**Wi-Fi Training Program**

**Assignment Solutions – Module 2**

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

SplitMAC is where the MAC layer functions are divided between the Access Point (AP) and the Wireless Controller (WLC). The AP handles the real-time parts like acknowledging frames, encryption, and roaming decisions. On the other hand, the WLC handles the management side like authentication and managing associations. By doing this, the AP can react faster to wireless events and the controller takes care of the bigger management tasks. This helps improve the performance of the AP because it doesn’t have to do all the heavy work by itself.

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

CAPWAP stands for Control and Provisioning of Wireless Access Points. It's basically the protocol that manages communication between lightweight APs and the controller. The flow usually goes like this: when an AP boots up, it sends a discovery message, and the controller responds. The AP then joins the controller and establishes a secure control tunnel. After that, the AP and controller exchange control messages like configuration details. Also, there can be a separate tunnel for data traffic (client data) if needed.

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

CAPWAP mostly works around Layer 2 (Data Link) and Layer 3 (Network) in the OSI model. There are two tunnels in CAPWAP: one is the control tunnel, which carries management traffic like configuration and AP updates, and the second is the data tunnel that carries user traffic (like the actual internet browsing traffic of wireless clients). The control tunnel is encrypted and secured, while the data tunnel may or may not be encrypted depending on the setup.

**4. Whats the difference between Lightweight APs and Cloud-based APs**

| **Lightweight APs** | **Cloud-based APs** |
| --- | --- |
| Need a physical controller (WLC) onsite | Managed through a cloud controller |
| Manual setup and updates | Updates and configs are pushed automatically |
| Good for traditional enterprise setups | Good for distributed or remote networks |
| Local dependency | Internet dependency (needs cloud access) |

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

Once the CAPWAP tunnel is established, it’s kept alive through keepalive or heartbeat messages that the AP and controller exchange regularly. If the AP doesn’t hear back from the controller after a few tries, it assumes the connection is lost and tries to re-establish the tunnel or join another available controller. The tunnel also uses DTLS encryption for security during all management communication.

**6. Whats the difference between Sniffer and monitor mode , use case for each mode**

| **Mode** | **Description** | **Use Case** |
| --- | --- | --- |
| Sniffer Mode | Captures and forwards raw 802.11 frames to analysis tools (e.g., Wireshark) | Troubleshooting wireless issues, packet analysis |
| Monitor Mode | AP passively listens and reports RF conditions without serving clients | Spectrum analysis, rogue AP detection, wireless surveys |

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

If the controller is far away over a WAN connection, the best mode for the APs would be FlexConnect. FlexConnect allows the APs to keep working even if the WAN link to the controller goes down. The APs can locally switch traffic and even handle client authentication on their own without always depending on the controller. This is super useful for branch offices or remote sites.

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

1. **Configuration Complexity**: Manual configuration on each AP.
2. **Management Overhead**: No centralized management, difficult troubleshooting.
3. **Firmware Updates**: Need individual updates.
4. **Roaming Issues**: No seamless roaming; clients might face disruptions.
5. **Scalability Problems**: Adding APs becomes harder.
6. **Security**: Harder to maintain consistent security policies across all APs.

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

If the AP is in local mode and the WLC goes down, clients will get disconnected because the AP can’t operate independently in this mode. It needs the controller to continue managing clients. The AP itself might reboot and keep trying to rejoin a controller. So basically, wireless connectivity would be lost until the WLC comes back or the AP finds a backup controller.