Question 1

a) Briefly explain the functions of each layer of the OSI Reference Model.

The OSI (Open Systems Interconnection) Reference Model consists of seven layers, each with specific functions:

1. Physical Layer (Layer 1):
    - Function: Handles the physical connection between devices. It deals with the transmission and reception of raw bit streams over a physical medium (e.g., cables, switches).
    - Examples: Ethernet, USB, Bluetooth.
2. Data Link Layer (Layer 2):
    - Function: Responsible for node-to-node data transfer and error detection and correction. It ensures that data is transferred correctly between two physically connected devices.
    - Examples: Ethernet, Wi-Fi (802.11), MAC addresses.
3. Network Layer (Layer 3):
    - Function: Manages data routing, forwarding, and addressing between networks. It determines the best path for data to travel from source to destination.
    - Examples: IP (Internet Protocol), ICMP (Internet Control Message Protocol).
4. Transport Layer (Layer 4):
    - Function: Provides reliable data transfer services to the upper layers. It ensures complete data transfer through error recovery and flow control.
    - Examples: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
5. Session Layer (Layer 5):
    - Function: Manages sessions or connections between applications. It establishes, maintains, and terminates communication sessions.
    - Examples: NetBIOS, RPC (Remote Procedure Call).
6. Presentation Layer (Layer 6):

- **Function:** Translates data between the application layer and the network. It handles data encoding, encryption, and compression.
- **Examples:** SSL/TLS (Secure Sockets Layer/Transport Layer Security), JPEG, ASCII.

7. **Application Layer (Layer 7):**
    - **Function:** Provides network services directly to end-user applications. It facilitates communication between software applications and lower layers.
    - **Examples:** HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol).

b) The Frame Check Sequence (FCS) is an important functionality in networking.

i. At which layer is FCS performed?

Answer: Data Link Layer (Layer 2).

ii. Describe how FCS works in the end-to-end delivery of data from a sender to a receiver.

Frame Check Sequence (FCS):

- **Purpose:** FCS is used to detect errors in frames transmitted over a network.
- **Working:**
    i. **Sender Side:**
        - When a data frame is created, the sender calculates a checksum based on the frame's contents using a CRC (Cyclic Redundancy Check) algorithm.
        - This checksum is appended to the frame as the FCS.
    ii. **Transmission:**
        - The frame, including the FCS, is transmitted over the network to the receiver.
    iii. **Receiver Side:**
        - The receiver extracts the frame and calculates its own checksum using the same CRC algorithm on the received data.

- The receiver compares this calculated checksum with the received FCS.
- If the two checksums match, the data is considered to be intact and error-free.
- If there is a mismatch, it indicates that the data has been corrupted during transmission, and the receiver can request a retransmission of the frame.

c) X.25 is a legacy suite of protocols used for packet switching. With the help of a diagram, describe the different devices in the X.25 protocol.

X.25 Protocol:

- Definition: X.25 is an ITU-T standard protocol suite for packet-switched data communication in public data networks.
- Devices:
    i. DTE (Data Terminal Equipment):
        - End-user devices that generate and consume data (e.g., computers, terminals).
    ii. DCE (Data Circuit-terminating Equipment):
        - Network devices that establish, maintain, and terminate the data connection (e.g., modems, packet-switching nodes).
    iii. PAD (Packet Assembler/Disassembler):
        - Devices that convert data from asynchronous terminal formats into the synchronous format required for transmission over an X.25 network, and vice versa.

Diagram:

```
[DTE] <--> [DCE] <--> [PAD] <--> [X.25 Network] <--> [PAD] <--> [DCE] <--> [DTE]
```

This should comprehensively answer all parts of Question 1. If you need further clarification or additional details, please let me know!

Question 2

Let's address each part of Question 2 based on the provided instructions.

a) Explain the differences between multimode and single mode optical fiber links.

Multimode Optical Fiber:

- Core Diameter: Larger core diameter (50 or 62.5 microns).
- Light Propagation: Allows multiple modes (paths) of light to propagate.
- Distance: Suitable for shorter distances (up to 2 km).
- Bandwidth: Lower bandwidth compared to single mode.
- Cost: Less expensive and easier to work with due to the larger core size.
- Applications: Typically used for local area networks (LANs) and within buildings.

Single Mode Optical Fiber:

- Core Diameter: Smaller core diameter (8 to 10 microns).
- Light Propagation: Allows only one mode (path) of light to propagate.
- Distance: Suitable for longer distances (up to 100 km or more).
- Bandwidth: Higher bandwidth and less signal attenuation compared to multimode.
- Cost: More expensive and requires more precise alignment due to the smaller core size.
- Applications: Typically used for telecommunications and long-distance data transmission.

b) Twisted pair and coaxial cables are two different types of medium which are also utilized in networks. Describe how each works and list one (1) application for each.

Twisted Pair Cable:

- Working: Consists of pairs of insulated copper wires twisted together. The twisting reduces electromagnetic interference (EMI) and crosstalk between pairs.

Commonly used types include unshielded twisted pair (UTP) and shielded twisted pair (STP).
- Application: Used in Ethernet networks for data transmission (e.g., Cat5e, Cat6 cables in LANs).

Coaxial Cable:

- Working: Consists of a central conductor surrounded by an insulating layer, a metallic shield, and an outer insulating layer. The metallic shield provides protection against EMI and allows for higher frequency transmission over longer distances compared to twisted pair cables.
- Application: Used in cable television (CATV) systems and broadband internet connections.

c) In a typical household scenario, there are many requests coming from different devices to use the Internet. However, the ONT device, acting also as a NAT box, is allocated a single public IP address.

Explain how the NAT box knows how to redirect these requests to their respective PCs.

Network Address Translation (NAT):

- Working:
    - Translation Table: The NAT box maintains a translation table that maps each internal private IP address and port number to the external public IP address and port number.
    - Outgoing Requests: When a device in the household sends a request to the internet, the NAT box replaces the private IP address and port number with the public IP address and a unique port number. This information is stored in the translation table.
    - Incoming Responses: When the response arrives from the internet, the NAT box uses the port number in the translation table to identify the corresponding internal private IP address and port number. It then forwards the response to the correct device within the household.

d) In addition to the IP protocol, the internet also uses other control protocols in the network layer. Two of these protocols are ICMP and DHCP. Briefly explain how each of them work.

ICMP (Internet Control Message Protocol):

- Purpose: Used for network diagnostics and error reporting. It is primarily utilized by network devices to send error messages and operational information.
- Working: Commonly used messages include Echo Request and Echo Reply (used by the `ping` command) to test connectivity, and Destination Unreachable messages to indicate that a destination cannot be reached.

DHCP (Dynamic Host Configuration Protocol):

- Purpose: Automates the process of assigning IP addresses and other network configuration parameters to devices on a network.
- Working:
    - DHCP Discover: The client broadcasts a DHCP Discover message to locate available DHCP servers.
    - DHCP Offer: A DHCP server responds with a DHCP Offer message containing an available IP address and configuration information.
    - DHCP Request: The client responds with a DHCP Request message indicating it accepts the offered IP address.
    - DHCP Acknowledgment: The DHCP server sends a DHCP Acknowledgment message confirming the IP address assignment and providing any additional configuration details.

Question 3

a) Briefly describe the process of Stop-and-wait ARQ and Go Back N ARQ in detecting errors.

Stop-and-wait ARQ:

- Process:
    i. Sender: Sends one frame and waits for an acknowledgment (ACK) from the receiver before sending the next frame.
    ii. Receiver: Receives the frame, checks for errors, and sends an ACK if the frame is error-free. If an error is detected, the receiver discards the frame and does not send an ACK.
    iii. Timeout: If the sender does not receive an ACK within a certain period, it assumes the frame was lost or damaged and retransmits the frame.
- Error Detection: Relies on ACKs and timeouts to ensure each frame is correctly received.

Go Back N ARQ:

- Process:
    i. Sender: Can send multiple frames (up to a window size N) before needing an ACK for the first frame. Frames are sent in sequence.
    ii. Receiver: Receives frames and sends cumulative ACKs. If a frame is received with errors, the receiver discards it and all subsequent frames until the errored frame is correctly received.
    iii. Retransmission: If an error is detected or an ACK is not received for a frame within the window, the sender goes back and retransmits that frame and all subsequent frames in the sequence.
- Error Detection: Uses cumulative ACKs and retransmission of a sequence of frames to ensure error-free delivery.

b) Using a suitable example, differentiate between vertical redundancy check and longitudinal redundancy check.

Vertical Redundancy Check (VRC):

- Also Known As: Parity Check.
- Process:
    - Adds a parity bit to each data unit (byte, character) to ensure the total number of 1s is even (even parity) or odd (odd parity).
- Example:
    - Data: `1011001` (7 bits)

    - Even Parity: Add a parity bit `1` to make the total number of 1s even: `10110011`

Longitudinal Redundancy Check (LRC):

- Process:
    - Adds a parity bit to a block of data units by performing a bitwise XOR operation across each bit position in the block. This generates a parity byte.
- Example:

```
Data Block:
10110011
11001010
00101101
11100001
```

    - Perform bitwise XOR on each column:

```
Parity Byte:
11110101
```

    - Data Block with LRC:

```
10110011
11001010
00101101
11100001
11110101 (LRC)
```

c) Some networking protocols are designed to optimize the routing of traffic when multiple stations are transmitting concurrently using the same communications channel. ALOHA is one such protocol designed to avoid collisions.

i. Explain how ALOHA works.

ALOHA Protocol:

- Process:
    i. **Transmission:** A station transmits data whenever it has data to send.
    ii. **Collision:** If two stations transmit simultaneously, a collision occurs, and both transmissions are garbled.
    iii. **Acknowledgment:** The sender listens for an acknowledgment. If an ACK is received, the transmission was successful.
    iv. **Retransmission:** If no ACK is received within a certain time, the sender waits for a random period and retransmits the data.

Efficiency: ALOHA's efficiency is low (18.4%) due to a high probability of collisions.

ii. Using a suitable diagram, explain how SLOTTED ALOHA improves the transmission of information in shared channels.

SLOTTED ALOHA:

- Improvement:
    - Divides time into discrete slots, and transmissions can only begin at the start of a time slot.
    - Reduces the probability of collisions since collisions can only occur when two stations transmit in the same slot.

Diagram:

```
Time Slots:
 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
 Station 1:    [-----]
 Station 2:            [-----]

Only one transmission per slot:
[Transmission]
[    Slot    ]
```

Efficiency: SLOTTED ALOHA has higher efficiency (36.8%) compared to pure ALOHA.

Question 4

a) Explain the impact of signal loss and fading, multipath distortion, and shared airwaves on the performance of Wireless Networks.

Signal Loss and Fading:

- Impact:
    - Signal loss refers to the reduction in signal strength as it travels through the air. This can be due to distance, obstacles (like walls), and environmental factors.
    - Fading occurs due to variations in the transmission medium, leading to fluctuations in signal strength.
    - Performance: Signal loss and fading can result in lower data rates, higher error rates, and reduced coverage area. It can cause interruptions and degrade the quality of communication.

Multipath Distortion:

- Impact:
    - Occurs when transmitted signals take multiple paths to reach the receiver due to reflections, refractions, or scattering.
    - These multiple signals can arrive at different times, causing interference and distortion.
    - Performance: Multipath distortion can cause signal interference, leading to higher error rates, reduced data throughput, and poor signal quality.

Shared Airwaves:

- Impact:
    - Wireless networks operate in shared frequency bands, meaning multiple devices and networks use the same airwaves.
    - Performance: This can lead to congestion, increased collisions, and interference, reducing the overall network performance and causing

delays and packet loss.

b) Briefly describe the key components in a Wireless Network.

Key Components:

1. Access Points (APs):
    - Devices that allow wireless devices to connect to a wired network using Wi-Fi.
    - Act as a bridge between the wireless and wired portions of the network.
2. Wireless Controllers:
    - Centralized devices that manage multiple access points, providing configuration, management, and security.
3. Client Devices:
    - Devices such as laptops, smartphones, tablets, and IoT devices that connect to the network wirelessly.
4. Antennas:
    - Transmit and receive radio signals, extending the coverage and improving the signal quality of wireless networks.
5. Wireless Network Interface Cards (NICs):
    - Hardware installed in client devices, enabling them to connect to wireless networks.
6. Router:
    - Directs data packets between networks, typically integrating with an access point in home networks.

c) Explain how CSMA works in Wireless Networks.

Carrier Sense Multiple Access (CSMA):

- Process:
    i. Carrier Sensing: Before transmitting, a device listens to the channel to check if it is free (no other device is transmitting).
    ii. Collision Avoidance: If the channel is free, the device proceeds to transmit its data. If the channel is busy, the device waits for a random period before checking again.

iii. **Acknowledgment:** After transmitting, the device waits for an acknowledgment from the receiver. If an acknowledgment is received, the transmission is successful. If not, the device assumes a collision occurred and retransmits after a random backoff period.

In Wireless Networks:

- Wireless networks often use CSMA/CA (Collision Avoidance) to reduce the probability of collisions since they cannot detect collisions as easily as wired networks.
- **Steps:**
    i. **Request to Send (RTS):** The sender sends an RTS frame to the receiver indicating it wants to transmit data.
    ii. **Clear to Send (CTS):** The receiver responds with a CTS frame if it is ready to receive.
    iii. **Data Transmission:** The sender transmits the data.
    iv. **Acknowledgment (ACK):** The receiver sends an ACK frame upon successful receipt of the data.

d) Explain how buffering and traffic shaping work in the improvement of QoS, and provide one application where each technique is particularly useful.

Buffering:

- **Working:** Temporary storage of data packets in a buffer (memory) to manage variations in data flow. It smooths out bursts of traffic and prevents packet loss by holding excess data until the network can handle it.
- **Improvement in QoS:** Reduces jitter and smooths data delivery, ensuring a consistent flow of data. Helps in handling network congestion and preventing packet loss.
- **Application:** Video streaming services like Netflix use buffering to ensure smooth playback despite network variability.

Traffic Shaping:

- **Working:** Controls the volume and rate of traffic being sent into the network. It

prioritizes certain types of traffic, regulates bandwidth usage, and ensures critical applications receive the necessary bandwidth.

- Improvement in QoS: Ensures that high-priority traffic (e.g., VoIP, streaming) is transmitted smoothly without interruptions. It helps in managing network congestion and maintaining performance for critical applications.
- Application: VoIP services use traffic shaping to prioritize voice packets, ensuring clear and uninterrupted communication.

Question 5

a) Describe the different layers in the TCP/IP Reference model.

The TCP/IP Reference Model consists of four layers:

1. Application Layer:
    - Function: Provides protocols and services directly to end-users and applications.
    - Examples: HTTP, FTP, SMTP, DNS, Telnet.
2. Transport Layer:
    - Function: Provides end-to-end communication services for applications. It ensures complete data transfer and error recovery.
    - Examples: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
3. Internet Layer:
    - Function: Handles logical addressing, routing, and packet forwarding. It ensures that data packets reach their destination across multiple networks.
    - Examples: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).
4. Network Access Layer (Link Layer):
    - Function: Manages the physical transmission of data on the network. It includes hardware addressing and error detection.
    - Examples: Ethernet, Wi-Fi (802.11), PPP (Point-to-Point Protocol).

b) Transport Protocols include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Compare and contrast TCP and UDP.

Transmission Control Protocol (TCP):

- Connection-oriented: Establishes a connection before transmitting data.
- Reliability: Provides error checking, retransmission, and acknowledgment to ensure reliable data transfer.
- Flow Control: Manages data flow to prevent congestion.
- Sequence: Data is transmitted and received in order.
- Use Cases: Suitable for applications that require reliable communication, such as web browsing (HTTP), email (SMTP), and file transfer (FTP).

User Datagram Protocol (UDP):

- Connectionless: Sends data without establishing a connection.
- Unreliable: Does not guarantee data delivery, no error checking, or retransmission.
- No Flow Control: Transmits data without managing data flow.
- Sequence: Data may arrive out of order.
- Use Cases: Suitable for applications that require fast, efficient transmission and can tolerate some data loss, such as video streaming, online gaming, and VoIP.

Comparison:

- TCP: Reliable, connection-oriented, with flow control and error checking.
- UDP: Unreliable, connectionless, with no flow control or error checking.

c) TCP Service Model includes the use of ports. What are ports?

Ports:

- Definition: A port is a numerical identifier in the TCP/IP networking model that is used to distinguish between different services or applications running on the same host.
- Function: Ports allow multiple network services to run on a single IP address by differentiating traffic based on port numbers.

- **Range:** Port numbers range from 0 to 65535. Ports 0-1023 are known as well-known ports, 1024-49151 are registered ports, and 49152-65535 are dynamic or private ports.

d) Routing protocols utilize algorithms to dictate how to route traffic. Two such algorithms are the 'Distance Vector Algorithm' and 'Link State Algorithm'. Explain how each work.

Distance Vector Algorithm:

- **Function:** Each router maintains a table (vector) of the minimum distance (cost) to every other router and periodically shares this information with its immediate neighbors.
- **Working:**
    i. **Initialization:** Each router knows the distance to its direct neighbors.
    ii. **Update:** Routers exchange distance vectors with neighbors.
    iii. **Calculation:** Each router updates its table based on the received vectors, choosing the shortest path to each destination.
    iv. **Convergence:** This process continues until all routers have consistent distance vectors.
- **Example Protocol:** RIP (Routing Information Protocol).

Link State Algorithm:

- **Function:** Each router maintains a map of the entire network (link-state database) and uses it to calculate the shortest path to every other router.
- **Working:**
    i. **Initialization:** Each router discovers its neighbors and measures the cost to each.
    ii. **Flooding:** Routers broadcast link-state packets (LSPs) to all other routers in the network.
    iii. **Database Update:** Each router updates its link-state database with the received LSPs.
    iv. **Shortest Path Calculation:** Routers use Dijkstra's algorithm to calculate the shortest path to every destination based on the link-state database.

v. **Routing Table Update:** Each router updates its routing table with the shortest paths.

- **Example Protocol:** OSPF (Open Shortest Path First).