Question 1

a) Define 172.22.10.* /23 in terms of its type of IP and Subnet Mask

The IP address 172.22.10.* with a /23 subnet mask falls under Class B IP addresses. Class B IP addresses range from 128.0.0.0 to 191.255.255.255.

- **Type of IP:** Private IP
- **Subnet Mask:** /23 translates to 255.255.254.0 in decimal form.

b) How many valid hosts are available with /23

A /23 subnet mask provides 2^9 - 2 = 510 valid host addresses.

c) Fill in the blanks in the table

We need to calculate the network address, valid host range, broadcast address, and number of idle IP addresses for each department.

Call Centre (200 Users)

- **Network Address:** 172.22.10.0 /24
- **Valid Host Address Range:** 172.22.10.1 to 172.22.10.254
- **Broadcast Address:** 172.22.10.255
- **Number of Idle IP Addresses:** 54 (Since 254 - 200 = 54)

Supervisor (120 Users)

- **Network Address:** 172.22.11.0 /25
- **Valid Host Address Range:** 172.22.11.1 to 172.22.11.126
- **Broadcast Address:** 172.22.11.127
- **Number of Idle IP Addresses:** 6 (Since 126 - 120 = 6)

Finance (60 Users)

- **Network Address:** 172.22.11.128 /26

- **Valid Host Address Range:** 172.22.11.129 to 172.22.11.190
- **Broadcast Address:** 172.22.11.191
- **Number of Idle IP Addresses:** 2 (Since 62 - 60 = 2)

ICT (50 Users)

- **Network Address:** 172.22.11.192 /26
- **Valid Host Address Range:** 172.22.11.193 to 172.22.11.254
- **Broadcast Address:** 172.22.11.255
- **Number of Idle IP Addresses:** 12 (Since 62 - 50 = 12)

d) Differentiate between Private and Public IP

i. Differences

- **Private IP:** These are used within a local network and are not routable on the internet. They are used for internal communication within a network.
- **Public IP:** These are assigned by the ISP and are routable on the internet. They are used for communication between devices across the internet.

ii. Valid Private IP Address Ranges

- **Class A:** 10.0.0.0 to 10.255.255.255
- **Class B:** 172.16.0.0 to 172.31.255.255
- **Class C:** 192.168.0.0 to 192.168.255.255

Summary Table

Departments	Network Address	Valid Host Address Range	Broadcast Address	Number of Idle IP Address
Call Centre	172.22.10.0 /24	172.22.10.1 - 172.22.10.254	172.22.10.255	54
Supervisor	172.22.11.0 /25	172.22.11.1 - 172.22.11.126	172.22.11.127	6
Finance	172.22.11.128/	172.22.11.129 -	172.22.11.191	2

Departments	Network Address	Valid Host Address Range	Broadcast Address	Number of Idle IP Address
	26	172.22.11.190		
ICT	172.22.11.192/ 26	172.22.11.193 - 172.22.11.254	172.22.11.255	12

Question 2

Sure, let's address each part of the question based on the provided diagram and instructions.

a) Explain why routing tables are important for packet flow.

Routing tables are crucial for packet flow because:

- **Path Determination:** They determine the best path for data packets to travel from the source to the destination based on various metrics such as hop count, bandwidth, delay, and cost.
- **Efficiency:** Routing tables help optimize the network's efficiency by ensuring that packets take the most efficient route, which can minimize congestion and reduce transmission times.
- **Scalability:** They allow networks to scale by dynamically adjusting routes based on changes in the network topology.
- **Reliability:** Routing tables improve reliability by providing alternative routes in case of link failures or other issues.

b) Explain why Static Routing is simpler than Dynamic Routing and how Dynamic Routing is more complex.

Static Routing:

- **Simplicity:** Static routing is simpler because routes are manually configured by network administrators. There is no need for complex algorithms or protocols to

determine the best path.
- **Predictability:** It is predictable since the routes do not change unless manually updated, making it easier to manage and troubleshoot.

Dynamic Routing:

- **Complexity:** Dynamic routing is more complex because it involves the use of routing protocols (such as RIP, OSPF, BGP) that automatically adjust routes based on the network conditions.
- **Real-Time Updates:** It requires routers to exchange routing information, calculate the best paths using algorithms, and update their routing tables in real-time, which involves more processing power and memory.
- **Adaptability:** Dynamic routing is adaptive to changes in the network topology, which can include link failures, adding new routes, or changing the cost of routes.

c) Using a static, non-adaptive routing mechanism, work out and show your workings for the following:

i. Enumerate all the steps for a static, non-adaptive routing mechanism

1. **Define Network Topology:** Identify all routers and links between them with their respective metrics.
2. **Manual Configuration:** Manually configure the static routes on each router. This involves specifying the destination network, the next hop, and the metric.
3. **Routing Table Update:** Update the routing tables of all routers with the static routes.
4. **Verify Configuration:** Verify the static routes using commands like `show ip route` to ensure they are correctly configured.
5. **Test Connectivity:** Test the connectivity between source and destination using tools like ping and traceroute.
6. **Monitor and Maintain:** Periodically monitor the network to ensure the static routes are still valid and make adjustments if there are changes in the network topology.

ii. The best route from B to H

To find the best route from B to H, we need to look for the path with the lowest metric (cost):

1. **B -> D -> F -> H** with a metric of $2 + 1 + 2 = 5$

So, the best route from B to H is B -> D -> F -> H.

iii. The second-best route from B to H

To find the second-best route, we need to find the path with the next lowest metric:

1. **B -> C -> F -> H** with a metric of $3 + 3 + 2 = 8$

So, the second-best route from B to H is B -> C -> F -> H.

iv. The longest route from Source to Destination

The longest route from B to H (without revisiting nodes) is:

1. **B -> A -> G -> D -> F -> H** with a metric of $2 + 1 + 3 + 1 + 2 = 9$

So, the longest route from B to H is B -> A -> G -> D -> F -> H.

Summary

Description	Path	Metric
Best route from B to H	B -> D -> F -> H	5
Second-best route from B to H	B -> C -> F -> H	8
Longest route from Source (B) to Destination (H)	B -> A -> G -> D -> F -> H	9

Question 3

Let's address each part of Question 3 based on the provided instructions.

a) Vertical Redundancy Check (Even Parity Checking) for data 110001

Even Parity Check:

- Count the number of 1s in the data.
- Data: 110001
    - Number of 1s: 3

For even parity, the number of 1s should be even. Since there are 3 (odd number), the parity bit should be 1 to make it even.

Answer: Parity Bit = 1

b) LRC (Longitudinal Redundancy Check) for data 11100111 11011101 00111001 10101001

Step 1: Arrange the data in a table

```
1 1 1 0 0 1 1 1
1 1 0 1 1 1 0 1
0 0 1 1 1 0 0 1
1 0 1 0 1 0 0 1
```

Step 2: Calculate the parity bit for each column

```
1 1 1 0 0 1 1 1
1 1 0 1 1 1 0 1
0 0 1 1 1 0 0 1
1 0 1 0 1 0 0 1
---------------
1 0 1 0 1 0 1 1 (Parity bits for each column)
```

Answer: Parity Bits = 10101011

c) Calculate the sender side Checksum for data 10110011 10101011 01011010 11010101

Step 1: Add the binary numbers

```
  10110011
  10101011
+ 01011010
+ 11010101
-----------
100011001
```

Step 2: If the sum exceeds 8 bits, wrap around the overflow

- 100011001 (9 bits)
- Wrapping around the overflow: 00011001 (carry out 1 + 1 = 2)

Step 3: Calculate the checksum by taking one's complement

- 00011001 (One's complement: 11100110)

Answer: Sender Checksum = 11100110

d) Calculate the receiver side Checksum

The receiver side checksum calculation involves adding the received data, including the checksum, and checking if the result is all ones.

Step 1: Add the data with the sender checksum

```
  10110011
  10101011
  01011010
  11010101
+ 11100110
-----------
110111101
```

Step 2: Wrap around the overflow

- 110111101 (9 bits)
- Wrapping around the overflow: 10111101 (carry out 1 + 1 = 2)

Step 3: If the result is not all ones, there is an error

- 10111101 (not all ones, so wrap around again)
- Wrapping around the overflow: 0111111

Answer: Receiver Checksum = 01111111

e) How would you know that the data has been correctly transmitted?

You would know that the data has been correctly transmitted if the final checksum at the receiver's end is all ones. This indicates that there were no errors during the transmission.

Answer: The data is correctly transmitted if the final checksum at the receiver's end is all ones (11111111).

This covers all parts of Question 3 comprehensively. If you need further clarification or details, please let me know!

Question 4

a) Define the Proxy server with a clearly labeled diagram.

Definition:
A Proxy server acts as an intermediary between a client seeking resources and the server providing those resources. It handles client requests by forwarding them to the appropriate server and then returning the server's response back to the client. This can help with improving security, performance, and resource management.

Diagram:

```
[Client] ---> [Proxy Server] ---> [Internet]
            ^                  |
            |                  v
            <--- Response <---
```

1. **Client:** A device requesting access to resources.
2. **Proxy Server:** The intermediary that processes and forwards requests.
3. **Internet/Server:** The destination where the resources are hosted.

b) How the Proxy server would add value to the organisation's network infrastructure by describing two (2) advantages of the Proxy.

1. **Security:** A proxy server can provide enhanced security by acting as a firewall and filtering requests to prevent unauthorized access and malicious activities. It can also anonymize the client's IP address, making it harder for attackers to target individual devices.
2. **Performance Improvement:** By caching frequently accessed resources, a proxy server can reduce load times and bandwidth usage, leading to improved performance and reduced latency for users accessing the same resources repeatedly.

c) There are four (4) types of Proxy mentioned, how would a High Anonymity Proxy be helpful to the organisation

A High Anonymity Proxy (also known as an Elite Proxy) provides the highest level of anonymity by not revealing that the user's request is being proxied. It completely hides the user's IP address, making it very difficult for the target server to determine the original source of the request.

Benefits:

1. **Enhanced Privacy:** By concealing the user's IP address, it provides maximum privacy and prevents tracking by third parties.
2. **Increased Security:** Reduces the risk of targeted attacks and data breaches by masking the user's identity.

d) Are there any risks associated with the Proxy Server? If Yes provide two (2) risks that may influence the decision of the CFO for not implementing the Proxy server.

1. **Single Point of Failure:** If the proxy server goes down, it can disrupt access to the internet or internal resources, causing potential downtime and productivity loss.
2. **Potential Bottlenecks:** A proxy server can become a bottleneck if it is not properly configured or if it is handling a large volume of requests, leading to slower response times and reduced performance.

e) IP assignment may be done via a DHCP server. What is a DHCP Server

A DHCP (Dynamic Host Configuration Protocol) server automatically assigns IP addresses and other network configuration parameters to devices on a network, allowing them to communicate with other IP networks. It ensures that each device has a unique IP address and reduces the need for manual IP configuration.

f) Describe the four (4) steps of the DHCP server with the help of a diagram.

DHCP Process:

1. **DHCP Discover:** The client sends a broadcast message to the network to find available DHCP servers.
2. **DHCP Offer:** A DHCP server responds with an offer, including an IP address and other configuration information.
3. **DHCP Request:** The client responds to the DHCP server, indicating it accepts the offered IP address.
4. **DHCP Acknowledgment:** The DHCP server sends an acknowledgment to the client, confirming the IP address assignment and providing any additional configuration details.

Diagram:

```
[Client] ---> [DHCP Discover] ---> [DHCP Server]
[Client] <--- [DHCP Offer] <--- [DHCP Server]
[Client] ---> [DHCP Request] ---> [DHCP Server]
[Client] <--- [DHCP Acknowledgment] <--- [DHCP Server]
```

This should comprehensively answer all parts of Question 4. If you need further clarification or additional details, please let me know!