Network Security or Networking

UNIT -I

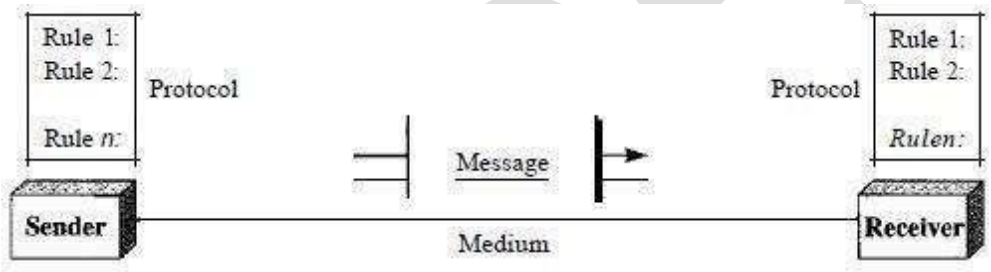
Introduction to Computer Networks

Data Communication: When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

Computer Network: A computer network is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered a computer network.

Components:

A data communications system has five components.



1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves

5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (Os or Is). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers:

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution.* For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image. After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only blackand- white dots (e.g., a chessboard), a I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three

primary colors: *red*, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio:

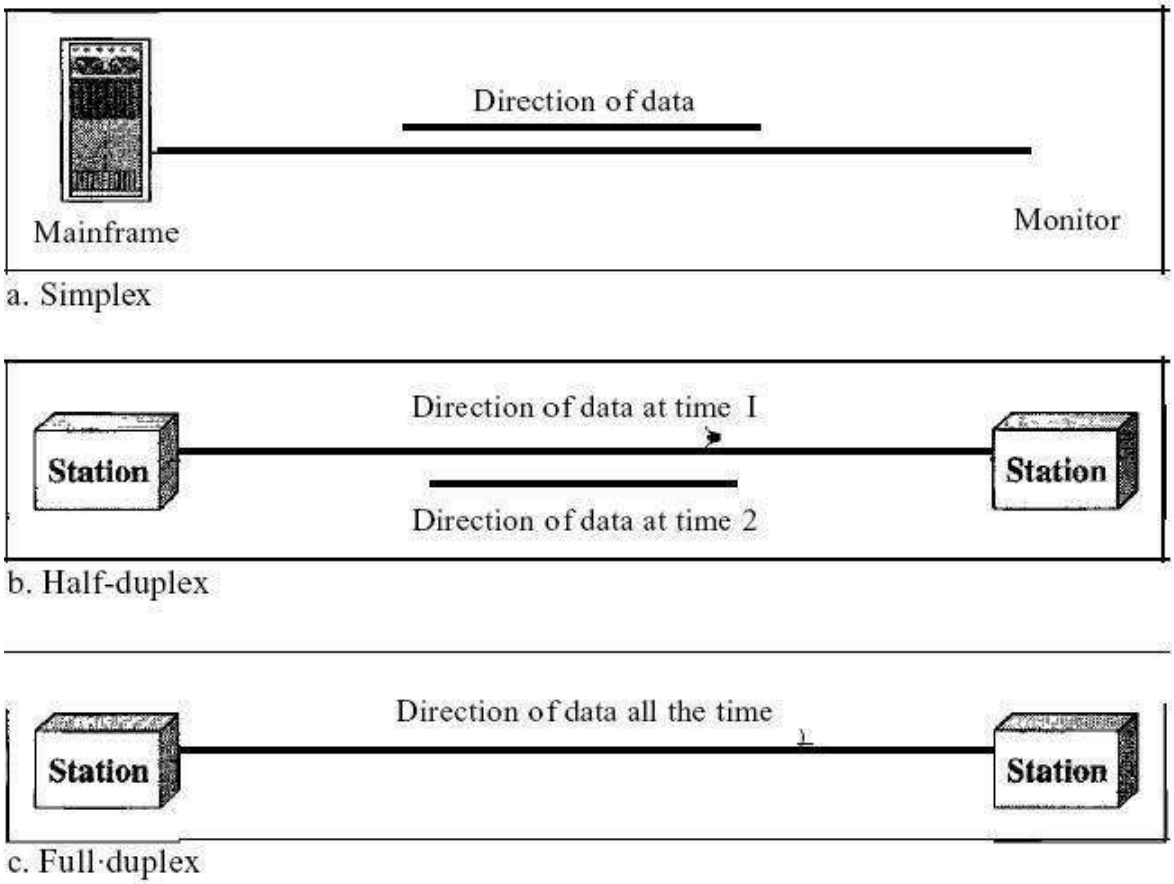
Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal. In Chapters 4 and 5, we learn how to change sound or music to a digital or an analog signal.

Video:

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again we can change video to a digital or an analog signal.

1.1.1 Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure



Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex:

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa The half-duplex mode is like a one-lane road with traffic allowed in both directions.

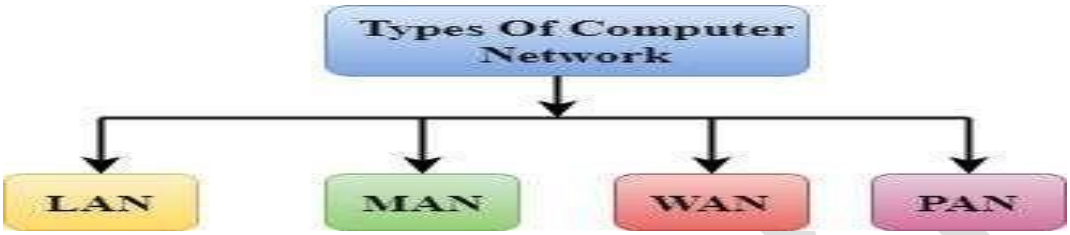
When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction. *Full-Duplex:*

In full-duplex both stations can transmit and receive simultaneously (see Figure c). The full-duplex mode is like a tW<D-way street with traffic flowing in both directions at the same time. In full-duplex mode, si~nals going in one direction share the capacity of the link: with signals going in the other din~c~on. This sharing can occur in two ways: Either the link must contain two physically separate t:nmsmissiIDn paths, one for sending and the other for receiving; or the capacity of the ch:arillilel is divided between signals traveling in both directions. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

Types of Computer Networks:

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

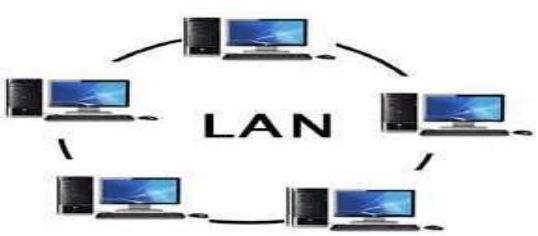


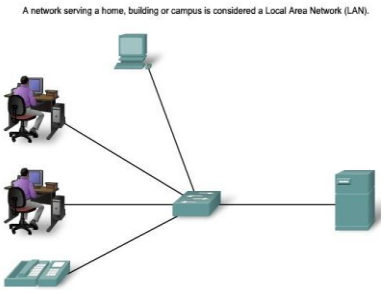
5

1. **Local Area Network (LAN).**
2. **Metropolitan Area Network (MAN).**
3. **Wide Area Network(WAN).**
4. **Personal Area Network.** A **Personal Area Network** (**PAN**) is the most basic type, usually used for homes or home offices. ...

Local Area Network (LAN) :

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





Metropolitan Area Network(MAN) : A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.

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

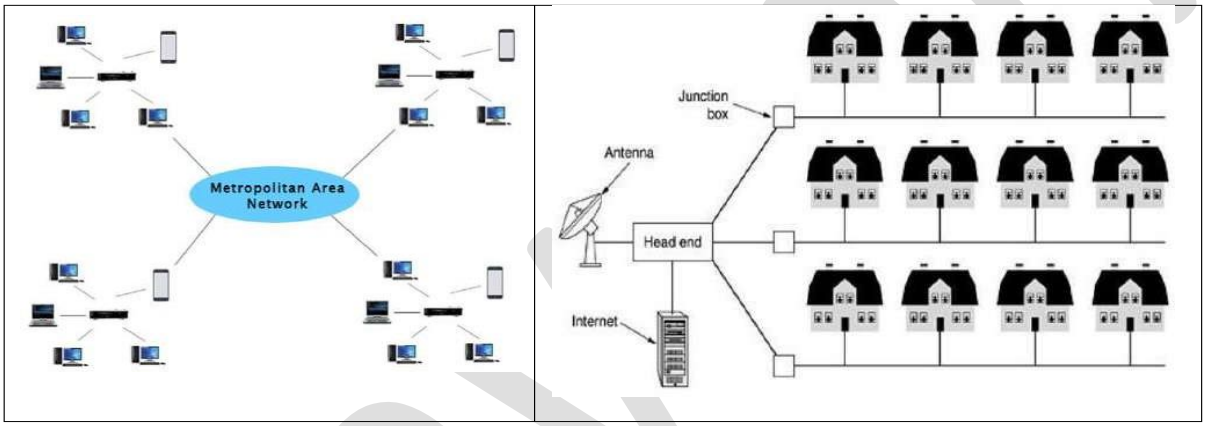
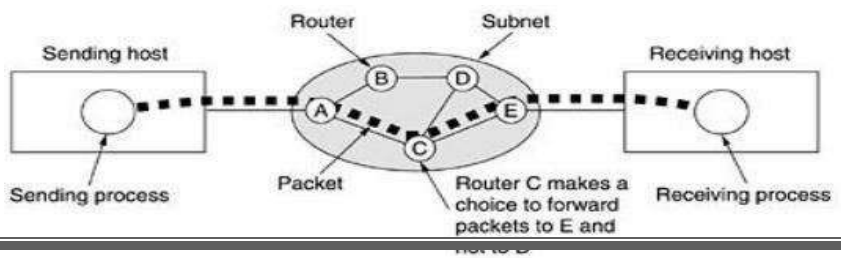


Fig.: Metropolitan area network based on cable TV. Wide Area Network (WAN) :

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not

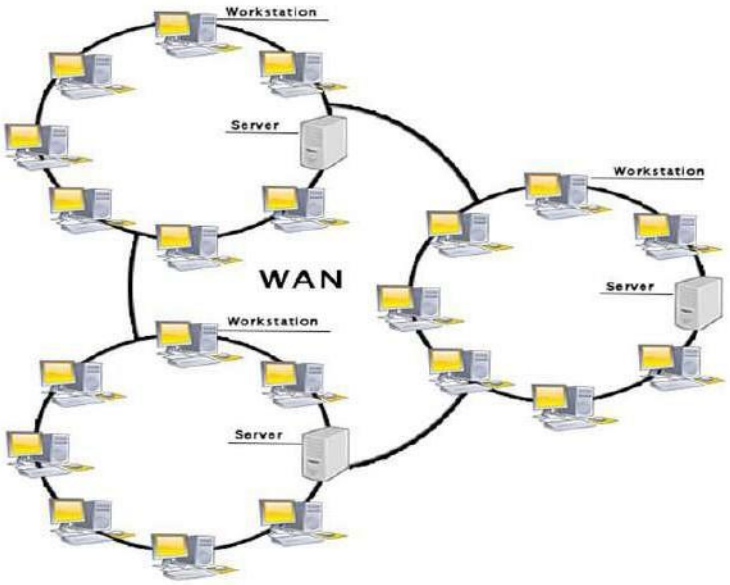
share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one route to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there



until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet.

Fig.: A stream of packets from sender to receiver

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



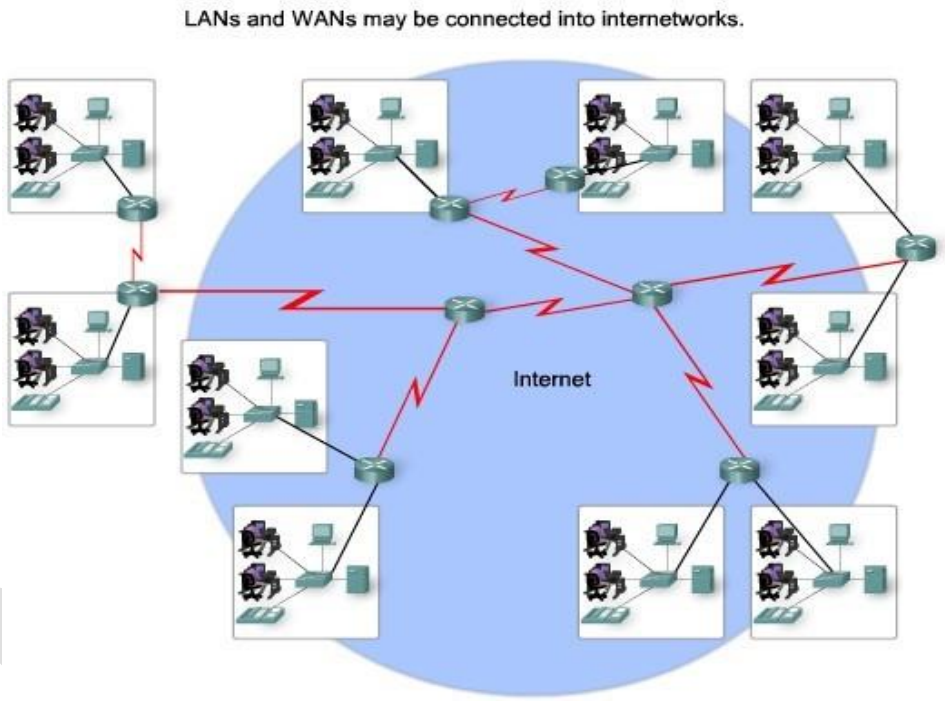
Personal Area Network (PAN):

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

Internet:

The network formed by the co-operative interconnection of a large number of computer networks.

• Network of Networks
• No one owns the Internet
• Every person who makes a connection owns a slice of the Internet.
• There is no central administration of the Internet.



Internet is comprises of :

A community of people : who use and develop the network.

*A collection of resources:*that can be reached from those networks.

A setup to facilitate collaboration: Among the members of the research and educational communities worldwide.

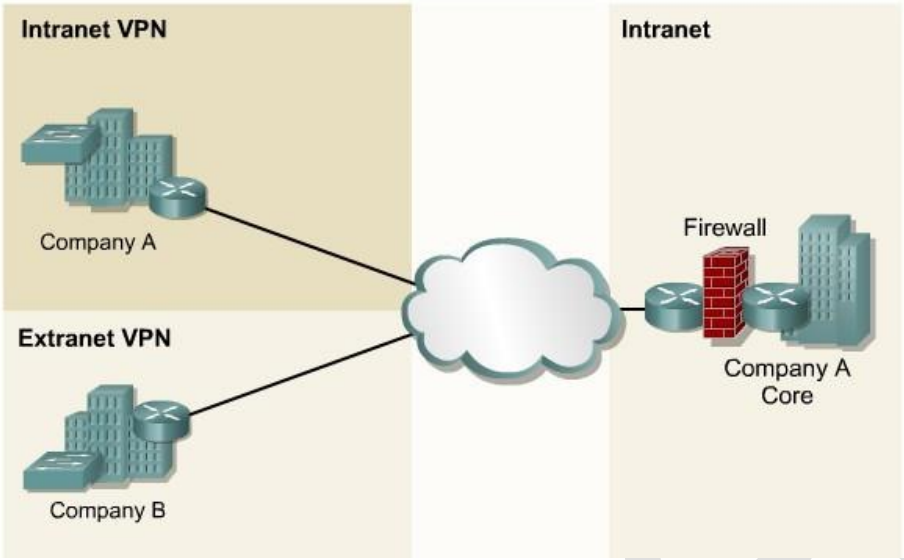
The connected networks use the TCP/IP protocols:

important Internet applications:
world wide web(WWW) File Transfer Protocol(FTP)Electronic Mail
Internet Relay Chat

Intranet:

A private TCP/IP internetwork within an organization that uses Internet technologies such as Web servers and Web browsers for sharing information and collaborating. Intranets can be used to publish company policies and newsletters, provide sales and marketing staff with product information, provide technical support and tutorials, and just about anything else you can think of that fits within the standard Web server/Web browser environment.

Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization. Intranets are designed to permit users who have access privileges to the internal LAN of the organization. Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data.


Intranet VPN
Intranet
Company A
Firewall
Extranet VPN
Company A
Core
Company B

Extranet:

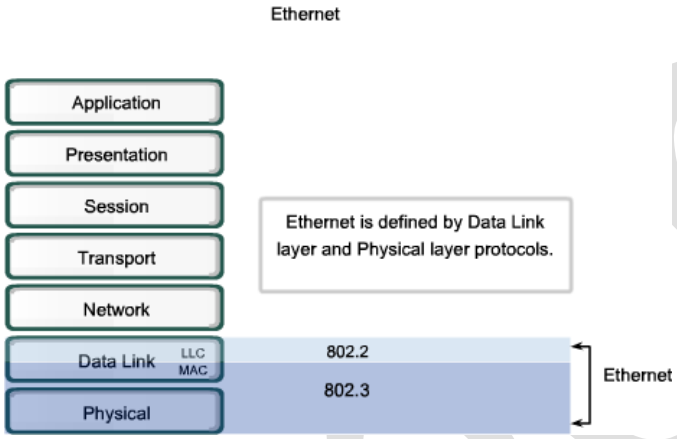
Extranets refer to applications and services that are Intranet based, and use extended, secure access to external users or enterprises. This access is usually accomplished through passwords, user IDs, and other application- level security. An extranet is the extension of two or more intranet strategies with a secure interaction between participant enterprises and their respective intranets.

Part of a Company's Intranet that is extended to users outside the company(eg. Normally over the Internet). In its simplest form, a private TCP/IP network that securely shares information using Hypertext Transfer Protocol (HTTP) and other Internet protocols with business partners such as vendors, suppliers, and wholesale customers.An extranet is thus a corporate intranet that is exposed over the Internet to certain specific groups that need access to it. Extranets built in this fashion follow the client/server paradigm, with Web servers such as Apache.

Extranets are a powerful tool because they let businesses share resources on their own private networks over the Internet with suppliers, vendors, business partners, or customers. Extranets are typically used for supporting real-time supply chains, for enabling business partners to work together, or to share information such as catalogs with customers. The power of the extranet is that it leverages the existing technology of the Internet to increase the power, flexibility, and competitiveness of businesses utilizing well-known and easily used tools such as Web servers and Web browsers. Extranets also save companies money by allowing them to establish business-to- business connectivity over the Internet instead of using expensive, dedicated leased lines. Extranets can also savemoney by reducing phone and fax costs.

Ethernet:

Ethernet is a family of LAN technologies,that may be best understood with the OSI reference model.



Ethernet technologies have three part names:

1. Speed
2. Signal Method (BaseBand and BroadBand).
3. Medium

Eg. 100BASET

• 100 Mbps

• Baseband

• Unshielded Twisted Pair

10BASE5, 10Mbps, Baseband, 5*100Meters.

Baseband:

A signaling technology that sends digital signals over a single frequency as discrete electrical pulses. The baseband signal is bidirectional so that a baseband system can both transmit and receive signals simultaneously. Use time-division multiplexing **(TDM)** to accommodate multiple channels over a single baseband transmission line. Baseband signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation. Eg. Ethernet

Braodband:

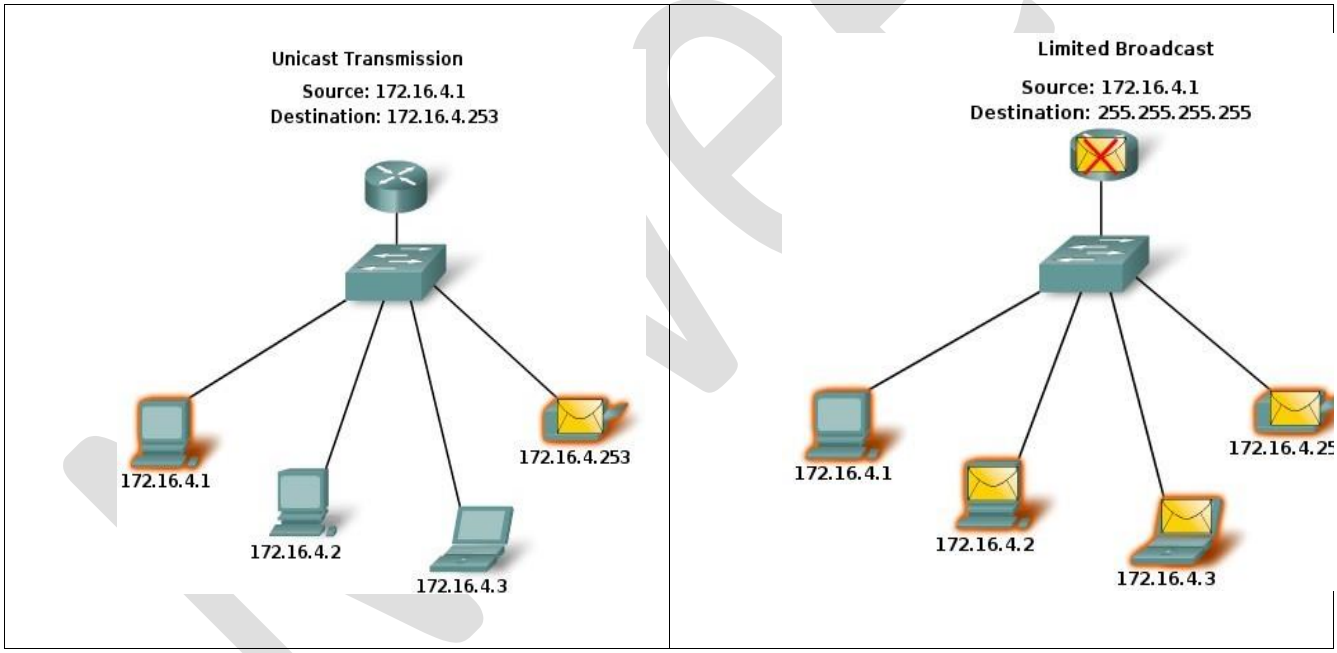
A signaling technology that sends signals simultaneously over a range of different frequencies aselectromagnetic waves. These signals are unidirectional—traveling in only one direction at a time—so a broadband system can generally either transmit or receive but cannot do both simultaneously. Broadband signalscan be regenerated using amplifiers in order to travel longer distances before becoming attenuated. Broadband transmissions are divided into multiple bands or channels by multiplexers using a multiplexing scheme such as frequency-division multiplexing **(FDM).**

Eg.One good example of broadband signaling would be how you view different channels

through your cable boxand a signal coaxial cable carrying multiple signals in cable television.

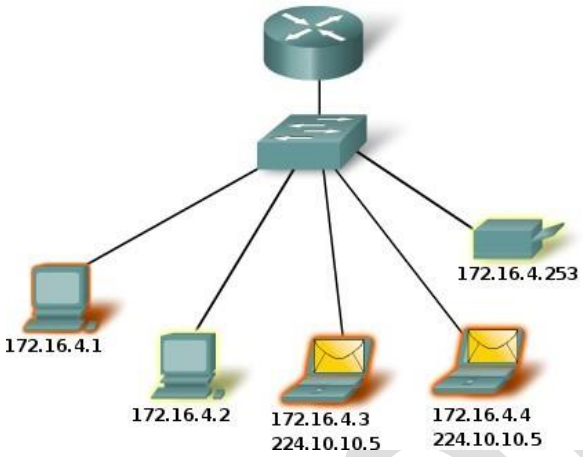
Modes of communication:

In an IPv4 network, the hosts can communicate one of three different ways:
Unicast - the process of sending a packet from one host to an individual host
Broadcast - the process of sending a packet from one host to all hosts in the network
Multicast - the process of sending a packet from one host to a selected group of hosts

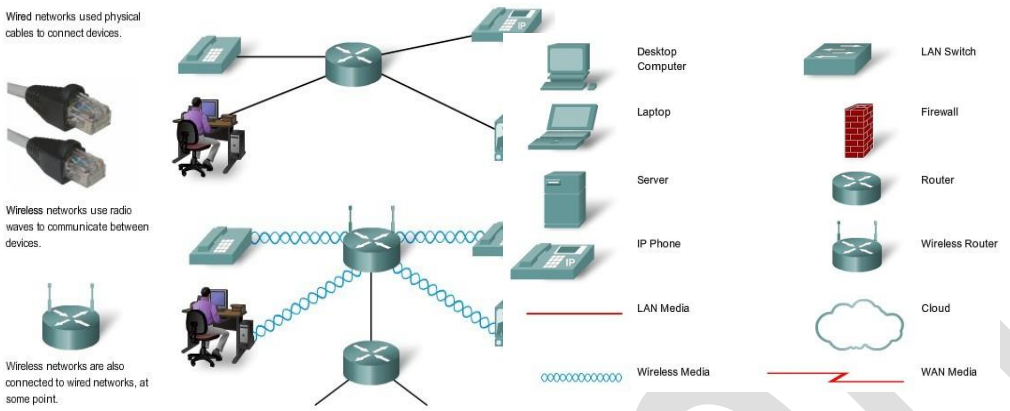


Multicast Transmission

Source: 172.16.4.1

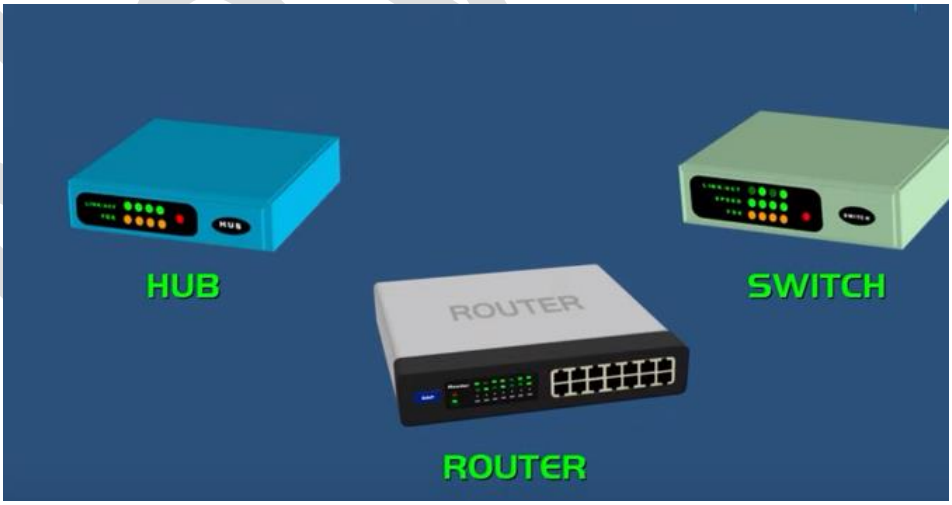


Elements of Network:



Component of Internet:

A network (or internet) is formed using Hardware (or network device) and network software orApplication and protocols.



Hardware or Network device:

1. Hub:

- It is uses to connect systems or nodes or networks.
- It has direct connection to a node (point to point connection).
- It suffers from high collision of data, results to data loss.
- A hub takes data from input port and retransmits the input data on output port.

2. Repeater:

- A repeater is a device which regenerates or amplifies the data or signal so that it can betravel to the other segment of cable.
- It is use to connect two networks that uses same technology and protocol.
- It does not filter or translate any data.
- Work in physical layer.

3. Bridge:

- It is used to connect two networks.
- It divides the collision domain based on number of ports or interface present in a bridge.
- It uses the packet switches that forward and filter the frames using LAN destination address.
- Bridge examines the destination address of frame and forwards it to the interface or portwhich leads to the destination.
- It uses the routing table for routing frame from one node to other using MAC address.
- It works in Data Link Layer.

4. Switch :

- It is similar to bridge. It has more number of interfaces as compared to bridge.
- It allows direct communication between the nodees

- It works in Data Link Layer.
- It uses MAC address for data transmission and communication.

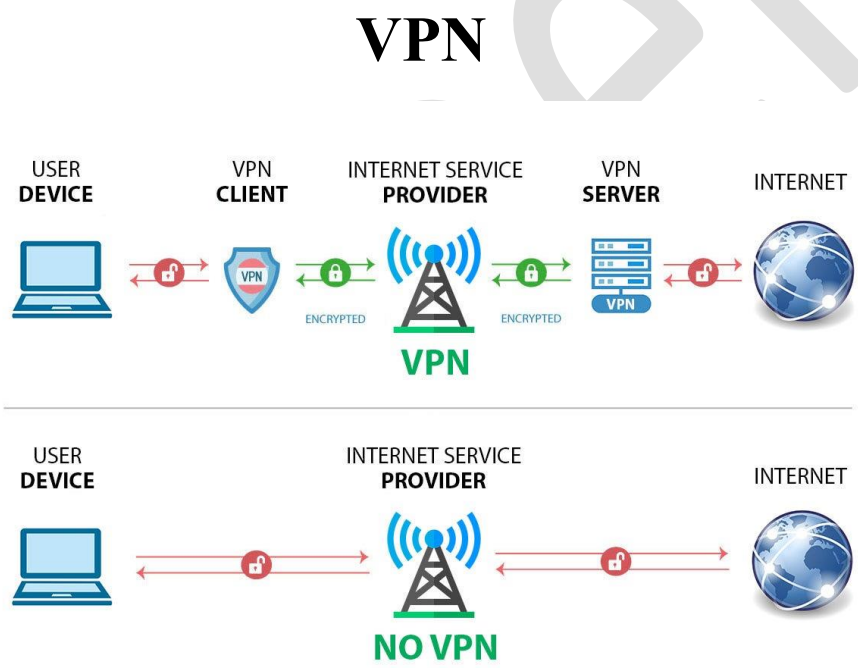
5. Router:

- It is used to connect different types of network (types- architecture/ Protocol).

- It work similar to bridge but it uses IP address for routing data.
- Router can't be used for connecting Systems.
- It works in Network Layer.

6. Gateways:

Gateways make communication possible between systems that use different communication protocols, data formatting structures, languages and architectures. Gateways repackage data going from one system to another. Gateways are usually dedicated servers on a network and are task-specific



Types of Virtual Private Network (VPN) and its Protocols VPN stands for Virtual Private Network (VPN), that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel.

Virtual Private Network (VPN) is basically of 2 types:

1.Remote Access VPN: Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both. An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites.

Users aware of Internet security also use VPN services to enhance their Internet security and privacy. 2.

2 .Site to Site VPN: A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

• Intranet based VPN: When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.

• Extranet based VPN: When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

Basically, Site-to-site VPN create a imaginary bridge between the networks at geographically distant offices and connect them through the Internet and sustain a secure and private communication between the networks. In Site-to-site VPN one router acts as a VPN Client and another router as a VPN Server as it is based on Router-to-Router communication. When the authentication is validated between the two routers only then the communication starts.

Types of Virtual Private Network (VPN) Protocols:

1.Internet Protocol Security (IPSec): Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection. IPSec runs in 2 modes:

2. • (i) Transport mode • (ii) Tunneling mode The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system.

3.Layer 2 Tunneling Protocol (L2TP): L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

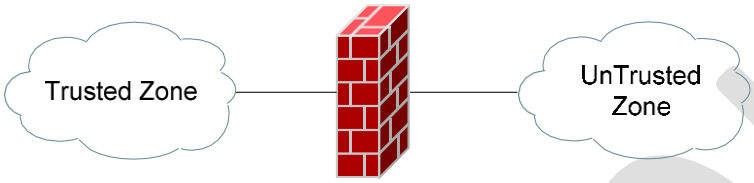
4.Point–to–Point Tunneling Protocol (PPTP): PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

5.SSL and TLS: SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have “https” in the initial of the URL instead of “http”.

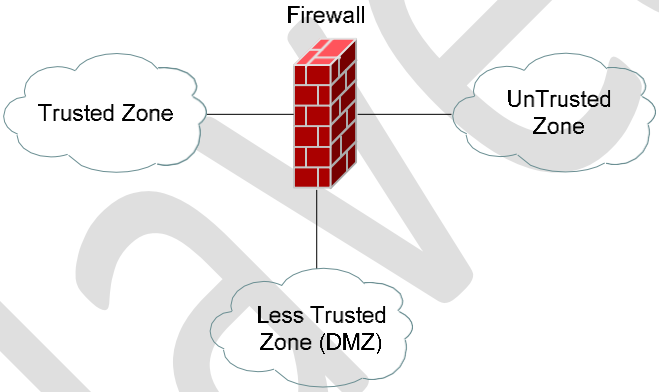
6.OpenVPN: OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol. 7.Secure Shell (SSH): Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.\

FIREWALL

Traditionally, a firewall is defined as any device (or software) used to filter or control the flow of traffic. Firewalls are typically implemented on the network perimeter, and function by defining **trusted** and **untrusted zones**:



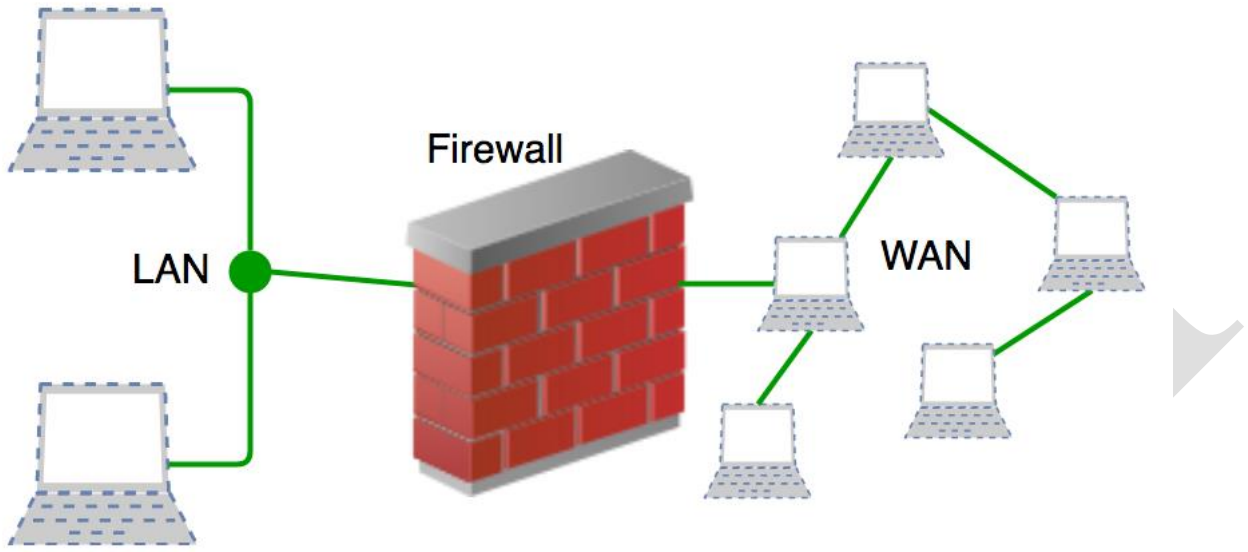
A firewall is not limited to only two zones, but can contain multiple 'less trusted' zones, often referred to as **Demilitarized Zones (DMZ's).**



To control the *trust* value of each zone, each firewall interface is assigned a *security level*, which is often represented as a numerical value or even color. For example, in the above diagram, the Trusted Zone could be assigned a security value of 100, the Less Trusted Zone a value of 75, and the Untrusted Zone a value of 0.

As stated previously, traffic from a *higher* security to *lower* security zone is (generally) allowed by default, while traffic from a *lower* security to *higher* security zone requires explicit permission

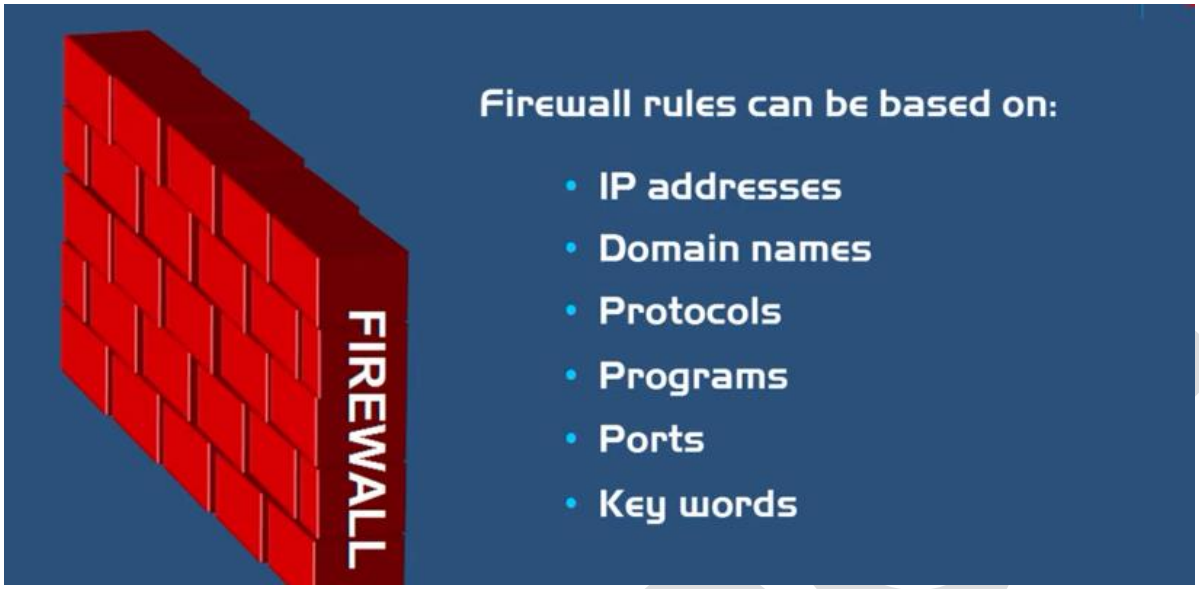
.



Working of Firewall

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from Human Resources department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both Human Resource and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming.

Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.



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

Types of Firewall

Firewalls can be categorized based on their generation.

1. Packet Filtering Firewall

Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be filtered according to the following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

- Incoming packets from network 192.168.21.0 are blocked.
- Incoming packets destined for the internal TELNET server (port 23) are blocked.
- Incoming packets destined for host 192.168.21.3 are blocked.
- All well-known services to the network 192.168.21.0 are allowed.

2. Stateful Inspection Firewall

Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

3. Software Firewall

A software firewall is any firewall that is set up locally or on a cloud server. When it comes to controlling the inflow and outflow of data packets and limiting the number of networks that can be linked to a single device, they may be the most advantageous. But the problem with software firewall is they are time-consuming.

4. Hardware Firewall

They also go by the name "firewalls based on physical appliances." It guarantees that the malicious data is halted before it reaches the network endpoint that is in danger.

5. Application Layer Firewall

Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy.

6. Next Generation Firewalls (NGFW)

NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

7. Proxy Service Firewall

This kind of firewall filters communications at the application layer, and protects the network. A proxy firewall acts as a gateway between two networks for a particular application.

8. Circuit Level Gateway Firewall

This works as the Sessions layer of the OSI Model's . This allows for the simultaneous setup of two Transmission Control Protocol (TCP) connections. It can effortlessly allow data packets to flow without using quite a lot of computing power. These firewalls are ineffective because they do not inspect data packets; if malware is found in a data packet, they will permit it to pass provided that TCP connections are established properly.

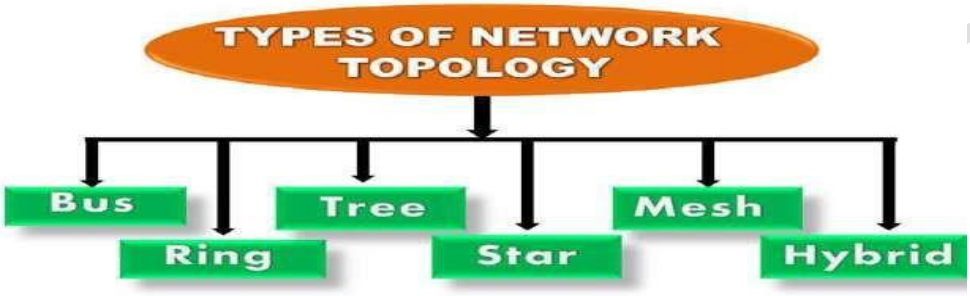
Functions of Firewall

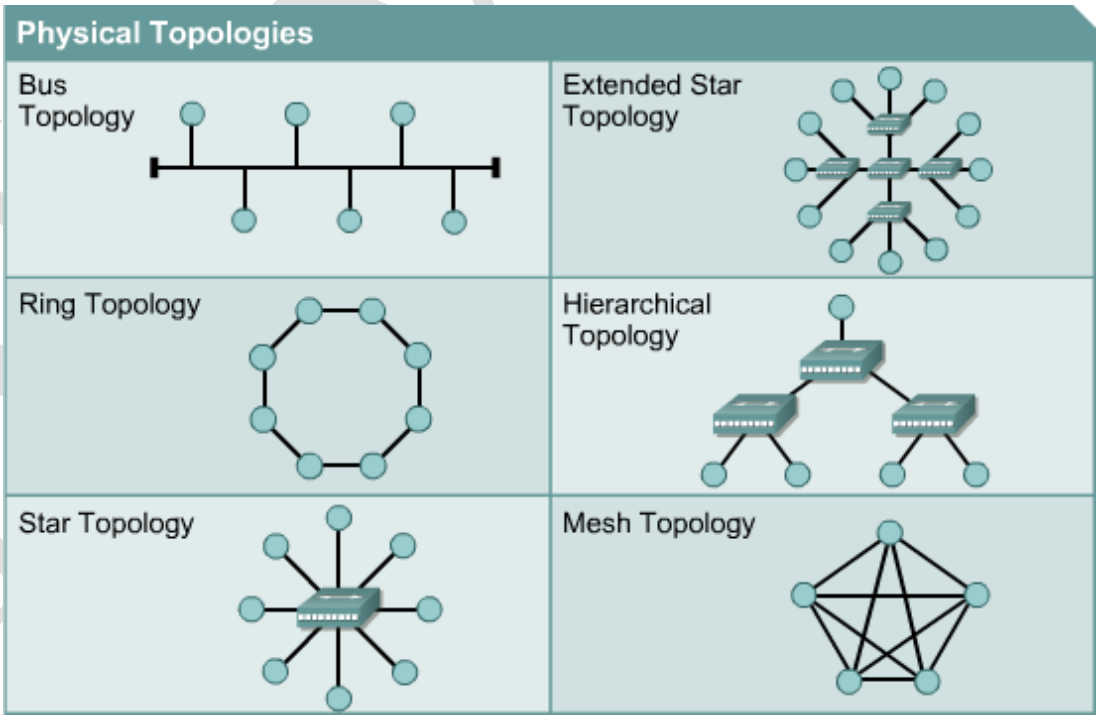
- Every piece of data that enters or leaves a computer network must go via the firewall.
- If the data packets are safely routed via the firewall, all of the important data remains intact.
- A firewall logs each data packet that passes through it, enabling the user to keep track of all network activities.
- Since the data is stored safely inside the data packets, it cannot be altered.
- Every attempt for access to our operating system is examined by our firewall, which also blocks traffic from unidentified or undesired sources

Topologies

What is Topology? :

- Topology defines the structure of the network of how all the components are interconnected to each other.
- There are two types of topology: **physical and logical topology**.
- Physical topology is the geometric representation of all the nodes in a network.





1. Bus Topology:

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (Ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.

- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

Advantages and Disadvantages of Bus Topology: Advantages of Bus Topology :

- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology :

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.

It is slower than the ring topology.

2 Ring Topology :

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.

Token passing: It is a network access method in which token is passed from one node to another node.

Token: It is a frame that circulates around the network

Working of Token passing :

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

Advantages and Disadvantages of Ring topology : Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology :

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.

- **Failure:** The breakdown in one station leads to the failure of the overall network.

- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.

- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

3. Star Topology:

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Advantages and Disadvantages of Star topology of Star topology: Advantages of Star topology :

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology.In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network.

- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.

- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.

- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.

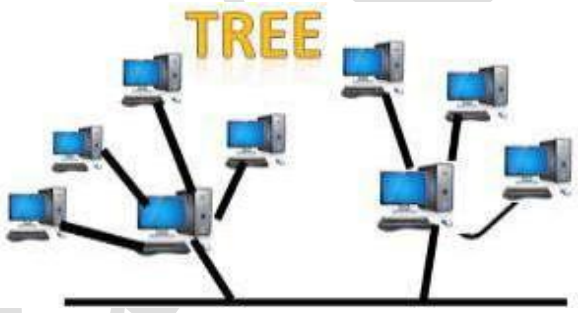
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology :

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

4. Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent -child hierarch



Advantages and Disadvantages of Tree topology:

Advantages of Tree topology:

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments

.

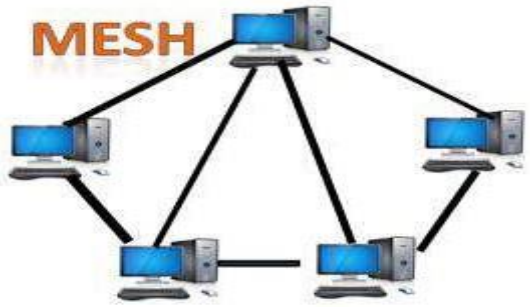
Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to rec

5. Mesh topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:

Number of cables = (n*(n-1))/2;
Where n is the number of nodes that represents the network.



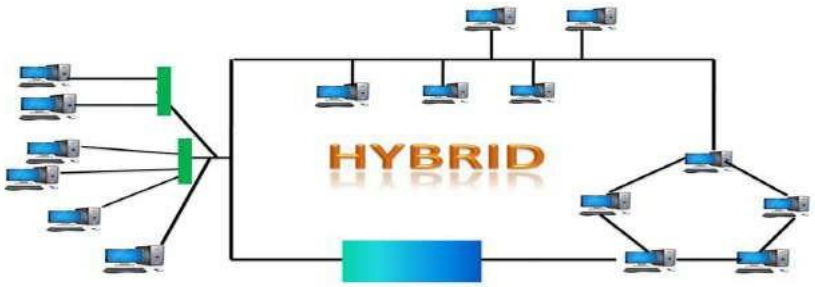
Advantages and Disadvantages of Mesh topology : Advantages of Mesh topology:

- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other Devices Disadvantages of Mesh topology
- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.

- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

6. Hybrid Topology

- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.



THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.