Access Point:

- A device that allows wireless devices to connect to a wired network using Wi-Fi.
- Access Point is a device that creates wireless local area network, or Wireless LAN.
- Access Point is a device creates Wireless LAN usually in an office or large building.
- AP is the device that allows multiple wireless devices to connect with each other.
- AP connects multiple wireless devices together in single or multiple wireless networks.
- AP is a networking device that is used to form wireless local area network in home.
- An access point connects to a wired router, switch, or hub via an Ethernet cable.
- AP is hardware device used to connect computer, laptops and mobile with each other.
- Wireless networks are suitable for those places where cables are difficult to install.
- An access point can also be used to extend the wired network to the wireless devices.
- The AP converts the wireless frequency subject into digital signals and then vice versa.

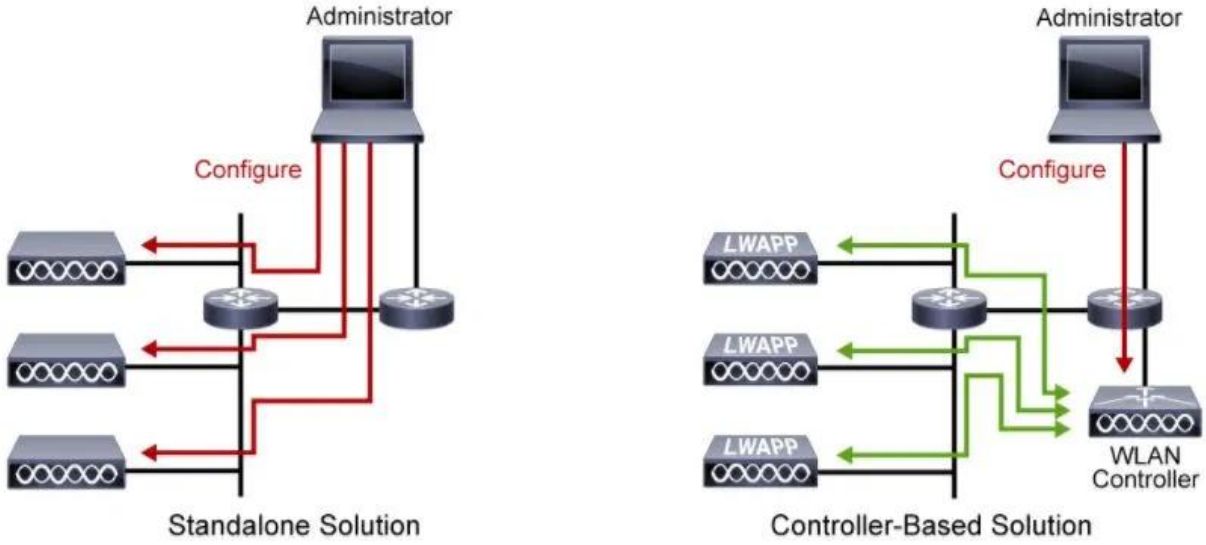
AP Categories:

Autonomous APs:

- These are standalone devices configured using a command line interface or a GUI.
- Autonomous APs are useful in situations where only couple of APs are required in org.
- Such as home router is autonomous AP because entire configuration resides on device.
- If wireless demands increase, more Access Points (APs) would be required to deploy.
- Each AP operate independent of other APs & each AP require manual configuration.
- Each AP operates independent of other APs & each AP require manual management.
- This would become overwhelming if many Access Points (APs) were needed in case.
- Autonomous Access Points is Standalone mode and Management address for remote.
- Single and standalone access points (APs) can offer the functionabilities of BSS only.
- APs can operate in autonomous or lightweight mode this depends on image that run.
- Autonomous AP called Mobility Express, is used when don't have Wireless Lan Controller.
- Standalone APs can be organized one-by-one & proffer staring functionality by themselves.

Controller-Based APs:

- These devices require no initial configuration and are often called lightweight APs (LAPs).
- LAPs use Lightweight Access Point Protocol to communicate with WLAN controller (WLC).
- Controller-based APs are useful in situations where many APs are required in the network.
- As more APs are added, each AP is automatically configured and managed by the WLC.
- Notice in the figure that the WLC has four ports connected to the switching infrastructure.
- These four ports are configured as a link aggregation group (LAG) to bundle them together.
- Much like how the EtherChannel operates, LAG provides redundancy and load-balancing.
- All ports on switch that are connected to WLC need to be trunking and EtherChannel on.



Cisco Wireless AP Modes:

From The WLC, can configure a lightweight AP to operate in one of the following modes:

Local:

- Default lightweight mode that offers one or more functioning BSSs on specific channel.
- Local mode is the default mode of Access Point AP it offers a BSS on a specific channel.
- During when it is not transmitting, AP scans other channels to measure level of noise.
- Also, measure interference, discover rogue devices, and match against 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.
- AP in monitor mode doesn't transmit at all, it's dedicated sensor that Detects rogue APs.

FlexConnect:

- It's possible to connect a local mode Access Point at a remote branch to the HQ's WLC.
- AP encapsulates all wireless client data through the CAPWAP tunnel over the WAN link.
- Secondly, when WAN link is down, your wireless network at the branch site is offline too.
- An Access Point (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 Access Point in sniffer mode dedicates it's time to receive 802.11 wireless frames.
- AP dedicates its radios to receiving 802.11 traffic from other sources, much like sniffer.
- The captured traffic is then forwarded to the PC running network analyzer software.
- Software such as LiveAction Omnipeek or Wireshark, where it can be analyzed further.
- This can be useful if you want to troubleshoot a problem and you can't be on-site.

Rogue Detector:

- AP Rogue detector mode makes the Access Point (AP) detect rogue devices full-time.
- The Access Point checks for MAC addresses it sees in the air and on the wired network.

Bridge:

- The Access Point becomes a dedicated point-to-point or point-to-multipoint bridge.
- Becomes dedicated bridge point-to-point or point-to-multipoint between two networks.
- The Two APs in bridge mode can be used to link two locations separated by a distance.
- While Multiple APs in bridge mode can form an indoor or outdoor the mesh network.

Flex+Bridge:

- The Access Point (AP) can operate in either FlexConnect or Bridge or Mesh mode.
- The FlexConnect operation is enabled on a Wireless Mesh Access Point (AP).

SE-Connect:

- The Access Point (AP) dedicates its radios to spectrum analysis on all wireless channels.
- Can remotely connect PC running software such as MetaGeek Chanalyzer or Cisco Spectrum
- Expert to AP to collect & analyze spectrum analysis data to discover sources of interference.