**VISHAL G WIFI ASSIGNMENT MOD 2**

**1. Brief about SplitMAC architecture and how it improves the AP's performance, give humanised answer in third person**

SplitMAC architecture is a networking approach that divides the functions of a traditional access point (AP) between the AP itself and a centralized wireless LAN controller (WLC). Instead of handling everything on the AP, tasks like encryption, frame management, and policy enforcement are split between the AP and the controller.

This setup significantly improves the AP’s performance by reducing its processing load. Since the controller manages complex tasks like authentication, roaming, and traffic management, the AP can focus on efficiently handling wireless signals and forwarding data. This leads to better scalability, improved security, and smoother roaming experiences for users. Additionally, centralizing management simplifies network administration, making it easier to implement updates, enforce policies, and optimize performance across multiple APs.

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

CAPWAP (Control and Provisioning of Wireless Access Points)

CAPWAP is a network protocol that allows a centralized Wireless LAN Controller (WLC) to manage multiple lightweight Access Points (APs) efficiently. It standardizes the communication between APs and controllers, ensuring security, scalability, and simplified network management. CAPWAP operates over UDP and supports both control and data plane traffic, typically using:

Control Channel (UDP 5246) – Securely exchanges management information (e.g., configuration, authentication).

Data Channel (UDP 5247) – Handles actual user traffic between the AP and the WLC.

**Flow Between AP and Controller in CAPWAP**

**Discover Phase:**

The Access Point (AP) boots up and begins searching for a Wireless LAN Controller (WLC). It can discover the controller through various methods such as broadcasting, DHCP options, or DNS resolution. Once an available controller is identified, the AP initiates a connection to establish communication.

**Join Phase:**

The AP undergoes authentication with the WLC to verify its legitimacy. A CAPWAP tunnel is then established, ensuring secure communication between the two. The controller validates the AP’s credentials before permitting further interactions, ensuring that only authorized APs are integrated into the network.

**Configuration phase:**

The WLC provisions the AP with essential operational settings, including SSIDs, security policies, and Quality of Service (QoS) parameters. If the AP’s software is outdated, it downloads and installs the necessary firmware updates to maintain compatibility and security.

**Data Exchange Phase:**

The AP starts forwarding user data through the CAPWAP tunnel, while the WLC manages key network functions such as authentication, traffic handling, and seamless roaming. This division of tasks ensures efficient performance, with the AP focusing on radio transmission while the controller manages higher-level network operations.

**Monitoring and management phase:**

The WLC continuously oversees AP performance, dynamically adjusting configurations to optimize efficiency. If an AP experiences failure, the controller redistributes its workload, minimizing service disruption and ensuring network stability.

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

CAPWAP primarily operates at Layer 3 (Network Layer) of the OSI model. It encapsulates wireless management and data traffic within UDP packets, allowing communication between Access Points (APs) and Wireless LAN Controllers (WLCs) over IP networks. While CAPWAP can also function at Layer 2 (Data Link Layer) in local deployments, its design is optimized for Layer 3, enabling centralized AP management across distributed networks.

**Two Tunnels in CAPWAP and Their Purpose**

CAPWAP establishes two separate tunnels between the AP and the WLC: the Control Tunnel and the Data Tunnel.

The Control Tunnel (UDP Port 5246) is responsible for exchanging management and control information between the AP and WLC. This tunnel is encrypted to secure configuration updates, authentication, and AP monitoring. It ensures that sensitive network policies and settings remain protected from potential security threats.

The Data Tunnel (UDP Port 5247) handles actual user data traffic between the AP and WLC. This tunnel is responsible for forwarding packets while ensuring authentication and policy enforcement. Encryption in the data tunnel is optional to reduce processing overhead, depending on the network's security requirements.

By separating control and data traffic, CAPWAP enhances security, reduces the processing load on APs, and improves overall network scalability, making wireless deployments more efficient and manageable.

**4. What’s the difference between Lightweight APs and Cloud-based APs**

Lightweight APs rely on an on-premises Wireless LAN Controller (WLC) to manage configurations, security policies, and traffic flow. They act as radio transmitters while the controller handles decision-making and traffic processing. In contrast, cloud-based APs are managed through a cloud-hosted controller, eliminating the need for on-premises hardware. Configuration, monitoring, and updates are performed remotely via a web-based or mobile interface.

Lightweight APs require a local controller, which means they work best in enterprise environments with centralized management and on-site IT teams. On the other hand, cloud-based APs can be deployed anywhere with internet access, making them ideal for distributed offices, remote locations, and businesses that need easy scalability.

When it comes to maintenance and updates, lightweight APs depend on IT teams to manually update firmware and manage configurations through the WLC. Cloud-based APs, however, receive automatic updates and configurations from the cloud, reducing the need for on-site maintenance and ensuring that the system is always up to date.

Scalability is another key difference. Lightweight APs scale by adding more APs, but each must connect to a WLC, which may require additional licensing or hardware expansion. Cloud-based APs, however, scale effortlessly by registering new APs to the cloud dashboard without requiring additional physical infrastructure.

Security and data handling also differ between the two. Lightweight APs use encrypted CAPWAP tunnels to send data to the controller, ensuring secure communication within the network. Cloud-based APs may route traffic locally but rely on cloud security measures, such as firewalls and access controls, to protect the network from potential threats.

Cost considerations play a significant role in the choice between these two architectures. Lightweight APs require an initial investment in WLC hardware and licensing, leading to higher upfront costs but no recurring cloud subscription fees. Cloud-based APs, on the other hand, often operate on a subscription model, reducing initial costs but adding long-term operational expenses.

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

The CAPWAP tunnel between an Access Point (AP) and a Wireless LAN Controller (WLC) is maintained through continuous communication and periodic control messages. This ensures the AP remains connected to the controller and can receive configurations, security policies, and updates.

Once the AP successfully discovers and joins the WLC, it establishes two separate CAPWAP tunnels: one for control traffic (UDP port 5246) and another for data traffic (UDP port 5247). The control tunnel remains active at all times, even when no client data is being transmitted. This tunnel is encrypted to ensure secure communication and prevent unauthorized access.

To maintain the tunnel, the AP and WLC exchange heartbeat messages (keepalive packets) at regular intervals. These messages confirm that the connection is still active. If the WLC does not receive a heartbeat response from the AP within a predefined timeout period, it assumes the AP is unreachable and may trigger reconnection attempts or failover mechanisms.

In case of network disruptions or temporary connectivity issues, CAPWAP includes mechanisms for tunnel re-establishment. If an AP loses its connection to the WLC, it will attempt to reconnect automatically using the discovery process. If multiple controllers are available, the AP can fail over to a secondary WLC to ensure continuous service.

Additionally, CAPWAP supports Dynamic Channel Assignment and Load Balancing, allowing the controller to adjust AP configurations in real time. This helps maintain optimal performance and reliability within the wireless network.

**6. What’s the difference between Sniffer and monitor mode, use case for each mode**

Sniffer mode and monitor mode are both used for capturing wireless network traffic, but they serve different purposes and operate at different levels.

In sniffer mode, an Access Point (AP) captures wireless traffic and forwards it to a Wireless LAN Controller (WLC) or a network analyzer for monitoring and analysis. The AP remains connected to the network and can selectively capture packets for troubleshooting, security auditing, or performance analysis. Since it operates as part of the network, sniffer mode does not disrupt regular Wi-Fi operations.

In monitor mode, a wireless adapter or AP captures all wireless traffic on a particular channel without being connected to any network. It passively listens to all frames, including management, control, and data packets, even if they are not addressed to it. This makes monitor mode useful for security assessments, network forensics, and detecting rogue APs or unauthorized devices. Unlike sniffer mode, monitor mode does not interact with the network, making it more suitable for passive surveillance.

While both modes are used for capturing wireless traffic, sniffer mode is more suited for active troubleshooting and performance analysis within a managed network, whereas monitor mode is ideal for passive security analysis and forensic investigations.

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

If the Wireless LAN Controller (WLC) is deployed over the WAN, the best AP mode for local network operation is FlexConnect Mode (formerly known as H-REAP, Hybrid Remote Edge AP).

In FlexConnect mode, the AP can locally switch client traffic without sending it to the WLC. This reduces WAN dependency and prevents latency issues caused by routing all data through the remote WLC. When the AP has connectivity with the WLC over WAN, it behaves like a lightweight AP, with the controller managing authentication, policy enforcement, and SSID settings.

If WAN connectivity to the WLC fails, the AP continues operating independently in standalone mode. It maintains local authentication (if configured) and ensures that wireless services remain active without network disruption. This allows clients to stay connected even when the WLC is unreachable.

FlexConnect minimizes WAN traffic by sending only control traffic to the WLC while locally forwarding user data. This approach ensures network continuity and reduces latency, improving performance for users in the local network. Since it does not require constant communication with the controller, it also optimizes bandwidth usage, making it more efficient for branch offices and remote sites.

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

**Lack of Centralized Management**

Each autonomous AP must be configured and managed individually, which increases administrative overhead. Updates, security policies, and SSID changes must be manually applied to each AP, making network maintenance complex and time-consuming.

**Roaming Issues**

Since each AP operates independently, seamless roaming between APs is not efficient. Students and staff moving across campus may experience frequent disconnections or authentication delays, affecting the user experience for applications like video conferencing or VoIP calls.

**Channel and Interference Management**

Without a central controller, APs cannot dynamically adjust channels to avoid interference. Manual configuration is required to prevent co-channel interference, which can degrade network performance due to overlapping frequencies.

**Security and Policy Enforcement**

Implementing consistent security policies, such as WPA3 authentication, VLAN segmentation, and access control, becomes difficult across multiple autonomous APs. Any misconfiguration in one AP could lead to security vulnerabilities or unauthorized access.

**Bandwidth and Load Balancing**

Autonomous APs lack load balancing capabilities. If too many users connect to a single AP while others remain underutilized, network congestion occurs, leading to slow speeds and reduced service quality.

**Network Scalability**

As the number of APs increases, maintaining a scalable and efficient network becomes difficult. Manually adjusting power levels, SSIDs, and frequency bands for every AP does not scale well, making future expansions more challenging.

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

If a wireless client is connected to a lightweight AP running in local mode and the WLC goes down, the impact can be significant since the AP heavily relies on the controller for key functions like authentication, policy enforcement, and traffic forwarding.

One of the first issues that arise is that new clients trying to connect to the network will fail authentication. Since the AP depends on the WLC to verify credentials, it cannot handle authentication requests on its own. If DHCP is managed by the WLC, clients may also fail to get an IP address, leaving them unable to access the network.

For clients that are already connected, the experience varies depending on how traffic is handled. If the network is using central switching, where all data is tunneled through the WLC, those clients will lose connectivity since there is no longer a path for their traffic. In some cases, clients might remain connected for a short while, but eventually, sessions will drop, especially for real-time applications like video calls or VoIP.

Roaming between APs also becomes a problem because the WLC plays a crucial role in ensuring seamless handovers between access points. Without the controller, devices moving across different APs may experience connection drops or interruptions in service, which can be particularly frustrating for users on active calls or streaming.

If the network is designed with a backup WLC, the APs will try to reconnect to the secondary controller. In this case, service can resume with minimal disruption. However, if there is no failover mechanism in place, clients will be disconnected until the primary WLC is restored.