WIFI - Module 2 – Assignment:

Q1. Brief about Split MAC Architecture and how it improves the APs Performance:

SplitMAC Architecture:

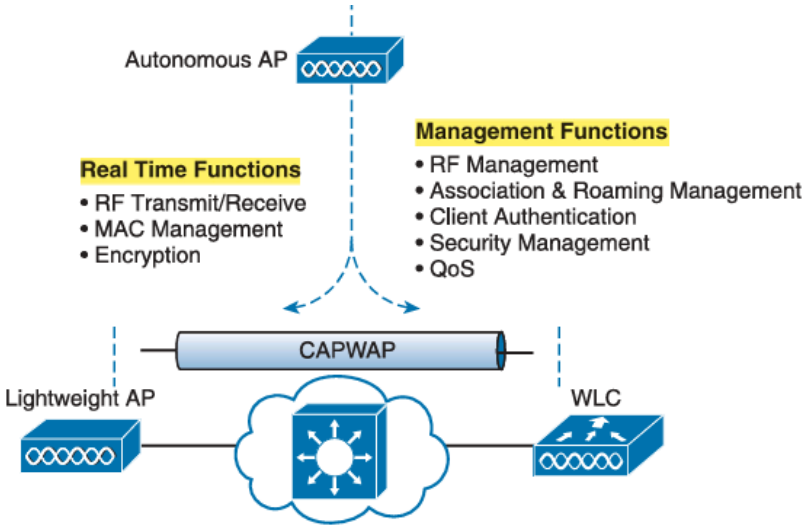
SplitMAC is a wireless networking architecture that divides the functionality of the MAC (Medium Access Control) layer between two entities:

- Access Points (APs)
- Central Controller (e.g., WLAN Controller or a centralized server)

The primary goal of SplitMAC is to offload complex and resource-intensive MAC layer functionalities from the APs to a centralized controller, while keeping time-sensitive tasks at the AP itself.

How It Works:

- Local MAC Functions (handled by AP):
    - Time-critical operations such as frame acknowledgment, retransmissions, and contention resolution
    - Functions that require real-time responsiveness
- Central MAC Functions (handled by Controller):
    - Association management, authentication, roaming support
    - Load balancing, frequency/channel assignment, and traffic shaping
    - Network-wide policies and optimizations



How SplitMAC Improves AP Performance:

1. Reduces Computational Load on APs:
    - By delegating heavy, non-time-critical MAC functions to the controller, APs are freed from complex processing tasks.
2. Better Resource Utilization:
    - APs can focus on high-speed packet forwarding and RF management, leading to lower latency and higher throughput.
3. Centralized Management:
    - The controller can perform global optimizations, such as dynamic channel allocation and handover decisions, improving overall network performance.
4. Enhanced Scalability:
    - Because the intelligence is centralized, adding more APs does not significantly increase the complexity or management overhead.
5. Improved Mobility and Handoffs:
    - Seamless handovers can be managed centrally, reducing disruption when clients move across APs.

Q2. Describe about CAPWAP, explain the flow between AP & Controller:

What is CAPWAP?

CAPWAP (Control and Provisioning of Wireless Access Points) is a standardized protocol (defined in RFC 5415) that enables communication between Wireless Access Points (APs) and a centralized Wireless LAN Controller (WLC).

It was designed to simplify, secure, and standardize the control and management of APs in enterprise WLAN architectures, especially in scenarios where APs are LAP and rely on the controller for decisions and configurations.

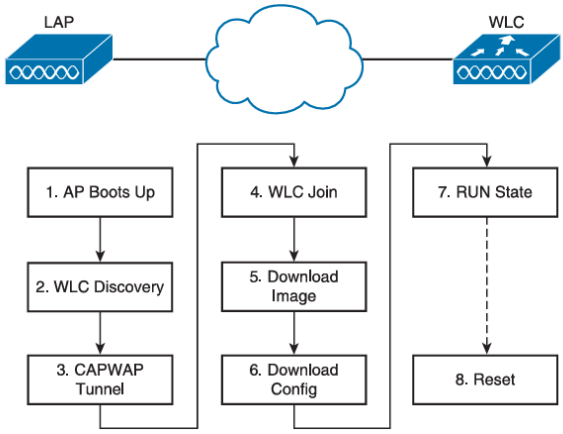
Key Features of CAPWAP:

- Tunneling Protocol: Creates a control tunnel and a data tunnel between AP and controller.
- Encapsulation: Encapsulates 802.11 wireless frames within IP/UDP for transmission over wired infrastructure.
- Security: Supports DTLS (Datagram Transport Layer Security) to secure control messages.
- Interoperability: Makes it easier to use APs and controllers from different vendors (though in practice, full interoperability still depends on vendor implementations).

CAPWAP Architecture:

There are two main tunnels established between AP and Controller:

1. Control Tunnel:
    - Uses UDP port 5246
    - Manages AP configuration, firmware updates, radio management, etc.
2. Data Tunnel:
    - Uses UDP port 5247
    - Forwards client data (optional; can be centralized or split tunneling)

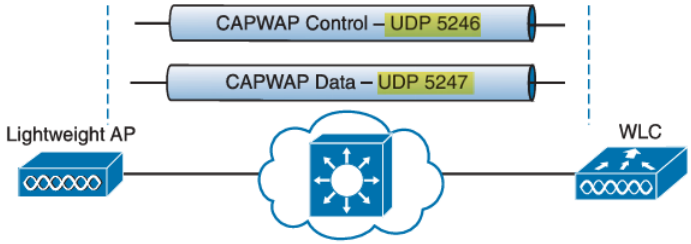


Communication Flow (Step-by-step):

1. **AP Bootup:** Sends DHCP request to get IP address.
2. **Discovery Phase:**
    - AP sends CAPWAP Discovery Request (broadcast/multicast or directed)
    - WLC responds with Discovery Response
3. **Join Phase:**
    - AP sends CAPWAP Join Request to selected WLC
    - WLC authenticates and replies with Join Response, and the CAPWAP tunnel is established.
4. **Image Download:**
    - If the AP's software version is not compatible, the WLC pushes the correct image to the AP.
5. **Configuration Phase:**
    - Once joined, the WLC pushes configuration settings (SSIDs, security policies, etc.) to the AP.
6. **Operational Phase:**
    - The AP is now operational. CAPWAP Data Tunnel carries user data from AP to WLC.

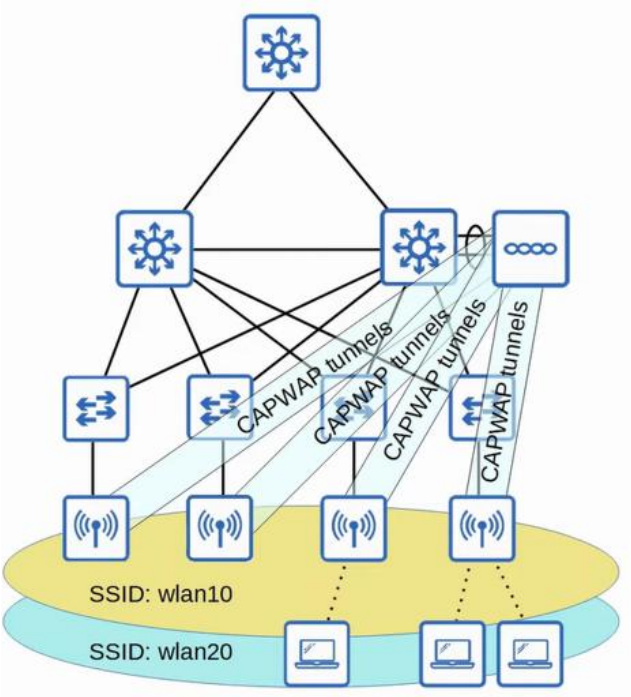
Q3. Where this CAPWAP fits in OSI model, what are the two tunnels in CAPWAP and its purpose

- CAPWAP fits at OSI Layer 3 and 4.
- CAPWAP uses IP addressing to allow communication between APs and WLCs across subnets or different networks. Thus, Layer 3 operation ensures that CAPWAP traffic can be routed over the internet, VPNs, or private WANs.
- In layer 4 because it provides UDP transport + DTLS encryption for security.
- It uses two tunnels: a. Control Tunnel (UDP port 5246): For AP-WLC communication and management. b. Data Tunnel (UDP port 5247): For forwarding client data traffic.



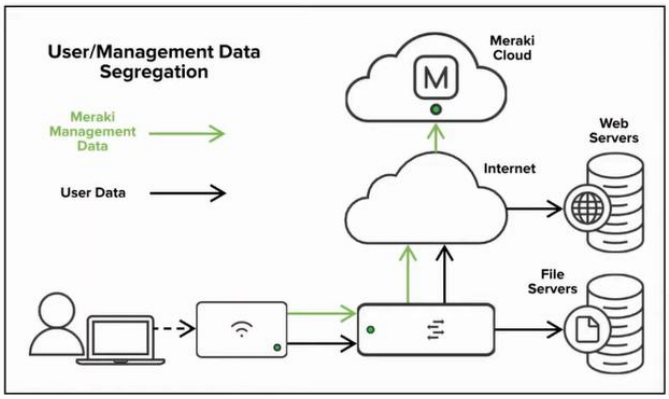
Q4. Whats the difference between Lightweight APs and Cloud-based APs

LAP :



Lightweight APs:

- Controlled by a centralized Wireless LAN Controller.
- Security, configuration, firmware updates reside in the controller. The AP just forwards data and control messages.
- Requires on-premise hardware controller for deployment.
- Highly scalable, but complex.
- Internet connectivity not required for management.
- Typically used in large enterprise environments with many APs and a need for centralized control.



Cloud-based APs:

- Managed via cloud controller (Meraki, Aruba Central, etc.)
- APs connect to and get configurations from the cloud. No on-premise controller needed.
- No need for physical controllers.
- Very scalable and simple.
- Requires internet for full functionality.
- Ideal for distributed networks or organizations with multiple remote location

Q5. How the CAPWAP Tunnel is maintained between AP and Controller

APWAP Tunnel Maintenance Mechanisms:

1. Keep-Alive Messages (Echo Requests/Responses):
    - The AP periodically sends Echo Requests to the controller.
    - The controller replies with Echo Responses.
    - This mechanism ensures the tunnel is alive and the controller is reachable.
2. Session Timeouts:
    - If Echo messages are missed beyond a certain threshold, the AP considers the controller unreachable and tears down the tunnel, restarting the discovery/join process.
3. DTLS Session Refresh:
    - The DTLS session used in the control tunnel may be periodically refreshed for security and stability.
    - Re-keying can occur based on timer or controller policy.
4. State Management:
    - Both AP and controller maintain state information about each other (e.g., configurations, client associations, QoS policies).
    - If the tunnel is disrupted, the AP may enter a "standby" or "disconnected" state, waiting to rejoin the controller.

Q6. What's the difference between Sniffer Mode and Monitor Mode, use case for each mode

Definition:

In Sniffer Mode, the Access Point (AP) functions like a wireless packet capture device. It captures 802.11 wireless frames over the air and forwards the raw packet data to a remote analyser tool (like Wireshark) for in-depth analysis.

Purpose:

Used for troubleshooting, protocol analysis, and detailed examination of wireless traffic at the MAC layer.

Operation:

- The AP captures all wireless frames on a specific channel.
- It encapsulates the raw 802.11 frames in a Remote Packet Capture (RPCAP) format.
- These frames are forwarded to a PC running Wireshark or another analyser tool.
- The AP does not serve clients or participate in WLAN operations while in sniffer mode.

Use Case:

- Deep packet inspection
- Debugging authentication and association failures
- Analyzing wireless protocol behavior
- Identifying interference, retransmissions, or rogue devices

Example:

During testing of a custom IoT device's Wi-Fi module, an engineer uses an AP in sniffer mode to capture and analyze malformed DHCP request packets that prevent proper IP assignment.

Monitor Mode:

Definition:

In Monitor Mode, the Access Point scans all channels to detect wireless security threats, rogue APs, and other wireless devices. It operates passively, without serving any clients. It is used for wireless intrusion detection, spectrum analysis, rogue AP detection, and RF monitoring.

Operation:

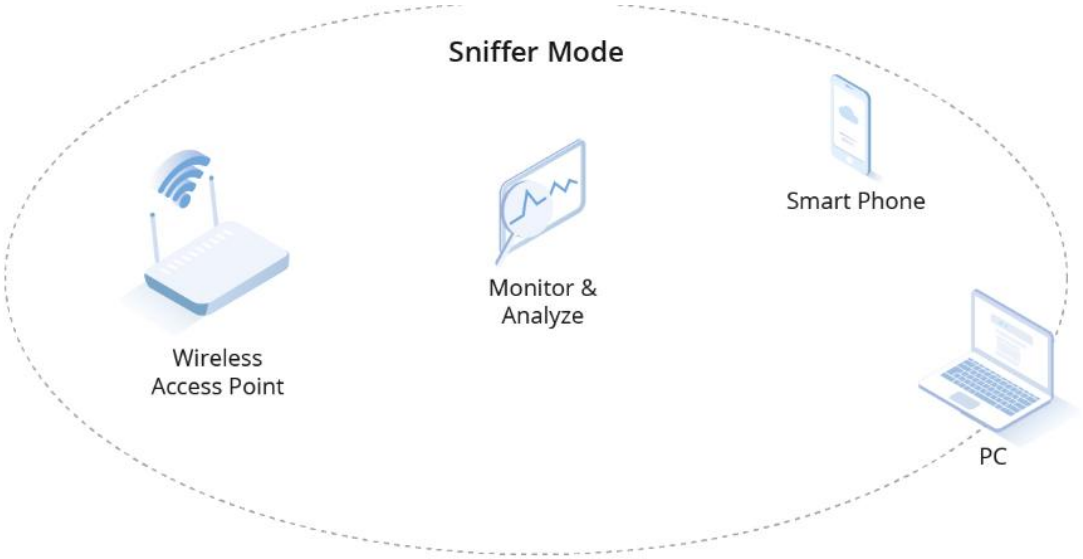
The AP constantly listens on all available channels (channel scanning). It reports Rogue APs, Unauthorized clients, RF interference sources, Signal strength levels. The data is sent to the WLC or Wireless Intrusion Prevention System (WIPS) for centralized analysis.

Use Case:

- Wireless intrusion prevention
- Identifying unauthorized access points (rogue APs)
- Monitoring channel utilization and interference
- Performing RF coverage surveys

Example:

A financial institution configures APs in monitor mode throughout its offices to detect any employee trying to set up unauthorized personal hotspots, helping enforce strict network compliance policies.



Q8. What are challenges if deploying autonomous APs (more than 50) in large network like university

- **Manual Configuration:**
  Each AP must be individually configured (SSID, security, channel, power, VLANs), leading to high administrative overhead.
- **Inconsistent Settings:**
  Errors and inconsistencies are likely across APs, causing network instability or degraded performance.
- **Lack of Central Management:**
  There's no centralized platform to monitor, update, or manage all APs.
- **No Unified Policy Enforcement:**
  Security and QoS policies must be replicated manually on every device.
- **Poor Seamless Roaming:**
  Clients roaming between APs may experience re-authentication delays, dropped connections, or IP address changes.
- **No Fast-Roaming Support (e.g., 802.11r/k/v):**
  These advanced features typically require a controller to coordinate AP behaviour.
- **Channel Interference:**
  Without centralized RF management, overlapping channels may cause interference.
- **Manual Power Adjustment:**
  Each AP's transmit power must be fine-tuned manually for optimal coverage and minimal overlap.
- **Limited Monitoring Capabilities:**
  Logs and performance data are local to each AP, making large-scale monitoring tedious.
- **Inefficient Troubleshooting:**
  Diagnosing issues across 50+ APs requires checking devices individually.

Q9. What happens on wireless client connected to Lightweight AP in local mode if WLC goes down

- **New client associations fail**: No new clients can join the WLAN because the AP can't authenticate or assign IP addresses without the WLC.
- **Ongoing client sessions drop:** Most of the time, existing client sessions are disconnected because LWAP loses the CAPWAP (Control and Provisioning of Wireless Access Points) tunnel to the WLC.WAP is not autonomous and does not have configuration logic to continue operation independently.
- **No roaming support:** Seamless Layer 2/3 roaming also stops since it's centrally managed by the WLC.

Q7. If WLC deployed in WAN, which AP mode is best for local network and how?

- If the WLC is deployed over a WAN, the best AP mode to use for the local network is FlexConnect Mode.
- FlexConnect allows an AP to maintain local switching and limited autonomy even when the WLC is located remotely.

Local switching:

- The AP can switch client traffic locally, directly into the local VLAN, instead of tunneling it back to the WLC over the WAN.
- This greatly reduces WAN bandwidth usage, especially for data-heavy applications.

Continuous operation:

- If the WAN connection to the WLC fails, the AP can continue to maintain wireless service for clients.
- This is called " FlexConnect standalone operation".

Centralised anagement:

- While data stays local, control and configuration are still managed centrally through the WLC.
- This provides a balance of central control and local efficiency.