Lightweight APs

Lightweight APs, often associated with protocols like CAPWAP (Control and Provisioning of Wireless Access Points), are designed to work in a centralized architecture where most of the intelligence and control reside in a Wireless LAN Controller (WLC).

- Lightweight APs operate in a controller-based architecture. They rely on a WLC to handle complex tasks such as authentication, encryption, policy enforcement, and RF management.
- The AP itself performs basic functions like transmitting and receiving wireless signals, while the WLC manages higher-level operations.

- Management is centralized through the WLC, which communicates with the AP using protocols like CAPWAP.
- The WLC pushes configurations, firmware updates, and policies to the AP, ensuring consistency across the network.

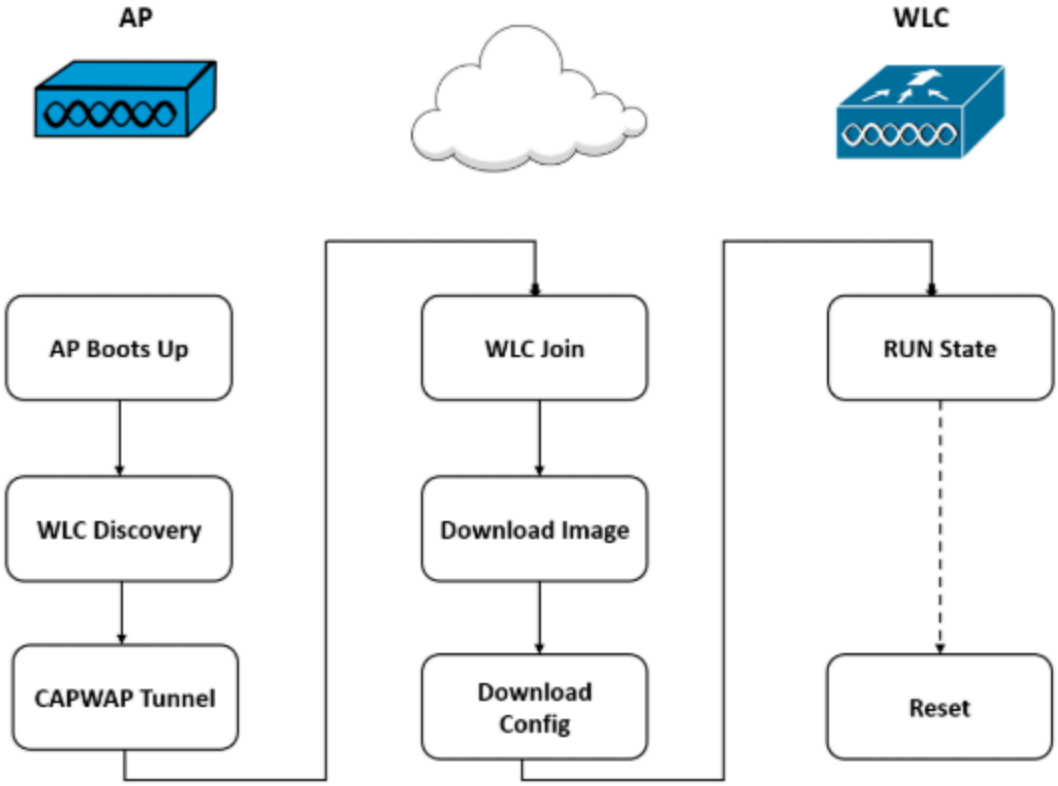
- Typically deployed in on-premises environments where the WLC is physically located within the organization's network infrastructure.
- Suitable for enterprises with a dedicated IT team to manage the WLC and network.

- Lightweight APs are heavily dependent on the WLC for operation. If the WLC goes offline, the APs may lose functionality or operate in a limited mode, depending on the vendor implementation (e.g., some APs can fall back to a standalone mode).

- Scalability is limited by the capacity of the WLC. Adding more APs may require upgrading the controller or deploying additional controllers.

Use Case :
large enterprises with complex networks where centralized control and policy enforcement are critical, such as

- campuses,
- hospitals, or
- corporate offices.



Flow of Lightweight APs

Cloud-based APs

Cloud-based APs are part of a more modern, distributed architecture where management and control are offloaded to the cloud, reducing the need for on-premises hardware like a WLC.

- Cloud-based APs are managed through a cloud-hosted management platform, eliminating the need for a local WLC.
- The AP handles more functions locally (e.g., data forwarding, encryption) and communicates with the cloud for configuration and monitoring.

- Management is performed via a web-based dashboard or app hosted in the cloud, allowing administrators to configure and monitor APs from anywhere.
- The cloud platform handles tasks like firmware updates, analytics, and policy enforcement, often with a more user-friendly interface.

- Deployed in environments where simplicity and remote management are priorities. The APs connect directly to the internet to reach the cloud management platform.
- Ideal for distributed networks, such as retail chains, small businesses, or organizations with multiple locations.

- Cloud-based APs require an internet connection to communicate with the cloud management platform. However, many are designed to continue functioning (e.g., providing Wi-Fi access) even if the cloud connection is lost, though management features may be unavailable.

- Highly scalable since the cloud platform can manage thousands of APs across multiple locations without the need for additional on-premises hardware.
- Scaling is as simple as adding more APs, as the cloud infrastructure handles the increased load.

<u>Use Case:</u>
Best for organizations that need flexibility, remote management, and minimal on-premises infrastructure, such as

- small to medium-sized businesses,
- distributed enterprises, or
- temporary setups.