Moulik Tammana

Wi-Fi Training Program Module – 2

Q1. Brief about Split MAC architecture and how it improves the AP's performance.

The Access Point (AP) and a central Wireless LAN (WLAN) controller share the MAC (Medium Access Control) layer operations in a Wi-Fi network design known as Split MAC. Wireless communication management, including channel access, frame control, and security, is handled by the MAC layer. Uses split MAC architecture is done such that the lower MAC functions are done by the AP and the upper MAC functions are moved and centralized into the controller.

How Split MAC works in the following manner:

- **AP (Lightweight AP): Handles time-sensitive MAC operations such as frame transmission, acknowledgments, and encryption.**
- **WLAN Controller: Manages higher-level MAC functions like authentication, association, and roaming decisions.**

Split MAC will improve the performance:

- **Reduced Processing Load: Since high-level MAC functions are handled by the central controller, the APs require less processing power, allowing for cost-effective and scalable deployments.**
- **Efficient Roaming: Client handoffs between APs are managed centrally, reducing delays and improving mobility performance.**
- **Better Network Management: Centralized control allows easier configuration, monitoring, and troubleshooting of multiple APs.**
- **Enhanced Security: The WLAN controller can enforce security policies uniformly across all connected APs.**
- **Optimized Spectrum Utilization: APs can focus on efficient data transmission, while the controller handles load balancing and interference management.**

Q2. Describe about CAPWAP, explain the flow between AP and Controller.

CAPWAP (Control and Provisioning of Wireless Access Points) is a standardized protocol that enables centralized control of wireless access points (APs) by a wireless LAN controller (WLC).

Key feature of CAPWAP is:

- **Encapsulation & Tunneling: CAPWAP encapsulates wireless data traffic in tunnels between the AP and the WLC.**
- **Security: Uses DTLS (Datagram Transport Layer Security) for encrypting control messages.**
- **Support for Different Deployments: Works with Lightweight APs where the WLC makes centralized decisions, simplifying AP configurations.**

CAPWAP flow between AP and WLC:

- **IP address assignment is done to the AP by contacting the DHCP server using the DORA process.**
- **Discovery Phase: Broadcast CAPWAP Discovery request and the WLC responds with a Discovery Response, providing its details.**
- **Join Phase: The AP sends a CAPWAP Join Request to the to the discovered WLC and the WLC verifies the AP's credentials and responds with a CAPWAP Join Response.**
- **Configuration Phase: The WLC sends configuration parameters (SSID, VLAN, security settings, etc.). If the AP's firmware does not match the WLC's version, the AP downloads the correct firmware and reboots.**
- **Once clients associate with an Access Point (AP), their data is encapsulated within CAPWAP and sent to the Wireless LAN Controller (WLC). The WLC acts as the central management point, processing, routing, and monitoring the APs while ensuring seamless mobility for wireless clients.**

Q3. Where this CAPWAP fits in OSI model, what are the two tunnels in CAPWAP and its purpose.

CAPWAP operates in multiple layers in the OSI layer:

- **Layer 7- Application Layer: CAPWAP provides management functionalities like AP configuration, firmware updates, and status monitoring.**
- **Layer 4 - Transport Layer: CAPWAP uses UDP as its transport protocol, specifically UDP ports 5246 (Control) and 5247 (Data).**
- **Layer 3 - Network Layer: CAPWAP packets are encapsulated in IP packets, allowing communication over different networks.**
- **Layer 2 – Data Link Layer: CAPWAP can be transported over Ethernet or Wi-Fi networks**

CAPWAP establishes two tunnels between the AP and WLC:

- **Control Tunnel (UDP 5246): Encrypted using DTLS, used for AP management, configuration, and firmware updates.**
- **Data Tunnel (UDP 5247): Transports client traffic, can be encrypted or unencrypted, and forwards packets based on network policies.**

Q4. What's the difference between Lightweight APs and Cloud-based Aps.

- **Management:**
  Lightweight APs: Centrally managed by a wireless LAN controller (WLC) on-site or in a data center.
  Cloud-based APs: Managed remotely through a cloud-based interface, no on-site controller required.
- **Configuration:**
  Lightweight APs: Rely on the WLC for configuration, policy enforcement, and real-time adjustments.
  Cloud-based APs: Configured via a web portal or app, with settings stored and applied from the cloud.
- **Scalability:**
  Lightweight APs: Scalable but requires additional hardware (controllers) as the network grows.
  Cloud-based APs: Highly scalable with minimal hardware, as the cloud handles increased demand.
- **Deployment:**
  Lightweight APs: Best for large, centralized environments like enterprises with complex networks.
  Cloud-based APs: Ideal for distributed or small-to-medium setups, like remote offices or retail chains.
- **Features:**
  Lightweight APs: Advanced features (e.g., roaming, load balancing) managed by the controller.
  Cloud-based APs: Feature-rich via cloud updates, including analytics, but may vary by provider.
- **Maintenance:**
  Lightweight APs: Requires on-site IT expertise for controller maintenance and updates.
  Cloud-based APs: Updates and maintenance handled automatically via the cloud.

Q5. How the CAPWAP tunnel is maintained between AP and controller.

1. CAPWAP Tunnel Establishment

- **Discovery Phase: The AP discovers the WLC through various methods, such as DHCP (Option 43), DNS resolution, or broadcasting.**
- **DTLS Handshake (if enabled): A secure Datagram Transport Layer Security (DTLS) tunnel is established for control messages.**
- **Join Request & Response: The AP sends a join request, and the WLC responds with a join response.**
- **Configuration & Image Download: The AP receives its configuration and may download a firmware update if required.**

2. Tunnel Maintenance

- **Heartbeat Keepalives: APs send periodic keepalive messages (CAPWAP control packets) to the WLC to ensure the connection is alive.**
- **Control & Data Plane Separation: The Control Plane is used for AP-WLC communication and the Data Plane is used for forwarding client data, which can be done in centralized or local mode.**
- **Sequence Numbering & Retransmission: CAPWAP uses sequence numbers to track packets and retransmits lost packets.**
- **DTLS Rekeying (if enabled): If DTLS is used, session keys are periodically refreshed to maintain security.**
- **Timeout & Reconnection: If the AP doesn't receive responses from the WLC within a defined timeout period, it will attempt to rejoin the controller.**
- **Heartbeat & Echo Mechanism: The AP-WLC tunnel is monitored using periodic CAPWAP echo requests and responses.**

Q6. What's the difference between Sniffer and monitor mode, use case for each mode.

Sniffer mode and monitor mode are both light weight Aps modes.

Sniffer Mode: The AP captures and forwards all 802.11 frames to a central system like a WLC or Wireshark. It does not interact with clients but passively collects packets for network troubleshooting, performance analysis, and security monitoring. This helps detect interference, authentication issues, and unauthorized access.
Use Cases: Wi-Fi troubleshooting, performance analysis, packet inspection in managed networks.

Monitor Mode: A device passively listens to all wireless traffic on a channel without joining any network. Used for intrusion detection and security audits, it helps monitor rogue APs, analyse channel usage, and detect attacks.
Use Cases: Wireless security audits, penetration testing, network forensics, detecting rogue APs.

Q7. If WLC deployed in WAN, which AP mode is best for local network and how?

In FlexConnect mode APs behave like local APs by default but switch into Autonomous mode when connection to WLC is lost.
Local Switching: If the WAN link to the WLC fails, the AP can continue forwarding local traffic without interruption. The AP will use cached authentication credentials to authenticate new users.
Centralized Control: When the WAN link is up, the AP communicates with the WLC for configuration updates, policy enforcement, and monitoring.
Seamless Failover: Even if the WAN link goes down, clients remain connected to the local network, and once the WAN connection is restored, the AP re-establishes communication with the WLC.

Q8. What are challenges if deploying autonomous APS (more than 50) in large network like university.

Autonomous APs operate independently without a central controller, which can lead to difficulties in management, scalability, and performance optimization.

- **Scalability Issues: Managing a large number of APs individually can be complex and time-consuming, especially when configuring SSIDs, security policies, and firmware updates.**
- **Interference Management: Without centralized coordination, APs may cause channel overlap and co-channel interference, leading to degraded network performance.**
- **Roaming Challenges: Clients moving across campus may experience delays or connection drops due to the lack of seamless roaming features like fast handoff and session persistence.**

- **Security Concerns: Ensuring uniform security policies, authentication mechanisms, and access controls across all APs can be difficult without a centralized management system.**
- **Load Balancing: Autonomous APs do not dynamically distribute client connections, leading to congestion on some APs while others remain underutilized.**
- **Troubleshooting Complexity: Identifying and resolving network issues requires manual intervention for each AP, increasing downtime and maintenance efforts.**
- **Firmware and Configuration Management: Updating firmware or applying network-wide changes must be done manually on each AP, which is inefficient and error-prone.**

Q9. What happens on wireless client connected to Lightweight AP in local mode if WLC goes down.

When a wireless client is connected to a Lightweight AP in Local Mode and the WLC goes down, several issues arise. Local Mode APs depend on the WLC for control and forwarding traffic, meaning a controller failure disrupts network operations.

- **Client Disconnection: Since Local Mode APs tunnel all client traffic to the WLC, a WLC failure results in an immediate loss of connectivity for all associated clients.**
- **No New Client Authentication: Without the WLC, the AP cannot authenticate new clients, preventing new connections from being established.**
- **Loss of Centralized Management: Configuration updates, security policies, and monitoring features become unavailable until the WLC is restored.**
- **AP Reboot or Standby Mode: Some APs may enter a recovery or reboot state, attempting to reconnect to the WLC, leading to temporary service disruptions.**
- **No Data Forwarding: Local Mode APs do not support local switching, meaning all client traffic is lost when the WLC is unreachable.**
- **Roaming Failures: Clients moving between APs may experience connection drops since AP handoff requires communication with the WLC.**