Unit-2
Data Communication and Networking

Total Questions Asked in Exam=2
Long Answer Question=1 (8 Marks)
Multiple Choice Question=1 (1 Mark)
Total Marks= 9 Marks

Data Communication:
The process of transferring data and information between the communicating devices or nodes from one location to another using communication channels is called data communication. It might use either guided or unguided media for data transmission. The data communication process is governed by some sorts of rules called protocols.
Examples: Sending emails, text messages through our smartphones.

Telecommunication:
The communication that takes place over a significant distance is called telecommunication. It is carried out when the sender (transmitter) and receiver are at different geo-locations.
Example: Communication through cellular phones

Data Communication System:
A group or a set of communicating tools and devices to facilitate data communication and information sharing among the devices is known as data communication system.

Elements of Data Communication System:
A data communication system comprises of following components:
a) Transmitter (Sender)
b) Receiver
c) Transmission Media
d) Protocols
e) Message

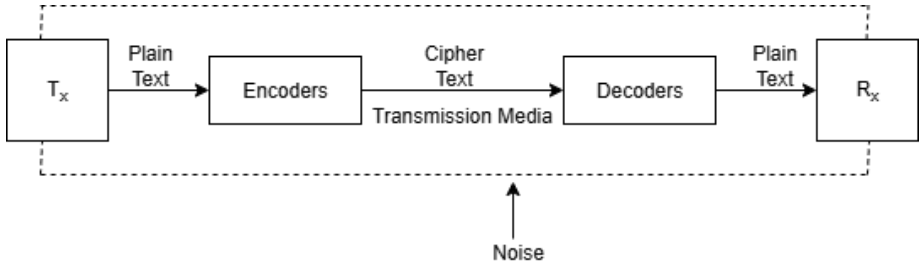

Fig.: Data Communication System

a) **Transmitter (T_x):**
It refers to a communicating device that is responsible for transmitting the data and information to other devices in a communication system. The data delivered from a sender is converted into some other messages hiding their original data using some cryptographic algorithms. The process of converting the plain text into cipher text using some cryptographic algorithms is called encryption.

b) **Receiver(R_x):**
It is a communicating device that is responsible for accepting the transmitted data and information in a communication system. The transmitted data (i.e., cipher text) is again converted into its original form at receiving side. The process of recovering the original message from the cipher text is known as decryption.

c) **Transmission Media:**
The channels through which data gets transmitted between the communicating devices (i.e., sender and receiver) are called transmission media. They may be either guided (Twisted Pair Cable, Co-axial, Fiber-optic cable) or unguided (Infrared, Microwave, Radio wave, etc.)

d) **Protocols:**
Protocols can be defined as the set of rules that govern the data communication process in a communication system. They define a specific format for exchanging data between the devices.
Examples: SMTP, NCP, TCP/IP, POP, IMAP, HTTP/HTTPS, etc.

e) Message:

Message refers to the data and information being transmitted between the communicating devices through the transmission media. The authenticity and integrity of the message is checked by using digital signature in a computer network.

Data Transmission Modes:

The way by which data gets transmitted in between the communicating devices through any communication media is known as data transmission mode. It defines how data is sent between the devices.

Types of Data Transmission Modes:

The data transmission modes can be broadly classified into following types:

a) Simplex Mode
b) Half Duplex Mode
c) Full Duplex Mode

a) Simplex Mode:

The data transmission mode in which data is transmitted in only one direction from sender to receiver is called simplex mode. It is 7unidirectional flow of data, where the receiver can't acknowledge to the sender. So, there is no guarantee of reliable data transfer.

Examples: Radio, TV Broadcasting, etc.

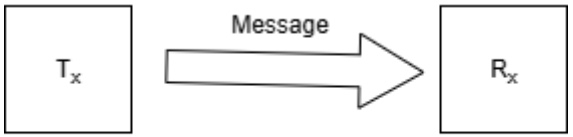

Fig.: Simplex Mode

b) Half Duplex Mode:

The data transmission mode in which data is transmitted in both the directions but not simultaneously (i.e., only one direction at a time) is called half-duplex mode. It is a bidirectional flow of data but the receiver can't provide the acknowledgement signal to the sender while transmitting the data by a sender. This mode uses the same communication channel for data transmission.

Example: Walkie-Talkie

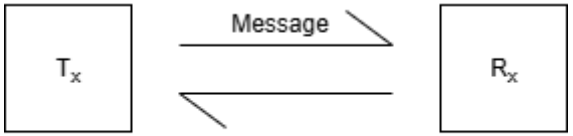

Fig.: Half-duplex Mode

c) Full Duplex Mode:

It is a data transmission mode in which data is transmitted in both the directions (i.e., from sender to receiver and vice-versa) simultaneously. It uses different channels for data communication so bidirectional data flow is possible at the same. It is one of the fastest data transmission modes.

Example: Communication using cellular phones

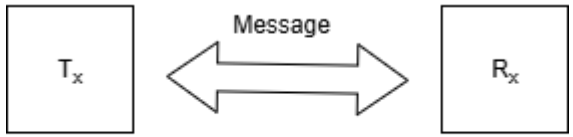

Fig.: Full Duplex Mode

Computer Network:

A group or a set of computers and other computing devices interconnected with an intend to share data, information and resources using wired or wireless media is called computer network or networking. It allows the communicating devices to share some sort of data and information from one location to another.

The computer network increases the data availability and helps the corporates to lower down the operational costs.

Types of Computer Network:

Computer network can be broadly classified into following types based on area of coverage or geographical location.

a) Local Area Network (LAN)
b) Metropolitan Area Network (MAN)
c) Wide Area Network (WAN)

Comparison Among LAN, MAN and WAN: (Important for 8 Marks)

Key Aspects	Local Area Network (LAN)	Metropolitan Area Network (MAN)	Wide Area Network (WAN)
Definition	It is a computer network that spans within a room or a building.	It is a computer network that spans beyond LAN and can cover a city or a state.	It is a computer network that spans beyond MAN and can connect the existing technologies.
Ownership	Privately owned small network.	Ownership is with single organization.	Ownership is with multiple organizations.
Transmission Media	Mostly wired (guided) media preferred.	Both wired and wireless media	Mostly wireless (unguided) media preferred.
Data Transfer Speed	It has the highest data transfer speed up to GBps.	It has moderate data transfer speed (i.e., slower than LAN)	It has least data transfer speed among all.
Transmission Errors	Least data transmission errors.	Moderate i.e., more than LAN and less than WAN.	Highest among all.
Coverage Area	A room or a building, not expanding more than 2-5 kms.	A city or a state.	A country or the whole globe.
Examples	Network of Computer Lab	Network of Ghorahi	Internet

Advantages of Computer Network:

Computer Network offers lots of advantages. Some of the common advantages of computer network are:

a) **Facilitates Communication:**
It allows people to transmit data and information from one location to another at cheaper cost. We can share the data within a quick period of time due to computer network.

b) **Resources Sharing:**
Computer network allows us to share the hardware and software resources among the wide range of users so that we do not need to configure the printers, and other resources to each of the device.

c) **Reduces Operational Costs:**
The sharing of resources saves our cost of operation as the same hardware and software can be accessed from different communicating devices.

d) **Backup and Recovery:**
Backup refers to the process of copying same piece of information over the multiple location. Computer network helps to store data at networked locations such as cloud, so that it will be easy to recover the data once it gets lost or damaged.

e) **Database Sharing:**
It helps the corporates or business firm to share the data across its branches at different locations. Due to accessibility of database from multiple locations, concurrency can be achieved.

f) **Improves data availability:**
The data stored at networked location can be accessed from anywhere anytime. This increases the availability of data among the devices.

Disadvantages of Computer Network:

The disadvantages of computer network are as follows:

a) **Expensive:**
Due to the requirement of hardware and software tools, it requires a lot of initial investment to configure or setup a computer network. So, it expensive to setup.

b) **Requires skilled Manpower:**
A network administrator is required to monitor, troubleshoot and fix the issues encountered in a computer network. It is quite difficult to manage a computer network without having skilled manpower.

c) **Risk of spreading Malwares:**
Malwares like computer virus, worms, etc. can be transmitted across the hosts (devices) by means of computer network, causing harm to our data and information.

d) **Potential risk of Cyber Crimes:**
The misuse of computer network may increase the risk of cyber crimes like hacking, piracy, phishing attack, etc. by misinterpreting our data.

Transmission Media:

The channels through which data gets transmitted in between the communicating devices are called transmission media. They act as the bridge between a sender and a receiver that enables the communication between them. They are often called communication media.
Examples: Twisted Pair Cable, Fiber-optic Cable, Microwave, Radio wave, etc.

Types of Transmission Media:

The transmission media can be broadly classified into two categories as:

a) Guided or Bounded Media
b) Unguided or Unbounded Media

a) Guided Media:

The transmission media that need physical conductors (i.e., wires or cables) to transmit the data between the communicating devices are called guided media. They are also called bounded media because the data signals are bounded to flow by a cabling system and are guided to flow in a specific direction.
Guided media transmit the data in the form of voltage, electric current or light. They are less prone to external barriers or noise while transmitting the data.
Examples: Twisted pair cable, Fiber-optic cable, Co-axial Cable

b) Unguided Media:

The transmission media that do not use any physical wire or cabled to transmit the data between the communicating devices are called unguided media. They are also called unbounded or wireless media. They are called unbounded media as the data signals are free to flow in any direction and they are not guided as well.
Unguided media uses electromagnetic waves to propagate the data from one place to another. That's why, there is high possibility of attenuation and multipath propagation of the signals. And, the unguided media is more prone to external barriers during the data transmission.
Examples: Infrared, Microwave, Radio wave, Commun ication Satellite, etc.

Differences between Guided Media and Unguided Media:

Guided Transmission Media	Unguided Transmission Media
1. They need physical wires or cables for data transmission.	1. They do not need any physical wires or cables for data transmission.
2. They transmit data in the form of voltage, current or light.	2. They transmit data in the form of electromagnetic waves.
3. The data signals are bounded by a cabling system.	3. The data signals are not bounded by a cabling system.
4. The signals are directed to flow in a particular direction.	4. The signals are free to move in any directions.
5. They offer greater bandwidth than unguided media.	5. They have less bandwidth than guided media.
6. They are less affected by the external environmental factors.	6. They are highly affected by the external environmental factors.
7. They have higher data transfer speed than unguided media.	7. Data transfer speed is low.
8. Better Fault Tolerance against Noise.	8. Fault Tolerance is low.
9. No multipath propagation occurs.	9. Multipath Propagation is more common.
10. They are cheaper.	10. They are expensive

Examples: Twisted pair, Co-axial Cable, etc.	Examples: Infrared, Microwave, Radiowave, etc.

Network Topology:

The physical layout or the structure of network nodes and links during the configuration in a network is called network topology. It defines the pattern of organizing the network devices (called nodes) and communication media (called links) in a network.

There are following different types of Network topologies (LAN Topologies)

a) Bus Topology
b) Star Topology
c) Ring Topology
d) Mesh Topology
e) Tree Topology

a) Bus Topology:

A network topology in which a common cable or line (backbone cable) is used to connect all the nodes is called bus topology. It is often called linear topology. It is one of the simplest and cheapest topology to set up and is useful for the smaller networks.

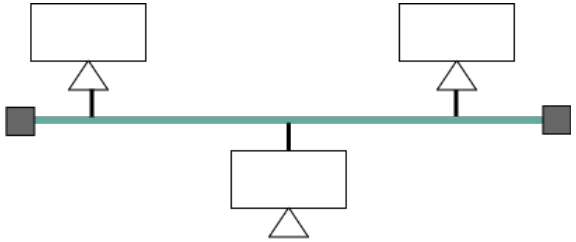

Fig: Bus Topology

Advantages:

i. Simple and Easy to setup.
ii. Cheapest topology among other topologies.
iii. Easy to add and remove nodes to and from a network.
iv. Failure of each node doesn't affect others.

Disadvantages:

i. Failure of backbone cable affects the whole network.
ii. Efficiency decreases on increasing the number of nodes.
iii. High data traffic.
iv. Security concerns may arise as the data sent by a node is visible to other nodes as well.

b) Star Topology:

A network topology in which a central device (i.e., a hub or a switch) is used to connect every node is called star topology. The data sent by a node is first transmitted to a central device and it forwards the data to the intended destination. So, there exists centralized control over the data.

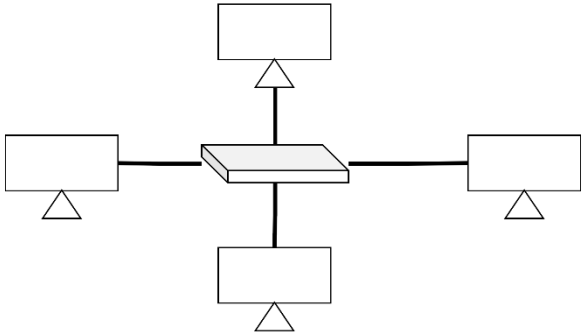

Fig: Star Topology

Advantages:

i. Centralized control over data.
ii. Failure of each node doesn't affect others.
iii. Troubleshooting is easy.
iv. Easy to setup and scalable (i.e., Adding and removing nodes to and from a network is easy).

Disadvantages:

i. Failure of a central device affects the whole network.
ii. Performance is limited by a central device.
iii. High Data Traffic.
iv. Expensive to set up due to central device and cable length.

c) Ring Topology:

A network topology that connects the nodes in a closed circular loop forming a ring like structure is called ring topology. In this topology, each device is configured to other devices in either side. The data is transmitted either in clockwise direction or anticlockwise direction

through intermediate nodes before reaching to the targeted device.

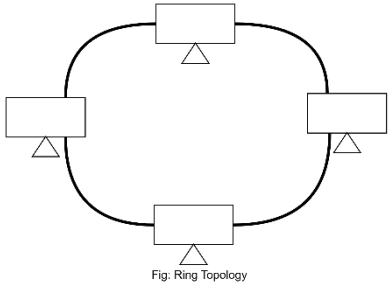

Fig: Ring Topology

Advantages:

i. No central device is required.
ii. Cheaper than star topology.
iii. Each node acts as a repeater so, data transmission errors are less.
iv. Less data traffic.

Disadvantages:

i. Failure of each node affects the whole network.
ii. Difficult to troubleshoot.
iii. It is not as easy as star topology to add or remove nodes.
iv. Requires more time to transmit the data to the intended node.

Network Architecture: (Important)

The design and structure of a computer network that devices how the communicating devices or nodes interact with each other is called network architecture. It acts as the blueprint of any computer network that also defines network's performance, reliability and speed. It includes both physical layout and logical design.

Types of Network Architecture:

There are mainly two types of network architecture as follows:

a) Client/Server Architecture
b) Peer-to-Peer (P2P) Architecture

a) Client/Server Architecture:

A network architecture in which a dedicated server is used to provide the services as requested by the clients is called client/server architecture. Clients are the end devices, where the users run applications but the server is the most powerful computing device that handles the client's requests.

This type of architecture focuses on services and is considered best if data security is our major concern.

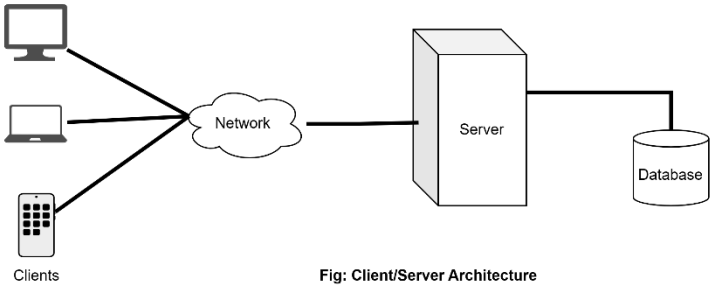

Fig: Client/Server Architecture

Advantages:

i. Provides centralized control over the data and resources.
ii. Easy to setup and configure.
iii. Data backup and recovery is easy.
iv. Provides high data security than P2P architecture.
v. More scalable and robust for business organizations and large networks.

Disadvantages:

i. Expensive to setup due to dedicated server.
ii. Failure of a server affect the whole network.
iii. Bottleneck issue is more common on increasing data traffics.
iv. Not suitable for smaller networks.
v. Efficiency decreases on increasing the number of devices.

b) Peer-to-Peer(P2P) Architecture:

A network architecture in which every computing node (i.e., peers) has equal authority to access the data and resources is called peer-to-peer architecture. Each peer acts as both client and server, so there is no need of dedicated server.

This type of architecture mainly focuses on connectivity and is considered best when data security is not our major concern. It is inexpensive to setup as compared to client/server architecture.

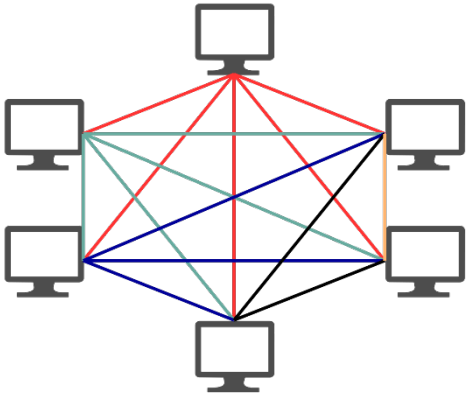

Fig: Peer-to-Peer (P2P) Architecture

Advantages:

i. Cheaper to setup as compared to client/server architecture.
ii. Failure of each peer doesn't affect others.
iii. Load balancing is better.
iv. No dedicated server is required to manage the entire connection.
v. Suitable for a computer network with smaller size.

Disadvantages:

i. Poor data security than client/server architecture.
ii. It is more complex to setup and configure the architecture.
iii. Each peer has to back-up its own data.
iv. Not scalable as client/server architecture.
v. Not appropriate for larger networks.

OSI (Open System Interconnection) Reference Model:

A network model introduced by ISO (International Organization for Standardization) for the reliable communication between the devices manufactured by different vendors or companies is called OSI reference model. It includes a set of protocols to perform specific tasks in each layer. It makes communication possible among inter-operability devices.

OSI-RM is a common standard that consists of 7 different layers and each layer has its own distinct function. That's why, it is also called layered architecture.

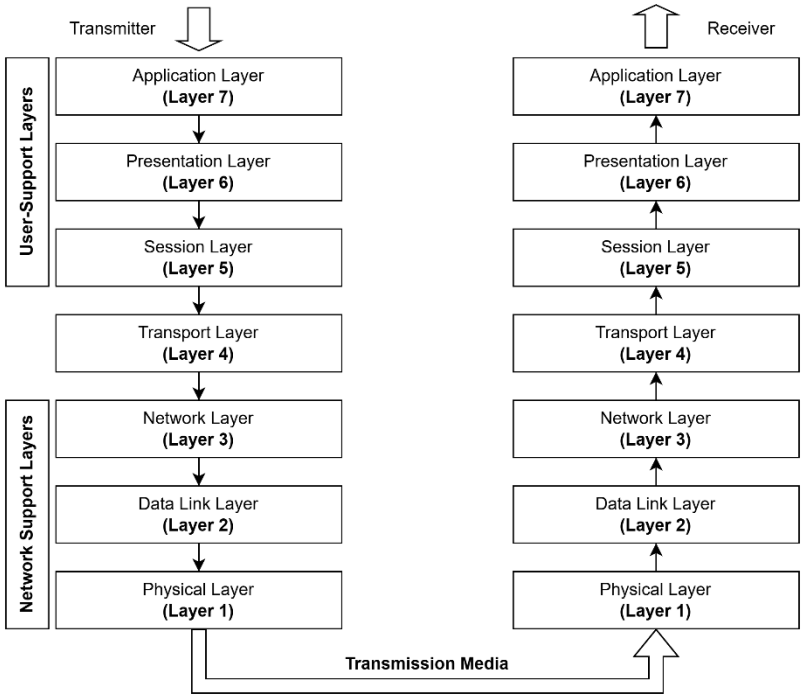

Fig: Layers of OSI Reference Model

a) **Application Layer:**
It is the layer 7 of OSI reference model that is mainly responsible for providing user interface to use the services like email services, remote file control, database services, etc. It uses the protocols like HTTP/HTTPS, FTP, SMTP, etc.

b) **Presentation Layer:**
It is the layer 6 of OSI reference model that is concerned with the translation, encryption/decryption and compression/decompression of the data sent by application layer. It changes the data to different formats that a computer can understand. Some common data formats are BCD(Binary Coded Decimal), ASCII(American Standard Code for Information Interchange), EBCDIC(Extended Binary Coded Decimal Interchange Code), etc.

c) **Session Layer:**
It is the layer 5 of OSI reference model responsible for dialog control, synchronization of data and session management. Session is the time

period required by a device to remain intact with another communicating device. Dialog control involves establishing, maintaining and terminating session.

d) **Transport Layer:**
It is the layer 4 of OSI reference model responsible for data segmentation and port addressing. Segmentation is the process of breaking down the data into smaller chunks called segments for the reliable delivery of data. Each segment is stamped with port number and sequence number.

e) **Network Layer:**
It is the layer 3 of OSI reference model that is responsible for logical addressing and routing. In this layer, IP (Internet Protocol) address of both sender and receiver is attached to each segment, transforming into packets. Routing involves identifying best route for data packets transmission.

f) **Data Link Layer:**
It is the layer 2 of OSI reference model that is responsible for data framing, physical addressing, flow control, error control and access control. The data packets sent by Network layer are stamped with MAC (Media Access Control) Address of both the sender and receiver in data link layer. The lost data packets are retransmitted to ensure reliable transfer of data packets.

g) **Physical Layer:**
It is the layer 1 of OSI reference model that deals with the physical characteristics of the transmission media, line configuration, transmission modes, and topology. It released data (i.e., stream of bits) into the communication media for its transmission.

IP (Internet Protocol) Address:

IP address is a numeric address assigned uniquely to each device in a computer network. It is assigned by a central authority called IANA (Internet Assigned Numbers Authority). It is a logical address that remains unique within a single network.

An IP address consists of two parts: Network ID and Host ID. It is represented in dotted decimal notation separated by periods or dots (.). The basic format of IPv4 address is:

XXXXXXXX. XXXXXXXX. XXXXXXXX. XXXXXXXX

Where, X represents a binary bit (either 0 or 1).

Example: 10000000.00000011.10100000.00001010

Decimal Notation: 128 . 3 . 160 . 10

Types of IP Address:

IP Addresses can be divided into two different types as:

a) IPv4 (Internet Protocol Version-4) Address
b) IPv6 (Internet Protocol Version-6) Address

a) IPv4 Address:

IPv4 is a 32 bits numeric address, consisting of 4 octets separated by periods. Each octet has 8 bits. The IPv4 address looks like the following:

In Binary Representation: 10000000.00000011.10100000.00001010

Decimal Notation: 128.3.160.10

IPv4 Classful Addressing:

IPv4 addresses can be classified into different classes to standardize the IP ranges across the devices connected in a network. It makes routing more efficient. The different classes of IPv4 addresses are:

i. Class-A IP Address
ii. Class-B IP Address
iii. Class-C IP Address
iv. Class-D IP Address
v. Class-E IP Address

i. **Class-A IP Address:**
It is a type of IPv4 address in which Network ID is 8 Bits long and Host ID is 24 Bits. The higher order bit of the first octet in Class-A IP Address is always set to zero (0). It is used for large sized networks as it can provide 2^{24} (16777216) Host addresses.
The Class-A IP header format is given below:

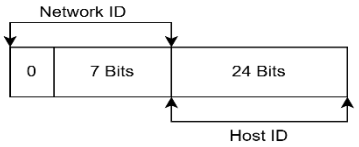

Fig: Class-A IP Address Header

It has a total of 2^7 (128) Network Addresses. The IP address for Class-A ranges from 0.0.0.0 to 127.255.255.255. But, 0.0.0.0 and 127.0.0.0 IPs are reserved. So, the usable IP address ranges from 1.0.0.0 to 126.255.255.255. The default subnet mask for Class-A is 255.0.0.0.

ii. **Class-B IP Address:**

It is a type of IP address in which Network ID is 16 Bits long and Host ID is 16 Bits. The higher order bits of first octet are always set to **10**. It is used for medium sized networks as it can provide 2^{16} (65,536) host addresses. The IP header format for Class-B IP is given below:

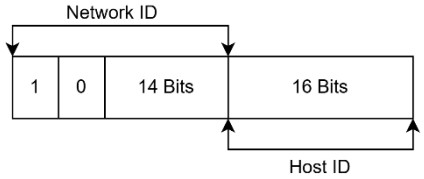

Fig: Class-B IP Address Header

Class-B IP address ranges from 128.0.0.0 to 191.255.255.255. It can provide 2^{14} (16,384) network addresses. The default subnet mask for Class-B IP address is 255.255.0.0.

iii. **Class-C IP Address:**

It is a type of IP address in which Network ID is 24 Bits long and Host ID is only 8 Bits long. The higher order bits of first octet in Class-C IP are always set to **110**. It is best for smaller networks as it can provide 2^8 (256) host addresses. The IP header for Class-C IP is given below:

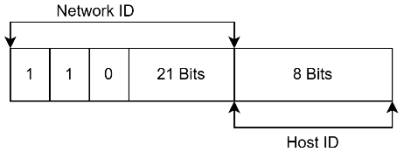

Fig: Class-C IP Address Header

Class C IP address has a total of 2^{21} (20,97,152) Network Addresses. The IP Address for Class-C ranges from 192.0.0.0 to 223.255.255.255. The default subnet mask for Class-C IP is 255.255.255.0.

b) <u>IPv6 Address:</u>

IPv6 is an IP address that uses alphanumeric characters to uniquely identify each device connected in a network. It is 128 Bits long and is written in hexadecimal values in 8 different groups separated by colons (:). Each group consists of 4 hexadecimal values and each of them requires a total of 16 bits to represent in binary.

IPv6 is a new addressing scheme that can address up to 4 times more devices than IPv4 can do. It has a larger address space characterized by better routing and mobility. The IPv6 header has the following format:

Fig: IPv6 Header Format

Example:

bc01:2a3f:33d0:0000:0001:1f2a:7d21:315c

<u>Note:</u>

- **Mac Address** is a physical address that is provided by the device manufacturer and assigned uniquely to every device. It is 48 bits long and is expressed in hexadecimal values separated by colons. Each group consists of 2 hexadecimal characters and there exists a total of 6 groups.
- Generic example of MAC address: fe:80:ec:1f:21:a9

<u>Transmission Impairments:</u>

The issues that may arise during the transmission of data due to imperfections of communication media are called transmission impairments. The defects or faults on transmission media cause transmission impairments. Some of the common transmission impairments are:

a) **Attenuation:**

The loss or the reduction in the energy of transmitting signal is called attenuation. Due to the external barriers and objects signals get absorbed and attenuation occurs.

b) **Noise:**

The unwanted signal or barrier that may affect the transmitting signal is called noise. This may cause transmission errors on the data.

c) **Echo:**
The reflected signal that gets generated during the propagation of transmitting signal is called echo.

d) **Singing:**
The echo that is out of control is called singing. It is the echo that gets generated continuously in the transmission media.

e) **Jitter:**
The time delay or variation of transmitting signals while reaching to the receiving device is called jitter.

f) **Distortion:**
The change in the shape or wave form of a transmitting signal is called distortion. It is more common in compound signal.

g) **Crosstalk:**
The interference created by a transmitting signal to another one flowing through the nearby medium is called crosstalk.

h) **Bandwidth:**
The total amount of data that can be transmitted by a communication media in a specific period of time is called bandwidth. The bandwidth for the digital systems is measured in bps (bits per second), whereas cps (cycles per second) for analog systems.

Internet:

Internet is a global public network that uses TCP/IP to connect the devices across the world. It was introduced by Mercantile Communication in Nepal for the first time. It has access to every people that's why, it is called public network.

The organizations that provide internet connectivity to the people so that they can access internet services are called ISPs (Internet Service Providers). The major ISPs of Nepal are NTC, Worldlink, Subisu, ViaNet, ClassicTech, CGNet, etc.

Intranet:

A private network that is designed for the organization or a company to provide services to the authorized users is called intranet. It has limited services and considered more secure than internet. It is only accessible to the users once they get authenticated.

Network Conencting Devices:

The hardware devices that are used while configuring a network are called network connecting devices. The most common network connecting devices are:

Devices	Description/Use cases
Switch	Multiport repeater that forwards data packets to the destination node after inspecting the packets
Router	Used for data routing, path determination so that data packets can be transmitted through best route
Bridge	Used to connect network segments that have similar protocols
Gateway	Used to connect multiple network segments with different protocols
NIC (Network Interface Card)	Used as an interface between the communication media and computer system
Repeater	Used to boost or strengthen the amplitude of the weak signal so that it can be transmitted in long distance