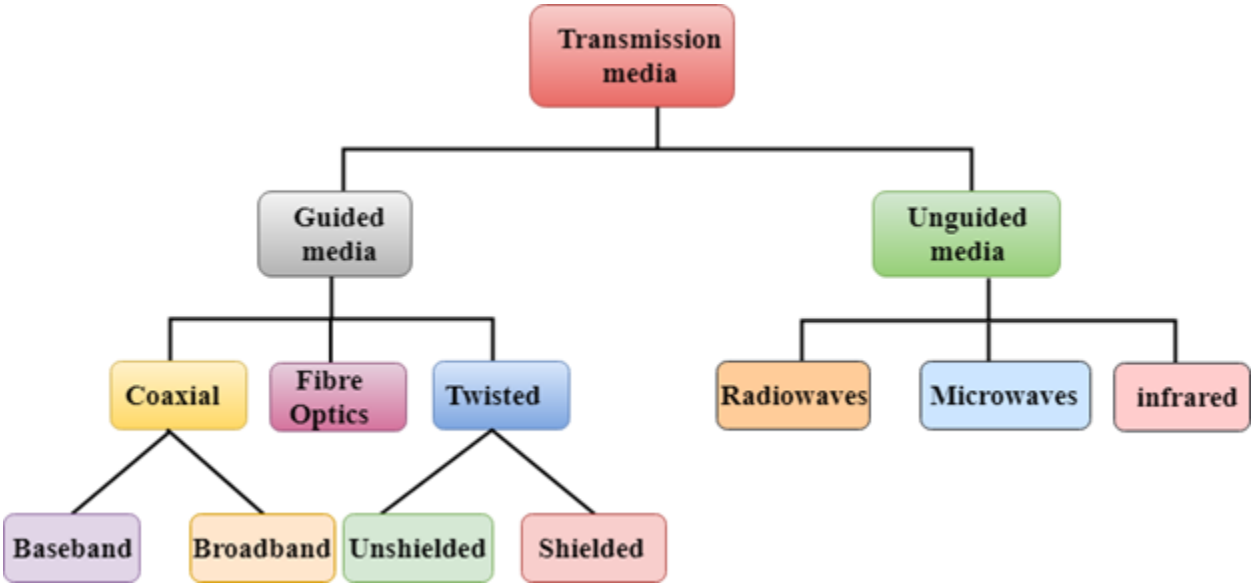
Unit - I
1. Introduction to computer network 13
3.1 What is Network? , Benefits of Networking
1.2 Wired Transmission media – Magnetic media, Twisted Pair, Coaxial Cable, Fiber Optics
1.3 Wireless Transmission media – The Electromagnetic Spectrum, Radio Transmission, Microwave Transmission, Infrared
1.4 Topologies with advantages & disadvantages:-Bus, Ring, Star, Tree, Mesh
1.5 Types of Networks – LAN, MAN, WAN

What is 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.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

- Classification Of Transmission Media:



- Guided Transmission Media
- UnGuided Transmission Media

Magnetic Media

Any storage medium that utilizes magnetic patterns to represent information is considered magnetic media

The term 'magnetic media' is used to describe any record format where analogue or digital information is recorded to and retrieved from a coated matrix that can be magnetised. Common types of magnetic media are: ... video and computer tapes on open reels or in cassettes. hard disk drives, (HDD) floppy disks

One of the most convenient way to transfer data from one computer to another, even before the birth of networking, was to save it on some storage media and transfer physical from one station to another.

Though it may seem old-fashion way in today's world of high speed internet, but when the size of data is huge, the magnetic media comes into play.

For example, a bank has to handle and transfer huge data of its customer, which stores a backup of it at some geographically far-away place for security reasons and to keep it from uncertain calamities. If the bank needs to store its huge backup data then its,transfer through internet is not feasible.The WAN links may not support such high speed.Even if they do; the cost too high to afford.

In these cases, data backup is stored onto magnetic tapes or magnetic discs, and then shifted physically at remote places

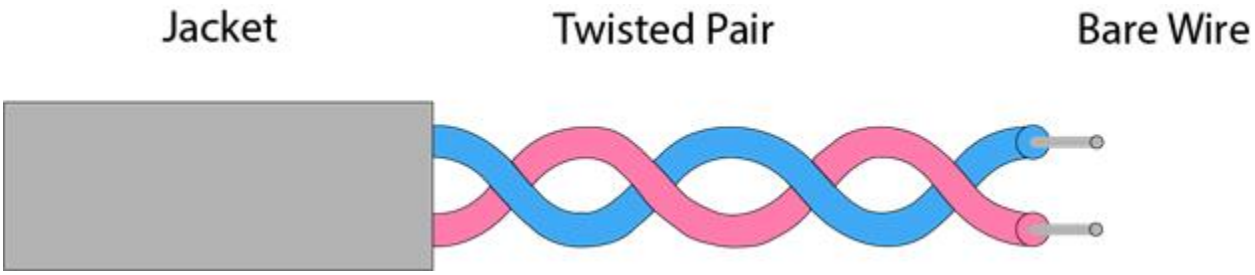
Twisted Pair Cable

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference. The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk. There are two types of twisted pair cables:

- Shielded Twisted Pair (STP) Cable
- Unshielded Twisted Pair (UTP) Cable

STP cables comes with twisted wire pair covered in metal foil. This makes it more indifferent to noise and crosstalk.

UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.



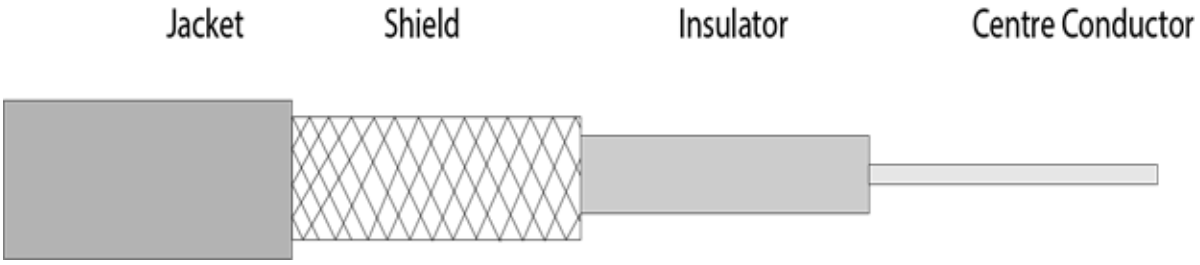
Coaxial Cable

Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor.The core is enclosed in an insulating sheath.The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath.This all is covered by plastic cover.

Because of its structure,the coax cable is capable of carrying high frequency signals than that of twisted pair cable.The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

There are three categories of coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG stands for Radio Government.

Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.



Coaxial cable is of two types:

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

Advantages Of Coaxial cable:

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

Disadvantages Of Coaxial cable:

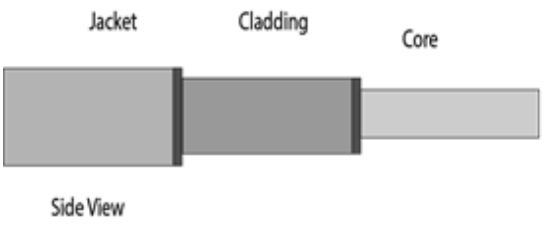
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

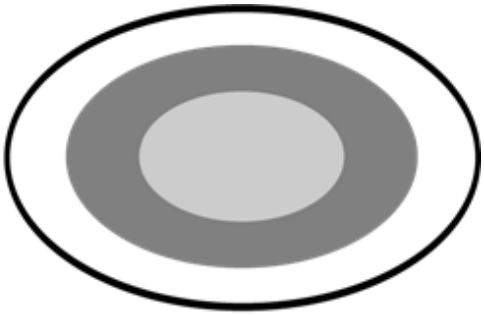
Fiber Optics

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.

Fiber Optic provides the highest mode of speed. It comes in two modes, one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.

Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.





Basic elements of Fibre optic cable:

- Core: The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- Cladding: The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- Jacket: The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

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

Wireless Transmission Media

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.

Electromagnetic spectrum

The electromagnetic spectrum is the range of frequencies (the spectrum) of electromagnetic radiation and their respective wavelengths and photon energies.

The range of wavelengths or frequencies over which electromagnetic radiation extends.

Electromagnetic spectrum, the entire distribution of electromagnetic radiation according to frequency or wavelength. Although all electromagnetic waves travel at the speed of light in a vacuum, they do so at a wide range of frequencies, wavelengths, and photon energies. The electromagnetic spectrum comprises the span of all electromagnetic radiation and consists of many sub ranges, commonly referred to as portions, such as visible light or ultraviolet radiation. The various portions bear different names based on differences in behavior in the emission, transmission, and absorption of the corresponding waves and also based on their different practical applications. There are no precise accepted boundaries between any of these contiguous portions, so the ranges tend to overlap.

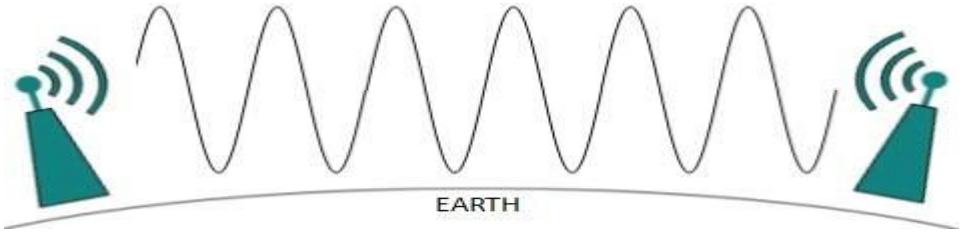
The entire electromagnetic spectrum, from the lowest to the highest frequency (longest to shortest wavelength), includes all radio waves (e.g.,
commercial radio and television, microwaves, radar), infrared radiation, visible light, ultraviolet radiation, X-rays, and gamma rays. Nearly all frequencies and wavelengths of electromagnetic radiation can be used for spectroscopy.

Radio Transmission

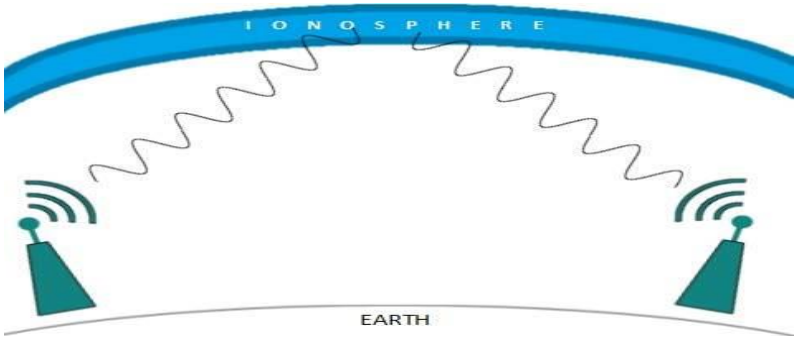
Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike. Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies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



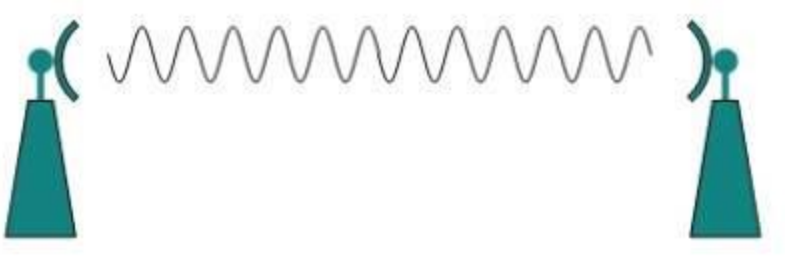
Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.



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 radiation (IR), or infrared light, is a type of radiant energy that's invisible to human eyes but that we can feel as heat. All objects in the universe emit some level of IR radiation, but two of the most obvious sources are the sun and fire.

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.

Advantages

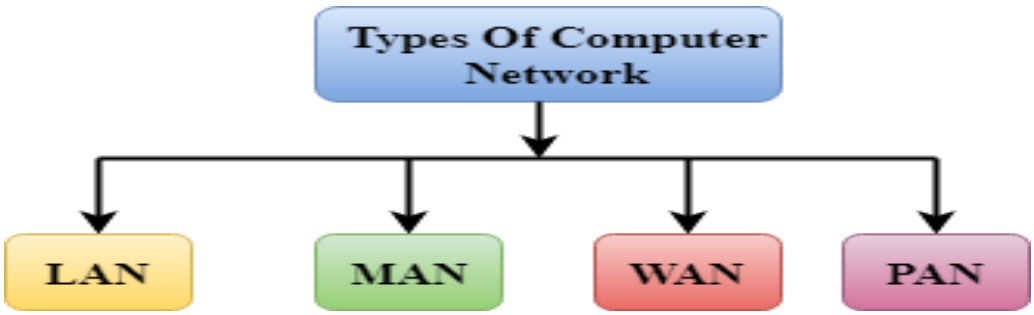
1) Infrared transmission requires minimum power to operate and can be set up at a low cost.
2) This is a secure way to transfer data between devices as the signal cannot pass beyond a room or chamber.

Disadvantages

1) The speed of data transfer in infrared is slow.
2) Infrared can be used for a small range distance.

Types of network

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.



LAN (Local Area Network)

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.

Key Point:-

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

Advantages of LAN

1. **Resource Sharing:** LAN provides resource sharing such as computer resources like printers, scanners, modems, DVD-ROM drives, and hard disks can be shared within the connected devices. This reduces cost and hardware purchases.

2. **Software Applications Sharing:** In a Local Area Network, it is easy to use the same software in a number of computers connected to a network instead of purchasing the separately licensed software for each client a network.
3. **Easy and Cheap Communication:** Data and messages can easily be shared with the other computer connected to the network.
4. **Centralized Data:** The data of all network users can be stored on a hard disk of the central/server computer. These help users to use any computer in a network to access the required data.
5. **Data Security:** Since data is stored on the server computer, it will be easy to manage data at only one place and the data will be more secure too.
6. **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In school labs and internet Cafes, single internet connection is used to provide internet to all connected computers.

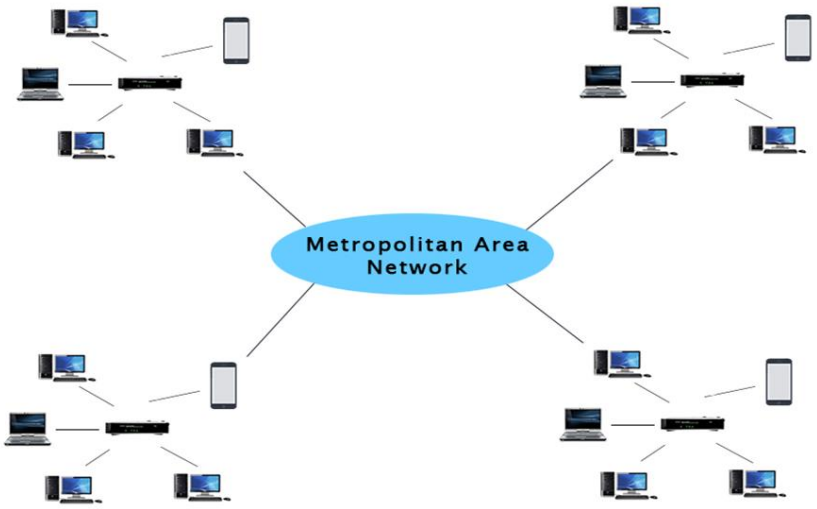
Disadvantages of LAN

1. **High Setup Cost:** The initial setup costs of installing Local Area Networks is high because there is special software required to make a server. Also, communication devices like an Ethernet cable, switches, hubs, routers, cables are costly.
2. **Privacy Violations:** The LAN administrator can see and check personal data files of each and every LAN user. Moreover, he can view the computer and internet history of the LAN user.
3. **Data Security Threat:** Unauthorized users can access important data of an office or campus if a server hard disk is not properly secured by the LAN administrator.
4. **LAN Maintenance Job:** *Local Area Network requires a LAN Administrator* because there are problems such as software installations, program faults or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is required to maintain these issues.
5. **Covers Limited Area**: LANs are restricted in size they cover a small area like a single office, single building or a group of nearby buildings.

MAN

A metropolitan area network (MAN) is smaller than a wide area network (WAN) but larger than a local area network (LAN).

A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN).



- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

Advantages of a MAN Network

1: Less Expensive:
It is less expensive to attach MAN with WAN Network. MAN gives you good efficiency of data. All data on MAN is easily manageable in a centralized way.
2: Sending Local Emails:
You can send local emails fast and free on MAN.
3: High Speed than WAN:
The speed of data can easily reach 1000 Mbps, as MAN uses fiber optics. Files and database transfer rates are fast.
4: Sharing of the Internet:
With the installation of MANs, users can share their internet connection. In this way, multiple users can get the same high-speed internet.
5: Conversion of LAN to MAN is Easy:
MAN is a combination of two or more LAN network. So it is a faster way to connect two LAN networks together. It is possible by the fast configuration of links.
6: High Security:
MAN's has a high-security level than WAN.

Disadvantages of MAN Network

1: Difficult To Manage:
It is very difficult to manage if the size and number of LANs network increase. This is due to security and extra configuration problems.

2: Internet Speed Difference:
As it cannot work on phone copper wires. Copper wires affect the speed of MAN.So high cost is needed for fiber optics.

3: Hackers Attack:
In this network, there is a high risk of attacking hackers as compared to LAN. So data may be a leak. Highly security staff is the need in MAN.

4: Technical Staff Requires to Set up:
Highly technical people require to setup MAN. The technical people are network administrators and troubleshooters.

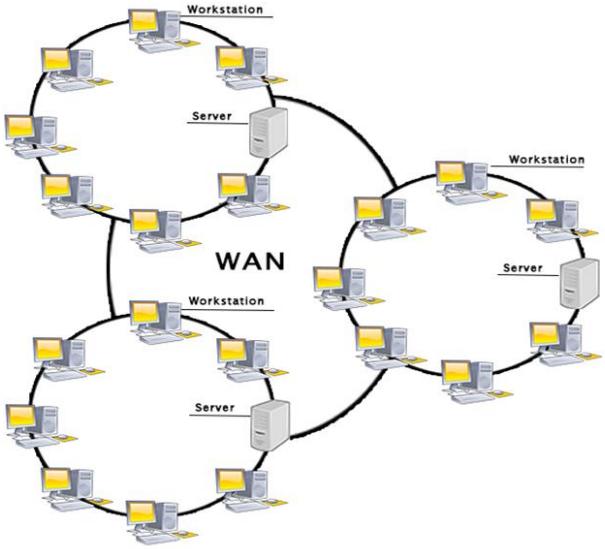
5: Need more wires:
In MAN more than LAN network, cables require. As you know, it is a combination of two LANs.

WAN

A wide-area network (WAN) is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet the world's largest WAN.

Today, there are several types of WANs, built for a variety of use cases that touch virtually every aspect of modern life.

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, and Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

3. Reference Model and Ethernet
4.

2.1 The need for layered architecture (protocol hierarchies)
2.2 OSI reference Model
2.3 TCP/IP reference Model
2.4 Ethernet Technology - Types of Ethernet, properties of Ethernet, Collision detection and Recovery, Ethernet hardware address, Ethernet Frame Format
2.5 Wireless LAN

2.6 Bluetooth

A protocol is a set of rules and conventions agreed upon and followed by the communicating entities for data communication. A protocol outlines the what, how and when of a communication.

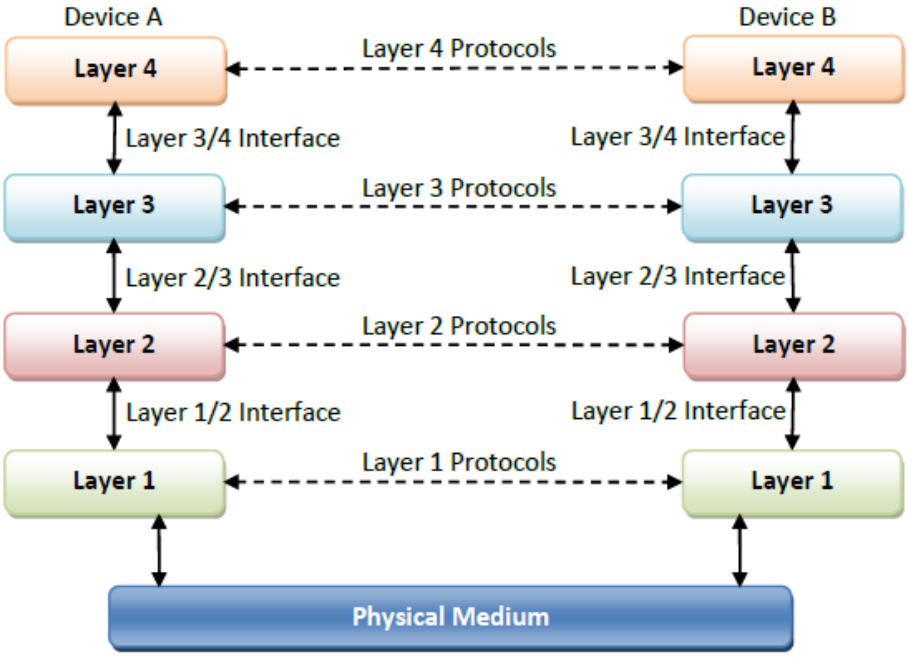
The three aspects of a protocol are −

- Syntax − It defines the format of data that is to be sent or received.
- Semantics − It defines the meaning of each section of bits that are transferred.
- Timings − It defines the time at which data is transferred as well as the speed at which it is transferred.

Protocol Hierarchies

Most networks are organized as a stack of layers, one on the top of another. The number of layers and their names vary from network to network. Each layer has a specified function and adheres to specified protocols. Thus we obtain a stack of protocols.

The following figure illustrates a four-layer network −



The above figure represents communication between Device A and Device B. The data stream from one device to the other is not sent directly but has to pass through a number of layers. The layers in the same levels are called peers and have a set of protocols for communication. Between each adjacent layer is an interface that defines the services that are being offered by a lower layer to the next higher layer. The dotted arrows depict virtual communication between peer layers, while the solid arrows represent the physical communications between the adjacent layers.

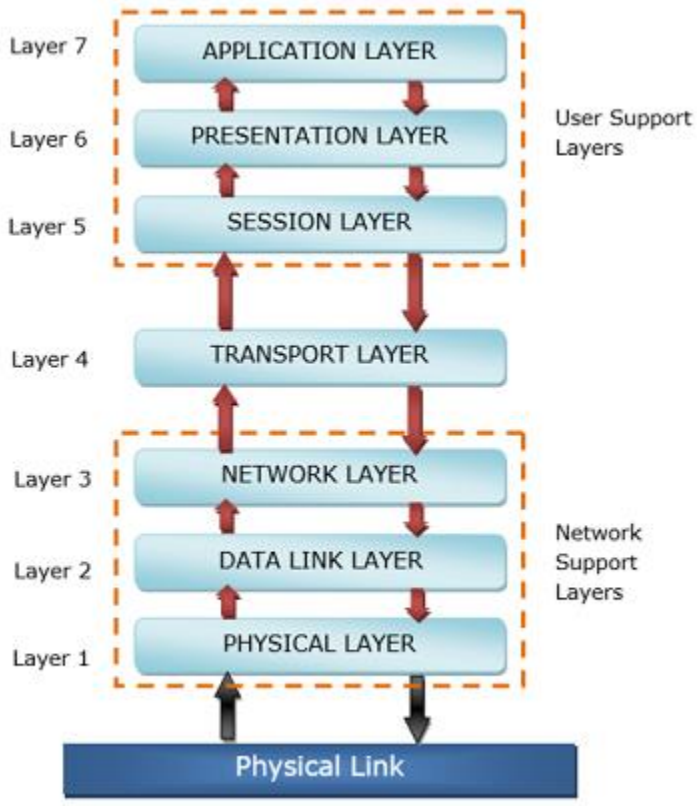
Let us consider a situation where Device A wants to send a message to Device B. Device A passes its information to the highest layer. As soon as a data stream reaches a layer, it performs some specified functions on it and passes it to the layer below. This continues until the data stream reaches the lowest layer. Layer 1 passes a bit stream of 0s and 1s to the physical medium that communicates it to the Layer 1 of the receiving end. Each layer in the receiving end performs certain functions on the data stream adhering to the protocol with its peer and passes it to the layer above

- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.

- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

2.2 OSI reference Model

OSI or Open System Interconnection model was developed by International Standards Organization (ISO). It gives a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. It has seven interconnected layers.



The physical layer, data link layer and the network layer are the network support layers. The layers manage a physical transfer of data from one device to another. Session layer, presentation layer, and application layer are the user support layers. These layers allow

communication among unrelated software in dissimilar environments. Transport layer links the two groups.

The main functions of each of the layers are as follows −

- Physical Layer − its function is to transmit individual bits from one node to another over a physical medium.
- Data Link Layer − It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
- Network Layer − It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.
- Transport Layer −It is responsible for delivery of the entire message from the source host to destination host.
- Session Layer − It establishes sessions between users and offers services like dialog control and synchronization.
- Presentation Layer − It monitors syntax and semantics of transmitted information through translation, compression, and encryption.
- Application Layer − It provides high-level APIs (application program interface) to the users.

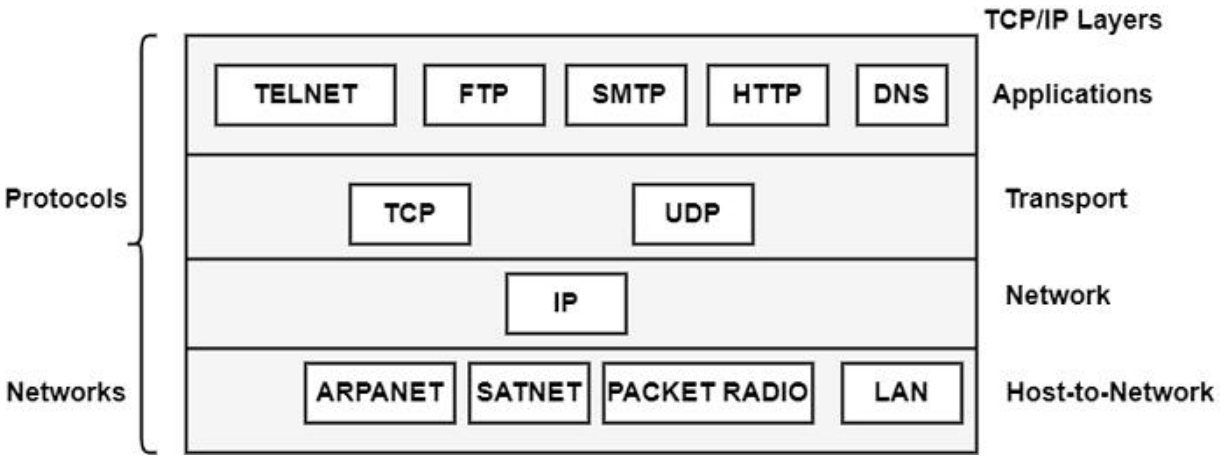
2.3 TCP/IP reference Model

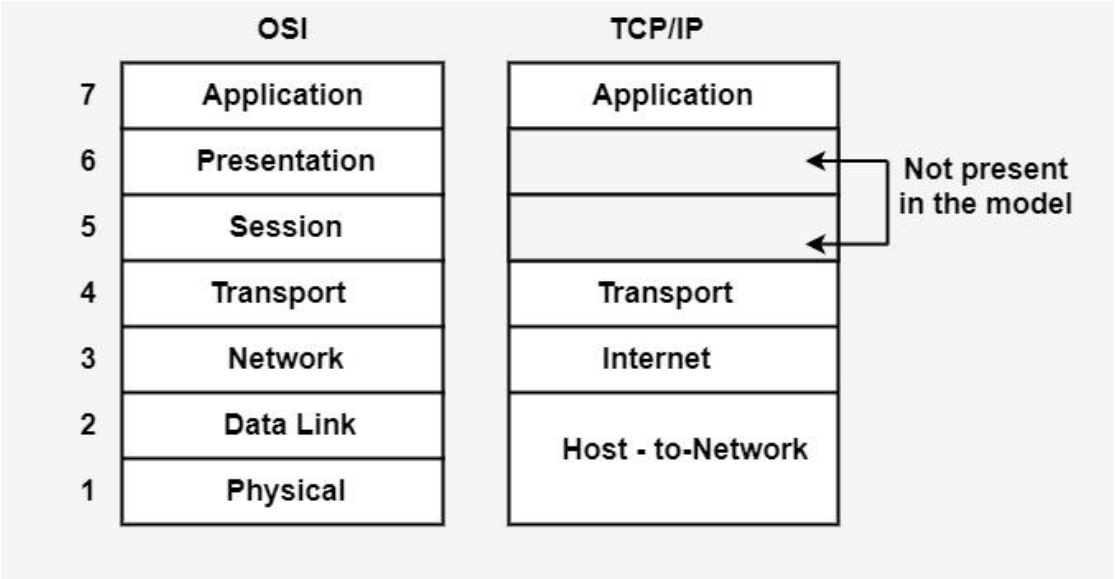
TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- Host-to- Network Layer −It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- Internet Layer −It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- Transport Layer − It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Application Layer − this is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.





Host to Network Layer

This is the lowest layer in the TCP/IP reference model. The layer functioning is usually different in various relations. The main function of this layer is to instruct the upper layer when the host is linked to the network so that they can establish sending the data packets.

Internet Layer

The functioning of the TCP/IP model's internet layer is similar to the OSI model's network layer's functioning. This layer's function is to enable the host to add packets into any relation and then create them transit separately to the target.

Transport Layer

The transport layer is placed above the internet layer of the TCP model. This layer functioning is equal to the functioning of the transport layer in the OSI model. In the transport layer, the byte flow is split into communication, and these communications are developed to the internet layer. It can support the functions like segmentation and disintegration of messages. This protocol is used in this layer are TCP and UDP.

TCP

TCP represents Transmission control protocol. It is a dependable connection-oriented protocol. It enables a byte flow broadcasted from one system to be delivered to another system without learning some bug. It can also manage flow control.

UDP

An uncertain, connectionless protocol used for applications that do not need the TCPs series or flow control. It can be used in sending speech or video.

Application Layer

This is the highest layer of the TCP/IP layer. The application program's layer view is a user-oriented layer that helps services provide the network's end-user precisely. A message or information to be transmitted across the network introduce the TCP/IP model and then carry down into the communication line up to host to the network layer of destination and then upwards up to the receiver end framework application layer.

This layer uses various protocols to transfer the data between applications. Some standard protocols used in this layer are −

FTP (File Transfer Protocol)

It is used for file transmission between internetwork nodes.

SMTP (Simple Mail Transfer Protocol)

It can be used for exchanging email.

TELNET

TELNET represents Terminal Network. It allows the client to create host-based software by initiating one of the host terminals. It also supports connectivity between the diverse operating framework.

DNS (Domain Name Systems)

The DNS can change the domain name into IP addresses. The TCP/IP protocol needs the IP address that recognizes linking a host to the computer network.

HTTP (Hypertext Transfer Protocol)

HTTP is an internet protocol created for particular software, the World Wide Web (WWW).

2.5 Wireless LAN

(wireless Local Area Network) A communications network that provides connectivity to wireless devices within a limited geographic area.

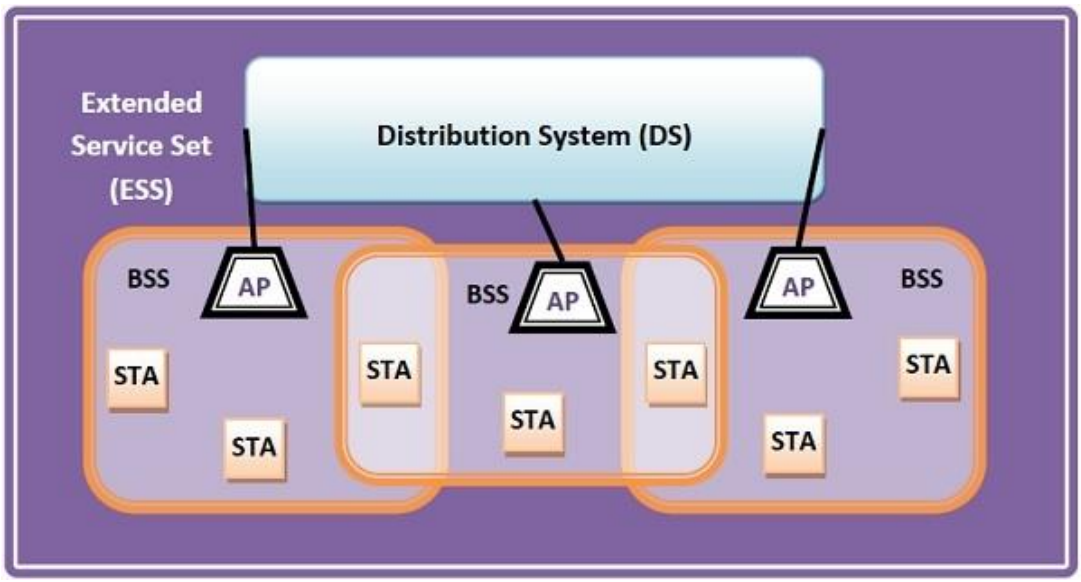
A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. This gives users the ability to move around within the area and remain connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.

Most WLANs are based upon the standard IEEE 802.11 standard or WiFi.

Components of WLANs

The components of WLAN architecture as laid down in IEEE 802.11 are −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types −
    - Wireless Access Point (WAP or AP)
    - Client
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories −
    - Infrastructure BSS
    - Independent BSS
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.



Types of WLANS

WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.

- **Infrastructure Mode** – Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** – Clients transmit frames directly to each other in a peer-to-peer fashion.

Advantages of WLANs

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user,

adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

- **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

- They provide clutter-free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at greater ease than wired LANs.
- The system is portable within the network coverage. Access to the network is not bounded by the length of the cables.
- Installation and setup are much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
- **Proprietary Solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.
- **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
- **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
- **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
- **License free operation:** LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.

- **Robust transmission technology:** If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

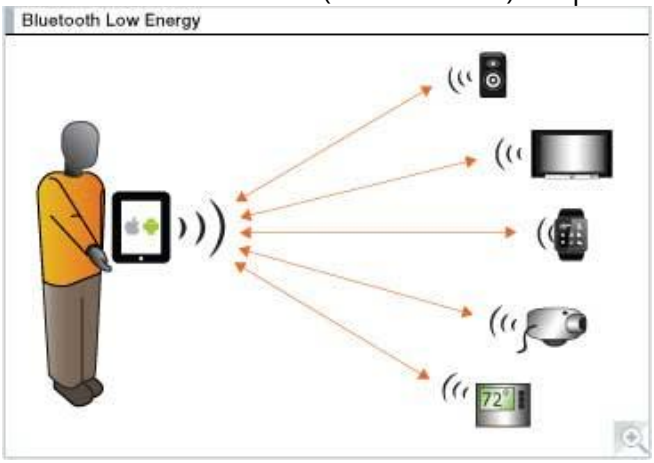
- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

Bluetooth

Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz, and building personal area networks (PANs).

Bluetooth is a wireless technology that allows the exchange of data between different devices.

While Bluetooth uses wavelength to transmit information, it generally only works within a short distance for the devices to stay connected. In the simplest terms, Bluetooth is the technology that enables exchange of data between devices within a short amount of distance. Most Bluetooth devices have a **maximum connectivity range of about 30 feet**, and that distance is reduced when obstacles (such as a wall) are present.



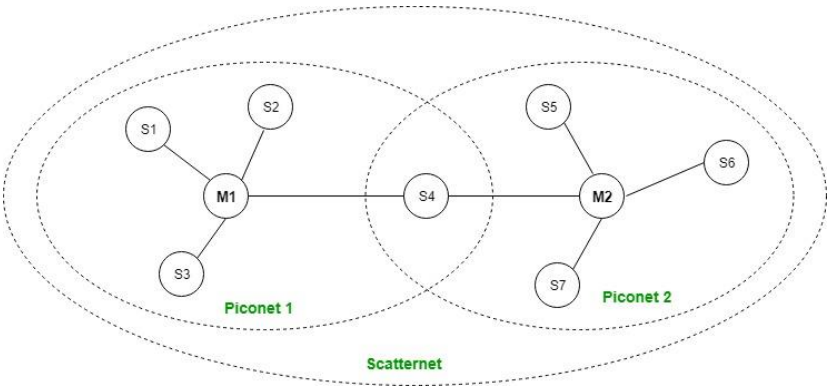
Piconet

A collection of devices connected via Bluetooth technology in an ad hoc fashion. A piconet starts with two connected devices, such as a PC and cellular phone, and may grow to eight connected devices. All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a master for synchronization purposes, and the other(s) as slave(s) for the duration of the piconet connection.

A piconet is an ad hoc network that links a wireless user group of devices using Bluetooth technology protocols. A piconet consists of two or more devices occupying the same physical channel (synchronized to a common clock and hopping sequence). It allows one master device to interconnect with up to seven active slave devices. Up to 255 further slave devices can be inactive, or parked, which the master device can bring into active status at any time, but an active station must go into parked first.

Some examples of piconets include a cell phone connected to a computer, a laptop and a Bluetooth-enabled digital camera, or several PDAs that are connected to each other.

A group of devices are connected via Bluetooth technology in an ad hoc fashion. A piconet starts with two connected devices, and may grow to eight connected devices. Bluetooth communication always designates one of the Bluetooth devices as a main controlling unit or master unit.



Scatternet:

It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.

Advantages

- It avoids interference from other wireless devices.
- It has lower power consumption.
- It is easily upgradeable.
- It has range better than Infrared communication.
- The Bluetooth is used for voice and data transfer.
- Bluetooth devices are available at very cheap cost.
- No line of sight hence can connect through any obstacles.
- Free to use if the device is installed with Bluetooth.
- The technology is adopted in many products such as head set, in car system, printer, web cam, GPS system, keyboard and mouse.

Disadvantages

- It can lose connection in certain conditions.
- It has low bandwidth as compared to Wi-Fi.
- It allows only short range communication between devices.
- Security is a very key aspect as it +can be hacked.

2.4 Ethernet Technology - Types of Ethernet, properties of Ethernet, Collision detection and Recovery, Ethernet hardware address, Ethernet Frame Format

What is Ethernet?

A system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems.

Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).

It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3. Ethernet has since been refined to support higher bit rates, a greater number of nodes, and longer link distances, but retains much backward compatibility. Over time, Ethernet has largely replaced competing wired LAN technologies such as Token Ring, FDDI and ARCNET.

Ethernet network is used to create local area network and connect multiple computers or other devices such as printers, scanners, and so on. In a wired network, this is done with the help of fiber optic cables, while in a wireless network, it is done through wireless network technology. An Ethernet network uses various topologies such as star, bus, ring, and more.

Types of Ethernet Networks?

Fiber optic media converters connect an Ethernet device with CAT5/CAT6 copper cables to a fiber optic cable. An Ethernet network usually is active in a 10-km periphery. This extension to fiber optic cable significantly increases the distance covered by the network. Here are some types of Ethernet networks:

- **Fast Ethernet**: As the term suggests, this is quite a high-speed internet, and can transmit or receive data at about 100 Mbps. This type of network is usually supported by a twisted pair or CAT5 cable. If a laptop, camera, or any other device is connected to a network, they operate at 10/100Base Ethernet and 100Base on the fiber side of the link.
- **Gigabit Ethernet**: This type of network transfers data at an even higher speed of about 1000 Mbps or 1Gbps. Gigabit speed is an upgrade from Fast Ethernet which is slowly being phased out. In this type of network, all the four pairs in the twisted pair cable contribute to the data transfer speed. This network type finds a large application in video calling systems which use CAT5e or other advanced cables. For extended networks, the distance of up to 500m, 1000Base SX fiber cables may be used for multimode, as well as 1000Base LX for single mode systems. VERSITRON manufactures Gigabit Ethernet Media Converters that can handle 10/100/1000Base speeds on the Ethernet side and 1000Base Gigabit speed on the fiber side by using Fiber SFP modules.
- **10-Gigabit Ethernet**: This is an even more advanced and high speed network type with a data transfer rate of 10 Gigabit/second. It is supported by CAT6a or CAT7 twisted pair cables, as well as fiber optic cables. By using a fiber optic cable, this network area can be extended up to around 10,000 meters.
- **Switch Ethernet**: This type of network requires a switch or hub. Also, instead of a twisted pair cable, a normal network cable is used in this case. Network switches are used for data transfer from one device to the other, without interrupting any other devices in the network.

What Are the Various Types of Ethernet Cables?

Ethernet may be either a wired or wireless network. In a wired network, various types of cables are used. Here are some widely used Ethernet cables:

- **10Base2**: This is a thin twisted pair coaxial cable.
- **10Base5**: This is thick twisted pair coaxial cables.
- **10Base T**: This is a twisted pair cable which offers a speed of around 10 Mbps.
- **100BaseTX**: This is a twisted pair cable and offers a speed of 100 Mbps.
- **100Base FX**: Fiber optic protocol which offers a speed of 100 Mbps.
- **1000Base SX**: Fiber optic protocol which utilizes a wavelength of 850nm for multimode networks.
- **1000Base LX**: Fiber optic protocol which utilizes a wavelength of 1310 nm, for multimode networks and up to 1550nm for single mode networks.

The Ethernet properties are:

1. Protocol simplicity
2. Relative low cost and elegant implementation of LAN system.
3. High flexibility due to the bus topology and the cable tapping facility resulting in easy addition or removal of devices and systems.
4. High reliability which assures the continuation of the operation of the network even if one or more workstation fail.
5. Uses decentralized access control.
6. Ethernet is a broadcast network.
7. Ethernet provides best effort delivery. It does not provide any information to the source of the frame sent by it has successfully reached the destination.

Collision detection and Recovery

In Ethernet world, the result of two nodes transmitting in the same time. The frames from each machine impact and collide when they meet on the physical media.This contention-based methods allow any device to try to access the medium whenever it has data to send. To prevent complete "choking" on the media, these methods use a Carrier Sense Multiple Access (CSMA) process to first detect if the media is transmitting any signal in that moment. If there is a signal on the media from another computer, it means that another device is talking. When the device attempting to transmit sees that the media is in use, it will wait and try again after a short period of time. If no carrier signal is detected, the device transmits its data. Ethernet and wireless networks use contention-based media access control.

It is possible that the CSMA process will fail and two devices will transmit at the same time. This is called a data collision. If this occurs, the data sent by both devices will be corrupted and will need to be resent. As the number of nodes increases on a shared media, the probability of successful media access without a collision decreases. Additionally, The recovery mechanisms required to correct errors due to these collisions further diminishes the overall throughput.

- CSMA/CD Protocol
  It is used when more that two computers are sharing the same medium tipicaly something that is happening in LAN networks when computers are connected trough hub. CSMA/CD is a practice used for multiple access control protocols. Transmission will be taken place by a particular station at a time but when more than one station will transmit at the same time as a result collision can be occurred. In that moment

- CSMA/CA Protocol
  CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) that has been introduced to get better the CSMA performance. According to that a station will sense the transmission medium before sending the frame. CASMA/CA protocol is used in wireless (802.11) LANs. Moreover, when a station sense collision in case of CSMA/CA, it first waits for some time after that but before packets transmission, it will listen to the channel for its idleness, if so packets transmission will start otherwise it will waits for the medium to become unoccupied.

The two main portions in the process of collision detection are:

- Detecting that whether a collision is occurred or not
- And if yes, then responding to that collision
-

Ethernet hardware address

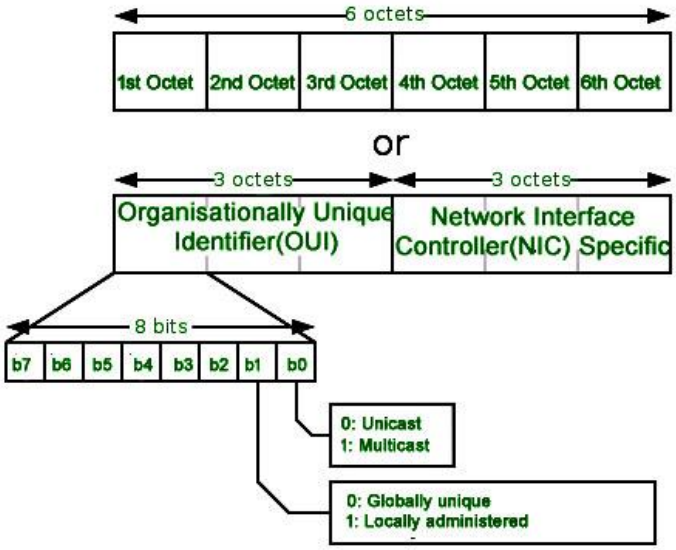
In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer. In this article, we will discuss about addressing in DLL, which is MAC Address.

Media Access Control (MAC) Address –

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is worldwide unique, since millions of network devices exists and we need to uniquely identify each.



Format of MAC Address –

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique Identifier**). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

Here are some OUI of well known manufacturers :

CC:46:D6 - Cisco

3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard

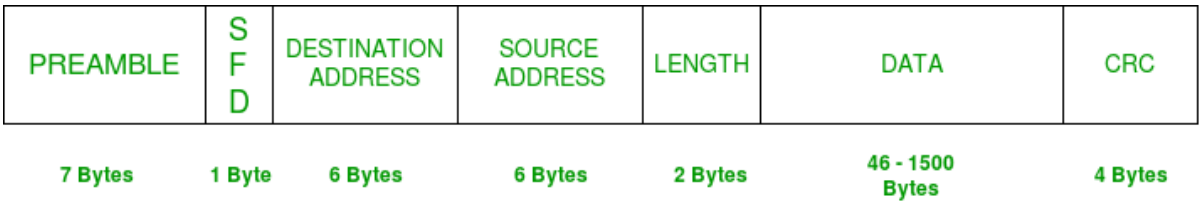
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

The rightmost six digits represents **Network Interface Controller**, which is assigned by manufacturer.

Ethernet Frame Format

Basic frame format which is required for all MAC implementation is defined in IEEE 802.3 standard. Though several optional formats are being used to extend the protocol's basic capability. Ethernet frame starts with Preamble and SFD, both works at the physical layer. Ethernet header contains both Source and Destination MAC address, after which the payload of the frame is present. The last field is CRC which is used to detect the error. Now, let's study each field of basic frame format.

Ethernet (IEEE 802.3) Frame Format –



IEEE 802.3 ETHERNET Frame Format

- PREAMBLE – Ethernet frame starts with 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays. But today's high-speed Ethernet don't need Preamble to protect the frame bits. PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
- Start of frame delimiter (SFD) – This is a 1-Byte field which is always set to 10101011. SFD indicates that upcoming bits are starting of the frame, which is the destination address. Sometimes SFD is considered the part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
- Destination Address – This is 6-Byte field which contains the MAC address of machine for which data is destined.

- Source Address – This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.

- Length – Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.
- Data – This is the place where actual data is inserted, also known as Payload. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.
- Cyclic Redundancy Check (CRC) – CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

Unit - III

3. Internet Basics and Networking Protocol 13

3.1 Internet- Architecture, Internet Service Providers (ISP), Internet Addressing System: IP Address, DNS, URL
3.2 Concept of Intranet & Extranet
3.3 Networking protocol: IP,TCP,FTP,HTTP,DHCP

Internet- Architecture

The Internet today is made up of thousands of overlapping hierarchical networks.Because of this, it is not practical to attempt a detailed description of the exact architecture or topology of the Internet. However, an overview of the common, generalcharacteristics can be made.

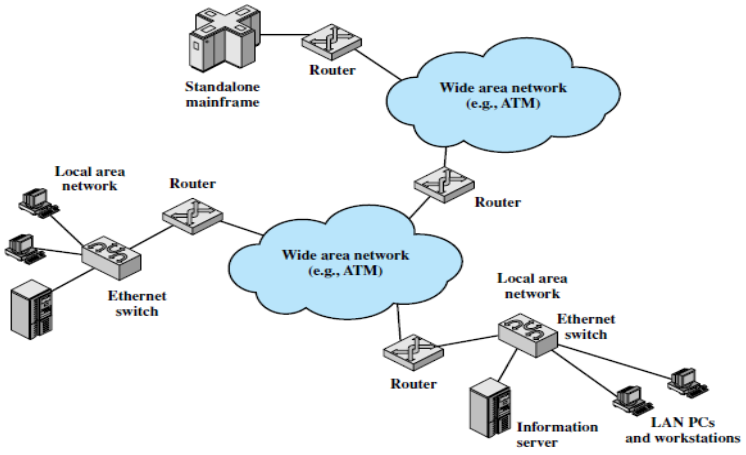


Figure 1.4 Key Elements of the Internet

A key element of the Internet is the set of hosts attached to it. Simply put, ahost is a computer.Today, computers come in many forms, including mobile phonesand even cars. All of these forms can be hosts on the Internet. Hosts are sometimesgrouped together in a LAN.This is the typical configuration in a corporate environment.

Individual hosts and LANs are connected to an Internet service provider(ISP) through a point of presence (POP).The connection is made in a series of stepsstarting with the customer premises equipment (CPE).The CPE is the communicationsequipment located onsite with the host.For many home users, the CPE is a 56-kbps modem.This is perfectly adequatefor e-mail and related services but marginal for graphics-intensive Web surfing.

Newer CPE offerings provide greater capacity and guaranteed service in somecases. A sample of these new access technologies includes DSL, cable modem, andsatellite. Users who connect to the Internet through their work often use workstationsor PCs connected to their employer-owned LANs, which in turn connectthrough shared organizational trunks to an ISP. In these cases the shared circuit isoften a T-1 connection (1.544 Mbps), while for very large organizations T-3 connections(44.736 Mbps) are sometimes found. Alternatively, an organization's LAN.

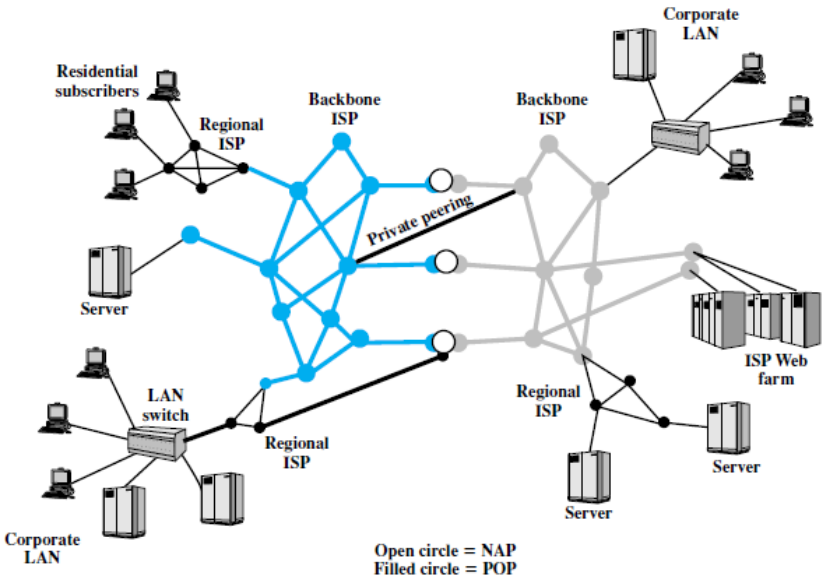


Figure 1.5 Simplified View of Portion of Internet

may be hooked to a wide area network (WAN), such as a frame relay network,
which in turn connects to an ISP.The CPE is physically attached to the "local loop" or "last mile."This is the infrastructurebetween a provider's installation and the site where the host is located. Forexample, a home user with a 56K modem attaches the modem to the telephone line.The telephone line is typically a pair of copper wires that runs from the house to acentral office (CO) owned and operated by the telephone company. In this instancethe local loop is the pair of copper wires running between the home and the CO. If thehome user has a cable modem, the local loop is the coaxial cable that runs fromthe home to the cable company facilities.The preceding examples are a bit of an oversimplification,but they suffice for this discussion. In many cases the wires that leave ahome are aggregated with wires from other

homes and then converted to a differentmedia such as fiber. In these cases the term local loop still refers to the path from thehome to the CO or cable facility.The local loop provider is not necessarily the ISP. Inmany cases the local loop provider is the telephone company and the ISP is a large,national service organization. Often, however, the local loop provider is also the ISP. The ISP provides access to its larger network through a POP. A POP is simplya facility where customers can connect to the ISP network.The facility is sometimesowned by the ISP, but often the ISP leases space from the local loop carrier.A POP can be as simple as a bank of modems and an access server installed in a rack at theCO. The POPs are usually spread out over the geographic area where the provider offers service. The ISP acts as a gateway to the Internet, providing many importantservices. For most home users, the ISP provides the unique numeric IP addressneeded to communicate with other Internet hosts. Most ISPs also provide name resolutionand other essential network services.

ISP
(Internet Service Providers)
that provide Internet access to homes and businesses, data centers andcolocation facilities full of server machines, and regional (mid-level) networks.The data centers serve much of the content that is sent over the Internet. Attached to the regional networks are more ISPs, LANs at many universities and companies,and other edge networks.

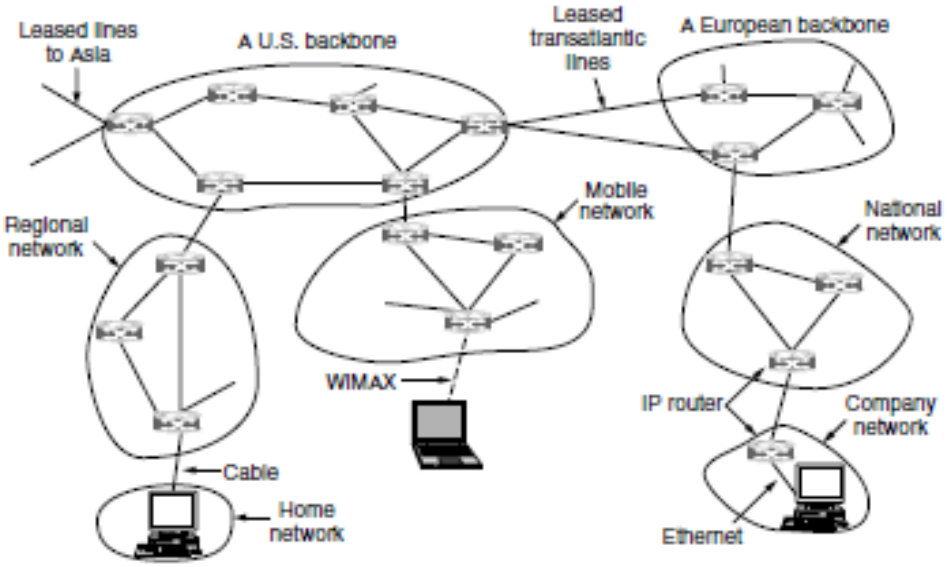
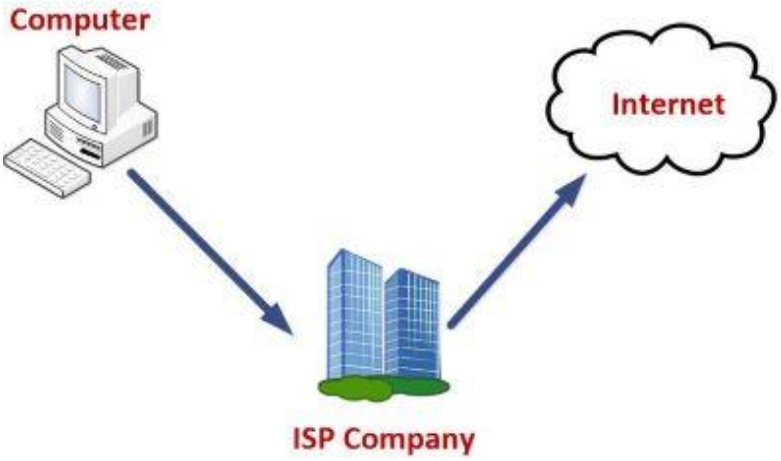


Figure 5-45. The Internet is an interconnected collection of many networks.

ISP stands for Internet Service Provider. It is a company that provides access to the internet and similar services such as Website designing and virtual hosting. For example, when you connect to the Internet, the connection between your Internet-enabled device and the internet is executed through a specific transmission technology that involves the transfer of information packets through an Internet Protocol route.



Data is transmitted through different technologies, including cable modem, dial-up, DSL, high speed interconnects. Accordingly, based on the method of data transmission, the Internet access provided by ISPs can be divided into many types, some of which are as follows:

Dial-up Internet access: It is the oldest technology to provide Internet access by modem to modem connection using telephone lines. In this method, the user's computer is connected to a modem with a telephone line. This method has become outdated today due to slow connection speed. However, in remote areas, this method can be used where the broadband network is not available.

DSL: DSL, which stands for 'digital subscriber line' is an advanced version of the dial-up Internet access method. It uses high frequency to execute a connection over the telephone network and allows the internet and the phone connection to run on the same telephone line. This method offers an Asymmetric Digital Subscriber (ADSL), where the upload speed is less than the download speed, and a Symmetric Digital Subscriber Line (SDSL), which offers equal upload and download speeds. Out of these two, ADSL is more popular among users and is popularly known as DSL.

Wireless Broadband (WiBB): It is a modern broadband technology for Internet access. It allows high-speed wireless internet within a large area. To use this technology, you are required to place a dish on the top of your house and point it to the transmitter of your Wireless Internet Service Provider (WISP).

Wi-Fi Internet: It is the short form for "wireless fidelity," which is a wireless networking technology that provides wireless high-speed Internet connections using radio waves. To use the internet, you are required to be within the range of wi-fi network. It is commonly used in public places such as hotels, airports, restaurants to provide internet access to customers.

ISDN: It is a short form of Integrated Services Digital Network. It is a telephone system network which integrates a high-quality digital transmission of voice and data over the same standard

phone line. It offers a fast upstream and downstream Internet connection speed and allows both voice calls and data transfer.

Ethernet: It is a wired LAN (Local Area Network) where computers are connected within a primary physical space. It enables devices to communicate with each other via a protocol (a set of rules or common network language). It may provide different speeds such as 10 Mbps, 100 Mbps and 10 Gbps.

Internet Addressing System: IP Address, DNS, URL

Internet addresses are made up of a network address and a host (or local) address. This two-part address allows a sender to specify the network as well as a specific host on the network. A unique, official network address is assigned to each network when it connects to other Internet networks.

TCP/IP includes an Internet addressing scheme that allows users and applications to identify a specific network or host with which to communicate.

An Internet address works like a postal address, allowing data to be routed to the chosen destination. **TCP/IP** provides standards for assigning addresses to networks, subnetworks, hosts, and sockets, and for using special addresses for broadcasts and local loopback.

Internet addresses are made up of a network address and a host (or local) address. This two-part address allows a sender to specify the network as well as a specific host on the network. A unique, official network address is assigned to each network when it connects to other Internet networks. However, if a local network is not going to connect to other Internet networks, it can be assigned any network address that is convenient for local use.

The Internet addressing scheme consists of Internet Protocol (IP) addresses and two special cases of IP addresses: broadcast addresses and loopback addresses.

- Internet addresses
  The Internet Protocol (IP) uses a 32-bit, two-part address field.
- Subnet addresses
  Subnet addressing allows an autonomous system made up of multiple networks to share the same Internet address.
- Broadcast addresses
  The TCP/IP can send data to all hosts on a local network or to all hosts on all directly connected networks. Such transmissions are called *broadcast messages*.
- Local loopback addresses
  The Internet Protocol defines the special network address, 127.0.0.1, as a local loopback address.

IP Address

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

An Internet Protocol address (IP address) is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was standardized in 1998. IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites.

IP addresses provide a way of doing so and form an essential part of how the internet works.

An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

Types of IP addresses

There are different categories of IP addresses, and within each category, different types.

Consumer IP addresses

Every individual or business with an internet service plan will have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.

Private IP addresses

Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network.

Public IP addresses

A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

Public IP addresses

Public IP addresses come in two forms – dynamic and static.

Dynamic IP addresses

Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP addresses means they don't have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.

Static IP addresses

In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web.

DNS

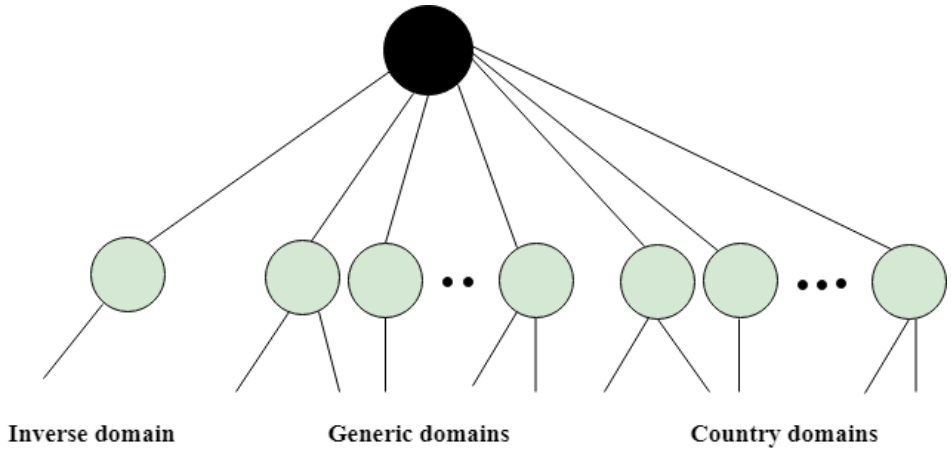
The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

The Domain Name System (DNS) is the hierarchical and decentralized naming system used to identify computers, services, and other resources reachable through the internet or other internet protocol networks. The resource records contained in the DNS associate domain names with other forms of information. These are most commonly used to map human-friendly domain names to the numerical IP addresses computers need to locate services and devices using the underlying network protocols, but have been extended over time to perform many other functions as well

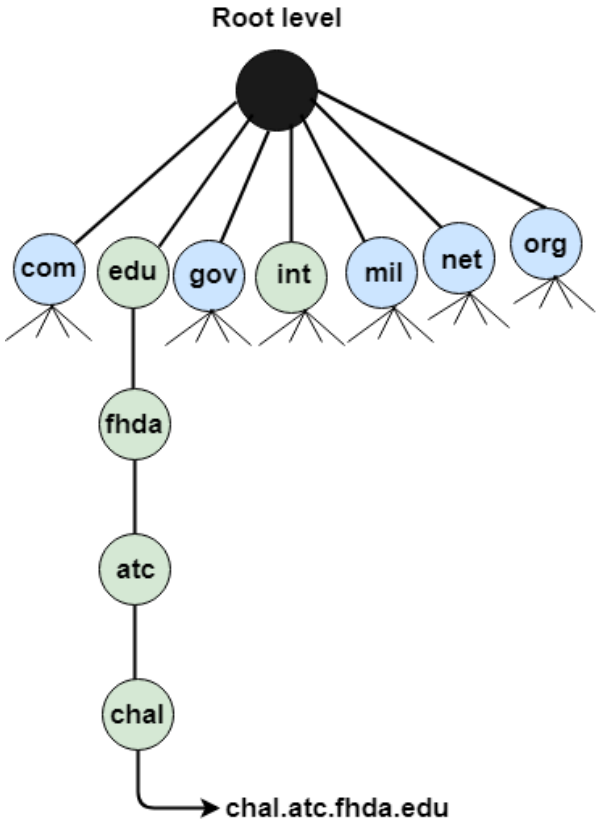
DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.DNS is required for the functioning of the internet. Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.

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



Generic Domains

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



Country Domain

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

Inverse Domain

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

URL

URL stands for **Uniform Resource Locator** that identifies a particular Internet resource. URL helps the user locate a web page, gopher service, library catalogue, image, or text file locations. URLs are the standard addressing system of the www. A complete URL provides the web client with all the information it needs to contact a server and make a request for information.

A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files).

Every URL contains the following information:

- The scheme name or protocol.
- A colon, two slashes.
- A host, normally called a domain name but sometimes as a literal IP address.
- A colon followed by a port number.
- Full path of the resource.

A URL can be entered manually by typing it in the address bar of your web browser. If the URL does not contain a valid server, a browser may display a "Server not found" error and if the path in the URL is incorrect, the browser may display a "404 error". A URL does not contain spaces and uses forward slashes to represent different directories So, dashes and underscores are used separate the words of a web address.

URLs divided into three essential parts:

Example: https://www.mmnilanga.com/software

1. P**rotocol(http ://)** – The information appearing before the colon in any URL indicates the type of information server or protocol. For example, http:// indicates that the server to be connected is a www server.
2. **Domain name (www.mmnilanga.com)** – The second piece of information is the address of the server. In this example, ecomputernotes.com is the name of the machine at PS Exam on the World Wide Web.
3. **Resource name (software.htm)** – The third piece of information is the path to the actual document requested. In this example, the URL indicates that the document in the system directory and is named software.htm.

Concept of Intranet & Extranet

An intranet is a private network used by employees to communicate and collaborate. ... An extranet is a private network, too. It works similarly to a company intranet; however an extranet allows access to authorized users from outside the company. These external users may include suppliers and partners.

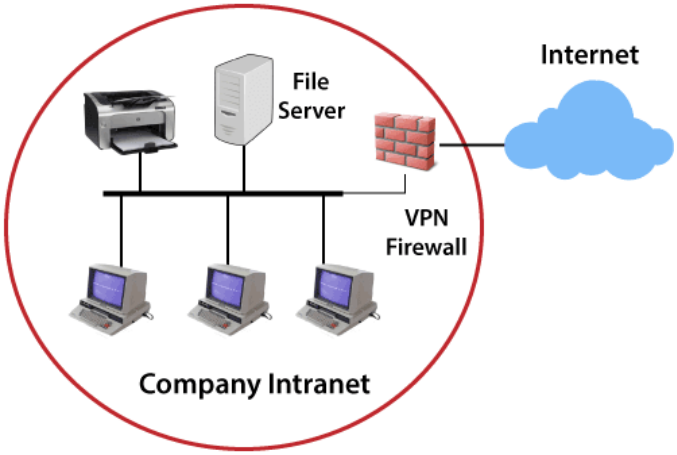
Intranet and extranet software supports two different areas in a business, but has similar goals: to improve how employees work with clients and each other. Sometimes they are combined in the same software, other times, separately.

Once integrated into a business model, these portals can make day-to-day activities more efficient, more streamlined, better connected, and more productive.

Intranet

The intranet is a private network that belongs to a particular organization. It is designed for the exclusive use of an organization and its associates, such as employees, customers, and other authorized people. It offers a secure platform to convey information and share data with authorized users. Confidential information, database, links, forms, and applications can be made available to the staff through the intranet. So, it is like a private internet or an internal website that is operating within an organization to provide its employees access to its information and records. Each computer in intranet is identified by a unique IP Address.

It is based on internet protocols (TCP/IP) and is protected from unauthorized access with firewalls and other security systems. The firewall monitors the incoming and outgoing data packets to ensure they don't contain unauthorized requests. So, users on the intranet can access the internet, but the internet users can't access the intranet if they are not authorized for it. Furthermore, to access the intranet, the authorized user is required to be connected to its LAN (Local Area Network).



Some of the benefits of the intranet are:

- It is cheap and easy to implement and run, and is more safe than the internet and extranet.
- It streamlines communication that enables the company to share its data, information, and other resources among employees without any delay. The entire staff can receive company's announcements, ask questions, and access internal documents.
- It provides a secure space to store and develop applications to support business operations.

- It improves the efficiency of the company by speeding up workflow and reducing errors. Thus, it helps achieve targets by completing the tasks on time.
- It offers a testing platform for new ideas before they are uploaded on the company's internet webpage. Thus, it helps maintain the credibility of the company
- Information is shared in real-time, or updates are reflected immediately to all the authorized users.
- Modern intranets also offer a mobile app that allows employees to stay connected on the go.
- It aids in project management and tracking workflow and teams' progress.
- It can work with mobile devices, which means it can provide information that exists on intranet directly to mobile devices of employees such as phones, tablets, etc.
- It can also be used to motivate employees, facilitate employee recognition, and to reward them for performing beyond expectations.

Disadvantages of Intranet:

- It may be costly to set up an Intranet due to hidden costs and complexity.
- If the firewall does not work properly or not installed, it can be hacked by someone
- High-security passwords are required, which cannot be guessed by outside users
- There is always a fear of losing control over the intranet
- Sometimes document duplication may happen which can cause confusion among employees
- You have to give access to multiple users, so you may find it hard to control this network.

Examples of Intranet:

Educational Intranet: It is generally found in a school, college, etc., For example, a school intranet is intended to allow teaching staff to communicate with each other and get information about upcoming updates such as exam dates, schools functions, holidays, etc.

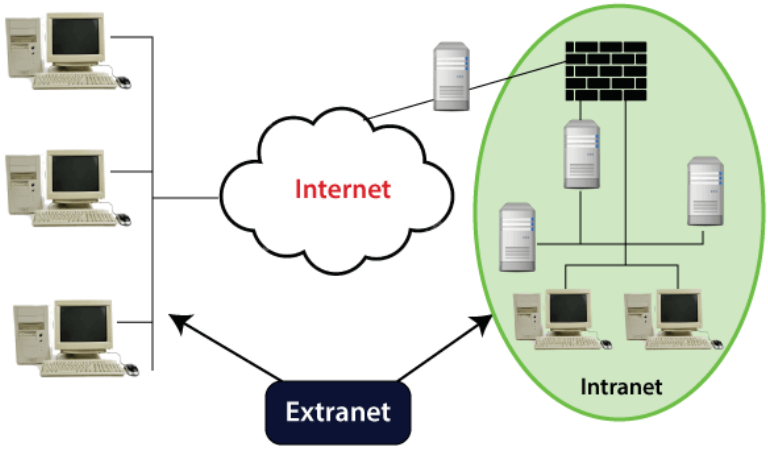
Real Estate Intranet: The intranet of a real estate company allows its sales team to have access to all important brochures, templates, forms that they may need to close a sale. Employees also remain up to date with important events like meetings, training, sessions, etc. It can also be used to share motivational messages with the team.

Health Care Intranet: In the healthcare sector, in big hospitals, the Intranet helps health care professionals to work as a team to provide proper care and treatment to their patients. Doctors can share reports, treatment procedures, bills and claims can be settled easily without moving from one department to another department.

IT Sector Intranet: In the IT sector three is always a lot of information that needs to be shared with all the employees at one go. It may be related to a project that needs to be completed within the given time frame, such as guidelines, terms and conditions, and rules that are to be followed while working on a project.

Extranet

Extranet is a part of an organization's intranet. It is a communication network that is based on internet protocols (TCP/IP). It provides controlled access to firm's intranet to its trading partners, customers, and other businesses. So, it is a private network that securely shares internal information and operations of a firm with authorized people outside the firm without giving access to the company's entire network. The users are required to have IDs, passwords, and other authentication mechanisms to access this network.



Some of the benefits of extranet:

- It acts as a single interface between the company and its trading partners.
- It automates the firm's processes like automatically places an order with suppliers when inventory drops.
- It improves customer service by providing customers a platform to resolve their queries and complaints.
- It enables the firm to share information with trading partners without engaging in paper-based publishing processes.
- It streamlines business processes that are repetitive in nature, such as ordering from a vendor on a regular basis.

Limitations of Extranet:

- **Hosting:** If you host extranet pages on your own server, it requires a high bandwidth internet connection, which is may be very expensive.
- **Security:** You need extra firewall security if you host it on your own server. It increases the workload and makes security mechanism very complex.
- **Dependency:** It is dependent on the internet as outsiders cannot access information without using the internet.
- **Less Interaction:** It reduces the face to face interaction between customers, business partners, vendors, etc., which results in poor relationship building.

Intranet	Extranet
It is a private network, which cannot be accessed externally.	It may not be called a private network, as it can be assessed externally. It provides limited access to authorized outside-users such as vendors, partners, etc.
It connects the employees of the company.	It connects the company's employees with partners.
It is an independent network, not a part or extension of any other network.	It is an additional part of company's Intranet.
Communication takes place only within the organization that owns the network.	External users such as suppliers, customers, and partners are allowed to be a part of intranet to get information, updates, about the organization.
Intranet is a tool for sharing information throughout the organization.	Whereas Extranet is a tool for sharing information between the internal members and external members.
Intranet is owned by a single organization.	While Extranet is owned by either a single or a many organization.
In intranet, security is implemented through a firewall.	Whereas in this, security is implemented through a firewall in order to separate the extranet and the internet.
Intranet is managed by an organization.	Whereas Extranet is managed by many organizations.
Intranet is the limited and compromised version of Extranet.	While Extranet is the limited and compromised version of Internet.
It’s restricted area is upto an organization.	It’s restricted area is upto an organization and some of its stakeholders.
Example: WIPRO using internal network for its business operations.	Example: DELL and Intel using network for business related operations

3.3 Networking protocol: IP,TCP,FTP,HTTP,DHCP

3.3 Networking protocol: IP,TCP,FTP,HTTP,DHCP

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

IP

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

TCP

The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets.

TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets. Since TCP is the protocol used most commonly on top of IP, the Internet protocol stack is sometimes referred to as TCP/IP.

TCP stands for **Transmission Control Protocol**. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.

Features of TCP protocol

Transport Layer Protocol

TCP is a transport layer protocol as it is used in transmitting the data from the sender to the receiver.

Reliable

TCP is a reliable protocol as it follows the flow and error control mechanism. It also supports the acknowledgment mechanism, which checks the state and sound arrival of the data. In the acknowledgment mechanism, the receiver sends either positive or negative acknowledgment to the sender so that the sender can get to know whether the data packet has been received or needs to resend.

Order of the data is maintained

This protocol ensures that the data reaches the intended receiver in the same order in which it is sent. It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.

Connection-oriented

It is a connection-oriented service that means the data exchange occurs only after the connection establishment. When the data transfer is completed, then the connection will get terminated.

Full duplex

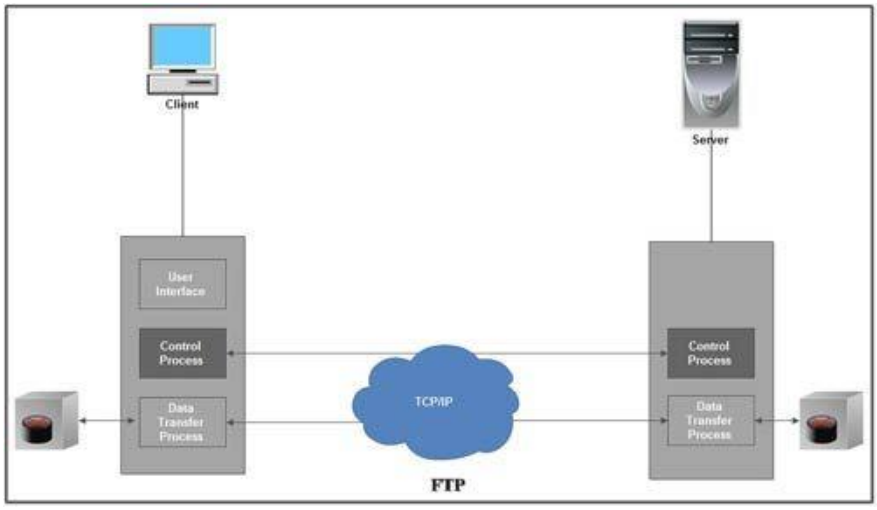
It is a full-duplex means that the data can transfer in both directions at the same time.

Stream-oriented

TCP is a stream-oriented protocol as it allows the sender to send the data in the form of a stream of bytes and also allows the receiver to accept the data in the form of a stream of bytes. TCP creates an environment in which both the sender and receiver are connected by an imaginary tube known as a virtual circuit. This virtual circuit carries the stream of bytes across the internet.

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.
- 

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.

HTTP

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

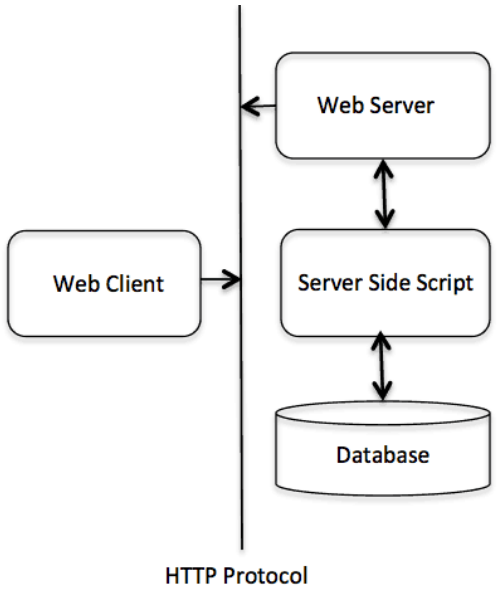
Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

There are three basic features that make HTTP a simple but powerful protocol:

- HTTP is connectionless: The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client waits for the response. The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only. Further requests are made on new connection like client and server are new to each other.
- HTTP is media independent: It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- HTTP is stateless: As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

Basic Architecture

The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:



The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

Server

The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else

that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.

- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP

There are following benefits of DHCP:

Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

4. Network Security

4.1 Network Security issues
4.2 Traditional Cryptography- substitution Ciphers, Transposition Ciphers
4.3 Two fundamental cryptographic principles
4.4 DES

4.1 Network Security issues

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or intranets to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Intrusion Detection Systems

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

4.2 Traditional Cryptography- substitution Ciphers, Transposition Ciphers

Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication.

Components

There are various components of cryptography which are as follows −

Plaintext and Ciphertext

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

Cryptography focuses on four different objectives:

1. Confidentiality: Confidentiality ensures that only the intended recipient can decrypt the message and read its contents.
2. Non-repudiation: Non-repudiation means the sender of the message cannot backtrack in the future and deny their reasons for sending or creating the message.
3. Integrity: Integrity focuses on the ability to be certain that the information contained within the message cannot be modified while in storage or transit.
4. Authenticity: Authenticity ensures the sender and recipient can verify each other’s identities and the destination of the message.

Substitution Cipher Technique

- The art of writing, coding, and analyzing usually in cryptography, a substitution cipher is a technique of encryption by which characters of plain text are replaced with another symbol or number according to a permanent set of procedures.
- The plain text includes characters, letters, triplets, pairs, etc.
- The letters of standard alphabets are replaced with ciphertext in the substitution cipher technique.
- In this technique, the substitution of punctuation and spaces are also applied.
- It replaced the plain text characters with other characters, symbols, numbers.
- In this technique character's identity is also changed even as its location remains unchanged.
- Two kinds of algorithms: Monoalphabetic and Polyalphabetic substitution cipher are mainly used in the **Substitution Cipher Technique.**

Transposition Cipher Technique:

- Transposition cipher changes the position of symbols instead of substituting one character for another.
- It rearranges the location of plain text characters.
- In this technique the location of the character is changed other than the identity of the character is not changed.
- Transposition ciphers are of two kinds, Keyless and Keyed transportation cipher.
- The long sections of readable plaintext will be disclosed by keys that were neared to the right key.

Fundamental Cryptographic Principles

(1) Redundancy:

- The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message.
- Cryptographic principle 1: "Messages must contain some redundancy."
- In other words, upon decrypting a message, the recipient must be able to tell whether it is valid by simply inspecting it and perhaps performing a simple computation.

- This redundancy is needed to prevent active intruders from sending garbage and tricking the receiver into decrypting the garbage and acting on the "plaintext."
- However, this same redundancy makes it much easier for passive intruders to break the system.

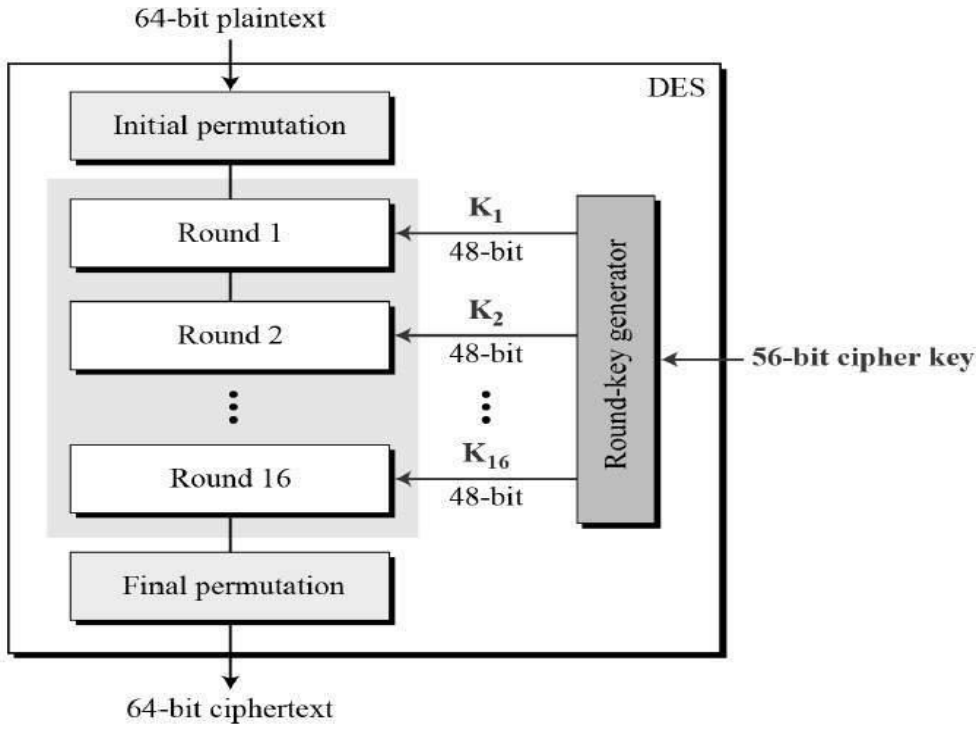
(2) Freshness:

- The second cryptographic principle is that some measures must be taken to ensure that each message received can be verified as being fresh, that is, sent very recently.
- This measure is needed to prevent active intruders from playing back old messages.
- Cryptographic principle 2: “Some method is needed to foil replay attacks.”
- One such measure is including in every message a timestamp valid only for, say, 10 seconds.
- The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

DES

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −



It is a symmetric key algorithm, which means that the same key is used for encrypting and decrypting data.