# MODULE 2 ASSIGNMENT

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

**SplitMAC architecture** is a fundamental concept in enterprise wireless networks, particularly in environments using lightweight access points (APs) managed by a wireless LAN controller (WLC). In this architecture, the functions of the MAC (Media Access Control) layer are divided between the AP and the WLC to optimize performance and manageability. The AP is responsible for handling real-time, time-sensitive MAC functions such as frame acknowledgments, encryption/decryption, retransmissions, and power-saving mechanisms. These tasks require immediate responses and are best performed locally on the AP to reduce latency and improve reliability.

On the other hand, non-time-sensitive functions such as client authentication, association, roaming decisions, radio resource management (RRM), and policy enforcement are offloaded to the centralized WLC. This separation allows the controller to make intelligent, global decisions about the wireless network using information from all connected APs, leading to better channel utilization, load balancing, and security enforcement.

By offloading complex decision-making and management tasks to the WLC, SplitMAC reduces the processing load on individual APs and simplifies configuration and updates across the network. This results in enhanced scalability, as more APs can be deployed and managed efficiently, and improved network performance through centralized optimization and reduced contention. Overall, SplitMAC architecture enables more flexible, secure, and high-performing wireless network deployments in large-scale enterprise environments.

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

CAPWAP (Control And Provisioning of Wireless Access Points) is a protocol used to connect and manage lightweight APs from a central Wireless LAN Controller (WLC). It helps in simplifying configuration, firmware updates, and traffic management in large wireless networks.

Simple Flow Between AP and Controller:

- AP gets IP using DHCP.
- AP discovers the WLC (using DHCP option 43, DNS, or broadcast).
- AP sends Join Request to the WLC.
- WLC authenticates the AP and forms a secure control tunnel (UDP port 5246).
- WLC sends config/firmware to the AP.
- A data tunnel is created (UDP port 5247) for client traffic.
- AP starts working and serves wireless clients as per the controller's instructions.

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

CAPWAP in OSI Model:

- CAPWAP works at Layer 2 (Data Link Layer) and Layer 3 (Network Layer).
- It mainly uses UDP for communication between AP and WLC.

Two Tunnels in CAPWAP:

- Control Tunnel (UDP port 5246):
  - Used to send configuration, management, and firmware updates.
  - Encrypted using DTLS for security.
- Data Tunnel (UDP port 5247):
  - Used to carry client traffic (like internet browsing, video, etc.) between AP and WLC.
  - May or may not be encrypted, depending on setup.

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

| **Feature** | **Lightweight APs** | **Cloud-Based APs** |
|---|---|---|
| Controller Type | Managed by an on-premises WLC | Managed by a cloud-based controller |
| Deployment | Requires local WLC hardware | Managed over the internet from cloud dashboard |
| Configuration | Centralized via WLC | Centralized via cloud interface |
| Updates | Pushed from local WLC | Pushed from the cloud automatically |
| Reliability | Depends on WLC availability | Depends on internet connectivity |
| Scalability | Limited to WLC capacity | Easily scalable via cloud |
| Use Case | Good for enterprise campuses | Ideal for distributed sites and SMBs |

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

- The CAPWAP tunnel is maintained using UDP ports 5246 (control) and 5247 (data).
- The control tunnel is encrypted using DTLS (Datagram Transport Layer Security) for secure communication.
- Keepalive messages (also called heartbeats) are sent regularly between the AP and the WLC to ensure the connection is still active.
- If the AP stops receiving responses from the WLC for a certain time (timeout), it assumes the tunnel is broken and will try to re-discover and rejoin the controller.

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

| Feature | Sniffer Mode | Monitor Mode |
|---|---|---|
| Purpose | Captures and forwards wireless packets to a tool | Observes wireless activity without serving clients |
| Data Handling | Sends data to a protocol analyzer (e.g., Wireshark) | Just listens and doesn’t transmit anything |
| Client Support | Cannot serve clients | Cannot serve clients |
| Use Case | Deep packet analysis, troubleshooting | RF spectrum analysis, rogue AP detection |
| Traffic View | Sees detailed frame-level data | Sees overall channel usage and interference |

**Use Cases:**

- Sniffer Mode: Used by network engineers for packet capture and protocol-level analysis (e.g., troubleshooting authentication issues).
- Monitor Mode: Used for site surveys, detecting interference, or finding rogue APs without disrupting the network.

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

The best AP mode in this case is FlexConnect Mode (also known as HREAP).

- In FlexConnect, the AP can switch client traffic locally, even though it is controlled by a WLC over the WAN.
- If the WAN link to the WLC is up, the AP behaves normally—clients authenticate via the WLC, and policies are applied.
- If the WAN link goes down, the AP enters standalone mode:
    - Clients stay connected
    - Local switching continues
    - Cached credentials (for pre-authenticated users) are used

Ideal For:

- Remote offices
- Branch locations
- Any site where the WLC is not local

So, FlexConnect Mode ensures reliable local connectivity even when the WLC is far away or temporarily unreachable.

8. What are challenges if deploying autonomous APs (more than 50) in large network like university
    - No Centralized Management:
        - Each AP needs to be configured and managed individually.
        - Time-consuming and prone to inconsistent settings across APs.
    - Difficult Firmware Updates:
        - Updates must be applied manually on each AP.
        - Increases operational effort and risk of missed updates.
    - Poor Roaming Experience:
        - Clients may face disruptions or delays when moving between APs.
        - No centralized roaming coordination like in controller-based setups.
    - Channel and Power Conflicts:
        - Without central control, APs may cause interference by using overlapping channels.
        - Manual tuning is complex in large environments.
    - Security Management:
        - Applying uniform security policies (like WPA3 or 802.1X) is harder.
        - Increases risk of misconfiguration or security gaps.
    - Troubleshooting is Complex:
        - No central visibility into the network.
        - Issues like client drops, interference, or AP failures are harder to detect and resolve.
    - Scalability Issues:
        - Managing 50+ APs without automation or central tools is not scalable.
        - Difficult to expand as user demand grows.
    - Higher Operational Cost:
        - Requires more IT staff effort to maintain and monitor the network.

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

   In local mode, a lightweight AP relies heavily on the Wireless LAN Controller (WLC) for operation. If the WLC goes down, here's what happens:

   **Immediate Effects:**

   - New Clients Cannot Join:
     - AP cannot authenticate or associate new clients.
     - Because all client management is handled by the WLC.
   - Existing Clients Get Disconnected:
     - Lightweight APs in local mode cannot operate independently.
     - Without the WLC, the CAPWAP tunnel drops, and AP stops broadcasting SSIDs.
   - No Data Forwarding:
     - Even if a client is still connected briefly, data traffic cannot be forwarded properly.
     - Because the data plane is also controlled via the WLC.