Unit 1 (Introduction to Networks)

Computer network definition

1:Communication is a process in which two or more computers or other devices transfer's data and instructions, share information and resources.
2: A group of two of more computers that shares services and interacting in some manner is known as Computer Network. This interaction is, accomplished through a shared communication link, with the shared components being data.
3: A network is a collection of machines those are linked both physically and through software components to facilitate communication and the sharing of information.
4: A network is a set of devices often mentioned as nodes connected by media link.
5: A node can be a device which is able to send or receive data generated by other nodes on the network, for e.g. a computer, printer etc. These links connecting the devices are called Communication channels.

Need of computer network

The following are the potential needs and benefits of a computer network:

File Sharing

Networking helps the network users to share data files.

Computers connected to a network share files and documents with each other.

Personal computers connected to a business network can select to which files and folders should be made available to be shared in the network.

Information Sharing:

Computers connected to a network are capable of sharing and exchanging data and information between different individual users, it is necessary to interconnect the individual users' computers.

Resource Sharing :

When computers are interconnected, users connected to the network can share the expensive resources like a laser printer, bulk storage, and large enterprise software.

Sharing Media:

In computer network sharing media is very easy.

Similar to file sharing, computers are capable of streaming music, videos and movies from one computer to another.

Applications of computer network

1: Computer network applications are software applications those utilize Internet or other network hardware infrastructure to execute important functions like file transfer within a network. It helps to transfer data from one point to another within a network.

2: There are two types of network applications:-

a: Pure Network Applications: These applications are developed only to use in networks. These applications help in the transfer of data and to communicate within a network. These applications have a separate and distinct user interface.

b: Stand Alone Applications: These are the applications those run on standalone computers. To enhance their activity, these programs are rebuilding to run on network environments. For e.g. word processors, database management systems,spreadsheets,graphicspresentations, project management etc. They function even when the computer is offline.

Difference

A pure network application is designed to operate primarily over a network and depends on network services to function. These types of applications typically require a network connection and rely on the network to transfer data, communicate with other applications, and perform other network-related tasks. On the other hand, a standalone application is designed to operate independently of a network connection and can function without the need for network services. These types of applications are installed on a local machine and can perform their tasks without the need for a network connection.

Components of computer network

Textbook

Network benefits

Sharing Information (File Sharing, E-mail):Networks allow users to share

information in various ways. The most conventionalway of sharing information is

to share specificfiles. For example, many people can work together on a single document like spreadsheet file or word-processing.

Sharing Resources (Printer Sharing, Application Services):Certain computer resources, such as printers or hard drives, can be set up so that network users can share them. Sharing these resources can result in significant cost savings.

Facilitating Centralized Management: One of the most common reasons for

networking in many businesses is so that several users can work together on a single business application. For example, an accounting department may have accounting software that can be used from several computers at the same time, or a sales handling division may have an order application which runs on different computers to manage large volume of orders.

Managing software: Using the network helped in reduction of software costs.

It happens when all users on a network used the same software and when software is bought in bulk quantities gets a discount.

Maintaining the Network: Purchasing similar equipment for use on the network means that network maintenance costs are reduced because there are fewer dissimilar components.

Backing up data: If a hardware or software failure causes information or applications lost, vital information and necessary applications can be restored with the help of existing backup.

Peer-to-Peer Network

1: Peer-to-peer networks have no centralized control.

2: All computers on a peer-to-peer network can be considered equals.

3: Each computer controls its own information and is capable of functioning as either a client or a server depending on which is needed at the time.

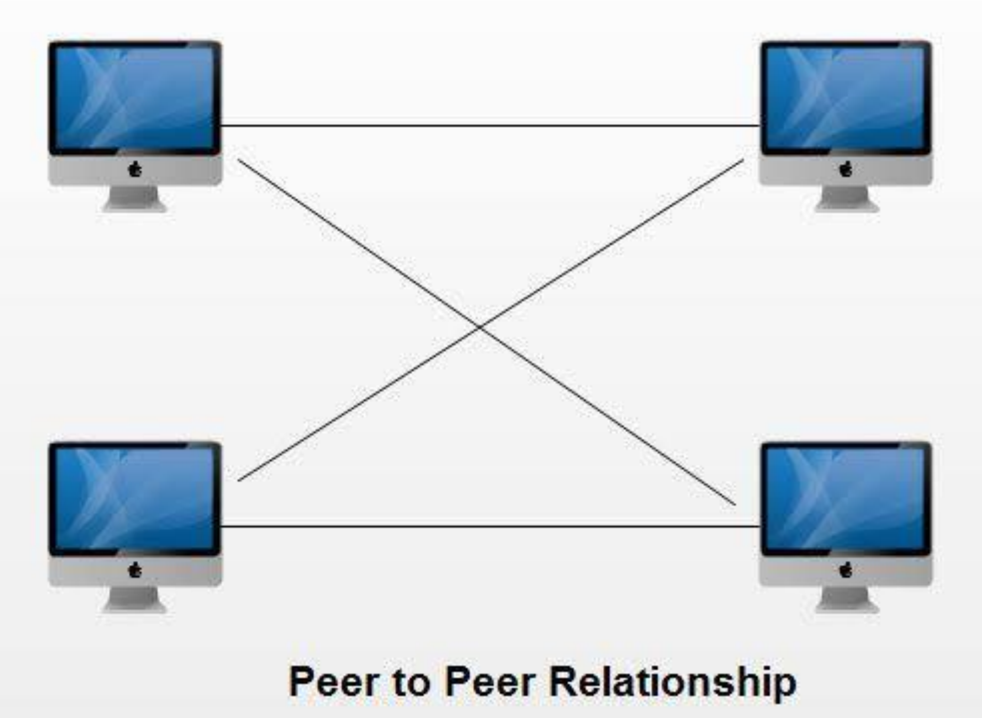
4: Peer-to-peer networks are very popular since they are inexpensive and easy to

install are used inhome networks and in small companies.

5: Many operating systems comes with built in peer-to-peer networking capability.

6: While peer-to-peer networks are inexpensive to set up, they are extremely limited in scope. The maximum number of peers that can be accepted to operate on a

peer-to-peer network is ten. They are, therefore, not appropriate for larger, more secure networks.



Server-Based Network

1: A server-based network provides centralized control and is created for secure operations.

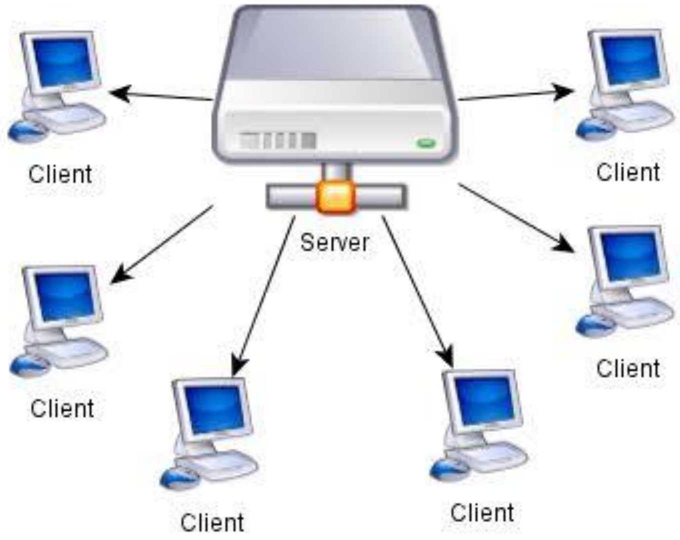
2: Although there are both clients and servers on a server-based network, network is controlled by a dedicated server.

3: In a server-based network,a dedicated server serves its network clients

by storing data, applications, and other resources, and then provides access to those resources when called for by a client.

4: Dedicated servers can also control the entire network‘s security from one central location or share that control with other specially configured servers.

5: Server-based networks are often used in businesses and organizations, where security and centralized management of resources are important.



Types of servers

Application server

1: An application server is a type of server that is designed to host and run specific application software.

2: This software is typically designed to provide a specific set of services or functions, such as web services, database management, or business logic processing.

3: They are generally built to support multiple platforms and programming languages, thus providing a common platform for different applications.

4: Application servers can also provide additional services like load balancing, security, caching, messaging, and others that the application can use.

5: Many application servers are platform-agnostic, meaning they can run on different operating systems and hardware platforms.

Email server

1: An email server is a software or hardware system that manages the sending, receiving, and storage of electronic messages.

2: Email servers can be used to manage the flow of email within an organization, as well as for sending and receiving messages from external sources.

3: Email servers can also include additional features such as spam filtering, virus scanning, and encryption to protect against security threats.

4: Some common email server software include Microsoft Exchange, Postfix, and Sendmail.

File server

1: A file server is a dedicated computer having central storage and

management of data files.

2: It typically includes a variety of services such as file sharing, storage, and backup.

3: File servers can be integrated with other systems such as email servers, database servers, and web servers to provide additional functionality.

4: They can also provide web-based access to files, allowing users to access their files from any device with a web browser.

5: With the implementation of Cloud technology, file servers can also be replaced by cloud-based file storage services such as Google Drive, Dropbox and OneDrive.

Print server

1: A print server is a computer or device that is used to manage one or more printers on a network.

2: It typically includes a variety of services, such as print job management, print queue management, and printer status monitoring.

3: Print servers can be used to manage the flow of print jobs within an organization, allowing multiple users to share a single printer or a group of printers.

4: They can also provide web-based access to printers, allowing users to submit print jobs from any device with a web browser.

5: Some print servers can also support multiple protocols such as LPR (Line Printer Remote), IPP (Internet Printing Protocol) and SNMP (Simple Network Management Protocol).

Unit 2 (Network Toplogies and Networking Devices)

Network topology

1: Network topology refers to the physical and logical layout of a network, including the arrangement of devices and the connections between them.
2: Common types of network topologies include bus, star, ring, and mesh.
3: The choice of topology can affect the performance and reliability of a network.

Selection criteria to choose type of topology

1: Size (no. of nodes) of the system.

2: The cost of the components and service required.

3: Architecture of network.

4: Cable type.

5: Expandability of the network.

6: Reliability

7: Scalability

8: Bandwidth capacity

9: Ease of installation

10: Ease of troubleshooting

Types of topology

1: topology of a network is the geometric representation of the relationship of all the links and linking devices (called nodes) to each other.

There are two types of topologies-

Physical topology: The complete physical structure of transmission media is

called physical topology. This refers to the layout of cabling, the location of nodes and interconnection between the nodes and cabling.

Logical Topology: The logical topology refers to how data is actually transferred

on a network. This represents the way that data passes through the network from one device to another.

Network control

Network control devices are the physical

entities connected to a network.

These devices are classified into two types:

End User Devices: Include computers, printers, scanners, and other devices that

provide services.

Network devices: Include all devices that connects the end-user devices to

communicate.End user devices that provide users with a connection to the network are also called hosts.

Need of a network control Device

1: Network Control devices are used to

expand a single network without breaking it into new pass or connecting it through another different network.

2: All networks require devices to provide

connectivity and functionality

3: Allows a greater number of nodes to be connected to the network.

4: Extends the distance over which a network can extend.

5: Localizes traffic on the network.

6: Can merge existing networks.

7: Isolates network problems so that they can be diagnosed more easily.

Network Control Devices layer

1: Operating below the Physical Layer.(Ex. Passive Hub).

2: Operating at the Physical Layer (Ex. Repeater or Active Hub).

3: Operating at the Physical and Data Link Layers (Ex. Bridge or Two – Layer Switch).

4: Operating at the physical, data link, and network layers (Ex. Router or Three- LayerSwitch).

5: Operating at all five layers (Ex.

Gateway).

Network control devices

Connectors:

1: Connectors are used to connect the guided (wired) transmission media to devices like the hub, server, workstations etc.

2: Jacks and plugs are male connectors and Sockets and Ports are female

connectors.

3: Also they can be classified by their different pinning configurations, such as DB9 and DB15 connectors that have 9 and 15 pins, respectively.

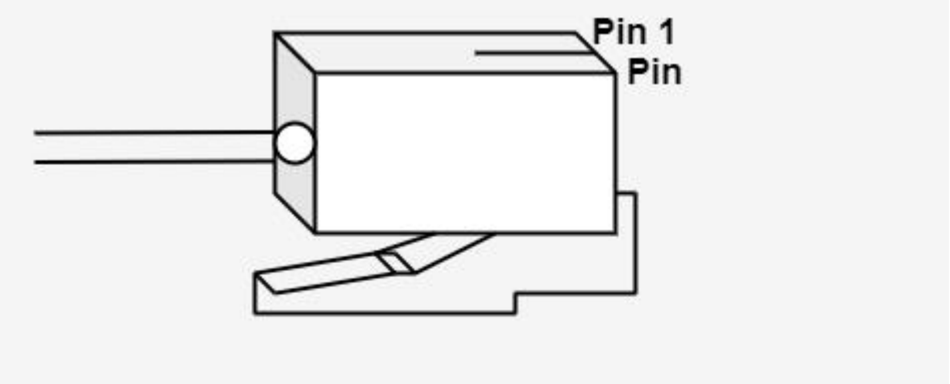
Types of connectors:

Twisted pair cable

1: UTP (Unshielded Twisted Pair) is used rather than STP (Shielded Twisted Pair) in almost all cases because it is less costly,

simpler to install and handle.

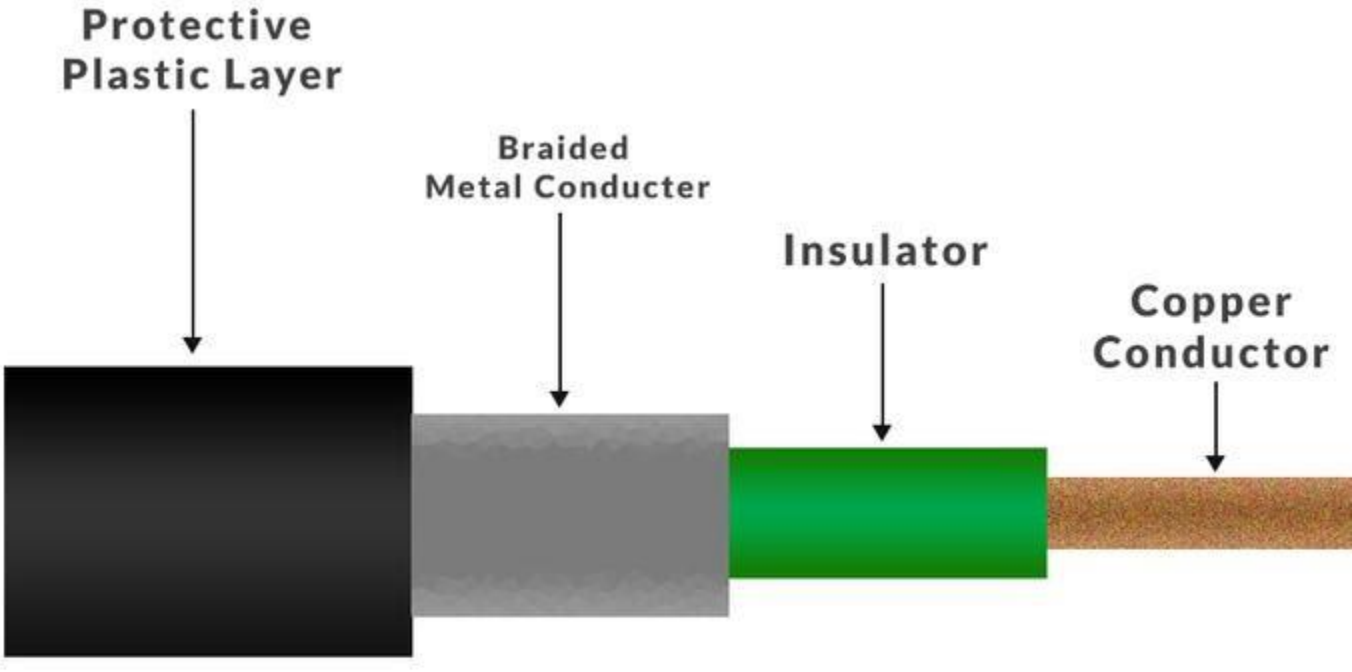
2: The standard UTP connector is RJ45 (RJ represents Registered Jack). RJ45 connector is similar to modular telephone connectors used in homes but it is larger.



Coaxial Cable

1: A coaxial cable is an electrical cable with a copper conductor and an insulator shielding around it and a braided metal mesh that prevents signal interference and cross talk.

2: Coaxial cable is also known as coax.

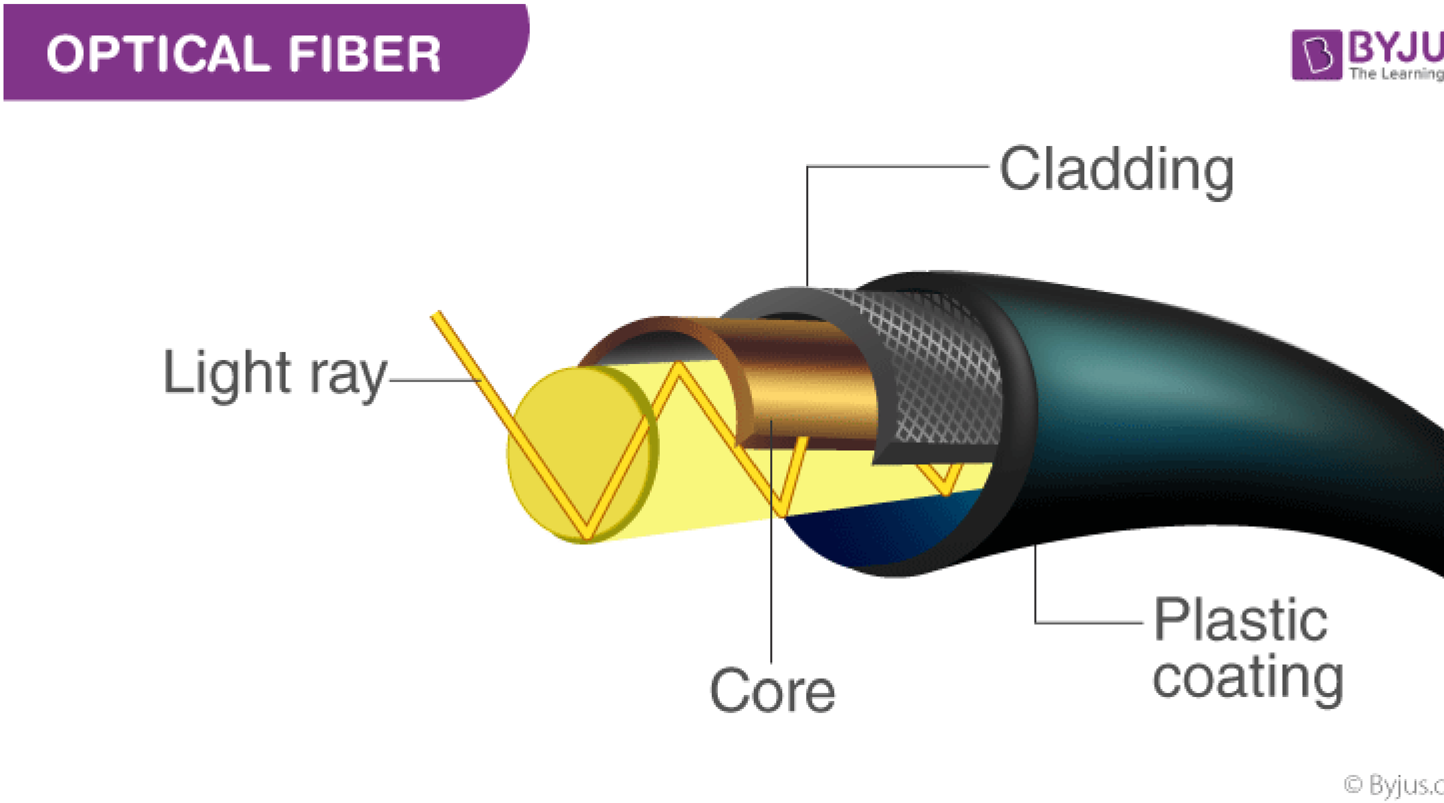


Fiber-optic Cable

1: Fiber optics, or optical fiber, refers to the technology that transmits information as light pulses along a glass or plastic fiber.

2: A fiber optic cable can contain a varying number of these glass fibers -- from a few up to a couple hundred.

3: Another glass layer, called cladding, surrounds the glass fiber core.



Examples

1: RS232 and V35 for serial interface.

2: RJ45 and BNC connectors for Ethernet.

3: SC or ST connectors for fiber optic.

Hub

1: Hub is the most basic networking device that connects multiple computers or other network devices together. Hub is a device that splits a network connection into multiple computers.

2: It is like a distribution center.

3: Hubs are commonly used to connect segments of a LAN.

Types of Hub:

Passive Hub

1: They do not have ability to amplify or regenerate the signal of incoming packets before broadcasting them out to the network.

2: They are just used for creating a connection between various devices. **3:** Passive hub only receives signal and then forward it to multiple devices.

Active Hub

1: They does have the ability to amplify or regenerate the signal of incoming packets before broadcasting them out to the network.

2: They not only amplifies the incoming signal but also forward it to multiple

devices.

3: It is also known as multiport repeater.

4: It upgrades the properties of incoming signal before sending them to destination.

Intelligent Hub

1: This adds extra features to an active hub.

2: It is capable to perform tasks of both Active and Passive hubs.

3: It also performs other tasks

like Bridging and routing.

4: Intelligent Ethernet hubs also possesses remote management capabilities.

Advantages:

1: A hub allows you connect clients to share and conversations with a

network protocol analyzer.

2: A hub also can modulate signal of the cable, if needed.

3: Using hub save money because switches are costly then hub.

Disadvantages:

1: Hub can‘t control traffic of data. Cause it receive all attachment post.

2: Hubs have limited port to connect client, so it is not suitable for large network.

3: It works as a query system. When NIC send a work to the hub then hub

make this work pending and process one by one. So it‘s time consuming.

Repeator

1: A repeater is an electronic device that regenerates weak or corrupted signals at the physical layer.

2: It copies and regenerates the signal bit by bit, without amplifying it, so that it can be transmitted at the maximum length in the network.

3: Repeaters are used to increase the usable length of the cable and connect segments of the same LAN, but they cannot do intelligent routing like bridges and routers.

4: Repeaters are commonly used with coaxial network configurations and segments that have the same access method.

5: They do not connect two different LANs of different protocols.

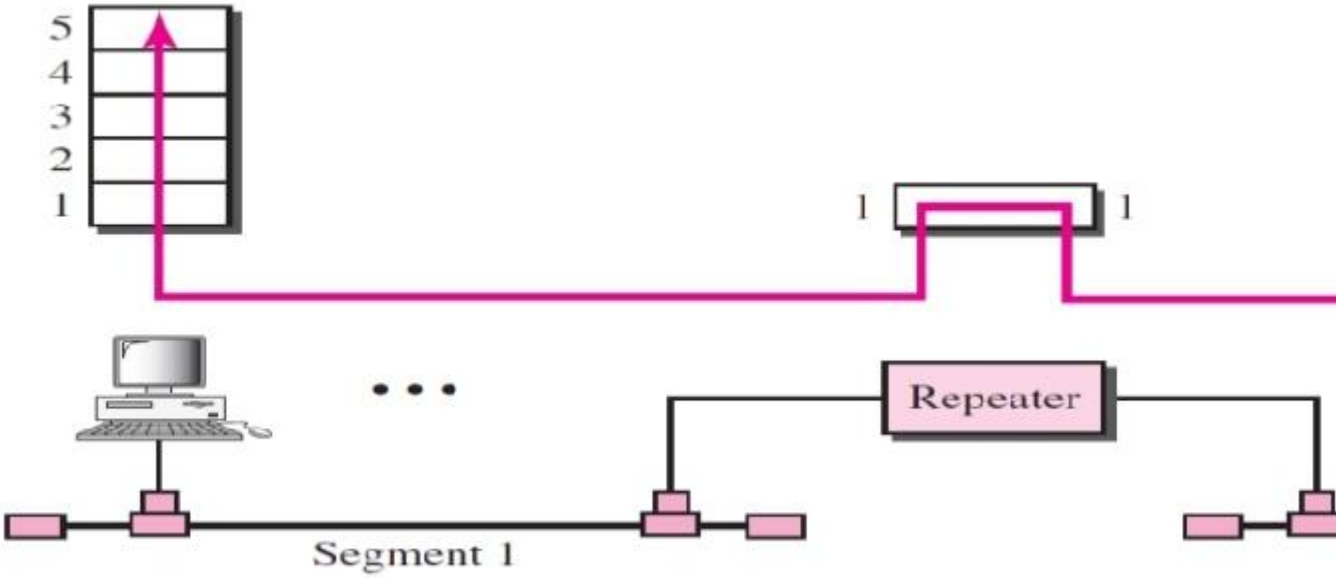


Figure 2.14:Repeater connecting two segments

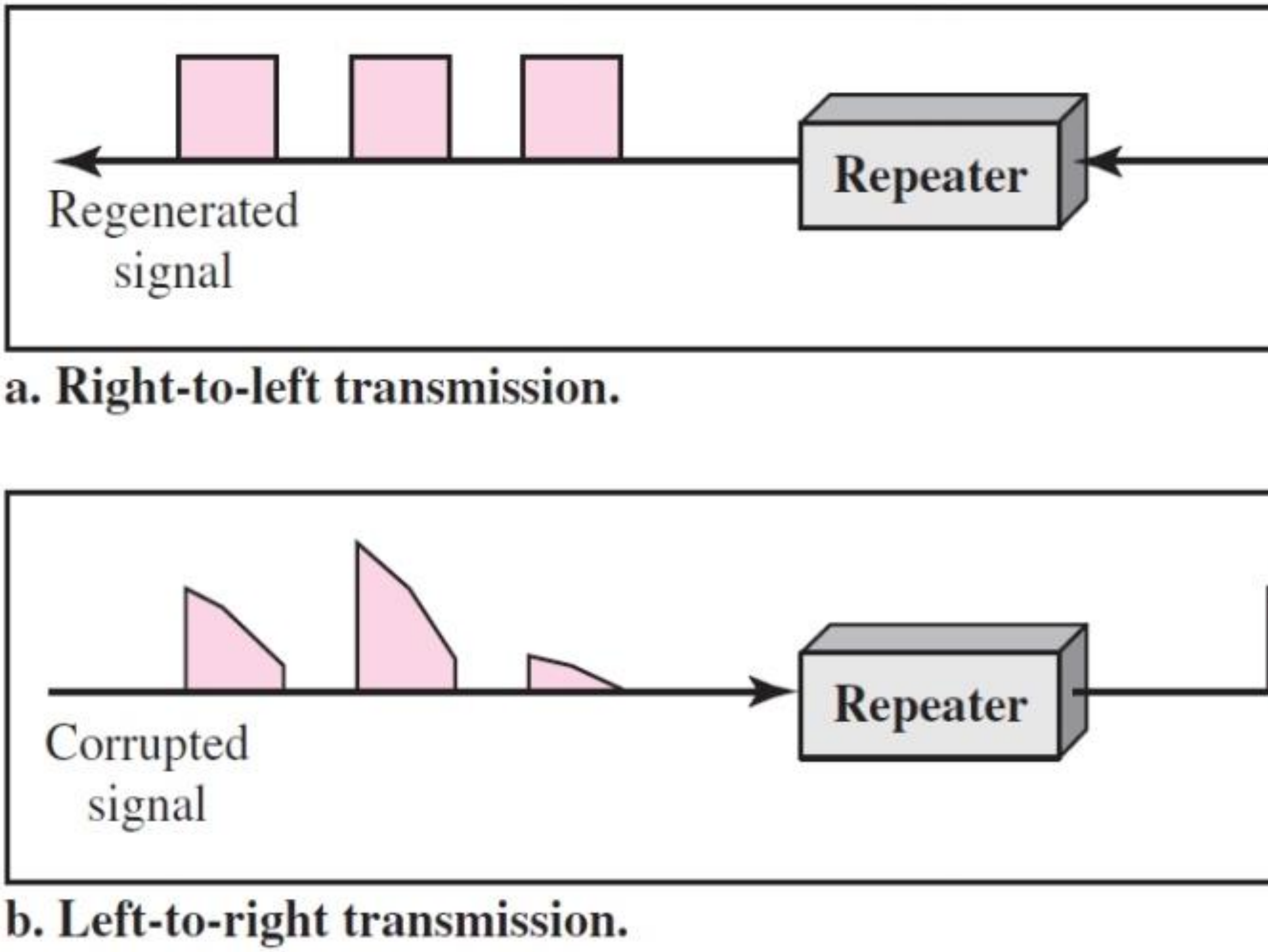

Repeater
Regenerated signal
a. Right-to-left transmission.
Repeater
Corrupted signal
b. Left-to-right transmission.

Figure 2.15: Functionality of a Repeater.

Advantages:

1: Repeaters increase the usable distance of the network.

2: Repeaters have little impact on network performance because they don‘t do any packet processing.

3: Repeaters can connect networks using different physical media.

Disadvantages:

1: Repeaters cannot connect different network architectures.

2: Repeaters do not reduce network traffic.

3: Too many repeaters on a network create noise on the wire and increase the likelihood of packet collisions.

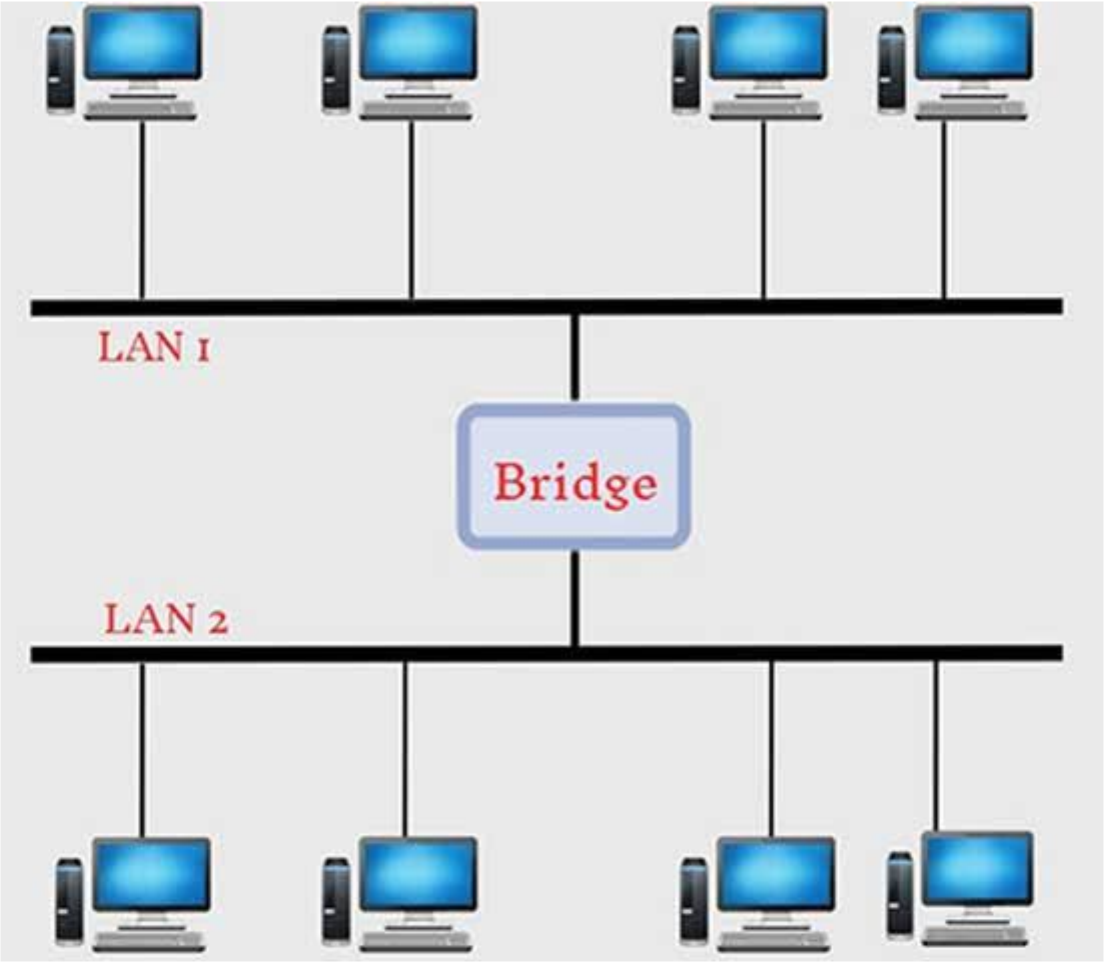
Bridge

1: The bridge is a networking device in a computer network that is used to connect multiple LANs to a larger LAN.

2: A bridge works at the data link layer of the OSI (Open Systems Interconnection) model and is responsible for forwarding and filtering network traffic between two or more network segments.

3: Bridges are often used to extend the reach of a LAN beyond its physical limitations.

4: For example, if a LAN is spread across multiple buildings or floors of a building, bridges can be used to connect those segments together and make them function as a single logical network.



types of Bridges:

Transparent bridge

1: The term "transparent" refers to the fact that the bridge is invisible to network users and applications - it does not require any special configuration or software to be installed on the computers that are connected to the network.

2: The primary function of a transparent bridge is to forward network traffic between different network segments while minimizing unnecessary traffic on the network.

Source route bridge

1: In an SRB network, each device includes a source routing header in the data packet, which specifies the path that the packet should follow through the network.

2: When the packet arrives at an SRB, the bridge examines the source routing header and uses the information to determine the path that the packet should follow through the network.

Translational bridge

1: translational bridge is a device that connects two different types of network media, allowing communication between them.

2: For example, a translational bridge can convert signals from a fiber optic cable to signals that can be transmitted over a twisted pair cable, allowing communication between two devices connected to different types of media.

Advantages:

1: Bridges can extend a network by acting as a repeater.

2: Bridges can reduce network traffic on a segment by subdividing network communications.

3: Bridges reduce collisions.

Disadvantages:

1: Bridges are more expensive than repeaters.

2: Does not limit the scope of broadcasts.

3: Does not scale to extremely large network.

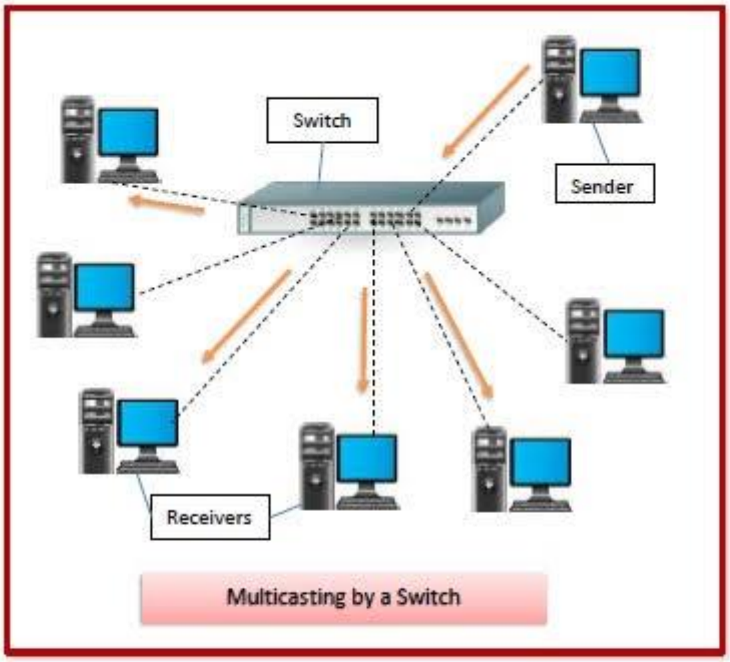
Switch

1: A switch is a device that connects devices on a LAN and operates at Layer 2 of the OSI model.

2: When a device on the network sends a data packet, the switch examines the destination Media Access Control (MAC) address in the packet's header and uses it to determine which port to forward the packet to.

3: The switch maintains a table that maps MAC addresses to specific ports so that it can quickly forward packets to the correct destination.

4: Unlike hubs, which simply broadcast data to all connected devices, switches provide dedicated communication channels between connected devices, allowing for faster and more efficient data transfer.



Switches data transmission methods:

Cut-through transmission:

1: It allows the packets to be forwarded as soon as they are received.

2: The method is prompt and quick but the possibility of error checking gets overlooked in such kind of packet data transmission.

Store and forward:

1: In this switching environment the entire packet are received and checked before being forwarded ahead.

2: The errors are thus, eliminated before being propagated further.

3: The downside of this process is that error checking takes relatively longer time consequently making it a bit slower in processing and delivering.

Fragment Free:

1: In a fragment free switching environment, a greater part of the packet is examined so that the switch can determine whether the packet has been caught up in a collision.

2: After the collision status is determined, the packet is forwarded.

Advantages:

1: Switches increase available network bandwidth.

2: Switches reduce the workload on individual computers.

3: Switches increase network performance.

Disadvantages:

1: At times switches when in Promiscuous mode is an opening for Security attacks [Spoofing IP address or capturingEthernet Frames using ethereal].

2: Handling Multicast packets needs quite a bit ofconfiguration & proper designing.

3: Not as good as a router in limiting Broadcasts.

Router

1: A router is a networking device that forwards data packets between computer networks.

2: It acts as a central hub that connects devices on a local area network (LAN) to the internet or other networks.

3: Routers use routing tables and protocols to determine the best path for data to take between networks.

4: They also typically include firewall and security features to protect the network from unauthorized access.

5: Routers can be either wired or wireless, and can be used in homes, businesses, and other organizations to provide internet access and connect devices to each other.

ways through which a router can receive information :

Static routing:

1: Static routing is a type of network routing method in which network administrators manually configure the routes that network traffic will take through the network.

2: In static routing, the administrator manually specifies the next hop for each possible destination network or IP address.

3: Static routing can be used in small networks that have a limited number of network devices and simple network topologies.

Dynamic routing:

1: Dynamic routing is a type of network routing method in which network devices, such as routers, exchange routing information with each other in order to automatically update and adjust their routing tables based on changes in the network topology.

2: This allows for more efficient and effective routing of network traffic, as the routing tables are constantly updated to reflect the current state of the network.

3: Dynamic routing is often used in large and complex networks, as it reduces the amount of manual configuration required and can adapt to changes in the network topology more quickly and effectively.

Advantages:

1: Reduce network traffic by creating collision domains.

2: Reduce network traffic by creating broadcast domains

3: Able to function on LAN & WAN.

Disadvantages:

1: Highly expensive than Hub, Bridge & Switch.

2: Slower than bridges or repeaters because they must analyze a data

transmission from the Physical to the Network layer.

3: Dynamic router communications (inter-router communication) causes

additional network traffic.

Gateway

1: gateway is an internetworking system capable of connecting two networks that use different protocols.

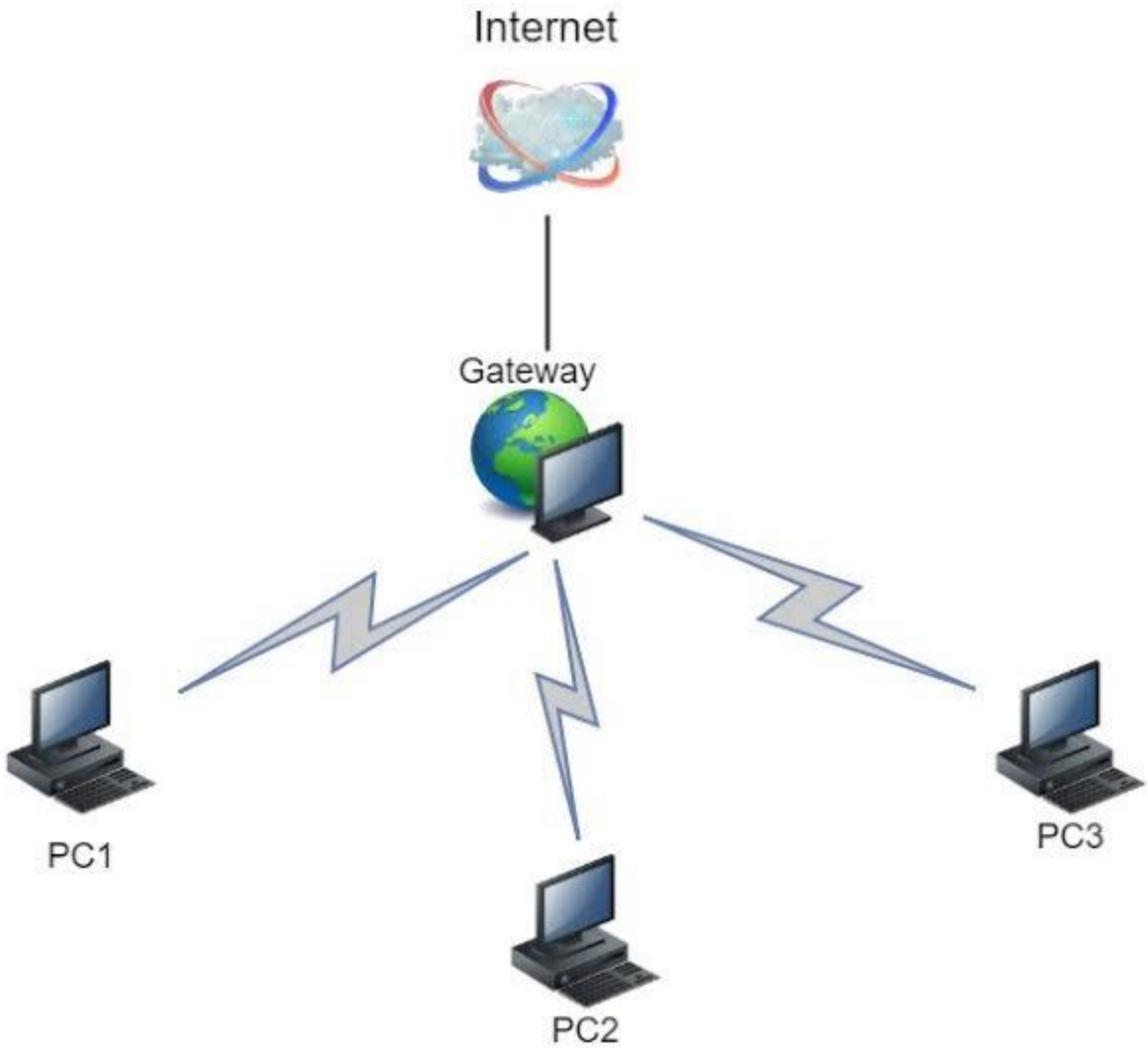
2: In fact gateway is any device,

system, or software application that can interpret data from one format to another.

3: The main feature of a gateway isthat it converts only the format of the data, not the data.

4: A gateway can be either hardware or software-based, and it is typically used to connect LANs (Local Area Networks) or WANs (Wide Area Networks) together.

5: For example, a router that connects a LAN to the Internet is acting as a gateway.



Advantages:

1: Used to expand the network.

2: Gateway is a server so it provides some security.

3: Provides a connection between internal network and external network.

Disadvantages:

1: gateways are critical to network connectivity, they can create a single point of failure. If a gateway fails, it can cause network downtime and disrupt communication between network segments.

2: Configuring and managing gateways can be complex, especially for larger and more complex networks.

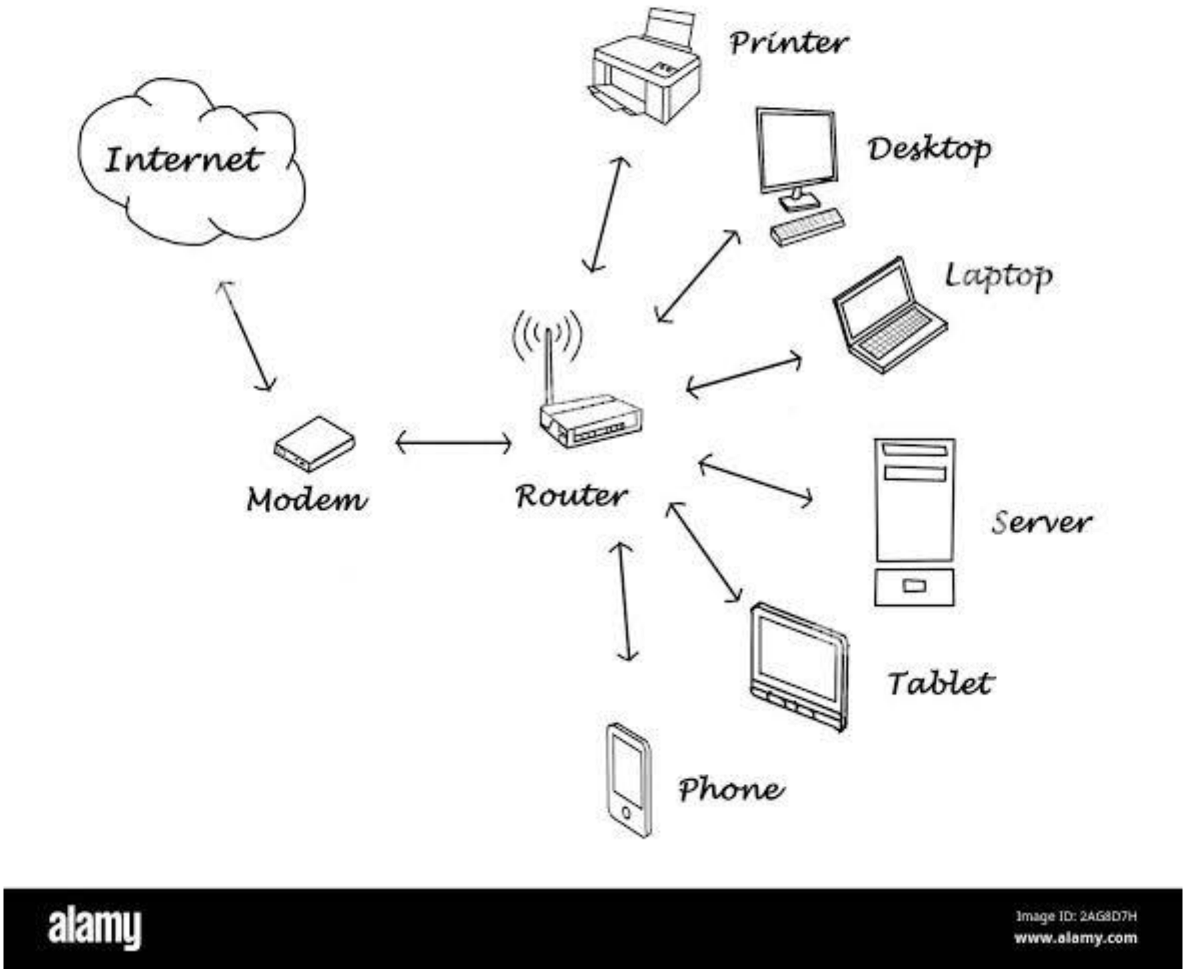
3: Gateways can be expensive, especially if they are hardware-based. This can be a barrier to entry for smaller organizations or those with limited IT budgets.

Modem

1: A modem (short for modulator-demodulator) is a device that converts digital signals from a computer or other digital device into analog signals that can be transmitted over telephone lines or other communication channels, and vice versa.

2: When a modem receives digital data from a computer, it modulates the digital data into an analog signal that can be transmitted over a telephone line or other communication channel.

3: When the analog signal reaches the destination, the modem on the other end demodulates the signal back into digital data that can be understood by the receiving device.



Types of Modem:

Internal modem

1: An internal modem is a type of modem that is installed inside a computer or other digital device.

2: They may be connected to the motherboard of the computer through a PCI or PCIe slot, or through a USB header on the motherboard.

3: They typically offer faster and more reliable performance than external modems, as they are not subject to external interference or signal loss.

External Modem:

1: An external modem is a type of modem that is a separate device that connects to a computer or other digital device through a cable.

2: External modems can be connected to a computer through a variety of interfaces, including USB, Ethernet, and serial ports.

3: They can be easily moved between computers or other devices, and can be shared among multiple devices through a router or switch.

NIC device driver

1: The NIC device driver acts as an interface between the NIC hardware and the operating system, allowing the computer to transmit and receive data over the network.

2: It provides the necessary instructions and protocols for the computer to communicate with other devices on the network.

3: NIC device drivers are essential for the proper functioning of a computer's network capabilities, and are typically included with the operating system or provided by the manufacturer of the NIC.

4: They may need to be updated periodically to ensure compatibility with new network technologies and to address any security or performance issues.

Client server architecture

1: Client-server architecture is a network

architecture in which many computers requesting services or resources on the

network are clients and one or more computer providing services or resources is a server.

2: Servers are powerful computers or processes dedicated to managing disk

drives (file servers), printers (print servers), or network traffic (network servers).

3: Clients are PCs or workstations on which users run applications.

4: Clients rely on servers for resources, such as files, devices, and even processing power.

DHCP

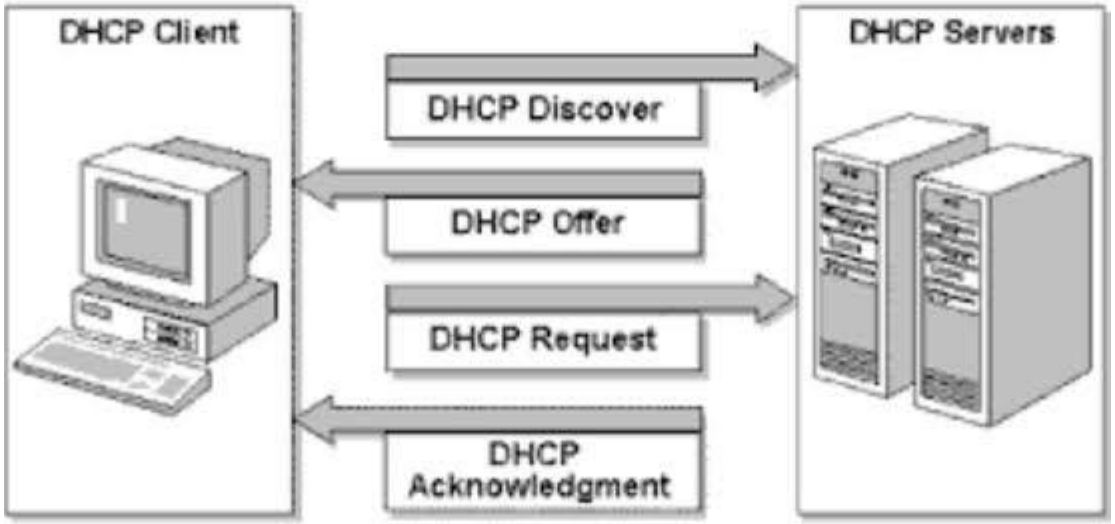
1: DHCP stands for Dynamic Host Configuration Protocol.

2: It is a network protocol that enables devices to obtain IP addresses and other configuration information automatically from a DHCP server.

3: In a DHCP-enabled network, a DHCP server is responsible for assigning IP addresses to devices on the network. **4:** When a device connects to the network, it sends a broadcast message requesting an IP address.

5: The DHCP server then assigns an available IP address to the device and provides other network configuration information, such as the subnet mask, default gateway, and DNS server addresses.

How DHCP Works



DHCP Server Optional Parameters

Command options	*Description*
domain-name	Specifies the domain name for the DHCP clients

root-path	Specifies the name of the path that contains the client‘s root file system in NFS notation
log-servers	Defines a list of log servers available to the client
broadcast-address	Defines a broadcast address for the network

---

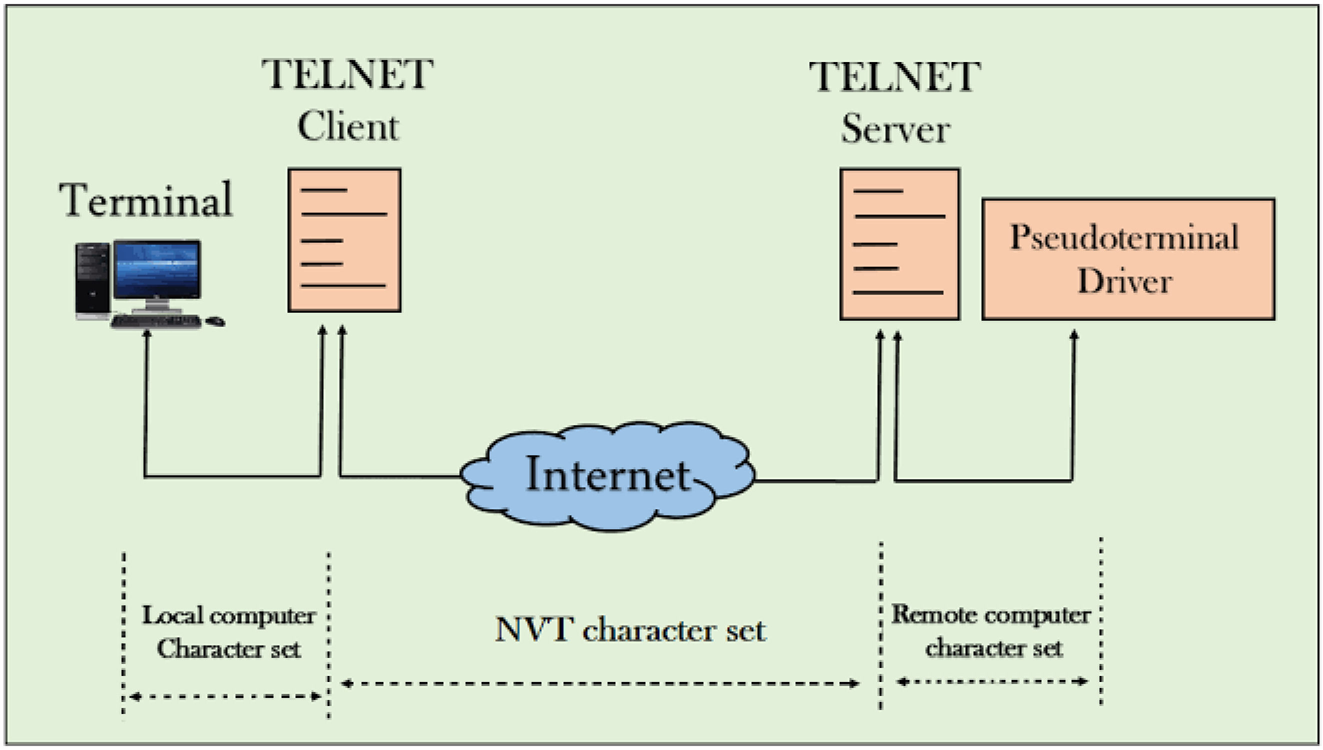
TELENET

1: TCP protocol is used to connect the remote computers, the TELNET protocol makes it possible to use them.

2: The TELNET protocol offers a user the possibility toconnect and log on to any other hosts in the network from user‘s own computer by offering aremote log on capability.

3: When using TCP, data is transmitted in the form of segments, with each segment containing a sequence number and an acknowledgment number.

4: The sequence number identifies the position of the data in the stream, while the acknowledgment number is used to confirm receipt of the data by the receiving endpoint.



TELNET commands

Name	*description*
ABORT	about process
SUSP	suspend process
NOP	no operation
BRK	Break

File Transfer Protocol (FTP)

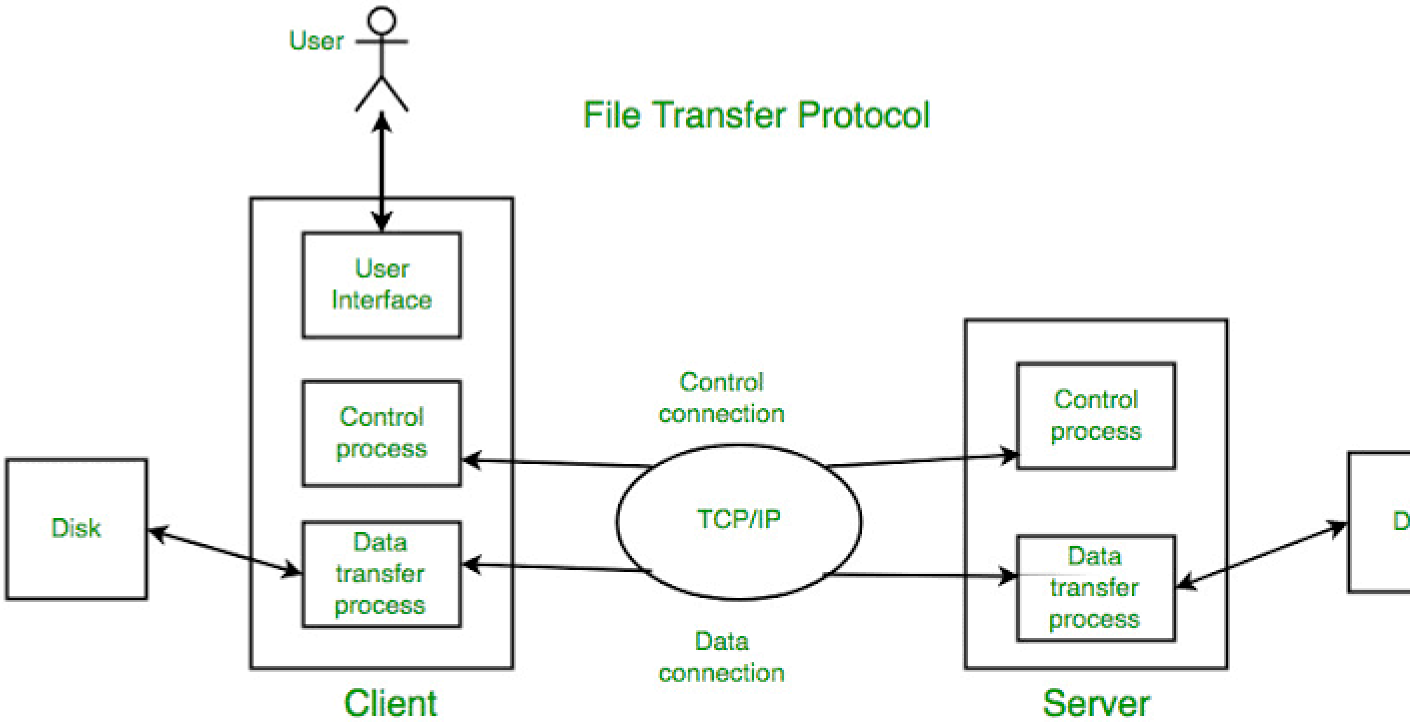
1: File Transfer Protocol (FTP) is a protocol used for transferring files between computers on a network.

2: FTP is based on a client-server architecture, where a client program is used to connect to an FTP server, which serves as the host for the files being transferred.

3: FTP uses a command channel and a data channel to transfer files.

4: The command channel is used for sending commands from the client to the server, while the data channel is used for transmitting the actual file data.

5: FTP can use either the standard TCP/IP protocol or a secure version called SFTP (Secure File Transfer Protocol).



FTP command (command type -access)

Command	*description*

USER	identity user
PASS	Provide password
QUIT	logout
ACCT	provide account

Unit 3 (Transmission Media)

Need of Transmission media

1: The need for transmission media in computer networks arises from the fact that data cannot be transmitted through air or space without a physical medium.
2: Therefore, a transmission medium is essential to transmit data over long distances between computers, servers, and other network devices.
3: A transmission media can be defined as the physical path through which data is transmitted from one device to another.

Selection Criteria

Following factors are to be considered while choosing Transmission Medium:

1: Type of Media.

2: Transmission Rate.

3: Flexibility.

4: Radiation.

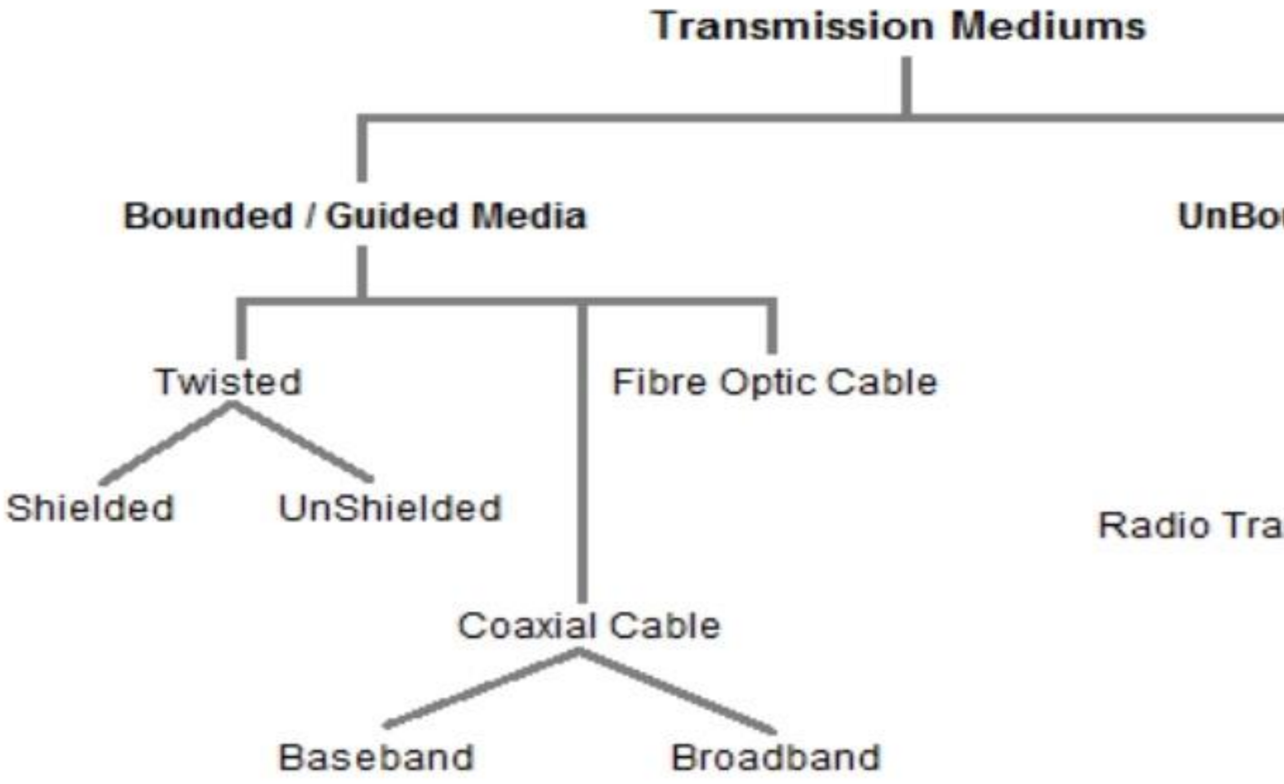
5: Cost and Ease of Installation.

6: Reliability.

7: Resistance to Environmental Conditions.

8: Distances.

Types of Transmission Media



Guided Media

1: It uses physical links, such as coaxial or fibre optic cables, to transmit data to the desired connection.

2: Most cables are made of copper and bound by some form of jacket material.

3: Because they are tangible, this type of

media is limited to a fixed location.

4: Popular bound transmission media in use are twisted pair cable, co-axial cable and fibre optical cable.

5: Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost, etc.

Cable Characteristics:

Following characteristics are to be considered while choosing cable:

1: The type of cable to be used for networking. Like (UTP, STP Coaxial or Fibre Optic).

2: The bandwidth of a communication system is the highest frequency range that it uses.

3: The actual data through put of a cable, after applying encoding and compression schemes to more efficiently use the bandwidth of the cable.

4: Cost required to purchase the cable.

5: Cost required to install the cable in the network.

6: The capacity of cable to tolerate electromagnetic interference.

Coaxial cable:

1: Coaxial cable, commonly referred to as coax, is a type of electrical cable consisting of a central conductor, surrounded by an insulating layer, which in turn is surrounded by a conducting shield.

2: The shield is usually made of braided wire or foil, and is often covered by an outer insulating jacket.

3: Coaxial cable is commonly used for transmitting radio frequency (RF) signals, such as those used for cable television, internet, and telephone services.

4: The central conductor carries the signal, while the shield prevents interference from external sources, and also helps to contain the signal within the cable.

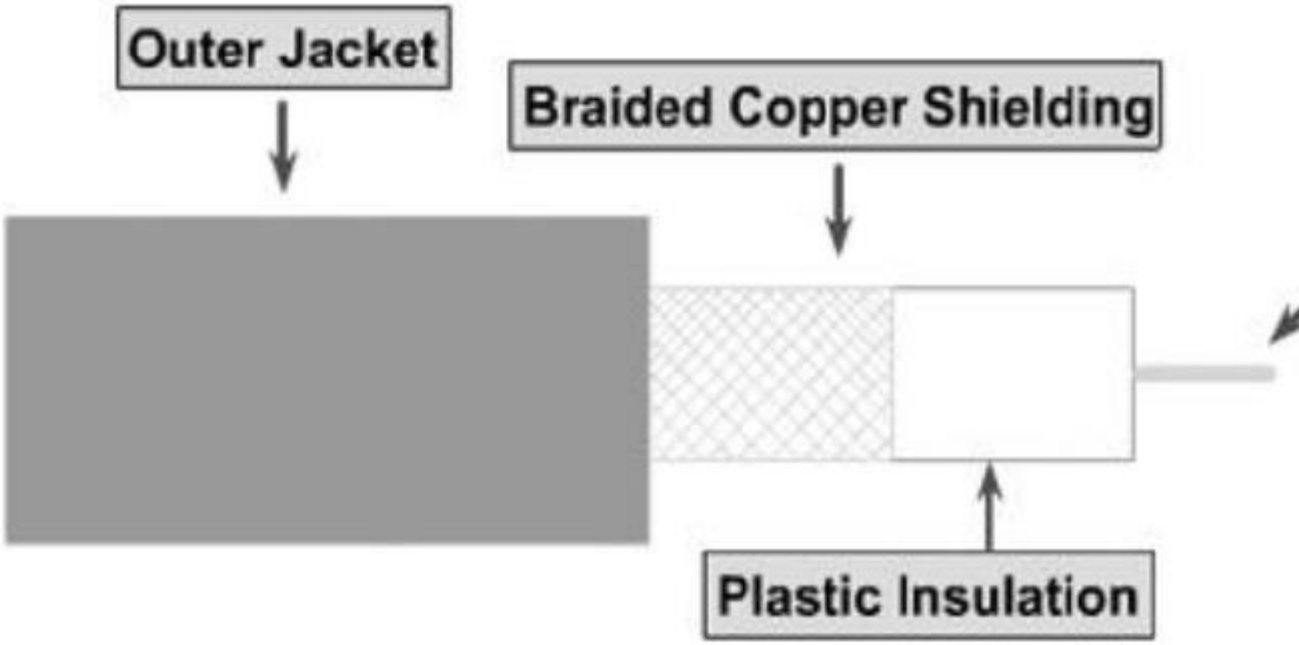


Figure 3.6: Coaxial Cable

Features of coaxial cable:

1: Speed and throughput: 10 to 100 Mbps.

2: Media and connector size: Medium.

3: Maximum cable length: 500 m (medium).

4: It provides better immunity than twisted pair.

5: This cable is able to transmit data at higher rates.

Properties of coaxial cable:

1: Gauge of coaxial cable is thicker than the twisted pair.

2: Coaxial cables consist of a single, twoconductor wire, with a centre conductor and an outer shield (conductor), which is of solid metal.

3: Not as limited as UTP, amplifiers or other intermediate devices can be used to extend high frequency transmissions over long distances.

Applications of coaxial cables:

1: Analog telephone networks.

2: Digital telephone network.

3: Cable TV.

4: Traditional Ethernet LANs.

5: Digital transmission.

6: Thick Ethernet.

Types of coaxial cable:

1: Baseband: A baseband coaxial cable transmits a single signal at a time

at very high speed. A baseband cable is

mainly used for LANs. 50 ohm (Ω)Baseband coaxial cables are used for digital transmission.

2: Broadband: A broadband coaxial cable can transmit many simultaneous signals using different frequencies.Covers large area as compared to Baseband Coaxial

Cable. 75 ohm (Ω)Broadband coaxial cables are used for analog transmission.

Advantages of coaxial cable:

1: It can be used for both analog and digital transmission.

2: It offers higher bandwidth as compared to twisted pair cable and can span longer distances.

3: Because of better shielding in coaxial cable, loss of signal or attenuation is less.

4: It has lower error rates as compared to twisted pair.

Disadvantages of coaxial cable:

1: Coaxial cable can be expensive compared to other types of cables, such as twisted pair cables.

2: Coaxial cable can be vulnerable to electromagnetic interference (EMI) and radio frequency interference (RFI). This can cause noise or distortion in the transmitted signal.

3: Coaxial cable can be difficult to install in certain environments, such as walls or ceilings. This can require special tools and techniques, which can add to the installation cost.

4: Coaxial cable is relatively inflexible compared to other types of cables, such as fiber optic cables or twisted pair cables.

Fiber optic cable

1: Fiber optic cable is a type of high-speed data transmission cable that uses strands of glass or plastic fibers to transmit digital signals over long distances.

2: The cable consists of a core, cladding, and outer jacket.

3: The core is the central part of the cable where the light travels, the cladding is a layer that surrounds the core and helps to keep the light signal inside, and the outer jacket protects the cable from external factors such as moisture, heat, and physical damage.

4: Fiber optic cables are widely used in telecommunications and networking applications due to their ability to transmit data over long distances at very high speeds with low signal loss.

Advantages of fibre optic cable:

1: Fibre optic cables have a much

greater bandwidth than metal cables. No other cable-based data transmission medium provides the bandwidth like it.

2: Fibre has a very low rate of bit error hence it is highly resistive to electromagnetic interference. Mostly fibre-optic transmission is noise free.

3: When high frequency signal are broadcasted through convention coaxial cable, it loss half of its power only after a few hundred meters whereas the optical

Fibre loss the same amount of power in 15 km or more.

4:The transmission rate of optical Fibre is

10 GB/sec whereas coaxial cable is 1 GB/sec.

5: Because of light weight and small size of the cable it has good capability of carrying a large number of signals.

Disadvantages of fibre optic cable:

1: Fibre optic cables are very expensive to

install**.**

2: The test equipments that are used typically and traditionally for conventional networking are of no use in a Fibre optic network. Expensive and specialized

optical test equipments are required for fiber optic cable.

3: Since it is small and compact, it

is highly susceptible to physical damage during installation or construction activities.

4: Optical Fibre cables are more brittle than electrical wires.

5: Most Fibre become opaque when exposed to radiation.

Unguided media

1: Unbound transmission media are the ways of transmitting data without using any cables.

2: It uses wireless links hence known as unbounded media, and also known as unguided or wireless media.

3: Unlike bound media, it transmits data without using any physical connectors between two communicating devices.

4: It uses microwave, infrared or radio signals to transmit information.

5: These media are not bounded by physical geography.

6: Unguided Media transmits electromagnetic waves without using a solid conductor.

7: Electromagnetic waves do not require any media to propagate and can travel even through vacuum.

Microwave communication

1: Microwave communication is method of

wirelessly sending data.

2: In microwave transmission information is transmitted by electromagnetic waves.

3: A microwave is an electromagnetic wave with a very short wavelength, between .039 inches (1 millimetre) and 1 foot (30 centimetres).

4: This part of the radio spectrum ranges across frequencies of roughly 1.0 gigahertz (GHz) to 300 GHz. These correspond to wavelengths From 30 centimetres down to 0.1 cm

5: Within the electromagnetic spectrum, microwaves can be found between radio

waves and shorter infrared waves.

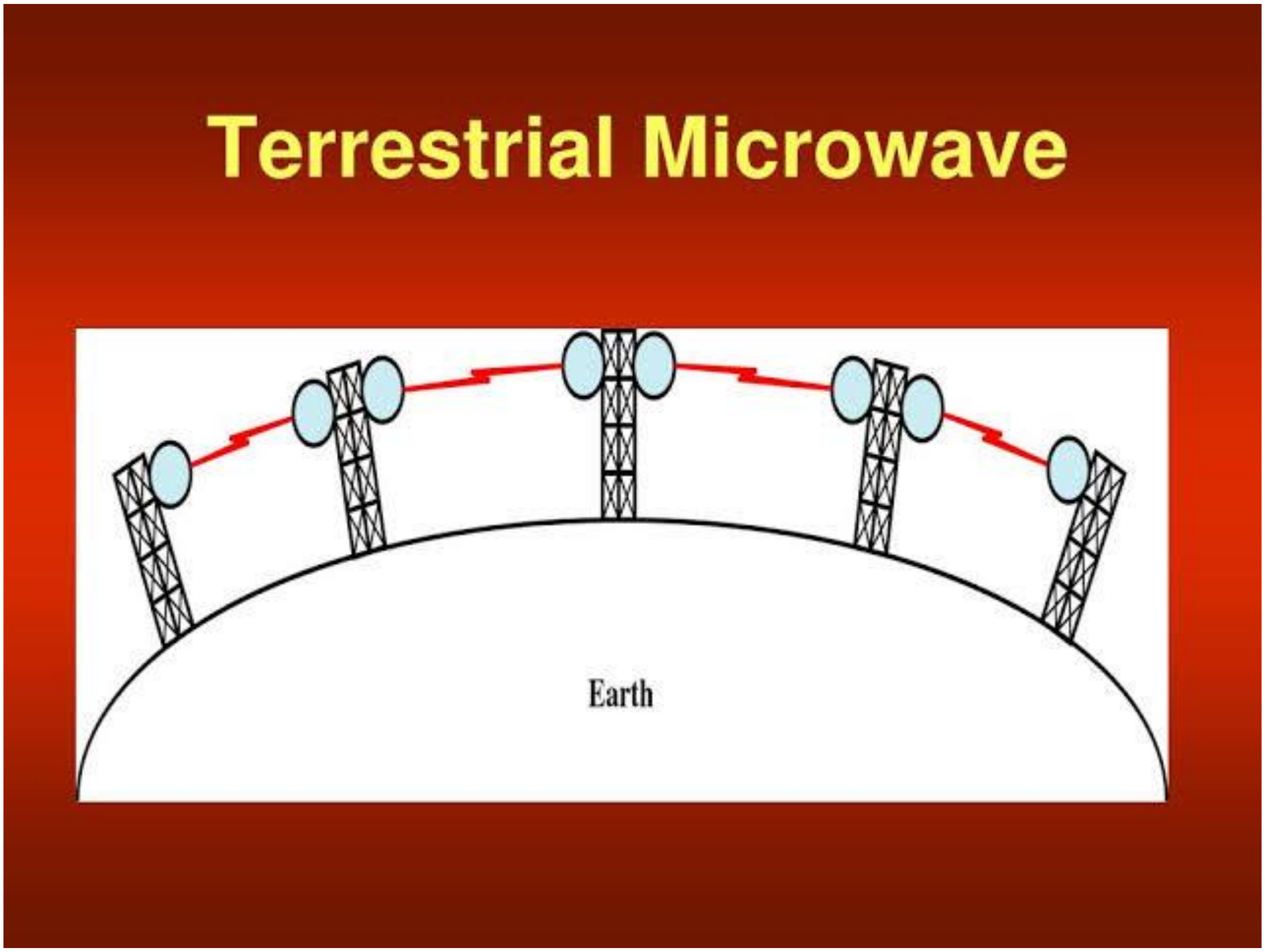
6: Their short wavelengths make microwaves ideal for use in radio and television broadcasting.

Microwave Transmission is divided into two type:

1: Terrestrial microwave refers to the use of microwave frequencies to transmit information over the Earth's surface.

2: This technology is commonly used in telecommunications and broadcasting to transmit data, voice, and video signals over long distances.

3: Terrestrial microwave links typically operate in the range of 1 GHz to 30 GHz, with wavelengths ranging from 30 cm to 1 cm. These frequencies allow for high-bandwidth transmissions over long distances without the need for expensive fiber optic cables.



Advantages:

1: Terrestrial microwave networks are capable of transmitting large amounts of data at high speeds, making them ideal for applications such as video conferencing, file sharing, and real-time data transfer.

2: Terrestrial microwave networks are generally less expensive to build and maintain than traditional wired networks.

3: Terrestrial microwave networks are highly reliable, with low signal loss and minimal interference from other sources.

4:Terrestrial microwave networks can be quickly deployed and easily reconfigured to meet changing needs.

5: Terrestrial microwave networks are inherently secure because the signals are difficult to intercept and cannot be easily disrupted.

Disadvantages:

1: Terrestrial microwave signals require an unobstructed line of sight between the transmitter and receiver. This means that microwave towers need to be placed at high elevations, which can be difficult in areas with rough terrain or dense vegetation.

2: Terrestrial microwave signals can be affected by severe weather conditions such as heavy rain, fog, and snow.

3: Terrestrial microwave networks have limited bandwidth compared to wired networks.

4: Terrestrial microwave networks are subject to various regulatory restrictions and licensing requirements, which can be a barrier to entry for some organizations.

Satellite microwave

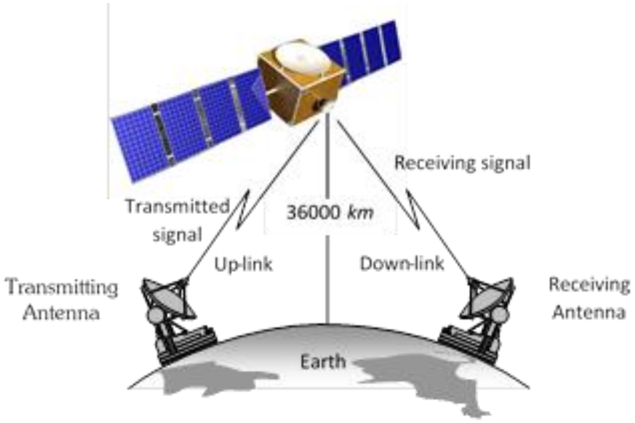
1: Satellite microwave refers to the use of microwave frequencies for communication between satellites in space and ground-based stations.

2: It involves the transmission of information in the form of electromagnetic waves.

3: Satellite microwave technology is widely used for a variety of applications, including television broadcasting, navigation, and weather forecasting.

4: The signals are transmitted from a ground station to a satellite in space, which then relays the signal to another ground station or to another satellite in orbit.

5: Satellite microwave links typically operate at higher frequencies than terrestrial microwave links, often in the range of 10 GHz to 30 GHz, with wavelengths ranging from 3 cm to 1 cm.



Radio wave communication

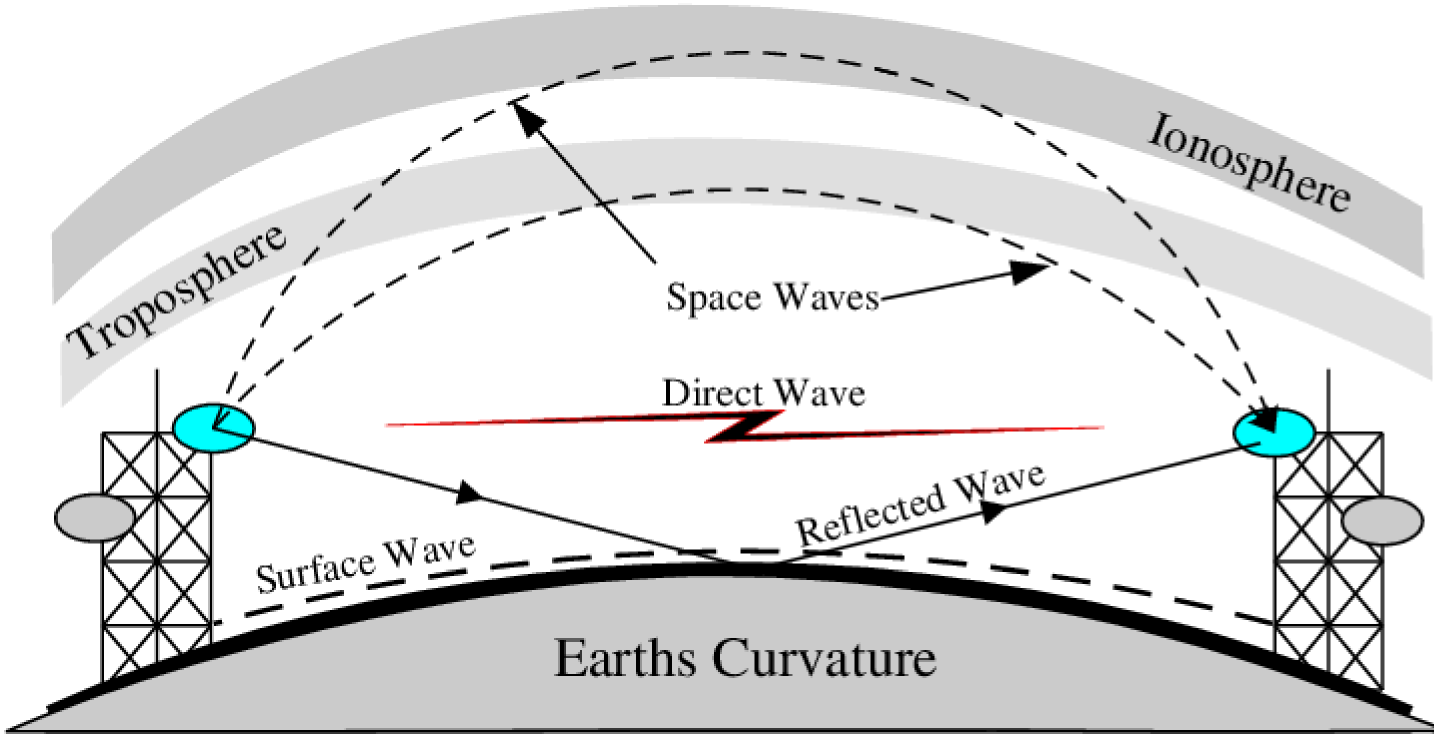
1: Radio wave communication is a method of transmitting information wirelessly using radio waves.

2: Radio waves are a type of electromagnetic radiation that have a frequency range between 3 kHz and 300 GHz.

3: They are used for various types of communication, including television and radio broadcasting, cell phone communication, and satellite communication.

4: In radio wave communication, a transmitter converts an electrical signal into a radio wave and sends it through the air to a receiver.

5: The receiver then converts the radio wave back into an electrical signal that can be understood by the device receiving the transmission.



---

infared communication

1: Infrared communication, also known as IR communication, is a wireless communication technology that uses infrared light to transmit data between two devices.

2: Infrared light is a type of electromagnetic radiation with a wavelength longer than visible light but shorter than radio waves.

3: IR communication is commonly used in remote controls for TVs, DVD players, and other home appliances.

4: In this application, the remote control sends a series of IR signals to the device it's controlling to change the channel, adjust the volume, or perform other functions.

5: One of the benefits of IR communication is its low power consumption, making it a good choice for battery-powered devices.

6: However, IR signals are limited to line-of-sight communication, meaning that the receiver must be within the direct path of the transmitter.

7: This can be a limitation in certain applications where obstacles can block the transmission.

Bluetooth architecture

1: The Bluetooth technology was developed to provide a wireless interconnect between small mobile devices and their peripherals.

2: Bluetooth technology was designed to connect mobile devices over apersonal and private connection.

3: It uses radio frequency for communication and also maintains a high level of security.

4: Robustness, low power and low cost are some of the key features of Bluetooth technology.

5: A uniform structure is defined for a wide range of devices to connect and communicate with each other.

6: Now Bluetooth is globally accepted

that Bluetooth enabled devices, which is almost everywhere in the world can

connect to other devices in proximity.

Bluetooth architecture defines two types of networks:

Piconet:

1: Piconet is a Bluetooth network that consists of one primary (master)

node and seven active secondary (slave) nodes.

2: Thus, piconet can have upto eight

active nodes (1 master and 7 slaves) or stations within the distance of 10

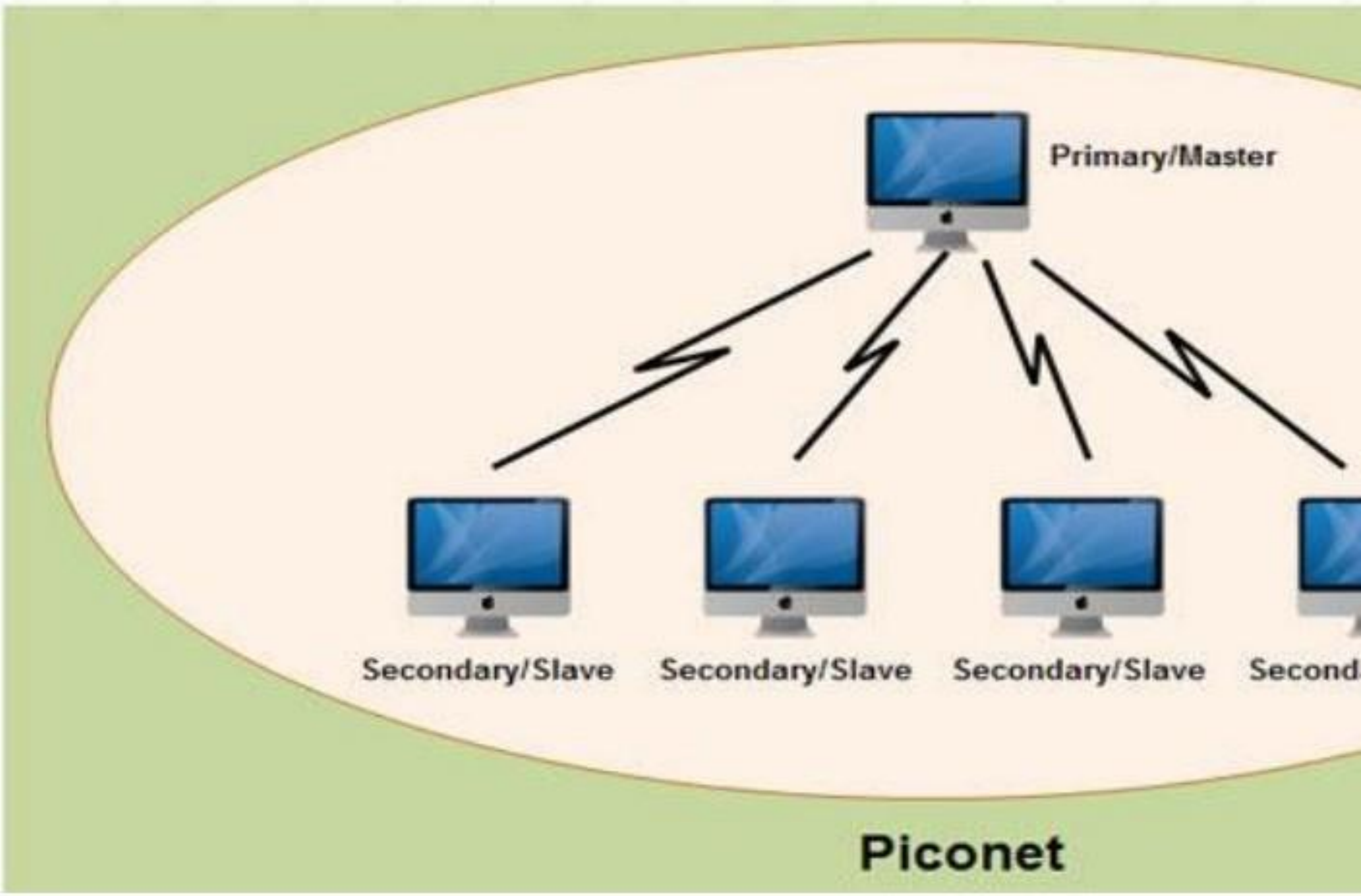
meters.

3: There can be only one primary or master station in each piconet.

4: The communication between the primary and the secondary can be one-to-one or oneto-many.

5: All communication is between master and a slave.

6: Salve -slave communication is not p/ossible in addition to seven active slave station, a piconet can have upto 255 parked nodes.
7: These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.



scatternet:
1: Scattemet is formed by combining various piconets.
2: A slave in one piconet can act as a master or primary in other piconet.
3: Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master.
4: This node is also called bridge slave.
5: Thus a station can be a member of two piconets.
6: A station cannot be a master in two piconets.

Wifi

1: Wi-Fi (short for Wireless Fidelity) is a wireless networking technology that allows electronic devices to connect to the internet and communicate with one another without the need for physical cables or wires.

2: Wi-Fi operates using radio frequencies, typically in the 2.4GHz and 5GHz bands, to transmit data between devices.

3: To use Wi-Fi, you need a wireless-enabled device such as a smartphone, laptop, or tablet, and a Wi-Fi access point or router, which connects to the internet through an internet service provider (ISP).

4: When a device connects to a Wi-Fi network, it sends and receives data wirelessly through the access point or router.

5: Wi-Fi has become an essential part of modern life, providing fast and convenient internet connectivity in homes, offices, public spaces, and even on airplanes.

6: However, Wi-Fi signals can be affected by a range of factors, including distance, obstructions, and interference from other electronic devices, which can reduce the strength and reliability of the connection.

Wi-max

1: WiMAX (Worldwide Interoperability for Microwave Access) is a wireless communication technology that provides high-speed data transfer over a wide area.

2: It is based on the IEEE 802.16 standard and operates in the microwave frequency range.

3: WiMAX is designed to provide wireless broadband access to customers over a large area, similar to Wi-Fi, but with a larger coverage range

4:WiMAX can deliver high-speed internet. connectivity to businesses, homes, and mobile devices over a radius of up to 30 miles (50 km), making it a popular solution for internet service providers (ISPs) in rural areas where laying cables can be difficult and expensive.

5: WiMAX also provides a secure and reliable connection, making it suitable for businesses and government organizations.

6: In recent years, WiMAX has faced stiff competition from other wireless technologies such as LTE (Long-Term Evolution), and has largely been replaced by 4G and 5G mobile networks.

6: However, it is still used in certain regions and for specific applications, such as fixed wireless broadband and point-to-point connectivity.

Band in cellular telephony

1: In cellular telephony, a band refers to a range of frequencies within the electromagnetic spectrum that is designated for use by mobile devices.

2: The frequency band used by a cellular network determines the type of technology used by mobile devices and affects the network's coverage, capacity, and performance.

3: There are several frequency bands used for cellular communication, including:

(1): Low Bands (below 1 GHz) - This includes bands such as 700 MHz and 900 MHz. They offer better coverage and penetration but limited bandwidth.

(2): Mid Bands (1-6 GHz) - This includes bands such as 1800 MHz and 2.6 GHz. They offer a balance of coverage and capacity and are commonly used for 4G LTE networks.

(3): High Bands (above 6 GHz) - This includes bands such as 24 GHz and 28 GHz. They offer high capacity but limited coverage due to their shorter range and limited ability to penetrate buildings.

4: Different countries and regions may allocate different frequency bands for cellular communication, which can affect device compatibility and roaming.

5: Additionally, newer cellular technologies such as 5G are designed to use higher frequency bands to enable faster data transfer rates and support more connected devices.

Calls using mobile phone

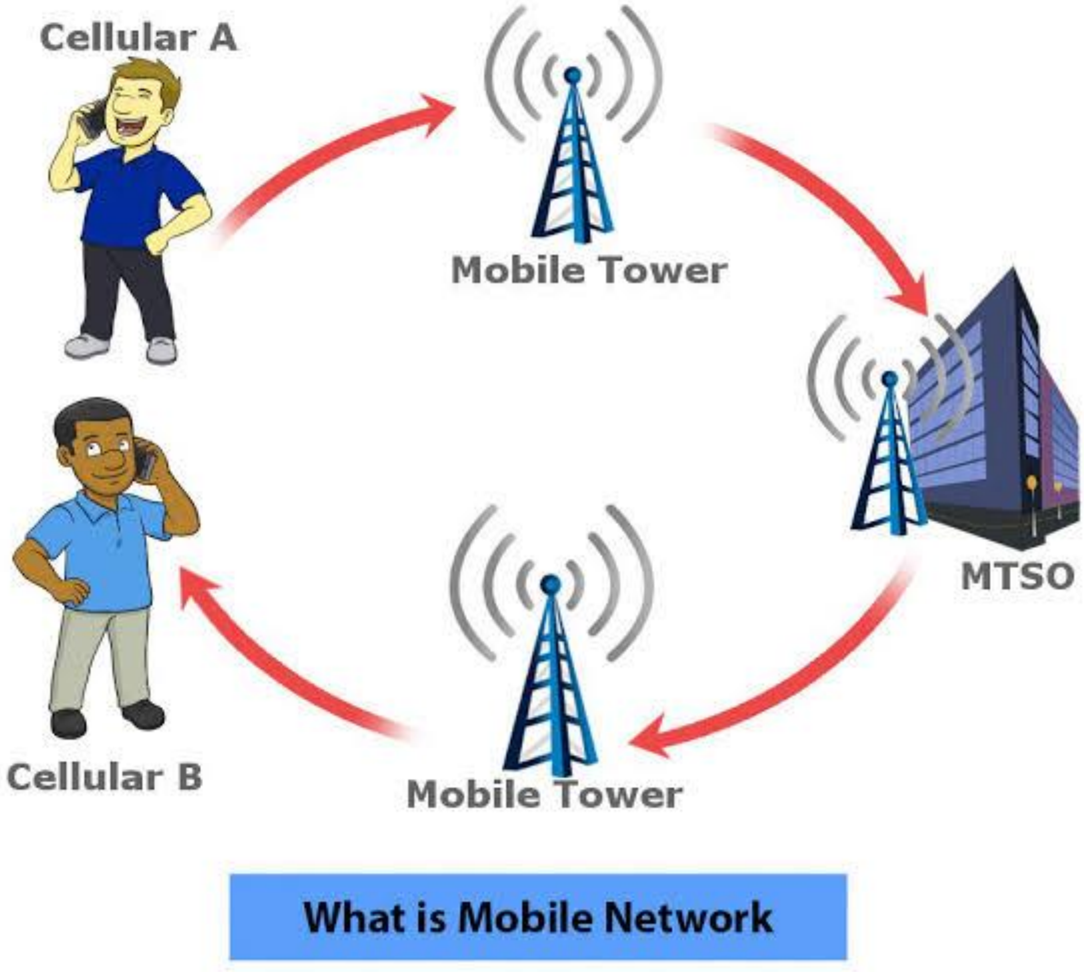
1: Call is made from the mobile phone by entering 10-digit phone number. The mobile phone itself scans the band & seeks a channel for setting up the call.

2: After seeking, it sends this number to the closest cell office, which in turn , sends it to the CTO.

3: If the called party is available, CTO lets MTSO (mobile telephone switching office) know.

4: At this point, MTSO allocates an empty voice channel to the cell to establish the connection.

5: The mobile phone adjust its tuning to the new channel & the dialog begins.



Call from Land Phone to a mobile phone

1: The telephone central office sends the number to the MTSO.

2: The MTSO performs a lookup to see where the mobile phone is currently placed by sending appropriate query signal to all the cells.

3: This process is known paging.

4: The cell where the mobile phone is currently located responds to the MTSO.Incoming calls work differently.

5: To start with idle phone is continuously listen to paging channel to detect messages at directed at them.

6: The MTSO then transmit the incoming call signal to that mobile phone & when the mobile phone is answered.

Transmitting Operation

1: Transmitting data involves sending information from the mobile device to the cell tower.

2: The device converts the data into radio waves that are transmitted through the air to the tower.

3: The tower then sends the data to the network, which routes it to its intended destination.

Receiving Operation

1: Receiving data involves the opposite process, where the tower sends data to the mobile device.

2: The tower receives the data from the network and converts it into radio waves that are transmitted to the mobile device.

3: The device then receives the data and displays it to the user.

Handoff Operation

1: Handoff is the process of transferring a connection from one cell tower to another as a mobile device moves from one area to another.

2: As the user moves out of range of one tower, the device automatically searches for the nearest tower with the strongest signal and establishes a connection with it.

3: The handoff process is seamless and transparent to the user, ensuring uninterrupted connectivity while the device is in motion.

Unit 4 (Network Architecture and Protocols)

Layered architecture

1: Layered architecture, also known as layered protocol architecture, is a way of organizing the functions and protocols of a computer network into distinct layers.
2: Each layer is responsible for a specific set of tasks, and communicates with the layers above and below it through standardized interfaces.
3: The most common layered architecture model used in computer networks is the OSI (Open Systems Interconnection) model, which consists of seven layers:

Physical layer: This layer is responsible for the transmission and reception of raw bit streams over a physical medium, such as a cable or wireless link.

Data link layer: This layer provides reliable transmission of data frames between two nodes on a network, and includes functions such as error detection and correction.

Network layer: This layer is responsible for addressing and routing data between different networks, and includes protocols such as IP (Internet Protocol).

Transport layer: This layer provides end-to-end communication between applications on different devices, and includes protocols such as TCP (Transmission Control Protocol).

Session layer: This layer manages the establishment and termination of sessions between applications, and includes protocols such as SSH (Secure Shell).

Presentation layer: This layer is responsible for the presentation and formatting of data, and includes functions such as encryption and compression.

Application layer: This layer provides services to end-user applications, such as email, file transfer, and web browsing.

means of encapsulation header and tail.

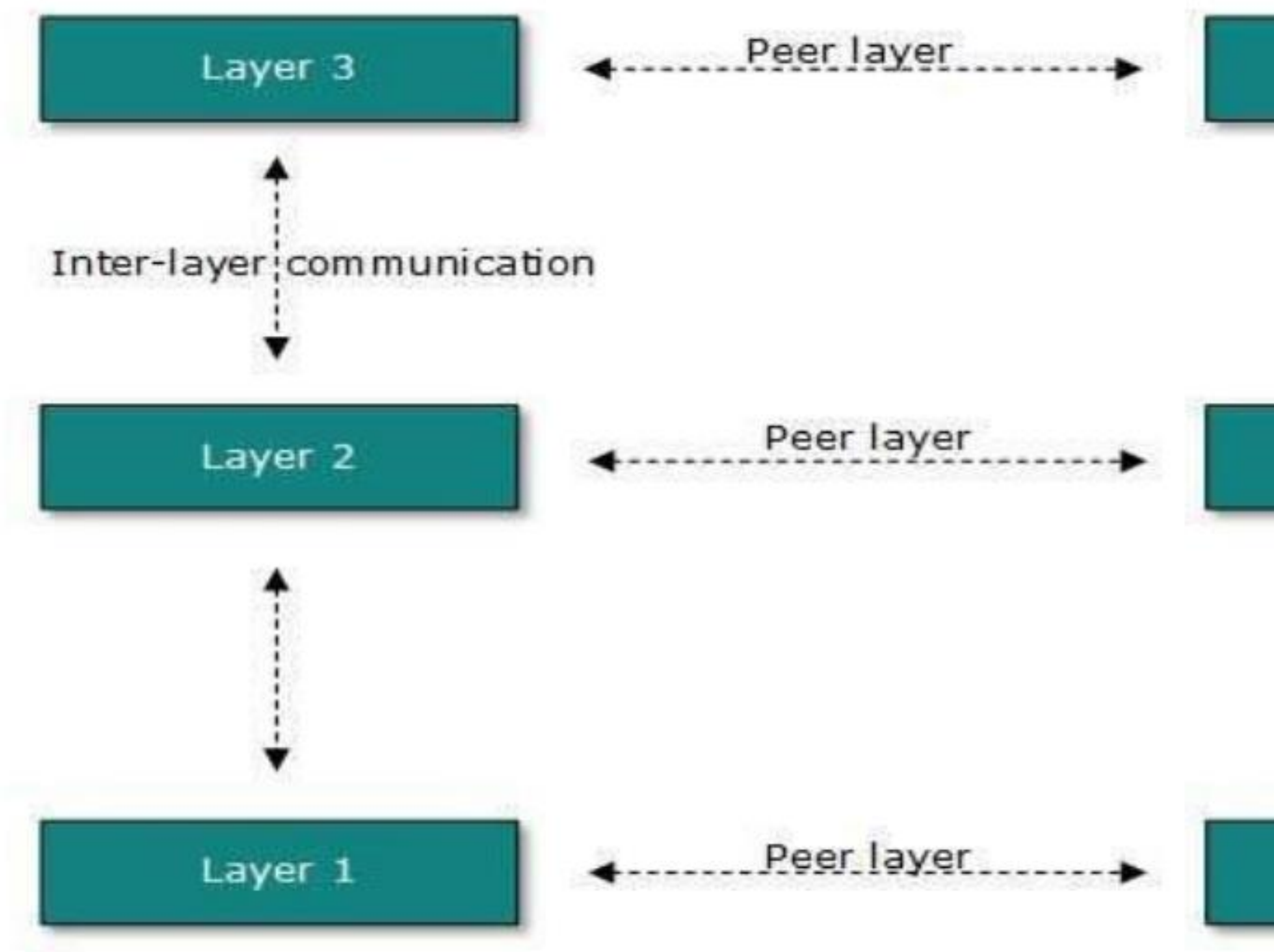


Figure 4.1 Layered Architecture

Benefits of layered architecture

1: It increases flexibility, maintainability, and scalability to modify and develop network services.

2: It enables teams to work on different parts of the application parallel with

minimal dependencies on other teams.

3: It enables us to maintain security along with privacy in an easier way.

4: It also helps you to test the components independently of each other.

5: Due to segmentation, it is possible to break complex problems into smaller

and more manageable pieces.

Peer to peer process

1: A peer-to-peer (P2P) network is a type of computer network in which all devices, or nodes, are considered equal peers and can act as both clients and servers.

2: This allows nodes to share files and resources with other nodes on the network without relying on a centralized server.

3: The P2P process involves node discovery, resource discovery, resource sharing, and dynamic and decentralized node participation through mechanisms like Distributed Hash Tables (DHTs).

Interfaces between layer

1: The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.

2: Each interface defines the information and services a layer must provide for the layer above it.

3: Well-defined interfaces and layer functions provide modularity to a network.

4: As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

Organization of the layers

1: The seven layers can be thought of as belonging to three subgroups: Layers 1, 2, and 3-physical, data link, and network-are the network support layers; they deal withthe physical aspects of moving data from one device to another.

2: Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated

software systems.

3: Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.

4: The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

Protocols

1: Protocols are what describe the rules that control horizontal communication, that is, conversations between processes that run at corresponding layers within the OSI Reference Model.

2: At every layer (except layer one) these communications ultimately take the form of some sort of message that is sent between corresponding software elements on two or more devices.

3: Since these messages are the mechanism for communicating information between protocols, they are most generally called protocol

data units (PDUs).

4:Each PDU has a specific format that implements the features and requirements of the protocol.

.OSI model	*protocols*
Application layer	DHCP, FTP, HTTPS, IMAP, LDAP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
Presentation layer	JPEG, MIDI, MPEG, PICT, TIFF
Session layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
transport layer	TCP, UDP
Network Layer	ICMP, IGMP, IPSec, IPv4,
Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC,Token Ring
Physical layer	Bluetooth, Ethernet, DSL, ISDN, 802.11, Wi-Fi

Encapsulation

1. Encapsulation is the process of adding headers and trailers to a data unit at each layer of the OSI model.

2: Each layer adds its own header and trailer, which are specific to that layer and provide services such as addressing, error checking, flow control, and sequencing.

3: At each layer, the header and trailer are stripped off before the data is passed to the layer above it, and this is called decapsulation.

4: The original data is reconstructed at the receiving end by stripping off the headers and trailers in reverse order.

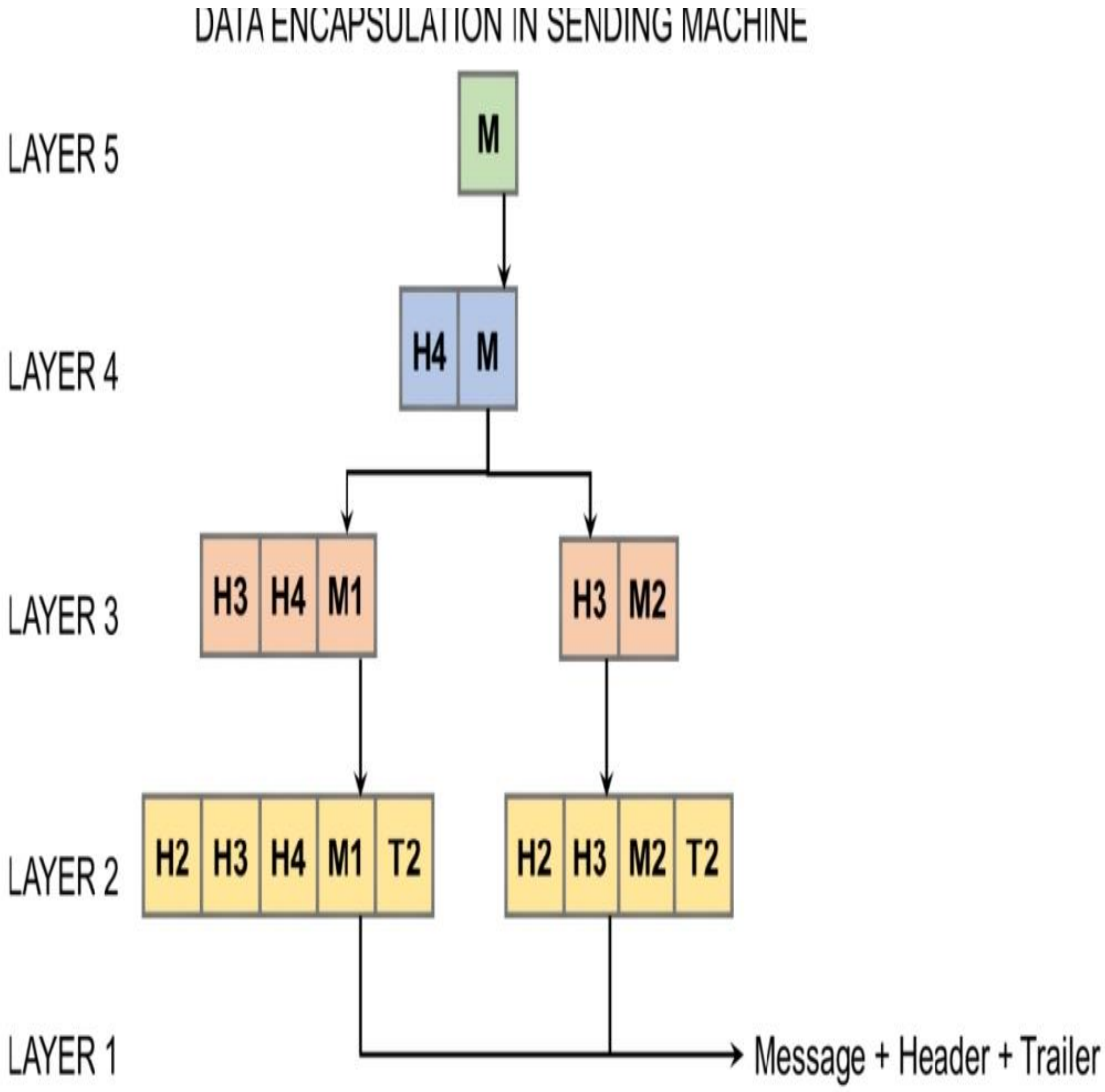


Figure 4.4: Five-layer stack for data encapsulation

Unit 5 (OSI Reference Model)

Layers of the OSI reference model

1: Model:OSI Reference Model was first introduced in the late 1970s.
2:'An open system is a set of protocols that allows any two different systems
to communicate regardless of their underlying architecture.
3: The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
4: The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.
5: The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.
6: The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
7: It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

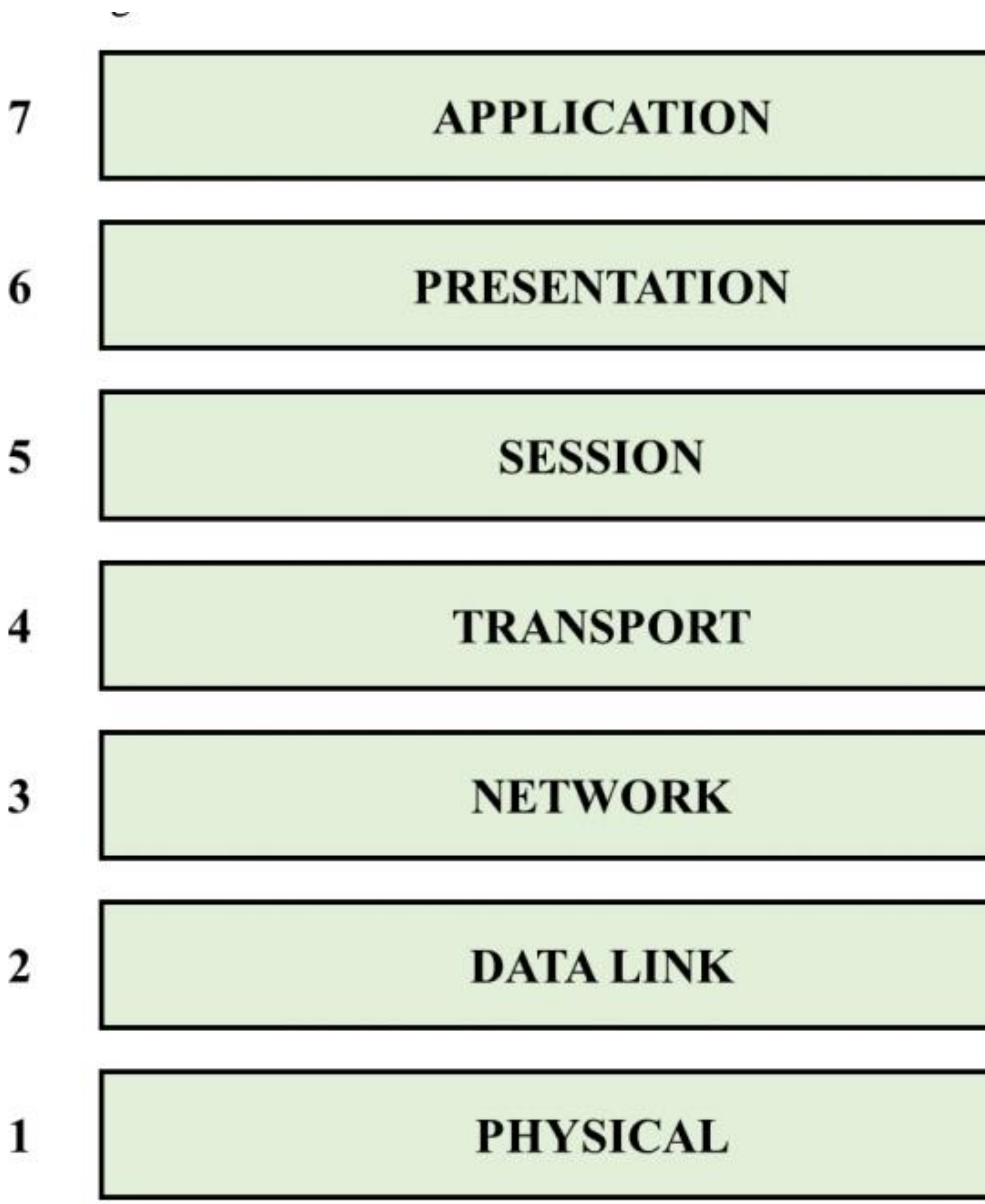


Figure 5.1: Seven layers of the OSI network model

Physical layer

1: The Physical Layer coordinates the functions required to carry a bit stream over a physical medium.

2: It deals with the mechanical and electrical specifications of the interface and transmission medium.

3: It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.

4: Figure 5.2 shows the position of thephysical layer with respect to the transmission medium and the data link layer.

5: Physical Layer is the lowest layer of the OSI model. It is related with the transmission and reception of the unstructured raw bit stream over a physicalmedium.

6: It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

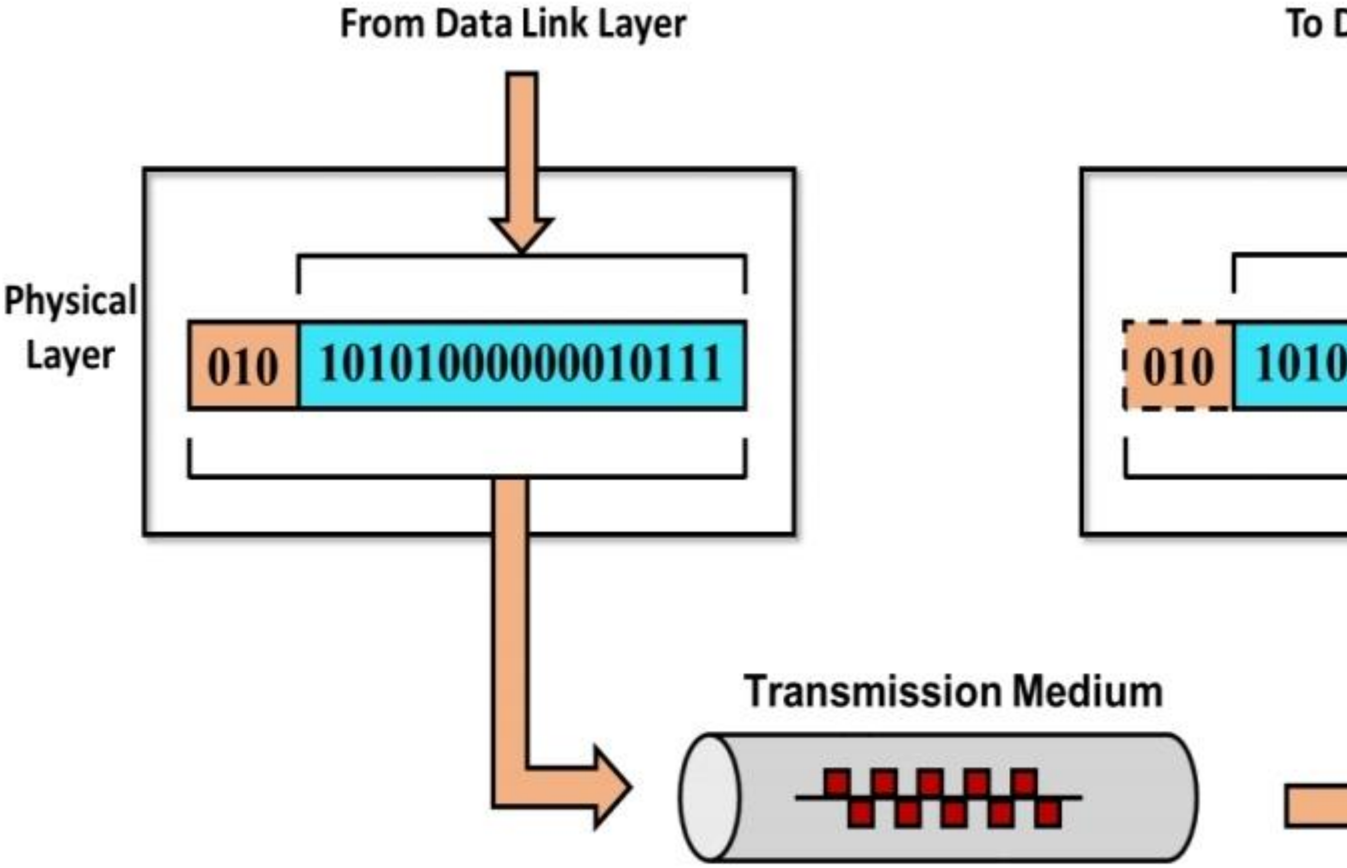


Figure 5.2:Physical Layer

Representation of bits (Data Encoding):

1: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization.

2: It determines:

•What signal state represents a binary 1.

•How the receiving station knows when a "bit-time" starts.

•How the receiving station delimits a frame.

Data rate: The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is howlong it lasts.

Synchronization of bits: The sender and receiver not only must use the same bit rate butalso must be synchronized at the bit level. In other words, the sender and the receiver clocksmust be synchronized.

Line configuration: The physical layer is concerned with the connection of devices to themedia. In a point-to-point configuration, two devices are connected through a dedicated *link.In* a multipoint configuration, a link is shared among several devices.

Physical topology: The physical topology defines how devices are connected to make anetwork. Devices can be connected by using a mesh topology, a star, a ring topology, a bustopology, or a hybrid topology.

Transmission Technique/Mode: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signalling.The physical layer also defines the direction of transmission betweentwo devices: simplex, half-duplex, or full-duplex.

Physical medium attachment, accommodating various possibilities in the medium:

- Will an external transceiver (MAU) be used to connect to the medium?
- How many pins do the connectors have and what is each pin used for?

Physical Medium Transmission: transmits bits as electrical or optical signals appropriate for the physical medium, and determines:

- What physical medium options can be used?
- How many volts/db should be used to represent a given signal state, using a given physical medium?

Data link layer

1: Data Link Layer provides error-free transfer of data frames from one node to

another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link.

2: To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link

between two nodes.

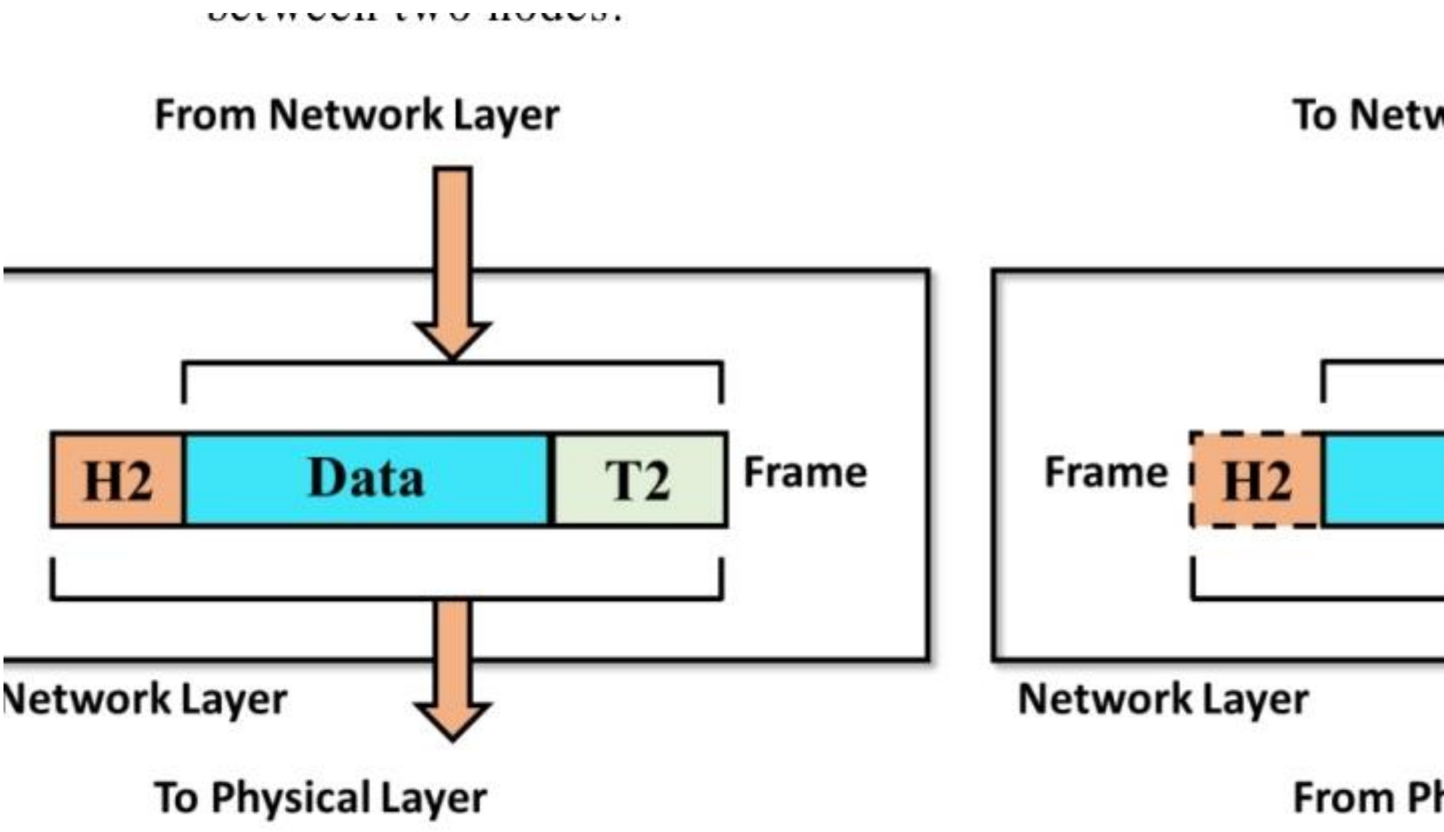


Figure 5.2: Data link Layer

Link Establishment and Termination: establishes and terminates the logical link between two nodes.

*Framing:*transmits/receives frames sequentially.The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

Frame Acknowledgment:

provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame Delimiting: creates and recognizes frame boundaries.

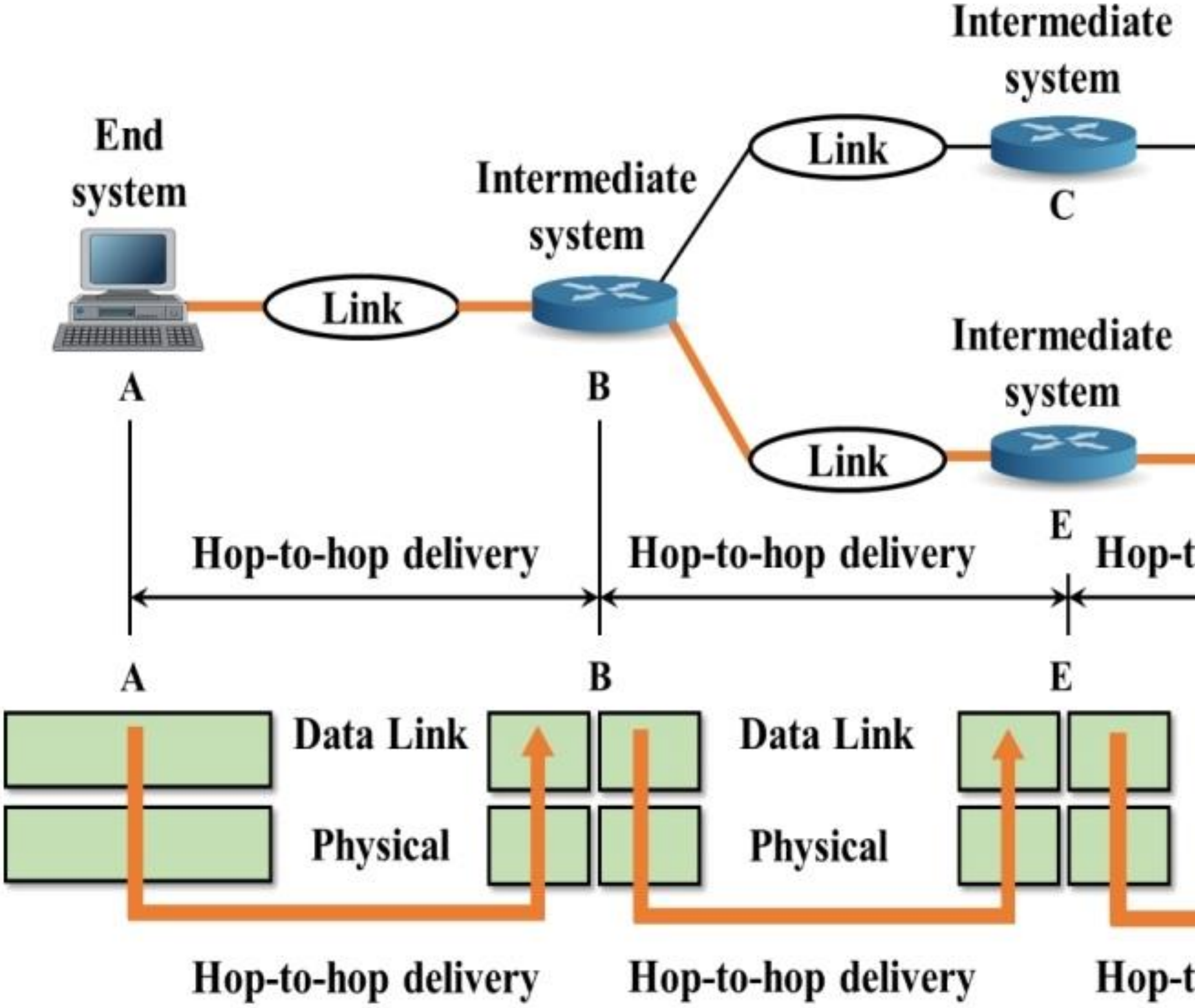


Figure 5.3Hop-to-hop delivery

Network Layer

1: The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

2: Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

3: Figure 5.4 shows the relationship of the network layer to the data link and transport layers.

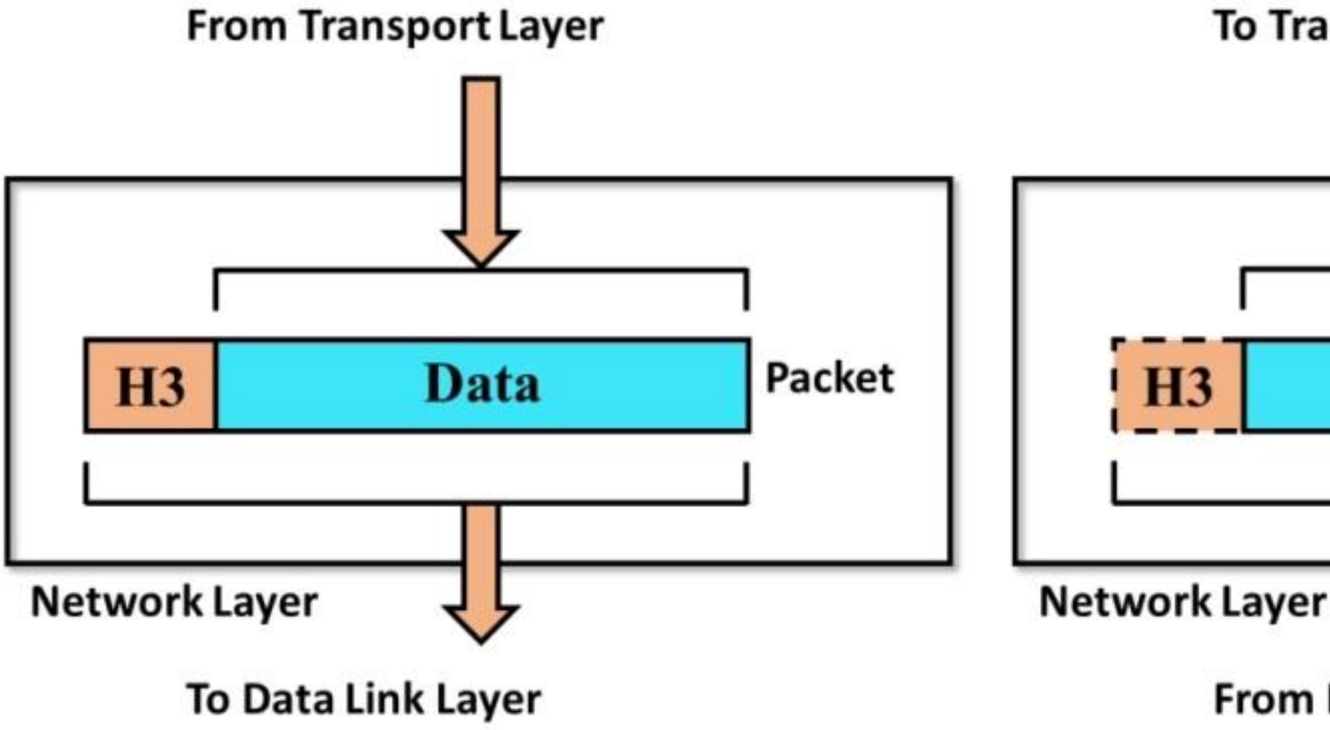


Figure 5.4: Network Layer

Logical Addressing:

1: The physical addressing implemented by the data link layer handles theaddressing problem locally.

2: If a packet passes the network

boundary, we need anotheraddressing system to help distinguish the source and destination systems.

3: The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

Routing

When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final *destination.One* of the functions of the network layer is to provide this mechanism.

Transport layer

1: The transport layer is responsible for process-to-process delivery of the entire message.

2: A process is an application program running on a host.

3: Whereas the network layer oversees source-to-destination delivery of

individual packets, it does not recognize any relationship between those packets.

4: It treats each one independently, as though each piece belonged to a separate

message, whether or not it does.

5: The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Figure 5.6 shows the relationship of the transportlayer to the network and session layers.

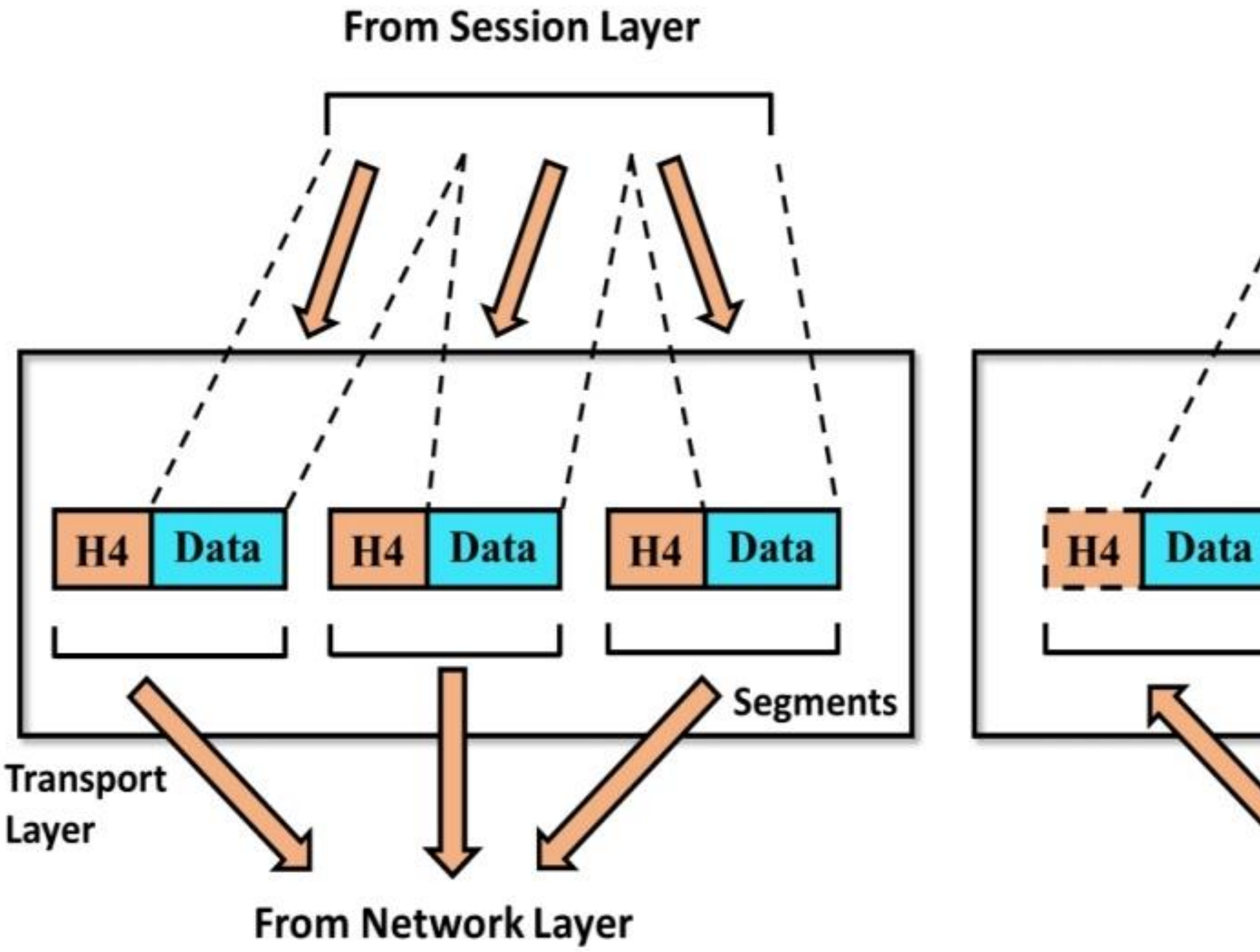


Figure 5.6: Transport Layer

Service-point addressing

1: Computers often run several programs at the same time.

2: For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.

3: The transport layer header must therefore include a type of address

called a service-point address (or port address).

Segmentation and reassembly

1: A message is divided into transmittable

segments, with eachsegment containing a sequence number.

2: These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets thatwere lost in transmission.

Flow control: Like the data link layer, the transport layer is responsible for

flow control.However, flow control at this layer is performed end to end rather

than across a single link.

Error control:

1: Like the data link layer, the transport layer is responsible for error control.

2: However, error control at this layer is performed process-toprocess rather than across a singlelink.

3: The sending transport layer makes sure

that the entire message arrives at the receivingtransport layer without error

(damage, loss, or duplication).

4: Error correction is usually achieved through retransmission.

Session layer

1: The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes.

2: The session layer is the network dialog controller.

3: It establishes, maintains, and synchronizes the interaction among communicating systems.

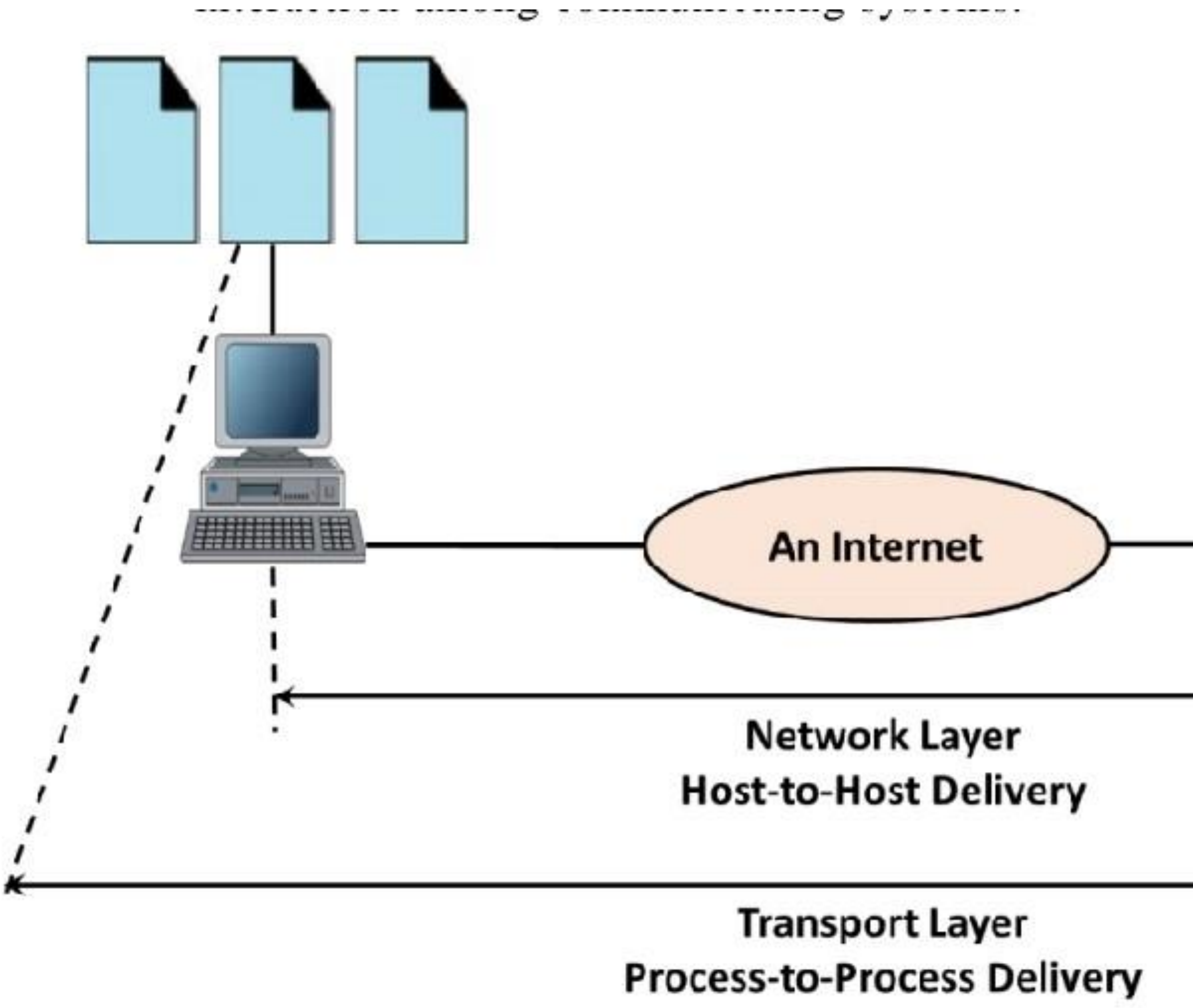
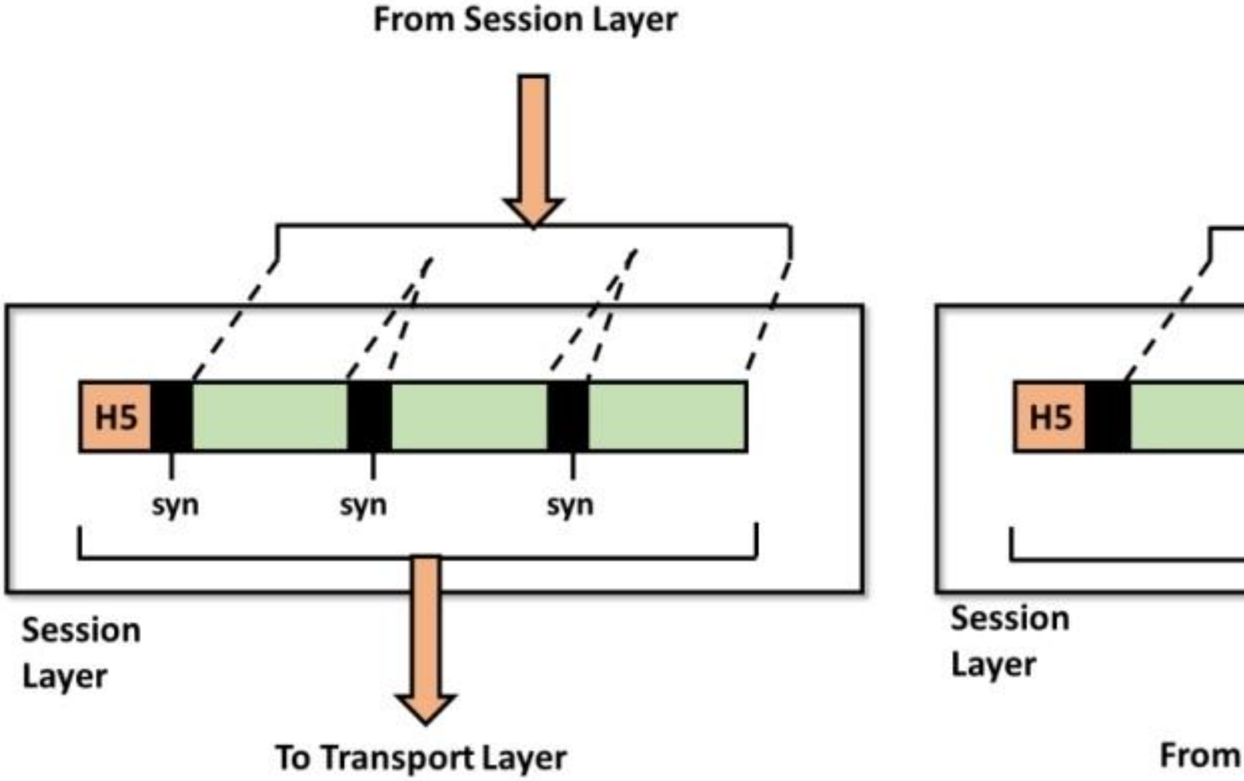


Figure 5.7: Reliable process-to-process delivery of a messag



Dialog control:

1: The session layer allows two systems to enter into a dialog.

2: It allows the communication between two processes to take place in either half

duplex or full-duplex mode.

Synchronization:

1: The session layer allows a process to add checkpoints, or synchronizationpoints, to a stream of data.

2: For example, if a system is sending

a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently.

3: In this case, if a crash happens during thetransmission of page 523, the only

pages that need to be resent after system recovery are pages501 to 523. Pages previous to 501 need not be resent.

Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Figure 5.9 shows the relationship between thepresentation layer and the application and session layers.

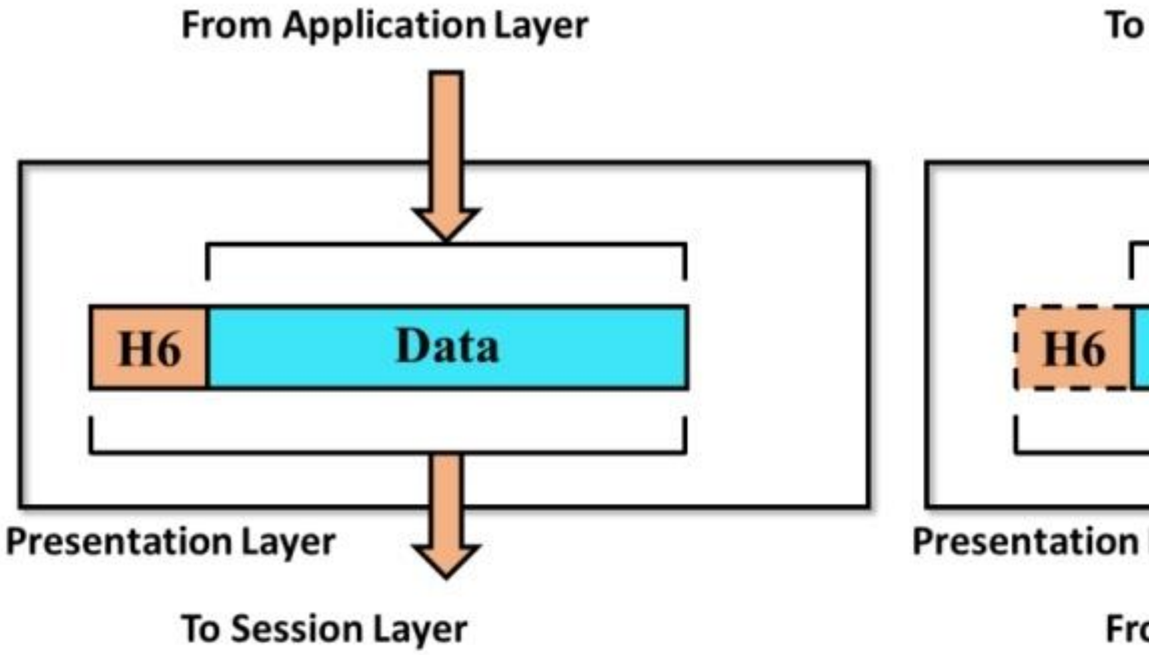


Figure 5.9 Presentation Layer

<u>*Translation*</u>:

1: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on.

2: The information must bechanged to bit streams before being transmitted.

3: Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.

4: The presentation layer at the sender changes the information from its

sender-dependent format into a common format.

5: The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption:

1: To carry sensitive information, a system must be able to ensure privacy.

2: Encryption means that the sender transforms the original information

to another form and sends the resulting message out over the network.

3: Decryption reverses the original process to transform the messageback to its

original form.

Compression:

1: Data compression reduces the number of bits contained in the information. **2:** Data compression becomes particularly important in the transmission of multimedia such as text,audio, and video.

Application Layer

1: The application layer enables the user, whether human or software, toaccess the network.

2: It provides user interfaces and support for services such as electronic mail,remote file access and transfer, shared databasecmanagement, and other types of distributed information services.

Figure 5.10 shows the relationship of the application layer to the user and the

presentation layer.

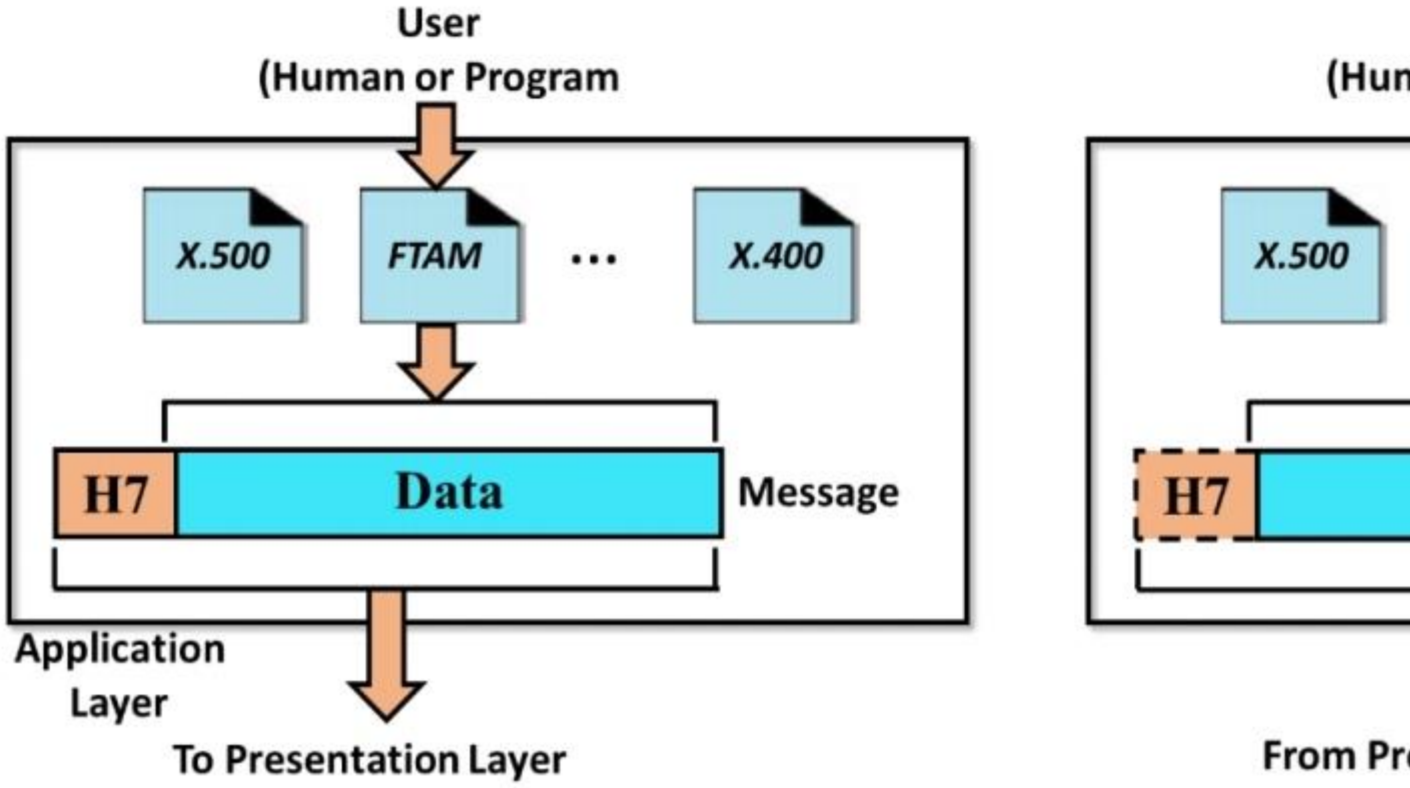


Figure 5.10: Application Layer

File transfer, access, and management:

This application allows a user to

access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Mail services: This application provides the basis for e-mail forwarding and storage.

Directory services: This application provides distributed database sources and access for global information about various objects and services.

Unit 6 (TCP / IP Suite)

Introduction

1: TCP/IP means Transmission Control Protocol and Internet Protocol.
2: Current internet architecture uses TCP/IP network model.
3: Protocols are set of rules used to control all the probable communication on the network.
4: The movement of data between the source and destination over the internet is described by these protocols.
5: These protocols provide simple naming and addressing schemes.
6: TCP/IP reference model was developed to:
(a): Support a flexible architecture byeasily adding more computersin a network.
(b): To keep network robust.
(c): To keep connections intact until the source and destination machines are functioning.

TCP/IP addressing mechanism in the internet

1: An IP address is a 32-bit numeric address, expressed in dotted decimal format (e.g., 192.168.0.1).

2: This IP address serves as the device's "Internet address," allowing it to be identified and located on the network.

3: IP addresses are typically assigned by Internet Service Providers (ISPs) to their customers.

4: There are two versions of the IP protocol currently in use: IPv4 and IPv6.

5: IPv4 addresses are the traditional 32-bit addresses, while IPv6 addresses are 128-bit addresses, designed to provide a much larger address space.

6: In addition to IP addresses, the TCP/IP addressing mechanism also includes a system of hierarchical domain names.

7: Domain names provide an easier-to-remember way of identifying devices on the Internet.

IP address notations

There are two prevalent notations to show an IPv4 address: Binary notation and Dotted-decimal notation.

Binary Notation:

1: In binary notation, the IPv4 address is displayed as 32 bits.

2: Each octet is often referred to as a byte.

3: So it is common to hear an IPv4 address referred to as a 32-bit address or a4-byte address.

4:The following is an example of an IPv4 address in binary notation:

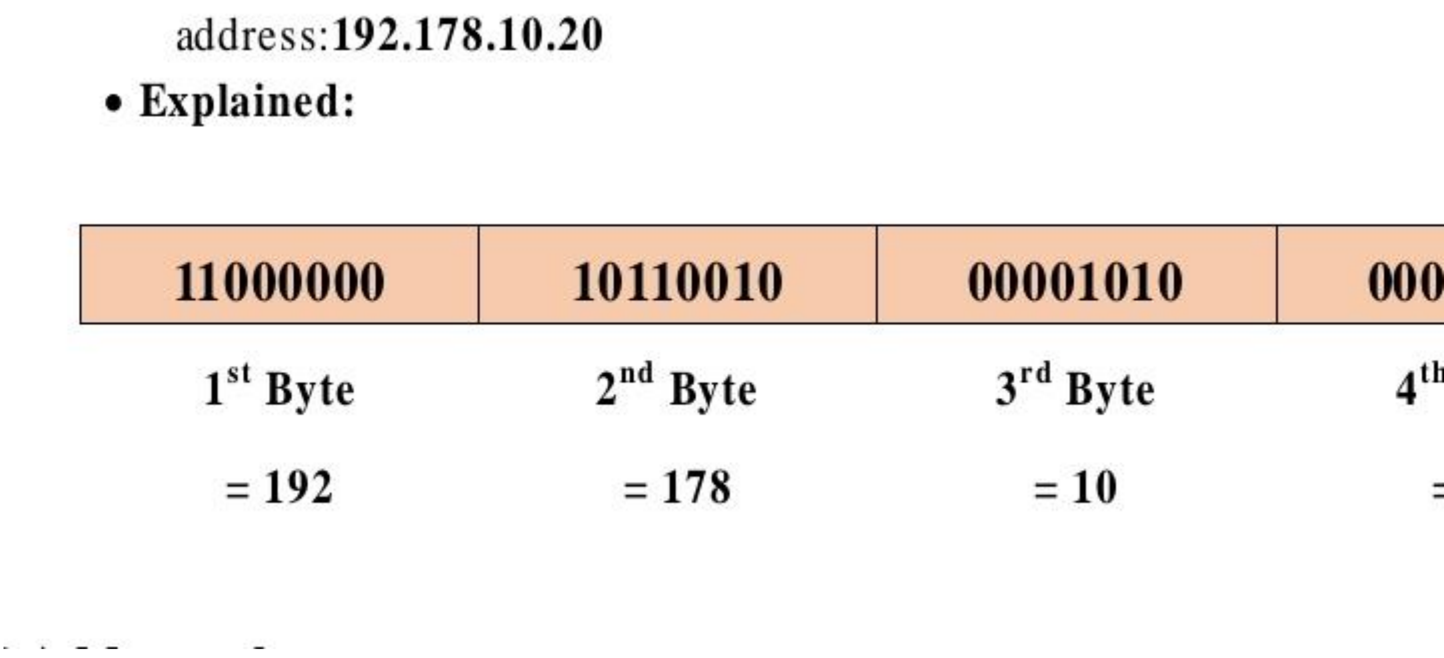
1100000010110010 0000101000010100.

Dotted-Decimal Notation:

1: To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot)separating the bytes.

2: Each byte is identified by a decimal number in the range [0 – 255].

3: The following is the dotted decimal notation of the above address: *192.178.10.20*



address:**192.178.10.20**

- **Explained:**

11000000	10110010	00001010	000
1st Byte	2nd Byte	3rd Byte	4th
= 192	= 178	= 10	=

IP address classes

Finding the address class:

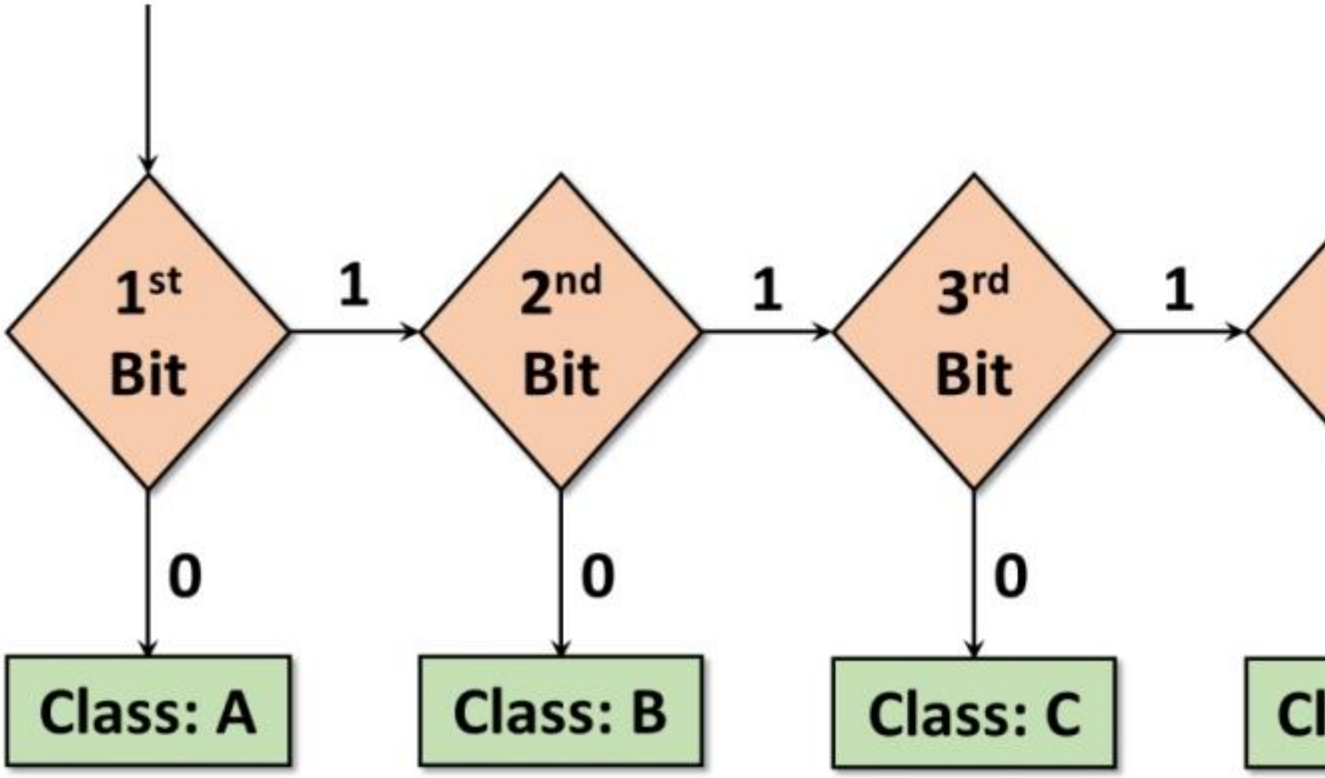


Fig: Finding Address Class

Classes and Blocks:

Class	Subnet Mask Decimal	No. of Hosts per Network	No of Networks	Sta
A	255.0.0.0	16 Million	127	1.0.0.0 -
B	255.255.0.0	6500	1600	128.0.0.
C	255.255.255.0	254	2 Million	192.0.0.
D	Reserved for multicast groups			224.0.0.

class A:

1: The high-order (First) bit in a class – Address is always set to zero.

2: The next seven bits complete the network ID.

3: The remaining 24 bits represent the host ID.

4: This allows for 128 networks and 16,777,214 hosts per network.

5: In this 7 bits are used for network field and 24 bits for host field.

6: Class A IP address range includes 1.0.0.0 to 127.255.255.255

Class B:

1: Class B addresses are assigned to medium-sized to large-sized networks.

2:The two high-order bits in a class B address are always set to binary 1 0.

3: The next 14 bits complete the network ID.

4: The remaining 16 bits represent the host ID.

5: This allows for 16,384 networks and 65,534 hosts per network.

6: Class B IP address range includes 128.0.0.0 to 191.255.255.255

Class C:

1: Class C addresses are used for small organizations with a small number of attached hosts or routers.

2: The three high-order bits in a class C address are always set to binary 1 1 0.

3: The next 21 bits complete the network ID.

4: The remaining 8 bits (last octet) represent the host ID.

5: This allows for 2097152 networks and 256 hosts per network.

6: Class C IP address range includes 192.0.0.0 to 223.255.255.255.

Class D:

1: Class D addresses are reserved for IP multicast addresses.

2: The four high-order bits in a class D address are always set to binary 1 1 1 0.

3: The remaining bits recognize hosts.

4: Class D IP address range includes 224.0.0.0 to 239.255.255.255

Class E:

1: Class E is an experimental address that is reserved for future use.

2: The high-order bits in a class E address are set to binary 1111.

3: Class E IP address range includes 240.0.0.0 to 255.255.255.255

Netid and Hostid

1: In classful addressing, an IP address in class A, B, or C is divided into Netid and Hostid.

2: These parts are of varying lengths, depending on the class of the address.

3: the concept does not apply to classes D and E.

4: In class A, one byte defines the Netid and three bytes define the Hostid.

5: In class B, two bytes define the Netid and two bytes define the Hostid.

6: In class C, three bytes define the Netid and one byte defines the Hostid.

Mask

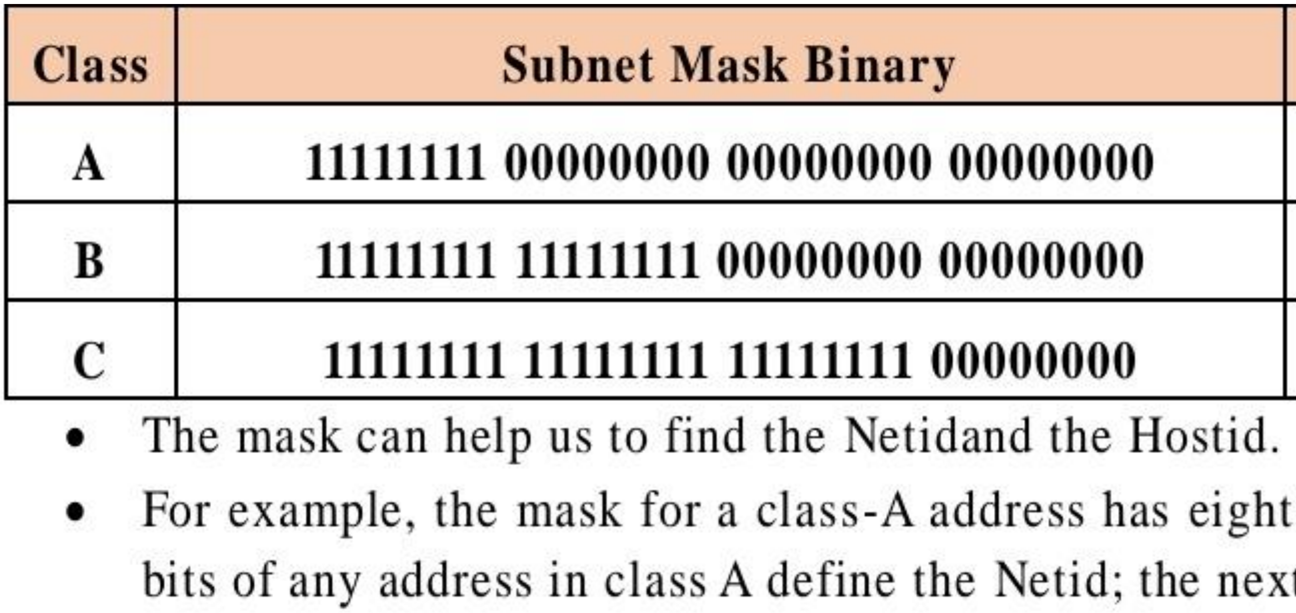
1: Although the length of the Netid and Hostid (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask/natural masks), a 32-bit number made of contiguous 1‘s followed by contiguous 0‘s.

2: The masks for classes A, B, and C are shown in Table.

3: The concept does not apply to classes D and E.

4: The mask can help us to find the Netidand the Hostid.

5: For example, the mask for a class-A address has eight 1s, which means the first 8 bits of any address in class A define the Netid; the next 24 bits define the Hostid.



Class	Subnet Mask Binary
A	11111111 00000000 00000000 00000000
B	11111111 11111111 00000000 00000000
C	11111111 11111111 11111111 00000000

- The mask can help us to find the Netidand the Hostid.
- For example, the mask for a class-A address has eight bits of any address in class A define the Netid; the next

---

Subnetting

1: If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.

2: Subnetting increases the number of 1‘s in the mask.

3: To create multiple logical networks that exist within a single Class A, B, or C network.

4: If subnet masking is not done, only one network from Class A, B, or C network can be used, which is unrealistic.

5: The subnet mask follows two rules:

(a): If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies the network.

(b): If a binary bit is set to a 0 (or off) in a subnet mask, the corresponding bit in the address identifies the host.

Supernetting

1: The most of the class A and class B addresses were exhausted; however, there was still a huge demand for midsize blocks.

2: The size of a class C block with a maximum number of 256 addresses did not satisfy the needs of most organizations.

3: One solution for this problem is supernetting.

4: In supernetting, an organization can combine several class C blocks to create a larger range of addresses.

5: In other words, several networks are combined to create a supernetwork or a supernet.

6: An organization can apply for a set of class C blocks instead of just one.

7: For example, an organization that needs 1000 addresses can be granted four contiguous class C blocks.

8: The organization can then use these addresses to create one supernetwork.

9: Supernetting decreases the number of 1‘s in the mask.

10: For example, If an organization is given four class C addresses, the mask changes from 24 to 22.

Address Depletion

1: The flaws in classful addressing scheme combined with the fast growth of the Internet lead to the near depletion of the available addresses.
2: Yet the number of devices on the Internet is much less than the 232 address space.
3: We have run out of class A and B addresses, and a class C block is too small for most midsize organizations.
4: One solution that has alleviated the problem is the idea of classless addressing.

Classless Addressing

1: To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented.

2: In this scheme, there are no classes, but the addresses are still granted in blocks.

Address Blocks

1: In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses.

2: The size of the block (the number of addresses) varies based on the nature and size of the entity.

2: For example, a household may be given only two addresses; a large organization may be given thousands of addresses.

3: An ISP, as the Internet service provider, may be given thousands of addresses based on the number of customers it may serve.

Restriction:

To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1. The addresses in a block must be contiguous, one after another.

2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8 ...).

3. The first address must be evenly divisible by the number of addresses.

TCP/IP Transport Layer

1: Also known as host-to-host layer.

2: This layer is concerned with the transmission of the data.

3: The two main protocols that operate at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

4: TCP is reliable transmission protocol and it guarantees that the proper data transfer will take place.

5: UDP is not designed to be reliable or guarantee data delivery.

Functions of Transport Layer

1: Service point addressing: **-** Delivery is from specific process on computer to specific process on another computer. For this transport layer uses port addresses.

2: Segmentation and reassemble: **-**Each segment of a message contains a sequence number which is used to reassemble the message correctly.

3: Connection control:**-**Logical connection is created between source and destination for the duration of complete message transfer.

4: Flow control:**-**Flow control is performed end to end.

5: Error control:**-**Error control is performed process to process. It ensures that entire message arrives at receivers transport layer without error (damage or loss or duplication).

6: Error correction is done by retransmission.

Layered structure of the TCP/IP model

1: The TCP/IP model is a networking protocol suite that consists of four layers, each of which is responsible for a different aspect of communication over the network. The four layers, in order from top to bottom, are:

Application layer: This layer is responsible for providing high-level services to applications, such as email, file transfer, and web browsing. Protocols at this layer include HTTP, FTP, SMTP, and Telnet.

Transport layer: This layer is responsible for establishing end-to-end connections between devices and ensuring that data is delivered error-free and in the correct order. Protocols at this layer include TCP and UDP.

Internet layer: This layer is responsible for routing packets across multiple networks and finding the best path for data to travel from the sender to the receiver. The primary protocol at this layer is IP.

Network access layer: This layer is responsible for transmitting data between devices on the same physical network. Protocols at this layer include Ethernet, Wi-Fi, and Token Ring.

TCP/IP protocol suite

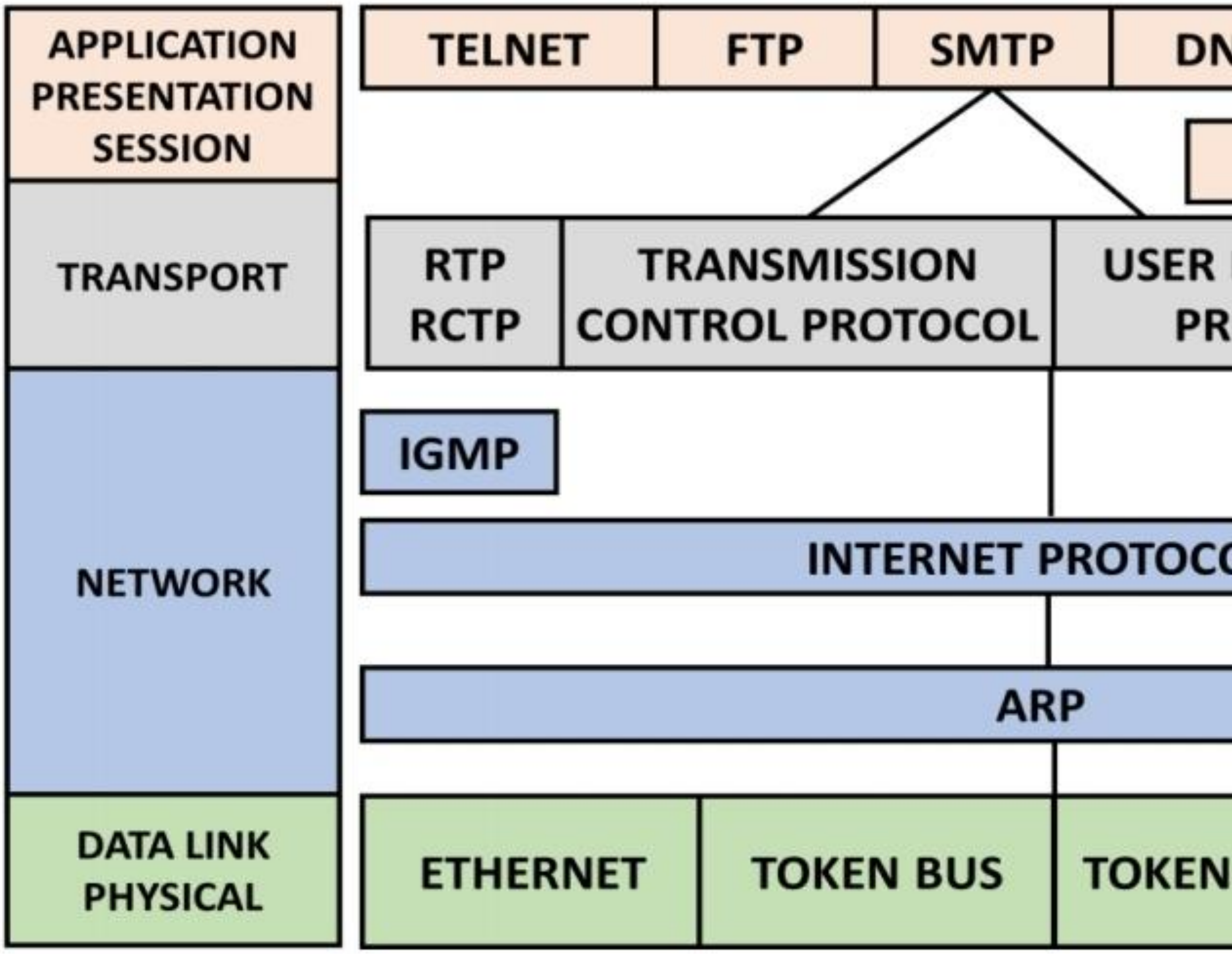


Fig: TCP/ IP Protocol Suite

---

slip (serial line internet protocol):

1: it designed to work over serial ports and modem connections.

2: defines a sequence of bytes that frame ip packets on a serial line.

3: commonly used for point-to-point serial connections running tcp/ip.

4: it is designed to transmit signals over a serial connection and has very low overhead.

5. data transmission with slip is very simple.

6. this protocol sends a frame composed only of data to be sent followed by an end of transmission

character (the end character, the ascii code 192).