# MODULE 2 ASSIGNMENT

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

- SplitMAC divides MAC layer functions between Access Points (APs) and Wireless LAN Controllers (WLCs).
- Real-time functions like client association, encryption, and packet buffering are handled by APs.
- Non-real-time tasks like authentication, load balancing, and QoS are managed by WLCs.
- This reduces the processing burden on APs, making them lightweight and improving performance.
- Centralized control through WLC enhances reliability, resource optimization, and faster network responses.

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

- CAPWAP (Control and Provisioning of Wireless Access Points) manages communication between APs and WLCs.
- The AP first gets an IP address using DHCP and discovers the WLC.
- After discovery, a secure DTLS tunnel is established for communication.
- AP sends a Join Request, receives a Join Response, and downloads necessary configurations.
- Regular keepalives maintain the connection, and updates are managed via control and data tunnels.

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

- CAPWAP operates across Layers 4 to 7 of the OSI model.
- Layer 4 (Transport) uses UDP, Layer 5 (Session) manages sessions, Layer 6 (Presentation) secures data, Layer 7 (Application) provides control functions.
- **Control Tunnel:** Handles AP management traffic (configuration, status updates).
- **Data Tunnel:** Carries client data traffic between AP and controller.
- Tunnels ensure separation of control and data for security and performance.

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

- **Lightweight APs** are managed by an on-premises WLAN Controller (WLC).
- **Cloud-based APs** are managed remotely through a cloud service.
- Lightweight APs depend on the WLC’s capacity for scaling; cloud APs are highly scalable.

- Cloud APs reduce upfront costs but may have recurring subscription fees.
- Security for Lightweight APs is locally managed, while Cloud APs depend on cloud security policies.

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

- AP and WLC exchange periodic **Keepalive** messages to verify data tunnel health.
- **Echo Request/Reply** messages check the status of the control tunnel.
- AP monitors the connection and attempts to re-establish tunnels if failures occur.
- CAPWAP supports automatic failover and tunnel restoration mechanisms.
- Regular configuration status updates keep the tunnel synchronized.

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

- **Monitor Mode:** AP passively listens to all wireless frames without transmitting.
- **Use case:** Detecting rogue APs and wireless intrusion detection in enterprise networks.
- **Sniffer Mode:** AP captures packets for a specific network/channel it is associated with.
- **Use case:** Troubleshooting network issues like slow internet or packet loss analysis.
- Monitor mode focuses on security surveillance; Sniffer mode is used for detailed packet inspection.

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

- **FlexConnect Mode** is the best choice when WLC is in the WAN.
- In FlexConnect, APs switch to local switching for client traffic if WLC becomes unreachable.
- APs handle authentication and forwarding locally during WAN outages.
- This ensures continuous wireless service without depending on WAN link stability.
- FlexConnect reduces WAN bandwidth usage by locally managing user traffic.

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

- **Manual configuration** is required for each AP, leading to high administrative overhead.
- **Scalability issues** arise as the number of APs grows, making management complex.
- **Inconsistent policies** due to lack of centralized control.

- **Security risks** because manual updates and monitoring are error-prone.
- Troubleshooting becomes difficult without centralized logging and visibility.

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

- In **Local Mode**, if WLC goes down, the Lightweight AP loses control functionality.
- Clients may get disconnected as AP cannot authenticate new sessions.
- AP cannot manage roaming or enforce security policies without WLC.
- Some APs switch to **Fallback/FlexConnect** mode if pre-configured, allowing local switching.
- If not configured, wireless services may stop until WLC comes back online.