Q3. Where this CAPWAP fits in OSI model, what are the two tunnels in CAPWAP and its purpose

Data Link Layer

If CAPWAP is used over Ethernet, it operates at Layer 2.

This allows APs and WLCs to communicate without requiring an IP network.

Network Layer

Most networks use Layer 3 CAPWAP over IP-based networks.

APs and WLCs communicate across different subnets using IP.

Transport Layer

CAPWAP encapsulates its control and data messages using UDP.

UDP 5246 → Used for control messages. **UDP 5247** → Used for data messages

Two tunnels in CAPWAP and its purpose

1. **Control Tunnel (Encrypted)**
   UDP Port 5246 is responsible for exchanging management and control information between the AP and WLC.
   Encrypted using DTLS (Datagram Transport Layer Security**)** to protect management communication.

2. **Data Tunnel**
   UDP Port 5247 handles actual user data traffic between the AP and WLC. This tunnel is responsible for forwarding packets while ensuring authentication and policy enforcement.

   Encryption in the data tunnel is optional to reduce processing overhead, depending on the network's security requirements.

Q4. What is the difference between Lightweight APs and Cloud-based Aps

Lightweight Aps:

Managed by an on-premises Wireless LAN Controller.

Control functions handled by WLC.

Traffic can be tunnelled to WLC or directly forwarded.

Suitable for large enterprises with dedicated IT teams.

Adding APs requires more controllers for large deployments.

Higher upfront cost due to WLC requirement.

Manual configuration via WLC, firmware updates pushed from WLC.

Cloud-based Aps:

Managed via a cloud controller hosted on the internet.

No need for on-premises WLC, reducing hardware costs.

Can be configured and monitored remotely via a web dashboard or mobile app.

Ideal for distributed networks, branch offices, and businesses with multiple locations.

Automatic updates and security patches handled by the cloud provider.

Highly scalable, as adding new APs does not require additional controllers.

Q5. How the CAPWAP tunnel is maintained between AP and controller

The CAPWAP tunnel between the Access Point and the Wireless LAN Controller is maintained using keepalive messages, retransmissions, and session timeouts. The tunnel operates over UDP ports 5246 and 5247.

1. CAPWAP Tunnel Establishment Process

Discovery Phase

The AP discovers the WLC using methods like DHCP Option 43, DNS resolution. The AP sends a CAPWAP Discovery Request. The WLC responds with a CAPWAP Discovery Response.

Join & Authentication Phase

The AP sends a Join Request to the selected WLC.The WLC authenticates the AP and sends a CAPWAP Join Response. DTLS encryption is established for secure control messages.

Configuration & Image Download Phase

The WLC checks the AP firmware version and pushes updates if needed. The AP receives configuration settings. The AP starts forwarding client traffic over the CAPWAP tunnel. The tunnel is continuously maintained through keepalive messages.

Keepalive Messages

The AP and WLC exchange keepalive messages periodically.

Default keepalive interval: 30 seconds.

If no response is received for three consecutive keepalives, the AP marks the WLC as unreachable and initiates failover.

If a keepalive response is not received, the AP retries sending it.

If the WLC fails to respond within a timeout period, the AP disconnects and searches for another WLC.

DTLS encryption ensures that control messages remain secure. Uses UDP port 5246 for encryption.