



# Question 1

a) Propose a high-level topology for MauClodio clearly mentioning all network devices, Telecommunication Lines, backbones, and network cabling, etc.

High-Level Topology:

1. **Network Devices:**

- **Routers:** Connect different LANs and manage traffic between stores and the internet.
- **Switches:** Connect devices within each store's LAN.
- **Access Points:** Provide wireless connectivity within each store.
- **Firewalls:** Protect each store's network from external threats.
- **Servers:** Host the store's website, database, and file storage.

2. **Telecommunication Lines:**

- **Internet Leased Lines:** High-speed internet connections for each store.
- **VPN (Virtual Private Network):** Secure connection between stores for data exchange and centralized management.

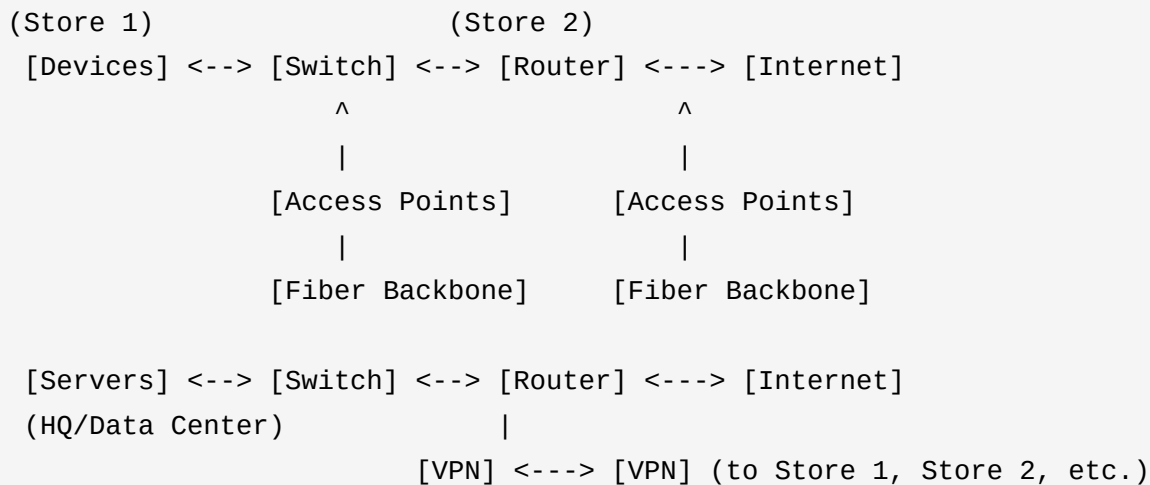
3. **Backbones:**

- **Fiber Optic Cables:** High-speed backbone connections within each store for connecting key network devices.
- **Ethernet Cables (Cat6):** Used for connecting devices within each store's LAN.

4. **Network Cabling:**

- **Structured Cabling System:** Organized cabling infrastructure within each store, ensuring efficient and reliable connectivity.

Diagram:



## b) Describe which equipment would form part of your LAN and WAN.

### LAN Equipment:

- **Switches:** Connect various devices within the local area network.
- **Access Points:** Provide wireless connectivity to devices.
- **Firewalls:** Protect internal network from unauthorized access.
- **Servers:** Host applications, files, and services for internal use.

### WAN Equipment:

- **Routers:** Connect different LANs over a wide area network and manage traffic.
- **VPN Devices:** Securely connect remote sites and users.
- **Modems/Leased Line Terminals:** Connect to the internet service provider.

## c) Enumerate two (2) main differences between a LAN and a WAN.

### 1. Geographical Coverage:

- **LAN (Local Area Network):** Covers a small geographical area, such as a single building or campus.
- **WAN (Wide Area Network):** Covers a large geographical area, connecting multiple LANs across cities, countries, or continents.

### 2. Ownership:

- **LAN:** Typically owned, managed, and maintained by a single organization.
- **WAN:** Often involves leased lines and services from telecommunication providers, with less direct control by the organization.

## d) Your service provider requested you to use 192.168.200.0/26.

### i. Explain what do you understand by 192.168.200.0.

- **192.168.200.0:** This is an IP address used as the network address for a subnet. It represents all the IP addresses within that subnet.

### ii. Explain the meaning of /26 and its purpose.

- **/26:** This represents the subnet mask, indicating that the first 26 bits of the IP address are used for the network portion, leaving the remaining 6 bits for host addresses. This allows for 64 IP addresses within the subnet ( $2^6$ ), with 62 usable for hosts (after accounting for network and broadcast addresses).

## e) Differentiate between Private IP and Public IP.

### Private IP:

- **Definition:** IP addresses reserved for use within private networks, not routable on the public internet.
- **Ranges:** 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, 192.168.0.0 to 192.168.255.255.
- **Purpose:** Used for internal communication within an organization.

### Public IP:

- **Definition:** IP addresses that are routable on the public internet and are unique across the entire internet.
- **Assigned By:** Internet service providers (ISPs).
- **Purpose:** Used for external communication, allowing devices to connect to the internet.

**f) List Private IP addresses for class A, B, and C.**

**Class A:**

- **Range:** 10.0.0.0 to 10.255.255.255

**Class B:**

- **Range:** 172.16.0.0 to 172.31.255.255

**Class C:**

- **Range:** 192.168.0.0 to 192.168.255.255
- 

## **Question 2**

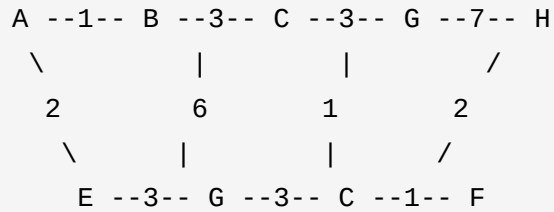
**a) Give two (2) examples of dynamic routing algorithms.**

1. **RIP (Routing Information Protocol):**
  - **Type:** Distance Vector Routing Protocol
  - **Characteristics:** Uses hop count as the metric, broadcasts the entire routing table to all neighbors every 30 seconds.
2. **OSPF (Open Shortest Path First):**
  - **Type:** Link State Routing Protocol
  - **Characteristics:** Uses Dijkstra's algorithm to calculate the shortest path, updates are only sent when there is a change in the network topology, uses cost as the metric.

**b) Find the route from source to destination node using a static, non-adaptive routing algorithm.**

**Given Network Diagram:**

Source Node (A) to Destination Node (H)



To find the best route using a static, non-adaptive routing algorithm, we will calculate the total metrics for each possible path from the source node (A) to the destination node (H):

1. Path A -> B -> C -> H
  - Total Metric:  $1 + 3 + 3 + 2 = 9$
2. Path A -> B -> D -> F -> H
  - Total Metric:  $1 + 4 + 1 + 2 = 8$
3. Path A -> E -> G -> H
  - Total Metric:  $2 + 3 + 7 = 12$
4. Path A -> E -> G -> C -> H
  - Total Metric:  $2 + 3 + 3 + 1 + 2 = 11$

The shortest path with the least total metric is:

Path A -> B -> D -> F -> H

- Total Metric: 8

Route:

- From A to B (Metric: 1)
- From B to D (Metric: 4)
- From D to F (Metric: 1)
- From F to H (Metric: 2)

So, the route from the source node (A) to the destination node (H) using a static, non-adaptive routing algorithm is **A -> B -> D -> F -> H** with a total metric of 8.

---

# Question 3

## a) Explain which subnet you would use and why?

Subnet Choice:

- **Subnet:** 192.168.150.0/26
- **Reason:** Each subnet with a /26 prefix allows for 62 usable host addresses ( $2^6 - 2 = 64 - 2$  for network and broadcast addresses), which is sufficient for the requirement of 40 to 50 computers per department. This ensures each department has its own subnet with adequate addresses for current needs and slight future growth.

## b) Produce the subnet prefix, show your workings.

Workings:

- Given IP: 192.168.150.0
- Subnet Mask: /26
  - /26 means the first 26 bits are for the network portion.
  - Subnet Mask: 255.255.255.192 (binary: 11111111.11111111.11111111.11000000)

## c) Calculate the number of Hosts per subnet.

Calculation:

- Total IP addresses in /26:  $2^{(32-26)} = 2^6 = 64$
- Usable Hosts:  $64 - 2 = 62$  (subtracting 2 for network and broadcast addresses)

## d) List the Network Addresses of all the subnets.

Subnets:

1. 192.168.150.0/26
  - Network Address: 192.168.150.0
2. 192.168.150.64/26

- Network Address: 192.168.150.64
- 3. 192.168.150.128/26
  - Network Address: 192.168.150.128
- 4. 192.168.150.192/26
  - Network Address: 192.168.150.192

**e) List the Broadcast Addresses of all the subnets.**

Broadcast Addresses:

1. 192.168.150.0/26
  - Broadcast Address: 192.168.150.63
2. 192.168.150.64/26
  - Broadcast Address: 192.168.150.127
3. 192.168.150.128/26
  - Broadcast Address: 192.168.150.191
4. 192.168.150.192/26
  - Broadcast Address: 192.168.150.255

**f) List the valid IP addresses of all the subnets.**

Valid IP Addresses:

1. 192.168.150.0/26
  - Valid IP Range: 192.168.150.1 to 192.168.150.62
2. 192.168.150.64/26
  - Valid IP Range: 192.168.150.65 to 192.168.150.126
3. 192.168.150.128/26
  - Valid IP Range: 192.168.150.129 to 192.168.150.190
4. 192.168.150.192/26
  - Valid IP Range: 192.168.150.193 to 192.168.150.254

**g) Explain what should be done if the number of users in one of your departments increases up to 65.**

Solution:

- **Subnet Reassignment:** Allocate a larger subnet to the department. For example, use a /25 subnet (255.255.255.128) which provides 126 usable IP addresses.
- **Reconfiguration:** Update the network configuration to reflect the new subnet and ensure all devices within the department are reconfigured with the new subnet.

Example Subnet for 65 users:

- **Subnet:** 192.168.150.0/25
  - **Valid IP Range:** 192.168.150.1 to 192.168.150.126
  - **Network Address:** 192.168.150.0
  - **Broadcast Address:** 192.168.150.127
- 

## Question 4

a) Explain the difference between OSI and TCP/IP protocol suite.

OSI Model:

- **Layers:** Consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- **Development:** Developed by the International Organization for Standardization (ISO) to standardize networking protocols and promote interoperability.
- **Usage:** Mostly theoretical, providing a guideline for understanding and designing network architecture.

TCP/IP Model:

- **Layers:** Consists of four layers: Network Interface, Internet, Transport, and Application.
- **Development:** Developed by the U.S. Department of Defense for ARPANET, the predecessor of the internet.
- **Usage:** Practical implementation of networking protocols used on the internet and many modern networks.



## Key Differences:

- **Number of Layers:** OSI has seven layers; TCP/IP has four layers.
- **Purpose:** OSI is a theoretical model; TCP/IP is a practical model used for real-world networking.
- **Layer Functions:** OSI layers are more granular; TCP/IP layers are broader.

## b) List and describe the different layers in the TCP/IP protocol suite.

### 1. Network Interface Layer:

- **Function:** Handles the physical transmission of data over the network. Includes hardware addressing and error detection.
- **Protocols/Examples:** Ethernet, Wi-Fi, ARP (Address Resolution Protocol).

### 2. Internet Layer:

- **Function:** Manages logical addressing, routing, and packet forwarding. Ensures that data packets reach their destination across multiple networks.
- **Protocols/Examples:** IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

### 3. Transport Layer:

- **Function:** Provides end-to-end communication services for applications. Ensures complete data transfer, error recovery, and flow control.
- **Protocols/Examples:** TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

### 4. Application Layer:

- **Function:** Provides network services directly to end-users and applications. Facilitates communication between software applications and lower layers.
- **Protocols/Examples:** HTTP, FTP, SMTP, DNS, Telnet.

## c) With the help of an example differentiate between UDP and TCP.

### UDP (User Datagram Protocol):

- **Characteristics:** Connectionless, unreliable, no error checking, no flow control.
- **Example:** Streaming a live video. UDP is used because it is faster and can tolerate some data loss. The protocol does not retransmit lost packets, so the video stream remains smooth even if some data is lost.

### TCP (Transmission Control Protocol):

- **Characteristics:** Connection-oriented, reliable, error checking, flow control, ensures in-order delivery of packets.
- **Example:** Sending an email. TCP is used because it guarantees that the email data is delivered correctly and in the right order. If any packets are lost or corrupted, TCP retransmits them.

## d) Elaborate on the need for IP and datagrams.

### IP (Internet Protocol):

- **Need:** Provides a logical addressing system that enables data to be routed between devices across different networks. It is essential for identifying the source and destination of data packets and ensuring they reach the correct location.

### Datagrams:

- **Need:** The basic units of data transfer in the IP layer. Datagrams are self-contained, independent packets that contain all the information needed for routing from the source to the destination. They allow for efficient and flexible data transfer, enabling the internet to function as a robust and scalable network.

e) “Three-Way Handshake or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client.”

i. List the four (4) message types of the TCP 3-way handshake.

1. **SYN (Synchronize):** The client sends a SYN packet to the server to initiate a connection.
2. **SYN-ACK (Synchronize-Acknowledge):** The server responds with a SYN-ACK packet to acknowledge the SYN request and synchronize its own sequence number.
3. **ACK (Acknowledge):** The client sends an ACK packet to acknowledge the server's SYN-ACK response, completing the handshake.

ii. Explain the process of the TCP 3-way handshake with the help of a clearly labeled diagram.

Process:

1. **Step 1 - SYN:**
  - The client sends a SYN packet to the server with an initial sequence number (Seq=1000).
2. **Step 2 - SYN-ACK:**
  - The server responds with a SYN-ACK packet, acknowledging the client's SYN (Ack=1001) and sending its own initial sequence number (Seq=2000).
3. **Step 3 - ACK:**
  - The client sends an ACK packet back to the server, acknowledging the server's SYN-ACK (Ack=2001).

Diagram:

```
Client                                Server
|                                    |
|-----SYN (Seq=1000)----->|
|                                    |
|<----SYN-ACK (Seq=2000, Ack=1001)|
|                                    |
|-----ACK (Ack=2001)----->|
|                                    |
Connection Established
```

---

## Question 5

a) When you sign up with an Internet Service Provider (ISP), you will either end up with a static IP address or a dynamic IP address.

i. Differentiate between a static IP address and a dynamic IP address.

Static IP Address:

- **Definition:** A static IP address is a fixed address that does not change. It is manually assigned to a device by an administrator.
- **Usage:** Commonly used for servers, network devices, and other critical systems that require a consistent address.

Dynamic IP Address:

- **Definition:** A dynamic IP address is temporarily assigned to a device by a DHCP server and can change over time.
- **Usage:** Commonly used for end-user devices like computers, smartphones, and tablets that do not require a consistent address.

## ii. How are the commands "ipconfig/release" different from "ipconfig/renew"?

ipconfig/release:

- **Function:** Releases the current IP address assigned to the device by the DHCP server.
- **Usage:** Used when you want to discard the current IP configuration and prepare to request a new IP address.

ipconfig/renew:

- **Function:** Requests a new IP address from the DHCP server.
- **Usage:** Used to obtain a new IP address after releasing the old one or to refresh the IP address lease.

## iii. Provide three (3) advantages of using static IP over dynamic IP.

1. **Consistency:** Static IP addresses remain constant, making it easier to locate and manage devices, particularly servers and network resources.
2. **Reliability:** Services hosted on devices with static IP addresses are more reliable as the IP address does not change, ensuring consistent access.
3. **Remote Access:** Easier to set up remote access and VPN connections since the IP address does not change.

## b) Enumerate the steps when a DHCP server assigned an IP address to a client.

1. **DHCP Discover:** The client sends a DHCP Discover message to locate available DHCP servers.
2. **DHCP Offer:** A DHCP server responds with a DHCP Offer message that includes an available IP address and other configuration details.
3. **DHCP Request:** The client sends a DHCP Request message indicating it accepts the offered IP address and configuration.
4. **DHCP Acknowledgment:** The DHCP server sends a DHCP Acknowledgment (ACK) message confirming the IP address assignment and providing the final configuration details.
5. **IP Address Assignment:** The client configures its network interface with the

assigned IP address and other parameters (e.g., subnet mask, default gateway, DNS servers).

## c) Define any three (3) of the following ICMP messages.

### i. Destination Unreachable

Destination Unreachable:

- **Definition:** Indicates that a packet could not reach its destination. This could be due to various reasons such as a network or host being unreachable, a port being unreachable, or communication being administratively prohibited.
- **Usage:** Helps in diagnosing network connectivity issues.

### ii. Echo Request

Echo Request:

- **Definition:** A type of ICMP message used to test connectivity between devices. It is sent by the `ping` command to request an echo reply from a specified destination.
- **Usage:** Used in network diagnostics to check if a device is reachable and how long it takes for a packet to travel to the destination and back.

### iii. Echo Reply

Echo Reply:

- **Definition:** A response to an Echo Request message. It indicates that the destination device is reachable and responsive.
- **Usage:** Used in conjunction with Echo Request to confirm network connectivity and measure round-trip time.

### iv. Parameter Problem

Parameter Problem:

- **Definition:** Indicates that a packet has been received with incorrect or invalid parameters in the header.
- **Usage:** Helps in diagnosing issues related to packet formatting and header

configuration.