About the Book:
Data Communication and Computer Networks provides a comprehensive introduction to the fundamental concepts, technologies, and applications that form the backbone of modern communication systems. The book begins with the basics of data transmission, encoding, and error detection, before moving into detailed discussions on network topologies, protocols, switching techniques, and layered architectures such as the OSI and TCP/IP models. It highlights both theoretical foundations and practical applications, making it suitable for students, educators, and professionals. Special emphasis is given to emerging trends, including wireless communication, cloud networking, cybersecurity, and the role of data communication in the Internet of Things (IoT). Each chapter is designed with clear explanations, illustrations, and real-world examples to simplify complex concepts. By blending fundamentals with advanced topics, this book serves as a reliable guide for building a strong understanding of computer networks and preparing readers for academic, research, or industry pursuits.

Dr. R. NANDHAKUMAR
Mrs. M. DHAVAPRIYA

FOUNDATIONS OF DATA COMMUNICATION AND COMPUTER NETWORKS

Dr. Nandhakumar, working as Assistant Professor & Head, UG Dept. of CS (SF) in Nallamuthu Gounder Mahalingam College, Pollachi with 17+ years of Experience. Published 30 Journals in Scopus & UGC Care list.

Mrs. M. Dhavapriya, working as Assistant Professor, UG Dept. of CS in Nallamuthu Gounder Mahalingam College, Pollachi with 14 years' Experience.

9 786209 050350

LAP LAMBERT Academic Publishing

Dr. R. NANDHAKUMAR
Mrs. M. DHAVAPRIYA

FOUNDATIONS OF DATA COMMUNICATION AND COMPUTER NETWORKS

Dr. R. NANDHAKUMAR
Mrs. M. DHAVAPRIYA

FOUNDATIONS OF DATA COMMUNICATION AND COMPUTER NETWORKS

LAP LAMBERT Academic Publishing

Imprint
Any brand names and product names mentioned in this book are subject to trademark, brand or patent protection and are trademarks or registered trademarks of their respective holders. The use of brand names, product names, common names, trade names, product descriptions etc. even without a particular marking in this work is in no way to be construed to mean that such names may be regarded as unrestricted in respect of trademark and brand protection legislation and could thus be used by anyone.

Cover image: www.ingimage.com

Publisher:
LAP LAMBERT Academic Publishing
is a trademark of
Dodo Books Indian Ocean Ltd. and OmniScriptum S.R.L publishing group

120 High Road, East Finchley, London, N2 9ED, United Kingdom
Str. Armeneasca 28/1, office 1, Chisinau MD-2012, Republic of Moldova, Europe
Managing Directors: Ieva Konstantinova, Victoria Ursu
info@omniscriptum.com

Printed at: see last page
ISBN: 978-620-9-05035-0

TABLE OF CONTENTS

1. INTRODUCTION TO COMPUTER NETWORKS

1.1 Data Communication

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

1.1.1 Components:

A data communications system has five components.

1. Message

2. Sender

3. Receiver

4. Transmission Medium

5. Set of rules (Protocol)

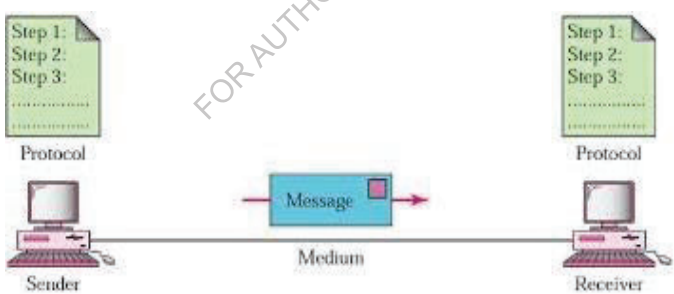


Fig 1.1: Process Communication

1. Message:

The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender:

The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver:

The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium:

The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves

5. Protocol:

A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

1.1.2 Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (Os or 1s).

Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers:

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. *For example*, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image. After an image is divided into pixels, each pixel is assigned a bit pattern.

The size and the value of the pattern depend on the image. For an image made of only blackand- white dots (e.g., a chessboard), a I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images.

One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it.

Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio:

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video:

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again we can change video to a digital or an analog signal.

1.2. Types of Communication in Data Communications:

Data Communication and Computer Networks, communication refers to the transmission of data between devices or systems. The types of communication can be classified in several ways:

1.2.1. Based on Direction of Data Flow

Type	Description	Example
Simplex	One-way communication. Data flows in only one direction.	Keyboard → Computer, TV broadcasting
Half-Duplex	Two-way communication, but only one direction at a time.	Walkie-talkies
Full-Duplex	Two-way communication, both directions simultaneously.	Telephone calls, Internet

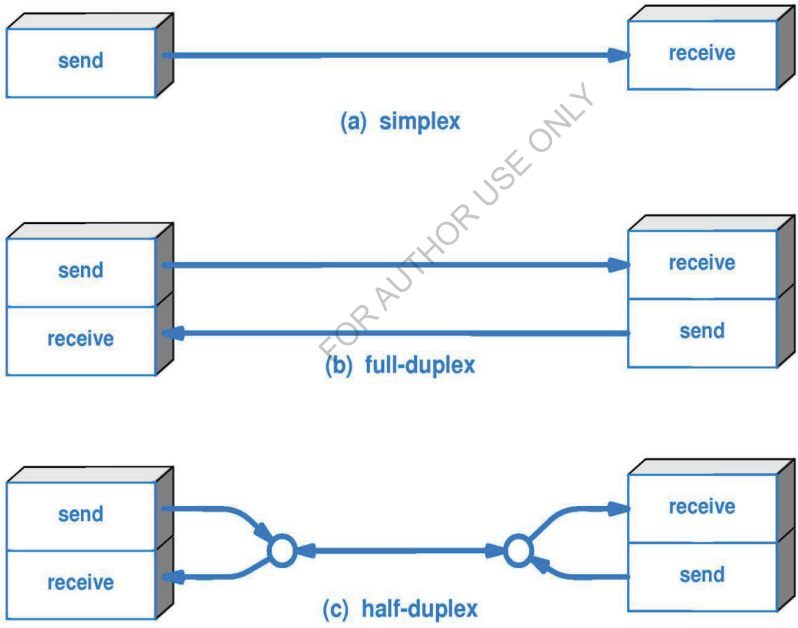


Fig 1.2: Types of Communication

1.2.2. Based on Transmission Technology

Type	Description	Example
Serial Communication	Data is sent one bit at a time over a single channel.	USB, RS-232
Parallel Communication	Multiple bits sent simultaneously over multiple channels.	Printer cables (old), data buses

1.2.3. Based on Mode of Transmission (Data Exchange)

Type	Description	Example
Synchronous	Data is sent in a continuous stream with synchronization.	Real-time voice/video
Asynchronous	Data sent in small packets with start/stop bits.	Email, SMS
Isochronous	Data is sent at regular intervals, time-sensitive.	Video conferencing, VoIP

1.2.4. Based on Communication Channels

Type	Description	Example
Wired Communication	Uses cables (coaxial, fiber optic, twisted pair) for transmission.	Ethernet, DSL
Wireless Communication	Uses electromagnetic waves to transmit data.	Wi-Fi, Bluetooth, Satellite

1.2.5. Based on Communication Scope

Type	Description	Example
LAN	Local Area Network, small geographic area	Office, Home
MAN	Metropolitan Area Network	City-wide cable networks
WAN	Wide Area Network	Internet, Global Networks
PAN	Personal Area Network	Bluetooth devices, Smartwatch

2. ERROR CLASSIFICATION IN DATA COMMUNICATION

In data communication, errors occur when the received data is different from the sent data. Errors can be introduced due to noise, interference, or faults in the transmission medium. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Data (Implemented either at the Data link layer or Transport Layer of the OSI Model) may get scrambled by noise or get corrupted whenever a message is transmitted. To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

2.1. Types of Errors:

Error Type	Description	Example
Single-bit Error	Only **one bit** in the data unit is altered.	Sent: 10010100 → Received: 10011100
Burst Error	**Two or more bits** are altered in the data unit.	Sent: 10010100 → Received: 11011110

2.2. Error Detection in Computer Networks

To detect errors, a common technique is to introduce redundancy bits that provide additional information. Various techniques for error detection include:

- Simple Parity Check
- Two-Dimensional Parity Check
- Checksum
- Cyclic Redundancy Check (CRC)

2.2.1. Simple Parity Check

Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.

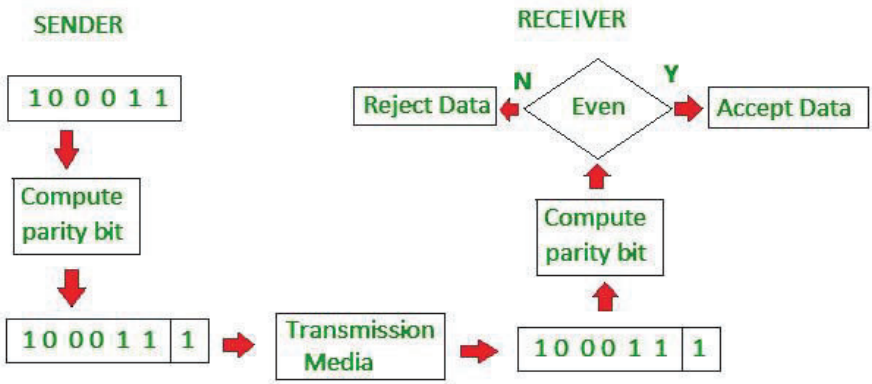


Fig 2.1: Simple Parity Check

Advantages of Simple Parity Check

- Simple parity check can detect all single bit error.
- Simple parity check can detect an odd number of errors.
- **Implementation**: Simple Parity Check is easy to implement in both hardware and software.
- **Minimal Extra Data**: Only one additional bit (the parity bit) is added per data unit (e.g., per byte).
- **Fast Error Detection**: The process of calculating and checking the parity bit is quick, which allows for rapid error detection without significant delay in data processing or communication.
- **Single-Bit Error Detection**: It can effectively detect single-bit errors within a data unit, providing a basic level of error detection for relatively low-error environments.

Disadvantages of Simple Parity Check

- Single Parity check is not able to detect even no. of bit error.
- **For example,** the Data to be transmitted is **101010**. Codeword transmitted to the receiver is 1010101 (we have used even parity).

  Let's assume that during transmission, two of the bits of code word flipped to 1111101.

  On receiving the code word, the receiver finds the no. of ones to be even and hence **no error,** which is a wrong assumption.

2.2.2. Two-Dimensional Parity Check

Two-dimensional Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, and then both are sent along with the data. At the receiving end, these are compared with the parity bits calculated on the received data.

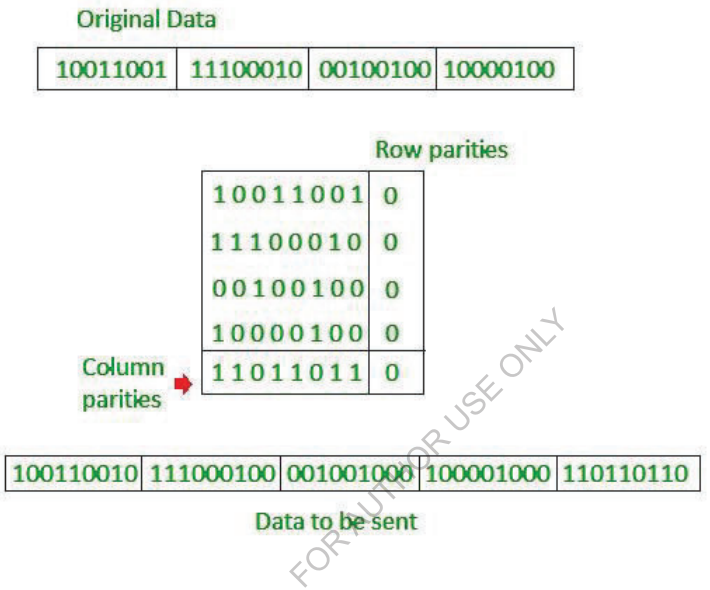


Fig 2.2: Two-Dimensional Parity Check

Advantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check can detect and correct all single bit error.
- Two-Dimensional Parity Check can detect two or three bit error that occur anywhere in the matrix.

Disadvantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check cannot correct two or three bit error. It can only detect two or three bit error.
- If we have a error in the parity bit then this scheme will not work.

2.2.3. Checksum

Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these

segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.

Checksum - Operation at Sender's Side

- Firstly, the data is divided into k segments each of m bits.
- On the sender's end, the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.

Checksum - Operation at Receiver's Side

- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

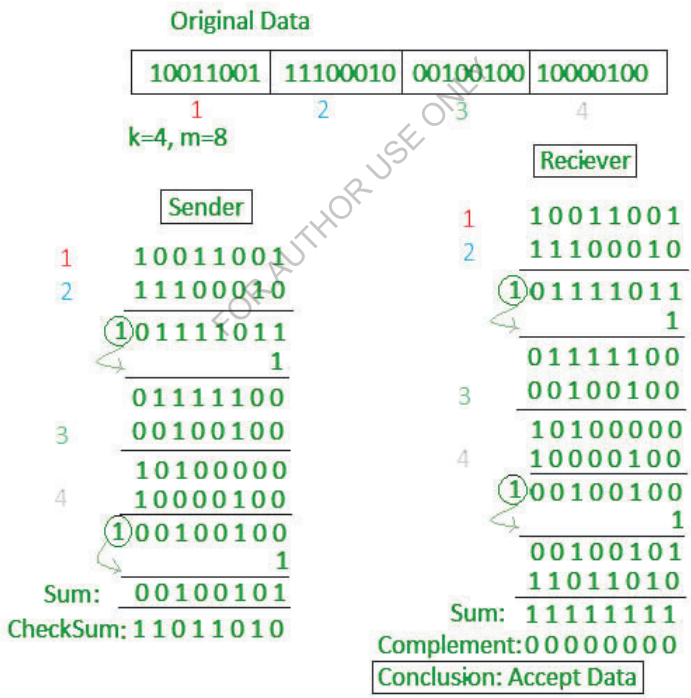


Fig 2.3: Checksum

2.2.4. Cyclic Redundancy Check (CRC)

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

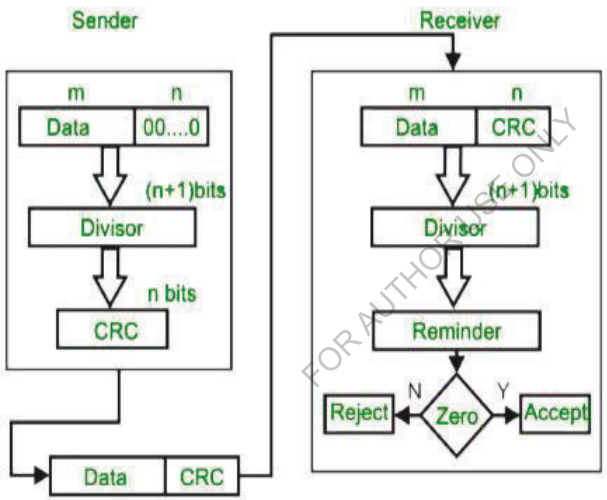


Fig 2.4: Cyclic Redundancy Check

CRC Working

We have given data word of length n and divisor of length k.

Step 1: Append (k-1) zero's to the original message

Step 2: Perform modulo 2 division

Step 3: Remainder of division = CRC

Step 4: Code word = Data with append k-1 zero's + CRC

Note:

- CRC must be k-1 bits
- Length of Code word = n+k-1 bits

Example:

Let's data to be send is 1010000 and divisor in the form of polynomial is x3+1. ***CRC method discussed below.***

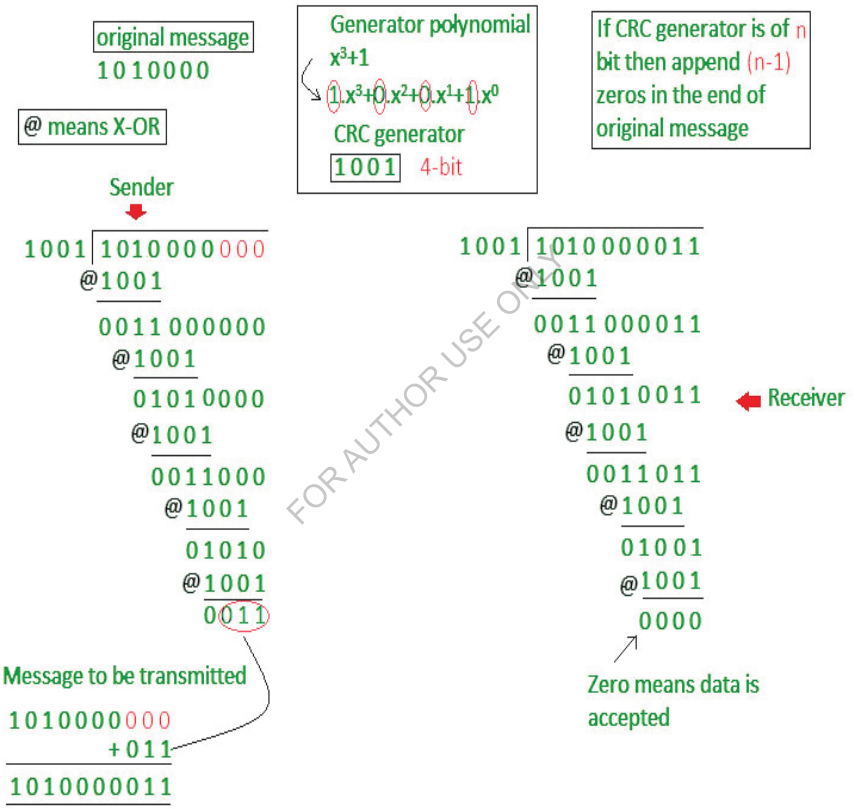


Fig 2.5 CRC method

2.2.5. Advantages of Error Detection

- **Increased Data Reliability:** Error detection ensures that the data transmitted over the network is reliable, accurate, and free from errors. This ensures that the recipient receives the same data that was transmitted by the sender.
- **Improved Network Performance:** Error detection mechanisms can help to identify and isolate network issues that are causing errors. This can help to improve the overall performance of the network and reduce downtime.
- **Enhanced Data Security:** Error detection can also help to ensure that the data transmitted over the network is secure and has not been tampered with.

2.2.6.Disadvantages of Error Detection

- **Overhead**: Error detection requires additional resources and processing power, which can lead to increased overhead on the network. This can result in slower network performance and increased latency.
- **False Positives:** Error detection mechanisms can sometimes generate false positives, which can result in unnecessary retransmission of data. This can further increase the overhead on the network.
- **Limited Error Correction:** Error detection can only identify errors but cannot correct them. This means that the recipient must rely on the sender to retransmit the data, which can lead to further delays and increased network overhead.

3. COMMUNICATION CHANNELS

Communication channels are the medium that connects two or more workstations. Workstations can be connected by either wired media or wireless media. It is also known as a transmission medium.

The transmission medium or channel is a link that carries messages between two or more devices. We can group the communication media into two categories:

- **Guided media transmission**
- **Unguided media transmission**

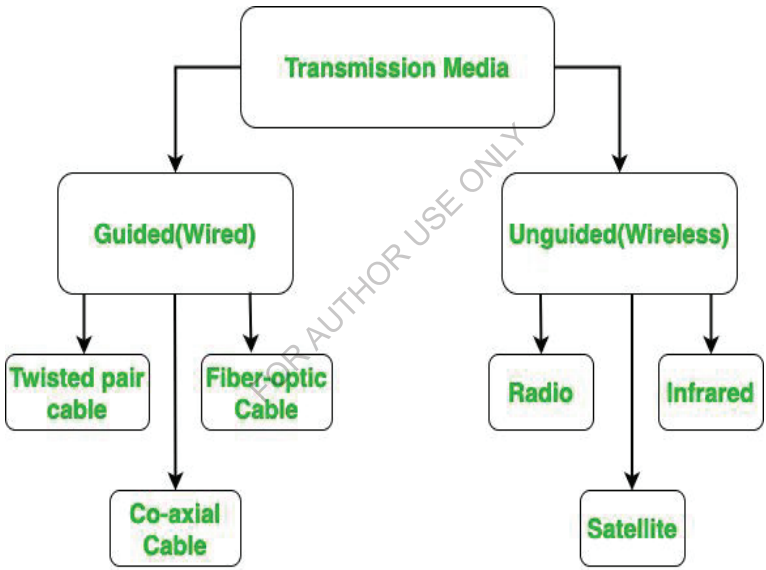


Fig 3.1 Transmission Media

3.1.Guided Media

Guided or Wired media allows signal energy enclosed and guided within a physical medium. This media is used either for point-to-point links or a shared link with various connections. In guided media, interruption is generated by outputs in the adjacent cables. Proper covering of guided media is required to reduce the interruption problem.

3.1.1. Twisted pair cable: It is the most common form of wire used in communication. In a twisted-pair cable, two identical wires are wrapped together in a double helix. The twisting of the wire reduces the crosstalk. It is known as the leaking of a signal from one wire to another due to which signal can corrupt and can cause network errors. The twisting protects the wire from internal crosstalk as well as external forms of signal interference.

Types of Twisted Pair Cable:

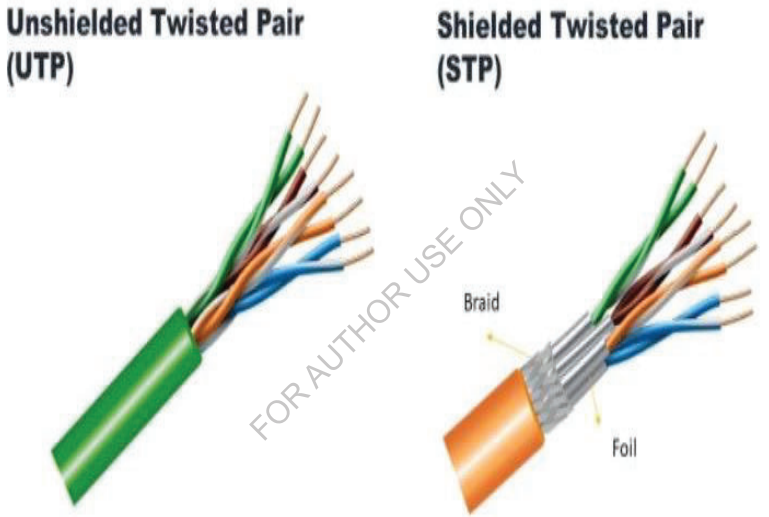


Fig 3.2: Types of Twisted Pair Cable

- **Unshielded Twisted Pa ir (UTP):** It is used in computers and telephones widely. As the name suggests, there is no external shielding so it does not protects from external interference. It is cheaper than STP.
- **Shielded Twisted Pair (STP):** It offers greater protection from crosstalk due to shield. Due to shielding, it protects from external interference. It is heavier and costlier as compare to UTP.

3.1.2. Coaxial Cable:

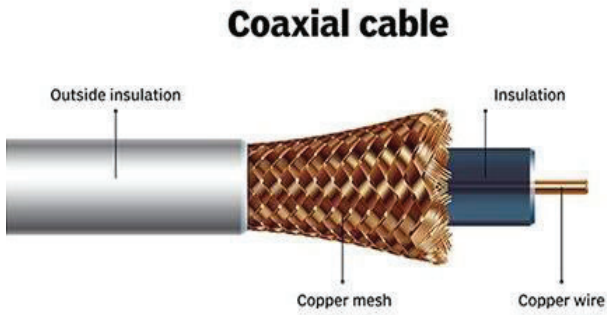


Fig 3.3: Coaxial Cable

It consists of a solid wire core that is surrounded by one or more foil or wire shields. The inner core of the coaxial cable carries the signal and the outer shield provides the ground. It is widely used for television signals and also used by large corporations in building security systems. Data transmission of this cable is better but expensive as compared to twisted pair.

3.1.3. Optical fibers:

Optical fiber is an important technology. It transmits large amounts of data at very high speeds due to which it is widely used in internet cables. It carries data as a light that travels inside a thin glass fiber.

The fiber optic cable is made up of three pieces:

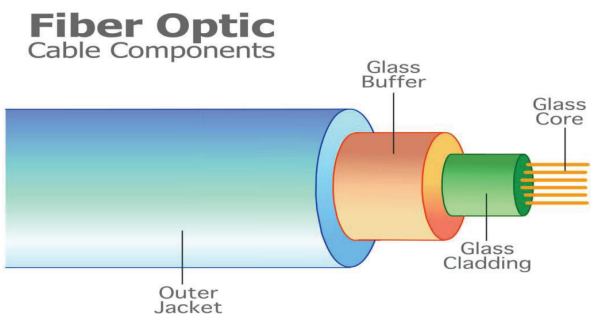


Fig 3.4: Optical Fiber

1. **Core:** Core is the piece through which light travels. It is generally created using glass or plastic.
2. **Cladding:** It is the covering of the core and reflects the light back to the core.
3. **Sheath:** It is the protective covering that protects fiber cable from the environment.

3.2.Unguided Media

The unguided transmission media is a transmission mode in which the signals are propagated from one device to another device wirelessly. Signals can wave through the air, water, or vacuum. It is generally used to transmit signals in all directions. Unguided Media is further divided into various parts:

***3.2.1. Microwave*:** Microwave offers communication without the use of cables. Microwave signals are just like radio and television signals. It is used in long-distance communication. Microwave transmission consists of a transmitter, receiver, and atmosphere. In microwave communication, there are parabolic antennas that are mounted on the towers to send a beam to another antenna. The higher the tower, the greater the range.

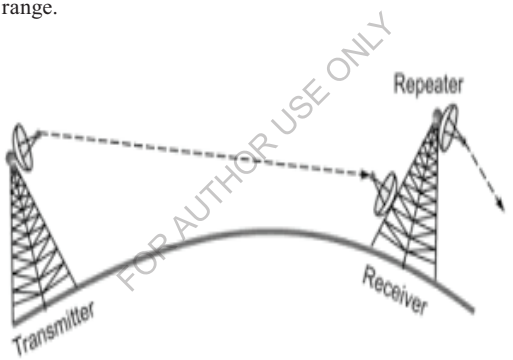


Fig 3.5: Microwave Transmission

Advantages:

- Cheaper than using cables
- Freedom from land acquisition
- Ease of communication in difficult terrains
- Communication over oceans

Disadvantages:

- Insecure communication.
- Out of phase signal.

- Susceptible to weather conditions.
- Bandwidth is limited.
- High cost of design, implementation, and maintenance.

3.2.2. Radio wave: When communication is carried out by radio frequencies, then it is termed radio waves transmission. It offers mobility. It is consists of the transmitter and the receiver. Both use antennas to radiate and capture the radio signal.

Radio Wave Components:

Transmitter: Responsible for encoding the signal.

Receiver: Responsible for decoding the signal.

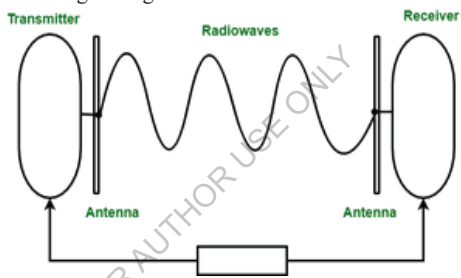


Fig 3.6: Radio Wave Components

3.2.3. Infrared: It is short-distance communication and can pass through any object. It is generally used in TV remotes, wireless mouse, etc.

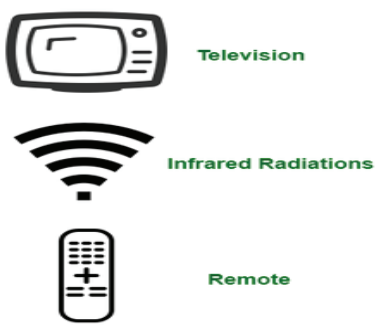


Fig 3.7: Infrared Communication

3.3. Comparison:

Guided Media (Wired/Bounded Media)

Type	Description	Speed & Bandwidth	Common Use Cases
Twisted Pair Cable	Two insulated copper wires twisted together to reduce interference.	Low to Moderate	Telephone lines, LANs
Unshielded (UTP)	No shielding, cheaper and widely used.		Ethernet cables
Shielded (STP)	Shielded to reduce EMI (electromagnetic interference).		Industrial networks
Coaxial Cable	Central conductor + insulating layer + metal shield + outer cover.	Moderate	Cable TV, broadband internet
Fiber Optic Cable	Uses light to transmit data; immune to EMI, long-distance and high speed.	Very High (Gbps-Tbps)	Internet backbone, WANs, ISPs

Unguided Media (Wireless/Unbounded Media)

Type	Description	Range	Common Use Cases
Radio Waves	Omni-directional, used for long-distance broadcasting.	Long	AM/FM Radio, Mobile networks
Microwaves	Line-of-sight (LOS), high frequency waves.	Medium to Long	Satellite, Cellular networks
- Terrestrial Microwave	Requires antennas placed on towers.	~50 km per hop	TV transmission, 4G towers
- Satellite Microwave	Signal sent to satellite and bounced back to earth station.	Global	GPS, Satellite TV, internet
Infrared (IR)	Short-range, cannot penetrate walls.	Very Short	TV remotes, wireless mouse
Bluetooth	Short-range wireless communication (PAN).	~10 meters	Wireless peripherals, IoT
Wi-Fi	Wireless LAN using radio waves (IEEE 802.11 standards).	30–100 meters	Home and office networks

4. NETWORK TOPOLOGY

Network topology refers to the physical and logical arrangement of devices and connections in a computer network. ***It defines how computers, routers, switches, and other network components are interconnected and how data flows between them***.

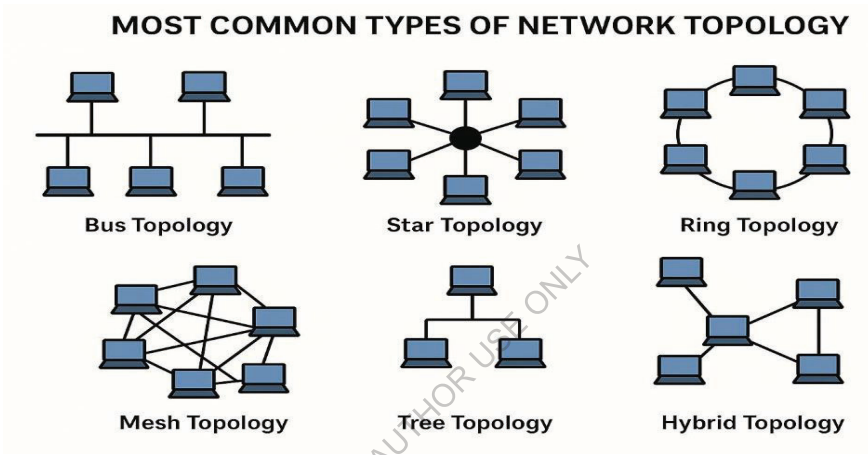


Fig 4.1: Types of Topology

4.1.Bus Topology:

All devices connect to a single cable (the bus).

Pros: Simple, inexpensive for small networks.

Cons: Difficult to troubleshoot, single point of failure.

4.2.Star Topology:

All devices connect to a central hub or switch.

Pros: Easy to install and manage, centralized control.

Cons: Single point of failure at the central device.

4.3.Ring Topology:

Devices connect in a closed loop, with data flowing in one direction.

Pros: Simple, can handle high traffic.

Cons: Difficult to troubleshoot, failure of one device can disrupt the entire network.

4.4.Mesh Topology:

Devices are interconnected with multiple paths, providing redundancy.

Pros: Highly reliable, fault-tolerant.

Cons: Complex and expensive to implement.

4.5.Tree Topology:

A hierarchical structure, combining characteristics of bus and star topologies.

Pros: Scalable, good for larger networks.

Cons: Can be complex, single point of failure at the root.

4.6. Hybrid Topology:

Combines two or more different topologies.

Pros: Flexibility to adapt to specific needs.

Cons: Can be complex to design and manage.

4.7.Comparison Table:

Topology	Cost	Cable Length	Scalability	Reliability	Use Case
Bus	Low	Low	Low	Low	Small offices, old LANs
Star	Medium	Medium	High	Medium	Homes, offices (Ethernet)
Ring	Medium	Medium	Low	Medium	Legacy systems (FDDI)
Mesh	High	Very High	Low	Very High	Military, mission-critical apps
Tree	High	High	High	Medium	Universities, large organizations
Hybrid	High	Depends	Very High	High	Internet, enterprise networks

5. OSI REFERENCE MODEL

The Open Systems Interconnection Model (OSI Model) is a conceptual model that describes how data is transmitted from one system to another system irrespective of distance and location. It consists of seven-layer architecture. All seven layers contribute to the transmission of data from one system to another system. All the seven layers are shown in the diagram below.

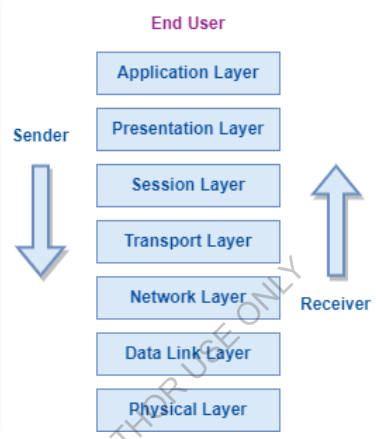


Fig 4.2: OSI Layers

5.1. Physical Layer:

The Physical Layer is the lowest layer of the OSI model. It is responsible for transmitting individual bits from over a medium. It converts the bits into signals. The bit rate or data rate control is done at the physical layer. It is also responsible for how the actual physical devices are connected.

Some of the functionalities of the physical layer are:

Physical topology - It defines the arrangement of the devices in a network.

Data rate - Data rate or the number of bits sent per second is controlled by the physical layer.

Transmission mode - It is the data flow between two devices.

It is of three types.

Simplex - Data flows in one direction only.

Half-duplex - Data flows in both directions but not at the same time.

Full-duplex - Data flows in both directions at the same time.

5.2. Data Link Layer:

The data link layer acts as a link between two nodes and transfers data or frames from one node to another node. Frames are created by the data link layer. It is the responsibility of the data link layer to transfer the error-free data from one node to another node.

It is divided into two sub-layers.

Media Access Control (MAC) - It is responsible for controlling devices' access to a medium.

Logical Link Control (LLC) - It is responsible for frame synchronization, identification of network layer protocol, and error control.

Some of the functionalities of the data link layer are:

Framing - The data in the form of bits are grouped in packets called frames. Frames are made identifiable to the receiver by attaching special bit patterns as the header or trailer of the frame.

Physical Addressing - The data link layer adds the MAC address (physical address) of the sender and the receiver for the smooth transmission of the data.

Flow Control - Flow control is necessary for saving the data from being corrupted. It is done by maintaining the constant data rate on both sender and receiver ends.

Error Control - This is the function of the data link layer to transfer the non-erroneous data. The erroneous data are traced and retransmitted by the data link layer.

Access Control - The data link layer helps to determine which device has control over a link shared by multiple devices.

5.3. Network Layer:

The Network Layer is responsible for transferring the data from the source to the destination by routing it through the intermediate nodes. Among the different possible paths, it chooses the best possible path to transfer the data from source to destination.

Some of the functionalities of the network layer are:

Packetizing - If the message to be is large to be transmitted, it is split into several fragments and then delivered independently and reassembled at the destination node.

Logical Addressing - The network layer adds the IP address of the source and destination to the header of the frames for its identification among all the devices.

Routing - The best possible path is chosen by the network layer for the transfer of the data from source to destination and this is called routing.

5.4. Transport Layer:

The transport layer creates various smaller units called segments out of the message received from the application layer. It adds source and destination port numbers in the header for the right transfer of the data. The main responsibility of the transport layer is the end-to-end delivery of the message and to ensure flow and error control.

Some of the functionalities of the transport layer are:

Segmentation - The message received from the upper layer is divided into smaller units called segments and is reassembled at the destination by the transport layer.

Port Addressing - The source and destination port numbers are added to the header for the correct handover of the data.

Connection Control - There can be two types of services between two devices

Connection-Oriented - In this, the connection is established for the data transmission and is disconnected after the transmission.

Connectionless - It is less reliable and faster and doesn't require establishing a connection before data transmission.

Error Control - It checks for erroneous data and retransmits the data on a failed delivery.

5.5. Session Layer:

The main responsibility of the session layer is to establish, maintain and synchronize the communication among the devices. It allows communication either in half-duplex or full-duplex. It synchronizes the communication between the devices to avoid data loss.

Some of the functionalities of the session layer are:

Dialog Control - It allows communication between two systems in half-duplex or full-duplex.

Synchronization - It allows a process to add checkpoints to avoid data loss during a crash.

5.6. Presentation Layer - The presentation layer establishes context between application layer entities. The main responsibility of the presentation layer is concerning the syntax and semantics of the data

exchange between the devices. It transforms data into the form that the application accepts. It is also sometimes called the syntax layer.

Some of the functionalities of the presentation layer are:

Translation - It is the conversion of the data into a commonly acceptable format.

Encryption - Encryption is done to secure the data from unauthorized access. The data is converted into a different code that is not understandable and is decrypted into an understandable form at the receiver's end.

Compression - Compression means compressing the data that is reducing the number of bits that need to be transmitted. It is helpful in the transfer of multimedia messages.

5.7. Application Layer:

This is the closest layer to the end-user. It interacts directly with the software application. It acts as a window for the user and the software applications to access network services. It handles identifying communication partners and determining resource availability.

Some of the functionalities of the application layer are:

File transfer and access management - This allows the user to access the files on a remote computer.

Mail services - It provides access to send or receive email.

Summary:

Layer	Name	Example Protocols	Role
7	Application	HTTP, FTP, SMTP, DNS	User interface, network services **(e.g., browser, email)**
6	Presentation	SSL, JPEG, ASCII, MPEG	Data format, encryption, **compression**
5	Session	NetBIOS, RPC, PPTP	Session control
4	Transport	TCP, UDP	Reliable delivery, segmentation
3	Network	IP, ICMP, OSPF, RIP	Routing, addressing
2	Data Link	Ethernet, MAC, PPP	Physical addressing, framing
1	Physical	Cables, Hubs, NIC, Modem	Transmitting raw bits

6. TYPES OF NETWORKS

6.1. Introduction

In today's interconnected world, networks play a vital role in communication, data exchange, business operations, and daily life. A network can be defined as a system that enables multiple devices—such as computers, mobile phones, printers, and servers—to communicate and share resources like files, applications, and the internet.

Networks are not uniform; they vary in scale, design, and purpose. For example, a small home setup connecting a laptop to a printer is a type of network, while the Internet, which spans the globe and connects billions of devices, is also a network. This chapter explores the different types of networks, their characteristics, applications, and advantages.

6.2 Classification of Networks

Networks can be classified based on:

- **Coverage Area (Geographical Range)**
- **Architecture (How resources are organized)**
- **Topology (How devices are arranged)**
- **Specialization (Purpose-built networks)**

6.2.1 Networks Based on Geographical Area

(a) Personal Area Network (PAN)

A **PAN** is the smallest type of network, designed for an individual's personal devices.

- **Range:** Up to 10 meters.
- **Technologies:** Bluetooth, Infrared, NFC.
- **Applications:**
    - Connecting wireless headphones or smartwatches.
    - File sharing between a smartphone and laptop.

- Tethering mobile internet to another device.

Example: Connecting a fitness tracker to a mobile phone via Bluetooth.

(b) Local Area Network (LAN)

A **LAN** connects devices within a limited area, such as a home, office, or campus.

- **Range:** Up to a few kilometers.
- **Technologies:** Ethernet cables, Wi-Fi.
- **Applications:**
  - Sharing printers and scanners in offices.
  - Accessing centralized files in a lab.
  - Online multiplayer gaming in cafes.

Case Study: A college campus LAN links classrooms, labs, and the library.

(c) Metropolitan Area Network (MAN)

A **MAN** covers a city or metropolitan region.

- **Range:** 10–50 km.
- **Technologies:** Fiber optics, microwave links, WiMAX.
- **Applications:**
  - Broadband services provided by ISPs.
  - City-wide Wi-Fi in public places.
  - Linking municipal offices.

(d) Wide Area Network (WAN)

A **WAN** spans across countries or continents, interconnecting multiple LANs and MANs.

- **Range:** Unlimited (global).
- **Technologies:** Satellite communication, fiber optics, leased lines.
- **Applications:**

- The **Internet** (largest WAN).
- Banking networks connecting ATMs.
- Corporate global branches.

(e) Global Area Network (GAN)

A **GAN** is an interconnected worldwide network that integrates multiple WANs.

- **Range:** Worldwide.
- **Applications:**
  - Satellite internet.
  - International mobile roaming.
  - Global airline communication systems.

6.2.2 Networks Based on Architecture

(a) Client–Server Network

- **Structure:** Centralized; servers provide services to multiple clients.
- **Advantages:** High security, centralized management, scalable.
- **Disadvantages:** Costly, dependent on server availability.
- **Example:** Banking systems, school databases.

(b) Peer-to-Peer (P2P) Network

- **Structure:** All devices are equal and share resources directly.
- **Advantages:** Cost-effective, easy to set up.
- **Disadvantages:** Limited security, not scalable.
- **Example:** File-sharing networks like BitTorrent.

6.2.3 Networks Based on Topology

Network topology is the physical or logical arrangement of devices.

- **Bus Topology:** One main cable; easy but prone to failure.

- **Star Topology:** All nodes connect to a central hub; reliable but hub-dependent.
- **Ring Topology:** Nodes connected in a circle; data passes in one direction.
- **Mesh Topology:** Every node connects to multiple nodes; very reliable but expensive.
- **Hybrid Topology:** Combination of two or more topologies.

6.2.4 Specialized Networks

- **Storage Area Network (SAN):** High-speed network connecting storage devices to servers.
- **Virtual Private Network (VPN):** Secure connection over public networks.
- **Wireless Networks:** Wi-Fi, WiMAX, Cellular (2G–5G).
- **Enterprise Private Network (EPN):** Built by organizations for secure communication across branches.

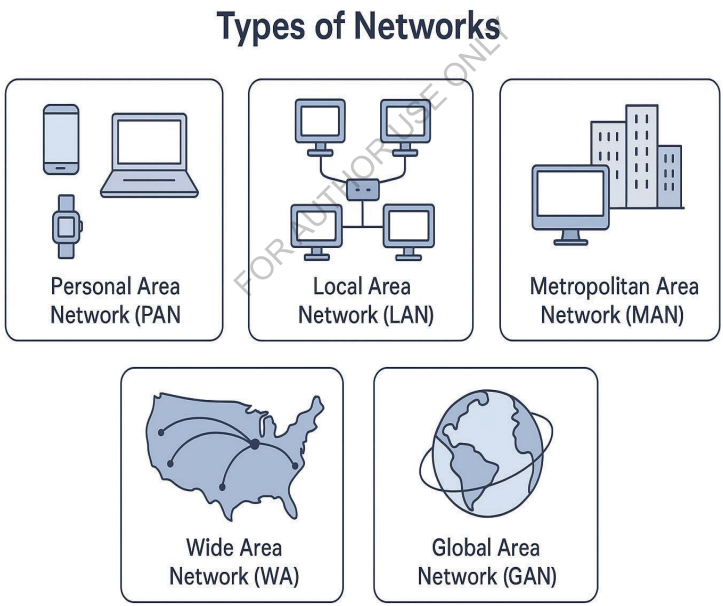


Fig 6.1: Types of Networks

6.3 Comparative Summary

Type	Coverage Area	Technology	Examples	Applications
PAN	Few meters	Bluetooth, NFC	Smartwatch, earbuds	Personal device connectivity
LAN	Few km	Wi-Fi, Ethernet	Office Wi-Fi, labs	File & printer sharing
MAN	Up to 50 km	Fiber, WiMAX	City broadband	Municipal, ISP services
WAN	Global	Satellite, Fiber	Internet, ATMs	Cloud, e-commerce
GAN	Worldwide	Satellite	Mobile roaming	International services

6.4 Advantages and Disadvantages of Different Networks

- **PAN: Easy and low-cost, but very limited range.**
- **LAN: High speed and secure, but restricted to small areas.**
- **MAN: Useful for cities, but requires expensive infrastructure.**
- **WAN: Global access, but high setup and maintenance costs.**
- **GAN: Enables worldwide communication, but depends on satellite technology.**

7. SWITCHING

7.1. What is Switching?

Switching is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called **switches**. A computer user experiences switching all the time for example, accessing the Internet from your computer device, whenever a user requests a webpage to open, the request is processed through switching of data packets only.

Switching takes place at the Data Link layer of the OSI Model. This means that after the generation of data packets in the Physical Layer, switching is the immediate next process in data communication.

Introduction to Switch

- A switch is a hardware device in a network that connects and helps multiple devices share a network without their data interfering with each other.
- A switch works like a traffic cop at a busy intersection. When a data packet arrives, the switch decides where it needs to go and sends it through the right port.
- Some data packets come from devices directly connected to the switch, like computers or VoIP phones. Other packets come from devices connected through hubs or routers.
- The switch knows which devices are connected to it and can send data directly between them. If the data needs to go to another network, the switch sends it to a router, which forwards it to the correct destination.

7.2.What is Network Switching?

A switch is a dedicated piece of computer hardware that facilitates the process of switching i.e., incoming data packets and transferring them to their destination. A switch works at the Data Link layer of the OSI Model. A switch primarily handles the incoming data packets from a source computer or network and decides the appropriate port through which the data packets will reach their target computer or network.

A switch decides the port through which a data packet shall pass with the help of its destination MAC(Media Access Control) Address. A switch does this effectively by maintaining a switching table, (also known as forwarding table). A network switch is more efficient than a network Hub or repeater because it maintains a switching table, which simplifies its task and reduces congestion on a network, which effectively improves the performance of the network.

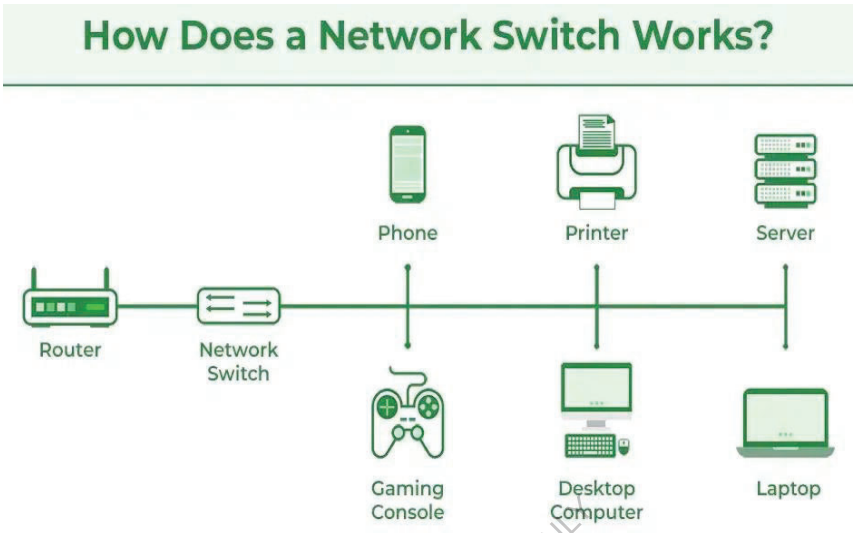


Fig 7.1: Working of Network Switch

The switching process involves the following steps:

- **Frame Reception:** The switch receives a data frame or packet from a computer connected to its ports.
- **MAC Address Extraction:** The switch reads the header of the data frame and collects the destination MAC Address from it.
- **MAC Address Table Lookup:** Once the switch has retrieved the MAC Address, it performs a lookup in its Switching table to find a port that leads to the MAC Address of the data frame.
- **Forwarding Decision and Switching Table Update:** If the switch matches the destination MAC Address of the frame to the MAC address in its switching table, it forwards the data frame to the respective port. However, if the destination MAC Address does not exist in its forwarding table, it follows the flooding process, in which it sends the data frame to all its ports except the one it came from and records all the MAC Addresses to which the frame was delivered. This way, the switch finds the new MAC Address and updates its forwarding table.
- **Frame Transition:** Once the destination port is found, the switch sends the data frame to that port and forwards it to its target computer/network.

7.3.Types of Switching

There are three types of switching methods:

- Message Switching
- Circuit Switching
- Packet Switching
    - Datagram Packet Switching
    - Virtual Circuit Packet Switching

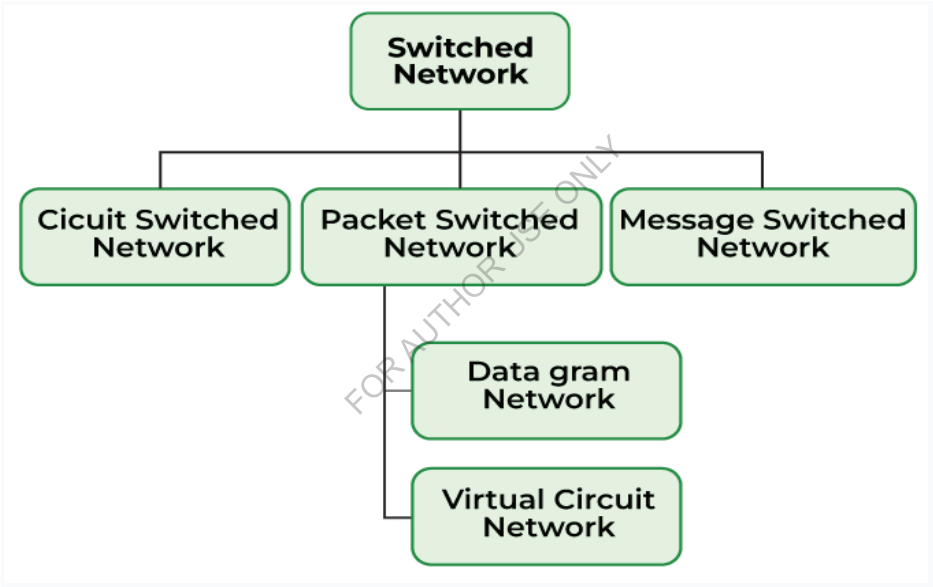


Fig 7.2: Types of Switching

7.3.1. Message Switching: This is an older switching technique that has become obsolete. In message switching technique, the entire data block/message is forwarded across the entire network thus, making it highly inefficient.

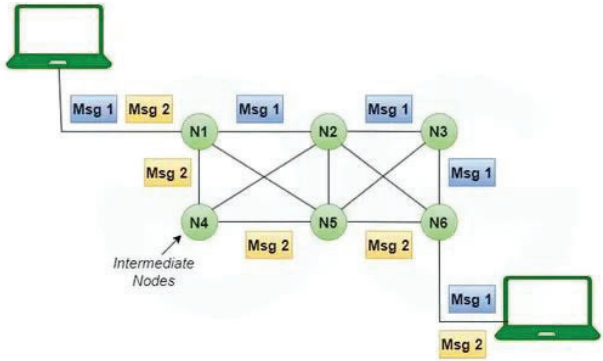


Fig 7.3: Message Switching

7.3.2. Circuit Switching: In this type of switching, a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely. This approach is better than message switching as it does not involve sending data to the entire network, instead of its destination only.

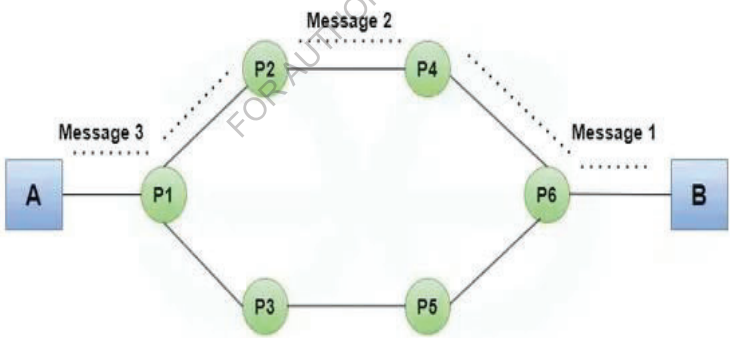


Fig 7.4: Circuit Switching

7.3.3. Packet Switching: This technique requires the data to be broken down into smaller components, data frames, or packets. These data frames are then transferred to their destinations according to the available resources in the network at a particular time. This switching type is used in

modern computers and even the Internet. Here, each data frame contains additional information about the destination and other information required for proper transfer through network components.

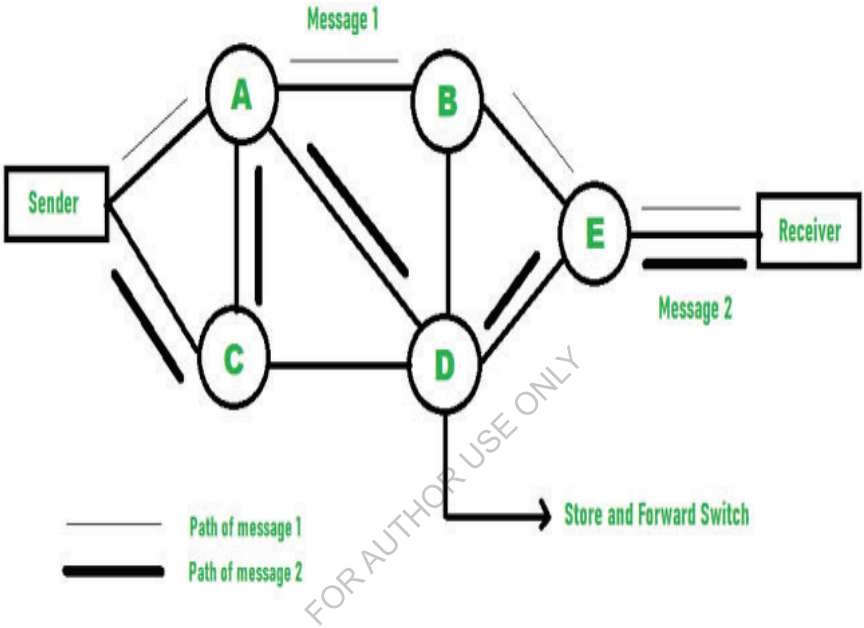


Fig 7.5: Packet Switching

7.3.3.1. Datagram Packet Switching:

It is a packet switching method that treats each packet, or datagram, as a separate entity. Each packet is routed via the network on its own. It is a service that does not require a connection. Because there is no specific channel for a connection session, there is no need to reserve resources. As a result, packets have a header with the entire destination's information. The intermediate nodes assess a packet's header and select an appropriate link to a different node closer to the destination.

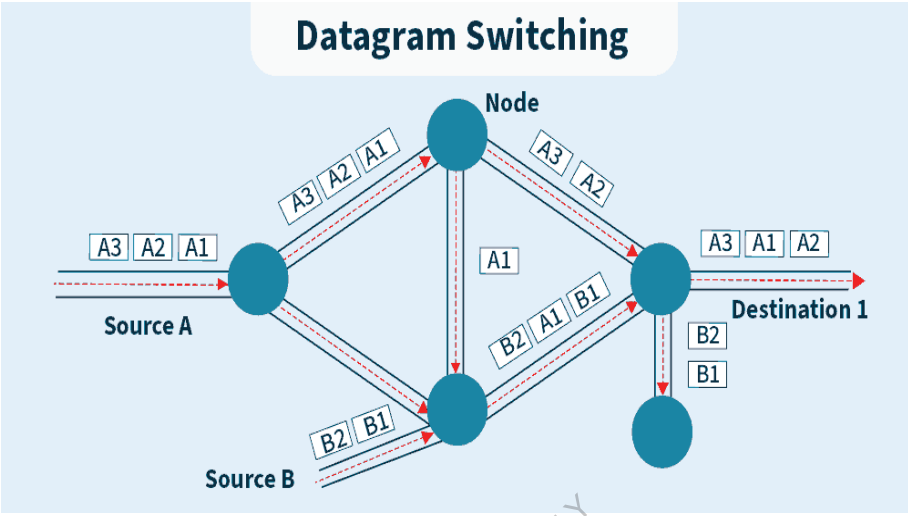


Fig 7.6: Datagram Switching

Advantages of Datagram Switching

- *Scalability:* Datagram switching is highly scalable and can handle large amounts of traffic on a network.
- *Flexibility*: Datagram switching is flexible and can support variable packet sizes and data rates.
- *Simple routing:* Datagram switching does not require a pre-established path for each packet, allowing packets to be routed dynamically.
- *Lower latency*: Datagram switching typically has lower latency than virtual circuit switching, as packets are sent immediately without any delay for setup.

Disadvantages of Datagram Switching

- *Higher error rates:* Datagram switching is more susceptible to errors than virtual circuit switching, as there is no guaranteed delivery or error correction.
- *Lack of QoS:* Datagram switching does not provide any Quality of Service guarantees, meaning that different types of traffic may be treated equally.
- *Increased network congestion:* Without a pre-established path for each packet, datagram switching can lead to increased network congestion and potential delays.

7.3.3.2. Virtual packet switching:

This approach in which a path is built between the source and the final destination through which all packets are routed throughout a call is known as virtual circuit switching. Because the connection looks to the user to be an infatuated physical circuit, this path is referred to as a virtual circuit. Other communications, on the other hand, may be sharing parts of the same path. Before the data transmission can commence, the source and destination must agree on a virtual circuit path. For the decision, all intermediary nodes between the two places add a routing entry to their routing database. Additional parameters, like the utmost packet size, also are exchanged between the source and therefore the destination during call setup. The virtual circuit is cleared after the info transfer is completed.

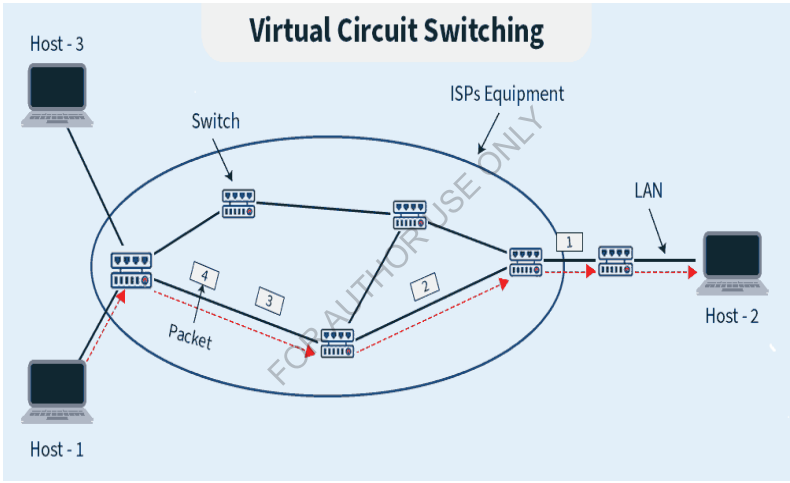


Fig 7.7: Virtual Circuit Switching

Advantages of Virtual Circuit Switching

- *Guaranteed delivery:* Virtual circuit switching provides guaranteed delivery of packets, reducing the likelihood of lost or corrupted data.
- *Lower error rates:* Virtual circuit switching typically has lower error rates than datagram switching due to its error correction mechanisms.
- *QoS support:* Virtual circuit switching supports Quality of Service guarantees, allowing for prioritization of different types of traffic.

- *Efficient use of bandwidth:* Virtual circuit switching establishes a pre-determined path for each packet, resulting in efficient use of bandwidth.

Disadvantages of Virtual Circuit Switching

- *Limited scalability:* Virtual circuit switching is less scalable than datagram switching and may not be suitable for large networks.
- *Increased setup time:* Virtual circuit switching requires a setup time for each connection, which can lead to increased latency and delay.
- *Fixed data rates:* Virtual circuit switching typically supports fixed data rates, which may not be suitable for applications that require variable packet sizes or data rates.

7.4. Difference between Datagram Switching and Virtual Circuit Switching

Datagram Switching	Virtual Circuit Switching
It is connection less service. There is no need for reservation of resources as there is no dedicated path for a connection session.	Virtual circuits are connection-oriented, which means that there is a reservation of resources like buffers, bandwidth, etc. for the time during which the new setup VC is going to be used by a data transfer session.
All packets are free to use any available path. As a result, intermediate routers calculate routes on the go due to dynamically changing routing tables on routers.	The first sent packet reserves resources at each server along the path. Subsequent packets will follow the same path as the first sent packet for the connection time.
Data packets reach the destination in random order, which means they need not reach in the order in which they were sent out.	Packets reach in order to the destination as data follows the same path.
Every packet is free to choose any path, and hence all the packets must be associated with a header containing information about	All the packets follow the same path and hence a global header is required only for the first packet of connection and other packets will not require it.

the source and the upper layer data.	
Datagram networks are not as reliable as Virtual Circuits.	Virtual Circuits are highly reliable.
Efficiency high, delay more	Efficiency low and delay less
But it is always easy and cost-efficient to implement datagram networks as there is no need of reserving resources and making a dedicated path each time an application has to communicate.	Implementation of virtual circuits is costly as each time a new connection has to be set up with reservation of resources and extra information handling at routers.
A Datagram based network is a true packet switched network. There is no fixed path for transmitting data.	A virtual circuit network uses a fixed path for a particular session, after which it breaks the connection and another path has to be set up for the next session.
Widely used in Internet	Used in X.25, ATM(Asynchronous Transfer Mode)

8. TCP/IP MODEL

The TCP/IP model is a framework that is used to model the communication in a network. It is mainly a collection of network protocols and organization of these protocols in different layers for modeling the network.

8.1.Role of TCP/IP

One of its main goals is to make sure that the data sent by the sender arrives safely and correctly at the receiver's end. To do this, the data is broken down into smaller parts called packets before being sent. These packets travel separately and are reassembled in the correct order when they reach the destination. This helps prevent errors and makes sure the message is complete and accurate.

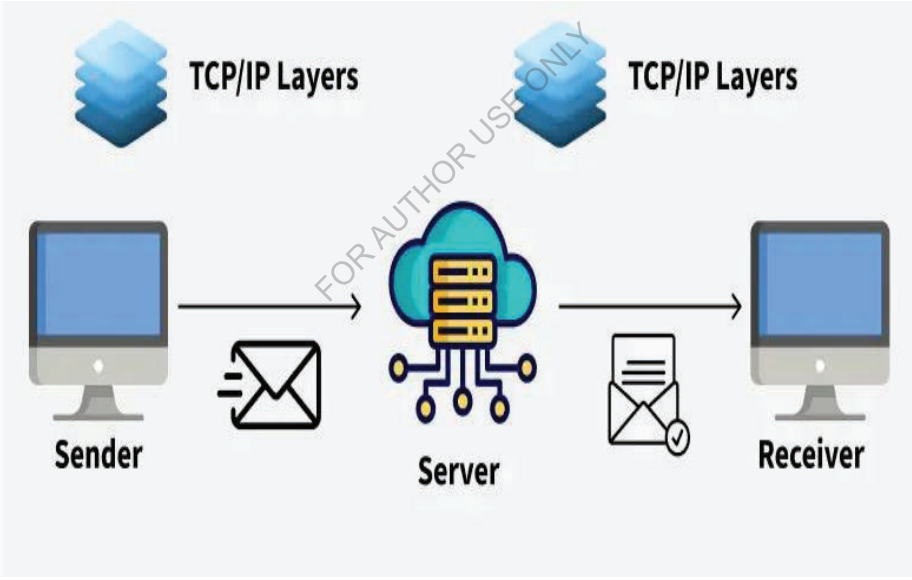


Fig 8.1: TCP/ IP

8.2.TCP/IP Model *(Transmission Control Protocol / Internet Protocol)*

The **TCP/IP model** is the foundational networking model for the **Internet** and modern communication. It defines **how data is transmitted between computers** across networks.

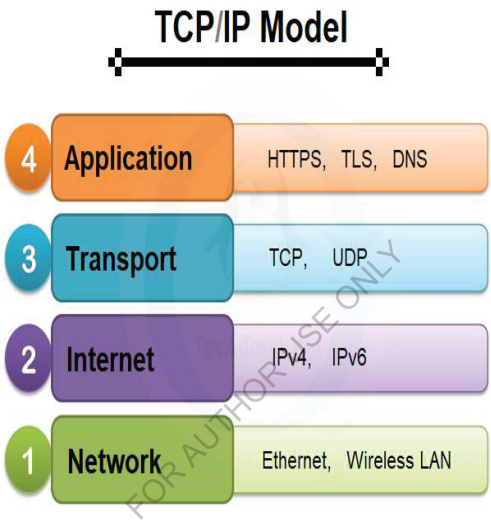


Fig 8.2: TCP/ IP Model

8.2.1. Application Layer:

This layer provides the interface for applications to access network services. It includes protocols like HTTP, FTP, SMTP, and DNS.

8.2.2. Transport Layer:

This layer manages end-to-end communication between applications. Key protocols here are TCP (Transmission Control Protocol) for reliable, connection-oriented communication and UDP (User Datagram Protocol) for faster, connectionless communication.

8.2.3. Internet Layer:

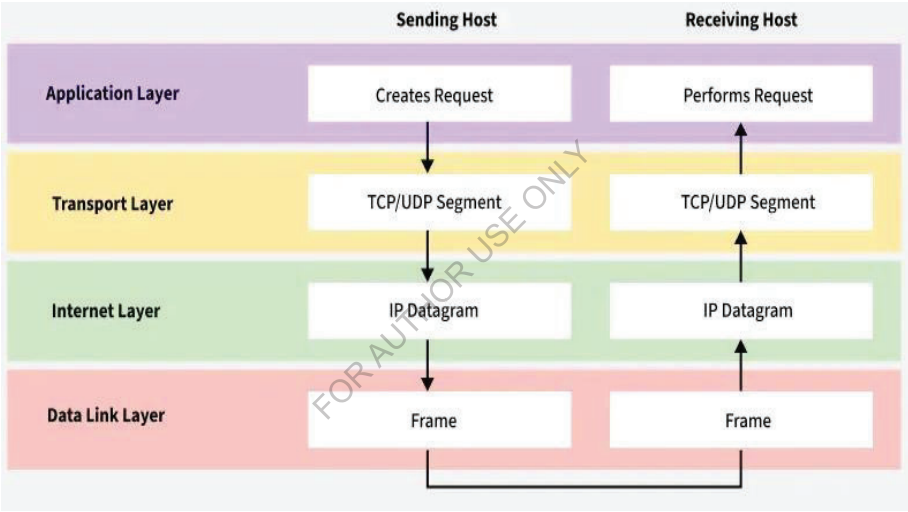
Also known as the Network layer, this layer handles addressing and routing of data packets. The main protocol is IP (Internet Protocol) which is responsible for delivering packets across networks.

8.2.4. Network Access Layer:

This layer deals with the physical and data link aspects of network communication, including how data is transmitted over the physical medium (e.g., Ethernet, Wi-Fi).

8.3. Working of TCP/IP Model

The working of TCP/IP can be explained with the help of the diagram given below and explained:



When Sending Data (From Sender to Receiver)

- **Application Layer**: Prepares user data using protocols like HTTP, FTP, or SMTP.
- **Transport Layer (TCP/UDP)**: Breaks data into segments and ensures reliable (TCP) or fast (UDP) delivery.
- **Internet Layer (IP)**: Adds IP addresses and decides the best route for each packet.
- **Link Layer (Network Access Layer)**: Converts packets into frames and sends them over the physical network.

When Receiving Data (At the Destination)

- **Link Layer**: Receives bits from the network and rebuilds frames to pass to the next layer.

- **Internet Layer**: Checks the IP address, removes the IP header, and forwards data to the Transport Layer.
- **Transport Layer**: Reassembles segments, checks for errors, and ensures data is complete.
- **Application Layer**: Delivers the final data to the correct application (e.g., displays a web page in the browser).

8.4.Why TCP/IP is Used over the OSI Model?

TCP/IP is used over the OSI model because it is simpler, practical, and widely adopted for real-world networking and the internet. The diagram below shows the comparison of OSI layer with the TCP :

Reason	Explanation
Simpler Structure	TCP/IP has only 4 layers, compared to 7 in OSI, making it easier to implement and understand in real systems.
Protocol-Driven Design	TCP/IP was designed based on working protocols, while the OSI model is more of a theoretical framework.
Flexibility and Robustness	TCP/IP adapts well to different hardware and networks and includes error handling, routing, and congestion control.
Open Standard	TCP/IP is open, free to use, and not controlled by any single organization, helping it gain universal acceptance.
Actual use vs Conceptual Model	The OSI model is great for education and design principles, but TCP/IP is the one actually used in real-world networking.

Advantages of TCP/IP Model

- **Interoperability** : The TCP/IP model allows different types of computers and networks to communicate with each other, promoting compatibility and cooperation among diverse systems.
- **Scalability** : TCP/IP is highly scalable, making it suitable for both small and large networks, from local area networks (LANs) to wide area networks (WANs) like the internet.
- **Standardization** : It is based on open standards and protocols, ensuring that different devices and software can work together without compatibility issues.
- **Flexibility** : The model supports various routing protocols, data types, and communication methods, making it adaptable to different networking needs.
- **Reliability** : TCP/IP includes error-checking and retransmission features that ensure reliable data transfer, even over long distances and through various network conditions.

Disadvantages of TCP/IP Model

- **Security Concerns** : TCP/IP was not originally designed with security in mind. While there are now many security protocols available (such as SSL/TLS), they have been added on top of the basic TCP/IP model, which can lead to vulnerabilities.
- **Inefficiency for Small Networks** : For very small networks, the overhead and complexity of the TCP/IP model may be unnecessary and inefficient compared to simpler networking protocols.
- **Limited by Address Space** : Although IPv6 addresses this issue, the older IPv4 system has a limited address space, which can lead to issues with address exhaustion in larger networks.
- **Data Overhead** : TCP the transport protocol, includes a significant amount of overhead to ensure reliable transmission.

Comparison of OSI and TCP Reference Model:

Layer No.	TCP/IP Layer	Corresponding OSI Layers	Functions
4	**Application Layer**	OSI Layers 5, 6, 7	Provides services for user applications (e.g. web, email)
3	**Transport Layer**	OSI Layer 4	Ensures reliable or best-effort data delivery
2	**Internet Layer**	OSI Layer 3	Logical addressing and routing (IP)
1	**Network Access Layer**	OSI Layers 1 & 2	Physical transmission, framing, MAC addressing

8.5. What is an IP Address?

Imagine every device on the internet as a house. For you to send a letter to a friend living in one of these houses, you need their home address. In the digital world, this home address is what we call an IP (Internet Protocol) Address. It's a unique string of numbers separated by periods (IPv4) or colons (IPv6) that identifies each device connected to the internet or a local network.

An IP address, or Internet Protocol address, is a unique string of numbers assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as an identifier that allows devices to send and receive data over the network, ensuring that this data reaches the correct destination.

8.5.1.Types of IP Address

IP addresses can be classified in several ways based on their structure, purpose, and the type of network they are used in. Here's a breakdown of the different classifications of IP addresses:

8.5.1.1. Based on Addressing Scheme (IPv4 vs. IPv6)

IPv4:

This is the most common form of IP Address. It consists of four sets of numbers separated by dots. For example, 192.158.1.38. Each set of numbers can range from 0 to 255. This format can support over 4 billion unique addresses. Here's how the structure is broken down:

Four Octets: Each octet represents eight bits, or a byte, and can take a value from 0 to 255. This range is derived from the possible combinations of eight bits (2^8 = 256 combinations).

Example of IPv4 Address: 192.168.1.1

- 192 is the first octet
- 168 is the second octet
- 1 is the third octet
- 1 is the fourth octet

Each part of the IP address can indicate various aspects of the network configuration, from the network itself to the specific device within that network. In most cases, the network part of the address is represented by the first one to three octets, while the remaining section identifies the host (device).

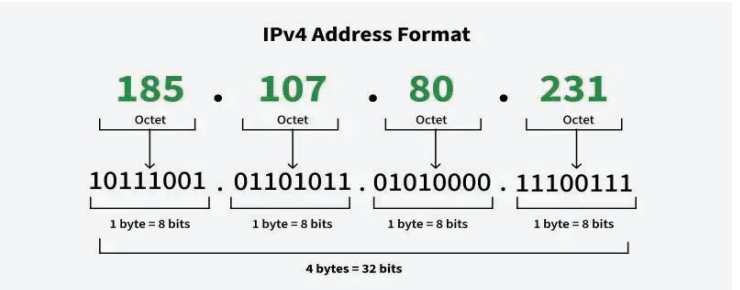


Fig 8.3: IPv4 Address Format

IPv6:

IPv6 addresses were created to deal with the shortage of IPv4 addresses. They use 128 bits instead of 32, offering a vastly greater number of possible addresses. These addresses are expressed as eight groups of four hexadecimal digits, each group representing 16 bits. The groups are separated by colons.

Example of IPv6 Address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Each group (like 2001, 0db8, 85a3, etc.) represents a 16-bit block of the address.

8.5.1.2.Based on Usage (Public vs. Private)

Public IP Addresses

A Public IP address is assigned to every device that directly accesses the internet. This address is unique across the entire internet. Here are the key characteristics and uses of public IP addresses:

- *Uniqueness:* Each public IP address is globally unique. No two devices on the internet can have the same public IP address at the same time.
- *Accessibility:* Devices with a public IP address can be accessed directly from anywhere on the internet, assuming no firewall or security settings block the access.
- *Assigned by ISPs:* Public IP addresses are assigned by Internet Service Providers (ISPs). When you connect to the internet through an ISP, your device or router receives a public IP address.
- *Types:* Public IP addresses can be static (permanently assigned to a device) or dynamic (temporarily assigned and can change over time).

Example Use: Public IP addresses are typically used for servers hosting websites, email servers, or any device that needs to be accessible from the internet. For instance, if you host a website on your own server at home, your ISP must assign a public IP address to your server so users around the world can access your site.

Private IP Addresses

Private IP addresses are used within private networks (such as home networks, office networks, etc.) and are not routable on the internet. This means that devices with private IP addresses cannot directly communicate with devices on the internet without a translating mechanism like a router performing Network Address Translation (NAT). Key features include:

- *Not globally unique:* Private IP addresses are only required to be unique within their own network. Different private networks can use the same range of IP addresses without conflict.
- *Local communication:* These addresses are used for communication between devices within the same network. They cannot be used to communicate directly with devices on the internet.
- *Defined ranges:* The Internet Assigned Numbers Authority (IANA) has reserved specific IP address ranges for private use:
  - IPv4: 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, 192.168.0.0 to 192.168.255.255
  - IPv6: Addresses starting with FD or FC

Example Use: In a typical home network, the router assigns private IP addresses to each device (like smart phones, laptops, smart TVs) from the reserved ranges. These devices use their private IPs to communicate with each other and with the router. The router uses NAT to allow these devices to access the internet using its public IP address.

8.5.1.3. Based on Assignment Method (Static vs. Dynamic)

Static IP Addresses:

- These are permanently assigned to a device, typically important for servers or devices that need a constant address.
- Reliable for network services that require regular access such as websites, remote management.

Dynamic IP Addresses:

- Temporarily assigned from a pool of available addresses by the Dynamic Host Configuration Protocol (DHCP).
- Cost-effective and efficient for providers, perfect for consumer devices that do not require permanent addresses.

8.6. How Do IP Addresses Work?

Here's how IP addresses work:

1. Unique Identification

Every device connected to a network, such as computers, smartphones, and servers, is assigned an IP address. This address is used to identify the device on the network, similar to how a home address identifies a specific location.

2. Communication Protocol

The Internet Protocol (IP), part of the broader suite of internet protocols, uses these addresses to facilitate the routing of data packets between devices. Each piece of data sent over a network is broken into smaller units called packets. Each packet includes both the sender's and the recipient's IP addresses.

3. Data Routing

When a device sends information to another device over the internet:

- The data is divided into packets.
- Each packet contains the IP address of the device it is destined for.
- Routers within the network read the destination IP address on each packet and determine the best path for the packet to travel. Routers communicate with each other to update and maintain records of the fastest, most efficient routes for data.

4. Local Area Networks (LAN) and Wide Area Networks (WAN)

- LAN: On local networks, IP addresses can be assigned manually by an administrator (static IP) or automatically by a DHCP server. Devices within the same network communicate directly using their local IP addresses.
- WAN: For devices on different networks, the data must travel through multiple routers across the internet. Each router makes independent decisions about the best route for the packets based on the destination IP address.

5. Network Address Translation (NAT)

Most devices on a home or small business network share a single public IP address when accessing the internet, even though each device has its own private IP address within the local network. NAT is a process where multiple local IP addresses are mapped to a single public IP address. This conserves IP addresses and adds a layer of security by hiding internal IP addresses from the external network.

8.7. IP addresses classifications: For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes:

IP addresses are also classified into different classes based on their range and intended use:

- Class A (1.0.0.0 to 127.255.255.255):
  - Used for very large networks (like multinational companies).
  - Supports up to 16 million hosts per network.
  - Example: 10.0.0.1 (Private IP in this class).
- Class B (128.0.0.0 to 191.255.255.255):
  - Used for medium-sized networks, such as large organizations.
  - Supports up to 65,000 hosts per network.
  - Example: 172.16.0.1 (Private IP in this class).
- Class C (192.0.0.0 to 223.255.255.255):
  - Used for smaller networks, like small businesses or home networks.
  - Supports up to 254 hosts per network.
  - Example: 192.168.1.1 (Private IP in this class).
- Class D (224.0.0.0 to 239.255.255.255):
  - Reserved for multicast groups (used to send data to multiple devices at once).
  - Not used for traditional devices or networks.
- Class E (240.0.0.0 to 255.255.255.255):
  - Reserved for experimental purposes and future use.

IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (27-2)
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

9. NETWORK DEVICES

Network devices are physical devices that allow hardware on a computer network to communicate and interact with each other. Network devices like hubs, repeaters, bridges, switches, routers and gateways help manage and direct data flow in a network. They ensure efficient communication between connected devices by controlling data transfer, boosting signals, and linking different networks. Each device serves a specific role, from simple data forwarding to complex routing between networks.

9.1. Functions of Network Devices

- Network devices help to send and receive data between different devices.
- Network devices allow devices to connect to the network efficiently and securely.
- Network devices improve network speed and manage data flow better.
- It protects the network by controlling access and preventing threats.
- Expand the network range and solve signal problems.

9.2. Common types of Networking Devices and their uses

Network devices work as a mediator between two devices for transmission of data, and thus play a very important role in the functioning of a computer network. Below are some common network devices used in modern networks:

- Access Point
- Modems
- Firewalls
- Repeater
- Hub
- Bridge
- Switch
- Routers
- Gateway
- NIC

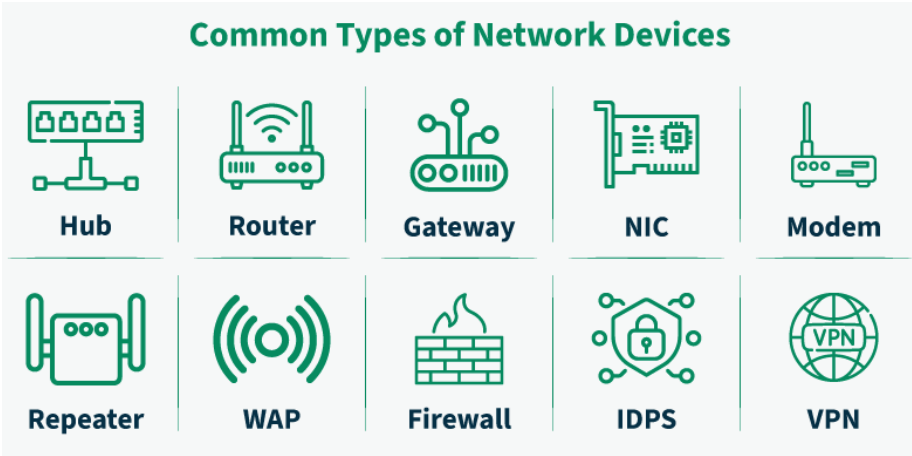


Fig 9.1: Types of Network Devices

9.2.1.Access Point

An access point in networking is a device that allows wireless devices, like smart phones and laptops, to connect to a wired network. It creates a Wi-Fi network that lets wireless devices communicate with the internet or other devices on the network. Access points are used to extend the range of a network or provide Wi-Fi in areas that do not have it. They are commonly found in homes, offices, and public places to provide wireless internet access.

9.2.2.Modems

Modem is also known as modulator/demodulator is a network device that is used to convert digital signal into analog signals of different frequencies and transmits these signals to a modem at the receiving location. These converted signals can be transmitted over the cable systems, telephone lines, and other communication mediums. A modem is also used to convert an analog signal back into digital signal. Modems are generally used to access the internet by customers of an Internet Service Provider (ISP).

Types of Modems

There are four main types of modems:

- **DSL Modem**: Uses regular phone lines to connect to the internet but it is slower compared to other types.
- **Cable Modem**: Sends data through TV cables, providing faster internet than DSL.

- **Wireless Modem**: Connects devices to the internet using Wi-Fi relying on nearby Wi-Fi signals.
- **Cellular Modem**: Connects to the internet using mobile data from a cellular network not Wi-Fi or fixed cables.

9.2.3.Firewalls

A firewall is a network security device that monitors and controls the flow of data between your computer or network and the internet. It acts as a barrier, blocking unauthorized access while allowing trusted data to pass through. Firewalls help protect your network from hackers, viruses, and other online threats by filtering traffic based on security rules. Firewalls can be physical devices (hardware), programs (software), or even cloud-based services, which can be offered as SaaS, through public clouds, or private virtual clouds.

9.2.4.Repeater

A repeater operates at the physical layer. Its main function is to amplify (i.e., regenerate) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

9.2.5.Hub

A hub is a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub:** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub:** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

9.2.6. Bridge

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It typically connects multiple network segments and each port is connected to different segment. A bridge is not strictly limited to two ports, it can have multiple ports to connect and manage multiple network segments. Modern multi-port bridges are often called Layer 2 switches because they perform similar functions.

Types of Bridges

- **Transparent Bridges:** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:** In these bridges, routing operations is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

9.2.7. Switch

A switch is a multiport bridge with a buffer designed that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Types of Switch

- **Unmanaged Switches:** These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
- **Managed Switches:** These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
- **Smart Switches:** These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.

- **Layer 2 Switches:** These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
- **Layer 3 switches:** These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
- **PoE Switches**: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
- **Gigabit switches:** These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
- **Rack-Mounted Switches:** These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
- **Desktop Switches:** These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
- **Modular Switches**: These switches have modular design that allows for easy expansion or customization. They are suitable for large networks and data centers.

9.2.8.Router

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

9.2.9.Gateway

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers.

9.2.10.NIC

NIC (Network Interface Card) is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique ID that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC is a layer 2 device which means that it works on both the physical and data link layers of the network model.

10. RECENT TRENDS IN NETWORKS AND COMMUNICATION

Recent trends in computer networks include the rise of 5G and Wi-Fi 6, edge computing, network automation, and a growing emphasis on security with technologies like SASE (Secure Access Service Edge). Other notable trends are the increasing adoption of Software-Defined Networking (SDN), Multi-Cloud Networking (MCN), and the integration of Artificial Intelligence (AI) and Machine Learning (ML) for network management.

5G and Wi-Fi 6/6E:

These technologies are driving faster speeds, lower latency, and increased capacity for connected devices, enabling new applications like IoT and augmented reality.

Edge Computing:

This involves processing data closer to the source, reducing latency and bandwidth consumption, and is particularly relevant for IoT devices and applications requiring real-time processing.

Network Automation:

AI and ML are being used to automate tasks like network monitoring, troubleshooting, and resource allocation, improving efficiency and reducing manual effort.

Secure Access Service Edge (SASE):

This security framework combines network and security services into a cloud-delivered model, providing secure access to resources from anywhere.

Software-Defined Networking (SDN):

SDN decouples the control plane from the data plane, allowing for greater flexibility and programmability in network management.

Multi-Cloud Networking (MCN):

As organizations adopt multi-cloud strategies, MCN solutions are needed to manage and connect resources across different cloud providers.

AI and ML in Networking:

AI and ML are being used to optimize network performance, predict failures, and automate tasks, leading to more intelligent and efficient networks.

- **Quantum Networking:**

While still in its early stages, quantum networking offers the potential for ultra-fast and secure communication, but requires significant research and development.

- **Metaverse:**

The metaverse, a virtual shared space, is driving new demands for network infrastructure and capabilities.

- **Blockchain Technology and Networking:**

Blockchain is being explored for secure data transfer and transaction management within networks, particularly in business applications.

10.1. Cloud Networking

Cloud Networking is a service or science in which a company's networking procedure is hosted on a public or private cloud. Cloud Computing is source management in which more than one computing resources share an identical platform and customers are additionally enabled to get entry to these resources to a specific extent. Cloud networking in a similar fashion shares networking however it gives greater superior features and network features in the cloud with interconnected servers set up under cyberspace.

What is Cloud Networking?

Cloud Networking refers to the infrastructure and processes in the cloud computing environment that are involved in connecting and managing the network resources. It includes the design, deployment, and optimization of networks facilitating communication and data transfer between various services hosted on cloud platforms. Cloud networking facilitates organizations to establish secure, scalable, and high-performance network architectures following to their specific requirements. It involves implementing virtualized networking technologies, such as virtual private clouds (VPCs), software-defined networking (SDN), and load balancing, to ensure reliable connectivity, efficient resource utilization, and seamless integration with cloud services. Ultimately, cloud networking plays a critical role in enabling organizations to leverage the benefits of cloud computing, including agility, flexibility, and cost-effectiveness, while meeting their networking needs.

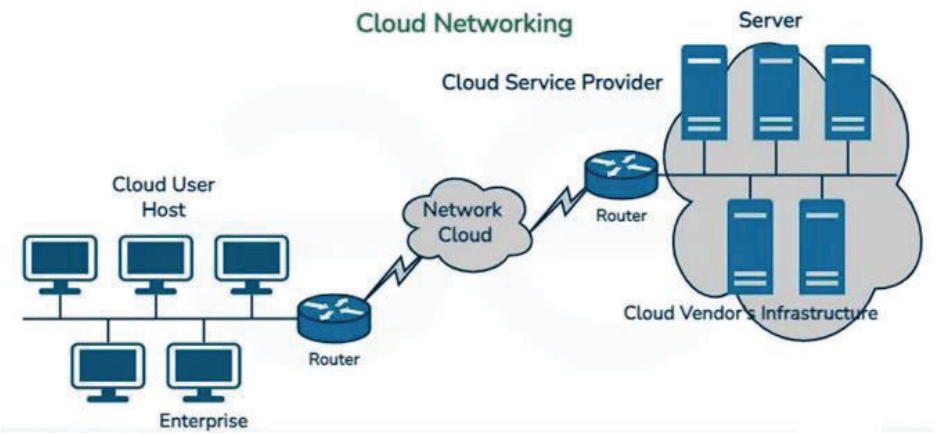


Fig 10.1: Cloud Networking

Why Cloud Networking?

- It is in demand by many companies for its speedy and impervious delivery, fast processing, dependable transmission of information without any loss, and pocket-friendly set-up. Benefited corporations who select Cloud Networking consist of internet service providers, e-commerce, cloud service providers, community operators, and cloud service providers.
- It permits users to boost their networks in accordance with necessities in cloud-based services. An actual cloud network provides high-end monitoring to globally positioned servers, controls site visitors'ors flow between interconnected servers, protects structures with superior network safety, and offers visibility to users by means of its centralized management. The web access can be expanded and made greater reliable bandwidth to promote a couple of network features into the cloud.
- It ensures overall performance and safety in multi-cloud surroundings so that Information technology receives greater visibility by means of supplying end-users with the necessities and experience they need. Workloads are shared between cloud surroundings using software program as provider application. Safety is given to user to get entry to web page and infrastructure by means of transferring functions to the cloud with standard security model. The gateway offers contextual access code and multi-layer firewall. Applications and offerings are given to allotted data centers in cloud environment.
- Software-Defined Wide Area Network is technology that makes use of bunch of networking switches and routers to virtually get entry to machine from hardware to software program deployed on white

box. Confidential units and information are set up on primary branch workplace or consumer region and given unique access to administrator to get admission to its superior networking functions, cloud optimization software, and firewalls. It is massive range of array with network features deployed in cloud platform.

- Software-defined Wide range community offers standard load balancing approach and combines all stages of network to user experience. It offers greater visuality with assist of intelligent analytics. Giving options to every cloud user may be challenging however leverage of all offerings and supplying them special answer by means of SD-WAN from ceasing to cease applications.

10.2.Cloud Networking Basics

Cloud Networking basics include the fundamental principles and components which involving in establishing and managing network resources within a cloud environment. The following are the key aspects included in cloud networking basics:

- *Virtualization:* Usage of virtualized networking technologies for creating virtual networks, subnets, and network interfaces, enables flexible resource allocation and isolation.
- *Software-Defined Networking (SDN):* It implements SDN principles for central managing of networks and automate the network configurations improving agility and scalability.
- *Virtual Private Clouds (VPCs):* VPCs facilitates in creating isolated network environments within the cloud, allowing organizations to define their own IP address ranges, subnets and route tables for enhancing security and control.
- *Monitoring and Optimization:* On usage of network monitoring tools and performance optimization techniques it helps in monitor network traffic, identify bottlenecks, and optimize resource utilization for improved efficiency and cost-effectiveness.
- *Load Balancing:* Load Balancing helps in distributing incoming network traffic across multiple servers or instances to ensure optimal performance, scalability, and fault tolerance.

10.3. Types of Cloud Networking

Utilization of virtualized networking technologies over the cloud environment for managing network resource is known as cloud networking. Cloud networking provides scalability and centralized management of network resources. The following are the types of cloud networking:

1. Cloud Networking

Cloud Networking comes with utilizes virtualized networking technologies to manage network resources within a cloud environment, providing scalability and centralized management.

- Virtualized Infrastructure: It involves utilization of virtualized networking technologies for creating and managing the network resources over the cloud.
- Scalability And Flexibility: Coud Networking offers flexibility anbd scalability for organziations to dynamically adjust their network configurations to meet up their changing demands.
- Centralized Management: It provides centralized management and automation of network configurations for enhancing agility and reducing administrative overhead.

2. Multi Cloud Networking

Multi Cloud Networking comes with facilitating connectivity and traffic distribution over multiple cloud service platforms with ensuring interoperability and security across diverse multi cloud environments. The following are its functionalities:

- Interoperability: Facilitates connectivity and communication between multiple cloud environments and on-premises infrastructure.
- Traffic Distribution: Enables load balancing and traffic routing across diverse cloud platforms to optimize performance and resource utilization.
- Security and Compliance: Implements consistent security policies and compliance measures across multiple clouds, ensuring data protection and regulatory compliance.

3. Hybrid Cloud Networking

Hybrid Cloud Networking comes with involving integration of on-premises infrastructure with public and private cloud environments. It provides seamless data flexibility with hybrid connectivity.

- Integration Of Environments: It develops a single network based architecture with linking public and private cloud environments with on premised infrastructure.
- Data Mobility: It helps with smoother transfer of workloads and data in between on-premise and cloud environments. It facilitates with resource optimization and agility.

10.4. Benefits of Cloud Networking

The following are the advantages of Cloud Networking:

- *On-Demand Self Service:* Cloud computing provides required application, services, and utility to client. With login key, they can begin to use besides any human interplay and cloud service providers. It consists of storage and digital machines.
- *High Scalability:* It requests grant of resources on large scale besides any human intervention with every service provider.
- *Agility:* It shares the assets efficiently amongst customers and works quickly.
- *Multi-sharing:* By distributed computing, distinctive clients from couple of areas share identical resources through fundamental infrastructure.
- *Low Cost:* It is very economical and can pay in accordance with its usage.
- *Services in pay per use Model:* Application Programming Interface is given to clients to use resources and offerings and pay on service basis.
- *High availability and Reliability:* The servers are accessible at the proper time besides any delay or disappointment.
- *Maintenance:* It is user-friendly as they are convenient to get entry to from their location and does not require any installation set up.

Disadvantages of Cloud Networking

The following are the Disadvantages of Cloud Networking:

- *Dependency on internet connectivity:* Cloud networking requires a strong and reliable internet connection. If the connection is slow or unreliable, it can cause performance issues and disrupt network access.
- *Security concerns:* Cloud networks are susceptible to cyber-attacks, and security breaches can compromise the sensitive data stored on the cloud. This risk is mitigated through proper security measures, but there is always some level of vulnerability.
- *Limited control:* When you use a cloud network, you are dependent on the cloud provider to manage and maintain the network infrastructure. This can limit your control over the network and how it is managed.

- *Cost:* Cloud networking can be expensive, particularly for large-scale enterprise networks. The costs can add up quickly, especially when you factor in the ongoing maintenance and support costs.
- *Lack of customization:* Cloud networking solutions are typically pre-configured and may not offer the level of customization that some organizations require. This can limit your ability to tailor the network to your specific needs.

Cloud Networking Services Examples

The following are the Cloud Networking Services Examples:

- *Virtual Private Networking (VPN):* In the Cloud: Setting the VPN services within the cloud environments helps for securing remote access and transfer the data.
- *Hub and Spoke Network Topology:* Establishment of Hub and spoke technology helps in centralizing the traffic management and in optimizing the resource utilization.
- *Sofftware-Defined Networking (SDN):* On usage of SDN technologies facilitates in dynamically manage and configure the network infrastructure in cloud environments for improving agility and scalability.

Use Cases of Cloud Networking Services

The following are the use cases of Cloud Networking Services:

- *Extended On-premises Networks:* It facilitates with seamless integration of on-premise network infrastructure with cloud environments using VPNs for having secured communication and resource access.
- *Automated Network Security:* Implementing automated network security facilitates with automatic patch deployment and having enforced policy-based security measures.
- *Traffic Inspection and Cloud Management:* Implementation of hub-spoke network topology helps in efficiently managing the network traffic and fulfilling resource based specific needs such as isolation of customers for compliance or performance reasons.

10.5.Cloud Computing Vs Cloud Networking

The following is the comparison table of cloud computing and cloud networking:

Aspect	Cloud Computing	Cloud Networking
Definition	It facilitates with delivery the services over the internet.	It facilitates with managing and optimizing network infrastructure.
Key Components	It contains components such as Virtual Machines, Storage, Databases	It contains components such as VPCs, SDN, and Routing.
Benefits	Scalability, Cost-effectiveness, flexibility	Enhanced Security, efficient traffic management
Key Providers	AWS, Microsoft Azure, GCP	Cisco, VMware, cloud Providers
Use Cases	It helps in hosting applications, data analytics and AI/ML	It secures remote access, traffic routing and resource optimization.

Why should we care about Cloud Networking?

The following are the reasons to care about cloud networking:

- *Enhanced Connectivity and Flexibility*: Cloud Networking provides seamless connectivity between on-premises and cloud environments by offering flexibility to access resources from anywhere, anytime and from any device.

- *Improved Security and Compliance*: Proper implementation of cloud networking solutions and securitymeasures helps in encryption and access controls with ensuring protection of sensitive data with regulatory requirements.

- *Cost Efficiency and Scalability*: Cloud Networking supports organizations to scale their network infrastructure as per their needs. It provides cost effective solutions for both small and large enterprises.

What make a successful Multi Cloud Networking Strategy?

A successful multi-cloud networking strategy depends on seamless integration, strong security and efficient management. It involves in establishment of resilient connectivity between cloud platforms using

technologies such as VPNs and SDN. On following the security measures such as encryption and access controls must be consistently applied across all clouds for safeguarding sensitive data.

Usage of effective management tools facilitates in centralized monitoring and controlling for having optimized utilization of resources. Organizations can enhances the strengths of multiple clouds for minimizing complexities and maximize the benefits of their cloud environments.

IT Teams are Responsible for Cloud Networking

IT teams are responsible for cloud networking for handing the following tasks:

Network Architecture Design and Implementation: To ensure designing and deploying network architectures facilitates with seamless connectivity between on-premises infrastructure and cloud environments.

Configuration and Management of Networking Technologies: Configuring and managing the VPNs, SDN solutions and other networking technologies is responsible for IT teams to enable a secured communication and data transfer.

Network Security Implementation: Implementation of strong security measures such as access controls, Encryption, Assign Access Roles and permissions to prevent unauthorized access to cloud resources are

REFERENCES:

1. Andrew S. Tanenbaum, David J. Wetherall, *Computer Networks*, 5th Edition, Pearson Education, 2011.
2. Behrouz A. Forouzan, *Data Communications and Networking*, 5th Edition, McGraw-Hill, 2012.
3. William Stallings, *Data and Computer Communications*, 10th Edition, Pearson, 2013.
4. James F. Kurose, Keith W. Ross, *Computer Networking: A Top-Down Approach*, 8th Edition, Pearson, 2021.
5. Larry L. Peterson, Bruce S. Davie, *Computer Networks: A Systems Approach*, 6th Edition, Morgan Kaufmann, 2019.
6. Douglas E. Comer, *Internetworking with TCP/IP Principles, Protocols, and Architecture*, 6th Edition, Pearson, 2014.

7. Uyless Black, *Computer Networks: Protocols, Standards and Interfaces*, 2nd Edition, Prentice Hall, 1993.
8. Radia Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, 2nd Edition, Addison-Wesley, 1999.
9. Olivier Bonaventure, *Computer Networking: Principles, Protocols and Practice*, 2nd Edition, 2016 (open-access).
10. Andrew S. Tanenbaum, Todd Austin, *Structured Computer Organization*, 6th Edition, Pearson, 2013 (for foundational architecture and networking context).