Wireless Architectures

802.11 frame format: depending on the version and message type some fields might not be present in frame.
Frame control: provides info as message type and subtype, Duration/id: depending on type can indicate the time in micros the channel will be dedicated for transmission of frame or an identifier for the association.
Addresses: 6bytes , 1→ Destination address (final recipient), Source Address (Original Sender), Receiver Address (Immediate recipient), Transmitter Address (Immediate Sender).
Sequence Control: to resemble fragments and eliminate duplicate frames.
QoS control: to prioritize certain traffic. HT (High Throughput Control): added in 802.11n to enable ht operations.
FCS: frame check sequence for error checking.
Association process:for a station to send traffic through AP, it must be associated with it, connection states: not authenticated or associated, authenticated but not associated and authenticated and associated.
For a station to scan for Ap: active scanning → through probe request and response, passive scanning, by listening for beacon messages from Ap. (sent periodically to advertise BSS).
3 message types: 1- management→ as beacon, probe request/response, authentication, association request/response.
2-control: to control access to medium and assist with delivery of management and data frames as RTS, CTS, ACK.
3- Data: to send actual data packets.

Deployment methods: Autonomous Aps are self contained systems that don't rely on a WLC, are configured individually using a CLI, telnet/SSH or HTTP/HTTPs web GUI connection, an ip address for remote management should be configured, rf parameters as transmit power, channel must be manually configured, security policies are handled individually by each AP, Qos rule, … etc are configured on each AP, has no central monitoring/management, autonomous Aps connect to the wired network with a trunk link (the management traffic used to connect to other Aps as well as other devices should be in a separate VLAN), data traffic from wireless clients has a very strict direct path to the wired network or to other wireless clients associated with the same Aps, each VLAn has to stretch across the entire network which is a bad practice due to large broadcast domains, spanning tree will disable links, adding an deleting VLANs is labor intensive, used for small nets.
Lightweight Ap: the function of Ap is split between the Ap and a wireless LAN controller (WLC), handle real time operations as transmitting/receiving RF traffic, encryption/decryption, sending beacons/probes, WLC carries out other functions as RF management, security/QoS management, client authentication, association, roaming management
Called split Mac architecture, WLC can be located in the same subnet/VLAN as lightweight Aps it manages or in different subnet/VLAN, authenticate each other via digital certificates installed on each device, use CAPWAP protocol to communicate baes on older protocol LWAPP, creates two tunnels between each Ap and WLC as control tunnel using UDP 5246 to configure Aps, control/mange operations (all traffic is encrypted), data tunnel using UDP 5247, all traffic from wireless clients is sent through this tunnel to the WLC (not directly to wired network), not encrypted by default, can be configured to be encrypted using DTLS (Datagram Transport layer Security), Aps can connect to switch access ports.
Lightweight benefits: scalabilty, dynamic channel assignment where WLC can auto-select appropriate channel for each Ap, transmit power optimization: auto set by WLC, self-healing wireless coverage: when an Ap stops functioning the WLC can increase the transmit power of nearby Aps to avoid coverage holes, seamless roaming, client load balancing: if a client is in range of 2 Aps, the WLC can associate it with the least used Ap, Security/QoS management is central ensuring consistency across the network.
.

Lightweight modes: 1-local: the Ap offers one or multiple BSSs for client to associate with.
2- flexConnect: as local mode but allows Ap to locally switch traffic between wired and wireless networks if tunnels to WLC go down.
3- Sniffer: doesn’t offer BSS for clients, yet capture frames and send them to a device running a software as wireshark.
4- Monitor: the Ap doesn’t offer a BSS for clients, it receives 802.11 frames to detect rouge devices then sends de-authentication messages to disassociate them from their AP.
5- rouge detector: AP doesn’t use radio, it listens to traffic on wired network only, receives a list of suspected rouge clients and AP MAC addresses from WLC, by listening to ARP on wired network and correlating it with info it receives from WLC, it can detect rouge devices.
SE (Spectrum Expert) Connect: Ap is dedicated to RF spectrum analysis on all channels, it can send info to software as Cisco spectrum expert on a PC to collect/analyze data to detect interference.
Bridge/Mesh: AP can be a dedicated bridge between sites over long distances, a mesh can be made between access points.
Flex plus bridge: adds flex functionality to bridge/mesh.
Cloud based Aps: between autonomous ans split Mac architecture, autonomous Aps that are centrally manged in cloud as Cisco Meraki, only engagement/control traffic is sent to the cloud while data traffic is sent directly to the wired network line like when using autonomous Aps.

WLC deployment models:1- Unified: a hardware appliance deployed in a central location of the network, can support up to 6000 Aps, for ore Aps, more WLCs can be used.
2- cloud based WLC: the WLC is a VM running on a server typically in a private cloud data center, support up to 3000 Aps, if more Aps needed, more WLCs Vms can be deployed.
3- embedded WLC: the WLC is embedded within a switch, support up to 200 Aps.
Mobility express, the WLC is embedded within Ap, the Ap containing WLC builds internal CAPWAP tunnels to it, support up to 100 Aps..