Wi-Fi Training Program

Module 2 Assignment Answers

Siddharth Balaji

Q1. Brief about SplitMAC architecture ad how it improves the AP's performance.

SplitMAC architecture is a concept used to split the functionality of the MAC layer between the Access Point (AP) and a central Wireless LAN Controller (WLC).

It is used in enterprise grade Wi-Fi solutions.

The AP will handle real-time operations which are:

- ACKs
- frame retransmissions
- beaconing
- and encryption/decryption

WLC handles:

- client authentication
- roaming control
- and load balancing.

SpliMAC's contribution to improve performance:

Centralized Management:
WLC can manage multiple Aps which allows for centralized policy enforcement, security management, and software updates which will make the network more scalable and efficient.

Enhanced Roaming:
Faster and smoother client roaming is possible since the WLC has a global view of the network and can make optimized roaming decisions.

Enhanced Scalability:
The APs are lightweight (LWAPs), simpler and can be deployed in large numbers with minimal configuration.

Better Load Balancing & RF Management:
The WLC can monitor the RF environment and client loads across APs to optimize channel allocation and balance traffic.

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

CAPWAP stands for Control and Provisioning of Wireless Access Points.

It's a network protocol that enables Lightweight Access Points (LWAPs) to communicate with a Wireless LAN Controller (WLC).

1. Discovery Phase:

The AP will find the WLC using any of the following methods:

1. DHCP Option 43
2. DNS (CISCO-CAPWAP-CONTROLLER)
3. Broadcast or pre-configured IP

2. Join Request / Response:

- AP sends a CAPWAP Join Request to WLC.
- WLC validates the APand respondss with a Join Response.

3. Authentication & Configuration:

- In case the AP is outdated, the WLC pushes the correct firmware information.
- AP and WLC exchange certificates or shared keys.
- WLC sends config info such as SSID, channels, transmit power and VLAN settings to the AP.

4. Data Tunnel is established:

- A separate CAPWAP data tunnel is formed for client traffic.
- The AP can now forward the client data through the CAPWAP tunnel.
- Now the AP is fully functional and can serve clients.

Q3. Where does CAPWAP fit in the OSI model? What are the two tunnels in CAPWAP and their purpose?

CAPWAP is used in Layer 3 (Network) and Layer 4 (Transport).

In Layer3, it uses IP for routing between AP and WLC.

In layer 4, it uses UDP port 5246 for control and port 5247 for data tunnels.

<u>The two tunnels in CAPWAP are:</u>

CONTROL TUNNEL:

- It uses UDP 5246.
- It encrypts and secures the communication between the AP and WLC.
- It handles management traffic such as AP discovery, joining, configuration and keepalives.

DATA TUNNEL:

- It uses UDP 5247.
- It carries client data traffic between the AP and WLC (directly to LAN or forward to WLC).

Q4. Difference between Lightweight APs and Cloud-based Aps.

FEATURE	LIGHTWEIGHT APs	CLOUD-BASED APs
Controller	On-site WLCs are required	Cloud-based controller at cloud vendor's data centre
Management	Centralised using on-site WLC	Centralised remote management using cloud dashboard
Scalability	Limited to the capacity of WLC	It is highly scalable irrespective of location
Deployment of complexity	Requires expertise in network engineering	It is easy as it follows plug-and-play.
Cost	High as initial hardware investment on WLC is required	Low cost as it is subscription based.
Maintenance	Done by network admins locally.	It is automated via cloud.

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

The CAPWAP tunnel is maintained through the following mechanisms:

KEEPALIVE MESSAGES:
The AP and WLC exchange keepalive messages periodically over control tunnel.
The default interval is 30 seconds but can be configured as per need.
If WLC doesn't respond to three keepalives then it is considered to be down. Now, the AP attempts to reconnect with it.

DTLS ENCRYPTION:
Datagram Transport Layer Security is used to secure the CAPWAP control tunnel.
DTLS is maintained to protect traffic.

HEARTBEAT TIMER:
It is also called echo interval and both the AP and LWC maintain timers to monitor the tunnel health.
If a response is not received within the time interval, it s assumed that the AP is unreachable.

AUTOMATIC REJOIN:
If the CAPWAP tunnel is dropped, a new join request is sent and will attempt to reconnect.

Q6. Difference between Sniffer and Monitor Mode, and Use Cases

MODE	DESCRIPTION	USE CASE
SNIFFER	AP captures and forwards 802.11 packets for analysis	Wireless packet analysis and troubleshooting
MONITOR	AP detects and reports on wireless threats, rogue APs, and interferences.	Wireless security, rogue AP detection and intrusion detection

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

The ideal AP mode is FlexConnect mode is best suited.

FlexConnect is specifically designed for remote or branch offices.

Specifically, WLC is located in a central data centre and the AP is in a remote local network.

- It allows local switching of client traffic and provides centralized management.
- There are other modes like local, monitor and sniffer which are not suited for this scenario.

Q8. Challenges of deploying more than 5 autonomous APs in large network like a universities.

NO CENTRALISED MONITORING:
Without centralised monitoring, it is tough to monitor, troubleshoot and detect client connection issues, signal strength, and network health.

COMPLEX CONFIGURATION AND MANAGEMENT:
Each AP has to be configured one by one and ensure that each one is updated manually.

RF INTERFERENCE AND CHANNEL MANAGEMENT:
Often, the APs will overlap on the same channels and interference.

SCALABILITY ISSUES:
When a large number of APs are added to the network, the overhead of managing each AP increases.

SECURITY CONCERNS:
Applying the same policy manually to each AP is difficult and mistakes during this will lead to vulnerabilities.

CLIENT ROAMING:
APs will not communicate with each other and clients will experience disconnection and latency.

Q9. What happens when the WLC goes down while a wireless client is connected to a Lightweight AP in local mode?

- The CAPWAP control tunnel between the LWAP and the WLC is lost.
- Already connected client may stay connected for a short while but will face low network access.
- Authentication is not available.
- New DHCP assignments cannot be made.
- No roaming across APs
- AP will enter recovery mode and stop serving clients and will send a discover message to join another controller.