6 CHAPTER

INTRODUCTION TO COMPUTER NETWORKS

Topic No.	Title	Page No.
6.1	Network as a System	127
6.2	Fundamental Concepts in Data Communication	127
6.3	Networking Devices	131
6.4	Network Topologies	135
6.5	Transmission Modes	140
6.6	The OSI Networking Model	142
6.7	IPV4 and IPV6	146
6.8	Protocols and Network Services	146
6.9	Network Security	148
6.10	Types of Networks	151
6.11	Real World Applications of Computer Networks	156
6.12	Standard Protocols in TCP/IP Communications	156
6.13	Network Security Methods	156
*	Summery	158
*	Exercise	159
*	Answer Keys	163

6.1 NETWORK AS SYSTEM AND
6.2 FUNDAMENTAL CONCEPTS IN DATA COMMUNICATION

LONG QUESTION

Q.1 Explain the concept of a computer network as a system, focusing on its primary components, objectives, and real-world applications. Provide examples to illustrate the functionality of each component and objective.

Ans. 1. Understanding Computer Networks as a System

A computer network is a system of interconnected devices and computers that can exchange data and operate together. It enables communication, resource sharing, and collaborative work among devices. Networks vary in size and complexity, ranging from small-scale Local Area Networks (LANs) to large-scale Wide Area Networks (WANs) like the Internet.

2. Primary Components of a Computer Network

The main components of a computer network include:

a) Nodes

These are devices connected to the network, such as computers, smartphones, and printers. **Example:** In an office, a computer (node) can send print jobs to a printer (another node) over the network.

b) Links

Links are the connections between nodes, which can be wired (Ethernet cables) or wireless (Wi-Fi).

Example: Ethernet cables in an office connect desktop computers to the network, while Wi-Fi links mobile devices.

c) Switches

Switches connect multiple nodes within a network and manage data transfer by forwarding data packets to the intended destination.

Example: A switch in an office ensures that files sent from one computer reach another without broadcasting to all devices.

d) Routers

Routers connect different networks and direct data packets between them, often using a routing table to find the most efficient path.

Example: In a home network, a router connects your local devices to the Internet, ensuring efficient data flow.

3. Objectives of Computer Networks

The primary objectives of a computer network include:

a) Resource Sharing

Networks allow devices to share resources like printers, storage, and software, reducing costs and improving efficiency.

Example: Multiple computers in an office can use a single networked printer instead of each having a dedicated printer.

b) Data Communication

Networks facilitate the transfer of data, enabling communication through emails, instant messaging, and video conferencing.

Example: Employees in different cities collaborate via video conferencing tools like Microsoft Teams.

c) Connectivity and Collaboration

Networks enable remote access and real-time collaboration, enhancing productivity.

Example: A team can co-edit a shared document in Google Drive regardless of their locations.

4. Real-World Applications

Computer networks have transformative applications across various sectors:

a) Business

Companies use networks for efficient communication, data management, and resource sharing. **Example:** Intranets allow employees to securely access company resources.

b) Education

Networks provide platforms for online learning and collaboration. **Example:** Universities use Learning Management Systems (LMS) like Moodle for virtual classrooms.

c) Healthcare

Healthcare networks enable the sharing of patient records and remote consultations. **Example:** Hospitals use Electronic Health Records (EHR) systems for efficient patient care management.

Q.2 Explain the components of data communication and their functions in a network.

Ans: Introduction

Data communication involves the transfer of data between devices over a network. It relies on five key components that work together to ensure effective communication: the sender, receiver, message, protocol, and medium.

1. Sender

Function:

The sender is the device that sends the data. It could be a computer sending an email or a smartphone sending a message. The sender initiates the communication process by transmitting the data to the receiver.

2. Receiver

Function:

The receiver is the device that receives the data sent by the sender. Examples of receivers include smartphones or computers. The receiver processes the data after receiving it and may present it to the user or use it for further operations.

3. Message

Function:

The message is the data being communicated. This could be a text message, an email, or a file being transferred. The message carries the actual information that needs to be communicated between the sender and receiver.

4. Protocol

Function:

The protocol is a set of rules that govern the communication process. It ensures that the data is sent and received correctly and in a format that both the sender and receiver understand. For instance, the HTTP protocol is used for communication over the web.

5. Medium

Function:

The medium is the physical or wireless path through which data travels. It could be a wired medium like Ethernet cables or a wireless medium like Wi-Fi. The medium is crucial as it determines the speed, reliability, and quality of the communication.

SHORT QUESTIONS

Q.16 What is the purpose of a computer network?

Ans:

PURPOSE OF A COMPUTER NETWORK

The purpose of a computer network is to allow devices and computers to connect and share resources, such as printers and storage, improving communication and collaboration. Networks facilitate data transfer and access to resources, enabling both personal and business efficiency.

Q.17 What are the key components of a computer network?

Ans:

COMPONENTS OF A COMPUTER NETWORK

The key components of a computer network include nodes (devices like computers and printers), links (wired or wireless connections), switches (devices connecting multiple nodes), and routers (devices that connect different networks and direct data packets between them).

Q.18 Explain how a switch works in a network.

Ans:

SWITCH WORKS IN A NETWORK

A switch works by forwarding data packets to the correct destination based on the MAC address. When a file is transferred, the switch examines the MAC address of the destination and forwards the packet to the correct port where the destination device is connected.

Q.19 What is the role of a router in a network?

Ans:

ROLE OF A ROUTER IN A NETWORK

A router connects different networks and directs data packets between them. It ensures that data is sent along the correct paths, which is critical for communication across different networks such as local and wide area networks.

Q.20 How does resource sharing benefit a network?

Ans:

RESOURCE SHARING BENEFIT A NETWORK

Resource sharing allows devices to share resources like printers and storage, which reduces costs and improves efficiency. For example, multiple computers in an office can share a single printer, eliminating the need for multiple devices and simplifying management.

Q.21 What is meant by data communication?

Ans:

MEANT BY DATA COMMUNICATION

Data communication refers to the exchange of data between a sender and a receiver through a communication medium. This process involves transmitting messages according to established protocols, which enables data transfer across networks.

Q.22 What is the significance of the World Wide Web (WWW)?

Ans:

SIGNIFICANCE OF THE WORLD WIDE WEB (WWW)

The World Wide Web (WWW), invented by Tim Berners-Lee in 1989, revolutionized the way we access and share information online. It allows for the interlinking of websites through hyperlinks and web browsers, creating a vast interconnected space for communication, education, and commerce.

Q.23 Explain the concept of packet switching.

Ans:

CONCEPT OF PACKET SWITCHING

Packet switching involves breaking data into smaller packets, each of which has a destination address. The packets travel independently across the network, possibly taking different paths. Once they reach the destination, the packets are reassembled into the original data message.

Q.24 What is a protocol in data communication?

Ans:

PROTOCOL IN DATA COMMUNICATION

A protocol is a set of rules that govern how data is exchanged between devices in a network. Protocols ensure that the sender and receiver can understand the format, sequence, and processing of the transmitted data, such as the HTTP protocol used in web communication.

Q.25 What is the importance of a communication medium in data communication?

Ans:

COMMUNICATION MEDIUM IN DATA COMMUNICATION

The communication medium is the path through which data travels between devices. It can be a physical medium like Ethernet cables or a wireless medium like Wi-Fi. The medium impacts the speed, reliability, and quality of data transmission, making it essential for effective communication.

MULTIPLE CHOICE QUESTIONS

14. What is a computer network?
(A) A single device
(B) A group of linked devices
(C) A storage device
(D) A software program

15. Which of the following is the largest network?
(A) Local Area Network (LAN)
(B) Wide Area Network (WAN)
(C) The Internet
(D) Bluetooth network

16. Which component connects multiple devices within a network?
(A) Router
(B) Switch
(C) Modem
(D) Server

17. What is the primary function of a router?
(A) Connect devices within a network
(B) Direct data packets between networks
(C) Store data
(D) Encrypt data

18. What are the devices that are connected to the network called?
(A) Routers
(B) Switches
(C) Nodes
(D) Links

19. Which of these is an example of a network link?
(A) Router
(B) Ethernet cable
(C) Server
(D) Printer

20. What does a switch use to forward data packets to the correct destination?
(A) IP address
(B) MAC address
(C) DNS address
(D) Email address

21. Which of the following is a primary objective of computer networks?
(A) Security
(B) Data communication
(C) Database management
(D) Hardware development

22. What is an example of resource sharing in a computer network?
(A) Sending emails
(B) Video conferencing
(C) Sharing a printer
(D) File encryption

23. What facilitates real-time collaboration in a network?
(A) Email
(B) Cloud-based services
(C) Antivirus software
(D) USB drives

24. Who invented the World Wide Web (WWW)?
(A) Steve Jobs
(B) Tim Berners-Lee
(C) Bill Gates
(D) Mark Zuckerberg

25. Which of these is an example of data communication?
(A) Storing files
(B) Sending an email
(C) Creating a document
(D) Designing a webpage

26. What is a protocol in data communication?
(A) A device that sends data
(B) A physical path for data transmission
(C) A set of rules for communication
(D) The data being transferred

27. What is an example of a communication medium?
(A) Wi-Fi
(B) Laptop
(C) Switch
(D) Server

28. What is a common example of a message in data communication?
(A) A document file
(B) A Wi-Fi signal
(C) A router's settings
(D) A web page address

6.3 NETWORKING DEVICES

LONG QUESTION

Q.1 Explain the functions and importance of networking devices, including switches, routers, and access points, in managing network traffic.

Ans: Introduction

Networking devices such as switches, routers, and access points are essential for the efficient management and flow of data in a network. These devices ensure that data is transmitted accurately and efficiently between devices and across different networks. Each device plays a unique role in the overall network architecture.

1. Switches

Function:

A switch is a networking device that connects multiple devices within a single network. It uses the Media Access Control (MAC) address of devices to direct data to the correct destination. Initially, when a switch does not know the destination device's address, it broadcasts data to all connected devices. Over time, as the switch learns the addresses of devices, it begins sending data only to the correct device, which improves network efficiency.

Importance:

Switches are vital because they manage data traffic within a local network, ensuring that information is delivered quickly and without congestion. By reducing unnecessary data traffic, switches help in maintaining the performance and reliability of the network.

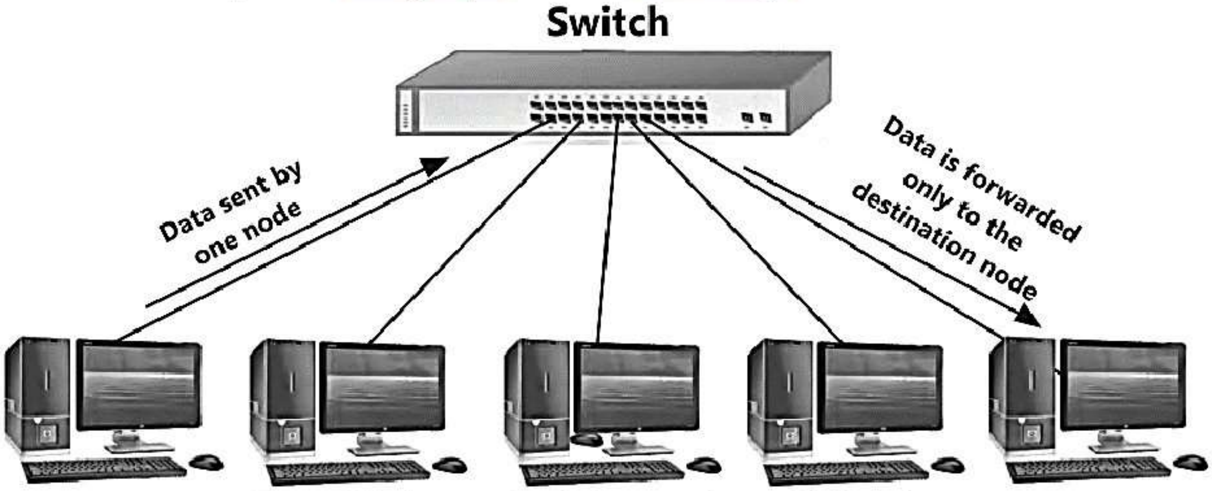


Figure 6.3: A network switch connecting multiple devices.

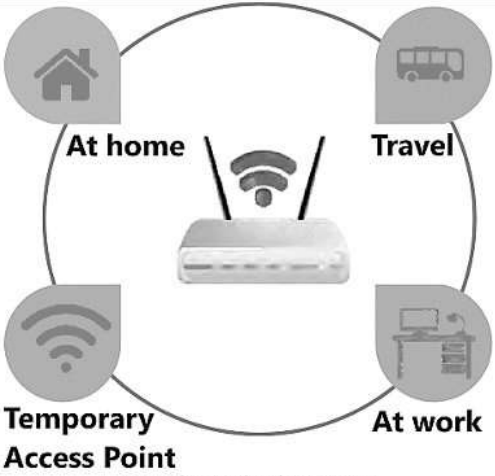
2. Routers

Function:

Routers are used to interconnect different networks, such as a home network and the internet. They are responsible for directing data packets between networks, ensuring that data reaches its correct destination. Routers use a routing table to determine the most efficient path for each data packet, which helps avoid delays and ensures the efficient delivery of data.

Importance:

Routers are crucial for network communication beyond local areas. They allow different networks to communicate with each other, enabling internet access and communication between geographically dispersed networks. They also ensure data is directed along the most efficient paths.



Mobile Wi-Fi Router
Figure 6.2: A typical home router

3. **Access Points**

Function:

An Access Point (AP) acts as a bridge between wireless devices and a wired network. It receives data from the wired network and transmits it wirelessly to devices such as smartphones and laptops. Conversely, it also receives data from wireless devices and sends it to the wired network.

Importance:

Access Points are important in modern networks because they allow wireless devices to connect to a network without physical cables. They are especially useful in environments where a large number of devices need internet access or where mobility is required, making them ideal for schools, offices, and large venues.

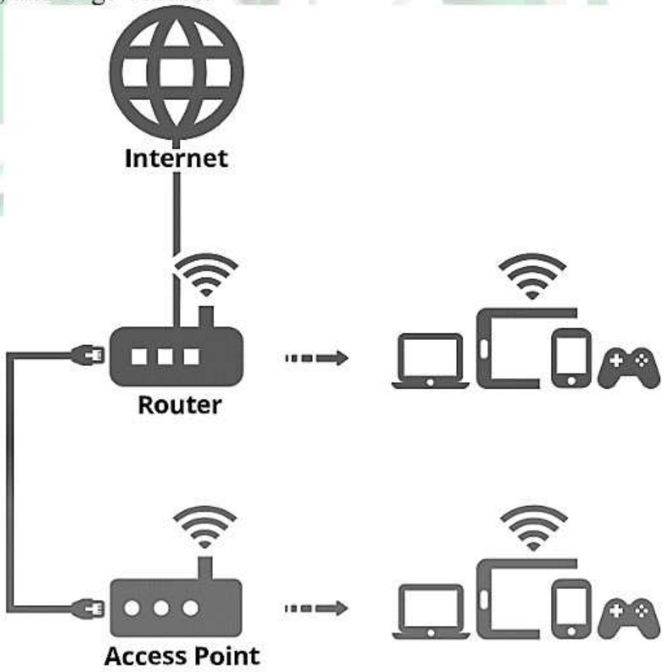


Figure 6.4: A typical Access Point

SHORT QUESTIONS

Q.1 What is the function of a switch in a network?

Ans: **FUNCTION OF A SWITCH IN A NETWORK**

A switch connects multiple network devices like computers, printers, and servers. It allows these devices to communicate efficiently by forwarding data to the correct device using the device's MAC address.

Q.2 How does a router work to manage network traffic?

Ans: **ROUTER WORK TO MANAGE NETWORK TRAFFIC**

A router directs data packets between different networks. It uses a routing table to determine the best path for each data packet, ensuring that data reaches its destination efficiently.

Q.3 What is the difference between a switch and a router?

Ans: **DIFFERENCE BETWEEN A SWITCH AND A ROUTER**

A switch connects devices within the same network and directs data to the correct device using MAC addresses. A router connects different networks and directs data packets between them, ensuring efficient data transfer across networks.

Q.4 How does a switch forward data to the correct device?

Ans: **SWITCH FORWARD DATA TO THE CORRECT DEVICE**

A switch uses the MAC addresses of devices to forward data packets. When a packet reaches the switch, it reads the destination MAC address and sends the packet only to the device with that address.

Q. 5 Why is a router important for connecting networks?

Ans: **ROUTER IMPORTANT FOR CONNECTING NETWORKS**

A router is essential because it connects different networks, such as a home network to the internet. It directs data packets between these networks, ensuring that data can flow between them and reach its intended destination.

Q.5 What is the role of an Access Point (AP) in a network?

Ans: **AN ACCESS POINT (AP) IN A NETWORK?**

An Access Point (AP) allows wireless devices, like smartphones and laptops, to connect to a wired network. It receives data from the wired network and transmits it wirelessly to the devices, and also transmits data from wireless devices to the network.

Q.6 How does an Access Point transmit data?

Ans: **ACCESS POINT TRANSMIT DATA**

An Access Point transmits data by using radio waves, similar to how radio stations broadcast signals. It allows wireless communication between devices and the network.

Q.7 What is a routing table, and why is it important?

Ans: **ROUTING TABLE, AND WHY IS IT IMPORTANT**

A routing table is used by a router to store information about possible paths for data packets. It helps the router make efficient decisions on the best route for each packet, ensuring data is delivered effectively.

Q.8 Why should a switch be placed in a cool, ventilated area?

Ans: **SWITCH BE PLACED IN A COOL, VENTILATED AREA**

A switch should be placed in a cool, ventilated area to prevent overheating. Overheating can reduce the performance and lifespan of the switch, so proper ventilation is important for maintaining its efficiency.

Q.9 What are the benefits of using an Access Point in large environments like offices or stadiums?

Ans: Access Points can connect hundreds of devices simultaneously, making them ideal for large environments such as offices, schools, and stadiums. They provide wireless access, allowing multiple devices to connect to the network without physical cables.

MULTIPLE CHOICE QUESTIONS

1. **What is the primary function of a switch in a network?**
(A) To store data
(B) To direct data to the correct device
(C) To connect devices to the internet
(D) To monitor network traffic

2. **At which layer of the OSI model does a switch operate?**
(A) Layer 1
(B) Layer 2
(C) Layer 3
(D) Layer 4

3. **What address does a switch use to forward data packets?**
(A) IP address
(B) MAC address
(C) DNS address
(D) URL address

4. **How does a router direct data packets?**
(A) By checking the source IP address
(B) By finding the best path for each packet
(C) By using MAC addresses
(D) By broadcasting data to all devices

5. **Which device interconnects multiple networks?**
(A) Switch
(B) Router
(C) Access Point
(D) Hub

6. **What does a router use to decide the best path for data packets?**
(A) MAC address
(B) IP address
(C) Routing table
(D) DNS table

7. **What does an Access Point (AP) facilitate?**
(A) Wired network connections
(B) Wireless device connections to a wired network
(C) Wired internet connections only
(D) Data storage in the cloud

8. **How does an Access Point transmit data?**
(A) By using fiber optics
(B) By using radio waves
(C) By using Ethernet cables
(D) By using Bluetooth

9. **Which of the following devices often combines a switch and a wireless access point?**
(A) Router
(B) Hub
(C) Server
(D) Laptop

10. **Where should an Access Point be placed for optimal performance?**
(A) Near a computer
(B) In a central location
(C) Close to a switch
(D) Near the router only

11. **What does a switch do when it first receives data?**
(A) It forwards data to all connected devices
(B) It checks the IP address
(C) It stores data for later use
(D) It immediately sends data to the destination

12. **What is the role of a router in a network?**
(A) To store data
(B) To connect devices within a network
(C) To connect different networks and direct data packets
(D) To forward data within a single network

13. **Which of these devices transmits data wirelessly?**
(A) Switch
(B) Router
(C) Access Point
(D) Hub

14. **What technology does an Access Point use to communicate with devices?**
(A) Ethernet cables
(B) Bluetooth
(C) Radio waves
(D) Fiber optics

15. **Which of the following is an example of a device that allows wireless devices to connect to the internet?**
(A) Switch
(B) Router
(C) Access Point
(D) Server

6.4 NETWORK TOPOLOGIES

LONG QUESTION

Q.1 Describe the different types of network topologies (bus, star, ring, and mesh) and explain their advantages and disadvantages.

Ans:

1. **Bus Topology**

- **Description:**

  Bus topology is a simple and cost-effective method where all devices are connected to a single communication line called the bus. Data sent by any device is broadcasted to all devices, but only the intended recipient processes it.

- **Advantages:**

  Easy and inexpensive to set up

  Requires less cabling compared to other topologies

- **Disadvantages:**

  If the central cable fails, the entire network goes down

  Not suitable for large networks due to performance degradation

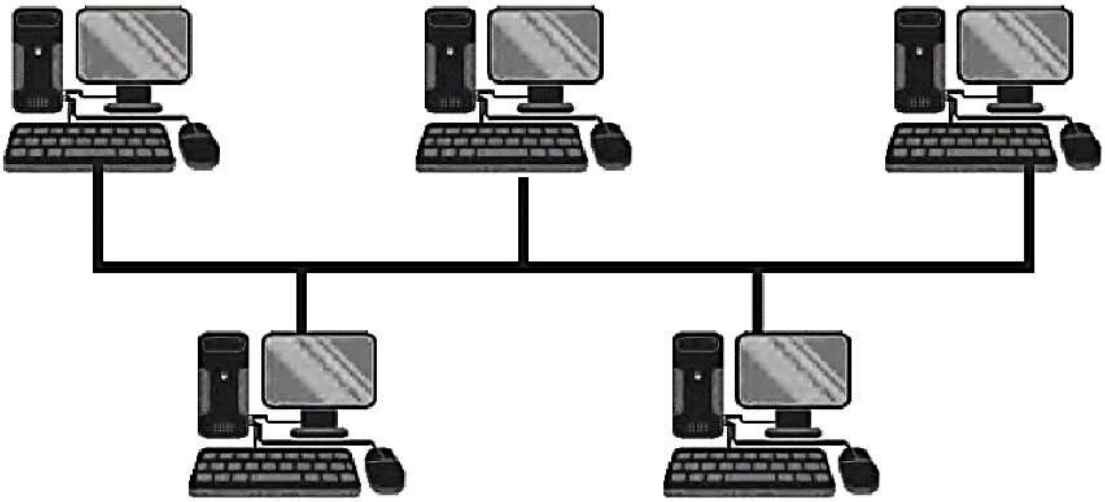


Figure 6.5: Bus Topology

2. **Star Topology**

- **Description:**

  In star topology, each device is connected to a central hub or switch. Devices communicate by sending data through the hub, which repeats it to the intended recipient.

- **Advantages:**

  If one device fails, it doesn't affect the entire network

  Easy to expand by adding more devices

- **Disadvantages:**

  If the central hub fails, the entire network fails

  Requires more hardware compared to bus topology.

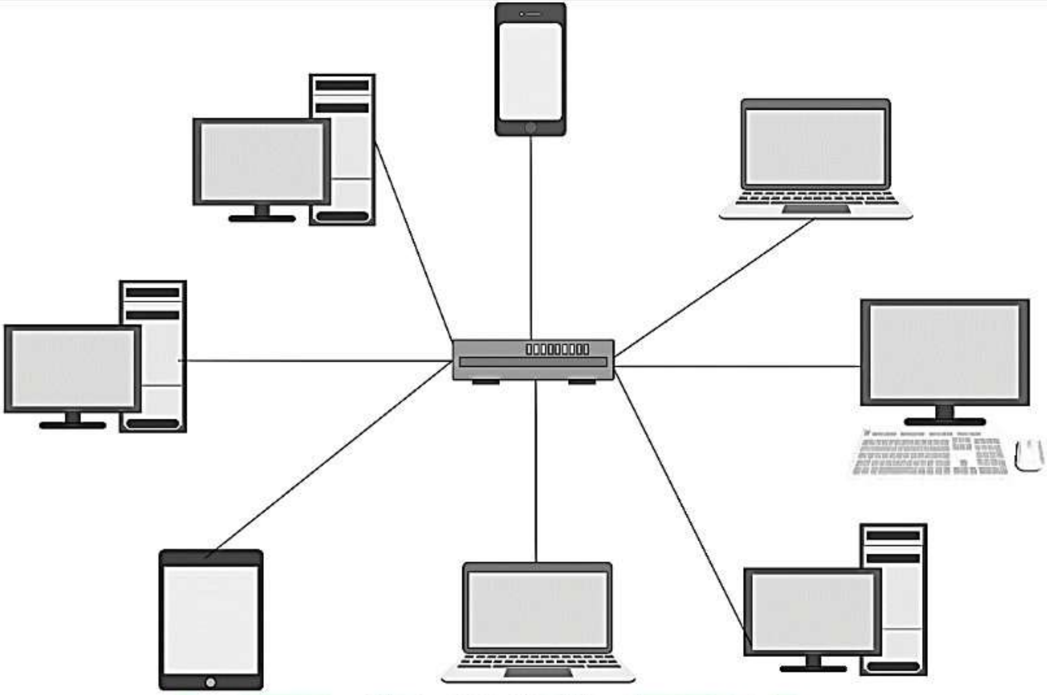


Figure 6.6: Star Topology

3. **Ring Topology**

- **Description:**
  Ring topology connects devices in a circular fashion. Data travels in one direction from one device to the next until it reaches its destination.
- **Advantages:**
  Can handle high traffic
  The arrangement allows efficient data transmission
- **Disadvantages:**
  A failure in any device or connection can affect the entire network
  However, a two-way ring can mitigate this issue

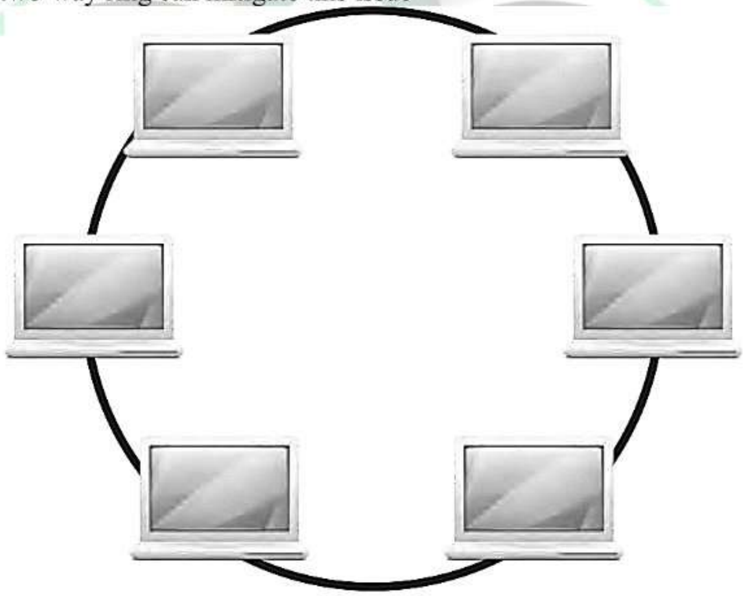


Figure 6.7 Ring Topology

4. **Mesh Topology**

- **Description:**
  Mesh topology connects every device to every other device, ensuring high redundancy. If one link fails, data can be rerouted through other links.
- **Advantages:**
  Highly reliable due to multiple redundant connections
  Ensures network operation even if a link fails
- **Disadvantages:**
  Expensive and complex to implement
  Requires more cabling and hardware compared to other topologies

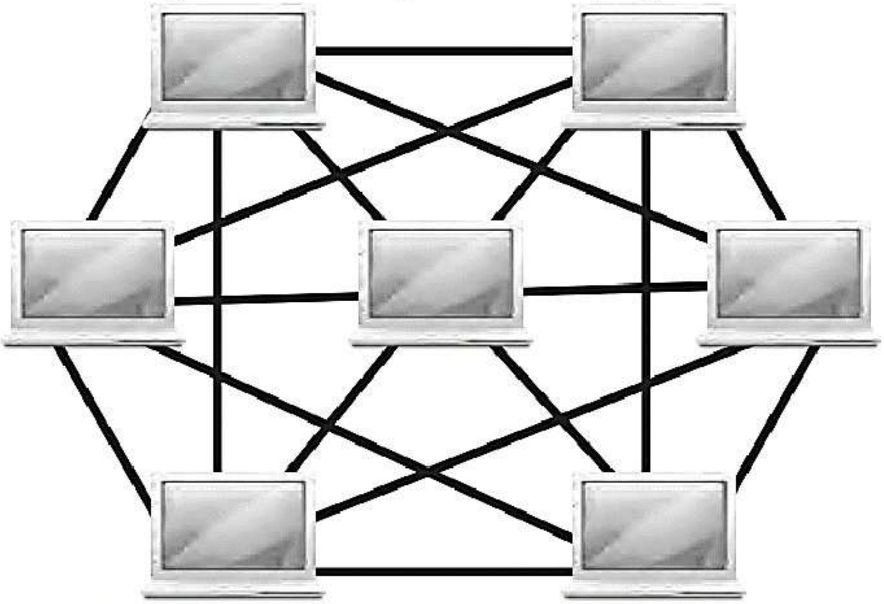


Figure 6.8: Mesh Topology

SHORT QUESTIONS

Q.1 What is bus topology and how does it function?

Ans: **TOPOLOGY AND HOW DOES IT FUNCTION**

In bus topology, all devices are connected to a single communication line called the bus. Data sent by any device is broadcasted to all devices on the network, but only the intended recipient processes it. However, if the main cable fails, the whole network goes down, making it less reliable for large-scale networks.

Q.2 Describe the advantages and disadvantages of star topology.

Ans: **ADVANTAGES AND DISADVANTAGES OF STAR TOPOLOGY**

Star topology uses a central hub or switch to connect devices. The main advantage is that if one device fails, it doesn't affect the entire network. However, the failure of the central hub causes the entire network to fail. It is reliable and easy to set up but requires more hardware.

Q.3 How does data transmission work in a ring topology?

Ans: **DATA TRANSMISSION WORK IN A RING TOPOLOGY**

In a ring topology, each device is connected in a circle, and data travels in one direction from one device to the next until it reaches its destination. This arrangement can handle high traffic, but if one device or connection fails, the whole network is affected, though a two-way ring can help solve this issue.

Q.4 What are the benefits of using mesh topology?

Ans:

BENEFITS OF USING MESH TOPOLOGY

Mesh topology connects every device to every other device, providing high redundancy. If one link fails, data can be rerouted through another link, ensuring the network remains operational. This makes mesh topology very reliable but can be expensive and complex to set up.

Q.5 How does a hub work in star topology?

Ans:

HUB WORK IN STAR TOPOLOGY

In star topology, the hub connects all devices within the network. It serves as a repeater, forwarding data to all connected devices. However, unlike a switch, it broadcasts data to every device, not just the intended recipient, which can lead to inefficiency in larger networks.

Q.6 What is the role of a central hub in star topology?

Ans:

ROLE OF A CENTRAL HUB IN STAR TOPOLOGY

The central hub in a star topology acts as the main point for communication. Each device communicates with the hub, which then relays the data to the appropriate device. The hub does not affect the other devices directly unless it fails, making it a critical component for the network's functionality.

Q.7 What makes mesh topology highly reliable?

Ans:

MESH TOPOLOGY HIGHLY RELIABLE

Mesh topology is highly reliable because every device is connected to every other device. If one link fails, data can be rerouted through alternative paths, ensuring that the network remains operational. This redundancy is what makes mesh topology suitable for environments requiring high uptime.

Q.8 What can cause issues in bus topology, and how can they be prevented?

Ans: topology, and how can they be prevented

In bus topology, a failure in the main communication line (the bus) can bring down the entire network. Preventive measures include regular maintenance and using higher-quality cables. However, for large networks, other topologies like star or mesh may be more effective.

Q.9 Explain the main difference between star and ring topologies.

Ans:

DIFFERENCE BETWEEN STAR AND RING TOPOLOGIES

In star topology, all devices are connected to a central hub, and data is directed from the hub to the devices. In contrast, in ring topology, each device is connected to two other devices, forming a circular network where data travels in one direction around the ring.

Q.10 Why might mesh topology be considered expensive to implement?

Ans:

CONSIDERED EXPENSIVE TO IMPLEMENT

Mesh topology is expensive to implement because every device is connected to every other device, requiring more cabling and hardware. This makes it ideal for environments that need high reliability but may be overkill for smaller networks.

MULTIPLE CHOICE QUESTIONS

1. **What does a bus topology use to connect devices?**

(A) A hub (B) A central switch
(C) A single communication line (D) Multiple communication lines

2. **What happens if the main cable fails in a bus topology?**

(A) Only one device is affected
(B) The whole network goes down
(C) Data flow is redirected
(D) The network continues to function without issues

3. **In a star topology, how do devices communicate with each other?**

(A) Through a shared communication line (B) Through a central switch or hub
(C) Directly with each other (D) Using wireless connections

4. **What is the function of a hub in a star topology?**
   (A) To store data (B) To repeat data flow
   (C) To connect devices to the internet (D) To filter data

5. **In a ring topology, how does data travel?**
   (A) In all directions (B) In a circular pathway in one direction
   (C) Directly from one device to another (D) Through a central hub

6. **What issue can arise in a ring topology if one connection fails?**
   (A) The data will slow down (B) Only one device will be affected
   (C) The entire network can be affected (D) The network will reroute automatically

7. **How does a 2-way ring improve a ring topology?**
   (A) It allows for faster data transfer
   (B) It prevents data loss
   (C) It helps resolve the issue when one connection fails
   (D) It reduces the number of devices needed

8. **What is a key feature of a mesh topology?**
   (A) Every device is connected to a central hub (B) Each device is connected to every other device
   (C) Data is transferred in one direction (D) Devices are connected in a circular fashion

9. **What is the advantage of mesh topology?**
   (A) Reduced network traffic (B) High redundancy and reliability
   (C) Easy to set up (D) Low cost

10. **In mesh topology, what happens if one link fails?**
    (A) Data is lost (B) Data is rerouted through other links
    (C) The network stops functioning (D) Devices have to reconnect manually

11. **What is the main disadvantage of bus topology?**
    (A) It requires many devices
    (B) It is expensive to set up
    (C) If the main cable fails, the entire network goes down
    (D) It is not efficient for high traffic

12. **Which of the following topologies uses a central hub for communication?**
    (A) Bus topology (B) Star topology
    (C) Ring topology (D) Mesh topology

13. **What does a ring topology resemble in its function?**
    (A) A classroom with a chalkboard (B) A relay race with baton passing
    (C) A central switch connecting devices (D) A network of roads in a city

14. **What is the primary benefit of using mesh topology?**
    (A) It simplifies network setup (B) It provides multiple routes if one link fails
    (C) It reduces network traffic (D) It uses less hardware

15. **What is a major limitation of bus topology?**
    (A) High reliability
    (B) The difficulty of expanding the network
    (C) A single cable failure can bring down the whole network
    (D) High cost for setup

6.5 TRANSMISSION MODES

LONG QUESTION

Q.1 Explain the three primary transmission modes (Simplex, Half-Duplex, and Full-Duplex) and provide examples for each, highlighting their advantages and disadvantages.

Ans:

1. Simplex Communication

Description:

Simplex communication is a one-way data transmission mode. Data flows in a single direction from the sender to the receiver, with no possibility for the receiver to send data back to the sender.

- **Example:**
  An example of Simplex communication is the connection between a keyboard and a computer. The keyboard sends data to the computer, but the computer cannot send data back to the keyboard.
- **Advantages:**
  Simple to implement
  Efficient for applications that require only one-way communication
- **Disadvantages:**
  Limited to one-way communication only, so not suitable for interactions where feedback is needed

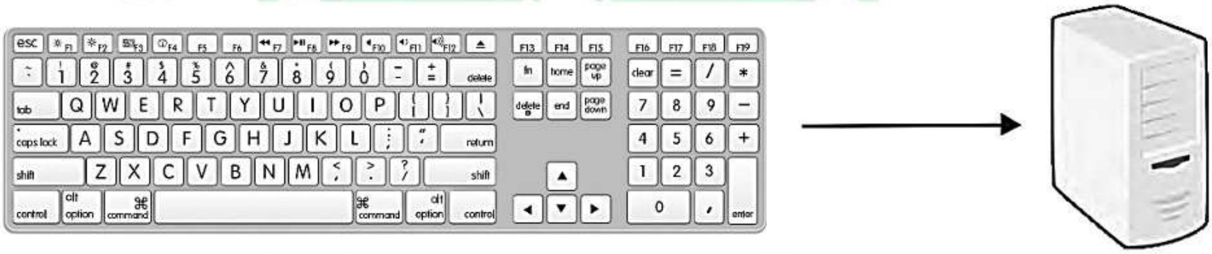


Figure 6.9: Simplex Communication

2. Half-Duplex Communication

- **Description:**
  Half-Duplex communication allows data to be sent in both directions, but not simultaneously. One device transmits, while the other device waits for its turn to transmit.
- **Example:**
  A walkie-talkie is a good example of Half-Duplex communication. One person speaks while the other listens, and the roles are reversed when the first person finishes speaking.
- **Advantages:**
  Allows bidirectional communication
  Requires less complex technology than Full-Duplex
- **Disadvantages:**
  Only one device can communicate at a time, which can cause delays
  Not as efficient as Full-Duplex for real-time interactions

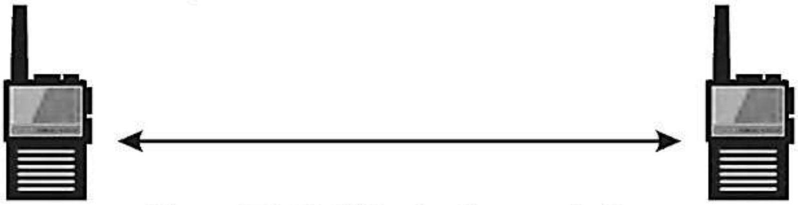


Figure 6.10: Half-Duplex Communication

3. Full-Duplex Communication

Description:

Full-Duplex communication allows for two-way data transmission simultaneously. Both devices can transmit and receive data at the same time, providing the most efficient form of communication.

- **Example:**
  A telephone conversation is an example of Full-Duplex communication, where both parties can talk and listen at the same time.
- **Advantages:**
  Provides real-time, uninterrupted communication
  Highly efficient for modern communication systems
- **Disadvantages:**
  Requires more complex technology
  Can be more expensive to implement

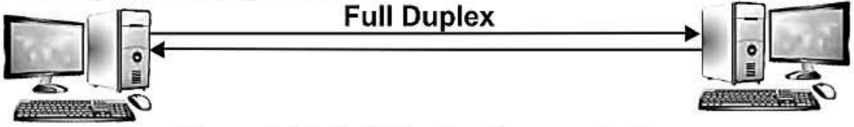


Figure 6.11: Full-Duplex Communication

SHORT QUESTIONS

Q.1 What is Simplex communication?

Ans: **SIMPLEX COMMUNICATION**

Simplex communication is a one-way transmission mode where data flows in only one direction. An example of this is the communication from a keyboard to a computer. In Simplex communication, the direction of data flow is fixed, making it ideal for applications that require only one-way communication.

Q.2 What happens in Half-Duplex communication?

Ans: **HAPPENS IN HALF-DUPLEX COMMUNICATION**

In Half-Duplex communication, data can be transmitted in both directions, but not simultaneously. Only one device can transmit at a time, while the other device waits for its turn. An example is a walkie-talkie, where one person must wait for the other to finish speaking before responding.

Q.3 How does Full-Duplex communication differ from Half-Duplex?

Ans:

Full-Duplex communication allows for simultaneous two-way data transmission, meaning both devices can send and receive data at the same time. In contrast, Half-Duplex allows data to be transmitted in both directions, but not at the same time, requiring devices to take turns.

Q.4 What are some real-life examples of Full-Duplex communication?

Ans: **REAL-LIFE EXAMPLES OF FULL-DUPLEX COMMUNICATION**

A common example of Full-Duplex communication is a telephone conversation. Both people can speak and listen at the same time, which makes communication more efficient. Full-Duplex systems are widely used in modern communication technologies like video calls and internet browsing.

Q.5 Why is Full-Duplex communication more efficient than Half-Duplex?

Ans: **FULL-DUPLEX COMMUNICATION MORE EFFICIENT THAN HALF-DUPLEX**

Full-Duplex communication allows data to be sent and received simultaneously, which leads to more efficient communication. In Half-Duplex, one device must wait for the other to finish transmitting, which can slow down the exchange of information.

Q.6 What were the limitations of early telephones in terms of communication mode?

Ans: **LIMITATIONS OF EARLY TELEPHONES IN TERMS OF COMMUNICATION MODE**

Early telephones used Half-Duplex communication, meaning that only one person could speak at a time. This limited the natural flow of conversation, as the other person had to wait until the speaker finished before responding.

MULTIPLE CHOICE QUESTIONS

1. Which of the following is true for Simplex communication?

(A) Data flows in both directions simultaneously
(B) Data flows in only one direction
(C) Data flow can change direction
(D) Devices can transmit and receive data simultaneously

2. **Which device is an example of Simplex communication?**
(A) Telephone (B) Computer to printer
(C) Keyboard to computer (D) Walkie-talkie

3. **What is the key characteristic of Half-Duplex communication?**
(A) Data flows in both directions simultaneously
(B) Data flows in only one direction
(C) Data flows in both directions, but not at the same time
(D) Devices can only send data

4. **Which of the following is an example of Half-Duplex communication?**
(A) Internet browsing (B) Walkie-talkie communication
(C) Telephone conversations (D) Computer to printer

5. **What does Full-Duplex communication allow?**
(A) One device sends data while the other listens
(B) Data transmission in both directions at different times
(C) Data transmission in both directions simultaneously
(D) Only one device can transmit data at a time

6. **Which of the following is an example of Full-Duplex communication?**
(A) Keyboard to computer (B) Telephone conversation
(C) Walkie-talkie (D) Printer to computer

7. **Which of the following is an advantage of Full-Duplex communication?**
(A) Simultaneous sending and receiving of data (B) Reduced need for devices
(C) Data flows in only one direction (D) It is easier to set up

8. **In which type of communication can both devices transmit and receive at the same time?**
(A) Simplex (B) Half-Duplex
(C) Full-Duplex (D) None of the above

9. **What was the characteristic of the first telephones?**
(A) Full-Duplex (B) Simplex
(C) Half-Duplex (D) Multi-Duplex

10. **What is the main difference between Half-Duplex and Full-Duplex communication?**
(A) Half-Duplex allows data flow in only one direction
(B) Full-Duplex allows simultaneous two-way communication
(C) Half-Duplex is faster than Full-Duplex
(D) Full-Duplex uses fewer devices

6.6 THE OSI NETWORKING MODEL

LONG QUESTION

Q.1 Explain the 7 layers of the OSI model, their functions, and provide real-life examples for each layer.

Ans: Introduction

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a networking system into seven distinct layers. Each layer has a specific function, and these layers work together to ensure smooth and efficient communication between devices in a network.

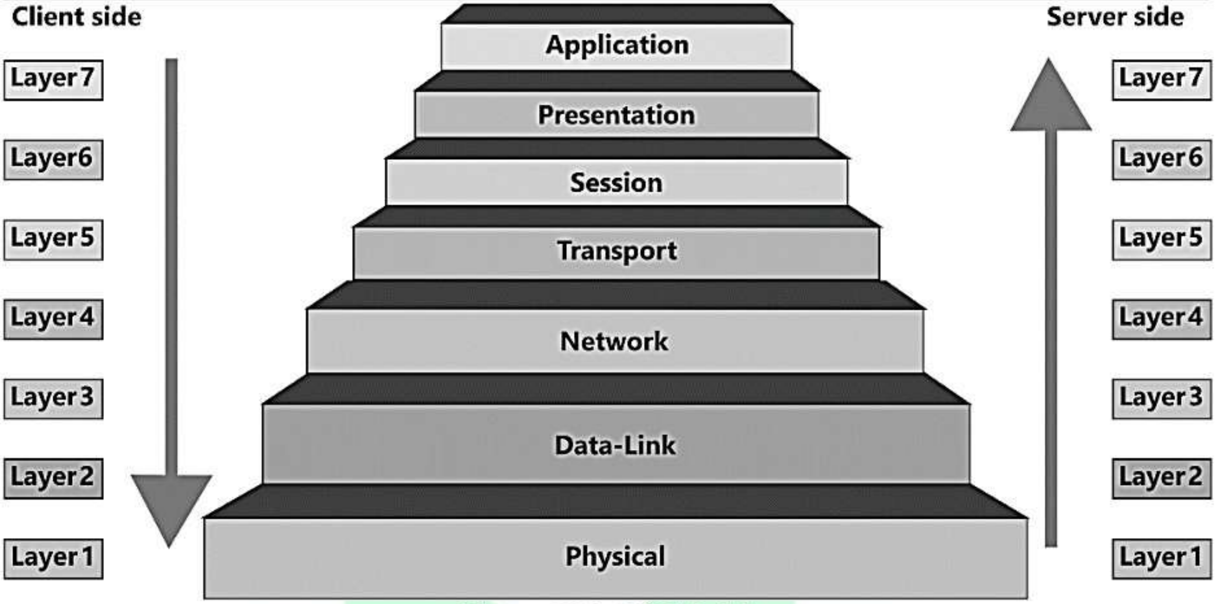


Figure 6.12: OSI Model

Layer 1: Physical Layer

- **Function:**
  The Physical Layer deals with the actual hardware connection between devices. It is responsible for transmitting raw data bits over a physical medium like cables, connectors, and switches. It also includes the voltage levels used for transmission.
- **Example:**
  An example of the Physical Layer is the network cables that connect computers or devices. Without the physical medium, no communication can occur.

Layer 2: Data Link Layer

- **Function:**
  The Data Link Layer ensures error-free data transfer between nodes on the same network. It provides error detection and correction, as well as managing the flow of data to prevent collisions.
- **Example:**
  Think of traffic lights at intersections controlling the flow of cars (data) and preventing collisions (errors). This layer ensures smooth data transfer.

Layer 3: Network Layer

- **Function:**
  The Network Layer is responsible for determining the best path for data to travel between networks. It uses IP addresses to route data from one device to another across different networks.
- **Example:**
  A GPS system finding the best route to travel from one location to another can be compared to the Network Layer's task of finding the best path for data.

Layer 4: Transport Layer

- **Function:**
  The Transport Layer ensures that data is reliably transferred from one device to another. It handles error checking and data flow control, ensuring that data is delivered in the correct order and without errors.
- **Example:**
  This layer is like a delivery service, ensuring that your package arrives at its destination safely and on time, without damage or loss.

Layer 5: Session Layer

- **Function:**
  The Session Layer manages communication sessions between devices. It establishes, maintains, and terminates connections between applications on different devices.
- **Example:**
  In a phone call, the Session Layer manages the call's setup, connection, and termination when you hang up.

Layer 6: Presentation Layer

- **Function:**
  The Presentation Layer is responsible for translating, encrypting, and compressing data to make it readable by the receiving system. It ensures that the data is in a format that the application can process.
- **Example:**
  Imagine a translator converting a book from one language to another, ensuring that the content can be understood by speakers of different languages.

Layer 7: Application Layer

- **Function:**
  The Application Layer provides network services directly to the end users. It supports services like email, file transfers, and web browsing, and enables user applications to interact with the network.
- **Example:**
  The Application Layer is like a waiter in a restaurant, taking your order (request) and bringing your food (data) to you.

SHORT QUESTIONS

Q.1 What is the function of the Physical Layer in the OSI model?

Ans: **FUNCTION OF THE PHYSICAL LAYER IN THE OSI MODEL**

The Physical Layer is responsible for the actual connection between devices in a network. It handles the transmission of unprocessed data bits over a physical medium, such as network cables, repeaters, and hubs. It deals with the hardware aspects of data transmission, including the voltage levels used to send the data.

Q.2 Explain the role of the Data Link Layer.

Ans: The Data Link Layer ensures error-free data transmission by detecting and correcting errors and managing node-to-node data transport. It handles the flow of data between devices on the same network and ensures that data is correctly delivered from one device to another by preventing collisions.

Q.3 How does the Network Layer function in the OSI model?

Ans: **NETWORK LAYER FUNCTION IN THE OSI MODEL**

The Network Layer is responsible for data transfer between different networks. It uses IP addresses to route data to its destination, determining the best possible path for data to travel from the source device to the destination device.

Q.4 What is the primary responsibility of the Transport Layer?

Ans: **PRIMARY RESPONSIBILITY OF THE TRANSPORT LAYER**

The Transport Layer ensures that data is transferred accurately from one system to another. It manages data flow control and error checking, ensuring reliable data transfer between the source and destination systems. Protocols like TCP (Transmission Control Protocol) are used in this layer for reliable communication.

Q.5 What does the Session Layer manage?

Ans: **SESSION LAYER MANAGE**

The Session Layer manages communication sessions between applications. It is responsible for establishing, maintaining, and terminating connections between devices, ensuring that the communication is properly organized and completed.

Q.6 Describe the function of the Presentation Layer.

Ans: **FUNCTION OF THE PRESENTATION LAYER**

The Presentation Layer is responsible for translating, encrypting, and compressing data to ensure that it is readable by the receiving system. It formats the data between the application layer and the network, making it possible for different systems to understand each other's data.

Q.7 What services are provided by the Application Layer?

Ans: **SERVICES ARE PROVIDED BY THE APPLICATION LAYER**

The Application Layer is the closest layer to the end user. It provides services directly to applications, such as email, web browsing, and file transfer. It serves as an interface for users to interact with network services.

Q.8 How does the OSI model relate to daily life?

Ans: The OSI model helps us understand how various networking protocols interact, much like how different departments in an office work together to achieve a common goal. Each layer of the OSI model has a specific function, such as data transmission, routing, and error checking, which ensures that communication between devices is efficient and reliable. Examples, like traffic lights (Data Link Layer) and a GPS system (Network Layer), help illustrate these layers in everyday scenarios.

MULTIPLE CHOICE QUESTIONS

1. **Which layer of the OSI model is responsible for error detection and correction?**
   (A) Physical Layer (B) Data Link Layer
   (C) Transport Layer (D) Network Layer
2. **Which layer determines the best path for data to travel between networks?**
   (A) Transport Layer (B) Data Link Layer
   (C) Network Layer (D) Application Layer
3. **What does the Physical Layer deal with?**
   (A) Error detection (B) Data encryption
   (C) Data transmission via physical medium (D) Data routing
4. **Which of the following is an example of the Data Link Layer?**
   (A) IP address routing (B) Traffic lights managing data flow
   (C) Delivery service ensuring data arrives (D) Network cables connecting devices
5. **Which layer is responsible for ensuring reliable data transfer between systems?**
   (A) Network Layer (B) Application Layer
   (C) Transport Layer (D) Session Layer
6. **Which of the following is an example of the Presentation Layer?**
   (A) A GPS system finding the best route
   (B) A translator converting a book to another language
   (C) A phone call setup
   (D) Error-free data transmission
7. **Which layer is the closest to the end user?**
   (A) Application Layer (B) Transport Layer
   (C) Data Link Layer (D) Session Layer
8. **What is the primary function of the Session Layer?**
   (A) Route data between networks
   (B) Establish, maintain, and terminate connections
   (C) Encrypt and compress data
   (D) Detect and correct errors
9. **Which layer manages data flow control and error checking?**
   (A) Transport Layer (B) Physical Layer
   (C) Data Link Layer (D) Network Layer

10. **Which layer uses IP addresses to route data between networks?**
(A) Application Layer (B) Data Link Layer
(C) Network Layer (D) Presentation Layer

6.7 IPV4 AND IPV 6 AND
6.8 PROTOCOLS AND NETWORK DEVICES

LONG QUESTION

Q.1 Explain the differences between IPv4 and IPv6, including their address schemes, and the role of DNS and DHCP in network communication.

Ans: Introduction

IPv4 and IPv6 are both versions of the Internet Protocol, which is used to assign unique addresses to devices connected to the internet. However, there are significant differences between them in terms of address space and functionality. Additionally, protocols like DNS and DHCP play crucial roles in simplifying network communication.

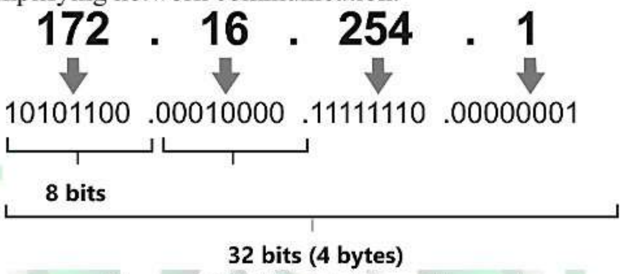


Figure 6.13: IPv4 Address Format

Differences Between IPv4 and IPv6

IPv4:

IPv4 is the fourth version of the Internet Protocol and is the most widely used today. It uses a 32-bit address scheme, which allows for a total of approximately 4.3 billion unique addresses (2^32). An IPv4 address is written in four sets of decimal numbers, each ranging from 0 to 255 (e.g., 192.168.1.1). However, with the growing number of devices connected to the internet, the IPv4 address pool has started to deplete.

IPv6:

IPv6, on the other hand, is the most recent version of the Internet Protocol, designed to replace IPv4. It uses a 128-bit address scheme, allowing for an almost limitless number of unique addresses (2^128). An IPv6 address is written in eight groups of four hexadecimal digits (e.g., 2001:0000:130F:0000:0000:0900:876A:130B). IPv6 was developed to address the depletion of IPv4 addresses and to provide sufficient address space for the rapidly growing number of internet-connected devices.

Role of DNS and DHCP

DNS (Domain Name System):

DNS is a system that translates human-readable domain names (such as www.example.com) into IP addresses, making it easier for users to access websites. Without DNS, users would need to remember the numerical IP addresses of websites, which is not practical. DNS acts like a phonebook for the internet, converting domain names to the corresponding IP addresses.

DHCP (Dynamic Host Configuration Protocol):

DHCP is a protocol that automatically assigns IP addresses to devices on a network. When a device connects to a network, DHCP ensures that it is given a unique IP address from the available address pool. This eliminates the need for manual configuration of IP addresses, simplifying network management.

SHORT QUESTIONS

Q.1 What is the main difference between IPv4 and IPv6?

Ans: **DIFFERENCE BETWEEN IPV4 AND IPV6**

The main difference is the length of the address. IPv4 uses a 32-bit address scheme, which allows for approximately 4.3 billion unique addresses. IPv6 uses a 128-bit address scheme, which allows for an almost limitless number of unique addresses, addressing the depletion issue of IPv4 addresses.

Q.2 Why was IPv6 developed?

Ans: **IPV6 DEVELOPED**

IPv6 was developed to address the depletion of IPv4 addresses due to the rapid growth of the internet and the increasing number of connected devices. IPv6 provides a larger address space to accommodate future growth.

Q.3 How does DNS simplify internet browsing?

Ans: **DNS SIMPLIFY INTERNET BROWSING**

DNS simplifies internet browsing by translating domain names (like www.example.com) into IP addresses, allowing users to access websites using human-readable names instead of numerical IP addresses.

Q.4 What is the function of DHCP in a network?

Ans: **FUNCTION OF DHCP IN A NETWORK**

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network. This simplifies network management by ensuring each device receives a unique IP address without manual configuration.

Q.5 Give an example of an IPv4 address.

Ans: **IPv4 ADDRESS**

An example of an IPv4 address is 192.168.1.1. IPv4 addresses are written in four sets of decimal numbers, each ranging from 0 to 255.

Q.6 What is the primary function of HTTP?

Ans: **PRIMARY FUNCTION OF HTTP**

HTTP (Hypertext Transfer Protocol) is used for transferring web pages over the internet. It facilitates communication between web browsers and servers to display websites to users.

Q.7 How does IPv6 ensure better network addressing?

Ans: **IPv6 ENSURE BETTER NETWORK ADDRESSING**

IPv6 uses a 128-bit address scheme, providing a significantly larger address space compared to IPv4's 32-bit scheme. This large address pool ensures that there are enough IP addresses for all devices in the future.

Q.8 How does IPv4 handle address assignment?

Ans: **IPv4 HANDLE ADDRESS ASSIGNMENT**

IPv4 addresses are assigned in a 32-bit format, typically written as four decimal numbers separated by dots (e.g., 192.168.1.1). This format allows for a limited number of addresses, which is why IPv6 is being adopted to accommodate more devices.

MULTIPLE CHOICE QUESTIONS

1. **What is the primary function of an IP address?**
(A) To assign names to devices (B) To identify devices on the internet
(C) To transfer data between devices (D) To secure network communication

2. **How many unique addresses can IPv4 support?**
(A) 4.3 million (B) 4.3 billion
(C) 32 million (D) 128 billion

3. **What is the bit length of an IPv4 address?**
(A) 64 bits (B) 128 bits
(C) 32 bits (D) 64 bytes

4. Which version of IP is designed to replace IPv4?

(A) IPv1 (B) IPv2
(C) IPv6 (D) IPv5

5. How many bits are used in an IPv6 address?

(A) 32 bits (B) 64 bits
(C) 128 bits (D) 256 bits

6. What problem does IPv6 address that IPv4 cannot?

(A) Low-speed internet connections (B) Internet security
(C) Depletion of IPv4 addresses (D) Shortage of bandwidth

7. What does DNS stand for?

(A) Domain Name Service (B) Dynamic Network Service
(C) Domain Name System (D) Digital Network Service

8. What is the role of DHCP?

(A) Assigns domain names to devices (B) Converts domain names to IP addresses
(C) Automatically assigns IP addresses to devices (D) Encrypts network data

9. Which protocol is used for transferring web pages over the internet?

(A) FTP (B) HTTP
(C) SMTP (D) TCP/IP

10. What is an example of an IPv6 address?

(A) 192.168.1.1 (B) 172.16.254.1
(C) 2001:0000:130F:0000:0000:0900:876A:130B (D) 255.255.255.0

6.9 NETWORK SECURITY

LONG QUESTION

Q.1 Explain the importance of network security, including the key concepts like firewalls, encryption, and common threats like malware and phishing.

Ans: Introduction

Network security is crucial for protecting data, ensuring privacy, and maintaining the availability of network resources. With the rise of cyber threats and the increasing number of devices connected to networks, understanding and implementing effective network security measures is vital.

Importance of Network Security

- **Data Protection:**
  Network security ensures that sensitive information, such as personal data or corporate secrets, is protected from unauthorized access or alteration. This is achieved through various measures like encryption and secure authentication methods.
- **Preventing Attacks:**
  Network security helps defend against malicious attacks, such as malware, that can disrupt services, steal data, or corrupt systems. These attacks can have severe consequences, including financial losses and damage to reputation.
- **Maintaining Privacy:**
  Privacy is safeguarded by controlling who can access sensitive data. Network security mechanisms ensure that only authorized users are granted access to personal and confidential information.
- **Ensuring Availability:**
  Network security measures ensure that network resources are always accessible to authorized users. Attacks like Denial of Service (DoS) are mitigated to prevent service disruptions.

Key Concepts in Network Security

- **Firewalls:**
  Firewalls are essential in network security, acting as barriers between trusted internal networks and untrusted external networks. They monitor and control the flow of traffic based on predetermined security rules, preventing unauthorized access.

- **Encryption:**
  Encryption is the process of converting data into a secure format to prevent unauthorized users from reading it. By transforming data into ciphertext, it ensures that sensitive information remains secure during transmission.

Common Threats:

- **Malware:**
  Malware, including viruses, worms, and ransomware, is designed to damage or steal data. It is a primary threat to network security, as it can spread through networks and compromise system integrity.
- **Phishing:**
  Phishing is an attempt to deceive users into revealing confidential information, such as login credentials, by impersonating trusted entities. It is one of the most common social engineering attacks.
- **Denial of Service (DoS) Attacks:**
  DoS attacks aim to overwhelm a network with excessive traffic, disrupting normal operations and denying service to legitimate users. This type of attack can cause significant downtime and loss of service.

Man-in-the-Middle Attacks:
In these attacks, a third party intercepts communication between two parties to steal or alter data. These attacks can compromise data integrity and confidentiality.

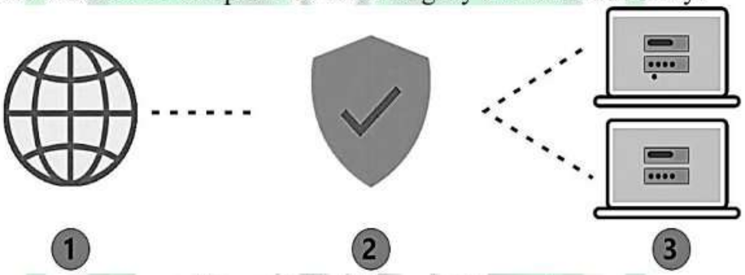


Figure 6.14: Firewall Concept

SHORT QUESTIONS

Q.1 What is network security?

Ans: **NETWORK SECURITY**

Network security involves measures designed to protect data, prevent unauthorized access to networks, and defend against malicious attacks. It ensures data privacy, the availability of resources, and the overall integrity of the network.

Q.2 Why is network security important?

Ans: **NETWORK SECURITY IMPORTANT**

Network security is vital to protect sensitive data from unauthorized access, defend against malicious attacks, maintain privacy, and ensure the availability of network resources for legitimate users.

Q.3 What role do firewalls play in network security?

Ans: **FIREWALLS PLAY IN NETWORK SECURITY**

Firewalls are security systems that monitor and control incoming and outgoing network traffic. They follow predefined security rules to block harmful traffic and prevent unauthorized access to a network.

Q.4 What is encryption in network security?

Ans: **ENCRYPTION IN NETWORK SECURITY**

Encryption is the process of converting readable data (plain text) into an unreadable format (ciphertext) to protect it from unauthorized access. Only those with the correct decryption key can convert the data back to its original form.

Q.5 What is the process of decryption?

Ans: **PROCESS OF DECRYPTION**

Decryption is the process of converting encrypted data (ciphertext) back into its original readable form (plain text). This is done using a decryption key, which reverses the encryption process.

Q.6 How does encryption protect data during communication?

Ans: **ENCRYPTION PROTECT DATA DURING COMMUNICATION**

Encryption protects data by transforming it into a secure format that can only be understood by authorized recipients with the decryption key. This ensures that sensitive information cannot be intercepted and read by unauthorized parties.

Q.7 What is the significance of passwords in network security?

Ans: **SIGNIFICANCE OF PASSWORDS IN NETWORK SECURITY**

Passwords are a critical part of network security as they help verify the identity of users. They ensure that only authorized individuals can access network resources, protecting sensitive data and systems from unauthorized use.

Q.8 What is malware, and how does it affect a network?

Ans: **MALWARE, AND HOW DOES IT AFFECT A NETWORK**

Malware refers to malicious software such as viruses, worms, and ransomware that can damage or steal data. It poses a serious threat to network security by corrupting systems, compromising data, and disrupting network operations.

Q.9 What is phishing, and how does it threaten network security?

Ans: **PHISHING, AND HOW DOES IT THREATEN NETWORK SECURITY**

Phishing is a deceptive practice where attackers trick users into revealing sensitive information, such as usernames, passwords, or credit card details, through fake emails or websites. It compromises network security by stealing confidential data.

Q.10 What is a Denial of Service (DoS) attack?

Ans: **DENIAL OF SERVICE (DOS) ATTACK**

A Denial of Service (DoS) attack overwhelms a network with excessive traffic, disrupting its normal operation and making it unavailable to legitimate users. This attack can cause significant service interruptions and damage to the network.

Q.11 How does a Man-in-the-Middle (MITM) attack work?

Ans: **MAN-IN-THE-MIDDLE (MITM) ATTACK WORK**

A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts communication between two parties to steal or alter information. This type of attack can compromise data integrity and privacy during transmission.

Q.12 How was encryption used during World War II to help the Allies?

Ans: **ENCRYPTION USED DURING WORLD WAR II TO HELP THE ALLIES**

During World War II, the Allies used the Enigma machine to encrypt their communications. The ability to decrypt German Enigma-encrypted messages allowed the Allies to intercept and understand enemy plans, contributing to their victory.

MULTIPLE CHOICE QUESTIONS

1. **What is the primary goal of network security?**

(A) Data analysis (B) Data protection
(C) Data storage (D) Data sharing

2. **Which of the following is NOT a function of network security?**

(A) Preventing unauthorized access (B) Safeguarding personal information
(C) Ensuring data alteration (D) Defending against attacks

3. **What is a firewall used for in network security?**

(A) Encrypting data (B) Controlling network traffic
(C) Managing passwords (D) Detecting malware

4. **Which of the following processes is used to convert encrypted data back to its original form?**
(A) Encryption (B) Authentication
(C) Decryption (D) Ciphertext

5. **What is malware?**
(A) A network security tool (B) Malicious software that damages or steals data
(C) A type of firewall (D) A secure data transfer method

6. **Which of these is a method of protecting sensitive information?**
(A) Phishing (B) Encryption
(C) Denial of Service (D) Man-in-the-Middle

7. **Which attack type involves overwhelming a network with traffic to make it unavailable?**
(A) Phishing (B) Denial of Service (DoS)
(C) Malware (D) Man-in-the-Middle

8. **What is the purpose of passwords in network security?**
(A) To encrypt data
(B) To prevent malware
(C) To ensure only authorized users access resources
(D) To manage network traffic

9. **What does a man-in-the-middle attack involve?**
(A) Storing data securely
(B) Intercepting communication between two parties
(C) Blocking network traffic
(D) Encrypting data for security

10. **Which event was significantly impacted by the ability to decrypt Enigma messages?**
(A) The Cold War (B) World War II
(C) The Space Race (D) The Korean War

6.10 TYPES OF NETWORKS

LONG QUESTION

Q.1 Describe the different types of networks, including PAN, LAN, MAN, WAN, and CAN, and explain their key differences and uses.

Ans: Introduction

There are various types of networks, each designed to meet different communication needs. These networks differ in terms of their geographical range, purpose, and the devices they connect. The main types of networks include Personal Area Networks (PAN), Local Area Networks (LAN), Metropolitan Area Networks (MAN), Wide Area Networks (WAN), and Campus Area Networks (CAN).

Personal Area Network (PAN)

A PAN is the smallest type of network, typically used for communication between personal devices such as smartphones, laptops, and tablets. It covers a very limited range, usually a few meters. The most common example of a PAN is a Bluetooth connection between a smartphone and a wireless headset.

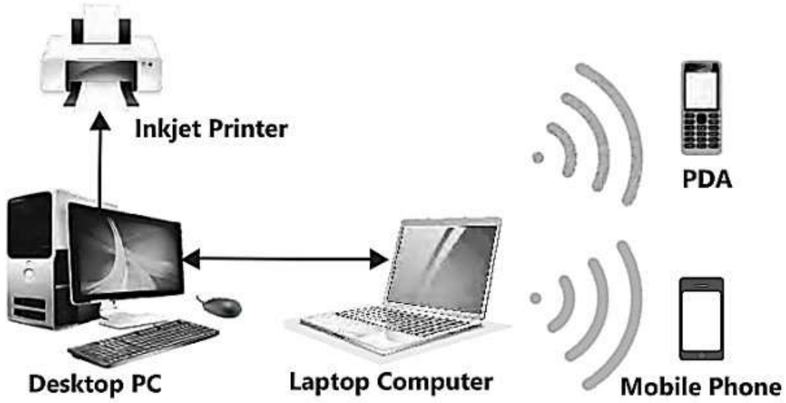


Figure 6.15: Personal Area Network (PAN)

Local Area Network (LAN)

A Local Area Network (LAN) connects devices within a limited area, such as a home, office, or school. It enables efficient communication and resource sharing among devices like computers, printers, and servers. A LAN can cover areas up to a few kilometers and is widely used in schools, offices, and residential complexes.

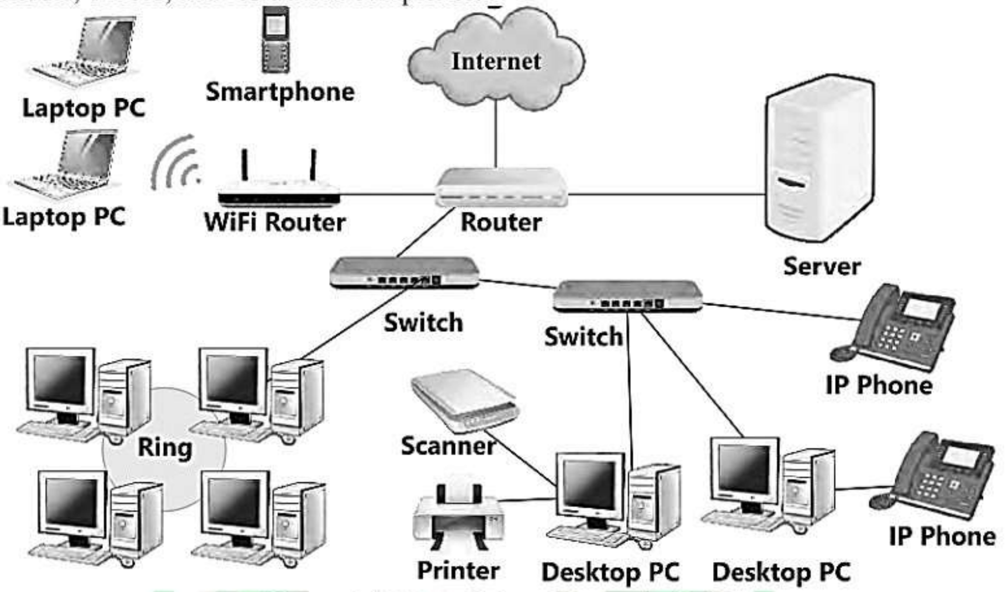


Figure 6.16: Local Area Network (LAN)

Metropolitan Area Network (MAN)

A Metropolitan Area Network (MAN) spans a larger geographical area, such as a city or a large campus. It connects multiple LANs, allowing for communication between devices spread across a larger area. A MAN can cover up to 50 kilometers and is commonly used by universities or large corporations to connect their different branches within a city.

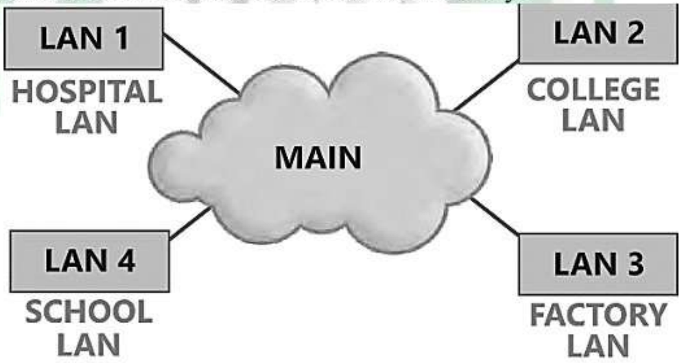


Figure 6.17: Metropolitan Area Network (MAN)

Wide Area Network (WAN)

A WAN covers a vast geographical area and connects multiple LANs and MANs. It can span cities, countries, or even continents. The internet is the largest and most well-known example of a WAN. WANs are essential for multinational corporations to link their offices worldwide, ensuring efficient data sharing and communication.

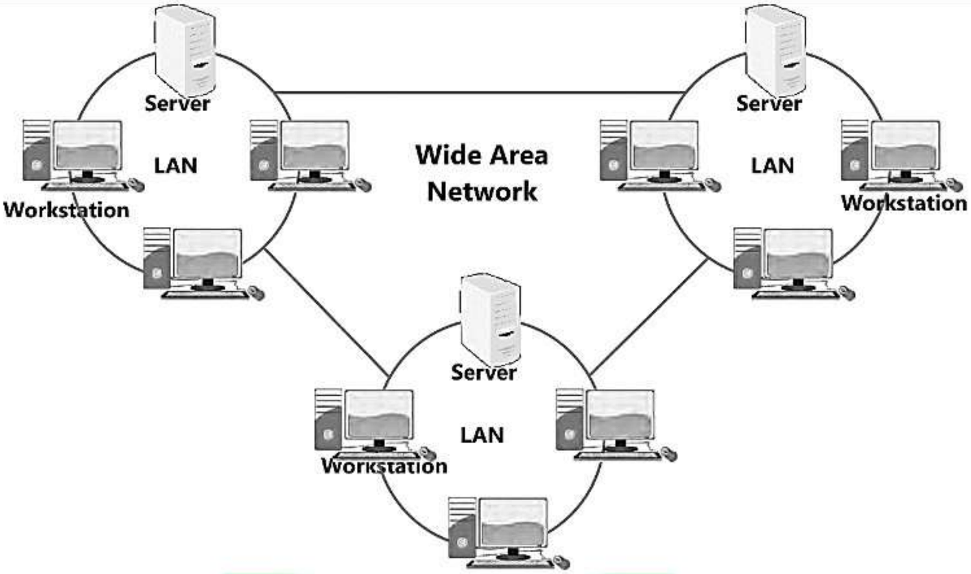


Figure 6.18: Wide Area Network (WAN)

Campus Area Network (CAN)

A Campus Area Network (CAN) is used to connect multiple LANs within a limited area, such as a university campus or business park. It allows departments or buildings within a campus to share resources and communicate effectively. CANs are ideal for educational institutions and business complexes where several buildings need to be interconnected.

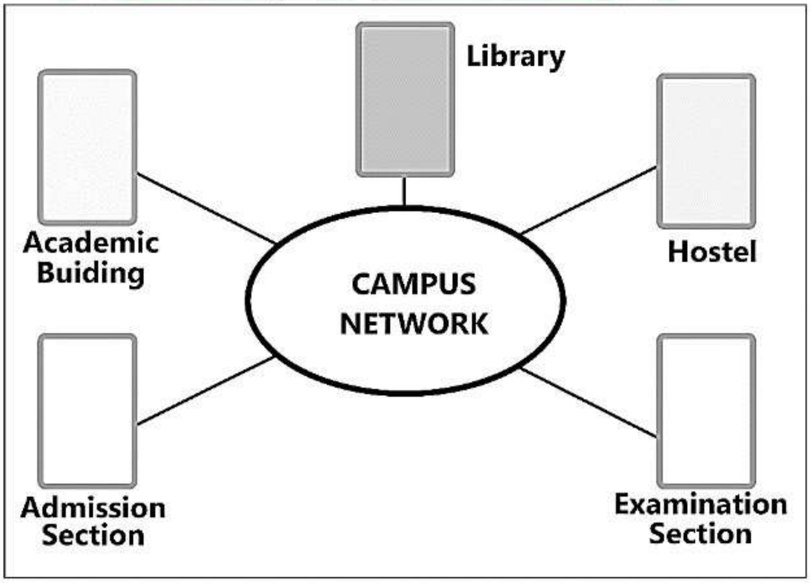


Figure 6.19: Campus Area Network (CAN)

Key Differences

The main differences between these networks lie in their geographical coverage and scale:

PANs are the smallest and used for personal devices in close proximity.

LANs connect devices within a building or small area.

MANs span a city or large campus.

WANs cover large, often global areas.

CANs connect multiple LANs within a campus-like setting.

Each network type serves specific needs and is designed to handle different communication and data-sharing requirements across varying distances.

SHORT QUESTIONS

Q.1 What is a Personal Area Network (PAN)?

Ans: **PERSONAL AREA NETWORK (PAN)**

A Personal Area Network (PAN) is a small network designed for communication between personal devices like smartphones, tablets, and laptops within a short range, typically a few meters. Bluetooth connections between devices like a smartphone and wireless headset are common examples of PANs.

Q.2 How does a PAN differ from other types of networks?

Ans: **PAN DIFFER FROM OTHER TYPES OF NETWORKS**

A PAN is smaller in range compared to other networks, focusing on personal device communication within a limited area of a few meters, unlike Local Area Networks (LANs) or Wide Area Networks (WANs), which cover larger areas.

Q.3 What is a Local Area Network (LAN)?

Ans: **LOCAL AREA NETWORK (LAN)**

A Local Area Network (LAN) connects devices within a small, localized area, such as a home, office, or school. It enables devices to communicate and share resources, such as files or printers, within a limited geographical space.

Q.4 What are some common examples of LANs?

Ans: **SOME COMMON EXAMPLES OF LANs**

Common examples of LANs include the computer network in a school that connects all the computers in a lab or the network that links devices within an office or home environment.

Q.5 What is the range of a Local Area Network (LAN)?

Ans: **RANGE OF A LOCAL AREA NETWORK (LAN)**

A Local Area Network (LAN) typically covers a small geographical area, such as a building or a group of buildings, and may extend up to a few kilometers in some cases.

Q.6 What is a Metropolitan Area Network (MAN)?

Ans: **METROPOLITAN AREA NETWORK (MAN)**

A Metropolitan Area Network (MAN) connects multiple Local Area Networks (LANs) within a city or large campus. It spans a larger geographical area, typically covering up to 50 kilometers, and is used for city-wide connectivity.

Q.7 How does a MAN differ from a WAN?

Ans: A Metropolitan Area Network (MAN) covers a city or large campus, while a Wide Area Network (WAN) connects devices and networks across a much larger geographical area, including different cities or countries.

Q.8 What is the purpose of a Wide Area Network (WAN)?

Ans: **PURPOSE OF A WIDE AREA NETWORK (WAN)**

A Wide Area Network (WAN) is used to connect multiple LANs and MANs, spanning a large geographical area, including different cities or even countries. The internet is the largest example of a WAN.

Q.9 How is a WAN beneficial for multinational companies?

Ans: **WAN BENEFICIAL FOR MULTINATIONAL COMPANIES**

A WAN enables multinational companies to connect branch offices across different countries, allowing them to share resources, communicate, and access centralized data, regardless of their physical locations.

Q.10 What is a Campus Area Network (CAN)?

Ans: **CAMPUS AREA NETWORK (CAN)**

A Campus Area Network (CAN) connects multiple LANs within a limited geographical area, such as a university campus or business park. It facilitates communication and resource sharing between various departments and buildings within that area.

Q.11 What is the maximum range of a Metropolitan Area Network (MAN)?

Ans: **MAXIMUM RANGE OF A METROPOLITAN AREA NETWORK (MAN)**

A MAN can cover up to 50 kilometers, making it ideal for connecting multiple LANs across a city or a large campus.

Q.12 How does a Virtual Private Network (VPN) enhance security for WANs?

Ans: **VIRTUAL PRIVATE NETWORK (VPN) ENHANCE SECURITY FOR WANS**

A Virtual Private Network (VPN) provides a secure way to connect to a WAN, encrypting the data being transferred to protect it from unauthorized access, especially when using public or unsecured networks.

Q.13 Why is a PAN used for communication between personal devices?

Ansr: **PAN USED FOR COMMUNICATION BETWEEN PERSONAL DEVICES**

A PAN is ideal for communication between personal devices due to its short range, typically a few meters. This makes it perfect for connecting devices like smartphones, wireless headsets, and tablets in close proximity.

Q.14 What are the advantages of using a LAN in a school or office setting?

Ans: **ADVANTAGES OF USING A LAN IN A SCHOOL OR OFFICE SETTING**

A LAN allows for fast and efficient communication between devices within a small area, such as a school or office, enabling resource sharing like printers, files, and internet connections, all within a manageable space.

Q.15 What is the main difference between a LAN and a MAN?

Ans: **MAIN DIFFERENCE BETWEEN A LAN AND A MAN**

The main difference between a LAN and a MAN is the geographical coverage. A LAN connects devices within a smaller, more localized area (e.g., a building), while a MAN spans a larger area like a city or large campus.

MULTIPLE CHOICE QUESTIONS

1. **What is the range of a Personal Area Network (PAN)?**
(A) A few meters (B) A few kilometers
(C) Hundreds of kilometers (D) Global

2. **Which of the following is an example of a PAN?**
(A) A network connecting multiple schools
(B) Bluetooth connections between a smartphone and a wireless headset
(C) A network covering a city
(D) Connecting offices of a multinational company

3. **What is the purpose of a Local Area Network (LAN)?**
(A) To connect devices across a city
(B) To connect devices within a small geographical area
(C) To connect different countries
(D) To connect personal devices within a range of meters

4. **Which of the following is an example of a LAN?**
(A) A network connecting different branches of a company worldwide
(B) The network that connects all computers in a school lab
(C) A network that spans an entire city
(D) A connection between a smartphone and a wireless headset

5. **What does a Metropolitan Area Network (MAN) typically cover?**
(A) A single building (B) A city or large campus
(C) A personal device (D) Multiple countries

6. **What is the largest example of a Wide Area Network (WAN)?**
(A) Bluetooth (B) A local office network
(C) The internet (D) A campus network

7. **What is a Campus Area Network (CAN)?**
(A) A network that connects devices in a home
(B) A network covering a city
(C) A network that connects multiple LANs within a limited geographical area
(D) A global network for multinational companies

8. **What is the primary use of a Virtual Private Network (VPN) in relation to a WAN?**
(A) To encrypt local network traffic
(B) To securely connect to a WAN and protect data
(C) To connect devices within a single building
(D) To connect personal devices like smartphones

9. **Which network connects various branches of a university across a city?**
(A) LAN (B) MAN
(C) WAN (D) PAN

10. **What is the ideal geographical area for a MAN?**
(A) A few meters (B) A city or large campus
(C) A building (D) Multiple countries

6.11 REAL-WORLD APPLICATIONS OF COMPUTER NETWORKS, 6.12 STANDARD PROTOCOLS, 6.13 NETWORK SECURITY MODELS

LONG QUESTION

Q.1 Explain the role of networks in various sectors such as business, education, and healthcare, and describe the standard protocols and network security methods used to ensure efficient and secure communication.

Ans: Introduction

Networks are integral to sectors like business, education, and healthcare, ensuring efficient communication and secure data sharing. Various protocols like TCP/IP manage data transmission, while security methods safeguard information.

Role of Networks in Different Sectors

1. **Business:**
Networks support communication, resource sharing, and data management. Businesses use intranets to securely share resources and information internally.

2. **Education:**
Networks enable online learning and access to educational content. LMS platforms like Blackboard and Moodle are used to deliver courses and track student progress.

3. **Healthcare:**
Networks help manage patient data, facilitate telemedicine, and ensure secure access to medical resources. EHR systems store patient information efficiently, improving care quality.

Standard Protocols in TCP/IP Communication

1. **TCP:** Ensures reliable data transfer by managing data packet transmission.
2. **IP:** Handles addressing and routing of data packets across networks.
3. **UDP:** Provides faster data transfer, though less reliable, useful for time-sensitive applications like streaming.
4. **DNS:** Translates domain names to IP addresses for easier website access.
5. **DHCP:** Automatically assigns IP addresses to devices on a network, simplifying management.

Network Security Methods

1. **Firewalls:** Control network traffic based on security rules, preventing unauthorized access.
2. **Encryption:** Secures data by converting it into unreadable formats, ensuring privacy.
3. Antivirus Software: Detects and removes malware, ensuring network security.

Conclusion

Networks streamline operations in business, education, and healthcare, enhancing communication and resource sharing. Protocols like TCP/IP ensure efficient data transfer, while firewalls, encryption, and antivirus software provide robust security to protect sensitive information.

SHORT QUESTIONS

Q.1 How are networks used in business?

Ans: **NETWORKS USED IN BUSINESS**

Networks enable efficient communication, resource sharing, and data management within businesses. Intranets are used to securely share information and resources.

Q.2 What role do networks play in education?

Ans: **NETWORKS PLAY IN EDUCATION**

Networks facilitate online learning platforms, virtual classrooms, and access to educational resources. Learning Management Systems (LMS) are used to deliver course content and assessments.

Q.3 How do networks benefit healthcare?

Ans: **NETWORKS BENEFIT HEALTHCARE**

Healthcare networks allow for the secure sharing of patient information, telemedicine, and access to medical databases, with Electronic Health Records (EHR) systems storing patient data efficiently.

Q.4 What is TCP/IP, and why is it important?

Ans: **TCP/IP, AND WHY IS IT IMPORTANT**

TCP/IP is a suite of protocols essential for internet communication, ensuring reliable data transfer and proper addressing and routing of data packets.

Q.5 What is the function of Transmission Control Protocol (TCP)?

Ans: **FUNCTION OF TRANSMISSION CONTROL PROTOCOL (TCP)**

TCP ensures reliable data transfer by managing the transmission and correct order of data packets between devices.

Q.6 How does the Internet Protocol (IP) work in TCP/IP communication?

Ans: **INTERNET PROTOCOL (IP) WORK IN TCP/IP COMMUNICATION**

IP addresses and routes data packets to their correct destination across networks by assigning unique IP addresses to devices.

Q.7 What is the role of the User Datagram Protocol (UDP)?

Ans: **ROLE OF THE USER DATAGRAM PROTOCOL (UDP)**

UDP enables faster but less reliable data transfer, suitable for applications requiring speed over reliability, like live video streaming.

Q.8 What is the Domain Name System (DNS), and why is it necessary?

Ans: **DOMAIN NAME SYSTEM (DNS), AND WHY IS IT NECESSARY**

DNS translates domain names into IP addresses, allowing easier access to websites without needing to remember complex IP addresses.

Q.9 Why is encryption important in network security?

Ans: **ENCRYPTION IMPORTANT IN NETWORK SECURITY**

Encryption converts data into a secure format, ensuring that only authorized parties can access the original information.

Q.10 What is the purpose of antivirus software in network security?

Ans: **PURPOSE OF ANTIVIRUS SOFTWARE IN NETWORK SECURITY**

Antivirus software detects and removes malicious software, preventing threats like viruses and malware from compromising network security.

MULTIPLE CHOICE QUESTIONS

1. Which protocol ensures reliable data transfer in TCP/IP?

(A) UDP (B) IP
(C) TCP (D) DNS

2. What does the Domain Name System (DNS) do?

(A) Routes data packets (B) Translates domain names to IP addresses
(C) Assigns IP addresses automatically (D) Detects malicious software

3. **What type of network is commonly used by businesses for secure communication and resource sharing?**
(A) LAN (B) Intranet
(C) VPN (D) MAN

4. **Which protocol automatically assigns IP addresses to devices on a network?**
(A) TCP (B) DNS
(C) DHCP (D) UDP

5. **Which of the following is an example of a Learning Management System (LMS) used in education?**
(A) Blackboard (B) Zoom
(C) Skype (D) Google Meet

6. **What is the primary function of firewalls in network security?**
(A) Detect malware (B) Monitor and control network traffic
(C) Encrypt data (D) Provide secure connections

7. **Which healthcare system allows efficient storage and retrieval of patient data?**
(A) ERP (B) EHR
(C) DNS (D) LMS

8. **Which of the following provides faster, but less reliable, data transfer?**
(A) TCP (B) IP
(C) UDP (D) DNS

9. **Which network security method detects and removes malicious software?**
(A) Encryption (B) Firewalls
(C) Antivirus software (D) VPN

10. **Which network is used in educational institutions for delivering course content and assessments?**
(A) VPN (B) LAN
(C) Intranet (D) LMS

SUMMARY

- A computer network is a system of interconnected computers and devices that communicate and share resources.
- The primary objectives of computer networks are to enable resource sharing, data communication, and connectivity between devices.
- Data communication involves the exchange of data between a sender and a receiver through a communication medium.
- Protocols are sets of rules that govern data communication. Common protocols include TCP/IP, HTTP, FTP and SMTP.
- A router is a device that connects different networks together and directs data packets between them.
- When you send data over the internet, it gets broken down into smaller pieces called packets.
- A switch is a network device that connects multiple devices (like computers, printers, and servers) within a Local Area Network (LAN).
- An Access Point (AP) is a network device that allows wireless devices to connect to a wired network.
- Network topologies refer to the arrangement of different elements (links, nodes, etc.) in a computer network.
- In a Bus topology, all devices share a single communication line called a bus. Each device is connected to this central cable.
- In a Star topology, all devices are connected to a central hub or switch. The hub acts as a repeater for data flow.
- In a Ring topology, each device is connected to two other devices, forming a circular data path. Data travels in one direction, passing through each device.

- In a Mesh topology, each device is connected to every other device. This provides high redundancy and reliability.
- In Simplex communication, data transmission is unidirectional, meaning it flows in only one direction.
- In Half-Duplex communication, data transmission can occur in both directions, but not simultaneously.
- In Full-Duplex communication, data transmission can occur in both directions simultaneously.
- The Open Systems Interconnection (OSI) Model is a framework used to understand how different networking protocols interact.
- Internet Protocol (IP) addresses are unique identifiers assigned to devices connected to the Internet. There are two primary versions: IPv4 and IPv6.
- DNS translates domain names to IP addresses, making it easier for users to access websites.
- DHCP automatically assigns IP addresses to devices on a network, simplifying network management.
- Network security involves measures to protect data and prevent unauthorized access to computer networks.
- Encryption transforms data into a secure format that can only be read or understood by authorized parties with the correct decryption key.
- A PAN is a small network used for communication between personal devices, such as smartphones, tablets, and laptops, within a short range.
- A LAN is a network that connects computers and devices within a limited area, such as a home, school, or office building.
- A MAN is a network that spans a city or a large campus, connecting multiple LANs together.
- A WAN covers a large geographical area, connecting multiple LANs and MANs. The internet is the largest example of a WAN.
- A CAN is a network that connects multiple LANs within a limited geographical area, such as a university campus or a business.

EXERCISE

MULTIPLE CHOICE QUESTIONS

35. What is the primary objective of computer networks?
(A) Increase computational power
(B) Enable resource sharing and data communication
(C) Enhance graphic capabilities
(D) Improve software development

36. Which device is used to connect multiple networks and direct data packets between them?
(A) Switch (B) Hub
(C) Router (D) Modem

37. Which layer of the OS model is responsible for node-to-node data transfer and error detection?
(A) Physical Layer (B) Data Link Layer
(C) Network Layer (D) Transport Layer

38. What is the function of the Domain Name System (DNS)?
(A) Assign IP addresses dynamically (B) Translate domain names to IP addresses
(C) Secure data communication (D) Monitor network traffic

39. Which method of data transmission uses a dedicated communication path?
(A) Packet Switching (C) Full-Duplex
(B) Circuit Switching (D) Half-Duplex

40. What is encapsulation in the context of network communication?
(A) Converting data into a secure format (B) Wrapping data with protocol information
(C) Monitoring network traffic (D) Translating domain names to IP addresses

41. Which protocol is used for reliable data transfer in the TCP/IP model?

(A) HTTP (B) FTP

(C) TCP (D)

42. What is the main purpose of a firewall in network security?

(A) Convert data into a secure format (B) Monitor and control network traffic

(C) Assign IP addresses (D) Translate domain names

43. Which network topology connects all devices to a central hub?

(A) Ring (B) Mesh

(C) Bus (D) Star

44. What is a key benefit of using computer networks in businesses?

(A) Increase computational power

(B) Enable resource sharing and efficient communication

(C) Enhance graphic capabilities

(D) Improve software development

SHORT QUESTIONS

Q. 14 Define data communication and list its key components.

Ans: Data communication refers to the exchange of data between a sender and a receiver through a communication medium. It is crucial for enabling communication and collaboration in computer networks.

Key components of data communication:

1. Sender: The device that sends the data (e.g., a computer sending an email).
2. Receiver: The device that receives the data (e.g., a smartphone receiving the email).
3. Message: The data being communicated (e.g., the content of an email).
4. Protocol: A set of rules governing data communication (e.g., HTTP for web communication).
5. Medium: The physical or wireless path for data transfer (e.g., Ethernet cables or Wi-Fi).

Q. 15 Explain the role of routers in a computer network.

Ans: Routers are networking devices that interconnect multiple networks or allow devices to connect to a network. They direct data packets between networks by determining the best path for each packet to reach its destination using a routing table. Routers play a key role in ensuring efficient data transmission within local networks and across the internet.

Q. 16 What are the main functions of the Network Layer in the OSI model?

Ans: The Network Layer is responsible for transferring data across different networks. It determines the best path for data to travel from the source to the destination using IP addresses. It also handles packet routing and forwarding, ensuring that data reaches its intended target efficiently.

Q. 17 Describe the difference between packet switching and circuit switching.

Ans: Packet Switching: Data is divided into packets, each of which can take a different route to the destination. This method is efficient and allows for better utilization of network resources.

Circuit Switching: Establishes a dedicated communication path between sender and receiver before data transmission begins. This method is less flexible but ensures a constant connection.

Q. 18 What is the purpose of the Dynamic Host Configuration Protocol (DHCP)?

Ans: DHCP is a network protocol that automatically assigns IP addresses to devices on a network, simplifying network management. For example, when a device connects to a Wi-Fi network, DHCP assigns it an IP address, enabling seamless communication.

Q. 19 How does encapsulation ensure secure communication in a network?

Ans: Encapsulation involves wrapping data with protocol-specific information (headers and footers) as it moves through the OSI layers. This ensures that data is securely and accurately transmitted between devices, as each layer adds specific information needed for successful delivery.

Q. 20 Differentiate between TCP and UDP in terms of data transfer reliability.

Ans: TCP (Transmission Control Protocol): Ensures reliable data transfer through error checking, acknowledgment of received data, and retransmission of lost packets. It is used in applications where data accuracy is critical, such as file transfers.

UDP (User Datagram Protocol): Provides faster but less reliable data transfer, as it does not perform error checking or retransmission. It is used in real-time applications like video streaming and online gaming.

Q. 21 Explain the importance of encryption in network security.

Ans: Encryption protects data by converting it into a secure format that can only be read by authorized parties with the correct decryption key. It ensures data confidentiality, integrity, and security, preventing unauthorized access during transmission.

Q. 22 What are the advantages of using a star topology in a network?

Ans: Easy to set up and manage.

High reliability: A failure in one node does not affect others.

Simple troubleshooting and scalability, as devices are connected to a central hub or switch.

Q. 23 How do firewalls contribute to network security?

Ans: Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between trusted internal networks and untrusted external networks, helping to prevent unauthorized access and cyberattacks.

LONG QUESTIONS

1. **Discuss the objectives of computer networks and provide examples of how they facilitate resource sharing and data communication.**
   See Topic 6.1
2. **In a Simplex communication system, assume data is transmitted at a rate of 500 bits per second (bps). Compute the time to transmit a message if:**
   (a) it is of 10 kilobits. (b) it is of 10 kilobytes.
   To solve the problem of computing the time required to transmit data in a simplex communication system, we use the formula:
   Transmission Time=Data Size /Transmission Rate
   Given:
   - Transmission Rate = 500 bps

   Part (a): Transmission of 10 kilobits
   - Data Size = 10 kilobits=10×1024=10,240 bits

   Transmission Time=10,240 bits/500 bps=20.48 seconds
   Part (b): Transmission of 10 kilobytes
   - Data Size = 10 kilobytes=10×1024×8=81,920 bits

   Transmission Time=81,920 bits500 bps=163.84
   Final Answers:
   - **(a)**: It takes **20.48 seconds** to transmit 10 kilobits of data.
   - **(b)**: It takes **163.84 seconds** to transmit 10 kilobytes of data
3. **Describe how data is transmitted across computer networks using packet switching and circuit switching.**
   See Topic 6.1
4. **Discuss the role and importance of protocols in data communication. Explain the functions of key protocols such as TCP/IP, HTTP, DNS, and DHCP.**
   See Topic 6.8
5. **Evaluate different methods of network security, including firewalls, encryption, and antivirus software.**
   See Topic 6.9
6. **Describe real-world applications of computer networks in business, education, and healthcare.**
   See Topic 6.11
7. **Compare and contrast the different types of network topologies (star, ring, bus, and mesh).**
   See Topic 6.4
8. **Consider a shift cipher with a shift amount of 4.**
   (a) Encrypt the message "SECURITY":
   Using a shift cipher with a shift amount of 4, each letter in the plaintext is shifted 4 places forward in the alphabet:
   S → W

E → I
C → G
U → Y
R → V
I → M
T → X
Y → C
Encrypted message: "WIGYVMXC".

(b) Decrypt the message "WMXYVMI":

To decrypt, each letter in the ciphertext is shifted 4 places backward in the alphabet:
W → S
M → I
X → T
Y → U
V → R
M → I
I → E
Decrypted message: "SITURIE".

9. An IPv4 address is a 32-bit number. Calculate the total number of unique IPv4 addresses possible.

(a) Show the calculation for the total number of IPv4 addresses:
An IPv4 address uses 32 bits, so the total number of unique addresses is calculated as:
This represents all possible combinations of 32 bits.

(b) How many addresses are left if 10% of the total addresses are reserved for special purposes?
If 10% of the total addresses are reserved:
Rounded down, approximately 429,496,729 addresses are reserved.
The remaining addresses are:
Available addresses: 3,865,470,567.

ANSWER KEYS

TOPIC 6.1 NETWORK AS SYSTEM 6.2 FUNDAMENTAL CONCEPTS IN DATA COMMUNICATION

1	B	2	C	3	B	4	B	5	C
6	B	7	B	8	B	9	C	10	B
11	B	12	B	13	A	14	A	15	

TOPIC 6.3 NETWORKING DEVICES

1	B	2	B	3	B	4	B	5	B
6	C	7	B	8	B	9	A	10	B
11	A	12	C	13	C	14	C	15	C

TOPIC 6.4 NETWORK TOPOLOGIES

1	C	2	B	3	B	4	B	5	B
6	C	7	C	8	B	9	B	10	B
11	C	12	B	13	B	14	B	15	C

TOPIC 6.5 TRANSMISSION MODES

1	B	2	C	3	C	4	B	5	C
6	B	7	A	8	C	9	C	10	B

TOPIC 6.6 THE OSI NETWORKING MODEL

1	B	2	C	3	C	4	B	5	C
6	B	7	A	8	B	9	A	10	C

TOPIC 6.7 IPV4 AND IPV6 6.8 PROTOCOLS ANS NETWORK DEVICES

1	B	2	B	3	C	4	C	5	C
6	C	7	C	8	C	9	B	10	C

TOPIC 6.9 NETWORK SECURITY

1	B	2	C	3	B	4	C	5	D
6	B	7	B	8	C	9	B	10	B

TOPIC 6.10 TYPES OF NETWORKS

1	A	2	B	3	B	4	B	5	B
6	C	7	C	8	B	9	B	10	B

TOPIC 6.11 REAL WORLD APPLICATIONS OF COMPUTER NETWORK 6.12 STANDARD PROTOCOLS 6.13 NETWORK SECURITY MODELS

1	C	2	B	3	B	4	C	5	A
6	B	7	B	8	C	9	C	10	D

TEXTBOOK EXERCISE MCQs

1	B	2	C	3	B	4	B	5	B
6	B	7	C	8	B	9	D	10	B