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

SplitMAC is used in Lightweight Wireless Access Point (LWAP) architecture, where the AP's functions are split between the AP and the Wireless LAN Controller (WLC).

The AP handles real-time functions (like frame transmission and encryption), and the WLC handles management functions (like authentication, QoS, and roaming decisions).

WLC takes care of control and management functions like user authentication, encryption, security policies, Qos, roaming, and IP address assignment via its built in DHCP functionality.

This separation offloads complex processing tasks from the APs, significantly reducing their computational load and allowing them to focus solely on maintaining robust wireless connectivity.

The WLC, acting as the central brain of the network, ensures efficient traffic management, secure access control, and seamless mobility such as during handovers between APs without causing service interruptions.

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

CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol used to manage communication between lightweight access points (APs) and wireless LAN controllers (WLCs).

It ensures secure data transmission and encryption while providing centralized control for wifi networks. CAPWAP encapsulates the data exchanged between APs and WLCs, separating control traffic (management and security data) from data traffic (regular data transfer).

It operates exclusively with lightweight APs, which depend on the WLC for wifi transmission and data management. When an AP powers on, it obtains an IP address via DHCP or static configuration and then searches for a WLC using DHCP options, DNS, or broadcast, upon receiving a CAPWAP discovery request, the WLC responds with a discovery response.

The AP then sends a join request, which the WLC authenticates before responding with a join response, allowing the AP to connect to the WLC. If the AP is outdated, the WLC provides updated configuration, including wifi settings, SSID, encryption, and VLAN information. Following successful connection, the AP encapsulates data into CAPWAP packets, which the WLC processes and transmits.

The AP regularly sends heartbeat messages to confirm an active connection, attempting to reconnect if the WLC connection is lost.

**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 Aps:**

|  |
| --- |
| Uses an on-premises Wireless LAN Controller (WLC) |

|  |
| --- |
|  |
| Communicates with WLC using CAPWAP | |

|  |
| --- |
|  |
| Centralized but requires local WLC hardware | |

|  |
| --- |
|  |
| More complex, needs proper WLC setup | |

|  |
| --- |
|  |
| Handled by the WLC locally | |
| | **Cloud-Based APs** | | --- |  |  | | --- | |  | | Managed via a cloud-based controller | |  |  | | --- | |  | | Uses HTTPS or proprietary protocols to cloud | |  |  | | --- | |  | | Centralized via web/cloud dashboard | |  |  | | --- | |  | | Easier, plug-and-play with internet connection | |  |  | | --- | |  | | Handled by the cloud controller | |  |  | | --- | |  | | |

|  |
| --- |
|  |

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

The Control and Provisioning of Wireless Access Points (CAPWAP) protocol is used to manage communication between wireless access points (APs) and a central controller. Maintaining the CAPWAP tunnel involves several key processes:

1. When an AP boots up, it discovers the controller using methods like DHCP option 43 or DNS. Once the AP identifies the controller, it initiates a CAPWAP tunnel by establishing a secure connection (usually using DTLS) to the controller.
2. To maintain the tunnel, the AP and controller exchange keep-alive messages at regular intervals. This ensures that both parties are still reachable and that the tunnel remains active. If either side fails to receive a keep-alive message within a specified timeout period, it may assume the other side is down and take appropriate action.
3. The CAPWAP protocol manages sessions between the AP and the controller. This includes handling session timeouts and re-establishing sessions if they are lost. The controller can also manage multiple APs, ensuring that each maintains its own session.

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

|  |
| --- |
| **Sniffer Mode** |

|  |
| --- |
|  |
| Captures wireless packets for analysis | |

|  |
| --- |
|  |
| Captures 802.11 frames without participating | |

|  |
| --- |
|  |
| Often associates with the controller (like LWAP to WLC) | |

|  |
| --- |
|  |
| Used with tools like Wireshark, AirMagnet | |

|  |
| --- |
|  |
| Captures actual data frames (headers, payload, etc.) | |

|  |
| --- |
|  |
| **Monitor Mode** | |

|  |
| --- |
|  |
| Passively monitors the RF environment | |

|  |
| --- |
|  |
| Does not transmit or associate with any SSID | |

|  |
| --- |
|  |
| No association to any AP or SSID | |

|  |
| --- |
|  |
| Used for spectrum analysis, channel monitoring | |

|  |
| --- |
|  |
| Captures RF signal characteristics, interference | |

|  |
| --- |
|  |

**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**

Interference

Configuration and management issue

Position and placement of access point

Load balancing between APS

Troubleshooting issues

High cost of maintanence

Policy enforcement and security configuration issues

Handoff handling issues

Network and VLN isolation and management issues

**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