Wifi Training Assignment 2

- Yuvan Shankar G

Problem1:

- Divides MAC layer tasks between AP and central controller.
- AP handles time-sensitive tasks like acknowledgments, retransmissions, and beaconing.
- Controller manages client authentication, roaming, security policies, and load balancing.
- Reduces processing burden on AP, improving performance.
- Enhances scalability by allowing more APs without overloading individual units.
- Simplifies AP design, making them more cost-effective.
- Enables centralized management for easier configuration and troubleshooting.
- Provides better roaming experience with controller-managed handoffs.
- Improves network-wide load balancing and channel optimization.
- Enhances security with centralized policy control and faster threat response.

Problem2:

- AP powers on and sends a discovery request to find available controllers.
- Controller responds with a discovery response.
- AP selects a controller based on priority or response criteria.
- AP and controller establish a secure DTLS tunnel for communication.
- AP sends a join request to the controller.
- Controller authenticates the AP and sends a join response.
- AP downloads its configuration from the controller, including SSIDs, security settings, and channel information.
- AP and controller exchange keep-alive messages to ensure the connection is active.
- Client traffic and management frames are tunneled through CAPWAP between AP and controller.
- Controller centrally manages client authentication, security policies, and traffic forwarding decisions.

Problem3:

- CAPWAP operates at Layer 2 (Data Link Layer) and Layer 3 (Network Layer) of the OSI model.
- Uses UDP as the transport protocol.
- Two tunnels are established in CAPWAP: Control Tunnel and Data Tunnel.
- Control Tunnel uses UDP port 5246.
- Data Tunnel uses UDP port 5247.
- Control Tunnel carries management and configuration messages between AP and controller.
- Control Tunnel is secured with DTLS encryption.
- Data Tunnel carries actual client data traffic between AP and controller.

- Data Tunnel can be encrypted for confidentiality.
- Separation of tunnels improves security and network efficiency.
- Control Tunnel remains active for continuous AP management even without client data.
- Data Tunnel handles user traffic and can be bypassed if local switching is configured.

Problem4:

- Lightweight APs require an on-premises physical controller to manage and configure them.
- Cloud-based APs are managed through a cloud controller accessible over the internet.
- Lightweight APs use protocols like CAPWAP to communicate with the physical controller.
- Cloud-based APs use secure cloud APIs and tunnels to connect with the cloud controller.
- In lightweight AP setups, controller hardware must be installed and maintained locally.
- In cloud-based setups, no physical controller is needed on-site, reducing hardware costs.
- Lightweight APs are suitable for environments with strict on-premises control requirements.
- Cloud-based APs offer easier scalability, especially for distributed or multi-site networks.
- Management and updates for lightweight APs happen through the local controller.
- Management and updates for cloud-based APs happen automatically from the cloud.
- Lightweight APs might need manual firmware updates and scaling.
- Cloud-based APs get automatic updates and can scale quickly without additional hardware.
- Cloud-based solutions provide easier remote management and monitoring.
- Lightweight APs generally depend on the availability of the on-prem controller; if it fails, APs lose management.

Problem5:

- CAPWAP tunnel is established over UDP, using ports 5246 for control and 5247 for data.
- After AP discovers the controller, it initiates a DTLS handshake to secure the control tunnel.
- DTLS provides encryption, integrity, and authentication for control messages.
- Control tunnel is maintained continuously for management communication.
- Periodic keep-alive messages (heartbeat) are exchanged to check tunnel health.
- If keep-alive responses fail, the tunnel is considered broken, and AP retries connection.
- Data tunnel is created after the control tunnel is established, for client traffic.
- Both tunnels are stateless (UDP), so reliability is ensured at the protocol level using sequence numbers and acknowledgments.
- Tunnel remains active as long as AP is powered and network connectivity is stable.
- If controller fails, AP attempts to discover backup controllers and re-establish tunnels.

Problem6:

- Sniffer mode captures and forwards 802.11 wireless frames to a remote analyzer tool like Wireshark.
- Monitor mode captures and analyzes wireless traffic locally on the device itself.
- Sniffer mode is typically used with an AP configured to send raw packets to an external system.

- Monitor mode is used in wireless adapters or APs to capture frames without forwarding them.
- Sniffer mode is helpful for remote packet capture and centralized troubleshooting.
- Monitor mode is useful for local diagnostics, debugging, and site surveys.
- Sniffer mode requires integration with external tools or centralized packet analyzers.
- Monitor mode works independently, and tools like Wireshark can run directly on the device.
- Sniffer mode APs stop serving clients while in sniffer mode.
- Monitor mode radios are dedicated to monitoring and do not serve clients.
- Use case for sniffer mode: centralized packet capture in enterprise networks.
- Use case for monitor mode: onsite interference detection, rogue AP detection, and spectrum analysis.

Problem7:

- FlexConnect mode is best suited for APs when WLC is deployed over WAN.
- In FlexConnect, AP can locally switch client traffic without sending it to the remote controller.
- Reduces dependency on WAN link for data forwarding, improving performance and reliability.
- AP maintains local bridging for client traffic even if WAN link to WLC fails.
- Control traffic like authentication can still happen over WAN when available.
- FlexConnect supports local authentication to keep services running during WAN outages.
- Minimizes WAN bandwidth usage by keeping local traffic within the LAN.
- Enables VLAN tagging and traffic segmentation locally at the AP.
- Suitable for branch offices and remote sites with centralized controller architecture.
- FlexConnect APs reconnect to WLC over WAN for updates, policies, and management.

Problem8:

- Each autonomous AP requires individual manual configuration, increasing administrative overhead.
- Difficult to maintain consistent SSIDs, security policies, and VLAN settings across all APs.
- Troubleshooting becomes complex due to lack of centralized monitoring and logs.
- Roaming between APs is not seamless, causing session drops and poor user experience.
- No centralized control for load balancing, leading to uneven distribution of clients.
- Updating firmware or security patches must be done manually on each AP.
- Inconsistent RF management may lead to channel overlap and co-channel interference.
- Scaling the network beyond 50 APs adds significant operational complexity.
- Lack of central visibility makes detecting rogue APs and security threats difficult.
- No centralized captive portal or guest access control, complicating user onboarding.
- Increased risk of configuration errors across multiple APs.
- High operational costs due to manual maintenance and limited automation.

Problem9:

- In local mode, Lightweight AP forwards both control and data traffic to the WLC.
- If WLC goes down, AP loses control and data tunnel connectivity.
- Existing wireless clients are disconnected because AP cannot process client data locally.
- New client associations and authentications fail since AP relies on WLC for these processes.
- AP continues to send keep-alive messages trying to reach the WLC.
- Without WLC, AP cannot enforce security policies or manage client sessions.
- AP effectively becomes non-functional for client traffic until WLC is restored.
- Services like roaming, authentication (e.g., 802.1X), and DHCP relay are disrupted.
- Once WLC is back online, AP re-establishes CAPWAP tunnels and resumes normal operation.