Name: Afreen S

University: Vellore Institute of Technology (VIT)

WiFi Training Program

Assignment – Module 2

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

Light Weight Aps use Split MAC architecture where the lower MAC functions are done by the AP and the upper MAC functions are moved and centralized into the controller. Aps perform functions such as client association, sending out beacons/probes, encrypting data, sounding, MU-MIMO/OFDMA, aggregation, ACKS, etc. Functions such as RRM, QoS management, Load balancing, traffic shaping/policing, mobility, authentication/security, etc.. are handled by controller.

Split MAC architecture offloads high-level processing tasks from the AP to the controller, reducing AP workload, improving network efficiency, and enhancing scalability. By handling real-time packet transmission at the AP and centralizing control functions, this approach leads to better performance, improved security, and optimized resource utilization in large-scale wireless networks.

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

CAPWAP (Control and Provisioning of Wireless Access Points) is a standardized protocol defined in **RFC 5415** that enables communication between a **lightweight access point (AP)** and a **wireless LAN controller (WLC)**. It is designed to **centrally manage APs**, providing configuration, firmware updates, security, and tunneling of user data.

Flow:

(Client) → (AP) → [CAPWAP Data Tunnel] → (Controller) → (LAN/Internet)

Control Messages (Encrypted with DTLS)

- AP → Controller: Discovery Request, Join Request, Heartbeats
- Controller → AP: Configuration, Firmware Updates, Policy Push

Client Data Traffic

- CAPWAP encapsulates client traffic between AP and controller over **UDP 5247**
- The controller can either **route the traffic or bridge it locally at the AP** (depending on CAPWAP mode)

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

CAPWAP operates at **Layer 2 (Data Link) and Layer 3 (Network)** of the OSI model.

- It encapsulates **wireless frames** for transport over an **IP network**.
- Works over **UDP** (ports 5246 for control and 5247 for data).
- **Control Tunnel (UDP 5246, Encrypted)**
  - Handles **AP management, authentication, configuration, and firmware updates**.
  - Uses **DTLS encryption** to ensure secure communication.
- **Data Tunnel (UDP 5247, Optional Encryption)**
  - Encapsulates and forwards **client traffic** between AP and controller.
  - Can be **tunneled to the controller** or **locally switched at the AP** based on configuration.

CAPWAP ensures **centralized AP management** while maintaining efficient data forwarding and security.

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

Feature	Lightweight APs	Cloud-Based APs
Management	Controlled by an on-premises Wireless LAN Controller (WLC)	Managed through a cloud-based dashboard
Control Plane	Uses CAPWAP for communication with the WLC	Cloud controller manages APs via HTTPS/API
Deployment Model	Requires a local controller for AP operation	No on-site controller needed, managed over the internet
Scalability	Limited to the number of APs a WLC can handle	Easily scalable with cloud-based subscription models
Data Plane	Data can be tunneled to the WLC or locally switched	Data is typically locally switched at the AP
Configuration Updates	Applied via the WLC	Pushed from the cloud automatically
Redundancy	Requires backup WLCs for failover	Cloud controllers are highly available
Ideal Use Case	Large enterprises with strict security policies and local network control	Distributed offices, retail stores, and organizations needing remote AP management

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

Discovery Phase

- AP discovers the controller using **DHCP, DNS, or static configuration**.
- Sends a **CAPWAP Discovery Request**, and the controller responds with a **Discovery Reply**.

Secure DTLS Handshake (For Control Tunnel)

- The AP and controller establish a **DTLS-encrypted Control Tunnel (UDP 5246)**.
- Ensures **secure transmission** of control messages.

AP Joins the Controller

- AP sends a **CAPWAP Join Request**.
- Controller validates and responds with a **CAPWAP Join Reply**.

Configuration & Policy Updates

- Controller sends AP configurations (SSID, QoS, VLAN, Security settings).
- AP applies settings and begins **client data handling**.

Heartbeat Messages (Keepalive Mechanism)

- AP periodically sends **CAPWAP Echo Requests** to the controller.
- If the controller responds with **Echo Replies**, the tunnel remains active.
- If no response is received, the AP attempts to **failover to another controller**.

Data Tunnel for Client Traffic

- A separate **Data Tunnel (UDP 5247)** is used for forwarding user traffic.
- It remains open as long as the **AP is active and authenticated**.

Rekeying & Session Maintenance

- If encryption is enabled, periodic **DTLS rekeying** ensures security.
- Controller monitors AP **health, load, and performance** to maintain stability.

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

Feature	Sniffer Mode	Monitor Mode
Definition	Captures **wireless traffic** and forwards it to a remote device (e.g., Wireshark on a PC) for analysis.	Passively listens to all Wi-Fi frames on a channel without associating with any network.
Association with AP	Requires a controller/AP to forward packets to an external analyzer.	Does not associate with any AP or transmit frames.
Traffic Visibility	Captures only **802.11 frames** for a specific SSID or AP.	Captures **all wireless frames** (management, control, and data) on a selected channel.
Encryption Handling	Cannot decrypt encrypted packets unless provided with keys.	Captures raw encrypted traffic; decryption depends on external tools.
Use Case	- Troubleshooting connectivity issues. - Analyzing specific AP-client interactions. - Used with **Wireshark** or Cisco WLCs.	- **Wireless security analysis** (e.g., detecting rogue APs, attacks). - **Site surveys** to analyze Wi-Fi coverage/interference. - Used in **penetration testing** tools like Aircrack-ng.

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

When a **Wireless LAN Controller (WLC)** is located across a **WAN**, the best AP mode for the local network is:

❖ **FlexConnect Mode (Cisco) / Local Switching Mode (Other Vendors)**

How FlexConnect Works:

1. **Local Authentication & Switching:**
    - AP **authenticates clients locally** without relying on the WLC.
    - Client data traffic is **switched locally** at the AP instead of tunneling it back to the controller.
2. **WAN Failover Handling:**
    - If the WAN link to the controller **fails**, APs continue operating in **standalone mode**.
    - Clients can still connect, authenticate (if pre-configured), and access local network resources.

3. **Control & Management via CAPWAP:**
    - APs establish a **CAPWAP control tunnel** with the remote WLC for centralized management.
    - Configuration updates and monitoring are still performed by the controller over WAN.

Why FlexConnect is Best for WAN-Connected WLCs?

✓ **Reduces WAN bandwidth usage** by locally switching traffic.
✓ **Ensures continued network operation** even if WAN connectivity is lost.
✓ **Optimized for branch offices and remote locations** with a central controller.

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

❖ **Lack of Centralized Management**

- Each AP operates independently, requiring **manual configuration and monitoring**.
- Difficult to apply **consistent security, SSIDs, and policies** across APs.

❖ **Complex Roaming & Mobility**

- Clients may experience **delays or disconnections** while roaming between APs.
- No seamless **802.11r fast roaming** or **CAPWAP-based handoff**.

❖ **RF Interference & Channel Management**

- Without centralized **Radio Resource Management (RRM)**, APs may cause **channel overlap** and **co-channel interference**.
- **Manual RF tuning** is needed, which is inefficient for large deployments.

❖ **Increased Network Congestion**

- No load balancing; some APs may be **overloaded** while others remain underutilized.
- High-density areas (e.g., lecture halls) may experience **performance degradation**.

❖ **Security & Policy Enforcement**

- Requires **manual updates** for security patches, VLANs, and authentication settings.
- No centralized **802.1X, firewall rules, or ACL enforcement**.

❖ **Troubleshooting & Monitoring Difficulties**

- No **centralized logging** for AP status, client connections, or failures.
- Diagnosing connectivity issues requires **manual checks on each AP**.

❖ **Scalability Issues**

- Adding new APs requires **individual setup**.

- Expanding the network becomes time-consuming and **resource-intensive**.

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

Existing Clients Get Disconnected

- All **connected clients are dropped** since the AP relies on the WLC for handling authentication, policy enforcement, and traffic forwarding.

New Client Connections Fail

- The AP stops broadcasting SSIDs because it cannot authenticate new clients without the WLC.

AP Reboots or Goes Into "Discovery Mode"

- The AP continuously **searches for an available WLC** via **DHCP, DNS, or static configuration**.
- If it finds a backup WLC, it **joins the new controller** and resumes operation.

No Local Switching (Unlike FlexConnect Mode)

- In Local Mode, **all client traffic is tunneled to the WLC** using CAPWAP.
- Since the WLC is down, the AP **cannot process or switch traffic**.