Q1

Vertical platforms build a separate platform for each application service domain and proceeds with the service meanwhilethe horizontal platform is designed to operate independently of things and services, accommodating a variety of devices. It also provides commonly required function from different services.

Q2

AWS IoT

Microsoft Azure IoT

Google Cloud IoT

IBM Watson IoT

Q3

Use Case: Smart Home Automation Mashup

1. **Components**:
   * Smart Thermostat: Monitors and controls the home's heating and cooling system.
   * Smart Lock: Provides remote locking and unlocking of doors.
   * Motion Sensors: Detects movement in different areas of the house.
   * Weather Service API: Provides real-time weather data.
2. **Scenario**: The homeowner wants to create an automation scenario that adjusts the thermostat and controls the smart lock based on the weather conditions and occupancy status to save energy and enhance security.
3. **Mashup Support**: The IoT platform offers mashup support, allowing the homeowner to integrate data and actions from different devices and services seamlessly.
4. **Automation Rules**: Using the mashup support, the homeowner creates the following rules:
   * If motion is detected and it's daytime, adjust the thermostat to a comfortable temperature.
   * If no motion is detected and its nighttime, lower the thermostat to save energy.
   * If rain is detected by the weather service, lock all exterior doors automatically.
   * When the homeowner arrives (detected through a geolocation service), unlock the front door.
5. **Execution**: The IoT platform utilizes the mashup rules to control the devices and services accordingly. For instance, when motion is detected during the day, the thermostat adjusts to the desired temperature. If rain is detected, the smart lock engages, enhancing home security.

Q4

M2M

Q5

True

Q6

The OSI (Open Systems Interconnection) model is a framework with seven layers that standardizes how devices communicate in a network. Each layer has specific functions, like managing data transmission, routing, and encryption. It's important because it promotes interoperability, simplifies network design, and serves as a common reference for developing and understanding networking protocols.

Q7

The OSI model and the TCP/IP model are related by their layered approaches to network communication. The TCP/IP model is rooted in the practical implementation of internet protocols, while the OSI model provides a broader conceptual framework. Understanding both models can provide a comprehensive view of networking concepts and protocols.

And they are related in:

**Layer Correspondence**: The OSI model has seven layers, while the TCP/IP model has four layers. The layers in the TCP/IP model can be loosely mapped to the layers in the OSI model as follows:

* OSI Physical Layer corresponds to TCP/IP Network Interface Layer.
* OSI Data Link Layer corresponds to TCP/IP Network Interface Layer.
* OSI Network Layer corresponds to TCP/IP Internet Layer.
* OSI Transport Layer corresponds to TCP/IP Transport Layer.
* OSI Session, Presentation, and Application Layers correspond to TCP/IP Application Layer.

Q8

For example, users in a company are experiencing slow file transfer speeds when sending large files between computers in the same local network.

Diagnosis Using the OSI Model:

1.Physical Layer:

- Check for physical issues like faulty cables or loose connections that might affect the network link.

2.Data Link Layer:

- Verify that the network interface cards (NICs) on both computers are functioning properly and are set to the correct speed and duplex settings.

3.Network Layer:

- Use the `ping` command to test network connectivity and latency between the two computers. High latency or packet loss could indicate network congestion or routing issues.

4.Transport Layer:

- Check if the TCP or UDP ports being used for file transfer are open and not blocked by firewalls.

5.Session Layer:

- Verify that there are no issues with session establishment or maintenance. Check if the file transfer application is using proper protocols for data exchange.

6.Presentation Layer:

- Ensure that there are no issues with data compression, encryption, or conversion that might be affecting the file transfer process.

7.Application Layer:

- Check the file transfer application itself for any settings that could impact transfer speed. Consider using different applications to identify if the issue is application specific.

Q9

a. **Recommended Network Topology**: For a small office with 15 employees, a **Star Topology** would be a suitable recommendation.

**Reasoning**:

* **Ease of Setup and Management**: The Star Topology is straightforward to set up and manage. All devices are connected to a central hub (switch), making it easy to add or remove devices without affecting the entire network.
* **Reliable Communication**: In a Star Topology, each device has its own dedicated connection to the central switch. This isolation ensures that if one device or cable fails, it doesn't impact the rest of the network.
* **Scalability**: As the office grows, new devices can be easily added to the switch without disrupting existing connections.
* **Centralized Management**: With a single central hub, network monitoring, security management, and updates can be more efficiently handled.

b. **Increasing Network Reliability and Redundancy**:

1. **Redundant Links**: Implement **redundant links** between critical devices and the central switch. This ensures that if one link fails, there is an alternate path for communication.
2. **Uninterruptible Power Supply (UPS)**: Connect the central switch and important devices to a UPS to ensure that network equipment remains powered during power outages.
3. **Network Monitoring**: Use network monitoring tools to proactively identify issues and respond quickly to failures.
4. **Regular Backups**: Regularly back up network configurations and critical data to prevent data loss in case of a failure.
5. **Fault-Tolerant Hardware**: Choose high-quality and fault-tolerant networking hardware that is less likely to fail.
6. **Load Balancing**: Implement load balancing techniques to distribute network traffic evenly across available links, reducing the risk of congestion and failures.
7. **Network Segmentation**: Divide the network into segments based on departments or functions. This limits the impact of failures to specific segments rather than affecting the entire network.
8. **Network Isolation**: Isolate critical devices or servers in a separate network segment to protect them from potential security breaches or issues in other parts of the network.
9. **Remote Access and Monitoring**: Set up remote access and monitoring capabilities to allow administrators to manage and troubleshoot the network even when they are not on-site.

Q10

To create an efficient and reliable network for the corporate headquarters with the different departments, I would propose a network design that incorporates a combination of network topologies to meet the specific needs of each department. Here's a comprehensive network design that addresses the requirements:

1. **Administration Department: Star Topology**
   * The Administration department usually requires centralized control and management.
   * A star topology with the central hub acting as the main server would be suitable.
   * All devices in the Administration department connect directly to the central hub, providing efficient communication within the department.
   * This topology simplifies management and troubleshooting.
2. **Research and Development Department: Mesh Topology**
   * The Research and Development (R&D) department requires maximum reliability due to critical projects.
   * A mesh topology is ideal for the R&D department as it offers high redundancy and fault tolerance.
   * Each device in the R&D department connects to every other device, ensuring multiple paths for data transmission.
   * This topology minimizes downtime and ensures constant connectivity for critical projects.
3. **Marketing Department: Ring Topology**
   * The Marketing department requires seamless collaboration and communication.
   * A ring topology is well-suited for the Marketing department, as each device connects to two adjacent devices, creating a circular communication path.
   * This setup allows efficient communication within the department, promoting collaboration.
   * However, the reliability might not be as high as in a mesh topology, so careful consideration should be given to backup links.
4. **Customer Support Department: Bus Topology**
   * The Customer Support department typically requires a straightforward and cost-effective network setup.
   * A bus topology can serve this purpose, where all devices are connected to a central backbone (main cable).
   * This topology allows for easy scalability and cost-effectiveness in a department with potentially large numbers of devices.

Interactions and Collaboration:

* The use of these different topologies ensures that each department's unique requirements are met while promoting inter-departmental collaboration.
* Inter-departmental communication can be achieved through the use of routers or layer 3 switches that connect the different departments.
* Critical inter-departmental data sharing, such as between R&D and Marketing, can occur over redundant paths provided by the mesh and ring topologies.
* To increase the reliability of the R&D department, redundant connections to the mesh topology can be established, ensuring that even if one link fails, alternative paths are available.

Key Considerations:

* Network security measures, such as firewalls and intrusion detection/prevention systems, should be implemented at key entry and exit points.
* Network segmentation can be applied to isolate sensitive data and ensure proper access control.
* Regular monitoring and maintenance will be essential to identify and address any potential issues promptly.

Q11

False

Q12

b. Detecting errors in data transmission

Q13

c. 2^32

Q14

c. Directs data to a specific recipient using its unique address.

Q15

b. Distributing software updates to devices in a local network.