WiFi Assessment 2 - Module 2

Name	T K Gowtham
Email ID	gowthamkamalasekar@gmail.com
College	VIT Chennai

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

- SplitMAC architecture is a wireless architecture used in LWAP (Lightweight Wireless Access Point) to divide the functionality of Access Point with AP and the WLC (Wireless LAN Controller).
- The AP functions are divided into Management functions and real time functions.
- Management functions are handled by WLC and Real time functions are handled by AP.
- Management functions consist of functions like client authentication, security management, Roaming (association and reassociation), QoS.
- Real time functions consist of functions like transmission of 802.11 frames, MAC management and encryption.
- The WLC binds with one or more LWAPs and communicates to it through CAPWAP tunnels.
- The splitMAC improves the performance by
    - Reducing AP load : AP needs only to handle real time functions and the rest can be handled by WLC.
    - Centralized control : WLC controls all the other APs, so better traffic handling, security and policy management.
    - Seamless roaming : WLC takes care of client authentication, so clients can roam between multiple APs without any hiccups.
    - Improved security : Encrypted data is sent and received through CAPWAP tunnel.
    - Efficient resource utilization : AP becomes lightweight, reduces hardware complexity and cost.

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

- Control and Provisioning of Wireless Access Point is a tunneling and management Protocol that allows centralized control of WAP via WLC.
- Helps in managing, configuring and securing the WAPs.
- It enables LWAPs by offloading the management tasks to a central WLC.
- Supports secure communication via DTLS (Datagram Transport Layer security).
- Flow between AP and Controller :
    - AP discovery and Join : AP looks for WLC using DHCP, DNS or Static IP and sends discovery requests to available controllers, WLC responds with Discovery Response.
    - AP authentication and association : AP sends a Join request to WLC and WLC validates the AP and sends a Join response. The AP is now associated with WLC.
    - WLC pushes AP configuration such as SSID, VLAN and security policies, AP applies the settings and starts broadcasting the wireless network.
    - Established the CAPWAP tunnel between WLC and AP.
    - Clients are associated with AP and data from clients are encapsulated in CAPWAP and sent to WLC which processes and routes the packets as per the network policies.
    - WLC will then continuously monitor AP, apply updates and manage roaming. If a client moves between APs, WLC ensures seamless handover.

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

- CAPWAP operates at Layer 2 and 3 (Data link and Network layer) of the OSI model.
- Layer 2 : The AP and WLC must be in the same subnet
- Layer 3 : The AP and WLC can be in different subnets, making it suitable for large networks.
- CAPWAP established two UDP based tunnels between the AP and WLC and they are :
    - Control Tunnel :
        - UDP port 5246
        - Used for management functions communication
        - Handles AP authentication, configuration, firmware updates and control messages.
        - Uses DTLS encryption.
    - Data Tunnel :
        - UDP port 5247
        - Used for client data traffic.
        - Encapsulates and forwards user traffic from AP to WLC.
        - Encryption and decryption based on network configuration.
- The tunnels help centralize wireless network management.

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

Lightweight AP	Cloud Based AP
Managed by WLC controller	Managed centrally by a cloud based controller.
Uses splitMAC architecture, Lower MAC function handled by AP, Upper MAC function by WLC.	Hybrid of autonomous and lightweight AP.
Control and data traffic pass through the controller using CAPWAP tunnels.	Data plane traffic is not sent to the cloud.
Used in large scale uniform network deployment where cost is reduced by centralizing intelligence into the controller.	Used in distributed enterprises with multiple smaller sites worldwide.
WLC controller handles QoS, traffic and security.	Cloud controller configures APs and collects metrics for analytics.
Uses CAPWAP for communication between AP and WLC	Uses cloud API to manage and communicate with AP remotely.

- Lightweight AP rely on WLC controllers making them efficient for large and uniform deployment.
- Cloud based AP provides flexibility for distributed networks without sending data traffic to the cloud, making them more scalable for organizations with multiple sites.

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

- CAPWAP establishes and maintains a secure communication tunnel between AP and WLC.
- AP Discover and connection : As AP boots up, it discovers the WLC using DHCP or DNS.
- CAPWAP establishes tunnels such as Control tunnel/Management tunnel and Data tunnel.
- AP and WLC exchange heartbeat (keep-alive) messages periodically to maintain the tunnel, which is called keep-alive mechanism.
- If the WLC does not receive a response from an AP within a certain time, it marks the AP as disconnected and initiates recovery.
- If the tunnel breaks due to network issues, AP will automatically try to reconnect to the same WLC or a backup controller.
- Some networks use redundant WLC for High availability where AP failover to a secondary controller if the primary WLC goes down.

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

Sniffer Mode	Monitor Mode
Does not provide BSS. Only acts as passive packet capture device	Does not provide BSS but remains active in monitoring the wireless environment.
Captures packets and forwards them to the controller for processing	Continuously monitors the air to detect rogue devices and collect telemetry data.
Packet analysis for troubleshooting and debugging	Wireless security, rogue AP detection, and analytics.
Captures packets over the air and sends them to the WLC or a monitoring system.	Collects various wireless metrics and sends analytics to the WLC.
Use case : for network troubleshooting, packet analysis and performance monitoring.	Use case : for security monitoring, detecting rogue APs, and wireless analytics.

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

- When a WLC is deployed in WAN, the best AP mode for the local network is FlexConnect Mode.
- FlexConnect mode allows APs to operate even if the connection to the WLC is lost. It provides the best balance of local traffic handling and central management.
- Local Switching : If the WAN link to the WLC fails, the AP can continue forwarding local traffic without interruption. The AP will use cached authentication credentials to authenticate new users.
- Centralized Control : When the WAN link is up, the AP communicates with the WLC for configuration updates, policy enforcement and monitoring.
- Seamless Failover : Even if the WAN link goes down, clients remain connected to the local network and once the WAN connection is restored, the AP re-estabilishes communication with the WLC.
- Hence, it reduces WAN dependency, ensures high availability, supports local authentication and optimizes performances.

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

Autonomous APs operate independently without a central controller, making them difficult to manage in large-scale deployment like university. The challenges are :

- Lack of centralized management → Each AP requires manual setup, updates and configuration.
- Increased interference and channel management issues → No auto-channel selection, leading to co-channel interference.
- Difficult roaming and handover → No fast roaming support, causing disconnects during movements.
- Security and authentication challenges → Hard to manage security policies and implement AAA authentication.
- Inefficient load balancing → APs don't share client loads, causing overloading issues.
- High maintenance effort → Troubleshooting and updates must be done per AP manually.
- Scalability issues → Adding APs increases interference and manual effort.

A lightweight AP with WLC is a much better approach for large networks. It offers :

- Centralized management of all APs
- Seamless roaming between APs
- Better security and authentication
- Automatic channel and power management to reduce interference.
- Easier troubleshooting and monitoring through a centralized dashboard.

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

If a WLC goes down while a wireless client is connected to LAP in local mode :

- Existing clients stay connect
- No new client connections are created since authentication is handled by WLC.
- No roaming between APs as roaming decisions are managed by WLC.
- Features like QoS, ACLs, and advanced security policies may not work properly.
- If the WLC was handling traffic, APs might lose connectivity to the wired network.
- Failsafe mode → some APs support Mobility Express or FlexConnect Mode, allowing them to continue limited operation even without the WLC.
- For full redundancy, secondary WLC or flexConnect mode should be used.