COMPUTER NETWORKS

DEFINITION OF A NETWORK

A computer network is a group of computers and other computing hardware devices that are linked in order to share resources, exchange files, or allow electronic communications between network nodes while using a set of common communication protocols. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

BASIC NETWORK CONCEPTS

Network nodes

A network node is an electronic device that is connected to a network and is capable of creating, receiving or transmitting information over a communication channel. For example, if a network connects a file server, five computers, and two printers, there are eight nodes on the network. Each device on the network has a network address, which uniquely identifies each device. This helps to keep track of where data is being transferred to and from on the network.

Network address

A network address is any logical address that uniquely distinguishes a network node or host on a network. It is numeric and has two parts, the network ID and the host ID. Examples; Telephone number (in the public switched telephone network), MAC (Media access control) address (in Ethernet), IP (Internet Protocol) address (in IP networks including the internet), IPX address (in Netware)

Communication channels

A communication channel refers either to a physical transmission medium such as a wire, or to a logical connection over a multiplexed medium such as a radio channel that can be used to transmit data from one network device to another. Examples; Coaxial cable, fiber Optics, twisted pair, radio frequency, Microwave system, Infrared, communication satellite, Bluetooth, Wi-Fi.

Network protocols

Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. Essentially, it allows connected devices to

communicate with each other, regardless of any differences in their internal processes, structure or design. Protocols may be implemented by hardware, software or a combination of both.

Types of protocols include:

- *Hyper Text Transfer Protocol* (HTTP): Used over the world wide web (shows information in web pages).
- *Transmission Control Protocol*(TCP): Used for communication over a network.
- *Internet Protocol*(IP): An addressing protocol (Makes sure data/signals are transmitted to the right address.
- *File Transfer Protocol* (FTP): Used to transfer files to different networks.
- *Simple Mail Transfer Protocol*(SMTP): Manages the transmission and outgoing e-mails over the internet.

USES OF COMPUTER NETWORKS

Sharing Resources: Computer networks allow businesses and organizations to have a number of computers that share data and resources even if they are not in the same physical location. Users of these computers can share information (for example; business documents, multimedia (audio/video), graphics, images, e-books etc.), software (such as Anti-virus, operating systems, enterprise software, executable software etc.), and even hardware (like printers, CD-ROM drives, hard disk drives, scanners, copiers etc.), because the computers are linked through the network.

Facilitate User communication: Computer networks enable fast interpersonal communication within an organization. People can communicate efficiently and easily. Various communication means such as emails, instant messaging, online chats, voice/video telephone calls and video conferencing, allow people to communicate and share texts photos, videos, ideas remotely.

Client- Server Configurations: Through a computer network, the employees of an organization can access the organization's databases remotely. In a client-server configuration, the organization's data is stored in servers, which are powerful computers that can hold massive amounts of data and are managed by system administrators. The employees use the simpler computers on their desks, called clients, to access the data from the server remotely. The client server model works best for organizations that have different branches but need to share information.

E-commerce: Computer networks have paved way for a variety of businesses and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items online, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically. Online business platforms have

been created and these come with convenience of doing business with customers over the internet. The recent pandemic has even pushed more businesses to launch online. Without the computer networks, many businesses would not have been able to.

BENEFITS OF COMPUTER NETWORKS

Cost reduction: With computer networking, costs are cut through sharing of resources (hardware & software) between multiple users. Two or more users are able to access shared application or software over the network with the help of the client/server application. In hardware, sharing users on the network can access hardware devices like printer, hard disk, Ram etc. with the help of a centralized computer or device. For example, you can purchase one printer rather than five, saving you the purchase price as well as the ongoing maintenance costs. A shared internet connection allows you to control internet access with a firewall or a proxy server, protecting your company from liability due to employee misuse.

Efficiency and Collaboration: Networks make it far easier for employees to share information and collaborate on work. Carrying papers from office to office, or even a portable storage device of some kind is just not as efficient as storing the information on a centralized server for access by all who are authorized to access it. This can speed up project delivery and enhance the creativity of your team hence saving time.

Centralized storage and back up: Networks allow you to store the data centrally and ensure that all critical data gets backed up on a pre-determined schedule. You can automate the procedure so that no user intervention is involved other than an operator checking the logs each day. All the data of the organization can be stored in a remote server that can be accessed at any given time, that way all authorized users within an organization can be able to access it. If in case one of the employees happens to loose data, there won't be any problem in retrieval since all the data will already be backed up in the central server.

Increased productivity: Computer networks allow employees to be more productive. They can deal with more customers in less time since they have instant access to shared customer and product databases. Information can easily be found on search engines such as google, Bing. Employees have opportunities for genuine multitasking thanks to the way web browsers can segregate data for them.

Optimize convenience and flexibility: Computer networks enable flexible operations. The data is not stored in a local server making it accessible with internet connectivity. You can access your data from any device. This enhances free movement while accessing your data wherever you may be.

Improved quality of output: Since all employees work from a single source of information, errors can be reduced and inconsistencies controlled.

LIMITATIONS OF COMPUTER NETWORKS

Security issues: One of the major drawbacks of computer networks is the security issues involved. If a computer is a standalone, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a computer hacker can get unauthorized access by using specialized tools developed for this purpose hence making networks such as the internet unsafe. In case of big organizations, various network security software is used to prevent the theft of any confidential and classified data.

Rapid spread of computer viruses & malware: If any computer system in a network gets infected with a virus, there is a possible threat of other devices on the network getting infected too. Virus can easily spread on a network, because of the inter-connectivity of workstations/various devices hence corrupting files and damaging operating systems. Besides, multiple systems with shared resources are the best propagating ground for viruses. Likewise, if malware unintentionally gets installed on the central server, all connected clients to the server in the network will inevitably get infected. Spam remains to be a setback on the internet.

Expensive to set up: The initial set up cost of a computer network can be high depending on the number of computers to be connected. Costly devices like routers, switches, hubs etc., can add up to the bills of a person trying to install a computer network. Purchasing the network cabling and file servers is also an added expense. Having to buy NICs (Network Interface Cards) for each workstation, in case they are not inbuilt may also increase the cost exorbitantly.

Dependency on the main file server: In case the main file server of a computer network breaks down, it will bring the entire network to a standstill hence disrupting business operations. If the file server breaks down, the files on the file server become inaccessible. Email might still work if it is on a separate server. The computers can still be used but are isolated.

Needs an Efficient Handler: Managing a big network is complex, it involves advanced configuration and complicated installations. The technical competences and expertise needed to operate and oversee a computer network is substantially high. In other words, it requires a skilled network manager with experience to be hired atop training.

Lack of Independence: As networks generally have a centralized server and dependent clients, the client users usually do not have any control whatsoever. Centralized decision making can occasionally hinder how a client user desires to use his computer.

Lack of Robustness: If the core file server of a computer network fails, the entire system may become useless. If there is a failure in the main connecting server or a bridging device in the network, the entire network will come to a halt.

Accessibility: Even though most of the modern computers provide free access, there are still connectivity issues in some countries. Particularly countries those are developing, people residing there suffer from connectivity challenges. Unless these challenges are resolved, there is no assurance of true global network.

TYPES OF COMPUTER NETWORKS

Computer networks can be classified into different categories. The classifications help to explain the types of networks in use today, and what they're used for. The following are the criteria widely used;

- Classification based on Scale (geographical spread/physical size)
- Classification based on Functional relationships (Network architecture)
- Classification based on network topology

CLASSIFICATION BASED ON SCALE

Based on geographical spread, networks can be classified into the following three categories;

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

LOCAL AREA NETWORK (LAN): Local area network (LAN) LAN is a computer network that consists of few or more computers and other communication devices connected in the form of a network within a well-defined area such as a room or a building. A typical example is a college or university computer network. Users in a LAN can share both hardware and sharable software resources. For example, hardware resources include expensive laser printer, plotter, fax machines, modem, etc. Almost all local area networks use a single communication media, as it restricted to a limited area. All network resources and their management activities are controlled using special system software called Network Operating System (NOS). The basic hardware device used for creating a LAN is a switch which is used for connecting the different nodes among each other.

A LAN can be wired or wireless. In a wired LAN, devices are connected and communicate over Ethernet cables i.e. RJ45 connector / CAT5 (Ethernet) cable. The cable provides a simple interface for connecting multiple devices such as computers/ workstations, servers, routers and switches. In a wireless LAN, devices are connected and communicate via Wi-Fi with the help of a router. The router provides wireless connections to any Wi-Fi enabled devices within range of the router's wireless signal. This includes laptops, tablets, smartphones, smart appliances, smart TVs. Examples of a LAN; Personal Area Network (PAN), Home Area Network (HAN).

CHARACTERISTICS OF A LOCAL AREA NETWORK (LAN)

- LANs are in a narrower geographic scope (office, campus, school and home area), coverage area is generally a few kilometers (close proximity)- within a radius of 0.1 km i.e. 100 meters.
- They can be used even without telecommunication lines hence they may not need internet access.
- LANs have higher data transfer speeds because data only has to travel a short distance.
- In LAN you can connect various nodes/multiple devices of a single building sharing a transmission medium.
- Because LANs are geographically small, they usually use cables or low-power radio (wireless) for connections.
- The communication quality is better in LAN; the transmission error rate is low as compared to WAN.

METROPOLITAN AREA NETWORK (MAN): A MAN is a large computer network that connects Local area networks in a metropolitan area such as a city or town and handles the bulk of communications activity across that region. A MAN is more extensive than a LAN. The name metropolitan is due to the ability to cover a relatively larger area of a city, from a few tens to a maximum of hundred kilometers. Different hardware and transmission media are often used in a MAN for efficient transmission of data. The main purpose of MAN is to connect LANs in a metropolitan region to Wider Area Networks like the internet in the long run. As a rule, MAN does not belong to any particular organization, in most cases, a group of users or a provider who takes charge for the service own its connecting elements and other equipment. In most cases, a government builds and maintains a metropolitan fiber optic network, then leases fiber to private companies. For example; *(The government of Uganda, through NITA-U, is implementing the National data transmission Backbone infrastructure and e-government infrastructure project to connect all major towns across the country including government ministries, departments and agencies via an optic fiber cable network so as to reduce the cost of public administration, support delivery of secure e-government services as well as enhance communications services in the*

*country)***.** The transmission support for the MAN is represented by the links of fiber optic cable laid in a ring formation in a metropolitan area. Example of a MAN; Campus Area Network (CAN)-A campus area network (CAN) is a large network that connects multiple buildings on a school or business campus. CANs may also be considered MANs, since they connect multiple LANs but are not large enough to be considered a WAN. The MAN can be used to provide services including telecoms, Internet access, cable television and CCTV to businesses and citizens in these metropolitan areas.

CHARACTERISTICS OF A METROPOLITAN AREA NETWORK (MAN)

- Network size generally ranges from 5 to 50 km. It may be as small as a group of buildings on campus to as large as covering the whole city.
- In general, a MAN is not owned by a single organization as in LAN. The MAN, its communication links and equipment are owned by either a consortium of users or by a single network provider who sells the service to the users. This level of service provided to each user must therefore be negotiated with the MAN operator, and some performance guarantees are normally specified.
- Data rates are moderate to high.
- It facilitates the sharing of regional resources.
- The network size falls intermediate between LANs and WANs.
- They provide uplinks for connecting LANs to WANs such as the Internet.
- Because MANs are smaller, they are usually more efficient than WANs, since data does not have to travel over large distances.

WIDE AREA NETWORK (WAN): Wide area network (WAN) WAN is a computer network that spans a large geographical area. It uses dedicated or switched connections to link computers in geographically remote locations. Wide area networks are implemented to connect a large number of LANs and MANs. Due to this reason, it is possible to see a large number of heterogeneous components in a wide area network. Different communication media used, and the network spreads across several national boundaries. Computers connected to a WAN are often connected to a public network. They can also be connected through leased lines or satellite links. The government or multinational organizations mostly use WAN because of the considerable investment made to implement them. Data can easily be relayed to clients (staff, students, buyers and suppliers) from various locations across the world. As organizations grow and become international, WANs allow them to communicate between branches, share information and stay connected. Students at universities might rely on WANs to access library databases or university research. The public, can rely on WANs to communicate, bank, shop and more. The internet is considered the largest WAN in the world. If it weren't for wide-area networks (WAN) it wouldn't be possible to telecommute, to create unified networks for organizations with far-flung locations, or to do anything online.

CHARACTERISTICS OF A WIDE AREA NETWORK (WAN)

- WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
- They facilitate the sharing of regional resources.
- They provide uplinks for connecting LANs and MANs to the Internet.
- Communication links are provided by public carriers like telephone networks, network providers or phone companies, cable systems, satellites etc.
- Typically, they have low data transfer rate and high propagation delay, i.e. they have low communication speed.
- They generally have a higher bit error rate.

CLASSIFICATION BASED ON FUNCTIONAL RELATIONSHIPS (NETWORK ARCHITECTURE)

Network architecture describes how tasks are located to all of the computers in the network. Computer networks can be classified according to the functional relationships which exist between the elements of the network. This classification is also called network architecture and there are two types;

- *Client-Server network*
- *Peer-to-Peer network*

CLIENT-SERVER NETWORK: CSN (Client/Server Network) is type of computer network in which a centralized and powerful computer (server) provides resources other personal computers that are less powerful or workstations (as clients) connected on the network. In this architecture, system is generally decomposed into client and server processor or processes. This architecture supports separation of functionality commonly based on concept of service. A server is a computer on a network that provides a resource that can be used by any authorized client station. Servers are usually always on and connected to the internet, so that users can access the resources and services at any time. Servers may include; Web servers (store and provide web pages), Email servers (direct email to the intended recipient and sometimes filter out spam), File servers (provide data files to users), Database servers (provide data storage and manipulation)

CHARACTERISTICS OF THE CLIENT-SERVER NETWORK

- It works with a system of request and response. The client sends a request to the server and the server responds with the desired information.
- The client and server should follow a common communication protocol so they can easily interact with each other.
- A server can only accommodate a limited number of client requests at a time. So it uses a system based on priority to respond to the requests.

ADVANTAGES

- A special Network Operating System (NOS) is provided by server to provide resources to many users that request them.
- It is also very easy and simple to set up and manage data updates. This is because data is generally stored in centralized manner on server.
- All the required data is concentrated in a single place i.e. the server which makes it easy to protect the data and provide authorization and authentication.
- The server need not be located physically close to the clients. Yet the data can be accessed efficiently.
- All the nodes i.e. clients and server may not be built on similar platforms (hardware, operating systems, mobile, client-server, cloud platforms) yet they can easily facilitate the transfer of data.

DISADVANTAGES

- If all the clients simultaneously request data from the server, it may get overloaded. This may lead to congestion in the network.
- If the server fails for any reason, then none of the requests of the clients can be fulfilled.
- The cost of setting and maintaining a client server model are quite high.

PEER-TO-PEER NETWORK: A peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer. It is a decentralized and distributed network architecture in which individual nodes in the network (called "peers") act as both suppliers and consumers of resources. All nodes are equal participants in the sharing of resources and tasks are equally divided between all nodes. Each device in the network is considered to be a peer with functions that contribute to the network. Tasks (such as searching for files or streaming audio/video) are shared amongst multiple interconnected peers who each make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for

centralized coordination by servers. A simple P2P network can be a simple collection of two computers and a printer. Computer 1 will be able to print on the printer connected to computer 2, if computer 2 sets up the sharing permissions for the printer.

CHARACTERISTICS OF PEER-TO-PEER NETWORK

- P2P networks have decentralized resources because every computer can function as both a server and a client i.e. one computer might assume the role of server for one transaction while acting as a client for another transaction.
- P2P networks can share resources such as files, equipment (printers) among network devices without the use of a dedicated server. So if the nodes increase then the resource sharing capacity of the P2P network increases. This is different than client server networks where the server gets overwhelmed if the nodes increase.
- All the computers on the network store their data using individual security but share data with all the other nodes.

ADVANTAGES

- Each computer in the peer to peer network manages itself. So, the network is quite easy to set up and maintain.
- In the client server network, the server handles all the requests of the clients. This provision is not required in peer to peer computing and the cost of the server is saved.
- It is easy to scale the peer to peer network and add more nodes. This only increases the data sharing capacity of the system.
- None of the nodes in the peer to peer network are dependent on the others for their functioning.

DISADVANTAGES

- It is difficult to back up the data as it is stored in different computer systems and there is no central server.
- It is difficult to provide overall security in the peer to peer network as each system is independent and contains its own data. This can lead to denial of service attacks.

CLASSIFICATION BASED ON NETWORK TOPOLOGY

The term topology refers that way in which the end points, or stations, attached to the network are interconnected or it is the arrangement of systems in a computer network. The network topology can be categorized into:

- Mesh topology
- Star topology
- Bus topology
- Ring topology
- Hybrid topology

MESH TOPOLOGY

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. Dedicated means that the traffic links only between the two devices it connects. Mesh topologies are used where the reliability of network communication is very important. These are highly applicable in; Military organizations -often used to avoid breakdowns in communication. Cities-are increasingly using wireless mesh networks to help monitor traffic flow, sewage treatment and to help control street lighting. Emergency services, such as police and fire services, also use wireless mesh networks to ensure that communication is reliable. Some utility companies who provide water and electricity, use mesh networks to allow smart meters to send readings automatically.

CHARACTERISTICS OF A MESH TOPOLOGY

- All the network nodes are interconnected to each other. There is no central connection point. Instead each node is connected to at least one other node and usually to more than one.
- Each computer not only sends its own signals but also act as relays, passing on a message towards its final destination.
- Each node is capable of sending messages to and receiving messages from other nodes.

ADVANTAGES

- Messages can be received more quickly if the route to the intended recipient is short.
- Messages should always get through as they have many possible routes on which to travel. If one cable fails, data has alternative paths to get to its destination. Reliable and robust.

- Multiple connections mean each node can transmit to and receive from more than one node at the same time hence no node is isolated.
- New nodes can be added without interruption or interfering with other nodes.
- Each connection can carry its own data load.
- Point-to-point links make full identification and fault detection easy.
- Security and privacy for data because there is a point to point link thus unauthorized access is not possible since data travels along the dedicated line.
- No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.

DISADVANTAGES

- Full mesh networks can be impractical to set up because of the high number of connections needed.
- Many connections require a lot of maintenance.
- Cabling cost is more.
- Installation and configuration is difficult. Bulk wiring is required hence making it tedious and headache.
- Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link

STAR TOPOLOGY

Star topology is the network in which each station is directly connected to a central connecting node called hub/switch. In star topology all the devices are not directly connected to one another. All nodes indirectly connect to each other through one or more switches/Hubs. The switch acts as a central point through which all communications are passed. This topology does not enable the direct traffic between the devices in the network. Each device needs only one link and one input/output port to connect to the number devices in the network. This type of topology is used in local area networks (LAN). Star topologies tend to be found in large organizations, such as educational establishments and businesses, where high performance is a must. They are also found in home networks, especially those that are wireless. In this case, a router with a wireless access point (WAP) provides the central connection for all nodes.

CHARACTERISTICS OF A STAR TOPOLOGY

- All cables run to a central connection point that way; If one cable breaks or fails, only the computer that is connected to that cable is unable to use the network.
- As the network grows or changes, computers are simply added or removed from the central connection point, which is usually a hub or switch.

- Every node has its own dedicated connection to the hub.

ADVANTAGES

- Each node is separately connected, therefore a failure of one node or its link, (transmission media), does not affect any other nodes/or stop the other nodes from working smoothly.
- Easy to set up and modify (upgrade), Only the central site will have to be updated. New nodes can be added to the network simply by connecting them to the switch.
- Star networks tend to have higher performance as a message is passed on to its intended recipient only if a switch is used.
- Easy fault detection (and remove parts) because the link can be easily identified.

DISADVANTAGES

- The whole network fails if the switch fails as no node can communicate.
- A wired star topology requires plenty of cable - in a large network this can be expensive. Cost of installation is high. Because there is so much cabling used to connect individual computers to the central point, this may increase the cost of expanding and maintaining the network.
- Hub requires more resources and regular maintenance because it is the central system of star topology.

BUS TOPOLOGY

In a bus topology, a long and single cable acts as a backbone to connect all the devices (file server, work stations and peripherals) in a network. Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. The tap connects the drop line to the main cable. The main cable also has a terminator on each end to ensure that the network functions correctly. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker the farther it has to travel. For this reason, there is a limit on the number of taps a bus can support and on the distance between those taps. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

The bus carries data along the central cable. As the data arrives at each computer system, it checks the destination address to see if it matches. If the address does not match, the node ignores the **packet**. If the address of the node matches that contained in the data, it processes the data. Bus topologies are not widely used in modern networking as they are not well suited to dealing with large amounts of data. But they can be used when a small,

cheap and often temporary network is needed that does not rely on very high data-transfer speeds.

CHARACTERISTICS OF A BUS TOPOLGY

- It transmits data only in one direction.
- Every device is connected to a single cable in the network.
- Terminators are required at both ends of the backbone cable.
- Only one computer can send data on the bus at any one time.
- The number of devices connected to the bus affects the performance of the network.
- All nodes are connected to the bus cable directly by drop lines and there is no other connection between nodes.

ADVANTAGES

- Easy installation, each drop line cable needs to be connected with backbone cable.
- Less cables required than Mesh and star topology hence making it cheaper to install.
- Easy to add more nodes to the network.

DISADVANTAGES

- Not scalable as there is a limit of how many nodes you can connect with backbone cable. As more nodes are added, the performance of the network can be reduced, making this unsuitable for large local area networks (LANs).
- If the entire network shuts down, it can be difficult to identify where the fault has occurred.
- Entire network shuts down if there is a break in the main cable.
- Not meant to be used as a stand-alone solution in a large building.
- Having one backbone increases the chances of data collision, which then causes the network to slow down.
- As all computers on the bus can see all data that is transmitted, it is not classed as a secure network and can easily be hacked.

RING TOPOLOGY

A ring topology is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network. Data travels from node to node, with each node along the way handling every packet. Most ring topologies allow packets to travel only in one direction, called a unidirectional ring

network. Others permit data to move in either direction, called bidirectional. Signals pass through the ring in a single direction until they reach the final destination. These topologies are used in school campuses and some office buildings.

CHARACTERISTICS OF RING TOPOLOGY

- Data flows in a single loop continuously. In a ring network, packets of data travel from one device to the next until they reach their destination.
- Every device is connected to a single cable forming a ring and data transmission is along that backbone cable.
- The ends of the backbone cable will be connected to the first node so that it will form a closed ring or circle.
- Data transmission using the token passing scheme method is performed alternately in one direction.

ADVANTAGES

- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Additional workstations can be added without impacting performance of the network.

DISADVANTAGES

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.
- If the cable is disconnected or the node is corrupted then the network will crash.

HYBRID TOPOLOGY

Hybrid topology is an integration of two or more different topologies in a network. The resultant topology will have the advantages and disadvantages of all the constituent basic topologies. This combination of topologies is done according to the requirements of the organization. For example, if there is a ring topology in one office department while a bus topology in another department, connecting these two will result in hybrid topology (ring bus network). Hybrid topology networks are used in various places such as; Schools, University campuses, Multi-national organizations, Banks etc. A hybrid

topology will exhibit characteristics of all the constituent topologies, thereby limiting the inherent weaknesses of each topology.

CHARACTERISTICS OF HYBRID TOPOLOGY

ADVANTAGES

- Highly reliable: This increase in reliability is due to sub networks. In case of problem in one or more sub network, whole Computer Network can still be operational.
- Effective: Since it's a combination of two or more topologies, it maximizes strengths of constituent topologies while their weaknesses are neutralized. For example, ring topology has good data reliability (achieved by use of tokens) and star topology has high tolerance capability (as each node is not directly connected to the other but through a central device) so these two can be used effectively in a hybrid star-ring topology.
- Flexibility: You can extend this Type of Network easily. In such Networks you have a lot of extension points. So, it is highly scalable. You can easily upgrade and downgrade Computer Network in accordance with user needs.

DISADVANTAGES

- Complexity of design: It's not easy to design, configure and install this type of architecture. Sometimes trouble shooting requires a great deal of expertise. Many network engineers feel problems even in establishing this type of topology.
- It is costly: it is highly expensive to create, extend and manage. hybrid architectures are usually larger in scale, they require a lot of cables, cooling systems and sophisticated network devices. The hubs which are attached to combine different topologies are expensive. These hubs are different from normal hubs and are more intelligent in performance.
- Hardware changes are required in order to connect one topology to another.

NETWORK DESIGN PARAMETERS

Security: Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources.

The transfer of data between devices in a network is another concern to an organization. Security is not inherent in computer networks as there many points where the transfer of data can be monitored or intercepted, yet the kind of data we transfer can be extremely

sensitive (personal information, bank details, trade secrets etc.). When securing the network, ensured confidentiality, availability and maintenance of integrity is key. Confidentiality can be guaranteed by preventing unauthorized access to or theft of content using authentication systems that require strong passwords, and by encrypting content where appropriate. Integrity can be maintained by stopping the data from being modified or corrupted before it reaches its destination, and by ensuring the content is coming from a trusted source. Such tools as digital signatures and checksums are useful tools for this. Availability can be ensured by preventing Denial of Service attacks on the network. Denial of Service often occurs because of a computer virus, which can be prevented by using firewalls and anti-virus software.

Scalability & Future Considerations: Scalability means the ability to grow based on the needs and have good performance after growth. The best example of scalability is the Internet itself, as many new users are connecting through internet and communicating with other devices, the network is working properly. It would be frustrating and costly if you had to rebuild sections of or an entire network just because you need to add some devices. When implementing a computer network, do not just think about your current needs. Anticipate your future needs, whether immediate and/ or long term. Opt for a network design that does not necessitate major re-cabling or re-architecture at break points. Wireless infrastructure can be simple to reconfigure during growth or change, but planning for this up front is important. You do not want to invest in a solution that cannot grow with your business or will be obsolete a few months down the road. While technology is changing and advancing, your network should be able to adapt to meet your evolving needs. In any case, planning for growth in the initial stages can save future expenditures. The price difference, for example, between a 16-port switch and a 32-port switch can be negligible when compared to the cost of purchasing a new switch to replace one that is too small.

Fault Tolerance: Fault tolerance refers to the ability of the network to continue operating without interruption when one or more of its components fail. The objective of creating a fault-tolerant network is to prevent disruptions arising from a single point of failure which in turn ensures high availability and business continuity of mission critical applications or systems. Fault tolerance can be achieved by anticipating failures and incorporating preventative measures in the network design. For example; regular data backups in case of data loss on any of the devices on the network, create a mirror of the data on an alternative location. Set up alternate network devices to use as alternative access points.

Cost: Your budget also determines the type of network design that you are going to implement. It's important to factor in all your costs for equipment such as modems,

routers, servers, hubs, cabling, switches etc., maintenance and operation costs and see if it benefits you better in the long run. Remember the network must be cost effective in design and implementation.

Please also note that, although wireless and client-server networks are more expensive, they also provide more in-depth business IT solutions that could help you gain higher ROI in the future.

NETWORK DEVICES

Network devices are physical devices used for communication between the different hardware on a computer network. Specifically, they mediate data transmission in a computer network. A "network" device is a component that makes up the network infrastructure such as modems, routers and switches. A "networked" device on the other hand refers to equipment that connects to a network, which includes computers, printers, fax machines etc. The different types of network devices include;

NETWORK HUB: A network hub is used to connect multiple network hosts as well as aiding data transfer. A network host may be a computer or other device connected to a computer network. When using a hub, data is transferred in form of packets on a computer network. Data packets are units of data collected into one set that travel along a given network path. When a host sends a data packet to the network hub, the hub copies the data packet to all of its ports regardless of where the packet is actually destined. The hub is not able to determine to which port a packet should be sent. By passing to every port, this ensures that it will reach its intended destination. This means that all the ports know about the data and the port for whom the packet is intended, claims the packet. The networking protocols have ways of determining which computer on the network needs to process the data. Hubs cannot filter data, so data packets are sent to all connected devices. Because of this working, a network hub cannot be so safe and secure. In addition, copying the data packets on all the ports will make the hub slower. The entire network shuts down if there is a problem with the hub.

NETWORK SWITCH: While the hub is used for data transfer, a switch is used for "filtering and forwarding" of data. Whenever a data packet is obtained from the interfaces in the switch, then the data packet can be filtered and transmitted to the interface of the proposed receiver. A switch is aware of addresses associated with each of its ports and forwards each incoming data frame to the correct port. It uses the CAM (Content Addressable Memory) address table to forward the data frame to the correct switch port by their MAC addresses. Switches generally have more intelligent roles than hubs. Switches are far more superior than hubs as they minimize the traffic on a network, decrease bandwidth usage and only send data to the intended computers. For instance,

Computer A wants to send data to Computer C. The switch would see that Computer A is on port 1 while Computer C is on port 4. The switch can then send data directly between them, with the data arriving at port 4 and leaving the switch at port 1. This process hugely reduces bandwidth usage when compared to a hub.

ROUTER: A router is an electronic device that interconnects two or more computer networks and selectively interchanges packets of data between them. It determines the route your data packets take in travel from the source to destination and also routes them in that direction. The router determines where the destination is and how it should be reached by consulting its routing table. The data packets also contain the address of the destination. Routers use this destination address to send the packet between networks until it reaches its destination. A router helps to connect your LAN to a WAN such as the internet. So when you enter a search term on Google, your router directs this packet to Google's servers for processing. Routers are the backbone of large computer networks like the internet. Without the development of network routers, the Internet would not have become as extensive. Routers play a vital role in controlling network traffic and keeping the network efficient. Routers forward messages over the most efficient path and can alter this path as needed.

BRIDGE: A large network can be divided into multiple parts which are called segments. Each segment can use its own network protocol, security rules, firewalls and so on. Nodes on different segments cannot directly communicate with each other. To make this possible, a bridge is added between the segments**.** A bridge is a network device that connects two segments of a network together. It is used to divide larger networks into small manageable sections. They do this by sitting between two physical network segments and managing the flow of data between the two. By looking at the MAC address of the devices connected to each segment, bridges can elect to forward the data (if they believe that the destination address is on another interface), or block it from crossing (if they can verify that it is on the interface from which it came). The bridge lets packet pass that are destined for a host on the other side. This seems to turn the two segments into one big network again, but there is an important difference. Data packets generated on one segment and intended for that same segment are not passed to the other segment. This saves on data transmission on the network as a whole. If a router connects two different types of networks, then a bridge connects two sub networks (that use the same protocol) as a part of the same network. You can think of two different labs or two different floors connected by a bridge.

GATEWAY: A gateway is a network device that forms a passage between two networks operating with different transmission protocols. A gateway translates one data format to another. The intention is to only translate the data format and not the data itself. In many

cases, the gateway functionality is incorporated into another device. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway. A gateway acts as the meeting point or go between point between 2 different networks, using different protocols e.g. Network A uses one protocol, Network B uses another. A computer from A wants to communicate with a machine from B but due to the difference in protocols, it does not know how to communicate. It can adopt or add B's protocol but this is a tasking process and is not really efficient. Instead, a gateway will translate the request from the computer in A's network, into B's language and then translate the reply from B's language into A's, so the two machines can communicate without any change in protocol.

REPEATER: Repeaters (also known as signal boosters) are network devices that amplify or regenerate an incoming signal (attenuated signal) before retransmitting it. They are incorporated in networks to extend the length or the coverage area. They are used as a connection between two LANs thus forming a large single LAN. It can also be defined as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances. As signals travel along a network cable (or any other medium of transmission), they lose signal strength (the further the signal travels away from the source), a process called signal attenuation. This poses a limitation upon the length of the LAN or coverage area of cellular networks. If a cable is long enough, the attenuation will finally make a signal unrecognizable by the receiver. Installing repeaters at certain intervals will enable the signal to travel longer distances over the network. A repeater regenerates the received signals and then retransmits the regenerated (or conditioned) signals on other segments. For example: Inside MUBS (University campus), Berlin (hostel) might be far away from the main building where the ISP line comes in. If management wants to pull a wire in between the hostel and main building, they will have to use repeaters if the distance is much because different types of cables have limitations in terms of the distance they can carry the data for.

NETWORK INTERFACE CARD: A network interface card is a hardware device that connects a computer to a network and allows the computer to be identified amongst others in a network. NICs can exist in almost any networked device including PCs, laptops, servers, printers, telephones, scanners etc. It may enable a wired connection (such as Ethernet) or a wireless connection (such as Wi-Fi) to a local area network. Without a NIC, a computer cannot be connected over a network. It is also called network interface controller, network adapter or LAN adapter. Utilizing network cards to connect to a network allow users to share data such as companies being able to have the capability of having a database that can be accessed all at the same time, send and receive e-mail

internally within the company or share hardware devices such as printers. In other words, it allows the computer to communicate to other computers on a network.

MODEM: A modem stands for Modulator + Demodulator. It is a hardware device that modulates and demodulates the signal between the digital data of a computer and the analog signal of a telephone line. It converts data to a signal so it can be easily sent and received over a phone line, cable or satellite connection. You get an internet connection through a wire to your house. This wire is used to carry our internet data outside to the internet world. However, our computer generates binary data or digital data in form of 0s and 1s and on the other hand, a wire carries an analog signal and that's where the modem comes in. Modems are used for data transfer from one computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying messages across phone lines. Modulator converts data signals from digital mode to analog mode at the transmitting end and the de-modulator converts the same from analog to digital at the receiving end.