CAPWAP

CAPWAP, or Control and Provisioning of Wireless Access Points, is a standard protocol used to manage and control wireless access points (APs) in a centralized manner, typically through a Wireless LAN Controller (WLC). Developed by the IETF, CAPWAP aims to provide a standardized way to centralize the configuration, firmware management, and monitoring of APs, while also supporting the separation of data and control planes in wireless networks.

CAPWAP operates by establishing a communication tunnel between the AP and the WLC. This allows the WLC to handle tasks such as authentication, encryption, and policy enforcement, while the AP focuses on radio frequency (RF) management and client connectivity. The protocol supports both local MAC (Media Access Control) and split MAC architectures:

Local MAC: The AP handles most of the 802.11 functions, with the WLC providing control and management.
Split MAC: The AP handles real-time functions (e.g., frame exchange), while the WLC manages higher-layer functions (e.g., authentication and encryption).

CAPWAP uses UDP as its transport protocol and operates over two main ports: one for control messages (default 5246) and another for data traffic (default 5247).

Flow Between AP and Controller

The interaction between an AP and a WLC in a CAPWAP-based system follows a structured flow.

Discovery:
When an AP is powered on, it enters a discovery phase to locate a WLC. It uses methods like DHCP options, DNS resolution, or broadcast/multicast messages to find available controllers. The AP sends a Discovery Request message to potential WLCs.
Join Process:

- The WLC responds with a Discovery Response, providing details about itself (e.g., IP address, capacity).
- The AP selects a WLC and sends a Join Request, including its certificate or credentials.
- The WLC verifies the AP's identity and sends a Join Response. If successful, a secure DTLS (Datagram Transport Layer Security) tunnel is established for control messages.

Configuration and Image Download:

- The WLC pushes the configuration to the AP, including settings for SSIDs, security policies, and RF parameters.
- If needed, the AP downloads the latest firmware image from the WLC.

Run State:

- The AP enters the Run state, where it starts serving clients. Control messages (e.g., statistics, configuration updates) continue to flow over the DTLS tunnel.
- Data traffic from wireless clients can either be tunneled back to the WLC (central switching) or locally bridged by the AP (local switching), depending on the network design.

Ongoing Communication:

- The AP periodically sends status updates (e.g., client associations, interference data) to the WLC.
- The WLC can send commands to the AP, such as channel changes or power adjustments, to optimize the wireless network.

Data Flow

Control Plane: All management and control messages (e.g., configuration, status) are exchanged over the secure DTLS tunnel between the AP and WLC.

Data Plane: In a split MAC architecture, client data traffic is encapsulated and tunneled to the WLC over a separate CAPWAP data channel (using UDP port 5247). In local MAC, the AP handles data traffic directly, reducing the load on the WLC.