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

SplitMAC is a wireless networking architecture where the MAC (Media Access Control) layer responsibilities are divided between two components:

1. **Access Point (AP)**
2. **Wireless LAN Controller (WLC)**

Working Of SplitMAC:

- Low-level MAC functions (like beacon generation, acknowledgment, retransmission) are handled locally at the AP.
- High-level MAC functions (like association, authentication, roaming, security policies) are handled centrally by the WLC.
- This architecture is commonly used in Lightweight Access Points that depend on a centralized controller.

SPLITMAC improves performance by:

Centralized Control: All high-level logic is offloaded to the WLC, reducing the processing burden on the AP.

Simplified Aps = Faster Deployment: APs become simpler and easier to manage, making them cost-effective and faster to deploy.

Real-Time RF Management: The controller can analyze the entire network and push optimized channel/power settings to APs.

Efficient Roaming: Client roaming decisions are centrally handled, resulting in faster and more seamless transitions between APs.

Consistent Security Enforcement: Security policies are uniformly applied via the controller, ensuring better control over the network.

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

CAPWAP (Control and Provisioning of Wireless Access Points) is a network protocol used to manage and control Access Points (APs) by a centralized Wireless LAN Controller (WLC).
It provides:

- **Tunneling** for separating control and data traffic
- **Standardized communication** between AP and WLC
- **Encryption & authentication** for secure management

1. AP Bootup
The Access Point powers on and obtains an IP address via**DHCP**.
2. WLC Discovery
AP tries to discover the controller using:

- DHCP option 43
- DNS lookup (cisco-capwap-controller.localdomain)
- Broadcast or static IP configuration

3. **CAPWAP Discovery Request/Response**
AP sends a Discovery Request to the WLC.
WLC replies with a Discovery Response.
4. **Join Process**
AP sends a Join Request to the controller.
WLC accepts with a Join Response if allowed.
5. **Image and Config Download**
If the AP's software is outdated, WLC upgrades it.
Then the AP downloads its configuration.
6. **Establish Control and Data Tunnels**
CAPWAP control and data tunnels are formed.
7. **AP is Ready**
AP starts broadcasting SSIDs and serves clients under WLC’s control.

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

CAPWAP fits at **Layer 3 (Network Layer)** and **Layer 4 (Transport Layer)** of the OSI model. It uses **UDP** as its transport protocol, specifically UDP port 5246 for control messages and 5247 for data messages. It encapsulates wireless management and data traffic within IP packets, enabling communication between Access Points (APs) and Wireless LAN Controllers (WLCs) over IP networks.

Two Tunnels in CAPWAP:

1. Control Tunnel

The **Control Tunnel** in CAPWAP is used to carry all management and control traffic between the Access Point (AP) and the Wireless LAN Controller (WLC). This includes messages for AP discovery, join process, configuration updates, keep-alive packets, and system monitoring. The control tunnel operates over **UDP port 5246** and is often encrypted using **DTLS (Datagram Transport Layer Security)** to ensure secure communication between the AP and the controller.

2. Data Tunnel

The **Data Tunnel** is responsible for transporting actual client data traffic—such as web browsing, video streaming, or email—from the AP to the WLC. This tunnel ensures that all user data is forwarded to the controller for processing, policy enforcement, and routing. The data tunnel uses **UDP port 5247** and supports optional encryption, providing secure and efficient transport of user traffic over the network.

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

Lightweight Access Points (LWAPs)
Lightweight APs are dependent on a centralized **Wireless LAN Controller (WLC)** to manage all control and configuration tasks.

These APs forward both management and data traffic to the controller via **CAPWAP tunnels**, making the WLC essential for operation.

Cloud-based Access Points
Cloud-based APs are managed and configured through a **cloud controller** hosted on the internet, eliminating the need for an on-premises hardware controller.

They offer **remote monitoring, centralized configuration, and analytics** via a web interface, and often operate independently even during cloud disconnection

The main difference lies in the **management location**—lightweight APs rely on an **on-site controller**, whereas cloud-based APs are managed **remotely via the internet**, offering more flexibility and scalability in distributed environments.

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

AP Boot-Up and IP Acquisition

- The AP powers on and obtains an IP address from a DHCP server.
- It also receives WLC discovery information via DHCP option 43 or other methods like DNS, static IP, or broadcast.

WLC Discovery and Join Process

- The AP sends a **CAPWAP Discovery Request** to the WLC.
- The WLC replies with a **Discovery Response**.
- The AP then sends a **Join Request**, and the WLC responds with a **Join Response**.

Tunnel Establishment

- After joining, the AP and WLC establish **two logical tunnels** over UDP:
  - **Control Tunnel (UDP Port 5246)**: For management traffic (e.g., configuration, monitoring, keep-alives).
  - **Data Tunnel (UDP Port 5247)**: For client/user traffic (e.g., internet access).

Security of Tunnels

- The **control tunnel** is secured using **DTLS (Datagram Transport Layer Security)** to ensure encrypted and authenticated management communication.
- The **data tunnel** may also be encrypted based on configuration and policies.

Keep-Alive Messages:

- The AP sends **CAPWAP echo requests (keep-alive messages)** periodically to the WLC.
- The controller responds with echo replies to confirm that the connection is still active.
- This process helps to monitor the tunnel's health continuously.

Tunnel Maintenance and Re-establishment:

- If the controller doesn't receive a response within a specified time (e.g., after 3 missed keep-alives), it assumes the AP is down.
- The AP may then try to **reboot or reconnect** to the controller automatically to re-establish the CAPWAP tunnels.

Data Transmission and Control Updates:

- Once the tunnel is active, all control and client data pass through it.
- Configuration changes or firmware updates from the WLC are sent via the control tunnel, while user traffic flows through the data tunnel.

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

Sniffer Mode :

- Function: In Sniffer mode, the AP captures all wireless packets on a specific channel and forwards them to the controller or a network analyzer for inspection.
- No Client Service: It does not broadcast SSIDs or serve clients.
- Primary Use Case: Useful for packet-level analysis, troubleshooting wireless issues, or analyzing security threats using tools like Wireshark.
- Example: You enable Sniffer mode on an AP to trace client disconnections or diagnose authentication failures.

Monitor Mode :

- Function: In Monitor mode, the AP scans all channels continuously, collecting RF metrics, rogue AP detection, and spectrum data.
- No Client Service: Like sniffer mode, it does not serve clients or broadcast SSIDs.
- Primary Use Case: Used for RF health monitoring, rogue device detection, spectrum planning, and wireless intrusion prevention (WIPS).
- Example: You use Monitor mode to detect unauthorized APs or to optimize channel allocation in a high-density environment.

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

If the WLC (Wireless LAN Controller) is deployed in a WAN, the best AP mode for a local network is Flex Connect mode.

If the WLC (Wireless LAN Controller) is deployed in a WAN, the best AP mode for a local network is Flex Connect mode.

In Flex Connect mode, the Access Point (AP) is capable of switching traffic locally at the branch site, even when it is connected to a remote WLC over the WAN. When the WAN link is up, the AP uses the controller for configuration, authentication, and central management. If the WAN link goes down, the AP enters standalone mode and continues to serve users locally using pre-downloaded configuration and policies. This ensures local switching of client traffic, reduced latency, and continued network availability during WAN outages.

Flex Connect mode is best because it minimizes WAN dependency, saves bandwidth, and improves user experience by allowing traffic to stay local, while still benefiting from centralized WLC management when available.

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

   Here are the key challenges of deploying more than 50 autonomous APs in a large network like a university:

1. **Manual Configuration and Management**: Each autonomous AP must be configured individually, making setup and updates time-consuming and error-prone across dozens of devices.
2. **Lack of Centralized Control:** There's no central management platform to monitor performance, troubleshoot issues, or push security policies, leading to inefficiencies.
3. **Inefficient Radio Resource Management:** Without a controller to coordinate channel and power levels, autonomous APs may cause interference, resulting in poor coverage and signal overlap.
4. **Scalability Issues**: As the network grows, maintaining consistency in configuration and performance becomes increasingly difficult without centralized control.
5. **Security Policy Inconsistency:** Applying and maintaining uniform security settings (like encryption, authentication) across all APs is challenging and may lead to vulnerabilities.
6. **Client Roaming Limitations:** Seamless handoff between APs is harder to manage, which can impact user experience for mobile users moving across the campus.
7. **Firmware and Update Management:** Updating firmware on each AP manually is time-consuming and can lead to version mismatches, causing instability in the network.
8. **Monitoring and Troubleshooting Complexity:** Without centralized logging and alerting, detecting and resolving network issues becomes more reactive and less efficient.

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

   If a wireless client is connected to a lightweight AP in local mode and the WLC goes down, the following will happen:

1. **Client disconnection:** The client will lose its connection because all control and data traffic in local mode is tunneled through the WLC. Without the WLC, the AP cannot process client traffic.

2. **No new associations:** The AP will stop accepting new client associations since it relies on the WLC to handle authentication and policy enforcement.

3. **Ap keeps rebooting or goes into discovery mode:** The AP will try to re-establish communication with the controller. If it fails continuously, it may keep rebooting or stay in a CAPWAP discovery state, waiting for a WLC to become available.

4. **Network outage for wireless clients:** Since local mode does not support standalone operation, wireless services will be down until the WLC is restored or the AP is switched to a mode like Flex Connect, if supported and configured.