Classification of Computer Network/Network. based on 9 various criteria.

Classification of Computer Networks Based on 9 Different Criteria

Computer networks can be classified based on various factors, such as geographical coverage, topology, transmission mode, and more. Here are **9 different criteria** for classification:

1.Based on Geographical Coverage

- **Personal Area Network (PAN)** – Covers a very small area (e.g., Bluetooth, USB connections).
- **Local Area Network (LAN)** – Covers a small region like an office or campus.
- **Metropolitan Area Network (MAN)** – Covers a city-wide area.
- **Wide Area Network (WAN)** – Covers a country or even worldwide (e.g., the Internet).

2.Based on Transmission Technology

- **Wired Network** – Uses physical cables (e.g., Ethernet, Fiber-optic).
- **Wireless Network** – Uses radio waves, infrared, or satellite communication (e.g., Wi-Fi, 5G).

3.Based on Communication Mode

- **Simplex** – One-way communication (e.g., TV, radio).
- **Half-Duplex** – Two-way communication, but one at a time (e.g., walkie-talkies).
- **Full-Duplex** – Two-way communication simultaneously (e.g., telephones).

4.Based on Topology (Physical Structure)

- **Bus Topology** – Single backbone cable connects all devices.
- **Star Topology** – All nodes connect to a central hub or switch.
- **Ring Topology** – Each device connects to two others in a circular structure.
- **Mesh Topology** – Each device is interconnected with others (full/partial mesh).
- **Hybrid Topology** – Combination of two or more topologies.

5.Based on Ownership

- **Private Network** – Owned by an organization or individual (e.g., company intranet).
- **Public Network** – Open to the public (e.g., the Internet).

6.Based on Purpose and Functionality

- **Storage Area Network (SAN)** – Dedicated network for high-speed storage access.
- **Enterprise Private Network (EPN)** – Used by businesses to connect branches securely.
- **Virtual Private Network (VPN)** – Secure connection over a public network.

7.Based on Connection Type

- **Point-to-Point Network** – Direct connection between two devices.
- **Multipoint Network** – Multiple devices share the same communication link.

8.Based on Security and Accessibility

- **Intranet** – Private network for internal organization use.
- **Extranet** – Controlled access network allowing external entities to connect.
- **Internet** – Global public network connecting millions of devices.

9. Based on Data Transmission Mode

- **Packet-Switched Network** – Data is sent in packets (e.g., the Internet).

- **Circuit-Switched Network** – Dedicated path is established for communication (e.g., telephone networks).

Write about different types of network protocol for 5 marks.

Different Types of Network Protocols

Network protocols are a set of rules that govern data communication between devices. They ensure proper data transmission, security, and communication across networks. Here are some key types of network protocols:

1.Transmission Control Protocol/Internet Protocol (TCP/IP)

- TCP ensures reliable, error-free data transmission.
- IP is responsible for addressing and routing packets across networks.
- Used for communication over the Internet.

2.Hypertext Transfer Protocol (HTTP/HTTPS)

- HTTP is used for web communication and accessing websites.
- HTTPS is a secure version with encryption for data protection.
- Example: Browsing websites like Google and Facebook.

3.File Transfer Protocol (FTP)

- Used for transferring files between a client and a server.
- Supports authentication (username/password) for secure access.
- Example: Uploading/downloading files from a website.

4.Simple Mail Transfer Protocol (SMTP) & Post Office Protocol (POP3)/IMAP

- **SMTP**: Used for sending emails.
- **POP3/IMAP**: Used for receiving emails (POP3 downloads, IMAP syncs emails).
- Example: Gmail, Outlook email services.

5.Domain Name System (DNS)

- Translates domain names (e.g., www.google.com) into IP addresses.
- Helps users access websites without remembering numerical IPs.

What do you mean by layered network arcitecture. write it for 3 marks

Layered Network Architecture

Layered network architecture is a structured approach to designing communication systems by dividing network functions into multiple layers. Each layer has specific tasks and interacts only with the layers directly above and below it.

Key Features:

1. **Modularity** – Breaks down complex networking tasks into smaller, manageable layers.
2. **Interoperability** – Different vendors can develop networking components that work together.
3. **Standardization** – Follows established models like the **OSI Model (7 layers)** and **TCP/IP Model (4 layers)**.

Examples:

- **OSI Model**: Includes layers like Physical, Data Link, Network, Transport, etc.
- **TCP/IP Model**: Used for the Internet, including layers such as Network Interface, Internet, Transport, and Application.

Layered architecture simplifies troubleshooting, improves flexibility, and enhances communication efficiency in networks.

Describe OSI reference model. [Need to write about each layer shortly]

OSI Reference Model

The **OSI (Open Systems Interconnection) reference model** is a **seven-layer framework** developed by the **International Organization for Standardization (ISO)** to standardize network communication. Each layer has specific functions and interacts with the layers above and below it.

Seven Layers of the OSI Model

1. **Physical Layer**
    - Deals with raw data transmission through physical media like cables, radio waves, etc.
    - Example: Ethernet cables, Wi-Fi signals.
2. **Data Link Layer**
    - Ensures error-free data transfer between two directly connected devices.
    - Uses MAC (Media Access Control) addresses for device identification.
    - Example: Switches, MAC addresses.
3. **Network Layer**
    - Handles IP addressing and routing of data packets.
    - Ensures data reaches the correct destination.
    - Example: Routers, IP addresses.
4. **Transport Layer**
    - Ensures reliable or fast data transmission using **TCP (reliable)** or **UDP (fast, unreliable)**.
    - Example: TCP for emails, UDP for video streaming.
5. **Session Layer**
    - Manages and controls communication sessions between applications.
    - Example: Video conferencing applications maintaining session states.
6. **Presentation Layer**
    - Converts, encrypts, and compresses data for transmission.
    - Ensures proper data format across different systems.
    - Example: SSL/TLS encryption, data compression formats.
7. **Application Layer**
    - Provides network services to end users like email, web browsing, and file transfer.
    - Example: HTTP (web browsing), FTP (file transfer), SMTP (email).

Importance of the OSI Model:

- Helps in designing and troubleshooting networks.
- Provides a universal standard for different devices and protocols.
- Enhances interoperability between network systems.

Write about TCP/IP Protocol suit. write for 5 marks.

TCP/IP Protocol Suite

The **TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite** is a set of communication protocols that define how data is transmitted over the Internet and other networks. It is the foundation of modern networking, including the Internet.

Layers of TCP/IP Model

The TCP/IP model consists of **four layers**, which correspond to the OSI model:

1. **Network Interface Layer (Link Layer)**
   - Handles physical network connections (wired/wireless).
   - Manages MAC addresses and hardware addressing.
   - Example: Ethernet, Wi-Fi.
2. **Internet Layer**
   - Responsible for IP addressing and routing of data packets.
   - Ensures data is delivered to the correct destination across networks.
   - Example: Internet Protocol (IP), Address Resolution Protocol (ARP).
3. **Transport Layer**
   - Ensures reliable or fast delivery of data.
   - Uses **TCP (Transmission Control Protocol)** for reliable data transfer and **UDP (User Datagram Protocol)** for fast but unreliable transfer.
   - Example: TCP for emails, UDP for video streaming.
4. **Application Layer**
   - Provides network services for end users.
   - Includes protocols for web browsing, email, and file transfers.
   - Example: **HTTP/HTTPS (Web), FTP (File Transfer), SMTP (Email), DNS (Domain Name System).**

Features of TCP/IP Protocol Suite

✓ **Scalability** – Supports small and large networks.
✓ **Interoperability** – Works across different devices and platforms.
✓ **Reliability** – TCP ensures error-free, ordered delivery of data.
✓ **Global Standard** – Used as the foundation for the Internet.

What do you mean by Framming and flow control. marks (2+2).

Framing (2 Marks)

Framing is a **data-link layer** function that breaks the data stream into manageable units called **frames** before transmission. It helps in **error detection, synchronization, and proper data delivery**.

Types of Framing:

1. **Character Count** – Uses a count field to specify frame length.
2. **Character Stuffing** – Uses special characters to mark frame boundaries.
3. **Bit Stuffing** – Adds extra bits to differentiate data from control information.

🔷 **Example:** Ethernet frames in LANs.

Flow Control (2 Marks)

Flow control is a **mechanism to regulate data transmission speed** between a sender and a receiver to prevent data loss or overflow.

Types of Flow Control:

1. **Stop-and-Wait** – The sender waits for acknowledgment after sending each frame.
2. **Sliding Window** – The sender can send multiple frames before needing acknowledgment.

🔷 **Example:** TCP uses flow control to manage data transmission efficiently.

Write about Point to Point Protocol on internet. for marks (3)

Point-to-Point Protocol (PPP) on the Internet

The **Point-to-Point Protocol (PPP)** is a **data-link layer** protocol used for direct communication between two network devices, such as a computer and an Internet Service Provider (ISP). It is commonly used for **dial-up, DSL, and VPN connections.**

Features of PPP

1. **Encapsulation of Data** – Transmits different types of network traffic (e.g., IP, IPX).
2. **Authentication Support** – Uses protocols like **PAP (Password Authentication Protocol)** and **CHAP (Challenge Handshake Authentication Protocol)** for secure access.
3. **Error Detection** – Ensures reliable data transmission by detecting errors in frames.
4. **Compression** – Reduces the size of data packets for efficient transmission.
5. **Multilink Support** – Allows multiple physical links to be combined for higher bandwidth.

Uses of PPP

✓ Used in **modems, DSL, and VPNs** for establishing Internet connections.
✓ Helps in **remote access and secure data transmission**.
✓ Works with **serial links and point-to-point network setups**.

Write about Error recovery Protocol using Stop and Wait AR queue. for marks 5.

Error Recovery Protocol Using Stop and Wait ARQ (Automatic Repeat Request)

The **Stop-and-Wait ARQ** is a simple error recovery protocol used in communication systems to ensure reliable data transmission. It works by sending a single data frame and then waiting for an acknowledgment (ACK) from the receiver before sending the next frame. If the acknowledgment is not received within a specific time, the frame is retransmitted.

Working of Stop-and-Wait ARQ

1. **Sender Side**:
    - The sender transmits a data frame.
    - It then **waits for an acknowledgment** (ACK) from the receiver.
    - If an acknowledgment is received within the timeout period, the sender proceeds to the next frame.
    - If **no ACK** is received (due to errors or loss of the packet), the sender retransmits the same frame after the timeout period.
    -

2. **Receiver Side**:
    - The receiver waits for the incoming data frame.
    - Once received, the receiver checks the frame for **errors**.
    - If the frame is error-free, it sends an **ACK** to the sender, indicating successful reception.
    - If errors are detected in the frame, the receiver discards it and does **not send an acknowledgment**, prompting the sender to retransmit the frame.

Key Features of Stop-and-Wait ARQ

1. **Error Detection**:
    - The receiver checks for errors in the received frame, typically using checksum or cyclic redundancy check (CRC).
    - If errors are found, no acknowledgment is sent, prompting the sender to resend the frame.
2. **Timeout Mechanism**:
    - A timer is set when the sender transmits a frame. If the **timeout expires** without receiving an ACK, the sender will **retransmit** the same frame.
3. **Acknowledgment**:
    - ACKs are sent by the receiver to indicate the successful receipt of a frame.
    - The sender waits for the ACK before transmitting the next frame.
4. **Simplicity**:
    - The Stop-and-Wait ARQ protocol is **simple** and easy to implement but not efficient for high-speed communication due to the long wait times between sending frames.

Advantages

1. **Reliability**: Ensures that all frames are successfully received without errors, with retransmissions in case of lost or corrupted frames.
2. **Simple**: Easy to understand and implement in network communication.

Disadvantages:

1. **Inefficiency**: Stop-and-Wait ARQ has low throughput because the sender waits for an acknowledgment before sending the next frame, leading to idle time.
2. **Slow for High Latency**: In high-latency networks, the sender spends a significant amount of time waiting for ACKs, reducing overall efficiency.