Name: Devansh Srivastava

Registration number: 21BCE0527

Wi-Fi Training Programme

Module 2

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

Ans: SplitMAC architecture divides traditional Wi-Fi access point functions between two devices:

- **Access Point (AP)**: Handles real-time, time-sensitive PHY and lower MAC functions
- **Controller (WLC)**: Manages non-real-time upper MAC functions and system-wide coordination

Key performance improvements:

- Centralizes administration, security policy, and configuration
- Provides dynamic RF management across multiple access points
- Supports seamless roaming without session break
- Decreases processing load on individual APs
- Makes large-scale deployment and update easier
- Allows consistent enforcement of policy network-wide
- Supports advanced capabilities such as load balancing and interference mitigation

This separation creates more efficient, scalable, and manageable wireless networks.

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

Ans: CAPWAP (Control And Provisioning of Wireless Access Points) is a
protocol used to facilitate communication between wireless APs and controllers.

Main elements of CAPWAP:

- Standard-based protocol (RFC 5415) for AP management
- Utilizes UDP as transport (ports 5246 for control, 5247 for data)
- Supports encrypted communication using DTLS

Flow of communication between AP and controller:

- Discovery: AP finds available controllers through broadcast, multicast, DNS, or static configuration
- Authentication: Mutual authentication between AP and controller using X.509 certificates
- Join: AP becomes part of controller and forms secure CAPWAP tunnel

  Configuration: Controller loads configuration to the AP
- Operation: Continuous flow of control and data messages
- Monitoring: Routine heartbeats and status indication

- Failover: AP will be able to detect failure in controller and will failover

During operation, management frames and client data will be tunneled between the AP and the controller depending upon deployment mode.

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

Ans: CAPWAP operates at Layer 2 and Layer 3 of OSI model.

Two tunnels are created between AP and WLC:

- Control Tunnel: Handles management/config messages (encrypted).
- Data Tunnel: Carries actual user data traffic (can be encrypted).

This separation enhances security and performance.

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

Lightweight APs	**Cloud-based Aps**
1. It is a part of legacy split-MAC design	1. Connected to cloud-hosted controller/management platform
2. Need on-premises controllers (WLC)	2. Employ internet connections to access cloud controllers
3. Employ CAPWAP or proprietary protocols for communications	3. Typically have greater local intelligence and failover
4. Controller generally in same data centre or campus	4. Can run standalone if internet connection is lost
5. Restricted functionality without controller link	5. Typical subscription-based pricing model
6. It has lower latency for local traffic	6. Simpler remote management and multi-site rollout
7. Better adapted to environments where local data processing is needed	7. Self-healing updates and feature deployment
8. Generally higher up-front investment (controller hardware)	8. Lower initial cost but continuous subscription charges

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

Ans: CAPWAP Tunnel Maintenance:-

1. CAPWAP tunnel is established after AP finds the WLC.
2. Tunnel is kept alive by periodic keepalives (echo requests).
3. If WLC is inaccessible or doesn't answer, AP retries or restarts.
4. Tunnel supports safe, encrypted data flow and management

6. What is the difference between Sniffer and monitor mode, use case for each mode

Sniffer Mode:	**Monitor Mode:**
• AP works as a stand-alone packet capture device	• AP maintains normal operation while monitoring the RF environment
• Sends all the captured packets to an outboard analysis system	• Can serve clients while monitoring
• Does not support servicing clients in sniffer mode	• Primarily used for ongoing spectrum analysis and RF optimization
• Mainly employed for problem-specific troubleshooting	• Provides statistics rather than full packet captures
• Captures whole 802.11 frames including headers	• Identifies interference, channel utilization, and neighbouring networks
• Usually plugged into network analysis tools	• Used for automatic RF adjustments (power, channel selection)
• Valuable in security auditing and intrusion detection	• Less resource-intensive than full packet capture
• Can be programmed to only focus on unique channels or frequencies	• Part of normal operation in enterprise Wi-Fi systems

Use cases for Sniffer Mode:

- Troubleshooting client connectivity issues
- Analysing authentication failures
- Detecting rogue APs and security threats

Use cases for Monitor Mode:

- Continuous RF environment assessment
- Automatic channel selection and power adjustment
- Interference detection and classification

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

Ans: Best AP Mode for WLC Deployed Across WAN is FlexConnect mode.

When deploying branch offices with a central WLC connected by a wide area network, this option is utilized. In this mode, APs are still managed and controlled centrally by the WLC, but they are able to locally switch client data traffic at the branch.

It is best because:

- **Local data switching:** IT reduces latency and preserves WAN capacity by keeping client traffic inside the local network rather than tunnelling it over the WAN.
- **WAN redundancy:** APs can use locally determined parameters to continue offering wireless services in the event that the WAN link breaks.
- A**daptability in authentication:** If WAN is available, central authentication may be used; if not, local authentication can be used.

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

Ans: Some significant challenges are:

- **Configuration management:** APs need to be individually configured and updated
- **Unreliable policies:** Difficulty implementing consistent security and access policies
- **No single point of monitoring:** Need to monitor each AP independently for issues
- **Difficult troubleshooting:** No one view of the wireless network
- **Manual firmware updates:** Time-consuming to update each AP independently
- **Limited roaming:** AP-to-AP transitions are not necessarily seamless
- **Radio coordination issues:** No automatic RF management of APs
- **Security risks:** Too easy to miss critical security patches

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

Ans: Following things can happen:

1. In Local Mode, AP relies on WLC for control as well as data.
2. When WLC fails, AP loses management/control functions.
3. Current clients can remain briefly connected, yet new connections drop and data forwarding stops.
4. AP can reboot or go into recovery mode if WLC is still inaccessible.