TDM)**, and the digital counterpart still maintains the connection until broken.

Encryption and Decryption-:



Encryption is the process of translating plain text data **(plaintext)** into something that appears to be random and meaningless **(ciphertext).** Decryption is the process of converting **ciphertext** back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of **ciphertext,** the key that was used to encrypt the data must be used. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key. It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.

Private Key encryption -: Private Key encryption -Private Key means that each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to the other computer. Private key requires that you know which computers will talk to each other and install the key on each one. Private key encryption is essentially the same as a secret code that the two computers must each know in order to decode the information. The code would provide the key to decoding the message. Think of it like this. You create a coded message to send to a friend where each letter is substituted by the letter that is second from it. So "A" becomes "C" and "B" becomes "D". You have already told a trusted friend that the code is "Shift by 2". Your friend gets the message and decodes it. Anyone else who sees the message will only see nonsense.

Public key encryption -: Public key encryption uses a combination of a private key and a public key. The private key is known only to your computer while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key provided by the originating computer and its own private key.

Digital signature-:

A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it. Digital signatures rely on certain types

of encryption to ensure authentication. **Encryption** is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. **Authentication** is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures.

Unicasting, Multicasting and Broadcasting?

- If the message is sent from a source to a single destination node, it is called **Unicasting**.
- If the message is sent to some subset of other nodes, it is called **Multicasting**.
- If the message is sent to all the m nodes in the network it is called **Broadcasting**.

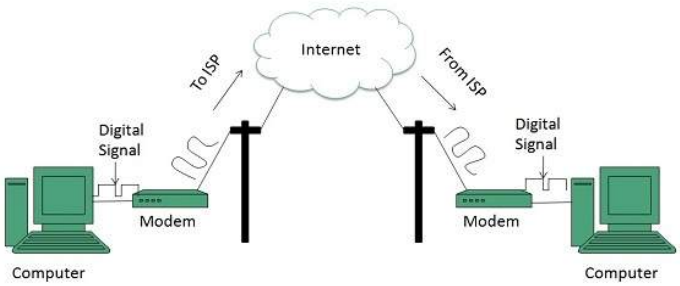
Connection Types : There exist several ways to connect to the internet. Following are these connection types available:

- Dial-up Connection
- ISDN
- DSL
- Cable TV Internet connections
- Satellite Internet connections
- Wireless Internet Connections

Dial-up Connection: **Dial-up** connection uses telephone line to connect PC to the internet. It requires a modem to setup dial-up connection. This modem works as an interface between PC and the telephone line. There is also a communication program that instructs the modem to make a call to specific number provided by an ISP. Dial-up connection uses either of the following protocols:

- Serial Line Internet Protocol (SLIP)
- Point to Point Protocol (PPP)

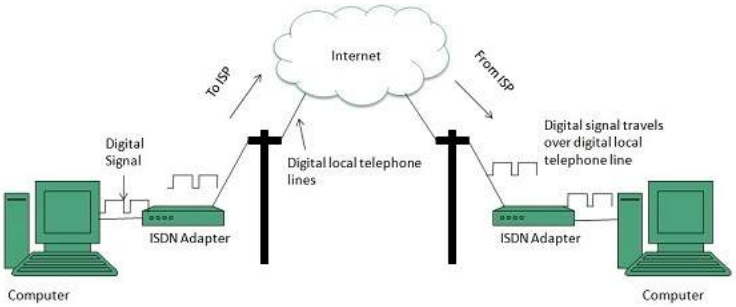
The following diagram shows the accessing internet using modem:



ISDN(Integrated Services Digital Network): **ISDN** is acronym of **Integrated Services Digital Network.** It establishes the connection using the phone lines which carry digital signals instead of analog signals. There are two techniques to deliver ISDN services:

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)

Key points:

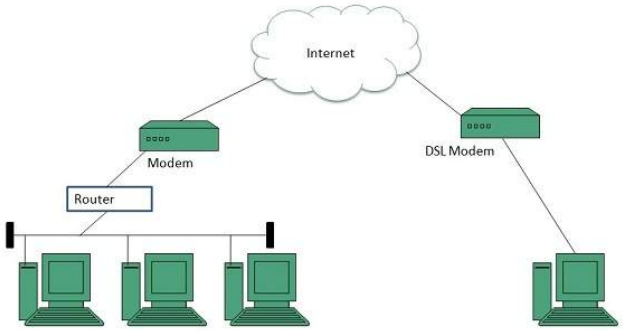


- The BRI ISDN consists of three distinct channels on a single ISDN line: t1o 64kbps B (Bearer) channel and one 16kbps D (Delta or Data) channels.
- The PRI ISDN consists of 23 B channels and one D channels with both have operating capacity of 64kbps individually making a total transmission rate of 1.54Mbps.

- The following diagram shows accessing internet using ISDN connection:

DSL(Digital Subscriber Line): **DSL** is acronym of **Digital Subscriber Line.** It is a form of broadband connection as it provides connection over ordinary telephone lines. Following are the several versions of DSL technique available today:

- Asymmetric DSL (ADSL)
- Symmetric DSL (SDSL)
- High bit-rate DSL (HDSL)
- Rate adaptive DSL (RDSL)
- Very high bit-rate DSL (VDSL)
- ISDN DSL (IDSL)



Internet Access Using DSL Modem

All of the above mentioned technologies differ in their upload and download speed, bit transfer rate and level of service. The following diagram shows that how we can connect to internet using DSL technology:

Wireless Internet Connection: Wireless Internet Connection makes use of radio frequency bands to connect to the internet and offers a very high speed. The wireless internet connection can be obtained by either WiFi or Bluetooth.

Key Points:

- Wi Fi wireless technology is based on IEEE 802.11 standards which allow the electronic device to connect to the internet.
- Bluetooth wireless technology makes use of short-wavelength radio waves and helps to create personal area network (PAN).