1...
Introduction to Computer Networks

Learning Objectives...

- To understand the concept of Networking.
- To learn the Goals, Applications and Components of computer network.
- To study the concept of Topology and Types of Network.
- To learn about Transmission technologies.

1.1 INTRODUCTION

1.1.1 Introduction to Network

- Network is a connection of multiple network devices via any medium.
- A computer network is a set of computers sharing resources located on or provided by network nodes.
- The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address, that helps in identifying a device.
- A network is built up through multiple devices such as cables, hub, switch, router, modem, repeater, bridge, etc.

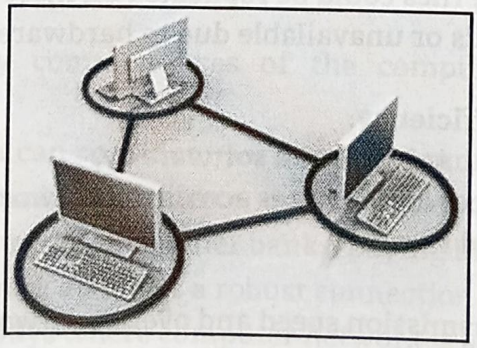


Fig. 1.1

1.1.2 Networking/Computer Networking

- Networking is a process of communication/transmission of data between devices.
- In computer networking two or more computers are linked together to enable communication and data exchange through either a physical cable or a wireless device.
- Nodes and links are the basic building blocks in computer networking.
- Computer networking is the practice of connecting computing and other devices to communicate, share resources and information.

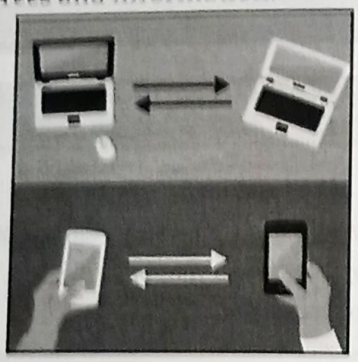


Fig. 1.2

1.2 GOALS, APPLICATIONS AND COMPONENTS

1.2.1 Goals of Computer Network

1. **Resource Sharing:**
   - Network shares among all the connected devices regardless of physical location.
   - They can share devices like printer, fax, scanner, data, software, etc.
2. **High Reliability:**
   - Provides high reliability by having alternative sources of data.
   - Network should prevent data loss and ensure continuous operation.
   - For example, all the files could be replicated on more than one machines, so if one of the machines fails or unavailable due to hardware failure, the network will not be impacted.
3. **Minimize Cost/Cost Efficiency:**
   - Reduces the cost of hardware and software by,
     - Sharing resources and services across the network.
     - Data backup and recovery
4. **High Performance:**
   - Enhances data transmission speed and overall network efficiency.
   - This can be calculated by transit time and response time.

   (a) **Transit time:** Amount of time taken by message to travel from one device to another.

   (b) **Response Time:** Time required between inquiry and response.

5. **Scalability:**
   - Allows easy expansion and addition of new nodes or devices without significant changes to the network infrastructure.
6. **Security:**
   - Protects data and resources from unauthorized access and ensures privacy and integrity.
7. **Distribution of workload:**
   - Large amount of work can be distributed among network users.
8. **Power communication medium:**
   - Easy to communicate, share documents, data, etc.

1.2.2 Applications of Computer Network

- Computer network has become an essential part of business, industry, entertainment world and even in daily lives.
- Some of applications are as below:

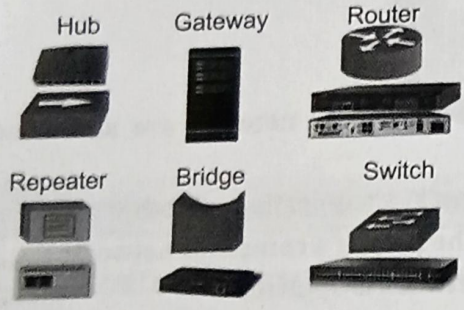
1. **Business Applications:**
   - There are many common uses of the computer network are as business applications.
   - Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network.
   - Below are some ways where business network is applied.
     (a) Printer sharing
     (b) Communication Medium
     (c) Software sharing
     (d) Connected by Switch
     (e) Connected by network
     (f) Server Client Model
2. **Home Applications:**
   - There are many common uses of the computer network are as home applications.
   - For example, you can consider user-to-user communication, access to remote instruction, electronic commerce, entertainment, managing bank accounts, transferring money to some other banks, paying bills electronically, etc.
   - A computer network arranges a robust connection mechanism among users.
   - Below are some ways where computer network is applied.
     (a) Router sharing
     (b) Person to person communication
     (c) Interactive entertainment

(d) Printer sharing
(e) File sharing

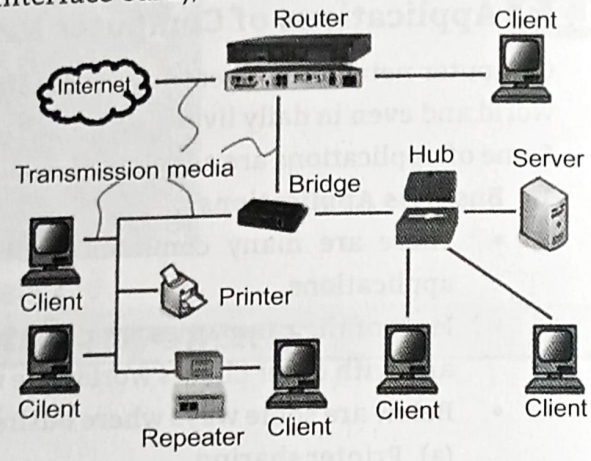
3. **Social media:** It includes Facebook, Instagram, etc.
4. **E-commerce:** It includes online shopping, bill payments, banking, investments, etc.
5. **Education:** It includes admission, bill payments, id card preparation, etc.
6. **Security:** It includes multiple aspects like defence, army, etc.

1.2.3 Components of Computer Network

- Network is built/implemented through multiple devices such as hub, switch, router, cables, bridge, repeater, NIC (Network Interface Card), etc.



(a)



(b)

Fig. 1.3

1.3 TOPOLOGY

- Topology in computer networks refers to the arrangement or layout of different elements (links, nodes, etc.) in a computer network.
- It essentially defines how devices (such as computers, routers, switches) are interconnected and how data flows within the network.

1.3.1 Types of Topology

- There are several types of network topologies:

1. **Bus Topology:**
   - All devices share a single communication line or cable.
   - Data travels in both directions along the cable, with terminators at each end to prevent signal reflection.
   - **Advantages:** Easy to implement, requires less cable.
   - **Disadvantages:** If the main cable fails, the entire network goes down; difficult to troubleshoot.

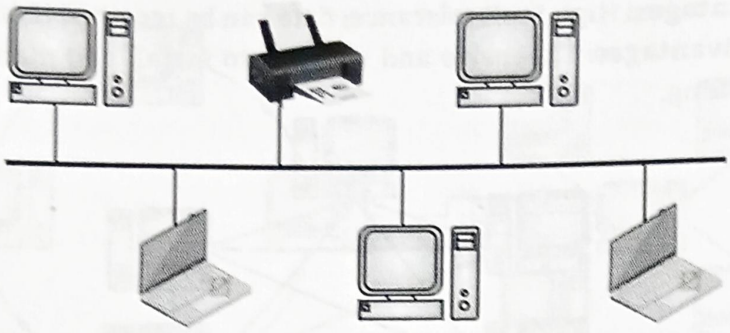


Fig. 1.4: Bus Topology

2. **Star Topology:**
   - All devices are connected to a central hub or switch.
   - Data passes through the central hub before reaching its destination.
   - **Advantages:** Easy to install and manage; if one device fails, it doesn't affect the others.
   - **Disadvantages:** If the central hub fails, the entire network is affected; more cable is required compared to bus topology.

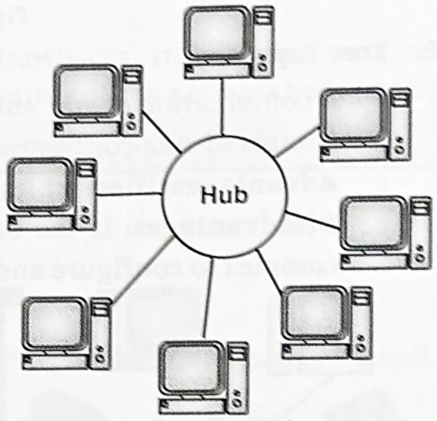


Fig. 1.5: Star Topology

3. **Ring Topology:**
   - Devices are connected in a circular fashion, with each device having exactly two neighbors.
   - Data travels in one direction (unidirectional) or both directions (bidirectional) along the ring.
   - **Advantages:** Data packets travel at high speeds; no collisions occur.
   - **Disadvantages:** If one device fails, it can affect the entire network; difficult to troubleshoot.

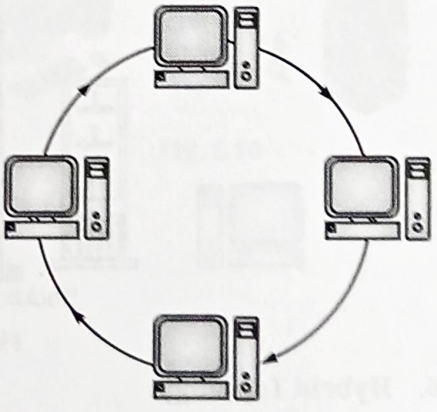


Fig. 1.6: Ring Topology

4. **Mesh Topology:**
   - Every device is connected to every other device in the network.
   - Provides high redundancy and reliability.

- **Advantages:** High fault tolerance; data can be rerouted if one path fails.
- **Disadvantages:** Expensive and complex to install and manage; requires a lot of cabling.

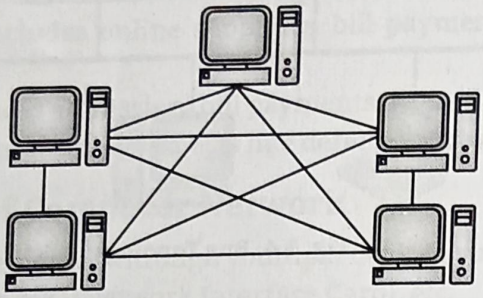


Fig. 1.7: Mesh Topology

5. **Tree Topology:**
   - A combination of star and bus topologies.
   - Groups of star-configured networks are connected to a linear bus backbone.
   - **Advantages:** Hierarchical, scalable, and easy to manage.
   - **Disadvantages:** If the backbone line breaks, the entire segment goes down; complex to configure and maintain.

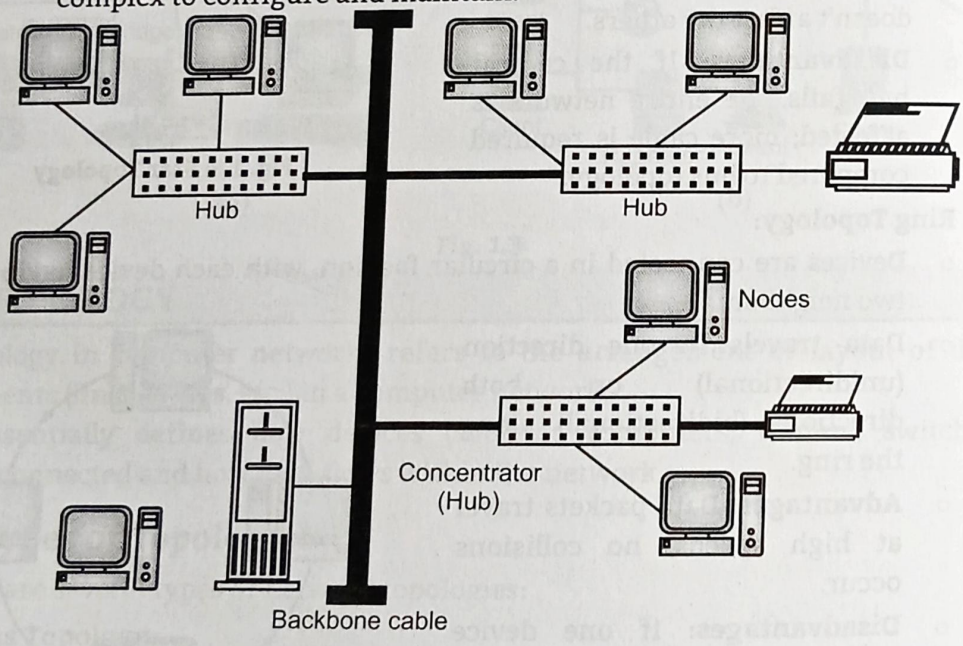


Fig. 1.8: Tree Topology

6. **Hybrid Topology:**
   - A mix of two or more different topologies.
   - Inherits the strengths and weaknesses of the combined topologies.
   - **Advantages:** Flexible and scalable.
   - **Disadvantages:** Complex and can be expensive to implement.

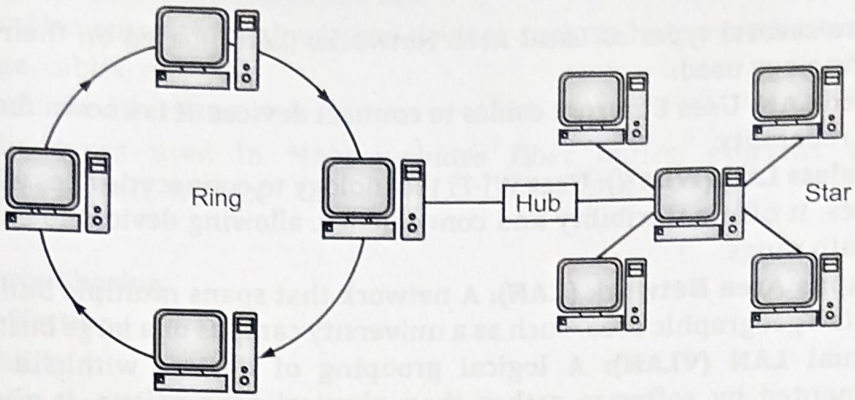


Fig. 1.9

- Each topology has its own set of benefits and drawbacks, and the choice of topology depends on the specific requirements and constraints of the network being designed.

1.4 TYPES OF NETWORK

- A computer network can be categorized by their size.

1.4.1 LAN

- LAN stands for Local Area Network.
- LAN is a network where a group of computers connected to each other in a small area.
- For Examples, Building, office, college, school, etc.
- It covers geographical area from 1km to 10 km.
- LAN is implemented through various devices such as hub, switch, router, repeater, NIC, bridge, cables, etc.
- It was established in 1960s.
- The media types used in LAN includes copper and fiber cabling.

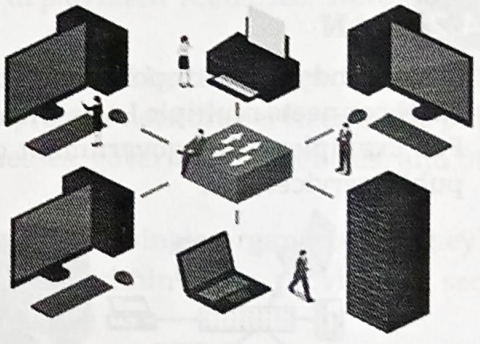


Fig. 1.10

Advantages:

1. Resource Sharing
2. Cost effective
3. Scalability
4. Low latency
5. Efficient communication
6. High Speed Data Transfer
7. More secure

Types:

- There are several types of Local Area Networks (LANs) based on their configuration and technology used:
  1. **Wired LAN:** Uses Ethernet cables to connect devices. It is known for its high speed and reliability.
  2. **Wireless LAN (WLAN):** Uses Wi-Fi technology to connect devices without physical cables. It offers flexibility and convenience, allowing devices to connect within a certain range.
  3. **Campus Area Network (CAN):** A network that spans multiple buildings within a limited geographic area, such as a university campus or a large business complex.
  4. **Virtual LAN (VLAN):** A logical grouping of devices within a LAN that are segmented by software rather than physical connections. It allows for better network management and security by separating traffic for different departments or functions.
  5. **Peer-to-Peer LAN (P2P):** A simple network where each computer has equal status and can communicate directly with every other computer. It is often used in small networks without a central server.
  6. **Client-Server LAN:** A network where devices (clients) connect to a central server that manages resources, applications, and data. This type of LAN is common in larger organizations.
- Each type of LAN serves different needs and can be chosen based on the specific requirements of the network environment.

1.4.2 MAN

- MAN stands for Metropolitan Area Network
- MAN connects multiple LANs within metropolitan area such as city or a large campus.
- For Examples, City, government offices, corporate branches, educational institutes, public services, etc.

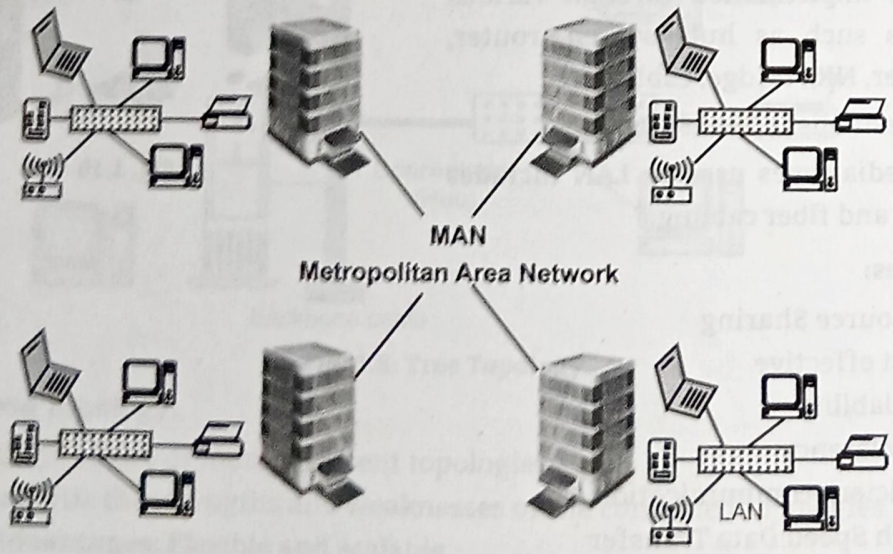


Fig. 1.11: MAN

- It covers geographical area up to 100 km.
- MAN is implemented through various devices such as hub, switch, router, repeater, NIC, bridge, cables, etc.
- It was established in 1980s.
- The media types used in MAN includes fiber optics, ethernet and wireless technologies as Wifi, WiMAX.

Advantages:

1. Resource Sharing
2. Cost effective
3. Scalability
4. Efficient communication
5. Lower latency compared to WAN, but higher latency compared to LAN
6. High Speed Data Transfer compared to WAN, but lower compared to LAN

Disadvantages:

1. Higher latency compared to LAN
2. Lower data transfer speed compared to LAN
3. Lesser secure than LAN

Types:

- Metropolitan Area Networks (MANs) can be categorized based on various factors such as their architecture, technologies used, and deployment scenarios. Here are some types of MANs:

1. **Public MAN:** These are typically owned and operated by telecom providers or ISPs (Internet Service Providers) and are used to provide network services to the public. They offer connectivity solutions for businesses, government agencies, and other organizations within a metropolitan area.
2. **Private MAN:** These are owned and managed by a single organization. They are used to connect multiple buildings or campuses within a city, providing a secure and dedicated network infrastructure for internal use.
3. **Wired MAN:** Utilizes wired technologies such as fiber optics, Ethernet, and coaxial cables to connect different parts of the network. This type often provides high-speed and reliable connectivity.
4. **Wireless MAN (WMAN):** Uses wireless technologies like Wi-Fi, WiMAX (Worldwide Interoperability for Microwave Access), or LTE (Long-Term Evolution) to provide network connectivity. This type is beneficial in areas where laying cables is difficult or costly.
5. **Hybrid MAN:** Combines both wired and wireless technologies to leverage the benefits of both. For example, a fiber optic backbone might be used for high-speed data transfer, while wireless connections provide flexibility and coverage in specific areas.

6. **Optical MAN:** Utilizes optical fiber technology for high-speed data transfer over long distances within a metropolitan area. These networks are known for their high bandwidth and low latency.
7. **Carrier Ethernet MAN:** Uses Ethernet technology to provide high-speed network services over a metropolitan area. It is often used by telecom providers to offer Ethernet-based services to businesses and organizations.

- Each type of MAN has its advantages and is suited to different use cases depending on the specific requirements and constraints of the environment in which it is deployed.

1.4.3 WAN

- WAN stands for Wide Area Network.
- WAN connects multiple small networks such as LANs and MANs.
- For Examples, Country, continent, etc.
- It covers larger geographical are a beyond 100 km.
- It was established in 1969.

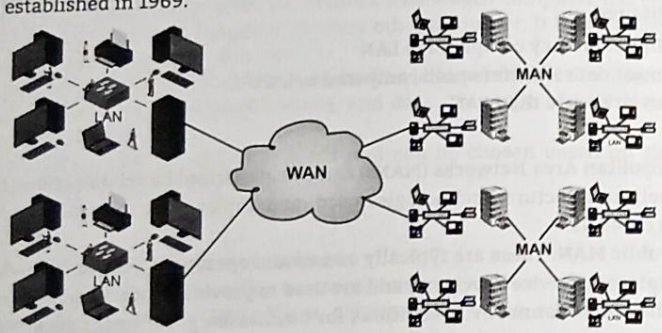


Fig. 1.12

Advantages:

1. Resource Sharing
2. Scalability
3. Efficient communication

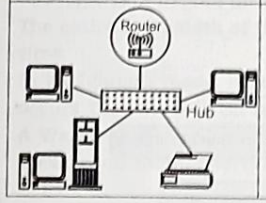
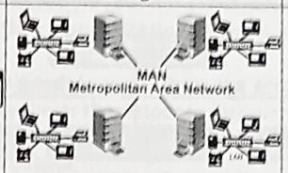
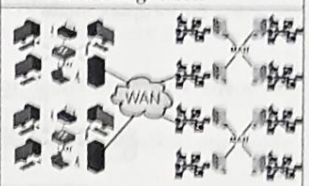
Disadvantages

1. Higher latency compared to LAN and MAN.
2. Lower data transfer speed compared to LAN and MAN.
3. More costly than LAN and MAN.
4. Lesser secure than LAN and MAN.

Types

1. Leased Line WAN
2. Packet switch WAN
3. MPLS WAN (Multiprotocol Label Switching WAN)
4. SD WAN (Software Defined WAN)
5. VPN (Virtual Private Network)
6. Satellite WAN
7. Mobile WAN

1.5 COMPARISON AMONG LAN, MAN AND WAN

LAN	MAN	WAN
• Local Area Network	• Metropolitan Area Network	• Wide Area Network
• Small Area Covered	• Large Area Covered	• Large Area Covered
• Ownership Private	• Ownership Private & Public	• Ownership Private & Public
• Easy to Design & Maintain	• Difficult to Design & Maintain	• Difficult to Design & Maintain
• Low setup cost	• Moderate setup cost	• High setup cost
• High data transfer rate	• Medium data transfer rate	• Low data transfer rate
• More Secure	• Less Secure	• Less Secure
• Range up to 1 km	• Range up to 100 km	• Range up to 100000 km
• Short Propagation Delay	• Moderate Propagation Delay	• Long Propagation Delay
• More Fault Tolerance	• Less Fault Tolerance	• Less Fault Tolerance
• Less Congestion	• More Congestion	• More Congestion
		

1.6 TRANSMISSION TECHNOLOGIES

- It is classified into point to point and broadcast networks

1.6.1 Point-to-Point (P2P) Networks

- Communication between two directly interconnected devices is referred as point to point communication.
- P2P connection provides a dedicated link between individual pairs of machines.
- It is mostly implemented in a larger network, for example WAN.
- No extra cost is required to set up point to point network.

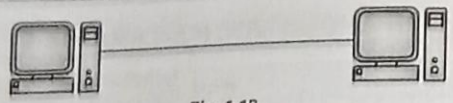


Fig. 1.13

1.6.2 Broadcast Networks

- Transmitting data from one source host to all other hosts present in the same or other network is called broadcast.
- It is called a one to all transmission.
- Broadcast network has single communication channel.
- It is mostly implemented in a smaller network, for example LAN.

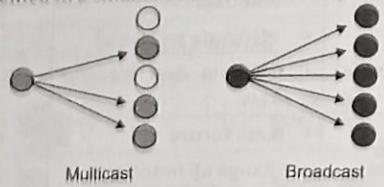


Fig. 1.14: Broadcast Network

1.7 MODES TO TRANSMISSION

- Modes of transmission can be categorised as below
  - Simplex mode
  - Half-duplex mode
  - Full-duplex mode

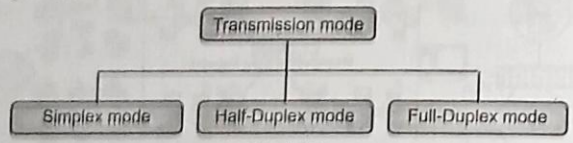


Fig. 1.15

1.7.1 Simplex

- In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
- This transmission mode is not very popular as mainly communications require the two-way exchange of data.
- Example: Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.

- Another example of simplex modes are loudspeakers, TV broadcasting, TV remote, etc. The main advantage of Simplex mode uses the full capacity of the channel to send data in one direction.

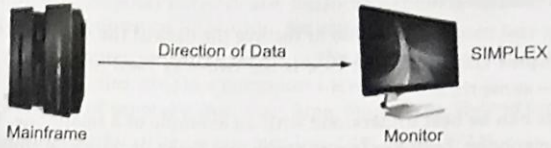


Fig. 1.16

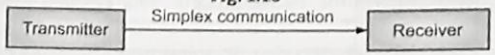


Fig. 1.17: Simplex Communication

Advantage of Simplex mode:

1. In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

Disadvantage of Simplex mode:

1. Communication is unidirectional, so it has no inter-communication between devices.

1.7.2 Half Duplex

- In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
- Messages flow in both the directions, but not at the same time.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
- A Walkie-talkie is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens.

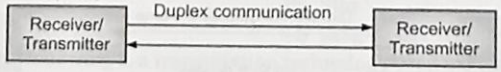


Fig. 1.18

Advantage of Half-duplex mode:

1. In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

1. In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

1.7.3 Full Duplex

- The communication between the sender and receiver can occur together in the full duplex transmission mode.
- The sender and receiver can send or receive the data at the same time.
- The full-duplex transmission mode is the two-way road in which traffic can go both ways at the same time.
- Full-duplex can be best understood with an example of a telephone. When two people talk on a telephone, both are free to speak and listen at the same time.

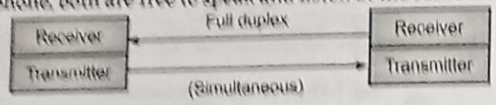


Fig. 1.19

Advantage of Full-duplex mode:

1. Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

1. If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

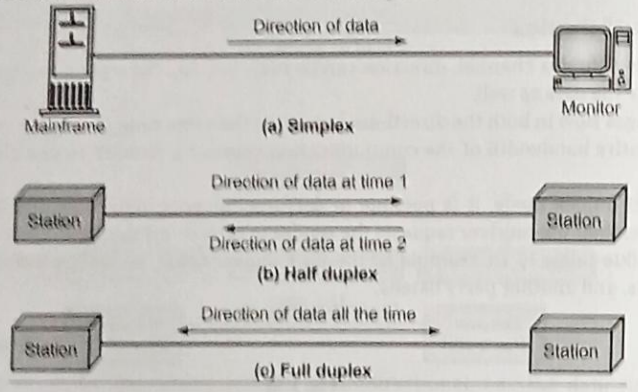


Fig. 1.20

Summary

- A computer network is a set of computers sharing resources located on or provided by network nodes.
- Networking is a process of communication/transmission of data between devices.
- Computer networking is the practice of connecting computing and other devices to communicate, share resources and information.

- Goals of computer network are: Resource sharing, High Reliability, Minimize cost/Cost efficiency, High Performance, Scalability, Security, Distribution of workload, Power communication medium
- Applications of computer network are: Business Applications, Home Applications, Social Media, E-Commerce, Education, Security.
- Topology in computer networks refers to the arrangement or layout of different elements (links, nodes, etc.) in a computer network.
- There are 6 types of topology: Bus, Star, Ring, Mesh, Tree, Hybrid topology.
- A computer network can be categorized into LAN, MAN, WAN.
- Transmission technologies are classified into Point-to-Point and Broadcast networks.
- There are 3 modes of transmission: Simplex, Half-duplex and Full-duplex.

Check Your Understanding

1. Which of the following is NOT a basic network topology?
   (a) Star (b) Mesh
   (c) Bridge (d) Ring
2. Which network type is typically used in a single building?
   (a) LAN (b) MAN
   (c) WAN (d) SAN
3. A network where every device connects to every other device is called:
   (a) Star (b) Ring
   (c) Mesh (d) Bus
4. Full-duplex communication allows data to flow:
   (a) In one direction only
   (b) In both directions, but one at a time
   (c) In both directions simultaneously
   (d) Only with acknowledgment
5. Which topology suffers from a single point of failure?
   (a) Bus (b) Star
   (c) Mesh (d) Ring
6. Which of the following is a transmission technology used in LANs?
   (a) Point-to-point (b) Satellite
   (c) Microwave (d) Broadcast
7. What does MAN stand for?
   (a) Managed Area Network (b) Metropolitan Area Network
   (c) Main Access Network (d) Manual Access Network
8. Which mode of communication is used in traditional TV broadcasting?
   (a) Simplex (b) Half Duplex
   (c) Full Duplex (d) None of the above

9. Which of these is NOT a goal of networking?
   (a) Resource sharing (b) Reducing data
   (c) Reliability (d) Cost efficiency
10. In which topology is each node connected to a central device?
   (a) Bus (b) Ring
   (c) Mesh (d) Star

Answers

1. (c)	2. (a)	3. (c)	4. (c)	5. (b)	6. (d)	7. (b)	8. (a)	9. (b)	10. (d)

Practice Questions

Q.I Answer the following questions in short:

1. What is a computer network?
2. Define networking in simple terms.
3. List any two goals of computer networking.
4. Pros and cons of LAN and MAN.
5. List different types of topologies.
6. What is a ring topology?
7. Which topology uses a central hub?
8. Differentiate between LAN and WAN (at least two differences).
9. What is meant by simplex communication?
10. What are the types of MAN?

Q.II Answer the following questions in detail:

1. Explain the concept of computer networking. Include its goals.
2. List and explain at least four applications of computer networking in real-world scenarios.
3. What are Modes of Communication, explain each.
4. Describe the main goals of a computer network and how they are achieved.
5. Discuss the essential components required for building a computer network and their functions.
6. Compare and contrast five different types of network topologies with advantages and disadvantages.
7. Describe the different types of networks: LAN, MAN, and WAN. Provide examples for each.
8. What are transmission technologies? Explain the differences between point-to-point and broadcast networks.
9. Explain simplex, half-duplex, and full-duplex modes of communication with real-life examples.
10. Discuss how hybrid topology combines the features of two or more basic topologies. Provide an example.

2...
Network Models

Learning Objectives...

- To learn the concept of OSI Reference Model.
- To understand about Functionalities of OSI Layer.
- To study the TCP/IP Reference Model.
- To understand the TCP/IP Protocol Suite and Transport Layer Protocols.

2.1 OSI REFERENCE MODEL

- OSI model stands for Open Systems Interconnection (OSI) model. Established by International Organisation for Standardization (ISO) in 1970s. This is also referred as ISO OSI model.
- OSI model is not a protocol, it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.
- It has 7 layers; each layer has well-defined functions. The names of layers are Application, Presentation, Session, Transport, Network, Datalink and Physical layer.
- It is a theoretical/conceptual framework.
- Application, Presentation and Session layers are referred as Software layers. Transport layer is referred as Backbone/Heart of network. Network, Datalink and Physical layer are referred as Hardware layers.
- Fig. 2.1 illustrate how it works at Sender's and Receiver's side.

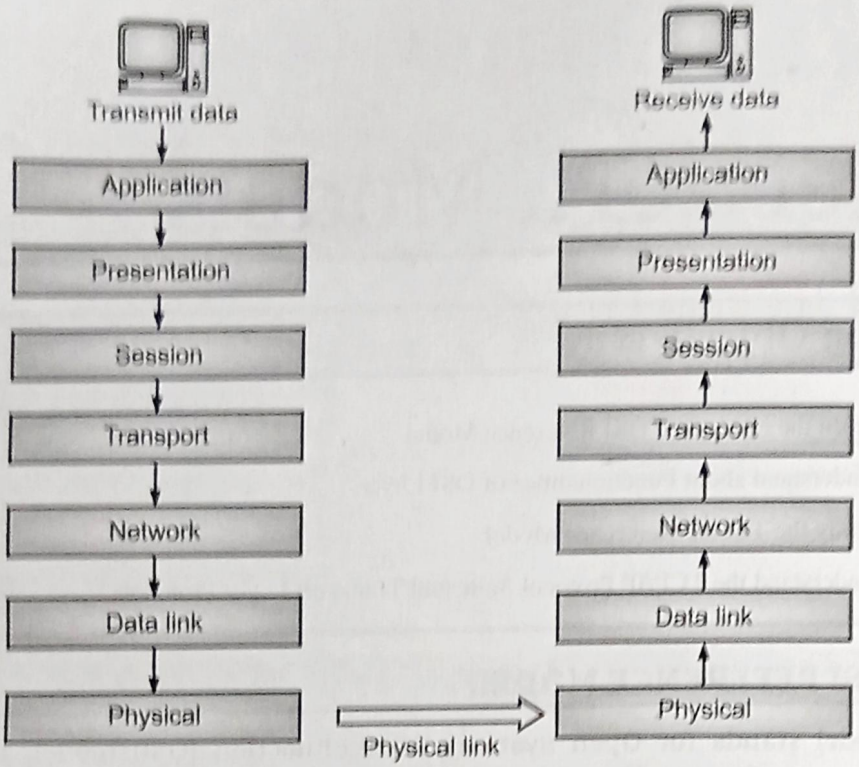


Fig. 2.1

2.2 FUNCTIONALITIES OF OSI LAYER

- The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and standardize the functions of a telecommunication or computing system independent of its underlying internal structure and technology.
- OSI model divides network communication into seven layers, each with specific functions.
- Here are the functionalities of each layer:

1. **Application Layer:**
   - **User Interface:** Provides network services directly to end-users and applications.
   - **Application Services:** Offers services such as email, file transfer, and web browsing.
   - **Protocol Implementation:** Implements protocols for specific network services (e.g., HTTP, FTP, SMTP).
2. **Presentation Layer:**
   - **Data Translation:** Translates data between the application layer and the network.
   - **Data Encryption and Decryption:** Provides security through encryption and decryption.
   - **Data Compression:** Reduces the size of data to optimize bandwidth usage.

- **Data Formatting:** Ensures data is presented in a readable format for the application layer.

3. **Session Layer:**
   - **Session Management:** Establishes, manages, and terminates sessions between applications.
   - **Synchronization:** Controls the dialog between two devices, ensuring they remain in sync.
   - **Dialog Control:** Manages data exchange (half-duplex or full-duplex) between devices.
4. **Transport Layer:**
   - **End-to-End Communication:** Ensures reliable data transfer between two endpoints.
   - **Error Detection and Recovery:** Detects and recovers from errors in data transmission.
   - **Flow Control:** Manages the rate of data transmission to prevent congestion.
   - **Segmentation and Reassembly:** Divides large data streams into smaller segments and reassembles them.
   - **Multiplexing:** Allows multiple applications to share the same network connection.
5. **Network Layer:**
   - **Logical Addressing:** Assigns IP addresses to devices and ensures packets are sent to the correct destination.
   - **Routing:** Determines the best path for data to travel across networks.
   - **Packet Forwarding:** Moves packets through intermediate devices (routers) to reach the destination.
   - **Fragmentation and Reassembly:** Breaks large packets into smaller ones for transmission and reassembles them at the destination.
6. **Data Link Layer:**
   - **Frame Formatting:** Converts raw bits into frames (structured packets of data).
   - **MAC Addressing:** Provides physical addressing using MAC addresses.
   - **Error Detection and Correction:** Detects and corrects errors that occur in the physical layer.
   - **Flow Control:** Manages the rate of data transmission between devices to prevent overflow.
7. **Physical Layer:**
   - **Physical Connection:** Establishes, maintains, and deactivates the physical connection.
   - **Transmission of Bits:** Transmits raw bitstream over a physical medium.
   - **Signalling:** Defines the electrical, optical, or electromagnetic signals used to transmit data.
   - **Data Rate Control:** Manages the data transmission rate.

- Each layer of the OSI model interacts with the layers directly above and below it, ensuring a comprehensive approach to network communication and providing a standard for different network technologies and software to interoperate effectively.

APPLICATION	Network process to Application, User and APIs, resource sharing, remote file access, etc.	DATA
PRESENTATION	Translation of data like character encoding, encryption/decryption, data compression, etc.	DATA
SESSION	Establish, maintain and gracefully shut down the session.	DATA
TRANSPORT	Reliable end to end communication, segmentation, flow control, acknowledgement, and multiplexing	SEGMENT
NETWORK	Path determination, logical addressing, routing, traffic control	PACKET
DATA LINK	Reliable node to node transmission of frames, MAC and LLC, sublayers, Physical addressing,	FRAMES
PHYSICAL	Transmission/Reception of binary bit streams over physical medium, encoding/decoding at bit level	BITS

Fig. 2.2

2.3 TCP/IP REFERENCE MODEL

- The TCP/IP model stands for Transmission Control Protocol/Internet Protocol.
- TCP/IP model is also called as Internet Reference Model.

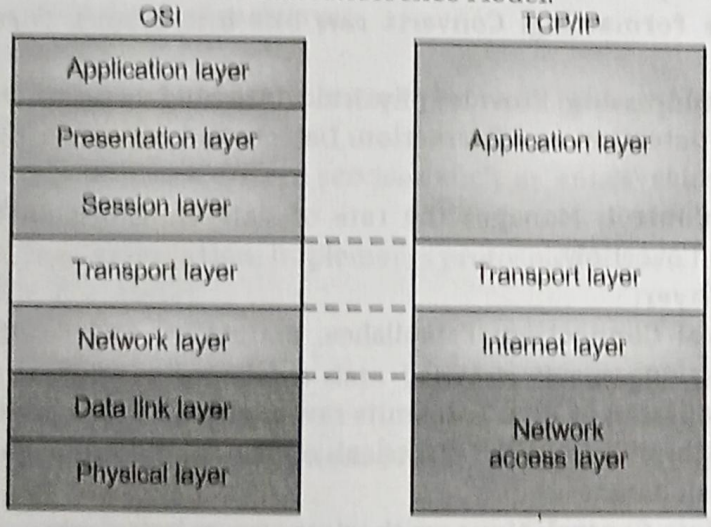


Fig. 2.3

- The TCP/IP model is structured into four layers, each providing specific functionalities that ensure the reliable transmission of data across networks.
- It has 4 layers; each layer has well-defined functions. The names of layers are Application, Transport, Network, Internet and Network Interface/Access Layer (Link Layer).
- It is a practical/reality framework.
- Here are the detailed functionalities of each layer:

1. **Application Layer:**
   - **User Interface:** Provides the protocols and services that enable user applications to interact with the network.
   - **Data Representation:** Ensures that data is presented in a format that can be understood by both the sender and the receiver.
   - **Application Services:** Offers various network services such as email, file transfer, and web browsing.
   - **Session Management:** Establishes, manages, and terminates communication sessions between applications.
2. **Transport Layer:**
   - **End-to-End Communication:** Provides communication between two endpoints (devices) on the network.
   - **Error Detection and Recovery:** Detects errors in the transmitted data and ensures retransmission if necessary.
   - **Flow Control:** Manages the rate of data transmission to prevent network congestion.
   - **Segmentation and Reassembly:** Divides large data streams into smaller segments for transmission and reassembles them at the destination.
   - **Multiplexing:** Allows multiple applications to use the network simultaneously by assigning different ports to each application.
3. **Internet Layer:**
   - **Logical Addressing:** Assigns IP addresses to devices and ensures data packets are sent to the correct destination.
   - **Routing:** Determines the best path for data to travel across multiple networks from the source to the destination.
   - **Packet Forwarding:** Moves packets through intermediate devices like routers to reach the final destination.
   - **Fragmentation and Reassembly:** Breaks down large data packets into smaller ones for transmission and reassembles them at the destination.
4. **Network Interface/Access Layer (Link Layer):**
   - **Physical Transmission:** Manages the hardware aspects of data transmission, such as cables, switches, and network interface cards.
   - **Frame Formatting:** Defines the format of data packets for transmission over the network hardware.

Aspect	OSI Model	TCP/IP Model
Stands for	Open System Interconnection	Transmission Control Protocol/Internet Protocol
Number of layers	7 layers	4 layers
Framework	Theoretical	Practical/Reality
Kind of model	This is just a reference model	Implementation of OSI model
Developed by	ISO	DOD (Department of Defence)
Protocol Implementation	OSI model was developed before protocols were defined/implemented.	TCP/IP model was developed after protocols were defined/implemented.
Protocol dependent/independent	Protocol independent model	Protocol dependent model
Layers Differences/ Separation	Separate application, presentation, session, datalink and physical layers.	Presentation and Session layers are clubbed under Application layer and Datalink and physical layers are grouped as Network access/interface layer.

2.5 TCP/IP PROTOCOL SUITE

- The TCP/IP model is structured into four layers, each providing specific functionalities that ensure the reliable transmission of data across networks.
- It has 4 layers; each layer has well-defined functions and assigned with dedicated protocols.
- Application layer has below protocols:

  Name System: DNS (Domain Name System)

  Web: HTTP & HTTPS

  File Transfer: FTP (File Transfer Protocol) & TFTP (Trivial File Transfer Protocol)

Email:

SMTP (Simple Mail Transfer Protocol)
POP (Post Office Protocol)
IMAP(Internet Message Access Protocol)

- Transport layer has below protocols:
  TCP (Transmission Control Protocol)
  UDP (User Datagram Protocol)
- Internet layer has below protocols:
  IP (Internet Protocol)
  Routing protocols:
  RIP (Routing Information Protocol)
  BGP (Border Gateway Protocol)
  OSPF (Open Shortest Path First)
  EIGRP (Enhanced Interior Gateway Routing Protocol)
- Network access/interface layer has:
  Protocol: PPP (Point to Point Protocol)
  Technologies: Ethernet, Interface Devices, Frame Relay, etc.

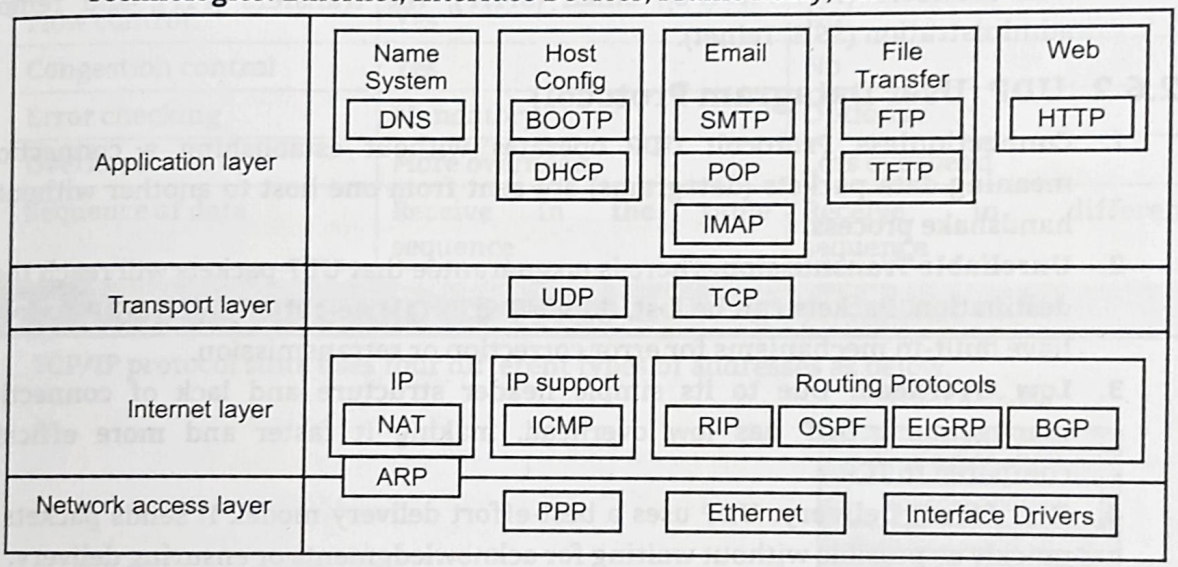


Fig. 2.4

2.6 TRANSPORT LAYER PROTOCOLS

2.6.1 TCP (Transmission Control Protocol)

- TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite, which is used for transmitting data over a network. Here are some key points about TCP:

1. **Connection-Oriented:** TCP establishes a connection between the sender and receiver before data can be sent. This process involves a three-way handshake: SYN, SYN-ACK, and ACK.

2. **Reliable Data Transfer:** TCP ensures that data is delivered accurately and in the same order it was sent. It achieves this through error-checking mechanisms, acknowledgments, and retransmissions of lost packets.
3. **Flow Control:** TCP uses flow control to ensure that a sender does not overwhelm a receiver with too much data at once. This is managed through a sliding window mechanism.
4. **Congestion Control:** TCP adjusts the rate of data transmission based on network congestion. Algorithms like TCP Tahoe, TCP Reno, and others help manage congestion and ensure efficient use of network resources.
5. **Segmentation and Reassembly:** Large messages are divided into smaller segments for transmission and reassembled at the destination.
6. **Ports:** TCP uses port numbers to identify specific processes or services on a device. This allows multiple applications to use the network simultaneously without interference.
7. **Applications:** TCP is used by many important Internet applications, including web browsers (HTTP/HTTPS), email (SMTP), file transfers (FTP), and remote administration (SSH, Telnet).

2.6.2 UDP (User Datagram Protocol)

1. **Connectionless Protocol:** UDP operates without establishing a connection, meaning data packets (datagrams) are sent from one host to another without a handshake process.
2. **Unreliable Transmission:** There is no guarantee that UDP packets will reach their destination. Packets can be lost, duplicated, or arrive out of order. UDP does not have built-in mechanisms for error correction or retransmission.
3. **Low Overhead:** Due to its simple header structure and lack of connection management, UDP has low overhead, making it faster and more efficient compared to TCP.
4. **Best Effort Delivery:** UDP uses a best-effort delivery model. It sends packets as quickly as possible without waiting for acknowledgments or ensuring delivery.
5. **Simple Header Structure:** The UDP header consists of only four fields: Source Port, Destination Port, Length, and Checksum. This simplicity contributes to the protocol's efficiency.

Applications Suited for UDP:

(i) Real-time applications (e.g., video streaming, VoIP, online gaming) where low latency is critical.

(ii) Broadcast and multicast communication, where data is sent to multiple recipients.

(iii) Services like DNS queries and SNMP that benefit from UDP's simplicity and speed.

2.6.3 Difference Between TCS and UPD

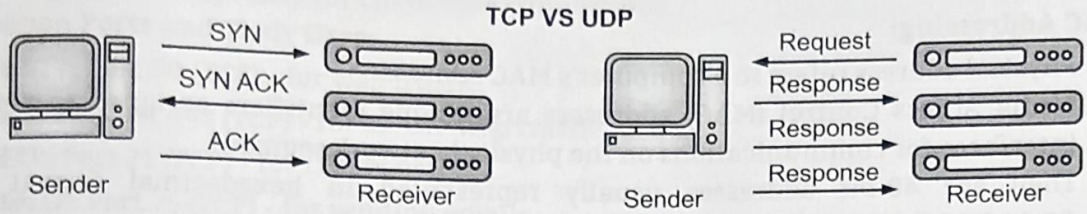


Fig. 2.5

Table 2.2

Aspect/Item	TCP	UDP
Full form	Transmission Control Protocol	User Datagram Protocol
Connection	Connection Oriented	Connectionless
Reliability	Reliable	Less Reliable
Data sending speed	Slow transmission	Fast transmission
Flow control	Yes	No
Congestion control	Yes	No
Error checking	Mandatory	Optional
Overhead	More overhead	Less overhead
Sequence of data	Receive in the same sequence	Receive in different sequence

2.7 ADDRESSING AND ITS TYPES

- TCP/IP protocol suite uses four different types of addresses as below.

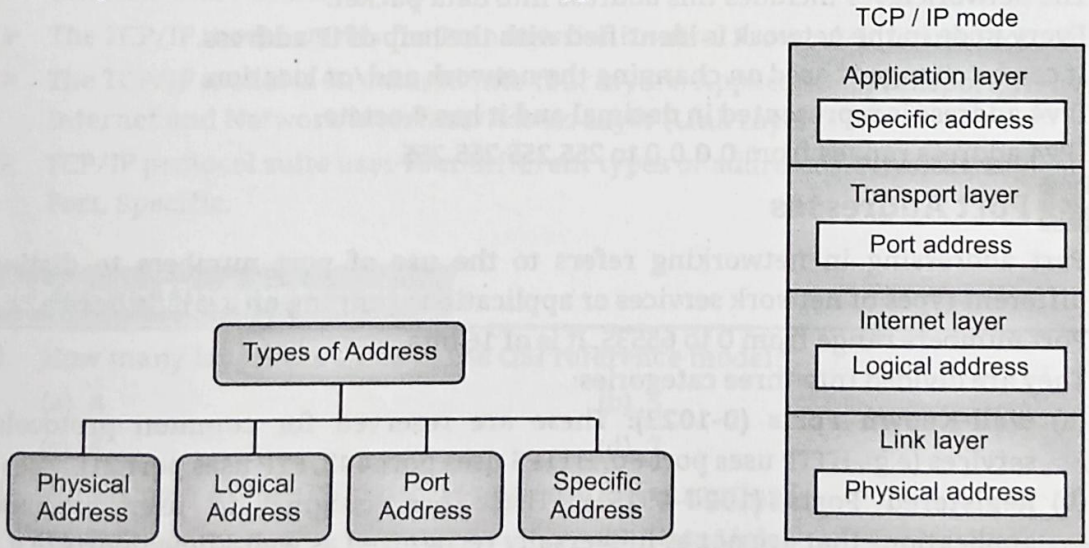


Fig. 2.6

2.7.1 Physical Address

MAC Addressing:

- Physical address refers to a computer's MAC address.
- Media Access Control (MAC) addresses are unique identifiers assigned to network interfaces for communications on the physical network segment.
- They are 48-bit addresses usually represented in hexadecimal format (e.g., 00:1A:2B:3C:4D:5E).
- The data link layer includes this address into data frame.
- Physical address is also referred as MAC, LAN and Data Link layer address.

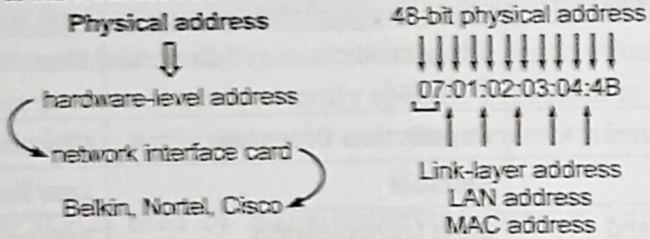


Fig. 2.7

2.7.2 Logical Address

- Logical address is referred as IP Addressing.
- Internet Protocol (IP) addresses are numerical labels assigned to devices participating in a network that uses the Internet Protocol for communication.
- IPv4 addresses are 32-bit numbers, typically shown in decimal format as four octets separated by periods (e.g., 192.168.1.1).
- IPv6 addresses are 128-bit numbers, shown in hexadecimal format and separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- The network layer includes this address into data packet.
- Every node in the network is identified with the help of IP address.
- It can be changed based on changing the network and/or location.
- IPv4 address is represented in decimal and it has 4 octets.
- IPv4 address ranges from 0.0.0.0 to 255.255.255.255.

2.7.3 Port Addresses

- Port addressing in networking refers to the use of port numbers to distinguish different types of network services or applications running on a single device.
- Port numbers range from 0 to 65535. It is of 16 bits.
- They are divided into three categories:
  - (a) **Well-Known Ports (0-1023):** These are reserved for common protocols and services (e.g., HTTP uses port 80, HTTPS uses port 443, FTP uses port 21).
  - (b) **Registered Ports (1024-49151):** These are assigned to user processes or applications that are not as universally recognized as well-known ports (e.g., 3306 for MySQL).

(c) **Dynamic or Private Ports (49152-65535):** These are used for temporary or private purposes, typically for client-side connections.

Common Ports and Their Uses:

- **HTTP:** Port 80 (TCP) - for web traffic.
- **HTTPS:** Port 443 (TCP) - for secure web traffic.
- **FTP:** Port 21 (TCP) - for file transfer.
- **SMTP:** Port 25 (TCP) - for sending emails.
- **DNS:** Port 53 (UDP) - for domain name resolution.
- **SSH:** Port 22 (TCP) - for secure shell access.

2.7.4 Specific Address

- A few of the applications generally have simple, such as email address or University Resource Locators (URL).
- Specific address is friendly address.
- These kinds of addresses are designed for a specific address. However, this address gets changed according to the required logical and port addresses sent from the sender computer.
- Examples are:

  electronicscrunch@gmail.com, customercare@gmail.com

  www.welearn.com, www.welearn.edu

Summary

- OSI model stands for Open Systems Interconnection (OSI) model.
- OSI model has 7 layers: Application, Presentation, Session, Transport, Network, Datalink and Physical layer.
- The TCP/IP model stands for Transmission Control Protocol/Internet Protocol.
- The TCP/IP model is structured into four layers: Application, Transport, Network, Internet and Network Interface/Access Layer (Link Layer).
- TCP/IP protocol suite uses four different types of addresses: Physical, Logical, Port, Specific.

Check Your Understanding

1. How many layers are there in the OSI reference model?

   (a) 4 (b) 5

   (c) 6 (d) 7

2. Which layer of the OSI model is responsible for routing?

   (a) Transport (b) Data Link

   (c) Network (d) Session

3. TCP is a:
   (a) Connectionless protocol
   (b) Reliable, connection-oriented protocol
   (c) Transport layer device
   (d) Network layer protocol
4. Which of the following addresses is used by switches to forward data?
   (a) Logical address (b) Port address
   (c) Specific address (d) Physical address
5. Which protocol is faster but unreliable, TCP or UDP?
   (a) TCP (b) UDP
   (c) Both (d) None
6. What is the full form of TCP/IP?
   (a) Transmission Control Protocol/Internet Protocol
   (b) Transfer Control Protocol/Internet Protocol
   (c) Tele Communication Protocol/Internet Protocol
   (d) None of the above
7. Which layer of the OSI model ensures error-free delivery?
   (a) Application (b) Presentation
   (c) Transport (d) Network
8. Which addressing type is assigned by the MAC manufacturer?
   (a) Logical Address (b) Physical Address
   (c) Port Address (d) IP Address
9. Which model uses only 4 layers to describe network functionality?
   (a) ISO Model (b) OSI Model
   (c) TCP/IP Model (d) Hybrid Model
10. A port address is mainly used in which layer?
   (a) Data Link Layer (b) Transport Layer
   (c) Network Layer (d) Physical Layer

Answers

1. (d)	2. (c)	3. (b)	4. (d)	5. (b)	6. (a)	7. (c)	8. (b)	9. (c)	10. (b)

Practice Questions

Q.1 Answer the following questions in short:

1. What does OSI stand for?
2. Name any two functions of the transport layer.
3. What is the purpose of the session layer in the OSI model?

3...

Network Connectivity Devices and Technologies

Learning Objectives...

- To understand the Categories of Connectivity Devices.
- To learn the concept of Hub, Switch, Router, Repeaters, Bridges, Gateways, Modem.
- To study Network security devices and Ethernet and wireless technologies.

3.1 CATEGORIES OF CONNECTIVITY DEVICES

- There are a number of connecting devices to build or establish a network, out of which some devices are shown in Fig. 3.1:

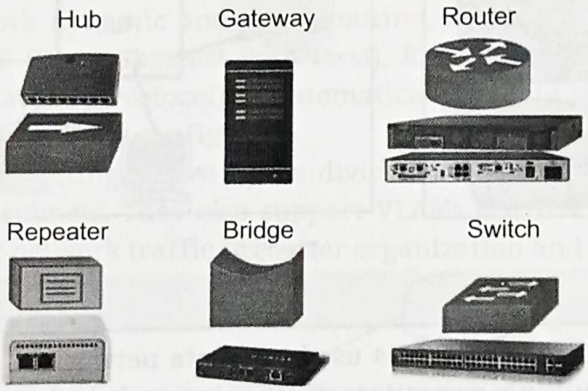


Fig. 3.1

3.2 HUB

- A hub is a basic device used to connect multiple computers or other network devices in a Local Area Network (LAN). It is a hardware device, which is used to create network.

- It operates at the physical layer (Layer 1) of the OSI model and is used to transmit data packets to all devices on the network.
- Transmission mode of Hub is half duplex.
- Hubs transmit data packets to all devices connected to them.
- There are two main types of hubs:

1. **Passive Hub:**
   - Does not amplify or regenerate the signal.
   - Simply connects all the network devices together and passes on the signal.
   - Relies on the connected devices to manage the data traffic.
2. **Active Hub:**
   - Amplifies and regenerates the signal before passing it on to other devices.
   - Requires an external power source.
   - Helps in extending the distance over which data can travel in the network by boosting the signal strength.

- A third, less common type is:

3. **Intelligent Hub (Smart Hub):**
   - Provides additional features such as remote management and monitoring of the network traffic.
   - Can include features like switching and routing, making them more versatile than basic hubs.
   - Often used in more complex network environments where network performance and monitoring are crucial.

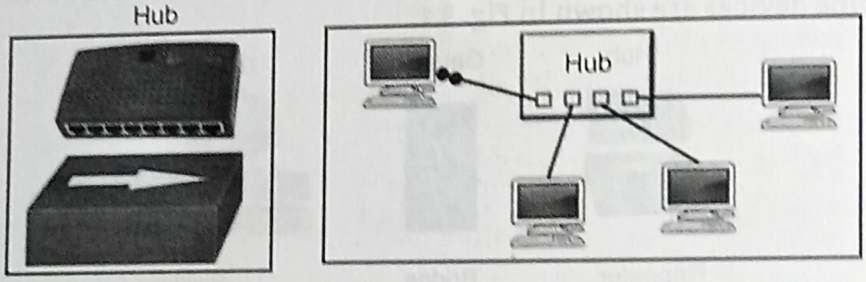


Fig. 3.2

3.3 SWITCH

- It is a hardware device, which is used to create network. A switch is a basic device used to connect multiple computers or other network devices.
- It operates at the data link layer (Layer 2) of the OSI model.
- Transmission mode of Switch is both half duplex and full duplex, but mostly operates in full duplex.
- Switches maintain a MAC address table that maps each connected device's MAC address to the corresponding port on the switch.
- Switches examine the data packets (frames) they receive and forward them only to the specific device for which the data is intended.

- Switches can be easily scaled to support larger networks by adding more switches and connecting them together, allowing for flexible network expansion.

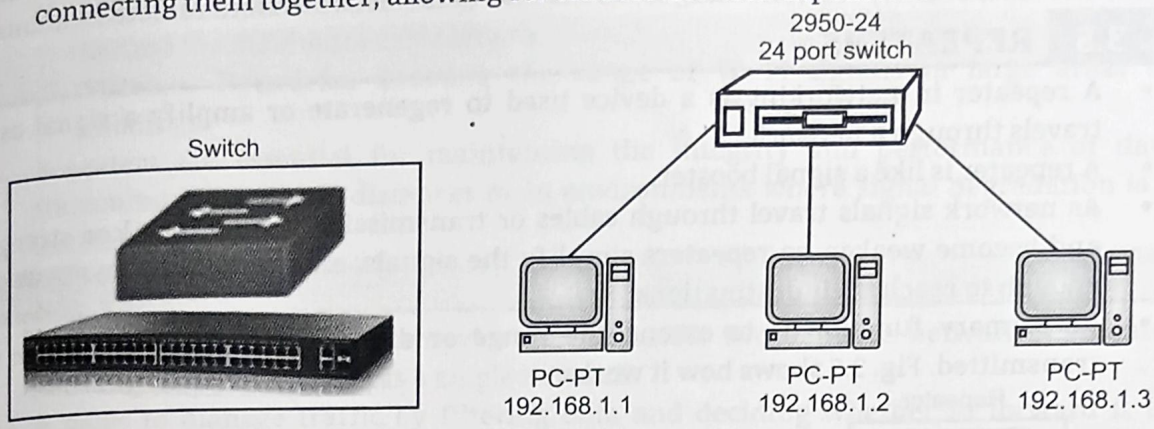


Fig. 3.3

3.4 ROUTER

- Routers connect multiple networks, such as different LANs or a LAN to a WAN (Wide Area Network), facilitating communication between them. It is a hardware device, which is used to create network.
- It operates at the network layer (Layer 3) of the OSI model.
- Transmission mode of Router is full duplex.
- Routers use IP addresses to determine the best path for forwarding data packets to their destination.
- They maintain routing tables that store information about network paths and use routing algorithms to find the most efficient route.
- Routers support both dynamic and static routing, in dynamic routing, routers use protocols like OSPF (Open Shortest Path First), RIP (Routing Information Protocol), and BGP (Border Gateway Protocol) to automatically update routing tables, in static routing, routes are manually configured.
- Routers support subnetting, allowing the division of a larger network into smaller, more manageable subnets. They also support VLANs (Virtual Local Area Networks), which can segment network traffic for better organization and security.

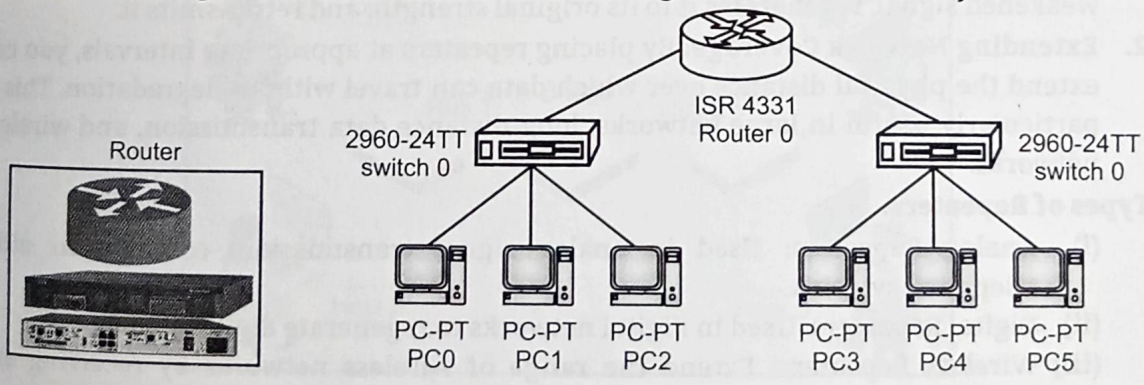
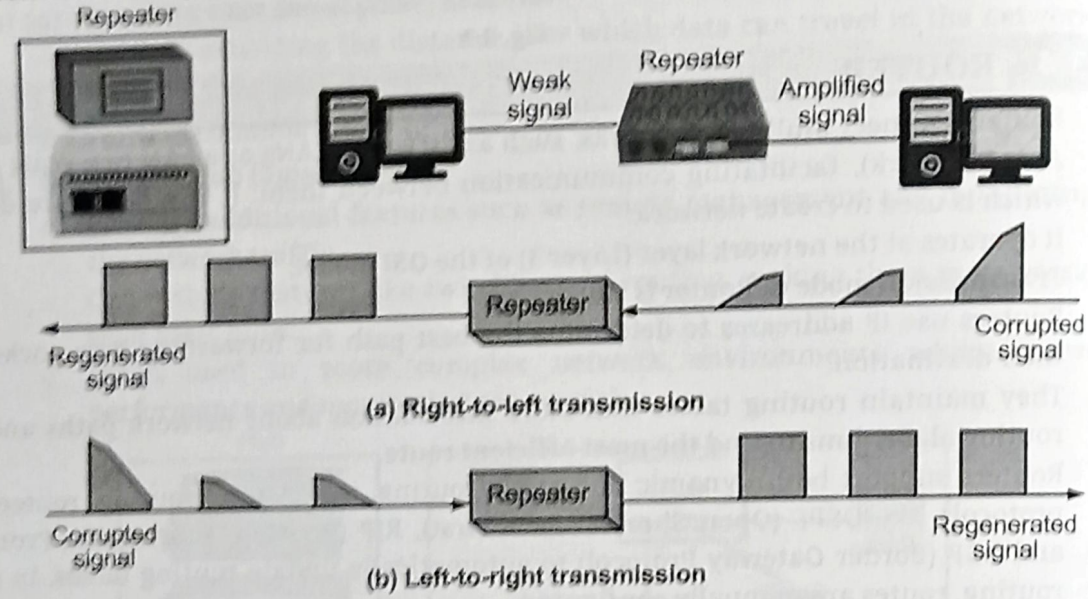


Fig. 3.4

- Routers can provide remote access capabilities and support VPN (Virtual Private Network) connections, enabling secure access to the network from remote locations.

3.5 REPEATERS

- A repeater in networking is a device used to regenerate or amplify a signal as it travels through a network.
- A repeater is like a signal booster.
- As network signals travel through cables or transmission media, they lose strength and become weaker, so repeaters simplify the signals, ensuring they remain strong enough to reach their destinations.
- Its primary function is to extend the range or distance over which data can be transmitted. Fig. 3.5 shows how it works.



(a) Right-to-left transmission

(b) Left-to-right transmission

Fig. 3.5

1. **Signal Regeneration:** As data travels through a network cable, the signal can degrade or weaken due to distance, interference, or other factors. A repeater takes the weakened signal, regenerates it to its original strength, and retransmits it.
2. **Extending Network Coverage:** By placing repeaters at appropriate intervals, you can extend the physical distance over which data can travel without degradation. This is particularly useful in large networks, long-distance data transmission, and wireless networks.

Types of Repeaters:

(i) Analog Repeaters: Used in analog signal transmission, common in older telephone systems.

(ii) Digital Repeaters: Used in digital networks to regenerate digital signals.

(iii) Wireless Repeaters: Extend the range of wireless networks by receiving and retransmitting wireless signals.

Applications:

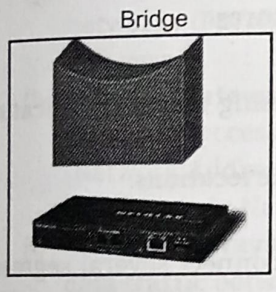
(i) **Wired Networks:** Extending the reach of Ethernet or other wired networks beyond the maximum cable length.

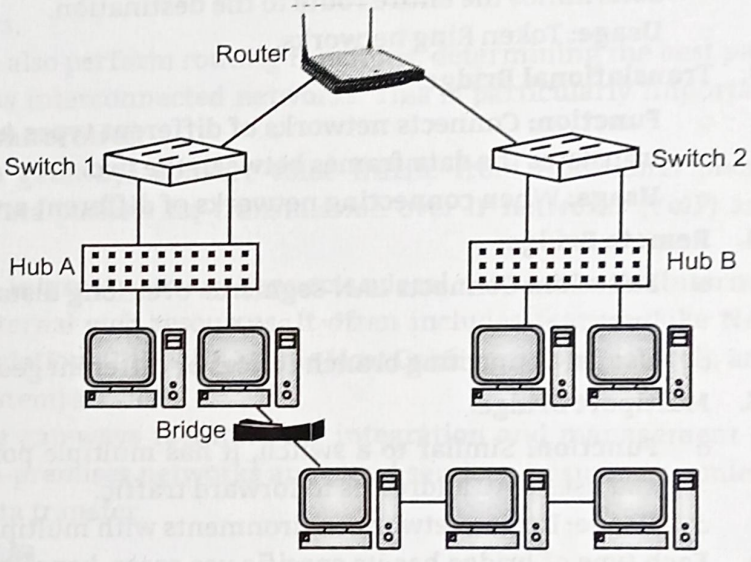
(ii) **Wireless Networks:** Boosting the range of Wi-Fi signals in large areas or buildings.

- Repeaters are essential for maintaining the integrity and performance of data transmission over long distances or in environments where signal degradation is a concern.

3.6 BRIDGES

- A bridge in networking is a device that connects two or more network segments, allowing them to function as a single network.
- It helps to manage traffic by filtering data and deciding whether to forward it to another segment.





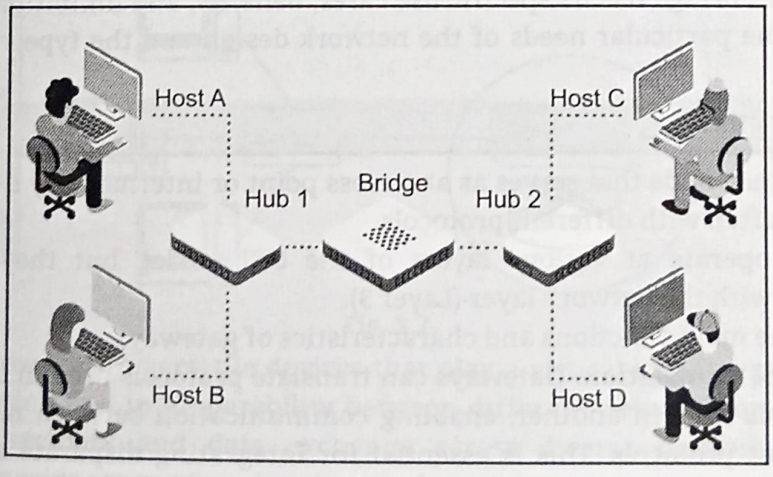


Fig. 3.6

- Bridges reduce network congestion by dividing large networks into smaller, more manageable sections.
- They work at the data link layer (Layer 2) of the OSI model.
- Overall, bridges improve network performance and efficiency by ensuring data is sent only where it needs to go.

3.6.1 Types of Bridge

1. **Transparent Bridge:**
   - **Function:** Learns the MAC addresses of devices on each segment and forwards frames based on this information.
   - **Usage:** Common in Ethernet networks.
2. **Source-Route Bridge:**
   - **Function:** Used primarily in Token Ring networks, where the source device determines the entire route to the destination.
   - **Usage:** Token Ring networks.
3. **Translational Bridge:**
   - **Function:** Connects networks of different types (e.g., Ethernet to Token Ring) and translates the data frames between the two.
   - **Usage:** When connecting networks of different architectures.
4. **Remote Bridge:**
   - **Function:** Connects LAN segments over long distances using telecommunications links.
   - **Usage:** Connecting branch offices or different geographic locations.
5. **Multiport Bridge:**
   - **Function:** Similar to a switch, it has multiple ports to connect several segments and uses MAC addresses to forward traffic.
   - **Usage:** Larger network environments with multiple segments.

- Each type of bridge has its specific use cases, benefits, and limitations, and is chosen based on the particular needs of the network design and the type of network being connected.

3.7 GATEWAYS

- A gateway is a node that serves as an access point or intermediary between different networks, often with different protocols.
- Gateways operate at various layers of the OSI model, but they are commonly associated with the network layer (Layer 3).
- Here are the main functions and characteristics of gateways:

(a) **Protocol Translation:** Gateways can translate protocols used in one network into protocols used in another, enabling communication between networks that use different protocols. This is essential for integrating disparate systems, such as connecting an IP-based network with a non-IP-based network.

(b) **Network Interconnection:** Gateways connect different networks, allowing devices on separate networks to communicate. This can include connecting a Local Area Network (LAN) to a Wide Area Network (WAN) or connecting networks within different organizations.

(c) **Data Format Translation:** Besides protocol translation, gateways can also handle data format translation, converting data from one format to another as it passes between networks. This ensures that the data is usable on both sides of the gateway.

(d) **Application Layer Gateways:** These gateways operate at the application layer (Layer 7) and are used to manage specific types of traffic such as email, voice, and video. Examples include email gateways that filter spam and virus-infected messages.

(e) **Firewall and Security:** Many gateways include firewall capabilities to filter traffic and enforce security policies, protecting the network from unauthorized access and cyber threats.

(f) **Routing:** Gateways can also perform routing functions, determining the best path for data to travel across interconnected networks. This is particularly important in complex network architectures.

(g) **VoIP Gateways:** These gateways convert voice traffic from traditional phone networks (PSTN) into data packets for transmission over IP networks (VoIP) and vice versa.

(h) **Internet Gateways:** An internet gateway connects a local network to the internet, providing access to external web resources. It often includes features like NAT (Network Address Translation), DHCP (Dynamic Host Configuration Protocol), and DNS (Domain Name System) services.

(i) **Cloud Gateways:** These gateways facilitate the integration and management of data traffic between on-premises networks and cloud services, ensuring seamless communication and data transfer.

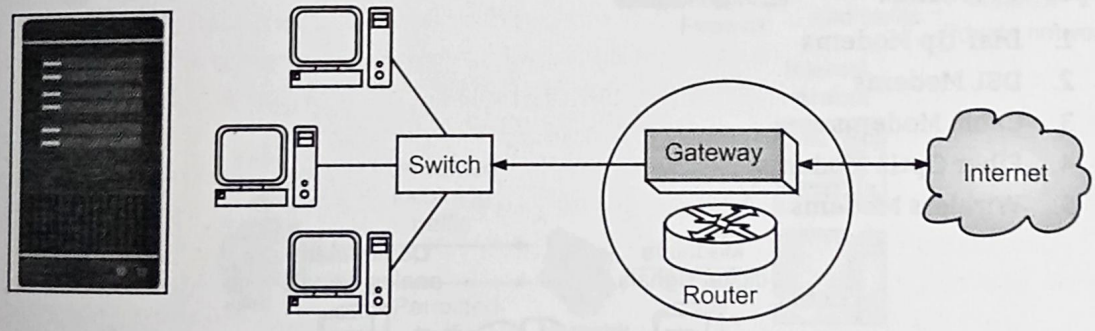


Fig. 3.7

- Overall, gateways are versatile devices that play a critical role in ensuring seamless communication and interoperability between different networks and systems. They enable connectivity and data exchange across diverse network environments, supporting a wide range of applications and services.

3.8 MODEM

- A modem (short for modulator-demodulator) is a device that converts digital data from a computer or other digital device into analog signals that can be transmitted over telephone lines, cable systems, or other analog communication mediums, and vice versa.
  - **Modulation and Demodulation:** The primary function of a modem is to modulate digital data into analog signals for transmission over an analog medium and to demodulate incoming analog signals back into digital data that can be understood by digital devices.
  - **Connection Interface:** Modems typically connect to a computer or a router using Ethernet or USB interfaces. The modem acts as a bridge between the local network and the wider internet.
  - **Data Transmission Speeds:** The speed of a modem depends on the type and technology used. For example, fiber optic modems can support gigabit speeds, while older dial-up modems are much slower.
  - **Error Correction and Compression:** Modems often include features for error correction and data compression to improve the efficiency and reliability of data transmission.
  - **Configuration and Management:** Modems can usually be configured and managed through a web interface, allowing users to set up connections, monitor performance, and troubleshoot issues.
- Overall, modems are essential devices for connecting local networks to the broader internet, enabling data transmission over various types of communication mediums.
- They play a crucial role in ensuring that digital data can be transmitted efficiently and reliably across different types of networks.

Types of Modems:

1. Dial-Up Modems
2. DSL Modems
3. Cable Modems
4. Fiber Optic Modems
5. Wireless Modems

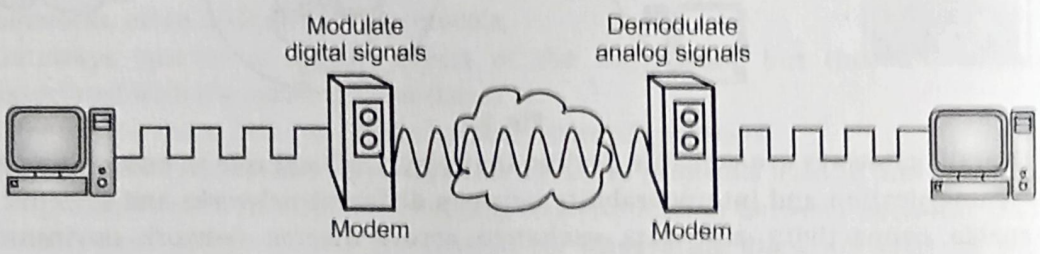


Fig. 3.8

3.9 NETWORK SECURITY DEVICES

3.9.1 Firewalls

- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- Firewalls are essential for protecting networks from unauthorized access, cyberattacks, and other security threats.
- Firewalls analyse network traffic and decide whether to allow or block specific traffic based on security rules.
- It controls incoming and outgoing traffic based on predefined rules.
- These rules can be based on IP addresses, ports, protocols, and other criteria.
- Table 3.1 illustrates how it maintains the table.

Table 3.1

Sr. No.	Source IP	Det. IP	Source Port	Dest. Port	Action
1.	192.168.21.0	--	--	--	deny
2.	--	--	--	23	deny
3.	--	192.168.21.3	--	--	deny
4.	--	192.168.21.0	--	>1023	Allow

- Firewall is a device that can be either hardware or software.
- It works on network and transport layers.
- It can block IP address, services like http, https, etc.

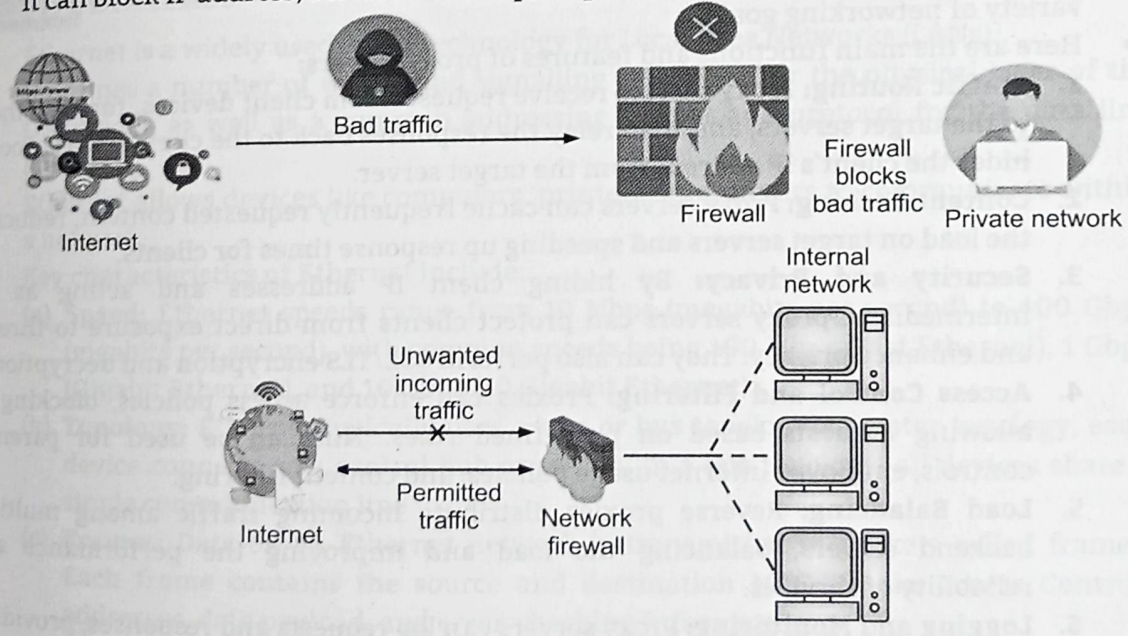


Fig. 3.9

- **Access Control:** Firewalls enforce access control policies, determining which users or devices can access specific network resources, this helps prevent unauthorized access and data breaches.
- **Application Control:** Advanced firewalls can control access to specific applications and services, enforcing policies based on the application rather than just IP addresses and ports.
- Firewalls are a critical component of a comprehensive network security strategy, providing a first line of defence against cyber threats and helping to ensure the integrity, confidentiality, and availability of network resources.

Types of Firewalls:

1. Packet-Filtering Firewalls
2. Stateful Inspection Firewalls
3. Proxy Firewalls
4. Next-Generation Firewalls (NGFWs)

3.9.2 Proxy Server

- A proxy server is an intermediary server that sits between client devices and target servers.
- It manages requests and responses to improve performance, security, and privacy.
- It hides the client's IP address from the target server.
- Proxy servers play a crucial role in managing and securing network traffic, improving performance, and enhancing privacy.
- They are widely used in both enterprise and personal environments to achieve a variety of networking goals.
- Here are the main functions and features of proxy servers:
  1. **Traffic Routing:** Proxy servers receive requests from client devices, forward them to the target servers, and then relay the responses back to the clients. This process hides the client's IP address from the target server.
  2. **Content Caching:** Proxy servers can cache frequently requested content, reducing the load on target servers and speeding up response times for clients.
  3. **Security and Privacy:** By hiding client IP addresses and acting as an intermediary, proxy servers can protect clients from direct exposure to threats and enhance privacy. They can also perform SSL/TLS encryption and decryption
  4. **Access Control and Filtering:** Proxies can enforce access policies, blocking or allowing requests based on predefined rules. This can be used for parental controls, employee internet usage policies, and content filtering.
  5. **Load Balancing:** Reverse proxies distribute incoming traffic among multiple backend servers, balancing the load and improving the performance and reliability of services.
  6. **Logging and Monitoring:** Proxy servers can log requests and responses, providing valuable data for monitoring network activity, troubleshooting issues, and auditing purposes.

7. **Bypassing Restrictions:** Clients can use proxy servers to bypass geographic restrictions, censorship, and firewall rules by masking their IP addresses.

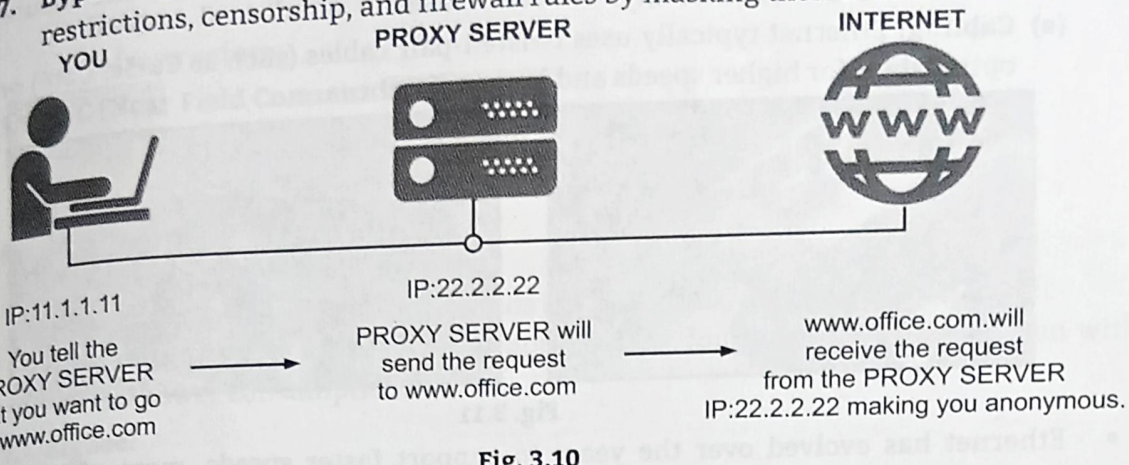


Fig. 3.10

Types of Proxy Servers:

1. Forward Proxy
2. Reverse Proxy
3. Transparent Proxy
4. Anonymous Proxy
5. High Anonymity Proxy (Elite Proxy)

3.10 ETHERNET AND WIRELESS TECHNOLOGIES

3.10.1 Ethernet

- Ethernet is a widely used wired technology for Local Area Networks (LANs).
- It defines a number of wiring and signalling standards for the physical layer of the OSI model, as well as a common addressing format and protocol for the data link layer.
- Ethernet allows devices like computers, printers, and servers to communicate within a network.
- Key characteristics of Ethernet include:
  - **(a) Speed:** Ethernet speeds range from 10 Mbps (megabits per second) to 400 Gbps (gigabits per second), with common speeds being 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), and 10 Gbps (10 Gigabit Ethernet).
  - **(b) Topology:** Ethernet typically uses a star or bus topology. In a star topology, each device connects to a central hub or switch. In a bus topology, all devices share a single communication line.
  - **(c) Frames:** Data on an Ethernet network is transmitted in packets called frames. Each frame contains the source and destination MAC (Media Access Control) addresses, data payload, and error-checking information.
  - **(d) Medium Access Control (MAC):** Ethernet uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol to manage how devices share the

communication channel. This protocol helps prevent collisions and ensures that data is transmitted smoothly.

(e) **Cabling:** Ethernet typically uses twisted-pair cables (such as Cat5e, Cat6) or fiber optic cables for higher speeds and longer distances.

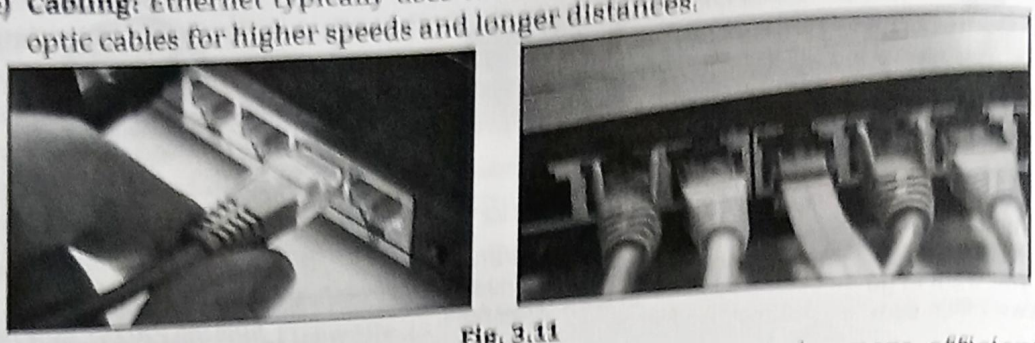


Fig. 3.11

- Ethernet has evolved over the years to support faster speeds, more efficient data transmission, and better scalability, making it a foundational technology for modern networking.

3.9.2 Wireless Technologies

- Wireless technologies in networking enable devices to communicate without physical connections, offering flexibility and mobility.
- Here are some key wireless technologies:

1. **Wi-Fi (Wireless Fidelity):**
   - **Standards:** IEEE 802.11 family (a/b/g/n/ac/ax).
   - **Frequency Bands:** Typically, 2.4 GHz and 5 GHz, with newer standards using 6 GHz.
   - **Speed:** Varies by standard, from 54 Mbps (802.11g) to several Gbps (802.11ax).
   - **Usage:** Home and office networking, public hotspots.
2. **Bluetooth:**
   - **Standard:** IEEE 802.15.1.
   - **Frequency Band:** 2.4 GHz.
   - **Range:** Short range, typically up to 100 meters.
   - **Usage:** Personal Area Networks (PANs), connecting peripherals (keyboards, mice, headphones).
3. **Cellular Networks:**
   - **Generations:** 2G, 3G, 4G (LTE), 5G.
   - **Frequency Bands:** Various, depending on the technology and region.
   - **Speed:** Varies by generation, with 5G offering up to several Gbps.
   - **Usage:** Mobile phone connectivity, mobile internet.
4. **WiMAX (Worldwide Interoperability for Microwave Access):**
   - **Standard:** IEEE 802.16.
   - **Frequency Bands:** 2.3 GHz, 2.5 GHz, 3.5 GHz, 5.8 GHz.

- **Speed:** Up to 1 Gbps.
- **Usage:** Broadband internet access, especially in areas without wired infrastructure.

5. **NFC (Near Field Communication):**
   - **Range:** Very short, typically a few centimetres.
   - **Usage:** Contactless payments, data exchange between devices.
6. **LoRa (Long Range):**
   - **Standard:** LoRaWAN.
   - **Frequency Bands:** Sub-GHz bands (e.g., 433 MHz, 868 MHz, 915 MHz).
   - **Usage:** Internet of Things (IoT) applications, long-range communication with low power consumption.
7. **Zigbee:**
   - **Standard:** IEEE 802.15.4.
   - **Frequency Bands:** 2.4 GHz, 868 MHz, 915 MHz.
   - **Usage:** Smart home devices, IoT applications, low-power and low-data-rate communication.

- These technologies cater to different networking needs, from high-speed data transfer and internet connectivity to low-power communication for IoT devices.

Summary

- Hub, Gateway, Router, Repeater, Bridge, Switch are connecting devices to build or establish a network.
- A hub is a basic device used to connect multiple computers or other network devices in a Local Area Network (LAN). There are two main types of Hubs: Passive and Active Hub.
- A switch is a basic device used to connect multiple computers or other network devices.
- Routers connect multiple networks, such as different LANs or a LAN to a WAN (Wide Area Network), facilitating communication between them.
- A repeater in networking is a device used to regenerate or amplify a signal as it travels through a network.
- A bridge in networking is a device that connects two or more network segments, allowing them to function as a single network.
- A gateway is a node that serves as an access point or intermediary between different networks, often with different protocols.
- A modem (short for modulator-demodulator) is a device that converts digital data from a computer or other digital device into analog signals that can be transmitted over telephone lines, cable systems, or other analog communication mediums, and vice versa.

- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- A proxy server is an intermediary server that sits between client devices and target servers.
- Ethernet defines a number of wiring and signalling standards for the physical layer of the OSI model, as well as a common addressing format and protocol for the data link layer.

Check Your Understanding

1. Which of the following devices operates at the physical layer (Layer 1) of the OSI model?
   (a) Router (b) Switch
   (c) Hub (d) Bridge
2. Which type of hub can monitor traffic and provide statistics?
   (a) Passive hub (b) Active hub
   (c) Intelligent hub (d) None of the above
3. A switch operates at which OSI layer?
   (a) Layer 1 (b) Layer 2
   (c) Layer 3 (d) Layer 4
4. Which of the following devices can break up broadcast domains?
   (a) Hub (b) Repeater
   (c) Router (d) Switch
5. What is the main function of a repeater?
   (a) Filtering traffic
   (b) Breaking broadcast domains
   (c) Amplifying and regenerating signals
   (d) Assigning IP addresses
6. Which type of bridge selects the path based on the source of the data?
   (a) Transparent Bridge (b) Source Routing Bridge
   (c) Translational Bridge (d) Remote Bridge
7. Which device connects different network architectures such as Ethernet and Token Ring?
   (a) Router (b) Gateway
   (c) Bridge (d) Switch
8. What does a firewall primarily provide?
   (a) Speed enhancement (b) IP address assignment
   (c) Network security (d) Data compression

9. Which device stores and forwards web requests to reduce load on the main server?
   (a) Modem (b) Switch
   (c) Proxy Server (d) Bridge
10. Which device connects a LAN to the internet via telephone lines?
   (a) Modem (b) Hub
   (c) Bridge (d) Switch

Answers

1. (c)	2. (c)	3. (b)	4. (c)	5. (c)	6. (b)	7. (b)	8. (c)	9. (c)	10. (a)

Practice Questions

Q.I Answer the following questions in short:

1. What OSI layer does a switch operate on?
2. Define a passive hub.
3. Name any two types of bridges.
4. What is the primary function of a router?
5. What is the difference between a modem and a router?
6. What layer does a bridge operate on?
7. Name any two network security devices.
8. What is the purpose of a repeater in networking?
9. What does a proxy server do?
10. Define a smart hub.
11. List out the wireless technologies.

Q.II Answer the following questions in detail:

1. Explain the differences among a hub, switch, and router in terms of OSI model layers and functionality.
2. Describe the different types of hubs and their uses.
3. Discuss the different types of bridges and explain their specific use cases.
4. What is a gateway and how does it work?
5. Explain how a firewall protects a network.
6. Describe the role of a proxy server in network security and performance.
7. Discuss Ethernet and wireless technologies.
8. Describe how a modem works and its role in internet connectivity.
9. Discuss how different network connectivity devices work together in a typical enterprise network setup.
10. Explain repeater with its functionality, types and applications.

4...

IP Addressing and Sub-netting

Learning Objectives...

- To understand the concept of IPv4.
- To learn about IPv6.

4.1 INTRODUCTION TO IPv4

4.1.1 IPv4 Address

- IPv4, or Internet Protocol version 4, is one of the core protocols of the Internet Protocol Suite.
- It is used to identify and locate devices on a network, as well as to route traffic between them.
- IPv4 addresses are 32-bit numbers, typically shown in decimal format as four octets separated by periods (e.g., 192.168.1.1).
- IPv4 address is represented in decimal and it has 4 octets.
- IPv4 address ranges from 0.0.0.0 to 255.255.255.255.
- Every node in the network is identified with the help of IP address.
- It can be changed based on changing the network and/or location.

Address Classes:

- IPv4 addresses are divided into different classes (A, B, C, D, E) based on their range and intended use shown in Table 4.1.

Table 4.1: Classes of IPv4 Address

Address Class	1st Octet range in decimal	1st Octet bits (Blue bits do not change)	Network (N) and Host (H) Portion	Default mask (Decimal)	Number of possible networks and hosts per network
A	0–127	00000000 - 01111111	N.H.H.H	255.0.0.0	128 Nets (2^7) 16,777,214 hosts ($2^{24}-2$)
B	128–191	10000000 - 10111111	N.N.H.H	255.255.0.0	16,384 Nets (2^{14}) 65,534 hosts ($2^{16}-2$)
C	192–223	11000000 - 11011111	N.N.N.H	255.255.255.0	2,097,150 Nets (2^{21}) 254 hosts (2^8-2)
D	224–239	11100000 - 11101111	NA (Multicast)	-	-
E	240–255	11110000 - 11111111	NA (Experimental)	-	-

Parts of IPv4:

1. **Network Part:**
   - This part shows which network the IP address belongs to.
   - It also helps identify the type or class of the network (like Class A, B, or C).
2. **Host Part:**
   - This part identifies the specific device (like a computer or phone) on the network.
   - Each device on the same network gets a unique host part.
3. **Subnet Mask:**
   - A subnet mask tells you which part of the IP address is the network and which is the host.
   - It looks like an IP address and also has 32 bits (e.g., 255.255.255.0).

For Example,

For the IP address **192.168.1.1**:

- **Network Part:** 192.168.1
- **Host Part:** 1
- **Subnet Mask:** 255.255.255.0

4.1.2 IPv4 Subnetting

- IPv4 Subnet mask:
  (i) A subnet mask is used to specify which portion of the IP address is the network and which portion is the host.
  (ii) It also has 32 bits and is usually written in the same format as the IP address (e.g., 255.255.255.0).
- Subnetting in IPv4 is a technique used to divide a larger network into smaller, more manageable sub-networks, or subnets.
- This process enhances network performance, improves security, and makes better use of IP address space.
- Here's a detailed overview of how subnetting works in IPv4:

What is a Subnet Mask?

- A **subnet mask** helps split an IP address into two parts:
  - **Network part** (which network it belongs to)
  - **Host part** (which device it is on that network).
- It is a 32-bit number, written like an IP address (e.g., 255.255.255.0).

What is Subnetting?

- **Subnetting** means dividing a big network into smaller pieces, called subnets.
- It helps with:
  - Better performance.
  - More efficient use of IP addresses.
  - Improved security and organization.

How Subnetting Works (Step-by-Step):

1. **Decide How Many Subnets You Need**
   Example: If you need 8 subnets, you must find how many bits to "borrow" from the host portion of the address.
2. **Calculate Bits Needed for Subnets**
   Use the formula: 2^n = number of subnets
   Example: If you borrow 3 bits, $2^3 = 8$ subnets.
3. **Update the Subnet Mask**
   Take the default subnet mask (like 255.255.255.0, which is /24) and add the borrowed bits.
   Example: Borrowing 3 bits gives /27, which is 255.255.255.224.
4. **Split the Network into Subnets**
   Each subnet will now have a fixed number of addresses.
   With a /27 mask, each subnet has 32 addresses (including network and broadcast addresses).
5. **Assign IP Addresses**
   Each subnet will have:
   - A network address
   - A range of usable IPs
   - A broadcast address

For Example,

- **Original Network:** 192.168.1.0/24
- **Need:** 4 subnets
- **Bits Needed:** 2 bits (since $2^2 = 4$)
- **New Subnet Mask:** /26 → 255.255.255.192

Subnets Created:

1. **192.168.1.0/26**
   - **Usable IPs:** 192.168.1.1 to 192.168.1.62
   - **Broadcast:** 192.168.1.63
2. **192.168.1.64/26**
   - **Usable IPs:** 192.168.1.65 to 192.168.1.126
   - **Broadcast:** 192.168.1.127
3. **192.168.1.128/26**
   - **Usable IPs:** 192.168.1.129 to 192.168.1.190
   - **Broadcast:** 192.168.1.191
4. **192.168.1.192/26**
   - **Usable IPs:** 192.168.1.193 to 192.168.1.254
   - **Broadcast:** 192.168.1.255

4.1.3 IPv4 Header

- The IPv4 header is a crucial part of the IPv4 protocol, which is used for routing packets across networks. It contains important information about the packet, including how it should be processed and where it should be delivered. Here's a detailed breakdown of the IPv4 header fields:

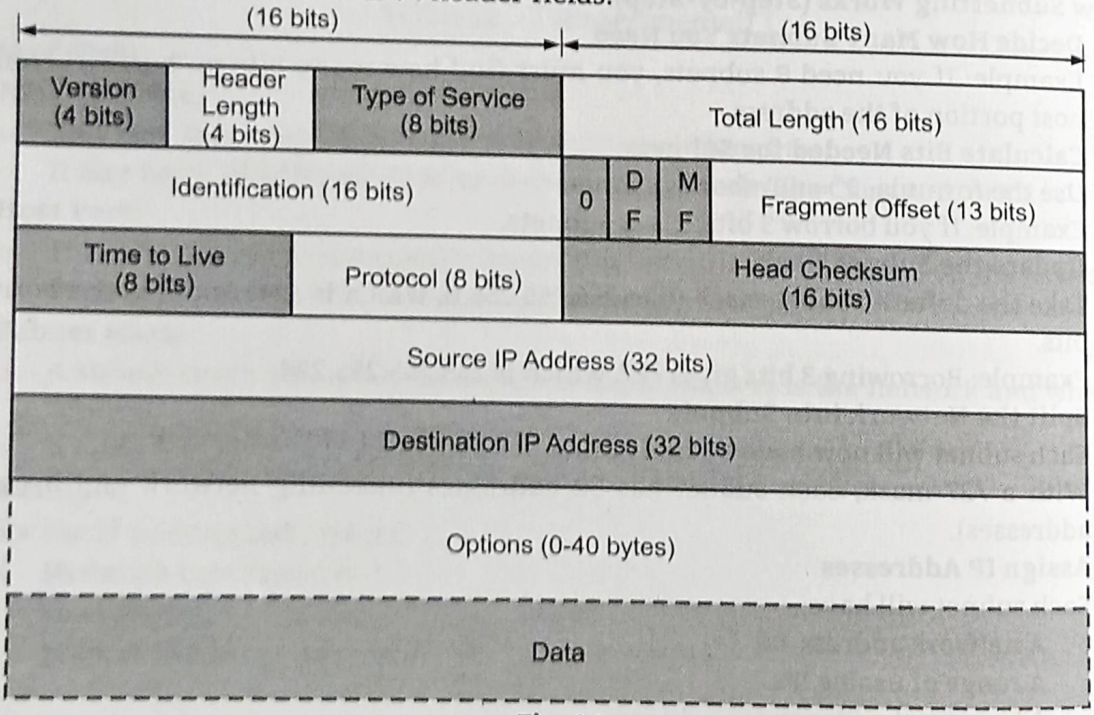


Fig. 4.1

IPv4 Header Structure:

- The IPv4 header is 20 to 60 bytes long, with the minimum length being 20 bytes. It consists of several fields, each serving a specific purpose:

1. **Version (4 bits):** Indicates the IP protocol version. For IPv4, this is always 4.
2. **IHL (Internet Header Length) (4 bits):** Specifies the length of the header in 32-bit words. The minimum value is 5, which means the header is 20 bytes long. If the IHL is greater than 5, it indicates that there are optional fields present.
3. **Type of Service (ToS) (8 bits):** Specifies the desired quality of service for the packet. This field has been redefined as the Differentiated Services Field (DSCP) and ECN (Explicit Congestion Notification) in modern implementations.
4. **Total Length (16 bits):** Indicates the total length of the IP packet, including both the header and the data. The maximum value is 65,535 bytes.
5. **Identification (16 bits):** Used for uniquely identifying the packet, especially when it is fragmented. It helps in reassembling the fragments at the destination.
6. **Flags (3 bits):** Indicates control flags for fragmentation:
   - **Bit 0:** Reserved, must be zero.
   - **Bit 1:** Don't Fragment (DF) flag. If set, the packet should not be fragmented.
   - **Bit 2:** More Fragments (MF) flag. If set, there are more fragments after this one.
7. **Fragment Offset (13 bits):** Indicates the position of the fragment in the original packet, measured in 8-byte units. It is used to reassemble the original packet from fragments.
8. **Time to Live (TTL) (8 bits):** Specifies the maximum number of hops (routers) the packet can pass through before being discarded. It helps prevent packets from looping indefinitely.
9. **Protocol (8 bits):** Indicates the protocol used in the data portion of the packet. For example:
   - 1 for ICMP
   - 6 for TCP
   - 17 for UDP
10. **Header Checksum (16 bits):** Used for error-checking the header. It ensures the integrity of the header data by detecting any corruption during transmission.
11. **Source IP Address (32 bits):** The IP address of the sender of the packet.
12. **Destination IP Address (32 bits):** The IP address of the intended recipient of the packet.
13. **Options (Variable length):** Optional field that can be used for various network functions, such as timestamping or security. This field is not always present and can extend the header length beyond 20 bytes.
14. **Padding (Variable length):** Added to ensure the header length is a multiple of 32 bits if the Options field is used. Padding is not a separate field but part of the header's variable length.
15. **Data (Variable length):** The actual payload or data being transmitted by the packet.

4.2 INTRODUCTION TO IPV6

4.2.1 IPv6 Address

- An IPv6 address is a type of IP address used to identify devices on a network, especially on the Internet. It's part of the latest version of the IP protocol, which was developed to address the limitations of IPv4, particularly the exhaustion of available IP addresses.
- Here's a quick rundown of what you need to know about IPv6 addresses:
  1. Format: IPv6 addresses are 128 bits long, compared to IPv4's 32 bits. This gives a vastly larger address space. An IPv6 address is typically written in hexadecimal, divided into eight groups of four hexadecimal digits, separated by colons.
     For example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  2. Abbreviation: Leading zeros in each group can be omitted, and one or more groups of all zeros can be replaced with a single colon (::). For example, the address above could be abbreviated as: 2001:db8:85a3::8a2e:370:7334
  3. Types:
     Unicast: Identifies a single unique device.
     Multicast: Identifies a group of devices.
     Anycast: Identifies a group of devices, but data is sent to the nearest one.
  4. Features: IPv6 supports features like simplified security, better multicast and anycast support, and simplified header structure compared to IPv4.
  5. Addressing: IPv6 addresses are usually assigned based on geographic regions, and they can be either global (publicly routable) or local (private to within a specific organization).

4.2.2 IPv6 Header

- The IPv6 header consists of several fields, each serving a specific function. Here's a detailed breakdown:

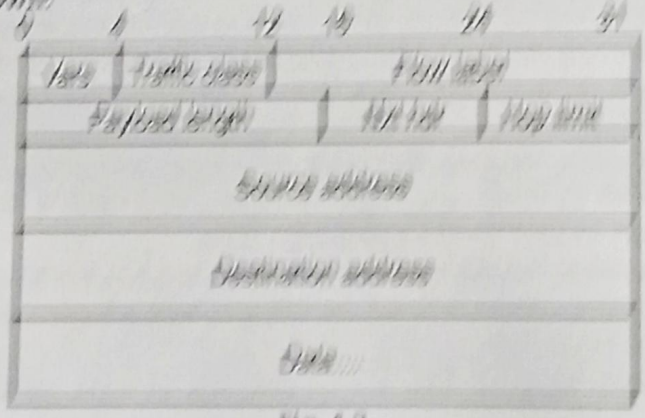


Fig 4.3

1. **Version (4 bits):** Indicates the IP protocol version. For IPv6, this field is always set to 6.
2. **Traffic Class (8 bits):** Used for defining the class or priority of the packet. It's similar to the Type of Service (ToS) field in IPv4 but is divided into two parts: the most significant 6 bits are used for Differentiated Services Code Point (DSCP), and the least significant 2 bits are used for Explicit Congestion Notification (ECN).
3. **Flow Label (20 bits):** Used to label sequences of packets that require special handling, such as real-time data or high-priority data. It allows routers to identify and handle packets with specific flow characteristics.
4. **Payload Length (16 bits):** Specifies the length of the payload (data) following the IPv6 header, in bytes. This field does not include the length of the header itself.
5. **Next Header (8 bits):** Indicates the type of the next header or extension header that follows the IPv6 header. This is similar to the protocol field in IPv4. For example:
   (a) 6 for TCP
   (b) 17 for UDP
   (c) 58 for ICMPv6
6. **Hop Limit (8 bits):** Replaces the TTL (Time to Live) field in IPv4. It specifies the maximum number of hops (routers) the packet can pass through before being discarded. Each router along the path decrements this value by one.
7. **Source Address (128 bits):** The IPv6 address of the originator of the packet.
8. **Destination Address (128 bits):** The IPv6 address of the intended recipient of the packet.

Summary

- IPv4, or Internet Protocol version 4, is one of the core protocols of the Internet Protocol Suite.
- Subnetting allows you to create multiple subnets from a single network, optimizing the use of IP addresses and improving network management.
- By understanding how to calculate subnet masks and determine the range of each subnet, you can effectively manage and scale your IPv4 network.
- The IPv4 header is a crucial part of the IPv4 protocol, which is used for routing packets across networks.
- An IPv6 address is a type of IP address used to identify devices on a network, specifically on the internet.

Check Your Understanding

1. How many bits are in an IPv4 address?
   (a) 32
   (b) 64
   (c) 128
   (d) 256

2. Which of the following is a valid IPv4 address?
   (a) 192.168.1.256 (b) 10.0.0.1
   (c) 123.456.78.90 (d) 300.1.1.1
3. What does subnetting do?
   (a) Increases IP address size
   (b) Divides a network into smaller sub-networks
   (c) Encrypts IP traffic
   (d) Assigns MAC addresses
4. How many bits are in an IPv6 address?
   (a) 32 (b) 64
   (c) 96 (d) 128
5. Which of the following is a valid IPv6 address?
   (a) 192.168.1.1 (b) FE80::0202:B3FF:FE1E:8329
   (c) 10.0.0.256 (d) 1234:5678:90AB:
6. What field in the IPv4 header determines the lifetime of a packet?
   (a) Source IP (b) Protocol
   (c) Time to Live (TTL) (d) Fragment Offset
7. Which protocol is used to resolve IPv4 addresses to MAC addresses?
   (a) DNS (b) DHCP
   (c) ARP (d) ICMP
8. Which of the following is not part of the IPv4 header?
   (a) Source Address (b) Destination Address
   (c) Flow Label (d) TTL
9. What field was introduced in the IPv6 header that does not exist in IPv4?
   (a) TTL (b) Fragment Offset
   (c) Flow Label (d) Header Checksum
10. Why was IPv6 introduced?
    (a) To replace DNS
    (b) To increase bandwidth
    (c) To overcome IPv4 address exhaustion
    (d) To increase packet size

Answers

1. (a)	2. (b)	3. (b)	4. (d)	5. (b)	6. (c)	7. (c)	8. (c)	9. (c)	10. (c)

5...
Routing Protocols

Learning Objectives...

- To understand the Structure of Router.
- To learn the concept of Routing Tables and Types of Routing.
- To study about Intra and Inter Domain Routing.
- To understand the concept of Distance Vector Routing, RIP, OSPF, EIGRP & BGP.

5.1 STRUCTURE OF A ROUTER

- A router is a networking device that directs data packets among different networks, ensuring they reach their correct destinations. Its structure typically includes several key components:

1. **Central Processing Unit (CPU):** The brain of the router, responsible for executing instructions and managing network traffic. It handles routing algorithms, processes incoming and outgoing packets, and manages overall router operations.
2. **Memory:**
   - **RAM (Random Access Memory):** Temporary storage used for processing data and storing routing tables, packet buffers, and running processes.
   - **ROM (Read-Only Memory):** Stores the router's firmware and basic operating system code that is used to start up and run the router.
3. **Routing Table:** A database maintained by the router that contains information about the network topology, including routes to various network destinations. It is used by the router to make decisions about where to forward packets.
4. **Network Interfaces:**
   - **Ethernet Ports:** Physical connections for wired network connections. These ports connect the router to Local Area Networks (LANs) or other devices.
   - **Wireless Interfaces:** For routers with wireless capabilities, these components handle communication with wireless devices using standards like Wi-Fi.
   - **WAN Port:** A specific port for connecting to an external network, typically the Internet.
5. **Switching Fabric:** The internal network within the router that moves data between different ports and interfaces. It ensures that packets are directed to the correct output port.

6. **Power Supply:** Provides electrical power to all components of the router. This could be an internal power supply or an external adapter, depending on the router design.
7. **Cooling System:** Some routers, especially high-performance or enterprise models, have cooling systems (like fans) to dissipate heat generated by the internal components.
8. **LED Indicators:** Lights on the router that show the status of various functions, such as power, network activity, and connectivity.
9. **Management Interface:** Often includes a web-based or command-line interface for configuring and managing the router's settings, monitoring performance, and troubleshooting.
10. **Firmware/Operating System:** The software that controls the router's hardware and enables its functionality. This software includes the operating system and the network protocols necessary for routing.

- Each of these components plays a crucial role in ensuring that the router efficiently and effectively directs data between networks.

5.2 ROUTING TABLES

- A routing table is a fundamental component of a router or a networked computer that stores the routes (paths) to various network destinations. It is used to determine the best path for forwarding data packets to their destination.

Key Components of a Routing Table:

1. **Destination Network:**
   - This is the IP address of the network to which the packet is destined. The routing table will have entries for different network addresses.
2. **Subnet Mask:**
   - The subnet mask is used to specify the network portion of an IP address. It helps in determining the range of IP addresses within a particular network.
3. **Gateway (Next Hop):**
   - The gateway is the IP address of the next hop, which is usually the next router in the path towards the destination network. If the packet's destination is not within the local network, it must be forwarded to another router (gateway).
4. **Interface:**
   - The interface is the network interface (such as Ethernet port) through which the packet should be sent. Each entry in the routing table specifies the interface used to reach the next hop.
5. **Metric:**
   - The metric is a value that indicates the cost of using a particular route. It could be based on hop count, bandwidth, delay, or other factors. Lower metrics are preferred, as they indicate a more optimal route.

6. **Route Type:**
   - This indicates how the route was learned: either dynamically via routing protocols (like OSPF, BGP, RIP) or statically configured by a network administrator.

Example of a Routing Table Entry:

Destination Network	Subnet Mask	Gateway	Interface	Metric
192.168.1.0	255.255.255.0	192.168.1.1	eth0	10
10.0.0.0	255.0.0.0	10.0.0.1	eth1	20
0.0.0.0	0.0.0.0	192.168.1.254	eth0	10

Routing Table Lookup Process:

1. **Packet Arrival:** When a data packet arrives at a router, the router examines the destination IP address of the packet.
2. **Matching Process:** The router compares the destination IP address against the entries in its routing table. It uses the subnet mask to determine the most specific match.
3. **Forwarding Decision:** Once a match is found, the router determines the next hop and the interface to forward the packet.
4. **Packet Forwarding:** The packet is sent to the determined interface, towards the next hop or final destination.

Types of Routes in the Routing Table:

(i) **Directly Connected Routes:** These are networks directly connected to one of the router's interfaces.
(ii) **Static Routes:** Manually configured routes by a network administrator.
(iii) **Dynamic Routes:** Routes learned and updated automatically via routing protocols.

5.3 TYPES OF ROUTING

- **Static** and **dynamic** routing are two fundamental methods used to determine the path that data packets take to reach their destination within a network. Each method has its advantages and disadvantages, and they are often used in different scenarios depending on the network's size, complexity, and requirements.

5.3.1 Static Routing

- Static routing involves manually configuring routes on a router. These routes do not change unless manually updated by a network administrator.

Key Features of Static Routing:

1. **Manual Configuration:** Routes are manually configured by the network administrator. The administrator must define the path that packets should take to reach a particular destination.
2. **Simplicity:** Static routing is straightforward and easy to implement in small networks with simple topologies.

3. **No Overhead:** Static routing does not generate routing protocol traffic, meaning it does not consume bandwidth or router processing power for exchanging routing information.
4. **Predictability:** Since routes are manually configured and do not change, network behaviour is predictable and stable.
5. **Security:** Static routes are more secure because they do not expose the network to routing updates from other networks, which could potentially be malicious.

Disadvantages of Static Routing:

1. **Lack of Scalability:** Static routing is impractical for large or complex networks, as it requires manual updates for every route, which can be time-consuming and prone to human error.
2. **No Automatic Failover:** If a link goes down, a static route does not automatically find an alternative path. The administrator must manually configure a new route, leading to potential downtime.
3. **Maintenance:** As the network grows or changes, maintaining static routes becomes increasingly difficult and error-prone.

Configuration:

Router>**enable**

Router# **configure terminal**

Router(config)#**ip route [destination_network] [subnet_mask] [next_hop_ip | exit_interface]**

For example,

To add a static route to network **192.168.2.0** via the next hop **10.0.0.0**

Router(config)# **ip route 192.168.2.0 255.255.255.0 10.0.0.0**

Router(config)# exit

5.3.2 Dynamic Routing

- Dynamic routing involves the use of routing protocols to automatically discover and maintain routes in the network. Routers using dynamic routing exchange routing information with each other, allowing them to automatically adjust to changes in the network topology.

Key Features of Dynamic Routing:

1. **Automatic Route Discovery:** Routers using dynamic routing protocols automatically discover routes to all destinations in the network. They dynamically adjust routes in response to changes such as link failures or topology changes.
2. **Scalability:** Dynamic routing is well-suited for large and complex networks, as it can automatically scale to accommodate network growth and changes.
3. **Automatic Failover:** If a route becomes unavailable, dynamic routing protocols automatically find an alternative path, minimizing downtime and ensuring network resilience.

4. **Load Balancing:** Some dynamic routing protocols support load balancing, where traffic is distributed across multiple routes with equal or unequal costs.
5. **Routing Protocols:** Common dynamic routing protocols include OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol), RIP (Routing Information Protocol), and BGP (Border Gateway Protocol).

Disadvantages of Dynamic Routing:

1. **Complexity:** Dynamic routing is more complex to configure and manage than static routing, requiring a deeper understanding of routing protocols and their configuration.
2. **Resource Consumption:** Dynamic routing protocols consume bandwidth and processing power as routers exchange routing information and calculate optimal paths.
3. **Potential Instability:** In certain situations, dynamic routing protocols can lead to routing loops or route flapping (frequent changes in route availability), which can cause network instability if not properly managed.
4. **Security Concerns:** Dynamic routing protocols are susceptible to attacks, such as route injection or spoofing, if not properly secured. For example, attackers could inject incorrect routing information to disrupt network traffic.

Configuration for RIP dynamic routing:

Router>**enable**
Router# **configure terminal**
Router(config)#**router rip**
Router(config-router)# **network 192.168.1.0**
Router(config-router)# **network10.0.0.0**
Router(config-router)#**exit**
Router(config)#

5.3.3 Comparison of Static and Dynamic Routing

Table 5.1

Feature	Static Routing	Dynamic Routing
Configuration	Manual	Automatic (using routing protocols)
Scalability	Low (best for small networks)	High (suitable for large, complex networks)
Flexibility	Low (requires manual updates)	High (adapts automatically to changes)
Failover Support	None (manual intervention required)	Automatic (finds alternative paths)

Contd ...

Complexity	Simple to configure but hard to maintain as the network grows	More complex to configure but easier to manage in large networks
Overhead	None (no routing protocol traffic)	High (routing protocols generate traffic)
Predictability	High (routes are fixed and predictable)	Variable (routes can change dynamically)
Security	High (no external route updates)	Lower (requires secure protocol configuration)

When to Use Static vs. Dynamic Routing:

Static Routing is ideal for:

(i) Small networks with a simple topology.
(ii) Environments where the network topology is stable and does not change frequently.
(iii) Situations where you need to control specific routes manually for security or policy reasons.

Dynamic Routing is ideal for:

(i) Large or complex networks where manual configuration would be impractical.
(ii) Environments were network topology changes frequently.
(iii) Networks that require automatic failover and load balancing.

- In many real-world networks, static and dynamic routing are used together. For example, static routing might be used for default routes or specific critical paths, while dynamic routing manages the broader network.

5.4 INTRA AND INTER DOMAIN ROUTING

- In networking, intra-domain and inter-domain routing are two essential concepts that define how data packets are routed within and between different networks.

5.4.1 Intra-Domain Routing

- **Definition:** Intra-domain routing refers to the process of routing data within a single Autonomous System (AS), which is a network or a group of networks under a common administration and with a common routing policy.
- **Protocols:** Common intra-domain routing protocols include:
  (a) **OSPF (Open Shortest Path First):** A link-state routing protocol that uses Dijkstra's algorithm to find the shortest path.
  (b) **RIP (Routing Information Protocol):** A distance-vector routing protocol that uses hop count as a routing metric.
  (c) **EIGRP (Enhanced Interior Gateway Routing Protocol):** A Cisco proprietary hybrid protocol that uses both distance-vector and link-state features.

- **Characteristics:**
  1. Routing within a single AS.
  2. **Optimization:** The focus is on optimizing routes within the AS, such as minimizing latency or maximizing bandwidth.
  3. **Hierarchical Structure:** Intra-domain routing protocols often divide the network into areas to reduce complexity and improve efficiency (e.g., OSPF areas).

5.4.2 Inter-Domain Routing

- **Definition:** Inter-domain routing is the process of routing data between different autonomous systems. This is essential for ensuring that data can travel across different networks, each with its own routing policies.
- **Protocols:** The primary protocol used for inter-domain routing is:
  (a) **BGP (Border Gateway Protocol):** A path-vector protocol that makes routing decisions based on paths, network policies, and rule-sets configured by the network administrator. BGP is responsible for maintaining the routing table between different autonomous systems.
- **Characteristics:**
  1. Routing between multiple ASes.
  2. **Policy-Based Routing:** BGP allows for complex routing policies, including route filtering and path selection based on various criteria, such as AS path length, route origin, or community values.
  3. **Scalability:** BGP is highly scalable and can handle a vast number of routes, making it suitable for the global Internet.

Key Differences between Intra and Inter Domain Routing:

(a) **Scope:** Intra-domain routing is limited to a single AS, while inter-domain routing involves multiple ASes.

(b) **Protocols:** Different protocols are used, with OSPF, RIP, and EIGRP being common for intra-domain, and BGP for inter-domain.

(c) **Routing Objectives:** Intra-domain routing focuses on efficiency within the AS, while inter-domain routing is more concerned with maintaining global reachability and enforcing routing policies across different ASes.

- These concepts are fundamental to understanding how the internet functions as a whole, with intra-domain routing managing traffic within networks, and inter-domain routing ensuring that networks can communicate with each other globally.

55 DISTANCE VECTOR ROUTING (DVR)

- DVR is a dynamic routing algorithm used in computer networks to determine the best path for data packets to travel from one node (router) to another. This method relies on each router sharing information with its immediate neighbours to build a routing table that directs packets across the network.

Key Concepts:

1. **Distance Vector:** Each router maintains a distance vector (a table) that contains the best-known distance (in terms of hop count, cost, or other metrics) to reach every possible destination and the direction (next hop) to reach that destination.
2. **Routing Table:** Each router has a routing table that stores:
   (i) The destination network.
   (ii) The distance to that network.
   (iii) The next hop to reach the destination.
3. **Initial Setup:** Initially, each router knows only the distance to itself (which is zero) and assumes the distance to all other routers is infinite.
4. **Exchange of Information:**
   (i) Routers periodically exchange their distance vectors with their immediate neighbors.
   (ii) When a router receives a distance vector from a neighbor, it compares the newly received information with its current routing table to see if there's a shorter path to any destination.
   (iii) If a shorter path is found, the router updates its routing table and informs its neighbors.
5. **Bellman-Ford Algorithm:**
   - Distance Vector Routing is based on the Bellman-Ford algorithm, which helps in updating the routing tables.
   - The algorithm operates in a distributed manner, and each router independently calculates its own routing table.
6. **Convergence:**
   - The process continues until the network converges, meaning all routers have consistent routing information.
   - Convergence can be slow, especially in large networks, and issues like routing loops can occur during this process.
7. **Count to Infinity Problem:**
   - A common issue with DVR is the "Count to Infinity" problem, were incorrect routing information loops between routers, causing delays in network convergence.
   - Various solutions, such as split horizon, route poisoning, and hold-down timers, are used to mitigate this problem.

Advantages of DVR:

1. **Simplicity:** Easy to implement and understand.
2. **Autonomous:** Each router operates independently.

Disadvantages of DVR:

1. **Slow Convergence:** Takes time for the network to stabilize after a change.
2. **Routing Loops:** Vulnerable to loops during the convergence process.
3. **Scalability:** Not ideal for large networks due to the slow convergence and excessive routing table size.

For Example,

- Imagine a network where each router only knows about its direct neighbors. By exchanging routing tables, each router gradually learns about the entire network and can find the shortest path to any destination. For instance, if router A wants to send data to router D, and the shortest path goes through routers B and C, the routing table at A will eventually reflect this path after several exchanges with its neighbours.

5.6 RIP (ROUTING INFORMATION PROTOCOL)

- RIP is one of the oldest distance-vector routing protocols used in computer networks. It is an Interior Gateway Protocol (IGP) designed to route data within an Autonomous System (AS). Here's an overview of RIP:

Key Features:

1. **Distance Vector Protocol:** RIP uses the distance-vector algorithm to determine the best path to a destination. It considers the number of hops (routers) to reach the destination, with each hop being assigned a cost of 1.
2. **Maximum Hop Count:** The maximum number of hops allowed in a RIP network is 15. If a route has more than 15 hops, it is considered unreachable.
3. **Updates and Timers:**
   (i) **Routing Updates:** RIP routers broadcast their routing tables to neighboring routers every 30 seconds. This helps keep the routing information updated across the network.
   (ii) **Timers:** RIP uses several timers, including the update timer (30 seconds), invalid timer (180 seconds), and hold-down timer (180 seconds) to manage the stability of the network.
4. **Versions:**
   (i) **RIPv1:** The original version, which is classful (doesn't support subnet information).
   (ii) **RIPv2:** An enhanced version that supports classless inter-domain routing (CIDR), multicast updates, and authentication.
5. **Convergence:** RIP has slower convergence compared to other modern protocols. Convergence is the time taken by the routers to update their routing tables and reach a consistent state after a network change.
6. **Split Horizon and Poison Reverse:** To prevent routing loops, RIP employs techniques like split horizon (a router does not advertise a route back to the interface from which it was learned) and poison reverse (advertising a route with an infinite metric to indicate it is unreachable).

Use Cases:

(i) **Small Networks:** Due to its simplicity and limitations like the maximum hop count, RIP is best suited for small to medium-sized networks.

(ii) **Educational Purposes:** RIP is often used in educational environments to teach the basics of routing protocols.

Limitations:

(i) **Scalability:** RIP is not suitable for large networks due to its hop count limitation.

(ii) **Slow Convergence:** Compared to more modern routing protocols like OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol), RIP converges slowly.

(iii) **Broadcasts:** RIPv1 uses broadcast routing updates, which can lead to unnecessary traffic on the network.

- Overall, RIP is a foundational protocol that laid the groundwork for more advanced routing protocols used in today's networks.

Configuration:

Router>**enable**

Router# **configure terminal**

Router(config)#**router rip**

Router(config-router)# **network 192.168.1.0**

Router(config-router)# **network10.0.0.0**

Router(config-router)#**exit**

Router(config)#

5.7 OPEN SHORTEST PATH FIRST (OSPF)

- OSPF is a dynamic routing protocol used in Internet Protocol (IP) networks. It belongs to the group of Interior Gateway Protocols (IGPs), meaning it operates within a single Autonomous System (AS). OSPF is widely used in large enterprise networks due to its scalability, fast convergence, and support for complex topologies.

Key Features of OSPF:

1. **Link-State Routing Protocol:** OSPF is a link-state protocol, meaning it builds a complete map (or topology) of the network by exchanging link-state advertisements (LSAs) with neighboring routers. Each router then uses this map to independently calculate the shortest path to every destination using Dijkstra's algorithm.
2. **Hierarchical Design:** OSPF networks can be structured hierarchically into areas, which helps reduce routing overhead and limits the scope of LSAs. The main area, called Area 0 or the backbone area, interconnects all other areas.
3. **Support for VLSM and CIDR:** OSPF supports Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR), allowing for more efficient IP address allocation.

4. **Fast Convergence:** OSPF quickly adapts to changes in the network topology (like link failures) by recalculating routes almost immediately.
5. **Equal-Cost Multi-Path (ECMP):** OSPF can distribute traffic across multiple paths that have the same cost, improving load balancing.
6. **Authentication:** OSPF includes features for authenticating the routing information exchanged between routers, enhancing security.
7. **Metric Calculation:** OSPF uses a cost metric based on link bandwidth to determine the shortest path. Lower cost routes are preferred.
8. **Neighbour Relationships:** OSPF routers establish neighbor relationships with directly connected routers to exchange routing information.

OSPF Operation:

1. **Router ID (RID):** Each OSPF router is identified by a unique Router ID, usually an IP address assigned to a loopback interface.
2. **Hello Protocol:** OSPF routers send Hello packets to discover and maintain neighbor relationships. These packets are sent periodically to ensure the link is active.
3. **Database Exchange:** After establishing neighbour relationships, routers exchange their link-state databases to ensure all routers have a consistent view of the network.
4. **Route Calculation:** Once the database exchange is complete, routers use Dijkstra's algorithm to calculate the shortest path to each destination.
5. **Flooding:** When a network change occurs, OSPF routers flood LSAs throughout the network to update the topology map.

OSPF Areas:

(i) **Area 0 (Backbone Area):** The central area that connects all other areas. All OSPF areas must connect to Area 0.
(ii) **Regular Areas:** Non-backbone areas that connect to Area 0.
(iii) **Stub Areas:** Areas that do not receive external route advertisements, reducing routing table size.
(iv) **Totally Stubby Areas:** A variant of stub areas where even internal OSPF routes from other areas are not propagated.
(v) **Not-So-Stubby Area (NSSA):** Allows external routes to be injected in a limited fashion.

OSPF vs. Other Protocols:

- Compared to other IGPs like RIP (Routing Information Protocol), OSPF is more complex but offers faster convergence, better scalability, and support for larger networks.
- Overall, OSPF is a powerful and flexible protocol, suitable for large and complex networks where fast convergence and efficient routing are essential.

Configuration:

```
Router>enable
Router# configure terminal
/* Router(config)#router ospf [process-id] */
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network10.0.0.0 0.255.255.255 area 0
Router(config-router)#exit
Router(config)#
```

5.8 EIGRP (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL)

- EIGRP is a dynamic routing protocol used in IP networks, developed by Cisco Systems. It's an advanced version of the Interior Gateway Routing Protocol (IGRP) and is primarily used within an Autonomous System (AS). EIGRP is known for its efficiency, scalability, and faster convergence compared to other routing protocols like RIP.

Key Features of EIGRP:

1. **Hybrid Routing Protocol:** EIGRP is often referred to as a hybrid routing protocol because it incorporates characteristics of both distance-vector and link-state protocols. It uses distance-vector calculations but also maintains a topology table like a link-state protocol.
2. **DUAL Algorithm:** EIGRP uses the Diffusing Update Algorithm (DUAL) to ensure loop-free and efficient routing. DUAL allows EIGRP to quickly converge and find backup routes without causing routing loops.
3. **Classless Protocol:** EIGRP supports Classless Inter-Domain Routing (CIDR), which allows for more efficient IP address utilization through Variable-Length Subnet Masking (VLSM).
4. **Fast Convergence:** EIGRP can quickly adapt to changes in the network, such as link failures, by recalculating routes almost instantly using DUAL.
5. **Equal and Unequal-Cost Load Balancing:** EIGRP supports both equal-cost and unequal-cost load balancing, allowing it to distribute traffic across multiple paths with different metrics.
6. **Scalability:** EIGRP is highly scalable and can handle large and complex networks with thousands of routes, making it suitable for large enterprise environments.
7. **Neighbour Discovery:** EIGRP routers establish neighbor relationships by exchanging Hello packets. Neighbors share routing information, and EIGRP ensures that only the necessary information is sent to minimize network traffic.

8. **Partial Updates:** Unlike some distance-vector protocols that send periodic full updates, EIGRP sends updates only when a change occurs, and only the affected part of the routing table is updated. This reduces bandwidth usage and improves efficiency.
9. **Metric Calculation:** EIGRP uses a composite metric based on several factors, including bandwidth, delay, load, and reliability. The metric calculation can be fine-tuned to meet specific network requirements.
10. **Support for Multiple Protocols:** Although primarily used for IP networks, EIGRP also supports routing for other network layer protocols like IPX and AppleTalk, though these are less common today.

EIGRP Operation:

- **Router ID:** Each EIGRP router is identified by a unique Router ID, which is usually an IP address from a configured interface.
- **Neighbour Table:** EIGRP maintains a table of neighboring routers that it has established adjacency with. This table is used to track the status and availability of neighbors.
- **Topology Table:** EIGRP maintains a topology table that contains all the routes advertised by neighboring routers. The DUAL algorithm uses this table to select the best path and backup paths.
- **Routing Table:** The best routes from the topology table are placed in the routing table and are used to forward traffic.
- **Reliable Transport Protocol (RTP):** EIGRP uses RTP to ensure the reliable delivery of routing updates between routers.
- **Successor and Feasible Successor:** The successor is the best route to a destination, while the feasible successor is a backup route that meets certain feasibility conditions. If the successor fails, the feasible successor is immediately promoted, leading to fast convergence.

EIGRP Metric Components:

(a) **Bandwidth:** The minimum bandwidth along the path to the destination.
(b) **Delay:** The cumulative delay along the path.
(c) **Load:** The load on the links, reflecting how busy they are.
(d) **Reliability:** The reliability of the links, indicating how often they fail.

EIGRP vs. Other Routing Protocols:

- Compared to RIP, EIGRP is faster and more efficient, supporting larger networks.
- Unlike OSPF, EIGRP uses a simpler metric system and can provide unequal-cost load balancing, but it is Cisco-proprietary, meaning it is only natively supported on Cisco devices.
- Overall, EIGRP is a robust and versatile routing protocol suitable for enterprise networks, especially those using Cisco equipment, offering a good balance of performance, efficiency, and scalability.

Configuration:

```
Router>enable
Router# configure terminal
/* Router(config)#router eigrp [Autonomous System-no] */
Router(config)#router eigrp 1
Router(config-router)#network192.168.1.0 0.0.0.255
Router(config-router)#network10.0.0.0 0.255.255.255
Router(config-router)#exit
Router(config)#
```

5.9 BORDER GATEWAY PROTOCOL (BGP)

- BGP is a standardized exterior gateway protocol used to exchange routing information between Autonomous Systems (ASes) on the internet. BGP is essential for the functioning of the global internet, as it determines how data packets are routed across different networks that are under separate administrative control.

Key Features of BGP:

1. **Path Vector Protocol:** BGP is a path vector protocol, which means it maintains the path (sequence of ASes) information that data must traverse to reach a destination. This helps prevent routing loops by rejecting paths that contain the AS number of the originating router.
2. **Inter-Domain Routing:** BGP is used for inter-domain routing, which involves routing between different autonomous systems, unlike protocols like OSPF and EIGRP, which are used within an AS (intra-domain routing).
3. **Scalability:** BGP is highly scalable and can handle the vast number of routes on the internet. It is designed to work efficiently in large and complex networks with multiple layers of hierarchy.
4. **Policy-Based Routing:** BGP allows for extensive routing policies based on various attributes, such as AS path, next-hop IP address, or multiple path metrics. This flexibility enables network administrators to define routing decisions based on business agreements, security policies, or network performance requirements.
5. **Reliable Transport:** BGP uses TCP (port 179) as its transport protocol, ensuring reliable delivery of routing updates. TCP's reliability mechanisms are crucial for maintaining BGP's stability.
6. **Incremental Updates:** Unlike some protocols that periodically exchange entire routing tables, BGP only sends updates when there is a change in the network. This reduces bandwidth usage and minimizes the processing load on routers.
7. **Route Aggregation:** BGP supports route aggregation, allowing multiple IP prefixes to be combined into a single summary route. This reduces the size of the routing table and improves efficiency.

8. **Multi-Protocol Extensions:** BGP is not limited to IPv4; it supports multiple address families through extensions, such as IPv6, multicast, and VPNs (Virtual Private Networks).
9. **Support for Load Balancing:** BGP can support load balancing across multiple links between ASes, allowing for efficient use of available bandwidth and improving redundancy.
10. **BGP Communities:** BGP communities are a mechanism for tagging routes with specific

Configuration:

R0 – AS 100

Router>**enable**

Router# **configure terminal**

/* Router(config)#**router bgp [Autonomous System-no] */**

Router(config)#**router bgp 100**

Router(config-router)#**network 10.0.0.0 mask 255.0.0.0**

Router(config-router)#**network 20.0.0.0 mask 255.0.0.0**

Router(config-router)#**network 192.168.1.0 mask 255.255.255.0**

Router(config-router)#**neighbor 20.0.0.2 remote-as 300**

Router(config-router)#**neighbor 10.0.0.2 remote-as 200**

Router(config-router)#**exit**

Router(config)

Summary:

Table 5.2

Feature	Static Routing	RIP (Routing Information Protocol)	OSPF (Open Shortest Path First)	EIGRP (Enhanced Interior Gateway Routing Protocol)	BGP (Border Gateway Protocol)
Type	Manual/Static	Distance-Vector	Link-State	Hybrid (Distance-Vector and Link-State)	Path-Vector
Metric/Algorithm	N/A	Hop Count	Link-State Database, Dijkstra's Algorithm	DUAL (Diffusing Update Algorithm)	Path Attributes
Scalability	Low	Limited (15 hops)	High	High	Very High
Convergence Speed	Immediate	Slow	Fast	Fast	Slow

Contd. ...

Complexity	Low	Low	Medium	Medium	High
Configuration	Manual, static routes added individually	Simple, automatic updates	Requires configuration of areas and routers	Requires configuration of AS and networks	Complex, policy-based configuration
Updates	Manual	Periodic (every 30 seconds)	Triggered by changes, incremental updates	Incremental updates and automatic summarization	Policy-based updates, manual intervention
Support for VLSM	No	RIP v1: No; RIP v2: Yes	Yes	Yes	Yes
Supports CIDR	No	No	Yes	Yes	Yes
Hierarchical Design	No	No	Yes (Areas)	No	No
Routing Updates	None (manually configured)	Periodic updates broadcasted to all neighbors	Link-State advertisements (LSAs)	Diffusing updates only to affected routers	Path information with attributes, exchanged between ASes
Best Used For	Small, simple networks or specific, stable routes	Small to medium-sized networks	Medium to large enterprise networks	Medium to large networks, particularly Cisco-centric	Internet routing, inter-domain routing

Key Points:

- **Static Routing:** Best for small or simple networks where manual control is preferred and routes don't change often.
- **RIP:** Suitable for small networks with its simple configuration and periodic updates. Limited scalability due to hop count constraint.
- **OSPF:** Ideal for larger networks with its hierarchical design and fast convergence. Requires more complex configuration but scales well.
- **EIGRP:** Provides efficient routing with fast convergence and good scalability, particularly in Cisco environments.
- **BGP:** The protocol of choice for Internet routing and large-scale networks, offering complex routing policies and extensive scalability.

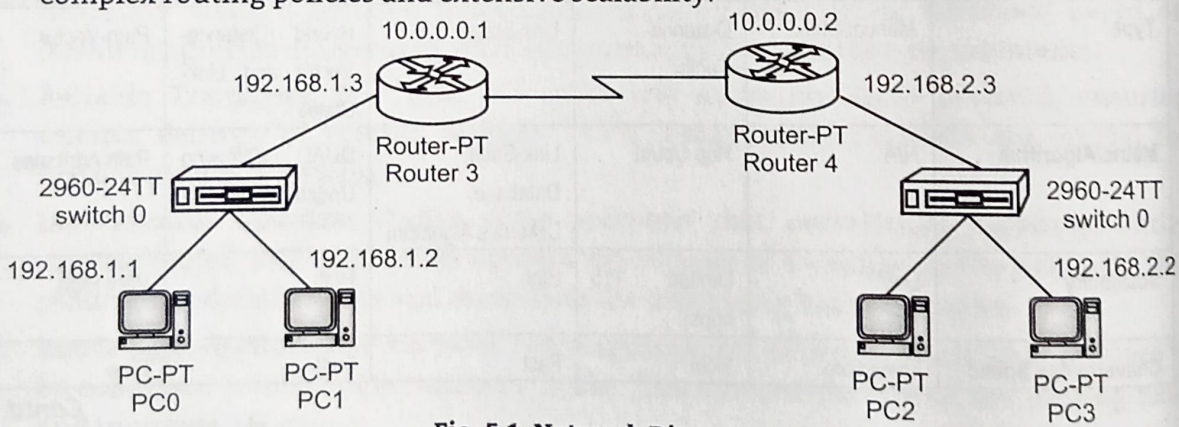


Fig. 5.1: Network Diagram

Configuration:

Table 5.3

Router	Static	RIP	OSPF	EIGRP	BGP
Router 0	Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.0	Router(config)#router rip Router(config-router)# network 192.168.1.0 Router(config-router)# network 10.0.0.0	Router(config)#router ospf 1 Router(config-router)# network 192.168.1.0 0.0.0.255 area 0 Router(config-router)# network 10.0.0.0 0.255.255.255 area 0	Router(config)#router eigrp 1 Router(config-router)# network 192.168.1.0 0.0.0.255 Router(config-router)# network 10.0.0.0 0.255.255.255	Router(config)#router bgp 100 Router(config-router)#network 10.0.0.0 mask 255.0.0.0 Router(config-router)#network 192.168.1.0 mask 255.255.255.0 Router(config-router)#neighbor 10.0.0.2 remote-as 200
Router 1	Router(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.0	Router(config)#router rip Router(config-router)# network 192.168.2.0 Router(config-router)# network 10.0.0.0	Router(config)#router ospf 1 Router(config-router)# network 192.168.2.0 0.0.0.255 area 0 Router(config-router)# network 10.0.0.0 0.255.255.255 area 0	Router(config)#router eigrp 1 Router(config-router)# network 192.168.2.0 0.0.0.255 Router(config-router)# network 10.0.0.0 0.255.255.255	Router(config)#router bgp 100 Router(config-router)#network 10.0.0.0 mask 255.0.0.0 Router(config-router)#network 192.168.2.0 mask 255.255.255.0 Router(config-router)#neighbor 10.0.0.1 remote-as 100
PC0	IP Address: 192.168.1.1 Gateway: 192.168.1.3	IP Address: 192.168.1.1 Gateway: 192.168.1.3	IP Address: 192.168.1.1 Gateway: 192.168.1.3	IP Address: 192.168.1.1 Gateway: 192.168.1.3	IP Address: 192.168.1.1 Gateway: 192.168.1.3
PC1	IP Address: 192.168.1.2 Gateway: 192.168.1.3	IP Address: 192.168.1.2 Gateway: 192.168.1.3	IP Address: 192.168.1.2 Gateway: 192.168.1.3	IP Address: 192.168.1.2 Gateway: 192.168.1.3	IP Address: 192.168.1.2 Gateway: 192.168.1.3

Contd...

PC2	IP Address: 192.168.2.1 Gateway: 192.168.2.3	IP Address: 192.168.2.1 Gateway: 192.168.2.3	IP Address: 192.168.2.1 Gateway: 192.168.2.3	IP Address: 192.168.2.1 Gateway: 192.168.2.3	IP Address: 192.168.2.1 Gateway: 192.168.2.3
PC3	IP Address: 192.168.2.2 Gateway: 192.168.2.3	IP Address: 192.168.2.2 Gateway: 192.168.2.3	IP Address: 192.168.2.2 Gateway: 192.168.2.3	IP Address: 192.168.2.2 Gateway: 192.168.2.3	IP Address: 192.168.2.2 Gateway: 192.168.2.3

Summary

- A router is a networking device that directs data packets among different networks, ensuring they reach their correct destinations.
- The routing table is essential for routers to make efficient forwarding decisions. It contains all the information needed to direct packets to their destination across interconnected networks. Proper configuration and maintenance of routing tables are crucial for the smooth operation of any network.
- Static and dynamic routing are two fundamental methods used to determine the path that data packets take to reach their destination within a network.
- Intra-domain and inter-domain routing are two essential concepts that define how data packets are routed within and between different networks.
- Distance Vector Routing is a foundational routing protocol that helps routers determine optimal paths based on distance metrics, although it has limitations in large and rapidly changing networks.
- RIP (Routing Information Protocol) is one of the oldest distance-vector routing protocols used in computer networks.
- OSPF (Open Shortest Path First) is a dynamic routing protocol used in Internet Protocol (IP) networks.
- EIGRP (Enhanced Interior Gateway Routing Protocol) is a dynamic routing protocol used in IP networks, developed by Cisco Systems.
- BGP (Border Gateway Protocol) is a standardized exterior gateway protocol used to exchange routing information between Autonomous Systems (ASes) on the internet.

Check Your Understanding

1. Which component of a router stores routing information?
   (a) CPU
   (b) Flash
   (c) Routing Table
   (d) NVRAM

2. Which type of routing requires manual configuration of paths?
   (a) Dynamic Routing (b) Static Routing
   (c) Default Routing (d) Border Routing
3. Which of the following is a Distance Vector routing protocol?
   (a) OSPF (b) EIGRP
   (c) RIP (d) BGP
4. Which protocol uses link-state routing?
   (a) RIP (b) OSPF
   (c) BGP (d) RIPv2
5. Which protocol is used for inter-domain routing?
   (a) RIP (b) OSPF
   (c) EIGRP (d) BGP
6. What is the administrative distance of a directly connected route?
   (a) 1 (b) 0
   (c) 110 (d) 120
7. What metric does RIP use to determine the best path?
   (a) Bandwidth (b) Hop Count
   (c) Delay (d) Cost
8. Which of the following protocols supports VLSM (Variable Length Subnet Masking)?
   (a) RIP v1 (b) RIP v2
   (c) Static Routing only (d) None
9. Which of the following routing protocols is proprietary to Cisco?
   (a) OSPF (b) RIP
   (c) EIGRP (d) BGP
10. What type of routing is OSPF categorized under?
    (a) Distance Vector (b) Static
    (c) Link-State (d) Path Vector

Answers

1. (c)	2. (b)	3. (c)	4. (b)	5. (b)	6. (b)	7. (b)	8. (b)	9. (c)	10. (c)

Practice Questions

Q.I Answer the following questions in short:

1. What is the main function of a router?
2. Define a routing table.
3. What is static routing?