MODULE 2

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

   In Wi-Fi, a split-MAC architecture distributes MAC layer functions between the Access Point (AP) and a Wireless LAN Controller (WLC), with the AP handling real-time tasks and the WLC managing higher-level network functions, improving overall network performance and management
   In a split-MAC architecture, the Media Access Control (MAC) layer functions are divided between the AP and the WLC:
   AP: handles real-time tasks like radio frequency traffic transmission, encryption/decryption, and beacon/probe transmission.
   WLC: manages higher-level network functions like authentication, association/disassociation, and dynamic channel assignment.

   Performance improvement

   ->APs are relieved from heavy MAC-layer tasks, enabling them to focus on fast packet forwarding and real-time responsiveness.

   ->The controller can optimize resource allocation and interference management across multiple APs, improving overall network efficiency.

   ->Makes it easier to deploy and manage a large number of APs as the complexity is centralized.

   -> Centralized security policies can be enforced across all APs, making it easier to manage and maintain security.

   -> The WLC manages roaming, ensuring smooth transitions between APs for mobile users.

   -> Client handoffs are quicker and smoother, thanks to controller-coordinated decisions, reducing latency and improving user experience.

   In general,
   Lightweight APs use a Split MAC architecture, where lower MAC tasks (like client association, beacons, encryption, MU-MIMO/OFDMA, ACKs) are handled by the AP, while higher-level functions (RRM, QoS, load balancing, mobility, security) are centralized in the controller.

This setup reduces AP workload, improves efficiency, and enhances scalability by combining real-time data handling at the AP with centralized control for better performance and resource optimization in large wireless networks.

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

About CAPWAP
The split-MAC architecture relies on the CAPWAP protocol to facilitate communication and data transfer between the APs and the WLC.
CAPWAP stands for Control And Provisioning of Wireless Access Points.
CAPWAP uses two tunnels: one for control and one for data.
CAPWAP is used because:

->Standardizes how APs communicate with controllers.

->Separates control traffic (management/config) from data traffic (actual user data).

->Supports SplitMAC architecture.

->Allows zero-touch provisioning – APs can automatically discover and join a controller.

Benefits:

->Simplifies AP management.

->Enhances security with encrypted tunnels.

->Enables scalable and flexible network deployment.

->Supports centralized troubleshooting and monitoring.

Flow between AP and Controller
The flow is explained by two phases namely the Discovery and Join phase and Control Plane.
Discovery and Join:
This is the initial setup phase when the AP first powers up and tries to connect to the controller (WLC – Wireless LAN Controller).

Steps involved are:

AP discovery:The AP searches for the WLC using different methods (DHCP, DNS, broadcast). It sends a CAPWAP Discovery Request.

WLC Response: The controller receives the request and replies with a CAPWAP Discovery Response.

Secure Connection Setup: Before sending sensitive data, the AP and controller secure the connection using DTLS (Datagram Transport Layer

Security) – similar to HTTPS for web. This ensures authentication and encryption between them.

Join Request/Response: The AP sends a Join Request to the WLC; The controller checks the AP's identity and, if approved, replies with a Join Response. This completes the control connection setup.

Control Plane – Ongoing Management:
Once joined, the AP and controller exchange control messages to manage the wireless network.
The Control Plane is responsible for all management and control functions between the Access Point (AP) and the Wireless LAN Controller (WLC).
It does not carry user data — only configuration, status, and management info.

Flow:
Client -> AP -> CAPWAP Data Tunnel -> Controller -> LAN

Control Messages(Encrypted with DTLS (Datagram Transport Layer Security): used in UDP):
AP -> Controller:
Discovery Request: AP sends this when it powers on, looking for a WLC.
Join Request: AP formally asks to join and be managed by the WLC.
Heartbeats: Regular keep-alive messages to check health/status.
Controller -> AP:
Configuration: WLC sends SSID settings, channel, security config, etc.
Firmware Updates: Controller can push AP software updates.
Policy Push: Sends access control, QoS, and other operational policies.

Client Data Traffic (Once the AP is fully joined and operational, it starts handling user (client) traffic):

CAPWAP encapsulates client traffic between AP and controller over UDP 5247.

CAPWAP encapsulates client data packets (like HTTP, VoIP, etc.) and sends them to the controller using UDP port 5247. This is known as the CAPWAP Data Tunnel.

The controller can either route the traffic or bridge it locally at the AP (depending on CAPWAP mode).

Why UDP?
The properties like Lightweight, Faster (no handshaking) makes UDP protocol better for real-time communication.

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

CAPWAP in OSI model
CAPWAP operates at Layer 2 (Data Link) and Layer 3 (Network) of the OSI model.
In Layer 4, Transport Layer: Uses UDP (ports 5246 & 5247) to transmit control and data packets.

In Layer 3, Network Layer: Runs over IP (IPv4/IPv6) for routing between AP and Controller.

In Layer 2, Data Link Layer: CAPWAP tunnels Layer 2 (Ethernet frames) or higher-layer data (e.g., IP packets) across the network.

Tunnels in CAPWAP:

1. Control Tunnel:

Handles AP management, authentication, configuration, and firmware updates.
It is Encrypted via DTLS.
UDP Port: 5246

2. Data Tunnel:

Encapsulates and forwards client traffic between AP and controller.
To forward client/user data traffic (e.g., HTTP, VoIP) between AP and controller.
UDP Port: 5247
Typically not encrypted. Thus optional encryption.

4. What are the differences between Lightweight APs and Cloud-based APs?

FEATURE	LIGHTWEIGHT AP	CLOUD BASED AP
DEFINITION	Lightweight APs are access points that do not make decisions on their own. They rely on a central Wireless LAN Controller (WLC) to manage configurations, policies, and client traffic.	Cloud-based APs are managed via the internet using a cloud dashboard (like Cisco Meraki, Aruba Central, TP-Link Omada).
CONTROL PROTOCOL	CAPWAP (UDP 5246 - control, 5247 - data)	HTTPS / REST APIs / Proprietary Cloud Protocol
CONTROLLER LOCATION	On-premises Wireless LAN Controller (WLC)	Cloud-hosted Controller (Vendor's cloud)
DEPLOYMENT MODEL	Requires a local controller for AP operation. Complexity: High – requires WLC setup and AP configuration	No on-site controller needed, managed over the internet. Complexity: Low – Zero-touch provisioning via cloud
SCALABILITY	High – scalable within controller's capacity. Limited to the number of APs a WLC can handle	Very High – infinite scaling via cloud backend. Easily scalable with cloud-based subscription models
DATA PLANE	Data can be tunnelled to the WLC or locally switched.	Data is typically locally switched at the AP.
REDUNDANCY/FAILOVER	Requires backup WLCs for failover.	Cloud controllers are highly available
TROUBLESHOOTING/MONITORING	Real-time via controller tools	Cloud-based analytics, alerts, remote troubleshooting
USE CASES	Enterprise campuses, large indoor deployments	SMBs, remote branches, distributed retail chains

6. What are the differences between Sniffer and Monitor mode, use case for each mode?

FEATURE	SNIFFER MODE	MONITOR MODE
DEFINITION AND ACTIVITY	Captures 802.11 frames for packet-level analysis-> wireless traffic and forwards it to a remote device (e.g., Wireshark on a PC) for analysis.	Observes RF spectrum and Wi-Fi activity. It passively listens to all Wi-Fi frames on a channel without associating with any network.
WHAT IT CAPTURES	Data, control, management frames from a **specific SSID** or channel	General RF activity across multiple channels (no association needed)
PURPOSE	Used by network administrators for troubleshooting, security auditing, and performance analysis, and can also be used	Used for wireless network sniffing, security analysis, and troubleshooting.

	by malicious actors to intercept sensitive data.	
ASSOCIATION WITH AP/CLIENT	Usually tied to a specific SSID, BSSID, or channel (AP or Controller)	No association – purely passive
OUTPUT FORMAT	Raw 802.11 packets – suitable for tools like Wireshark	Channel utilization, interference levels, noise metrics. Used in Aircrack-ng.
ENCRYPTION HANDLING	Cannot decrypt encrypted packets unless provided with keys.	Captures raw encrypted traffic; decryption depends on external tools.
USE CASES	Troubleshooting client connectivity, packet loss, frame analysis Often used with packet analyzers (e.g., Wireshark, Omnipeek) Analyzing specific AP-client interactions.	Site surveys, detecting rogue APs, checking channel interference Used with spectrum analyzers or controller monitoring tools Wireless security analysis (e.g., detecting rogue APs, attacks).

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

Best AP Connect Mode is FlexConnect Mode for vendors like Cisco.

FlexConnect Mode allows an AP to switch between centralized and local forwarding. It's designed for remote site deployments where the WLC is across a WAN link.

Working:

Local Authentication & Switching: The AP can authenticate clients locally without contacting the WLC. Useful for WAN outages or to reduce authentication latency.

Client data traffic is switched locally by the AP directly to the LAN or internet. Avoids tunnelling data through the CAPWAP data tunnel to the WLC, saving WAN bandwidth. Ideal for branch offices, retail stores, or remote clinics.

WAN Failover Handling: If the WAN link to the controller fails, APs continue operating in standalone mode. Clients can still connect, authenticate (if pre-configured), and access local network resources.

Control & Management via CAPWAP Tunnel: With a Centralised management, configuration updates and monitoring are still performed by the controller over WAN.

Local Redirection: If there are DHCP, DNS delays due to central WLC dependency, AP can locally provide DHCP, DNS redirection.

Bandwidth management: If Bandwidth usage is high if all traffic is tunnelled, it saves WAN bandwidth by keeping data local.

Thus, FlexConnect is best for WAN connected WLCs as they reduce bandwidth by local switching, ensures continuous network operation, efficient Failover handling, etc...

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

Some of the challenges are mentioned as follows:

- Management: Manual configuration of each IP, lack of centralization or mass provisioning.
- Scalability: Expansion of Networks are time consuming.
- Troubleshooting: Individual and manual assessions are time consuming.
- Firmware Updates: Time consuming Firmware updates.
- Radio Interference: No RF coordination, High chances of channel overlap and co channel interference.
- Load Balancing: Some APs overloaded while others idle as there are no client balancing logic.
- Authentication: Difficult to implement 802.1X enterprise auth without centralized control.
- Increased Network Congestion: Failed client balance logic.
- Guest Access Control: Difficult to enforce access policies consistently.

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

Maintaining CAPWAP Tunneling

When a Lightweight Access Point (AP) connects to a Wireless LAN Controller (WLC), it sets up a CAPWAP tunnel to separate control and data traffic.

CAPWAP creates two separate tunnels over UDP:

1. Control Tunnel (UDP 5246): to handle WLAN management, AP configuration, firmware updates, etc

2. Data Tunnel (UDP 5247): to carry client data between AP and controller

Tunnel Establishment Process

Steps:

1. Discovery: AP discovers WLC using DHCP,DNS or Broadcast.

2. DTLS Handshake: AP and WLC establish a secure CAPWAP tunnel using DTLS (Datagram Transport Layer Security) for encryption and authentication.

3. Join Process: AP sends a Join Request, and WLC replies with Join Response.

4. Configuration process: WLC sends configuration settings to AP via the control tunnel.

5. Once configured, AP is ready to send client traffic over the data tunnel.

Tunnel Maintainance

1. DTLS Keepalives: Heartbeat packets are exchanged over the control tunnel to monitor AP health.

2. Rekeying: DTLS sessions can be rekeyed to maintain encryption security.

3. Failover: If the controller supports HA (High Availability), CAPWAP tunnels can switch to a backup controller with minimal disruption.

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

In Local Mode, Lightweight APs rely heavily on the WLC for both control and some client-related functions.

In Local Mode, all client traffic is tunneled to the WLC using CAPWAP. Since the WLC is down, the AP cannot process or switch traffic.

1. CAPWAP Tunnel Breaks

-> AP loses the CAPWAP tunnel (UDP ports 5246/5247) with the WLC.

-> CAPWAP is essential for configuration, management and client authentication.

2. AP stops functioning

->The Lightweight AP in Local Mode reboots after losing connection with the WLC (default behavior).

->All connected clients are dropped since the AP relies on the WLC for handling authentication, policy enforcement, and traffic forwarding.

->The AP stops broadcasting SSIDs because it cannot authenticate new clients without the WLC.

->The AP continuously searches for an available WLC via DHCP, DNS, or static configuration.

->If WLC is still unavailable, the AP stays in a disconnected state and stops broadcasting SSIDs.