Wi-Fi Technology Fundamentals

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module-6

Advanced Wi-Fi Use Cases

Session-6a

WLAN Access Point and Controller Architectures

Recap .....
Module 5: Advanced Features and Standard Extensions

- ## Advanced MAC Features
  - DFS, 802.11k, RRM, ACS, 802.11v, WNM, 802.11r, Fast Roaming
- ## Wi-Fi6 New Features
  - OFDMA, Mu-MIMO, 1024QAM, BSS Coloring, TWT
- ## Wi-Fi6E New Features
  - 6GHz channels, Equipment/Device Classes, AFC, FILS, PSC, RNR, MBSSID
- ## Wi-Fi7 New Features
  - 320MHz, 4K QAM, 16x16, MLO, Multi-RU OFDMA, Preamble Puncturing, Multi AP coordination, Hybrid ARQ

Module 6: Advanced Wi-Fi Use Cases

- ## WLAN AP/Controller Architectures
  - Thick/Thin APs, Physical Controller, LWAPP, Cloud Controller
- ## Smart Wi-Fi Features
  - Traffic Shaping/Policing, Advanced Analytics, AI/ML
- ## Wi-Fi Mesh Networks
  - Mesh Topologies, Various Deployment Models, Mesh Access/Backhaul/Roaming
- ## Wi-Fi Monetization
  - Location Based Analytics, WiFi Sensing, IT to OT

How to Stay Connected?

Access Course Webpage

Click here: Wi-Fi Technology Fundamentals Course (candelatech.com)

✓ Access course notes, slides, video recordings

Register to Get Updates

Click Here: Registration (zoho.in)

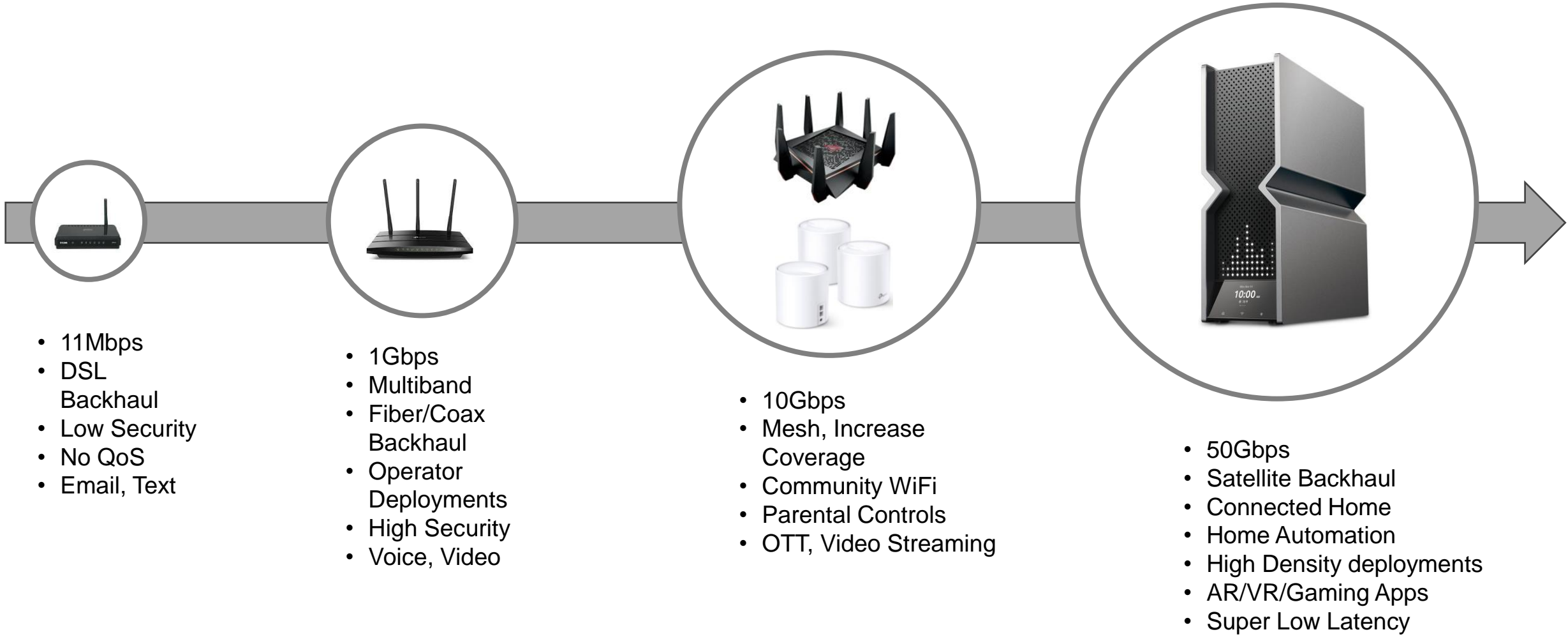✓ Provide basic contact into to get calendar invites, reminders and updates about the material and sessions.

Join Whatsapp Group

Click here: WhatsApp Group Invite

✓ Provide basic contact into to get whatsapp messages about calendar invites, reminders and updates about the material and sessions.

Residential WiFi Router Evolution

- 11Mbps
- DSL Backhaul
- Low Security
- No QoS
- Email, Text

- 1Gbps
- Multiband
- Fiber/Coax Backhaul
- Operator Deployments
- High Security
- Voice, Video

- 10Gbps
- Mesh, Increase Coverage
- Community WiFi
- Parental Controls
- OTT, Video Streaming

- 50Gbps
- Satellite Backhaul
- Connected Home
- Home Automation
- High Density deployments
- AR/VR/Gaming Apps
- Super Low Latency

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Residential WiFi Managed and Unmanaged

- Most residential WiFi networks are fully managed, where the operators provide the Modem and the WiFi router
- The routers and modem are remotely managed by the operator and the network installation and testing is also done by the operator.
- In some cases the WiFi networks can be unmanaged when the users purchase their own WiFi routers and setup their own WiFi network.

ISP home network components

Some internet service providers offer a single device to cover all home network functions, but some providers may not, which requires customers to build out their networks.

| NETWORK FUNCTIONS	ISP CUSTOMER PREMISES EQUIPMENT OFFERINGS		
	Access only	Basic networking	All-in-one device
Access Allows access to ISP's network	✔	✔	✔
Router Manages inbound and outbound traffic		✔	✔
Switch Manages wired traffic in your home		✔	✔
Access Point Manages wireless traffic in your home			✔
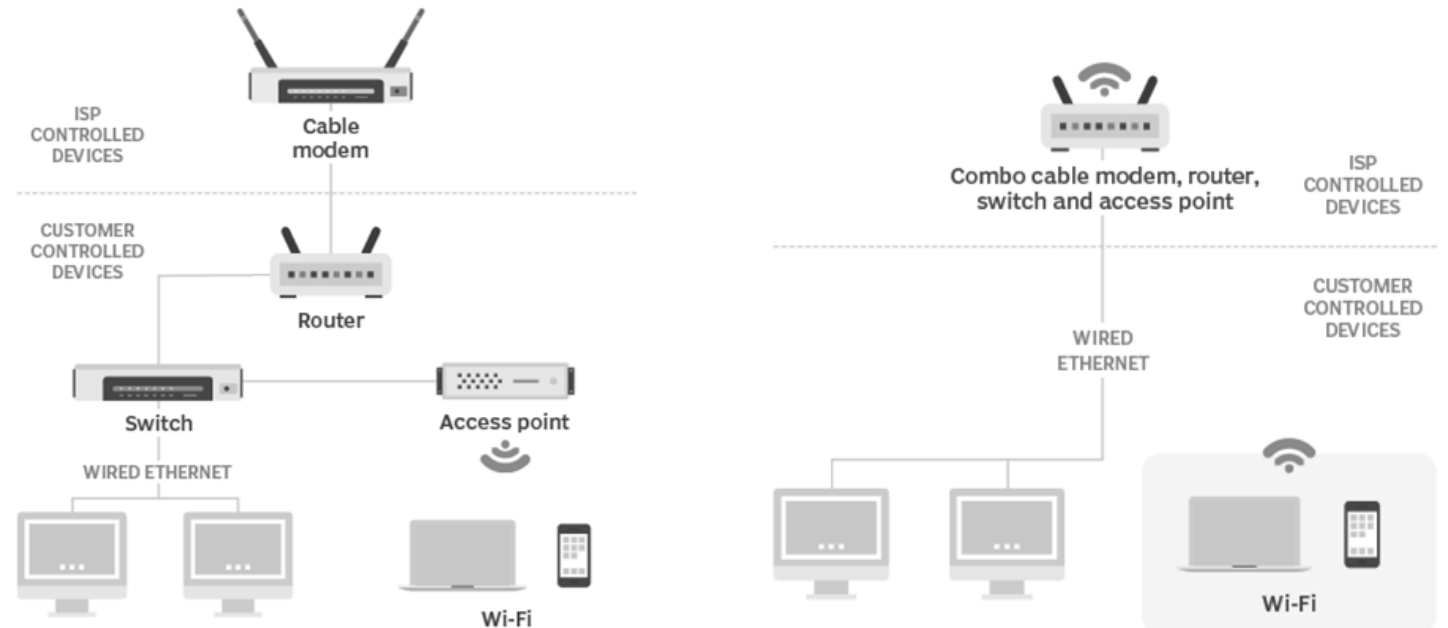
Parental Controls/Smart WiFi Features

- Track all devices in the home
- Customize internet usage per family member of group of members or guests
- Set Screen Time Limits
- Track usage history and website history per user
- Filter content based on user and age group
- Pause WiFi
- Location Tracking
- Set bedtimes
- Set rewards

Wi-Fi Smart Home/Home Automation

- The concept of the smart home automation is to be able to seamlessly control and configure various smart devices in the home that use various wireless access technologies and protocols
- The main building blocks of a smart home are:
  - Home Media Gateway/Hub,
  - WiFi Router
  - Smart Speaker/Controller
  - Smart home apps
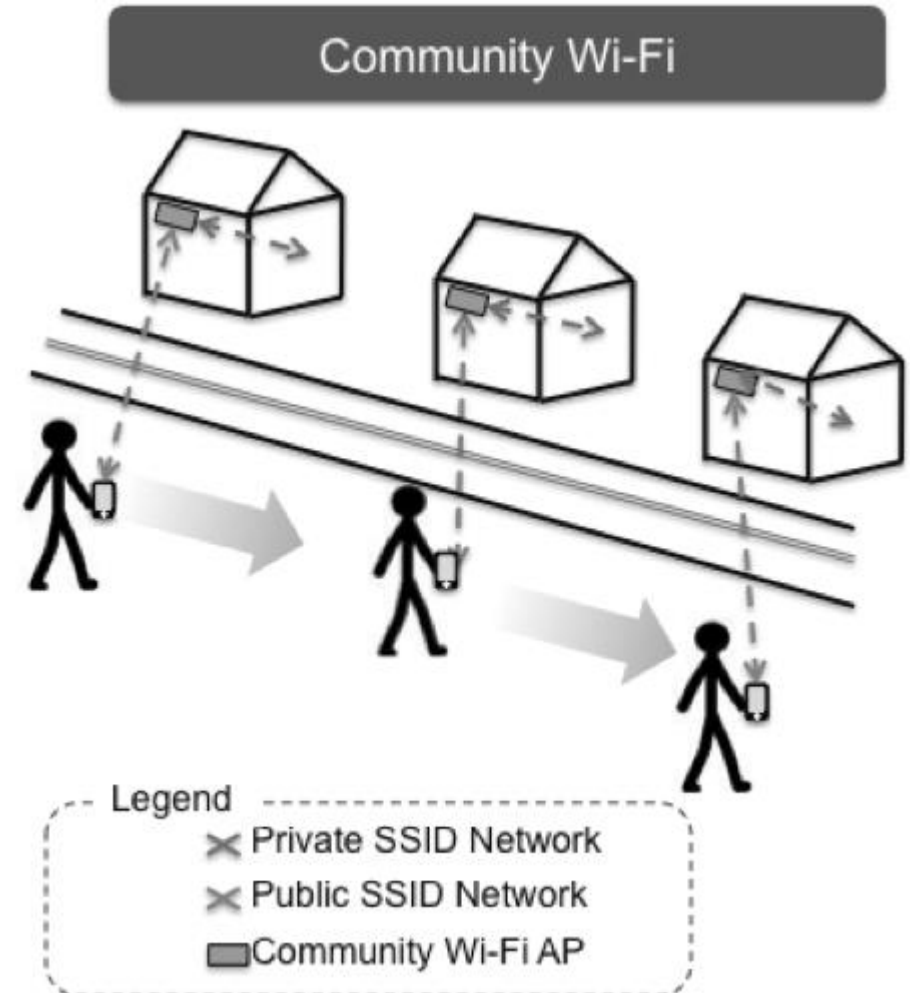 - Appliance/Device provider Cloud
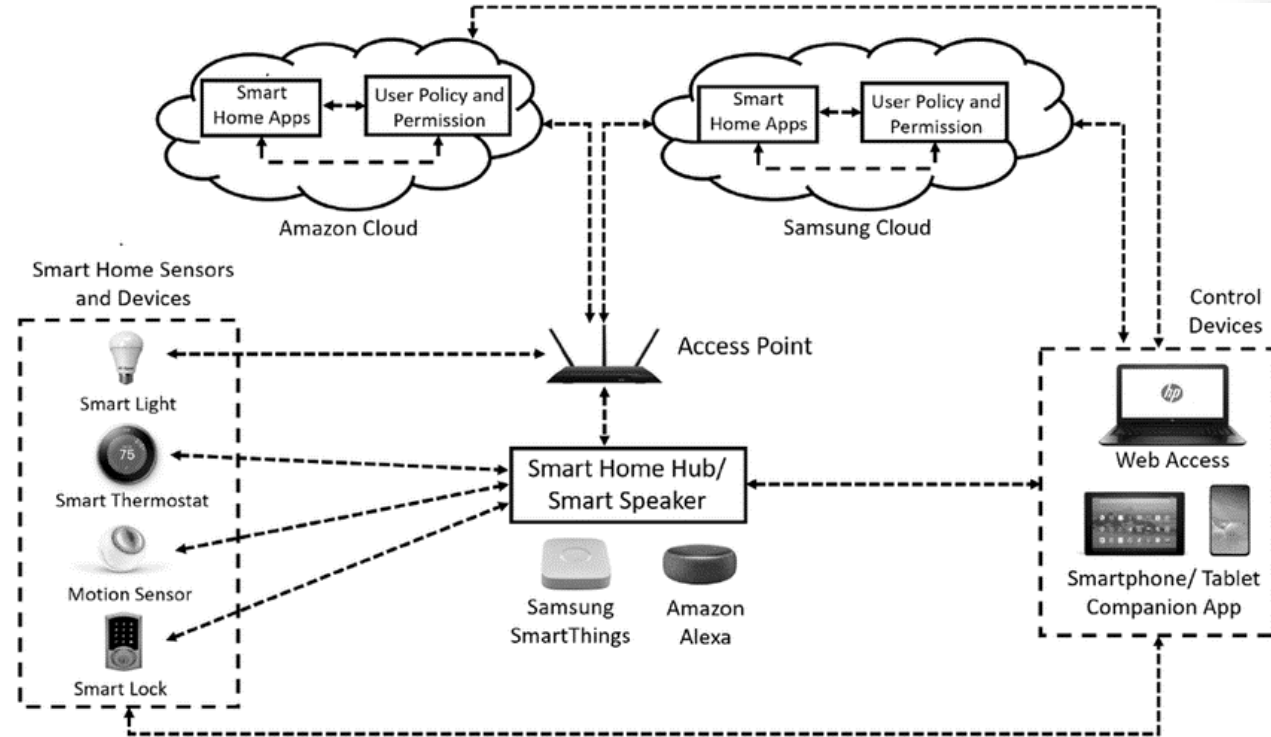
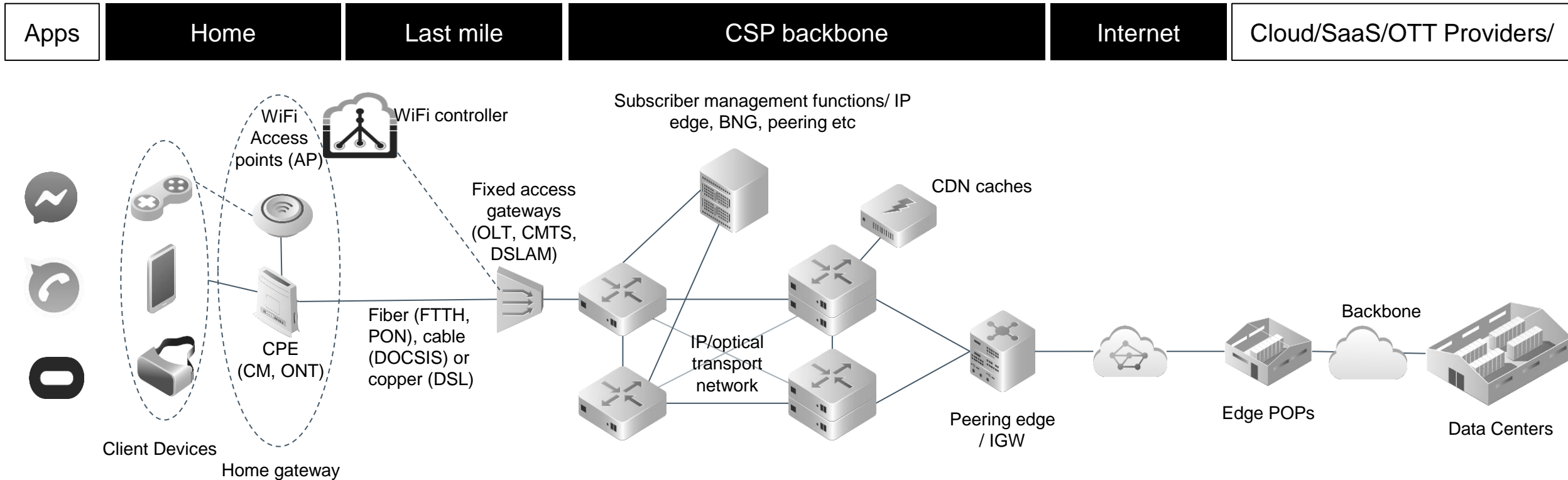One Smart Home.
One App.
Complete control at your fingertips

- Smart home systems can be provided and managed by the same service provider providing internet access and WiFi.
- Or smart home system can be purchased from third party solution providers and setup and self managed on an operator WiFi network.

Community WiFi Networks

- Most modern residence have 1Gbps fiber links coming to the houses.
- Some of this bandwidth can be opened up for community use in the form of community WiFi networks
- These networks need to be secure and should can cause any disruption to the home WiFi network.
- Operators can provide a community WiFi network SSID that the by passers can connect to using the service provider credentials.
- Operators make sure that the home WiFi network does not get effected by community use of the in home router.

Operator Managed Residential Networks

Apps	Home	Last mile	CSP backbone	Internet	Cloud/SaaS/OTT Providers/

WiFi Access points (AP)

WiFi controller

Subscriber management functions/ IP edge, BNG, peering etc

Fixed access gateways (OLT, CMTS, DSLAM)

CDN caches

Fiber (FTTH, PON), cable (DOCSIS) or copper (DSL)

CPE (CM, ONT)

IP/optical transport network

Backbone

Peering edge / IGW

Edge POPs

Data Centers

Client Devices

Home gateway

- Operators manage the network end to end.
- The network provisioning, configuration, accounting, troubleshooting, customer support are all handled in a centralized fashion.
- OTT video services, Smart home automation, home security services can all be bundled into a managed services offering by the operators.
- Operators can also offer cellular failover, community WiFi and other managed WiFi features.

Enterprise WiFi Network Evolution
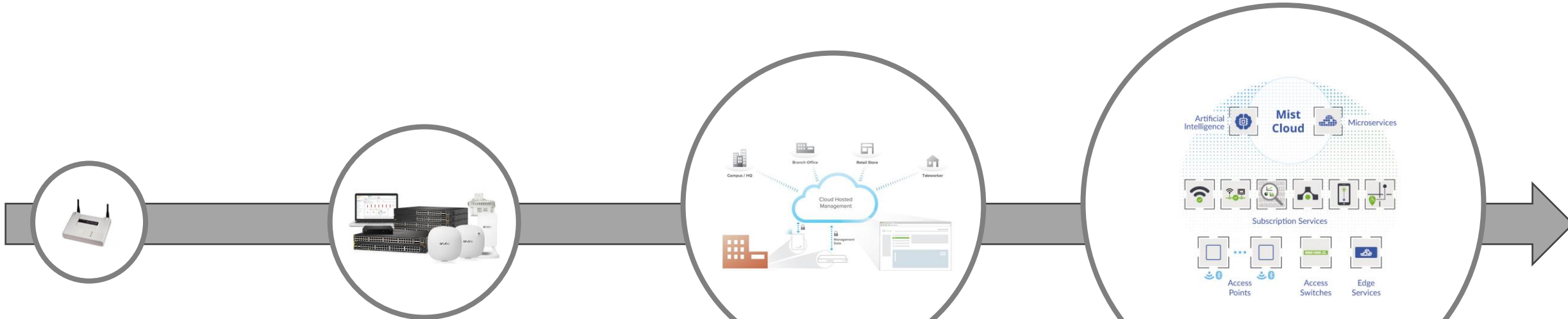

- 11Mbps
- Low Security
- No QoS
- Email, Text

- 1Gbps
- Controller based APs
- Large Scale Deployments
- High Security
- Web conferencing, VOIP

- 10Gbps
- Cloud Managed APs
- Centralized Control
- Analytics and Business Intelligence
- Video, Web Conferencing

- 50Gbps
- High Density Deployments
- IOT
- AI/ML in WiFi
- Network as a Service
- AR/VR
- WiFi Sensing

Enterprise WLANs Basic Network Topology

- Enterprise WiFi networks normally have several APs, Switches and Routers and a WLAN Controller.
- Enterprise WiFi networks can be deployed using the following deployment methods
  - **Autonomous APs**
  - **Light-weight APs**
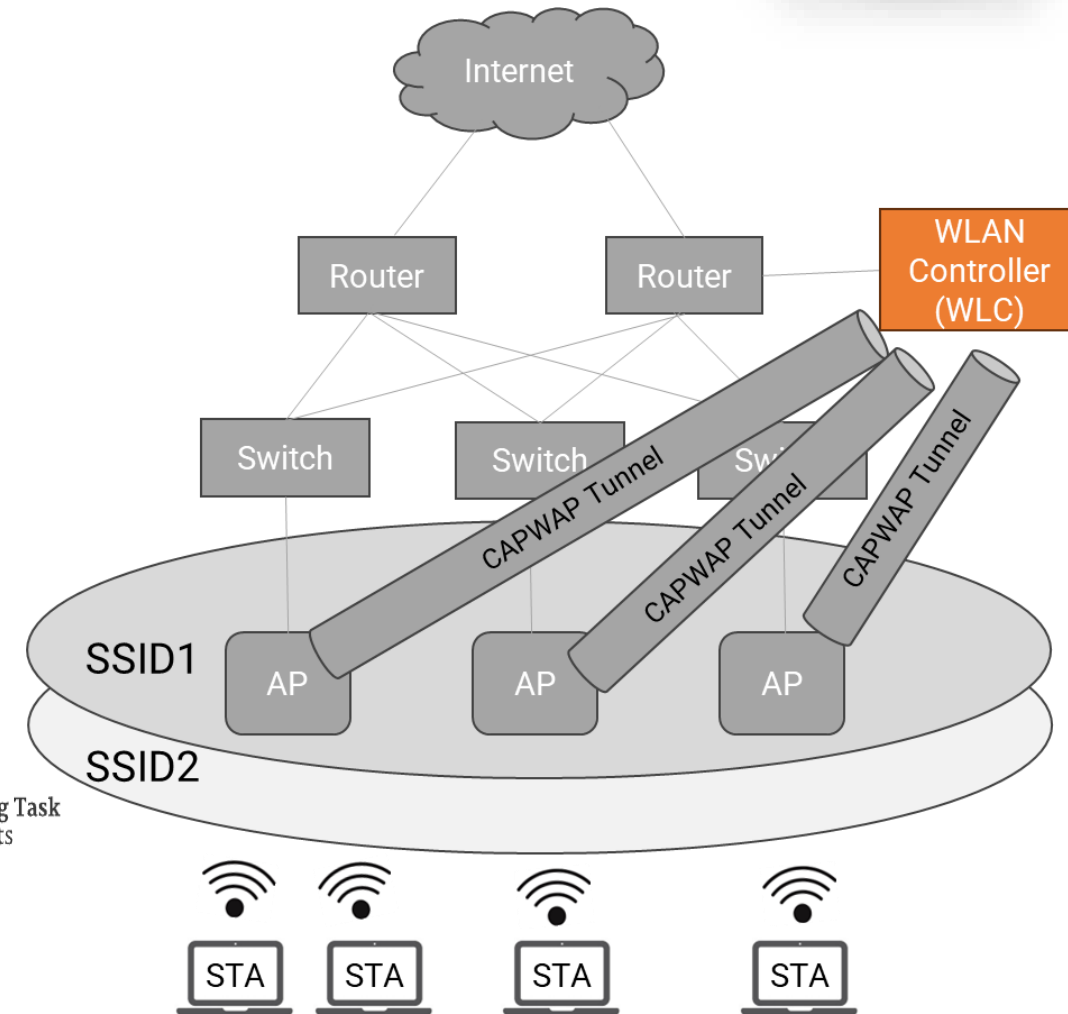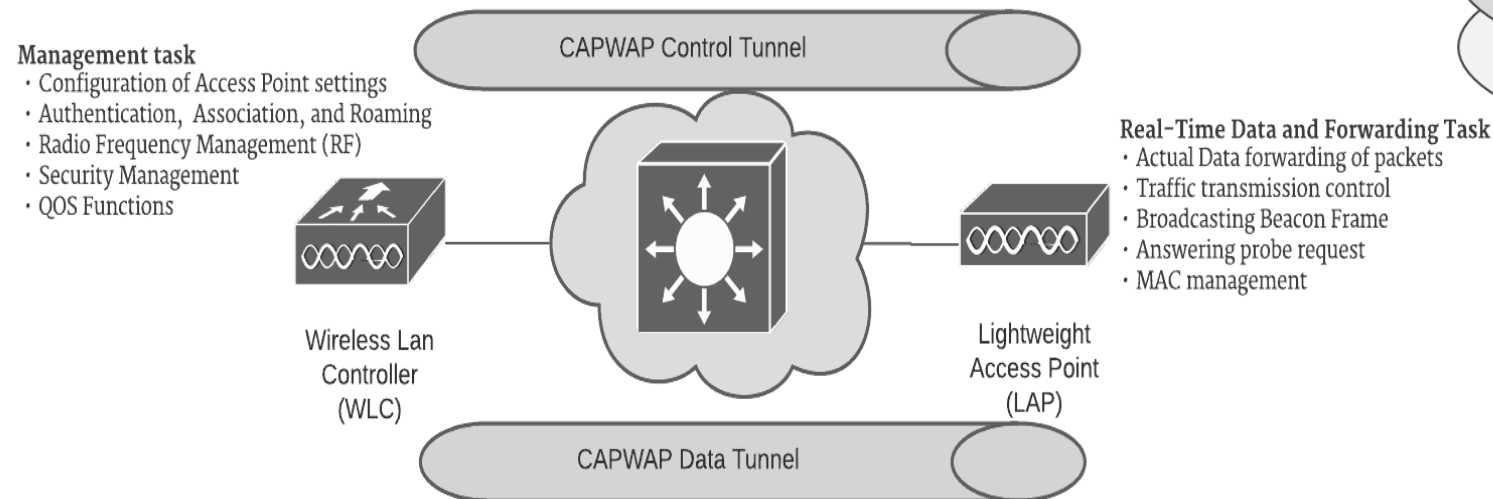 - **Cloud-based APs**
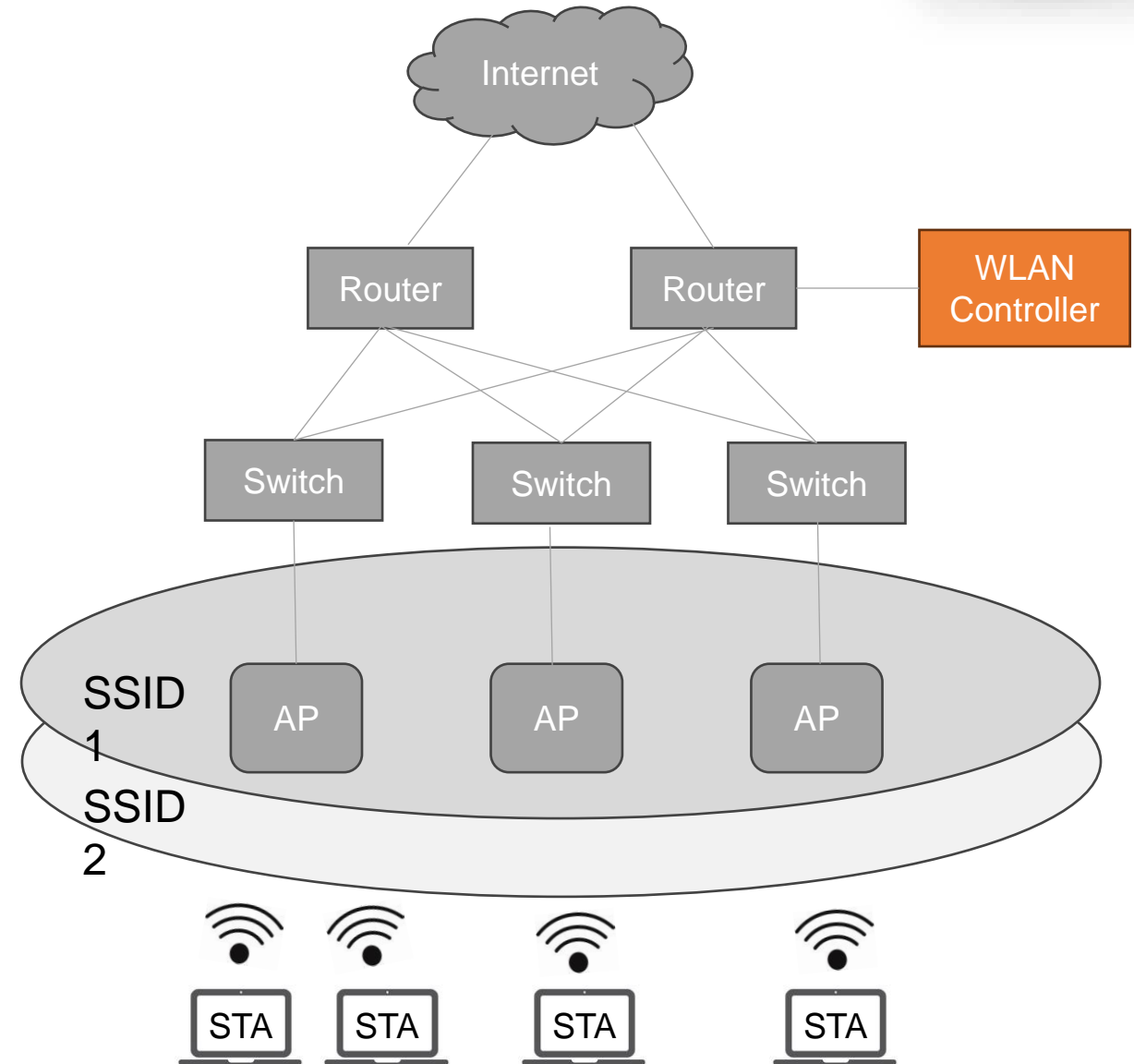
Autonomous APs

- Self contained APs that don't rely on WLAN controller for configuration.
- Each AP can be individually configured using SSH, Telnet, Console, HTTP/Web GUI
- Each AP needs to have a management IP address to configure it from the network.
- All RF parameters like transmit power, channel etc…should be manually configured on each AP.
- All security settings, MAC level features, firmware upgrades etc.. should be individually done on each AP.
- SSIDs need to be mapped to VLANs and each VLAN needs to span the entire network.
- There needs to be a separate management VLAN to manage all the APs.
- These VLANs have to be spread across the entire network which is normally a bad practice as it will create large broadcast domains.
- Only viable for small enterprise networks such as SOHO environments.

VLAN1(Data): SSID1
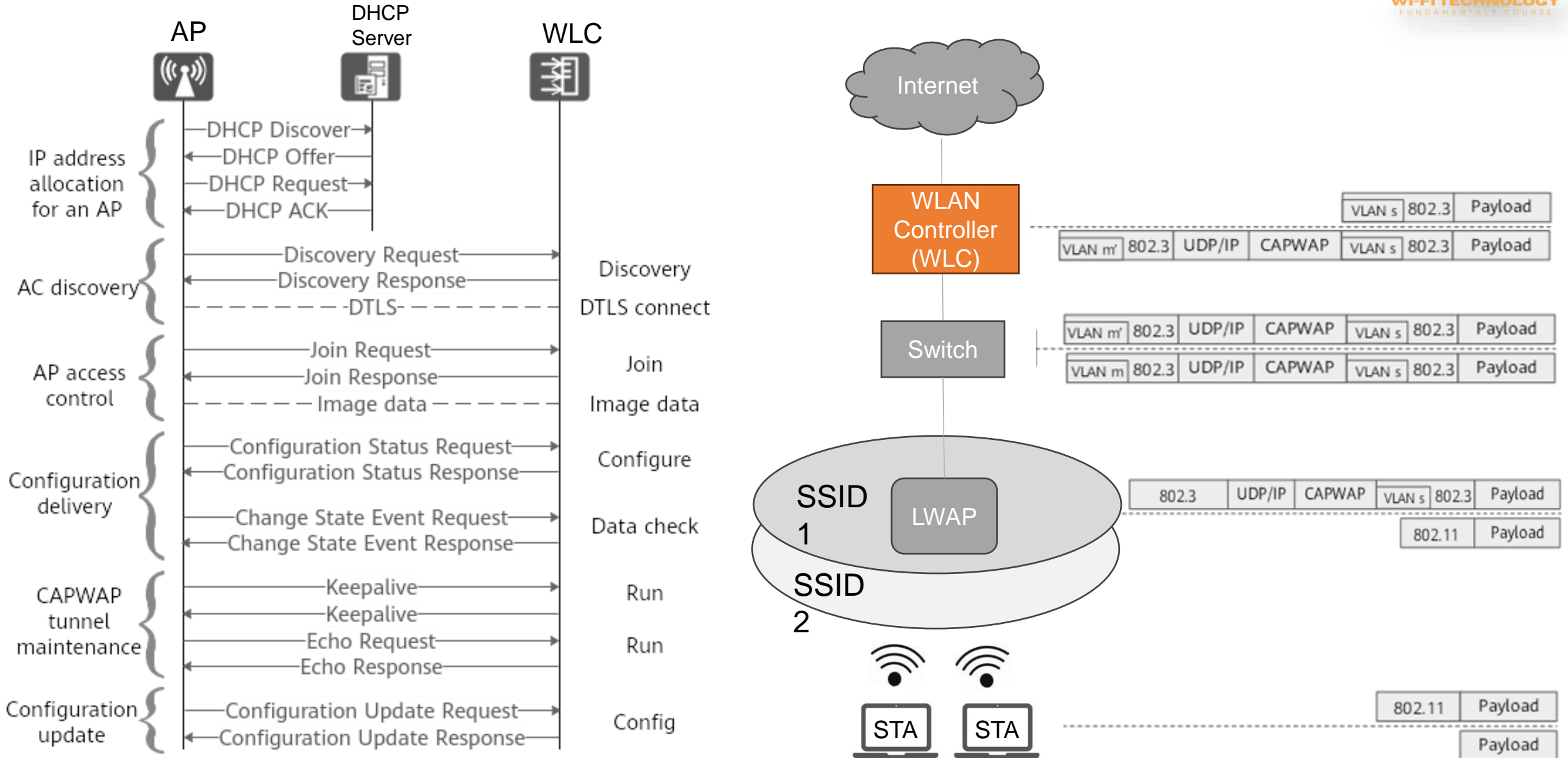VLAN2(Data): SSID2
VLAN3(Management)
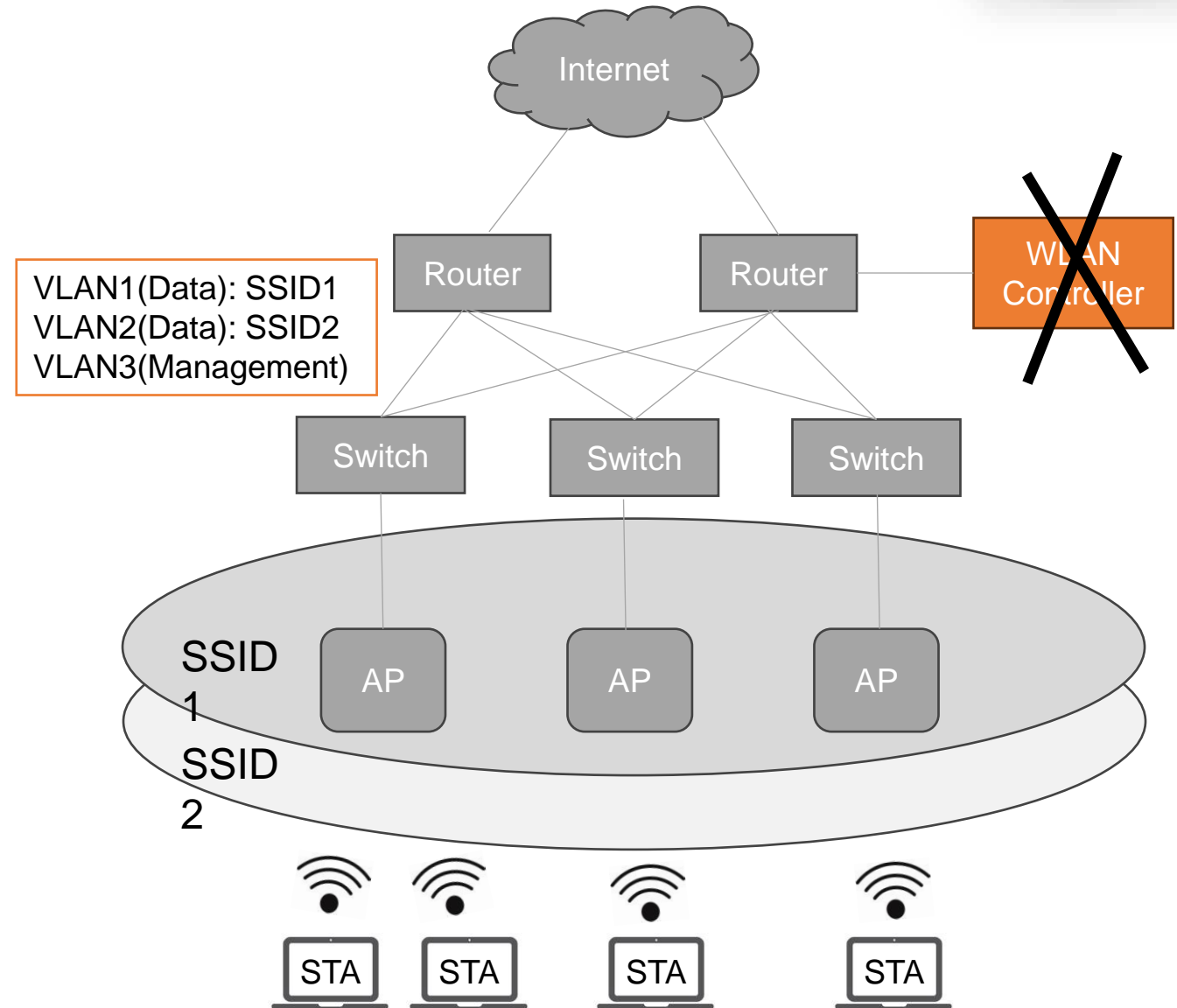
Light Weight APs

- All APs are managed by a WLAN controller on the network.
- Uses split MAC architecture where the lower MAC functions are done by the AP and the upper MAC functions are moved and centralized into the controller.
- APs perform functions such as client association, sending out beacons/probes, encrypting data, sounding, MU-MIMO/OFDMA, aggregation, ACKs etc..
- Functions such as RRM, QoS Management, Load balancing, traffic shaping/policing, mobility, authentication/security etc…are handled by the controller.
- The WLC and the APs uses a protocol called CAPWAP (Control and Provisioning of Wireless Access Points) to communicate with each other.
- Two tunnels are established:
    - Control Tunnel for all the control/management of the APs. All traffic on this tunnel is fully encrypted.
    - Data Tunnel for all the Data from/to APs pass through the controller.
- Light Weight APs with WLC is ideal for large scale uniform network deployments where its more efficient to reduce the cost of the AP hardware and push most of the intelligence and configurability into a centralized controller.
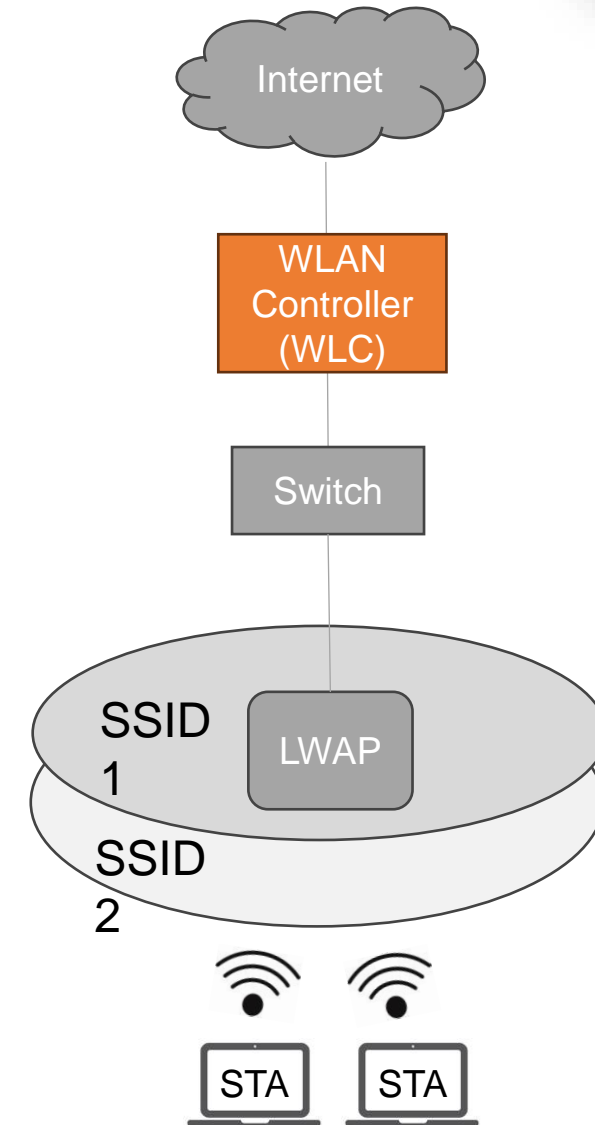

Management task
- Configuration of Access Point settings
- Authentication, Association, and Roaming
- Radio Frequency Management (RF)
- Security Management
- QOS Functions

CAPWAP Control Tunnel

Real-Time Data and Forwarding Task
- Actual Data forwarding of packets
- Traffic transmission control
- Broadcasting Beacon Frame
- Answering probe request
- MAC management

Wireless Lan Controller (WLC)

Lightweight Access Point (LAP)

CAPWAP Data Tunnel

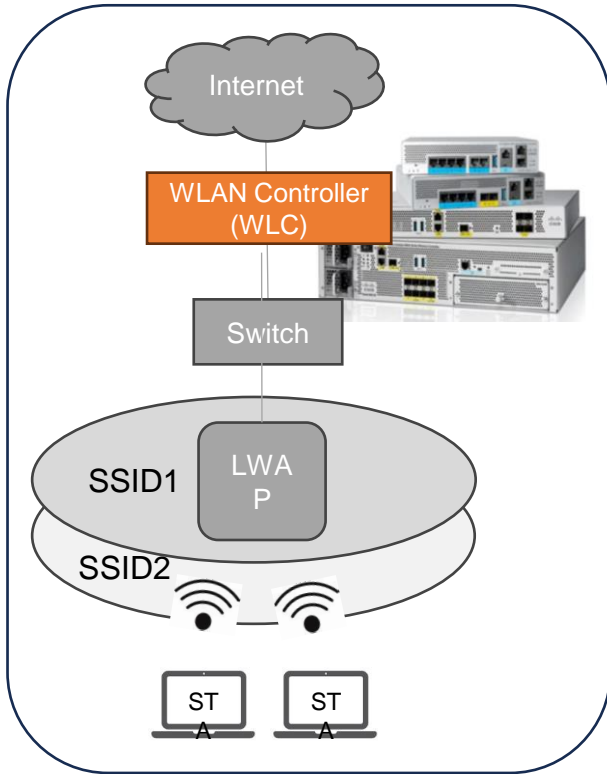# CAPWAP Connection and Encapsulation

Light Weight APs Modes

- Light weight APs can be configured in the following modes:
  - **Local** – Offers one or more BSSs and connects and provides network access to STAs. Control and Data plane traffic flows through CAPWAP tunnel to WLC
  - **FlexConnect** – APs behave like local APs by default but switch into Autonomous mode when connection to WLC is lost.
  - **Sniffer** - Does not offer BSS, but strictly acts as a device that capture packets on the air and sends them to controller for processing.
  - **Monitor** – Does not offer BSS, but continuously monitors the air to collect information about Rogue devices, collect other data and telemetry information for smart analytics and send that information to the WLC
  - **Spectrum Expert** – Does not offer a BSS. It uses all the radios to conduct detailed spectrum analysis across all the channels and bands and provide that information to WLC to help with spectrum analysis which is in turn used for better channel planning and RRM.
  - **Bridge/Mesh** – AP can be configured as a bridge or a mesh node that will wirelessly extend the range of another network.
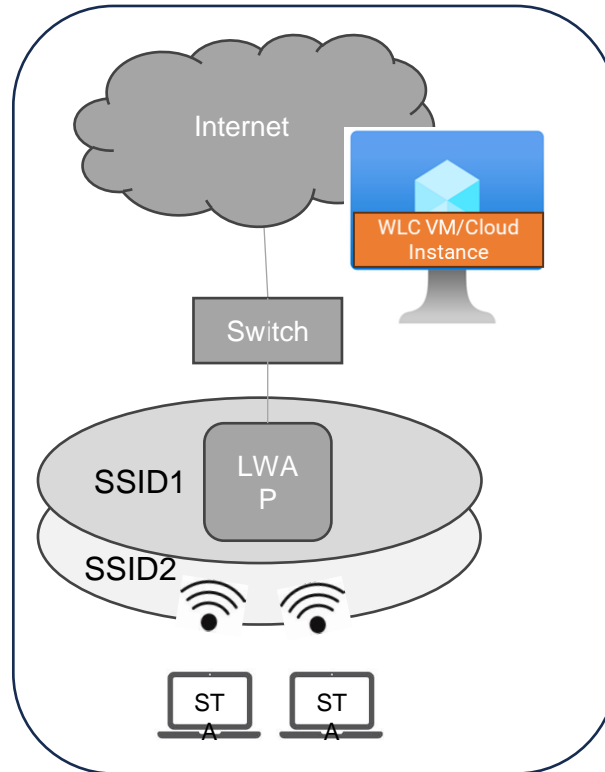
# WLAN Controller (WLC) Deployment Models

Internet | WLAN Controller (WLC) | Switch | SSID1 | SSID2 | LWAP | STA | STA

Internet | WLC VM/Cloud Instance | Switch | SSID1 | SSID2 | LWAP | STA | STA

Internet | Switch | WLAN Controller (WLC) | SSID1 | SSID2 | LWAP | STA | STA

Internet | Switch | SSID1 | SSID2 | LWAP | WLC | STA | STA

Unified WLC

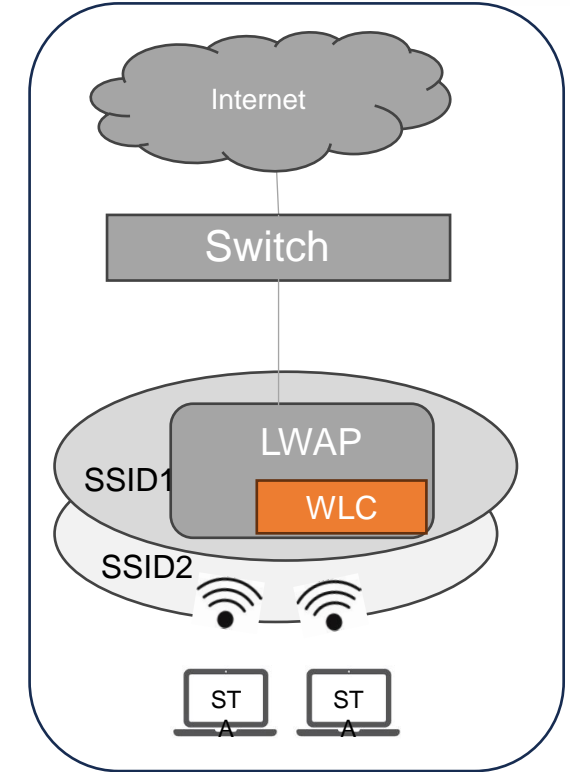- Physical controller location on premise
- Supports 1000s of APs

Cloud based WLC

- Controller instance hosted on VMs in the cloud or on premise.
- Not a cloud controller but yet not a physical box.
- Can support 1000s of APs
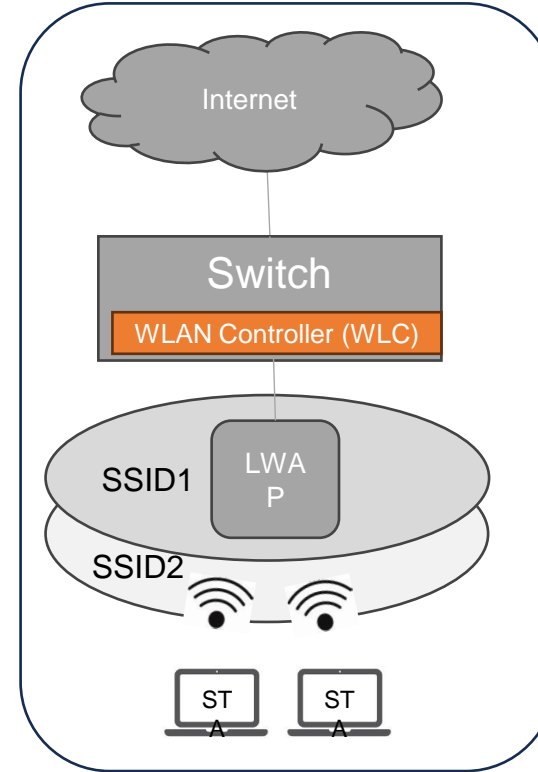
Embedded WLC

- Controller embedded in the local switches
- Can support a couple of hundred APs.
- Not meant for large networks

Mobility Express

- Controller embedded in one or more APs.
- Multiple APs can share the controller tasks
- Meant for small installations

Cloud Controller

- Autonomous APs that are centrally managed by the cloud.
- Architecture is somewhere in between fully standalone and light weight APs.
- This model is ideal for distributed enterprises with 100s of smaller sites around the world.
- The data plane traffic is not sent to the cloud.
- Cloud controller can do all the configurations and also get all the metrics, analytics etc from the APs in order to properly manage the networks.

Browser-based management
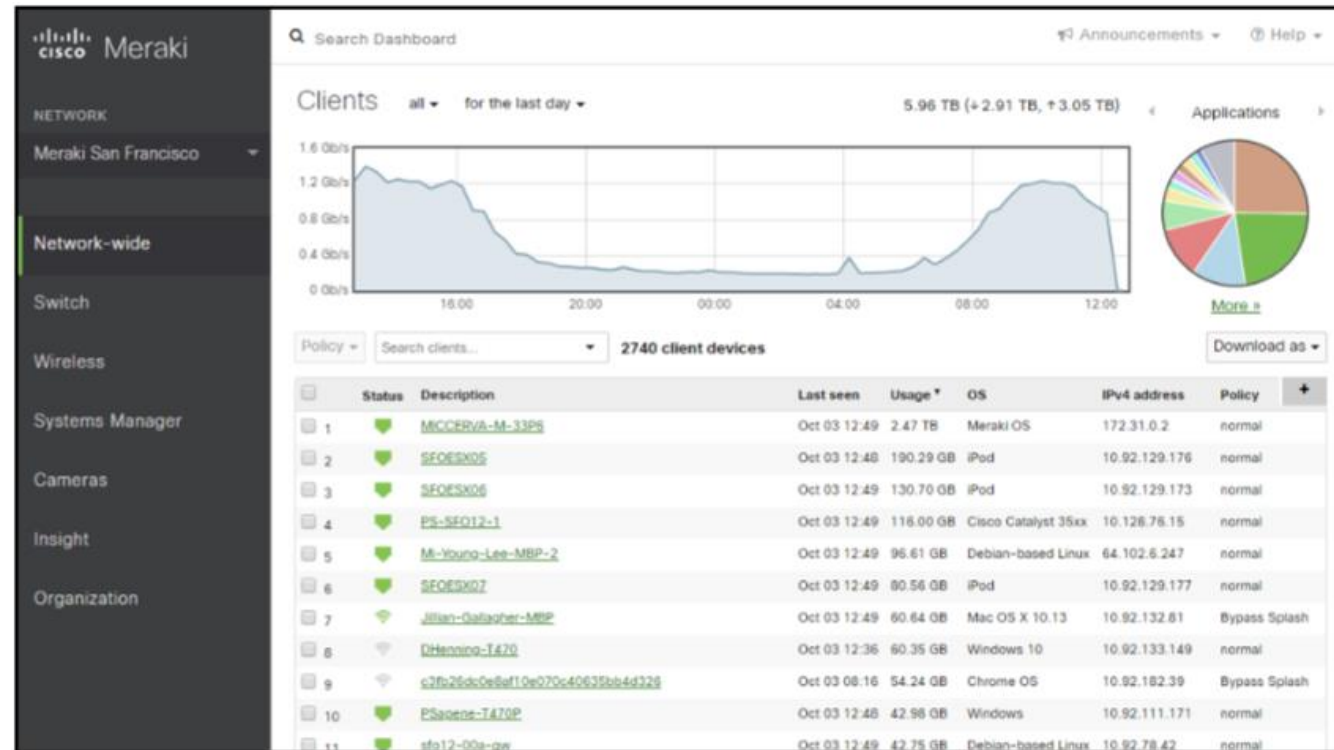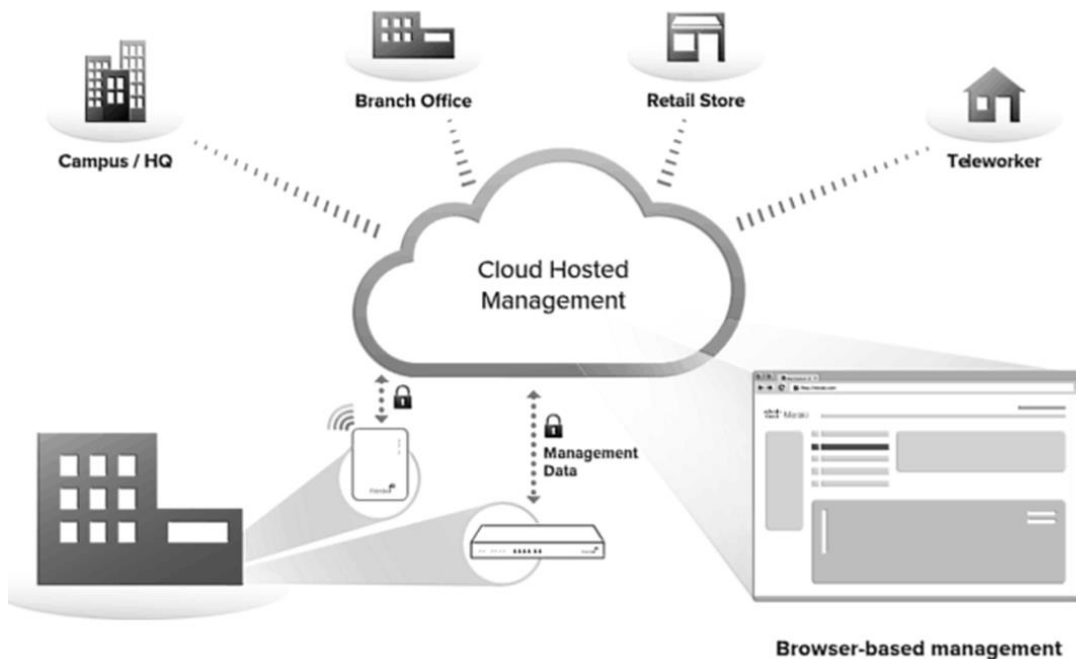

Cloud Controller Dashboard

AI/ML in Cloud Controllers

Wired, Wireless, and WAN Network Insights

- Networks insights on wired and wireless
- Security insights–rogues and honeypots
- Client connections–trend and counts
- Application visibility from Juniper Mist Wireless
- Queries (rank, list, trend, and counts)
- Custom queries–Unique devices on multiple WLANs (trend and counts)
- Average and historic service-level expectations beyond 7 days
- Trend reports for applications, traffic, and clients
- Insights on device OS and device manufacturer
- Traffic metrics on the basis of SSID, switch, switch interfaces, or WAN zones
- Access point ranking by clients and traffic
- Wireless security threat distribution and rogue access point trends
- Audit log reports for longer period
- Inventory reports
- WAN visibility for link QoE and application QoE

Engagement Analytics

- Visitor segmentation and reporting based on user-defined dwell times
- Dwell time that includes trends and averages for predefined labels for visitor segmentation
- Unique visitor trends based on predefined labels for visitor segmentation
- Dwell and visits per site, floor, and department
- Visitor segmentation between new and repeat based on a fixed, 7-day rolling window
- Heat maps including real-time and historical replay of visits and dwell times
- Visitor segmentation between new and repeat based on flexible and configurable time duration
- Data segmentation and reporting based on dynamic aggregation of dwell times for visitor segmentation
- Dwell time that includes trends and average for dynamically defined labels for visitor segmentation
- Unique visitor trends based on dynamically defined labels for visitor segmentation
- Ability to reprocess historical data sets based on changes in criteria
- Popular motion paths including traffic flows between zones
- Ingestion and reporting with location and third-party data such as sentiment, weather, and so on
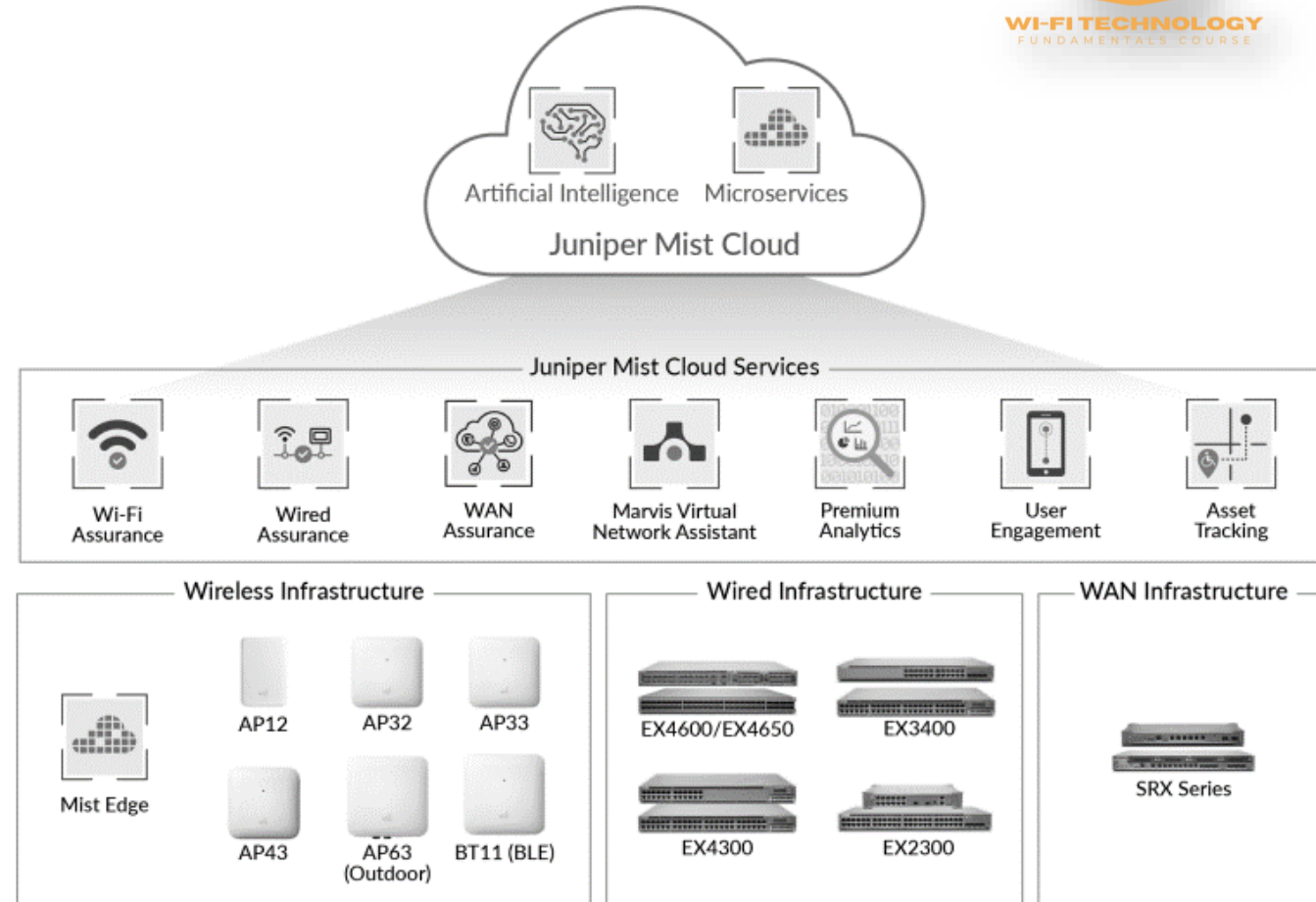
Proximity Tracking

- Ability to rewind and replay the location history of individuals
- Ability to identify users who were in close proximity to a selected individual
- Ability to identify encounter duration
- Ability to customize encounter duration and historic timeframes
- Heat map of zone occupancies based on preconfigured maximum capacity restrictions

Disaggregated Open Source Controller Technology - OpenWiFi
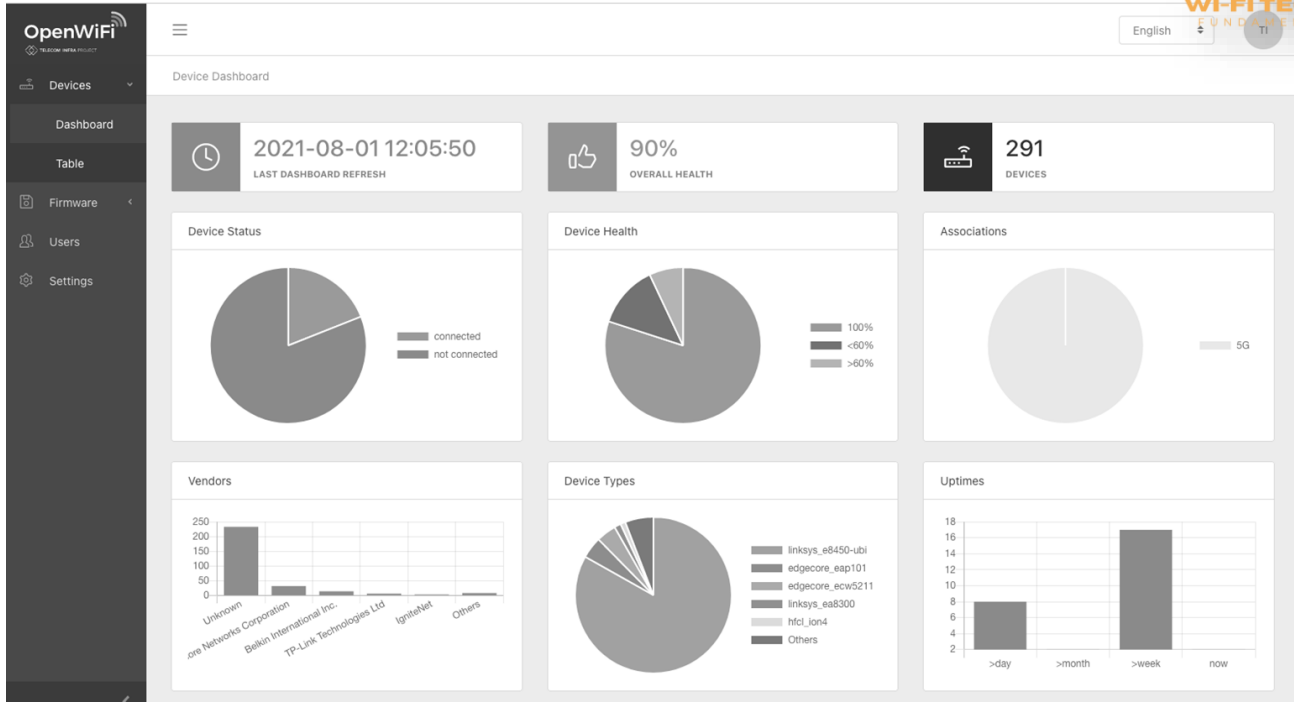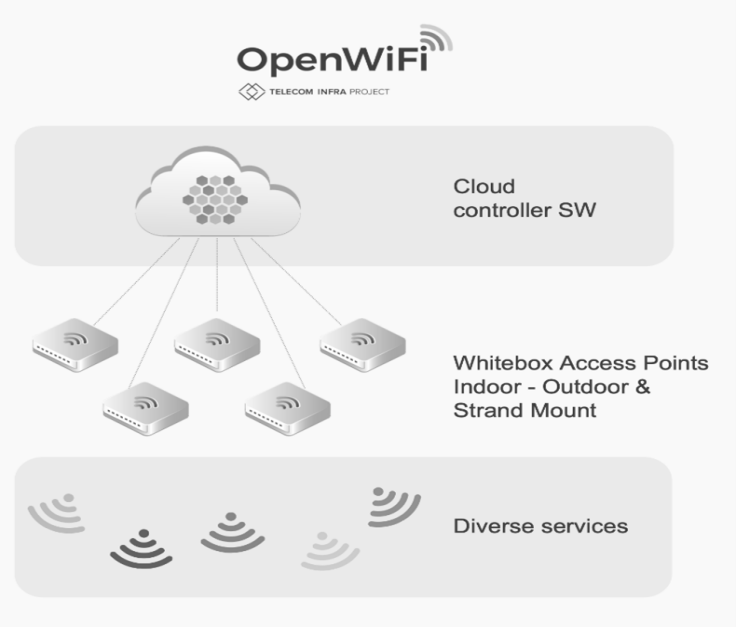
APs Interacting with Controller
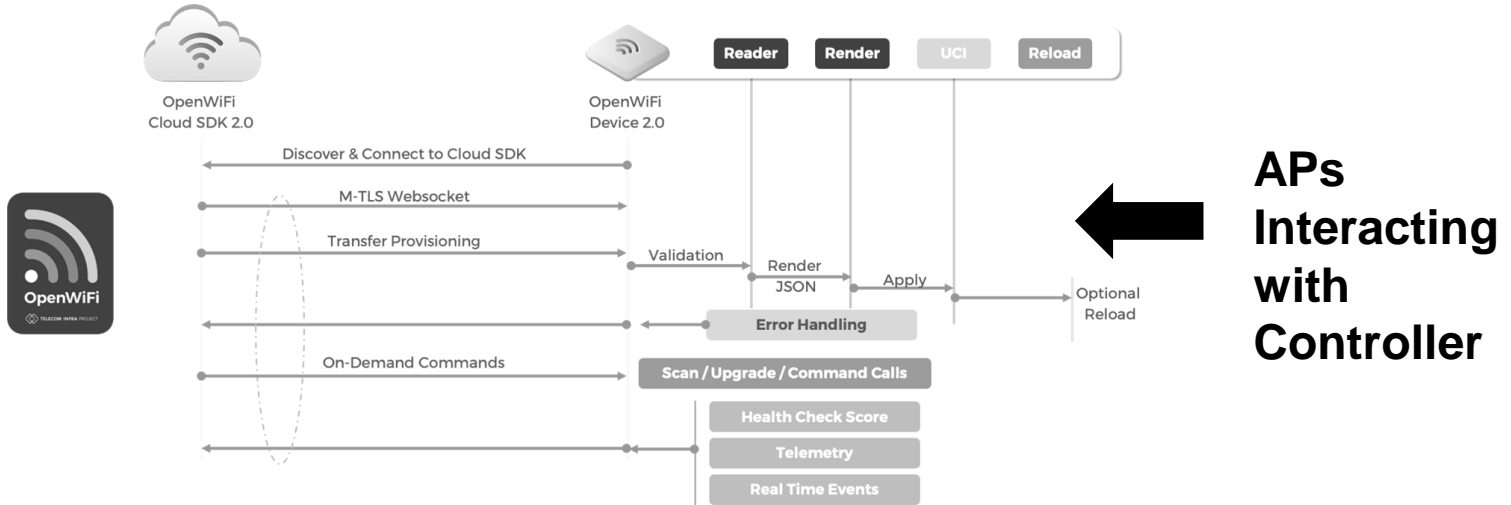
OpenWiFi Features
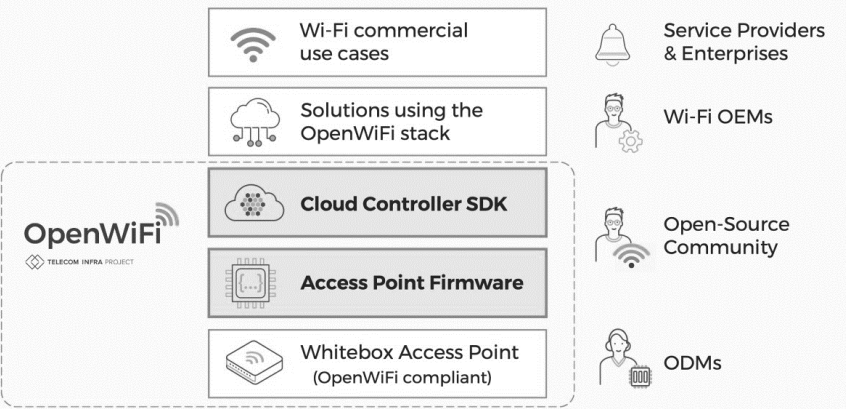
Each OpenWiFi AP offers:
- Multiple topologies including:
  - Local Breakout
  - Overlay including PPPoE, L2TP, L2oGRE
  - IEEE802.11s Mesh and Wireless Distribution System
  - Bridging, Virtual LAN, VxLAN, NAT Gateway
- Multi auth including WPA, WPA2, WPA3, Enterprise Radius models, M-PSK
- Passpoint R1 and R2 Mobile Offload
- Encrypted Zero Touch Provisioning and Cloud Discovery
- Autonomous RRM and Channel Control
- Wi-Fi Agile Multiband
- Multi-VAP including topology features per VAP
- Dynamic Air Time Fairness
- Over the air EDCH QoS, WMM QoS, 802.11-2016 Enterprise QoS
- Captive Portal
- Station and Network Telemetry

Cloud SDK in OpenWiFi offers:
- Zero Touch Provisioning & Discovery
- Integration Northbound Interface (NBI) RESTful
- Data model driven OpenAPI design
- Enterprise Message Bus data access
- Cloud Native & Agnostic micro services
  - Gateway Southbound
  - Security Northbound
  - Firmware Management
  - Web User Interface
  - Provisioning/Analytics

OpenWiFi AP Detail List:
- Wi-Fi 5 (ac) Wi-Fi 6 (ax) Wi-Fi 6E
- Dual Bank Bootloader
- Multi-SSID per Radio
- SSID Authentications: WPA/WPA2/WPA3 - Mixed, Personal, Enterprise
- 802.1Q VLAN per SSID
- 802.1d Bridge Mode per SSID
- RADIUS Accounting, Interim-Accounting, NAS-IP, CUI
- Network Address Translation Gateway Mode Operation
- Network Time Protocol Client
- Management VLAN
- Wi-Fi 6 (ax) Specific
  - BSS Coloring
  - UL/DL OFDMA sub-carrier allocation
  - Channel Switch Announcement
- Wi-Fi General Features
  - WMM® - Wi-Fi Multi Media
    - UAPSD Procedures (Unscheduled Power Save)
    - Upstream/Downstream Queues & L3 DSCP
    - Over The Air QoS EDCH Procedures
- WMM-Admission Control (AC)
- WMM-Power Save (PS)
- Wi-Fi Optimized Connectivity
  - (ai) Fast Initial Link Support
- Wi-Fi Agile Multiband
  - (k) Client Radio Resource Management - Directed Steering
  - (v) Network Assisted Roaming
  - (r) Fast BSS Transition
- Protected Management Frames (PMF)
  - (w) Management Frame Encryption
- Channel Switch Announcement (CSA)
- Dynamic Frequency Selection & Transmit Power Control (DFS/TPC)
- Beacon Rate
- Min Client Noise Immunity
- Basic Rate Control
- De-Auth RSSI Control
- Burst Beacon Support
- Per SSID Client Rate Limiting

- **Additional TIP AP NOS Features**
  - ISP WAN Profiles (PPPoE, L2TP, L2oGRE)
  - Embedded Captive Portal (Local Splash non-auth)
  - Link Layer Discovery Protocol (LLDP)
  - Dynamic Airtime Fairness
  - Service Flow QoS
  - Wireline & Wireless Tracing (PCAP Cloud Remote Troubleshooting)
  - Health Check Reports
  - Local Provisioning over SSID (when Cloud or WAN down)
  - Multimedia Heuristics (Detection of Unified Communication Sessions)
  - SSID Rate Limiting
  - GPS Reporting
  - Autonomous RRM Client Steering
  - Client / AP / Network Metric Telemetry

Cloud SDK additional features
- **Provisioning**
  - Device Identity (Model, MAC, Serial Number)
  - Device Software Upgrade
  - Multiple SSID Configuration
  - Bandwidth Rate Control per SSID
  - Multi-Radio 2.4/5/6GHz control
  - AP Network Mode Control (Bridge/NAT mode)
  - Security (WPA-Personal/WPA & WPA2/3 Personal Mixed/WPA & WPA2/3 Enterprise Mixed/WPA2/3 Personal/WPA2/3 Enterprise/WEP)
  - VLAN per SSID
  - VxLAN port configuration
  - NTP Enable/Disable
  - RTLS (Location Services) Enable/Disable
- **RF Control**
  - IEEE802.11r Fast BSS Transition per Radio Control
  - IEEE802.11k RRM Radio Information per Radio Control
  - IEEE802.11v Network Assisted Roaming per Radio Control
  - RRM Location AP Channel (uChannel) Provisioning
  - RRM Location Client Steering (uSteer) Threshold Provisioning
- **Remote Troubleshooting and Service Assurance**
  - Syslog
  - Health Check Reports
    - Remote DHCP, RADIUS, UE Network Analysis
  - Remote TTY Shell
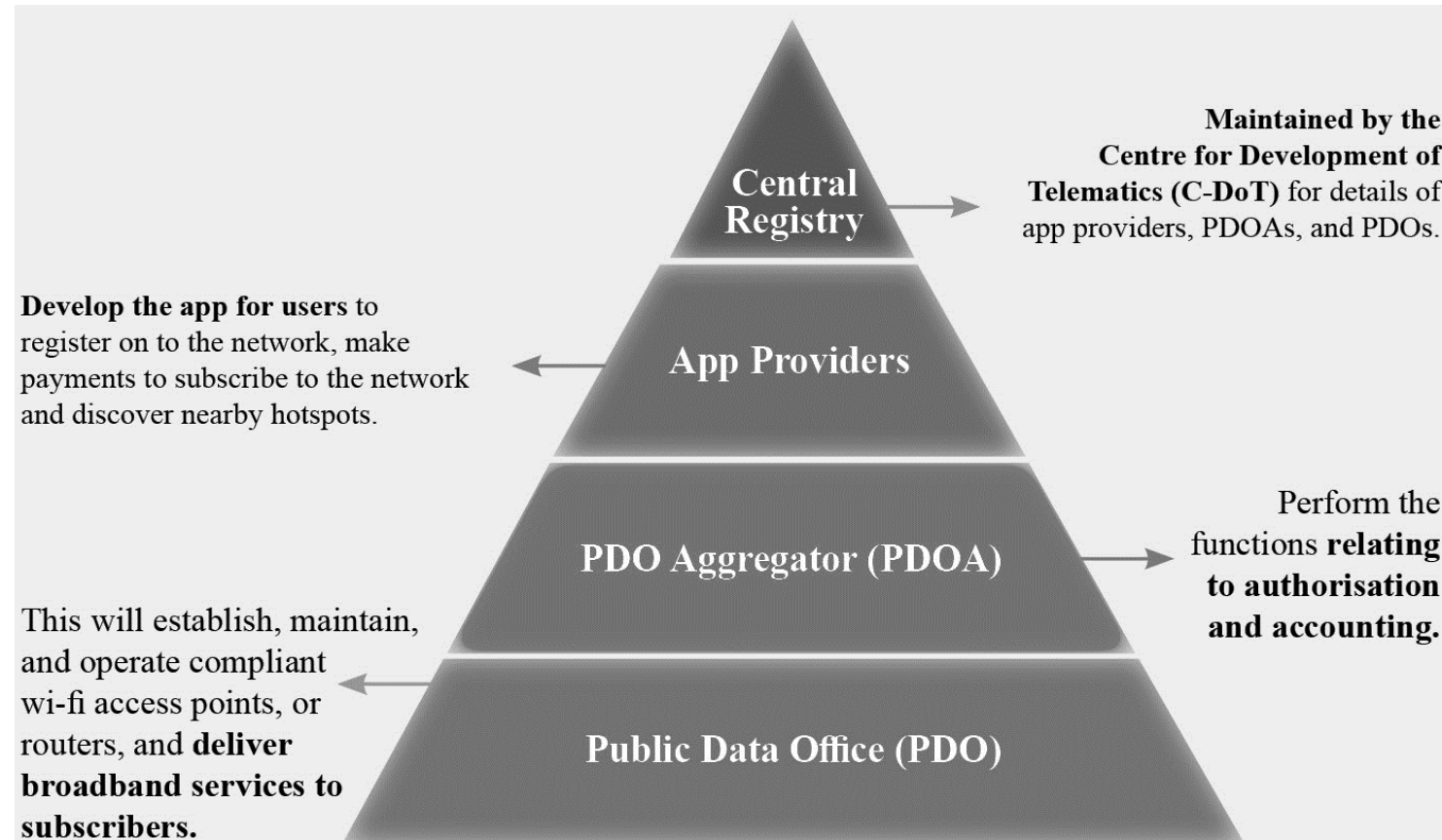 - Remote Packet Capture Analysis

PM-WANI Network

PM WANI (Wi-Fi Access Network Interface) is a scheme meant to increase Wi-fi access throughout the country. The WANI framework contains the following components:

- **Public Data Office (PDO):** It will establish, maintain, and operate only WANI compliant Wi-Fi Access Points and deliver broadband services to subscribers.
- **Public Data Office Aggregator (PDOA):** It will be an aggregator of PDOs and perform the functions relating to Authorization and Accounting.
- **App Provider**: It will develop an App to register users and discover WANI compliant Wi-Fi hotspots in the nearby area and display the same within the App for accessing the internet service.
- **Central Registry:** It will maintain the details of App Providers, PDOAs, and PDOs. To begin with, the Central Registry will be maintained by C-DoT.

The scheme shall work in the following manner:

- Any entity desirous of becoming a PDO sets up a Wi-Fi access point by purchasing network services from a service provider.
- The PDO registers with a PDOA that is registered on the App.
- Now, any potential user in the vicinity of a Wi-Fi access point, after registering and authenticating themself on the App, selects a PDO to connect to.
- This request is sent to the relevant PDOA who, after, authenticating the user, will display tariff plans to the user.
- Once the payment has been made to the PDOA, the PDOA registers the user and provides them with the requisite Wi-Fi access.

Central Registry — Maintained by the **Centre for Development of Telematics (C-DoT)** for details of app providers, PDOAs, and PDOs.

App Providers — Develop the app for users to register on to the network, make payments to subscribe to the network and discover nearby hotspots.

PDO Aggregator (PDOA) — Perform the functions relating to authorisation and accounting.

Public Data Office (PDO) — This will establish, maintain, and operate compliant wi-fi access points, or routers, and deliver broadband services to subscribers.

Source: https://internetfreedom.in/pm-wani-explainer/

References

WLC or Wireless LAN controller explained
https://www.youtube.com/watch?v=0lDiFNIKepM

Wireless Architecture: Free CCNA Course
https://www.youtube.com/watch?v=uX1h0F6wpBY

 About OpenWiFi
 https://openwifi.tip.build/

Meraki Cloud Controller Live Demo
https://meraki.cisco.com/form/demo/

Juniper Mist Premium Analytics
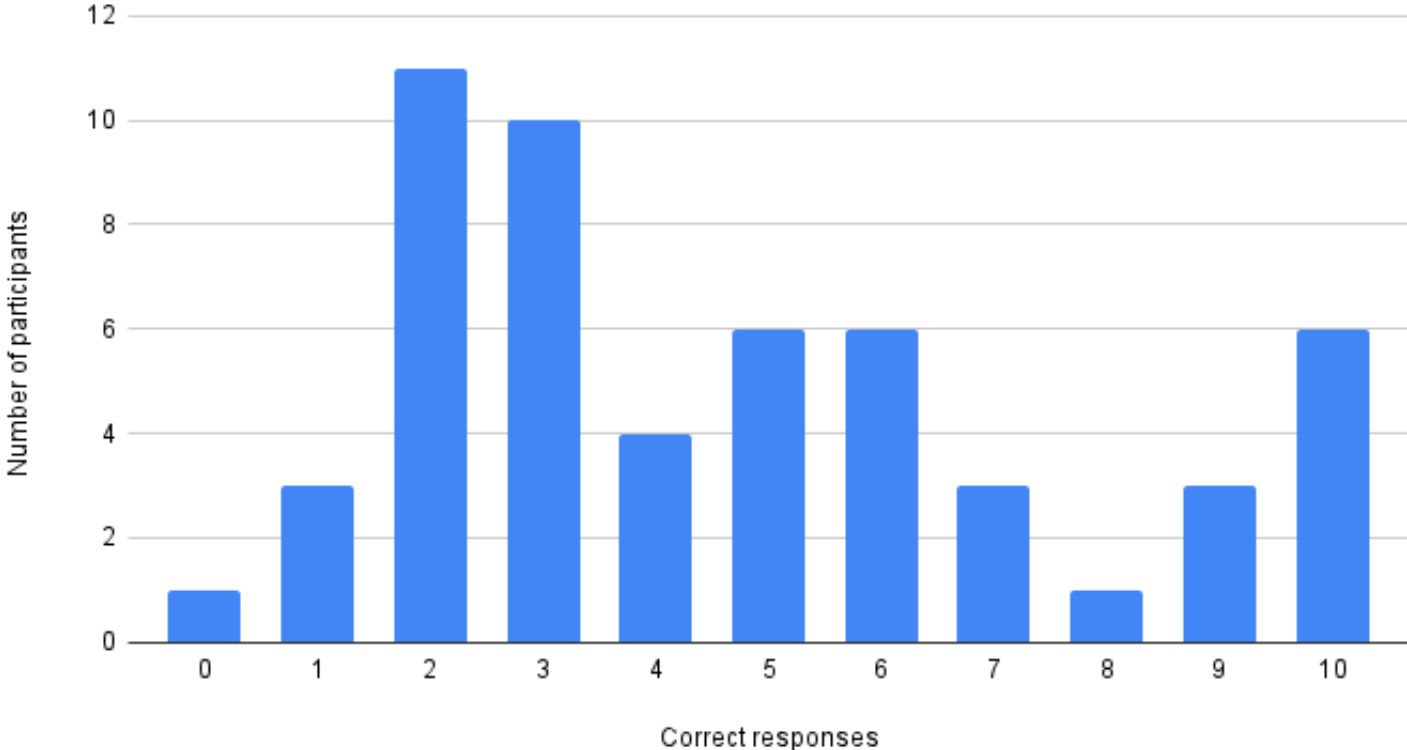https://www.juniper.net/us/en/products/juniper-mist-premium-analytics-datasheet.html

Quiz 5d Results

Shravani Jorrigala

Score distribution - quiz 5d

QUIZ!

?

TIME