Data Communication Model

1. Define data communication. Describe a simplified data communication model with a proper diagram.

Data communication: Data communication is the process of using computing and communication technologies to transfer data from one place to another and vice-versa.

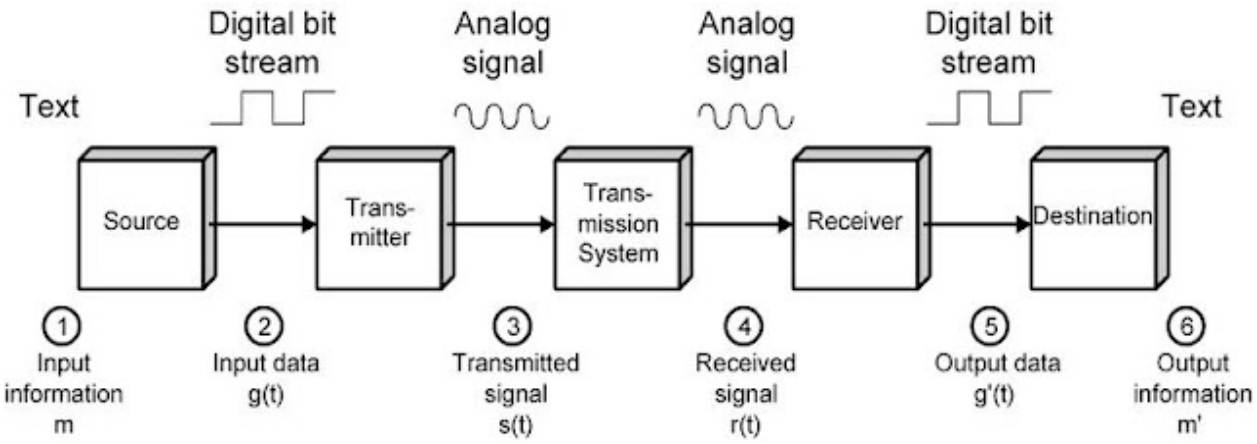


Figure: Simplified data communications model

The key elements of the data communication model are
(i) Source: This device generates the data to be transmitted; examples are telephones and personal computers.

(ii) Transmitter: The transmitter that transforms and encodes the information across some sort of transmission system. The device that converts the signal from the source in a transmittable form. So that the signal can propagate through the transmission medium is called the transmitter.

(iii) Transmission system: This can be a signal transmission line or a complex network connecting source and destination.

(iv) Receiver: The receiver accepts the signal from the transmission system and converts it into a form that can be handled by the destination device.
For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.

(v) Destination: The last component of a data communication system is called the destination. It receives the data from the receiver and concludes the communication process.

2. Fundamental Characteristics of Data Communications System

1. Delivery.
2. Accuracy.
3. Timelessness.
4. Jitter.
5. Speed.
6. Cost-Effective.
7. Efficient.

1. Delivery.

In data communication, data and information are shared between two devices.

When the data is sent from one end, it should be 100% delivered to the other end to successful data communication.

Therefore delivery plays an essential role in the field of data communication.

2. Accuracy.

In data communication, data and information sent from one computer are received by another computer and are accurate.

Therefore accuracy is considered to be one of the significant characteristics of data communication in the computer system.

3. Timelessness.

The data sent in the network are received in exact time and duration, making them a good source of data communications.

The data not received on time is useless regardless of how important the data is.

4. Jitter.

The quality is not perfect due to imperfect packet arrivals when sent from one computer in networks.

5. Speed.

The speed at which data is sent in the network is one of the significant characteristics of data communication.

Data plays a vital role in business and education; therefore, the information has to be speedily distributed among users.

The data that is received slowly delays the process of further processing.

6. Cost-Effective.

The Internet is the cheaper means of data communication. The Internet can share and transfer data from one place to another at fantastic speed and with low-cost accuracy.

7. Efficient.

They are very efficient and hence made remarkable growth in the previous years.

Data communications like email and video calling have made things even easier for communications at a low cost.

3. Explain LAN, MAN, and WAN

LAN stands for Local Area Network. It is a computer network that connects devices in a small geographical area, such as a home, office, or school. LANs are typically owned and operated by a single organization.

MAN stands for Metropolitan Area Network. It is a computer network that connects devices in a larger geographical area, such as a city or town. MANs are typically owned and operated by a consortium of organizations or a government agency.

WAN stands for Wide Area Network. It is a computer network that connects devices over a large geographical area, such as a country or continent. WANs are typically owned and operated by multiple organizations or by Internet service providers (ISPs).

4. The fundamental purpose of data communication

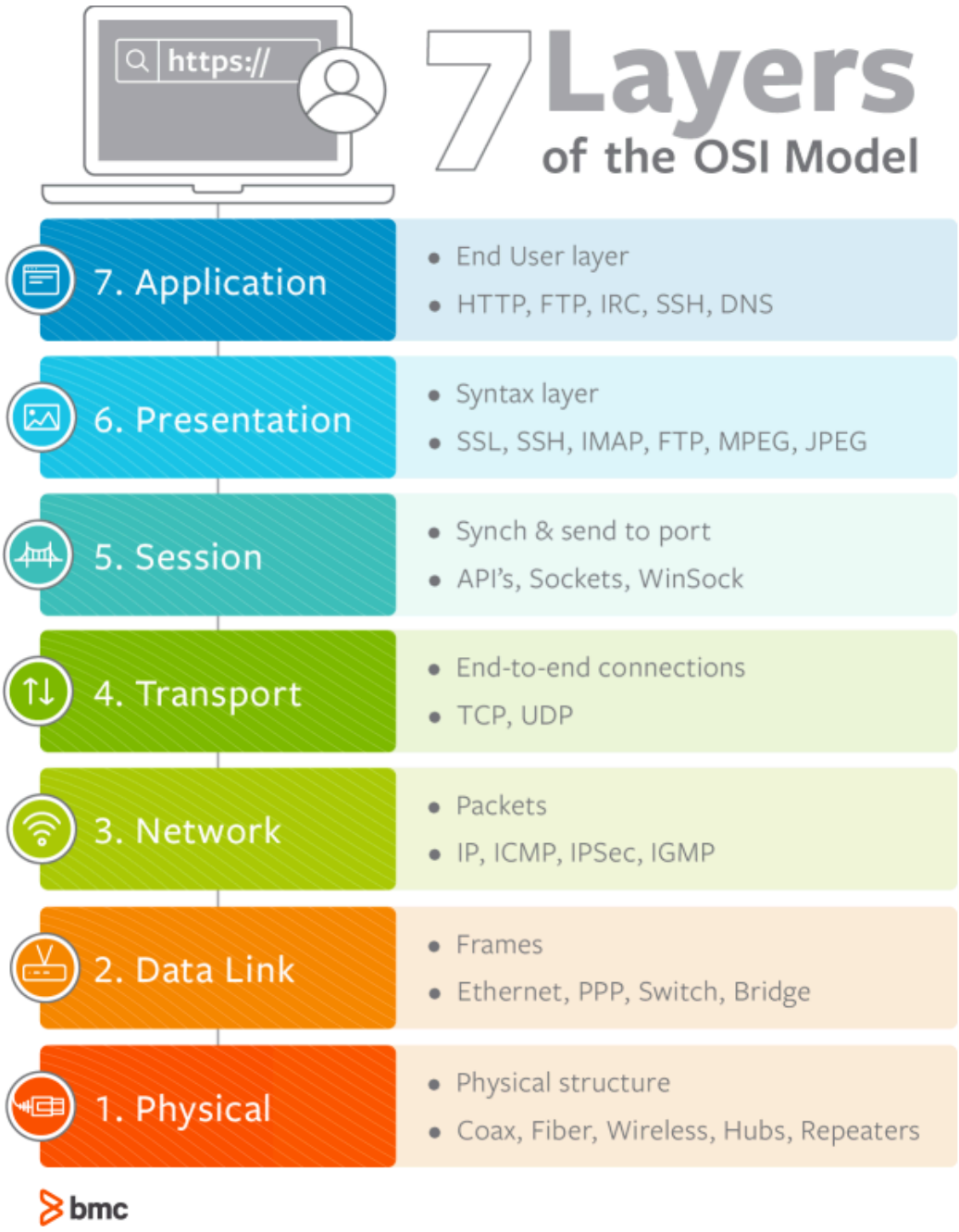
The fundamental purpose of data communication is to enable the exchange of information between devices or systems. Data communication involves the transmission of data (information) from one point to another through a medium such as cables, optical fibers, or wireless channels. The key objectives and purposes of data communication include:

- Information Exchange: The primary purpose is to facilitate the exchange of data or information between individuals, devices, or systems. This can include text, audio, video, or any other form of digital data.
- Resource Sharing: Data communication allows for the sharing of resources such as files, printers, and databases. Multiple users or devices can access and use shared resources in a networked environment.
- Remote Access: It enables users to access information and resources from remote locations. This is crucial for activities like remote work, accessing databases from different locations, and controlling devices from a distance.
- Collaboration: Data communication facilitates collaboration among individuals and teams. People can work together on projects, share ideas, and contribute to common goals even if they are geographically dispersed.

- Automation: In industrial and business settings, data communication plays a vital role in enabling automation. Devices and systems can communicate to control and monitor processes, leading to increased efficiency and productivity.

5. 7 layers of the OSI model

The seven layers of the OSI (Open Systems Interconnection.) model are



1. **Physical layer:** This layer is responsible for the physical transmission of data over a medium, such as an Ethernet cable or a Wi-Fi radio. It handles things like bit encoding, voltage levels, and signal timing.
2. **Data link layer:** This layer is responsible for framing data into packets and transmitting them reliably over a single link. It handles things like error detection and correction, flow control, and access control.
3. **Network layer:** This layer is responsible for routing packets across a network. It handles things like IP addressing, subnet masking, and routing protocols.
4. **Transport layer:** This layer is responsible for providing reliable end-to-end communication between applications. It handles things like sequence numbers, acknowledgment numbers, and flow control.
5. **Session layer:** This layer is responsible for establishing, managing, and terminating sessions between applications. It handles things like authentication, authorization, and session synchronization.
6. **Presentation layer:** This layer is responsible for transforming data into a format that can be understood by the receiving application. It handles things like data encryption, data compression, and character encoding.
7. **Application layer:** This layer is responsible for providing network services to applications, such as web browsing, email, and file transfer. It handles things like HTTP, FTP, and SMTP protocols.

The OSI model is a conceptual model, which means that it does not describe exactly how any particular network is implemented. However, it is a useful tool for understanding the different functions that are involved in network communication.

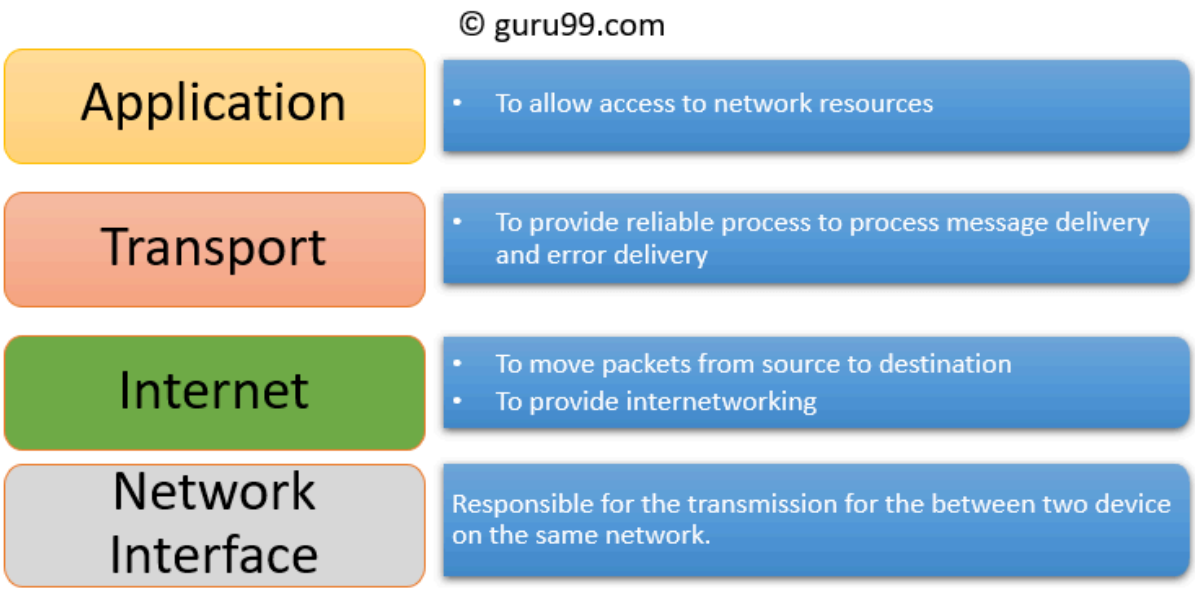
6. The TCP/IP model layers

Lec-3: TCP/IP Protocol Suite | Internet Protocol Suite | OSI vs TCP/IP

The TCP/IP model has four layers:

- Application layer: This layer is responsible for providing network services to applications, such as web browsing, email, and file transfer.
- Transport layer: This layer provides reliable communication between applications on different devices. It also provides flow control and congestion control to ensure that data is transmitted efficiently.

- Internet/ layer: This layer is responsible for routing packets across the network. It also provides IP addressing, which allows devices to be uniquely identified on the internet.
- Network access layer: This layer is responsible for transmitting and receiving packets over the physical medium, such as an Ethernet cable or a Wi-Fi radio.



The TCP/IP model is a layered architecture, which means that each layer provides services to the layer above it and uses the services of the layer below it. For example, the transport layer uses the services of the internet layer to route packets to the destination device.

Here is a brief overview of the functions of each layer:

Application layer:

- Provides network services to applications
- Examples: web browsing, email, file transfer

Transport layer:

- Provides reliable communication between applications on different devices
- Provides flow control and congestion control

- Examples: TCP, UDP

Internet layer:

- Routes packets across the network
- Provides IP addressing
- Example: IP

Network access layer:

- Transmits and receives packets over the physical medium
- Examples: Ethernet, Wi-Fi

The TCP/IP model is the most widely used network model in the world today. It is used to power the internet and many other types of networks.

Key elements of the protocol

In networking, a protocol is a set of rules that govern data communications. The key elements of a protocol are syntax, semantics, and timing.

The key elements of a protocol are:

- **Syntax:** The syntax of a protocol defines the format of the data that is exchanged between devices. This includes things like the order of the fields in a message, the type of data that each field can contain, and the use of special characters to indicate the start and end of a message.
- **Semantics:** The semantics of a protocol define the meaning of the data that is exchanged between devices. This

includes things like the definition of each field in a message, the actions that devices should take when they receive certain messages, and the handling of errors.

- **Timing:** The timing of a protocol defines when devices should send and receive data. This includes things like the maximum time that a device can wait for a response from another device, the number of times that a device should retransmit a message if it does not receive a response, and the mechanisms for handling synchronization between devices.

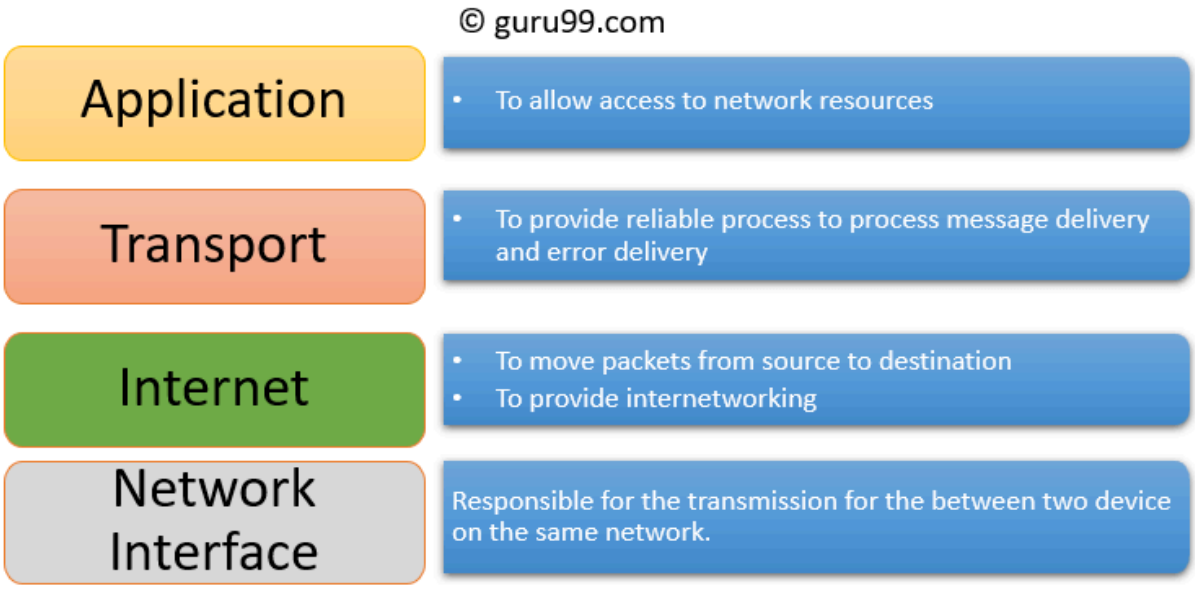
These three elements are essential for ensuring that devices can communicate effectively with each other using a protocol.

The TCP/IP model layers

The TCP/IP model has four layers:

- Application layer: This layer is responsible for providing network services to applications, such as web browsing, email, and file transfer.
- Transport layer: This layer provides reliable communication between applications on different devices. It also provides flow control and congestion control to ensure that data is transmitted efficiently.
- Internet/ layer: This layer is responsible for routing packets across the network. It also provides IP addressing, which allows devices to be uniquely identified on the internet.

- Network access layer: This layer is responsible for transmitting and receiving packets over the physical medium, such as an Ethernet cable or a Wi-Fi radio.



The TCP/IP model is a layered architecture, which means that each layer provides services to the layer above it and uses the services of the layer below it. For example, the transport layer uses the services of the internet layer to route packets to the destination device.

Here is a brief overview of the functions of each layer:

Application layer:

- Provides network services to applications
- Examples: web browsing, email, file transfer

Transport layer:

- Provides reliable communication between applications on different devices
- Provides flow control and congestion control
- Examples: TCP, UDP

Internet layer:

- Routes packets across the network
- Provides IP addressing
- Example: IP

Network access layer:

- Transmits and receives packets over the physical medium
- Examples: Ethernet, Wi-Fi

The TCP/IP model is the most widely used network model in the world today. It is used to power the internet and many other types of networks.

Difference between Connection-oriented and Connection-less Services:

S.NO	Connection-oriented Service	Connection-less Service
1.	Connection-oriented service is related to the telephone system.	Connectionless service is related to the postal system.

2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	Connection-oriented Service is necessary.	Connectionless service is not compulsory.
4.	Connection-oriented Service is feasible.	Connectionless service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
7.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
8.	Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
9.	Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
10.	Connection-oriented requires authentication.	Connection-less Service does not require authentication.

Topology

Types of Computer Network Topology

1. Physical topology
2. Logical Topology

Physical Topologies

The physical topology is the physical shape or layout of the wires that can be visible in a network. The Physical topology defines how devices are interconnected with or without wires. Physical topology is further divided into two sections.

1. Point-to-point connections
2. Multipoint connections

Point-to-point connections

In a point-to-point connection, a communication link is established between two devices with one wire or air (in the case of wireless). A simple example of a point-to-point connection is talking over the telephone between two persons where anyone else is not allowed to use the phone on either side.

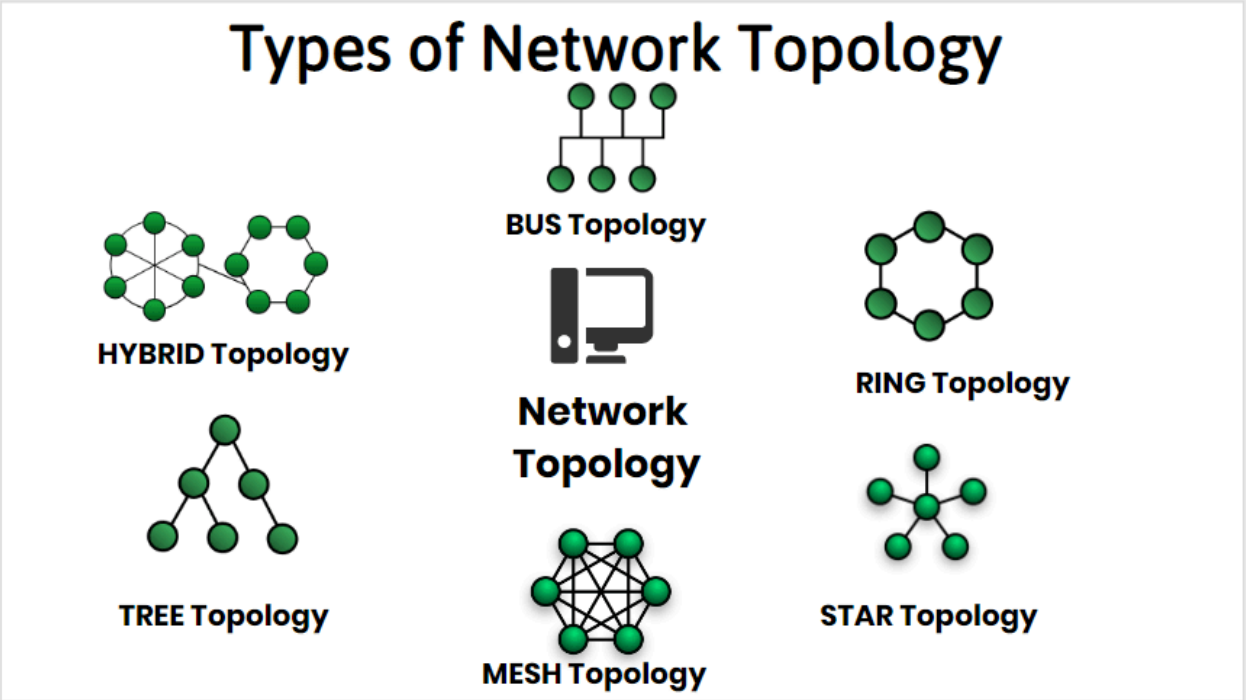
Multipoint Connection

Multiple devices or machines are involved in a multipoint connection. These devices mainly share cabling but each device needs to have a unique number to identify each other for sending data between them. A good example of a multipoint connection is communication between a group of computers in a network.

Logical Topology

A logical topology defines how devices communicate with each other across the physical topology. The physical and logical topologies are independent of each other. The physical topology refers to the physical layout of the wires whereas the logical topology refers to how data moves through the network. There are five types of logical topology that are used in a network.

- Star topology
- Hierarchical topology
- Bus topology
- Mesh topology
- Ring topology



Transmission Modes in Computer Networks

Transmission modes in computer networks define the direction of data flow between two devices. There are three main types of transmission modes: simplex, half-duplex, and full-duplex.

Simplex mode is a one-way transmission mode, meaning that data can only flow in one direction between two devices. An example of a simplex transmission mode is a keyboard connected to a computer. The keyboard can only send data to the computer, but cannot receive any data back.

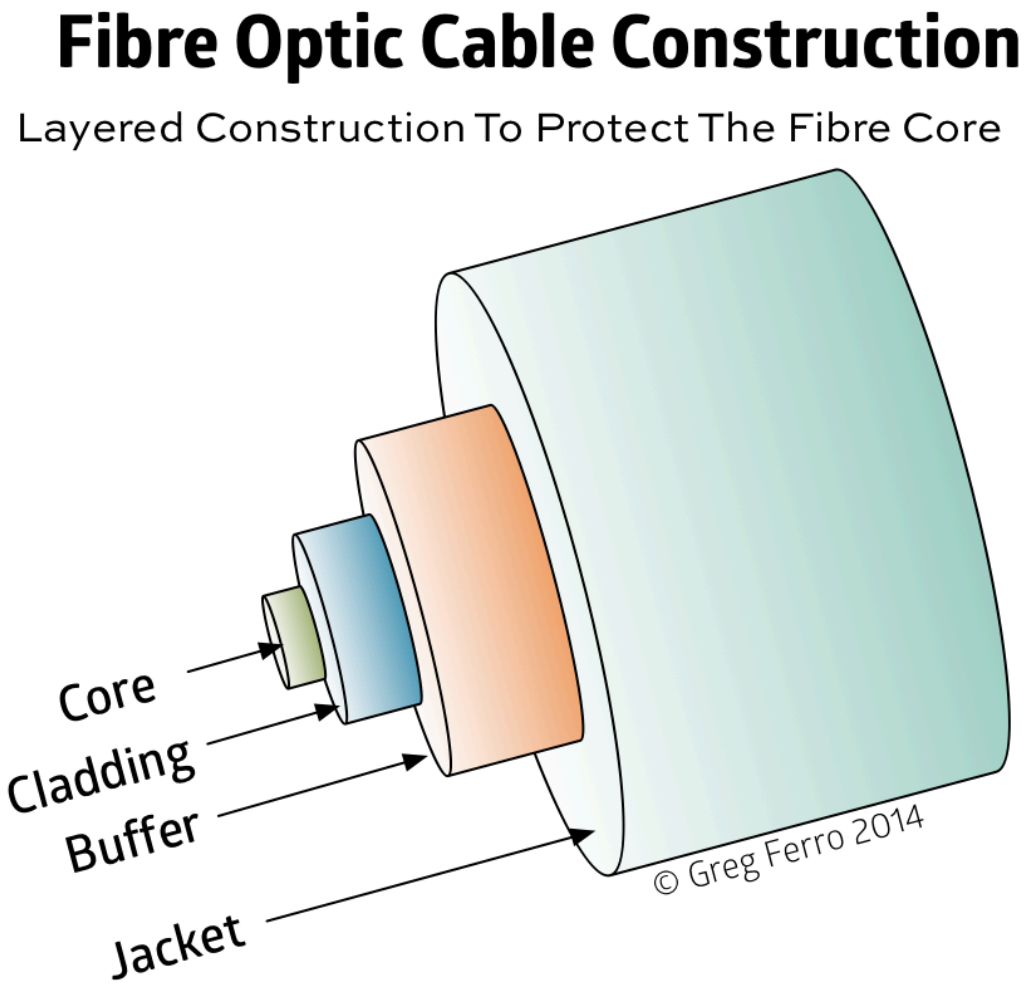
Half-duplex mode is a two-way transmission mode, but data can only flow in one direction at a time. An example of a half-duplex transmission mode is a walkie-talkie. Two people can use a walkie-talkie to communicate with each other, but only one person can speak at a time.

Full-duplex mode is a two-way transmission mode where data can flow in both directions simultaneously. An example of a full-duplex transmission mode is a telephone conversation. Two people can talk to each other on the phone at the same time.

Fibre-Optic Cable

Fiber-optic cable is a type of communication cable that uses light to transmit data. It is made up of thin strands of glass or plastic that are bundled together. Each strand is called a core, and it is

surrounded by a cladding material that has a lower refractive index. This difference in refractive index causes light to be trapped inside the core, and it is guided through the cable by total internal reflection.



Fiber-optic cable is made up of the following parts:

- Core: The core is the central part of the fiber-optic cable and is made of glass or plastic. It is through the core that the light travels, carrying the data.

- Cladding: The cladding is a thin layer of material that surrounds the core. It has a lower refractive index than the core, which helps to keep the light trapped inside the core.
- Buffer coating: The buffer coating is a protective layer that surrounds the cladding. It protects the fiber from damage and moisture.
- Outer jacket: The outer jacket is the outermost layer of the fiber-optic cable. It is made of a durable material, such as PVC or Kevlar, to protect the cable from the elements and physical damage.

Data rate and attenuation

Data rate is the rate at which data is transmitted over a network. It is typically measured in bits per second (bps). The higher the data rate, the more data that can be transmitted in a given period of time.

Attenuation is the loss of signal strength as it travels through a medium. It is typically measured in decibels per kilometer (dB/km). The higher the attenuation, the more signal strength is lost over a given distance.

There is a relationship between data rate and attenuation. The higher the data rate, the more susceptible the signal is to attenuation. This is because higher data rates require faster signal modulation, which can lead to more signal distortion.

In order to maintain a high data rate over long distances, it is important to use a transmission medium with low attenuation. Fiber-optic cable is a good example of a transmission medium with low attenuation. It can support data rates of up to terabits per second over distances of hundreds of kilometers.

CRC technique for error detection

Cyclic redundancy check (CRC) is a technique for detecting errors in data transmission. It works by appending a checksum to the end of the data. The checksum is a calculated value that is based on the contents of the data. When the data is received, the checksum is recalculated and compared to the original checksum. If the two checksums match, then the data is assumed to be error-free. If the two checksums do not match, then the data is assumed to be corrupted.

CRC is a very effective error detection technique. It can detect a wide range of errors, including single-bit errors, multiple-bit errors, and burst errors. CRC is also very efficient, meaning that it can be calculated quickly and easily.

CRC is used in a wide variety of applications, including data transmission, data storage, and data processing. Some common examples of CRC usage include

- Ethernet frames
- TCP/IP packets

- File systems (e.g., FAT, NTFS)
- Zip files
- DVDs and CDs
- RAM and other memory devices

CRC is a powerful tool for detecting errors in data transmission. By using CRC, you can help to ensure that your data arrives at its destination intact.

Propagation

Propagation in networking refers to the time it takes for a signal to travel from one point to another. It is a significant factor in determining the performance of a network, as it can limit the speed at which data can be transmitted.

The propagation speed of a signal depends on the medium through which it is traveling. For example, signals travel through the air at the speed of light, while they travel through copper wire at about 60% of the speed of light.

Propagation delay can be a significant limitation in high-speed networks. For example, in a 100 Gbps network, a propagation delay of 1 millisecond would limit the maximum distance between two devices to about 300 kilometers.

Packet switching and circuit switching

Packet switching and circuit switching are two different methods of switching used in communication networks to transfer data between two or more devices.

Packet switching is a connectionless method of switching. This means that a dedicated communication path between the source and destination devices is not established before data transmission begins. Instead, data is divided into smaller units called packets, and each packet is routed independently through the network. This allows multiple users to share the same network resources, and it makes packet switching more efficient than circuit switching for bursty traffic patterns.

Circuit switching is a connection-oriented method of switching. This means that a dedicated communication path between the source and destination devices is established before data transmission begins. This path is held open for the duration of the communication session, even if no data is being transmitted. This makes circuit switching more efficient than packet switching for continuous traffic patterns, such as a telephone call or a video stream.

The following table summarizes the key differences between packet switching and circuit switching:

Characteristic	Packet switching	Circuit switching
Connection-oriented	No	Yes
Dedicated path	No	Yes
Efficiency	Good for bursty traffic	Good for continuous traffic
Examples	Internet, IP networks	Telephone networks, SONET/SDH networks

X.25 protocol

X.25 is a packet switching protocol that was developed in the 1970s to provide a reliable way to transmit data over long distances. It is based on the HDLC (High-Level Data Link Control) protocol and provides a number of features that make it well-suited for a variety of applications, including:

- Error detection and correction: X.25 uses a variety of techniques to detect and correct errors that occur during data transmission.
- Flow control: X.25 uses flow control mechanisms to ensure that the sender does not overwhelm the receiver with data.
- Congestion control: X.25 uses congestion control mechanisms to prevent the network from becoming overloaded.

Set 2

Basics

Analog data signals are continuous signals that vary in amplitude and frequency over time. They are often used to represent physical phenomena, such as sound, light, and temperature.

Digital data signals are discrete signals that are represented by a series of bits. Each bit can be either 0 or 1. Digital data signals are often used to represent information in computers and other digital devices.

Frequency is used to identify different types of signals. For example, radio waves, microwaves, and light waves all have different frequency ranges.

Spectrum is used to allocate resources on a network. For example, different devices on a network may be assigned different frequency ranges to operate on. This helps to prevent interference between devices.

Bandwidth is used to determine the amount of data that can be transmitted over a network. For example, a network with a high bandwidth can transmit more data than a network with a low bandwidth.

Here are some examples of how frequency, spectrum, and bandwidth are used in networking:

- **Frequency**: Radio waves are used to transmit data over wireless networks. Different types of wireless networks, such as cellular networks and Wi-Fi networks, use different frequency ranges.
- **Spectrum**: The radio spectrum is a limited resource, and it is important to manage it carefully. The Federal Communications Commission (FCC) in the United States is responsible for allocating spectrum to different users.
- **Bandwidth**: The bandwidth of a network connection determines how much data can be transferred between two devices. For example, a network with a high bandwidth can support streaming video and other high-bandwidth applications.

Transmission impairments

Transmission impairments are any factors that can degrade the quality of a signal as it travels from the source to the destination. These impairments can be caused by a variety of factors, such as the distance traveled, the type of transmission medium used, and environmental conditions.

Some of the most common transmission impairments include:

- **Attenuation**: Attenuation is the loss of signal strength as it travels through a medium. This is caused by the medium absorbing or scattering the signal energy.
- **Distortion**: Distortion is the change in the shape of a signal as it travels through a medium. This can be caused by a variety of factors, such as the frequency response of the medium and the presence of noise.
- **Noise**: Noise is any unwanted signal that is added to the desired signal. This can be caused by a variety of factors, such as crosstalk from other signals, interference from natural sources, and thermal noise.

Transmission impairments can have a significant impact on the performance of a network. For example, attenuation can limit the distance that a signal can travel before it becomes too weak to be received. Distortion can make it difficult to decode the signal at the receiver. Noise can cause errors in the data transmission.

Different types of noise in data communication

There are many different types of noise in data communication, but some of the most common include:

- Thermal noise: Thermal noise is caused by the random movement of electrons in a conductor. It is a white noise, meaning that it is present at all frequencies.
- Shot noise: Shot noise is caused by the random arrival of electrons at a conductor. It is a Poisson process, meaning

that the number of arrivals in a given interval is random and independent of the number of arrivals in other intervals.

- Intermodulation noise: Intermodulation noise is caused by the nonlinear distortion of a signal. It occurs when two or more signals are mixed together, and the resulting signal contains new frequencies that are not present in the original signals.
- Crosstalk noise: Crosstalk noise is caused by the interference between two or more signals that are traveling through the same medium. It is typically caused by capacitive or inductive coupling between the signals.
- Impulse noise: Impulse noise is caused by sudden transient disturbances in a signal. It can be caused by a variety of factors, such as lightning strikes, power surges, and mechanical failures.

Noise can have a significant impact on the performance of a data communication system. It can cause errors in the data transmission, which can lead to lost packets, corrupted data, and even complete failure of the system.

Transmission media

It is the physical path over which data travels from one device to another in a computer network. It can be categorized into two types: guided and unguided.

Guided transmission (Wired or Bounded transmission media) media uses a physical cable or wire to guide the signal from the source to the destination. Examples of guided transmission media include:

- Twisted-pair cable: Twisted-pair cable is the most common type of guided transmission media. It consists of two insulated copper wires that are twisted together. Twisted-pair cable is relatively inexpensive and easy to install, but it has a lower bandwidth than other types of guided transmission media.
- Coaxial cable: Coaxial cable consists of a central copper conductor surrounded by an insulating layer and a braided copper shield. Coaxial cable has a higher bandwidth than twisted-pair cable, but it is more expensive and difficult to install.
- Fiber-optic cable: Fiber-optic cable consists of a core of thin glass or plastic fibers that transmit data using light signals. Fiber-optic cable has the highest bandwidth of all types of guided transmission media, but it is also the most expensive and difficult to install.

Unguided transmission media does not use a physical cable or wire to guide the signal from the source to the destination. Instead, the signal travels through the air or through other media, such as water or vacuum. Examples of unguided transmission media include:

- Radio waves: Radio waves are electromagnetic waves that can travel through the air. Radio waves are used in a variety of wireless networks, such as cellular networks and Wi-Fi networks.
- Microwaves: Microwaves are high-frequency electromagnetic waves that can travel through the air. Microwaves are used in a variety of wireless networks, such as microwave relay networks and satellite communication systems.
- Infrared light: Infrared light is electromagnetic radiation that is invisible to the human eye. Infrared light is used in short-range wireless communication applications, such as remote controls and infrared data ports.

The type of transmission media that is used in a computer network depends on a number of factors, including the distance between devices, the required bandwidth, and the budget.

VSAT

A very small aperture terminal (VSAT) communication system is a satellite-based communication system that uses small, low-cost antennas to transmit and receive data. VSAT systems are typically used in remote locations where other types of communication infrastructure, such as terrestrial networks, are not available or reliable.

VSAT systems consist of three main components:

- VSAT terminal: The VSAT terminal is the antenna and associated equipment that is used to transmit and receive data. VSAT terminals can be fixed or mobile.
- Satellite: The satellite provides the communication link between the VSAT terminals.
- Hub station: The hub station is a ground station that relays data between the VSAT terminals and the rest of the world.

VSAT systems can be used to transmit a variety of data types, including voice, video, and data. VSAT systems are commonly used for applications such as:

- Internet access: VSAT systems can be used to provide Internet access to remote locations.
- Voice and video communication: VSAT systems can be used to provide voice and video communication services to remote locations.
- Data transmission: VSAT systems can be used to transmit data between remote locations, such as between a remote office and a headquarters.
- Military and government applications: VSAT systems are also used by the military and government for a variety of applications, such as secure communication and disaster relief.

Port address logical address and physical address

Port address is a 16-bit number that identifies a specific application or service running on a computer. Port addresses are used by the operating system to direct incoming network traffic to the appropriate application.

The logical address is an IP address that identifies a specific device on a network. IP addresses are used by routers and other networking devices to route network traffic between different networks.

The physical address is a unique identifier that is assigned to each network interface card (NIC). Physical addresses are used by networking devices to communicate with each other at a low level.

The following table summarizes the key differences between port addresses, logical addresses, and physical addresses:

Characteristic	Port address	Logical address	Physical address
Type of identifier	16-bit number	32-bit number	48-bit number
Purpose	Identifies a specific application or service	Identifies a specific device on a network	Identifies a specific NIC
Example	80 for HTTP	192.168.1.1	00-AA-BB-CC-DD-EE