Wi-Fi TRAINING - MODULE 2

Akash S, embedUR Systems

Qn 1:

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

SplitMAC Architecture:

- SplitMAC is a smart design in wireless networks that divides MAC layer tasks between a lightweight **Access Point** (AP) and a **Wireless LAN controller** (WLC)
    - AP handles real time duties - sending frames
    - WLC handles complex duties - security and configuration

How it works?

- **Task Dividing:**
    - Real-time tasks stay with AP
    - Non Real-time tasks stay with WLC
- **Centralized Control:**
    - WLC takes care of all APs to coordinate and ensure policies in the network
- **Processing:**
    - This reduces the weight of APs
    - APs now can only oversee the client connectivity (No heavy lifting)

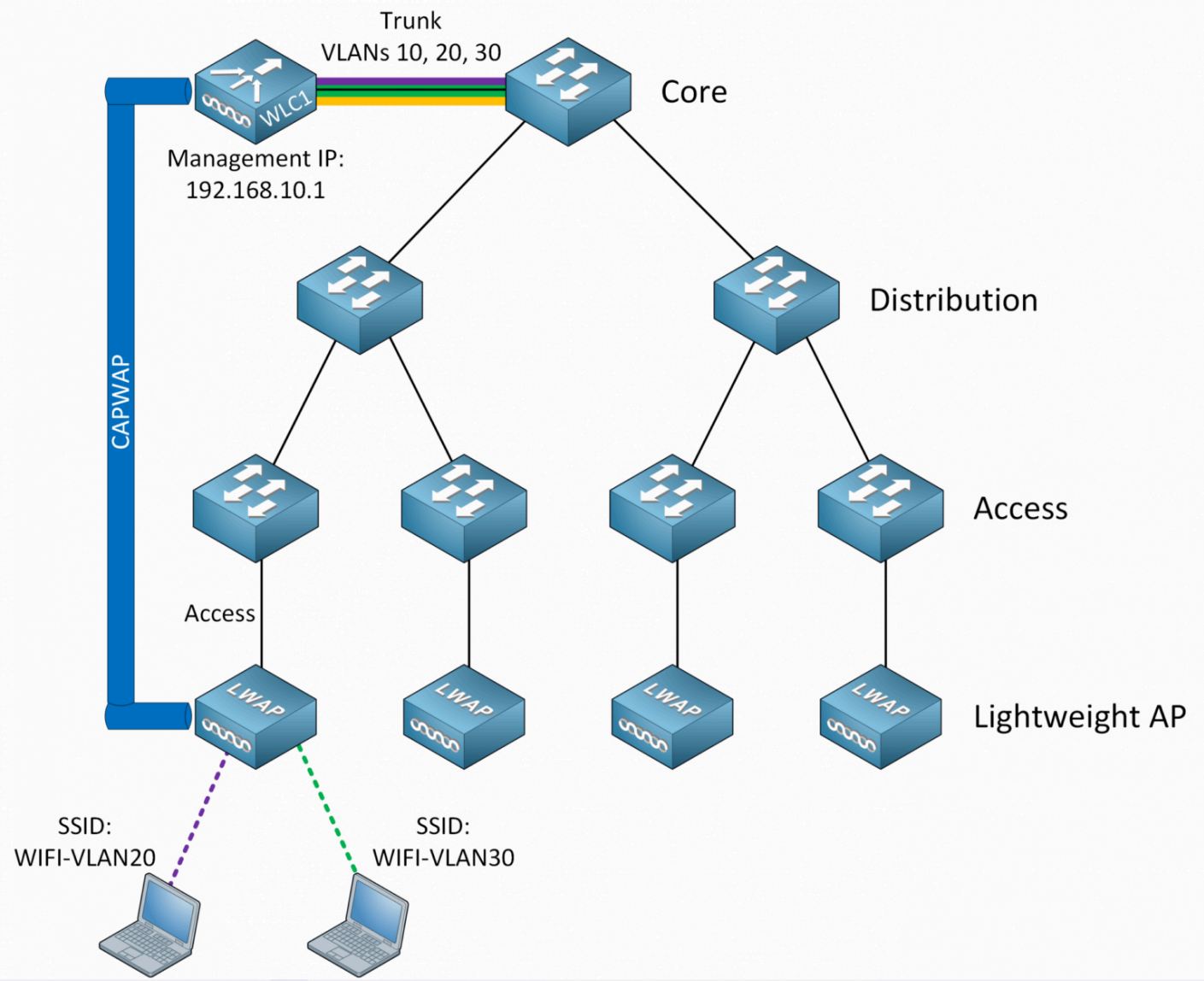
Benefits:

- APs are now free from overhead, so they can deliver at faster data rates - latency will be low
- **100s** of APs can connect to WLCs so that we can use it for large networks like Campuses
- The WLC optimizes channels and power levels, so it minimizes wifi congestion

- WLC takes care of client **handoffs**
- WLC manages encryption so that APs prioritize secure packet delivery

Why it is important:

- SplitMAC makes APs more efficient and reliable
- They make the APs more scalable - meaning, even when a large number of client gets connected, the **performance won't go down**
- This architecture is widely used in enterprise wifi networks to provide fast and secure connectivity



Qn 2:

Describe about CAPWAP, explain the flow between AP and Controller

CAPWAP:

- CAPWAP - **Control and Provisioning of Wireless Access Points**
- It is a protocol that enables a wireless LAN controller (WLC) to manage lightweight access points (APs) efficiently.
- It is like a communication lifeline between the brain (WLC) and the hands (APs) in a wireless network, ensuring everything runs smoothly.

Purpose:

- It standardizes how APs and the WLC talk, handling tasks like configuration, monitoring, and data tunneling.
- Built on a client-server model, CAPWAP uses **UDP** for fast, reliable communication, replacing older protocols like LWAPP.

Key Components:

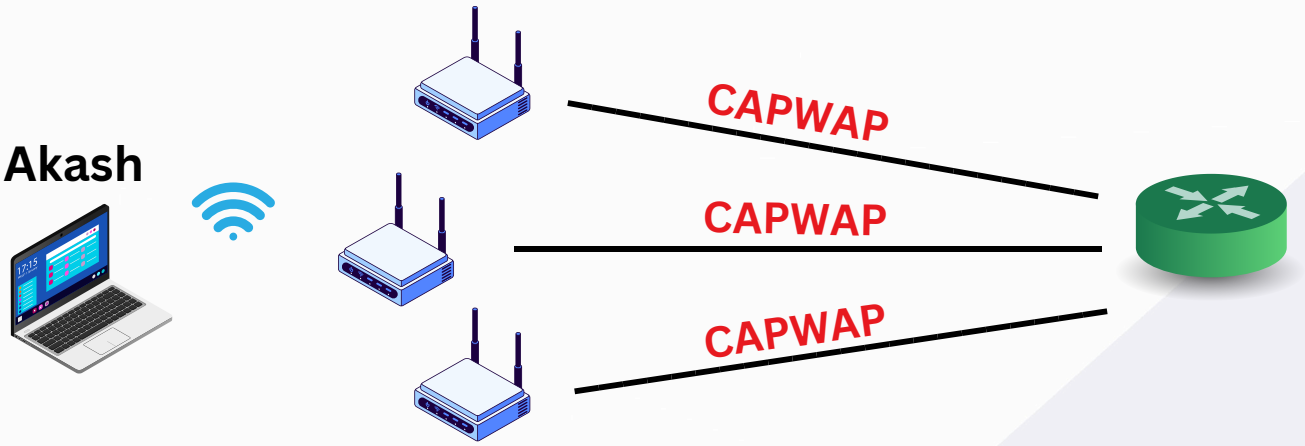
- **Control Channel:**
    - Manages Commands, Configurates and Status updates between WLC and AP
- **Data Channel:**
    - Carries user traffic (mainly for security)

Flow Between AP and Controller:

- **Discovery:**
    - When an AP powers up, it broadcasts a discovery request to find a WLC. The WLC responds with its details
    - Mainly to discover WLC
- **Association:**
    - The AP picks a WLC and establishes a secure CAPWAP connection using certificates or keys

- **Configuration:**
  - WLC sends the AP its settings—channel, power, SSID
- **Tunnel Setup:**
  - Two Tunnels form
    - One tunnel for **Control** - management traffic
    - One tunnel for **Data** - client traffic
- **Operation:**
  - AP starts serving clients, sending user data through the data tunnel while the WLC monitors and adjusts via the control tunnel
- **Maintenance:**
  - WLC periodically updates the AP—firmware, policies, or tweaks

Illustration:



Tunneling:

Qn 3:

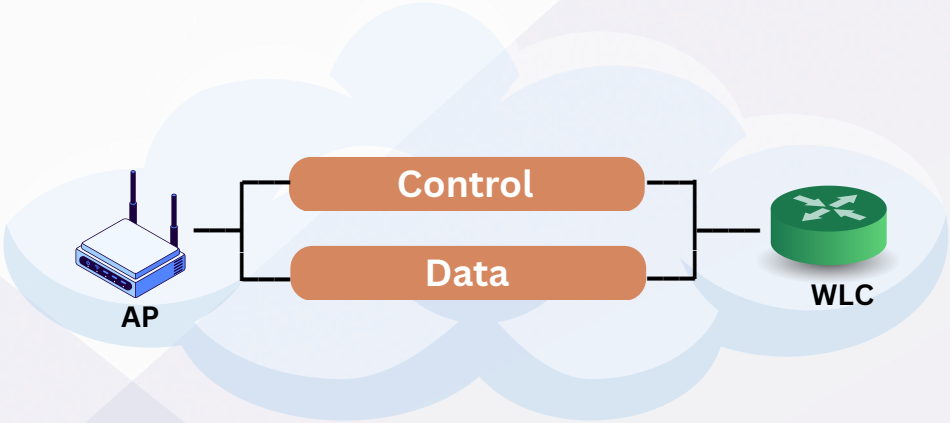
Where this CAPWAP fits in OSI model, what are the two tunnels in CAPWAP and its purpose

CAPWAP in OSI Layer:

- CAPWAP (Control and Provisioning of Wireless Access Points) operates across multiple layers of the OSI model making it a versatile protocol for wireless management
- **Layer 3 (Network)**:
  - CAPWAP runs over UDP/IP, using ports 5246 (control) and 5247 (data). This IP foundation lets it work across subnets, unlike older protocols tied to Layer 2
- **Layer 4 (Transport)**:
  - It uses UDP for speed and efficiency, avoiding TCP's overhead since wireless networks need quick, lightweight communication.
- **Layer 7 (Application)**:
  - CAPWAP protocol itself defines the rules for AP-WLC interaction like configuration and monitoring

Tunnels:

- There are two tunnels in CAPWAP
  - **Control Tunnel**
  - **Data Tunnel**



Control Tunnel:

- Carries management traffic between the AP and WLC
    - Like commands, configurations, status updates
- Lets the WLC tell the AP what to do, like changing channels or updating software, without slowing things down
- Uses port **5246** and **UDP** for fast messages
- If an AP starts acting up, the control tunnel lets the WLC spot the issue and send a fix right away
- It syncs multiple APs, so they work together like a team

Control

Data Tunnel:

- Carries the stuff users care about from AP to WLC or network
    - like web pages or video calls
- Keeps data safe and move smoothly
- Uses port **5247** and **UDP** for speed
- The data tunnel lets the WLC decide where your data goes—like to the internet or a secure server—keeping things orderly
- If one AP gets busy, the tunnel helps shift some load to others nearby, avoiding slowdowns.

Data

Why two Tunnels:

- Having two tunnels is like separate lanes for management and user traffic
    - it avoids mix-ups
    - speeds things up
    - keeps the AP focused on its job

Qn 4:

What's the difference between Lightweight APs and Cloud-based APs

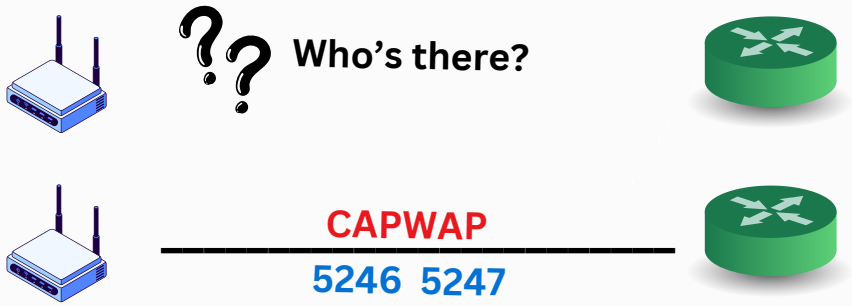
FEATURE	LIGHT-WEIGHT APs	CLOUD-BASED APs
Control Location	Managed by a local WLC onsite	Managed via the cloud over the internet
Setup	Needs WLC hardware installed	Just plug in and connect online
Scalability	Good for big local setups, WLC limits	Scales fast anywhere with internet
Cost	Higher upfront (WLC cost)	Lower start, may have cloud fees
Updates	WLC pushes updates locally	Cloud sends latest updates anytime
Reliability	Works without internet if WLC is up	Needs internet; may pause if it drops
Flexibility	Fixed to one network location	Works anywhere with a connection
Management	Hands-on, local IT team needed	Remote control from any device
Security	WLC locks it down onsite	Cloud handles security, needs trust

Qn 5:

How the CAPWAP tunnel is maintained between AP and controller

Setting up the tunnel:

- AP starts by finding the WLC, like sending out a “who’s there?” signal
- They connect using UDP ports 5246 for control and 5247 for data
- Certificates or keys lock the tunnel, keeping it safe from outsiders



Keeping it alive:

- AP and WLC send regular pings
- If the signal drops, they keep trying to reconnect automatically
- The tunnel stays active as long as the network’s humming

Handling Problems:

- If packets get lost, CAPWAP resends them to avoid gaps
- Errors get flagged fast so the WLC can sort things out
- Short outages do not make a huge problem
    - like the AP jumps back in quick

Updates:

- WLC sends new settings or software through the tunnel when needed.
- The connection adjusts on the fly, like tuning a radio.
- Keeps everything running smooth without starting over.

Qn 6:

What's the difference between Sniffer and monitor mode, use case for each mode

ASPECT	SNIFFER MODE	MONITOR MODE
What It Does	Captures all Wi-Fi packets to save	Watches all Wi-Fi traffic live
How It Works	Records data like a tape for analysis	Spies quietly, no sending back
Tools Needed	Needs software to review captures	Runs on basic supported hardware
Device Type	Often an AP feature	Usually for client devices (laptop)
Speed	Slower—stores everything first	Fast—sees it as it happens
Use Case 1	Troubleshoot by studying saved traffic	Check live traffic for instant insights
Use Case 2	Audit security with detailed logs	Test for hacks without connecting
Use Case 3	Test network in busy spots	Map signal strength on the go
Use Case 4	Analyze packet patterns over time	Spot interference in real-time

Qn 7:

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

Setup:

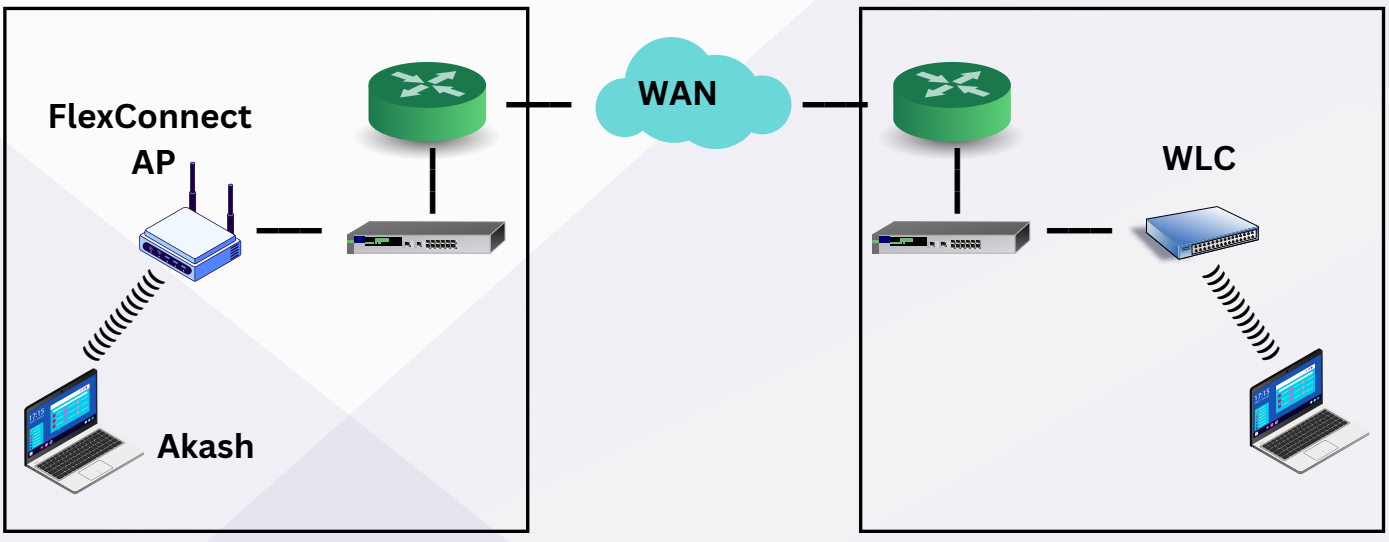
- WLC in the WAN means the controller is far away, connected over the internet, not onsite
- Local network needs an AP mode that keeps things running smoothly despite the distance
- Options like Local, FlexConnect, or Bridge mode come into play

Best Mode:

- **FlexConnect**
- FlexConnect is the top pick when the WLC is in the WAN
- It's like giving the AP a backup brain to handle local tasks if the WLC is out of reach
- Balances control from the WLC with independence at the AP

How FlexConnect Works:

- AP connects to the WLC over the WAN for big decisions
- Handles client data without always pinging the WLC
- Switches to standalone mode if the WAN link drops, keeping Wi-Fi alive

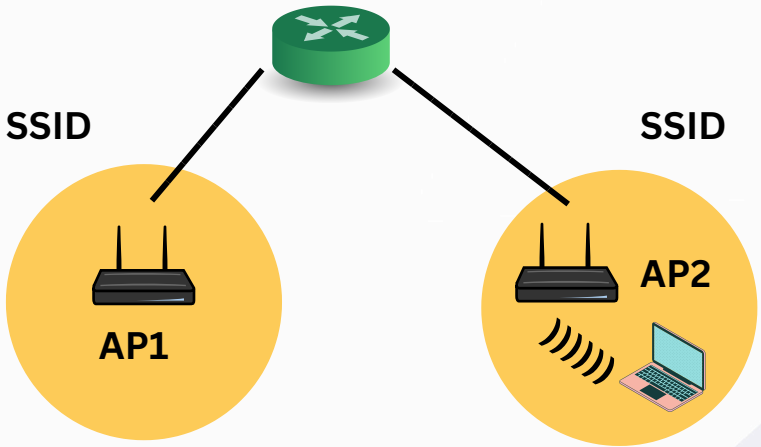


Qn 8:

What Are Challenges if Deploying Autonomous APs (More Than 50) in a Large Network Like a University?

Autonomous APs in Sri Krishna College of Engineering and Technology (SKCET):

- Autonomous APs work independently, each managing itself without a central controller
- At SKCET, with its big campus and 6000+ students, 50+ APs could mean one per classroom or lab
- Sounds simple, but lots of solo APs can stir up trouble in a busy college



Challenges:

Setup takes forever:

- Imagine configuring 50 APs across SKCET's **25 acres campus** each needs its own channel and SSID by hand
- One misstep like two APs on the same channel near the **ECE block**, and Wi-Fi slows down

Wi-Fi Clashes:

- There will be overlaps everywhere if it is not properly deployed
- With no teamwork between APs, 50+ APs might overlap
- Students streaming lectures or gaming in hostels could face lags

Roaming problems:

- Walking from the **Classroom** to the **Convention Centre**, our phone might cling to a weak AP signal
- No central system to pass smoothly to the next AP (call drops)
- At SKCET, with students rushing between classes, this could annoy everyone

Keeping track:

- Only when a student complains, we'll know what happens with APs
- Without dashboards, it is really difficult to track
- Scaling up for a new building means more manual mess

Security:

- A hacker could hit an outdated AP sneaking into SKCET's network

SKCET Campus with Autonomous APs:

Qn 9:

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

Setup:

- A lightweight AP in local mode depends on a Wireless LAN Controller (WLC) to run things
- A client, like a student's laptop, connects to this AP for Wi-Fi
- If the WLC goes down, the main controller is offline, and trouble starts

Connection drops fast:

- The AP loses its link to the WLC, which it needs to keep clients connected
- The client gets disconnected and can't access the internet or network
- It feels like the Wi-Fi just shuts off without warning

No new clients allowed:

- The AP stops letting new devices join the network
- Anyone trying to connect gets stuck

Data stops flowing:

- All traffic, like streaming or downloads, grinds to a halt
- The client sees error messages about no connection
- Local mode relies on the WLC for data, so there's no workaround

Data stops flowing:

- The AP doesn't quit and keeps looking for the WLC
- It sends out signals, waiting for the controller to come back
- Until that happens, it can't help clients at all

THE END

AKASH S