Name: J Kevin Immanuel
College: VIT Chennai

WIFI ASSESSMENT MODULE 2

Q1) Split mac architecture:

This architecture refers to a wifi design where the MAC layer is divided between two devices:
i) Access point (AP)
ii) Wireless LAN Controller (WLC)

There are mainly two functions performed by this architecture:

1) Time critical functions:

This function is performed by access point (AP). It handles low-latency operations like encryption/decryption, ACK and NACK, retransmissions.

2) Management/control functions:

This is performed by the WLC. It manages things like authentication, roaming, QOS, RF management and AP configs.

Improvement of AP performance:

1) Offloads control tasks.

Management and controltasks are performed by WLC. This frees up the AP's resources to focus on real time data transmissions, improving performance.

2) Lower latency due to less AP overhead:

With less control overhead on AP, there is more room for data traffic, leading to lower latency, high throughput and few transmissions.

Q2) CAPWAP and flow between AP and controller

CAPWAP - Control and Provisioning of Wireless Access Points.
It is a protocol that enables an access controller to manage a collection of wireless termination points

Goals of CAPWAP:

1) To centralize authentication and policy enforcement functions in wireless networks.
2) To shift higher-level protocol processing away from access points (APs).
3) To provide an extensible protocol that could be used with various types of APs

How does CAPWAP work:

First there is discovery phase. AP broadcasts discovery request message to find a controller. Controller sends response message and AP and controller create connection through Datagram Transport Layer Security protocol to exchange CAPWAP control and data messages.

Control messages contain information and instructions related to wireless local area network (WLAN) management. Data messages encapsulate forwarded wireless frames. Each is sent over a different User Datagram Protocol port.

CAPWAP has two modes of operations:

1) Split MAC
2) Local MAC

In split MAC mode, the CAPWAP protocol encapsulates all Layer 2 wireless data and management frames, which are then exchanged between the controller and AP. Local MAC mode enables data frames to be locally bridged or tunneled as Ethernet frames.

In either mode, the AP processes Layer 2 wireless management frames locally and then forwards them to the controller.

Q3) CAPWAP fits in which OSI layer? What are the two tunnels in CAPWAP and its purpose.

CAPWAP fits in the Layer 3 - Network Layer

There are two tunnels in CAPWAP : Control tunnel and Data tunnel.

Control tunnel: Control messages contain information and instructions related to wireless local area network (WLAN) management

Data tunnel: Data messages encapsulate forwarded wireless frames. Each is sent over a different User Datagram Protocol port

Q4) What is the difference between lightweight AP and Cloud-based AP?

1) Control location of Lightweight AP is managed by an on-premise WLC, whereas Cloud based AP control location is managed by cloud
2) Tunnels: Lightweight uses CAPWAP tunnels, cloud based uses HTTPS or proprietary protocols
3) Configuration: Lightweight AP config is pushed from WLC, cloud based AP config is pushed from cloud dashboard
4) Management access: Lightweight AP has no local ui and all the configs are through the controller, whereas a cloud based AP is managed through the cloud dashboard
5) Deployment: Lightweight AP requires a WLC to be installed and maintained, whereas a Cloud based AP does not require any controller and only needs internet access
6) Usecase: Enterprise environment with centralized control(Lightweight AP), Branched networks with minimal on-site IT (Cloud based AP).

Q5) How is CAPWAP tunnel maintained between AP and Controller?

First there is discovery phase. AP broadcasts discovery request message to find a controller. Controller sends response message and AP and controller create connection through Datagram Transport Layer Security protocol to exchange CAPWAP control and data messages.

To maintain the state of a CAPWAP tunnel, both ends of the tunnel periodically exchange different packets to detect tunnel connectivity.

1) Keepalive packets for a CAPWAP data tunnel (on the UDP port 5247)
2) Echo packets for a CAPWAP control tunnel (on the UDP port 5246)

Q6) What is the difference between sniffer and monitor mode. What are the use cases for each mode?

Sniffer mode:

An AP in sniffer mode dedicates its time to receive 802.11 wireless frames. The AP becomes a remote wireless sniffer; you can connect to it from your PC with an application like Wildpackets Omnipeek or Wireshark. This can be useful if you want to troubleshoot a problem and you can't be on-site. When an AP is in sniffer mode, it won't broadcast an SSID so clients can't connect to the AP.

Use case: Used for packet analysis in enterprise environments.

Monitor mode:

An AP in monitor mode doesn't transmit at all. It's a dedicated sensor that:

1) Checks Intrusion Detection System (IDS) events
2) Detects rogue APs
3) Determines the position of wireless stations

Because the AP is only in monitor mode, it won't broadcast an SSID so clients are unable to connect to the AP.

Use case: Used for intrusion detection and site surveys.

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

FlexConnect AP mode enables switching traffic between an SSID and a VLAN locally if the CAPWAP to the WLC is down, even when the AP is at a remote site. It can also be configured to egress at the access point's LAN port.

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

1) **Security**: Ensuring the network is secure and that autonomous functions do not introduce vulnerabilities.

2) **Scalability**: The network should be able to handle increasing demands without compromising performance.

3) **Interoperability**: Compatibility with existing systems and devices to ensure seamless operation.

4) **Compliance**: Meeting regulatory requirements and industry standards to avoid legal issues.

5) **Monitoring and Management**: Establishing tools and processes to monitor and manage the autonomous network effectively.

6) **Training and Skill Development**: Ensuring that staff are trained to understand and work with autonomous network technologies.

7) **Failover and Redundancy**: Implementing failover mechanisms and redundancies to prevent widespread network outages.

8) **Resource Optimization**: Ensuring resources are efficiently allocated and utilized within the network.

9) **Data Privacy**: Safeguarding sensitive data and ensuring proper handling and storage.

10) **Cost Considerations**: Evaluating the costs associated with deploying and maintaining autonomous networks.

Q9) What happens to a client connected to lightweight AP in local mode when the WLC goes down?

SInce the lightweight AP is in local mode and local mode relies on a separate WLC, if the WLC goes down, then there will be no network access to the wireless client.