Vivek Narayanan D
COIMBATORE INSTITUTE OF TECHNOLOGY

MODULE 2 ASSESSMENT

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

SplitMAC (Split Media Access Control) is an advanced wireless network architecture that improves Access Point (AP) performance by intelligently distributing MAC layer functions between a centralized controller and the APs themselves. Unlike traditional architectures—where APs either handle all MAC functions independently (autonomous APs) or rely entirely on a central controller—SplitMAC strikes a balance, optimizing efficiency, scalability, and latency.

SplitMAC enhances AP performance in several ways:

1. Reduced Latency – By keeping time-sensitive operations (like ACKs) local, SplitMAC minimizes delays compared to fully centralized systems where every frame must traverse a controller.
2. Better Scalability – Centralized control allows for coordinated RF management and load balancing across hundreds of APs without overburdening individual devices.
3. Improved Reliability – Localized data handling ensures uninterrupted operation even if the controller connection is temporarily lost.
4. Efficient Roaming – The controller manages seamless handoffs between APs, reducing packet loss during client transitions.
5. Optimized Resource Usage – APs avoid unnecessary processing, improving throughput and power efficiency.

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

The Control and Provisioning of Wireless Access Points (CAPWAP) is a network protocol that facilitates communication between Wireless Access Points (APs) and a centralized Wireless LAN Controller (WLC). It standardizes the management and provisioning of APs, allowing network administrators to centrally control wireless networks without manual configuration of each AP. CAPWAP plays a crucial role in large-scale wireless deployments by enabling APs to operate in a lightweight mode, meaning they delegate most control and

processing tasks to the WLC. This architecture helps reduce management complexity, enhances security, and ensures efficient utilization of network resources.

Flow Between AP and Controller

The communication between the AP and WLC using CAPWAP follows a structured sequence of events:

1. Discovery Phase

Before an AP can communicate with a WLC, it needs to discover one. This is done using one of the following methods like Broadcast or Multicast, DHCP Option 43, DNS Resolution, Static Configuration.

Once the WLC receives a discovery request, it responds with a discovery reply, listing its capabilities and current load to help the AP make a selection.

2. Join Phase

After discovering a suitable WLC, the AP sends a **CAPWAP Join Request** to establish a connection. The WLC validates the AP and responds with a **CAPWAP Join Response**, confirming its acceptance. This phase ensures that only authorized APs can connect to the network.

3. Configuration Phase

Once the AP joins, the WLC pushes necessary configurations, including:

- SSIDs and VLAN mappings
- Security settings (encryption, authentication)
- RF (Radio Frequency) parameters such as transmit power and channel settings
- QoS (Quality of Service) policies

The AP also downloads any required firmware updates during this phase.

4. Tunnel Establishment

CAPWAP establishes two tunnels between the AP and WLC:

1. **Control Tunnel** (Encrypted using DTLS)
2. **Data Tunnel** (Optional encryption)

5. Client Data Handling

After the AP is fully configured, it starts handling wireless client traffic. Based on the **AP mode**, client data can be processed in two ways:

- **Centralized Mode**: All traffic is sent through the CAPWAP Data Tunnel to the WLC for processing.

- **FlexConnect Mode**: Traffic can be forwarded locally without needing the WLC for every packet, reducing network congestion.

6. Heartbeat and Monitoring

The AP and WLC exchange periodic **heartbeat messages** to ensure connectivity. If the AP detects that the WLC is unreachable, it can switch to standalone mode (FlexConnect) or attempt to re-establish the connection.

3. Where does CAPWAP fit in the OSI model? What are the two tunnels in CAPWAP and their purpose?

CAPWAP (Control and Provisioning of Wireless Access Points) primarily operates at Layer 3 (Network Layer) of the OSI model. It encapsulates control and data traffic over IP, allowing communication between Access Points (APs) and the Wireless LAN Controller (WLC) across different networks. CAPWAP can also function over Layer 2 in some cases, but its main implementation relies on Layer 3 for flexibility and scalability.

CAPWAP establishes two separate tunnels between the AP and WLC to manage control and data traffic efficiently:

1. Control Tunnel (Encrypted with DTLS)

- Used for exchanging management and configuration commands between the AP and WLC.
- Ensures secure transmission of settings, firmware updates, and authentication data.
- Always encrypted to prevent unauthorized access.

2. Data Tunnel (Optional Encryption)

- Carries actual client data traffic between the AP and WLC.
- Can be encrypted if security policies require it, but encryption is optional to optimize performance.
- Supports flexible forwarding, where traffic can either be sent to the WLC (centralized) or handled locally by the AP (FlexConnect mode).

By separating control and data traffic, CAPWAP enhances security, improves network efficiency, and provides better management of wireless networks.

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

Feature	Lightweight APs	Cloud-Based APs
Control Plane	On-premises controller	Cloud-based platform
Management	Controller GUI/CLI	Web dashboard, mobile app
Deployment	Large enterprises	SMBs, remote sites
Scalability	High (with controller)	Moderate (cloud limits)
Cost	Higher (CAPEX)	Subscription-based (OPEX)
Internet Dependency	Minimal (local controller)	Critical (cloud required)

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

The CAPWAP (Control and Provisioning of Wireless Access Points) tunnel is maintained between the Access Point (AP) and the Wireless LAN Controller (WLC) through a combination of heartbeat messages, encryption, and failover mechanisms. The process ensures reliable communication, security, and continuous operation of the wireless network.

1. Heartbeat Messages for Connectivity

- The AP and WLC exchange periodic heartbeat messages to confirm the connection is active.
- If the AP does not receive a response from the WLC within a specified timeout period, it attempts to reconnect.
- If multiple heartbeats are missed, the AP may failover to a backup WLC or switch to standalone mode.

2. DTLS Encryption for Secure Communication

- CAPWAP uses DTLS (Datagram Transport Layer Security) to encrypt the control tunnel, preventing unauthorized access and attacks.
- The data tunnel may also be encrypted based on security policies but is optional to optimize performance.

3. Keepalive Mechanisms and Reconnection

- If an AP detects a lost CAPWAP connection, it enters discovery mode to find a WLC again.
- The AP may use cached controller information or DHCP Option 43/DNS to reconnect.
- If the AP fails to establish a connection, it may switch to local switching mode to continue serving clients.

4. CAPWAP Failover and Redundancy

- Many networks configure multiple WLCs for redundancy. If the primary WLC fails, APs automatically switch to a backup controller.
- Load balancing mechanisms distribute APs across multiple controllers to prevent overloading.

6. What's the difference between Sniffer and Monitor mode? Use case for each mode

1) Definition

- Sniffer Mode: The AP captures wireless traffic and forwards it to a remote device for analysis.
- Monitor Mode: The AP passively scans all RF channels to detect rogue APs, interference, and network issues.

2) Traffic Handling

- Sniffer Mode: Captures and mirrors live packets to a protocol analyzer.
- Monitor Mode: Does not forward traffic but listens for Wi-Fi threats and performance issues.

3) Use Case

- Sniffer Mode: Used for packet analysis, debugging, and troubleshooting wireless network issues.
- Monitor Mode: Used for wireless intrusion detection (WIDS), rogue AP detection, and RF interference analysis.

4) Network Impact

- Sniffer Mode: Can impact network performance as it redirects traffic.
- Monitor Mode: Has no impact on client communication since it does not participate in data forwarding.

5) Deployment

- Sniffer Mode: Requires an AP to be dedicated for packet capturing.
- Monitor Mode: APs can operate in this mode alongside normal functions in some cases.

Use Cases

- Sniffer Mode: Used by network engineers for Wi-Fi packet analysis and debugging.
- Monitor Mode: Used by security teams for wireless security monitoring and interference detection.

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

FlexConnect mode is best for local networks when the WLC is deployed in a WAN. It allows APs to continue switching client traffic locally even if the WLC connection is lost. This reduces WAN bandwidth usage and ensures uninterrupted connectivity for users.

How It Works

1. Control Plane (Centralized)

- AP communicates with the WLC over CAPWAP for management, authentication, and policies.
- Roaming, RF optimization, and security are still handled by the WLC.

2. Data Plane (Locally Switched)

- Client traffic (data VLANs) is forwarded directly to the local LAN switch, bypassing the WLC.
- Avoids backhauling all traffic over the WAN, reducing latency and bandwidth usage.

3. Fallback Mode

If the WAN link fails, FlexConnect APs can:

- Continue switching traffic locally.
- Authenticate clients via cached credentials (if configured).

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

- Management Overhead: Each AP requires individual configuration and monitoring, making large-scale deployments complex.
- Roaming Issues: Clients may face connectivity drops due to the lack of seamless handoff between APs.
- Security Risks: Ensuring consistent security policies across all APs is difficult without centralized control.
- Scalability Constraints: Managing SSIDs, frequency planning, and bandwidth allocation manually becomes inefficient.
- Firmware Updates: Keeping all APs updated requires significant administrative effort.

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

1) Client Disconnection

- In Local Mode, all client traffic is tunneled to the WLC for processing.
- If the WLC goes down, the CAPWAP tunnel collapses, and APs stop forwarding traffic.

2) Loss of Authentication

- New client connections will fail since the WLC handles authentication (802.1X, PSK, etc.).
- Existing clients may stay connected for a short time but will eventually disconnect.

3) AP Becomes Unusable

- The Lightweight AP does not switch traffic locally and relies entirely on the WLC.
- Without a WLC, the AP enters a "disconnected" state and stops serving clients.

4) Possible Failover Solutions

- Redundant WLC: If another WLC is available, APs can fail over automatically.
- FlexConnect Mode: If configured, APs can switch to Standalone Mode and continue local switching.

5) Recovery Process

- Once the WLC is restored, APs will rejoin automatically, and clients must reconnect.