Unit - I

Network and Information security Fundamentals : Network Basics, Network Components, Network Types, Network Communication Types, Introduction to Networking Models, Cyber Security Objectives and Services, Other Terms of Cyber Security, Myths Around Cyber Security, Recent Cyber Attacks, Generic Conclusion about Attacks, Why and What is Cyber Security, Categories of Attack.

Network Basics

Introduction of Data Communication

Computer Network consists of interconnection of autonomous nodes. A node is device which is capable of receiving and/or sending data. A node may be any computer, printer, router or anydevice that can receive and/or send data. Nodes are autonomous means; no device can forciblystart and/or stop the operation of other device. In computer networks the data and resources areshared among the authorized multiple users.

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

Delivery: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

Accuracy: The system must deliver the data accurately. Data that have been altered intransmission and left uncorrected are unusable.

Timeliness: The system must deliver data in a timely manner. Data delivered late are useless. Inthe case of video and audio, timely delivery means delivering data as they are produced, in thesame order that they are produced, and without significant delay. This kind of delivery is called*real-time* transmission.

Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in thedelivery of audio or video packets. For example, let us assume that video packets are sent every30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an unevenquality in the video is the result.

Network Components:
A data communications system has five components.

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

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

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

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

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

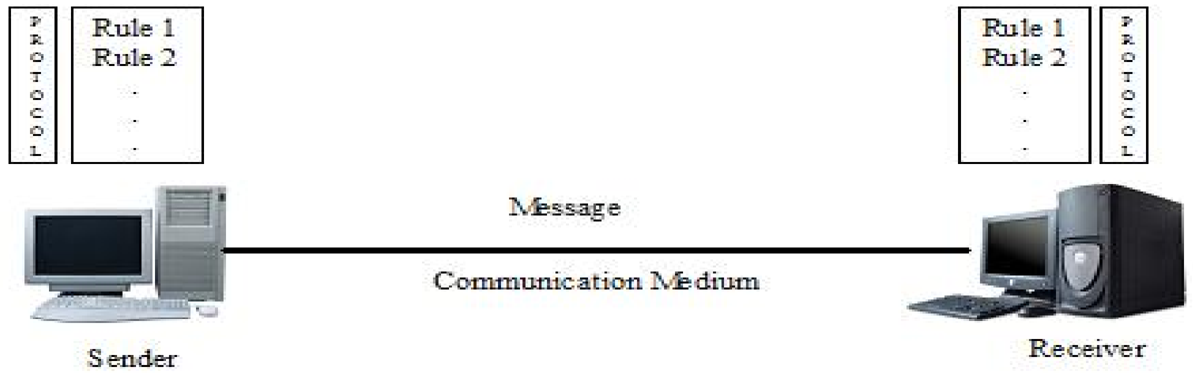


Fig:Components of Communication

Data Representation

Data refers to information that conveys some meaning based on some mutually agreed up rulesor conventions between a sender and a receiver and today it comes in a variety of forms such astext, graphics, audio, video and animation.

Text

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s).Different sets of bit patterns have been designed to represent text symbols. Each set is called acode, and the process of representing symbols is called coding. Today, the prevalent codingsystem is called Unicode, which uses 32 bits to represent a symbol or character used in anylanguage in the world.

Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not used torepresent numbers; the number is directly converted to a binary number to simplifymathematical operations.

Images

Images are also represented by bit patterns. In its simplest form, an image is composed of amatrix of pixels (picture elements), where each pixel is a small dot. The size of the pixeldepends on the *resolution.* For example, an image can be divided into 1000 pixels or 10,000pixels. In the second case, there is a better representation of the image (better resolution), butmore memory is needed to store the image. After an image is divided into pixels, each pixel isassigned a bit pattern. The size and the value of the pattern depend on the image. For an imagemade of only black and white dots (e.g., a chessboard), a 1-bit pattern is enough to represent apixel. If an image is not made of pure white and pure black pixels, you can increase the size ofthe bit pattern to include gray scale. For example, to show four levels of gray scale, you can use2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixelby 10, and a white pixel by 11. There are several methods to represent color images. Onemethod is called RGB, so called because each color is made of a combination of three primarycolors: *red,* green, and blue.

Audio

Audio refers to the recording or broadcasting of sound or music. Audio is by nature differentfrom text, numbers, or images. It is continuous, not discrete. Even when we use a microphone tochange voice or music to an electric signal, we create a continuous 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 discreteentity, arranged to convey the idea of motion. Again we can change video to a digital or an analogsignal.

Data Flow

Communications between any two devices may be one of the three modes. The data flow is also called modes of transmission.

- Simplex
- Half – Duplex
- Full – Duplex

Simplex

In simplex mode, the communication is unidirectional. Only one of the two devices on a link cantransmit; the other can only receive. Keyboards and traditional monitors are examples of simplexdevices. The keyboard can only introduce input; the monitor can only accept output. The simplexmode can use the entire capacity of the channel to send data in one direction.

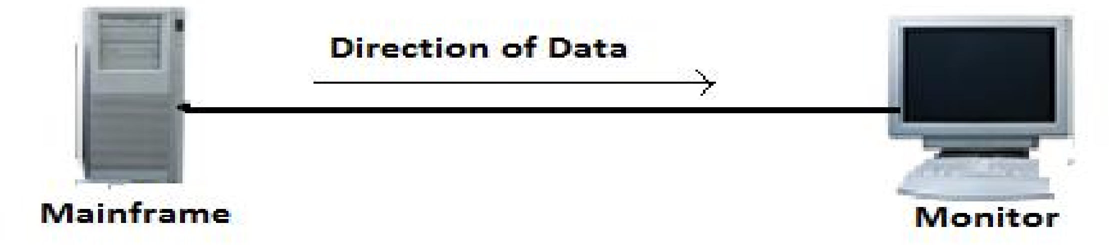


Fig: Simplex Mode

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When onedevice is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-laneroad with traffic allowed in both directions. When cars are traveling in one direction, carsgoing the other way must wait. In a half-duplex transmission, the entire capacity of a channel istaken 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 caseswhere there is no need for communication in both directions at the same time; the entire capacityof the channel can be utilized for each direction.

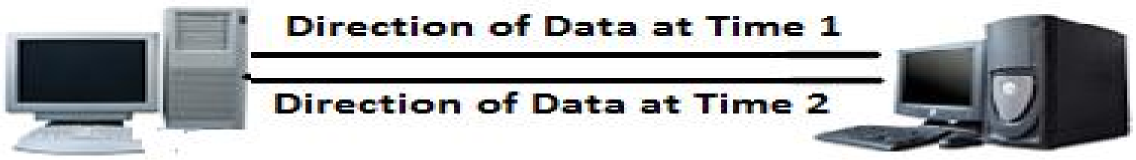


Fig: Half – Duplex Mode

Full-Duplex

In full-duplex mode also called duplex, both stations can transmit and receive simultaneously.The full-duplex mode is like a two-way street with traffic flowing in both directions at the sametime. In full-duplex mode, signals going in one direction share the capacity of the link: withsignals going in the other direction. This sharing can occur in two ways: Either the link mustcontain two physically separate transmission paths, one for sending and the other for receiving;or the capacity of the channel is divided between signals traveling in both directions. Onecommon example of full-duplex communication is the telephone network. When two people arecommunicating by a telephone line, both can talk and listen at the same time. The full-duplexmode is used when communication in both directions is required all the time. The capacity of thechannel, however, must be divided between the two directions.

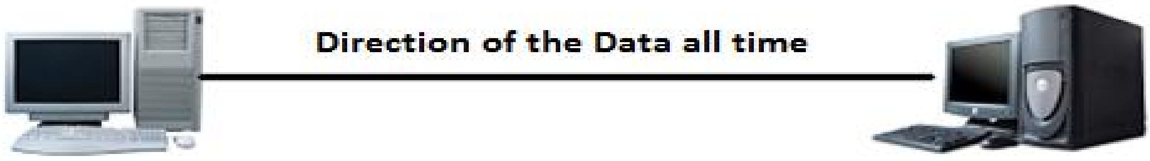


Fig: Full – Duplex Mode

Network Applications

Computer systems and peripherals are connected to form a network. They provide numerous advantages:

- Resource sharing such as printers and storage devices
- Exchange of information by means of e-Mails and FTP
- Information sharing by using Web or Internet
- Interaction with other users using dynamic web pages
- IP phones
- Video conferences
- Parallel computing
- Instant messaging

Networks

A network is a collection of nodes connected by communication links. A node can be acomputer, printer, or any other device capable of sending and/or receiving data generated byother nodes on the network. A communication link is a transmission medium between thesenodes.

Distributed processing

Most networks use distributed processing, in which a task is divided among multiple computers.Instead of one single large machine being responsible for all aspects of process, separatecomputers (usually a personal computer or workstation) handle a subset.

Network criteria

Most of the time, networks are used to transmit sensitive data. So, a network must be able tomeet a certain number of criteria. The most important of these are performance, reliability, andsecurity.

Performance

Performance can be measured in many ways, including transit time and response time. Transittime is the amount of time required for a message to travel from one device to another. Responsetime is the elapsed time between an inquiry and a response. The performance of a networkdepends on a number of factors, including the number of users, the type of transmissionmedium, the capabilities of the connected hardware, and the efficiency of the software.Performance is often evaluated by two networking metrics: throughput and delay. We often needmore throughput and less delay. However, these two criteria are often contradictory. If we try tosend more data to the network, we may increase throughput but we increase the delay because oftraffic congestion in the network.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure,the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network security issues include protecting data from unauthorized access, protecting data fromdamage and development, and implementing policies and procedures for recovery from breachesand data losses.

Physical Structures

- Types of Connections
- Physical Topology

Types of Connections

A network is two or more devices connected through links. A link is a communications pathwaythat transfers data from one device to another. For visualization purposes, it is simplest toimagine any link as a line drawn between two points. For communication to occur, two devicesmust be connected in some way to the same link at the same time. There are two possible typesof connections:

- point-to-point
- multipoint.

Point-to-Point

- A point-to-point connection provides a dedicated link between two devices. The entirecapacity of the link is reserved for transmission between those two devices.
- Most point-to-point connections use an actual length of wire or cable to connect the twoends, but other options, such as microwave or satellite links, are also possible.
- Example: When you change television channels by infrared remote control, you areestablishing a point-to-point connection between the remote control and the television'scontrol system.

Fig: Point-to-Point Connection

Multipoint

- Multipoint A multipoint (also called multidrop) connection is one in which more thantwo specific devices share a single link.

- In a multipoint environment, the capacity of the channel is shared, either spatially ortemporally.
- If several devices can use the link simultaneously, it is a *spatially shared* connection. Ifusers must take turns, it is a *timeshared connection.*

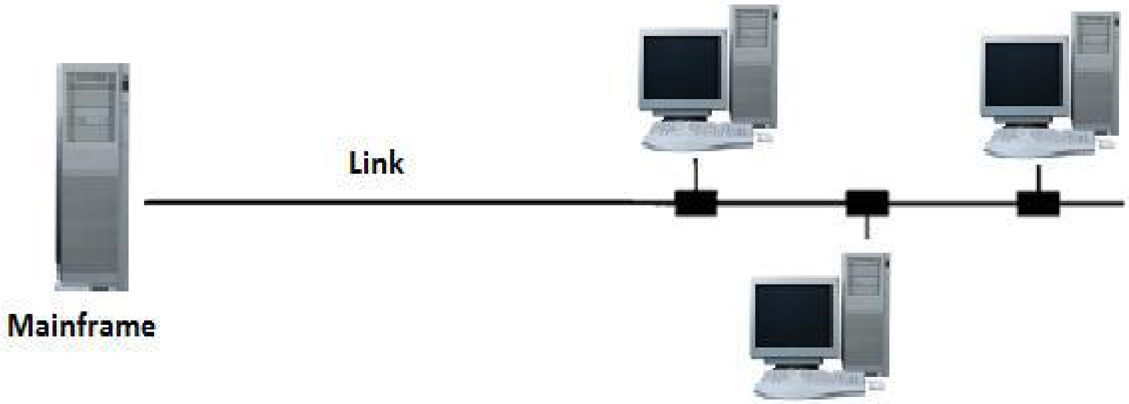


Fig: Multi-Point Connection

Physical Topology

- Topology refers to the way in which the network of computers is connected.
- Each topology is suited to specific tasks and has its own advantages and disadvantages.
- The choice of topology is dependent upon type and number of equipment being used,planned applications and rate of data transfer required, response time, and cost.
- Topology can also be defined as the *geometrically interconnection pattern by which thestations (nodes/computers) are connected using suitable transmission media*

Different Types of Topologies:

- Mesh
- Bus
- Star
- Ring
- Tree
- Unconstrained

Mesh Topology

- In this topology each node or station is connected to every other station.
- Two nodes are connected by dedicated point-point links between them. So the totalnumber of links to connect n nodes = n(n-1)/2; which is proportional to n^2.
- Media used for the connection (links) can be twisted pair, co-axial cable or optical fiber.
- With this topology there is no need to provide any additional information that is fromwhere the packet is coming, along with the packet because two nodes have a point-pointdedicated link between them.

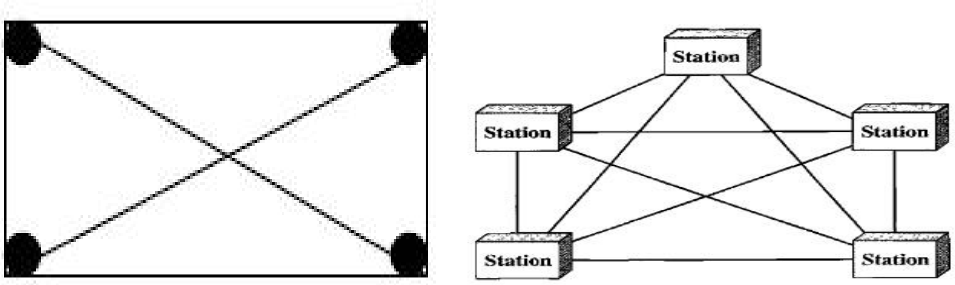


Fig: Mesh Topology with 4 and 5 nodes

Advantages

A mesh offers several advantages over other network topologies. First, the use of dedicated linksguarantees that each connection can carry its own data load. Second, a mesh topology is robust.If one link becomes unusable, it does not incapacitate the entire system. Third, there is theadvantage of privacy or security. When every message travels along a dedicated line, only theintended recipient sees it. Finally, point-to-point links make fault identification and faultisolation easy.

Disadvantages

The main disadvantages of a mesh are related to the amount of cabling and the number of I/Oports required. Installations and reconnections are difficult. Wiring can be greater than theavailable space (in walls, ceilings, or floors). Finally, the hardware required to connect each link(I/O ports and cable) can be expensive.

Bus Topology

- In Bus Topology, all stations attach through appropriate hardware interfacing known as atap, directly to a linear transmission medium, or bus.
- Full-duplex operation between the station and the tap allows data to be transmitted ontothe bus and received from the bus.
- A transmission from any station propagates the length of the medium in both directionsand can be received by all other stations.
- At each end of the bus there is a terminator, which absorbs any signal, preventingreflection of signal from the endpoints. If the terminator is not present, the endpoint actslike a mirror and reflects the signal back causing interference and other problems.

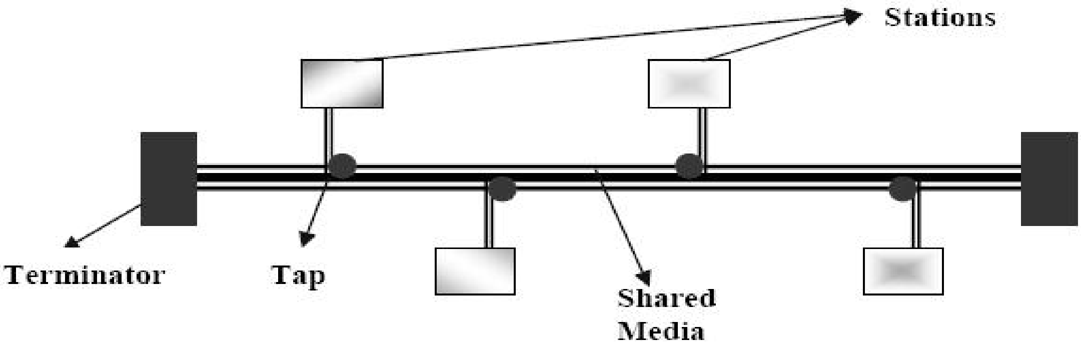


Fig: Bus Topology

Advantages

Advantages of a bus topology include ease of installation. Backbone cable can be laid along themost efficient path, then connected to the nodes by drop lines of various lengths. Only thebackbone cable stretches through the entire facility. Each drop line has to reach only as far as thenearest point on the backbone.

Disadvantages

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to beoptimally efficient at installation. It can therefore be difficult to add new devices. Signalreflection at the taps can cause degradation in quality. Adding new devices may thereforerequire modification or replacement of the backbone.

Star Topology

- In the star topology, each station is directly connected to a common central nodegenerally called as HUB.
- Typically, each station attaches to a central node, referred to as the star coupler, via twopoint-to-point links, one for transmission and one for reception.
- In general, there are two alternatives for the operation of the central node.
- One approach is for the central node to operate in a broadcast fashion. A transmission ofa frame from one station to the node is retransmitted on all of the outgoing links.
- Another approach is for the central node to act as a frame-switching device. An incomingframe is buffered in the node and then retransmitted on an outgoing link to thedestination station.

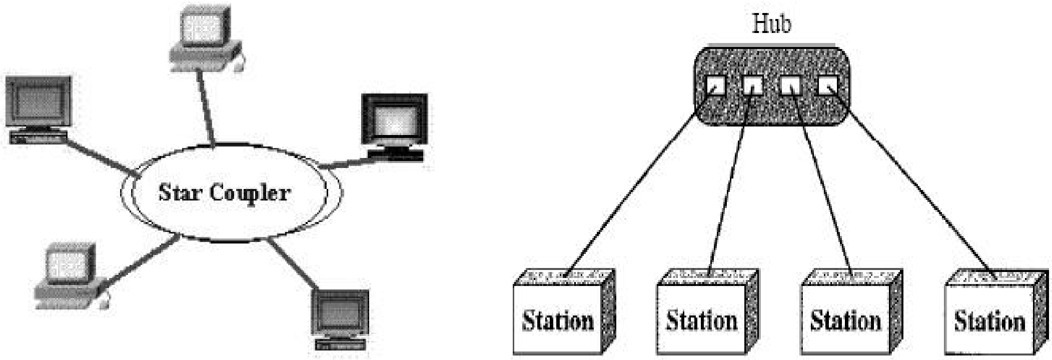


Fig: Star Topology with 4 and 5 nodes

Advantages

A star topology is less expensive than a mesh topology. In a star, each device needs only onelink and one I/O port to connect it to any number of others. This factor also makes it easy toinstall and reconfigure. Other advantages include robustness. If one link fails, only that link isaffected. All other links remain active. This factor also lends itself to easy fault identificationand fault isolation. As long as the hub is working, it can be used to monitor link problems andbypass defective links.

Disadvantages

One big disadvantage of a star topology is the dependency of the whole topology on one singlepoint, the hub. If the hub goes down, the whole system is dead. Although a star requires far lesscable than a mesh, each node must be linked to a central hub. For this reason, often more cablingis required in a star than in some other topologies.

Ring Topology

- In the ring topology, the network consists of a set of repeaters joined by point-to-pointlinks in a closed loop.

- The repeater is a comparatively simple device, capable of receiving data on one link andtransmitting them, bit by bit, on the other link as fast as they are received, with nobuffering at the repeater.
- The links are unidirectional; that is data are transmitted in one direction only and all areoriented in the same way. Thus, data circulate around the ring in one direction (clockwiseor counterclockwise).
- Each station attaches to the network at a repeater and can transmit data onto the networkthrough that repeater. As with the bus and tree, data are transmitted in frames.

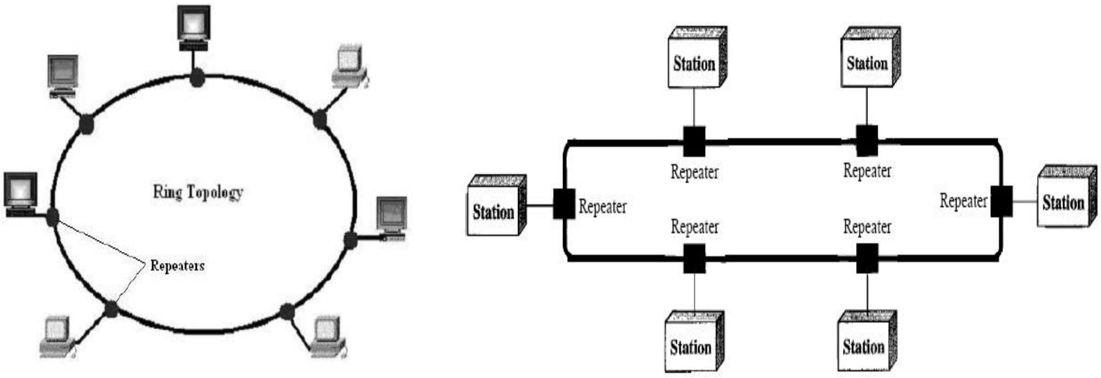
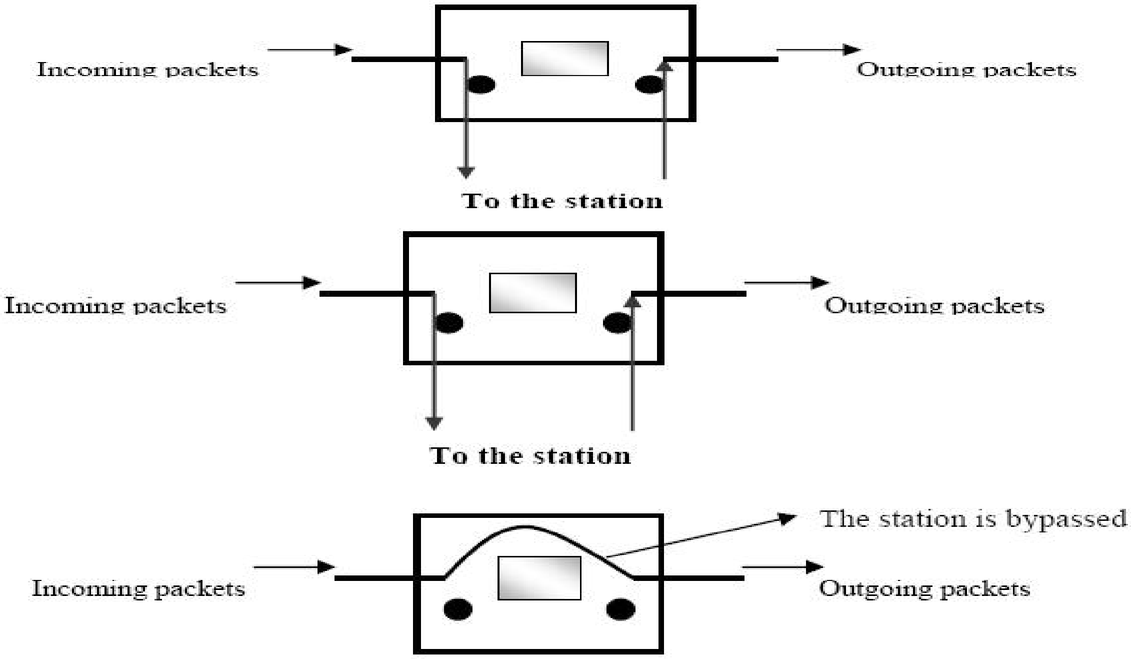


Fig: Ring Topology

Repeater: Repeater works in the following three modes:

- Listen mode: In this mode, the station listens to the communication going over the sharedmedium.
- Transmit mode: In this mode the station transmit the data over the network.
- By-Pass mode: When the node is faulty then it can be bypassed using the repeater inbypass mode, i.e. the station doesn't care about what data is transmitted through thenetwork.



Advantages

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediateneighbors (either physically or logically). To add or delete a device requires changing only twoconnections. In addition, fault isolation is simplified. Generally in a ring, a signal is circulatingat all times. If one device does not receive a signal within a specified period, it can issue analarm. The alarm alerts the network operator to the problem and its location.

Disadvantages

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (suchas a disabled station) can disable the entire network. This weakness can be solved by using adual ring or a switch capable of closing off the break.

Tree Topology

- This topology can be considered as an extension to bus topology. It is commonly used incascading equipments.
- For example, you have a repeater box with 8-port, as far as you have eight stations, thiscan be used in a normal fashion. But if you need to add more stations then you canconnect two or more repeaters in a hierarchical format (tree format) and can add morestations. In the figure R1 refers to repeater one and so on and each repeater is consideredto have 8-ports.
- This tree topology is very good in an organization as incremental expansion can be donein this way.
- Main features of this topology are scalability and flexibility. This is because, when theneed arises for more stations that can be accomplished easily without affecting thealready established network.

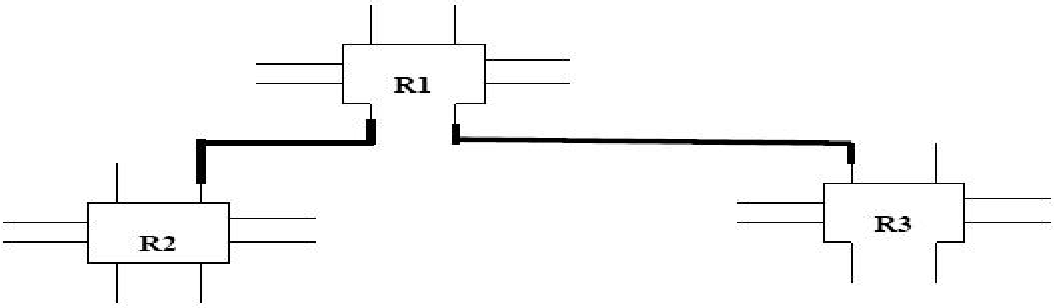


Fig: Tree Topology

Unconstrained Topology

- All the topologies discussed so far are symmetric and constrained by well-definedinterconnection pattern. However, sometimes no definite pattern is followed and nodesare interconnected in an arbitrary manner using point-to-point links as shown in Figure.▪ Unconstrained topology allows a lot of configuration flexibility but suffers from thecomplex routing problem.
- Complex routing involves unwanted overhead and delay.

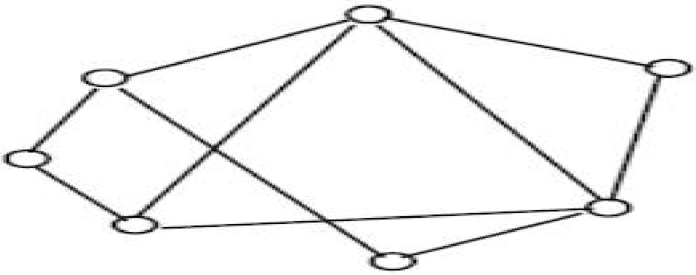


Fig: Unconstrained Topology

Hybrid Topology

A network can be hybrid. For example, we can have a main star topology with each branchconnecting several stations in a bus topology as shown in Figure.

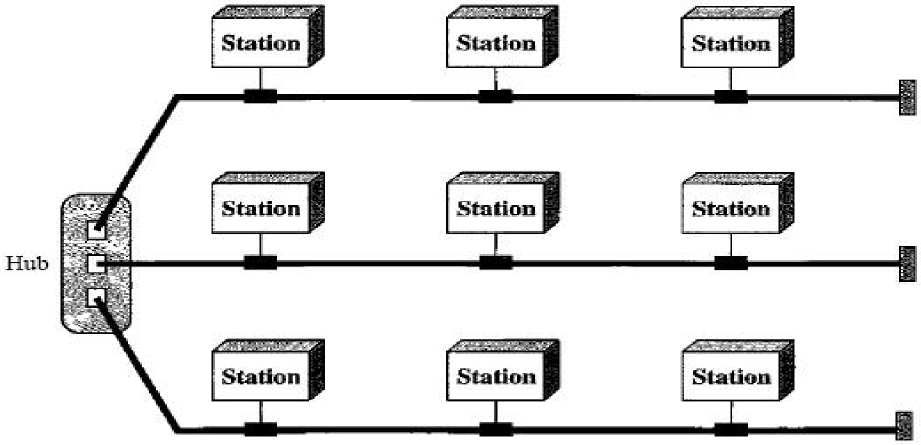


Fig: Hybrid Topology

Network Components

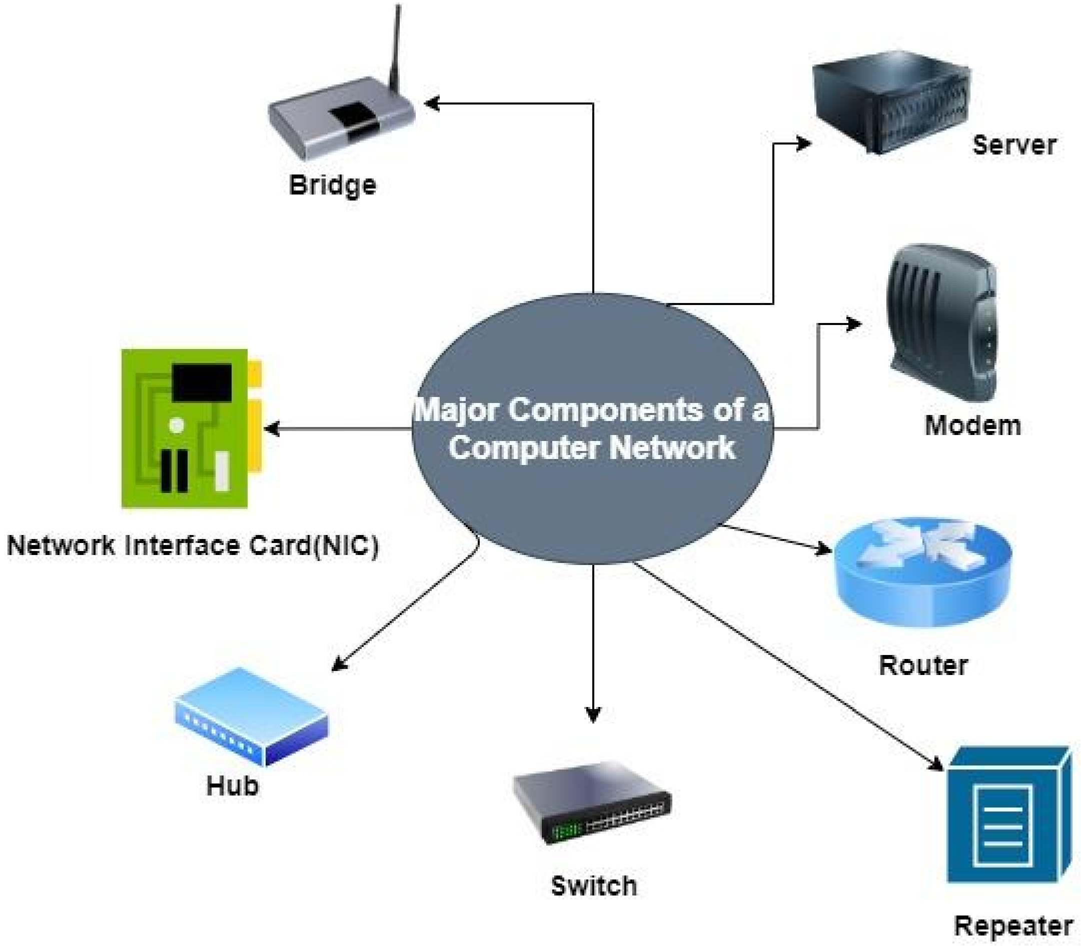
Components of Computer Networks

The key parts that are required to install a network are included in the components of the Computer network. From simple to complex there are numerous types of networks in Computer networks. The components that we need to install for a network mainly depend upon the type of Network. We can also remove some network components according to our needs.

For example: In order to establish a wireless network there is no need for cables.

Given below is a list of components of a Computer Network:

- Network Interface Card(NIC)
- HUB
- Switch
- Repeater
- Router
- Modem
- Server
- Bridge


Bridge
Server
Modem
Major Components of a Computer Network
Network Interface Card(NIC)
Router
Hub
Switch
Repeater

1. Network Interface Card(NIC)

- NIC mainly provide the physical interface between computer and cabling.NIC prepares data, sends the data, and controls the flow of data. It can also receive and translate the data into bytes for the CPU to understand.
- NIC is a hardware component that is mainly used to connect one computer with another on a Network.
- The main role of NIC is to move the serial signals on the network cables or media into parallel data streams inside the PCs.
- Transfer rate supported by NIC is 10Mb/s,100 Mb/s ,1000 Mb/s.
- Two or more NIC’s are used in the server in order to split the load.
- The main job of NIC is controlling access to the media.
- NIC can be wired or wireless. In wired NIC, there are cables and connectors that act as a medium to transfer data. While in the wireless card, the connection is generally made using an antenna that uses radio-wave technology

Factors to be taken into consideration when choosing a NIC:

1.Preparing data

2.Sending and Controlling data

3.Configuration

4.Drivers

5.Compatability

6.Performance

2. Hub

- Hubs are those devices that are used to link several computers together. Hubs repeat one signal that comes in on one port and then copies it to other ports.
- A network hub is basically a centralized distribution point for all the data transmission in a network.
- Hub is a passive device.
- The hub receives the data and then rebroadcasts the data to other computers that are connected to it. Hub mainly does not know the destination of a received data packet. Thus it is required to send copies of data packets to all the hub connections.
- Also, Hubs consumes more bandwidth on the network and thus limits the amount of communication.
- One disadvantage of using hubs is that they do not have the intelligence to find out the best path for the data packets which then leads to inefficiencies and wastage.

Types of Hub

1. Active Hub:

Active Hubs make use of electronics in order to amplify and clean up the signals before they are broadcast to other ports. Active Hubs are mainly used to extend the maximum distance between nodes. It works both as a wiring center as well as a repeater.

2. Passive Hub:

Passive Hubs are those hubs that connect only to Active Hubs. Passive Hubs are simply used to connect all ports together electrically and these are usually not powered. These hubs are cheaper than Passive hub. Passive hubs neither amplifies the signal nor regenerates the signal.

3. Intelligent Hub:

Intelligent hubs give better performance than active and passive hubs. Nowadays Intelligent hubs are widely used and are in more demand than active and passive hubs. These hubs are mainly used to connect various devices. It supports amplification and regeneration of signals at any point of incoming signals.

Intelligent hub sustains the network along with the selection path. The tasks of both passive and active are manageable by the intelligent hub.

With the help of an Intelligent hub, the Speed and efficiency of the whole network increases which helps to gain the fast and efficient performance of the network.

3. Switch

- Switch mainly resembles a Hub. It is a layer-2 device and it is used for the intelligent forwarding of messages. By intelligent we mean the decision-making ability of the switch. As hub works in the way by sending data to all ports on the device, whereas the switch sends the data to only that port that is connected with the destination device.
- The switch is a network component and is mainly used to connect the segments of the network.
- The switch is more intelligent than the network hub.
- Mainly Switches are capable of inspecting the data packets as soon as they are received, then determine the source and destination of that packet, and then forward it appropriately.
- Switch differs from the hub as it also contains ports of different speeds.
- Before forwarding the data to the ports switch performs the error checking and this feature makes the switch efficient.
- As the switch delivers the message to the connected device it was intended for, thus it conserves the bandwidth of the network and offers better performance than the hub.
- The most important feature of the switch is that it supports unicast(one to one), multicast(one to many), and broadcast(one to all) communications.
- The switch makes use of MAC address in order to send data packets to the selected destination ports.

Switches are categorized into 4:

1. Managed Switch

These are expensive switches and are mainly used in those organizations that have large and complex networks. Managed switches are configured using the Simple Network Management Protocol(SNMP). These switches provide a high level of security, complete management of the network thus beside their expensiveness these are used in large organizations because they provide high scalability and flexibility

2. Unmanaged Switch

These are cheap switches and are mainly used in home networks and in small businesses. The unmanaged switch does not need to be configured. Unmanaged switches can be easily set up just by plugging them into the network, after plugging they instantly start operating.

3. PoE Switch

These are referred to as Power over Ethernet switches. With the help of the PoE technology, these switches combine the data and power transmission over the same cable, and with the help of that devices connected to this switch are able to receive both electricity as well as data over the same line. Thus PoE switches offer more flexibility.

4. LAN Switch

LAN switch is referred to as Local Area Network switch and it is mainly used to connect devices in the internal local area network of an organization. These are helpful in reducing network congestion. Bandwidth with these switches is allocated in a manner such that there is no overlapping of data packets in the network.

4. Repeater

- The repeater is a Physical layer device. As the name suggests, the repeater is mainly used to regenerate the signal over the same network and it mainly regenerates before the signal gets corrupted or weak.
- They are incorporated into the networks in order to extend the coverage area. Repeaters can connect signals by making the use of diffrent types of cables.
- Repeaters are cost-effective.
- Repeaters are very easy o install, and after their installation, they can easily extend the coverage area of the network.
- But there is a problem with repeaters and it is they cannot those networks that are not of the same type.
- Repeaters do not help to reduce the traffic in the network.

Types of repeaters:

Types of repeaters that are available are as follows:

1. Analog Repeaters

These are only used to amplify the analog signals.

2. Digital Repeaters

These are only used to amplify digital signals.

3. Wired Repeaters

These repeaters are mainly used in wired Local area networks.

4. Wireless Repeaters

These are mainly used in wireless local area networks and also in cellular networks.

5. Local Repeaters

These are used to connect segments of a local area network that are separated by a small distance.

6. Remote Repeaters

These are mainly used to connect those local area networks that are far away from each other.

5. Router

- The router is a network component that is mainly used to send or receive data on the computer network. The process of forwarding data packets from the source to the destination is referred to as Routing.
- The router is a Network Layer(i.e Layer 3) device.
- The main responsibilities of the router are receiving data packets, analyzing them, and then forwarding the data packets among the connected computer networks.
- Whenever any data packet arrives, then first of all the router inspects the destination address and then consults with its routing tables in order to decide the optimal route and then transfers the packet along this route towards the destination.
- Routers are mainly used to provide protection against broadcast storms.
- Routers are expensive than a hub, switches, repeaters, and bridges.
- Routers can also connect different networks together and thus data packets can also be sent from one network to another network.
- Routers are used in both LAN as well as in WAN(wide area network).
- Routers share data with each other in order to prepare and refresh the routing tables.

Types of Routers:

Different types of routers are as follows:

1.Core Routers

Core routers are mainly used by service providers(like AT&T, Vodafone) or by cloud providers like (Amazon, Microsoft, and Google). Core Routers provide maximum bandwidth so as to connect additional routers or switches. Core routers are used by large organizations.

2.Edge Routers

An edge router is also known as a Gateway router or gateway simply. The gateway is the network's outermost point of connection with external networks and also includes the Internet. These routers are mainly used to optimize bandwidth and are designed in order to connect to other routers so as to distribute data to end-users. Border Gateway protocol is mainly used for connectivity by edge routers.

These are further categorized into two:

subscriber edge routers

label edge routers.

3. Brouters

Brouter means bridging routing device. These are special routers and they also provide functionalities of bridges. They perform the functioning of the bridge as well as of router; like a bridge, these routers help to transfer data between networks, and like the router, they route the data within the devices of a network.

4.Broadband Routers

It is a type of networking device that mainly allows end-users to access broadband Internet from an Internet service provider (ISP). The Internet service provider usually provides and configures the broadband router for the end-user.

5.Distribution Routers

These routers mainly receive the data from the edge router (or gateway) via a wired connection and then sends it on to the end-users with the help of Wi-Fi.

6.Wireless Routers

These routers combine the functioning of both edge routers and distribution routers. These routers mainly provide a WiFi connection to WiFi devices like laptops, smartphones, etc. These routers also provide the standard Ethernet routing. For indoor connections, the range of these routers is 150 feet while for outdoor connections it is 300 feet.

6. Modem

- The modem is basically a hardware component that mainly allows a computer or any other device like a router, switch to connect to the Internet. A modem is basically a shorthand form of **Modulator-Demodulator**.
- One of the most important functions of the modem is to convert analog signals into digital signals and vice versa. Also, this device is a combination of two devices: modulator and demodulator. The **modulator** mainly converts the digital data into analog data at the time when the data is being sent by the computer.
- The **demodulator** basically converts the analog data signals into digital data at the time when it is being received by the computer.

7. Server

A Server is basically a computer that serves the data to other devices. The server may serve data to other devices or computers over a local area network or on a Wide area network with the help of the Internet. There can be virtual servers, proxy servers, application servers, web servers, database servers, file servers, and many more.

Thus servers are mainly used to serve the requests of other devices. It can be hardware or software.

8. Bridge

It is another important component of the computer network. The bridge is also a layer-2(that is data link layer device). A bridge is mainly used to connect two or more local area networks together. These are mainly used as they help in the fast transferring of the data.

But these are not versatile like routers.

Thus Bridge can mainly transfer the data between different protocols (i.e. a Token Ring and Ethernet network) and operates at the data link layer or level 2 of the OSI (Open Systems Interconnection) networking reference model as told above.

Bridges are further divided into two:

Local bridge

These are ordinary bridges.

Remote bridges

These are mainly used to connect networks that are at a distance from each other. Generally Wide Area Network is provided between two bridges

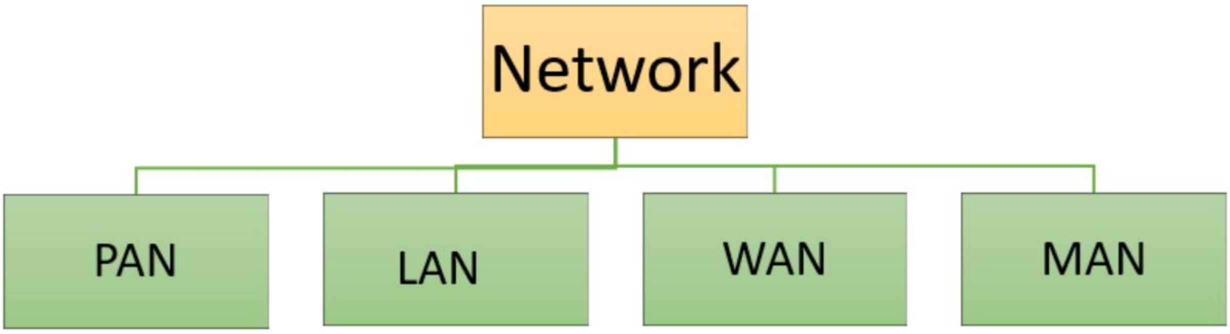
Some Bridge protocols are spanning tree protocol, source routing protocol, and source routing transparent protocol.

Network Types

Different Types of Computer Networks

There are various types of Computer Networking options available. The classification of network in computers can be done according to their size as well as their purpose.

The size of a network should be expressed by the geographic area and number of computers, which are a part of their networks. It includes devices housed in a single room to millions of devices spread across the world. Following are the popular types of Computer Network:



Some of the most popular computer network types are:

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

What is PAN (Personal Area Network)?

PAN (Personal Area Network) is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

Characteristics of PAN

- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.
- It can be wirelessly connected to the internet called WPAN.

Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

Here are the important pros/benefits of PAN network:

1.PAN networks are relatively secure and safe

2.It offers only short-range solution up to ten meters

3.Strictly restricted to a small area

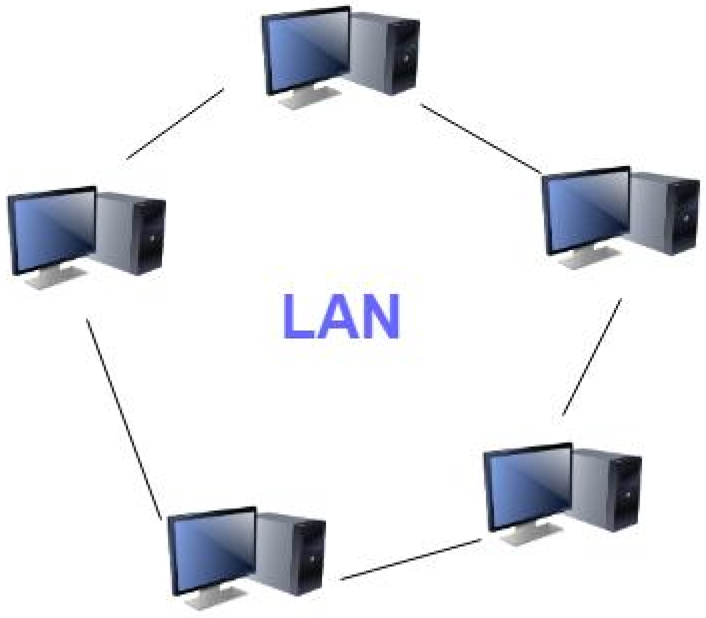
Disadvantages of PAN

1.It may establish a bad connection to other networks at the same radio bands.

Distance limits.

What is a LAN (Local Area Network)?

A Local Area Network (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium. It is a network which consists of less than 5000 interconnected devices across several buildings.



Local Area Network (LAN)

Characteristics of LAN

Here are the important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and ethernet.

Advantages of LAN

Here are the pros/benefits of LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

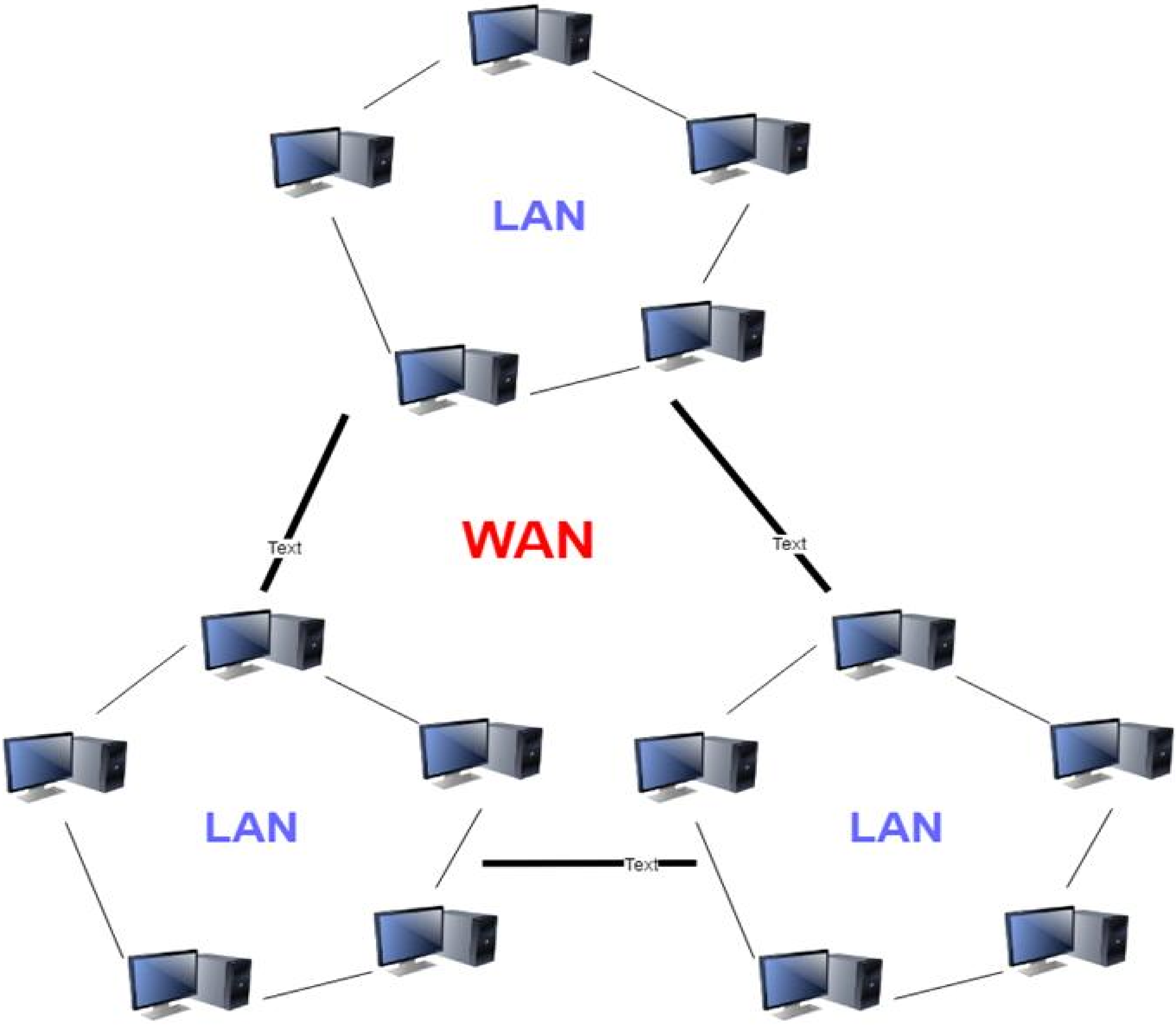
Here are the cons/drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.

- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

What is WAN (Wide Area Network)?

WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.



Wide Area Network (WAN)

Characteristics of WAN

Below are the characteristics of WAN:

- The software files will be shared among all the users; therefore, all can access to the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/pros of WAN:

- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

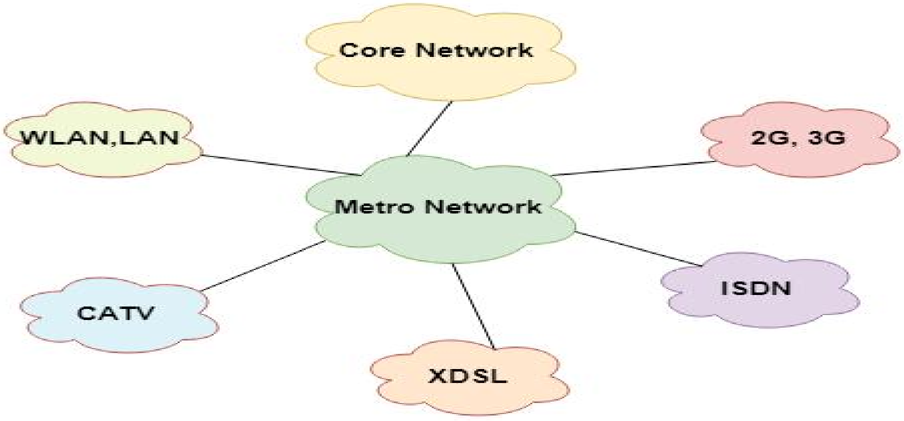
Disadvantages of WAN

Here are the drawbacks/cons of WAN network:

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.
- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of network in computer.

What is MAN (Metropolitan Area Network)?

A **Metropolitan Area Network** or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.



Metropolitan Area Network (MAN)

Characteristics of MAN

Here are important characteristics of the MAN network:

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are the pros/benefits of MAN network:

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

Here are drawbacks/cons of using the MAN network:

- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

Other Types of Computer Networks

Apart from above mentioned computer networks, here are some other important types of networks:

- WLAN (Wireless Local Area Network)
- Storage Area Network
- System Area Network
- Home Area Network
- POLAN- Passive Optical LAN
- Enterprise private network
- Campus Area Network
- Virtual Area Network

Let’s see all these different types of networks in detail:

1) WLAN

WLAN (Wireless Local Area Network) helps you to link single or multiple devices using wireless communication within a limited area like home, school, or office building. It gives users an ability to move around within a local coverage area which may be connected to the network. Today most modern day’s WLAN systems are based on IEEE 802.11 standards.

2) Storage-Area Network (SAN)

A Storage Area Network is a type of network which allows consolidated, block-level data storage. It is mainly used to make storage devices, like disk arrays, optical jukeboxes, and tape libraries.

3) System-Area Network

System Area Network is used for a local network. It offers high-speed connection in server-to-server and processor-to-processor applications. The computers connected on a SAN network operate as a single system at quite high speed.

4) Passive Optical Local Area Network

POLAN is a networking technology which helps you to integrate into structured cabling. It allows you to resolve the issues of supporting Ethernet protocols and network apps.

POLAN allows you to use optical splitter which helps you to separate an optical signal from a single-mode optical fiber. It converts this single signal into multiple signals.

5) Home Area Network (HAN)

A Home Area Network is always built using two or more interconnected computers to form a local area network (LAN) within the home. For example, in the United States, about 15 million homes have more than one computer.

These types of network connections help computer owners to interconnect with multiple computers. This network allows sharing files, programs, printers, and other peripherals.

6) Enterprise Private Network

Enterprise private network (EPN) networks are build and owned by businesses that want to securely connect numerous locations in order to share various computer resources.

7) Campus Area Network (CAN)

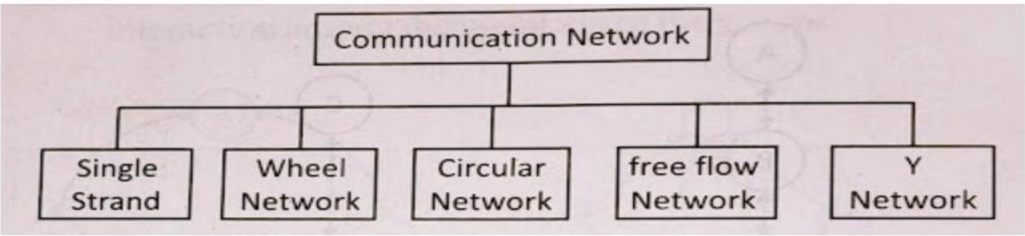
A Campus Area Network is made up of an interconnection of LANs within a specific geographical area. For example, a university campus can be linked with a variety of campus buildings to connect all the academic departments.

8) Virtual Private Network

A VPN is a private network which uses a public network to connect remote sites or users together. The VPN network uses “virtual” connections routed through the internet from the enterprise’s private network or a third-party VPN service to the remote site.

It is a free or paid service that keeps your web browsing secure and private over public WiFi hotspots.

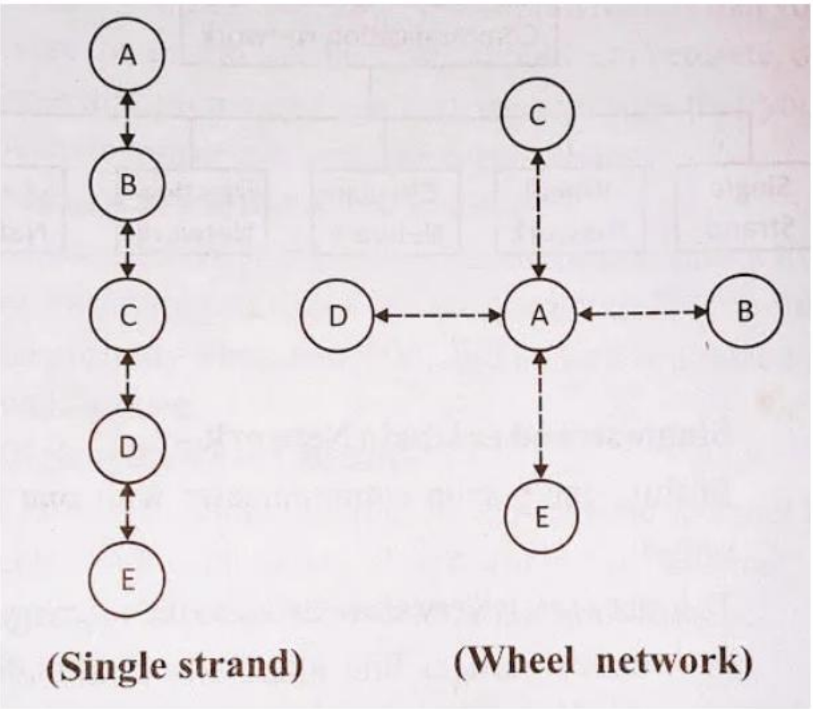
Network Communication Types



1. Single Strand or Chain Network

In this, a single person converses with just that one person.

- Because of the scalar chain of command's direct vertical message flow, this network operates relatively slowly.
- It can move in a straight line from top to bottom or from bottom to top. It is one of the types of communication networks.
- As a result, communication occurs through official channels, such as from superior to subordinate and vice versa.
- In the chain network, there is no horizontal communication.



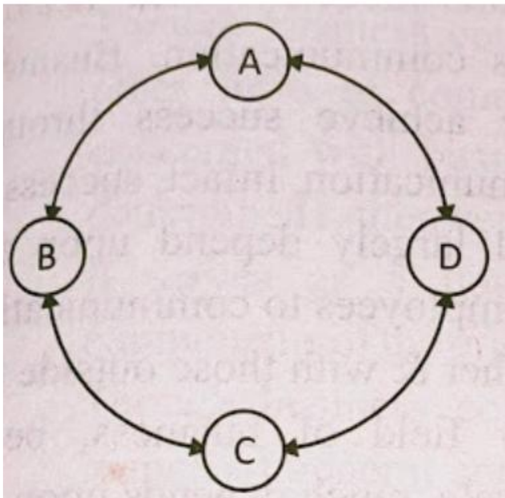
2. Wheel Communication Network

The wheel network represents the communication pattern that allows subordinates to communicate with and through one management.

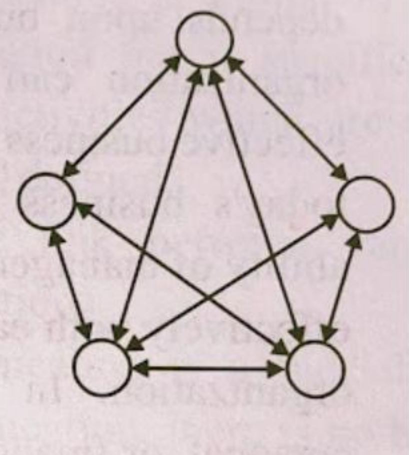
All communications must go via the manager, who serves as the network's central authority and resembles the hub of a wheel, hence the name "wheel network."

3. Circular Communication Network

The message circulates in a circle in a circular network. A circular network's main drawback is that communication takes longer. Only two neighbors can communicate with each other at a time.



Circular Network



Free Flow Network

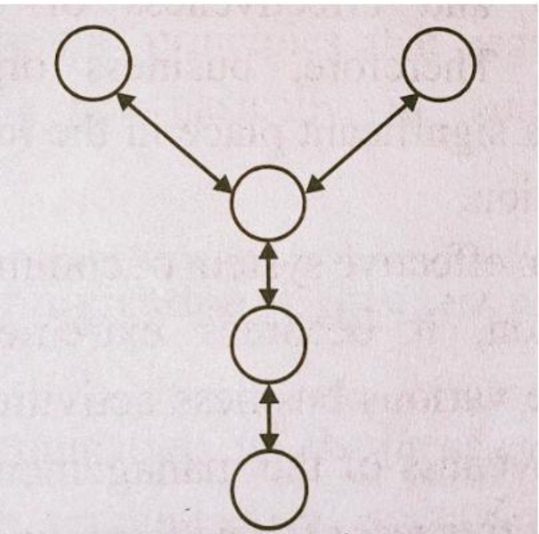
4. Free Flow Communication Network

The flow of information is unrestricted in such an organizational structure and organizational appraisal.

- Everyone in the company is allowed to communicate with anyone and everyone else.
- This network is either unstructured or informational.
- It's incredibly adaptable.

5. Y Communication Network

Information moves in this centralized network via predetermined paths. These networks might be suitable for straightforward tasks requiring little interaction between group members.



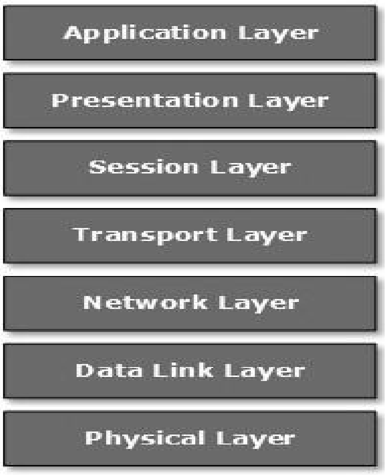
Y Network

As most people belong to many networks, different networks emerge in real life. The financial manager, for instance, might be at the hub of a chain and involved in the wheel and circle networks. As a result, modern enterprises use a variety of network arrangements.

Introduction to Networking Models

1. OSI Model:

Open System Interconnect is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). This model has seven layers:



Application Layer: This layer is responsible for providing interface to the application user. This layer encompasses protocols which directly interact with the user.

Presentation Layer: This layer defines how data in the native format of remote host should be presented in the native format of host.

Session Layer: This layer maintains sessions between remote hosts. For example, once user/password authentication is done, the remote host maintains this session for a while and does not ask for authentication again in that time span.

Transport Layer: This layer is responsible for end-to-end delivery between hosts.

Network Layer: This layer is responsible for address assignment and uniquely addressing hosts in a network.

Data Link Layer: This layer is responsible for reading and writing data from and onto the line. Link errors are detected at this layer.

Physical Layer: This layer defines the hardware, cabling, wiring, power output, pulse rate etc.

TCP/IP model:

1. The TCP/IP model was developed prior to the OSI model.

2. The TCP/IP model is not exactly similar to the OSI model.

3. The TCP/IP model consists of five layers: the application layer, transport layer, network

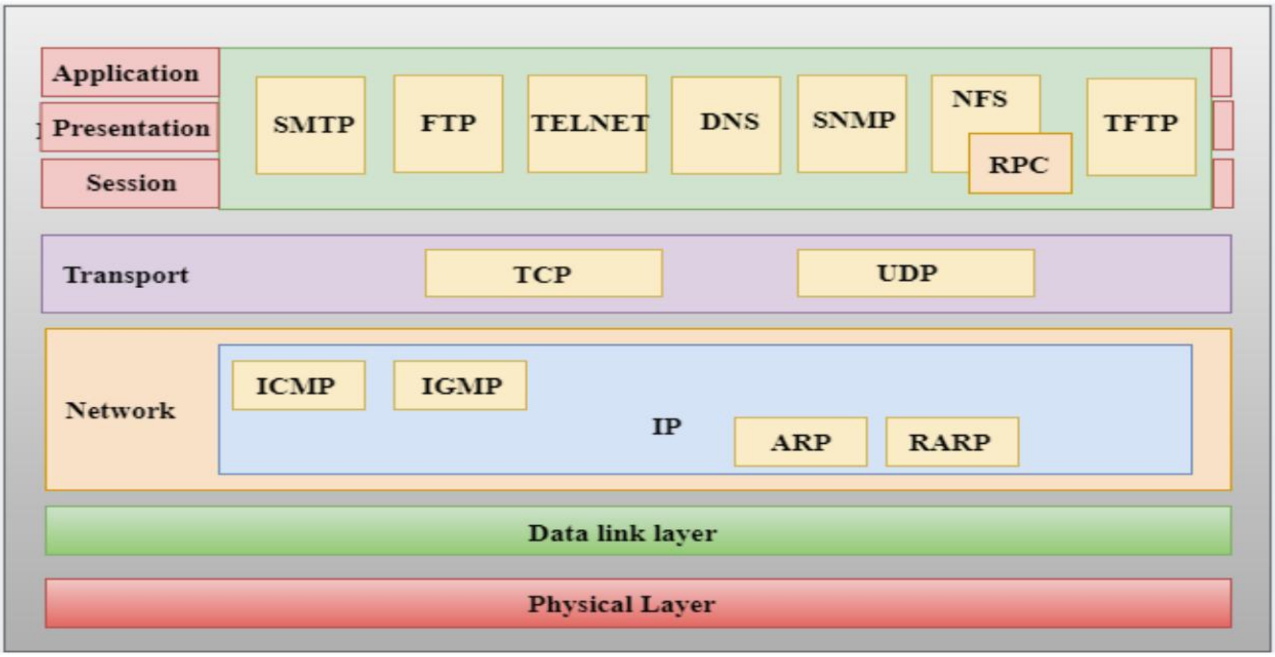
layer, data link layer and physical layer.

4. The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

5. TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

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

Functions of TCP/IP layers:



Main difference between TCP/IP and OSI Model:

1.TCP/IP Model is a communication protocols suite using which network devices can be connected to the Internet. On the other hand, the OSI Model is a conceptual framework, using which the functioning of a network can be described.

2.TCP/IP vs OSI: TWO are the different layers

The TCP/IP Model comprises four layers: Network Interface, Internet, Transport and Application. The OSI Model comprises seven layers: Physical, Data Link, Network, Transport, Session, Presentation and Application.

3.TCP/IP a part of the OSI Model

There is a separate layer for Data Link and Physical in the OSI Model, whereas, the TCP/IP has a single Network Interface layer for the same. Similarly, there is Application, Presentation and Session layers in OSI, which are combined into one layer (Application) for TCP/IP.

4.TCP/IP vs OSI: Which came first

Among TCP/IP and OSI, the Open Systems Interconnection model was introduced by the International Organisation of Standardization in 1984 and the TCP/IP model was introduced about 10 years before that.

Similarities between the OSI and TCP/IP model:

The following are the similarities between the OSI and TCP/IP model:

1.Share common architecture

Both the models are the logical models and having similar architectures as both the models are constructed with the layers.

2.Define standards

Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.

3.Simplified troubleshooting process

Both models have simplified the troubleshooting process by breaking the complex function into simpler components.

4.Pre-defined standards

The standards and protocols which are already pre-defined; these models do not redefine them; they just reference or use them. For example, the Ethernet standards were already defined by the

IEEE before the development of these models; instead of recreating them, models have used these pre-defined standards.

5.Both have similar functionality of 'transport' and 'network' layers

The function which is performed between the **'presentation'** and the **'network'** layer is similar to the function performed at the **transport** layer.

Cyber Security

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information.

Network security can be simply defined as protection of data during their transmission over the network from unauthorized party. It is susceptible to attacks by unauthorized party, both from inside and outside the network. But network security is generally taken as providing protection at the boundaries of an organization.

Information security on the other hand, is a somewhat more general concept of being sure information systems have confidentiality, integrity, and availability.
This can include network security as well as cryptography, access control (not only who has access but what they can do), physical security, and more. It covers everything from the earliest encryption codes to how computers are locked down.

How can we provide network security?

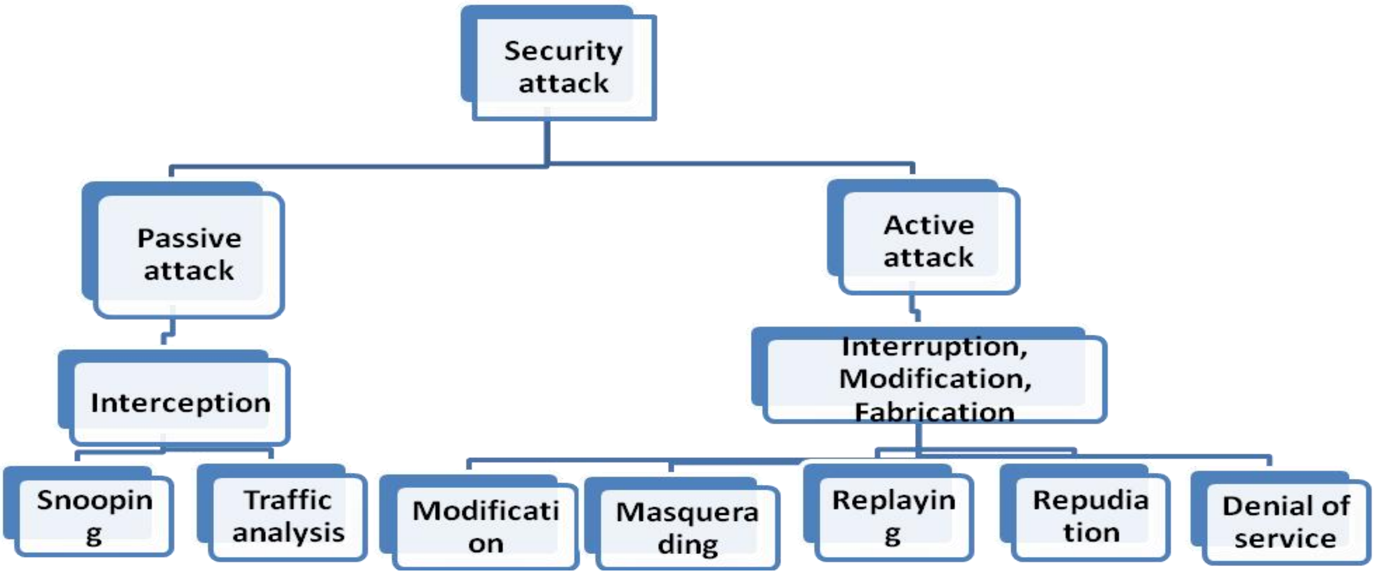
- The most important tool for network security is cryptography.
- Using the cryptography tool we can provide a security for network system

Aspects of Security: The aspects of information security is

- Security attack
- Security service
- Security mechanism

Security attack:
Any action that compromises the security of information owned by an organization is called security attack. Security attacks are usually classified in to two types:

- Passive attack
- Active attack



Passive attack:

In a passive attack, the attacker’s goal just to obtain information. This means that the attack does not modify data or harm the system (means sender & receiver and their communication). The system continues with its normal operations.

However, the attack may harm the sender or the receiver of the message, but the system is not affected. Here the system is not affected, for this reason, it is difficult to detect this type of attack until the sender or receiver finds out about the leaking of confidential information

- **This attack threaten confidentiality**
- **This attack can be prevented by encipherment of data**
- **Interception is a passive attack**

Passive attacks are:

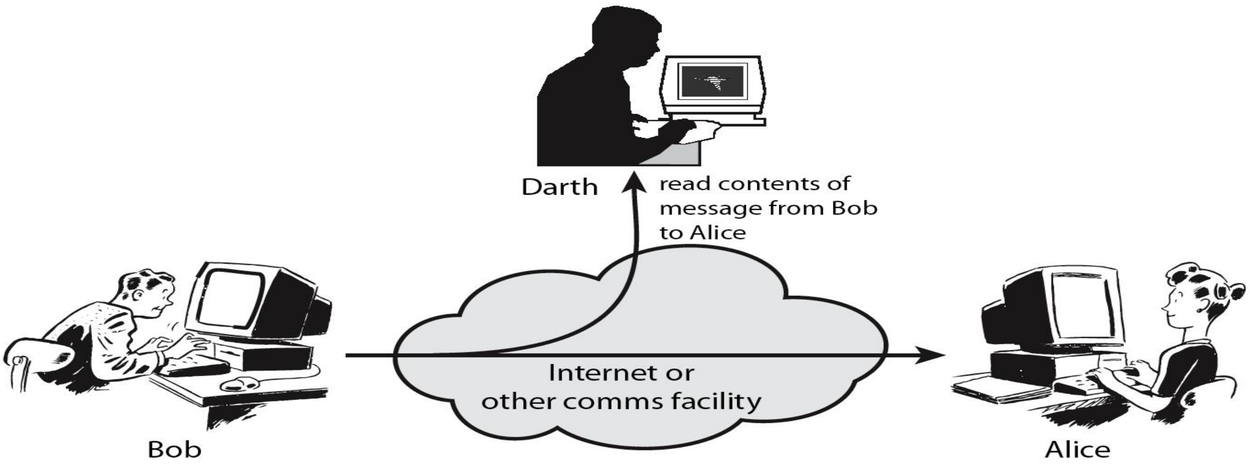
- Snooping (Release of message content)
- Traffic analysis

1.Snooping :

- Snooping refers to unauthorized party access to or interception of data is called snooping
- To prevent snooping, the data can be made non-intelligible to the interceptor by using encipherment techniques.

Example:

A file transferred through the internet may contain confidential information. An unauthorized entity may intercept the transmission and use the content for her own benefit.

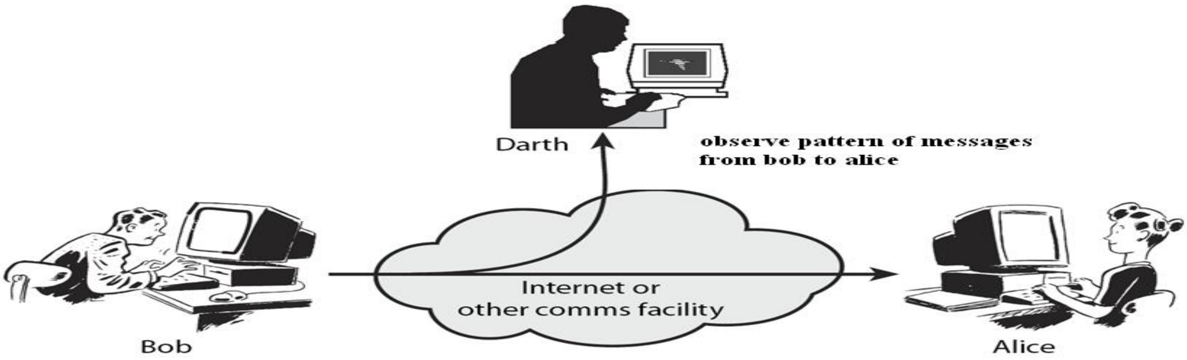

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

2.Traffic analysis:

suppose that we had a way of masking (encipherment) the content of message(data). The masking message is non-intelligible to the interceptor, but the interceptor can obtain information by monitoring online traffic.

Example:

Interceptor can find e-mail address of the sender or the receiver. She can collect the pair of requests and responses to help her nature of transaction.


Darth
observe pattern of messages from bob to alice
Internet or other comms facility
Bob
Alice

Active attack:

In active attack, the attacker's goal is not only obtain information and may change the data or harm the system. Here the system is affected, for this reason, it is normally easier to detect then to prevent
this attack threaten the integrity ,availability and authenticity. Interruption, modification, fabrication are active attacks.

Active attacks are:

- **Modification**
- **Masquerading or spoofing**
- **Replaying**

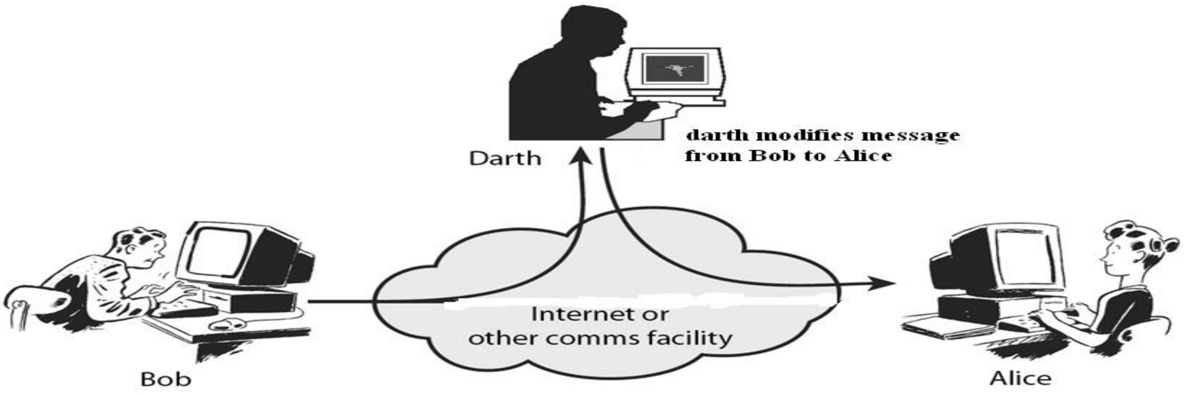
- **Repudiation**
- **Denial of service**

1.Modification:

An unauthorized party not only accessing the information and also modifies (tampers) the information and send to destination is called modification.

Example:

A customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the transaction to benefit herself.


Darth
darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

2.Masquerading:

An unauthorized entity act like as source entity to counter fit objects into the system to gain some information in called masquerading or spoofing

Example:

Some time the attacker act like source and gain the confidential information from the receiver for their own benefits.

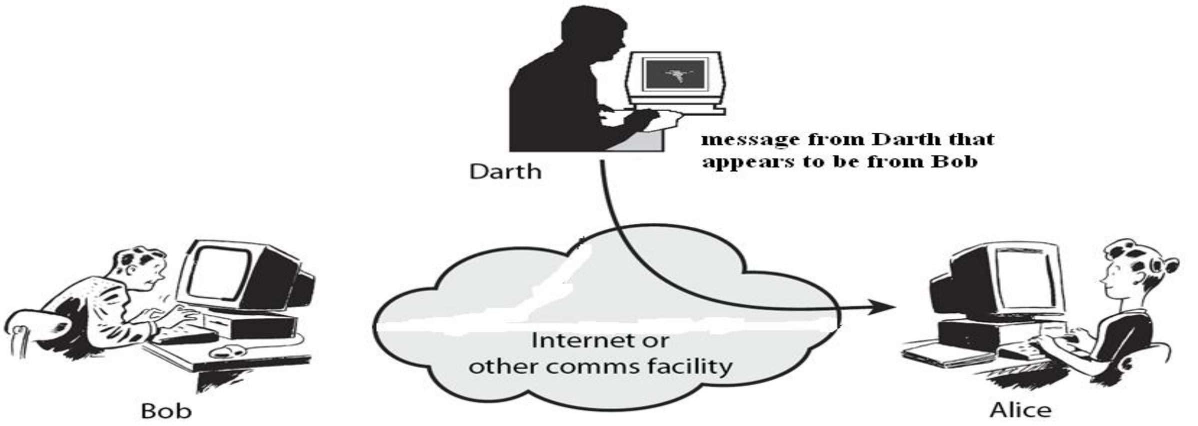
For example, from an employee; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade, since it makes it much easier for an attacker to gain access. Once the attacker has been authorized for entry, they may have full access to the organization's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete software and data, and make changes to network configuration and routing information.

3.Replaying:

Replaying is another type of attack. in this attack the attacker obtain a copy of the message sent by user and later tries to replay it.

Example:

A person send a request to her bank to ask for payment from the bank. In middle the attacker intercept the message and sends it again to receive another payment from the bank.


Darth
message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

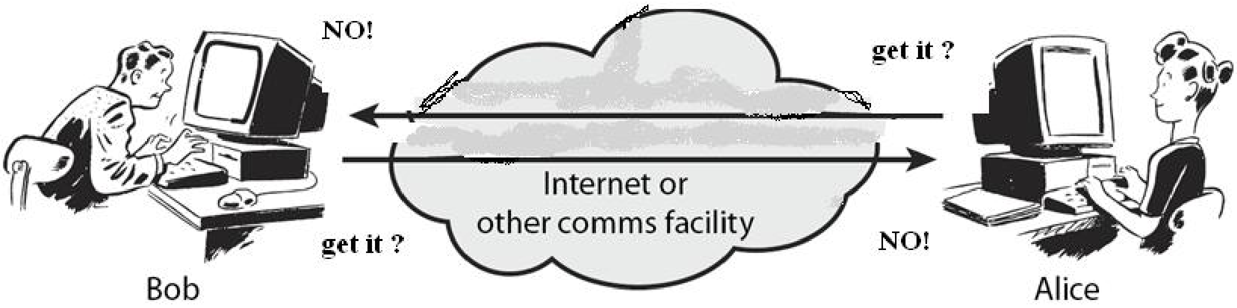
4.Repudiation:

This type of attack is different from other attacks because it is performed by one of the two parties in the communication : the sender or receiver. Repudiation is denying that you have sent or released a message, or denying that you have received or read message.

Example:

An example denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request.

An example denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and ask to be paid.



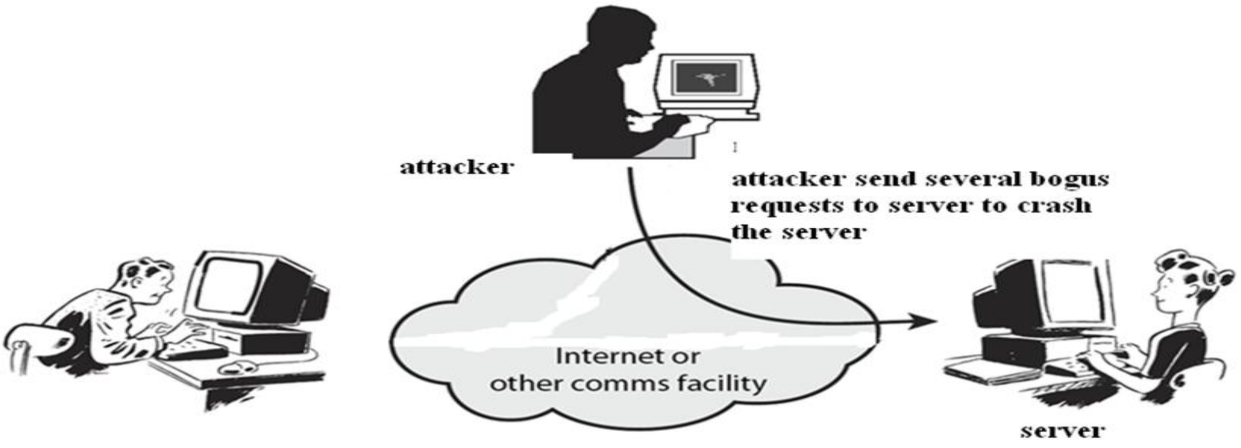
Denial of service:

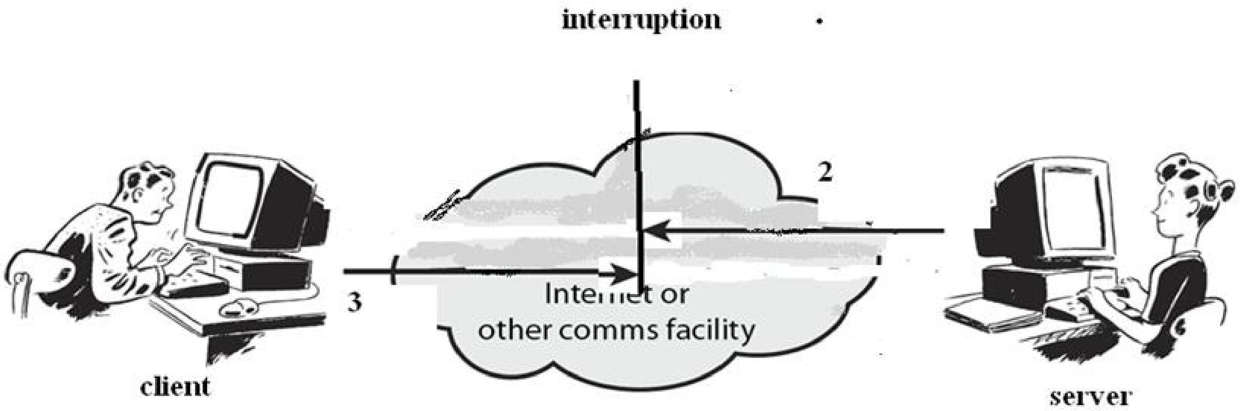
Denial of service (DoS) is very common attack . it may slow down or totally interrupt the service of the system.

The attacker can use several strategies to achieve this:

- The attacker might send so many bogus requests to a server that the server crashes because of the heavy load

- The attacker might intercept and delete a server's response to a client, making the client to believe that the server is not responding.
- The attacker might intercept and delete a client's requests to a server, making the client to believe that the server is not responding.


attacker
1
attacker send several bogus requests to server to crash the server
Internet or other comms facility
server



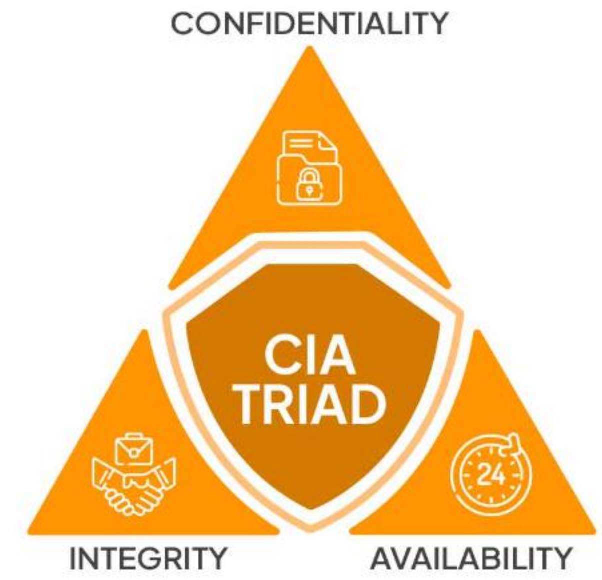
Cyber Security Objectives and Services

Cyber Security Objectives

The Objectives of cyber security is to ensure secure storage, control access and prevent unauthorized processing, transfer, or deletion of data. It safeguards the confidentiality, integrity, and availability of information.

A number of cyber security measures are put in place to protect networks and computer hardware from unwanted threats and damages. Organizations draft security goals and policies based on the cyber security standards they are required to uphold.

CIA triad stands upright on three pillars–Confidentiality, Integrity, and Availability. People, Processes, and Technology come together to attain these objectives of cyber security and ensure effective security systems.



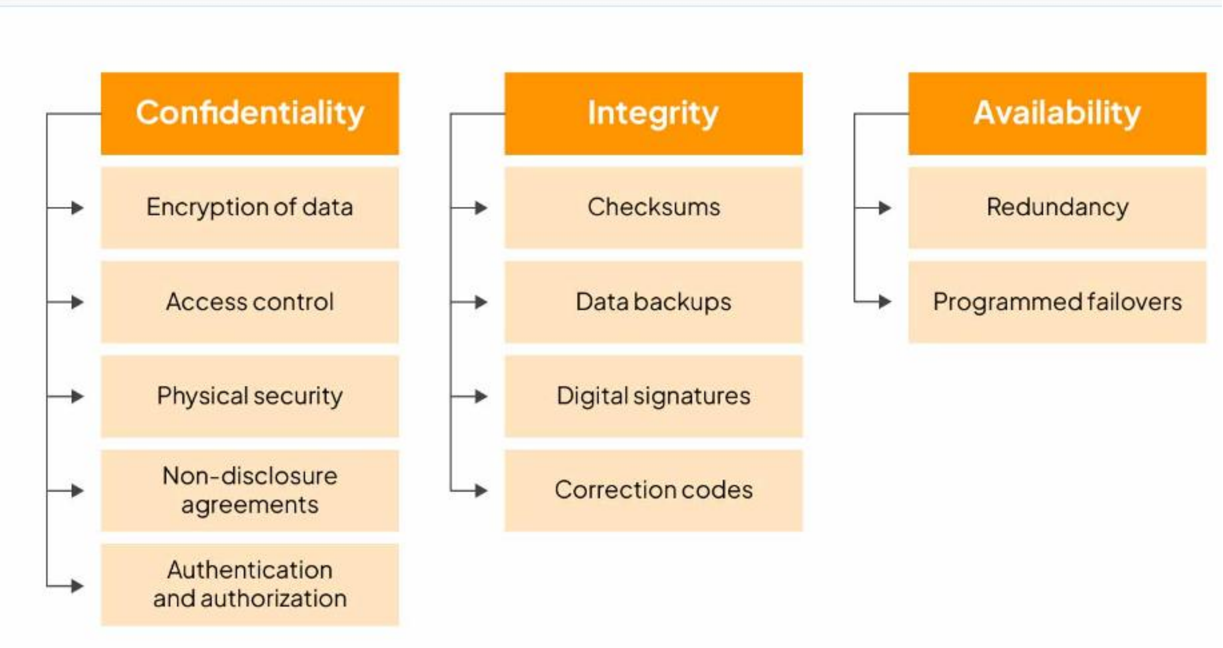
Confidentiality:
Collecting, storing, and sharing data in the digital space have made us prone to cyber attacks. Confidentiality states that only authorized people should be able to access sensitive information.

Any Personal Identifiable Information (PII) that can help recognize a person, any financial information such as transaction details made on e-commerce sites is supposed to be kept confidential.

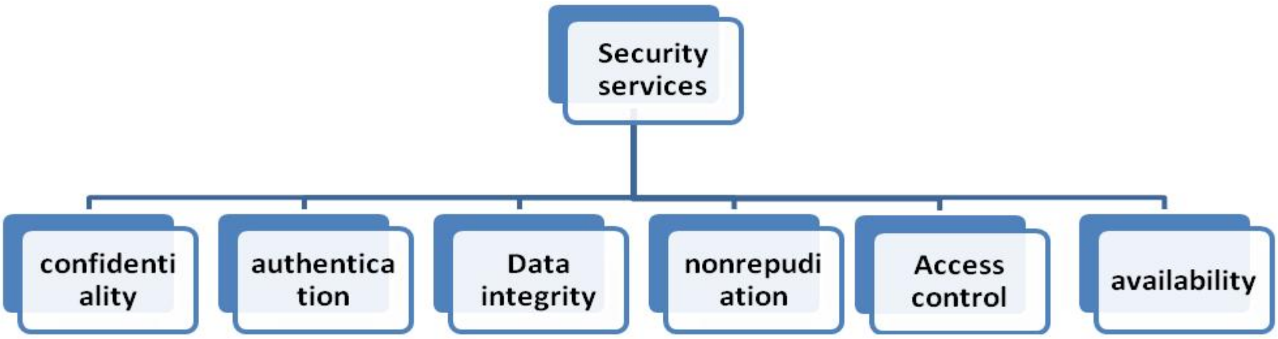
Integrity:
Integrity maintains the dependability of information and ensures that it has been in its original form throughout and is exact. Stored data or data disseminated or used should not be altered at any time unless authorized by a licensed individual or system

Availability:
Availability ensures the accessibility of information to authorized personnel at the right time. They should be able to process data whenever the need arises.

Tools to achieve CIA triad



Cyber Security services



1.Confidentiality:

Stored or transmitted information is accessible (even travel over insecure links) only authorized parties, it doesn't accessible to unauthorized parties. Means an unauthorized entity doesn't get information about the message.

Only sender and, intended receiver should "understand" message content.

- Sender encrypts the message
- Receiver decrypts the message

Confidentiality has been designed to prevent interception (such as snooping and traffic analysis). It is used for sensitive fields such as government and industry. It is important security service in information security
Confidentiality uses the encipherment, routing control security mechanisms.

2.Authentication: (who created or sent the data)

In authentication both sender and receiver should be able to confirm the proof identity for talking (communication) each other. Means the receiver knows for sure that the message comes from particular source.

Authentication is first step in any network security solution. Authentication has been designed to prevent fabrication (such as spoofing and replaying) attacks. Authentication uses the encipherment, digital signature security mechanisms.

3.Data integrity (or message authentication):

Integrity prevention of unauthorized party modification of information means an unauthorized entity can't alter the message.

Integrity can apply to stream of messages. Integrity includes both content of information and source of data. Integrity has been designed to prevent the modification security attack. Integrity uses the encipherment, digital signature, data integrity security mechanisms.

4.Non-repudiation:

Non-repudiation service is protection against denial by one of the parties(sender, receiver) in a communication. In this case the sender and receiver can keep proofs to avoid repudiation. Non-repudiation has been designed to prevent the repudiation security attack. Non-repudiation uses the digital signature, data integrity, notarization security mechanisms.

5.Availability:

The data must be available to the authorized parties when they required to access them is called availability. Availability has been designed to prevent the Denial of Service security attack. It is also prevent virus that deletes files. Availability uses data integrity, authentication exchange security mechanisms.

6.Access control:

Access control prevention of the unauthorized use of a resource means the host systems and applications are limited to access by the communication links and any unauthorized part can't access then. Access control uses the access control security mechanisms.

Other Terms of Cyber Security

1. Malware

As our first item among the leading cyber security terms, Malware, short for malicious software, is any type of harmful software designed to damage or disrupt a computer system.

Malware comes in different forms. Its aim is often to steal sensitive information or gain access to a computer system.

2. Phishing

Phishing is a type of cyber attack that attempts to fool users into providing sensitive information, such as passwords or credit card details, via fake emails and websites.

These phishing attacks may be carried out by individuals or large-scale organized cybercrime groups in an attempt to steal personal data or financial information.

3. DDoS Attack

A distributed denial of service (DDoS) attack involves the use of multiple devices to flood a website or server with traffic, resulting in its temporary shutdown.

These attacks are often motivated by financial gain or political motivations and can be extremely costly for businesses and organizations.

4. Ransomware

Ransomware is a type of cyber attack that locks users out of their computer systems until they pay a ransom, typically in the form of cryptocurrency, such as Bitcoin.

These attacks can be devastating to individuals and businesses, leading to lost data and high costs associated with restoring systems.

5. Botnet

A botnet is a network of compromised computers used to carry out cyberattacks on other systems.

Hackers will often infect computers using malware, then control those devices remotely to destroy data.

Then, they will proceed to steal information or carry out other illegal activities.

6. Zero-Day Attack

A zero-day attack refers to a type of cyber attack that exploits a vulnerability in software that no one is aware of yet.

These attacks are particularly dangerous, as they can bypass traditional security measures and defenses before developers have an opportunity to address the issue.

7. Trojan Horse

A Trojan horse (“trojan”) is malware that appears harmless but can perform malicious actions on an infected device once downloaded or opened.

These attacks are often disguised as legitimate applications or files. This is how they can trick users into clicking on them and releasing the trojan onto their computers.

8. Spyware

Spyware is a type of malware that can collect and transmit private user information without the user’s knowledge or consent.

These programs are often installed on users' devices as part of other types of malicious software, such as trojans or viruses.

9. Clickjacking

Clickjacking, also known as "UI redress attack," is another type of malicious cyber attack.

With clickjacking, an attacker tricks users into clicking on hidden elements in order to perform unwanted actions.

The attacker aims to hijack user accounts or steal sensitive information.

Clickjacking typically employs social engineering techniques like phishing to trick users into clicking harmful links or downloading dangerous files.

One way to prevent these attacks is to invest in end-to-end human factor solutions.

Myths Around Cyber Security

Myth 1 — Too much security diminishes productivity

There is a common idea that increased security makes it difficult for even employees to access what they need, not just hackers. Strict security policies such as regular monitoring and access control are believed to hinder productivity at work. However, doing away with security may have far-reaching consequences for your business. A successful attack like a DDoS attackor ransomware can bring your business to a standstill. Employees might not be able to access important files, networks, and information after an attack. The recovery takes days and sometimes even weeks.

Truth: Enhanced cybersecurity can boost productivity.

A modern cybersecurity approach uses security tools that have a built-in security feature that integrates seamlessly into your system. It also leverages advanced tech intelligence and analytics for real-time detection and mitigation of threats. This allows developers to concentrate on improving their productivity since they no longer need to worry about security issues.

Myth 2 — Cyberattacks are only caused by external threat actors

Insider threats are on the rise and are fast becoming a cause of concern for businesses. Insider threats can include employees, vendors, contractors, business partners, or an external intruder trying to impersonate an employee. A recent survey revealed that insider threats are responsible for 60% of data breaches.

In addition, you can never be fully aware of where these attacks can originate from, and traditional security solutions are largely ineffective when it comes to these threats. This makes them much harder to detect and contain than external threats.

Truth: Therefore, cyberattacks can very well start from someone you know.

Use a combination of behavioral analytics and privilege and access management to minimize insider threats. Additionally, conduct security awareness training sessions to educate employees about the dangers of insider threats and how to detect them.

Myth 3 — Cybercriminals only attack large businesses

Small and medium-sized businesses may often be under the false impression that their data isn't valuable to hackers. However, small and medium-sized businesses are one of the top targets for hackers.

A recent study revealed that hackers targeted small businesses nearly half of the time. But only 14% of these businesses were prepared to defend themselves in such a situation.

Truth: No business - no matter how large or small, is ever immune to hacking attempts and malicious attacks.

Hackers don't discriminate when it comes to their victims. So, don't let the size of your business, determine how valuable your data is or how secure your assets are.

Myth 4 — Anti-Virus or Anti-Malware Software is enough to secure my business

The anti-virus software is an essential part of your cybersecurity plan. However, it only secures one entry point into your system. Hackers have many ways to bypass anti-virus software and infiltrate networks with attacks such as targeted phishing attacks, and ransomware.

So, even with anti-malware software in place, hackers will have plenty of room to launch an attack.

Truth: Anti-virus software can only protect you from a unique set of recognized cyber threats, not from other emerging cyber threats.

As a business, you need to do much more to secure your data from hackers. Deploy an all-encompassing security solution like a Web Application Firewall that monitors threats continuously and provides end-to-end, 24*7 protection from cyber risks.

Myth 5 — Cybersecurity is too expensive

Even as malicious cyberattacks continue to make headlines and cost businesses millions, companies still wonder if cybersecurity investments are worth it. Data security is frequently overlooked and is only an afterthought for many enterprises. The average cost of a data breach in 2021 is $4.24 million, the highest in the last 17 years. And this figure does not include the damage that comes with the crippling reputational losses and customer losses from a breach.

Truth: The cost of a good cybersecurity solution is nothing compared to the cost of a successful attack.

Invest in a modern security solution like Indusface AppTrana**,** for example, that can protect you from the latest threats. Moreover, there are many precautionary measures that you can take with absolutely no additional cost to your business, such as strong passwords, multi-factor authentication, access management, and employee training.

Myth 6 — You don't require cybersecurity because you've never been attacked

If you've never experienced a cyberattack or data breach yourself, the chances are that you don't know just how much damage they can cause. You may also assume that your current security posture is strong enough to keep the bad actors away since you've never been attacked.

However, cyber threats and hacking tools are continuously evolving to become more and more sophisticated and undetectable each day. And any sensitive data is a potential target for a breach.

Truth: You could easily be the next target.

Develop a sound security strategy that helps you identify existing weaknesses and mitigate attack attempts before any significant damage is caused.

Myth 7 — You've achieved total cybersecurity

Cybersecurity is a continuous process that needs to be upgraded with the changes in the threat landscape. Therefore, never stop working on securing your IT assets. Your organization will always be susceptible to existing and emerging threats.

Truth: There is no such thing as total or perfect cybersecurity against cyberattacks.

Recent cyber attacks

Most Recent Cyber Attacks - Past Three Months

Under normal business circumstances, cyber attacks are an ever-increasing problem causing trillions of dollars in losses. To make matters worse, the war between Russia and Ukraine exacerbated these problems with a flurry of major politically-motivated cyber attacks in 2022. Here are some of the recent cyber attacks.

Hot Topic Attacks

In August 2023, American retailer Hot Topic notified its customers they had detected automated attempts by unauthorized third parties to log into customer accounts on both their website and their mobile app. The attack involved "valid account credentials (e.g., email addresses and passwords) obtained from an unknown third-party source."

Prospect Medical Holdings Ransomware Attack

In August 2023, more than one medical offices, facilities, and hospitals were forced offline by a ransomware attack. The company closed a few of its outpatient facilities and informed patients and families of the attack via its Facebook pages and websites. News organizations following the story reported that medical staff switched to manual information procedures while the network was offline.

Cyber Attacks in 2022

Finish Parliament Attack

In August 2022, the Finnish parliament's website experienced a DDoS attack while the parliament was in session. This denial-of-service attack may be part of a coordinated campaign by Russian state-sponsored hackers to disrupt the Finnish government's websites in retaliation for the application to join NATO. A DDoS attack temporarily blocks access to a website but does not cause permanent destruction.

Ukrainian State Nuclear Power Company Attack

The Russian “hacktivist” group called the People’s Cyber Army engaged 7.25 million bots in August 2022 in a bot attack to take the Energoatom website down. It used a flood of garbage web traffic and webpage requests. A disruption of online services lasted for a few hours, but no permanent negative impact remained. The attack was part of a Russian psyops campaign to create fear of a nuclear disaster and terrorize Europeans.

Greek Natural Gas Distributor Attack

Greek national gas distributor DESFA reported an incidence of a cyber attack in August 2022. The attack impacted part of the company’s IT infrastructure and caused a data leak. The ransomware operation of cybercriminals called Ragnar Locker is holding the stolen data hostage. They demand ransom not to expose sensitive data. The company refused to make a payment.

South Staffordshire Water Company Attack

In August 2022, the South Staffordshire Water Company reported an attack that caused a network disruption in its internal corporate network and a data loss. A cybercriminal ransomware group threatened to tamper with the water supplied by the company. The company disputed this claim. The criminals demanded payment to not release sensitive files and explain how the network breach happened.

Montenegro Government Attack

The government of Montenegro's digital IT infrastructure reported an unprecedented cyberattack in August 2022. No data breach occurred. However, certain governmental services and telecommunications experienced disruption, including border crossings and airport operations. The state-owned utility company, EPCG, switched to manual operations as a precautionary measure.

Estonian Government Attack

A DDoS attack disrupted many Estonian government websites for several hours in April 2022. The attack targeted websites for the president, the Ministry of Foreign Affairs, the Police and Border Guard, the identification card webpage, and the state services digital portal. Estonia’s condemnation of the Russian war on Ukraine makes the country a target for Russian hackers.

Islamic Culture and Communication Organization Attack

The Iranian Islamic Culture and Communication Organization (ICCO) experienced a severe attack in July 2022. Six ICCO websites went down, and 15 others changed to photos of Massoud Rajaivi, the Iranian Resistance leader. Additionally, there was data destruction on 44 servers and hundreds of computers. The ICCO also lost 35 databases with highly-confidential information about money laundering, spies, and terrorists living abroad.

Belgian Government and Military Attack

In July 2022, the Belgian government announced that three Chinese hacker groups, part of the known Chinese Advanced Persistent Threat actors, attacked Belgian public services and military defense forces. The Chinese government-sponsored attackers steal trade secrets and intelligence information. The Soft Cell Chinese group recently launched a new remote access trojan (RAT) malware in June 2022.

UK Military Social Media Breach

Hackers took over the Twitter account of the British Army in July 2022. The social media account underwent multiple name and photo changes. The content started promoting contests to win Angry Apes non-fungible tokens (NFTs), digital art stored on a blockchain. The army's YouTube page experienced an attack as well. Its name changed to Ark Invest, and the account promoted interviews of Elon Musk talking about cryptocurrency.

Lithuanian Energy Company Attack

A DDoS attack in July 2022 blocked access to the website of the Lithuanian energy company, Ignitis Group. The company managed the attack and limited the damage using DDoS Protection. No data breach occurred, but the attacks were persistent and ongoing. Pro-Russia group Killnet claimed responsibility. The attack retaliated against Lithuanian support of Ukraine in the war with Russia.

Generic Conclusion about Attacks

In conclusion, cyber-attacks continue to pose significant threats to individuals, businesses, and governments globally. These attacks exploit vulnerabilities in various systems, applications, and human behaviors to compromise data, disrupt operations, and cause financial and reputational damage. The evolving nature of cyber threats requires a proactive and multifaceted approach to cybersecurity. Here are some key takeaways:

Persistent Threat Landscape:

The cyber threat landscape is dynamic and persistent. Attackers continually adapt their techniques, making it essential for individuals and organizations to remain vigilant and stay updated on the latest threats and security measures.

Diverse Range of Attacks:

Cyber-attacks come in various forms, including malware, phishing, ransomware, supply chain attacks, and more. Attackers exploit vulnerabilities in software, hardware, and human behavior, underscoring the need for a holistic cybersecurity strategy.

Impact on Individuals and Organizations:

Cyber-attacks can have far-reaching consequences, affecting individuals through identity theft, financial loss, or privacy breaches. For organizations, the impact can be severe, leading to financial losses, reputational damage, operational disruptions, and legal ramifications.

Importance of Preparedness:

Preparedness is key to mitigating cyber risks. This involves implementing robust cybersecurity measures, conducting regular security assessments, staying informed about emerging threats, educating users, and having an incident response plan in place.

Collaborative Approach:

Cybersecurity is a shared responsibility that necessitates collaboration between individuals, organizations, governments, and cybersecurity professionals. Sharing threat intelligence, best practices, and working collectively to enhance cybersecurity infrastructure is vital for a more secure digital environment.

Continuous Learning and Adaptation:

Cybersecurity is an evolving field. Staying current with advancements in technology, threat landscapes, and security practices is crucial. Ongoing education and training are essential for individuals and professionals to adapt and respond effectively to emerging threats.

Regulatory Compliance and Standards:

Compliance with cybersecurity regulations and industry standards is important for organizations to maintain the trust of their stakeholders. Adhering to frameworks like GDPR, HIPAA, or ISO 27001 can help establish a solid foundation for robust cybersecurity practices.

Investment in Security Measures:

Allocating resources for cybersecurity investments, including advanced security solutions, employee training, and regular system updates, is a wise business decision. Proactive investments in cybersecurity can help prevent attacks and reduce potential damages.

User Awareness and Education:

Users are often the first line of defense against cyber-attacks. Educating individuals about cybersecurity best practices, how to identify phishing attempts, and promoting a culture of security consciousness can significantly enhance overall cybersecurity posture.

In this constantly evolving digital landscape, being proactive, adaptable, and informed is essential to effectively navigate and mitigate the risks associated with cyber-attacks.

Why and What is Cyber Security?

What is Cybersecurity?

Definition and Scope:

Cybersecurity involves the implementation of measures, practices, and technologies to protect digital assets, systems, networks, and data from cyber threats. These threats can range from malware, phishing, and ransomware to insider threats and more.

Components of Cybersecurity:

Cybersecurity comprises several components, including network security, endpoint security, application security, data security, identity and access management, cloud security, and security awareness training.

Principles and Objectives:

The main principles of cybersecurity include confidentiality, ensuring that only authorized users can access data; integrity, maintaining data accuracy and consistency and availability, ensuring that data and systems are accessible when needed.

Importance of Cyber Hygiene:

Practicing good cyber hygiene, which involves regularly updating software, using strong passwords, employing multi-factor authentication, and being cautious of suspicious emails or links, is fundamental to effective cybersecurity. It minimizes vulnerabilities and enhances overall protection.

Why is Cybersecurity Important?

Protection of Sensitive Data:

Cybersecurity is essential to safeguard sensitive and confidential information, such as personal data, financial records, intellectual property, and trade secrets. Unauthorized access or theft of this data can lead to severe financial and reputational damage.

Prevention of Financial Loss:

Effective cybersecurity measures help prevent financial losses that can result from cyber-attacks, including fraud, ransomware, identity theft, and unauthorized transactions. This protection is crucial for individuals and organizations alike.

Ensuring Business Continuity:

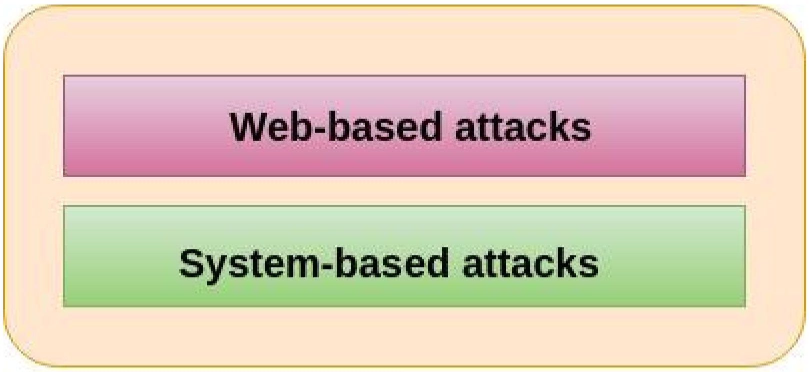
Cybersecurity ensures the continuous operation of businesses and organizations by preventing disruptions caused by cyber-attacks. Uninterrupted operations are vital for maintaining customer trust and sustaining revenue streams.

Categories of Attack

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

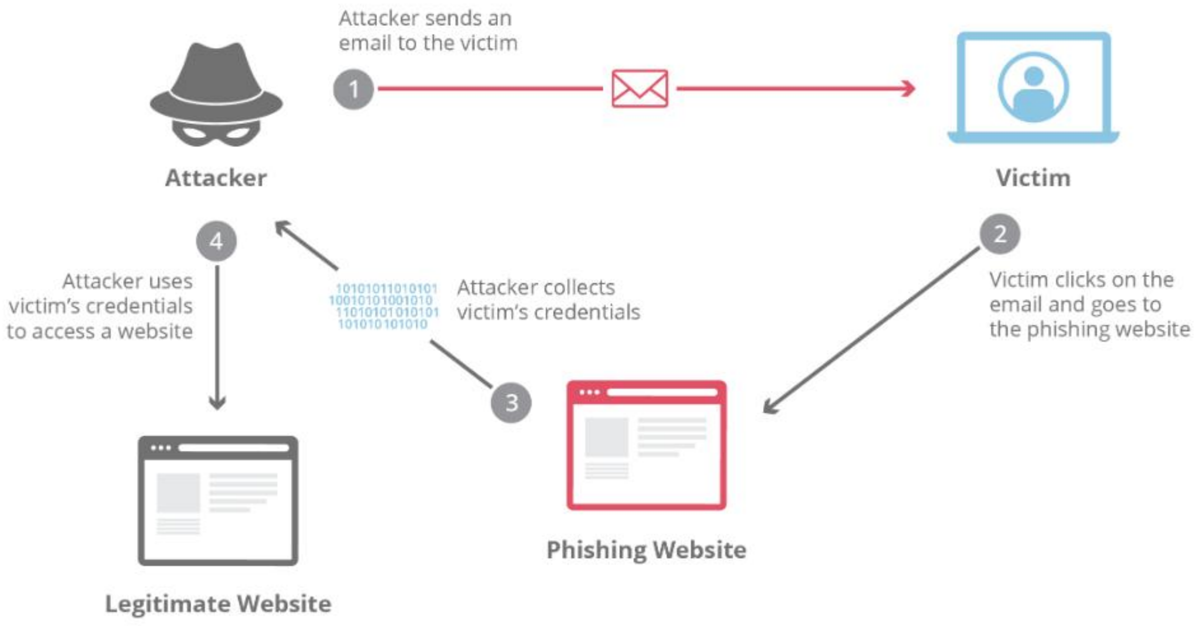
DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
4
Attacker uses victim's credentials to access a website
Legitimate Website
Phishing Website

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

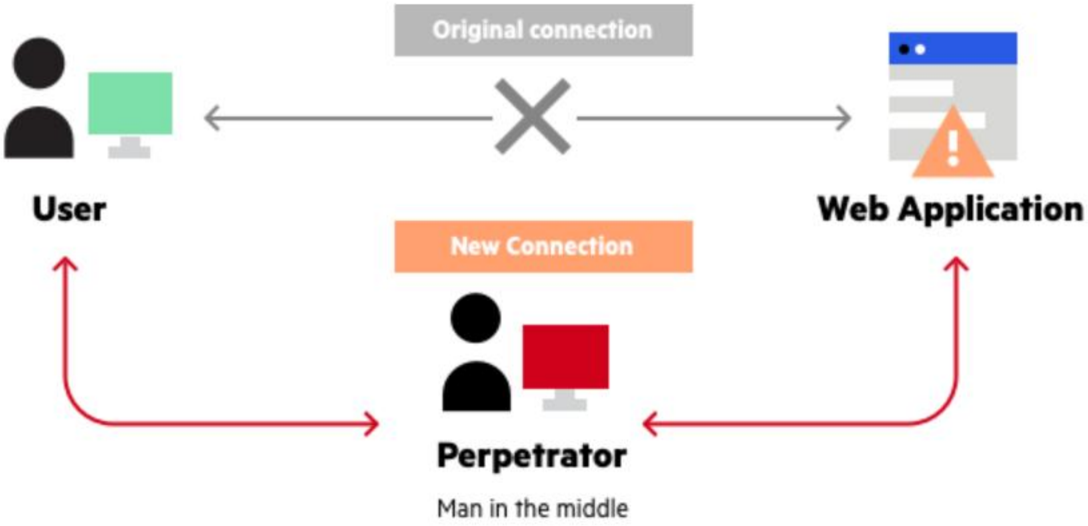
It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.



System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.