WIFI TRANING MODULE 2 ASSESSMENT SOLUTION

-BY SAKTHI KUMAR S

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

SplitMAC is a design approach used in wireless networks, particularly in controller-based (Lightweight) architectures, where the Media Access Control (MAC) layer functions are split between the Access Point (AP) and the Wireless LAN Controller (WLC).

SplitMAC Working:

- The MAC layer functions are divided into two parts:
    - Time-critical, real-time functions (e.g., RF modulation/demodulation, encryption, MAC retransmissions, acknowledgments, Frame transmission/reception, Beaconing and probing, RTS/CTS (collision avoidance), OFDMA and MU-MIMO operations, Physical carrier sensing and immediate power management, Encryption/decryption of data frames) are handled by the AP.
    - Management and control functions (e.g., client authentication, association, mobility management, and policy enforcement, Load balancing and bandwidth allocation, RF management: channel selection and transmit power control, QoS and traffic shaping, Interference mitigation and spectrum analysis) are handled by the WLC.
    - The communication interface enables co-ordination between AP and WLC by Control messages (e.g., configs, firmware updates), Status reports (e.g., AP load, client info), Performance stats for optimization, Data tunnelling when needed

How SplitMAC Improves AP Performance:

1. Reduces AP Complexity & Cost: Since APs offload complex management tasks to the WLC, they can be simpler and more cost-effective.
2. Improves Scalability: Centralized control allows easy management of hundreds or thousands of APs from one WLC.
3. Enhances Mobility & Roaming: WLC can manage seamless Layer 2 and Layer 3 roaming, enabling better user experience.
4. Better Resource Utilization: AP focuses on real-time transmission tasks, which improves radio performance and reduces latency.
5. Centralized Policy Enforcement & Security: WLC enforces access control, QoS, and security uniformly across all connected APs.

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

CAPWAP: Control And Provisioning of Wireless Access Points

CAPWAP (Control and Provisioning of Wireless Access Points) is a standardized protocol (RFC 5415) designed to manage Lightweight Access Points (APs) through a centralized Wireless LAN Controller (WLC). It supports the SplitMAC architecture, allowing APs to handle time-sensitive tasks while the controller manages configuration, authentication, and policies.

Key Features:

- Standardized communication between APs and controllers
- Secure control channel using DTLS
- Encapsulation of control and optional data traffic
- Operates over UDP ports 5246 (control) and 5247 (data)

CAPWAP Flow Between AP and Controller:

- AP Boot and Discovery: AP obtains IP via DHCP and discovers the WLC using DHCP Option 43, DNS, or static configuration.
- DTLS Tunnel Establishment: A secure DTLS control tunnel is established for management traffic.
- Join Phase: AP sends a Join Request, and the WLC replies with a Join Response if validated.
- Configuration Phase: WLC pushes configuration parameters (SSID, security, radio settings) to the AP.
- Run Phase (Keep-Alive): The AP enters the run state APs regularly report status (e.g., client info, RF metrics) to the WLC, which updates configurations as needed and sends keep-alive messages to the WLC at regular intervals to maintain the session.
- Data Tunnelling: Client traffic will be encapsulated and tunnelled to the WLC for processing.
- Failover and Rejoin: If the WLC becomes unreachable (keep-alive fails), the AP enters failover mode, searches for backup controllers, and initiates a rejoin process.

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

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

- Layer 3 – Network Layer:
  - CAPWAP uses IP for addressing and routing between APs and the controller.
- Layer 4 – Transport Layer:
  - It uses UDP for both control and data communication.
  - UDP Port 5246 for control messages
  - UDP Port 5247 for data encapsulation (optional)

Though CAPWAP affects MAC-layer functionality, it does so through control mechanisms implemented at these higher layers, not directly at Layer 2.

CAPWAP creates two separate tunnels between the AP and the WLC

1. Control Tunnel: Management Traffic
   - Purpose: Transports management and configuration messages.
   - Secured via: DTLS (Datagram Transport Layer Security)
   - Port: UDP 5246
   - Use Case: AP join, configuration, monitoring, and keep-alive.
2. Data Tunnel: Client traffic (used if centralized data forwarding is enabled)
   - Purpose: Carries encapsulated client data from the AP to the controller.
   - Port: UDP 5247
   - Use Case: When centralized switching/ Data forwarding is used (e.g., for enforcing security or QoS policies, centralized Data processing at the controller).

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

Lightweight Access Points

- Controller Location: Requires an on-premises Wireless LAN Controller (WLC) to function.
- Functionality: The AP handles only basic wireless tasks; all configurations, policies, and updates come from the WLC.
- Ideal For: Best suited for centralized deployments like campuses, offices, and large buildings.
- Dependency: If the controller fails, the APs lose most of their functionality (except in some modes like FlexConnect).
- Scalability: Adding more APs needs careful planning, as the controller must support the increased load.
- Management Interface: Managed and monitored locally through the WLC.

Cloud-Based Access Points

- Controller Location: No physical controller needed – fully managed via a cloud-based dashboard.
- Functionality: APs self-configure after connecting to the internet by pulling settings from the cloud.
- Ideal For: Perfect for distributed or remote environments (e.g., branch offices, retail chains).
- Automation: Firmware updates, monitoring, and configurations happen automatically through the cloud interface.
- Scalability: Easily scalable – just plug in new APs and they auto-register with the cloud.
- Maintenance: Reduces on-site IT workload with centralized, remote management.

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

CAPWAP uses two tunnels (Control and Data) over UDP to maintain communication between the AP and the controller.

Tunnel Establishment

- After booting, the AP discovers the controller (via DHCP Option 43, DNS, or static IP).
- It then initiates a DTLS-encrypted Control Tunnel over UDP port 5246 for secure management communication.
- If centralized switching is used, a Data Tunnel is also created over UDP port 5247 for client traffic encapsulation.

1. Control Tunnel Maintenance

- Keep-Alive Messages / Heart-Beat Messages: The AP sends keep-alive messages (echo requests) to the controller at regular intervals.
- Echo Response: The controller replies with echo responses, confirming the tunnel is alive.
- Session Timeout Handling: If the AP misses multiple echo responses (typically 3–5), it assumes the controller is unreachable and initiates failover or rejoin procedures.
- Re-Keying and Revalidation: Periodically, the DTLS session may be re-keyed to maintain secure encryption over time.

2. Data Tunnel

- If centralized data forwarding is configured, client data is encapsulated and forwarded through the data tunnel.
- This tunnel remains active as long as the control tunnel is healthy.
- Tunnels are built over UDP (ports 5246 and 5247).

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

Sniffer Mode

- In Sniffer Mode, the Access Point (AP) or wireless adapter captures wireless frames and forwards them to analysis tools like Wireshark for protocol-level inspection.
- It focuses on a specific channel and Service Set Identifier (SSID), making it useful for targeted packet analysis.
- The AP remains associated with any client or AP for transmitting purposes but can monitor the communication between specific clients and APs.
- It is mainly used in enterprise environments with centralized wireless LAN controllers (WLCs), allowing real-time troubleshooting without affecting the live network.
- This mode allows network administrators to analyse packet flow, validate QoS policies, assess voice/video quality, and debug specific client connectivity problems.

Use Cases:

Troubleshooting client roaming and session drops, Analysing VoIP or application performance, Capturing WPA/WPA2 handshake packets, Validating security and firewall rules, Forensic packet capture for network investigations

Monitor Mode

- In Monitor Mode, the device passively listens to all wireless frames across a channel or multiple channels without associating to any SSID or transmitting data.
- It captures broadcast and unicast frames from all surrounding wireless networks.
- This mode is ideal for wireless network analysis, especially when assessing interference, rogue devices, or signal coverage.
- It provides a comprehensive view of the wireless environment, making it useful for security assessments and wireless site surveys.

Use Cases:

Detecting rogue access points or unauthorized devices, RF interference analysis, Capturing hidden SSIDs, Performing wireless site surveys and coverage mapping, Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS) monitoring

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

If the Wireless LAN Controller (WLC) is deployed over the WAN (Wide Area Network), the best AP mode for ensuring local network reliability and efficiency is the FlexConnect Mode (previously known as H-REAP).

FlexConnect Mode: Best for Remote Sites with WAN-Hosted WLC

- FlexConnect allows Access Points (APs) to continue functioning locally even if the WLC over the WAN becomes unreachable.
- It enables local switching of client traffic directly onto the LAN instead of tunneling it back to the controller over the WAN.
- It reduces WAN bandwidth usage and ensures network continuity during WAN failures.

Key Features of FlexConnect Mode:

- Local Switching: Data traffic from wireless clients is switched locally at the AP, without traversing the WAN to reach the controller.
- Greatly reduces WAN load, improving performance for local resources (e.g., printers, servers).
- Centralized Management: Control and configuration still come from the WLC when it is reachable. APs receive policies, SSID settings, and security configurations from the controller.
- Standalone Operation During WAN Outage: In the event of a WAN failure, APs continue to support clients using pre-downloaded configurations.
- Enables critical services like authentication (with local RADIUS or caching), DHCP, and VLAN tagging to continue.

Use Case Scenarios: Ideal for branch offices, retail stores, and remote sites where WLC is centrally located in a data center or HQ.

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

Deploying a large number of autonomous (standalone) access points in a high-density environment like a university comes with several operational, performance, and management challenges:

1. Complex Configuration and Management

- Each AP must be manually configured and managed individually.
- Any change in SSID, security, or QoS policies must be applied separately to each AP.
- This is time-consuming and error-prone, especially during updates or troubleshooting.

2. Lack of Centralized Control

- No centralized platform to monitor AP status, client activity, or network health.
- Makes it difficult to manage client roaming, load balancing, or detect issues quickly.
- Troubleshooting and diagnostics must be done per device, increasing administrative overhead.

3. Inconsistent Policy Enforcement

- Security policies, access control, and QoS settings may be inconsistently applied across APs.
- Increases the risk of configuration mismatches, network instability, and potential security vulnerabilities.

4. Poor Mobility and Roaming Support

- Without a controller to coordinate roaming, clients may experience connection drops or latency while moving between APs.
- No seamless Layer 2 or Layer 3 roaming, which affects user experience in applications like VoIP or video streaming.

5. Inefficient RF Management

- Autonomous APs cannot perform coordinated RF optimization, such as dynamic channel assignment or transmit power adjustments.
- Leads to channel overlap, interference, and reduced network performance in dense deployments.

In large-scale environments like universities, managing over 50 autonomous APs becomes highly inefficient and unsustainable. A controller-based (Lightweight) or cloud-managed solution is preferred for centralized control, scalability, and better performance.

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

When a Lightweight Access Point (LAP) is operating in Local Mode, it heavily depends on the Wireless LAN Controller (WLC) for management and control functions. If the WLC becomes unreachable or goes down, the following happens:

1. Existing Client Sessions Stay Temporarily Active

- Clients already connected to the AP may continue communication for a short period (typically up to 30–60 seconds) depending on the AP-WLC heartbeat/keepalive timer.
- After this timeout, the AP recognizes the WLC as unreachable and terminates client sessions.

2. No New Client Associations

- New wireless clients cannot join the network because the AP needs the controller to authenticate and authorize new associations.
- Essential management functions like DHCP relay, AAA authentication, and policy enforcement are handled by the WLC and will fail.

3. Data Forwarding Stops

- Since Local Mode APs tunnel all traffic to the WLC, the loss of the controller means data traffic cannot be processed or forwarded.
- Clients will lose access to LAN or internet services.

4. AP Goes into Discovery Mode

- The AP attempts to re-discover and rejoin a WLC.
- If a backup WLC is available (with proper High Availability or mobility group settings), the AP can fail over and restore service.

In Local Mode, APs are highly dependent on the WLC. If the controller fails and there's no backup, wireless service will be disrupted. For better resilience, FlexConnect mode is preferred in remote or WAN-connected deployments.