Wi-Fi Training Program
Assignment Questions -Module 2

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

   In traditional Wi-Fi architectures, the Access Point (AP) handles all the MAC (Media Access Control) layer functions. This includes tasks like association, authentication, encryption, frame aggregation, and power management. As the number of clients and traffic load increases, the AP can become a bottleneck, leading to performance degradation.

   SplitMAC architecture addresses this issue by **distributing the MAC layer functions between the AP and a centralized Wireless LAN Controller (WLC)**. The real-time, time-sensitive functions like frame aggregation and 802.11 management frame processing are handled by the AP, while the non-real-time functions like authentication, security policy enforcement, and client management are handled by the WLC.

Performance Improvements:

- **Reduced Processing Load on AP:** By offloading complex tasks to the WLC, the AP has more processing power to handle data traffic, leading to higher throughput and lower latency.
- **Improved Scalability:** The WLC can manage multiple APs, simplifying network management and allowing for easier scaling of the wireless network.
- **Centralized Control:** The WLC provides a single point of control for the entire wireless network, enabling consistent policy enforcement, security management, and troubleshooting.
- **Optimized Roaming:** The WLC can facilitate faster and seamless roaming for clients moving between APs.
- **Enhanced Security:** Centralized security policies and authentication mechanisms improve overall network security.

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

CAPWAP (**Control and Provisioning of Wireless Access Points**) is a protocol that allows **wireless access points (APs) to communicate with a central Wireless LAN Controller (WLC)**. It provides a **secure, scalable, and efficient** method for managing APs in a network
Flow Between AP and Controller in CAPWAP

1. **AP Discovery**
   - The AP boots up and looks for a **WLC**.

    - It may discover the WLC using **DHCP, DNS, or static configuration**.

- **CAPWAP Tunnel Establishment**
    - The AP and WLC establish a **secure CAPWAP tunnel** (DTLS encryption is used for security).
    - This tunnel has two channels:
        - **Control Tunnel** (for configuration and management)
        - **Data Tunnel** (for forwarding client traffic)
- **AP Authentication and Configuration Download**
    - The WLC authenticates the AP.
    - The AP downloads its configuration (SSID, security settings, QoS rules, etc.).
- **Client Association and Data Forwarding**
    - Once the AP is configured, **wireless clients can connect** to the network.
    - The AP sends client data to the WLC through the CAPWAP **data tunnel**.
    - The WLC processes and forwards traffic to the appropriate destination.
- **AP Monitoring and Roaming**
    - The WLC continuously monitors APs and clients.
    - If a client moves between APs, the WLC manages the **roaming process** to ensure seamless connectivity.

3. Where Does CAPWAP Fit in the OSI Model, and What Are the Two Tunnels in CAPWAP?

CAPWAP primarily operates at Layer 3 (Network Layer) and Layer 4 (Transport Layer) of the OSI model.

- Layer 3: CAPWAP uses IP for communication between the AP and the WLC.
- Layer 4: CAPWAP uses UDP (User Datagram Protocol) as the transport protocol.

Two Tunnels in CAPWAP and their Purpose:

CAPWAP utilizes two distinct tunnels for communication between the AP and the WLC:

Control Tunnel:

- Purpose: This tunnel is used for the exchange of control and management information between the AP and the WLC.

Data Tunnel:

- **Purpose:** This tunnel is used for the forwarding of wireless client data between the AP and the WLC.

4. **What's the difference between Lightweight APs and Cloud-based Aps**

Feature	Lightweight APs	Cloud-Based APs
Management	**Requires on-premises WLC**	**Managed via cloud dashboard**
Scalability	**Scalable, but needs additional WLCs for large deployments**	**Highly scalable with no hardware controller needed**
Independence	**Dependent on WLC**	**Can work independently if cloud access is lost**
Deployment	**Best for large enterprises with IT teams**	**Best for distributed networks and remote locations**
Roaming Support	**Seamless roaming with WLC assistance**	**Roaming depends on cloud controller features**
Security	**Centralized security via WLC**	**Cloud security with automatic updates**

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

The CAPWAP (Control and Provisioning of Wireless Access Points) protocol ensures continuous communication between an Access Point (AP) and a Wireless LAN Controller (WLC) through two tunnels: the control tunnel and the data tunnel. Maintaining these tunnels is critical for efficient network operation, centralized management, and security.

1. Establishing the CAPWAP Tunnel

When an AP boots up, it follows a series of steps to establish a CAPWAP connection with the WLC:

- AP Discovery: The AP locates an available WLC using methods such as DHCP, DNS, or Layer 2 broadcasts.
- Handshake and Authentication: The AP and WLC exchange control messages to authenticate and initiate a session.
- DTLS Encryption Setup: A secure control tunnel is established over UDP port 5246.
- Configuration and Firmware Updates: The WLC provisions the AP with necessary settings, including SSIDs, security policies, and software updates.

- Data Tunnel Creation: A second tunnel over UDP port 5247 is established for client traffic.

2. Maintaining the CAPWAP Tunnel

Once established, the CAPWAP tunnel is maintained through continuous communication between the AP and WLC.

- Keep-Alive Messages: The AP periodically sends heartbeat messages to verify the WLC's availability.
- Control Plane Management: The WLC continuously updates AP settings, security policies, and radio parameters.
- Firmware and Patch Distribution: The AP receives periodic firmware updates and security patches via the control tunnel.
- Traffic Management: The WLC monitors and manages client data through the data tunnel, optimizing network performance.

3. Handling CAPWAP Tunnel Disruptions

If the CAPWAP tunnel is disrupted, different AP modes determine how the network operates:

- Standard Lightweight Mode: The AP loses connectivity until it re-establishes a connection with the WLC.
- FlexConnect Mode: The AP continues functioning independently, allowing local traffic switching while awaiting WLC recovery.
- Fallback Mechanisms: The AP attempts automatic reconnection using pre-configured WLC redundancy or backup mechanisms.

6. **What's the difference between Sniffer and monitor mode, use case for each mode**

Feature	**Sniffer Mode**	**Monitor Mode**
Purpose	Packet analysis via WLC	Passive network monitoring
Requires WLC	Yes	No
Captures Data	Sends to WLC or analyzer	Local capture on the device
Use Case	Troubleshooting, security monitoring	Site surveys, threat detection
Packet Types	802.11 frames relevant to active sessions	All packets on the selected channel

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

In scenarios where the Wireless LAN Controller (WLC) is deployed over a Wide Area Network (WAN), the most suitable AP mode for local network deployment is the **FlexConnect mode**.

Justification:

FlexConnect mode, formerly known as Hybrid Remote Edge Access Point (H-REAP), is specifically designed for remote-site deployments where APs are connected to the central WLC across a WAN link. This mode offers the following advantages:

- **Local Switching:** Client data traffic can be switched locally at the branch site, reducing WAN bandwidth consumption and latency.
- **Resilient Connectivity:** In the event of WAN link failure or unreachability of the WLC, FlexConnect APs can continue to serve clients using locally cached authentication credentials and policies.
- **Optimized Control Plane:** Management and control traffic is minimized across the WAN, ensuring efficient use of network resources.
- **Seamless User Experience:** Users at remote sites experience uninterrupted connectivity and authentication, even when the WLC is temporarily inaccessible.

Operational Behavior:

- **Connected Mode:** When the WAN link to the WLC is active, FlexConnect APs maintain control communication with the WLC and follow configured central or local switching policies.
- **Standalone Mode:** When the WAN link is down, APs autonomously handle client authentication and maintain local switching, ensuring continued network availability.

8. **What are the challenges if deploying autonomous Access Points (APs) (more than 50) in a large network like a university?**
   Deploying more than 50 **autonomous APs** (also known as **standalone APs**) in a large-scale environment such as a university campus presents several technical and operational challenges. Autonomous APs operate independently without centralized control, which limits their scalability and manageability in complex network environments.
   Key Challenges:

1. **Lack of Centralized Management:**
   - Each AP must be configured, monitored, and maintained individually.
   - Firmware updates, security policy changes, and performance tuning must be done manually for each AP, increasing administrative overhead.
2. **Inefficient Roaming and Handoff:**

- Without a centralized controller, seamless roaming between APs can be disrupted.
- Clients may experience delays or dropped connections during transitions between coverage areas, especially in mobile environments.

3. **Inconsistent Radio Resource Management (RRM):**
   - Autonomous APs cannot coordinate channel selection and transmit power adjustments across the network.
   - This can lead to co-channel interference, suboptimal coverage, and poor overall network performance.
4. **Scalability Issues:**
   - As the number of APs grows, managing them individually becomes increasingly complex and time-consuming.
   - Network monitoring and troubleshooting across a large number of standalone APs is inefficient and prone to errors.
5. **Security Concerns:**
   - Implementing and maintaining consistent security policies (such as WPA2-Enterprise or VLAN segmentation) is difficult without centralized control.
   - There is a higher risk of misconfiguration and non-uniform enforcement of access control policies.
6. **Limited Visibility and Analytics:**
   - Without centralized logging and monitoring, network administrators lack real-time visibility into traffic patterns, client behavior, and performance metrics.

9. What happens to a wireless client connected to a Lightweight AP in local mode if the WLC goes down?

When a **Lightweight Access Point (AP)** is operating in **local mode** and the **Wireless LAN Controller (WLC)** becomes unreachable (e.g., due to a WAN or controller failure), several behaviors are triggered depending on the AP's configuration and the client session status.

Behavior of the Wireless Client in This Scenario:

1. **Existing Wireless Clients (Already Authenticated):**
   - Clients that are already authenticated and associated with the AP **may continue to remain connected** for a short period.
   - However, without communication with the WLC, the AP cannot perform key functions such as reauthentication, policy updates, or client roaming.
   - Features like QoS, ACLs, or mobility (Layer 3 roaming) will no longer be enforced properly.
2. **New Wireless Clients (Attempting to Join):**
   - The AP cannot authenticate or associate new clients, as these operations rely on the WLC.

- As a result, **new client connections will fail** until the WLC becomes reachable again.

3. **Loss of Centralized Control and Services:**
   - The AP loses its control plane connection with the WLC.
   - Centralized features such as wireless intrusion detection, client tracking, and configuration updates are unavailable.