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

SplitMAC (Split Media Access Control) is a wireless network architecture that separates the MAC layer functionalities of a wireless access point (AP) into two parts:

Lower MAC (L-MAC)

- Resides on the Access Point (AP) hardware.
- Handles time-critical tasks like frame transmission/reception, ACKs, RTS/CTS, and contention resolution.
- Must operate with minimal latency.

Upper MAC (U-MAC)

- Resides on a central wireless controller (WLC).
- Handles non-time-critical tasks, such as authentication, association, roaming decisions, encryption key management, QoS policies, and configuration.

How SplitMAC Improves AP Performance

- By moving heavy and complex tasks like authentication and policy enforcement to a centralized controller, the AP can focus on efficient data transmission and real-time media handling.
- The WLC can make intelligent decisions across the entire wireless network, such as load balancing users across APs or coordinating handoffs during roaming.
- APs become lightweight (LWAPs), making them cheaper and easier to maintain. Firmware and policies can be centrally updated.
- Since most processing is offloaded to the controller, large numbers of APs can be deployed without overloading individual units.
- Centralized security policies (e.g., ACLs, encryption key handling) are harder to compromise at the AP level, improving the overall security posture.

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

CAPWAP (Control and Provisioning of Wireless Access Points) is a tunneling protocol that facilitates communication between lightweight access points (APs) and a centralized wireless LAN controller (WLC) over an IP network. The CAPWAP process begins with the discovery phase, where the AP locates the WLC using methods such as DHCP Option 43, DNS resolution (e.g., CISCO-CAPWAP-CONTROLLER.local), or static configuration. Once the WLC is discovered, the join phase is initiated, where the AP sends a CAPWAP Join Request. The WLC then authenticates the AP and responds with a Join Response. If the AP’s firmware version is not aligned with the controller’s requirements, the configuration and image download phase follows, during which the WLC updates the AP’s firmware and pushes configuration settings like SSID definitions, security policies, and VLAN mappings. After successful configuration, the AP transitions to the data transfer and management phase, where it begins forwarding client data through the secure CAPWAP tunnel while continuing to exchange control messages with the WLC for ongoing monitoring, policy enforcement, and management. This architecture ensures centralized control, simplified AP management, and enhanced scalability in enterprise wireless networks.

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

CAPWAP operates at Layer 3 (Network Layer) of the OSI model and uses UDP as its transport protocol to encapsulate both management and data traffic between lightweight access points (APs) and the wireless LAN controller (WLC). It establishes two separate tunnels: one for control traffic and another for data traffic. The control tunnel, which uses UDP port 5246, is responsible for encrypting and securing communication between the AP and the WLC. This tunnel carries management traffic such as AP authentication, configuration settings, firmware updates, and monitoring data, ensuring that control communications are isolated and protected from data transmissions.

The data tunnel, operating over UDP port 5247, handles the actual client data traffic. This tunnel can be configured for two types of switching modes: centralized switching, where all client traffic is tunneled back to the WLC for processing and policy enforcement, and local switching, where client traffic is bridged directly onto the local network by the AP without passing through the controller. This flexibility allows network administrators to balance between centralized control and optimal data routing based on deployment needs and performance considerations.

4. Difference between Lightweight APs and Cloud-based APs

Lightweight Access Points (APs) and Cloud-based APs differ significantly in their architecture and management approach. Lightweight APs rely on an on-premises Wireless LAN Controller (WLC) for centralized management within the local network. This setup typically involves a high initial investment in controller hardware and requires network engineering expertise for deployment and maintenance. Scalability is constrained by the capacity of the WLC, and network latency can vary depending on the physical location of the controller relative to the APs.

In contrast, Cloud-based APs are managed via a cloud-hosted controller, offering remote management through a web-based dashboard. This model supports greater scalability, making it suitable for organizations with multiple locations. The initial setup is simpler and more cost-effective, as it eliminates the need for dedicated controller hardware, instead using a subscription-based pricing model. Additionally, cloud infrastructure typically offers lower latency and improved performance, thanks to its distributed nature and global availability zones.

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

The CAPWAP tunnel is sustained through multiple mechanisms designed to ensure reliability and security in AP-to-controller communication. One key method is the use of heartbeat messages (keepalives), where the AP periodically sends signals to the WLC to confirm connectivity. If the WLC does not respond within a specified timeframe, the AP will attempt to reconnect or fail over to a backup controller, if one is configured. To maintain a secure connection, DTLS encryption is used for both the control and data tunnels, protecting management and client data traffic. The control tunnel handles communication between the WLC and AP for tasks such as configuration and monitoring, while the data tunnel is responsible for transporting client traffic. These tunnels, combined with failover mechanisms, ensure that network operations continue smoothly even in the event of controller unavailability.

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

Access Points (APs) can operate in specialized modes such as Sniffer Mode and Monitor Mode, each serving distinct purposes in network diagnostics and security. In Sniffer Mode, the AP captures raw 802.11 wireless frames and forwards them to a packet analysis tool like Wireshark. This mode is particularly useful for troubleshooting network issues, conducting security audits, and performing detailed packet analysis. On the other hand, Monitor Mode disables client connectivity and enables the AP to scan across all Wi-Fi channels. This allows it to detect rogue access points, identify sources of interference, and support RF (radio frequency) optimization. It is commonly used in wireless intrusion detection systems (WIDS) and for maintaining overall wireless network health and security.

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

FlexConnect Mode is an ideal solution for maintaining network continuity, especially in remote or branch office deployments. It enables access points to continue serving clients even if the connection to the Wireless LAN Controller (WLC) is lost, ensuring uninterrupted service. FlexConnect supports local authentication and local switching, which significantly reduces dependency on WAN connectivity by allowing traffic to be processed locally instead of being tunneled back to the controller. Additionally, it includes failover mechanisms that enhance network resilience and help maintain uptime during connectivity disruptions with the central controller.

8. Challenges of Deploying More than 50 Autonomous APs in a Large Network like a University

Deploying standalone access points without a centralized controller introduces several challenges that can impact network efficiency and reliability. Configuration overhead is a major concern, as each AP must be manually set up, leading to increased deployment time and complexity. The absence of centralized management makes troubleshooting and monitoring more difficult, requiring administrators to manage each device individually. Additionally, client roaming becomes problematic, with users potentially experiencing disconnections when moving between APs. Without coordinated control, RF interference and channel management suffer, as APs may not effectively regulate transmission power or select optimal channels, resulting in signal overlap and interference. Security management also becomes inconsistent, as it's challenging to enforce uniform security policies across multiple devices. Finally, scalability becomes a significant issue, as adding more APs complicates efforts to maintain seamless connectivity and consistent network performance.

9. What happens when the WLC goes down while a wireless client is connected to a Lightweight AP in localmode?

If the Wireless LAN Controller (WLC) becomes unavailable, existing clients typically remain connected, but their network access may be limited, especially for services that rely on controller communication. New client connections fail, as the processes of authentication and association require an active WLC. Additionally, client roaming between APs may not function properly, potentially leading to session drops and disconnections. In response to the loss of connectivity, some APs may reboot and attempt to connect to a backup WLC, if one has been configured. While local switching can still enable internal communication within the network, internet access and external services may be disrupted depending on the network configuration.