**WiFi Training Program - Module 2 Assignment Answers**

**Q1,Q2,Q3,Q5**

SPLIT MAC ARCHITECTURE:

1. MAC (Media Access Control) is a sub-layer of the Data Link Layer (Layer 2) in the OSI model. It governs how data packets are placed on the medium and how devices on a local network gain access to the physical transmission medium.

2. In general, MAC layer has four responsibilities such as MAC addressing, framing, fragmentation , access control.

3. Split MAC architecture primarily focusses on dividing the MAC layer responsibilities into entities especially in Lightweight Access Points , cloud managed Access points in enterprise Wifi and also in Public Wifi deployments.

4. In general, Following are done by Access points:

1. Creating WLAN

2. Broadcasting SSID.

3. Advertising its capabilities such as BSSID, encryption and security protocols, Authentication, Channel in use,

RF frequency in use and advanced technologies like RRM, DFS, MLO, BSS colouring etc.

4. Station Discovery

5. Authentication

6. Association.

7. Integration Service

8. Subclauses implementation like Security protocols, Access control list enforcement, VLAN segmentation, QoS based traffic maintenance.

5. With the help of WLC (Wireless LAN Controller), Light Weight APs (thin AP) splits the role of Access Points as Real time and Non real time functions those are:

1. Real time functions (handled by AP) - Time-critical operations like beacon generation, acknowledgment (ACKs) retransmissions, encryption/decryption, and RTS/CTS.

2. Non real time functions (handled by controller) - Functions like association, authentication, roaming decisions, radio resource management, and QoS policies.

6. Light weight AP architecture thus offers Centralized control and configuration as opposed to Fat APs offering distributed control and configuration. Thereby increasing scalability and lowers the computation needed from AP.

7. Global optimization can be done on WLC logic so eliminating the latency from AP in processing non real time functions along with crucial time sensitive functions.

8. It simplifies Authentication, Association request and response, Band steering, beam forming, QoS, security rules enforcements, Firewall settings if needed, VLAN segmentations, Rogue AP and anamolies detection, Governs conventional internet communication, helps in firmware updates if needed for AP, DFS, RRM, MLO, Roaming etc.

9. For all above mentioned non real time functions, Light Weight AP uses CAPWAP (Control And Provisioning of Wireless Access Points) Data and Control tunnels.

10. It is generally equipped with very light weight Firmware initially just to get IP and discover WLC and work with real time functions of access points thereby supporting Zero Touch Deployment (All initial configuration like SSID, channel configurations to be advertised to STAs even will be decided by WLC in this case).

11. Wireless LAN controllers can be deployed in four different ways as per requirements. They are as follows:

1. On-premises Controller -> Here, Via switches, it will be connected to Access points.

2. Virtual controller -> Here, in Virtual Machine, Controller logic is developed and maintained reducing hardware overhead.

3. Embedded controller -> In any High end AP, Controller is embedded for optimized performance.

4. Cloud managed controller -> for easy management.

12. CAPWAP communication provides two tunnels such as Data plane (UDP port : 5247) for exchanging data between AP and WLC in forward and reverse cases with internet infrastructure and Control plane (UDP port : 5246) for exchanging control requests and responses.

1. When AP gets powered ON, it will not have any Configurations pre loaded as in Fat AP thus it cannot function as standalone

unit.

2. Now, AP first sends DHCP discovery message and acquires IP , DNS, Default gateway, WLC IP (optionally) as DHCP offer.

3. Now, AP either sends broadcast message in the subnet to find WLC or sends target request to predefined WLC in flash

sending discovery request.

4. WLCs will reply with Discovery response stating its capabilities like Model number, Limit of AP etc.

5. This is followed by CAPWAP join request to WLC and followed by Join response to AP from WLP.

6. Now, control plane to be secured with DTLS (Datagram Transport Level Security) with ClientHello (with Client ciphers (

encryption schemes) and versions) and ServerHello (chosen parameters from ClientHello) , Certificate Exchange or PSK ,

finished handshake.

7. If WLC's firmware is working with updated version with respect to AP, then optionally Image Download request and response.

then, AP will be rejoined by booting process.

8. Via control plane, AP configuration will be provided such as SSID, channel details etc.

9. As usual, Clients can get associated with this AP, authentication and all other non real time functions will be directed to

WLC for further responses.

10. AP and WLC will periodically exchange and verify Keep Alive and echo packets for ensuring their existence.

11. Moreover, FlexConnect advancements can be done by splitting control information with WLC and bypassing controllers in case

of data traffic.

13. Wireless Access Points in lightweight mode can work on following modes in enterprise Wifi. They are as follows:

1. Default mode -> it conventionally serves Clients with Data and Control planes.

2. FlexConnect mode -> bypassing WLC for data communication.

3. Monitor mode -> used for Wireless Intrusion detection system to prevent Locations, interference etc.

4. Sniffer Mode -> in promiscuous mode, it acts as Wifi NIC and captures packets and exports to Capturing tools using Remote

capture protocol.

5. Spectrum Mode -> analyzes non wifi protocol usage and gives alerts with appropriate softwares.

6. Bridge Mode -> works either as WGB or client mode.

7. Repeater Mode -> it acts as Wifi extender or repeater.

14. CAPWAP primarily comes under Layer-3 and Layer-4 of OSI. It needs IP address during AP - WLC configuration and Transport layer port for communication.

**Q4.**

LIGHT WEIGHT ACCESS POINTS:

1. It is a type of Access point which offloads some of its crucial functions to Wireless LAN Controller thereby optimizing power usage.

2. Thus, it simply acts as Radio Front end and relay interface and does not operate independently as like Standalone or Fat AP.

3. It takes care only the integration service and encryption with basic client association and offloads the advanced technologies like RRM, DFS, Security enforcements, VLAN segmentation and management, Monitoring, roaming , client authentication etc.

4. In order to achieve this, LWAP uses CAPWAP communication. This basically forms a secured tunnel between AP and WLC with different UDP ports 5246 and 5247 maintaining control and data plane.

5. Once, it got powered ON, it does minimal processing that is getting IP from DHCP server and finds WLC via discovery message and establishes CAPWAP tunnel for data exchange and secures it with encryption schemes.

6. In case of mismatched firmware versions, WLC let the AP know and make it update to the current version.

7. Thus, WLC takes following tasks:

1. SSID Broadcasting with and without VLAN

2. Channel assignment (RRM)

3. Transmit power, gain control

4. Security policies and protocol enforcements

5. Roaming optimization protocols

6. MLO, band steering

8. In recent advancements, dynamic switching is possible that is data traffic bypasses WLC in case to reach main network infrastructure.

**Q6.**

LIGHT WEIGHT ACCESS POINT MODES :

1. Local Mode -> Default mode where access point serves clients and handles RF

2. FlexConnect Mode -> Allows AP to switch the data traffic locally instead of directing them towards WLC and then getting back the data locally using the WAN bandwidth unnecessarily.

3. Sniffer Mode -> captures raw packets and forwards to packet analyzer tools for further analysis.

4. Monitor mode -> For monitoring RF and detects interference or rogue AP detection.

5. Spectrum Mode -> analyzes the usage of shared medium for traffic congestion and technologies involved.

6. Bridge/Mesh Mode -> APs are the part of bridge or mesh wifi network.

SNIFFER MODE :

1. It is used for troubleshooting , protocol analysis and capturing 802.11 traffic.

2. It stops serving wireless clients in sniffer mode. WLC orders AP to act as wireless sniffer.

3. It requires the channel to be listened and destination port to export the captured raw packets (all types of frames) for analysis. This will be set by WLC.

4. It tunes to the specified channel and starts receiving all RF frames.

5. It encapsulates the captured frames as UDP packets and sends to the Destination IP and Port.

6. On the reception end, Lets say Wireshark will be made ready by listening to the same port for capturing all the raw frames. LWAP plugin might be required in wireshark for automatic content extraction from UDP packets.

Use case : Used in secured organizations and helps in Wrong or misclassification of legitimate AP to be rogue APs by analyzing the Frames from Wireless Intrusion Prevention System or Latency analysis by capturing association frames and authentication frames and roaming decision frames.

MONITOR MODE :

1. Instead of serving clients, it becomes RF sensor that analyzes the RF metrics and calculates interference, congestion and report it to WLc.

2. It checks for Rogue AP by detecting unauthorized broadcasting in airspace. Thereby helping in mitigating Evil Twin attacks , DoS etc.

3. May collect information on client location using RSSI and Signal strength data.

4. Reports noise floor, over utilization of channel by other technologies to WLC.

Use case : To comply with RF standards, RF Audit can be initiated in any campus by setting any AP to be in Monitor mode that finds rogue APs , interference, and technology congestion over airspace, microwave usage that causes interferences , Unauthorized wireless device usage in restricted areas etc.

**Q7.**

WIRELESS LAN CONTROLLER IN WAN DEPLOYMENT :

1. It is crucial in the cases where WLC and APs are connected in remote sites thus WLC may get connected with AP via WAN connection.

2. CAPWAP protocol will also be connected via WAN only.

3. In these cases, efficient WAN usage is crucial thus FlexConnect Mode can be associated with LWAP which switches data traffic that are non crucial locally without WLC interference.

4. VLAN decisions are given locally to APs and Local RADIUS and/or authentication cache is enabled thus it can independently act in cases of missing controller connectivity.

5. In general, in these cases, authentication, DTLS, heartbeat signals consume more frequent transmissions in WAN.

1. Thus in case of WLC WAN deployments, FlexConnect mode is the wise choice in Lightweight APs.

2. Because, in local mode, AP forwards all traffic to WLC and doesn't switch locally leads to centralized decision making in all aspects.

3. Moreover, if WAN fails, AP become useless and bandwidth congestion may introduce more latency and also it is not scalable.

4. FlexConnect mode is advantageous because it sends control plane traffic (heart beat, network health, management information, authentication, association etc.)to WLC over WAN but switches basic data traffic locally at the site (by bridging out the data to main network interface using appropriate backhaul).

5. In most cases, Severity of data traffic decides whether to get switched locally or via WLC. For example, Secure traffic like VoIP is tunneled to WLC rather printer traffic is handled locally.

6. In this mode, if WAN interface goes down, AP continues to broadcast SSID and authenticates users using cached credentials and local RADIUS implementation with predefined VLAN segmentation and data traffic local switching. It also supports roaming in case of WAN failure along with captive portal web authentication.

**Q8.**

1. Basically Autonomous APs run its own wireless stack that is handling client authentication , encryption, security policies, vlan management, integration services etc.

2. Each APs to be configured independently either via SSH or via inbuilt CLI with no automation may lead to misconfigurations due to human errors.

3. Each AP will have their own RF parameters set, it will not change based on the dynamic channel conditions by monitoring it leading to Interference, coverage loss etc.

4. Due to the lack of fast centralized control, roaming become less efficient and leads to frequent disconnections and re-authentications.

5. Due to inconsistent Security policy enforcements, it might become impossible to detect Rogue APs in the network.

6. Network analytics (gathering network insights for improved handling) (number of clients per AP and places where signals go weak) becomes impossible.

7. Firmware updates are to be done on individual APs

8. There will be not be any dynamic load balancing with RRM, DFS without central orchestration.

9. For any new APs being joined, every single process of configuration to be done independently without cloning.

10. Since all processes are done by APs itself, power optimization cannot be done.

11. It is tedious in mesh networks without auto adjustments based on Dynamic paths and AP failure.

**Q9.**

1. Light weight AP in local mode relies heavily on WLC (for authentication, association, policy enforcement, roaming, vlan assignments and managements, DHCP relay, Firewall, QoS) thereby both data and control messages are tunnelled accordingly to WLC and get routed or decided respectively.

2. Generally, WLC sends KeepAlive packets to APs for ensuring active connection via CAPWAP.

However, if WLC becomes disconnected, APs detect contiguous loss of keepalive messages and declares WLC to be unreachable for certain number of CAPWAP heartbeats missing.

3. thus AP goes into Standby or orphan mode as it cannot handle even local data traffic independently in basic mode.

4. Clients may get disconnected since Data packets will not flow through main network infrastructure and DHCP offer may not get renewed if lease time expires (in case DHCP is managed by WLC)

5. Client authentication will fail as it is handled by WLC.

6. No updated configuration will be received by AP based on dynamic channel condition.

7. In this condition, AP will try to find new WLC by issuing discovery broadcast request across subnet or targeted request to primary, secondary WLC preconfigured.

8. However, it takes time as it needs to send Discovery request and expects response and followed by CAPWAP establishment and security schemes and begins its broadcasting.

9. Thus it is advantageous to use FlexConnect Mode or using primary, secondary or tertiary WLCs with local authentication cache and vlan cache.