ASSESSMENT MODULE 2

SARAVANAN P CIT, COIMBATORE

1. Explain SplitMAC architecture and its benefits to AP performance.

SplitMAC (Split Media Access Control) is a smart wireless network design that divides MAC layer tasks between the access points (APs) and a central controller. In contrast to traditional systems where APs either function independently or entirely depend on a controller, SplitMAC creates a hybrid approach to boost efficiency, flexibility, and response time.

Benefits to AP performance:

- Lower Latency: Time-critical operations like acknowledgments are handled by the AP, reducing delays caused by sending all data to the controller.
- Improved Scalability: The controller takes over tasks like RF management and load balancing, enabling the network to scale smoothly.
- Enhanced Reliability: Even if the controller link breaks, local functions on the AP continue working.
- Seamless Roaming: The controller coordinates smooth transitions between APs, minimizing disconnections.
- Resource Optimization: Delegating tasks appropriately enhances processing efficiency and energy use.

2. What is CAPWAP and how do AP and Controller communicate through it?

CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol used to manage communication between Access Points and the Wireless LAN Controller (WLC). It simplifies large network setups by enabling centralized configuration of lightweight APs.

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:

- Control Tunnel (Encrypted using DTLS)
- 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 network

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

Feature	**Lightweight APs**	**Cloud-Based APs**
Controller	On-premises WLC	Cloud-based management
Management	WLC GUI or CLI	Web interface or app

Feature	**Lightweight APs**	**Cloud-Based APs**
Deployment	Enterprises with centralized control	Distributed environments, SMBs
Cost Model	Higher upfront (CAPEX)	Subscription-based (OPEX)
Scalability	Highly scalable with multiple WLCs	Scalable based on cloud license
Internet Need	Not required once WLC is connected	Always needs internet access

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

- Heartbeat messages: Keepalive signals are exchanged to ensure the tunnel is alive.
- DTLS Encryption: Control tunnel is encrypted using DTLS to ensure secure management.
- Reconnect logic: If heartbeat fails, AP tries to reconnect using stored WLC info or discovery methods (like DHCP option 43).
- Failover: Backup WLCs can take over in case the primary is down.
- Flexibility: FlexConnect mode allows continued operation if WLC is unreachable.

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.

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

FlexConnect mode is ideal.

- Control traffic still goes to WLC over WAN.
- **Data traffic is locally switched**, reducing WAN load.
- If WAN/WLC is down, AP can still serve clients using cached policies (Standalone mode).
- Suitable for branch offices and remote sites.

8. What are the challenges of deploying autonomous APs (more than 50) in a large network like a university**?2**

- Manual Configuration: Each AP must be individually managed.
- Lack of Central Control: Hard to enforce uniform policies.
- Poor Roaming: No coordination between APs for handoff.
- High Admin Overhead: Monitoring, updates, troubleshooting becomes labor-intensive.
- Security Risk: Inconsistent settings may lead to vulnerabilities.
- No RF Optimization: No dynamic channel or power adjustment.

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

- Clients get disconnected: No data forwarding as WLC handles it.
- AP becomes inactive: Lightweight AP can’t function without WLC.
- No new associations: Authentication fails due to WLC being offline.
- Recovery: AP tries to rejoin WLC or fallback to backup controller.
- Exception: If AP is in FlexConnect mode, it may continue local switching.