Data Networking

Networking Concepts:

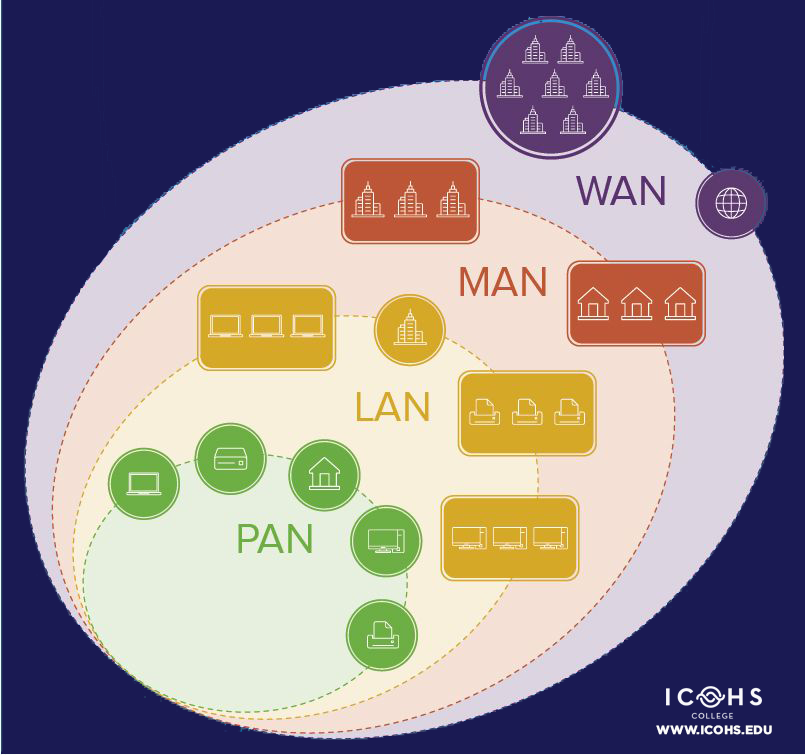
Data is basically any information which is in binary form. A system that transfers data between different nodes through data switching, system control and interconnection transmission lines is what we called as data network. The exchange of data between 2 devices via a transmission medium and following some kind of a protocol is known as data communication. Data networking and communication is used to transfer data to one or more points called as multipoint. It is of two types namely: Broadcast and Point-to-Point.

Broadcast: when data is transmitted from one point to multipoint then that is known as broadcasting of data. Data broadcasting is again of two types i.e. Independent data broadcasting and linked data broadcasting. Independent data broadcasting is the one which transmits supplementary information directly onto the main television such as news, weather forecast etc. Linked data broadcasting is the one which provides information about the characters of the television drama. For example, in a sports program one can check about the athletes, their information and their progress.

ISDB- T (Integrated Services Digital Broadcasting- Terrestrial) is able to send much more and detailed data through a communication line in order to complement broadcasting of data which has only limited Bandwidth.

Network Types and Topologies:

There are basically 4 types of Networks namely PAN, LAN, MAN, WAN. The figure shown below shows the basic types of data networks:



1. PAN (Personal Area Network) :- It is the smallest network which is personal to the users. It is basically involved with the personal usage of the person that’s why named as personal area network. Its range is around 10 meters. It includes Bluetooth, Zigbee , Smartphones, TV Remotes etc. It ranges generally from 10m to 100m with a speed of upto 250 Kbps in zigbee and 24Mbps in Bluetooth.

Some Standards are shown below;

Bluetooth:- Bluetooth was standardized by the IEEE with a standards

802.15.01

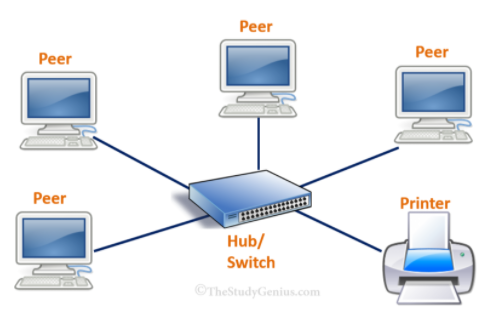
802.15.01B

802.15.1.1 Ratified as [IEEE Standard 802.15.1–2002](https://en.wikipedia.org/wiki/IEEE_802.15#Task_group_1_(WPAN/Bluetooth))

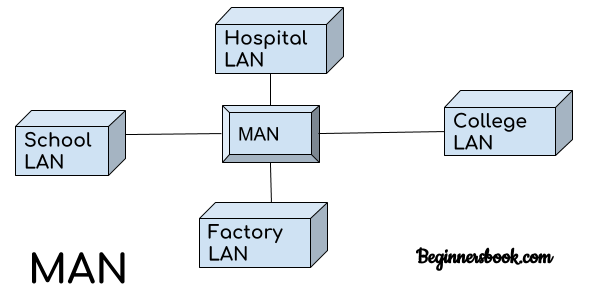
802.15.1.2 Ratified as [IEEE Standard 802.15.1–2005](https://en.wikipedia.org/wiki/IEEE_802.15#Task_group_1_(WPAN/Bluetooth))

And so on

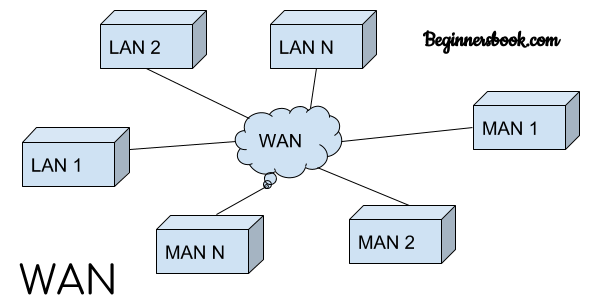
1. LAN (Local Area Network):- It is a network which is local to an area like school, college, office, building etc. It is a privately owned network which can be directly accessed by using an ethernet or a central device like switch or a hub. With Ethernet cables, the speed of data transfer can reach upto 54Mbps and with Gigabit Ethernet, it can reach upto 1Gbps. It ranges from basically 100m to 5km

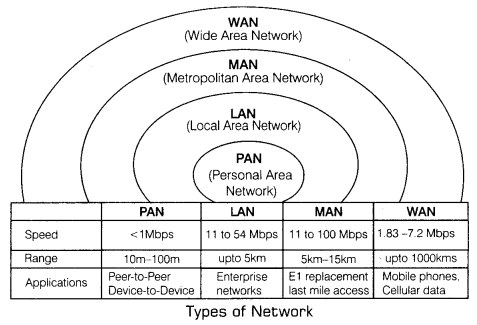


1. MAN (Metropolitan Area Network) :- When two or more LAN are interconnected then a MAN network is formed. It is bigger than LAN but smaller than WAN. For example, an organization has many branches at numerous locations which uses LAN network. So the organization can connect a telephone line over the LAN network to create a MAN network. Its speed is around 100Mbps with a range of upto 15Km.



1. WAN (Wide Area Network) :- It includes a large geographical area like a country or a continent and uses a carrier such as a telephone line or a satellite system etc. It is basically when multiple MANs and LANs are interconnected to form a network then a WAN network is formed. It Speed speed varies from 1.83 to 7.2 Mbps with a range of upto 1000km





The effectiveness of data communication system depends on 5 fundamental characteristics which includes:

Accuracy:- The accuracy of data transfer should be high i.e whatever data is transmitted must be received at the receiver site. The data that has been changed while transmission and useless.

Delivery:- The data must be delivered to the correct destination. The data transmitted, if received by some other receiver other that the intended one is useless.

Jitter:- Any abrupt change in the delay is what is known as jitter. It is basically defined as the variation in the arrival time of the packet.

Timeliness:- It indicates that the system must deliver the data timely. Any data delivered after the allotted time is useless. Such kind of D=delivery is known as rea-time transmission.

Latency:- It is the delay between the transmission time and the reception time. It is less than 10ms in 4G.

Network Topologies:

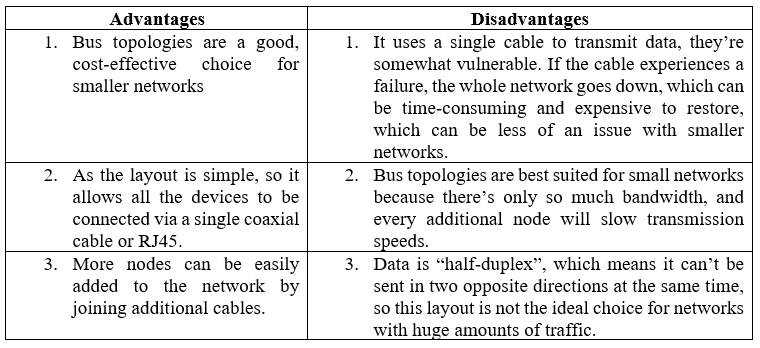
The way a network has been arranged to transfer the data is known as topology. Network topology is basically defines how a connection, device and nodes are interconnected in a network with respect to each other. There are two approaches to the network topology i.e physical and logical.

Physical :- It refers to the actual wired connections of how the networks are arranged.

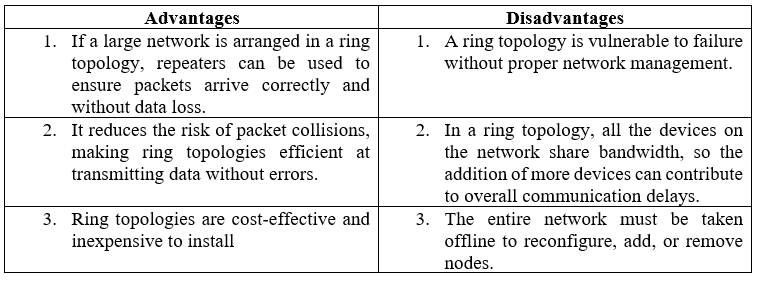
Logical :- The logical topology refers to the high level idea of the interconnection of nodes and devices on the network. It also determines how the data is transmitted over the network.

Types of Topologies: -

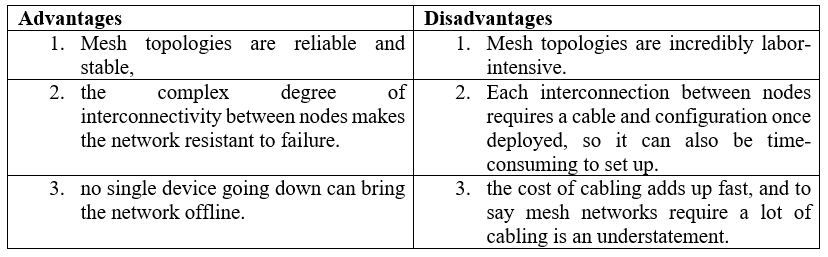
1. Bus Topology: It is responsible for the orientation of all the devices on a single cable from one end to another in a single direction. It is also known as line topology or the backbone topology. Advantages and disadvantages of Bus topology are as follows:



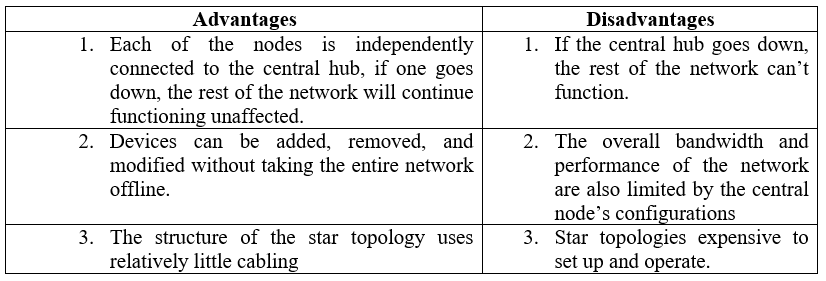
1. Ring Topology: It is a topology where nodes are arranged in rings. The data can travel in one or both direction through a ring network. Advantages and disadvantages of Ring topology are as follows:



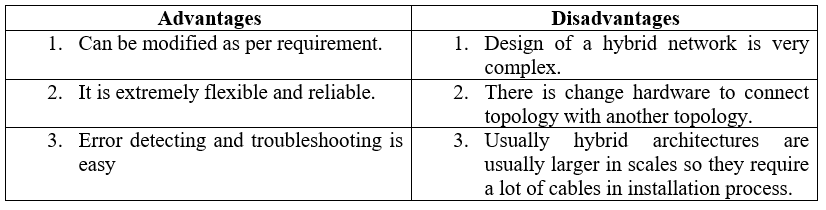
1. Mesh Topology: It is an integrated structure of point to point network. Here each node is connected to all the other nodes. Advantages and disadvantages of Mesh topology are as follows:

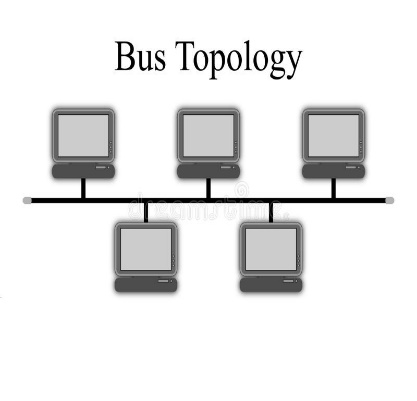
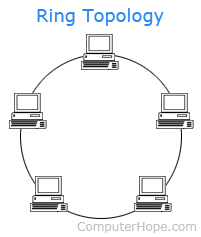
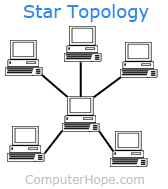
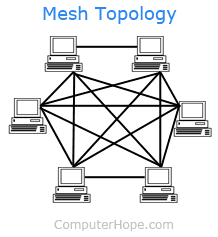
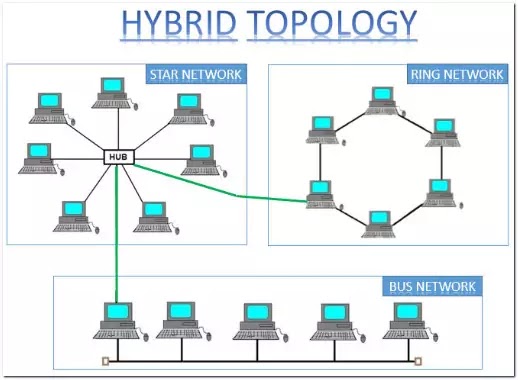


1. Star Topology: It is one of the most common topology in which every node is connected to a central hub via a fiber optic, twisted pair, or coaxial cable. The central hub is responsible for managing data transmission and hence functions as a repeater. Advantages and disadvantages of Star topology are as follows:



1. Hybrid Topology: It combines two or more different topologies. It is mostly used in larger companies where each department is having a personalized network topology as per their need. Advantages and disadvantages of Hybrid topology are as follows:

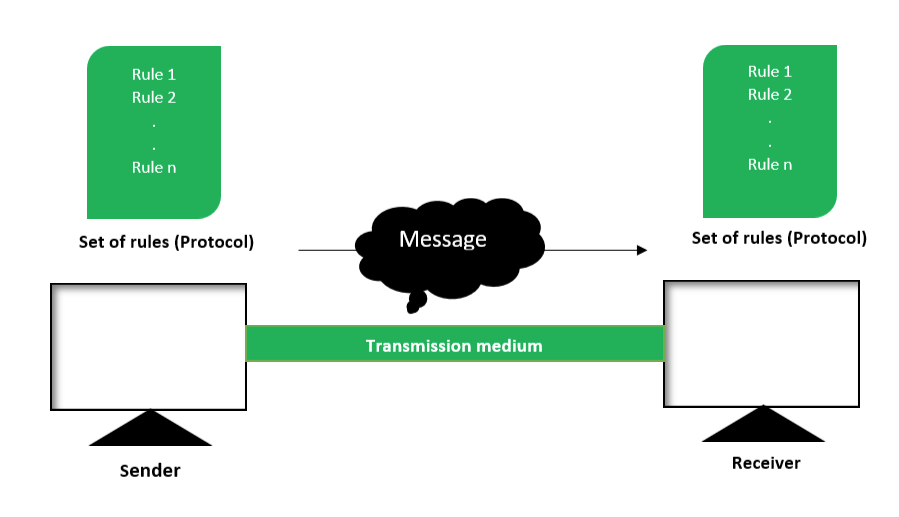


Data Communication system has five components namely:

1. Message: Any piece of data which needs to be communicated is a message. It is the most useful asset of a communication system.
2. Sender: Any device which is responsible for sending the data from transmitter is known as sender.
3. Receiver: It is the destination which receives the data send by the transmitter.
4. Transmission medium: The bridge between transmitter and receiver is known as medium. It could be through twisted pair cable, microwaves, fibre optic cable, radio waves, etc. . It can be simplex, half duplex or full duplex. Transmission medium in detail on wired and wireless is explained later.
5. Protocols: These are the set of rules which governs the transmission of data from transmitter to receiver.

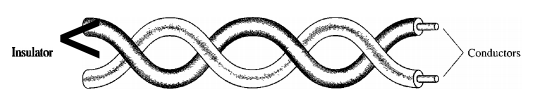
Lets take an example of data communication system in sending an email. Here the user who sends an email acts as a sender, the receiver of email is the reciver and message is the data. Email is an example of application layer where SMTP protocol is used. However there are many protocols involved in the whole process. Below is the explainationof whole OSI action in sending an email.



Wired and Wireless Networks:

1. Wired Networks: It is also known as guided media. It provides a channel from one device to another, using dual-twisted cable, coaxial cable, and fiber-optic cable. Signal movement for any of these devices is governed by medium.

Twisted Pair Cable: The twisted cable has two drivers (usually copper), each with its own plastic to divide, to twist together. One of the cables is used to carry signals to the receiver, while the other is only used as a ground reference. The recipient uses the difference between the two.

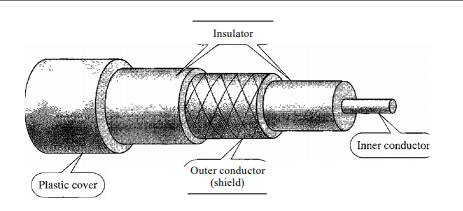


In addition to the signal sent by the sender on one of the cables, interference (sound) and the crosstalk can touch both wires and create unwanted signals.these are of two types:

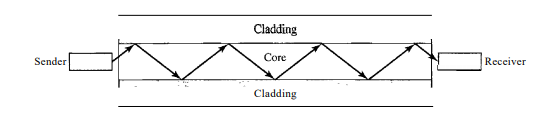
Shielded twisted pair & Unshielded twisted pair:

The commonly used twisted cable that is widely used in communication is called UTP. IBM has also produced a twisted type of cord for its use called shielded twisted-pair (STP). The STP cable consists of a metal foil or mesh cover that encloses two of the inserted conductors. Even metal wrapping improves cable quality by preventing sound intrusion or crosstalk, of course bulkier and more expensive.

Co-axial cable: These cables carry a relatively higher signal frequency than those of twisted-pair cable. This is because the medium of two wires are different.

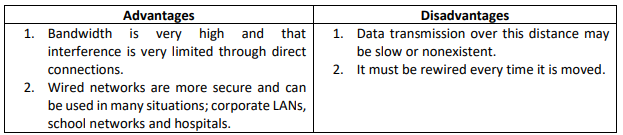


Fiber optic cable: These are made of plastic or glass and transmits signal in the form of light.



Most commonly used cable is UTP. Following Are the list of standard cables including RJ45. RJ 45 is an 8 pin cable which is used for computers, Ethernet network adapters etc.



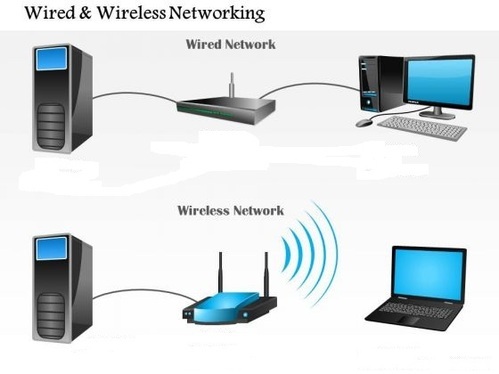


Wireless Networks are those which are made of wireless medium or unguided medium like radio waves, microwaves or infrared.

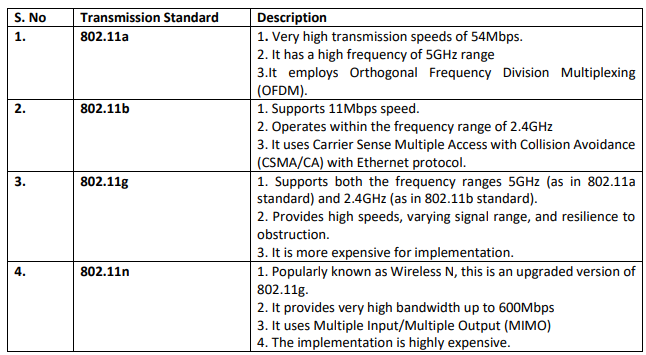
Radiowaves:- These are the EM Radiations in which wavelength are in the EM Spectrum which is longer than those of Infrared Radiations.

Microwaves:- It is a widely used radiations in the field of tool synthesis and chemical application of coordination compounds. It is used for point to point communication of data from one point to another. It is involved in long distance communication.

Infrared Waves: These are the waves which falls in the EM spectrum. These are basically used in TV etc. These radations are popularly known as heat radiations.



Some wireless standards are shown below:



Queuing and Scheduling :

The queuing and scheduling included in the interface allows the traffic to be divided into multiple lines so that the schedule can determine what type of action the traffic within each queue it receives. If the traffic placed on each queue is for a particular category of service, the scheduler may apply a separate code for different categories of service

Buffer and bandwidth are the two most important parameters which is associated with queuing and scheduling. Bufer is basically the queue length, that is, how much memory is available for storing packets. However, the whole package does not need to be lined up, sometimes stored as a notification, which is an indication of the content of the package. The buffer value can be defined either as the amount of time the packets are received on the interface when the queue is enabled or as a portable size depending on how many packets or notifications of the packs remain on the line at a time. The buffer value is the amount of memory available and can be defined as milliseconds of traffic or the total number of packets.

Bandwidth parameter means the scheduling component of the equation. The total amount of bandwidth is made available to scheduling and queuing proces. Scheduling determines how much is shared on each line. The total amount of bandwidth can be the speed of the interface or the size of the shaper if I is applied post scheduler.

The queue and schedule used, determine how resources are distributed. The need for queue and schdule is usually determined by the presence of traffic congestion. If resources are available and there is no resource competition, there is no need to line up. Another way to build traffic is to put more traffic on a connector than an outgoing line speed that can support it. Congestion can also be created incorrectly, by using a rate on the connector that sets the speed limit lower than the visible line speed. The remaining traffic was crashed or pressed back into memory, then separated from the actual lines. The scheduler also uses the queue and monitors the rate at which packets from each line are sent.

The packet enters the line at the tail, stays in line until it reaches the head, and then leaves the line. In the line system, packets may be discarded from the tail or head of the line, and both may be discarded at the same time. Usually, the packets are discarded at the tail. When the filling rate is much faster than the subtraction level, the buffer fills up completely. The result is that no packets can be placed in the buffer, and any newly arrived package should be discarded.

But the queue can throw packets from the head. The data at the head of the line are the ones that go from the tail to the head, so they are the ones that stay in line the longest. In overcrowding and resource starvation, the line does not find editing spaces. To avoid queuing up, and to have a long and hopeless period of traffic jams, it is often forced on all data in the queue how long they are allowed to stay in queue, waiting to be scheduled. The name of this is the aging of the packets, which means that the old packets are out of line because there is no point in trying to deliver them.

Tail drops and data aging are not associated. If, to remove the line, the rate at which the packets fall on the head of the queue cannot match the level at which the data enter the line at the tail, the drop of the packet may occur on both the tail and the head due to the wear of the packet.

Network Security:-

In order to send the data over the internet, security is one of the major concerns now-a-days. So, firewall is used for this purpose.

Stack and Heap overflow:

There are two types of overload: stack and heap .Stack and heap are two areas of memory structure shared when the system is running. Calling functions are stored in the stack, and dynamic variables are stored in a heap. A certain amount of memory is given to the buffer. Static variable storage (variables defined within a function) is called a stack, because it is actually stored in a stack in memory. The Heap data is a memory that is strongly distributed during operation. This data is actually not stored in a stack, but somewhere in the middle of a large "mass" of temporary, discarded memory used for this purpose. In fact, exploitation is a major factor, as there are no simple framework indicators (as there are stacks) that you can write over.

Attackers can use buffer overload to override a password, file name, or other data. When the file name is rewritten, a separate file will be opened. If this is a usable file, the code that was intended to be valid will apply.

The overflow of the buffer is based on how the editing languages ​​work. Most calling functions do not check to ensure that the buffer will be large enough to hold the copied data in it. System planners can use phones that perform these tests to prevent overcrowding, but many do not.

Creating a massive buffer attack requires the intruder to understand the assembly language and technical details about the OS in order to be able to write code that will fit into the stack. However, the code for this attack is usually published so that others, with little technical knowledge, can use it. Some types of fire extinguishers, called experimental firefighters, allow for buffer overflow attacks, while application gates (if properly configured) can filter out excessive buffer attacks.

Buffer overload occurs when a task / function writes more data to a variable (actually just a memory location) rather than a variable designed to capture The result is that data starts to overwrite other memory areas without computer experts to make things worse, most hardware structures (like Intel and Sparc) they use a stack (a storage repository) to store recovery addresses. So, the problem is that overloading the buffer will overwrite these recovery addresses, and the computer — not knowing anything better — will still try to use them. If the attacker has enough skills to accurately control which values ​​were used to overwrite recovery returns, the attacker can control the next (computer) operation of the computer.

**Firewall**:- It is a security system of the network which is used to monitors and controls all the outgoing and incoming network traffic depending upon the defined and advanced set of protocols. It is basically a software program which prevents illegal access to and from a private network.

A firewall usually performs the following task :

* Defend resources
* Manage and control network traffic
* Validate access
* Acts as an intermediary
* Record and report on events

Another way that allows a secure connection to another network over the internet is by establishing a VPN connection.

**VPN (Virtual Private Network) :-** It is an encrypted connection over the internet . VPN connects a laptop, PC or smartphone to another computer, somewhere over the internet and allows to browse the internet using that computer’s internet connection [8]. A VPN is formed by joining two or more VRF (Virtual Router Forwarding). So that they can share the routing table and can communicate with each other.

Tunneling is one of the most important process in VPN. In this data is send privately over the internet. In a tunnel connection , every packet is placed under another packet before sending over to the internet. This is known as encapsulation.

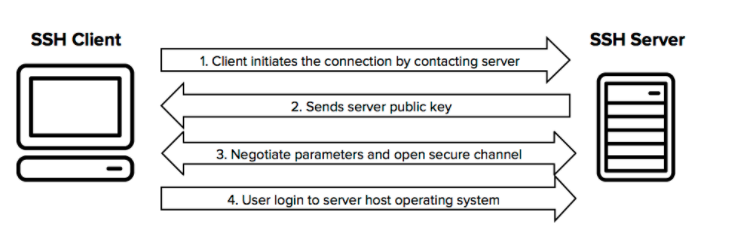
Cryptography: It is the process byy which data is protected and communicated over the internet with specific codes, so that the message will be read by the one for whom it is written. Crytography is the basically the study encryption and decryption

Encryption : It is the process of coding the message for a secure communication over the internet.

**SSH TTL, and MTLS:**

Tunneling process occurs with the help of dfferent protocols which includes SSH (Secure Shell), TTL(Time To Live) and MTLS (Mutual Transport Layer Security)

SSH: The SSH protocol uses encryption to protect the connection between the client and the server. All user authentication, commands, output, and file transfers are encrypted to protect against network attacks.



TTL: Life time (TTL) determines how long the query or content is stored. TTL's core business is focused on managing information packets regarding DNS requests. When one of these packages is created and transmitted online, there is a chance that it will pass, continuously, from a permanent route to a permanent route. To prevent this from happening, each packet has a specific TTL or hop limit. It is also possible to check the TTL data packet for details of how it went online during its journey.

Within each packet, there is a specified location where the TTL value is stored. This is the tag, and it shows how long the package should go over the internet. When the router receives the data packet, it removes one unit from the TTL number before sending it to the next location within the network. This continues to occur until the TTL inside the packet is dropped to zero.

At that point, the router removes the data packet and transmits the Internet Control Message Protocol (ICMP) message to the host where the package originates. ICMP is a protocol that allows devices to communicate and transmit errors regarding data packets.

MTLS: MTLS Agreements provide encrypted communications and authentication of final points on the Internet. The server-server connection depends on MTLS authentication. In an MTLS connection, the server from the message and server receives the exchange certificates from a trusted CA. Certificates prove the identity of each server.

Components or the connecting devices:

Devices which operates at different layers are known as connecting devices or the components. It includes routers, hub, switches, bridge, gateways.

The device which works below physical layer are known as passive hub. These are the repeaters which slows down the signal propagation.

The device which works at the physical layer are known as Active Hub. These are multiport repeaters which is used in star topology.

The device that works at physical and data link layer is known as bridge or a layer 2 switch

The device that operates at physical layer and network layer are called as router or a layer 3 switch.

The device that works at all the layers are known as gateway.

Following are the functions of Hub:

1. It amplifies signal
2. It do not filter data packets based on destination.
3. There is no path determination or switching.
4. It do not buffer incoming traffic.
5. It propagates signal through the network.

Functions of bridge:

1. It connects and passes packets between two ne segments.
2. It is intelligent than hub.

Functions of Switch:

1. It is a multiport bridge.
2. It isolates traffic in various domains.

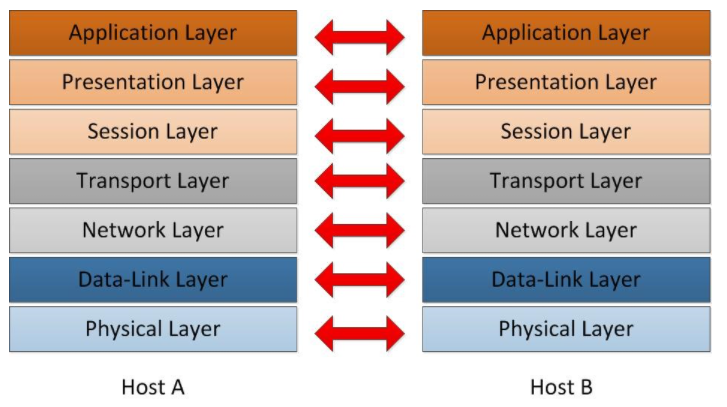
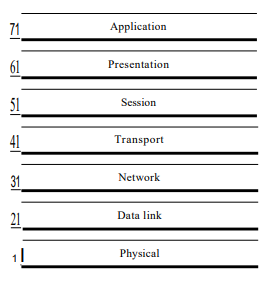
Functions of Router:

1. It routes the packet based on their logical address.
2. It is software oriented as router configurations are needed. It is faster than others.

OSI Model: **. Data (Packet) transmission over the internet :-**

When data is send from one server to another, it goes through all the 7 layers of the transmission model from top to bottom and bottom to top. At one side these layers talk to its upper layer and at the other side they talk to their lower layers. There is also side to side communication i.e each layer talks to their corresponding layer in the other side eg. application layer of one side communicates with only the application layer of the other side, it cannot talk to the presentation layer of the other side.

The communication between different layers for passing of the data and the network information is made possible by interfaces existing between each pair of adjacent layers. Layered functions and well defined interfaces provides modularity to the network. The OSI model is a layered framework for the designing of a network system that is establishes connection between all types of computer system.



Data is transmitted over the internet not in its actual form but rather they are subdivided into smaller packets and the transmission between computers (or server) across the internet is featured by different protocols [7]. It is a seven layered model consisting of physical, data link, internet (network), transport, session, presentation and application layer. When an email is send from one server to another, it goes to the application layer of the OSI model. It provides interface to the user in order to tell the computer how to handle the data. Gradually, the data and information moves to different layers using different protocols and reaches to its destination. The protocols has been discussed in the latter sections.

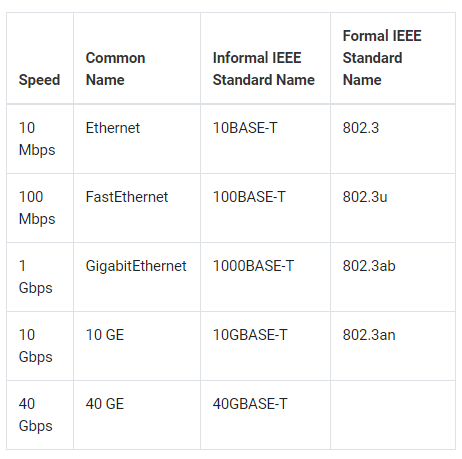
**Physical layer :-**

* It coordinates function required to carry a bit stream over physical layer.
* It is a peer-to-peer communication.
* It provides physical and electrical specification for device and medium.
* It is responsible for representation of bits and synchronization of sender and receivers clock.

**Data link layer:-**

* It makes the unliable physical layer to a reliable link.
* It converts bit streams into manageable units called frames.
* It provides physical addressing to the frames and responsible for node-to-node delivery.
* It is also responsible for error control and detection of damaged, duplicate or lost frames.
* Protocols at this layer includes:

1. Ethernet:- Ethernet is not a single thing, it refers to a family of standards. The main purpose of Ethernet is to act as a single LAN technology even if the data can pass through different types of connections (visible and copper cables, wireless connectors) at different speeds (from 10Mbps trough 100Gbps), because it uses the same data- various media and technologies. However, the network engineer should be aware of the names of at least the most commonly used Ethernet standards such as FastEthernet and GigabitEthernet.



IEEE standards include:

Logic Link Layer (LLC): 802.2

Wired Network or ethernet: 802.3

Wifi: 802.11

Bluetooth: 802.15

WiMax: 802.16

1. Token Ring :- It is a protocol used in communication of LAN Network. This topology is used to define the order in which the stations send. The connections of stations are shown below. Token is a three byte single frame. It travels around the ring. Token passing is the mechanism which is used here. Data packets are also transmitted in the same direction as that of the token. The station that carries the token is the one which transmits the data packets.
2. RS 232:- RS 232 is the communication protocol used for serial communication. It allows the connected servers to and its peripheral devices to allow serial exchange of data between them. RS 232 is used for connecting DTE i.e. data transmission equipment and DCE i.e data communication equipment.
3. FDDI/ FTTH :- It is Fiber distributed data interface/ Fiber to the home which is a set of ANSI and ISO standards for data transmission over LAN via fiber optics cable. It is applicable only to the LAN which is over the range of 200 km in diameters.

**Network layer:-**

* It is responsible for host to host delivery i.e source to destination delivery of the packets across multiple networks.
* It is responsible for providing logical address and also performs the function of routing.

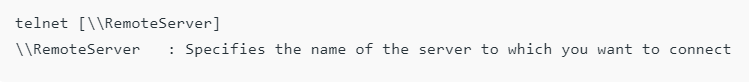
**Transport Layer:-**

* It is responsible for process to process delivery of the packets.
* It is also responsible for segmentation, sequencing and service-point addressing known as port address wich is used to achieve multiplexing.

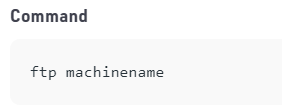
**Application Layer:-**

* It is the top most layer of the OSI model through which the user interacts. It is responsible for the services provided to the users. For example :- E-mail services, file transfer etc.
* This layer contains many protocols which includes,

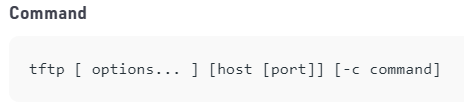
1. TELNET (TELecommunication NETwork): It allows the client to access the resources of the server It is responsible for file management and set up devices like switches. Port number is 23. Command is:



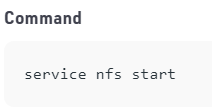
1. FTP (File Transfer Protocol): It is actually responsible for transfer of files. It promotes reliable and efficient data transfer via remote computers. Port number is 20 for data and 21 for control.



1. TFTP (Trivial File Transfer): It is a simplified version of FTP. If we know exactly what to find and where to find then TFTP is the protocol.



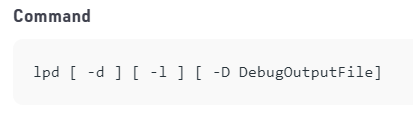
1. NFS (Network File Transfer): It allows the remote host to mount the file systems over the network and interact with those file systems as though they are mounted locally.



1. SMTP (Simple Mail Transfer Protocol): It is responsible for the movement of the emails on and across the networks. It works closely with MTA (Mail Transfer Protocol) to send data to the right email box. SMTP port number is 25.



1. LPD (Line Printer Daemon): It is responsible for printer sharing. Daemon is an agent or a server.



1. X-Windows :- It is responsible for writing the GUI based applications. It allows a program(client) to run on one server.
2. POP3 (Post Office Protocol version 3) : It is a mailing protocol which is used to receive emails to local email client from remote server. It works on two ports i.e.

Port 995 – It is used to connect using POP3 securely.

Port 110 – It is default non-encrypted port of POP3.

1. IMAP ( Internet Message Access Protocol): It is a mailing protocol which is used to receive emails to remote server from local client. It has two ports:

Port 993 – It is responsible for secure connection using IMAP securely.

Port 143 – It is default non-encrypted IMAP port.

**TCP/UDP and IP protocols: L4 Layer protocols:**

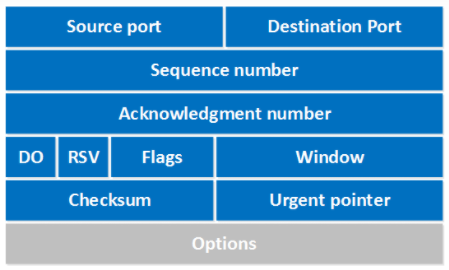
L4 layer is basically responsible for process to process communication. Process delivery requires two identifiers, an IP address and a port number, to each end to make a connection. The combination of IP address and port number is called a socket address. The client socket address describes the client process separately as the server socket address describes the server process. Transport layer protocol requires two socket addresses:

client socket address and

server socket address. These four pieces of information are part of the IP title and the headline of the transport layer protocol. L4 Protocols include TCP, UDP and IP. Following are their headers with explanation.

TCP(Transmission control protocol) Header:

TCP is a reliable protocol of transport layer. It establishes the path before sending the packet and each packet is acknowledged by the receiver.



// Source port: this is the 16th field that specifies the number in the sender port.

Destination port: this is a 16-point field that specifies the port number of recipients.

Sequence number: the sequence number is a 32 field indicating how much data is sent during the TCP period. If you set up a new TCP connection (3-way handshake) then the first sequence number is a random 32 bit number. The recipient will use this sequence number and send back to approve. Protocol analysts like the wireshark often use the same number sequence 0 because it is easier to read than a certain random higher number.

Notification number: this 32 bit field is used by the recipient to request the next part of TCP. This number will be the sequence number added by 1.

CAN: this is a 4 bit data offset field, also known as title length. Indicates the length of the TCP title so we know where the actual data starts.

RSV: these are 3 bits of specified field. They are not used and are always set to 0.

Flags: there are 9 bits of flags, and we call them bits bits. We use them to establish connections, send data and end connections. Window: A 16 bit window field specifies how many bytes the recipient is willing to receive. It is used so that the recipient can tell the sender that they would like to receive more data than they currently receive. It does this by specifying the number of bytes beyond the serial number in the consent field.

Checksum: 16 pieces are used in the checksum to check whether the TCP title is correct or not.

Emergency identifier: these 16 pieces are used when the URG bit is set, the emergency identifier is used to indicate where the emergency data ends.

Options: this field can be selected and can be between 0 and 320 bits. These fields can be seen in the wireshark platform. ///

