**1. Brief about SplitMAC architecture and how it improves the AP's performance**

SplitMAC architecture is a wireless networking approach commonly used in enterprise WLANs. It divides the MAC (Medium Access Control) layer functionalities between a Lightweight Access Point (LWAP) and a centralized Wireless LAN Controller (WLC), enhancing performance, manageability, and scalability.

Overview

In a traditional setup, all MAC functions are handled by the AP. In SplitMAC:

* LWAPs handle time-sensitive operations like frame acknowledgment, RTS/CTS, encryption/decryption, and beacon transmissions.
* WLCs manage higher-level, non-time-critical tasks such as authentication, association, mobility management, load balancing, and QoS enforcement.

Performance Improvements

* Reduced Processing Load:  
  LWAPs are freed from complex decision-making, allowing them to operate more efficiently with lower latency.
* Centralized Management:  
  The WLC provides a unified platform for configuring, monitoring, and controlling multiple APs.
* Seamless Roaming:  
  Clients experience uninterrupted connectivity when moving between APs, as roaming is handled centrally.
* Improved Scalability:  
  New APs can be added easily without complicating network management.
* Enhanced Security:  
  Centralized authentication and policy enforcement ensure consistent and secure access control across the network.

**2. Describe about CAPWAP, explain the flow between AP and Controller**

CAPWAP (Control and Provisioning of Wireless Access Points) is a standardized protocol (defined in RFC 5415) that facilitates communication between a Lightweight Access Point (LWAP) and a Wireless LAN Controller (WLC) in a SplitMAC architecture. It enables centralized management of wireless networks by securely controlling APs.

What is CAPWAP?

* CAPWAP encapsulates control and data messages between the AP and WLC.
* It supports automatic AP discovery, firmware management, configuration, and security handling.
* Operates over UDP (port 5246 for control, port 5247 for data).
* Ensures encryption and authentication using DTLS (Datagram Transport Layer Security) for control messages.

CAPWAP Flow Between AP and Controller

* Discovery:  
  The AP boots up and searches for a controller using methods like DHCP (Option 43), DNS, or broadcast.
* Join Process:  
  Once a controller is found, the AP initiates a join request. The controller responds with a join response, accepting the AP.
* DTLS Tunnel Establishment:  
  A secure DTLS tunnel is created between the AP and the controller for encrypted control communication.
* Configuration:  
  The controller pushes configuration settings (SSID, security, RF parameters) to the AP.
* Image Download (if needed):  
  If the AP's firmware is outdated, the controller upgrades it automatically.
* Data and Control Tunnels:
  + Control messages (e.g., configuration, management) are sent through the control tunnel.
  + Client data traffic can be sent either directly to the controller (central switching) or locally bridged by the AP.

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

CAPWAP in the OSI Model

* CAPWAP operates primarily at the Application Layer (Layer 7) of the OSI model.
* However, it also involves layers below:
  + Uses UDP at the Transport Layer (Layer 4).
  + Encapsulated over IP at the Network Layer (Layer 3).
* Control messages are secured using DTLS (Datagram Transport Layer Security), which functions between the Application and Transport layers.

Two Tunnels in CAPWAP and Their Purpose

CAPWAP uses two separate logical tunnels between the Access Point (AP) and the Wireless LAN Controller (WLC):

* Control Tunnel:
  + Transports CAPWAP control messages such as configuration, management, and monitoring commands.
  + Operates over UDP port 5246.
  + Secured using DTLS encryption for confidentiality and integrity.
  + Handles AP discovery, join process, configuration updates, and firmware downloads.
* Data Tunnel:
  + Carries client data traffic (e.g., web browsing, file transfers).
  + Operates over UDP port 5247.
  + Can support two types of traffic forwarding:
    - Central switching: All data passes through the controller.
    - Local switching: Data is handled locally by the AP.

**4. Whats the difference between Lightweight APs and Cloud-based Aps**

Access Points (APs) are essential components in wireless networks. Both Lightweight APs and Cloud-based APs aim to simplify management and improve scalability, but they differ in their architecture and control mechanisms.

Lightweight APs (LWAPs)

* Managed by a centralized Wireless LAN Controller (WLC) located within the network.
* Operate using SplitMAC architecture, handling time-sensitive functions locally and offloading control tasks to the WLC.
* Communication with the WLC happens over CAPWAP protocol.
* Ideal for large, campus-style enterprise networks with on-premise infrastructure.
* Offers centralized control, fast roaming, and strong QoS support.
* Requires local controller hardware and higher upfront investment.

Cloud-based APs

* Managed through a cloud-based controller hosted by the vendor (e.g., Cisco Meraki, Aruba Central).
* Do not require on-premise WLCs—management is done via a web dashboard or mobile app.
* Suitable for distributed networks, remote offices, and SMBs.
* Configuration, monitoring, and updates are handled via the internet.
* Scalable and cost-effective, as there's no need for local controller infrastructure.
* Dependent on internet connectivity for full management capabilities

**5. How the CAPWAP tunnel is maintained between AP and controller**

CAPWAP (Control and Provisioning of Wireless Access Points) is a standardized protocol that enables centralized control of Access Points (APs) by a Wireless LAN Controller (WLC). It uses two logical tunnels—**Control** and **Data**—to manage APs and forward client traffic. Maintaining these tunnels ensures reliable wireless network operations.

**CAPWAP Tunnel Establishment and Maintenance**

* **Discovery Phase:**
  + When an AP boots, it searches for a controller using methods like DHCP (Option 43), DNS, or broadcast.
* **Join Request:**
  + The AP sends a **Join Request** to the discovered WLC.
  + The WLC validates the AP and responds with a **Join Response**.
* **DTLS Tunnel Creation (Control Tunnel):**
  + A secure **DTLS (Datagram Transport Layer Security)** tunnel is created over **UDP port 5246**.
  + This tunnel handles management and control messages (e.g., configuration, monitoring, and firmware updates).
* **Data Tunnel Setup:**
  + A separate tunnel over **UDP port 5247** is established for **client data traffic**.
  + Can be centrally switched (through WLC) or locally bridged (by AP).
* **Heartbeat/Keepalive Messages:**
  + AP and controller exchange periodic **Keepalive packets** (Echo requests and responses).
  + These ensure the tunnel is alive and the AP is still connected.
* **Re-establishment on Failure:**
  + If the tunnel drops due to a network issue, the AP re-initiates the discovery and join process to re-establish the tunnel.

**6.Whats the difference between Sniffer and monitor mode, use case for each mode**

In wireless networking, Sniffer mode and Monitor mode are two special modes used for capturing and analyzing wireless traffic. Though similar in purpose, they differ in functionality and application.

Sniffer Mode

* Allows a device (typically an AP) to capture and forward 802.11 frames to a controller or analysis tool.
* Often used in enterprise WLANs where the captured data is sent to a central controller for analysis.
* Can work as part of a system like Wireless Intrusion Detection Systems (WIDS).
* Captures only the traffic related to configured channels and networks.

Use Case:

* Troubleshooting in enterprise networks: Capturing traffic to analyze performance issues or detect rogue APs, often sent to a controller using CAPWAP.

Monitor Mode

* A mode used by wireless network interfaces to passively listen to all wireless traffic, regardless of SSID or association.
* Captures all packets in the air, including management, control, and data frames on a specific channel.
* Doesn’t require connection to any network or controller.

Use Case:

* Security auditing and penetration testing: Used with tools like Wireshark or Aircrack-ng to analyze wireless traffic and identify vulnerabilities.

**7.If WLC deployed in WAN, which AP mode is best for local network and how?**

When a Wireless LAN Controller (WLC) is deployed in a Wide Area Network (WAN)—i.e., not locally within the same LAN as the Access Point (AP)—it is crucial to choose an AP mode that ensures local network performance, reliability, and survivability even during WAN outages.

Recommended AP Mode: FlexConnect Mode

* FlexConnect Mode is the most suitable AP mode when the WLC is located remotely over the WAN.
* It allows the AP to function independently of the controller for most local operations.

How FlexConnect Works

* The AP establishes a CAPWAP control tunnel with the WLC over the WAN.
* In connected mode, the AP can receive configurations and policy updates from the WLC.
* In standalone mode (if WAN fails):
  + The AP continues to serve clients using previously downloaded configurations.
  + Supports local switching, meaning client traffic is directly bridged to the local LAN, reducing latency.
  + Supports local authentication, allowing users to still connect to Wi-Fi during WLC unavailability.

**8. What are challenges if deploying autonomous APs (more than 50) in large network like university**

Autonomous Access Points (APs), also known as standalone APs, operate independently without relying on a central controller. While suitable for small setups, deploying more than 50 such APs in a large network like a university campus presents several significant challenges.

Challenges in a University Network

* Lack of Centralized Management
  + Each AP must be configured, updated, and monitored individually.
  + Increases administrative burden and chances of configuration errors.
* Inconsistent Policies
  + Maintaining uniform security settings, SSIDs, VLANs, and QoS policies across all APs is difficult.
  + Leads to inconsistent user experience.
* Complex Troubleshooting
  + No centralized logging or monitoring makes fault isolation slow and inefficient.
  + Manual diagnosis is time-consuming in large deployments.
* Inefficient Roaming
  + Client devices may experience frequent disconnections or delays while moving between APs.
  + Lack of coordination causes poor handoff between APs.
* Scalability Issues
  + Adding or modifying APs becomes labor-intensive as the network grows.
  + Managing firmware updates and changes at scale is impractical.
* Security Risks
  + Difficult to enforce network-wide security policies or detect rogue APs.
  + Increases vulnerability to misconfigurations and attacks.
* High Operational Cost
  + Requires more manpower and time for management.
  + No automation or centralized control leads to long-term inefficiencies.

**9. What happens on wireless client connected to Lightweight AP in local mode if WLC goes down.**

Lightweight Access Points (LWAPs) in Local Mode depend heavily on the Wireless LAN Controller (WLC) for control and management. In this architecture, both control and data traffic are centralized through the WLC.

Client Impact When WLC Fails

* CAPWAP Tunnel Loss
  + The LWAP loses its CAPWAP control tunnel with the WLC.
  + Without this tunnel, the AP cannot function in Local Mode.
* Client Disconnection
  + Clients currently connected to the AP will be disconnected.
  + The AP stops broadcasting SSIDs since it can no longer receive control information from the WLC.
* No New Client Associations
  + New clients will not be able to connect to the AP, as it is no longer advertising the wireless network.
* No Data Forwarding
  + Since Local Mode uses central switching, client data is routed through the WLC.
  + With the WLC down, no data traffic can be processed or forwarded.
* Limited Local Functionality
  + Local Mode LWAPs do not have autonomy; they rely on the WLC for all operations, unlike FlexConnect mode.
  + The AP effectively becomes non-functional until it reconnects to the WLC.