Module 2 Assignment answers

Sri Gnana Saravan.N

VIT Chennai

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

Solution:

SplitMAC Architecture:

• The Lightweight AP distributes functions between the Controller (WLC) and the AP at the MAC layer.

• The AP performs real-time functions (such as 802.11 RF actions).

• WLC deals with more complex procedures (such as authentication, roaming, and policy security).

Functions at Controller	**Functions at AP**
Authentication (AAA)	Frame acknowledgement
Association management	Beacon and probe response
Client IP assignment	Retransmissions
Policy enforcement	Basic encryption/decryption

Performance Improvement:

• Alters MAC architecture, thus reducing load on the APs.

• Built-in intelligence leads to streamlined efficiency in network management.

• Economical deployment and maintenance due to lightweight APs.

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

Solution:

CAPWAP (Control and Provisioning of Wireless Access Points):

- A protocol that standardizes how Lightweight APs and Controllers communicate.
- Encapsulates both Control messages and Data traffic between AP and WLC.

Flow:

1. AP Bootup ➔ DHCP (get IP address).
2. Discovery ➔ AP finds WLC (through broadcast, DNS, or DHCP option 43).
3. DTLS Setup ➔ Secure control tunnel established (encrypts control messages).
4. Join ➔ AP sends a Join Request, WLC sends Join Response.
5. Image Download ➔ If needed, AP gets firmware update.
6. Configuration ➔ WLC pushes SSIDs, security settings, policies.
7. Data Traffic ➔ CAPWAP data tunnel established for client traffic (optional, depending on AP mode).

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

Solution:

- Operates mainly at Layer 2 (Data Link) and Layer 3 (Network).
- Uses UDP transport (ports 5246 for control, 5247 for data).
- Control Tunnel — Carries AP management messages (config, firmware updates, keepalive).
- Data Tunnel — Carries actual client traffic (802.11 data frames) encapsulated inside IP/UDP packets.

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

Solution:

Feature	**Lightweight AP**	**Cloud-based AP**
Management	On-premises WLC	Cloud Controller
Control Tunnel	CAPWAP to WLC	HTTPS or similar to Cloud
Data Tunnel	CAPWAP to WLC	Local breakout (data remains at site)
Controller Hardware	Needed	Not needed (hosted in cloud)
Suitable for	Centralized environments (campus)	Distributed enterprises (multiple branches)

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

Solution:

- AP and WLC establish DTLS-secured tunnels.
- Keepalive messages are exchanged periodically over the Control Tunnel.
- If no response from WLC within a timeout period, AP will try to re-discover and rejoin a WLC.
- CAPWAP tunnels automatically renegotiate after failovers or WLC upgrades.

6. Whats the difference between Sniffer and monitor mode , use case for each mode?

Solution:

Feature	**Sniffer Mode**	**Monitor Mode**
BSS/SSID	Not broadcasted	Not broadcasted
Function	Capture raw 802.11 frames for analysis	Scan for rogue APs, client behavior, interference
Output	Packet data to Wireshark or server	Security and health telemetry to WLC
Use Case	Troubleshooting wireless issues	Wireless security, spectrum monitoring

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

Solution:

Best Mode:
FlexConnect Mode

Why FlexConnect?

- If WLC is far away (WAN), AP can:
    - Switch traffic locally (no need to send data over WAN to WLC).
    - Authenticate users locally even if WAN fails.
- Reduces WAN bandwidth usage.
- Increases reliability at branch offices.

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

Solution:

Challenges:

- **Manual Configuration**: Every AP must be individually configured — very time-consuming.
- **Firmware Upgrades**: Difficult to update all APs simultaneously.
- **Roaming Issues**: Seamless client roaming is hard to achieve without central control.
- **Security**: No centralized security policies — increased risk.
- **Monitoring**: Hard to troubleshoot or monitor network-wide events.
- **Scalability**: Adding more APs means more manual work.
- **Load Balancing**: Hard to balance client loads across APs manually.

Better Solution: Use Lightweight APs with a WLC or Cloud-managed APs.

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

Solution:

- AP loses connection to WLC.
- CAPWAP tunnels are down.
- AP stops serving clients.
- Wireless clients get disconnected because AP cannot continue operations without WLC (in Local Mode).
- AP tries to re-discover and rejoin WLC.
- If WLC comes back up, AP and clients can reconnect.
- If AP was in FlexConnect mode with local switching, clients would NOT get disconnected even if WLC went down.