1. Give me one difference between vertical and horizontal IoT platforms.
   Vertical IoT Platform:
   It builds a separate platform for each application service domain and proceeds with the service.
   Horizontal IoT Platform:
   It is designed to operate independently of things and services, accommodating a variety of devices. It also provides commonly required function from different services.

2. Provide 3 examples of popular IoT platforms.
   - AWS IoT (Amazon Web Services IoT).
   - Azure IoT (Microsoft Azure IoT).
   - Google Cloud IoT.

3. Give me a use case for mashup support.
   Travel Planner Application with Mashup Support:
   Scenario:
   A travel enthusiast, Galal, is planning a two-week vacation to a foreign country. He wants to make the most of his trip by exploring various destinations, finding the best deals on accommodations and activities, and creating a personalized itinerary. The Travel Planner application employs mashup support to seamlessly combine information from different sources, helping Galal plan his dream vacation efficiently.
   How Mashup Support Enhances the Experience:
   - Aggregated Destination Information:

   The Travel Planner application integrates data from travel blogs, official tourism websites, and user reviews to provide comprehensive information about various destinations. Galal can view a consolidated overview of popular tourist spots, historical landmarks, local cuisines, and cultural events all in one place.
   - Real-time Flight and Accommodation Data:

   By integrating with flight booking platforms and hotel reservation systems, the application displays real-time information about available flights, prices, and accommodation options. Galal can compare different airlines and hotels, filtering by preferences such as price range, amenities, and user ratings.
   - Customized Itinerary Creation:

   Using mashup support, the application combines scheduling features with data from attractions, restaurants, and local events. Galal can drag and drop activities onto his itinerary, and the application automatically calculates travel times and suggests optimal routes between destinations.
   - Budget Management and Deals Aggregation:

   The application collaborates with financial APIs to help Galal create and manage his travel budget. It tracks expenses, converts currencies, and offers insights into how much he has spent in different categories. Furthermore, the application uses mashup support to fetch and display special deals, discounts, and offers from various travel partners.
   - Interactive Maps and Navigation:

   Integrating map services and GPS data, the Travel Planner application generates interactive maps that highlight Galal's planned itinerary. He can visualize his daily

routes, points of interest, and nearby attractions, all overlaid on a user-friendly map interface.

- Social Integration and Sharing:

The mashup support extends to social media integration, allowing Galal to share his travel plans with friends and family. The application pulls in data from his social networks, such as friends' recommendations, photos, and check-ins, enriching his overall travel experience.

4. Choose the correct answer, one of the device management technology protocols is:
   a. ISBN
   b. OID
   c. DMS
   d. M2M

5. Choose the correct answer, orchestration service composition is a loosely coupled architecture:
   a. True
   b. False

6. What is the OSI model and why is it important in networking?
   The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes and defines the functions of a networking or telecommunication system.
   The OSI model is important in networking for several reasons:
   - Common Reference Framework: The OSI model provides a standardized reference framework that helps network engineers and developers understand how different networking technologies and protocols fit together. It serves as a common language for discussing and designing networking systems.
   - Modularity and Interoperability: The model's layered structure allows for modular design and development. Each layer can be developed independently, promoting interoperability among different networking devices and software from various vendors.
   - Troubleshooting and Isolation: When network issues arise, the OSI model helps network administrators and technicians pinpoint the source of the problem. By categorizing network functions into distinct layers, it becomes easier to identify which layer is experiencing issues.
   - Education and Learning: The OSI model is widely used as a teaching tool to help students and professionals learn about networking concepts, protocols, and technologies in a structured manner.
   - Protocol Development: The OSI model guided the development of various networking protocols, including the TCP/IP suite, which is the foundation of the modern internet.

7. How do the OSI model and the TCP/IP model relate to each other?
   The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are both conceptual frameworks used to understand and describe the various layers involved in computer networking. They were developed independently but serve similar purposes, helping to standardize

and organize the different functions and protocols that enable communication in a networked environment.

Here's how they relate to each other:

1. Layer Correspondence:
   - Physical Layer: Both models have an equivalent concept of the physical layer, which deals with the actual transmission and reception of raw data bits over a physical medium.
   - Data Link Layer: In the OSI model, this layer is responsible for framing data into frames, error detection and correction, and flow control. The TCP/IP model combines some functionalities of the OSI Data Link and Physical layers into its Network Access layer.
   - Network Layer: Both models have a network layer responsible for routing packets of data between devices in different networks. In the OSI model, this layer is primarily concerned with logical addressing and routing. In the TCP/IP model, this functionality is mostly performed by the Internet Protocol (IP).
   - Transport Layer: Both models have a transport layer that provides end-to-end communication services and ensures data delivery. The OSI model has multiple transport layer protocols, such as TCP and UDP, while the TCP/IP model mainly focuses on TCP and UDP.
   - Session, Presentation, and Application Layers (OSI): These layers in the OSI model handle functions related to user interfaces, data encryption/decryption, and managing communication sessions. The TCP/IP model does not explicitly separate these functions and incorporates them into its application layer.

2. Number of Layers:
   - The OSI model consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
   - The TCP/IP model has four layers: Network Access (combining some functions of OSI's Data Link and Physical layers), Internet, Transport, and Application.

In summary, while the OSI model and the TCP/IP model have similarities in terms of layer functionality and purpose, they are distinct conceptual frameworks developed for different purposes and in different contexts. The TCP/IP model is more closely aligned with the practical implementation of networking protocols that form the basis of the modern internet.

8. Provide an example of how the OSI model helps in diagnosing network issues.

   Let's say you're experiencing slow internet connectivity. Here's how you could use the OSI model to diagnose the issue:

   Scenario: Slow Internet Connectivity

   Step 1: Identify the Symptoms:

   In this case, the symptom is slow internet connectivity. Websites are taking a long time to load, and online activities like video streaming and file downloads are sluggish.

Step 2: Start at the Physical Layer (Layer 1):

Begin by checking the physical layer, which deals with the actual hardware components and physical connections. Make sure all cables are securely connected and not damaged. Check if there's any interference, like electromagnetic interference (EMI), that could affect the signal quality.

Step 3: Move to the Data Link Layer (Layer 2):

Proceed to the data link layer, which focuses on data framing, error detection, and MAC (Media Access Control) addresses. Check for any errors in the MAC address configuration or if there's a high number of collisions on the network. This might indicate a problem with the network switches or Ethernet cables.

Step 4: Investigate the Network Layer (Layer 3):

The network layer is responsible for routing and logical addressing. Verify that your IP address configuration is correct, including subnet masks and default gateways. Check for any routing issues, such as incorrect routes or routing loops.

Step 5: Examine the Transport Layer (Layer 4):

Move to the transport layer, which manages end-to-end communication and ensures reliable data delivery. Test whether there are any problems with TCP or UDP connections. For example, a high number of TCP retransmissions could point to network congestion or packet loss.

Step 6: Inspect the Session Layer (Layer 5) and Presentation Layer (Layer 6):

In many cases, issues at these layers are less common. However, if you suspect that the problem might be related to session establishment or data format translation (encryption/decryption), you can review configurations and settings in these layers.

Step 7: Analyze the Application Layer (Layer 7):

Finally, check the application layer, which directly interacts with end-user applications. Ensure that no particular application is consuming excessive bandwidth, causing slowdowns. You can use network monitoring tools to identify the culprit.

9. Your client is a small office with 15 employees. They need a network that is easy to set up and manage while ensuring reliable communication.
    a. What network topology would you recommend and why?
    Star Topology; this topology offers several advantages:
    - Easy Setup and Management: Star Topology is one of the simplest topologies to set up and manage. Adding or removing devices is straightforward, and troubleshooting is relatively easy since each device is directly connected to the central hub/switch.
    - Reliable Communication: Communication between devices is centralized through the hub/switch. If one device experiences a problem, it does not affect the rest of the network. This isolation helps to ensure reliable communication.
    - Scalability: As your office grows, you can easily add more devices by connecting them to the central hub/switch, making it a scalable solution.
    - Performance: Star Topology can provide good performance, especially in small networks, as each device has a dedicated connection to the central hub/switch.
    b. How can we increase the network reliability and increase failure?
    - Redundant Hardware: Have spare networking equipment (such as switches) on hand. If the central hub/switch fails, you can quickly replace it with the redundant hardware to minimize downtime.
    - Uninterruptible Power Supply (UPS): Use UPS units to provide backup power to networking equipment. This ensures that your network remains operational during power outages.
    - Network Monitoring: Implement network monitoring tools to constantly track the health and performance of the network. This allows you to identify and address potential issues before they cause significant disruptions.
    - Regular Backups: Ensure that critical network configurations are regularly backed up. In case of a failure, you can quickly restore the network settings to minimize downtime.
    - Firewall and Security Measures: Implement a firewall to protect the network from unauthorized access and potential threats. Regularly update security protocols to ensure the network's integrity.
    - Segmentation: Divide the network into segments, such as separating guest devices from internal devices. This helps contain potential issues and prevents them from affecting the entire network.
    - Network Documentation: Maintain detailed documentation of the network setup, configurations, and procedures. This documentation can be invaluable during troubleshooting and recovery efforts.
    - Employee Training: Provide basic network troubleshooting training to employees. This can help minimize downtime caused by simple issues that can be resolved without external support.

    Remember that while these measures can increase network reliability and fault tolerance, no network is completely immune to failures. It's essential to have a well-thought-out disaster recovery plan in place to handle more significant disruptions if they occur.

10. You are tasked with designing a network for a large corporate headquarters that consists of several departments, including Administration, Research and Development, Marketing, and Customer Support. Each department has specific

connectivity needs. The network should provide efficient communication within departments and also allow inter-departmental collaboration. Additionally, the Research and Development department handles critical projects that require maximum network reliability. Propose a comprehensive network design that incorporates different network topologies to fulfill these requirements. Justify your choice of topologies for each department and explain how they will interact to create an effective network infrastructure while increasing the reliability of the Research and Development department.

- Administration Department: Star Topology

The Administration department requires centralized control and communication. A star topology is suitable as it allows all devices to connect directly to a central hub (switch) in the department. This simplifies management and minimizes data collisions.

The central hub can have higher bandwidth and redundancy to ensure smooth communication within the department.

- Research and Development Department: Mesh Topology

Due to the critical nature of R&D projects, a mesh topology is ideal. Each device in the R&D department is directly connected to every other device. This redundancy ensures that even if one link fails, communication can continue through alternate paths.

The mesh topology's high fault tolerance and reliability are crucial for R&D projects that must proceed without interruptions.

- Marketing Department: Ring Topology

The Marketing department requires regular communication and collaboration. A ring topology can support this by connecting devices in a circular manner.

Each device connects to exactly two other devices, enabling efficient data transmission within the department.

In case of a single link failure, only the directly affected devices will experience downtime, minimizing the impact on overall operations.

- Customer Support Department: Bus Topology

The Customer Support department deals with numerous devices requiring frequent communication. A bus topology suits this need by connecting devices in a linear arrangement along a central backbone (bus).

This topology is cost-effective and simple to implement, making it suitable for the customer support environment.

Interactions and Collaboration:

Inter-departmental collaboration is facilitated by connecting each department's central switch to the corporate core switch. The core switch ensures efficient data flow between departments.

11. The session layer is responsible for session establishment:
    a. True
    b. False
12. Which role does CRC (Cyclic Redundancy Check) fulfill in the transport layer?
    a. Ensuring physical layer connectivity
    b. Detecting errors in data transmission
    c. Establishing end-to-end sessions

d. Segmenting data for efficient transfer

13. What is the maximum number of unique IPv4 addresses that can exist?
    a. 256
    b. 2^16
    c. 2^32
    d. 2^64
14. In unicast communication, the sender:
    a. Sends data to multiple recipients at once.
    b. Selects the destination using a multicast address.
    c. Directs data to a specific recipient using its unique address.
    d. Shares data with all devices on the network.
15. Anycast communication is commonly used in:
    a. Broadcasting live events to a wide audience.
    b. Distributing software updates to devices in a local network.
    c. Sending emails to a specific recipient.
    d. Point-to-point communication in a LAN.