Wireless Architectures

Client Association

Probe Request →
← Probe Response
Authentication Request →
← Authentication Response
Association Request →
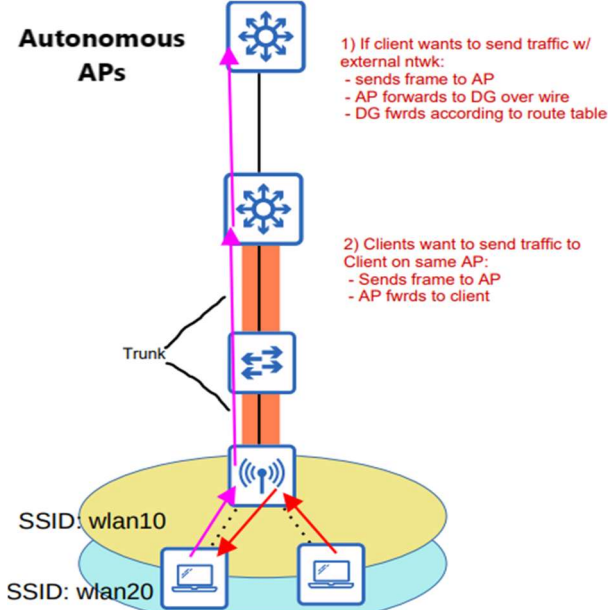← Association Response
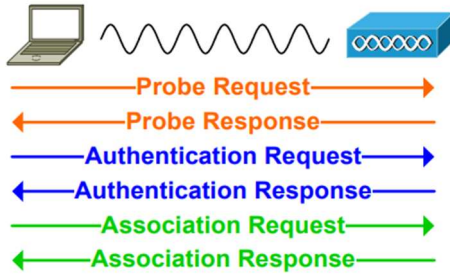
Three 802.11 message types:

1. **Management**: used to manage the BSS.

2. **Control**: Used to control access to the medium (radio frequency). Assists with delivery of management and data frames.

3. **Data**: Used to send actual data packets.

Type	Class
Association	Management
Authentication	Management
Probe	Management
Beacon	Management
Request to Send (RTS)	Control
Clear to Send (CTS)	Control
Acknowledgment (ACK)	Control
Data	Data

Three main wireless AP deployment methods: **1)** *Autonomous* **2)** *Lightweight* **3)** *Cloud-based*

---

1) **Autonomous**: Self-contained systems that do not rely on a WLC. Autonomous APs are configured individually. This type of AP management can also work as Repeater, Outdoor Bridge, and Workgroup Bridge.

Autonomous APs

1) If client wants to send traffic w/ external ntwk:
- sends frame to AP
- AP forwards to DG over wire
- DG fwrds according to route table

2) Clients want to send traffic to Client on same AP:
- Sends frame to AP
- AP fwrds to client

Trunk

SSID: wlan10
SSID: wlan20

2) **Lightweight**: In Lightweight APs (LAP), the function of AP is split between the AP and the WLC. This is also known as **split-MAC architecture**.

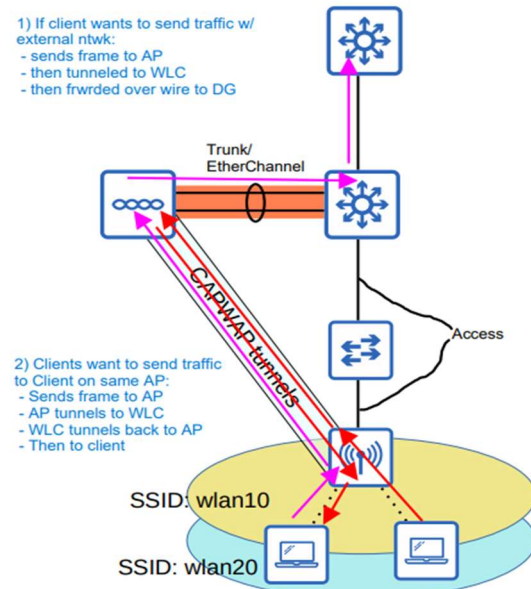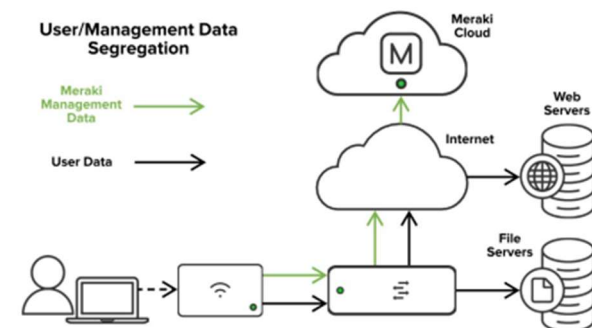| AP MAC Functions (real-time)	WLC MAC Functions (mgmt)
▪ Beacons and probe responses ▪ Transmitting/receiving frames (packets) over the RF ▪ Encryption of wireless frames	▪ Authenticating clients ▪ Managing client associations ▪ Processing clients that are roaming ▪ Assigning nonoverlapping channels ▪ Termination of 802.11 traffic on a wired interface

Traffic from clients flows via the AP through a **Control and Provisioning of Wireless Access Points (CAPWAP)** layer 3 tunnel to the WLC, and then enters the rest of the network via the WLC. The WLC do not need to be in the same VLAN as the LAPs.

The CAPWAP tunnel consists of two tunnels:
- *Control tunnel*: UDP port 5246, always encrypted.
- *Data tunnel*: UDP port 5247, can be encrypted or not.

The split-MAC architecture has several benefits, such as: Scalability, Dynamic channel assignment, transmit pore optimization, self-healing wireless coverage, seamless roaming, client load balancing, security/QoS management, etc.

1) If client wants to send traffic w/ external ntwk:
- sends frame to AP
- then tunneled to WLC
- then frwrded over wire to DG

Trunk/ EtherChannel

2) Clients want to send traffic to Client on same AP:
- Sends frame to AP
- AP tunnels to WLC
- WLC tunnels back to AP
- Then to client

CAPWAP tunnels

Access

SSID: wlan10
SSID: wlan20

3) **Cloud-based**: in-between autonomous AP and split-MAC architecture. Here, APs are autonomous but centrally managed in the cloud, such as Cisco Meraki.

User/Management Data Segregation

Meraki Cloud

Meraki Management Data →

User Data →

Web Servers

Internet

File Servers

LAPs CAN OPERATE IN SEVERAL MODES:
- *Local*: default, offers BSSs to wireless clients.
- *FlexConnect*: allows LAP to transform between split-MAC to autonomous modes depends on the status of the connection to WLC (if WLC goes down, it switches to autonomous mode). Also offers BSSs to wireless clients.
- *Monitor*: does not transmit, act as a sensor.
- *Sniffer*: sniff the traffic and send to an analyzer.
- *Rogue Detector*: detect rogue devices.
- *Bridge/Mesh*: form a dedicated bridge/mesh between sites even at long distance.
- *Flex plus Bridge*: adds FlexConnect to Bridge/Mesh.

WLC Deployments

Table 27-2 Summary of WLC Deployment Models

Deployment Model	WLC Location (DC, Access, Central, AP)	APs Supported	Clients Supported	Typical Use
Unified	Central	6000	64,000	Large enterprise
Cloud	DC	3000	32,000	Private cloud
Embedded	Access	200	4000	Small campus
Mobility Express	Other	100	2000	Branch location
Autonomous	N/A	N/A	N/A	N/A

In a split-MAC architecture, there are four main WLC deployment models:

1. **UNIFIED**: The WLC is a hardware appliance in a central location of the network *(supports about **6000** Aps)*
2. **CLOUD-BASED**: The WLC is a VM running on a server, usually in a private cloud in a data center *(supports about **3000** Aps)*
   a. This is not the same as the cloud-based AP architecture discussed previously.
3. **EMBEDDED**: The WLC is integrated within a switch *(supports about **200** Aps)*
4. **MOBILITY EXPRESS**: The WLC is integrated within an AP *(supports about **100** Aps)*

1. Unified WLC
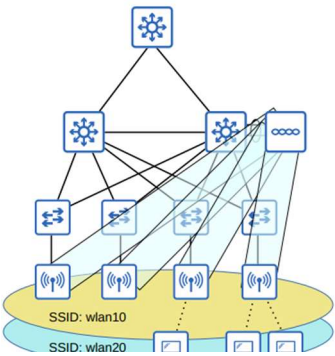
- The WLC is a hardware appliance deployed in a central location of the network.
- A unified WLC can support up to about 6000 APs.
- If more than 6000 APs are needed, additional WLCs can be added to the network.

SSID: wlan10
SSID: wlan20
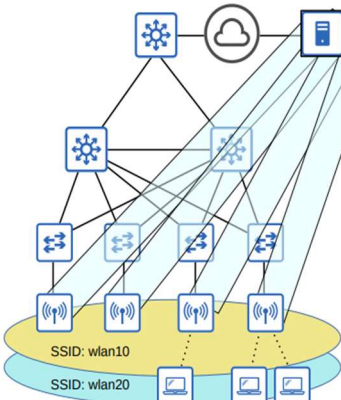
2. Cloud-based WLC

- The WLC is a VM running on a server, typically in a private cloud in a data center.
- Cloud-based WLCs can typically support up to about 3000 APs.
- If more than 3000 APs are needed, more WLC VMs can be deployed.

SSID: wlan10
SSID: wlan20
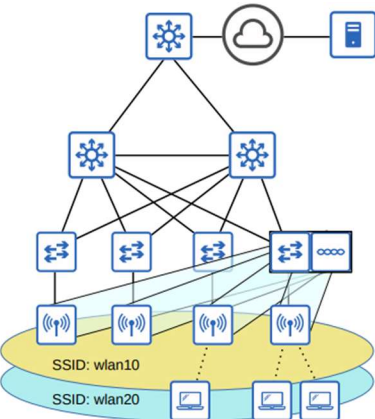
3. Embedded WLC

- The WLC is embedded within a switch.
- An embedded WLC can support up to about 200 APs.
- If more than 200 APs are needed, more switches with embedded WLCs can be added.

SSID: wlan10
SSID: wlan20

4. Cisco Mobility Express WLC
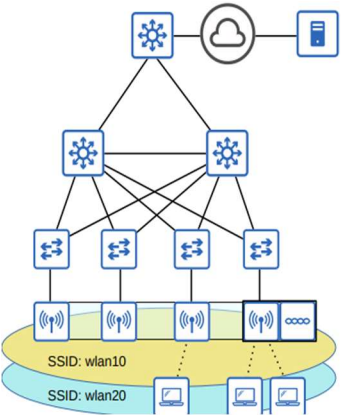
- The WLC is embedded within an AP.
- A Mobility Express WLC can support up to about 100 APs.
- If more than 100 APs are needed, more APs with embedded Mobility Express WLCs can be added.

SSID: wlan10
SSID: wlan20