UNIT 6

Introduction to Computer Networks

Student Learning Outcomes

By the end of this chapter, you will be able to:

- Understand and explain computer networks as systems, their objectives, components, and data communication among these components.
- Understand fundamental concepts in data communication, including sender, receiver, protocol, message, and communication medium.
- Understand key concepts related to computer networks, including networking devices, network topologies, and transmission modes.
- Understand the 7-layer OSI networking model and its related protocols.
- Understand the benefits of using computer networks, such as resource sharing and data communication.
- Understand how data is transmitted across computer networks, including packet and circuit switching, and secure communication through encapsulation.
- Understand how protocols, data, packets, and network services like DNS and DHCP function in a networked environment.
- Understand different methods of network security, their advantages, and disadvantages.
- Understand real-world applications of computer networks, including various network-based services and how they are used.
- Know standard protocols involved in TCP/IP communications.
- Know key networking terms like the 5-layer OSI networking model, packet switching, circuit switching, router, TCP/IP, IP, UDP, DNS, DHCP, host, browsers, layering, encapsulation, and various protocols involved in TCP/IP communications.
- Differentiate between components of data communication.
- Differentiate networking devices and network topologies.
- Differentiate transmission modes.
- Identify and describe different types of networks using the 7-layer OSI networking model.
- Explain how data is transmitted across networks and describe the standard protocols involved.
- Define and explain the uses of protocols, data, packets, and network services like DNS and DHCP.
- Describe different methods of network security and their advantages and disadvantages.

Introduction

In today's interconnected world, computer networks play a vital role in the functioning of societies and businesses. This chapter aims to provide a comprehensive understanding of computer networks as systems, including their components, objectives, and real-world applications.

6.1 Network as a System

A computer network is a system of linked devices and computers that may exchange data and operate together. Networks can range from small, Local Area Network (LANs, Local Area Networks) to large area network, WANs, including the Internet. Networks are arranged of various elements that work together to facilitate communication depicted in Figure 6.1.

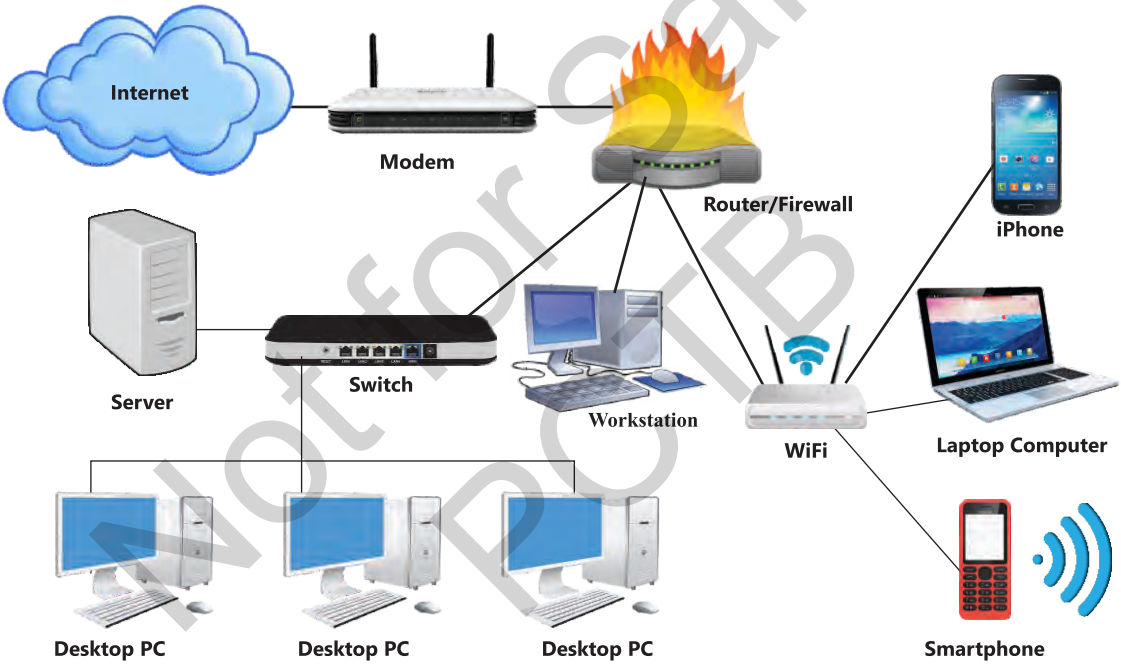
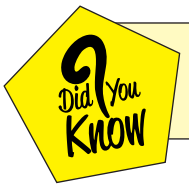


Figure 6.1: Network Diagram

The primary components include:

- **Nodes:** Devices that are connected to the network, such as computers, smartphones, and printers.
- **Links:** The connections between nodes, which can be wired (like Ethernet cables) or wireless (like Wi-Fi).
- **Switches:** Devices that connect multiple nodes within a network to forward data.
- **Routers:** Devices that connect different networks and direct data packets between them.



The Internet is the largest network, connecting all the networks worldwide!

- **Example of Using Switches**
- Imagine a file transfer in an office network. You send a file from your computer to a colleague's computer in another room.
- The file is split into packets, and each packet has the destination MAC address (your colleague's computer).
- The packets are sent to a network switch.
- The switch examines the Media Access Control address and forwards the packets only to the port where your colleague's computer is connected.
- Once all packets are received, your colleague's computer reassembles them into the original file.

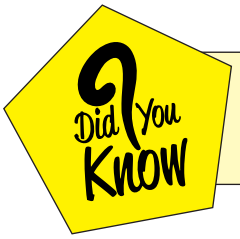
Example: Air Travel System
Think of sending people via air travel. Here's how it relates:

- When traveling, passengers (data) might be split into groups (packets) and assigned different flights (paths). In packet switching each group has a ticket with the final destination (IP address).
- These groups might take different routes, through various airports (routers), to reach the final destination.

6.1.1 Objectives of Computer Networks

The primary objective of computer network is to enable resource sharing, data communication and collaboration:

1. **Resource Sharing:** Computer networks allow devices to share resources, such as printers and storage, reducing costs and improving efficiency. **Example:** In an office network, multiple computers can share a single printer, reducing the need for multiple printers.
2. **Data Communication:** Networks facilitate data transfer, enabling communication through emails, instant messaging, and video conferencing. Example: Employees in different locations can collaborate through video conferencing tools like Zoom or Microsoft Teams.
3. **Connectivity and Collaboration:** Networks connect devices, allowing for remote access and collaboration, improving productivity and flexibility. Example: A team can work on a shared document in real-time using cloud-based services like Google Drive.



The World Wide Web (WWW) was invented by Tim Berners-Lee in 1989, revolutionizing how we access and share information.

6.2 Fundamental Concepts in Data Communication

Data communication involves the exchange of data between a sender and a receiver through a communication medium. Key components include the sender, receiver, message, protocol, and medium.

6.2.1 Components of Data Communication

It comprises of five basic components:

1. **Sender:** The device that sends the data. **Example:** A computer sending an email.
2. **Receiver:** The device that receives the data. **Example:** A smartphone receiving the email.
3. **Message:** The data being communicated. **Example:** The content of the email.
4. **Protocol:** A set of rules governing data communication. Example: The HTTP protocol used for web communications.
5. **Medium:** The physical or wireless path through which data travels. **Example**: Ethernet cable or Wi-Fi.

6.3 Networking Devices

Networking devices include hubs, switches, routers, and access points are responsible for the management and direction of network traffic.

6.3.1 Switch

Switch is a network device that connects multiple network devices such as computers, printers, and servers, within a network and allows these devices to communicate with each other efficiently. Switches play an important role in modern networks by efficiently managing data traffic and ensuring that information reaches the correct device.

How Does a Switch Work?

A switch is used at the Data Link layer which is called the Layer 2of the OSI model (Section 6.6). It uses hardware address of a device called Media Access Control (MAC)addresses to forward data to the correct device. When a data packet reaches at the switch, it reads the destination MAC address and sends the packet only to the device with that address, rather than broadcasting it to all devices.

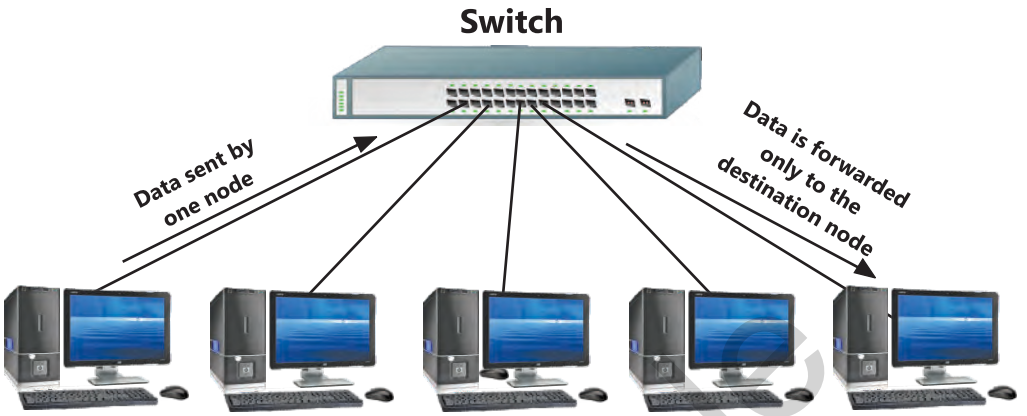


Figure 6.3: A network switch connecting multiple devices.

Tidbits

First time, switch forwards or broadcast data to all connected devices. Once it has learned address of devices, it starts sending data to exact destination.

Did You Know

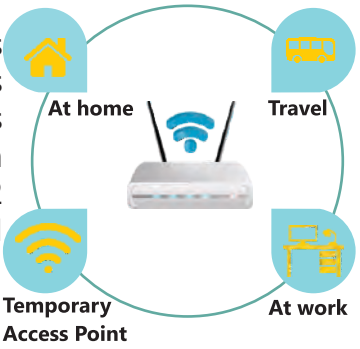
A switch is like a smart traffic conductor that directs data traffic only to the intended destination, making the network faster and more efficient.

Did you know that your home router often includes a switch and a wireless access point? This allows you to connect multiple devices both wired and wirelessly!

Tidbits

6.3.2 Router

A router is a networking device that interconnects networks or allows devices to connect to it. It directs data packets between different networks. Think of it as a traffic director on the internet, making sure that data gets from one place to another efficiently. Figure 6.2 illustrates how a mobile internet connection (via SIM card) integrates with a home network. Alternatively, an Ethernet cable can be used to obtain internet access and distribute it among home devices. In enterprise environments, different types of routers are employed, as depicted in Figure 6.2.



Mobile Wi-Fi Router

Figure 6.2: A typical home router

Did You Know

SIM stands for Subscriber Identity Module.

A SIM card is a small card inserted into a mobile device that contains unique information to identify and authenticate the subscriber on a mobile network. It allows the device to connect to the network, make calls, send messages, and access Internet.

How Does a Router Work?

Packets: Each packet contains part of the data and the address of the destination. The main job of router is to find the best path for each data packet to deliver its destination.

Did You Know

Routers use something called a routing table to decide the best path for data packets. This table lists the possible paths and helps the router make efficient decisions!

Class activity

Human Network Activity: Create a simple network using the students in the class. Assign roles like computer, router, and data packet. Use strings to represent Ethernet cables and have students pass a ball (representing data) along the strings to simulate how a router directs data.

To keep your network running smoothly, always use high-quality Ethernet cables and ensure your switch is placed in a cool, ventilated area to prevent overheating.

Tidbits

6.3.3 Access Point

An **Access Point (AP)** is a networking device that facilitates the connection of wireless devices to a wired network. It works as a link between your computers and smartphones or any other wireless device and the internet.

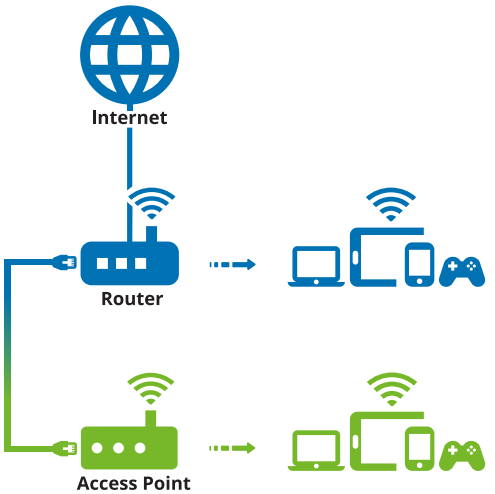


Figure 6.4: A typical Access Point

How Does an Access Point Work?

An Access Point works by receiving data from the wired network and transmitting it wirelessly to your devices. It also receives data from your wireless devices and sends it to the wired network.

Did You Know

Access Points use radio waves to transmit data, similar to how your favorite radio station broadcasts music!

Class activity

Create a human network with students. Assign roles such as Access Point, Router, and Devices. Use ropes to represent connections. Show how data moves from the Access Point to the Router and then to another network.

Did You Know

Did you know that modern Access Points can connect hundreds of devices simultaneously, making them perfect for schools, offices, and even stadiums?

Tidbits

When setting up an Access Point, place it in a central location to ensure the best coverage and signal strength for all your devices!

6.4 Network Topologies

Network topologies are methods used to define the arrangement of different devices in a computer network, where each device is called a node. The reliability and performance of a network are impacted by the way its devices are linked.

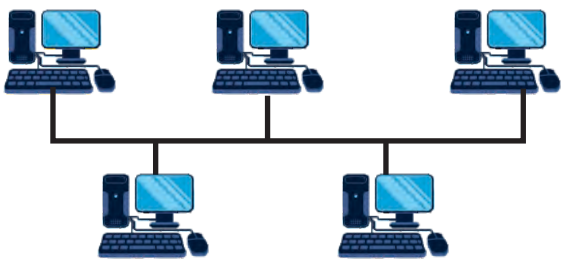


Figure 6.5: Bus Topology

6.4.1 Bus Topology

In a Bus topology, all devices share a single communication line called a bus. Each device is connected to this central cable.

Example: Imagine a chalkboard in a classroom where every student can see the notes written by the teacher. Here, the chalkboard represents the shared communication line.

Did You Know

Bus topology is easy to set up but if the main cable fails, the whole network goes down!

6.4.2 Star Topology

In a star topology each node in network communicates with the others via a central switch or hub. The hub works as a data flow repeater.

Example: Think of a school principal's office connected to all classrooms through intercoms. The principal's office is the hub, and the classrooms are the nodes.

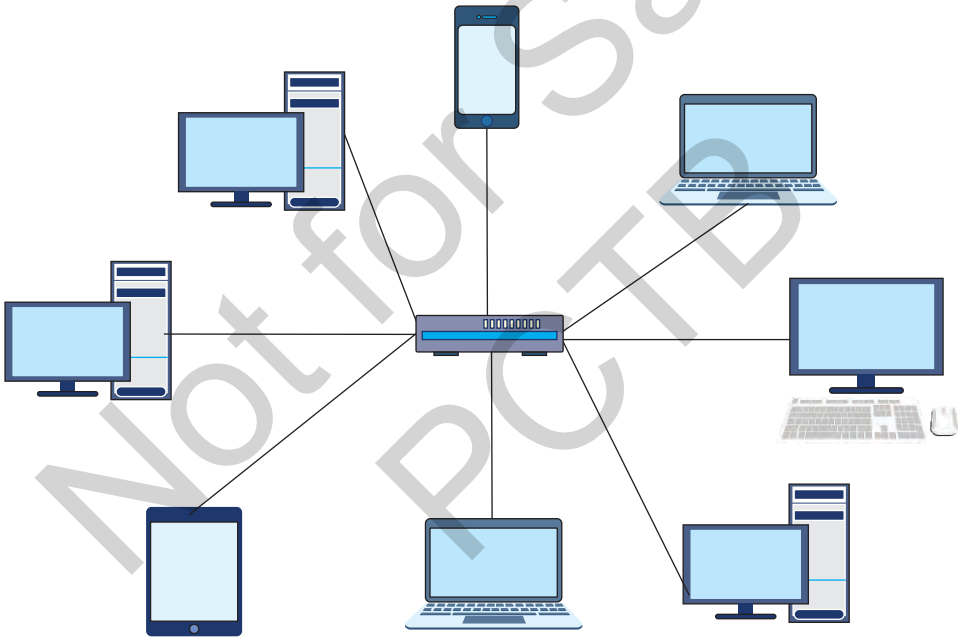


Figure 6.6: Star Topology

Class activity

Create a star topology model using strings and paper cups to simulate the connections between a central switch and peripheral nodes.

Did You Know

Hub is a networking device used to connect multiple computing devices in LAN-It always broadcasts data.

6.4.3 Ring Topology

In a Ring topology, each device is connected in a circular pathway with other devices. Data travels in one direction, passing through each device.

Example: Consider a relay race where each runner passes the baton to the next runner in a circle until it reaches the starting point again.

Figure 6.7 Ring Topology

Ring topology can handle high traffic, but if one connection fails, the whole network is affected. Then 2-way ring can solve this issue to some extent.

Tidbits

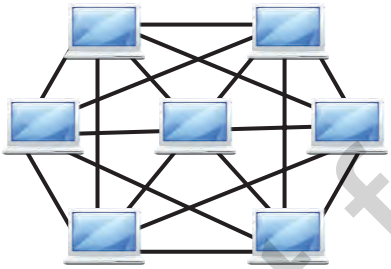


Figure 6.8: Mesh Topology

6.4.4 Mesh Topology

In a Mesh topology, each device is connected to every other device. This provides high redundancy and reliability.

Example: Imagine a city where every house is directly connected to every other house by roads. If one road is blocked, there are multiple alternative routes.

Did You Know

Mesh topology is very reliable because if one link fails, data can be rerouted through other links.

Class activity

Draw your own network diagram using one of the topologies and explain how data travels from one device to another.

6.5 Transmission Modes

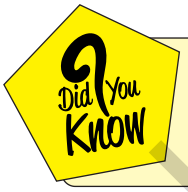
Network communication modes describe how data is transmitted between devices. There are three primary modes: Simplex, Half-Duplex, and Full-Duplex as shown in Figure 6.13. Let's explore each mode with examples and real-life analogies!

6.5.1 Simplex Communication

In Simplex communication, data transmission is unidirectional, meaning it flows in only one direction. A advice can either send or review data in this communication.

Figure 6.9: Simplex Communication

Example: Keyboard to computer is an example of simplex communication.



In Simplex communication, the direction of data flow is fixed, making it useful for applications where only one-way communication is needed!

6.5.2 Half-Duplex Communication

In Half-Duplex communication, data transmission can occur in both directions, but not simultaneously. One device must wait for the other to finish transmitting before it can start.

Figure 6.10: Half-Duplex Communication

Class activity

Use walkie-talkies or toy telephones to demonstrate Half-Duplex communication. Let students take turns speaking and listening.

6.5.3 Full-Duplex Communication

Full-duplex communication allows for simultaneous data delivery in both directions. Both devices may transmit and receive data simultaneously at the same time.

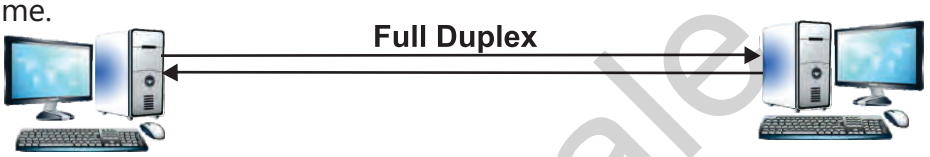


Figure 6.11: Full-Duplex Communication

Example:

Telephone conversations are an example of Full-Duplex communication. Both people can talk and listen at the same time without waiting for their turn.

Tidbits

Full-Duplex communication allows for more efficient data transmission, making it ideal for modern communication systems like internet browsing and video calls !

Did You Know

The first telephones were Half-Duplex, where only one person could speak at a time. Modern phones use Full-Duplex, allowing both people to talk and listen simultaneously!

Class activity

Draw a diagram of each communication mode and label the direction of data flow. Explain your diagrams to the class.

Did You Know

The first message sent over the ARPANET, the precursor to the internet, was "LO." It was meant to be "LOGIN," but the system crashed after the first two letters.

6.6 The OSI Networking Model

The Open Systems Interconnection (OSI) Model is a framework used to understand how different networking protocols interact. It has 7 layers, each with a specific function. Let's explore these layers with examples and relate them to daily life.

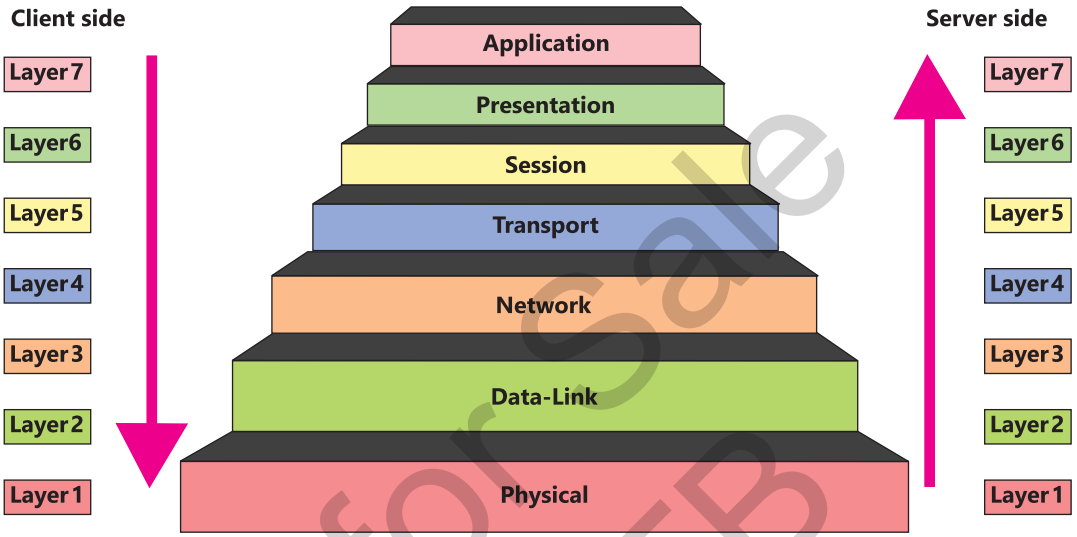
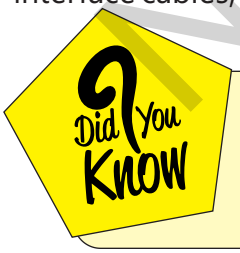


Figure 6.12: OSI Model

Layer 1: Physical Layer

The Physical Layer is liable for the actual connection between devices. The process of sending unprocessed data bits via a physical medium is the focus here.

Example: Imagine the hardware that connects computers, like a Network interface cables, repeaters, hubs and connectors.



The Physical Layer includes everything from the cables to the voltage levels used to transmit data!

Layer 2: Data Link Layer

Error detection and correction, as well as node-to-node data transport, are handled by the Data Link Layer. It ensures error-free data transmission from the Physical Layer.

Example: Think of the Data Link Layer as traffic lights at intersections, which manage the flow of cars (data) and prevent collisions.

Class activity

Draw a simple network with devices and label the physical connections and data link layer responsibilities.

Layer 3: Network Layer

The Network Layer is responsible for data transfer between different networks. It determines the best path for data to travel from the source to the destination.

Example: Imagine a GPS system finding the best route for you to travel from home to school.

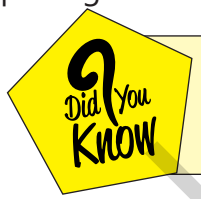
Tidbits

The Network Layer uses IP addresses to route data between networks!

Layer 4: Transport Layer

The Transport Layer ensures that data is transferred from one process rerunning on source end system to a process souring on destination end system. It manages data flow control and error checking.

Example: Think of the Transport Layer as a delivery service that ensures your package arrives safely and on time.



The Transport Layer uses protocols like Transmission Control Protocol (TCP) to ensure reliable data transfer!

Layer 5: Session Layer

The Session Layer manages sessions between applications. It establishes, maintains, and terminates connections between devices.

Example: Imagine a phone call where the session layer sets up the call, keeps it connected, and ends it when you hang up.

Class activity

Role-play a phone call and discuss how the session is established, maintained, and terminated.

Layer 6: Presentation Layer

The Presentation Layer translates data between the application layer and the network. It formats and encrypts data to ensure it is readable by the receiving system.

Example: Think of the Presentation Layer as a translator converting a book from one language to another so that more people can read it.

The Presentation Layer handles data encryption and compression!

Layer 7: Application Layer

The Application Layer is the closest to the end user. It provides network services directly to applications, such as email, web browsing, and file transfer.

Example: Imagine the Application Layer as a waiter taking your order in a restaurant and bringing your food.

Class activity

List the applications you use daily and identify which rely on the Application Layer for network services.

6.7 Ipv4 and Ipv6

Internet Protocol (IP) addresses are unique identifiers assigned to devices connected to the Internet. There are two primary versions: IPv4 and IPv6. Let's explore the differences between them with examples and relate them to daily life.

6.7.1 Internet Protocol version 4 (IPv4)

IPv4 is the fourth version of the Internet Protocol and the most widely used today. It uses a 32-bit address scheme, allowing for approximately 4.3 billion unique addresses. To find the total number of unique IPv4 addresses, we calculate 2^{32}, which represents all possible combinations of 32 bits, i.e., 2^{32} =4,294,967,296.

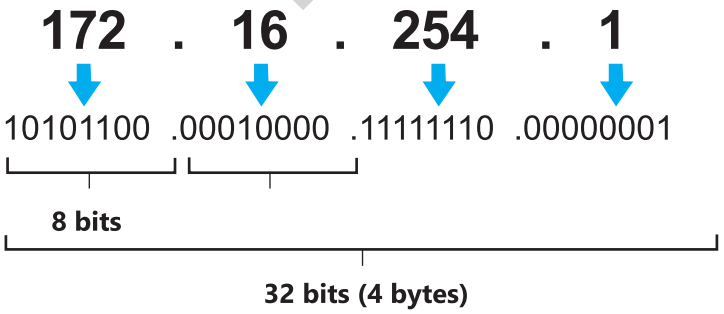
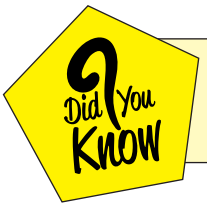


Figure 6.13: IPv4 Address Format

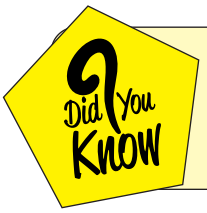


IPv4 addresses are written in four sets of decimal numbers, each ranging from 0 to 255 (e.g., 192.168.1.1).

6.7.1 Internet Protocol version 6 (IPv6)

IPv6 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.

Example: Imagine an IPv6 address like a digital fingerprint. It can provide a unique identifier not just for houses on a street, but for every grain of sand on a beach. e.g 2001 : 0000: 130 F : 0000 : 0000 : 0900 : 876A : 130B



IPv6 was developed to address the depletion of IPv4 addresses due to the rapid growth of the internet and connected devices.

6.8 Protocols and Network Services

6.8.1 Introduction to Protocols

Protocols are sets of rules that govern data communication. Common protocols include TCP/IP, HTTP, FTP and SMTP.

Example: HyperText Transfer Protocol (HTTP) is used for transferring web pages over the internet.

6.8.2 DNS and DHCP

Domain Name System (DNS)

DNS translates domain names to IP addresses, making it easier for users to access websites.

Example: When you type **www.example.com** in a browser, DNS translates it to the corresponding IP address.

Dynamic Host Configuration Protocol (DHCP)

DHCP automatically assigns IP addresses to devices on a network, simplifying network management.

Example: When a device connects to a Wi-Fi network, DHCP assigns it an IP address.

6.9 Network Security

Network security involves measures to protect data and prevent unauthorized

access to computer networks. Let's explore the importance of network security and some key concepts with examples.

6.9.1 Importance of Network Security

Network security is important for several reasons:

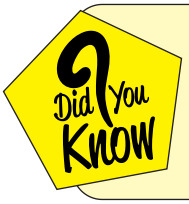
- **Data Protection:** Ensuring that sensitive information is not accessed or altered by unauthorized users.
- **Preventing Attacks:** Defending against malicious attacks that can disrupt networks and steal data.
- **Maintaining Privacy:** Safeguarding personal and confidential information from being compromised
- **Ensuring Availability:** Ensuring that network resources are available and accessible to authorized users.

6.9.2 Key Concepts in Network Security

Firewalls

Firewalls are security systems that monitor and control incoming and outgoing network traffic based on predetermined security rules.

Figure 6.14: Firewall Concept



Firewalls act as barriers between trusted internal networks and untrusted external networks, like a security checkpoint.

Encryption

Encryption transforms data into a secure format that can only be read or understood by authorized parties with the correct decryption key.

Decryption is the process of converting the encrypted data back to its original form.

Example:

Plain Text: Hello, World!

Encrypted Text (using a simple shift cipher): Khoor, Zruog! where each letter in the plaintext is replaced by the letter that is 3 positions down the alphabet.

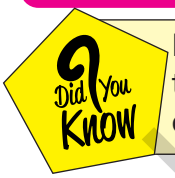
Decryption: Converting "Khoor, Zruog!" back to "Hello, World!" using the same shift cipher in reverse.

Ciphertext Exchanged Between Countries

Countries often exchange sensitive information securely using encryption. The encrypted data, known as ciphertext, can only be read by the intended recipient who has the decryption key. This ensures national security and protects classified information from being intercepted and read by unauthorized parties.

Class activity

Encrypt a simple message using a shift cipher with a key of 3 (each letter is shifted by 3 places in the alphabet). Then, exchange messages with a classmate and decrypt each other's messages.



During World War II, the Allies used the Enigma machine to encrypt their communications. The ability to decrypt German Enigma-encrypted messages significantly contributed to their victory.

Use strong encryption algorithms to protect sensitive information, making it unreadable to unauthorized users.

Tidbits

Passwords and Authentication

Passwords and authentication methods ensure that only authorized users can access network resources.

Class activity

Discuss the importance of strong passwords and practice creating secure passwords using a password generator.

6.9.3 Common Threats to Network Security

- **Malware:** Malicious software such as viruses, worms, and ransomware that can damage or steal data.
- **Phishing:** Attempts to trick users into revealing sensitive information

through deceptive emails or websites.

- **Denial of Service (DoS) Attacks:** Overwhelming a network with traffic to disrupt its normal operation and make it unavailable.
- **Man-in-the-Middle Attacks:** Intercepting communication between two parties to steal information or alter messages.

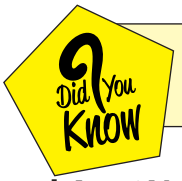
6.10 Types of Networks

Networks are classified based on their size, range, and purpose. Let's explore some common types of networks and understand how they work.

6.10.1 Personal Area Network (PAN)

Figure 6.15: Personal Area Network (PAN)

A PAN is a small network used for communication between personal devices, such as smartphones, tablets, and laptops, within a short range. **Example:** Bluetooth connections between a smartphone and a wireless headset form a PAN.



The range of a PAN is typically a few meters, perfect for personal device communication.

Local Area Network (LAN)

A LAN is a network that connects computers and devices within a limited area, such as a home, school, or office building.

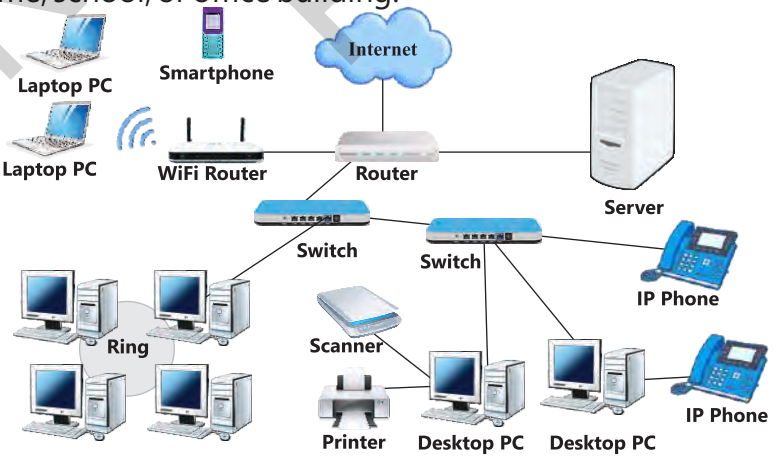


Figure 6.16: Local Area Network (LAN)

Example: The computer network in your school that connects all the computers in the lab is a LAN.

Class activity

Draw a diagram of your school's computer network, labeling the different devices and connections.

6.10.1 Metropolitan Area Network (MAN)

A MAN is a network that spans a city or a large campus, connecting multiple LANs together.

Example: The network that connects various branches of a university across a city is a MAN.

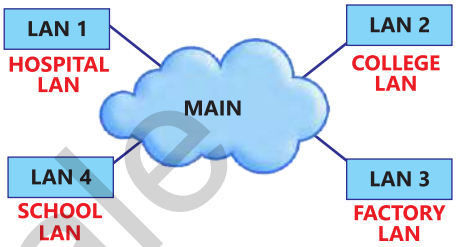
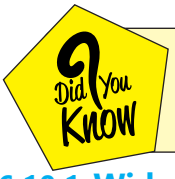


Figure 6.17: Metropolitan Area Network (MAN)



A MAN can cover an area of up to 50 kilometers, making it ideal for city-wide connectivity.

6.10.1 Wide Area Network (WAN)

A WAN covers a large geographical area, connecting multiple LANs and MANs. The internet is the largest example of a WAN.

Example: The network that connects different branch offices of a multinational company across countries is a WAN

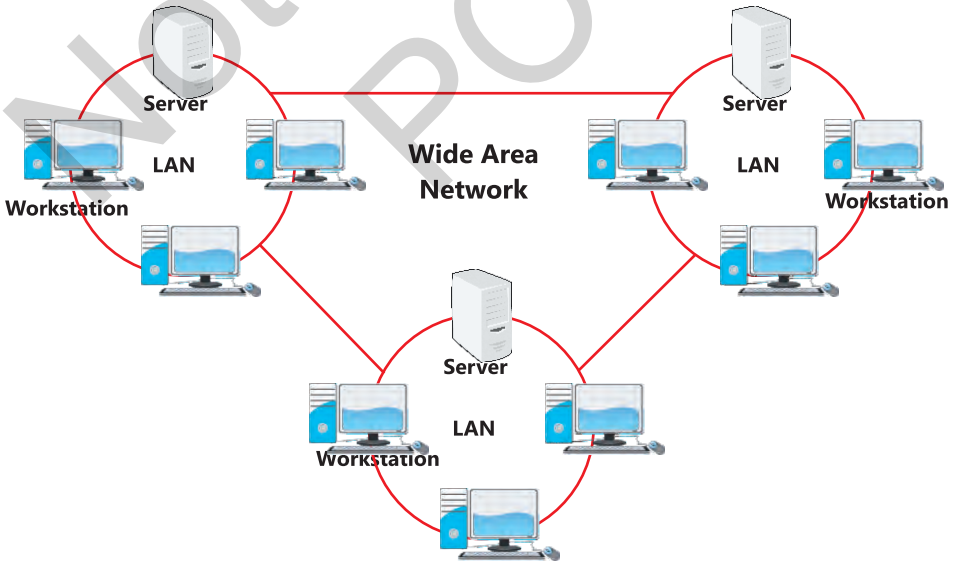


Figure 6.18: Wide Area Network (WAN)

Use a Virtual Private Network (VPN) to securely connect to a WAN and protect your data when accessing public networks.

Tidbits

6.10.1 Campus Area Network (CAN)

A CAN is a network that connects multiple LANs within a limited geographical area, such as a university campus or a business park.

Example: The network that connects various departments and buildings within a university is a CAN.

Understanding the different types of networks helps us comprehend how data travels from one device to another, whether within a single room or across the globe. Each network type serves a specific purpose and is designed to handle various ranges and sizes.

6.11 Real-World Applications of Computer Networks

6.11.1 Business

In business, networks enable efficient communication, resource sharing, and data management.

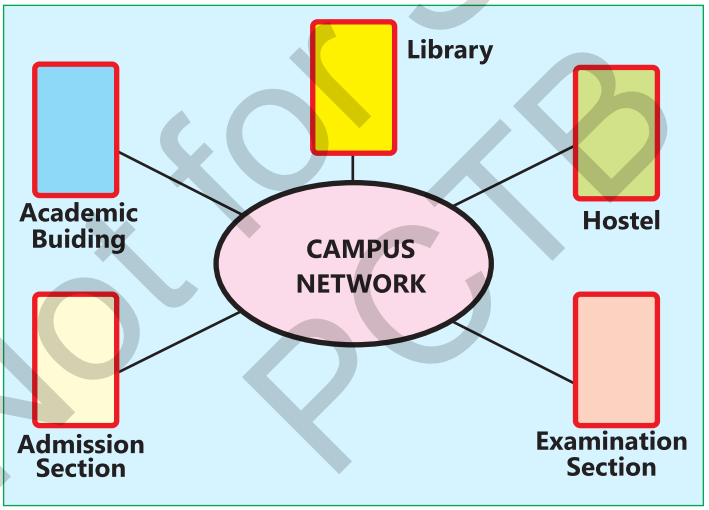


Figure 6.19: Campus Area Network (CAN)

Example: Companies use intranets to share information and resources securely within the organization.

6.11.1 Education

Educational institutions use networks to provide online learning platforms, virtual classrooms, and access to educational resources.

Example: Universities use Learning Management Systems (LMS) like Blackboard and Moodie to deliver course content and assessments.

6.11.2 Healthcare

Healthcare networks facilitate the sharing of patient information, telemedicine,

and access to medical databases.

Example: Hospitals use Electronic Health Records (EHR) systems to store and retrieve patient data efficiently.

6.12 Standard Protocols in TCP/IP Communications

6.12.1 Introduction to TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the fundamental suite of protocols for internet communication.

6.12.2 Key Protocols

- **Transmission Control Protocol (TCP):** Ensures reliable data transfer.
- **Internet Protocol (IP):** Handles addressing and routing of data packets.
- **User Datagram Protocol (UDP):** Provides faster, but less reliable, data transfer.
- **Domain Name System (DNS):** Translates domain names to IP addresses.
- **Dynamic Host Configuration Protocol (DHCP):** Automatically assigns IP addresses.

6.13 Network Security Methods

6.13.1 Firewalls

Monitor and control incoming and outgoing network traffic.

6.13.2 Encryption

Protects data by converting it into a secure format.

6.13.3 Antivirus Software

Detects and removes malicious software.

Example: A combination of firewalls, encryption, and antivirus software provides robust network security.

Class activity

Have students discuss the advantages and disadvantages of different network security methods.

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 (MCQs)

1. 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
2. Which device is used to connect multiple networks and direct data packets between them?
   (a) Switch (b) Hub (c) Router (d) Modem
3. Which layer of the OSI 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
4. 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
5. Which method of data transmission uses a dedicated communication path?
   (a) Packet Switching (b) Circuit Switching
   (c) Full-Duplex (d) Half-Duplex
6. 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
7. Which protocol is used for reliable data transfer in the TCP/IP model?
   (a) HTTP (b) FTP (c) TCP (d) UDP
8. 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
9. Which network topology connects all devices to a central hub?
   (a) Ring (b) Mesh (c) Bus (d) Star
10. 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

1. Define data communication and list its key components.
2. Explain the role of routers in a computer network.
3. What are the main functions of the Network Layer in the OSI model?
4. Describe the difference between packet switching and circuit switching.
5. What is the purpose of the Dynamic Host Configuration Protocol (DHCP)?
6. How does encapsulation ensure secure communication in a network?
7. Differentiate between TCP and UDP in terms of data transfer reliability.
8. Explain the importance of encryption in network security.
9. What are the advantages of using a star topology in a network?
10. How do firewalls contribute to network security?

Long Questions

1. Discuss the objectives of computer networks and provide examples of how they facilitate resource sharing and data communication.
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.
3. Describe how data is transmitted across computer networks using packet switching and circuit switching.
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.
5. Evaluate different methods of network security, including firewalls, encryption, and antivirus software.
6. Describe real-world applications of computer networks in business, education, and healthcare.
7. Compare and contrast the different types of network topologies (star, ring, bus, and mesh).
8. Consider a shift cipher with a shift amount of 4.
   (a) Encrypt the message "SECURITY".
   (b) Decrypt the message "WMXYVMI".
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.
   (b) How many addresses are left if 10% of the total addresses are reserved for special purposes?