CSE 3502

INFORMATION SECURITY MANAGEMENT

Digital Assignment – 1

F2 | SJT404
Dr. Lavanya K

WINTER SEMESTER 2021-22

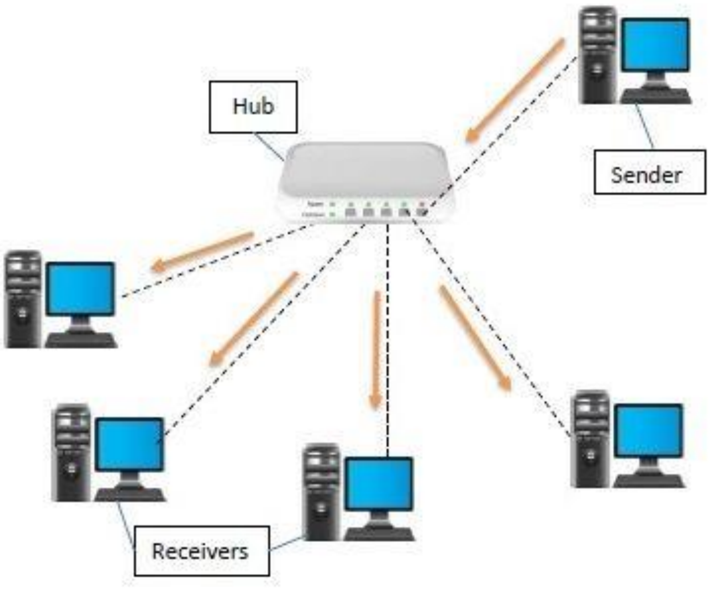
by

SHARADINDU ADHIKARI
19BCE2105

1. NETWORKING DEVICES

PART-A: Description

1.1. HUB



- **Characteristics**:
  - A hub is a physical layer device that connects many networking devices. They're typically used to connect computers in a local area network (LAN).
  - Hubs connect multiple computer networking devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. A hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.
  - It can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets; however, if the incoming data is analog, then the hub passes it on in signal form.
  - There are 3 types of Hubs:
    - Active Hubs: They function at the physical layer of the OSI model. Unlike passive hubs they need electricity. It has the ability to fix the damaged packets

when packets are sending, and also able to hold the direction of the rest of the packets and distribute them. If a port receives a weak signal, but still it is readable, then the active hub reconstructs the weak signal into a stronger signal before its sending to other ports. It can boost the signal if any connecting device is not working in the network. Therefore, it helps to make the continuity of services in LAN.

- Passive Hubs: To put it simply, a passive hub is a connector which connects wires coming from other devices. It does not have the capability to monitor information that it receives from various network segments. However, it is capable of determining the bugs and faulty hardware. Passive hubs tend to work without electricity. Additionally, the advanced passive hubs have AUI ports, which are connected as the transceiver according to the network design.

- Intelligent Hubs: It is a little smarter than passive and active hubs. These hubs have some kinds of management software that help to analyse the problem in the network and resolve them. It is beneficial to expend the business in networking; the management can assign users that help to work more quickly and share a common pool efficiently by using intelligent hubs. However, it offers better performance for the local area network. Furthermore, with any physical device, if any problem is detected, it is able to detect this problem easily.

- A Hub is a WIRED device.

- **OSI Layer**:

  A Hub, whether it is an active or passive one, functions in the physical layer of the OSI Model.

- **Purpose of the Device**:

  The main purpose of a hub is to allow communications between devices so that data can be transmitted from one computer to another. It is a piece of hardware and is most often used in a small LAN (Local Area Network) setting, where there is little likelihood of traffic conflicts. A hub is usually the easiest and cheapest way of connecting a few computers so that they can share communication resources like the Internet.

- **Contribution towards Network Security**:

  - Due to the fact that a hub lacks intelligence it is not known to contribute a lot to network security. Also, passive hubs do not require electricity and hence do not contribute anything towards network security while active hubs can perform basic collision detection and avoidance mechanisms.

  - Hubs perform basic collision detection.

  - When the collision occurs, the hosts who sent the frame detects it. The frames that were sent are destroyed then and hosts send a jam signal which shows that both hosts are about to wait.

  - Although most of the hubs can recognize network troubles or errors like collisions, broadcasting all information to the several ports can be a security risk and cause bottlenecks.

  - CSMA/CD: In this technique, before entering any host frame, it is checked whether the link is empty or not. If there is a signal in the link, then the host waits until the link is free. Then this host sends its own frame.

  - A managed hub has intelligence built into its firmware. It responds to management queries for statistics and to commands for setting the configuration.

  - Since Hubs act as a common connection point for devices in a network, it is often used to monitor network traffic.

1.2. SWITCH

- **<u>Characteristics</u>:**

  - A switch is a network device that connects different segments of a network. It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.

  - In a network, it acts as a hardware device that filters and forwards network packets from one networking device (switch, router, computer, server, etc.) to another.

  - Switches are more intelligent than hubs. They are used in modern ethernet LANs and are responsible for processing and routing data at the data link layer.

  - Based on the OSI Layer they operate on, there are majorly 2 types of switches:

    - <u>Layer 2 switches</u>: Used to reduce traffic on the local network. Forwards frames to destination on the basis of MAC address.

    - <u>Layer 3 switches</u>: Forwards network packets with the help of IP addresses.

- A Switch is a WIRED device.

- **OSI Layer**:

  - A Layer 2 switch operates in the Data Link Layer of the OSI Model.
  - A Layer 3 switch operates in the Network Layer of the OSI Model.

- **Purpose of the Device**:

  - Connection of multiple hosts: Normally, a switch provides a large number of ports for cable connections, allowing for star topology routing. It is usually used to connect multiple PCs to the network.

  - Keep electrical signal undistorted: When a switch forwards a frame, it regenerates an undistorted square electrical signal.

  - Message forwarding to a specific host: Like a bridge, a switch uses the same forwarding or filtering logic on each port. When any host on the network or a switch sends a message to another host on the same network or the same switch, the switch receives and decodes the frames to read the physical (MAC) address portion of the message.

  - Traffic management: A switch in networking can manage traffic either coming into or exiting the network and can connect devices like computers and access points with ease.

  - Increase LAN bandwidth: A switch divides a LAN into multiple collision domains with independent broadband, thus greatly increasing the bandwidth of the LAN.

- **Contribution towards Network Security**:

  A switch is best described as a high-performance hub that is uniquely intelligent. Data goes back and forth between the switch and during this time, the box records the MAC addresses. These addresses are unique identification numbers for hardware that is network enabled. Each sender and recipient will have different mac addresses. During this process of discovery, the hub then learns which device is linked to which port.

  By doing this, the hub knows and can identify where the traffic came from, accessing the mac address data and then directs it to the right port. As such, it ensures that the right data goes to the right computer system on the network. This is particularly crucial on a larger network and does offer enhanced security because it guarantees that data is not being sent to insecure areas on the network. As well as providing security benefits, it means that bandwidth levels are kept under a tighter level of control as well.

  Keeping this in mind, below I've listed some of Switches' major contribution towards Network Security:

- User Authentication: A switch performs any measures taken within a computer or a network to ensure the computer user's identity. ID theft is becoming increasingly more common in the digital world, making it an increasingly important facet of network security.

- Firewalls: An integrated platform that is used to combine the traditional firewall with other network filtering devices to provide greater network security. The platform performs several security checks simultaneously through data packet inspection and employing some manner of intrusion and prevention system along with antivirus inspection and third-party integration.

- Intrusion Detection: This is a software or device feature that is used to monitor a computer or a network of computers in order to detect malicious activity or possible violations of network policy. In the event of a problem being detected that could compromise network security, the software sends an immediate alert to the relevant authorities, and, depending on the setting, takes some form of action to shut down the lines of communication with the device posing a threat.

- Intrusion Prevention: The purpose of this kind of software is to take a pre-emptive approach towards network security. The device is programmed to actively take part in the identification of potential threats to network security and take swift action against them before the threat becomes a reality. Similar to an intrusion detection system, an intrusion prevention system monitors network traffic, but plays a more directly active role in neutralizing threats to security.

- Port Level Filters and Checks: Thanks to the internet, information can be shared more quickly than ever, through the world-wide network. The improvement in data sharing has also resulted in increasingly more mobile methods of data collection and transfer, such as thumb drives and hard disks. In order to ensure the network security is not threatened by these external devices, various port filters are available for the monitoring and detection of malicious software hiding within the external drives, which can enter the network through ports which are left unguarded.

1.3. ROUTER

- **Characteristics:**

  - A Router is a networking device that is used to extend or segment networks by forwarding packets from one logical network to another.

  - It forwards data packets between computer networks and are most often used in large internetworks that use the TCP/IP protocol suite and for connecting TCP/IP hosts and local area networks (LANs) to the Internet using dedicated leased lines.

  - An example: suppose we search for www.google.com in our web browser, then this will be a request which will be sent from our system to the Google's server to serve that webpage, now our request which is nothing but a stream of packets don`t just go to the Google's server straightaway; they go through a series of networking devices known as a router which accepts this packets and forwards them to correct path and hence it reaches to the destination server.

  - Because routers operate at a higher OSI level than bridges do, they have better packet-routing and filtering capabilities and greater processing power, which results in routers costing more than bridges.

  - Routers can be both WIRED and WIRELESS.

- **OSI Layer:**

  Routers work at the Network Layer (layer 3) of the Open Systems Interconnection (OSI) reference model for networking to move packets between networks using their logical addresses. This is the layer that the IP protocol works at.

- **Purpose of the Device:**

  - Main purpose of Routers includes managing traffic between networks connected to it by forwarding packets to their intended IP addresses:

  - Forwarding: The router receives the packets from its input ports, checks its header, performs some basic functions like checking checksum, and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.

  - Routing: Routing is the process by which the router ascertains what is the best path for the packet to reach the destination. It maintains a routing table which is made using different algorithms by the router only.

- **Contribution towards Network Security:**

- Routers select a path between networks, and they securely transmit information packets across that path toward an intended destination. In so doing, they draw on routing protocols and algorithms.

- Modern routers often have firewalls to protect against untrusted networks. They also are known for their VPN handling.

- Routers also commonly perform network address translation which restricts connections initiated from external connections.

- They also filter MAC addresses.

- <u>Network Isolation/segmentation</u>: Guest networks are merely an appetizer, using VLANs for network isolation is the main course. Devices that only need Internet access should be prevented from seeing and being seen by other devices on the LAN. This prevents a single hacked device from causing grief for other devices on your network.

1.4. MODEM

- **<u>Characteristics</u>:**

  - Modem are computer hardware device that converts data from a digital format into a format suitable for an analog such as telephone or radio.

  - It transmits data by modulating one or more carrier wave signals to encode digital information, while the receiver demodulates the signal to recreate the original digital information.

  - It also modulates and demodulates analog carrier signals (called sine waves) for encoding and decoding digital information for processing. Modems accomplish both of these tasks simultaneously and, for this reason, the term modem is a combination of "modulate" and "demodulate".

- The goal is to produce an electrical signal that can be transmitted easily and decoded reliably.

- Modems can be both WIRED and WIRELESS.

○ **OSI Layer:**

A modem operates in the 2nd layer of the OSI model which is the Data Link Layer.

○ **Purpose of the Device:**

- The modem takes signals from our ISP and translates them into signals our local devices can use, and vice versa.

- Then this data is transmitted over the telephone lines with using V.92, to analog modems which helping out for converting those signals back to digital form for readable format to computer. Some of the functions are:

- Data Compression: To decrease the amount of time when it tries to send data and for cutting down on the percentages of errors in the all flowing of signals, then modem required the data compression mechanism. So, this data compression method helps to reduce the size of signals, which are required for sending data.

- Error Correction: In the error correction techniques, all devices monitor all information while receiving is undamaged. It splits all information into small units that is called the “Frames”. In this process, it tags all frames along with checksums, but it is done before sending information. Checksum is a special technique that helps to check redundancy in the presented data in the computer. If this information matches with checksums then device grabs the verified information. That is sent by error-correcting modem. But if it gets to fail in matching with checksum then information is moved back.

- Modulate Signals: The main function of modem is to transmit and decode all signals which allow sending digital data from one node to other nodes without getting any damage of information.

- Flow Control: Each modem has different speed of sending signals. so, it can generate issues during to receive signals if any one device’s speed down of them. So, in the flow control technique, slower one signals the faster one to pause, by sending a ‘character’. If, slow device will try to send character to faster modem, then this character would be a signal to the faster modem for Pausing the information transfer until the slow modem gets caught up.

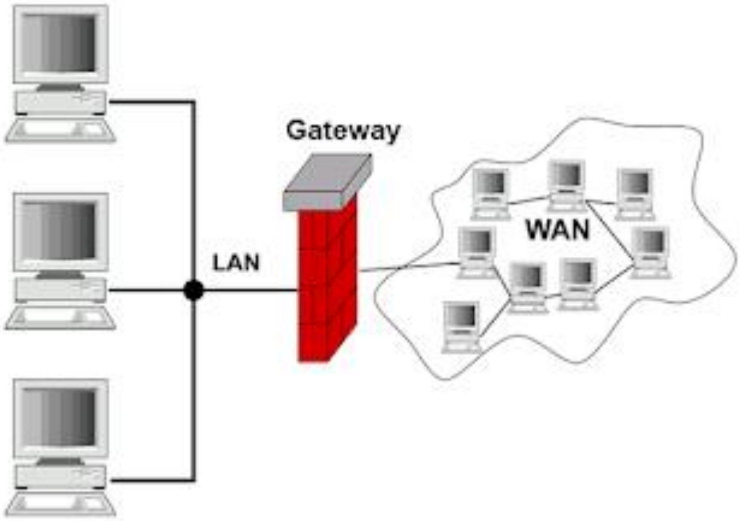
- **Contribution towards Network Security:**

  The modem does not contribute to network security because:

  - They are meant for converting signals from one form to the other which involves no security.
  - Modems are not intelligent enough to read packet headers thereby making it difficult to implement security mechanisms.
  - Security is handled much more effectively at the router and switch level.

  Iterating to the above points, modems raise a number of security concerns. It is because they create links between our computer and the outside world. Modems can be used by individuals inside our organization to remove confidential information and gain unauthorized access to our computer. If our modems can be reprogrammed or otherwise subverted, they can be used to trick your users into revealing their passwords. And, finally, an attacker can eavesdrop on a modem communication.

1.5. GATEWAY



- **Characteristics**:

  - A gateway is a hardware device that goes about as a “gate” between two networks. It might very well be a server, firewall, router, or another device that empowers traffic to stream all through the network.

  - It is a network node that forms a passage between two networks operating with different transmission protocols. 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.

  - It performs the task of being a translator between two systems that use different communication protocols, data frame formats or architecture.

  - On-premise of the direction of data flow, types of a gateway in networking are extensively separated into two classes:

    - Unidirectional Gateways: They permit data to stream just a single direction. Changes made in the source node are duplicated in the destination node, however not the other way around. They can be utilized as archiving devices.

    - Bidirectional Gateways: They permit data to stream in two directions. They can be utilized as synchronization devices.

  - Gateways can be both WIRED and WIRELESS.

- **OSI Layer**:

  - The Layer in which Gateway operates is heavily debated. Some argues that the most common type of gateways, the Network Gateway, operates at Layer 3 (i.e., Network Layer of OSI). While some say it operates at Layer 4 or above, others say it does at the 5th Layer.

  - Many research papers and classic textbooks also argue that, depending upon the functionality, a gateway can operate at any of the 7 layers of OSI model.

- **Purpose of the Device**:

  - The main purpose of Gateway is that in case any two systems do not share routing protocols, it takes a gateway to get them together.

  - Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network. The purpose is to translate all protocols on one network into the protocols on another.

- It forms a passage between two different networks operating with different transmission protocols. A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks. The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.

- It also stores information about the routing paths of the communicating networks. When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.

- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software. It uses packet switching technique to transmit data across the networks.

- **Contribution towards Network Security:**

  - Gateways come with a proxy server. A proxy can keep the internal network structure of a company secret by using network address translation, which can help the security of the internal network.

  - Secure web gateways offer a way to keep networks from falling victim to incursions through internet traffic and malicious websites. They prevent data from such places from entering the network and causing a malware infection or intrusion.

  - They are often embedded with a firewall as well.

  - Encrypted traffic analysis: The gateway compares all traffic to local and global threat lists and reputation sources first, then also analyses the nature of the traffic itself to determine if any content or code poses a threat to the network. This includes SSL-based encrypted traffic.

  - Integration with security monitoring: Security administrators are notified of any web gateway security problems via their monitoring solution of choice, typically a security information and event management (SIEM) solution.

  - Gateways also provide secure internet access when users are disconnected from the VPN.

PART-B: Comparison

- Differences between all Network Security Devices:

Sl.	Metric	Hub	Switch	Router	Modem	Gateway
1.	**OSI Layer**	Physical Layer Device (Layer 1)	Data Link Layer Device (Layer 2)	Network Layer Device (Layer 3)	Data Link Layer Device (Layer 2)	Operates up to 5 Layers of the OSI Model (can be 7; debated)
2.	**Purpose**	Connects segments of a LAN	Responsible for processing and routing data at the data link layer	Manages traffic between networks	Takes signals from ISP and translated into signals	Translates all protocols on one network into the protocols on another
3.	**Security**	Network Traffic Monitoring	Intrusion Prevention	Firewall	No Security feature	Integrates Proxy Server
4.	**Routing Mechanism**	Transmits data to all connected hosts	Uses MAC Address	Uses routing table and IP addresses of device	No routing mechanism	No routing mechanism
5.	**Data Transmission Form**	Electrical signals or bits	Frames	Packets	Electrical signals	Segments
6.	**Functionality**	A Hub is a multiport repeater in which a signal introduced at the input of any port appears at the	A Switch is a tele-communication device which receives a message from any device connected to it and then transmits the message only to the device for which the message is intended.	A router reads the header of incoming packet and forward it to the port for which it is intended there by determines the route. It can also perform filtering and encapsulation.	The main function of modem is to transmit and decode all signals which allow sending digital data from one node to other nodes without getting any damage of information.	The main function of a gateway is to translate one protocol to the other. It does not support dynamic routing.

7.	**Working Principle**	A Hub works on the basis of broadcasting.	Switch works on the basis of MAC address.	A router works on the basis of IP address.	A modem is typically used to send digital data over a phone line. The sending modem modulates the data into a signal that is compatible with the phone line, and the receiving modem demodulates the signal back into digital data.	Working principle of a gateway is to differentiate what is inside the network and what is outside the network.
8.	**Intelligence**	Hub is not an intelligent device that may include amplifier on repeater.	A Switch is an intelligent device as it passes on the message to the selective device by inspecting the address.	A router is more sophisticated and intelligent device as it can read IP address and direct the packets to another network with specified IP address.	A electronic equipment converts digital signal of our laptop to the analog signal and its vice-versa is also true.	It is a device that is used for the communication among the networks which have a different set of protocols
9.	**Network requirement**	At least single network is required to connect.	At least single network is required to connect.	Router needs at least two networks to connect.	Modems can communicate across multiple networks but need two in the least.	Gateways needs at least two networks to connect.

2. TYPES OF ROUTERS

There are five main types of routers in the market according to the application category. They are wired routers, wireless routers, core routers, edge routers and VPN routers.

2.1. WIRED ROUTERS

- A wired router makes use of physical cables with the purpose of connecting multiple devices which eventually creates a LAN.
- Wired router uses IEEE 802.3 and 802.1 protocols to establish wired connection between hosts within a LAN.
- Wired routers make use of physical ports in order to facilitate transmission of data between hosts in a local area network.

2.2. WIRELESS ROUTERS

- Wireless router distributes data packets by converting them into radio signals and thus creating a WLAN (wireless Local Area Network).
- Wireless routers use IEEE 802.11 protocol to create a Wireless Local area network in order to establish connection between various devices.
- Wireless routers are generally slower than wired routers as there is a lot of interference over a wireless network.

2.3. CORE ROUTERS

- This is a wired or wireless router that distributes data packets between one or more networks but not within a network.
- As their name indicates, edge routers are placed at the edge or boundary of networks, and typically connect to Internet service providers (ISPs) or other organizations' networks.
- Their job is to keep your network communicating smoothly with other networks.

2.4. EDGE ROUTERS

- These wired or wireless routers distribute data packets within networks, but not between multiple networks.
- They're designed to become the backbone of your network and do the heavy lifting of data transfer, which is why they're usually high-performance.

2.5. VPN ROUTERS

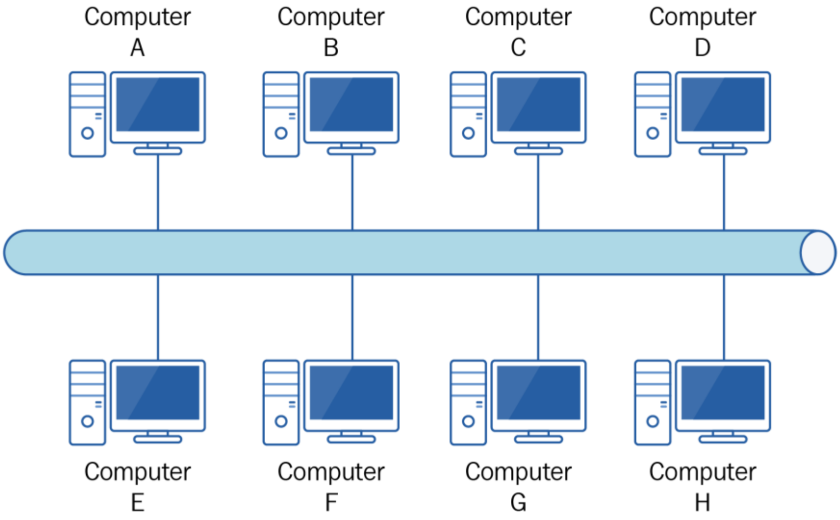
- A VPN router can be seen as a normal Gigabit router that has VPN client software installed on it. Every device that connects to the VPN router is protected by VPN at any time.
- It can bring numerous benefits of VPN connections to all devices.

3. TYPES OF NETWORK TOPOLOGY

In a computer network, there are 6 different types of network topology. Those are mentioned below:

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

3.1. BUS TOPOLOGY



About:

- Bus topology is a network, in which all the computer nodes and network system are connected to a single transmission channel.
- A single cable links all of the included nodes in a bus topology. The primary cable serves as the network's backbone. The computer server is one of the machines on the network. A linear bus topology is defined as having two terminals. Data can only be transmitted in one direction.
- Linear Bus topology: when it has exactly two endpoints.
  Distributed bus topology: when it has more than two endpoints.

Features:

- It transfers the data in a single direction.
- There is a single connection between the node/system and the channel.

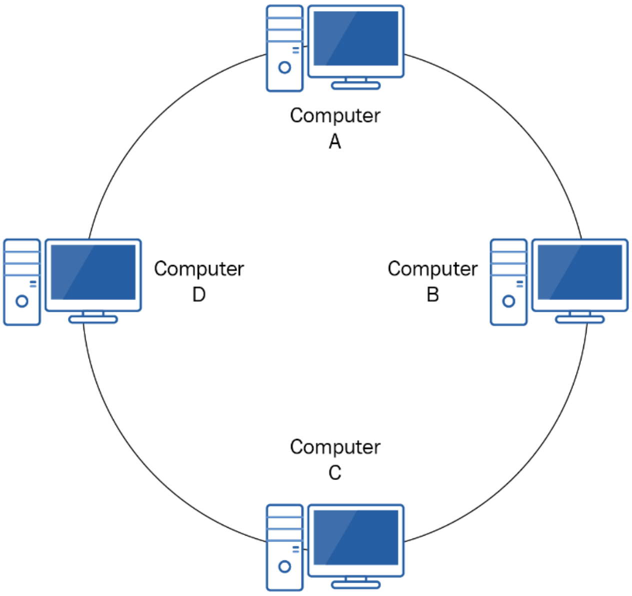
Advantages:

- Cost of the cable is very less as compared to other topologies, so it is widely used to build small networks.
- It is much easier to introduce a node into the network as it requires only one connection to the main cable.
- It is easy to expand and takes less time to set up.

Disadvantages:

- Single point of failure: In case if the common cable fails, then the entire system will crash down.
- No bi-directional communication.
- Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.

3.2. RING TOPOLOGY



About:

- In a ring network, every device has exactly two neighbouring devices for communication purposes. It is called a ring topology as its formation is like a ring.
- In this topology, every computer is connected to another computer. Here, the last node is combined with the first one.
- This topology uses a token to pass the information from one computer to another. In this topology, all the messages travel through a ring in the same direction (Unidirectional traffic).

Features:

- To prevent the loss of the transmission data from the first node to the last node say i.e,1000th node, number of repeaters are deployed in the network.
- Dual Ring Topology: Bidirectional connections between each network node.
- Data is transmitted in a sequential manner it can’t skip device in between.

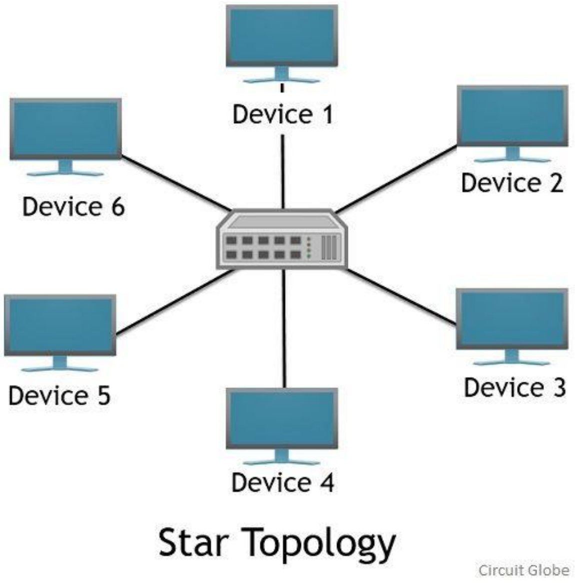
Advantages:

- Faster error checking and acknowledgment.
- Offers equal access to all the computers of the networks.
- Chance of collision is less.
- Cheap to set up and expand.

Disadvantages:

- Break in a single ring can risk the breaking of the entire network.
- In the ring, topology signals are circulating at all times, which develops unwanted power consumption.
- Difficult to troubleshoot.
- Adding or removing a computer will disturb the transmission of the data in the network.

3.3. STAR TOPOLOGY



About:

- In the star topology, all the computers connect with the help of a hub. This cable is called a central node, and all other nodes are connected using this central node. It is most popular on LAN networks as they are inexpensive and easy to install.
- All the data on the star topology passes through the central device before reaching the intended destination.

Features:

- Every computer is connected to the hub through a dedicated connection/cable.
- Hub also acts as a repeater.

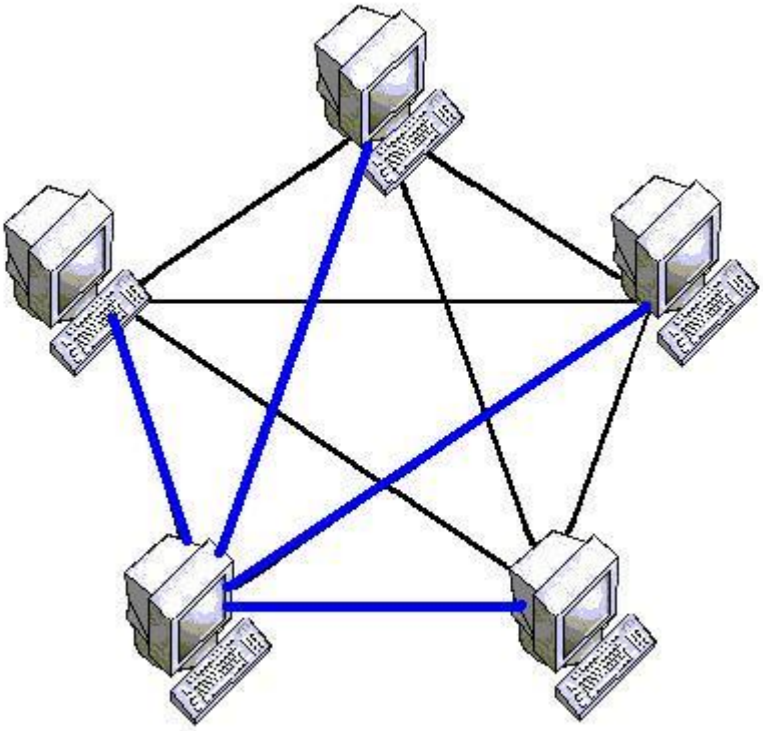
Advantages:

- In Star topology, addition, deletion, and moving of nodes is easy.
- With few nodes and limited network traffic, the topology has fast performance.
- Failure of one computer will not affect other computers in a network.
- Easy to troubleshoot.
- Hub can be easily replaced.

Disadvantages:

- If the hub or concentrator fails, attached nodes are disabled.
- That means, Failure of the hub will stop the transmission.
- The installation of star topology is costly
- Performance of transmission depends on the hub.

3.4. MESH TOPOLOGY



About:

- The mesh topology has a unique network design in which each computer on the network connects to every other. It develops a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, still data has an alternative path to reach its destination.

Features:

- The total number of ports that are required by each device is N-1. (If 5 devices are connected then 4 ports are required) The total number of dedicated links required to connect them is N(N-1)/2. i.e, if there are 5 computers connected to it than required dedicated link will be 5*4/2 = 10

- It can be divided into two kinds: 1. Fully connected mesh topology: all the nodes connected to every other node. 2. Partially connected mesh topology: It does not have all the nodes connected to each other.

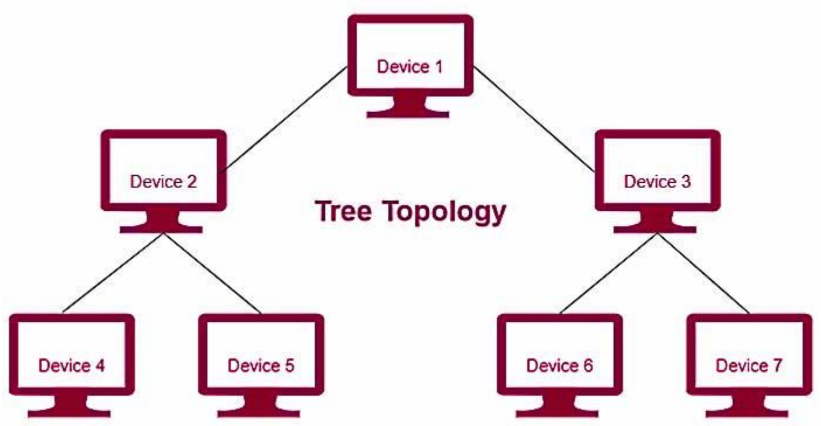
Advantages:

- No traffic problem as nodes have dedicated links.
- It has multiple links, so if any single route is blocked, then other routes should be used for data communication.
- It is robust. A fault is diagnosed easily.
- Provides privacy and security.

Disadvantages:

- It is expensive due to the use of more cables. No proper utilization of systems.
- Installation is complex because every node is connected to every node.
- The cost of implementation and maintenance is higher.
- Suitable for lesser number of devices, as cable cost is high.

3.5. TREE TOPOLOGY



About:

- There is a root node in a tree topology, and all other nodes are linked to form a hierarchy. Hierarchical topology is another name for it. This topology is known as a Star Bus topology because it combines many star topologies into a single bus.
- The tree topology, which is comparable to the bus and star topologies, is a highly frequent network.
- It is also known as hybrid topology that combines characteristics of linear bus and star topologies. It includes at least three specific levels.

Features:

- Usually implemented in WAN.

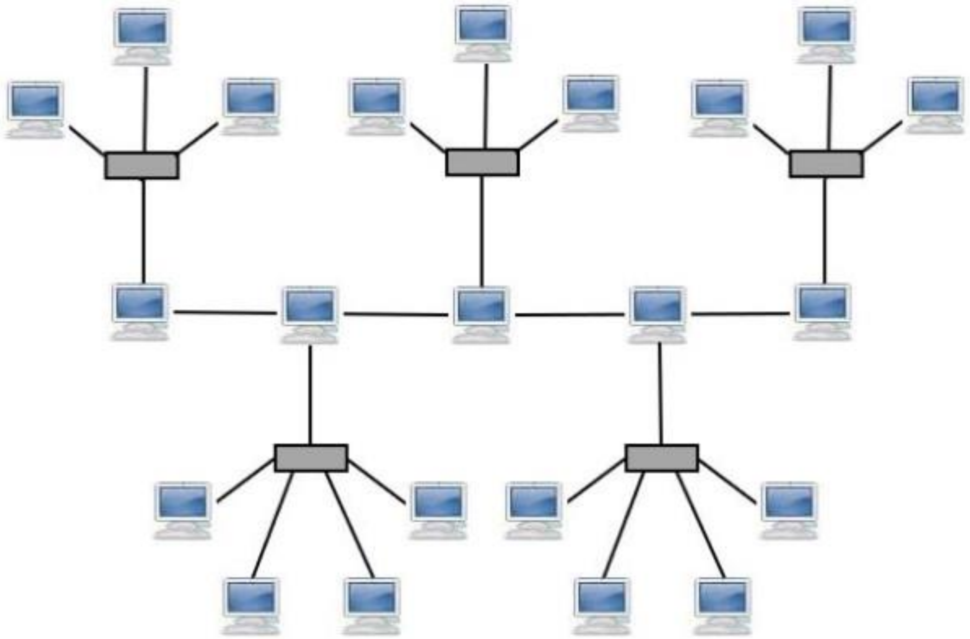
Advantages:

- Node expansion is fast and easy.
- Detection of error is an easy process.
- That is, Easier fault finding and maintenance
- Includes Features of star and bus topology.

Disadvantages:

- If more nodes are added, then its maintenance is difficult.
- If the hub or concentrator fails, attached nodes are also disabled.
- If the root node fails then the whole network will fail and will stop its processing.

3.6. HYBRID TOPOLOGY



s

About:

- Hybrid topology combines two or more topologies. For example, as you can see in the above image that in an office in one department, Star and P2P topology is used.
- A hybrid topology is always produced when two different basic network topologies are connected.

Features:

- Collection of two or more topology.

Advantages:

- Offers the easiest method for error detecting and troubleshooting.
- Highly effective and flexible networking topology.
- Easy to increase the size of the network by adding new components.

- Design in such a way that the strength of constituent topologies is maximized

Disadvantages:

- The design of hybrid topology is complex.
- It is one of the costliest processes in terms of installation and maintenance.

4. TYPES OF MODEMS

1. External modem

About:

- It is connected outside the system using a serial cable.

Characteristics:

- Installation is very easy.
- It provides high data transmission rates.
- It is very expensive.

2. Internal Modem

About:

- It is installed over a PCs motherboard

Characteristics:

- Mounted to an expansion slot of the motherboard.

- Data transmission is slow.
- It is complex to install.

3. Wireless Modem

About:

- Connected to computer systems without any cable.

Characteristics:

- They provide high transmission speed.
- They make use of radio frequencies to transmit data.
- Low cost of installation.

4. Dial-Up Modem

About:

- Dial-up modem instantiates the internet connection by connecting the ISP to thecomputer through the conventional telephone line.

Characteristics:

- It is used in PSTN(public switched telephone network) to provide internet access.
- Speed of transmission is very low.
- It is inexpensive and relatively easy to install.

5. Cable Modem

About:

- They use landline connections in order to allow computers to communicate with ISP.

Characteristics:

- They make use of the coaxial cable to connect with the landline.
- Their transmission rate is medium.
- They are connected to the computer using ethernet cable.
-

6. DSL Modem

About:

- DSL(Digital Subscriber line)allows the transmission of data over the normaltelephone line.

Characteristics:

- They provide a high transmission speed.
- It is used to connect to a computer or router to provide the internet connection usingthe ethernet or USB port.
- Low cost of installation.

7. **Satellite Modem**

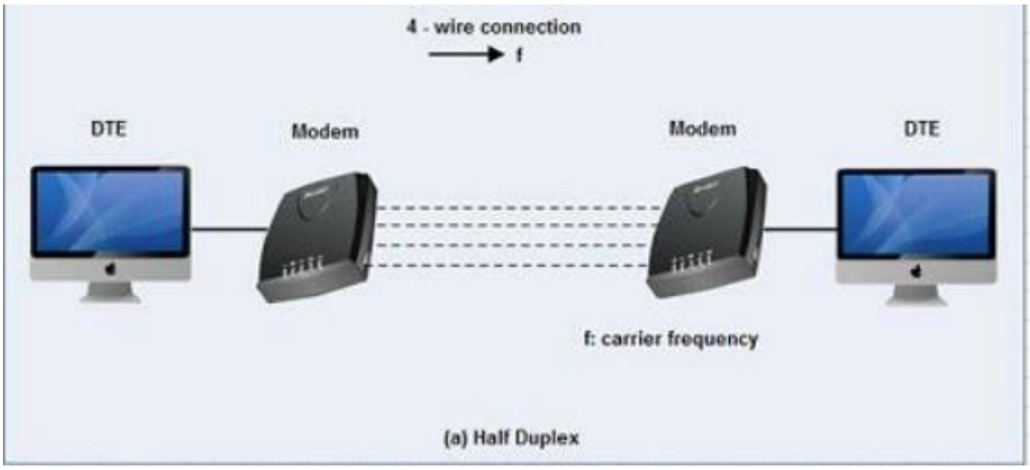
About:

- Do not need any telephone connection for the internet.

Characteristics:

- To send or receive data, it uses satellite technology.
- The speed of the modem is comparatively slower than DSL or cable Modem.
- Satellite modems are expensive modems

8. **Half Duplex Modem**



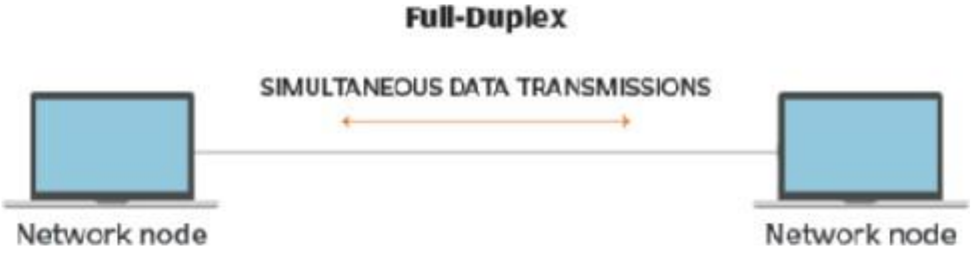
About:

- Allows transmission of the data in only one direction at a time.

Characteristics:

- They are inexpensive.
- Slow data transmission rates as only one party is permitted to send data at a time
- They are more widely used than full duplex modems.

9. Full Duplex Modem



About:

- Allows transmission of the data in both directions simultaneously.

Characteristics:

- They are expensive.
- Fast data transmission rates as both parties are permitted to send data simultaneously.
- They are less popular than full duplex modems.

10. 2-wired Modem

About:

- It uses a pair of wires hence called two-wire modems

Characteristics:

- Not very popular in comparison to 4 wired.
- Low transmission rates due to fewer wires.
- Less expensive and easy to install.

11. 4- Wired Modem

About:

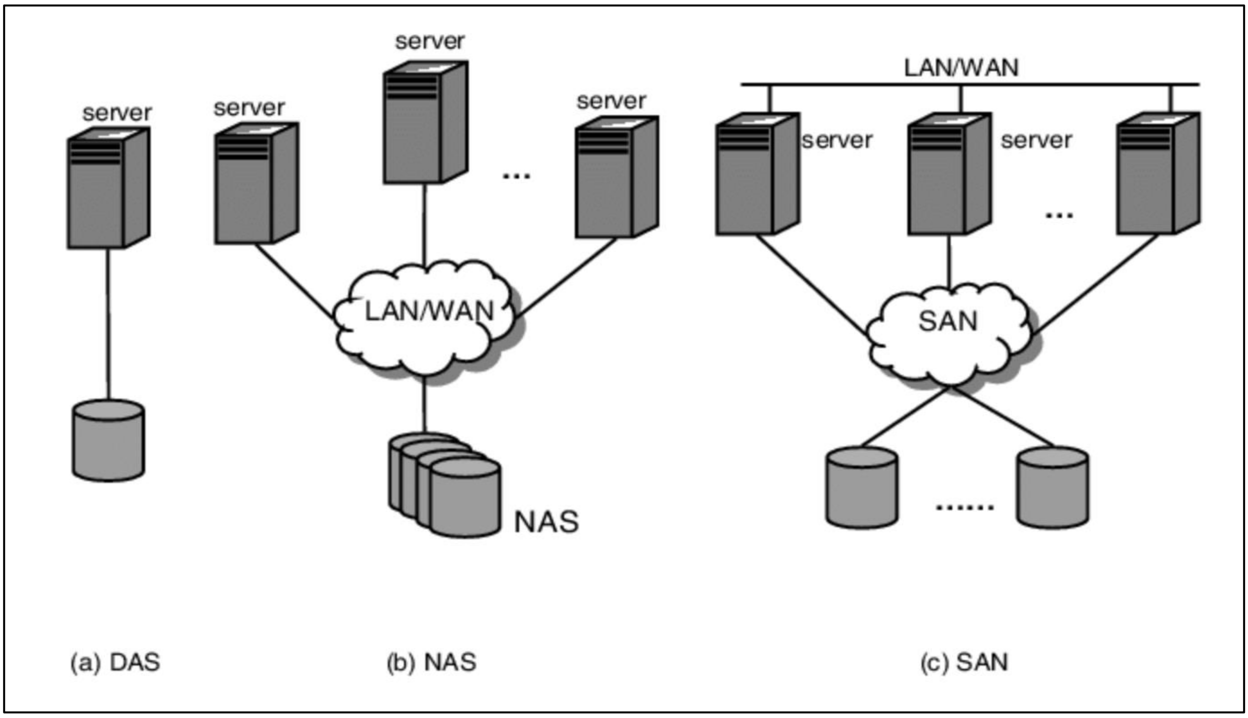
- It splits the pair of wires for incoming and outgoing data carriers.

Characteristics:

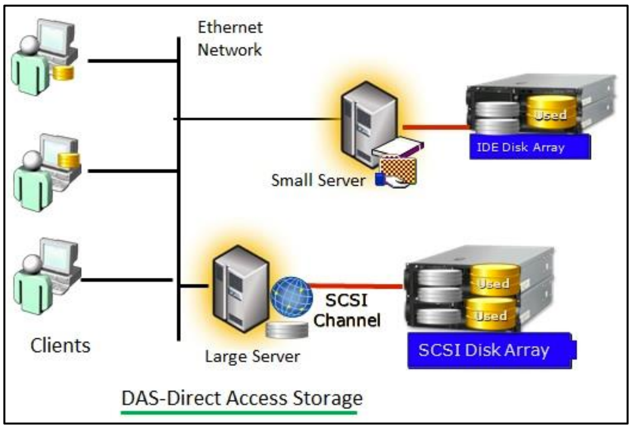
- It can transmit the same frequency on both ends.
- Faster data transmission rate than 2 wired modems.
- It is costlier than 2 wired modems.

5. NETWORK STORAGE

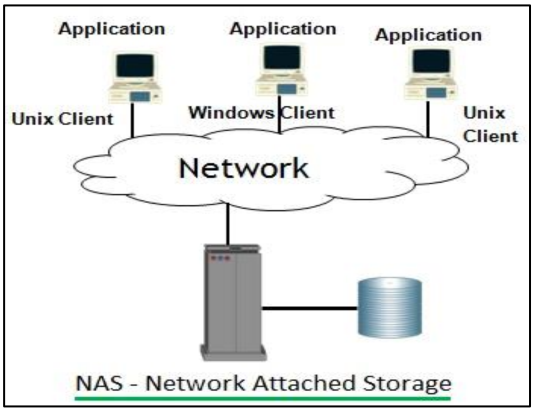
Storage Type	**DAS**	**NAS**	**SAN**
Full Form	Direct Access Storage	Network Attached Storage	Storage Area Network
Data transfer protocol	SCSI/FC/ATA	TCP/IP	FC
Use Standard File sharing protocol?	No	Yes(NFS/CIFS)	No
Centralized management	According to the environment	Yes	Yes(managementtool required)
Disaster tolerance	Low	High	High
Transfer object	Data	Document	Data
Storage type	Sectors	Shared Files	Blocks
Data Transmission	IDE/SCSI	TCP/IP	Fiber Channel
Access Mode	Clients or Servers	Clients or Servers	Storage type
Capacity in Bytes	10^9	10^9 to 10^{12}	$>10^{12}$
Complexity	Easy	Moderate	Difficult
Management cost (per GB)	High	Moderate	Low



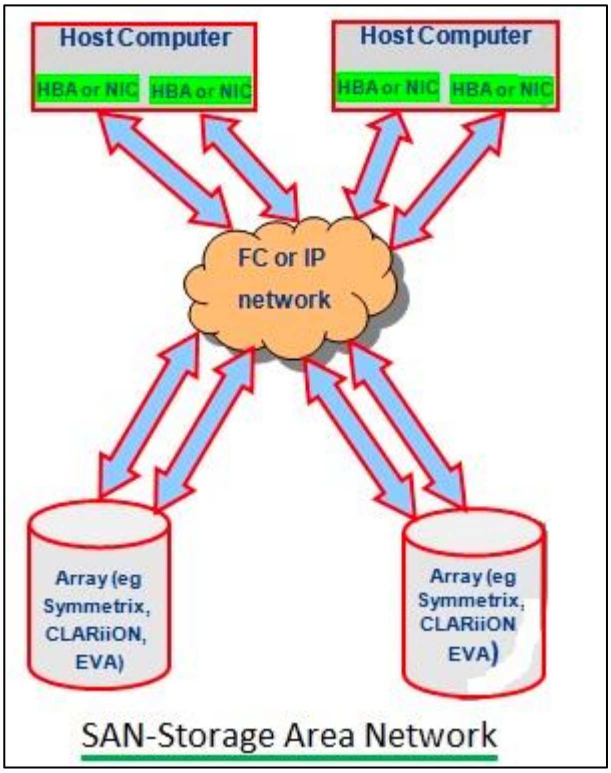
DAS:


Ethernet
Network
Used
IDE Disk Array
Small Server
SCSI
Channel
Used
Used
SCSI Disk Array
Clients
Large Server
DAS-Direct Access Storage

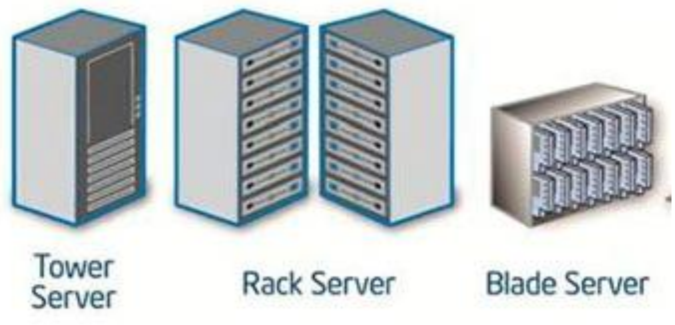
NAS:


Application
Application
Application
Unix Client
Windows Client
Unix
Client
Network
NAS - Network Attached Storage

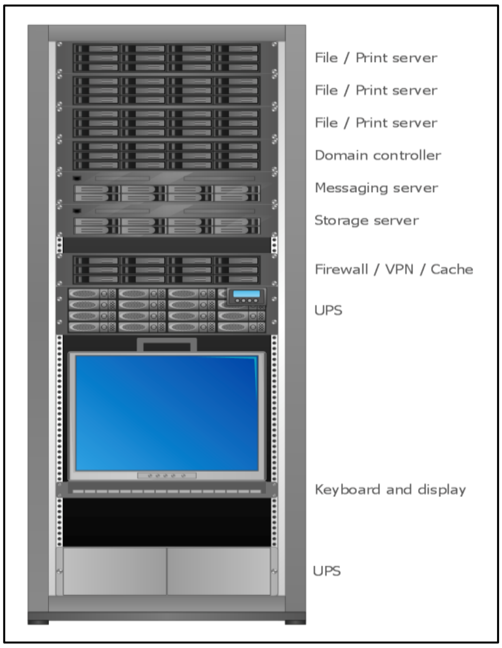
SAN:


Host Computer
HBA or NIC
HBA or NIC
Host Computer
HBA or NIC
HBA or NIC
FC or IP
network
Array (eg
Symmetrix,
CLARiiON,
EVA)
Array (eg
Symmetrix,
CLARiiON
EVA)
SAN-Storage Area Network

6. SERVER



1. Server Rack (Rack Mounted)



Characteristics:

- Specially designed to be installed in a framework called a rack, rack servers (also known as rack mount servers) are stored in mounting slots called bays and are secured in place with screws.
- Multiple servers, stacked one above the other, can be stored on a single rack which helps to consolidate network resources and minimize the amount of floor spacerequired
- Rack servers are available in four size options in the market, 1U, 2U, 4U and 8U.
- Rackmount servers are often used for mail and file servers.
- The basic components of a rack server are: motherboard, CPU, HBA, RAM, Drive Bays and a CPU.

2. Server Tower

Characteristics:

- A tower server is a computer that is structured in an upright cabinet that stands aloneand that is designed to function as a server.
- Easier cooling, owing to the fact that overall component density is fairly low.
- Tower servers are widely used thanks to their scalability and reliability features.
- In comparison to a blade server, tower servers are heavier and bulkier.
- They are often very noisy because each tower requires a dedicated fan.

3. Blade Server

Characteristics:

- Blade servers are designed to mitigate the space and energy constraints of a typicaldata center.
- The tasks of a blade server are: File sharing, database and application hosting, SSLencryption for web communications and hosting virtual server platforms.
- Each blade server in an enclosure may be dedicated to a single application.
- The modular design of the blade server helps to optimize server performance andreduce energy costs
- It reduces cabling, redundancy and requires minimum administration.

7. TYPES OF INTERFACES

The **TCP/IP** Network Interface layer formats IP datagrams at the Network layer into packets that specific network technologies can understand and transmit.

A network interface is the network-specific software that communicates with the network-specific device driver and the IP layer in order to provide the IP layer with a consistent interface to all network adapters that might be present.

The IP layer selects the appropriate network interface based on the destination address of the packet to be transmitted. Each network interface has a network address. The Network Interface layer is responsible for adding or removing any link layer protocol header required to deliver a message to its destination. The **network adapter** device driver controls the network adapter card.

Types of Interfaces:

1. WiFi

About:

- Wi-fi uses IEEE 802.11 protocol/standard for setting up Wireless Local area
networks.(a/b/g)
- The 802.11 standard provides multiple distinguishable radio frequency ranges for use in Wi-Fi communications: 900 MHz, 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, 5.9 GHz and 60 GHz bands
- The elements of a Wi-fi network are: Wireless Host, Base station(access point),Wireless Link(to connect host to base station), Wifi-cards and safeguards(firewall etc.).

2. Ethernet

About:

- Ethernet follows the IEEE 802.3 standard for establishing wired local area networks.
- Ethernet is known to provide services in Data link Layer(OSI layer 2) and Physical layer.
- Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses, and error-checking data so that damaged frames can be detected and discarded; most often, higher-layer protocols trigger retransmission of lost frames.

3. Bluetooth

About:

- Bluetooth is a radio wave technology that is mainly designed to enable wirelesscommunications over short distances.
- Bluetooth uses IEEE 802.15.1.
- It is known for Low cost, its ease of use, penetration through walls, ad hocconnection, and fast voice and data transfer.

4. LAN

About:

- In wired LANs, twisted pair cable and optical fiber cables are utilised to interconnect hosts.
- A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.
- Ethernet and Wi-Fi are the two most common technologies in use for local area networks