Q5)How the CAPWAP tunnel is maintained between AP and Controller

The **CAPWAP (Control and Provisioning of Wireless Access Points) tunnel** is the secure communication channel between **Lightweight APs (LAPs)** and the **Wireless LAN Controller (WLC)**. Here's how it's established and maintained:

## ****1. CAPWAP Tunnel Establishment Process****

### ****Step 1: AP Discovery****

The AP boots up and searches for a WLC using:

* **DHCP Option 43** (WLC IP addresses provided by DHCP server)
* **DNS Lookup** (e.g., CISCO-CAPWAP-CONTROLLER.localdomain)
* **Broadcast** (if no DHCP/DNS info is available)
* **Primed (Pre-configured) WLC List** (if manually set)

### ****Step 2: CAPWAP Join Process****

* The AP sends a **CAPWAP Discovery Request**.
* The WLC responds with a **CAPWAP Discovery Response**.
* The AP selects a WLC (based on priority or load) and initiates a **DTLS (Datagram Transport Layer Security) handshake** (for encryption).
* Once secured, the AP sends a **CAPWAP Join Request**.
* The WLC validates the AP and replies with a **CAPWAP Join Response** (approving the connection).

### ****Step 3: Firmware & Configuration Download****

* The WLC checks if the AP needs a firmware update.
* If required, the AP downloads the firmware via the CAPWAP tunnel.
* The WLC pushes the **configuration** (SSIDs, security policies, radio settings).

### ****Step 4: Operational State****

* The AP enters **operational mode** and starts broadcasting Wi-Fi networks.
* The **CAPWAP control tunnel (UDP 5246)** remains active for management.
* The **CAPWAP data tunnel (UDP 5247)** carries client traffic (if in split-MAC mode).

## ****2. How the Tunnel is Maintained?****

### ****Keepalive Mechanism (Heartbeats)****

* The AP and WLC exchange **CAPWAP Echo Request/Response** messages (default: every **30 seconds**).
* If **5 consecutive heartbeats fail**, the AP declares the WLC dead and starts rediscovery.

### ****DTLS Security****

* The **control tunnel** is always encrypted with **DTLS** (prevents hijacking).
* The **data tunnel** can optionally use DTLS (often disabled for performance).

### ****Path MTU Discovery****

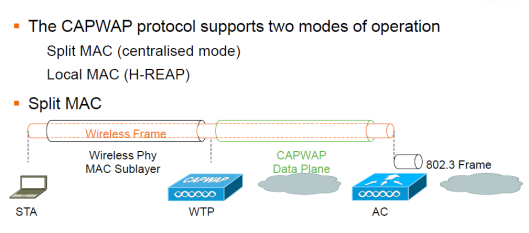
* CAPWAP performs **Path MTU Discovery** to avoid fragmentation in the network.
* Ensures optimal packet size for tunneled traffic.

### ****Failover & Redundancy****

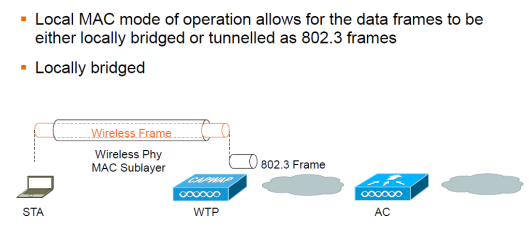
* If the primary WLC fails, the AP fails over to a backup WLC (if configured).
* APs can be configured with multiple WLCs in a **priority list**.

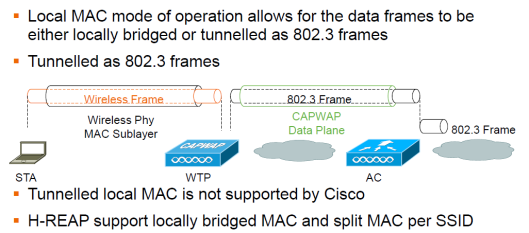
## ****CAPWAP Modes: Local vs. Split MAC****

|  |  |  |
| --- | --- | --- |
| **Mode** | **Where Traffic Goes** | **Use Case** |
| **Local MAC** | Data stays at AP (only control goes to WLC) | Good for small offices |
| **Split MAC** | All traffic tunnels to WLC (full control) | Enterprise networks (most common) |



In Local MAC mode AP is doing all of the functions including the one done by WLC in Split MAC architecture:





Below diagram shows the CAPWAP State machine where you need to understand this in order to determine from where you should start troubleshoot if something is not working:

