MODULE 1

LAYERED PROTOCOL MODEL (OSI), PROTOCOL LAYERS, NETWORK SECURITY AND ATTACK

COURSE CODE: 10ABTEC22113

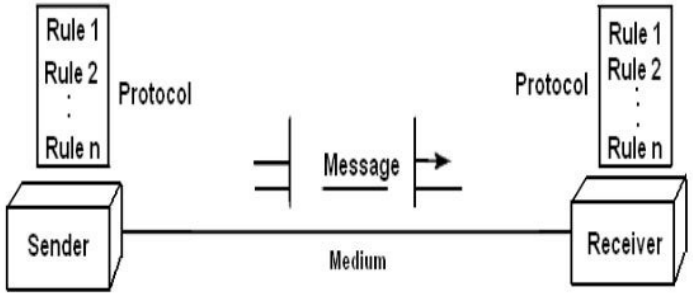
COURSE NAME: DATA COMMUNICATIONS

BASIC COMPONENTS

Basic components of data communication

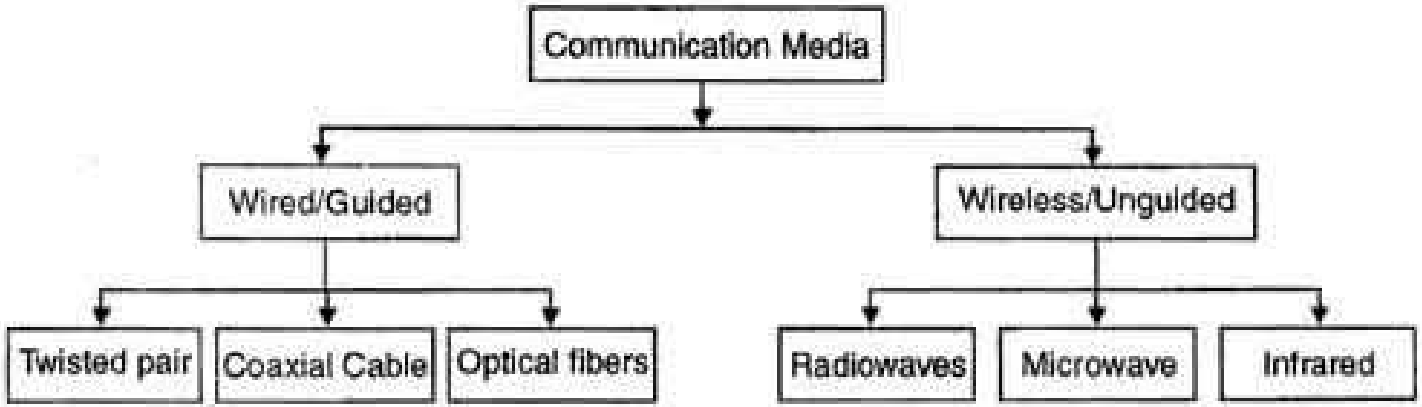
- Sender
- Receiver
- Information/data/message
- Transmission medium
- Protocol

Block Diagram



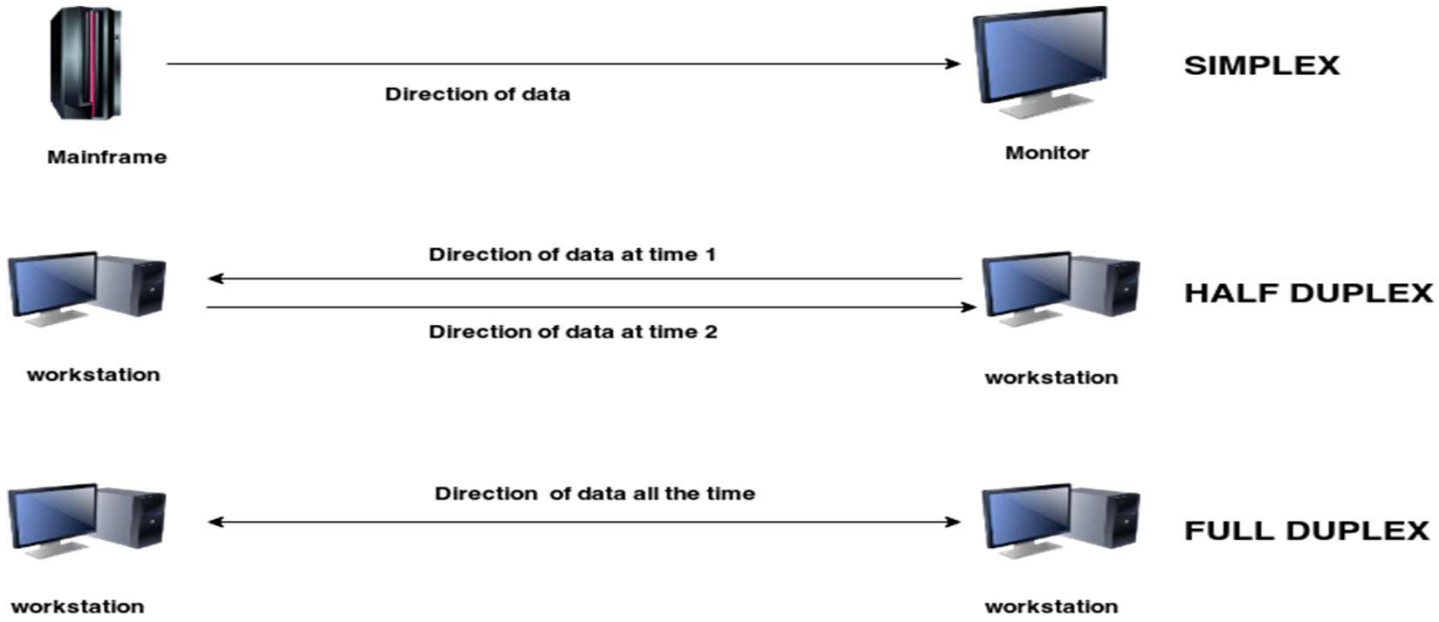
TYPES OF COMMUNICATION MEDIUM

Classification of transmission medium:



TYPES OF CONNECTIVITY

Types of connectivity/ Types of data flow



Types of connectivity/ Types of data flow

- ***There are three types of connectivity.***

1. ***Simplex:***
   - ***It will provide only one way communication.Example. Television and radio.***
-

1. ***Half Duplex:***
   - ***It will provide two way communication but not simultaneously.Example. Walkie-talkie.***
-

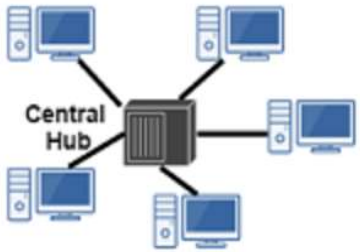
1. ***Full Duplex:***
   - ***It will provide two way communication simultaneously.Example. Mobile.***

TOPOLOGIES

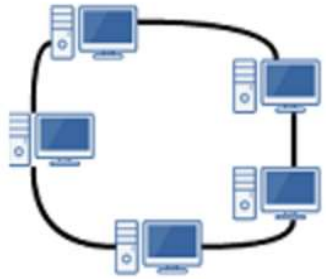
Topologies

- Star
- Bus
- Mesh
- Ring
- Hybrid

Bus

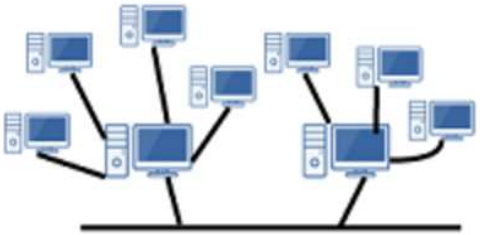


Star



Ring

Mesh



Tree

Point-to-Point

TOPOLOGIES

Topology (Infrastructure of the network)

It will show how the devices and system are been connected to each other is called as topology.

Network topology is always explained how many topologies has been maintain in the network.

There are five types of topologies.

1. ***Bus Topology.***
2. ***Ring Topology.***
3. ***Mesh Topology.***
4. ***Star Topology.***
5. ***Hybrid or Tree Topology***

TOPOLOGIES

1. ***Bus Topology:***

   This topology is very old, all the system have been connected through a cable called as backbone cable. This backbone cable must ends with terminators.

   If backbone cable is cut off, network will be down

2. Ring Topology:

This topology is used to connect only servers together. It is not used in the local area network. All the servers have been connected either in clockwise or anticlockwise direction to form a ring. Fiber optics cable is used in this topology. Topology is very expensive. Here one link is cutoff then entire network will be down

3. Mesh Topology:

All the system are been connected to each other with separate cables. This topology is suitable for very small network which consist of not more than three system in the network. Troubleshooting is very difficult and topology is not clean

4. Star Topology:

All the system and devices are connected together through cables. All the system and devices connected to a centralized device called as Ethernet hub

5. Hybrid or Tree Topology:

Tree Topology: - It is combination of bus and star topology.

Hybrid Topology: - It is the combination of star topology.

Bus Topology

Advantages of Bus Topology

1.It is easy to set up, handle, and implement.
2.It is best-suited for small networks.
3.It costs very less.

Disadvantages of Bus Topology

1.The cable length is limited. This limits the number of network nodes that can be connected.
2.This network topology can perform well only for a limited number of nodes.

Ring Topology

Advantages of Ring Topology

1.The data being transmitted between two nodes passes through all the intermediate nodes. A central server is not required for the management of this topology.
2.The traffic is unidirectional and the data transmission is high-speed.
3. It is less costly than a star topology.

Disadvantages of Ring Topology

1.The failure of a single node in the network can cause the entire network to fail.
2.The movement or changes made to network nodes affect the entire network's performance.

Mesh Topology

Advantages of Mesh Topology

1.The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.
2.The failure of a single node does not cause the entire network to fail as there are alternate paths for data transmission.
3.It can handle heavy traffic

Disadvantages of Mesh Topology

1.The arrangement wherein every network node is connected to every other node of the network, many connections serve no major purpose. This leads to redundancy of many network connections.
2.A lot of cabling is required. Thus, the costs incurred in setup and maintenance are high.
3.Owing to its complexity, the administration of a mesh network is difficult.

- **Advantages of Star Topology**

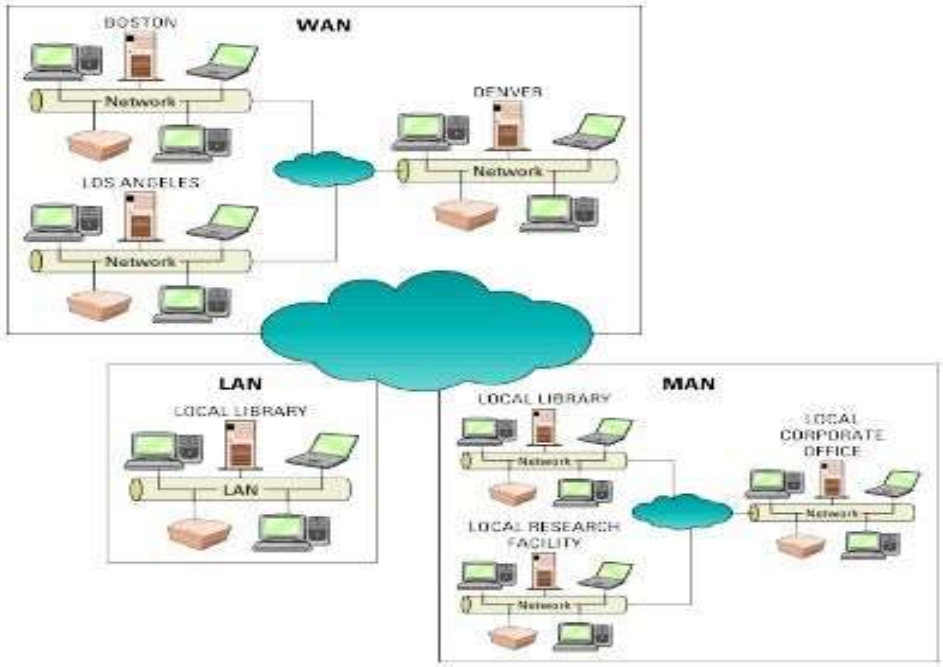
1. Due to its centralized nature, the topology offers simplicity of operation.
2. It also achieves isolation of each device in the network.
3. Adding or removing network nodes is easy, and can be done without affecting the entire network.
4. Due to the centralized nature, it is easy to detect faults in the network devices.
5. As the analysis of traffic is easy, the topology poses lesser security risk.
6. Data packets do not have to pass through many nodes, like in the case of a ring network. Thus, with the use of a high-capacity central hub, traffic load can be handled at fairly decent speeds.

- **Disadvantages of Star Topology**

1. Network operation depends on the functioning of the central hub. Hence, central hub failure leads to failure of the entire network.
2. Also, the number of nodes that can be added, depends on the capacity of the central hub.
3. The setup cost is quite high.

NETWORK TYPES

- ***The three types of networks include***:
  1. Local area network (LAN)
  3. Metropolitan area network (MAN)
  5. Wide area network (WAN)



NETWORK TYPES

- ***There are THREE classes.***

<u>LAN: Local Area Network</u>

- ***it is also called as intranet. The distance between to one PC and another PC must be equal to 1.25 miles.***

<u>MAN: Metropolitan Area Network</u>

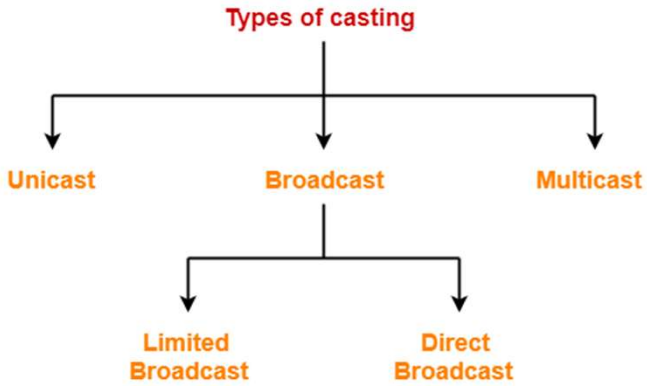
- ***it is called as the network in country. It is used to connect metropolitans (Delhi, Mumbai, Chennai, and Kolkata) in a country. Distance between two computers is about 10 miles.***
-

<u>WAN: Wide Area Network</u>

- ***it is use to connect country to country or continent to continent or around the globe.***

TYPES OF CASTING

Casting - transmitting the data in the form of packets over the internet is called casting.



- ***Casting will provide both audio and video signal. There are three types ofcasting.***

Unicast:

- ***Sending message from one to one. Example. SMS.***

Multicast:

- ***Sending message to groups or sending message from one to many or manyto one or many to many.***
- ***Example. Group SMS.***

Broadcast:

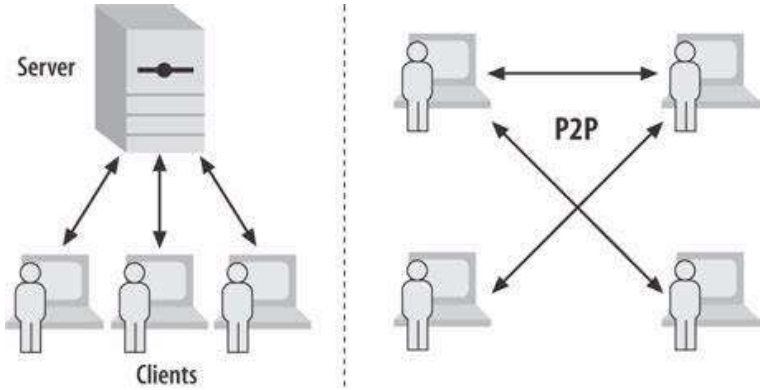
- ***sending message from one to all. Example. Common message.***

TYPES OF NETWORK ARCHITECTURE

1. ***Peer-to-peer Network:***
   a. *All the workgroup mission has been connected together.*
   b. *There is no centralized administration.*
   c. *Users are called as local user.*
   d. *Users cannot control through group policy.*
   e. *Security is low.*
   Example. Internet browsing center.
1. ***Server-Client Network:***
   a. *It consists of server and client together.*
   b. *There is centralized administration.*
   c. *Users are called as domain user.*
   d. *Users can control through group policy.*
   e. *Security is high.*
   Example. Company network.

Types of Network Architecture

- Peer to peer network
- Client – Server networks



- Network Edge

The **network edge** refers to the area where a device or local network interfaces with the internet. The network edge refers to endpoints. It is the first step between endpoints and the core of the network.

Some of the edge devices are Hub, Switch, Router, Firewall, Bridge, Modem

- Network Core

The network core is the actual service provider and connected to the used with the help of edge devices.

Eg. servers

10ABTEC22113: DATA COMMUNICATIONS

MODULE 1

DELAY, LOSS AND THROUPUT

DELAY

When the expected data does not arrive on the receiver end at a desired time, the packet is said to be in delay. Based on the purpose of delay, the delay is classified into

1. Processing delay
2. Queueing delay
3. Transmission delay
4. Propagation delay

TYPES OF DELAY

1. **Processing Delay**
   - The time required to examine the packet's header and determine where to direct the packet is part of the **processing delay**.
   - The processing delay can also include other facts, such as the time needed to check for bit-level errors in the packet.
   - A Processing delays in high-speed routers are typically on the order of microseconds or less.
2. **Queuing Delay**
   - At the queue, the packet experiences a queuing delay as it waits to be transmitted onto the link.
   - The length of the queuing delay of a specific packet will depend on the number of earlier-arriving packets that are queued and waiting for transmission onto the link.
   - If the queue is empty and no other packet is currently being transmitted, then our packet's queuing delay will be zero.
   - On the other hand, if the traffic is heavy and many other packets are also waiting to be transmitted, the queuing delay will be long.
   - Queuing delays can be on the order of microseconds to milliseconds in practice.
3. **Transmission Delay**
   - Assuming that packets are transmitted in a first-come first-serve manner, our packet can be transmitted only after all the packets that have arrive before it have been transmitted.
   - Denote the length of the packet by L bits, and denote the transmission rate of the link from router A to router B by R bits/sec.
   - For example, for a 10 Mbps Ethernet link, the rate R = 100 Mbps.
   - Transmission delay = L/R
   - This is the amount of time required to push (that is, transmit) all of the packet's bits into the link. Transmission delays are typically on the order of microseconds to milliseconds in practice.

4. **Propagation Delay**

- Once a bit is pushed into the link, it needs to propagate to router B. The time required to propagate from the beginning of the link to router B is the **propagation delay**.
- The bit propagates at the propagation speed of the link.
- The propagation speed depends on the physical medium of the link.
- The propagation delay is the distance between two routers divided by the propagation speed. T
  Propagation delay = *d/s*,
  where *d* is the distance between router A and router B and *s* is the propagation speed of the link.
- In wide-area networks, propagation delays are on the order of milliseconds.

Packet Loss

Basically this means that when sending a lot of packets in to a queue at a high rate (or at the same time), packet loss will be experienced as the queue will be m*axed out* and the router will drop packets. A lost packet can be retransmitted on an end-to-end basis in order to ensure that all data are eventually transferred from source to destination.

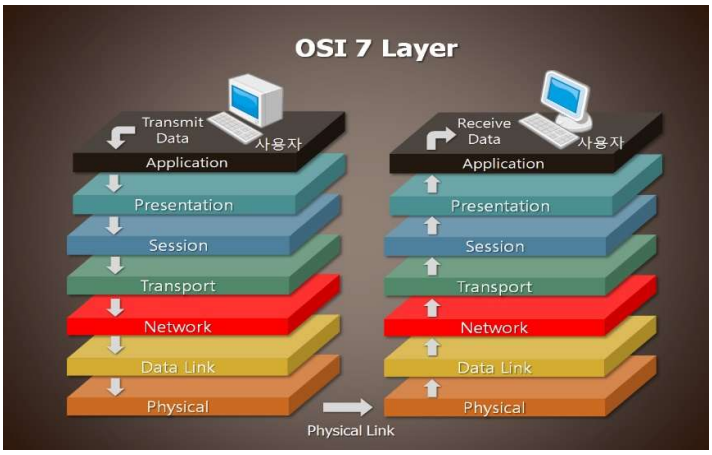
Throughput in Computer Networks

Imagine a large file being sent from *Host A* to *Host B* across a computer network.
The instantaneous throughput at any instant of time is the rate (in bits/sec) at which *Host B* is receiving the file.

The average throughput of the file is $\frac{F}{T}$ bits/sec, where the file consists of F bits and the transfer time is T (in seconds).

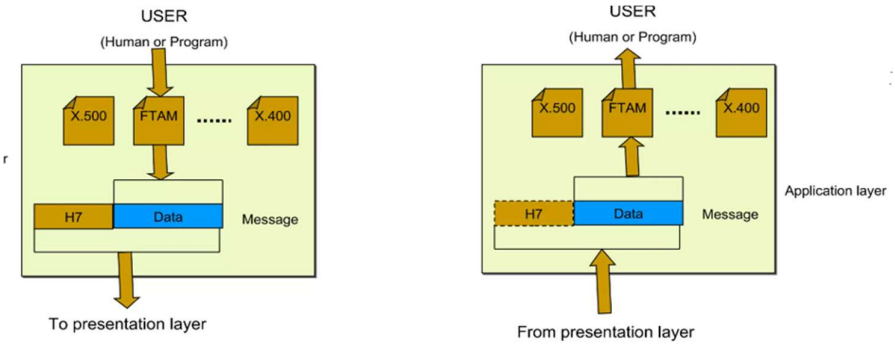
(OSI) Layered Network Model

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.



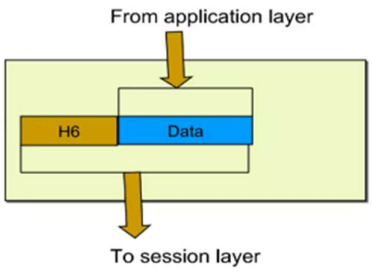
Application (Layer 7)

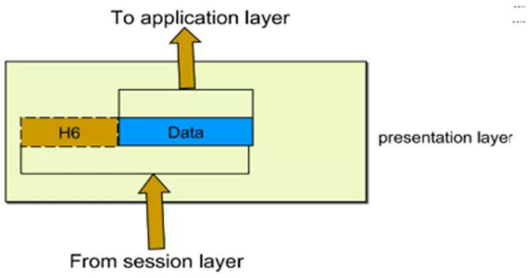
This layer supports application and end-user processes. This layer provides application services for file transfers, e-mail, and other network software services. HTTP, E-Mail and FTP are applications that exist entirely in the application level.



Presentation (Layer 6)

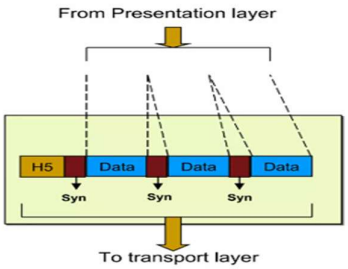
This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. It is sometimes called the syntax layer.

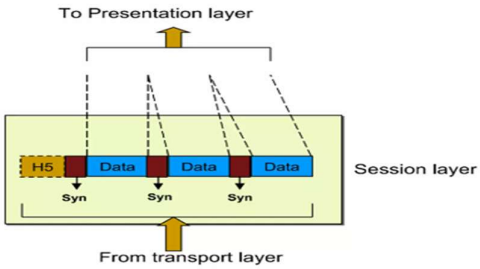




Session (Layer 5)

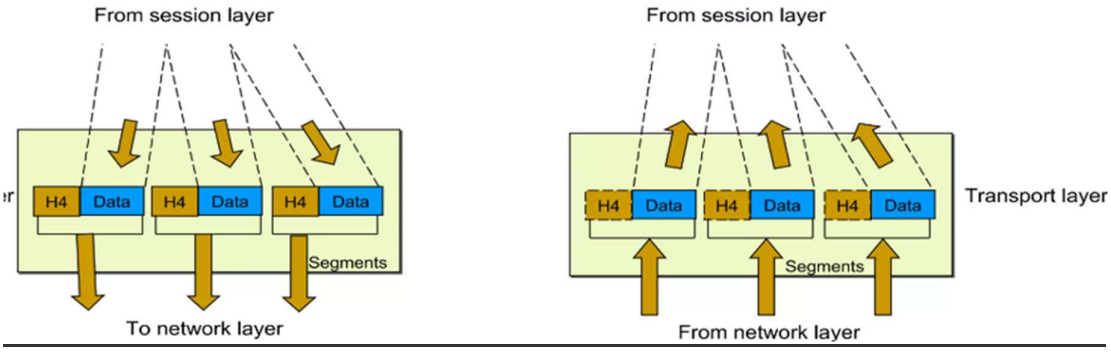
This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.





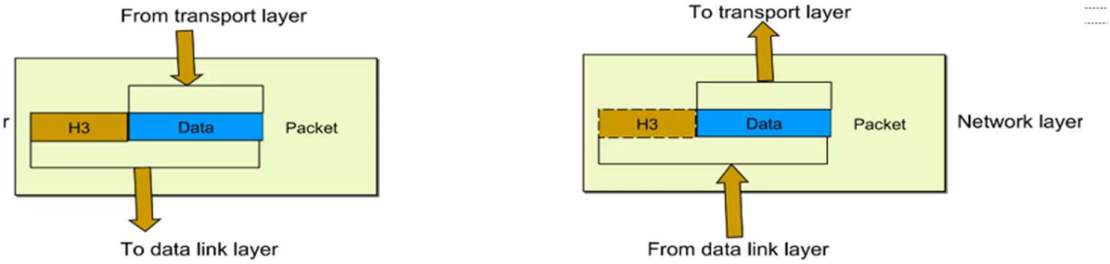
Transport (Layer 4)

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer. The two main protocols used in transport layer is TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Data is called as segments in transport layer.



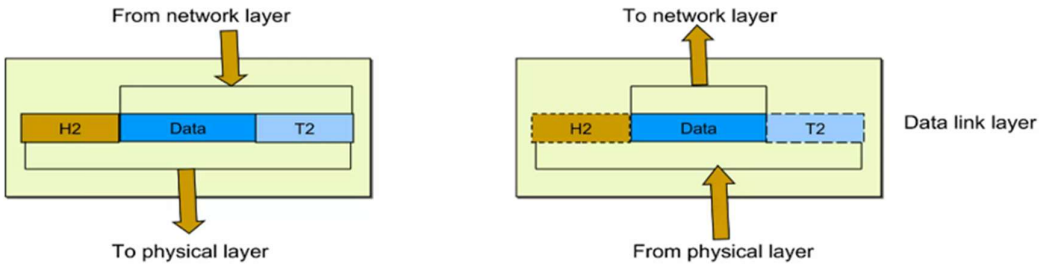
Network (Layer 3)

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing. Data is called as packets/ datagram.



Data Link (Layer 2)

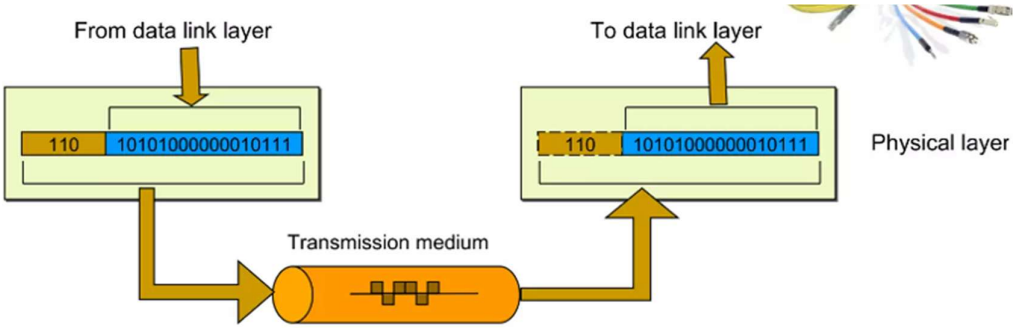
At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. Data is called as frames.



Physical (Layer 1)

This layer conveys the bit stream into electrical impulse, light or radio signal. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards

and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components



NETWORK ATTACK AND NETWORK SECURITY

The Open Systems Interconnection (OSI) security architecture provides a systematic framework for defining security attacks, mechanisms, and services.

NETWORK SECURITY

Network and Internet security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information.

A security mechanism is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols.

Security services include access control, data confidentiality, data integrity, availability and authentication.

- Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
- Confidentiality: This term covers two related concepts:
  - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- Integrity: This term covers two related concepts:
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- Availability: Assures that systems work promptly and service is not denied to authorized users.
- Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
  - Peer Entity Authentication: Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - Data-Origin Authentication: In a connectionless transfer, provides assurance that the source of received data is as claimed.
- Nonrepudiation: Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message.

The Challenges of Computer Security

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

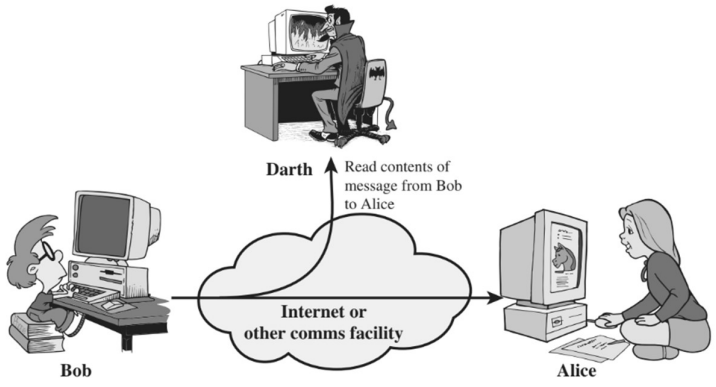
Security attacks are classified as

1. passive attacks, which include unauthorized reading of a message of file and traffic analysis
2. active attacks, such as modification of messages or files, and denial of service (DoS).

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

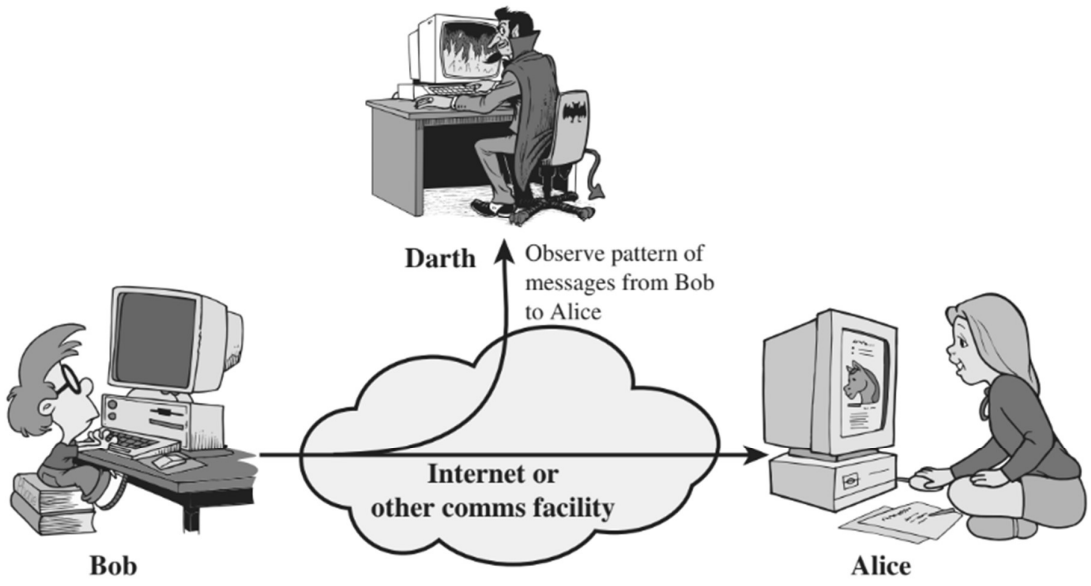
1. The release of message contents is easily understood (Figure a).
   We had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption.



(a) Release of message contents

2. A second type of passive attack, traffic analysis in (Figure b).

If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



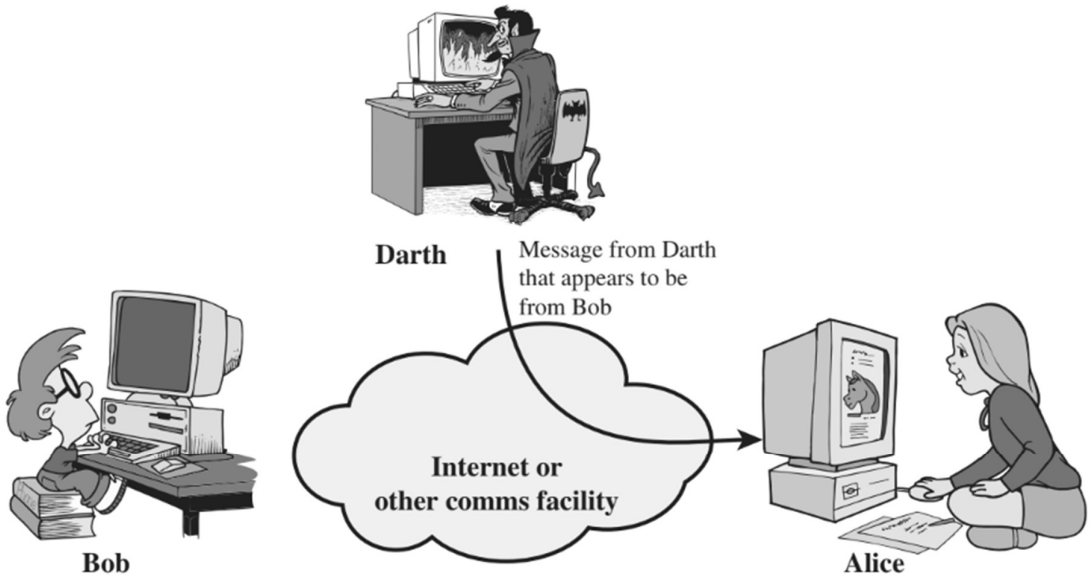
(b) Traffic analysis

Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks

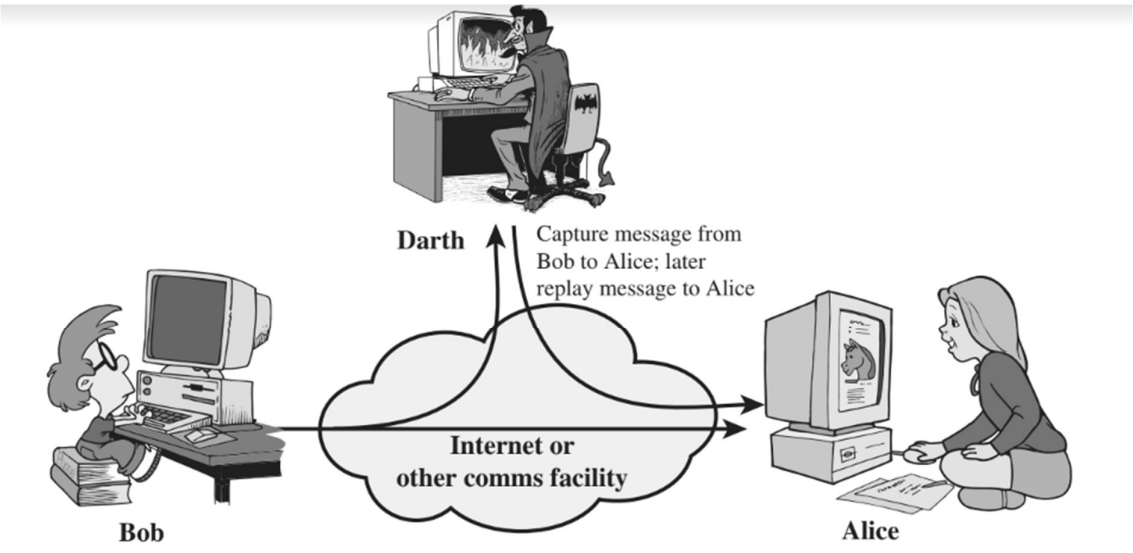
Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

1. A ***masquerade*** takes place when one entity pretends to be a different entity (Figure a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



(a) Masquerade

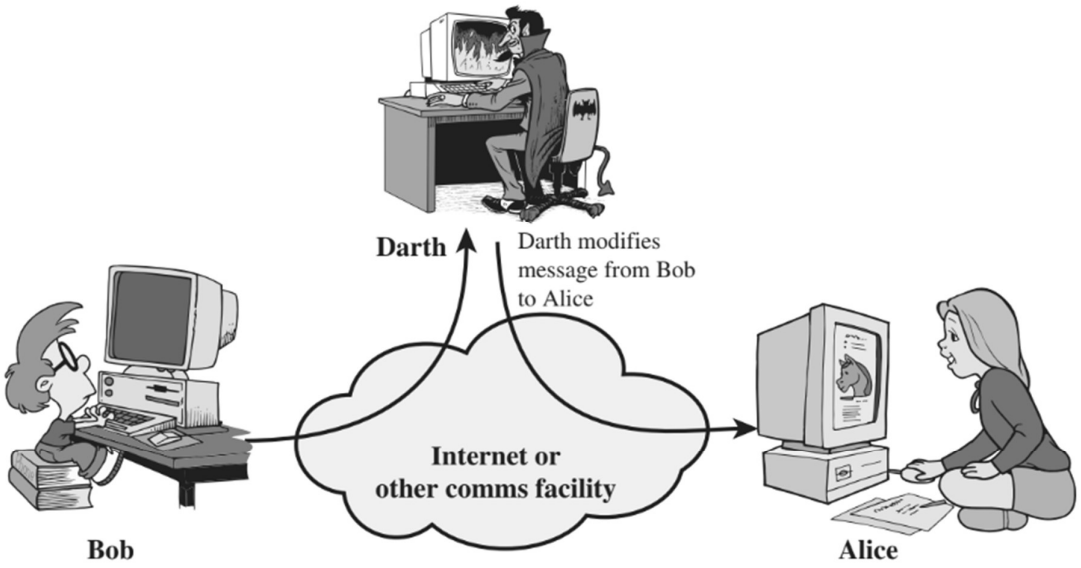
2. ***Replay*** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure b).



(b) Replay

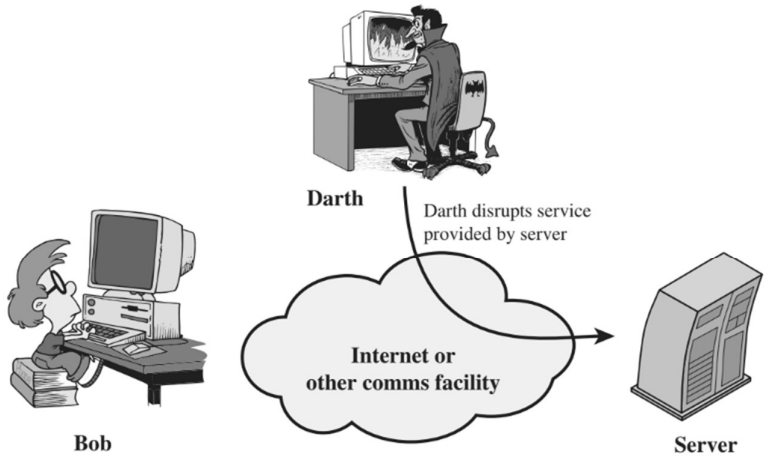
3. ***Modification*** of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect

(Figure c). For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”



(c) Modification of messages

4. The ***denial of service*** prevents or inhibits the normal use or management of communications facilities (Figure 1.3d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination



(d) Denial of service