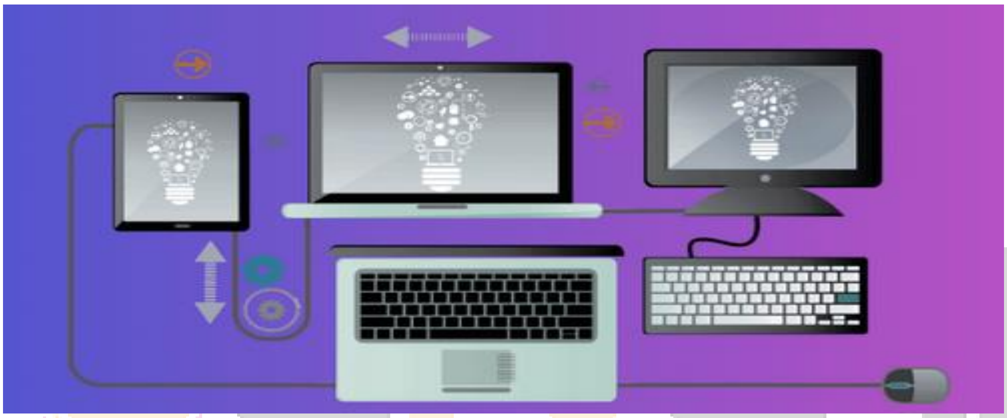
RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL
New Scheme Based On AICTE Flexible Curicula, B. Tech. First Year
Computer Science & Engineering, BT-205: Basic Computer Engineering

UNIT 4

INTRODUCTION TO COMPUTER NETWORK

A computer network is a group of devices connected with each other through a transmission medium such as wires, cables etc. These devices can be computers, printers, scanners, Fax machines etc. The purpose of having computer network is to send and receive data stored in other devices over the network. These devices are often referred as nodes.



GOALS OF COMPUTER NETWORK

- The main goal of networking is "**Resource sharing**", and it is to make all programs, data and equipment available to anyone on the network without the regard to the physical location of the resource and the user.
- A second goal is to provide "**high reliability**" by having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable, the other copies could be available.
- Another goal is "**saving money**". Small computers have a much better price/performance ratio than larger ones. Mainframes are roughly a factor of ten times faster than the fastest single chip microprocessors, but they cost thousand times more. This imbalance has caused many system designers to build systems consisting of powerful personal computers, one per user, with data kept on one or more shared file server machines. This goal leads to networks with many computers located in the same building. Such a network is called a LAN (local area network).
- Another closely related goal is to "**increase the systems performance**" as the work load increases by just adding more processors. With central mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and with even greater disruption to the users.
- Computer networks provide a "**powerful communication medium**". A file that was updated or modified on a network can be seen by the other users on the network immediately.

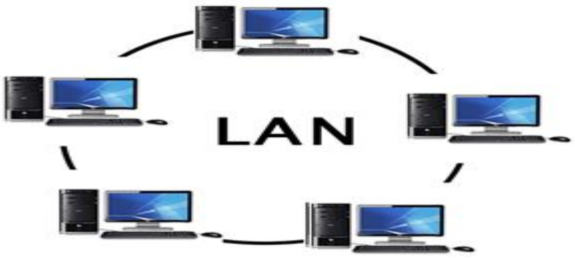
Computer Network Types:

A computer network can be categorized by their size. A computer network is mainly of four types:

- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

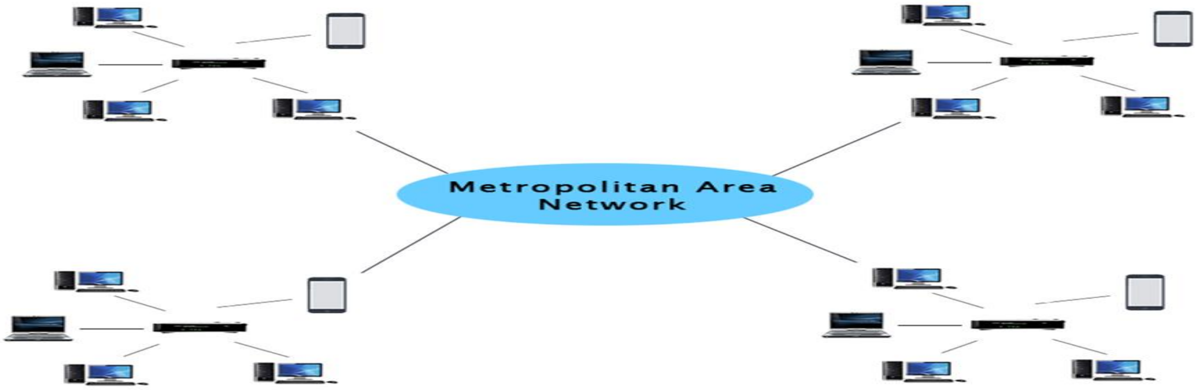
LAN (Local Area Network)

- 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.



MAN (Metropolitan Area Network)

- 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).

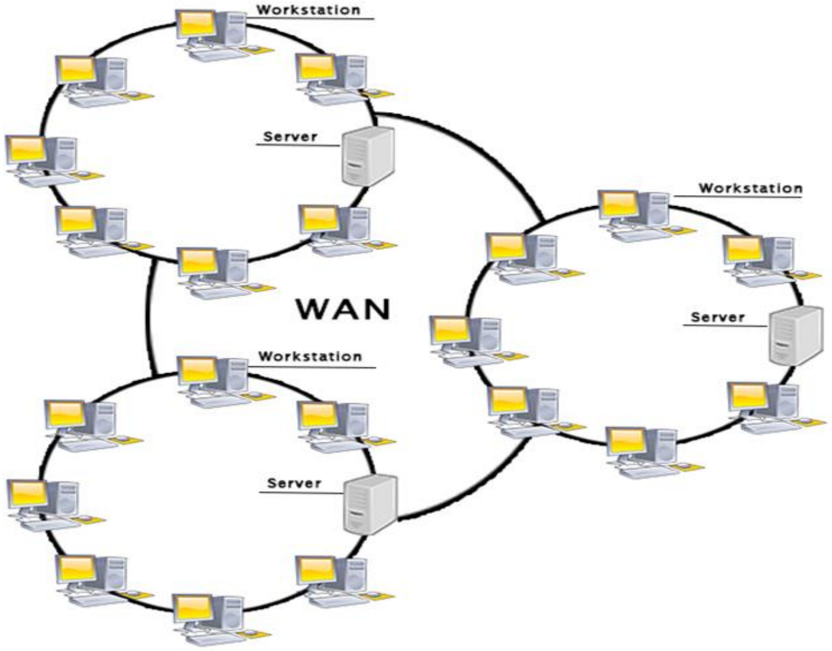


Uses Of Metropolitan Area Network:

- 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.

WAN (Wide Area Network)

- 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, fibre 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.

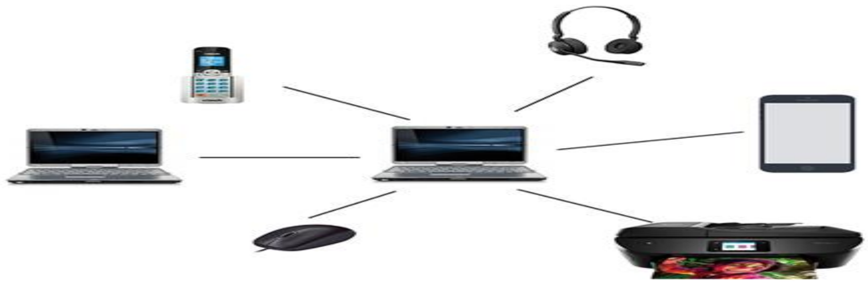
Advantages Of Wide Area Network:

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, 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.

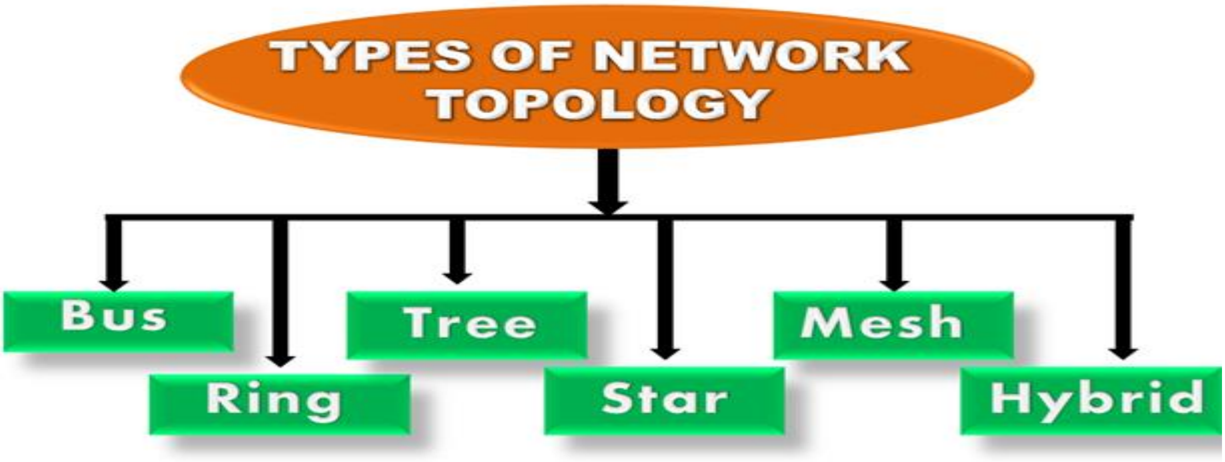
PAN (Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

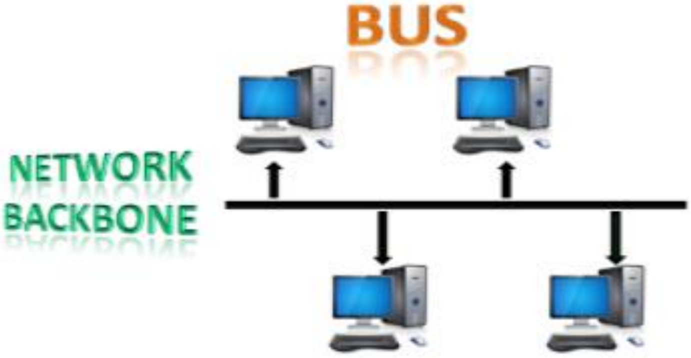


Network Topology:

Topology defines the structure of the network of how all the components are interconnected to each other.

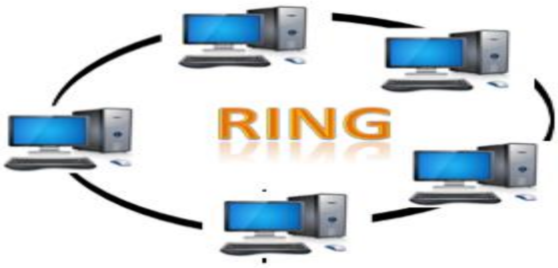


Bus Topology



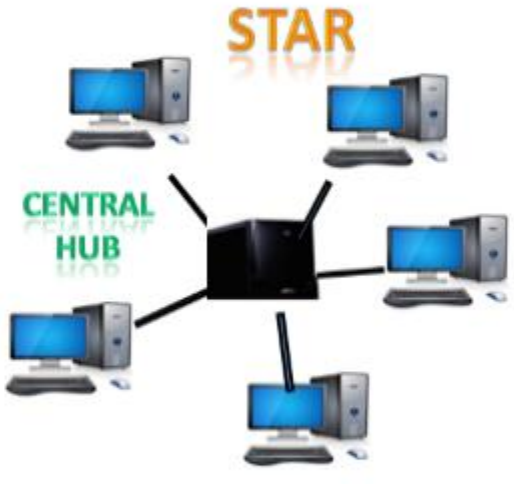
The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.

Ring Topology



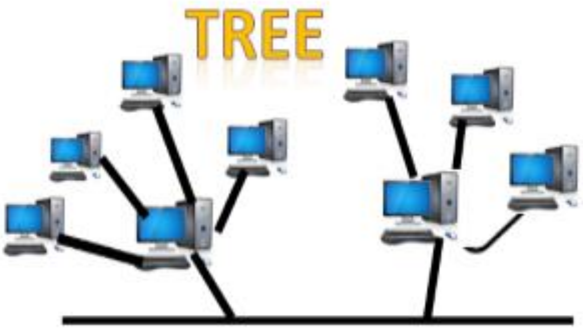
Ring topology is like a bus topology, but with connected ends.

Star Topology



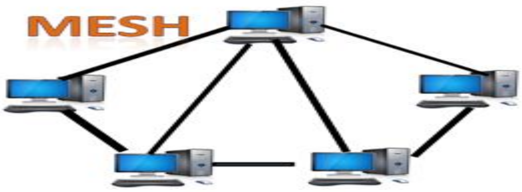
Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

Tree topology



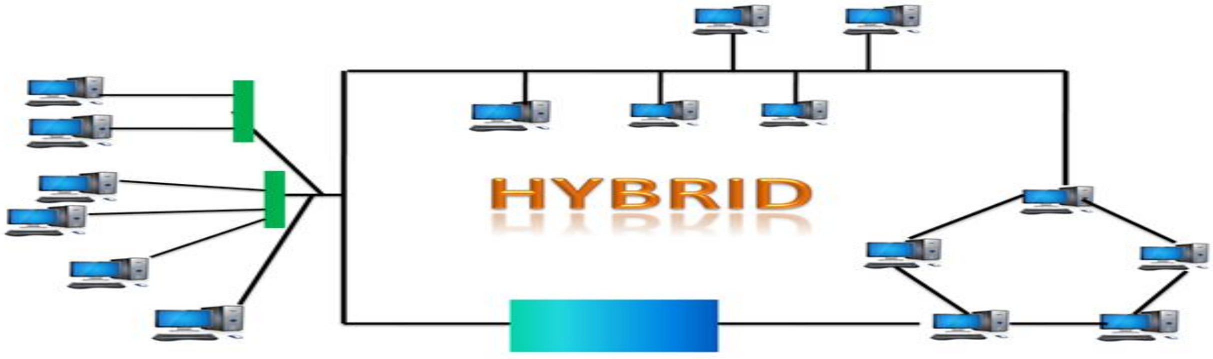
Tree topology combines the characteristics of bus topology and star topology. A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.

Mesh topology



Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

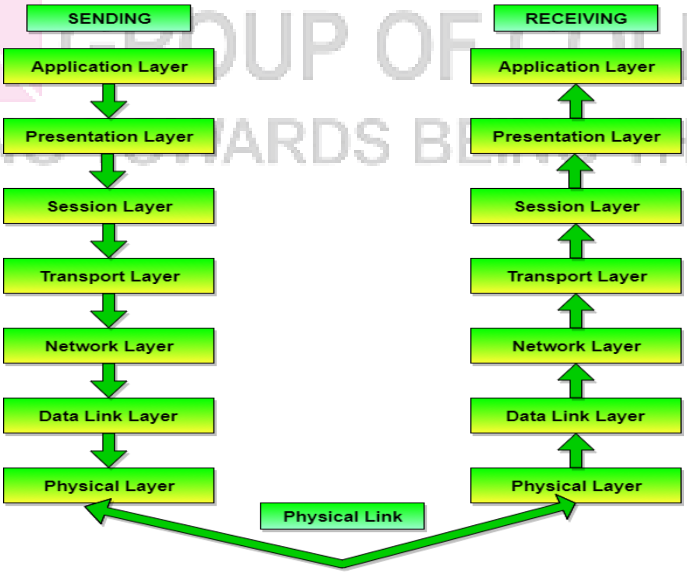
Hybrid Topology



The combination of various different topologies is known as **Hybrid topology**.

ISO-OSI MODEL

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Created at a time when network computing was in its infancy, the OSI was published in 1984 by the International Organization for Standardization (ISO). Though it does not always map directly to specific systems, the OSI Model is still used today as a means to describe Network Architecture.



Functions of the OSI Layers

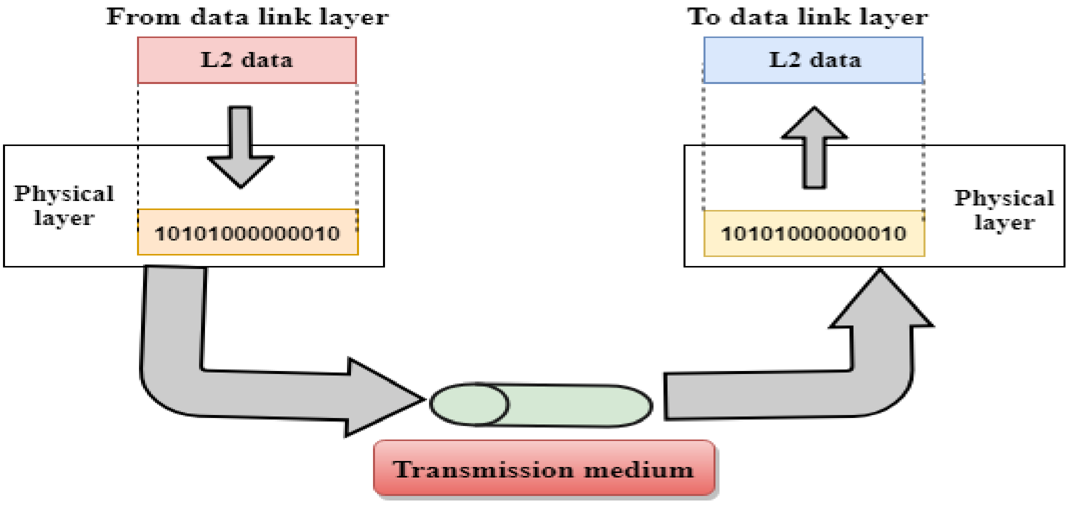
There are the seven OSI layers. Each layer has different functions. A list of seven layers is given below:

1. Physical Layer
2. Data-Link Layer

3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

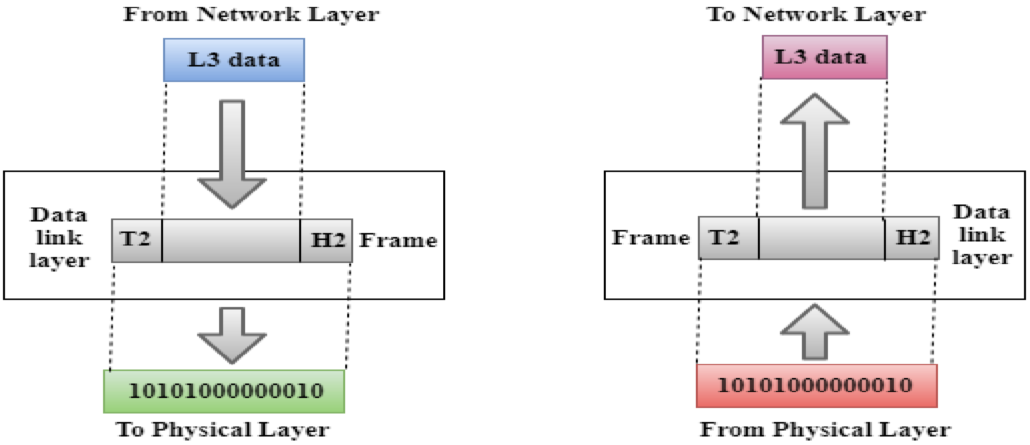
The functions of various layers in OSI model are given below:

1. **Physical layer**



- ❖ **Line Configuration**: It defines the way how two or more devices can be connected physically.
- ❖ **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- ❖ **Topology**: It defines the way how network devices are arranged.
- ❖ **Signals:** It determines the type of the signal used for transmitting the information.

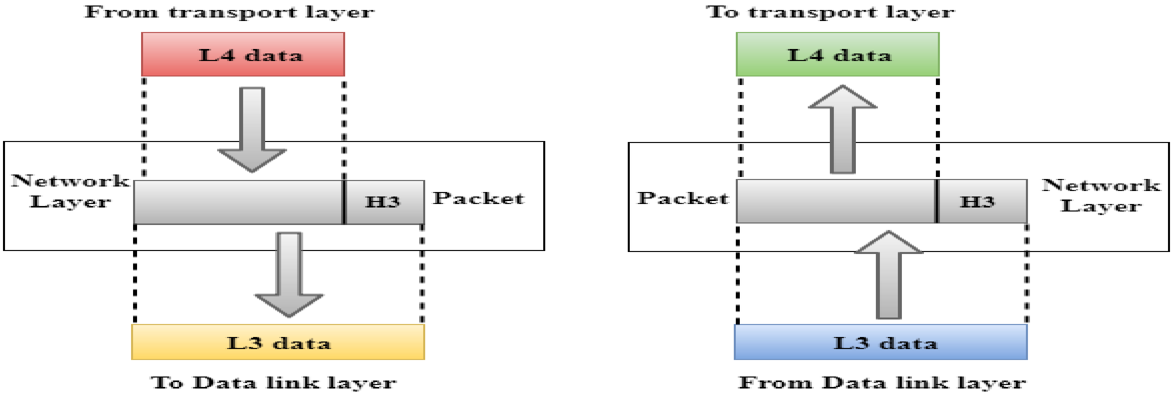
2. **Data-Link Layer**



- ❖ **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

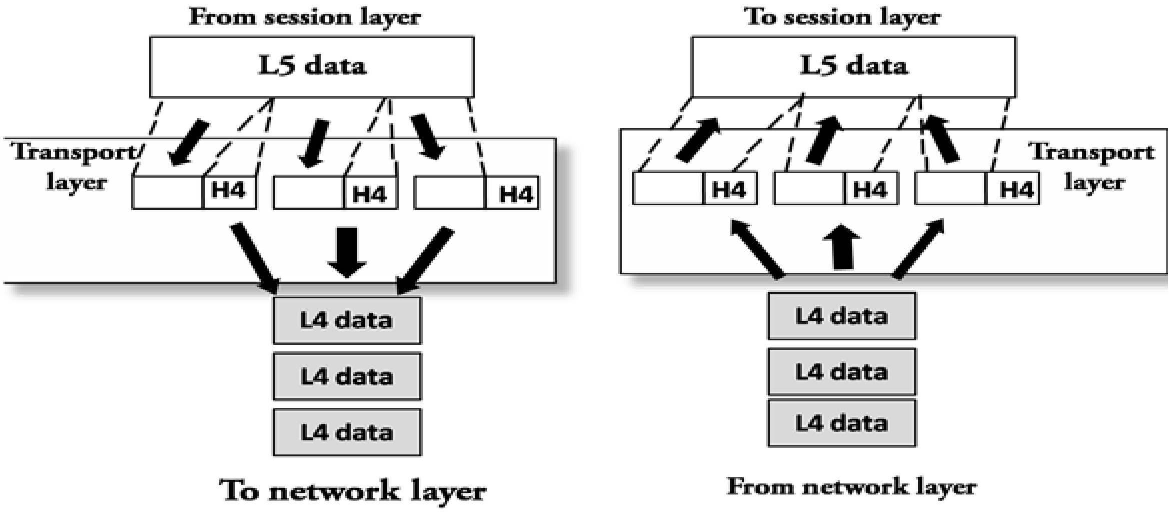
- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3. **Network Layer**



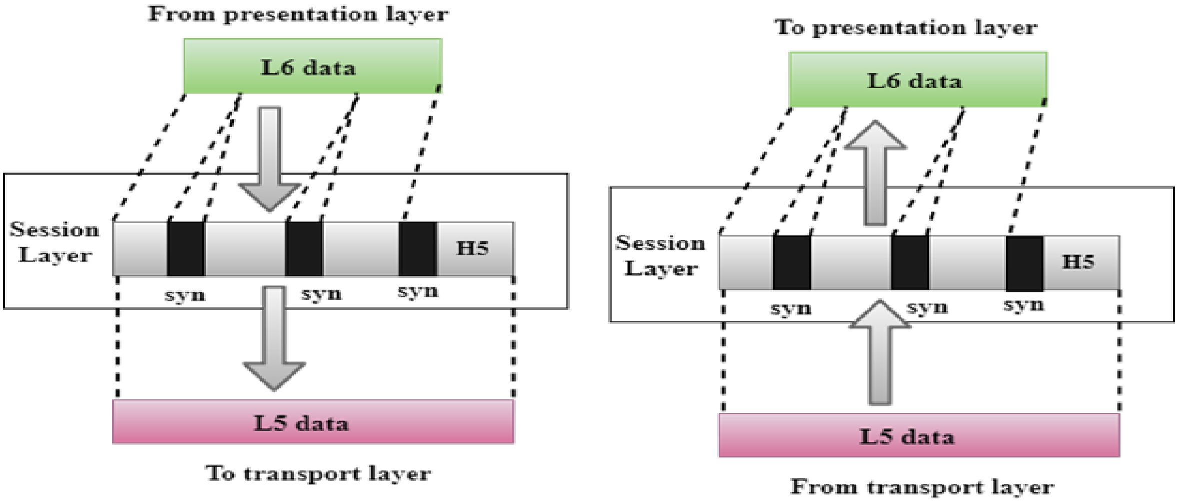
- **Internetworking**: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing**: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing**: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4. Transport Layer



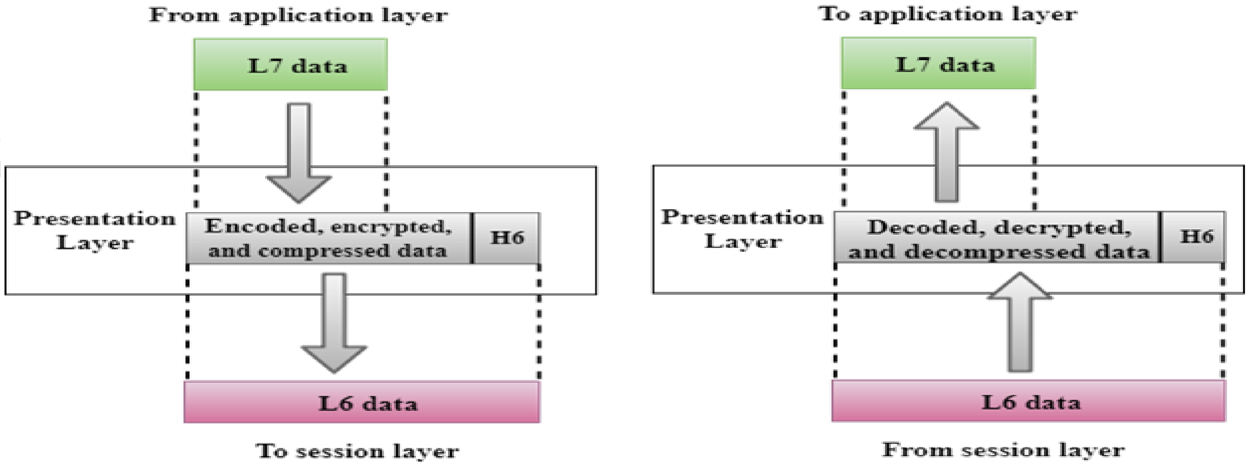
- ❖ **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- ❖ **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- ❖ **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- ❖ **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- ❖ **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5. Session Layer



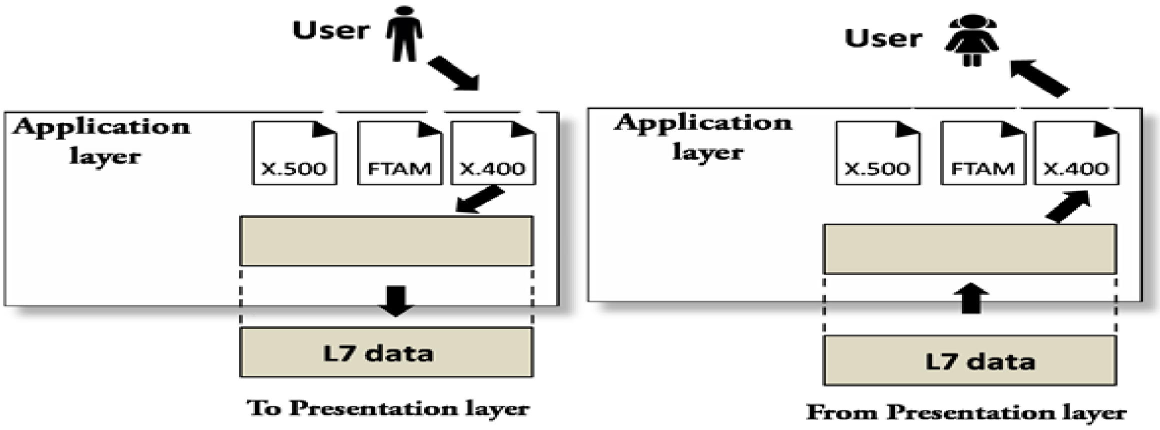
- ❖ **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- ❖ **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6. Presentation Layer



- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7. **Application Layer**



- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services**: An application provides the distributed database sources and is used to provide that global information about various objects.

INTERNETWORKING

Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.

Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the Internet Routing Protocol. The Internet is the largest pool of networks geographically located throughout the world but these networks are interconnected using the same protocol stack, TCP/IP. Internetworking is only possible when the all the connected networks use the same protocol stack or communication methodologies.

There are three types of Internetworking:

1. Extranet
2. Intranet
3. Internet

Extranet – It's a network of the internetwork that's restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.

Intranet – This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that's underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browseable data.

Internet – A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries those management assignments.

INTERNETWORKING DEVICES

An internetworking device is a widely-used term for any hardware within networks that connect different network resources. Key devices that comprise a network are routers, bridges, repeaters and gateways.

1. Repeaters

Repeaters are used to extend the length of the Network. Repeaters were created to regenerate and amplify weak signals, thus extending the length of the network. The basic function of a repeater is to retime, reshape, and reamplify the data signal to its original level.

Important features of a repeater are as follows:

- A repeater connects different segments of a LAN
- A repeater forwards every frame it receives
- A repeater is a regenerator, not an amplifier
- Repeaters operate at the physical layer of the OSI model.

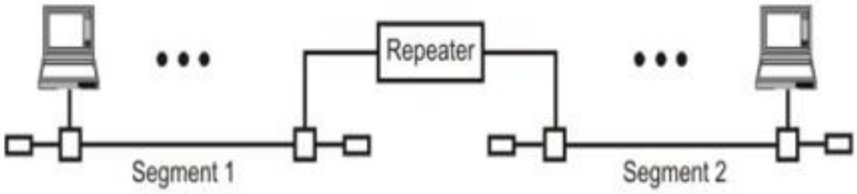


Figure 1.1 Repeaters connecting two LAN segments

2. Hubs

- Hub is a generic term, but commonly refers to a multiport repeater. It can be used to create multiple levels of hierarchy of stations.
- The stations connect to the hub with RJ-45 connector having maximum segment length is 100 meters. This type of interconnected set of stations is easy to maintain and diagnose. Hubs operate at the physical layer of the OSI model.

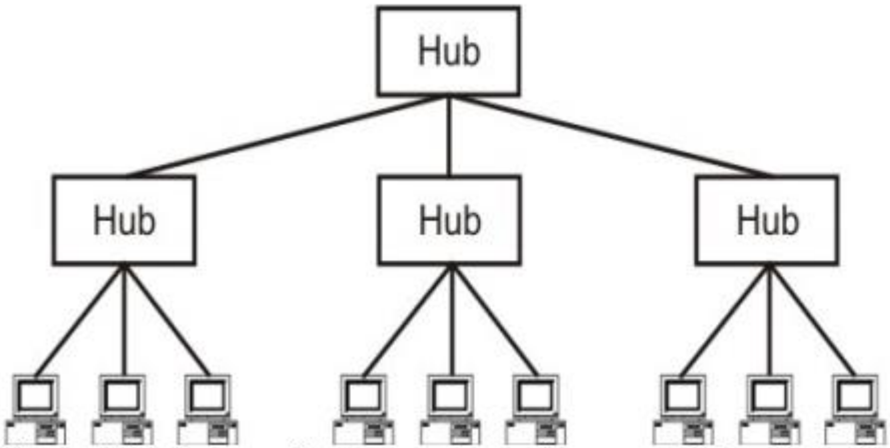
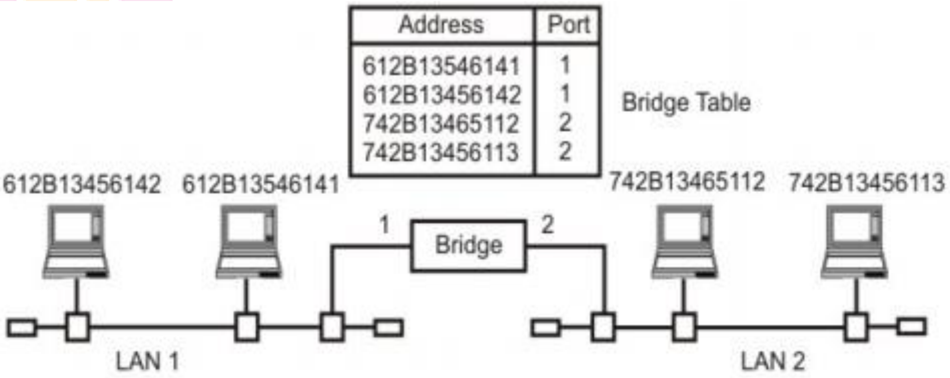


Figure 1.2 Hub as a multi-port repeater can be connected in a hierarchical manner to form a single LAN with many nodes

3. Bridges

- ❖ The device that can be used to interconnect two separate LANs is known as a bridge. It is commonly used to connect two similar or dissimilar LANs as shown in Fig. 1.3.
- ❖ The bridge operates in layer 2, that is data-link layer and that is why it is called level-2 relay with reference to the OSI model. It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations. A bridge must contain addressing and routing capability.



Address	Port
612B13546141	1
612B13456142	1
742B13465112	2
742B13456113	2

Figure 1.3 A bridge connecting two separate LANs

Key features of a bridge are mentioned below:
a. A bridge operates both in physical and data-link layer
.b. A bridge uses a table for filtering/routing
c. A bridge does not change the physical (MAC) addresses in a frame.
Types of bridges:
a. Transparent Bridges
b. Source routing bridges

4. Switches

A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames.
Some of important functionalities are:

- ❖ Ports are provided with buffer
- ❖ Switch maintains a directory: #address - port#
- ❖ Each frame is forwarded after examining the #address and forwarded to the proper port#
- ❖ Three possible forwarding approaches: Cut-through, Collision-free and Fully- buffered as briefly explained below.

  a. Cut-through: A switch forwards a frame immediately after receiving the destination address. As a consequence, the switch forwards the frame without collision and error detection.

  b. Collision-free: In this case, the switch forwards the frame after receiving 64 bytes, which allows detection of collision. However, error detection is not possible because switch is yet to receive the entire frame.

  c. Fully buffered: In this case, the switch forwards the frame only after receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.

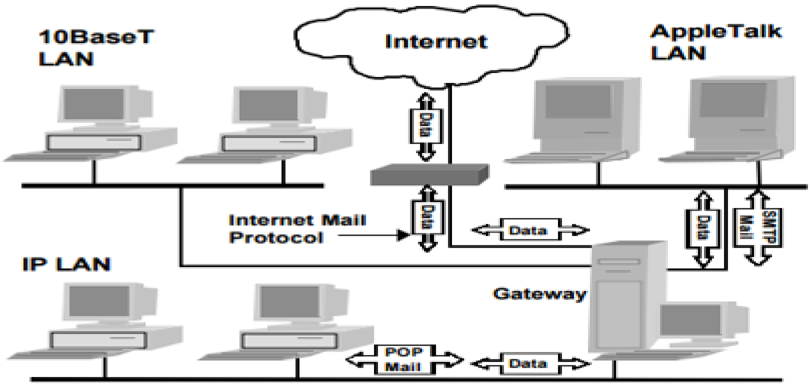
5. **Router**

- ❖ Routers link two or more different networks together, such as an Internet Protocol network. These networks can consist of various types of LAN segments, for example, Ethernet, token ring, or Fiber Distributed Data Interface (FDDI).
- ❖ A router receives packets and selects the optimum path to forward the packet across the network.
- ❖ Routers build a table of all the device addresses (routing table) across the networks.
- ❖ Using this table, the router forwards a transmission from the sending station to the receiving station across the best path. Routers operate at the network level of the OSI model.

6. **Gateways**

- ❖ Gateways are multi-purpose connection devices. They are able to convert the format of data in one computing environment to a format that is usable in another computer environment (for example, AppleTalk and DEC net).
- ❖ The term gateway is sometimes used when referring to a router.
- ❖ For example, gateways translate different electronic mail protocols and convey email across the Internet.

- **Gateways Translate Different Network Protocols**



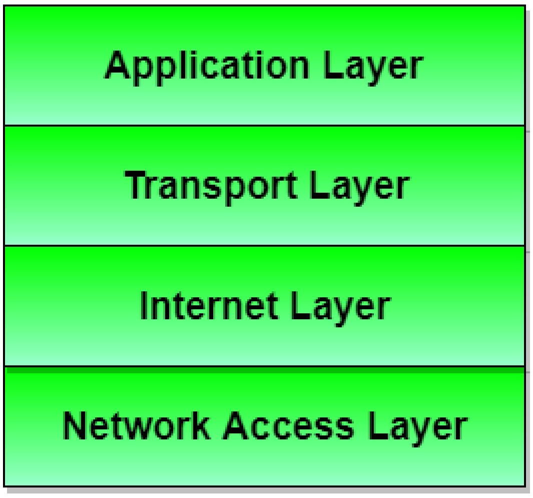
- Gateways can operate at all layers of the OSI model since them:

Gateways can operate at all layers of the OSI model since them:

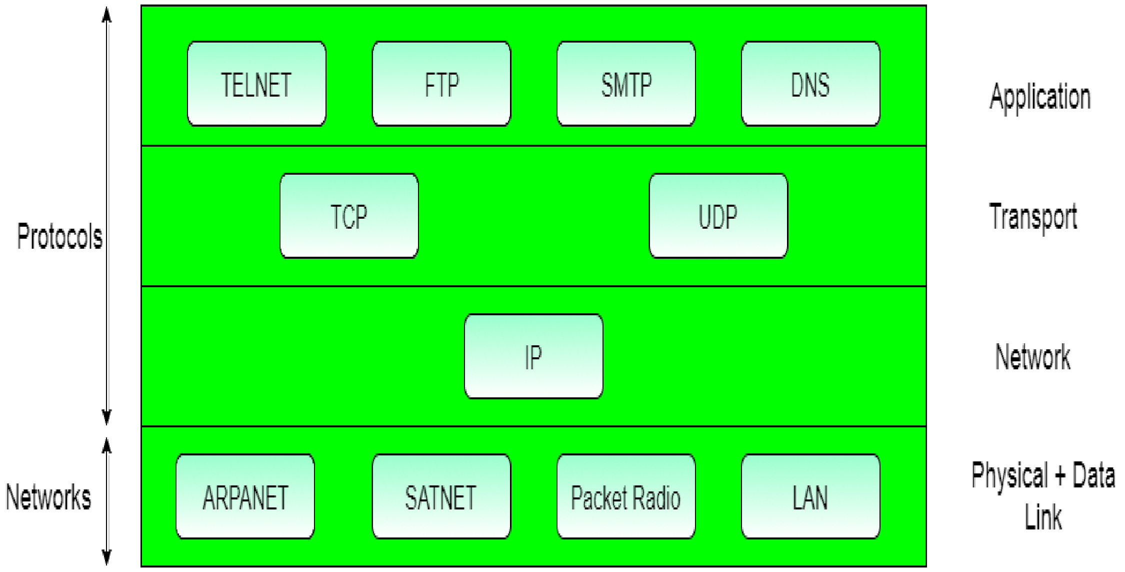
- ❖ Can provide a physical link between networks.
- ❖ Create junctions between dissimilar networks.
- ❖ Translate different network protocols and/ or applications (for example, electronic mail between the Internet and a commercial online service with its own mail protocol).

TCP/IP MODEL

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



Overview of TCP/IP

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of **Defence's Project Research Agency** (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Different Layers of TCP/IP Model are given bellows:

Layer 1: Host to network Layer

- Lower layer of the all
- Protocol is used to connect to the host, so that the packets can be sent over it.
- Varies from host to host and network to network.

Layer 2: Internet layer

- Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.
- The various functions performed by the Internet Layer are:
  - Delivering IP packets

  - Performing routing
  - Avoiding congestion

Layer 3: Transport Layer

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
- The applications can read and write to the transport layer.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

- **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
- **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
- **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
- **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
- It allows peer entities to carry conversation.
- It defines two end-to-end protocols: TCP and UDP

  - **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
  - **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

INTERNET

The **Internet** is the biggest world-wide communication network of computers. The Internet has millions of smaller domestic, academic, business, and government networks, which together carry many different kinds of information. The short form of internet is the 'net'. The World Wide Web is one of its biggest services. It is used by billions of people all over the world.
The Internet was developed in the United States by the "United States Advanced Research Projects Agency" (DARPA). The Internet was first connected in October, 1969 and was called ARPANET.
The World Wide Web was created at CERN in Switzerland in 1990 by a British (UK) scientist named Tim Berners-Lee.
Today, people can pay money to access the Internet from internet service providers. Some services on the Internet cost nothing to use. Sometimes people who offer these free services use advertising to make money. Censorship and freedom of speech on the Internet can be controversial.

Services on the internet

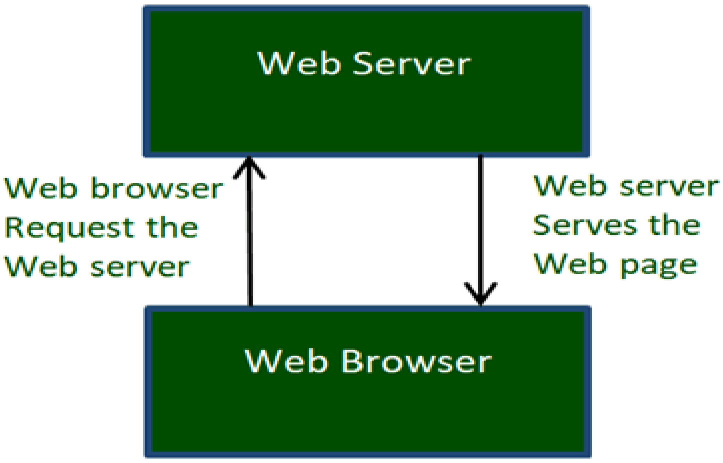
The Internet is used for many things, such as electronic mail, online chat, file transfer and other documents of the World Wide Web.
The most used service on the Internet is the World Wide Web (which is also called the "Web" or “www”). The web contains websites, including blogs and wikis like Wikipedia. Webpages on the Internet can be seen and read by anyone (unless the page needs a password, or it is blocked).
The second biggest use of the Internet is to send and receive e-mail. E-mail is private and goes from one user to another. Instant messaging (such as AIM or ICQ) is similar to email, but allows two or more people to chat to each other faster.
Some governments think the internet is a bad thing, and block all or part of it. For example, the Chinese government thinks that Wikipedia is bad. Many times no one in China can read it or add to it. Another example of the internet being blocked is in North Korea. Some parents block parts of the Internet they think are bad for children to see.

WORLD WIDE WEB

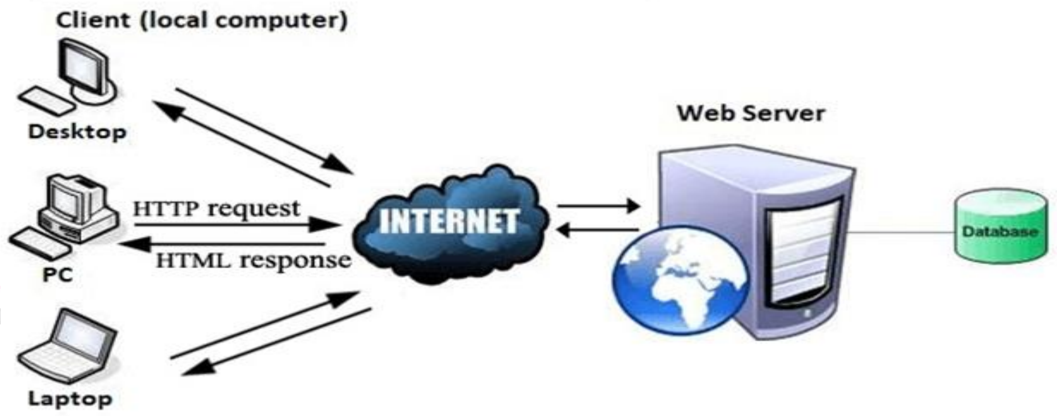
The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://www.example.com/), which may be interlinked by hypertext, and are accessible over the Internet. The resources of the WWW are transferred via the Hypertext Transfer Protocol (HTTP) and may be accessed by users by a software application called a web browser and are published by a software application called a web server.

How the World Wide Web Works?

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


Web Server
Web browser Request the Web server
Web server Serves the Web page
Web Browser

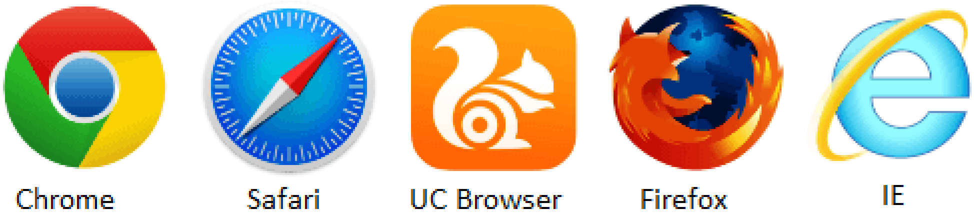
The Web works as per the internet's basic client-server format as shown in the following image. The servers store and transfer web pages or information to user's computers on the network when requested by the users. A web server is a software program which serves the web pages requested by web users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



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

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

Web Browser:



A web browser, which is commonly known as a browser, is a program that displays text, data, pictures, videos, animation, and more. It provides a software interface that allows you to click hyperlinked resources on the World Wide Web. When you double click the Browser icon installed on your computer to launch it, you get connected to the World Wide Web and can search Google or type a URL into the address bar.

In the beginning, browsers were used only for browsing due to their limited potential. Today, they are more advanced; along with browsing you can use them for e-mailing, transferring multimedia files, using social media sites, and participating in online discussion groups and more. Some of the commonly used browsers include Google Chrome, Mozilla Firefox, Internet Explorer, Safari, and more.

ELECTRONIC COMMERCE

E-Commerce or Electronic Commerce means buying and selling of goods, products, or services over the internet. E-commerce is also known as electronic commerce or internet commerce. These services provided online over the internet network. Transaction of money, funds, and data are also considered as E-commerce. These business transactions can be done in four ways: Business to Business (B2B), Business to Customer (B2C), Customer to Customer (C2C), Customer to Business (C2B). The standard definition of E-commerce is a commercial transaction which is happened over the internet. Online stores like Amazon, Flipkart, Shopify, Myntra, Ebay, Quikr, Olx are examples of E-commerce websites. By 2020, global retail e-commerce can reach up to $27 Trillion.

Examples of E-Commerce

- Amazon
- Flipkart
- eBay
- Fiverr
- Upwork
- Olx
- Quikr

Advantages of E-Commerce

- ❖ E-commerce provides the sellers with a global reach. They remove the barrier of place (geography). Now sellers and buyers can meet in the virtual world, without the hindrance of location.
- ❖ Electronic commerce will substantially lower the transaction cost. It eliminates many fixed costs of maintaining brick and mortar shops. This allows the companies to enjoy a much higher margin of profit.

- It provides quick delivery of goods with very little effort on part of the customer. Customer complaints are also addressed quickly. It also saves time, energy and effort for both the consumers and the company.
- One other great advantage is the convenience it offers. A customer can shop 24×7. The website is functional at all times, it does not have working hours like a shop.
- Electronic commerce also allows the customer and the business to be in touch directly, without any intermediaries. This allows for quick communication and transactions. It also gives a valuable personal touch.

Disadvantages of E-Commerce

- The start-up costs of the e-commerce portal are very high. The setup of the hardware and the software, the training cost of employees, the constant maintenance and upkeep are all quite expensive.
- Although it may seem like a sure thing, the e-commerce industry has a high risk of failure. Many companies riding the dot-com wave of the 2000s have failed miserably. The high risk of failure remains even today.
- At times, e-commerce can feel impersonal. So it lacks the warmth of an interpersonal relationship which is important for many brands and products. This lack of a personal touch can be a disadvantage for many types of services and products like interior designing or the jewelry business.
- Security is another area of concern. Only recently, we have witnessed many security breaches where the information of the customers was stolen. Credit card theft, identity theft etc. remain big concerns with the customers.
- Then there are also fulfillment problems. Even after the order is placed there can be problems with shipping, delivery, mix-ups etc. This leaves the customers unhappy and dissatisfied.

COMPUTER SECURITY BASICS

VIRUSES, WORMS AND TROJAN HORSES

All three of these terms are used to describe malicious software that has infiltrated your computer through the Internet. Your computer becomes infected with one of these parasites through a door into your computer; this door is opened when you download a piece of software, open an email or visit a website with an untrusted source. Once the malware enters your computer, it sleeps in your computer until its functions are triggered; the functions may vary depending on the type of malware.

A **virus** infects host files on your computer, and then it is transmitted to other users when you send out those files. This is how computer viruses spread. The virus effects may vary from decreased computer performance to a complete loss of the computer's functionality.

A **Trojan horse** or Trojan infiltrates your computer through a file that you download and open. Unlike viruses, most Trojans stay on your computer only. They cause damage, but they do not spread to other computers. A Trojan is a piece of malware that stays in one place rather than spreading.

A **computer worm** infiltrates your computer when you download a file or an email. The worm then clones itself and attacks other devices on your network. The worm will infect your files, and will spread to the computers of people who you communicate with, in the same way that it infiltrated your computer

Spyware In most cases, Spyware installs itself on your computer in the same way as a Trojan horse does. Spyware spies on everything you do: paying your bills online, watching online videos, using Facebook, etc. It compiles this information and sends it to a database that then affects your web browsing. Depending on your preferences and your browsing history, the database will suggest promotional offers or other scams. Spyware can also download and install viruses on your computer or open pop-up when you are surfing the web.

Malware: The term malware or malicious software is used for any type of software that can affect your computer equipment's performance and functionality, either locally or remotely. Computer viruses, Trojan horses and worms are all considered malware.

Anti-spyware is a type of software that is designed to detect and remove unwanted spyware programs. Spyware is a type of malware that is installed on a computer without the user's knowledge in order to collect information about them. This can pose a security risk to the user, but more frequently spyware degrades system performance by taking up processing power, installing additional software, or redirecting users' browser activity.

Anti-spyware may also be called apyware on the Internet. Because "a" and "s" sit next to each other on the keyboard, many people accidentally type "apyware" when they try to search "spyware." Manufacturers and other interested parties capitalize on this by advertising "apyware."

MONEY LAUNDERING

Criminals accumulate significant sums of money by committing crimes such as drug trafficking, human trafficking, theft, investment fraud, extortion, corruption, embezzlement or tax fraud. Money laundering is a serious threat to the legitimate economy and threatens the integrity of financial institutions. It also has adverse effects on economic power in certain sectors or industries. If left unchecked, it will corrupt society as a whole. Fighting money laundering serves several purposes. Societal importance Crime causes tangible and intangible damage to third parties, individuals and society as a whole. Money laundering can result in reducing the public's confidence in certain professions such as lawyers, accountants and notaries and confidence in economic sectors such as real estate, hospitality and banks and other financial institutions. Investing the proceeds of crime may also distort competition between businesses and entrepreneurs. Money laundering allows the criminal to start, continue and expand activities in legitimate sectors of the economy. It may create a perception that crime pays and may incentivise people to start a criminal career. To identify tax crimes & other financial crimes unusual transactions can indicate tax crimes and lead to the identification of those involved. However, taxing the income of criminals according to tax rules alone will not stop crime from happening or from being profitable. The detection of unusual transactions may also assist in identifying criminals and illegal activities of theirs involving other financial crimes. Sharing information with law enforcement authorities can lead to the start of a criminal investigation. To locate and confiscate criminal assets Identifying unusual transactions can provide insight into the flow of money and the eventual conversion of laundered criminal proceeds into assets such as real estate, vehicles, yachts, bank accounts and virtual assets. This will assist law enforcement authorities in seizing those assets during a criminal investigation.

IDENTITY THEFT

The definition of identity theft is the unauthorized use of someone's personal data or documents (usually social security card or credit cards) to obtain merchandise, services or credit. The frightening reality is that could happen to anyone.

Consider that once identity thieves grab your personal information, they can empty your bank account, run up charges on your credit cards, open new utility accounts and even get medical treatment on your health insurance. They can file a tax refund in your name — and get your refund. They can obtain a driver's license, passport or immigration papers. They can open bank accounts, forge checks, apply for loans and credit cards and open insurance accounts. They can assume your identity on social media. They might even give your name to the police during an arrest, triggering a legal chain of events that could affect voluminous areas of life. The list of things thieves can do with your personal information is frighteningly endless. This is a very serious matter that deserves constant attention.

Cyberpornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyberpornography is a criminal offense, classified as causing harm to persons. This kind of freedom also enables the computer experts to indulge into other unlawful cyber criminal activities such as hacking, bugging, cheating, fraud, etc. With the regular use of internet in mold of websites and blogging, people engage themselves in chatting on the internet without knowing the other person. There are many elements that have given birth to the sources concerning about the society where the Pornography has been the major issue in the society.

Porn today is more freely and widely available on Internet than ever before. Younger generation is therefore able to access it very easily and quickly than ever. This leads to the mentality of unemotional sex. And all this is because we have grown up in a culture where parents feel embarrassed; they are not comfortable to have a healthy conversation about sex with their children.

Well then it's time to open up and come out of our comfort zone to talk about the most hush-hush topic i.e. Pornography.

EMAIL SPOOFING

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of authentication, it is commonplace for spam and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message. The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can cause significant problems, and sometimes pose a real security threat. As an example, a spoofed email may purport to be from a well-known retail business, asking the recipient to provide personal information like a password or credit card number. The fake email might even ask the recipient to click on a link offering a limited time deal, which is actually just a link to download and install malware on the recipient's device.

One type of phishing – used in business email compromise – involves spoofing emails from the CEO or CFO of a company who works with suppliers in foreign countries, requesting that wire transfers to the supplier be sent to a different payment location.

How Email Spoofing Works

Email spoofing is possible because the Simple Mail Transfer Protocol (SMTP) does not provide a mechanism for address authentication. Although email address authentication protocols and mechanisms have been developed to combat email spoofing, adoption of those mechanisms has been slow.

Reasons for Email Spoofing

Although most well-known for phishing purposes, there are actually several reasons for spoofing sender addresses. These reasons can include:

Hiding the sender's true identity – though if this is the only goal, it can be achieved more easily by registering anonymous mail addresses.

Avoiding spam blacklists. If a sender is spamming, they are bound to be blacklisted quickly. A simple solution to this problem is to switch email addresses.

Pretending to be someone the recipient knows, in order to, for example, ask for sensitive information or access to personal assets.

Pretending to be from a business the recipient has a relationship with, as means of getting ahold of bank login details or other personal data.

Tarnishing the image of the assumed sender, a character attack that places the so-called sender in a bad light.

Sending messages in someone's name can also be used to commit identity theft, for example, by requesting information from the victim's financial or healthcare accounts.

Email Spoofing Protections

Since the email protocol SMTP (Simple Mail Transfer Protocol) lacks authentication, it has historically been easy to spoof a sender address. As a result, most email providers have become experts at detecting and alerting users to spam, rather than rejecting it altogether. But several frameworks have been developed to allow authentication of incoming messages:

SPF (Sender Policy Framework): This checks whether a certain IP is authorized to send mail from a given domain. SPF may lead to false positives, and still requires the receiving server to do the work of checking an SPF record, and validating the email sender.

DKIM (Domain Key Identified Mail): This method uses a pair of cryptographic keys that are used to sign outgoing messages, and validate incoming messages. However, because DKIM is only used to sign specific pieces of a message, the message can be forwarded without breaking the validity of the signature. This is technique is referred to as a "replay attack".

DMARC (Domain-Based Message Authentication, Reporting, and Conformance): This method gives a sender the option to let the receiver know whether its email is protected by SPF or DKIM, and what actions to take when dealing with mail that fails authentication. DMARC is not yet widely used.

DENIAL-OF-SERVICE (DOS)

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack. A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

How does a DoS attack work?

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

DoS attacks typically fall in 2 categories:

Buffer overflow attacks: An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.

Flood attacks: By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

What are some historically significant DoS attacks?

Historically, DoS attacks typically exploited security vulnerabilities present in network, software and hardware design. These attacks have become less prevalent as DDoS attacks have a greater disruptive capability and are relatively easy to create given the available tools. In reality, most DoS attacks can also be turned into DDoS attacks.

A few common historic DoS attacks include:

Smurf attack - A previously exploited DoS attack in which a malicious actor utilizes the broadcast address of vulnerable network by sending spoofed packets, resulting in the flooding of a targeted IP address.

Ping flood - this simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.

Ping of Death - often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

CYBER STALKING

In the real world, stalking is unwanted obsessive attention to a specific person. Physical stalking can involve following, secret surveillance, persistent and manipulative calling and texting, and other means of approaching the victim unexpectedly.

In the digital world, cyber stalkers are driven by the same intention – to embarrass, threaten, or harass their victims. However, they primarily rely on online technology to do it. Email, social networks, instant messaging, personal data available online – everything on the Internet can be used by cyber stalkers to make inappropriate contact with their victims. Cyberstalking is way more serious as it involves nefarious intentions, ranging from false accusations and defamation to sexual harassment and even encouraging others to harass the victim. In many cases, physical and digital stalking interconnects, making it even more threatening.

1: Catfishing

Catfishing occurs on social media sites when online stalkers create fake user profiles and approach their victims as a friend of a friend or expressing romantic interest. To look more like a real person, cyber stalkers sometimes copy the profiles of existing users, impersonating their identities.

2: Monitoring location check-ins on social media

If you're adding location check-ins to your Facebook and Instagram posts, you're making it super easy for a cyber stalker to track you by simply scrolling through your social media profiles. When combined together, location-tagged posts can indicate your behavior patterns quite accurately.

3: Visiting you virtually via Google Maps Street View

If a cyber stalker discovers their victim's home address, all they have to do is open Google Maps and type it in. By using Street View, they can see exactly how your home looks without even stepping into your neighborhood and drawing attention. Cyber stalkers can also virtually research your environment, surrounding houses, cameras, and alleys, to get a sense about the neighbors.

4: Hijacking your webcam

Hijacking a computer's webcam is one of the creepiest methods cyberstalkers use to invade their victims' privacy. Creepers would try to trick you into downloading and installing a malware-infected file that would grant them access to your webcam.

REFERENCES:

www.javatpoint.com
www.studytonight.com
www.toppr.com
wikipedia.org
www.oricom.ca/en/support/malware,-viruses,-worms,-trojan-horses-and-spyware/
searchsecurity.techtarget.com/definition/spyware
www.techopedia.com/definition/23142/anti-spyware
www.int-comp.org/careers/your-career-in-aml/what-is-money-laundering/
www.debt.org/credit/identity-theft/
www.yourdictionary.com/cyberpornography
www.barracuda.com/glossary/email-spoofing