black N White

NAME	
ROLL NUMBER	
SEMESTER	**II**
COURSE CODE	**DCA6206**
COURSE NAME	**COMPUTER NETWORKS & PROTOCOLS**

SET-I

Q.1) What is a Computer Network? Explain the different types of computer networks with suitable examples.

Answer . :-

A **computer network** is a collection of interconnected computing devices that are able to communicate with each other and share resources such as files, software, printers, and internet access. These connections can be established using physical wires (like Ethernet cables) or wireless methods (such as Wi-Fi or Bluetooth). The main objective of a computer network is to enable resource sharing, communication, and data exchange between devices in a reliable and efficient manner.

Computer networks are classified based on their scale, architecture, and purpose. The major types include LAN, MAN, WAN, PAN, and CAN. Each type serves different use cases and has unique characteristics.

1. Local Area Network (LAN):

A Local Area Network is a small network that connects computers and other devices within a limited area such as a home, school, or office. It typically uses Ethernet cables or Wi-Fi for connectivity.

- **Features:**
  - High speed (often 100 Mbps to 1 Gbps)
  - Low latency
  - Private ownership and management
- **Example:** A group of computers connected in a computer lab or office using a central switch or router.

2. Metropolitan Area Network (MAN):

A Metropolitan Area Network covers a larger area than a LAN, usually spanning an entire city or a large campus. It connects multiple LANs and is usually managed by a single organization or service provider.

- **Features:**
  - Medium-range coverage (up to 50 km)
  - Can use fiber optics or leased lines
  - Ideal for city-wide network connections
- **Example:** A government office connecting different departments located throughout a city.

3. Wide Area Network (WAN):

WANs cover vast geographical areas and are used to connect devices and LANs across cities, countries, or continents. They often rely on public networks, like telephone lines or satellites.

- **Features:**
  - Slower compared to LAN due to long distances
  - Use of routers, modems, and leased lines
  - Typically managed by multiple organizations
- **Example:** The Internet is the largest example of a WAN, connecting billions of devices globally.

4. Personal Area Network (PAN):

A Personal Area Network is used for connecting devices within the range of an individual user, usually within 10 meters.

- **Features:**
  - Very short range
  - Wireless technologies like Bluetooth, infrared, etc.
- **Example:** A mobile phone connected to a Bluetooth headset or smartwatch.

5. Campus Area Network (CAN):

A CAN connects multiple LANs within a campus or a group of buildings belonging to a single organization.

- **Features:**
  - Larger than LAN but smaller than MAN
  - Centralized network management
- **Example:** A university network connecting all departments and libraries.

Conclusion:

Computer networks are essential for communication and data sharing in today's digital world. Depending on the size and purpose, they are categorized into LAN, MAN, WAN, PAN, and CAN — each designed to meet specific connectivity needs.

ho toh zaroor batayein.

Q.2) Describe the OSI reference model in detail, explaining the functions of each layer.

Answer .:-

The **OSI (Open Systems Interconnection) reference model** is a conceptual framework developed by the **International Organization for Standardization (ISO)** that standardizes the functions of a telecommunication or computing system into **seven distinct layers**. It helps different systems communicate using standardized protocols and improves understanding of network architecture.

Each layer performs a specific role and interacts directly only with the layers immediately above and below it.

◇ **1. Physical Layer (Layer 1):**

- **Function:** This is the lowest layer of the OSI model. It deals with the **transmission of raw binary data (0s and 1s)** over a physical medium such as cables, radio frequencies, or fiber optics.
- **Responsibilities:**
  - Defines hardware components like cables, switches, and connectors
  - Manages bit rate and transmission mode (simplex, half-duplex, full-duplex)
- **Example Devices:** Hubs, cables, network interface cards (NICs)

◇ **2. Data Link Layer (Layer 2):**

- **Function:** It ensures **error-free transmission of data** between two devices on the same network. It groups bits into frames and handles **MAC addressing**.
- **Responsibilities:**
  - Error detection and correction

- Flow control
- Framing and physical addressing

- **Example Devices:** Switches, bridges

◇ **3. Network Layer (Layer 3):**

- **Function:** This layer is responsible for **routing data packets** across multiple networks. It determines the **best path** for data to travel.
- **Responsibilities:**
  - Logical addressing (IP addresses)
  - Packet forwarding and routing
  - Congestion control
- **Example Protocols:** IP, ICMP, IPsec

◇ **4. Transport Layer (Layer 4):**

- **Function:** It ensures **end-to-end communication** between devices. It provides **reliable or unreliable** delivery depending on the protocol used.
- **Responsibilities:**
  - Segmentation and reassembly of data
  - Error recovery and retransmission
  - Flow control
- **Example Protocols:** TCP (reliable), UDP (unreliable

◇ **5. Session Layer (Layer 5):**

- **Function:** It manages **sessions** (or conversations) between applications.
- **Responsibilities:**
  - Establishing, maintaining, and terminating sessions
  - Synchronization and dialog control
- **Example:** Remote Procedure Call (RPC), NetBIOS

◇ **6. Presentation Layer (Layer 6):**

- **Function:** It handles the **syntax and semantics of the information** exchanged between two systems. It acts as a translator.
- **Responsibilities:**
  - Data encryption and decryption
  - Data compression
  - Format translation (e.g., from ASCII to EBCDIC)
- **Example Formats:** JPEG, MP3, MPEG, SSL/TLS

◇ **7. Application Layer (Layer 7):**

- **Function:** This is the topmost layer where **users interact with the network** through applications.

- **Responsibilities:**
  - Network services like file transfer, email, and web browsing
  - Identifying communication partners
  - Resource availability checking
- **Example Protocols:** HTTP, FTP, SMTP, DNS

The OSI model provides a standardized approach for network communication by dividing it into seven layers. Each layer performs a specific role in data transmission, from physical hardware to end-user applications. Understanding these layers helps in diagnosing network issues and designing efficient communication systems.

Q.3 Define Transmission Media. Explain any four types of guided transmission media.

Answer .:-

Definition of Transmission Media:

Transmission media refers to the physical pathway through which data is transmitted from one device to another in a network. It serves as the carrier for signals in the form of electrical pulses, light waves, or electromagnetic waves.

Transmission media are broadly categorized into two types:

1. **Guided (Wired) Media:** Data signals are guided through a solid medium like cables.
2. **Unguided (Wireless) Media:** Data is transmitted through the air or vacuum using electromagnetic waves.

This answer focuses on **guided transmission media**, where signals are confined within a physical path.

Types of Guided Transmission Media:

Here are four commonly used guided transmission media:

1. Twisted Pair Cable:

- **Description:** It consists of pairs of insulated copper wires twisted together. The twisting reduces electromagnetic interference from external sources and crosstalk from adjacent pairs.
- **Types:**
  - **Unshielded Twisted Pair (UTP):** Commonly used in LANs and telephone networks.
  - **Shielded Twisted Pair (STP):** Has an extra shielding to reduce interference.

- **Speed & Distance:** Supports up to 1 Gbps over short distances (up to 100 meters).
- **Applications:** Used in Ethernet networks, telephone lines.

2. Coaxial Cable:

- **Description:** It has a central copper conductor surrounded by insulation, a metallic shield, and an outer insulating layer. The shielding protects signals from interference and allows better performance than twisted pair cables.
- **Speed & Distance:** Supports up to 10 Mbps to 100 Mbps, suitable for distances up to a few kilometers.
- **Applications:** Used in cable TV, CCTV systems, and early Ethernet (10Base2 and 10Base5).

3. Optical Fiber Cable:

- **Description:** Uses glass or plastic fibers to transmit data as light pulses. It offers high bandwidth and long-distance transmission with minimal signal loss.
- **Types:**
    - **Single-mode fiber:** For long-distance, high-speed communication.
    - **Multi-mode fiber:** For shorter distances with multiple light paths.
- **Speed & Distance:** Can support up to terabits per second over hundreds of kilometers.
- **Applications:** Used in backbone networks, internet infrastructure, and telecom.

4. Stripline and Microstrip Lines (Used in PCBs):

- **Description:** These are forms of guided media embedded within printed circuit boards (PCBs). A **stripline** runs between two ground planes, while a **microstrip** runs over a single ground plane.
- **Speed & Distance:** Suitable for high-frequency signals over very short distances (inside electronic devices).
- **Applications:** Used in high-speed digital circuits, routers, and computers.

Guided transmission media provide a reliable path for data transmission with physical control over the signal flow. The choice among twisted pair, coaxial, fiber optics, or specialized PCB lines depends on factors like bandwidth needs, distance, cost, and environment. These media play a crucial role in the design and performance of modern communication networks.

SET-II

Q.4) Differentiate between LAN, MAN, and WAN with suitable examples. Also, explain the concept of Network Topology.

Answer .:-

Computer networks are categorized based on their size and the area they cover. The three main types are:

1. Local Area Network (LAN):

- **Definition:** LAN connects computers and devices within a **limited area** like a room, building, or campus.
- **Characteristics:**
  - Covers a small area (typically up to a few kilometers)
  - High data transfer speeds (up to 1 Gbps or more)
  - Low cost and easy maintenance
  - Usually privately owned
- **Example:** A network connecting all computers in a college computer lab or office building.

2. Metropolitan Area Network (MAN):

- **Definition:** MAN spans a **larger area than a LAN**, typically covering a city or a large campus, and connects multiple LANs.
- **Characteristics:**
  - Medium-range network (up to 50 km)
  - Moderate speed and cost
  - May be owned by a single organization or a service provider
- **Example:** A university network connecting different campus buildings across a city.

3. Wide Area Network (WAN):

- **Definition:** WAN covers a **very large geographical area**, often a country or continent, and connects multiple LANs and MANs.
- **Characteristics:**
  - Large-scale network (global range)
  - Lower speeds due to long distances
  - Higher setup and maintenance cost
  - Usually owned by multiple organizations
- **Example:** The **Internet** is the largest example of a WAN.

Tabular Comparison:

Feature	LAN	MAN	WAN
Coverage Area	Small (building or campus)	Medium (city or metro region)	Large (country or world)
Ownership	Private	Private or public	Public or shared
Speed	High	Moderate	Lower than LAN/MAN
Cost	Low	Moderate	High
Example	Office Network	City-wide University Network	Internet or Bank's global network

Concept of Network Topology:

Network topology refers to the **physical or logical arrangement** of devices (nodes) and how they are connected in a network. It defines the structure and layout of communication paths.

Types of Network Topology:

1. **Bus Topology:**
   - All devices are connected to a single central cable (backbone).
   - Simple and cost-effective but hard to troubleshoot.
2. **Star Topology:**
   - All devices are connected to a central hub or switch.
   - Easy to manage and scalable.
3. **Ring Topology:**
   - Devices are connected in a circular manner.
   - Data travels in one direction; failure of one device can affect the entire network.
4. **Mesh Topology:**
   - Every device is connected to every other device.
   - Provides redundancy and reliability.
5. **Tree Topology:**
   - Combination of star and bus topology.
   - Hierarchical and suitable for large networks.
6. **Hybrid Topology:**
   - Mix of two or more topologies.
   - Offers flexibility and efficiency.

LAN, MAN, and WAN differ in terms of range, speed, and cost, and are used for different scales of networking. Network topology defines how devices are connected and plays a key role in network performance, fault tolerance, and management.

Q.5) Explain the TCP/IP model. How does it differ from the OSI model?

Answer .:-

TCP/IP Model:

The **TCP/IP (Transmission Control Protocol/Internet Protocol)** model is the foundation of communication on the internet. It is a **four-layered** model that defines how data is transmitted across networks and the internet. The TCP/IP model is simpler and more practical compared to the OSI model. It was developed based on standard protocols used in the internet and computer networks.

Four Layers of the TCP/IP Model:

1. **Application Layer (Layer 4):**
    - **Function:** This layer is responsible for user-level interactions and application communication. It provides end-user services like web browsing, email, and file transfer.
    - **Protocols:** HTTP, FTP, SMTP, DNS, Telnet.
    - **Example:** Web browsers, email clients.
2. **Transport Layer (Layer 3):**
    - **Function:** It ensures reliable communication between devices. It handles flow control, error detection, and retransmission of lost packets.
    - **Protocols:** TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
    - **Example:** Ensures that data is sent reliably, for example, when you access a website.
3. **Internet Layer (Layer 2):**
    - **Function:** This layer is responsible for addressing, routing, and forwarding data packets. It determines the best path for the data to travel across the network.
    - **Protocols:** IP (Internet Protocol), ICMP, ARP.
    - **Example:** IP addresses (IPv4 and IPv6) used for packet routing.
4. **Network Interface Layer (Layer 1):**
    - **Function:** It handles the physical transmission of data over network hardware. This layer defines the protocols for physical transmission and how data is placed on the medium.
    - **Protocols:** Ethernet, Wi-Fi, PPP.
    - **Example:** The physical network devices like routers, switches, and cables.

Differences Between the TCP/IP Model and OSI Model:

The **TCP/IP model** and **OSI model** are both reference models used to understand network communication, but they differ in structure, layers, and protocol approach.

Aspect	TCP/IP Model	OSI Model
Number of Layers	4 (Application, Transport, Internet, Network Interface)	7 (Application, Presentation, Session, Transport, Network, Data Link, Physical)
Development	Developed to standardize Internet protocols	Developed by ISO for general networking purposes
Layer Functionality	Merged the Application, Presentation, and Session layers into one	Each layer has a distinct role for application, presentation, and session
Model Approach	Protocol-centric and practical (Real-world protocols like TCP/IP are part of this model)	Conceptual model, more theoretical
Layer Definition	Fewer layers with more integrated functions	More layers with specific functionalities for each step
Protocol Dependency	Tightly bound to TCP/IP protocols	Can be implemented with different protocols
Focus	Primarily used for Internet communication	Used for understanding network architecture

The **TCP/IP model** is a practical, streamlined model designed for internet communication and networking, combining multiple OSI layers for simplicity. It's the foundation of how the internet works. On the other hand, the **OSI model** is a more theoretical, detailed approach with seven layers, focusing on clear separation of each communication function. Both models help to understand and design network communication, with TCP/IP being more widely used in real-world implementations.

Q.6) What is an IP address? Differentiate between IPv4 and IPv6 addressing schemes .

Answer .:-

An **IP address (Internet Protocol address)** is a unique identifier assigned to each device connected to a network, enabling it to communicate with other devices over the internet or local network. It serves two primary functions:

1. **Identification:** Identifies the device on the network.
2. **Location Addressing:** Helps in determining the device's location within the network to facilitate data transmission.

IP addresses come in two major versions: **IPv4** and **IPv6**, which differ in structure and functionality.

Differences Between IPv4 and IPv6 Addressing Schemes:

Feature	IPv4	IPv6
Address Length	32-bit	128-bit
Address Format	Four sets of decimal numbers (0–255), separated by dots (e.g., 192.168.1.1)	Eight groups of hexadecimal numbers (0–FFFF), separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Number of Addresses	Approximately 4.3 billion addresses	Over 340 undecillion (3.4 × 10^38) addresses
Address Representation	Written in **dotted decimal** format	Written in **colon hexadecimal** format
Address Types	Unicast, Broadcast, Multicast	Unicast, Multicast, Anycast
Header Size	20 bytes	40 bytes
Configuration	Manual or via DHCP	Can be configured automatically via SLAAC or DHCPv6
Security	Security not built-in; relies on external	Built-in security features like IPsec support

	protocols like IPsec	
Fragmentation	Supported by routers and sending devices	Only supported by sending devices (routers do not fragment packets)
Compatibility	Widely used and supported across networks	Not fully backward compatible with IPv4; requires transition mechanisms
Example Address	192.168.0.1	2001:0db8:85a3:0000:0000:8a2e:0370:7334

Detailed Comparison:

1. **Address Length:**
   - **IPv4:** 32-bit address length, providing approximately **4.3 billion unique addresses**. This was sufficient in the early stages of the internet but has become insufficient due to the exponential growth of internet-connected devices.
   - **IPv6:** 128-bit address length, offering **over 340 undecillion addresses**. This ensures an almost unlimited number of unique addresses, solving the address shortage problem.
2. **Address Format:**
   - **IPv4:** The address is written as four decimal numbers (each between 0 and 255), separated by periods (e.g., 192.168.1.1).
   - **IPv6:** The address is written as eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
3. **Security:**
   - **IPv4:** Security is optional and typically relies on external protocols like **IPsec** to ensure secure communication.
   - **IPv6:** Security is built into the protocol, with mandatory support for **IPsec** (Internet Protocol Security), enhancing network security.
4. **Network Address Translation (NAT):**
   - **IPv4:** Due to the limited address space, **NAT** is often used to allow multiple devices within a private network to share a single public IP address.
   - **IPv6:** NAT is not necessary because of the vast number of available addresses, allowing for direct end-to-end communication.
5. **Fragmentation:**
   - **IPv4:** Fragmentation of data packets is handled by both **sending devices** and **routers**.
   - **IPv6:** Fragmentation is handled only by the **sending device**. Routers do not perform fragmentation, making the protocol more efficient.

The transition from **IPv4 to IPv6** was necessary to accommodate the growing number of devices and the need for enhanced security and performance. While IPv4 remains the dominant addressing scheme, IPv6 offers a vastly larger address space, better

security features, and is designed to meet the future demands of internet-connected devices. The adoption of IPv6 is gradually increasing, ensuring that the internet continues to function efficiently and securely for years to come.