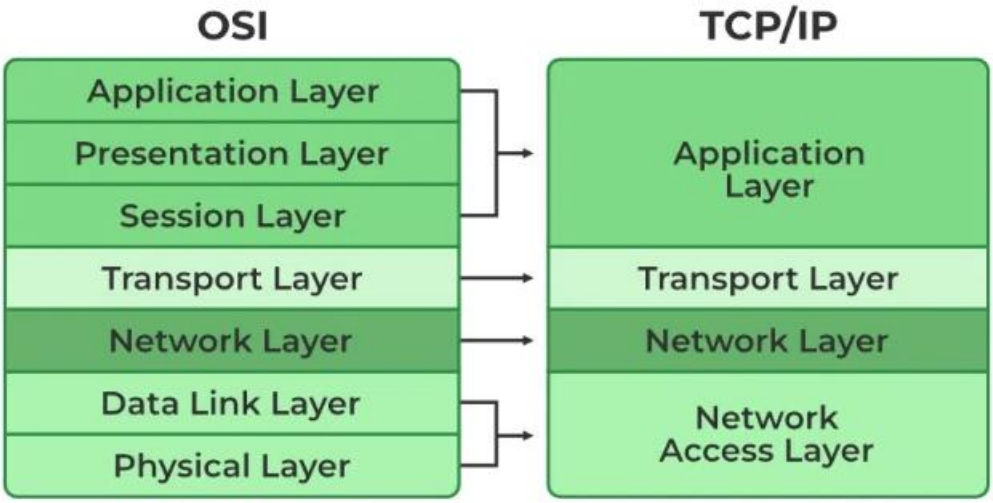
CNND DEC & MAY 2022 Answers

Q1

a) Explain TCP/IP reference model

The **TCP/IP Reference Model** is a conceptual framework used to design and implement networks. It forms the backbone of modern internet communication. The model simplifies how data is transmitted across interconnected devices and is based on standardized layers, each with specific functions.



TCP/IP and OSI

Layers of the TCP/IP Model:

1. **Application Layer**:
    - Provides user interfaces and network services.
    - Deals with protocols like HTTP (web browsing), SMTP (email), and FTP (file transfer).
    - Equivalent to the Application, Presentation, and Session layers of the OSI model.

2. **Transport Layer**:
    - Ensures reliable data transfer between devices using protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
    - Handles error checking, data segmentation, and flow control.

3. **Internet Layer**:
    - Handles the routing of data across networks by assigning IP addresses.
    - Protocols like IP (Internet Protocol) and ICMP (Internet Control Message Protocol) are used here.
    - Ensures the data packet reaches its destination.

4. **Network Access Layer (Link Layer)**:
    - Manages data exchange between the device and the physical network (like Ethernet or Wi-Fi).
    - Deals with hardware addressing (MAC addresses) and protocols like ARP (Address Resolution Protocol).

c) Explain different classes of IPV4 IP Address.

IPv4 addresses are **32-bit** binary numbers, divided into **five classes**: **A, B, C, D, and E**, based on their **starting bits** and **address range**.

1. Class A

- **Starting Bits**: 0
- **Range**: 1.0.0.0 to 126.255.255.255
- **Default Subnet Mask**: 255.0.0.0
- **Use**: For very **large networks** (e.g., ISPs)
- **Hosts per Network**: ~16 million

2. Class B

- **Starting Bits**: 10
- **Range**: 128.0.0.0 to 191.255.255.255
- **Default Subnet Mask**: 255.255.0.0
- **Use**: For **medium-sized networks**
- **Hosts per Network**: ~65,000

3. Class C

- **Starting Bits**: 110
- **Range**: 192.0.0.0 to 223.255.255.255
- **Default Subnet Mask**: 255.255.255.0
- **Use**: For **small networks**
- **Hosts per Network**: 254

4. Class D (Multicast)

- **Starting Bits**: 1110
- **Range**: 224.0.0.0 to 239.255.255.255
- **Use**: **Multicasting** (one-to-many communication)
- **Not used for normal host communication**

5. Class E (Reserved)

- **Starting Bits**: 1111
- **Range**: 240.0.0.0 to 255.255.255.255
- **Use**: **Experimental & research purposes only**

Q3

a) Explain TCP header with a diagram.

TCP (Transmission Control Protocol) is a **connection-oriented** and **reliable** transport layer protocol. It ensures proper delivery, sequencing, and error-checking of data between devices. The **TCP header** contains important control information and is typically **20 bytes** long (can be extended with options).

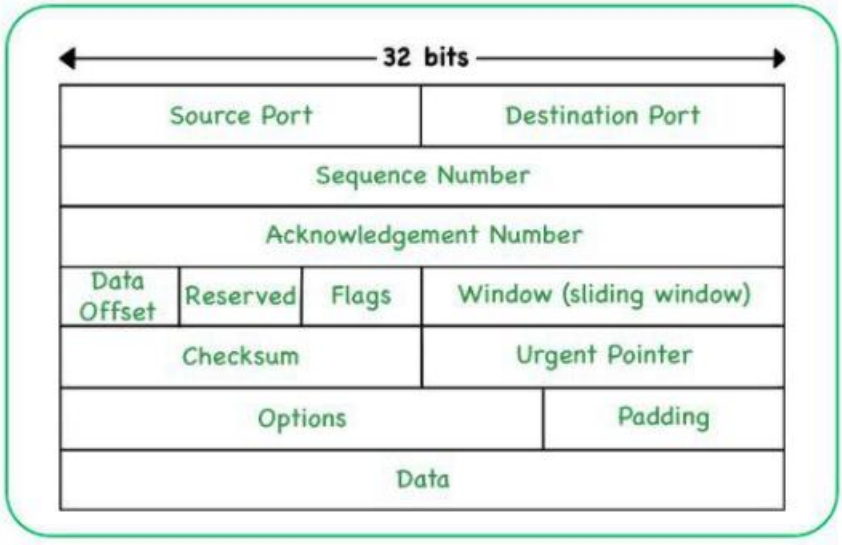


Diagram Showing the TCP packet Format

Explanation of TCP Header Fields:

1. **Source Port (16 bits):** Identifies the **sending port**.

2. **Destination Port (16 bits):** Identifies the **receiving port**.

3. **Sequence Number (32 bits):** Used to number the **first byte** of data in a segment. Important for data ordering.

4. **Acknowledgment Number (32 bits):** Indicates the **next expected byte** from the sender. Used for reliable communication.

5. **Data Offset (4 bits):** Also called **Header Length**. Specifies the **size of the TCP header**.

6. **Reserved (3 bits):** Reserved for **future use**; must be zero.

7. **Flags (9 bits):** Control bits such as:
    - **URG** (Urgent)
    - **ACK** (Acknowledgment)
    - **PSH** (Push)
    - **RST** (Reset)
    - **SYN** (Synchronize)
    - **FIN** (Finish)

8. **Window Size (16 bits):** Indicates the **number of bytes** the receiver is willing to accept.

9. **Checksum (16 bits):** Used for **error-checking** the TCP header and data.

10. **Urgent Pointer (16 bits):** Points to **urgent data**, used when **URG flag** is set.

b) UDP Applications

UDP (User Datagram Protocol) is used in applications where **speed is more important than reliability**. It is suitable for real-time communication and scenarios where occasional data loss is acceptable.

Applications of UDP:

1. **Video Streaming**
    - Used in platforms like YouTube Live, Netflix (in some cases), etc.
    - Slight loss of data does not affect video playback much.

2. **Voice over IP (VoIP)**
    - Examples: Skype, Zoom, WhatsApp calls.
    - Low latency is more important than perfect reliability.

3. **Online Gaming**
    - Real-time multiplayer games (e.g., PUBG, Fortnite).
    - Prioritizes speed over retransmission of lost data.

4. **DHCP (Dynamic Host Configuration Protocol)**
    - Used to assign IP addresses to devices in a network.

5. **SNMP (Simple Network Management Protocol)**
    - Used for monitoring and managing network devices.

Q4

a) Explain IPV6 Headers format with diagram

The **IPv6 (Internet Protocol version 6)** header is a streamlined and more advanced version of the IPv4 header, designed to address IPv4's limitations, such as address exhaustion and scalability issues. The IPv6 header is **fixed at 40 bytes** in size and has a simpler structure to improve processing efficiency.

Explanation of IPv6 Header Fields:

1. **Version (4 bits):** Specifies the IP version. For IPv6, this is **6**.

2. **Traffic Class (8 bits):** Indicates the **priority** of the packet and is used for **QoS (Quality of Service)**.

3. **Flow Label (20 bits):** Identifies packets belonging to the **same flow** for special handling (e.g., streaming or real-time applications).

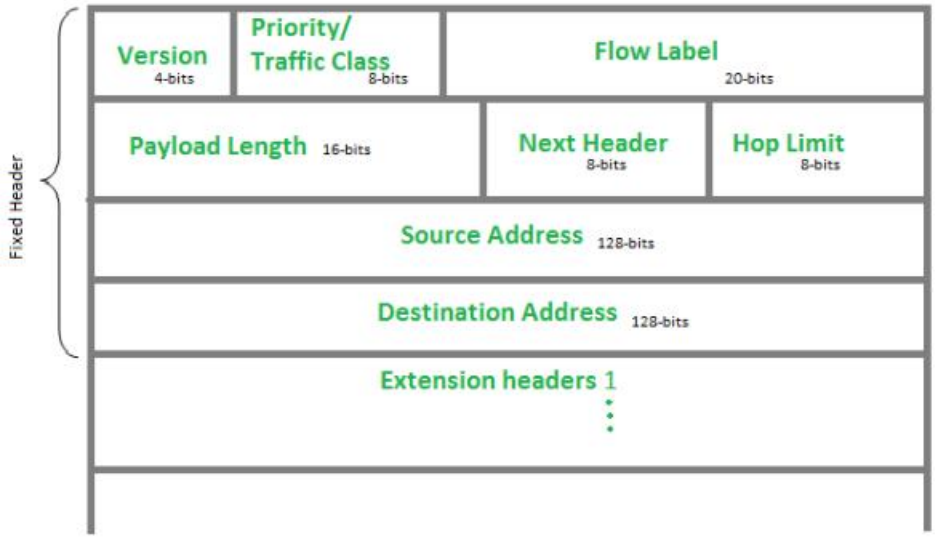
4. **Payload Length (16 bits):** Length of the **data** following the header, in bytes.

5. **Next Header (8 bits):** Indicates the type of header that comes **next** (e.g., TCP, UDP, or an extension header).

6. **Hop Limit (8 bits):** Similar to TTL in IPv4. Limits the number of hops a packet can take before being discarded.

7. **Source Address (128 bits):** The **IPv6 address of the sender**.

8. **Destination Address (128 bits):** The **IPv6 address of the receiver**.



b) Explain Fast Ethernet and Gigabit Ethernet?

Fast Ethernet
Definition:
Fast Ethernet is an enhanced version of traditional Ethernet that supports **data transfer speeds of up to 100 Mbps**.

Key Features:

- Speed: **100 Mbps**
- Standard: **IEEE 802.3u**
- Uses **twisted pair cables** (Cat5 or higher) or **fiber optics**
- Supports **star topology** using switches and hubs

Advantages:

- Faster than original 10 Mbps Ethernet
- Widely used in LANs for moderate-speed needs

Gigabit Ethernet
Definition:
Gigabit Ethernet is a high-speed Ethernet standard that supports data transfer at **1 Gbps (1000 Mbps)**.

Key Features:

- Speed: **1000 Mbps (1 Gbps)**
- Standard: **IEEE 802.3ab (for copper)**, **802.3z (for fiber)**
- Uses **Cat5e/Cat6 cables** or **fiber optic cables**
- Backward compatible with Fast Ethernet

Advantages:

- Ideal for high-speed networks
- Supports heavy data traffic, video streaming, and large file transfers
- Common in modern enterprise networks

Q6

a) Congestion Control

Congestion control is a mechanism used in computer networks to manage traffic flow and prevent network congestion. Congestion occurs when the network is overloaded with data packets, leading to delays, packet loss, and reduced performance.

Key Objectives

1. Ensure efficient use of network resources.
2. Prevent packet loss due to overloaded routers and switches.
3. Maintain an optimal level of throughput.

Congestion Control Methods

1. **Traffic Shaping**:
    - Regulates the flow of data to prevent bursts of traffic.
    - Examples: Leaky Bucket and Token Bucket algorithms.

2. **Window-Based Control**:
    - Adjusts the transmission rate based on the network's capacity.
    - Example: TCP Congestion Control using algorithms like Slow Start and Congestion Avoidance.

3. **Admission Control**:
    - Limits the number of active connections to reduce congestion.

b) Routing Algorithms

Routing algorithms are the methods used in computer networks to determine the best path for data packets to travel from a source to a destination. Their primary goal is to ensure efficient, reliable, and accurate delivery of data.

Types of Routing Algorithms:

1. **Static Routing**:
    - Routes are manually configured and do not change unless updated by a network administrator.
    - Example: Small networks with predictable traffic patterns.

2. **Dynamic Routing**:
    - Automatically adjusts routes based on network changes using routing protocols.
    - Example: RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol).

3. **Distance Vector Routing**:
    - Routers share their routing tables with neighbors periodically to calculate the best path.
    - Example: RIP.

4. **Link-State Routing**:
    - Routers have a complete view of the network topology and calculate the shortest path using algorithms like Dijkstra's.
    - Example: OSPF.

5. **Hybrid Routing**:
    - Combines elements of both distance vector and link-state routing.
    - Example: EIGRP (Enhanced Interior Gateway Routing Protocol).

CNND MAY 2022 Answers

What is congestion and what are the causes of congestion?

Congestion in a network occurs when the demand for resources exceeds the network's capacity, resulting in slowed or disrupted data transmission. Essentially, too much traffic flows through a network, causing bottlenecks and poor performance.

Causes of Congestion:

1. **High Traffic Load**:
    - Too many devices or applications generating data at the same time can overwhelm the network.

2. **Insufficient Bandwidth**:
    - When the network capacity is too small to handle the volume of data being transmitted.

3. **Faulty Network Devices**:
    - Malfunctioning routers, switches, or servers can lead to inefficient data handling.

4. **Network Design Issues**:
    - Poorly designed networks may struggle to handle traffic spikes effectively.

5. **Burst Traffic**:
    - Sudden surges of data, such as during live streaming or downloads, can overwhelm the network.

6. **Routing Problems**:
    - Inefficient routing algorithms or incorrect configurations can cause data packets to pile up at certain nodes.

Compare TCP and UDP

Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection	Connection-oriented	Connectionless
Reliability	Reliable (uses acknowledgements, retransmissions)	Unreliable (no guarantee of delivery)
Speed	Slower (due to overhead for reliability)	Faster (minimal overhead)
Data Ordering	Ensures proper sequencing of data	No sequencing; data may arrive out of order
Error Checking	Yes (error detection and correction)	Yes (only error detection, no correction)
Header Size	Larger (20–60 bytes)	Smaller (8 bytes)
Use Cases	Web browsing, emails, file transfer (HTTP, FTP)	Video streaming, gaming, VoIP (DNS, TFTP)
Flow Control & Congestion Control	Yes	No