Unit 6

INTRODUCTION TO COMPUTER NETWORK

Introduction

In today's interconnected world, computer networks play a vital role in the functioning of societies and businesses.

Network as a System

A computer network is a system of linked devices and computers that may exchange data and operate together.

Primary Components of Network

• **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.

Objectives of Computer Networks

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.

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.

Components of Data Communication

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.

Network Devices

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

1. **Switches:** Switch is a network device that connects multiple network devices such as computers, printers, and servers within a network. Switches 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. 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.

2. **Routers:** Devices that connect different networks and direct data packets between them.

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.

3. **Access Point**

An Access Point (AP) is a networking device that facilitates the connection of wireless devices to a wired network.

How Does an Access Point Work?

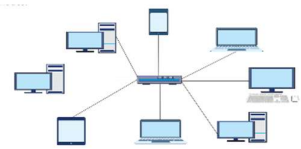
An Access Point works by receiving data from the wired network and transmitting it wirelessly to your devices. It also receives data from your wireless devices and sends it to the wired network.

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.

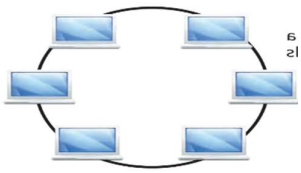
Bus Topology

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



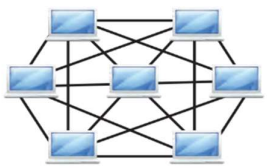
Star Topology

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.



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.



Mesh Topology

In a Mesh topology, each device is connected to every other device.

Transmission Modes

Network communication modes describe how data is transmitted between devices. There are three primary modes: Simplex, Half-Duplex, and Full-Duplex.

Simplex communication

In Simplex communication, data transmission is unidirectional, meaning it flows in only one direction. A device can either send or review data in this communication. Keyboard to computer is an example of simplex communication.

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. Walkie-talkies is an example of Half-Duplex communication.

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. Telephone conversations are an example of Full-Duplex communication.

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.

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.

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.

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.

Layer 4: Transport Layer

The Transport Layer ensures that data is transferred to destination. It manages data flow control and error checking.

Layer 5: Session Layer

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

Layer 6: Presentation Layer

The Presentation Layer translates data between the application layer and the network.

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.

IP Addresses

Internet Protocol (IP) addresses are unique identifiers assigned to devices connected to the Internet. There are two primary versions: IPv4 and IPv6.

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)

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.

Protocols and Network Services

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.

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.

Network Security

Network security involves measures to protect data and prevent unauthorized access to computer networks.

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.

Types of Networks

Networks are classified based on their size, range, and purpose.

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.

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.

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

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

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.

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.

Real-World Applications of Computer Networks

Business

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

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

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.

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.

Standard Protocols in TCP/IP Communications

Introduction to TCP/IP

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

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.

Network Security Methods

Firewalls

Monitor and control incoming and outgoing network traffic.

Encryption

Protects data by converting it into a secure format.

Antivirus Software

Detects and removes malicious software.

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