UNIT 1

5 Marks :

1. **Explain the history of computer networks.**

   History of Computer Networks

   - 1960s – ARPANET:
     The first computer network was ARPANET, developed by the U.S. Department of Defense. It used packet switching technology, which allowed breaking data into small packets and sending them across different paths. This laid the foundation for modern networking.
   - 1970s – Protocol Development:
     Researchers developed the TCP/IP protocol suite (Transmission Control Protocol / Internet Protocol). TCP/IP made it possible for different types of networks to interconnect and communicate, leading to the idea of an "internetwork."
   - 1980s – Expansion:
     Networking moved beyond research labs to universities and organizations. Local Area Networks (LANs) became popular in offices and campuses, while TCP/IP was adopted as the standard protocol.
   - 1990s – Internet Growth:
     ARPANET was decommissioned, but it had already grown into what we now call the Internet. With the invention of the World Wide Web (WWW) and web browsers, networking became accessible to the general public.
   - 2000s to Present – Modern Networks:
     High-speed broadband, wireless networks (Wi-Fi, 4G/5G), and Virtual Private Networks (VPNs) have made communication faster, mobile, and secure. Networking today supports global communication, e-commerce, cloud computing, and social media.

2. **Explain different types of network topologies.**

   The different types of network topologies are:

   1. Mesh Topology
      - Every node is connected to every other node.
      - Provides high reliability and fault tolerance.
      - Expensive and complex to install and maintain.
   2. Star Topology
      - All nodes are connected to a central hub or switch.
      - Easy to add/remove devices.
      - Failure of the central hub leads to network failure.
   3. Bus Topology
      - All devices share a single backbone cable.
      - Simple and cost-effective for small networks.

- Entire network fails if the backbone is damaged.

4. **Ring Topology**
    - Devices are connected in a circular path.
    - Data passes in one direction (unidirectional).
    - Failure of one device affects the whole network.
5. **Hybrid Topology**
    - Combination of two or more topologies (e.g., Star + Bus).
    - Flexible and scalable.
    - Costly and complex to design.

3. Explain ISO-OSI reference model.

The ISO-OSI (Open Systems Interconnection) model is a 7-layer reference model developed by the International Standards Organization (ISO) to standardize network communication. Each layer performs specific functions:

1. **Application Layer**
    - Provides interface between user applications and the network.
    - Services: file transfer, email, web browsing.
    - Protocols: HTTP, DNS, SMTP.
    - Example: WhatsApp, Firefox.
2. **Presentation Layer**
    - Deals with syntax and semantics of data.
    - Performs translation, encryption, and compression.
    - Ensures interoperability between different systems.
    - Protocols: SSL, AFP.
3. **Session Layer**
    - Establishes, maintains, and terminates sessions.
    - Provides dialog control and synchronization.
    - Manages token handling to avoid conflicts.
    - Protocols: RTCP, PPTP, PAP.
4. **Transport Layer**
    - Ensures end-to-end communication.
    - Performs segmentation, error detection, and retransmission.
    - Provides flow control and acknowledgment.
    - Protocols: TCP, UDP.
5. **Network Layer**
    - Responsible for logical addressing and routing.
    - Decides best path for packet delivery.
    - Handles packet forwarding and fragmentation.
    - Implemented by routers and switches.
6. **Data Link Layer**
    - Provides node-to-node communication.
    - Handles framing, MAC addressing, and error detection.
    - Divided into LLC (Logical Link Control) and MAC (Media Access Control).
    - Protocols: Ethernet, PPP.

7. Physical Layer
    - Deals with physical transmission of raw bits.
    - Defines hardware, cables, connectors, and signalling.
    - Responsible for bit synchronization and transmission modes.
    - Data represented as electrical/optical signals.

4. Explain TCP/IP reference model.

The TCP/IP model is a 4-layered architecture developed by the U.S. Department of Defence (DARPA). It is the foundation of the Internet and defines how data should be packetized, addressed, transmitted, and received.

1. Application Layer
    - Combines functions of OSI's Application, Presentation, and Session layers.
    - Provides services like file transfer, email, and web browsing.
    - Handles data formatting, encryption, and session management.
    - Protocols: HTTP, SMTP, DNS, FTP.
2. Transport Layer
    - Provides end-to-end communication between applications.
    - Ensures data segmentation, sequencing, flow control, and error detection.
    - TCP: Reliable, connection-oriented service.
    - UDP: Fast, connectionless service.
3. Internet Layer
    - Equivalent to OSI's Network Layer.
    - Handles logical addressing, packet forwarding, and routing.
    - Determines best path for data transmission.
    - Protocols: IP, ICMP, ARP.
4. Network Access Layer
    - Equivalent to OSI's Data Link + Physical layers.
    - Defines how data is physically transmitted over hardware.
    - Handles MAC addressing, framing, and error detection.

Protocols/Technologies: Ethernet, Wi-Fi, PPP.

5. Discuss Guided Transmission media and its types.

Guided Transmission Media:

- Guided media refers to transmission of data signals through a physical path.
- The medium directs the data signals from sender to receiver.
- Examples include Twisted Pair Cable, Coaxial Cable, and Optical Fiber.

Types of Guided Transmission Media:

1. Twisted Pair Cable
    - Consists of two insulated copper wires twisted around each other.
    - Reduces electromagnetic interference.
    - Used in LANs and telephone lines.
    - Cost-effective but limited in bandwidth and distance.

2. **Coaxial Cable**
    - Consists of a central copper conductor surrounded by insulation, shielding, and outer jacket.
    - Provides higher bandwidth than twisted pair.
    - Used in cable TV networks and broadband Internet.
    - Less affected by noise but costlier.
3. **Optical Fiber**
    - Uses thin strands of glass or plastic to transmit data as light signals.
    - Provides very high bandwidth and long-distance communication.
    - Immune to electromagnetic interference.
    - Used in Internet backbone, telecommunication, and high-speed data networks.

6. Explain Wireless Application Protocols (WAP) with block diagram.

Wireless Application Protocol (WAP):

- WAP is a standard protocol that enables mobile devices to access Internet services.
- It allows wireless devices like mobile phones and PDAs to connect to the web.
- Works on top of wireless networks such as GSM, CDMA, or GPRS.
- Provides services like browsing, e-mail, online banking, and e-commerce on mobile devices.

Key Features:

1. Open standard, supported by many manufacturers.
2. Works with multiple wireless technologies.
3. Supports multimedia (text, images, audio).
4. Secure communication with WTLS (Wireless Transport Layer Security).

Block Diagram of WAP Architecture:

```
+---------------------+
| Application Layer | → WAE (Wireless Application Environment)
+---------------------+
| Session Layer     | → WSP (Wireless Session Protocol)
+---------------------+
| Transaction Layer | → WTP (Wireless Transaction Protocol)
+---------------------+
| Security Layer    | → WTLS (Wireless Transport Layer Security)
+---------------------+
| Transport Layer   | → WDP (Wireless Datagram Protocol)
+---------------------+
| Bearer Services   | → GSM, CDMA, SMS, GPRS, etc.
+---------------------+
```

Layers of WAP Architecture:

1. Application Layer (WAE – Wireless Application Environment)
    - Provides applications and services to end-users.
    - Supports Wireless Markup Language (WML).
2. Session Layer (WSP – Wireless Session Protocol)
    - Manages sessions between client and server.
    - Provides services like connection establishment and release.

3. Transaction Layer (WTP – Wireless Transaction Protocol)
    - Ensures reliable request/response transactions.
    - Provides error handling and retransmission.
4. Security Layer (WTLS – Wireless Transport Layer Security)
    - Provides authentication and encryption.
    - Ensures secure data transmission.
5. Transport Layer (WDP – Wireless Datagram Protocol)
    - Adapts data to the underlying bearer network.
    - Works with technologies like GSM, CDMA, SMS.

7. Describe how twisted pair cables are used for data transmission.

- Structure: A twisted pair cable consists of two insulated copper wires twisted around each other. The twisting reduces electromagnetic interference and crosstalk from nearby pairs.
- Working:
    1. Data is transmitted in the form of electrical signals through the copper wires.
    2. The twists ensure that interference affects both wires equally, allowing the difference in signals to be detected at the receiver, thus improving signal clarity.
    3. Multiple pairs can be bundled together in a single cable to increase capacity.
- Types:
    - Unshielded Twisted Pair (UTP): Commonly used in LANs, telephone lines, and Ethernet networks.
    - Shielded Twisted Pair (STP): Has an additional shielding layer for better noise resistance, used in industrial and high-interference environments.
- Applications: Widely used for local area networking, connecting computers, switches, and routers, with data rates ranging from low (telephone lines) to high (up to 10 Gbps for modern Ethernet).

8. What is a Wireless LAN (WLAN)?

- Definition: A Wireless Local Area Network (WLAN) is a type of LAN that uses wireless technology (radio waves) instead of cables to connect devices such as laptops, mobiles, and printers within a limited area like homes, offices, or campuses.
- Technology: WLANs are commonly based on the IEEE 802.11 standard, popularly known as Wi-Fi. They allow devices to communicate with each other or connect to the Internet without physical wiring.
- Working:
    1. Devices connect to a central access point (AP) or router using wireless signals.
    2. The AP manages communication between devices and provides access to wired networks or the Internet.
- Advantages:
    - Provides mobility and flexibility for users.
    - Easy installation without the need for cables.
    - Cost-effective for extending networks.
- Examples: Home Wi-Fi networks, campus Wi-Fi systems, and public hotspots in airports and cafes.

9. Explain the concept of a Packet Radio Network.

- **Definition: A Packet Radio Network (PRN) is a type of wireless network where data is transmitted in the form of small packets using radio signals instead of wired connections.**
- **Concept:**
  1. **Data is divided into packets before transmission.**
  2. **These packets are broadcast over radio frequencies and received by other stations within range.**
  3. **Each packet contains addressing information so it can be correctly delivered to the intended destination.**
  4. **Intermediate stations can act as repeaters, forwarding packets to extend coverage.**
- **Features:**
  - **Provides communication in areas where wired infrastructure is not available.**
  - **Supports mobility of devices.**
  - **Works in environments like battlefields or remote locations.**
- **Applications: Used in military communication, emergency services, sensor networks, and as the basis for some wireless LAN technologies.**

10. What is a Virtual Private Network (VPN)?

- **Definition: A Virtual Private Network (VPN) is a technology that creates a secure and encrypted connection over a public network (such as the Internet). It allows users to access resources and communicate as if they were connected to a private network.**
- **Concept:**
  - **VPNs use tunnelling protocols to encapsulate data packets and transmit them securely across public networks.**
  - **Data is encrypted, ensuring that unauthorized users cannot access or interpret it.**
  - **VPNs also use authentication mechanisms to verify the identity of users and devices.**
- **Functions:**
  - **Protects sensitive information by maintaining privacy and confidentiality.**
  - **Provides secure remote access to organizational networks for employees working from outside.**
  - **Ensures data integrity and security during communication across untrusted networks.**
- **Applications:**
  - **Used by businesses for secure inter-office communication.**
  - **Employed by individuals to access restricted websites and safeguard online activities.**
  - **Supports secure transactions in banking, e-commerce, and government communication.**
- **Example: An employee working from home can connect to their company’s internal servers through a VPN, ensuring both security and privacy.**

10 Marks :

1. **Discuss OSI model.**

   The OSI (Open Systems Interconnection) model is a reference model developed by ISO in 1984. It divides the communication process into seven layers, each with specific responsibilities. It ensures interoperability between different systems and standardizes networking functions.

Layers of OSI Model

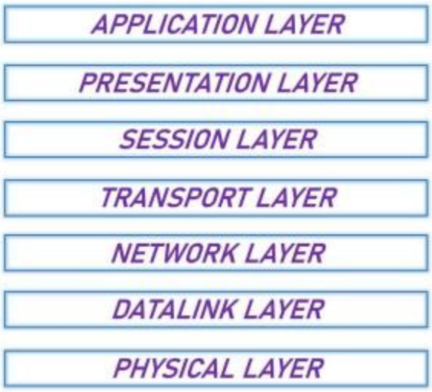
1. **Application Layer**
   - Provides interface between user applications and the network.
   - Services: File transfer, email, web browsing.
   - Protocols: HTTP, DNS, SMTP.
2. **Presentation Layer**
   - Deals with syntax and semantics of exchanged data.
   - Functions: Data translation, encryption/decryption, compression.
   - Ensures interoperability between different systems.
3. **Session Layer**
   - Establishes, manages, and terminates sessions between devices.
   - Provides dialog control (who transmits when) and synchronization (checkpoints in case of failure).
   - Protocols: RTCP, PPTP.
4. **Transport Layer**
   - Ensures reliable end-to-end delivery of data.
   - Performs segmentation, sequencing, error control, and flow control.
   - Protocols: TCP (reliable), UDP (fast).
5. **Network Layer**
   - Responsible for logical addressing and routing of packets.
   - Determines best path for data transmission.
   - Devices: Routers, Layer-3 switches.
   - Protocols: IP, ICMP.
6. **Data Link Layer**
   - Provides node-to-node delivery.
   - Handles framing, MAC addressing, and error detection/correction.
   - Divided into LLC (Logical Link Control) and MAC (Media Access Control).
   - Protocols: Ethernet, PPP.
7. **Physical Layer**
   - Concerned with transmission of raw bits over physical medium.
   - Defines hardware (cables, connectors, switches) and signaling.
   - Functions: Bit synchronization, transmission mode (simplex/half duplex/full duplex).

Key Features of OSI Model

- Each layer performs a well-defined function.
- Provides modularity and standardization.

- Data flows top-down at sender and bottom-up at receiver.
- Intermediate nodes use only physical, data link, and network layers.

Diagram of OSI Model :



2. Explain TCP/IP model.

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a 4-layered reference model developed by DARPA (U.S. Department of Defense). It defines how data is transmitted across networks and forms the foundation of the modern Internet.

Layers of TCP/IP Model

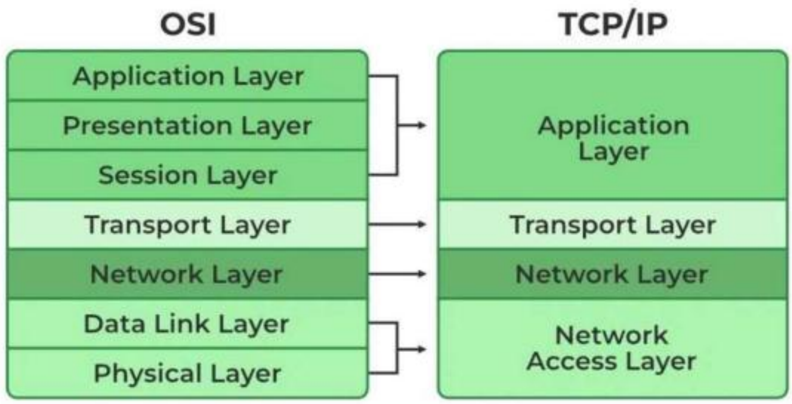
1. Application Layer
    - Combines functions of Application, Presentation, and Session layers of OSI.
    - Provides services for file transfer, email, browsing, and multimedia.
    - Handles data formatting, encryption, and session management.
    - Protocols: HTTP, FTP, SMTP, DNS.
2. Transport Layer
    - Provides end-to-end communication between processes.
    - Ensures segmentation, sequencing, error control, and flow control.
    - Supports two protocols:
        - TCP (Transmission Control Protocol): Reliable, connection-oriented, error-checked.
        - UDP (User Datagram Protocol): Fast, connectionless, best-effort delivery.
3. Internet Layer
    - Equivalent to OSI's Network Layer.
    - Handles logical addressing, routing, and packet forwarding.
    - Ensures data packets reach the correct destination across multiple networks.
    - Protocols: IP (IPv4, IPv6), ICMP, ARP.
4. Network Access Layer
    - Equivalent to OSI's Data Link and Physical layers.
    - Defines how data is physically transmitted over a specific medium.
    - Responsible for framing, MAC addressing, and error detection.
    - Technologies: Ethernet, Wi-Fi, PPP.

Key Features of TCP/IP Model

- Provides a protocol-specific framework (unlike OSI, which is protocol-independent).
- Basis of Internet communication and widely used in real-world networks.

- More flexible and practical than OSI, designed around working protocols.

Diagram of TCP/IP Model



3. **Describe OSI and TCP/IP model in comparison mode.**

The OSI and TCP/IP models are both layered architectures used in networking. OSI is a theoretical reference model, while TCP/IP is a practical protocol model used in real networks like the Internet.

Comparison of OSI and TCP/IP Models

S.No	Aspect	OSI Model	TCP/IP Model
1	No. of Layers	7 layers (Application, Presentation, Session, Transport, Network, Data Link, Physical).	4 layers (Application, Transport, Internet, Network Access).
2	Layer Grouping	Separate Presentation and Session layers.	Presentation and Session functions included in Application layer.
3	Functionality	Independent functions defined for each layer.	Some functions are combined in broader layers.
4	Standardization	Protocol-independent, only defines services and interfaces.	Protocol-specific, based on real protocols (TCP, IP).
5	Flexibility	More flexible, conceptual model for teaching and design.	More rigid, designed around existing protocols.
6	Development	Developed by ISO (International Organization for Standardization).	Developed by DARPA (U.S. Department of Defense).

7	Protocols	Does not specify standard protocols.	Specifies standard protocols like TCP, IP, UDP, FTP, HTTP, etc.
8	Usage	Used mainly as a reference model for understanding.	Used in real networks, including the Internet.
9	Communication Flow	Top-down (sender) and bottom-up (receiver) through all 7 layers.	Simplified flow through 4 practical layers.
10	Practicality	Theoretical model, rarely implemented fully.	Practical model, widely implemented worldwide.

✅ **Conclusion:**

- **OSI is mainly used for conceptual understanding and standardization, while TCP/IP is a practical implementation model used globally in networking and the Internet.**

4. Explain transmission media.

Transmission Media refers to the physical or wireless pathways that carry data signals from one device to another in a computer network. It is broadly classified into Guided Media (wired) and Unguided Media (wireless).

---

1. Guided Transmission Media

Signals are transmitted through a physical path such as cables.

- **Twisted Pair Cable**
  - **Two insulated copper wires twisted around each other.**
  - **Reduces interference and crosstalk.**
  - **Types: UTP (Unshielded) and STP (Shielded).**
  - **Commonly used in LANs and telephone lines.**
- **Coaxial Cable**
  - **Central copper conductor with insulating layer, metallic shield, and outer cover.**
  - **Provides higher bandwidth and noise immunity.**
  - **Used in cable TV networks and broadband.**
- **Optical Fiber Cable**
  - **Transmits data as light signals through glass or plastic fibers.**
  - **Very high bandwidth and long-distance capability.**
  - **Immune to electromagnetic interference.**
  - **Used in backbone Internet connections and telecommunication.**

---

2. Unguided Transmission Media (Wireless)

Signals are transmitted through the air using radio, microwave, or light waves.

- **Radio Waves**
  - **Used for long-distance communication.**

- Supports both unicast and broadcast transmission.
    - Applications: AM/FM radio, TV.
- Microwaves
    - Operate in high-frequency range.
    - Require line-of-sight transmission.
    - Applications: Satellite links, point-to-point communication.
- Infrared
    - Short-range communication using infrared rays.
    - Cannot penetrate walls.
    - Applications: TV remotes, short-distance device communication.
- Satellite Communication
    - Uses communication satellites for long-distance data transfer.
    - Provides global coverage.
    - Used in GPS, weather monitoring, and telecommunication.

✅ Conclusion:
Transmission media can be wired (guided) or wireless (unguided). The choice depends on distance, cost, speed, and application requirements.

5. Write a detailed note on Guided Transmission media.

Guided Transmission Media refers to the transmission of data signals through a physical path. The signal is directed along the medium, and the quality depends on the physical characteristics of the medium. Common types are Twisted Pair Cable, Coaxial Cable, and Optical Fiber Cable.

---

1. Twisted Pair Cable

- Structure: Two insulated copper wires twisted around each other to reduce electromagnetic interference.
- Types:
    - UTP (Unshielded Twisted Pair): Inexpensive, widely used in LANs and telephony.
    - STP (Shielded Twisted Pair): Has additional shielding for better resistance to noise.
- Features:
    - Low cost, easy to install.
    - Limited bandwidth and distance (up to a few hundred meters).
- Applications: Ethernet cables, telephone lines.

---

2. Coaxial Cable

- Structure: Central copper conductor, insulating layer, metallic shield, and plastic outer cover.
- Features:
    - Provides higher bandwidth than twisted pair.
    - Better protection against noise and interference.
    - More expensive than twisted pair.
- Applications: Cable TV networks, broadband Internet, CCTV systems.

---

3. Optical Fiber Cable

- **Structure: Thin glass or plastic core surrounded by cladding and protective outer coating.**
- **Working: Transmits data in the form of light signals.**
- **Features:**
  - **Very high bandwidth and long-distance capability.**
  - **Immune to electromagnetic interference.**
  - **Difficult and costly to install and maintain.**
- **Applications: Internet backbone, long-distance telecommunication, high-speed LANs.**

Key Points about Guided Media

- **Provides high security since signals remain in a physical path.**
- **Data transmission speed depends on the medium (fiber > coaxial > twisted pair).**
- **More suitable for short and medium distances, but fiber can cover very long distances.**

✅ **Conclusion:**

Guided transmission media plays a major role in networking by offering reliable, secure, and efficient communication. Among the three, optical fiber is the most advanced, while twisted pair remains the most commonly used due to its low cost.

6. Discuss Unguided Transmission media

Unguided Transmission Media refers to wireless communication where data signals are transmitted through the air without any physical conductor. It uses electromagnetic waves such as radio, microwave, or light waves. This type of medium supports mobility and long-distance communication.

Types of Unguided Transmission Media

1. **Radio Waves**
   - **Frequency range: 3 kHz – 1 GHz.**
   - **Can penetrate through buildings and walls.**
   - **Suitable for both short and long-distance communication.**
   - **Applications: AM/FM radio, television broadcasting, cordless phones.**
2. **Microwaves**
   - **Frequency range: 1 GHz – 300 GHz.**
   - **Require line-of-sight between sender and receiver.**
   - **Support very high data rates.**
   - **Applications: Satellite links, point-to-point communication, cellular networks.**
3. **Infrared Waves**
   - **Operate in short range (a few meters).**
   - **Cannot penetrate walls or obstacles.**
   - **Provide secure communication in closed spaces.**
   - **Applications: TV remote controls, wireless keyboards, short-range device communication.**
4. **Satellite Communication**

- Uses satellites orbiting the Earth to relay signals.
- Provides global coverage.
- Works by uplink (earth to satellite) and downlink (satellite to earth).
- Applications: GPS, weather monitoring, Internet backbone, military communication.

Key Features of Unguided Media

- Provides mobility and easy installation (no cables).
- Supports long-distance communication (satellite, radio).
- More prone to interference and noise compared to guided media.
- Bandwidth varies depending on the medium (microwave and satellite offer higher).

✅ Conclusion:

Unguided transmission media plays a vital role in modern communication systems, enabling wireless access, mobility, and global connectivity. It is widely used in radio, television, mobile communication, and satellite systems.

7. Explain about Wireless Networks.

Wireless Networks are communication systems where data is transmitted without physical cables, using electromagnetic signals like radio waves, microwaves, or infrared. They allow mobility, flexibility, and connectivity across different devices.

Features of Wireless Networks

- Mobility: Devices can move freely within the coverage area.
- Flexibility: Easy installation without cabling.
- Scalability: Supports addition of new devices without major setup changes.
- Cost-effective: Reduces infrastructure cost compared to wired networks.

Types of Wireless Networks

1. Packet Radio Networks
    - Data is divided into packets and transmitted using radio frequencies.
    - Each packet carries addressing information and can be relayed by intermediate nodes.
    - Applications: Military communication, emergency services, mobile ad-hoc networks.
2. Wireless LAN (WLAN)
    - Provides wireless connectivity within a limited area (home, office, campus).
    - Based on IEEE 802.11 standard (Wi-Fi).
    - Components: Access Points (AP) and wireless-enabled devices.
    - Applications: Home Wi-Fi, campus networks, public hotspots.
3. Wireless Application Protocol (WAP)
    - Standard for accessing Internet services on mobile devices.
    - Uses layered architecture (WAE, WSP, WTP, WTLS, WDP).
    - Applications: Mobile browsing, wireless e-mail, online banking.

4. Virtual Private Network (VPN) over Wireless
    - Securely connects remote users through encrypted wireless tunnels.
    - Ensures confidentiality and data integrity.
    - Applications: Remote work, secure enterprise communication.

Advantages of Wireless Networks

- Easy deployment and expansion.
- Supports mobility and remote access.
- Enables communication in areas where cabling is not possible.

Disadvantages of Wireless Networks

- More prone to interference and security issues.
- Limited bandwidth compared to wired networks.
- Performance depends on distance and obstacles.

✅ Conclusion:

Wireless networks are essential in modern communication, supporting technologies like Wi-Fi, WAP, and VPNs. They provide mobility and convenience, making them widely used in homes, businesses, and global communication systems.

8. **Describe segmentation and reassembly in the context of the transport layer. How does TCP handle it?**

1. Segmentation in Transport Layer

- The transport layer receives large data blocks from the application layer.
- These large messages cannot be transmitted as a single unit across the network.
- Segmentation is the process of breaking large data into smaller units called segments.
- Each segment is assigned a sequence number so that the receiver can correctly order them.
- Segmentation ensures efficient utilization of network resources and error recovery.

---

2. Reassembly in Transport Layer

- At the receiver side, the transport layer collects incoming segments.
- Using the sequence numbers, it reorders them into the correct sequence.
- Duplicate or corrupted segments are discarded.
- Finally, the complete message is reassembled and passed to the application layer.

---

3. How TCP Handles Segmentation & Reassembly

1. Segmentation by TCP (Sender side):
    - TCP divides the byte stream from the application into manageable segments.
    - Each segment includes a TCP header containing:
        - Source and Destination ports.
        - Sequence Number (for reordering).
        - Acknowledgment Number (for reliability).
2. Reassembly by TCP (Receiver side):

    - TCP uses the sequence numbers to reassemble segments into the original byte stream.
    - If segments arrive out of order, TCP buffers them until missing ones are received.
    - Acknowledgments are sent to confirm receipt, and lost segments are retransmitted.
3. Reliability in TCP:
    - Provides error detection using checksums.
    - Implements flow control and congestion control to maintain efficient transmission.
    - Ensures reliable, in-order, and error-free delivery to the application.

✅ Conclusion:

Segmentation and reassembly are crucial functions of the Transport Layer. TCP manages this using sequence numbers, acknowledgments, and retransmission, ensuring reliable end-to-end communication between applications.

9. Explain Wireless Application Protocols (WAP).

Wireless Application Protocol (WAP):

- WAP is a standard protocol that enables mobile and wireless devices to access Internet-based services and applications.
- It provides a framework for delivering information to handheld devices using wireless networks.
- WAP follows a layered architecture similar to the OSI model, ensuring interoperability between different devices and networks.

Layers of WAP Architecture

1. Wireless Application Environment (WAE)
    - Provides applications and services to end-users.
    - Uses Wireless Markup Language (WML) for content display on small screens.
    - Supports browsing, messaging, and interactive services.
2. Wireless Session Protocol (WSP)
    - Manages sessions between client (mobile device) and server.
    - Functions include session establishment, release, and data exchange.
    - Ensures efficient communication over wireless links.
3. Wireless Transaction Protocol (WTP)
    - Provides reliable request/response transactions.
    - Handles retransmissions, acknowledgments, and error detection.
    - Lightweight protocol suitable for mobile devices with limited resources.
4. Wireless Transport Layer Security (WTLS)
    - Ensures security in wireless communication.
    - Provides authentication, encryption, and data integrity.
    - Protects against eavesdropping and data tampering.
5. Wireless Datagram Protocol (WDP)
    - Works as the transport layer of WAP.

- Adapts higher layers to different bearer services (GSM, SMS, CDMA, etc.).
- Makes WAP independent of the underlying wireless network.

Block Diagram of WAP Architecture

```
+------------------------+
| Application Layer | → WAE (Wireless Application Environment)
+------------------------+
| Session Layer     | → WSP (Wireless Session Protocol)
+------------------------+
| Transaction Layer | → WTP (Wireless Transaction Protocol)
+------------------------+
| Security Layer    | → WTLS (Wireless Transport Layer Security)
+------------------------+
| Transport Layer   | → WDP (Wireless Datagram Protocol)
+------------------------+
| Bearer Services   | → GSM, CDMA, SMS, GPRS, etc.
+------------------------+
```

✅ **Conclusion:**

WAP is an important standard that allowed early mobile devices to access Internet content. By using a layered architecture (WAE, WSP, WTP, WTLS, WDP), WAP ensures efficient, secure, and device-independent communication over wireless networks.

10. Discuss WML and Virtual Private Network VPN Technology.

1. Wireless Markup Language (WML)

- Definition: WML is a markup language used in Wireless Application Protocol (WAP) to design and display content on small mobile device screens.
- Based on XML: It is an XML-based language optimized for handheld devices with limited resources.
- Structure: Content in WML is organized into decks (a collection of cards) and cards (individual units of user interaction).

Features of WML:

1. Lightweight and designed for mobile devices.
2. Supports text, hyperlinks, and simple user input forms.
3. Provides navigation between cards using links.
4. Compatible with wireless micro-browsers.

Applications of WML:

- Browsing Internet services on early mobile phones.
- Mobile-based messaging and banking services.
- Wireless e-commerce transactions.

---

2. Virtual Private Network (VPN) Technology

- Definition: A VPN is a technology that establishes a secure and encrypted tunnel over a public network (e.g., Internet), enabling private communication.
- Purpose: Allows users to securely access a private network from remote locations.

Working of VPN:

1. Data packets are encapsulated using tunneling protocols.
2. Information is encrypted to prevent unauthorized access.
3. Authentication mechanisms verify user/device identity.

Key Features of VPN:

- Confidentiality: Data is encrypted to prevent interception.
- Integrity: Ensures data is not altered during transmission.
- Authentication: Verifies the identity of users and devices.
- Remote Access: Provides employees secure access to company resources.

Applications of VPN:

1. Secure business communication for remote workers.
2. Protecting personal data while using public Wi-Fi.
3. Secure access to government and banking services.
4. Connecting branch offices of an organization through the Internet.

✅ Conclusion:

- WML enabled early mobile devices to access Internet services efficiently through WAP.
- VPN technology ensures secure and private communication over public networks, widely used in enterprises and personal security.

UNIT 2

5 Marks :

1. **Explain the significance of flow control and error control in data link protocols.**

Flow Control and Error Control in Data Link Protocols

Flow control and error control are two important functions of the Data Link Layer that ensure reliable communication between sender and receiver.

Flow Control:

Flow control is needed to prevent a fast sender from overwhelming a slow receiver. Since the receiver has limited processing speed and buffer space, the sender must adjust its transmission rate accordingly. Flow control ensures that data is sent at a rate that the receiver can handle, avoiding data loss. Two main techniques are used:

1. Feedback-based flow control – the receiver sends feedback to the sender about its readiness to receive more data.
2. Rate-based flow control – the protocol itself limits the rate of data transmission without requiring feedback.

Error Control:

Error control ensures that data frames are delivered accurately and in the correct order. Transmission errors may occur due to noise, interference, or other channel issues. To handle this, error control mechanisms detect errors using techniques such as parity bits, checksums, or cyclic redundancy checks (CRC). Once detected, errors are corrected either by retransmission (Automatic Repeat Request, ARQ) or by using forward error correction codes like Hamming code.

Significance:

- Flow control guarantees efficient use of resources by matching sender speed with receiver capacity.
- Error control ensures reliability by detecting and correcting errors, thereby maintaining data integrity.

  Together, they make data transmission between nodes reliable, orderly, and efficient.

2. **What is the difference between byte stuffing and bit stuffing?**

Aspect	Byte Stuffing	Bit Stuffing
Definition	Uses flag bytes at the start and end of a frame. If a flag byte occurs in the data, the sender inserts an ESC (escape byte) before it. Receiver removes ESC before delivering data.	Uses a bit pattern (01111110) to mark frame boundaries. If five consecutive 1s appear in the data, the sender inserts an extra 0 bit. Receiver removes the stuffed 0.
Unit of Operation	Works with characters/bytes (character-oriented).	Works with bits (bit-oriented).
Protocols Used	Used in BISYNC, PPP protocols.	Used in HDLC protocol.

Overhead	Increases frame size by inserting extra ESC bytes when needed.	Increases frame size by inserting extra 0 bits only when five 1s occur.
Transparency	Achieved by escaping reserved flag bytes within data.	Achieved by inserting bits so that flag pattern does not appear in data.

3. **How does Hamming Code help in error correction?**

Hamming Code for Error Correction

Hamming Code is an error-correcting code that can both detect and correct single-bit errors. It uses redundant parity bits placed at positions that are powers of 2 (1, 2, 4, 8...).

Working:

1. For a data word of *d* bits, *r* redundant bits are added such that:
$$2^r \geq d + r + 1$$
2. Each parity bit checks a group of bits according to its position.
3. At the receiver side, parity is recalculated:
   - If all parities are correct → no error.
   - If parities indicate a position → that bit is flipped to correct the error.

Significance:

- Corrects all single-bit errors.
- Detects (but does not correct) double-bit errors.
- Provides reliable data transmission over noisy channels.

Example:

For data 1010, three redundant bits are added to form 7-bit code. If the 4th bit is received in error, parity checks identify position 4, and the bit is corrected.

4. **Explain the working of a simplex stop-and-wait protocol for a noisy channel with acknowledgment and timeout.**

Simplex Stop-and-Wait Protocol for a Noisy Channel

In a noisy channel, data frames may get lost or corrupted during transmission. The simplex stop-and-wait protocol ensures reliable delivery using acknowledgment (ACK) and timeout.

Working

1. The sender transmits one frame and starts a timer.
2. The receiver checks the frame:
   - If correct → it sends back a positive ACK.
   - If damaged → the frame is discarded and no ACK is sent.
3. If the sender receives the ACK before the timer expires, it sends the next frame.
4. If the timer expires (ACK not received), the sender retransmits the same frame.
5. To avoid duplication, each frame carries a sequence number (0 or 1). The receiver uses this to discard duplicate frames.

Key Points

- Provides error control through acknowledgment and retransmission (ARQ).
- Uses timeout mechanism to handle lost frames or acknowledgments.
- Ensures reliable communication over noisy channels.

5. **Differentiate between static and dynamic channel allocation.**

Difference between Static and Dynamic Channel Allocation

Aspect	Static Channel Allocation	Dynamic Channel Allocation
Definition	The channel is divided among users in advance using fixed multiplexing techniques (e.g., FDM, TDM).	The channel is allocated to users on demand, depending on their transmission requirements.
Resource Utilization	Bandwidth may be wasted if some users are idle, as channels remain reserved.	Bandwidth is efficiently used since idle channels can be reassigned to active users.
Flexibility	Rigid and not adaptable to changing traffic conditions.	Flexible and adapts to varying and bursty traffic loads.
Suitability	Works well when the number of users is small and traffic is steady or continuous.	Works well when the number of users is large and traffic is random or bursty.
Performance	Poor for bursty traffic due to underutilization.	Better performance for bursty traffic due to efficient sharing of the channel.

In short:

- Static allocation → Fixed division, simple but inefficient with varying traffic.
- Dynamic allocation → On-demand sharing, efficient and flexible.

6. **Explain why is synchronization important in data link layer framing?**

Importance of Synchronization in Data Link Layer Framing

- Framing is the process of dividing the continuous bit stream from the physical layer into meaningful frames.
- Synchronization ensures that the receiver can correctly identify the start and end of each frame.

Reasons why synchronization is important:

1. Frame Boundary Detection – Without synchronization, the receiver cannot determine where one frame ends and the next begins.
2. Error-Free Communication – Proper synchronization prevents mixing of data bits between frames, reducing errors.
3. Efficient Decoding – Synchronization allows the receiver to interpret data correctly by aligning with the sender's frame structure.

4. Transparency – It ensures that control information (like flags or delimiters) is distinguished from actual data.
5. Reliable Communication – Synchronization avoids loss, duplication, or misinterpretation of frames during transmission.

In short: Synchronization in framing is essential so that the receiver can correctly separate frames, ensuring reliable and error-free data transmission.

7. Describe the concept of framing in the data link layer.

Framing in the Data Link Layer

- Definition: Framing is the process of dividing the continuous stream of bits received from the physical layer into manageable data units called frames. Each frame consists of a header, payload (data), and trailer.
- The data link layer encapsulates network layer packets into frames before transmission and ensures proper delivery at the receiver.

Purpose of Framing

1. Frame Boundary Identification – Allows the receiver to detect the start and end of each frame.
2. Error Detection – The trailer often carries error-detection codes (e.g., CRC).
3. Addressing – The header may contain physical addresses (MAC) of source and destination.
4. Reliable Delivery – Prevents data mixing and ensures correct reassembly.

Methods of Framing

1. Byte/Character Count – A field in the header specifies the number of bytes in the frame.
2. Flag Bytes with Byte Stuffing – Special flag bytes mark the beginning and end; ESC is used to differentiate flags in data.
3. Flag Bits with Bit Stuffing – Special bit pattern (01111110) marks boundaries; if five consecutive 1s occur, a 0 is inserted.
4. Physical Layer Coding Violations – Uses special signal patterns or encoding violations at the physical layer to mark frame boundaries.

In short: Framing in the data link layer organizes raw bit streams into structured frames, enabling synchronization, error detection, and reliable communication.

8. Define multiple access protocols. Why are they important in networking?

Multiple Access Protocols

- Definition: Multiple Access Protocols are rules and techniques used in computer networks to allow multiple devices (stations) to share a common communication channel efficiently without interfering with each other. Examples include ALOHA, CSMA, CSMA/CD, and CSMA/CA.

Importance in Networking

1. Efficient Channel Utilization – Ensures that the shared medium is used effectively without wastage.
2. Collision Management – Reduces or resolves data collisions when two or more stations transmit simultaneously.

3. Fair Access – Provides equal opportunity for all devices to access the medium.
4. Scalability – Supports a large number of users in broadcast networks such as LANs and wireless networks.
5. Reliable Communication – Improves performance by minimizing packet loss and retransmissions.

In short: Multiple access protocols are essential in networking as they manage how multiple devices share the same channel, ensuring fair, efficient, and reliable data transmission.

9. Compare Pure ALOHA and Slotted ALOHA in terms of efficiency and collision handling.

Feature	Pure ALOHA	Slotted ALOHA
Time Division	No time slots; stations transmit anytime	Time is divided into discrete slots; transmission only at slot start
Collision Handling	Collisions detected via acknowledgment; retransmit after random time	Collisions reduced because transmissions only start at slot boundaries; retransmit after random slot delay
Efficiency (Maximum Throughput)	~18.4% ($S = 1/(2e)$)	~36.8% ($S = 1/e$) – double that of Pure ALOHA
Collision Probability	Higher, as transmissions can start anytime	Lower, due to synchronized slotting
Implementation Complexity	Simple	Slightly more complex due to slot synchronization

10. Explain the purpose of CSMA/CA in wireless LANs like IEEE 802.11?

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is a protocol used in wireless LANs, such as IEEE 802.11, to manage how devices share the wireless medium and prevent data collisions. Unlike wired networks, wireless signals cannot be simultaneously detected by all devices due to the hidden node problem, where a device might not sense another transmitting station but could still interfere at the receiver.

The main purposes of CSMA/CA are:

1. Collision Prevention: Before transmitting, a device listens to the channel to check if it is idle. If the channel is busy, it waits for a random backoff period, reducing the chance of simultaneous transmissions.
2. Reliable Data Transmission: By avoiding collisions, CSMA/CA improves the probability that data reaches its destination successfully, reducing retransmissions and increasing overall network efficiency.

3. **Efficient Sharing of Medium: In a wireless environment where multiple devices contend for the same channel, CSMA/CA coordinates access, ensuring fair use and minimizing interference.**
4. **Support for ACK Mechanism: CSMA/CA often works with acknowledgment frames. After a successful transmission, the receiver sends an ACK to confirm receipt. If no ACK is received, the sender retransmits after a backoff, further mitigating data loss due to collisions.**

Overall, CSMA/CA is essential in wireless LANs to prevent collisions, maintain reliable communication, and optimize channel utilization in a medium where devices cannot always detect each other directly.

10 Marks :

1. **Explain simplex protocol for noisy and noiseless channel.**

   Simplex Stop-and-Wait Protocol (Noiseless Channel)

   - **In this protocol, communication is one-way (simplex).**
   - **The sender transmits one frame at a time and then waits for the receiver to process it before sending the next.**
   - **The channel is assumed to be error-free (no loss or corruption of frames).**
   - **Problem solved: It provides flow control – prevents the sender from flooding the receiver with more frames than it can process.**
   - **Working:**
     1. **Sender sends a frame.**
     2. **Receiver, after passing data to its network layer, sends back a dummy acknowledgement frame.**
     3. **On receiving acknowledgement, the sender sends the next frame.**
   - **Since no errors occur, there is no need for sequence numbers or retransmission.**

   Simplex Stop-and-Wait Protocol (Noisy Channel)

   - **Here, the channel is unreliable and can introduce errors (frames may be lost or damaged).**
   - **To handle errors, the protocol uses Automatic Repeat Request (ARQ).**
   - **Features:**
     - **Sender transmits one frame, then waits for a positive acknowledgement before sending the next.**
     - **A timer is used. If acknowledgement is not received within a fixed time (due to loss/damage), the sender retransmits the frame.**
     - **To avoid duplication, frames carry sequence numbers so that the receiver can detect and discard duplicates.**
   - **Operation:**
       - **Sender sends frame with a sequence number.**
       - **If receiver receives it correctly, it sends a positive acknowledgement.**
       - **If frame/ack is lost, timer expires and sender retransmits.**
       - **Receiver discards duplicate frames based on sequence number.**

   Key Difference

   - **Noiseless channel: Focus is on flow control only (no errors).**
   - **Noisy channel: Focus is on both error control + flow control (acknowledgements, retransmissions, sequence numbers, timers).**

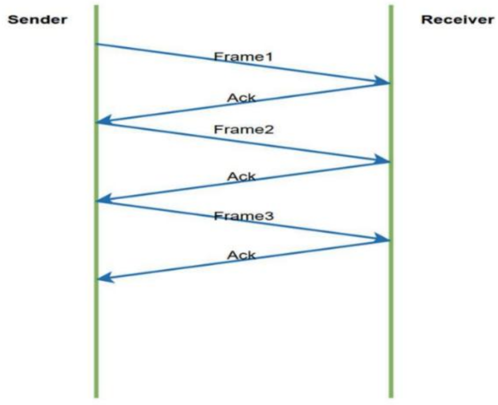


Fig: Stop-and-Wait Protocol Noiseless Channel

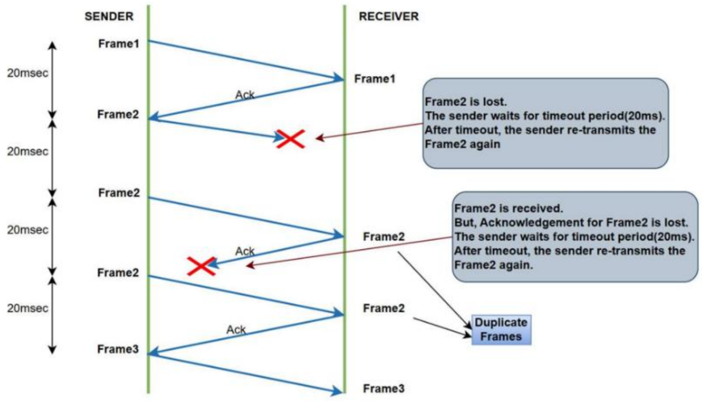


Fig: Stop-and-Wait Protocol Noisey Channel

2. **Explain Data link layer design Issues?**

Data Link Layer – Design Issues

The Data Link Layer (DLL) is the 2nd layer of the OSI model. It receives services from the physical layer and provides services to the network layer. Its main function is to ensure error-free, orderly delivery of frames from one node to another.

The main design issues (services provided by DLL) are:

---

1. Framing

- **DLL breaks the bit stream from the physical layer into frames.**
- **Each frame has a header and trailer to mark start and end.**
- **Techniques: Byte count, Byte stuffing, Bit stuffing, Physical layer coding violations.**

---

2. Physical Addressing

- **Frames include source and destination MAC addresses in the header.**
- **Ensures that the frame reaches the correct device on the same link.**

---

3. Flow Control

- **Prevents a fast sender from overwhelming a slow receiver.**
- **Achieved using stop-and-wait or sliding window methods.**
- **Uses acknowledgements to regulate the rate of transmission.**

---

4. Error Control

- **Ensures error-free transmission of frames.**
- **Errors are detected and corrected using parity check, checksum, CRC, hamming code.**
- **Uses acknowledgements + retransmissions (ARQ) for reliable delivery.**

---

5. Access Control

- **In broadcast networks (like LAN), multiple devices share the same channel.**
- **DLL decides which device gets to use the channel at a time (e.g., CSMA/CD, CSMA/CA).**

✅ **Summary:**

The DLL must handle framing, addressing, flow control, error control, and access control to provide reliable and efficient communication to the network layer.

3. **Cyclic Redundancy Check: Data = 100100, Generator Polynomial (Key) = x3 + x2 + 1 (1101)**
   Cyclic Redundancy Check (CRC)
   Given:
   - **Data = 100100**
   - **Generator Polynomial (Key) = x3+x2+1→ Binary = 1101**
   - **Degree of generator = 3 ⇒ Append 3 zeros to data.**

Step 1: Append Zeros
100100 ⇒ 100100000
(Appended 3 zeros because generator has 4 bits).

Step 2: Division by Generator (Modulo-2)
Perform binary division of 100100000 ÷ 1101:

1. **1001 ÷ 1101 → quotient 1, remainder = 1001 ⊕ 1101 = 0010**
   Bring down next bit → 0100
2. **0100 < 1101 → quotient 0, remainder stays 0100**
   Bring down next bit → 1000
3. **1000 < 1101 → quotient 0, remainder stays 1000**
   Bring down next bit → 0000
4. **0000 < 1101 → remainder = 001 (final).**

So, CRC bits = 001.

Step 3: Form Codeword
Replace the 3 zeros with CRC bits:
100100000⇒100100001

Step 4: Verification
At receiver side:
100100001÷1101=remainder 000 (valid)
Hence, no error in transmission.

Final Answer (10 Marks)

- **Appended Data = 100100000**
- **Generator Polynomial = 1101**
- **CRC bits = 001**
- **Transmitted Codeword = 100100001**
- **Verification remainder = 000 (error-free transmission)**

4. **Analyze A simplex stop and wait protocol for noisy channel?**
   Simplex Stop-and-Wait Protocol for Noisy Channel
   Introduction
   - **In a noisy channel, frames can be lost or damaged during transmission.**
   - **The simplex stop-and-wait protocol is modified to handle such errors.**

- This method is also known as Automatic Repeat reQuest (ARQ) or Positive Acknowledgement with Retransmission (PAR).

Working

1. Frame Transmission:
    - Sender sends one frame at a time.
    - Each frame carries a sequence number (usually 0 or 1).
2. Acknowledgement (ACK):
    - Receiver checks the frame.
    - If correct → sends positive ACK back.
    - If damaged/lost → receiver sends nothing.
3. Timer Mechanism:
    - Sender starts a timer after sending the frame.
    - If ACK is received before timeout → sender sends the next frame.
    - If timer expires (ACK lost or frame corrupted) → frame is retransmitted.
4. Duplicate Handling:
    - If a frame is retransmitted but the old one was already delivered, the receiver identifies duplicates using the sequence number and discards them.

Modes of Operation

- Normal Operation: Frame is received correctly and acknowledged.
- Timeout & Retransmission: When either frame or ACK is lost, sender retransmits after timeout.

Advantages

- Provides reliable and error-free transmission in noisy channels.
- Simple to implement.

Limitations

- Low efficiency (only one frame at a time).
- Wastage of bandwidth due to retransmissions and waiting.
- High delays in case of multiple errors.

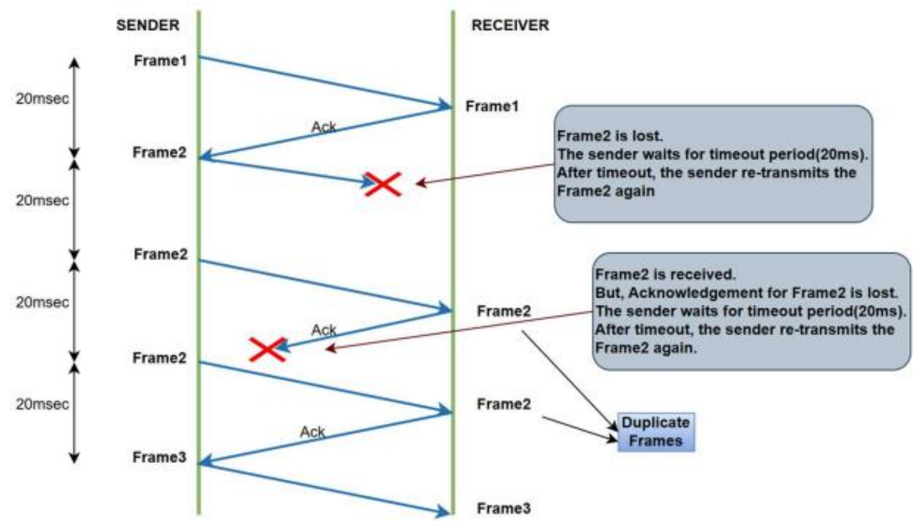


Fig: Stop-and-Wait Protocol Noisey Channel

5. **Elaborate about Multiple access protocols: ALOHA?**

Multiple Access Protocols – ALOHA

Introduction

- **In a broadcast network, many stations share a single communication channel.**
- **ALOHA is the simplest multiple access protocol, originally designed for wireless communication in Hawaii.**
- **Any station can transmit data at any time, but collisions may occur if two or more stations transmit simultaneously.**

Types of ALOHA

1. Pure ALOHA

- **Any station transmits whenever it has data.**
- **If two or more stations transmit at the same time, collision occurs → all collided frames are destroyed.**
- **Sender waits for an ACK from the receiver:**
    - **If ACK not received → retransmits after a random back-off time.**
- **Vulnerable time = 2 × frame transmission time (2Tfr).**
- **Efficiency ≈ 18% (only ~18% of the channel capacity is utilized).**

---

2. Slotted ALOHA

- **Time is divided into equal slots (each slot = one frame transmission time).**
- **A station can send only at the beginning of a slot.**
- **If two or more stations choose the same slot → collision occurs.**
- **Collided frames are retransmitted after a random slot delay.**
- **Vulnerable time = 1 × frame transmission time (Tfr).**
- **Efficiency ≈ 37% (better than pure ALOHA).**

Advantages

- **Very simple and decentralized protocol.**
- **Works well for low traffic conditions.**
- **Suitable for wireless LANs and satellite networks.**

Limitations

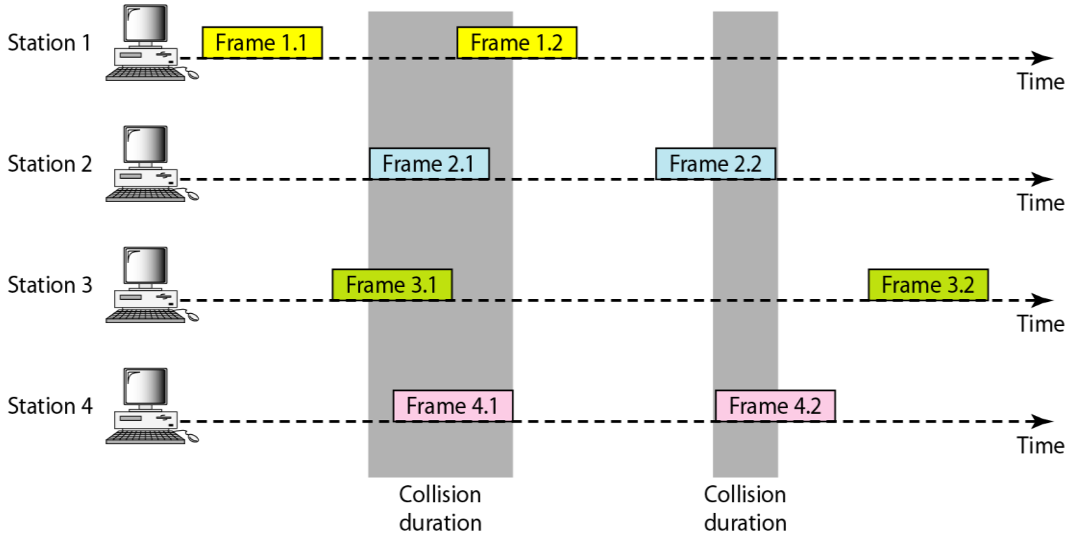
- **High collision rate at heavy traffic.**
- **Poor efficiency (18% for Pure ALOHA, 37% for Slotted ALOHA).**
- **Wastage of bandwidth due to retransmissions.**

✅ **Summary:**

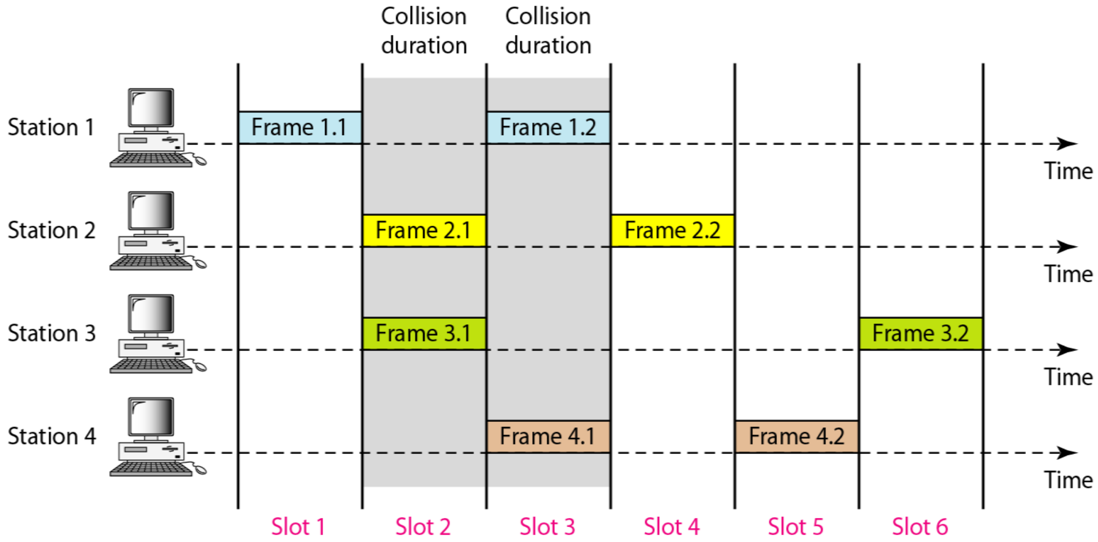
ALOHA is a random access protocol where stations transmit without prior coordination.

- **Pure ALOHA allows transmission anytime (efficiency 18%).**
- **Slotted ALOHA restricts transmission to time slots (efficiency 37%).**

Pure ALOHA:



Slotted ALOHA:



6. **Discuss about Wireless LANs?**

Wireless LANs (WLANs)

Introduction

- **A Wireless Local Area Network (WLAN) is a LAN that uses radio waves or infrared signals instead of cables.**
- **It allows devices like laptops, mobiles, and IoT devices to communicate within a limited area (office, campus, home) without physical wires.**
- **Most common standard: IEEE 802.11 (Wi-Fi).**

Characteristics of WLANs

1. **Wireless Medium – Uses radio frequency (2.4 GHz, 5 GHz, 6 GHz) instead of copper/fiber cables.**
2. **Mobility – Users can move freely within the coverage area while staying connected.**
3. **Flexibility – Easy installation, no cabling required.**
4. **Broadcast Nature – Frames are transmitted over the air; hence subject to interference and collisions.**

Components of WLAN

- **Access Point (AP): Central device that connects wireless stations to the wired network.**
- **Stations (STA): Wireless-enabled devices like laptops, smartphones.**
- **Distribution System: Interconnects multiple access points to extend coverage.**

Medium Access Control in WLAN

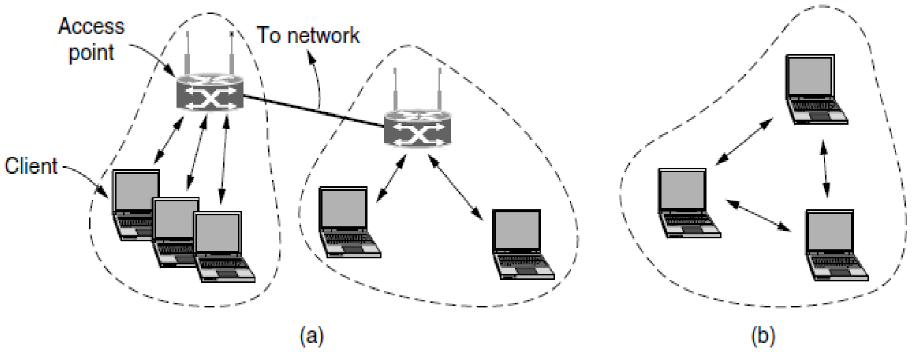
- **Because the medium is shared, WLANs use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).**
- **Steps:**
  1. **A station listens to check if the channel is idle.**
  2. **If idle → it sends data after a short waiting period.**
  3. **If busy → it waits for a random back-off time.**
  4. **Acknowledgement (ACK) is sent by receiver to confirm successful delivery (since collisions can't always be detected directly in wireless).**

Advantages

- **Mobility → users can connect anywhere within coverage area.**
- **Easy installation & scalability.**
- **Flexibility → supports laptops, smartphones, IoT devices.**

Disadvantages

- **Lower security (prone to eavesdropping, hacking).**
- **Interference from other devices (microwave, Bluetooth).**
- **Limited range compared to wired LANs.**



802.11 architecture. (a) Infrastructure mode. (b) Ad-hoc mode.

7. **Explain about A protocol using Go-Back-N.?**

Protocol using Go-Back-N ARQ

Introduction

- **Go-Back-N ARQ is a sliding window protocol used for error control in noisy channels.**
- **It allows the sender to transmit multiple frames (N frames) before receiving an acknowledgment.**
- **Improves efficiency compared to Stop-and-Wait, where only one frame is sent at a time.**

Working Principle

1. **Sender Side:**
   - Maintains a window of size N.
   - Can send up to N unacknowledged frames continuously (pipelining).
   - Each frame has a sequence number.
2. **Receiver Side:**
   - Receiver window size = 1 (it only accepts the next expected frame in order).
   - If the correct frame is received → sends ACK for the next expected frame.
   - If a frame is lost or damaged, receiver discards it and all subsequent frames (even if correct).
3. **Error Handling:**
   - If ACK is not received within timeout → sender goes back to the lost frame and retransmits that frame and all frames after it.

Example

- Window size = 4
- Frames sent: 0, 1, 2, 3
- If frame 1 is lost → receiver discards frames 2, 3.
- Sender times out → retransmits frames 1, 2, 3.

Advantages

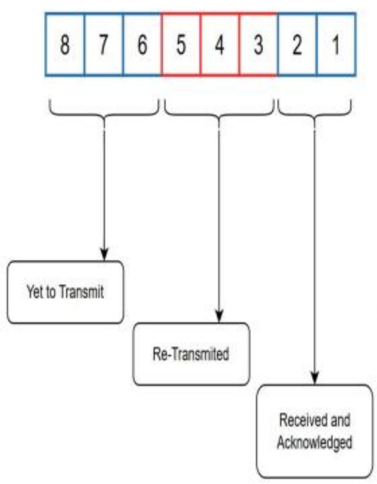
- More efficient than Stop-and-Wait (sends multiple frames).
- Provides reliable transmission with error control.

Limitations

- Wastage of bandwidth: Even correctly received frames after a lost one are retransmitted.
- Receiver is simple, but sender needs more buffer & timer management.

✅ Summary:

Go-Back-N ARQ is a sliding window protocol where the sender can transmit multiple frames before ACK, but if a frame is lost, it retransmits that frame and all subsequent frames. This increases efficiency compared to Stop-and-Wait but may waste bandwidth in case of frequent errors.



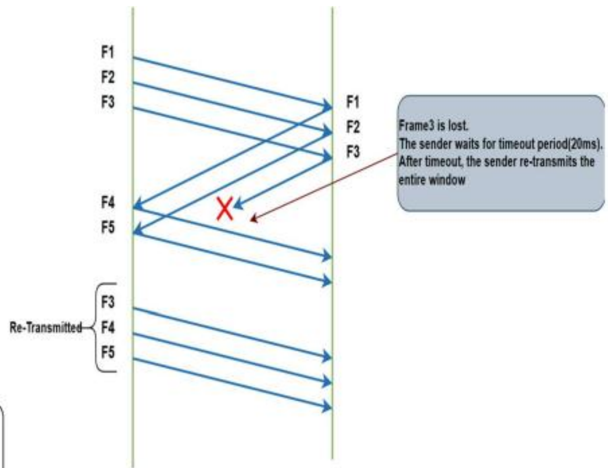


Fig: Go-Back-N ARQ Protocol

8. **Elaborate The channel allocation problem in detail?**

The Channel Allocation Problem

Introduction

- **In broadcast networks (like LANs and wireless), multiple users share a single communication channel.**
- **The channel allocation problem is: *How to allocate the single channel fairly and efficiently among multiple users who want to transmit at the same time?***
- **Improper allocation can cause collisions, idle channel time, or unfair access.**

Methods of Channel Allocation

1. Static Channel Allocation

- **Based on traditional multiplexing schemes (FDM, TDM).**
- **If there are N users, the channel is divided into N equal portions (frequency bands or time slots).**
- **Each user is assigned one fixed portion, whether or not they are active.**
- **Advantages: Simple, no collisions.**
- **Disadvantages:**
    - **Inefficient for bursty traffic (when users are idle, their bandwidth is wasted).**
    - **If more than N users want to transmit, they cannot access the channel.**

---

2. Dynamic Channel Allocation

- **No fixed division; the channel is allocated on demand.**
- **Assumptions made:**
    1. **Independent traffic – Each station generates frames independently.**
    2. **Single channel – All stations use the same channel for transmission/reception.**
    3. **Observable collisions – If two transmit simultaneously, signals collide, and both fail.**
    4. **Continuous or slotted time – Transmission can start anytime (continuous) or only at slot boundaries (slotted).**
    5. **Carrier sense or no carrier sense – Stations may or may not sense the channel before transmitting.**
- **Examples: ALOHA, Slotted ALOHA, CSMA, CSMA/CD, CSMA/CA.**

Summary

- **The channel allocation problem is fundamental in networks where multiple stations share the same medium.**
- **Static allocation (FDM/TDM) is simple but wastes bandwidth with bursty traffic.**
- **Dynamic allocation is more efficient, using protocols like ALOHA and CSMA to manage access and minimize collisions.**

✅ **Final Note (10 marks):**

Channel allocation is about who gets to use the channel, when, and how. It can be done either by static fixed division or by dynamic demand-based protocols, with dynamic methods being preferred in modern, bursty-traffic networks.

9. **Explain Carrier sense multiple access protocols.?**

Carrier Sense Multiple Access (CSMA) Protocols

Introduction

- **CSMA is a multiple access protocol used in broadcast networks (e.g., LAN, wireless) to reduce collisions.**
- **Before transmitting, each station "listens" (senses) the channel:**
  - **If channel is idle → it transmits.**
  - **If channel is busy → it waits.**
- **Still, collisions may occur due to propagation delay (two stations may sense idle at nearly the same time).**

Types of CSMA

1. 1-Persistent CSMA

- **Station senses the channel.**
- **If idle → it transmits immediately (with probability 1).**
- **If busy → it keeps sensing continuously and transmits as soon as the channel becomes free.**
- **Advantage: Simple, high channel utilization.**
- **Disadvantage: High chances of collision (many stations transmit immediately).**

---

2. Non-Persistent CSMA

- **Station senses the channel.**
- **If idle → it transmits immediately.**
- **If busy → instead of waiting continuously, it waits for a random time before sensing again.**
- **Advantage: Reduces collisions compared to 1-persistent.**
- **Disadvantage: Longer delay, channel may remain idle unnecessarily.**

---

3. p-Persistent CSMA (used in slotted channels)

- **Station senses the channel.**
- **If idle → it transmits with probability p, or defers with probability (1 – p) until the next time slot.**
- **If busy → it waits until the next slot and repeats the process.**
- **Advantage: Balances between throughput and collisions.**
- **Disadvantage: Needs slot synchronization.**

Advantages of CSMA

- **Reduces collisions compared to pure ALOHA.**
- **Simple and decentralized.**
- **Suitable for both wired (Ethernet) and wireless systems.**

Limitations

- **Collisions still occur due to propagation delay.**
- **Wasted bandwidth during collisions.**
- **Performance degrades with high traffic load.**

✅ **Summary:**

Carrier Sense Multiple Access (CSMA) protocols are listen-before-transmit techniques to minimize collisions. Variants are 1-persistent, non-persistent, and p-persistent CSMA, each balancing efficiency and collision probability differently.

```
              +---------------------+
              |   Sense the Channel  |
              +---------------------+
                  /              \
         Channel Idle        Channel Busy
               |                   |
    +----------------+     +------------------+
    | Transmit Frame |     |   1-Persistent    | → Keep sensing, send immediately
    +----------------+     |   Non-Persistent  | → Wait random time, sense again
                           |   p-Persistent    | → Send with probability p
```

10. Discuss Data link layer switching?

Data Link Layer Switching

Introduction

- **Switching at the data link layer is performed by LAN switches (Layer-2 switches).**
- **It improves performance of local area networks by reducing collisions and providing direct communication between devices.**
- **Unlike hubs (which broadcast frames everywhere), switches forward frames only to the intended destination using MAC addresses.**

Functions of Data Link Layer Switching

1. **Forwarding & Filtering**
   - **Switch receives a frame, checks the destination MAC address, and forwards it only to the correct port.**
   - **If destination is unknown → broadcast to all ports (except source port).**
2. **Learning**
   - **Switch maintains a MAC address table (forwarding table) by learning which devices are connected to which ports.**
   - **This table is updated dynamically.**
3. **Loop Avoidance**
   - **In networks with redundant paths, loops can occur.**
   - **Protocols like Spanning Tree Protocol (STP) are used to prevent infinite looping of frames.**

Types of Data Link Layer Switching

1. **Store-and-Forward Switching**
   - **Switch receives the entire frame, checks it for errors (CRC), and then forwards it.**
   - **More reliable but adds delay.**
2. **Cut-Through Switching**

- Switch forwards the frame as soon as the destination address is read (without waiting for full frame).
- Faster but errors may be forwarded.

3. Fragment-Free Switching
   - Hybrid approach → reads the first 64 bytes (where most errors occur) before forwarding.

Advantages

- Reduces collision domains → better performance than hubs.
- Provides full-duplex communication.
- Efficient use of bandwidth (no unnecessary broadcasting).

Disadvantages

- More expensive than hubs.
- Still vulnerable to broadcast storms (if too many broadcasts).
- Works only with MAC addresses, not IP-level routing.

✅ Summary:

Data Link Layer switching (Layer-2 switching) uses MAC addresses to forward frames intelligently. It provides learning, forwarding, filtering, and loop prevention, making LANs more efficient compared to hubs or repeaters.

```
         +-------------------+
         |      Switch       |
         |  (Layer-2 Device) |
         +-------------------+
          /       |       \
         /        |        \
        /         |         \
   PC-A          PC-B       PC-C
 (MAC: A)      (MAC: B)   (MAC: C)


Working:
- Switch builds MAC table:
   Port 1 → MAC A
   Port 2 → MAC B
   Port 3 → MAC C
- If PC-A sends data to PC-B:
   Switch forwards only to Port 2 (PC-B).
- No broadcast to PC-C → Efficient communication.
```