**Module 2**

**1. Brief about Split MAC architecture and how it improves the AP's performance**

The Split MAC architecture divides the MAC layer functionalities between the Access Point (AP) and the Wireless LAN Controller (WLC). This division is strategic—time-critical and basic operations are handled at the AP, while complex management and control operations are centralized at the WLC. This architecture improves performance, reduces AP complexity, and simplifies large-scale wireless deployments.

**Key Points:**

* **Local MAC at AP**: Handles real-time functions like:
  + Beacon generation
  + RTS/CTS (Request to Send/Clear to Send)
  + Acknowledgement
  + MAC-layer retransmissions
  + Encryption/decryption
* **Central MAC at WLC**: Manages higher-level tasks like:
  + Client authentication and roaming decisions
  + QoS policy enforcement
  + Security policies and access control
  + RF management (load balancing, interference mitigation)
* **Benefits**:
  + Reduces processing load on APs
  + Enables centralized configuration and updates
  + Improves scalability and consistency across the network

**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 and control multiple APs from a centralized controller. It simplifies wireless LAN deployment by separating management and data traffic into secure tunnels, enabling seamless AP provisioning, monitoring, and configuration from a WLC.

**Flow between AP and Controller:**

* **Discovery Phase**:
  + AP discovers the WLC via DHCP Option 43, DNS, or broadcast.
* **Join Process**:
  + AP sends join request to WLC.
  + Mutual authentication and capability exchange.
* **Tunnel Establishment**:
  + Two tunnels are created:
    - **Control Tunnel (UDP 5246)** – DTLS-encrypted; for configuration, management messages.
    - **Data Tunnel (UDP 5247)** – Carries client data between AP and WLC.
* **Configuration & Operation**:
  + WLC pushes configuration to AP.
  + AP handles radio operations; WLC processes client management and control functions.

**Benefits of CAPWAP:**

* Centralized AP provisioning and management
* Secure communication between APs and controller
* Simplified large-scale wireless deployments

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

CAPWAP operates mainly at Layer 3 (Network Layer) and Layer 4 (Transport Layer) of the OSI model. It encapsulates management and data traffic using UDP (ports 5246 for control and 5247 for data). CAPWAP establishes two tunnels:

* **Control Tunnel**: Secure DTLS-encrypted tunnel used to manage the AP, push configuration, and control messages.
* **Data Tunnel**: A separate UDP tunnel that transports actual user data between the AP and WLC. This separation ensures robust control over APs while optimizing performance and security of data traffic.

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

* **Lightweight APs** are dependent on a physical Wireless LAN Controller (WLC) to handle management tasks. They use protocols like CAPWAP to communicate with the WLC and cannot function independently for extended periods if the controller fails.
* **Cloud-based APs**, on the other hand, are managed via cloud platforms. They can be configured, monitored, and updated remotely through the internet. They offer scalability, ease of management, and are ideal for distributed environments. While both offer centralized control, cloud-based APs reduce infrastructure overhead and provide more flexible and remote management capabilities.

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

The CAPWAP tunnel is established and maintained using a secure handshake and keep-alive mechanisms. Once the AP discovers the controller, it establishes a DTLS-based control tunnel for secure communication. Periodic keep-alive messages ensure that the tunnel is active. If these messages fail to exchange within a timeout interval, the tunnel is considered down, prompting reconnection attempts. The control tunnel ensures encrypted communication, while the data tunnel handles client traffic. Both tunnels operate over UDP and are designed to be resilient to network disruptions.

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

* **Sniffer Mode**: In this mode, an AP captures 802.11 frames over the air and forwards them to a network analyzer like Wireshark. It's used for deep packet inspection, troubleshooting, and wireless analysis. The AP does not serve clients in this mode.
  + *Use Case*: Troubleshooting RF issues, analyzing security breaches, or capturing packets for performance tuning.
* **Monitor Mode**: The AP listens to all wireless traffic without associating with clients. It scans multiple channels for rogue APs, interference, and spectrum analysis.
  + *Use Case*: Wireless intrusion detection/prevention (WIDS/WIPS), rogue AP detection, and channel utilization monitoring.

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

When a Wireless LAN Controller (WLC) is located remotely over a Wide Area Network (WAN), using **FlexConnect mode** is optimal for local APs. FlexConnect allows the APs to locally switch traffic and authenticate users even when the controller becomes unreachable, ensuring uninterrupted service in local networks like branch offices or educational campuses.

**Why FlexConnect is best:**

* **Local switching**:
  + AP can switch traffic locally without routing it to the WLC.
  + Reduces latency and bandwidth usage over WAN.
* **Survivability**:
  + In case WAN or WLC fails, APs continue serving connected clients.
  + New client authentication can be supported via cached credentials.
* **Centralized management retained**:
  + Configuration and policy updates still come from WLC when reachable.
* **Use cases**:
  + Branch offices with remote WLC
  + University campuses with centralized IT hubs

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

Deploying over 50 autonomous APs in a large network poses multiple challenges:

* **Lack of Central Management**: Each AP must be configured and updated individually, leading to inconsistent settings and higher administrative overhead.
* **Scalability Issues**: Adding or changing APs becomes difficult without centralized control.
* **Roaming Inefficiency**: Seamless roaming is hard to achieve without coordination, resulting in dropped connections and authentication delays.
* **Security Gaps**: Inconsistent application of security policies increases risk.
* **Performance Monitoring**: Troubleshooting and performance monitoring is cumbersome without a unified dashboard or logs. In contrast, lightweight or cloud-managed APs address these limitations effectively.

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

In **local mode**, a lightweight AP functions as a "dumb" radio relying entirely on the WLC for decision-making and data forwarding. If the WLC goes down:

* **New clients** cannot associate or authenticate, as all control functions are lost.
* **Existing clients** may continue to communicate until the CAPWAP keep-alive times out, after which service is disrupted.
* **No roaming**, policy enforcement, or QoS decisions can be made. To avoid such outages, **FlexConnect mode** is recommended where APs can continue basic operations even without the WLC.