MODULE 2 ASSIGNMENT – WIFI TRAINING

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

SplitMAC Architecture is a design used in Wi-Fi networks where the MAC (Medium Access Control) functions are split between the Access Point (AP) and the Wi-Fi device (station), aiming to optimize performance.

Key Components:

- **AP (Access Point)**: Handles the **higher** MAC layer functions such as packet scheduling, encryption, and data transmission management.
- **Wi-Fi Device (Station)**: Handles the **lower** MAC layer functions, such as frame detection, contention, and acknowledgment.

How SplitMAC Improves AP Performance:

1. **Reduced Load on AP**
    - The AP offloads certain MAC layer functions (like frame detection and contention) to the Wi-Fi device, reducing the load on the AP.
    - This allows the AP to focus more on higher-level tasks such as managing multiple client devices efficiently.
2. **Improved Spectrum Efficiency**
    - The AP can better manage communication with multiple devices simultaneously by focusing on managing access and scheduling, thus minimizing congestion and collisions.
3. **Better Power Efficiency**
    - Devices can manage lower-level tasks independently, which helps reduce their power consumption, allowing the AP to focus on power-hungry tasks like transmitting high-bandwidth data.
4. **Increased Throughput**
    - By separating responsibilities, the AP can handle multiple clients more effectively, increasing overall throughput in dense environments.
5. **Enhanced Roaming**
    - Devices can perform lower MAC operations autonomously, facilitating faster transitions between APs when roaming, improving overall performance for mobile users.

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

CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol designed to manage multiple wireless Access Points (APs) from a central location, typically a **Wireless LAN Controller**

(WLC). CAPWAP allows for centralized management, configuration, and monitoring of APs in a network, making it easier to scale and maintain.

Key Functions of CAPWAP:

1. **Centralized Control**: The WLC controls the APs, pushing configurations and policies to them.
2. **Efficient Communication**: APs and WLC communicate through CAPWAP to exchange data, configuration updates, and other management information.

Flow Diagram

1. **AP Discovery** → AP sends a request for controller discovery.
2. **Join Process** → AP and WLC authenticate and exchange configuration details.
3. **Configuration Push** → WLC pushes network configurations (e.g., SSID, security) to the AP.
4. **Client Connection** → Clients connect to the AP, which forwards traffic to the WLC if needed.
5. **Monitoring and Maintenance** → WLC continuously monitors AP status, pushing updates when required.

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

CAPWAP in the OSI Model:

CAPWAP fits primarily in the **Data Link Layer (Layer 2)** and **Network Layer (Layer 3)** of the OSI model. Specifically:

- **Control Plane Communication (Layer 2)**: CAPWAP handles the control and management of the AP and WLC, which involves sending configuration updates, status information, and policy enforcement. This communication occurs over UDP (User Datagram Protocol) on ports 5246 and 5247.
- **Data Plane Communication (Layer 3)**: Data traffic, depending on the architecture, can be tunneled through the CAPWAP protocol to ensure central management and security.

Two Tunnels in CAPWAP and Their Purpose:

1. **Control Tunnel**:
    - **Purpose**: Carries control and management messages between the Access Point (AP) and the Wireless LAN Controller (WLC).
    - **Traffic Type**: Includes AP join requests, configuration changes, health status updates, and other management data.
    - **Protocol**: UDP port 5246 is used for control plane traffic.

- **Significance**: Ensures secure and efficient exchange of management and configuration data between AP and WLC.

2. **Data Tunnel**:
    - **Purpose**: Carries client data traffic (payload) between the AP and the WLC.
    - **Traffic Type**: Includes user data (e.g., internet traffic from clients) which is tunneled back to the WLC for centralized management and security.
    - **Protocol**: UDP port 5247 is used for data plane traffic.
    - **Significance**: Facilitates centralized control of data traffic, ensuring security policies (such as encryption, QoS) are applied at the controller level, and enabling seamless client roaming.

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

Feature	Lightweight APs	Cloud-based APs
Management	Managed by a centralized WLC (local controller)	Managed through a cloud platform (remote/cloud)
Control	Control and configuration done by WLC	Control and configuration done via the cloud
Deployment	Requires physical controllers on-premises	Managed remotely via the cloud, no need for local controllers
Scalability	Scalable, but may require more infrastructure for large setups	Easily scalable as APs are cloud-managed
Use Case	Large enterprises, campuses, high-density areas	Small businesses, remote or distributed networks
Example	Cisco Lightweight APs with WLC	Meraki, Aruba Cloud APs

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

- **Discovery Phase**:
- When the AP powers on, it sends out a **CAPWAP Discovery Request** (via DHCP, DNS, or statically configured IP) to find the WLC.
- The WLC responds with a **CAPWAP Discovery Response**, which includes the IP address of the controller.
- **Join Phase**:
- After discovering the WLC, the AP initiates a **CAPWAP Join Request** to establish a secure session with the WLC.
- The WLC replies with a **CAPWAP Join Response**, which includes necessary configuration information such as security credentials, tunneling parameters, and AP configurations.

- **Tunnel Establishment**:
- The **Control Tunnel** and **Data Tunnel** are established between the AP and the WLC:
    - The **Control Tunnel** (using UDP port 5246) is responsible for management and control messages (e.g., configuration, health checks).
    - The **Data Tunnel** (using UDP port 5247) handles the user data traffic, which is tunneled back to the controller for centralized management.
- **Authentication & Security**:
- The AP and WLC authenticate each other using certificates or pre-shared keys (PSK) to ensure secure communication.
- The **CAPWAP tunnel** encrypts both control and data plane communications to protect sensitive network data.
- **Heartbeat and Keep-alive**:
- To maintain the tunnel and ensure it stays alive, periodic **heartbeat messages** are exchanged between the AP and the WLC.
- These heartbeats are sent over the **Control Tunnel** to check the health of the connection and ensure the AP is still connected to the controller.
- **Session Maintenance**:
- As long as the AP and WLC continue exchanging heartbeats, the tunnel remains open.
- The WLC continuously monitors the AP's status, including its performance and any configuration changes.
- **Re-establishment**:
- If the CAPWAP tunnel is lost (due to network issues or controller failure), the AP will attempt to reconnect to the controller by repeating the discovery and join process.
- If there are multiple controllers configured, the AP will try to connect to an alternate controller if the primary one becomes unreachable.
- **Tunnel Termination**:
- The tunnel is terminated when the AP is shut down or when it is no longer in communication with the WLC. The controller will also terminate the tunnel when the AP is decommissioned or manually removed from the network.

6. What is the difference between Sniffer and Monitor mode? Explain with use case for each mode

Feature	Sniffer Mode	Monitor Mode
Purpose	Passive capture of network traffic	Capture and analyze all frames in range (including security analysis)
Capture Type	Captures frames from the network without any interaction	Captures all frames from any network in range, sometimes allowing packet injection
Network Interaction	No interaction with the network, purely passive	Can interact with the network (e.g., with packet injection for testing)
Use Case	Troubleshooting, packet analysis, monitoring security	Wireless network mapping, rogue AP detection, penetration testing
Device Role	Passive listening device	Listening device with additional capabilities (security testing, packet injection)

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

FlexConnect Mode is typically the **best choice** for local networks when the WLC is deployed in the WAN because:

- It allows for **local switching of data traffic**, which minimizes the impact of WAN latency and reduces the dependence on the WAN link for client data.
- It can **function during WAN outages**, ensuring that the AP continues to provide network access, though management and control may be limited.
- **Local Mode** could still be used, but **FlexConnect Mode** offers better redundancy and performance, especially in scenarios where constant WAN connectivity cannot be guaranteed.

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

- **Centralized Management**:
- No central controller to manage configurations, making it harder to apply uniform settings across all APs.
- **Configuration Consistency**:
- Ensuring all APs have the same settings (SSID, security policies) manually is time-consuming and prone to errors.
- **Roaming Issues**:
- Lack of coordination between APs can cause users to experience dropped connections or slow handoffs when moving between APs.
- **Scalability**:
- As the number of APs grows, managing each AP individually becomes less efficient, creating more administrative overhead.

- **Network Performance**:
- Manual interference management across APs may lead to channel congestion and poor load balancing, reducing overall network performance.
- **Security Risks**:
- Each AP must be secured individually, and misconfigurations could create vulnerabilities across the network.
- **Firmware Updates**:
- Manually updating firmware on each AP increases the risk of missing updates, leaving the network vulnerable.
- **Troubleshooting**:
- Diagnosing issues on individual APs without a centralized monitoring system can be difficult and slow.
- **High Administrative Costs**:
- The labor cost of maintaining and troubleshooting each AP individually increases with the number of APs.
- **Power and Connectivity**:
- Ensuring proper power supply and network connection to each AP can be logistically challenging in a large university setting.

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

Loss of Control Communication:

- The **Lightweight AP** loses the connection to the WLC, as it relies on the WLC for control traffic (such as configuration, management, and security policies).
- **Client Connectivity**:
- **Existing clients** that are already connected to the AP will **continue to stay connected** and may still be able to send and receive data traffic.
- However, new clients cannot connect because the AP cannot authenticate them without the WLC.
- **No Configuration Updates**:
- The AP will not be able to receive any new configuration changes, firmware updates, or security policy updates from the WLC until the WLC is back online.
- **Limited Functionality**:

- The AP will still operate as a basic access point for existing clients but will not have access to advanced features such as centralized security enforcement, roaming management, or monitoring from the WLC.
- **Disconnection Risk**:
- If the AP loses connection to the WLC for a prolonged period, existing clients may eventually be disconnected once their session expires or if they roam to another AP that is also dependent on the WLC.