CAPWAP - OSI Model

The Control and Provisioning of Wireless Access Points (CAPWAP) protocol does not map neatly to a single layer of the OSI model but operates across multiple layers, primarily spanning the Data Link Layer (Layer 2) and Network Layer (Layer 3), with some elements extending into the Application Layer (Layer 7) for management functions. Here's a breakdown:

Data Link Layer (Layer 2): CAPWAP is involved in the encapsulation and tunneling of 802.11 wireless frames between the Access Point (AP) and the Wireless LAN Controller (WLC). This includes handling MAC-layer functions, especially in split MAC architectures where the WLC manages higher-layer MAC operations.

Network Layer (Layer 3): CAPWAP uses IP for communication between the AP and WLC, and it relies on UDP as its transport protocol. The tunneling mechanism operates at this layer, allowing CAPWAP to encapsulate data across IP networks.

Application Layer (Layer 7): The control and management messages (e.g., configuration, status updates) are handled at a higher level, resembling application-layer protocols, as they involve structured data exchange between the AP and WLC.

In essence, CAPWAP is a tunneling and management protocol that bridges wireless-specific functions with IP-based network infrastructure, making it a cross-layer protocol.

Two Tunnels in CAPWAP and Their Purposes

CAPWAP establishes two distinct tunnels between the AP and the WLC to separate control and data traffic, enhancing efficiency and security. These tunnels are:

Control Tunnel:

- This tunnel is used for exchanging management and control messages between the AP and the WLC. It handles tasks such as AP discovery, joining, configuration updates, firmware downloads, and status reporting (e.g., client associations, RF statistics).
- The control tunnel is secured using Datagram Transport Layer Security (DTLS), which provides encryption and integrity for all control messages.
- It operates over UDP port 5246 by default.
- Key Function: Ensures centralized management and real-time adjustments to the wireless network, such as channel or power settings.

Data Tunnel:

- This tunnel is used to transport wireless client data traffic between the AP and the WLC, particularly in a split MAC architecture where the WLC handles higher-layer processing (e.g., encryption, authentication). In local MAC setups, this tunnel may be less utilized as the AP bridges traffic directly.
- Like the control tunnel, the data tunnel can be secured with DTLS to protect client data during transit.
- It operates over UDP port 5247 by default.
- Key Function: Facilitates centralized switching and policy enforcement for client data, allowing the WLC to aggregate and manage traffic before forwarding it to the wired network.