**WIFI – TRAINING PROGRAM**

**MODULE – 2**

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

All the network’s autonomous access points (APs) are protected by split MAC structures. Each AP operates under its own security policy. In order to manage security-related concerns, such as intrusion detection and prevention systems, QoS, bandwidth management, etc., a centralized location is used. According to the graphic below, any autonomous AP’s actions can be classified into two categories: group management functions, and real-time functions.

* The Autonomous AP management functions include RF power output management, QoS, security management, client authentication, and other management programs. On the other hand, real-time functions are concerned with the transfer of data frames, data encryption and decryption, and so on.
* Automated AP receives and transfers 802.11 frames in real-time. The autonomous AP communicates with the clients via the physical layer known as the MAC layer. The autonomous AP is governed by a centralized administrator for RF power output and security management.
* The hardware of an autonomous AP is known as a lightweight access point because it solely performs real-time operations. WLC is often in charge of managing autonomous AP (wireless LAN controller). The key things used for security performance are user authentication and security policy management, among other things. Layers 1 and 2 are utilized to move frames within the same RF domain.
* CAPWAP is an abbreviation for Control and Provisioning of Wireless Access Point tunneling protocol, which is used to encapsulate data within a wireless network. The CAPWAP connection is made up of two distinct tunnels, CAPWAP control messages, and CAPWAP data.

**Benefits and Challenges**

Benefits:

* Enhanced scalability and simplified management.
* Improved security through centralized policy enforcement.

Challenges:

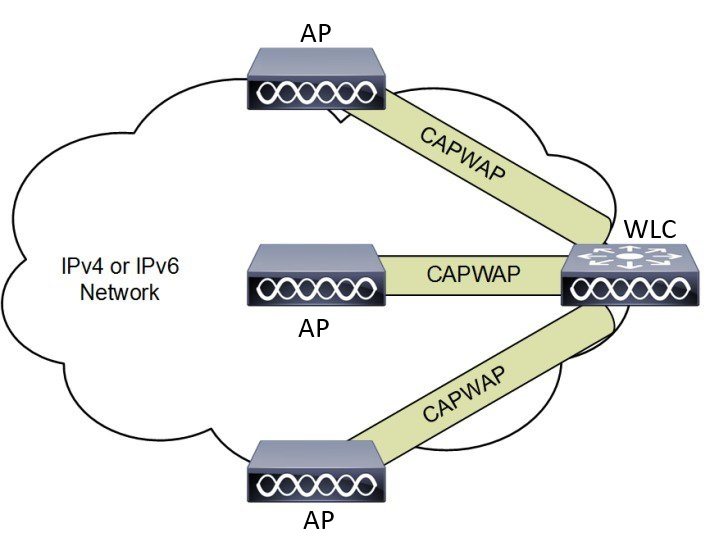
* Higher initial costs due to the need for WLCs.
* Potential single point of failure if redundancy is not implemented.

By distributing the MAC layer functions, SplitMAC offers several performance improvements:

1. **Reduced Processing Load on APs:** Offloading complex and less time-sensitive tasks to the WLC frees up the AP's processing resources. This allows the AP to handle the more critical, real-time wireless communication tasks more efficiently.
2. **Improved Airtime Efficiency:** With less processing overhead, APs can spend more time actually transmitting and receiving data rather than managing control functions. Centralized coordination by the WLC (like advanced frame aggregation and scheduling across multiple APs) can further optimize airtime utilization.
3. **Enhanced Scalability:** Because individual APs are less burdened, they can support a larger number of concurrent clients without significant performance degradation. The centralized WLC has the processing power to manage the higher-level functions for a multitude of APs.
4. **Better QoS Management:** The WLC can enforce consistent QoS policies across the entire wireless network, ensuring that critical traffic receives the necessary priority, even in congested environments.
5. **Simplified AP Management:** The WLC provides a central point for configuration, management, and monitoring of multiple APs, simplifying network administration.
6. **Describe about CAPWAP, explain the flow between AP and controller.**

CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol used to establish a secure communication tunnel between a Wireless LAN Controller (WLC) and Access Points (APs). This tunnel is used to exchange both control and data plane information. The flow between AP and controller involves an initial discovery phase, followed by a secure tunnel establishment, and then ongoing communication for control and data transfer.

* CAPWAP creates a direct link between wireless LAN controllers (WLC) and APs. This link is called a **CAPWAP tunnel**. It handles both control and data messages.
* CAPWAP works in two main ways: Split MAC and Local MAC. Split MAC is managed by the WLC and can cause higher latency. But, it makes management easier and boosts security. Local MAC, on the other hand, processes data at the AP, reducing latency but making management more complex.
* In **Split MAC mode**, all data and management frames go through the **CAPWAP tunnel** to the WLC. This can cause bandwidth issues and make the network more vulnerable to failures.
* The **Local MAC mode** is better for handling failures. It lets data be processed locally, reducing the amount of traffic sent to the WLC.



**AP to Controller (Control Plane - Uplink):**

* **Discovery Phase:** AP initiates the establishment of a control channel by transmitting discovery.
* **Association/Join Request:** Upon WLC discovery, the AP transmits an Association Request or Join Request frame containing AP identification and capabilities.
* **Authentication and Authorization:** The WLC authenticates the AP using protocol, CAPWAP, often involving shared secrets, MAC address-based access control lists, or X.509 certificates. Authorization determines the AP's allowed participation in the WLAN.
* **Configuration Transfer:** Following successful authentication and authorization, the WLC pushes configuration parameters to the AP via control messages
* **Status Reporting:** The AP periodically transmits status reports to the WLC using control messages, providing real-time operational metrics such as CPU/memory utilization, connected client count, radio interface statistics (transmit/receive errors, channel utilization), and detected rogue APs/clients within the Indian regulatory domain.
* **Event Notification:** The AP sends event-driven control messages to the WLC upon the occurrence of significant events, including client association/disassociation (802.11 association/deauthentication frames), authentication failures (RADIUS/AAA messages), and security-related events (e.g., intrusion attempts).
* **Radio Resource Management (RRM) Metrics:** The AP gathers and reports RF environment measurements to the WLC via control messages, facilitating centralized RRM algorithms for dynamic channel assignment (DCA) and transmit power control (TPC) optimized for the local RF landscape in India.

**Controller to AP (Control Plane - Downlink):**

* **Configuration Push:** The WLC initiates the transmission of control messages to the AP to update its operational parameters, deploy new WLAN configurations, modify security policies (e.g., key rotations adhering to security best practices in India), and push updated QoS profiles.
* **Management Directives:** The WLC sends control commands to the AP for remote management functions, including AP reboot (software or hardware), radio interface resets, initiation of packet captures for troubleshooting within the Indian network, and execution of diagnostic tools.
* **Policy Enforcement Instructions:** The WLC communicates policy enforcement mechanisms to the AP via control messages, instructing the AP on how to apply QoS markings (DSCP/802.1p), implement access control lists (ACLs) based on MAC/IP addresses relevant to the Indian network's security posture, and enforce traffic shaping policies to manage bandwidth consumption.
* **Firmware Distribution:** The WLC centrally distributes and manages AP firmware upgrades via control protocols, ensuring consistent software versions across the WLAN infrastructure in India, potentially including region-specific firmware releases.
* **Radio Resource Management (RRM) Commands:** The WLC sends control directives to the AP, instructing it to change its operating channel (based on DCA algorithms considering the RF spectrum in India), adjust its transmit power levels (TPC adhering to TRAI EIRP limits), and modify its neighbor reporting behavior for optimal co-channel interference mitigation.
* **Client Management Commands:** The WLC can send control messages to specific APs to execute client-specific actions, such as disassociating a client (sending 802.11 disassociation frames), applying specific rate limiting policies for a user within the Indian context, or initiating client authentication/re-authentication procedures.

**Data Plane Flow:**

* **Centralized Forwarding (Tunneling):** Client data frames encapsulated within protocols like CAPWAP are forwarded from the AP to the WLC over a data tunnel. The WLC then performs Layer 2/Layer 3 forwarding onto the wired infrastructure.
* **Local Switching/Forwarding:** The AP performs Layer 2/Layer 3 forwarding of client data frames directly onto the wired network infrastructure based on forwarding tables and VLAN assignments configured by the WLC. Control plane communication with the WLC remains for management and policy.

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

* CAPWAP (Control and Provisioning of Wireless Access Points) primarily operates at the Network Layer (Layer 3) of the OSI model. It utilizes IP addresses and UDP ports (5246 for control, 5247 for data).
* CAPWAP establishes two tunnels: a control tunnel for managing access point configuration and authentication, and a data tunnel for transmitting user data.

**Control Tunnel**:

* **Purpose**: Handles **management and control messages** between the AP and WLC.
* **Uses**: AP join requests, configuration updates, firmware upgrades, etc.
* **Protocol**: Encrypted using **DTLS (Datagram Transport Layer Security)**.

**Data Tunnel**:

* **Purpose**: Forwards **user data traffic** (like client device traffic) between AP and WLC.
* **Uses**: Transports data packets from client devices to the WLC (centralized switching).
* **Encryption**: Optional — based on configuration.

1. **What is the difference between Lightweight APs and Cloud-Based APs?**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Lightweight APs (LAPs)** | **Cloud-Based APs** |
| Initial Setup | Can be more complex, requiring WLC configuration and AP provisioning on the local network. | Generally simpler initial setup; APs often auto-provision upon connecting to the internet. |
| Ongoing Management | Requires dedicated IT staff to manage the on-premises WLC and network. | Can be managed by less specialized IT staff due to the intuitive cloud interface. |
| Network Visibility | Granular control and visibility within the local network. | Management visibility is through the cloud portal, which might have limitations in deep local network diagnostics. |
| Troubleshooting | Security posture is primarily managed and controlled within the organization's network in India. | Security relies on the cloud vendor's security measures, requiring trust in their infrastructure. |
| Security Considerations | Feature updates are typically controlled by the organization's IT team, tied to WLC software upgrades. | Feature updates are managed and rolled out by the cloud vendor, providing access to the latest features but with less direct control over timing. |
| Feature Updates | Often offers more granular customization options and deeper integration with other on-premises network systems | Customization and integration might be limited to the features and integrations provided by the cloud vendor. |

1. **How the CAPWAP tunnel is maintained between AP and Controller?**

In the context of Cisco [Wi-Fi](https://notes.networklessons.com/wireless-wi-fi-ieee-80211) deployments using [Wireless LAN Controllers (WLCs)](https://notes.networklessons.com/wireless-wireless-lan-controller), a CAPWAP tunnel is a connection that is established between a wireless access point (AP) and the WLC. This tunnel allows for a split in the traffic handling between [control traffic](https://notes.networklessons.com/network-control-plane) and [data traffic](https://notes.networklessons.com/network-data-plane):

1. **Control Traffic**: This is the traffic between the AP and the WLC that is used for management and control functions. This could include functions like the AP discovering the WLC, the AP joining the WLC, synchronization of configurations, and statistics gathering.
2. **Data Traffic**: This is the actual client data that the AP forwards to the WLC. The data from wireless clients is encapsulated in CAPWAP packets at the AP, sent to the WLC, decapsulated, and then typically routed to the enterprise network.

The CAPWAP tunnel between an Access Point (AP) and a Wireless LAN Controller (WLC) is maintained through a combination of periodic messaging, stateful connections, and mechanisms to detect and recover from failures

**1. Initial Establishment and Association:**

* The AP discovers and joins the WLC, establishing the CAPWAP control tunnel (UDP port 5246) and potentially the data tunnel (UDP port 5247). This involves a handshake and exchange of session parameters.

**2. Keep-Alive Mechanisms (Heartbeats):**

* Both the AP and the WLC periodically send **keep-alive messages (heartbeats)** over the control tunnel.
* These messages verify the active and responsive communication path, confirming the continued operational status of each device within the Indian network.
* The frequency is configurable, and a timeout period is defined. If a keep-alive isn't received within this period, the connection is considered lost, which is crucial for managing networks that might experience varying levels of connectivity across India.

**3. Stateful Connections:**

* CAPWAP maintains **stateful UDP connections** for both control and data tunnels.
* Both the AP and the WLC store information about the established tunnels (session IDs, sequence numbers for reliable control message delivery, expected peer state). This state awareness ensures proper interpretation of messages, especially important in potentially less reliable network segments within India.

**4. Error Detection and Handling:**

* CAPWAP incorporates error detection mechanisms. Control messages can include sequence numbers to identify lost or out-of-order packets, which can be more common in networks with varying quality of service across India.
* Retransmission of control messages is attempted upon detecting errors or missed acknowledgements within defined timeouts.
* Persistent communication failures lead to tunnel termination, necessitating re-discovery and re-joining, processes that need to be robust for APs in different geographical and infrastructure contexts within India.

**5. Tunnel Maintenance During Network Changes:**

* **Configuration Updates:** The WLC pushes configuration changes over the active control tunnel, ensuring consistent policies and settings are applied to APs across the Indian deployment.
* **Client Events and RRM:** Reports and commands related to client activity and radio resource management (considering TRAI regulations for spectrum usage in India) are exchanged via the persistent control tunnel.
* **Roaming (Centralized):** For centralized forwarding within a WLC-managed WLAN in India, the data path might be updated at the WLC, while the control tunnel to the serving AP remains active.

**6. Failure Detection and Recovery (Crucial for Diverse Network Conditions in India):**

* **Loss of Keep-Alives:** The primary indicator of a lost connection.
* **Control Tunnel Failure:** Leads to loss of configuration and management. APs attempt re-discovery and re-joining, a process that needs to be efficient even in potentially unstable network environments in India.
* **WLC Failure:** Causes loss of management. AP behavior depends on the last known configuration (local forwarding might continue). Redundant WLC deployments are vital for high availability in enterprise networks across India.

1. **What is the difference between Sniffer mode and Monitor mode, use case for each mode?**

**Monitor Mode:**

* **Functionality**: In Monitor mode, a wireless network interface card (NIC) is configured to passively listen to all wireless traffic on a specific frequency or channel without associating with any Access Point (AP) or participating in the network. It essentially becomes a radio receiver, capturing raw 802.11 frames as they are transmitted in the air.
* **Association**: The NIC does not associate with any BSSID (Basic Service Set Identifier, the MAC address of the AP).
* **Transmission**: The NIC cannot transmit any data in Monitor mode. It is purely a listening mode.
* **Frame Visibility**: It can capture all 802.11 frame types, including:
  + Management Frames: Beacons (advertising AP presence), Probe Requests/Responses (client discovery), Association/Authentication frames (client joining).
  + Control Frames: RTS/CTS, ACK frames (managing medium access).
  + Data Frames: The actual data being transmitted between clients and APs.
* **Channel Hopping**: Often, tools used in Monitor mode can instruct the NIC to hop between different Wi-Fi channels to capture a broader range of network activity.
* **Use Cases**:
  + Network Analysis and Troubleshooting: Identifying network congestion, interference from other wireless devices (important in densely populated areas in India), and analyzing Wi-Fi signal strength and coverage issues.
  + Security Auditing and Penetration Testing: Capturing handshake frames (e.g., during WPA/WPA2 authentication) to attempt offline password cracking. Observing network behavior for potential vulnerabilities.
  + **Wireless Intrusion Detection**: Monitoring for unauthorized APs (rogue APs) or suspicious client activity.
  + **Spectrum Analysis** (with appropriate tools): Understanding the utilization of different Wi-Fi channels in a specific area, which can be crucial for optimizing network deployments in India where spectrum availability and interference can be concerns.
  + **Learning and Education**: Understanding the underlying protocols and frame structures of Wi-Fi communication.

**Sniffer Mode**:

* **Functionality:** The term "Sniffer mode" is often used interchangeably with Monitor mode. However, in some contexts, it might imply a more focused or targeted form of passive listening. It might suggest that the capture is specifically aimed at a particular network (BSSID) or type of traffic.
* **Association**: Similar to Monitor mode, the NIC typically does not need to be associated with an AP to capture traffic in what is commonly understood as "Sniffer mode."
* **Transmission:** Like Monitor mode, transmission is generally not possible in a purely passive sniffing configuration.
* **Frame Visibility**: Usually captures the same range of 802.11 frames as Monitor mode.
* **Channel Hopping**: Channel hopping is also a common feature used in conjunction with "Sniffer mode" to follow target networks.
* **Distinction (Subtle):** The primary distinction, if any, lies in the *intent* of the capture. "Sniffing" often implies looking for specific information or traffic patterns related to a target, whereas "Monitor mode" might be a broader, less targeted observation of the wireless environment. However, tools often use the terms synonymously.

**Use Cases** (Largely Overlapping with Monitor Mode):

* **Targeted Network Analysis**: Analyzing the communication flow within a specific Wi-Fi network in your home, office, or a public hotspot in India.
* **Troubleshooting Specific Client-AP Communication Issues:** Observing the frames exchanged between a particular device and the access point it's connected to.
* **Security Analysis of a Specific Network**: Focusing on the authentication process or data exchange within a defined wireless network for security assessment.
* **Packet Capture for Debugging**: Gathering detailed packet information for developers or network engineers to diagnose communication problems.

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

FlexConnect is a mode for **Lightweight APs** that allows them to **locally switch traffic** and **locally authenticate clients** even when the WLC is at a remote location (like in a WAN). FlexConnect is best in WAN Deployments in the following ways:

**Local Switching**:

* Client data traffic is directly bridged to the **local LAN**, avoiding the WAN bottleneck.
* Reduces latency and saves WAN bandwidth.

**Local Authentication (FlexConnect Authentication)**:

* In standalone mode (when WLC is unreachable), APs can **authenticate users locally** using cached credentials or a RADIUS server.

**Survivability**:

* If WAN link to WLC goes down, APs in FlexConnect mode continue to operate using locally stored configuration.
* Provides uninterrupted service.

**Central Management Still Possible**:

* When the WAN link is up, APs are still centrally managed by the WLC.

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

Deploying autonomous APs (also called standalone APs) in a large network like a university—especially with more than 50 APs—presents major operational and technical challenges.

* Autonomous APs are independent wireless access points that : Are individually configured and managed , Operate without a central controller, Perform all control and data functions locally.

**1. Configuration Complexity**

* **Each AP must be manually configured**: SSIDs, encryption, VLANs, QoS, etc.
* Extremely **time-consuming and error-prone**, especially during setup and updates.
* No centralized way to **enforce security or policy consistency** across APs.

**2. Scalability Limitations**

* Standalone APs do **not scale well**.
* As the number of APs grows, managing them becomes chaotic.
* Troubleshooting becomes inefficient without centralized logs and visibility.

**3. No Centralized Management**

* You lack a **single pane of glass** to monitor and control the wireless network.
* No built-in support for:
  + **Client roaming** logs
  + **Real-time monitoring**
  + **Automatic radio frequency (RF) management**

**4. Client Roaming Inefficiency**

* Roaming between APs is **not seamless**.
* Each AP operates independently — no coordination to facilitate **fast or secure roaming** (e.g., 802.11r, 802.11k/v support is often missing).
* Leads to **dropped calls, streaming interruptions**, and poor user experience for mobile users.

**5. RF Interference and Channel Overlap**

* No automated **RF optimization**: Channels and power levels must be **manually planned and adjusted**.
* Very hard to maintain in dynamic environments (e.g., dorms, lecture halls, libraries).
* Risk of **co-channel interference** or **coverage gaps**.

**6. Firmware and Security Maintenance**

* Firmware upgrades must be done manually on each AP.
* Hard to ensure all APs are on **latest security patches**.
* Risk of inconsistent configurations leading to **vulnerabilities**.

**7. Monitoring and Troubleshooting**

* Lack of real-time monitoring dashboards.
* Hard to diagnose client issues (e.g., connectivity failures, roaming issues).
* No visibility into:
  + AP health
  + Client statistics
  + Bandwidth usage

**8. High Operational Costs**

* Though **initial CAPEX is lower** (no controller), **OPEX increases** over time due to:
  + More IT staff time needed
  + Manual labor for changes or troubleshooting
  + Downtime during configuration errors

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

In Local Mode, the AP:

* Sends all control and data traffic to the WLC via CAPWAP tunnel.
* Does not make any independent decisions.
* Acts as a "dumb" radio head relying completely on the WLC for client handling.

**1. New Client Connections Will Fail**

* APs can't accept new client associations.
* No authentication, DHCP relay, or IP assignment will happen for new devices.
* SSIDs may still be visible, but connection attempts will fail or time out.

**2. Existing Clients Will Eventually Be Disconnected**

* Current sessions may continue briefly if:
  + There's no roaming.
  + No re-authentication or DHCP renewal occurs.
* However, once the client needs to:
  + Re-authenticate (e.g., after session timeout),
  + Roam to another AP or
  + Renew IP via DHCP

**3. No Roaming Support**

* Seamless roaming between APs **requires coordination** from the WLC.
* With WLC down, **roaming fails** or becomes very slow and unsecure.

**4. No Central Services**

* Policies, access control lists (ACLs), VLAN tagging, guest access, etc., are all centrally managed.
* These features become **inaccessible** or behave unexpectedly.