CCNA 200-301, Volume I

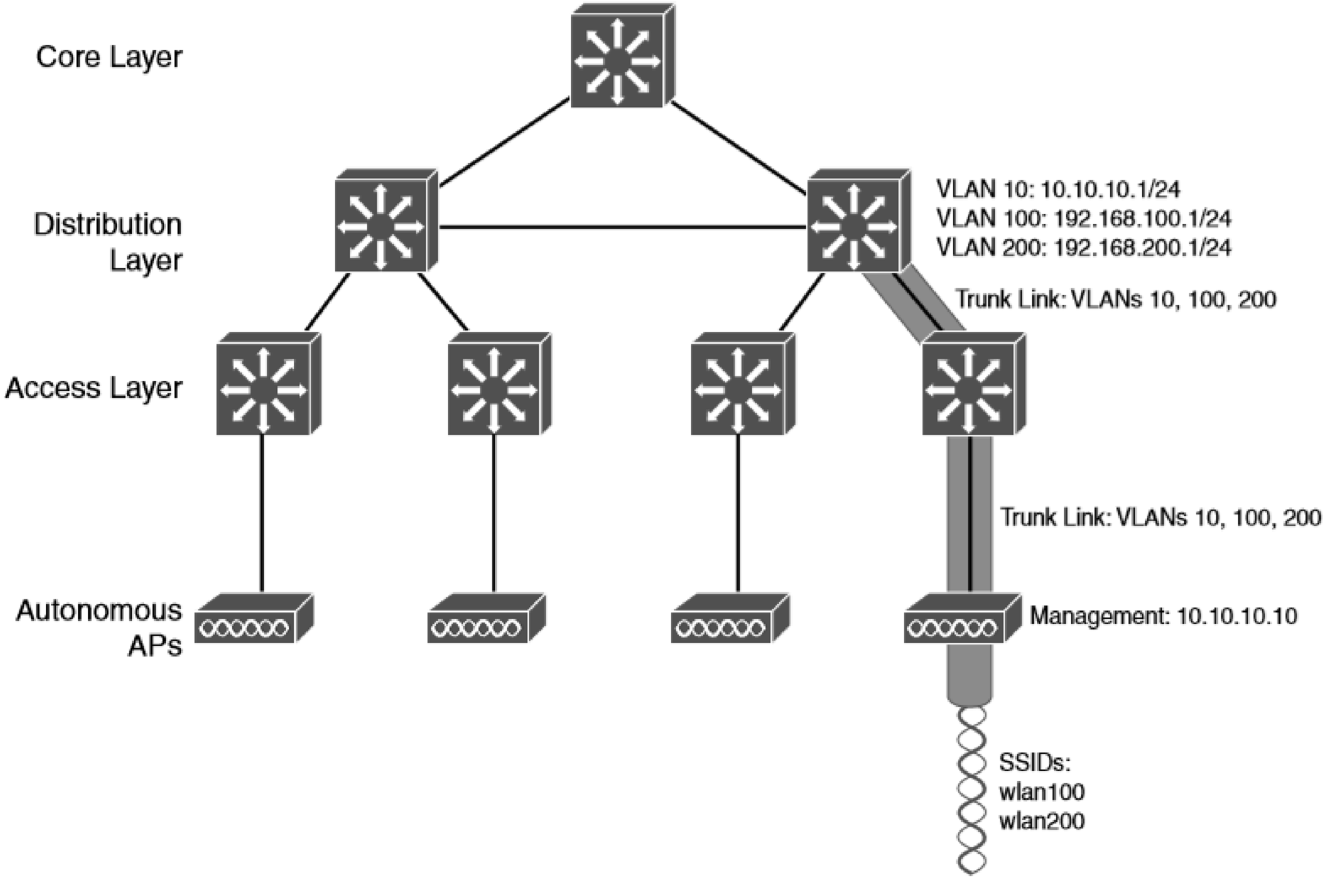
Chapter 27

Analyzing Cisco Wireless Architectures

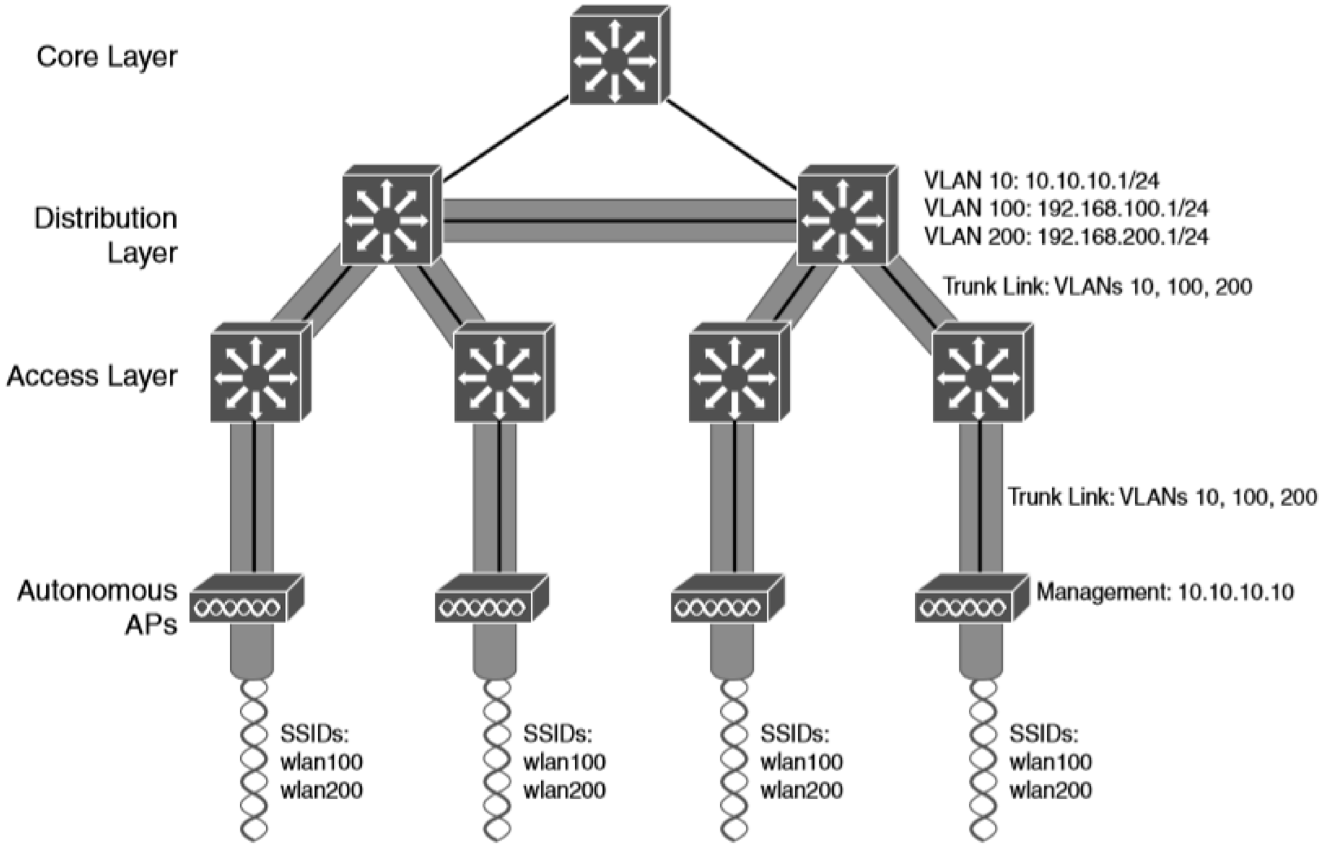
Objectives

- Autonomous AP Architectures
- Cloud-based AP Architecture
- Split-MAC Architectures
- Comparing Wireless LAN Controller Deployments
- Comparing Wireless LAN Controller Deployments

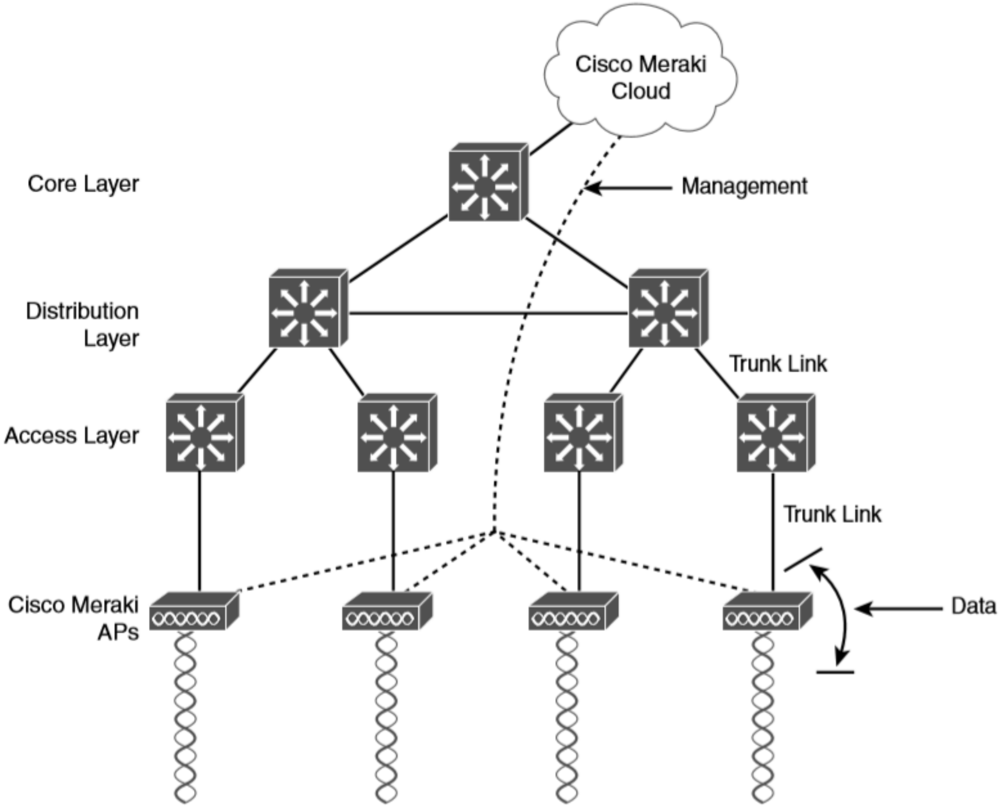
Wireless Network Architecture with Autonomous APs



Extent of a Data VLAN in a Network of Autonomous APs



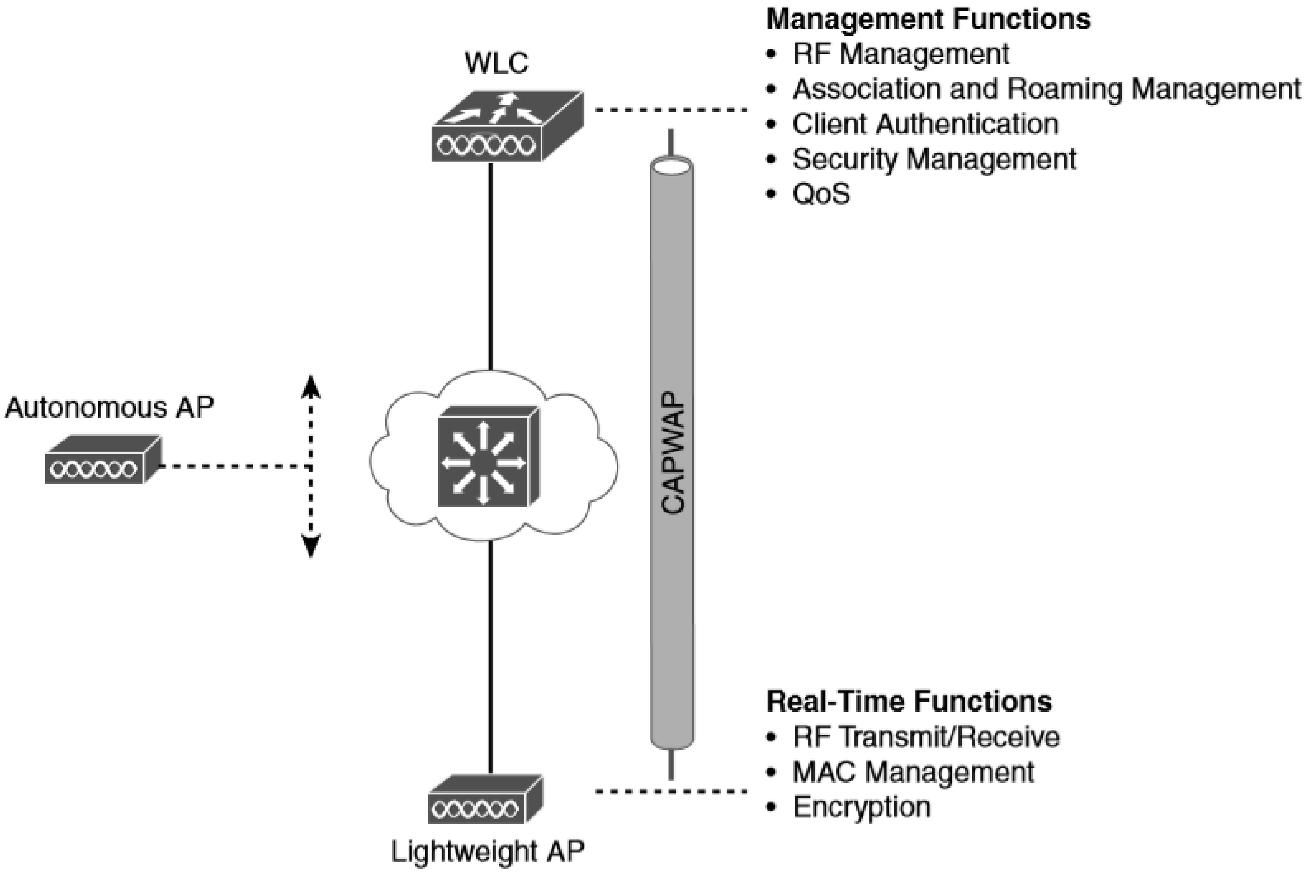
Cisco Meraki Cloud-Based Wireless Network Architecture



Notice that this network example consist of two distinct paths – one for data and one for management, corresponding to the following two functions:

- A control plane: Traffic used to control, configure, manage, and monitor the AP itself.
- A data plane: End-user traffic passing through the AP.

Autonomous Versus Lightweight Access Point



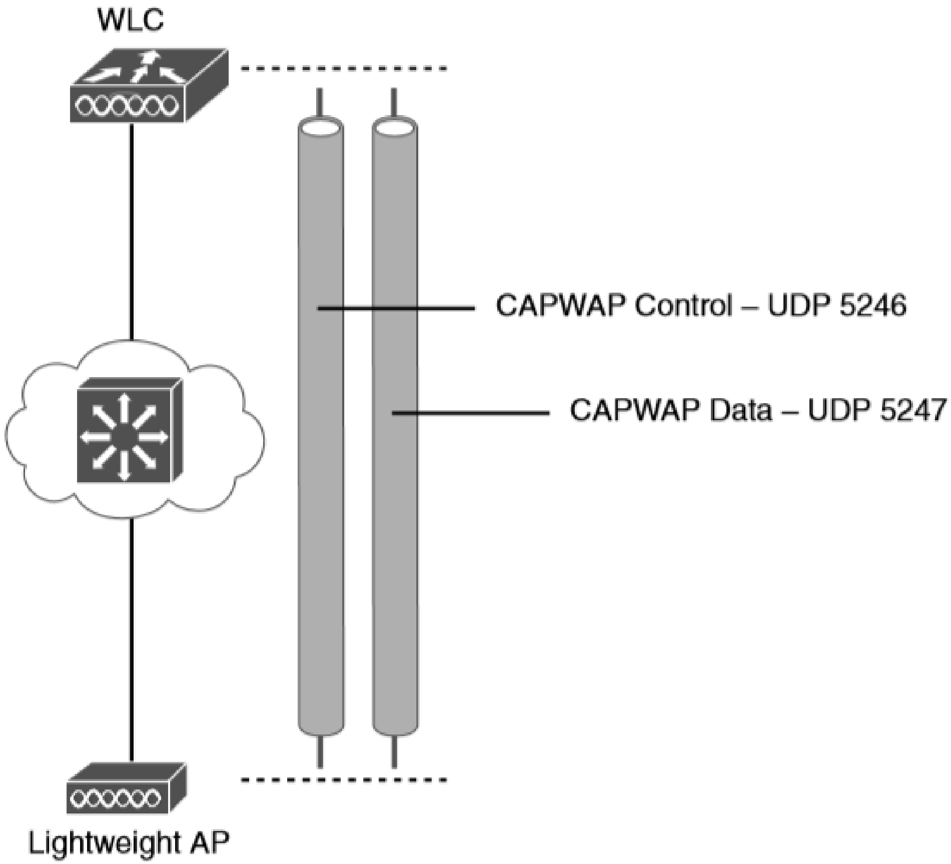
Management Functions

- RF Management
- Association and Roaming Management
- Client Authentication
- Security Management
- QoS

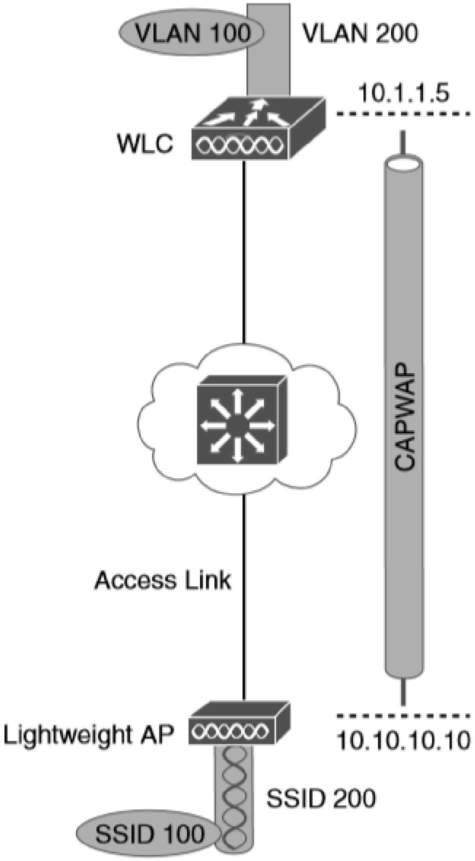
Real-Time Functions

- RF Transmit/Receive
- MAC Management
- Encryption

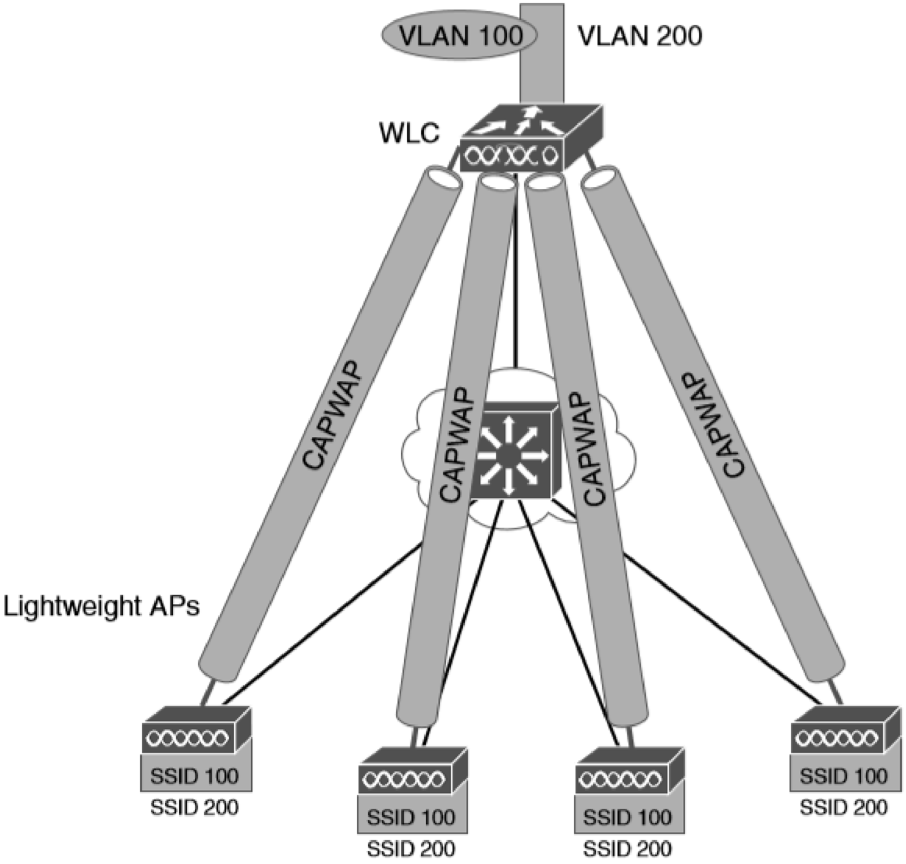
Linking a Lightweight AP and WLC with CAPWAP



Extent of VLAN 100 in a Cisco Wireless Network



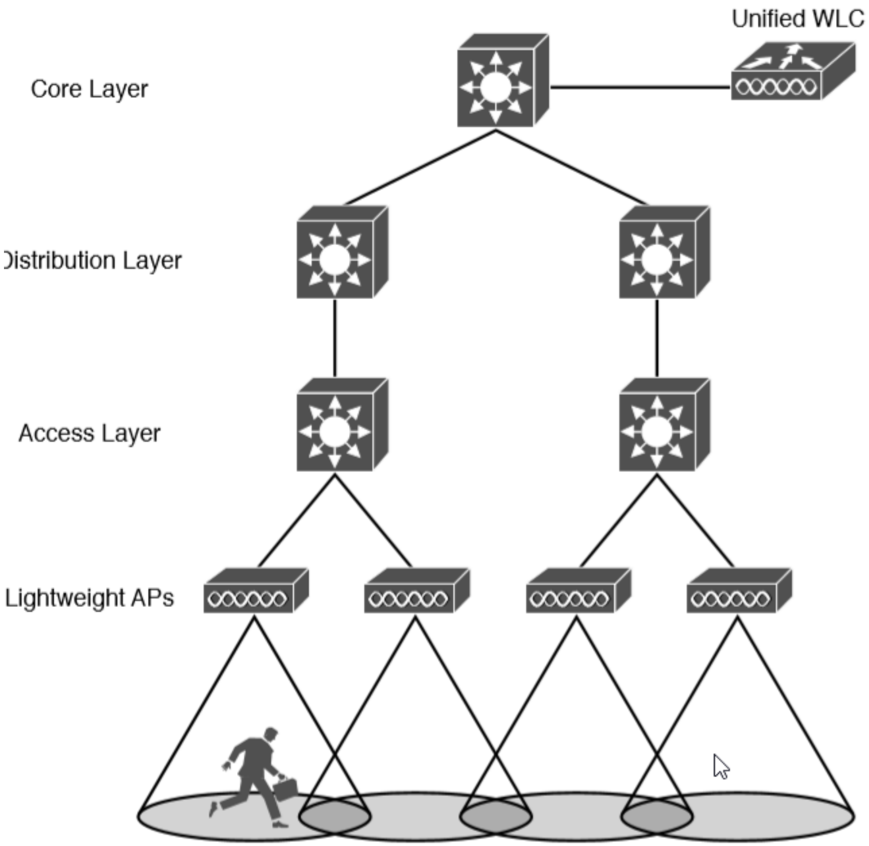
Using CAPWAP Tunnels to Connect APs to One Central WLC



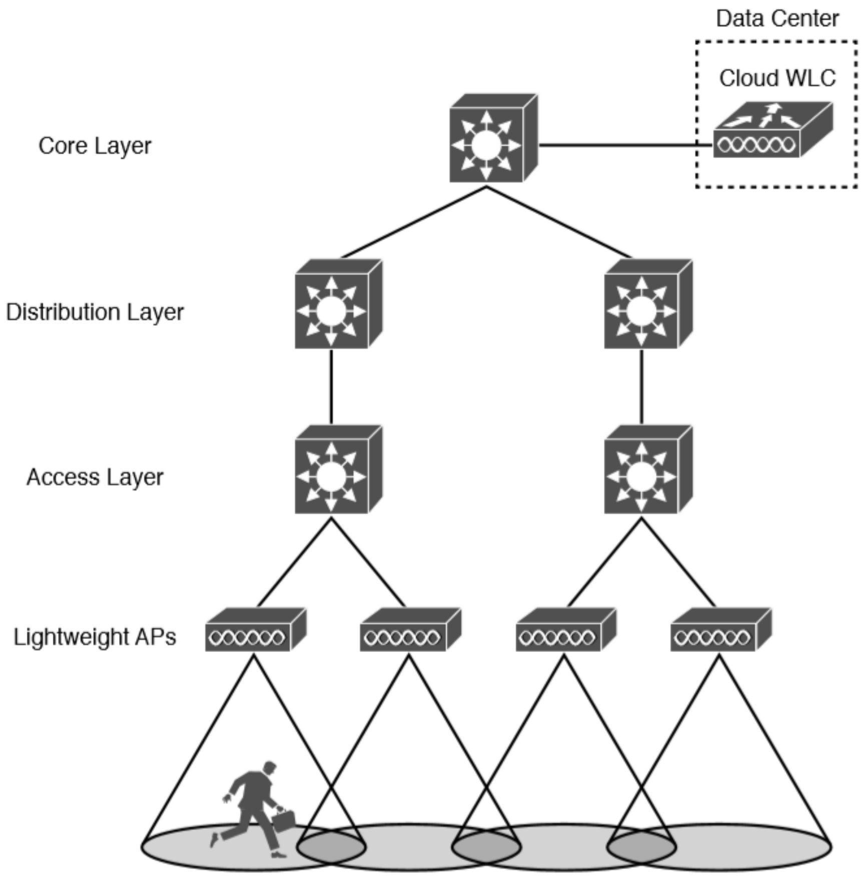
WLC Functions

- Dynamic channel assignment: The WLC can automatically choose and configure the RF channel used by each AP, based on other active access points in the area.
- Transmit power optimization: The WLC can automatically set the transmit power of each AP based on the coverage area needed.
- Self-healing wireless coverage: If an AP radio dies, the coverage hole can be “healed” by turning up the transmit power of surrounding APs automatically.
- Flexible client roaming: Clients can roam between APs with very fast roaming times.
- Dynamic client load balancing: If two or more APs are positioned to cover the same geographic area, the WLC can associate clients with the least used AP. This distributes the client load across the APs.
- RF monitoring: The WLC manages each AP so that it scans channels to monitor the RF usage. By listening to a channel, the WLC can remotely gather information about RF interference, noise, signals from neighboring APs, and signals from rogue APs or ad hoc clients.
- Security management: The WLC can authenticate clients from a central service and can require wireless clients to obtain an IP address from a trusted DHCP server before allowing them to associate and access the WLAN.
- Wireless intrusion protection system: Leveraging its central location, the WLC can monitor client data to detect and prevent malicious activity.

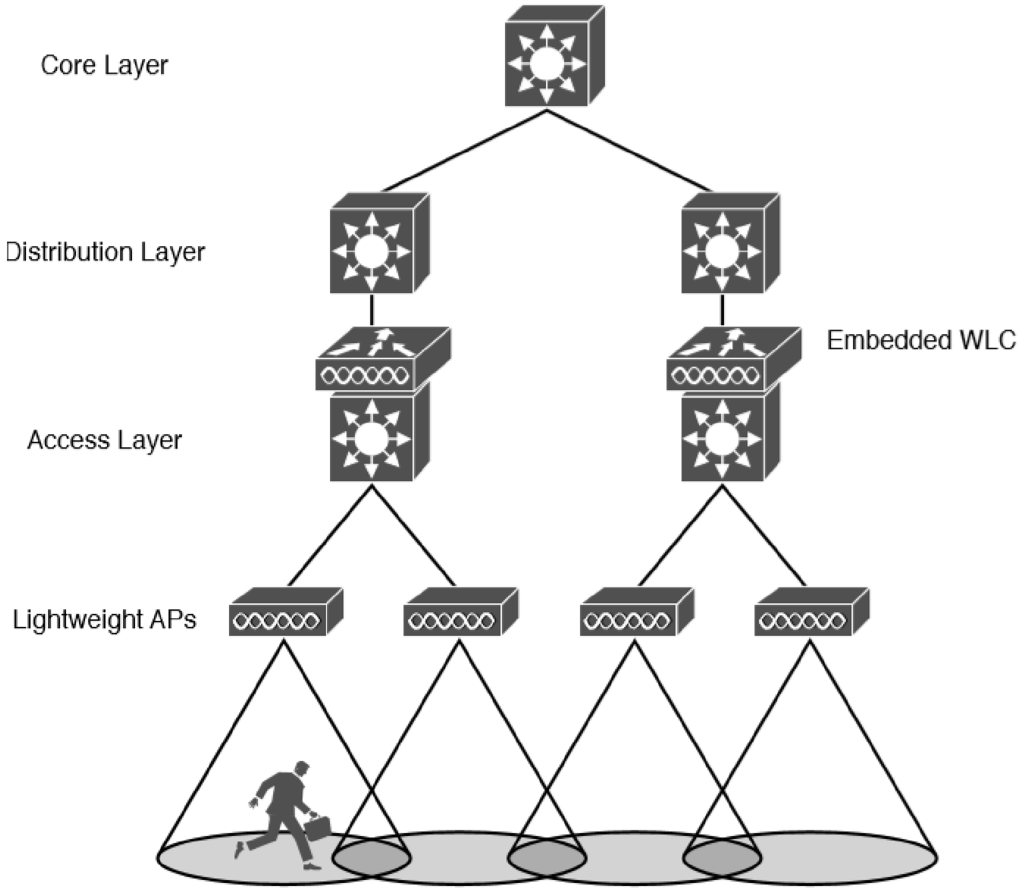
WLC Location in a Unified Deployment



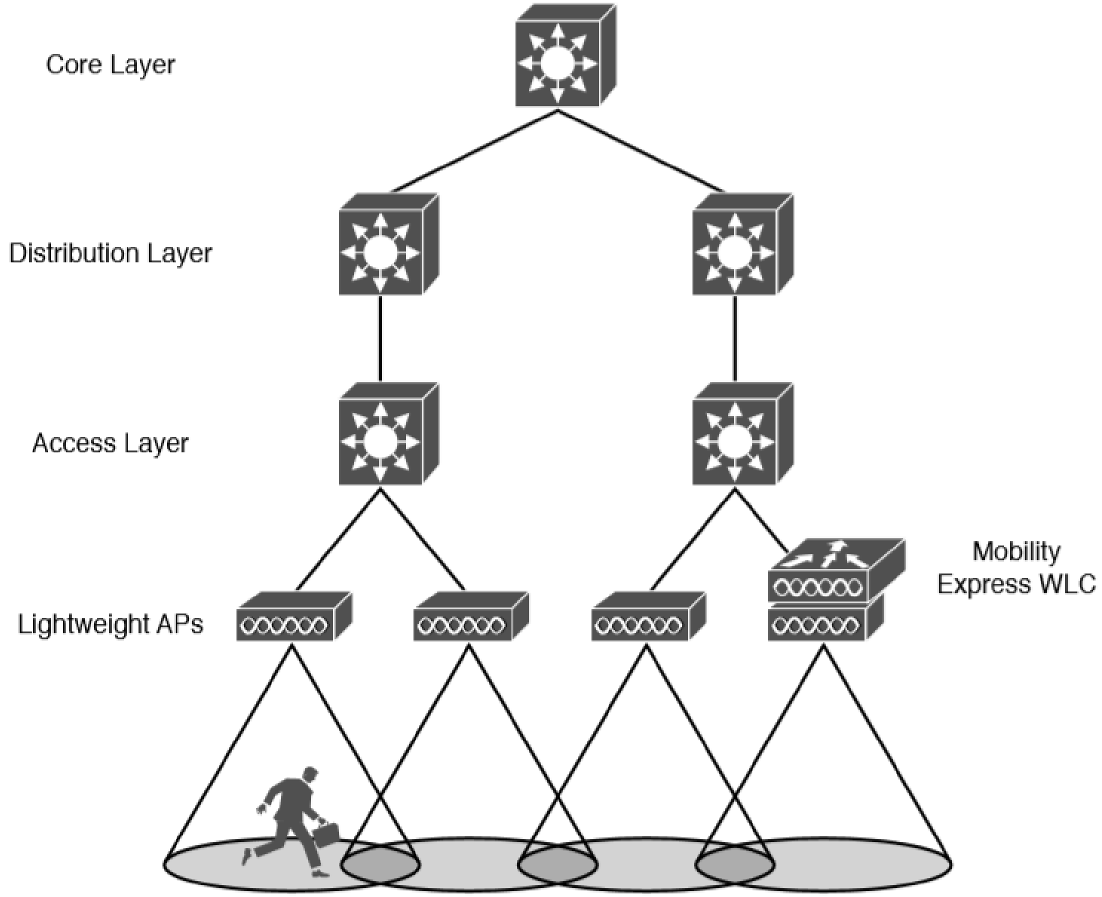
WLC Location in a Cloud-based Deployment



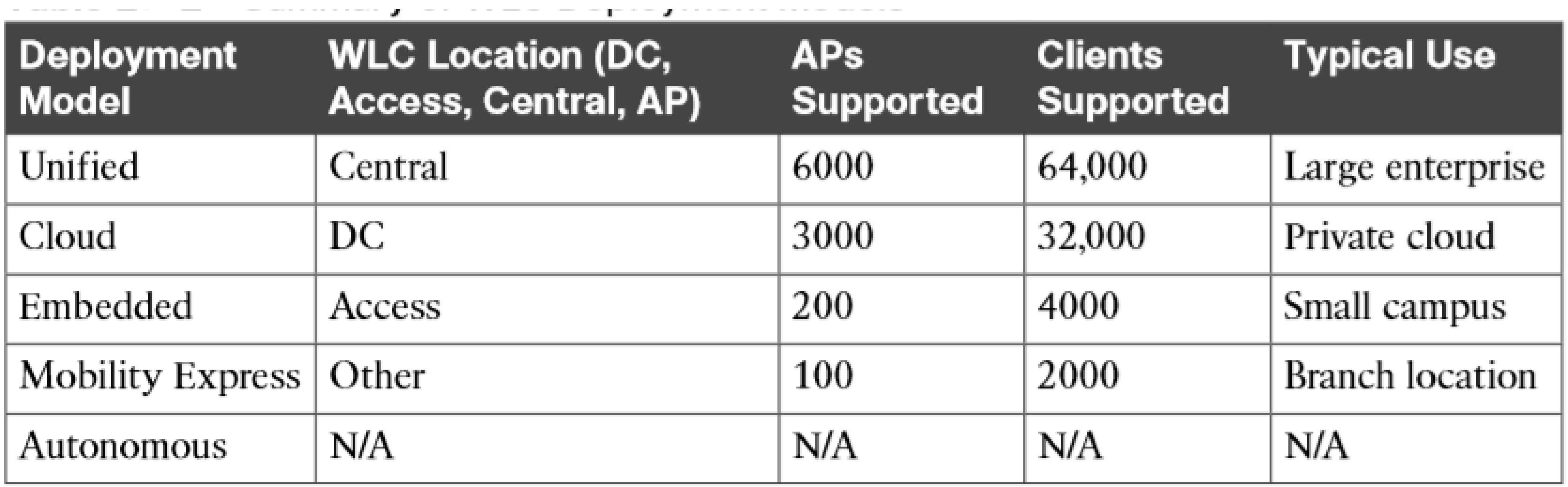
WLC Location in an Embedded Deployment



WLC Location in a Mobility Express Deployment



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

Cisco AP Modes

- Local: The default lightweight mode that offers one or more functioning BSSs on a specific channel. During times that it is not transmitting, the AP will scan the other channels to measure the level of noise, measure interference, discover rogue devices, and match against intrusion detection system (IDS) events.
- Monitor: The AP does not transmit at all, but its receiver is enabled to act as a dedicated sensor. The AP checks for IDS events, detects rogue access points, and determines the position of stations through location-based services.
- FlexConnect: An AP at a remote site can locally switch traffic between an SSID and a VLAN if its CAPWAP tunnel to the WLC is down and if it is configured to do so.
- Sniffer: An AP dedicates its radios to receiving 802.11 traffic from other sources, much like a sniffer or packet capture device. The captured traffic is then forwarded to a PC running network analyzer software such as Wildpackets OmniPeek or WireShark, where it can be analyzed further.

Cisco AP Modes (Continued)

- Rogue detector: An AP dedicates itself to detecting rogue devices by correlating MAC addresses heard on the wired network with those heard over the air. Rogue devices are those that appear on both networks.
- Bridge: An AP becomes a dedicated bridge (point-to-point or point-to-multipoint) between two networks. Two APs in bridge mode can be used to link two locations separated by a distance. Multiple APs in bridge mode can form an indoor or outdoor mesh network.
- Flex+Bridge: FlexConnect operation is enabled on a mesh AP.
- SE-Connect: The AP dedicates its radios to spectrum analysis on all wireless channels. You can remotely connect a PC running software such as MetaGeek Chanalyzer or Cisco Spectrum Expert to the AP to collect and analyze the spectrum analysis data to discover sources of interference.