Table of Contents

Unit: One Introduction to Computer Network

A computer network is a system that connects numerous independent computers in order to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily.

A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

A computer network consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a computer network. Hostnames and network addresses are used to identify them.

1.1 Introduction to Computer Network

The computer network is defined as a set of interconnected autonomous systems that facilitate distributed processing of information. It results in better performance with a high speed of processing.

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

Criteria of good network:

1. **Performance:** It can be measured in many ways, including transmit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of the network depends on a number of factors, including the number of users, the type of medium & hardware
2. **Reliability:** In the addition to accuracy is measured by frequency of failure, the time it takes a link to recover from failure, and the network's robustness in catastrophe.
3. **Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data loss.

Goal of Networking:

- Programs do not have to execute on a single system because of resource and load sharing.
- Reduced costs: Multiple machines can share printers, tape drives, and other peripherals.
- Reliability: If one machine fails, another can take its place.
- Scalability: (it's simple to add more processors or computers)
- Communication and mail (people living apart can work together)
- Information Access (remote information access, access to the internet, e-mail, video conferencing, and online shopping)
- Entertainment that is interactive (online games, videos, etc.)
- Social Networking

1.2 Advantages and Disadvantages of Computer Network

Advantages of Network:

These are the main advantages of Computer Networks:

1. **Central Storage of Data:** Files can be stored on a central node (the file server) that can be shared and made available to each and every user in an organization.
2. **Anyone can connect to a computer network:** There is a negligible range of abilities required to connect to a modern computer network. The effortlessness of joining makes it workable for even youthful kids to start exploiting the data.
3. **Faster Problem-solving:** Since an extensive procedure is disintegrated into a few littler procedures and each is taken care of by all the associated gadgets, an explicit issue can be settled in lesser time.
4. **Reliability:** Reliability implies backing up information. Due to some reason equipment crashes, and so on, the information gets undermined or

inaccessible on one PC, another duplicate of similar information is accessible on another workstation for future use, which prompts smooth working and further handling without interruption.

5. **It is highly flexible:** This innovation is known to be truly adaptable, as it offers clients the chance to investigate everything about fundamental things, for example, programming without influencing their usefulness.
6. **Security through Authorization:** Security and protection of information are additionally settled through the system. As just the system clients are approved to get to specific records or applications, no other individual can crack the protection or security of information.
7. **It boosts storage capacity:** Since you will share data, records, and assets with other individuals, you need to guarantee all information and substance are legitimately put away in the framework. With this systems administration innovation, you can do the majority of this with no issue, while having all the space you require for capacity.

Disadvantages of Network:

These are the main disadvantages of Computer Networks:

1. **It lacks robustness:** If a PC system's principal server separates, the whole framework would end up futile. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To manage these issues, gigantic systems ought to have a ground-breaking PC to fill in as a document server to influence setting up and keeping up the system less demanding.
2. **It lacks independence:** PC organizing includes a procedure that is worked utilizing PCs, so individuals will depend on a greater amount of PC work, rather than applying an exertion for their jobs that needs to be done. Besides this, they will be subject to the primary document server, which implies that, in the event that it separates, the framework would end up futile, making clients inactive.
3. **Virus and Malware:** On the off chance that even one PC on a system gets contaminated with an infection, there is a possibility for alternate frameworks to get tainted as well. Infections can spread on a system effectively, in view of the availability of different gadgets.
4. **Cost of the network:** The expense of executing the system including cabling and equipment can be expensive.

1.3 Application of Computer Network

Computer network has proven to be most essential technology in todays world. Every field has taken advantage of this technology. The application areas of computer network can be summarized as follows:

1. Resource Sharing: Resource sharing is an application of a computer network. Resource sharing means you can share one Hardware and Software among multiple users. Hardware includes printers, Disks, Fax Machines, etc. Computing devices. And Software includes Atom, Oracle VM Virtual Box, Postman, Android Studio, etc.

2. Information Sharing: Using a Computer network, we can share Information over the network, and it provides Search capabilities such as WWW. Over the network, a single information can be shared among the many users over the internet.

3. Communication: Communication includes email, calls, message broadcast, electronic funds transfer system etc.

4. Entertainment Industry: In Entertainment industry also uses computer networks widely. Some of the Entertainment industries are Video on demand, Multi person real-time simulation games, movie/TV programs, etc.

5. Access to Remote Databases: Computer networks allow us to access the Remote Database of the various applications by the end-users. Some applications are Reservation for Hotels, Airplane Booking, Home Banking, Automated Newspaper, Automated Library etc.

6. Home applications: There are many common uses of the computer network are as home applications. For example, you can consider user -to-user communication, access to remote instruction, electronic commerce, and entertainment. Another way is managing bank accounts, transferring money to some other banks, paying bills electronically. A computer network arranges a robust connection mechanism between users.

7. Business applications: The result of business application here is resource sharing. And the purpose of resource sharing is that without moving to the physical location of the resource, all the data, plans, and tools can be shared to any network user. Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network .

8. Mobile users: The rapidly growing sectors in computer applications are mobile devices like notebook computers and PDAs (personal digital assistants). Here mobile users/device means portable device. The computer network is widely used in new-age technology like smartwatches, wearable devices, tablets, online transactions, purchasing or selling products online, etc.

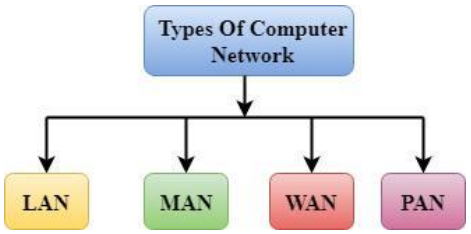
9. Social media: Social media is also a great example of a computer network application. It helps people to share and receive any information related to political, ethical, and social issues.

Unit: Two Network Types and Topologies

2.1. Introduction to 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)



2.2. Types of Network

LAN (Local Area Network)

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

- 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

There are various advantages of LAN, which are as follows:

- Inexpensive transmission media.
- It can simplify the physical association of a device to the media.
- It is used to high data transmission rates.
- Network data transmission is independent of the connected devices rates, making it accessible for the one-speed device to send data to another speed device.
- A large rate of interconnection between devices.
- Each connected device has the potential to interact with another device on the network.
- It is flexible and growth-oriented.
- It allows file locking.
- It provides full proof of the security system against illegal access to data.
- LANs are a productivity tool. In the case of business, a LAN should be an apparent contributor to raised profitability.

Disadvantages of LAN

There are various disadvantages to LAN, which are as follows

- LAN software needed a memory area in each of the mainframe used on the network. This decreases the memory space available for the user's program.
- Local area networking adds another phase of difficulty to the computer operation. Users can have a problem in understanding the network commands. The installation and authority of a LAN require far more technical and regulatory skills than installing and handling multiple computers that are not networked.
- Some security system should be executed if it is essential to protect private data.
- Some control on the part of the customer is lost. We have to share a printer with different customers.
- Some current application programs will not run in a network environment.

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.
- Personal Area Network covers an area of **30 feet**.

- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

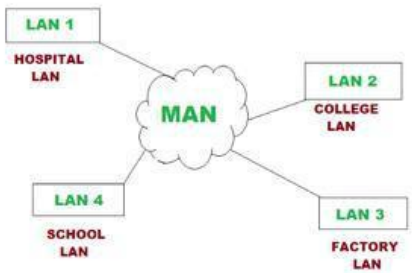
There are two types of Personal Area Network:

- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

MAN (Metropolitan Area Network)



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

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.

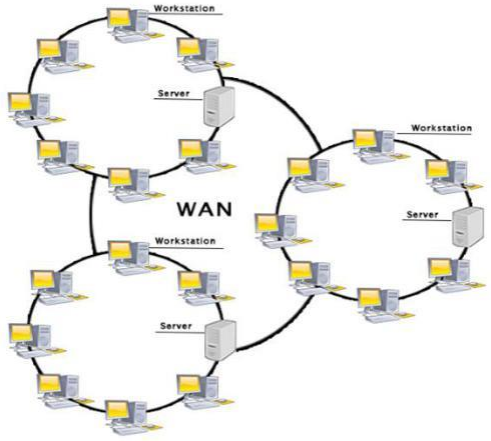
Advantages of MAN:

- It provides higher security compare to WAN
- It is wider than LAN
- It helps in cost-effective sharing of common resources such as printer etc.
- MAN require fewer resources compare to WAN. This saves the implementation cost
- The dual bus used in MAN help the transmission of data in both directions simultaneously
- It provides a good backbone for a large network and also provides greater access to WAN
- Increases the efficiency of handling data
- Increases the speed of transfer data
- Easy to implement link
- Save the cost attach to establish a wide area network

Disadvantages of MAN:

- More cable requires for a MAN connection from one place to another
- The data rate is slow compared to LAN
- It is difficult to make a system secure from hackers
- The large network difficult to manage
- Network installation require skilled technicians and network administrators. This increases overall installation and management costs
- Cost is higher than LAN
- While we move our network to another city or area it doesn't work

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, 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, 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.

Internetwork

An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**. An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**. An internetworking uses the **internet protocol**.

Types of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those

users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, at least it must have one connection to the external network.

2. Intranet: An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

2.3. Introduction to Network Topology

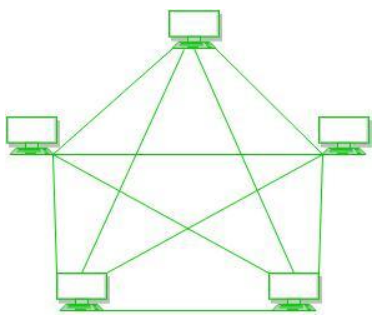
The arrangement of a network which comprises of nodes and connecting lines via sender and receiver is referred as network topology. The various network topologies are:

1. Mesh Topology
2. Star Topology
3. Bus Topology
4. Ring Topology

2.4. Types of Network Topology

a) Mesh Topology:

In mesh topology, every device is connected to another device via particular channel.



- If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is N-1. In the Figure 1, there are 5 devices connected to each other, hence total number of ports required is 4.
- If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is ${}^{N}C_2$ i.e. N(N-1)/2. In the Figure 1, there are 5 devices connected to each other, hence total number of links required is 5*4/2 = 10.

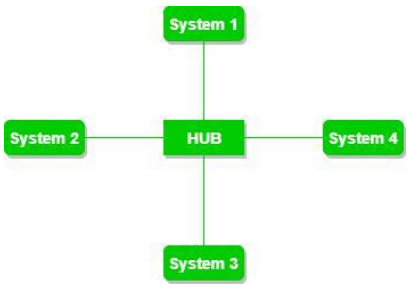
Advantages of mesh topology:

- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Problems with mesh topology:

- Installation and configuration are difficult.
- Cost of cables are high as bulk wiring is required, hence suitable for a smaller number of devices.
- Cost of maintenance is high.

b) Star Topology:



In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node. The hub can be passive in nature i.e. not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active hubs. Active hubs have repeaters in them.

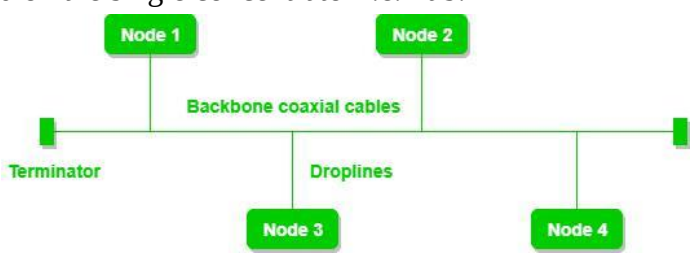
Advantages of star topology:

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub.

Problems with star topology:

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

c) Bus Topology:



Bus topology is a network type in which every computer and network device is connected to single

cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

Advantages of this topology:

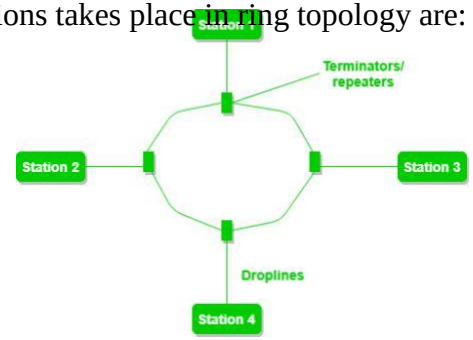
- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1? which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to build small networks.

Problems with this topology:

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

d) Ring Topology:

In this topology, it forms a ring connecting a device with its exactly two neighboring devices. The following operations takes place in ring topology are:



1. One station is known as **monitor** station which takes all the responsibility to perform the operations.
2. To transmit the data, station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after the transmitting the data and **Delay token release** releases the token after the acknowledgement is received from the receiver.

Advantages of ring topology:

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Problems with ring topology:

- Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

Unit: Three Network Device and Transmission Media

3.1 Introduction to various Network Devices and Tools

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub: -** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub: -** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

Types of Bridges

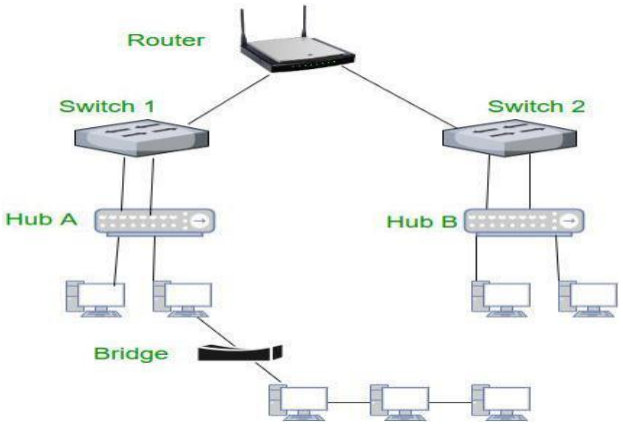
- **Transparent Bridges: -** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges: -** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. Brouter – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.



3.2 Introduction to Transmission Media

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signal travel through vacuum, air or other transmission mediums to travel between one point to another (from source to receiver).

Factors to be considered while choosing Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environment Conditions
4. Distances

3.3 Types of Transmission Media

Transmission media can be broadly divided into two categories:

Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/Guided are discussed below.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points:

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1 kHz.
- Typical delay is 50μs/km.
- Repeater spacing is 2km.

Twisted pair is of two types:

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

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation. An UTP cable consists of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.

Advantages:

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages:

- Bandwidth is low when compared with Co-axial Cable
- Provides less protection from interference.
- 100-meter limit.

Shielded Twisted Pair Cable

The cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk. It has same attenuation as unshielded twisted pair. It is faster the unshielded and co-axial cable. It is more expensive than co-axial an unshielded twisted pair.

Disadvantages:

- Difficult to manufacture
- Heavy

Advantage:

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signaling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Coaxial cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be solid wire or a standard one. it is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, braid or both. Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable. Here the most common coaxial standard.

- 50-Ohm RG-$_{7}$ or RG-$_{11}$: used with thick Ethernet.
- 50-Ohm RG-5^{8} :used with thin Ethernet.
- 75-Ohm RG-59 : used with cable television.
- 93-Ohm RG-62 : used with ARCNET.

There are two types of coaxial cables.

Base band

This is 50 ohm (Ω) coaxial cable which is used for digital transmission. It's mostly used for LAN's; Baseband transmit a single signal at a time with very high speed the major drawback is that it needs amplification after every 1000 feet.

Broad band

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signals using different frequencies. It covers large area when compared with baseband coaxial cable.

Advantages

- Bandwidth is high.
- Used in long distance telephone signal.
- Transmits digital signals at a very high rate of $_{10}$mbps.
- Much higher noise immunity.
- Data transmission without distortion.
- the can span to longer distance at higher speed as they have better shielding when compared to twisted pair cable

Disadvantage

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

Fiber optic cable

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates. In multimode fibres the core is 50 microns and in single mode fibres the thickness is 8 to 10 microns. The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fiber is grouped together in bundles protected by an outer shield. Fiber optic cable has bandwidth more than 2 GBps (Gigabytes per second)

Advantages

- Provides high quality transmission of signal at very high speed.
- These are not affected by electromagnetic interference so noise and distortion is very less.
- Used for both analog and digital signals.

Disadvantages

- It is expensive.
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

Unbounded/Unguided Transmission Media

Unguided or wireless media sends the data through air(or water), which is available to anyone who has a device capable of receiving them. Types of unguided /unbounded media are discussed below:

- Radio Transmission
- Micro Wave Transmission

Radio Transmission

Its frequency is between 10 kHz to 1 GHz. It is simple to install and has high attenuation. These waves are used for multicast communication.

Types of propagation Radio Transmission utilizes different types of propagation:

- ***Troposphere***: The lowest portion of earth's atmosphere extending outward approximately 30 miles from the earth's surface. Clouds, jet plane, wind is found here.
- ***Ionosphere***: the layer of the atmosphere above troposphere, but below space. Contains electrically charged particles.

Microwave Transmission

If signal travels at high frequency than the radio waves it requires the sender to be inside the receiver. It operates in a system with a low gigahertz range. It is mostly used for unicast communication. There are two types of microwave communication.

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of microwave Transmission

- Used for long distance telephone communication.
- Carries 1000's of voice channels at same time.

Disadvantages of microwave Transmission

- It is very costly.

Terrestrial Microwave

For increasing the distance served by terrestrial microwave repeaters can be installed with each antenna. The signals received by an antenna can be converted into transmittable form and relayed to next antenna as shown in fig below. It is an example of telephone system all over the world. There are two types of antennas used for terrestrial microwave communication: Parabolic and Horn

1. Parabolic Dish Antenna

In this line parallel to the line of symmetry reflects off the curve at angles in that they intersect at a common point called focus. This antenna is based on geometry of parabola.

2. Horn Antenna

It is like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.

Satellite Microwave

This is microwave relay station which is placed in outer space. The satellite are launched either by rocket or space shuttles carry them. These are positioned 3600KM above the equator with the orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationary relative earth and always stays over the same point on the ground. This is usually done to allow stat to aim antenna at a fixed point in the sky

Features of satellite microwave

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages Of Satellite Microwave

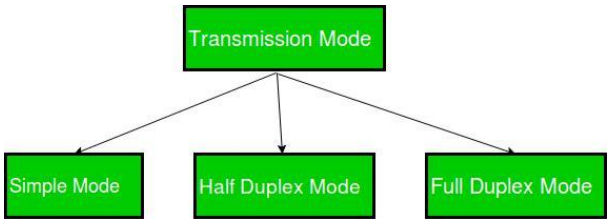
- Transmitting station can receive back its own transmission and check whether the satellite transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantage of Satellite Microwave

- Satellite manufacturing cost is very high.
- Cost of launching satellite is very expensive.
- Transmission highly depends on whether conditions, it can go down in bad weather

3.4 Transmission Modes

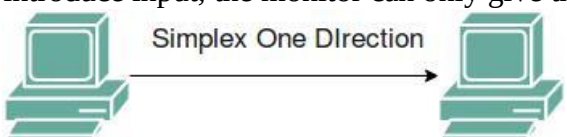
Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode: -



Simplex Mode

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

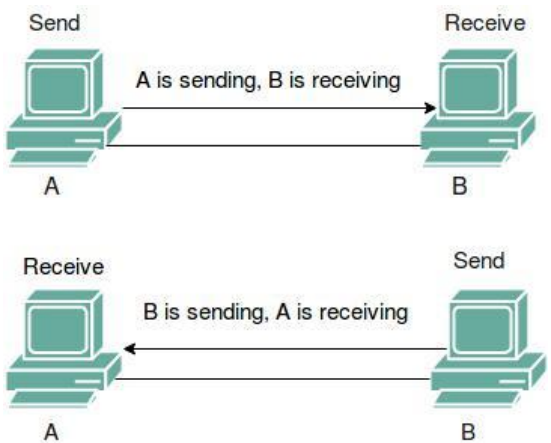
Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



Half-Duplex Mode

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



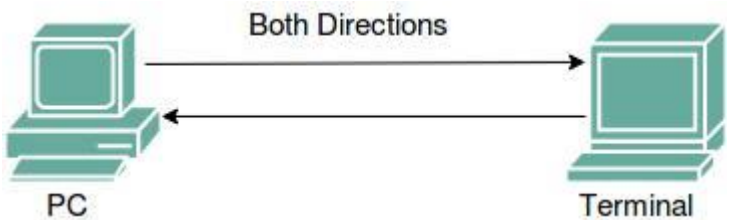
Full-Duplex Mode

In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- Or the capacity is divided between signals travelling in both directions.

Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two directions.

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



Unit: Four Network Architecture

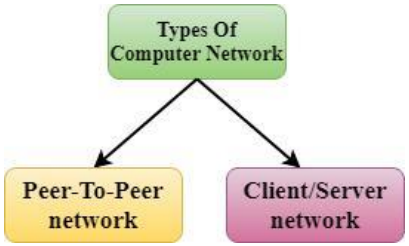
4.1 Introduction to Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

4.2 Types of Network Architecture

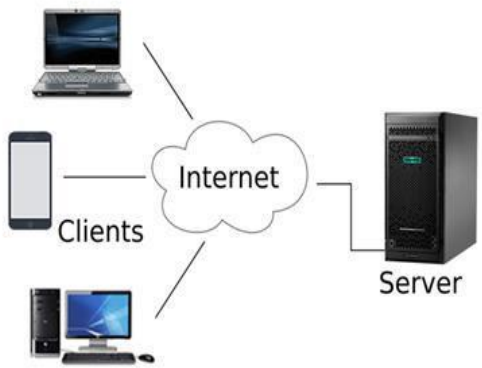
The two types of network architectures are:

- Peer-To-Peer network
- Client/Server network



4.3 CSA, Advantages and Disadvantages

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages of Client/Server network:

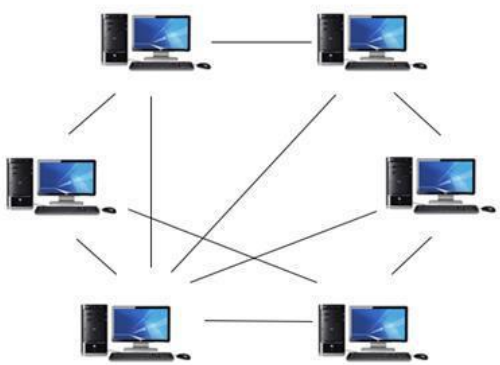
- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

4.4 P2P, Advantages and Disadvantages

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working. ○ It is easy to set up and maintain as each computer manages itself.

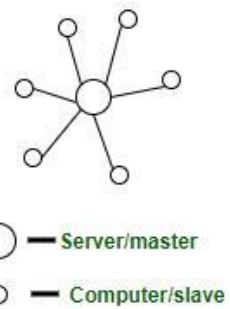
Disadvantages of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself

4.5 Centralized, Decentralized and Distributed Network

1. CENTRALIZED SYSTEMS:

Centralized systems are systems that use client/server architecture where one or more client nodes are directly connected to a central server. This is the most commonly used type of system in many organizations where a client sends a request to a company server and receives the response.



Architecture of Centralized System Client-Server architecture. The central node that serves the other nodes in the system is the server node and all the other nodes are the client nodes.

Example – Consider a massive server to which we send our requests and the server responds with the article that we requested. Suppose we enter the search term 'junk food' in the Wikipedia search bar. This search term is sent as a request to the Wikipedia servers (mostly located in Virginia, U.S.A) which then responds back with the articles based on relevance. In this situation, we are the client node, Wikipedia servers are the central server.

Characteristics of Centralized System

- **Presence of a global clock:** As the entire system consists of a central node (a server/ a master) and many client nodes (a computer/ a slave), all client nodes sync up with the global clock (the clock of the central node).
- **One single central unit:** One single central unit which serves/coordinates all the other nodes in the system.
- **Dependent failure of components:** Central node failure causes the entire system to fail. This makes sense because when the server is down, no other entity is there to send/receive responses/requests.

Scaling – Only vertical scaling on the central server is possible. Horizontal scaling will contradict the single central unit characteristic of this system of a single central entity.

Components of Centralized System –

Components of Centralized System are,

- Node (Computer, Mobile, etc.).
- Server.
- Communication link (Cables, Wi-Fi, etc.).

Limitations of Centralized System –

- Can't scale up vertically after a certain limit – After a limit, even if you increase the hardware and software capabilities of the server node, the performance will not increase appreciably leading to a cost/benefit ratio < 1.

- Bottlenecks can appear when the traffic spikes – as the server can only have a finite number of open ports to which can listen to connections from client nodes. So, when high traffic occurs like a shopping sale, the server can essentially suffer a Denial-of-Service attack or Distributed Denial-of-Service attack.

Advantages of Centralized System

- Easy to physically secure. It is easy to secure and service the server and client nodes by virtue of their location
- Smooth and elegant personal experience – A client has a dedicated system which he uses (for example, a personal computer) and the company has a similar system which can be modified to suit custom needs
- Dedicated resources (memory, CPU cores, etc)
- More cost-efficient for small systems up to a certain limit – As the central systems take fewer funds to set up, they have an edge when small systems have to be built
- Quick updates are possible – Only one machine to update.
- Easy detachment of a node from the system. Just remove the connection of the client node from the server and voila! Node detached.

Disadvantages of Centralized System

- Highly dependent on the network connectivity – The system can fail if the nodes lose connectivity as there is only one central node.
- No graceful degradation of the system – abrupt failure of the entire system
- Less possibility of data backup. If the server node fails and there is no backup, you lose the data straight away
- Difficult server maintenance – There is only one server node and due to availability reasons, it is inefficient and unprofessional to take the server down for maintenance. So, updates have to be done on-the-fly(hot updates) which is difficult and the system could break.

Applications of Centralized System

- Application development – Very easy to set up a central server and send client requests. Modern technology these days do come with default test servers which can be launched with a couple of commands. For example, Express server, Django server.
- Data analysis – Easy to do data analysis when all the data is in one place and available for analysis
- Personal computing

Uses

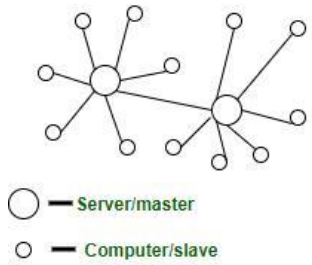
- Centralized databases – all the data in one server for use.
- Single-player games like Need For Speed, GTA Vice City – an entire game in one system (commonly, a Personal Computer)
- Application development by deploying test servers leading to easy debugging, easy deployment, easy simulation
- Personal Computers

Organizations Using: National Informatics Center (India), IBM

2. DECENTRALIZED SYSTEMS:

In decentralized systems, every node makes its own decision. The final behavior of the system is the aggregate of the decisions of the individual nodes. Note that there is no single entity that receives and responds to the request.

Architecture of Decentralized System



- peer-to-peer architecture – all nodes are peers of each other. No one node has supremacy over other nodes
- master-slave architecture – One node can become a master by voting and help in coordinating of a part of the system but this does not mean the node has supremacy over the other node which it is coordinating

Example – Bitcoin. Let's take Bitcoin for example because it is the most popular use case of decentralized systems. No single entity/organization owns the bitcoin network. The network is a sum of all the nodes who talk to each other for maintaining the amount of bitcoin every account holder has.

Characteristics of Decentralized System

- **Lack of a global clock:** Every node is independent of each other and hence, has different clocks that they run and follow.
- **Multiple central units (Computers/Nodes/Servers):** More than one central unit which can listen for connections from other nodes
- **Dependent failure of components:** one central node failure causes a part of the system to fail; not the whole system

Scaling – Vertical scaling is possible. Each node can add resources (hardware, software) to itself to increase the performance leading to an increase in the performance of the entire system.

Components

Components of Decentralized System are,

- Node (Computer, Mobile, etc.)
- Communication link (Cables, Wi-Fi, etc.)

Limitations of Decentralized System –

- May lead to the problem of coordination at the enterprise level – When every node is the owner of its own behavior, its difficult to achieve collective tasks

- Not suitable for small systems – Not beneficial to build and operate small decentralized systems because of the low cost/benefit ratio
- No way to regulate a node on the system – no superior node overseeing the behavior of subordinate nodes

Advantages of Decentralized System

- Minimal problem of performance bottlenecks occurring – The entire load gets balanced on all the nodes; leading to minimal to no bottleneck situations
- High availability – Some nodes (computers, mobiles, servers) are always available/online for work, leading to high availability
- More autonomy and control over resources – As each node controls its own behavior, it has better autonomy leading to more control over resources

Disadvantages of Decentralized System

- Difficult to achieve global big tasks – No chain of command to command others to perform certain tasks
- No regulatory oversight
- Difficult to know which node failed – Each node must be pinged for availability checking and partitioning of work has to be done to actually find out which node failed by checking the expected output with what the node generated
- Difficult to know which node responded – When a request is served by a decentralized system, the request is actually served by one of the nodes in the system but it is actually difficult to find out which node indeed served the request.

Applications of Decentralized System

- Private networks – peer nodes joined with each other to make a private network.
- Cryptocurrency – Nodes joined to become a part of a system in which digital currency is exchanged without any trace and location of who sent what to whom. However, in bitcoin, we can see the public address and amount of bitcoin transferred, but those public addresses are mutable and hence difficult to trace.

Uses

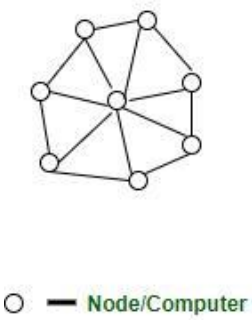
- Blockchain
- Decentralized databases – Entire databases split into parts and distributed to different nodes for storage and use. For example, records with names starting from 'A' to 'K' in one node, 'L' to 'N' in the second node, and 'O' to 'Z' in the third node
- Cryptocurrency

Organizations Using: Bitcoin, Tor network

3. DISTRIBUTED SYSTEMS:

A distributed system is a collection of computer programs that utilize computational resources across multiple, separate computation nodes to achieve a common, shared goal. Also known as distributed computing or distributed databases, it relies on separate nodes to communicate and synchronize over a common network. These nodes typically represent separate physical hardware devices but can also represent separate software processes, or other recursive encapsulated systems. Distributed systems aim to remove bottlenecks or central points of failure from a system.

The architecture of Distributed System



- peer-to-peer – all nodes are peers of each other and work towards a common goal
- client-server – some nodes become server nodes for the role of coordinator, arbiter, etc.
- n-tier architecture – different parts of an application are distributed in different nodes of the systems and these nodes work together to function as an application for the user/client

Example: Google search system. Each request is worked upon by hundreds of computers that crawl the web and return the relevant results. To the user, Google appears to be one system, but it actually is multiple computers working together to accomplish one single task (return the results to the search query).

Characteristics of Distributed System

- **Resource sharing:** A distributed system can share hardware, software, or data
- **Simultaneous processing:** Multiple machines can process the same function simultaneously
- **Scalability:** The computing and processing capacity can scale up as needed when extended to additional machines
- **Error detection:** Failures can be more easily detected
- **Transparency:** A node can access and communicate with other nodes in the system

Components of Distributed System

The components of Distributed System are,

- Node (Computer, Mobile, etc.)
- A communication link (Cables, Wi-Fi, etc.)

Limitations of Distributed System

- Difficult to design and debug algorithms for the system. These algorithms are difficult because of the absence of a common clock; so, no temporal ordering of commands/logs can take place. Nodes can have different latencies which have to be kept in mind while designing such algorithms. The complexity increases with the increase in the number of nodes. Visit this link for more information
- No common clock causes difficulty in the temporal ordering of events/transactions
- Difficult for a node to get the global view of the system and hence take informed decisions based on the state of other nodes in the system

Advantages of Distributed System –

- Low latency than a centralized system – Distributed systems have low latency because of high geographical spread, hence leading to less time to get a response

Disadvantages of Distributed System

- Difficult to achieve consensus
- The conventional way of logging events by absolute time they occur is not possible here

Applications of Distributed System

- Cluster computing – a technique in which many computers are coupled together to work so that they achieve global goals. The computer cluster acts as if they were a single computer
- Grid computing – All the resources are pooled together for sharing in this kind of computing turning the systems into a powerful supercomputer; essentially.

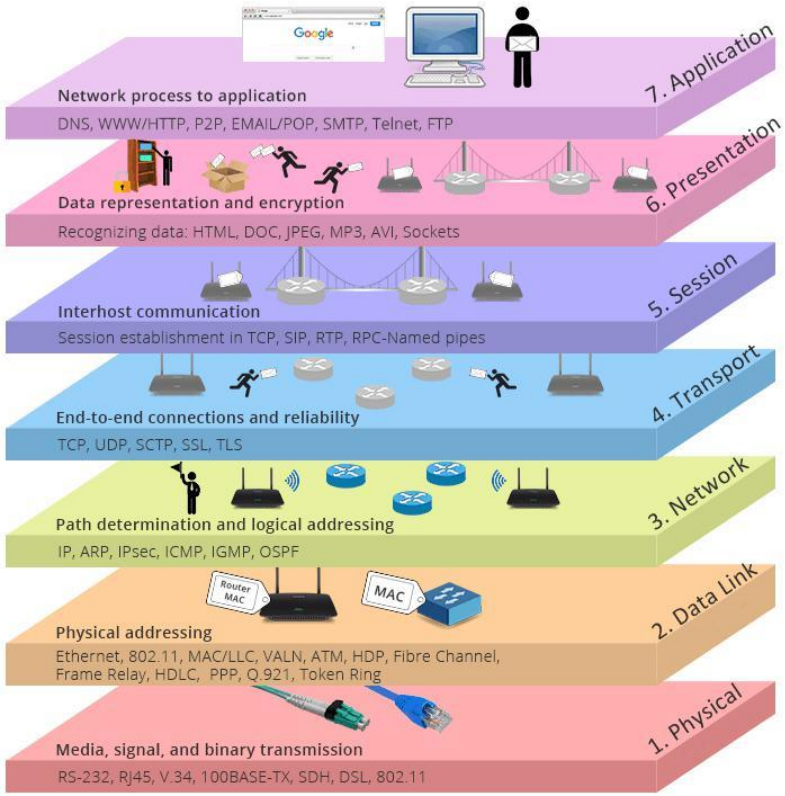
Uses

- SOA-based systems
- Multiplayer online games

Organizations Using Apple, Google, Facebook.

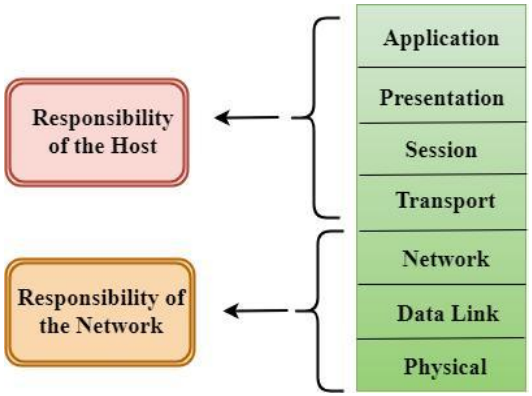
Unit: Five Reference Model and IP Addressing

5.1 OSI Reference Model



- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:

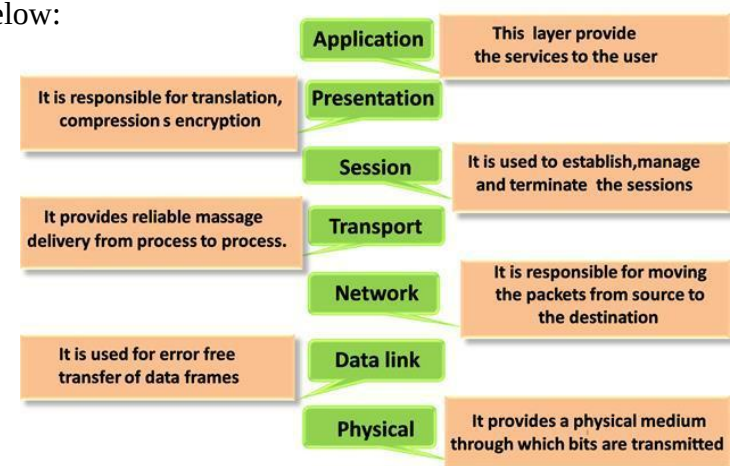


- The OSI model is divided into two layers: upper layers and lower layers.
  - The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

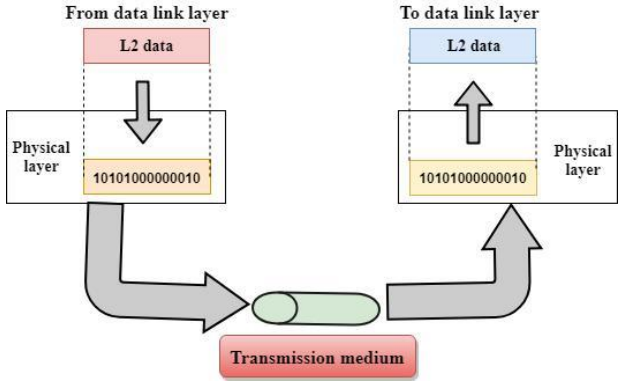
7 Layers of OSI Model

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

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



1) Physical layer

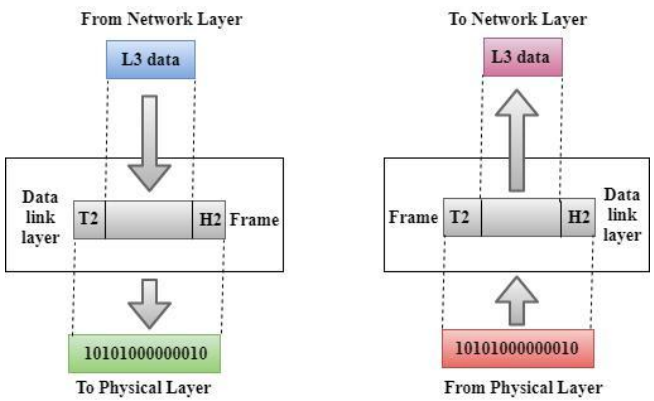


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a 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



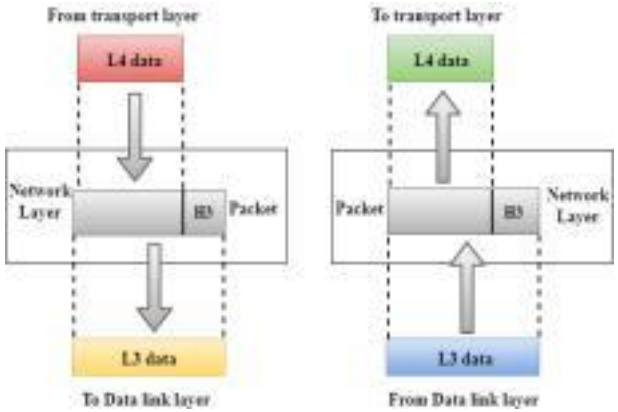
- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
  - **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  - **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the 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 occur, 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

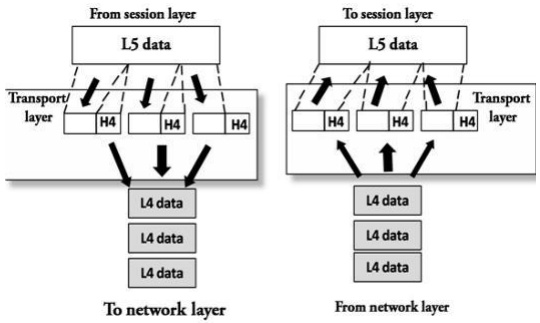


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of 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



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- It provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

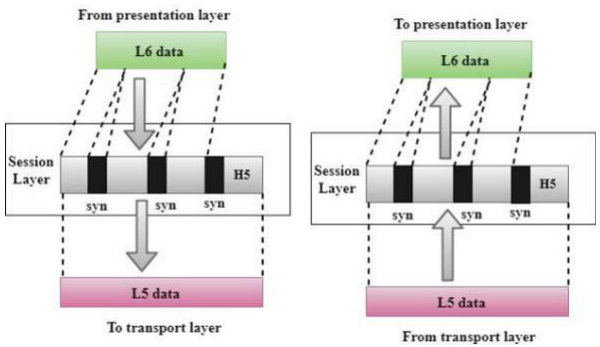
- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the 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

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

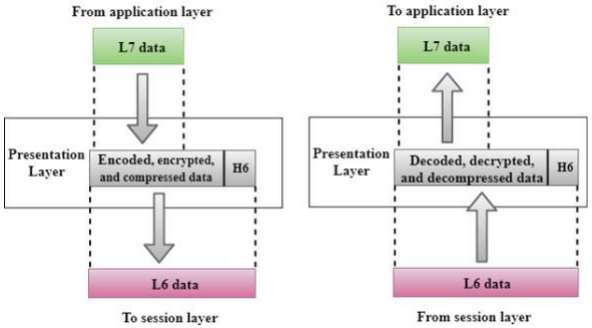


Functions of Session layer:

- **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

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

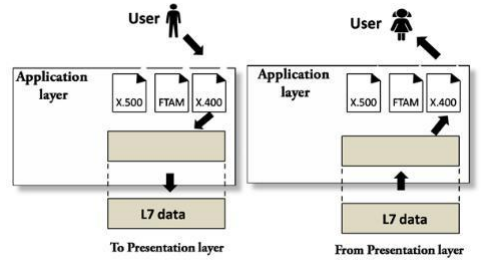


Functions of Presentation layer:

- **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

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

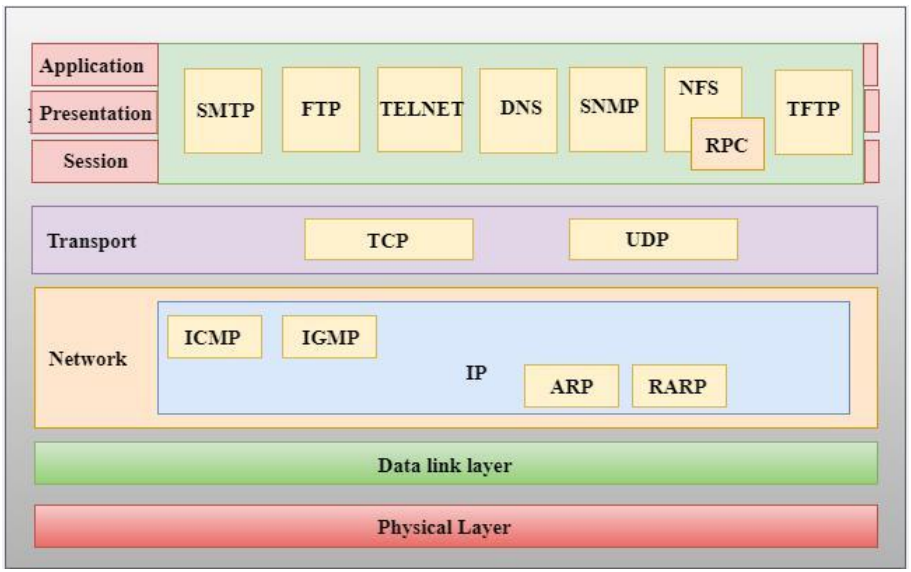


Functions of Application layer:

- **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.

5.2 TCP/IP Reference Model



- 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.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:

The functions of each layers of TCP/IP are as follows:

Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in

application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

5.3 Introduction to Protocols

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- **UDP consists of the following fields:**

  Source port address: The source port address is the address of the application program that has created the message.

  Destination port address: The destination port address is the address of the application program that receives the message.

Total length: It defines the total number of bytes of the user datagram in bytes.

Checksum: The checksum is a 16-bit field used in error detection.

- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

5.4 IP Address and its Class

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

An IP address is represented by a series of numbers segregated by periods(.). They are expressed in the form of four pairs - an example address might be 255.255.255.255 wherein each set can range from 0 to 255. IP addresses are not produced randomly. They are generated mathematically and are further assigned by the IANA (Internet Assigned Numbers Authority), a department of the ICANN.

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

1. Public IP Address: This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses are of two types,

- **Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IP Addresses. Now, your device has an IP Address and you can simply connect your device to the Internet and send and receive data to and from your device. The very next time when you try to connect to the internet with the same device, your provider provides you with different IP Addresses to the same device and also from the same available range. Since IP Address keeps on changing every time when you connect to the internet, it is called a Dynamic IP Address.
- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are used by DNS servers. What are DNS servers? Actually, these are computers that help you to open a website on your computer. Static IP Address provides information such as device is located on which continent, which country, which city, and which Internet Service Provider provides internet connection to that particular device. Once, we know who is the ISP, we can trace the location of the device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

2. Private IP Address: This is an internal address of your device which are not routed to the internet and no exchange of data can take place between a private address and the internet.

3. Shared IP addresses: Many websites use shared IP addresses where the traffic is not huge and very much controllable, they decide to rent it to other similar websites so to make it cost-friendly. Several companies and email sending servers use the same IP address (within a single mail server) to cut down the cost so that they could save for the time the server is idle.

4. Dedicated IP addresses: A dedicated IP Address is an address used by a single company or an individual which gives them certain benefits using a private Secure Sockets Layer (SSL) certificate which is not in the case of a shared IP address. It allows to access the website or log in via File Transfer Protocol (FTP) by IP address instead of its domain name. It increases the performance of the website when the traffic is high. It also protects from a shared IP address that is black-listed due to spam.

5.5 IPv4 Addressing

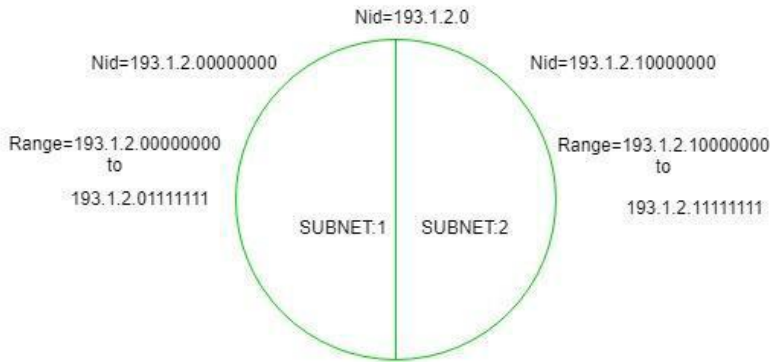
IPv4: Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4.
IPv4 can be written as: *189.123.123.90*

Classes of IPv4 Address: There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let's understand it with a simple example. If you have to find a word from a language dictionary, how long will it take? Usually, you will take less than 5 minutes to find that word. You are able to do this because words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionary that doesn't use any sequence or order to organize the words, it will take an eternity to find the word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses. For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes:

IP Class	Address Range	Maximum number of networks
Class A	0-126	126 (2^7-2)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

5.6 Sub netting

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 2^{24} for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts. **Now, let's talk about dividing a network into two parts:** To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets. **Note:** It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

Subnetting for a network should be done in such a way that it does not affect the network bits. In class C the first 3 octets are network bits so it remains as it is.

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

193.1.2.0 to 193.1.2.127

Subnet id of Subnet-1 is: 193.1.2.0

Direct Broadcast id of Subnet-1 is: 193.1.2.127

Total number of host possible is: 126 (Out of 128, 2 id's are used for Subnet id and Direct Broadcast id)

Subnet mask of Subnet- 1 is: 255.255.255.128

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

193.1.2.128 to 193.1.2.255

Subnet id of Subnet-2 is: 193.1.2.128

Direct Broadcast id of Subnet-2 is: 193.1.2.255

Total number of host possible is: 126 (Out of 128, 2 id's are used for Subnet id and Direct Broadcast id)

Subnet mask of Subnet- 2 is: 255.255.255.192

Finally, after using the subnetting the total number of usable hosts are reduced from 254 to 252.

5.7 Introduction to IPv6

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols. For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000111000
1101111111100001 0000000001100011 0000000000000000
0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

- **Rule 1:** Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

- **Rule 2:** If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

2001:0000:3238:DFE1:63::FEFB

- **Rule 3:** Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

Unit: Six Workgroup Computing

6.1 Introduction to workgroup

6.2 Components of workgroup

6.3 Types of workgroup

6.4 Advantages and Disadvantages of workgroup

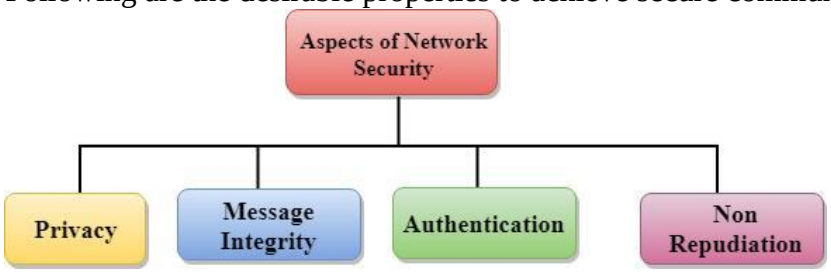
6.5 Application of workgroup

Unit: Seven Network Security

7.1 Introduction to Network Security

Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many **cyber threats**. The most basic example of Network Security is password protection which the user of the network oneself chooses.

Aspects of Network Security:
Following are the desirable properties to achieve secure communication:



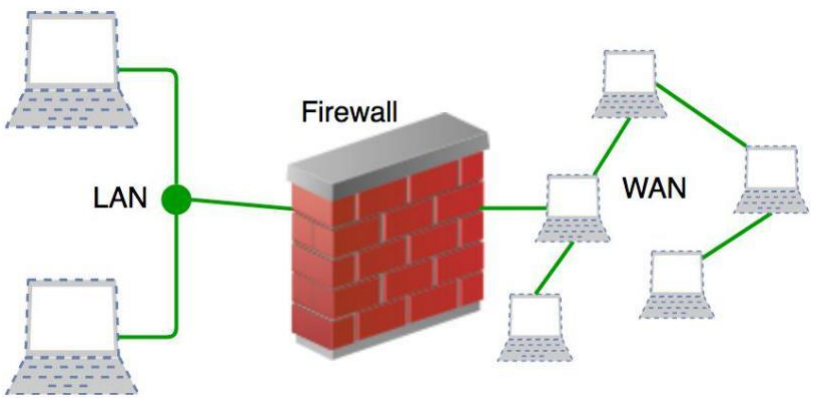
- **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
- **End-point authentication:** Authentication means that the receiver is sure of the sender's identity, i.e., no imposter has sent the message.
- **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

7.2 Types of Network Security

7.2.1 Firewall Protection

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic. **Accept:** allow the traffic
Reject: block the traffic but reply with an "unreachable error"
Drop: block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



How Firewall Works
Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined

like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

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

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Types of Firewall

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

1. **Host- based Firewalls:** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls:** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

7.2.2 Email Security

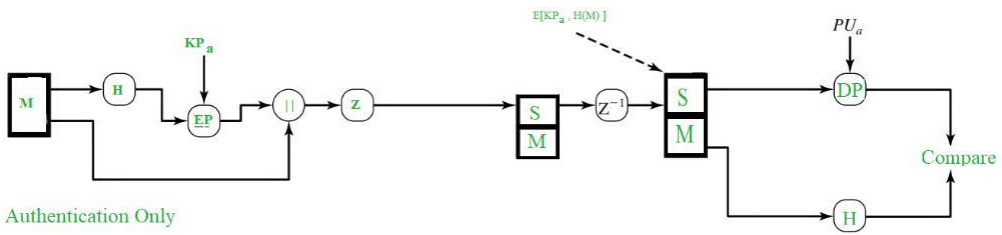
PGP (Pretty Good Privacy), is a popular program that is used to provide confidentiality and authentication services for electronic mail and file storage. It was designed by **Phil Zimmermann** way back in 1991. PGP software is an open source one and is not dependent on either the OS (Operating System) or the processor. The application is based on a few commands which are very easy to use. The following are the services offered by PGP:

1. Authentication 2. Confidentiality 3. Compression
4. Email Compatibility 5. Segmentation

In this article, we will see about Authentication and Confidentiality.

1. Authentication:

Authentication basically means something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password, that is an authentication verification procedure. In the email world, checking the authenticity of an email is nothing but to check *whether it actually came from the person it says*. In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience. The Authentication service in PGP is provided as follows:

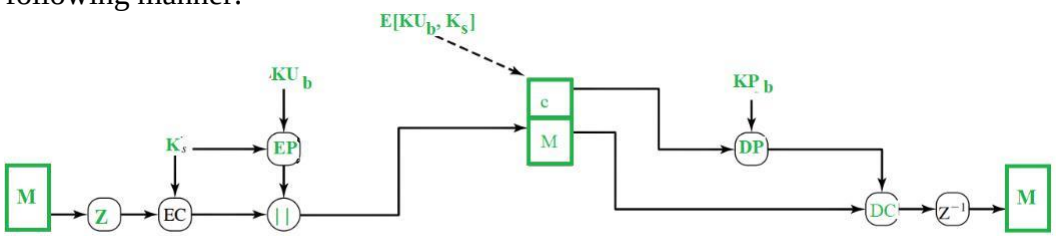


As shown in the above figure, the Hash Function (H) calculates the Hash Value of the message. For the hashing purpose, **SHA-1** is used and it produces a **160 bit** output hash value. Then, using the sender's private key (KP_a), it is encrypted and it's called as **Digital Signature**. The Message is then appended to the signature. All the process happened till now, is sometimes described as *signing the message* . Then the message is compressed to reduce the transmission overhead and is sent over to the receiver.

At the receiver's end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender's public key (PU_a) and the hash value is obtained. The message is again passed to hash function and it's hash value is calculated and obtained. Both the values, one from signature and another from the recent output of hash function are compared and if both are same, it means that the email is actually sent from a known one and is legit, else it means that it's not a legit one.

2. Confidentiality:

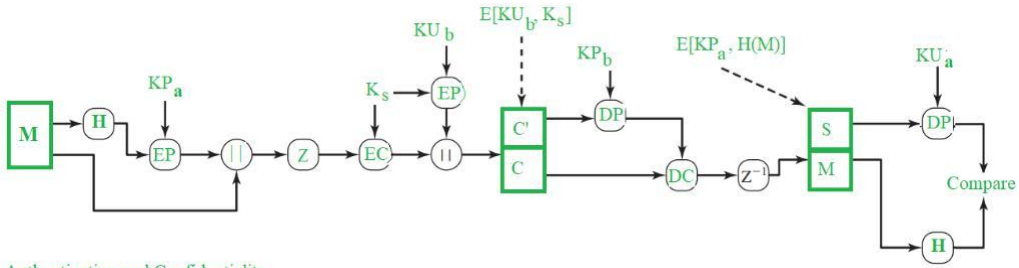
Sometimes we see some packages labelled as 'Confidential', which means that those packages are not meant for all the people and only selected persons can see them. The same applies to the email confidentiality as well. Here, in the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two. PGP provides that Confidentiality service in the following manner:



Only Confidentiality

The message is first compressed and a 128-bit session key (K_s), generated by the PGP, is used to encrypt the message through symmetric encryption. Then, the session key (K_s) itself gets encrypted through public key encryption (EP) using receiver's public key (KU_b). Both the encrypted entities are now concatenated and sent to the receiver.

At the receiver's end, the encrypted session key is decrypted using receiver's private key (KP_b) and the message is decrypted with the obtained session key. Then, the message is decompressed to obtain the original message (M). RSA algorithm is used for the public-key encryption and for the symmetric key encryption, CAST-128(or IDEA or 3DES) is used. Practically, **both** the Authentication and Confidentiality services are provided in parallel as follows:



Authentication and Confidentiality

Note:

M – Message
H – Hash Function
K_s – A random Session Key created for Symmetric Encryption purpose
DP – Public-Key Decryption Algorithm
EP – Public-Key Encryption Algorithm
DC – Asymmetric Decryption Algorithm
EC – Symmetric Encryption Algorithm
KP_b – A private key of user B used in Public-key encryption process
KP_a – A private key of user A used in Public-key encryption process
PU_a – A public key of user A used in Public-key encryption process
PU_b – A public key of user B used in Public-key encryption process
|| – Concatenation
Z – Compression Function
Z^{-1} – Decompression Function

7.2.3 Antivirus and Antimalware Software

Antivirus is a type of software program that helps in protecting the computer system from viruses. It detects the viruses in the computer system and destroys them. It protects the computer system from specific malware. It is used for protection from some traditional and simple threats that can harm the computer system. It is mostly used in personal computers for safety purposes. **Example:** Avast, QuickHeal, AVG

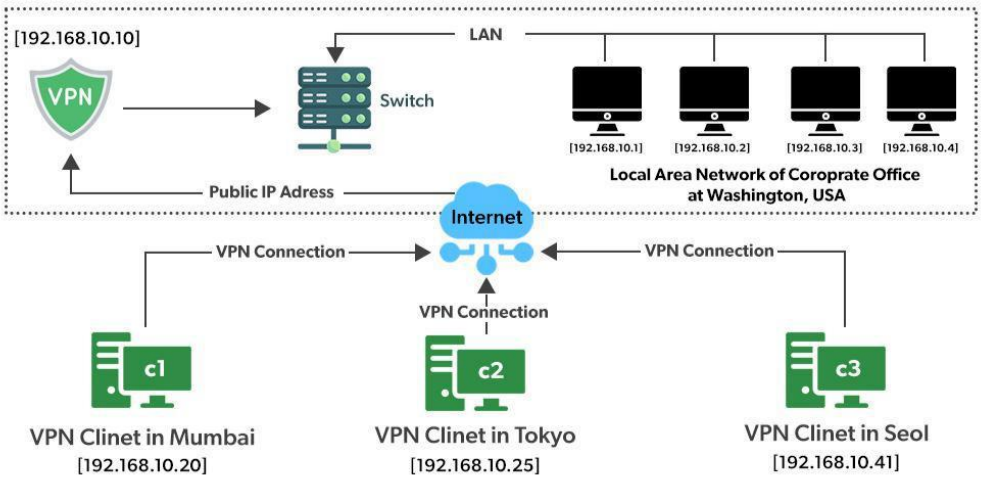
Antimalware:

Antimalware is also a software program but it protects the computer systems from all kinds of malware i.e., viruses, trojans, worms, etc. It protects the computer system from all kinds of malware. It is used for protection from some

new, sophisticated, and more dangerous threats that can harm the computer system. It is mostly used in organizational computers for safety purposes.
Example: MalwareBytes, SpyBot Search & Destroy

7.2.4 Virtual Private Network

A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet.



Data sent across the public Internet is generally not protected from curious eyes, but you can make your Internet communications secure and extend your private network with a virtual private network (VPN) connection. VPN uses a technique known as tunneling to transfer data securely on the Internet to a remote access.
The Internet connection over the VPN is encrypted and secure. New authentication and encryption protocols are enforced by the remote access server. Sensitive data is hidden from the public, but it is securely accessible to appropriate users through a VPN.

Advantages of VPN

1. Provide Safety Through Anonymity
2. Secure Connection for Remote Work
3. Bypass Geo-Locked Content
4. Cost-Effective Security
5. A VPN Can Prevent Bandwidth Throttling
6. VPNS Can Bypass Firewalls
7. VPNs Make Online Gaming Better

Disadvantages of VPN

1. A VPN May Decrease Your Speed
2. Dropped Connections
3. A VPN Isn't Legal in All Countries
4. Using the Wrong VPN Can Put Your Privacy in Danger
5. Quality VPNs Will Cost Money
6. The VPN Service Might Monitor Your Activity and Use Your Data

7.2.4 Network Access Control

Network Access Control is a security solution that uses a set of protocols to keep unauthorized users and devices out of a private network or give restricted access to the devices which are compliant with network security policies. It is also known as **Network Admission Control.** It handles network management and security that implements security policy, compliance, and management of access control to a network.

Authentication

authentication is the method to control whether a particular user has "any" type of access right to the system he is trying to connect to. Usually, this kind of access is associated with the user having an "account" with that system. User authentication depends up on factors that include something he knows (password), something he has (cryptographic token), or something he is (biometric). The use of more than one factor for identification and authentication provides the basis for Multifactor authentication.

Authorization

Authorization is the process of granting or denying specific access permissions to a protected resource. Authorization deals with individual user "rights". For example, it decides what can a user do, once authenticated; the user may be authorized to configure the device or only view the data.

Accountability

Accountability is an essential part of an information security plan. The phrase means that every individual who works with an information system should have specific responsibilities for information assurance. The tasks for which a individual is responsible are part of the overall information security plan and can be readily measurable by a person who has managerial responsibility for information assurance. One example would be a policy statement that all employees must avoid installing outside software on a company-owned information infrastructure. The person in charge of information security should perform periodic checks to be certain that the policy is being followed. Individuals must be aware of what is expected of them and guide continual improvement.

7.3 Common Network Security Threats

Here are the most common security threats examples:

1. Computer virus

Computer viruses are pieces of software that are designed to be spread from one computer to another. They're often sent as email attachments or downloaded from specific websites with the intent to infect your computer and other computers on your contact list by using systems on your network. Viruses are known to send spam, disable your security settings, corrupt and steal data from your computer including personal information such as passwords, even going as far as to delete everything on your hard drive.

2. Rogue security software

Rogue security software is malicious software that mislead users to believe that they have network security issues, most commonly a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users' security settings. They'll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

3. Trojan horse

Metaphorically, a "Trojan horse" refers to tricking someone into inviting an attacker into a securely protected area. In computing, it holds a very similar meaning a Trojan horse, or "Trojan," is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate program. They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you've immediately downloaded malware to your computer. Trojans also spread when you click on a false advertisement. Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

4. Adware and spyware

By "adware" we consider any software that is designed to track data of your browsing habits and, based on that, show you advertisements and pop-ups. Adware collects data with your consent and is even a legitimate source of income for companies that allow users to try their software for free, but with advertisements showing while using the software. The adware clause is often hidden in related User Agreement docs, but it can be checked by carefully reading anything you accept while installing software. The presence of adware on your computer is noticeable only in those pop-ups, and sometimes it can slow down your computer's processor and internet connection speed. When adware is downloaded without consent, it is considered malicious.

Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.

5. Computer worm

Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an

infected computer by sending itself to all of the computer's contacts, then immediately to the contacts of the other computers. A worm spreads from an infected computer by sending itself to all of the computer's contacts, then immediately to the contacts of the other computers Interestingly, they are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities. While we don't hear about them much today, computer worm is one of the most common computer network threats.

6. DOS and DDOS attack

A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can't really overload a server with a single other server or a PC anymore. In the past years it hasn't been that common if anything, then by flaws in the protocol.

Have you ever found yourself waiting impatiently for the online release of a product, one that you're eagerly waiting to purchase? You keep refreshing the page, waiting for that moment when the product will go live. Then, as you press F5 for the last time, the page shows an error: "Service Unavailable." The server must be overloaded! There are indeed cases like these where a website's server gets overloaded with traffic and simply crashes, sometimes when a news story break. But more commonly, this is what happens to a website during a DoS attack, or denial-of-service, a malicious traffic overload that occurs when attackers overflood a website with traffic. When a website has too much traffic, it's unable to serve its content to visitors.

A **DDoS attack**, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It's harder to overcome a DDoS attack. It's launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more. Since it's likely that not all of those machines belong to the attacker, they are compromised and added to the attacker's network by malware. These computers can be distributed around the entire globe, and that network of compromised computers is called botnet. Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.

7. Phishing

Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, credit card numbers. The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient's computer. It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information. Uncovering phishing domains can be done easily with SecurityTrails.

8. Rootkit

Rootkit is a collection of software tools that enables remote control and administration-level access over a computer or computer networks. Once remote access is obtained, the rootkit can perform a number of malicious actions; they come equipped with keyloggers, password stealers and antivirus disablers. Rootkits are installed by hiding in legitimate software: when you give permission to that software to make changes to your OS, the rootkit installs itself in your computer and waits for the hacker to activate it. Other ways of rootkit distribution include phishing emails, malicious links, files, and downloading software from suspicious websites.

9. SQL Injection attack

We know today that many servers storing data for websites use SQL. As technology has progressed, network security threats have advanced, leading us to the threat of SQL injection attacks. SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application's software. They use malicious code to

obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality. You can read more on the history of SQL injection attacks to better understand the threat it poses to cybersecurity.

10. MIM attacks

Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen to a communication which should, in normal settings, be private. As an example, a man-in-the-middle attack happens when the attacker wants to intercept a communication between person A and person B. Person A sends their public key to person B, but the attacker intercepts it and sends a forged message to person B, representing themselves as A, but instead it has the attackers public key. B believes that the message comes from person A and encrypts the message with the attacker's public key, sends it back to A, but attacker again intercepts this message, opens the message with private key, possibly alters it, and re-encrypts it using the public key that was firstly provided by person A. Again, when the message is transferred back to person A, they believe it comes from person B, and this way, we have an attacker in the middle that eavesdrops the communication between two targets. Here are just some of the types of MITM attacks:

- DNS spoofing
- HTTPS spoofing
- IP spoofing
- ARP spoofing
- SSL hijacking
- Wi-Fi hacking