Data Communication And Networking

Chapter 1:

Transferring data over a transmission medium between two or more devices, systems, or places is known as data communication.

Characteristics of Data Communication:

1. Delivery: Ensures data reaches the intended recipient without loss.
2. Accuracy: Guarantees that the received data matches the sent data, minimizing errors.
3. Timeliness: Requires data to be delivered within a specific time frame, crucial for real-time applications.
4. Jitter: Refers to the variability in packet arrival times, which can affect the quality of real-time communications.

Components of Data Communication

A communication system is made up of the following components:

1. **Message:** A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.
2. **Sender:** It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
3. **Receiver:** It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
4. **Transmission Medium :** Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
5. **Protocol:** When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless.

Data Flow:

Data can flow in different ways of data communication or transmission modes in networking. Those can be defined as one device to another or two devices can communicate in **Simplex, Half-Duplex, or Full-Duplex.**

Network Criteria

A Network is a group of connected devices capable of communicating. The device can be a computer, printer, or scanner that either receives or transmits data.

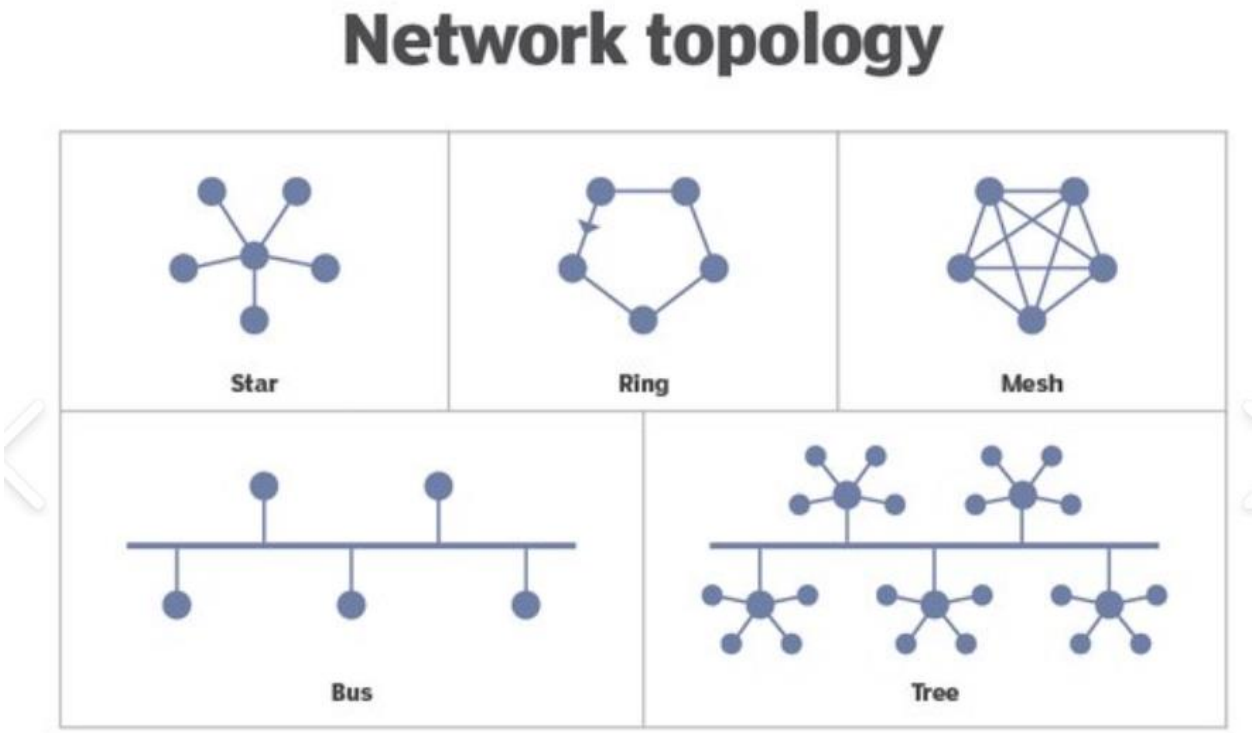
There are a lot of criteria that make a network better than others, but; there are three basic yet important criteria to be fulfilled for a network:

1. Performance
2. Reliability
3. Security

Topology:

Topology refers to the arrangement or layout of different elements (nodes, devices, and connections) in a network. It defines how devices are interconnected and how data flows between them. There are several common types of network topologies:

1. **Bus Topology**: All devices share a single communication line (the bus). Data travels in both directions along the bus, but if the bus fails, the entire network goes down.
2. **Star Topology**: All devices are connected to a central hub or switch. This topology is easy to manage and troubleshoot; if one connection fails, it does not affect the others.
3. **Ring Topology**: Each device is connected to two other devices, forming a circular pathway for data. Data travels in one direction, and a failure in one device can disrupt the entire network.
4. **Mesh Topology**: Every device is interconnected, allowing multiple pathways for data. This topology is highly reliable and resilient, as it can continue to function even if one or more connections fail.
5. **Tree Topology**: A hybrid of star and bus topologies, it features a hierarchical structure with a central root node connected to multiple levels of nodes. It allows for easy expansion but can be complex to manage.



Chapter 2:

Network Models

A **network model** refers to a conceptual or mathematical framework used to describe, analyze, and predict the behavior of complex networks.

Layered tasks in data communication refer to the concept of breaking down complex communication tasks into simpler, more manageable layers. This concept is widely used in networking to create modular and interoperable systems, where each layer is responsible for a specific part of the communication process. The two most common models used to describe layered tasks in data communication are the **OSI (Open Systems Interconnection) model** and the **TCP/IP model**.

OSI Model (7 Layers)

The OSI model defines seven layers, each with distinct responsibilities. Here's an overview of the layered tasks in the OSI model:

1. **Physical Layer**:

    - **Task**: Deals with the physical transmission of data over the network.
    - **Function**: Defines the hardware equipment, cabling, signaling, data rates, and how bits are transmitted over a medium (electrical, optical, or radio signals).
    - **Example**: Cables, switches, hubs, network interface cards (NICs).
2. **Data Link Layer**:
    - **Task**: Ensures reliable transmission of data across the physical link.
    - **Function**: Deals with frame creation, MAC (Media Access Control), error detection and correction, and flow control.
    - **Example**: Ethernet, Wi-Fi (802.11), PPP (Point-to-Point Protocol).
3. **Network Layer**:
    - **Task**: Handles logical addressing and routing of data.
    - **Function**: Provides the mechanisms for delivering packets across networks and deciding the best path to reach the destination.
    - **Example**: IP (Internet Protocol), routers.
4. **Transport Layer**:
    - **Task**: Provides reliable or unreliable delivery of data between hosts.
    - **Function**: Breaks large data streams into smaller packets, ensures error-free delivery, manages flow control, and reassembles packets into their original order.
    - **Example**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
5. **Session Layer**:
    - **Task**: Manages sessions or connections between applications.
    - **Function**: Establishes, maintains, and terminates sessions between devices (communication exchanges). Manages the dialog and synchronization between applications.
    - **Example**: NetBIOS, PPTP (Point-to-Point Tunneling Protocol).
6. **Presentation Layer**:
    - **Task**: Translates, encrypts, and compresses data.
    - **Function**: Ensures that data sent by the application layer is readable by the destination application. Converts data into a format usable by the application, encrypts/decrypts data, and compresses/decompresses it.
    - **Example**: SSL (Secure Socket Layer), TLS (Transport Layer Security), data encoding formats (e.g., ASCII, JPEG, GIF).
7. **Application Layer**:
    - **Task**: Provides network services directly to user applications.
    - **Function**: Defines protocols for communication between applications, allowing network services such as file transfer, email, and web browsing.
    - **Example**: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name System), SMTP (Simple Mail Transfer Protocol).

TCP/IP Model (4 Layers)

The **TCP/IP model** is more practical and condensed compared to the OSI model. It consists of four layers, and its layered tasks are as follows:

1. **Link Layer (Network Interface Layer)**:
    - **Task**: Handles communication between adjacent network nodes (similar to OSI's Physical and Data Link layers).
    - **Function**: Responsible for the physical transmission of data, addressing, and access control.
    - **Example**: Ethernet, Wi-Fi, ARP (Address Resolution Protocol).
2. **Internet Layer**:
    - **Task**: Manages logical addressing and packet forwarding across networks (similar to OSI's Network layer).
    - **Function**: Ensures that packets are routed across network boundaries using IP addresses. This layer also handles fragmentation and reassembly of packets.
    - **Example**: IP, ICMP (Internet Control Message Protocol).
3. **Transport Layer**:
    - **Task**: Provides end-to-end communication, reliable or unreliable.
    - **Function**: Similar to the OSI model, this layer ensures error-free, ordered data transmission (TCP) or fast, connectionless communication (UDP).
    - **Example**: TCP, UDP.
4. **Application Layer**:
    - **Task**: Provides communication services directly to applications.
    - **Function**: Combines the responsibilities of OSI's Application, Presentation, and Session layers. This layer manages communication protocols that allow users to interact with the network (web browsing, email, file transfer, etc.).
    - **Example**: HTTP, FTP, SMTP, DNS, Telnet.

The **DoD (Department of Defense) model**, also known as the **TCP/IP model**, is a conceptual framework for communication protocols that are used in networking.

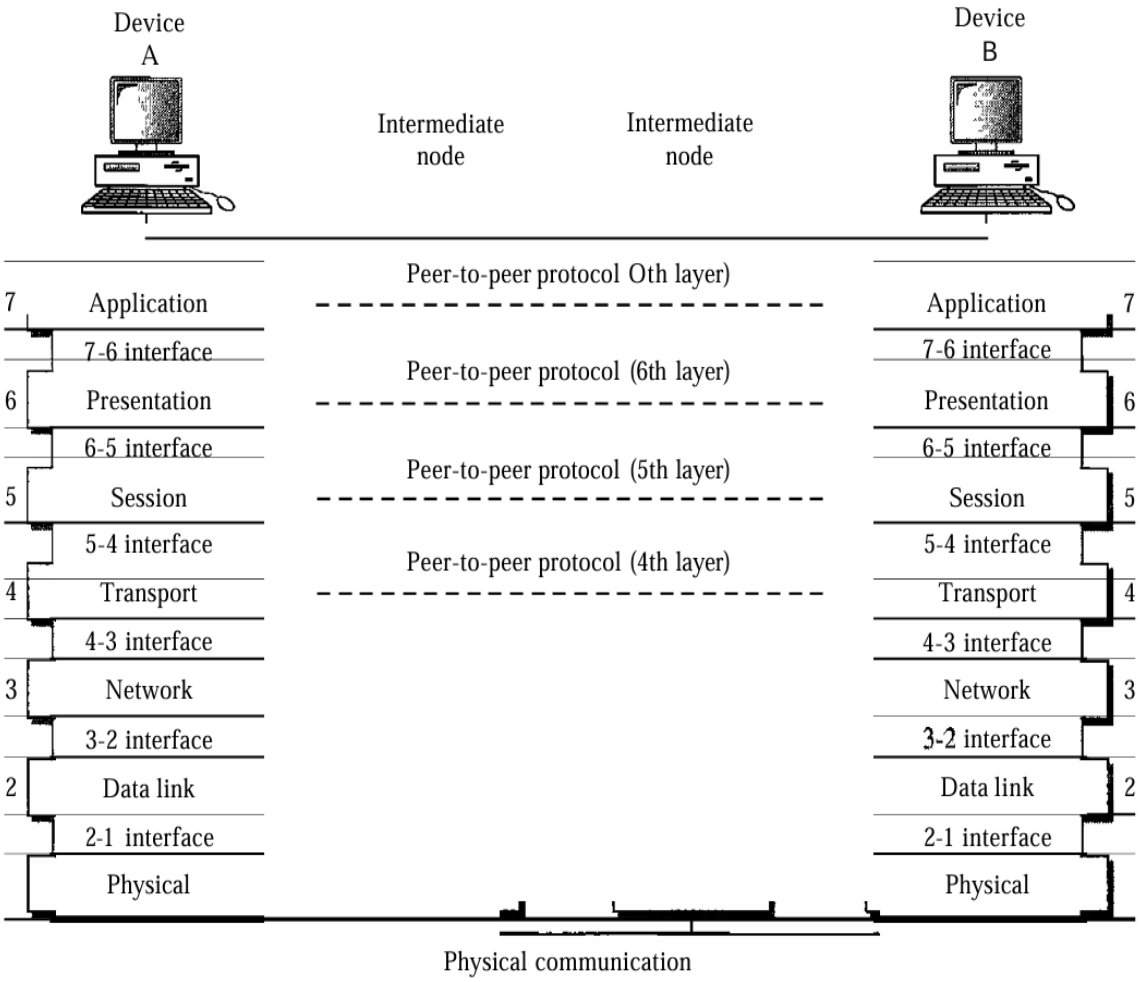
Layers of the DoD (TCP/IP) Model:

1. **Network Interface (Link) Layer**:
    - **Task**: Handles the hardware-to-hardware communication over a physical link.
    - **Function**: Manages physical transmission of data, access to the network medium, and delivery of frames within the same local network.
2. **Internet Layer**:
    - **Task**: Handles logical addressing, routing, and packet forwarding between networks.
    - **Function**: Ensures that data can travel from the source to the destination across multiple networks (inter-network communication) by assigning IP addresses and routing packets to their destination.
3. **Transport Layer**:
    - **Task**: Provides reliable or unreliable end-to-end communication between two hosts.

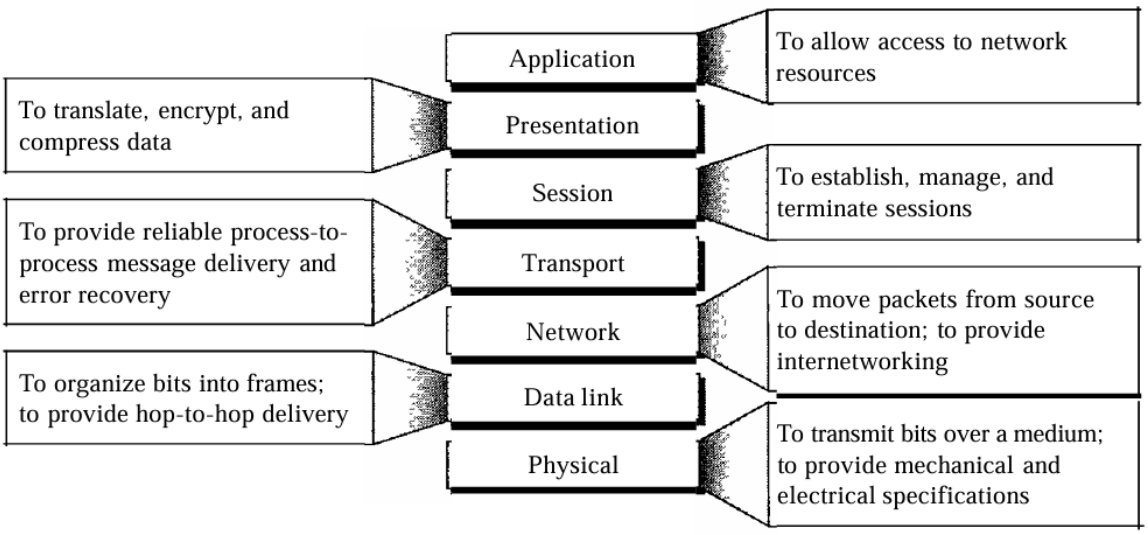
- **Function**: Manages flow control, error detection, retransmission, and ordering of data. It ensures that data is delivered reliably (TCP) or quickly with less overhead (UDP).

4. **Application Layer**:
   - **Task**: Provides network services directly to applications and end-users.
   - **Function**: Defines protocols that applications use to communicate over the network, enabling tasks like web browsing, email, file transfer, etc.

The interaction between layers in the OSI model:



Summary of Layers :



Addressing:

In data communication, "addressing" refers to the method by which systems or devices identify each other to ensure proper routing of data between sender and receiver. There are several key types of addressing used in different layers of data communication:

1. Physical Addressing (MAC Addressing)

- **Layer**: Data Link Layer (Layer 2 of the OSI model)
- **Purpose**: Identifies devices at the hardware level within a local network.

2. Logical Addressing (IP Addressing)

- **Layer**: Network Layer (Layer 3 of the OSI model)
- **Purpose**: Provides globally unique addresses for devices across different networks. This addressing system helps in routing data across multiple networks, such as the internet.

3. Port Addressing

- **Layer**: Transport Layer (Layer 4 of the OSI model)
- **Purpose**: Identifies specific processes or applications running on a device, allowing multiple applications to use the network simultaneously.

4. Service Addressing

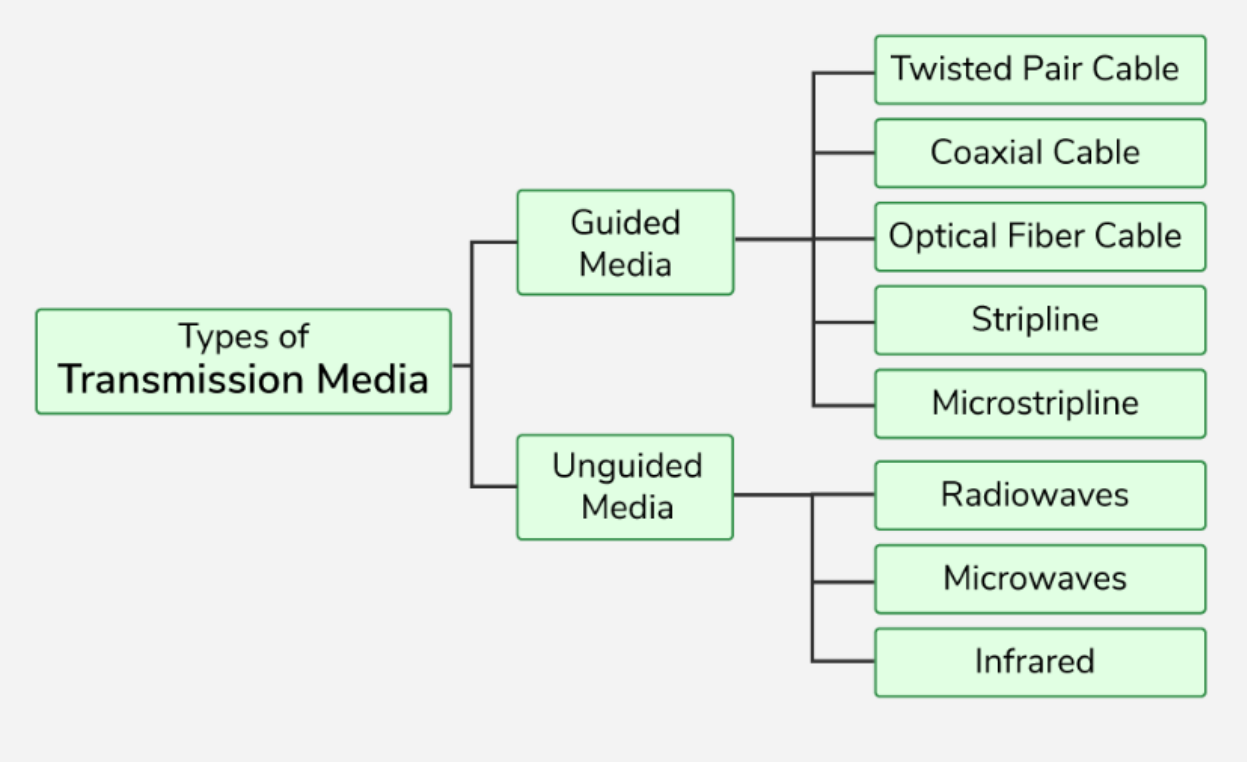
- **Layer**: Application Layer (Layer 7 of the OSI model)
- **Purpose**: Helps identify specific services on a network. It operates at a higher level, interacting with protocols that manage the format and reliability of data.

Chapter 7:

Transmission Media

Transmission media refer to the physical pathways through which data is transmitted from one device to another within a network.

A transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media: **Guided media** is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

- High Speed
- Secure
- Used for comparatively shorter distances

2. Unguided Media

It is also referred to as Wireless . No physical medium is required for the transmission of electromagnetic signals.

Features of Unguided Media

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

Difference between Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) :

Parameter	UTP	STP
Full Form	UTP stands for Unshielded Twisted Pair.	STP stands for Shielded Twisted Pair.
Grounding Cable	In UTP grounding cable is not necessary.	While in STP grounding cable is required.
Data Rate	Data rate in UTP is slow compared to STP.	Data rate in STP is high.
Cost	The cost of UTP is less.	While STP is costlier than UTP.
Maintenance	Less maintenance needed.	Much more maintenance is needed.
Noise	Noise is high compared to STP.	Noise is less.

Transmission Impairment:

In the data communication system, analog and digital signals go through the transmission medium. Transmission media are not ideal. There are some imperfections in transmission mediums. So, the signals sent through the transmission medium are also not perfect. This imperfection cause **signal impairment**.

There are three main causes of impairment are:

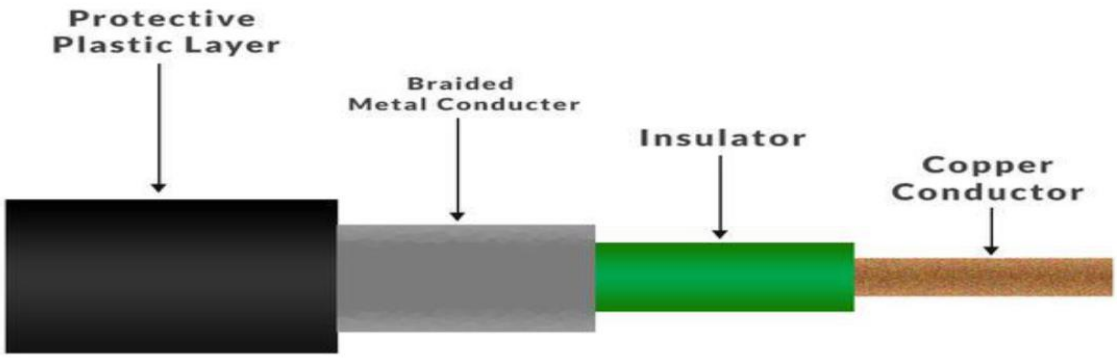
1. Attenuation
2. Distortion
3. Noise

Coaxial Cable:

Coaxial Cable is a type of guided media made of Plastics, and copper wires which transmit the signal in electrical form rather than light form. Coaxial cable is also known as **coax.**

Structure of Coaxial Cable

- **Copper conductor:** A central conductor, which consists of copper. The conductor is the point at which data is transmitted.
- **Insulator:** Dielectric plastic insulation around the copper conductor. it is used to maintain the spacing between the center conductor and shield.
- **Braided mesh:** The braid provides a barrier against EMI moving into and out of the coaxial cable.
- **Protective plastic layer:** An external polymer layer, which has a plastic coating. It is used to protect internal layers from damage.



Coaxial cable

Advantages of Coaxial Cable

- Coaxial cables support high bandwidth.
- It is easy to install coaxial cables.
- Coaxial cables have better cut-through resistance so they are more reliable and durable.
- Less affected by noise or cross-talk or electromagnetic inference.
- Coaxial cables support multiple channels

Disadvantages of Coaxial Cable

- Coaxial cables are expensive.
- The coaxial cable must be grounded in order to prevent any crosstalk.
- As a Coaxial cable has multiple layers it is very bulky.

Radio Waves:

Radio waves are a type of electromagnetic radiation with the longest wavelengths in the electromagnetic spectrum. They have have frequencies from 300 GHz to as low as 3 kHz, and corresponding wavelengths from 1 millimeter to 100 kilometers.

Microwave:

Microwave is a form of electromagnetic radiation with wavelengths ranging from about one meter to one millimeter corresponding to frequencies between 300 MHz and 300 GHz respectively.

Infrared:

Infrared, sometimes called infrared light, is electromagnetic radiation with wavelengths longer than those of visible light. It is therefore invisible to the human eye.

CHAPTER 9

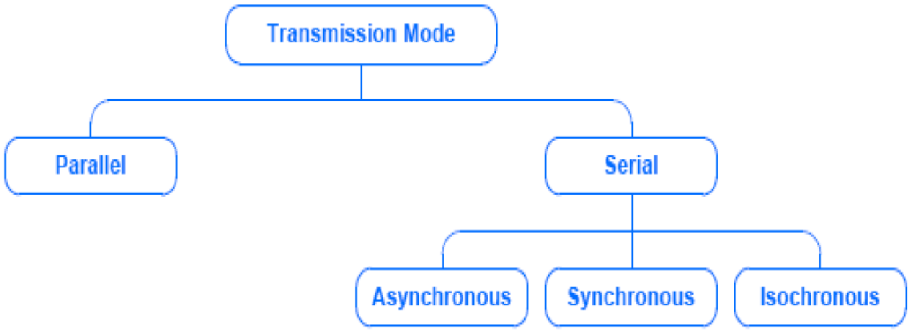
Transmission Modes

A *transmission mode* is the manner in which data is sent over the underlying medium

Transmission modes can be divided into two fundamental categories:

Serial — one bit is sent at a time

Parallel — multiple bits are sent at the same time



Parallel Transmission:

Parallel transmission allows transfers of multiple data bits at the same time over separate media.

- It is used with a wired medium
- The signals on all wires are synchronized so that a bit travels across each of the wires at precisely the same time

Serial Transmission:

Serial transmission sends one bit at a time.

Most communication systems use serial mode, because:

- serial networks can be extended over long distances at less cost
- using only one physical wire means that there is never a timing problem caused by one wire being slightly longer than another

Timing of Serial Transmission

- Serial transmission mechanisms can be divided into three broad categories (depending on how transmissions are spaced in time):
- Asynchronous transmission can occur at any time
- Synchronous transmission occurs continuously
- Isochronous transmission occurs at regular intervals

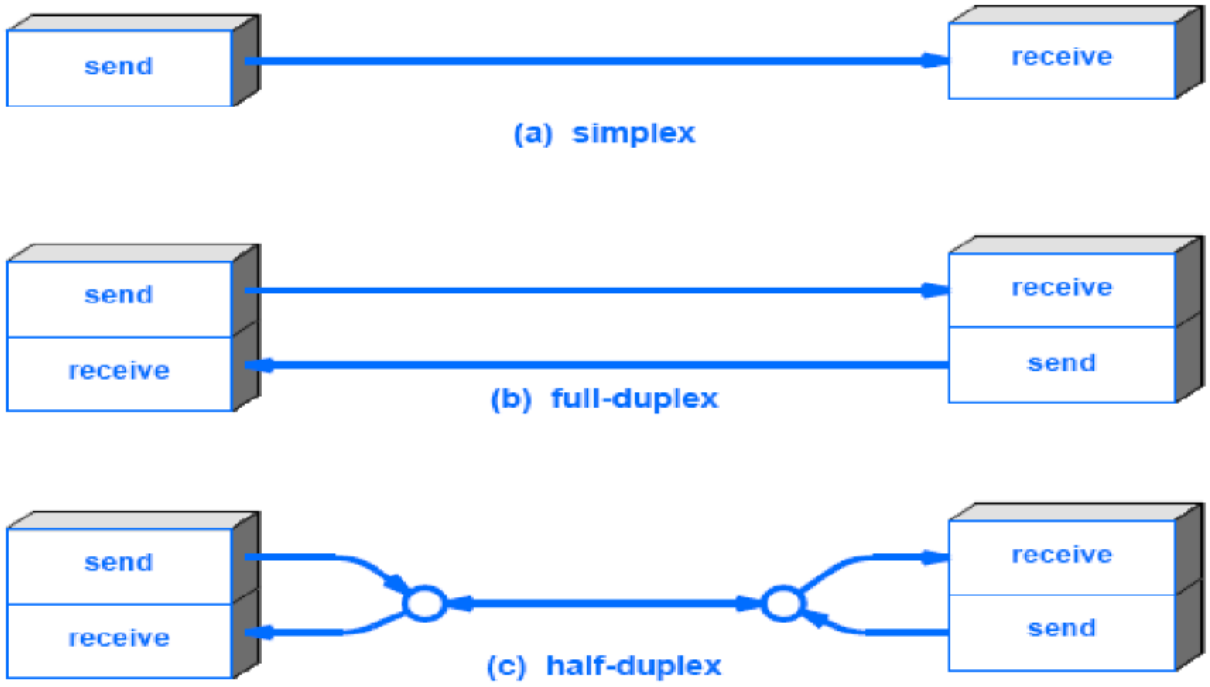
Simplex, Half-Duplex, and Full-Duplex Transmission

A communications channel can be classified as one of three types:

1. Simplex: A simplex mechanism can only transfer data in a single direction. It is analogous to broadcast radio or television

2. Full-Duplex: Full-duplex allows transmission in two directions simultaneously.

3. Half-Duplex: A half-duplex mechanism involves a shared transmission medium. The shared medium can be used for communication in each direction but the communication cannot proceed simultaneously.



Chapter 18:
Introduction to Network Layer

IP Adress

All the computers of the world on the Internet network communicate with each other with underground or underwater cables or wirelessly. If I want to download a file from the internet or load a web page or literally do anything related to the internet, my computer must have an address so that other computers can find and locate mine in order to deliver that particular file or webpage that I am requesting. In technical terms, that address is called **IP Address or Internet Protocol Address**.

Classification of IP Address:

1. Public IP Address: This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses are of two types,

- **Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IP Addresses.
- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are used by DNS servers.

2. Private IP Address: This is an internal address of your device which are not routed to the internet and no exchange of data can take place between a private address and the internet.

Classes of IPv4 Address:

There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes :

IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (2^7-2)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

Satellite:

A satellite or artificial satellite is an object intentionally placed into orbit in outer space. Satellites have a variety of uses, including communication relay, weather forecasting, navigation, broadcasting, scientific research, and Earth observation. Types of Satellite Global Positioning System (GPS) consists of up to 32 medium Earth orbit satellites in six different orbital planes, with the exact number of satellites varying as older satellites are retired and replaced. Operational since 1978 and globally available since 1994,

GPS is currently the world's most utilized satellite navigation system.

- Communications Satellite
- Remote Sensing Satellite
- Navigation Satellite
- Geocentric Orbit type satellites - LEO,MEO, HEO
- Global Positioning System (GPS)
- Geostationary Satellites (GEOs)
- Drone Satellite
- Ground Satellite
- Polar Satellite
- Nano Satellites, CubeSats and Small Sats

Classification of satellites on height above Earth's surface

Low-Earth orbits (LEO) — LEO satellites occupy a region of space from about 111 miles

(180 kilometers) to 1,243 miles (2,000 kilometers) above Earth. Satellites moving close

to the Earth's surface are ideal for making observations, for military purposes and for

collecting weather data.

Medium-Earth orbits (MEO) — These satellites park in between the low and high flyers,

so from about 1,243 miles (2,000 kilometers) to 22,223 miles (36,000 kilometers).

Navigation satellites, like the kind used by your car's GPS, work well at this altitude.

Sample specs for such a satellite might be an altitude of miles (20,200 kilometers) and

an orbital speed of 8,637 mph (13,900 kph).

Geosynchronous orbits (GEO) – GEO satellites orbit Earth at an altitude greater than

22,223 miles (36,000 kilometers) and their orbital period is the same as Earth’s

rotational period: 24 hours. Included in this category are geostationary (GSO) satellites,

which remain in orbit above a fixed spot on Earth. Not all geosynchronous satellites are

geostationary. Some have elliptical orbits, which means they drift east and west over a

fixed point on the surface during the course of a full orbit. Some have orbits that are not

aligned with Earth’s equator. These orbital paths are said to have degrees of inclination.

It also means the satellite’s path will take it north and south of Earth’s equator during

one full orbit. Geostationary satellites have to fly above Earth’s equator to remain in a

fixed spot above Earth. Several hundred television, communications and weather

satellites all use geostationary orbits. It can get pretty crowded.

ATM:

ATM stands for Asynchronous transfer mode. It is a switching technique used by

telecommunication networks that uses asynchronous time-division multiplexing to

encode data into small, fixed-sized cells. ATMs can be used for efficient data transfer

over highspeed data networks. ATM provides real-time and non-real-time services.

Services

The services provided by ATM are as follows−

• Available Bit Rate: It provides a guaranteed minimum capacity, but data can be burst

to higher capacities when network traffic is lower.

• Constant Bit Rate: It is used to specify a fixed bit rate so that data is sent in a steady

stream. This is analogous to a leased line.

• Unspecified Bit Rate: This doesn't assure any throughput level and is used for

applications, including file share that can tolerate delays.

• Variable Bit Rate (VBR): It can provide a determining throughput, but data is not

transmitted evenly. This makes it a famous choice for voice and video conferencing.

Benefits

The high-level benefits delivered through ATM services deployed on ATM technology

using international ATM standards can be summarized as follows−

Dynamic bandwidth for bursty traffic

Dynamic bandwidth for bursty traffic meeting application needs and delivering a high

utilization of networking resources; most applications are or can be viewed as inherently

bursty. For example, voice is bursty, as both parties are neither speaking at once nor all

the time; video is bursty, as the amount of motion and required resolution varies over

time.

Can handle mixed network traffic very efficiently

Variety of packet sizes makes traffic unpredictable. All network types of equipment

should incorporate elaborate software systems to manage the various sizes of packets.

ATM handles these problems efficiently with the fixed size cell.

cell network

All information is loaded into identical cells that can be sent with complete predictability and consistency.

ATM Cell Format :

As information is transmitted in ATM in the form of fixed-size units called cells. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload. 1. ATM Adaption Layer (AAL) – It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper layer services and helps them in mapping applications, e.g., voice, data to ATM cells. 2. Physical Layer – It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows: • It converts cells into a bitstream. • It controls the transmission and receipt of bits in the physical medium. • It can track the ATM cell boundaries. • Look for the packaging of cells into the appropriate type of frames. 3. ATM Layer – It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

ATM Applications:

1. ATM WANs – It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.

2. Multimedia virtual private networks and managed services – It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.

3. Frame relay backbone – Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.

4. Residential broadband networks – ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

5. Carrier infrastructure for telephone and private line networks – To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

X.25:

X.25 is generally a protocol that was developed by Telecommunication Standardization Sector (ITU-T) of International Telecommunication Union. It usually allows various logical channels to make use of the same physical line. It basically defines a series of documents particularly issued by ITU. These documents are also known as X.25 Recommendations. X.25 also supports various conversations by multiplexing packets and also with the help of virtual communication channels. X.25 basically encompasses or suits to the lower three layers of the Open System Interconnection (OSI) reference

model for networking. These three protocol layers are :

1. Physical Layer

2. Frame Layer

3. Packet Layer

These are explained as following below.

1. Physical Layer : This layer is basically concerned with electrical or signaling. The physical layer interface of X.25 also known as X.21 bis was basically derived from RS 232 interface for serial transmission. This layer provides various communication lines that transmit or transfer some electrical signals. X.21 implementer is usually required for linking.

2. Data Link Layer : Data link layer is also known as Frame Layer. This layer is an implementation or development of ISO High-Level Data Link Layer (HDLC) standard which is known as LAPB (Link Access Procedure Balanced). It also provides a communication link and transmission that is error-free among any two

physically connected nodes or X.25 nodes. LAPB also allows DTE (Data Terminal Equipment) or DCE (Data Circuit-Terminating Equipment) simply to start or end a communication session or start data transmission. This layer is one of the most important and essential parts of X.25 Protocol. This layer also provides a mechanism for checking in each hop during the transmission. This service also ensures a bit-oriented, error-free, and also sequenced and ordered delivery of data frames or packets.

3. Packet Layer : Packet layer is also known as Network Layer protocol of X.25. This layer generally governs the end-to-end communications among various DTE devices. It also defines how to address and deliver X.25 packets among end nodes and switches on a network with the help of PVCs (Permanent Virtual Circuits) or SVCs (Switched Virtual Circuits). This layer also governs and manages set-up and teardown and also flow control among DTE devices as well as various routing functions along with multiplexing multiple logical or virtual connections. This layer also defines and explains the format of data packets and also the procedures for control and transmission of data frames. This layer is also responsible for establishing a connection, transmitting data frames or packets, ending or terminating a connection, error and flow control, transmitting data packets over external virtual circuits.

Frame relay also deals with congestion within a network. Following methods are used to identify congestion within a network:

1. Forward Explicit Congestion Network (FECN) – FECN is a part of the frame header that is used to notify the destination about the congestion in the network. Whenever a frame experiences congestion while transmission, the frame relay switch of the destination network sets the FECN bit of the packet that allows the destination to identify that packet has experienced some congestion while transmission.

2. Backward Explicit Congestion Network (BECN) – BECN is a part of the frame header that is used to notify the source about the congestion in the network. Whenever a frame experiences congestion while transmission, the destination sends a frame back to the source with a

set BECN bit that allows the source to identify that packet that was transmitted had experienced some congestion while reaching out to the destination. Once, source identifies congestion in the virtual circuit, it slows down to transmission to avoid network overhead. 3. Discard Eligibility (DE) – DE is a part of the frame header that is used to indicate the priority for discarding the packets. If the source is generating a huge amount of traffic on the certain virtual network then it can set DE bits of less significant packets to indicate the high priority for discarding the packets in case of network overhead. Packets with set DE bits are discarded before the packets with unset DE bits in case of congestion within a network.

Advantages:

1. High speed

2. Scalable

3. Reduced network congestion

4. Cost-efficient

5. Secured connection

Disadvantages:

1. Lacks error control mechanism
2. 2. Delay in packet transfer
3. 3. Less reliable