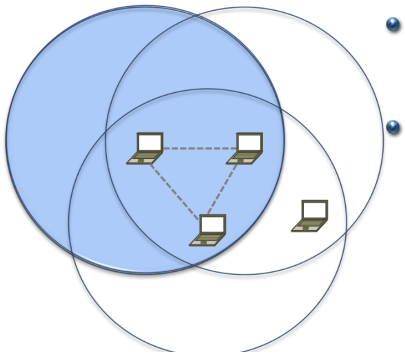
802.11 WiFi

- WiFi services are defined in the IEEE 802.11 standard
- IEEE: Institute of Electrical and Electronics Engineers

Wireless Network Types

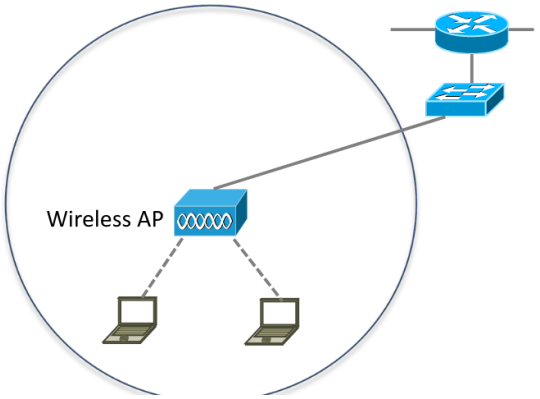
- **WPAN**: Wireless Personal Area Network
  - Devices are within 10 meters of each other
  - Bluetooth is often used
- **WLAN**: Wireless Local Area Network
  - Provides access to a campus (typically wired) network, without the need for a cable
  - Devices within 100m of a Wireless Access Point
- **WMAN**: Wireless Metropolitan Area Network
  - Covers a large area such as a city

Ad Hoc Networks

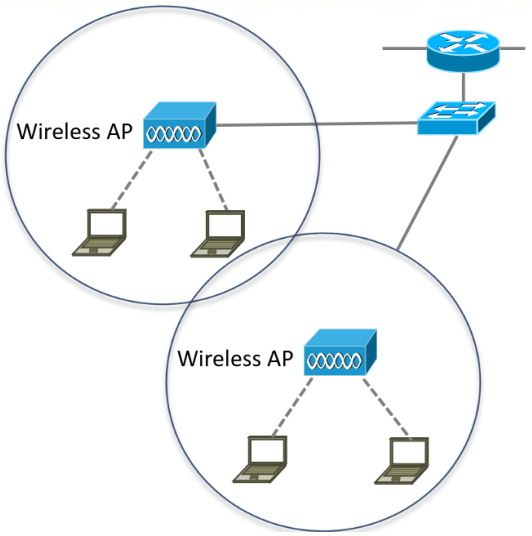


- Two or more wireless stations communicate directly with each other
- IBSS Independent Basic Service Set

Infrastructure Mode



- Stations communicate via a Wireless Access Point (AP)
- This can provide access to a wired network



- Multiple Access Points can be deployed to provide the required coverage area

Ad-Hoc vs Infrastructure Mode

- Wireless stations work in either Ad-Hoc or Infrastructure Mode
- They can not operate in both at the same time

WiFi Direct

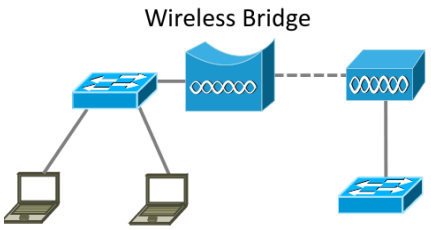
- WiFi Direct allows devices to be connected to an Access Point and also be part of a peer-to-peer wireless network
- It does not operate in Ad-Hoc IBSS mode, it is an extension to Infrastructure Mode
- WPS WiFi Protected Setup enables connection setup by pushing a button
- It is WPAN Wireless Personal Area Network

WiFi Direct Predefined Services

- Miracast to wireless external monitor

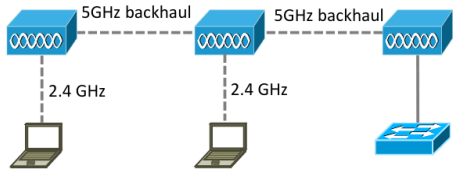
- DLNA Digital Living Network Alliance allows devices to stream music and video
- Direct Print

Wireless Bridges



- Wireless Bridges can be used to connect areas which are not reachable via cable to the network

Mesh Networks

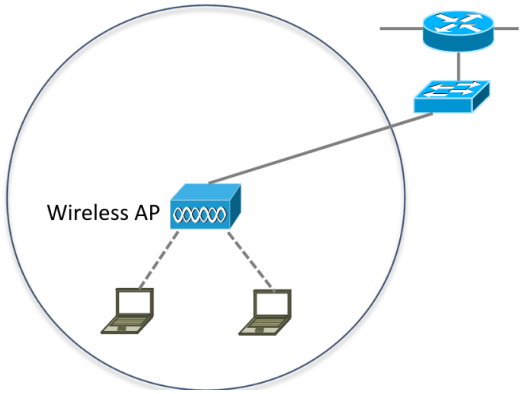


- Another option to spread the coverage area of a WLAN is Mesh
- One AP radio is used to serve clients
- The other radio connects to the backhaul network

Wireless Access Points

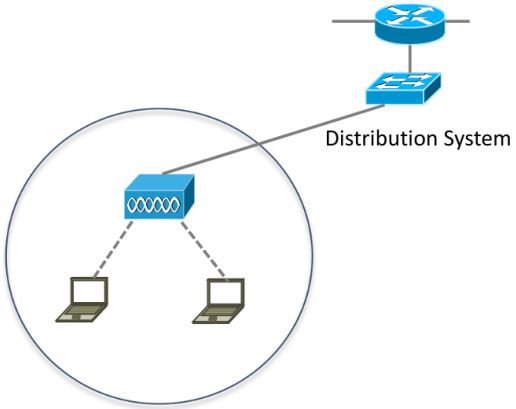
- Wireless Access Points provide connectivity between wireless stations, and between the wireless and wired networks
- Wireless is half-duplex
- Only one device can communicate at a time

BSS Basic Service Set



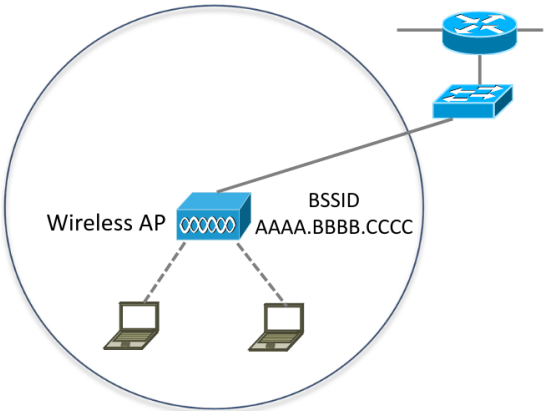
- An Access Point centralizes access and control over a group of wireless devices.
- The devices and their wireless settings make up a BSS

DS Distribution System



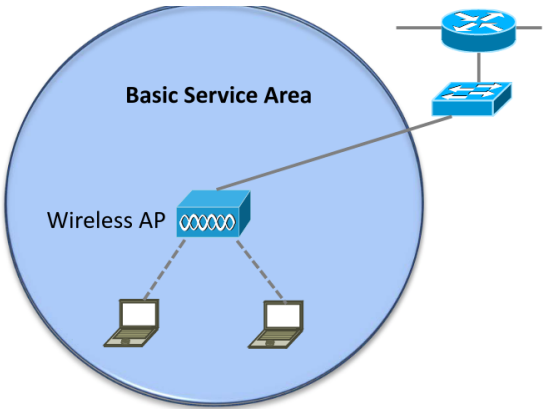
- A distribution system connects Wireless Access Points to the wired network

BSSID Basic Service Set Identifier



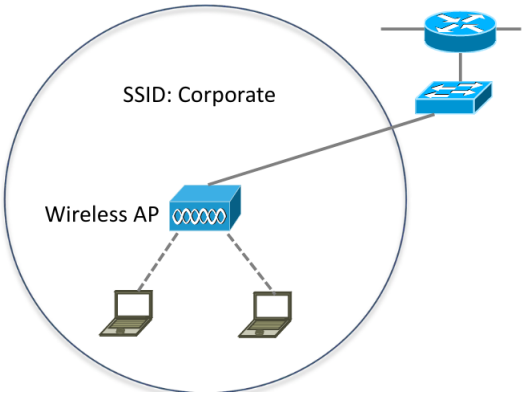
- Devices within Basic Service Sets are identified by their BSSID, which is based on their MAC address

BSA Basic Service Area



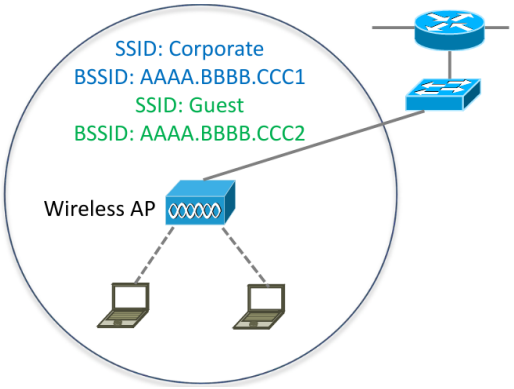
- The BSA is the wireless coverage area of an Access Point
- Also known as a wireless cell

SSID Service Set Identifier



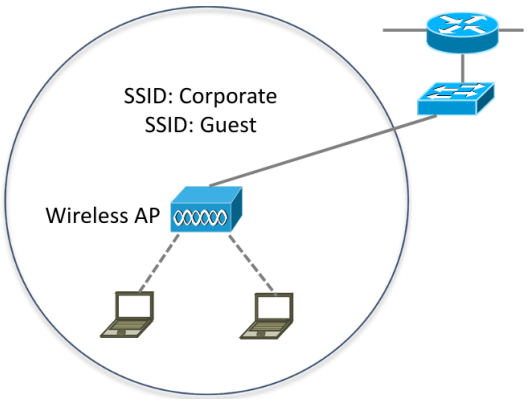
- The SSID is a unique identifier that names the wireless network (WLAN), for example ‘Corporate’

Multiple SSID Service Set Identifiers



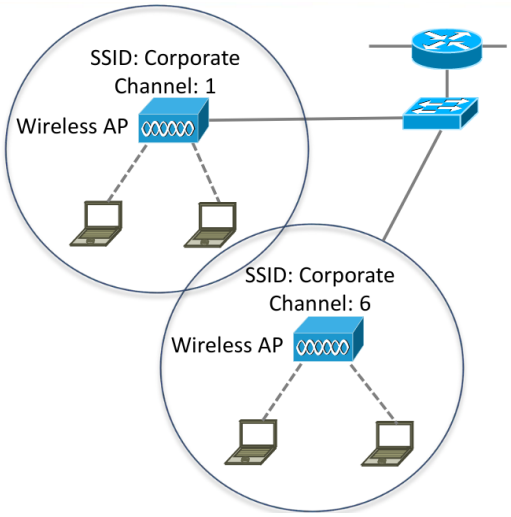
- A single Access Point can support multiple SSIDs
- For example ‘Corporate’ and ‘Guest’
- Different SSIDs can have different security settings and be mapped to different VLANs

Beacons



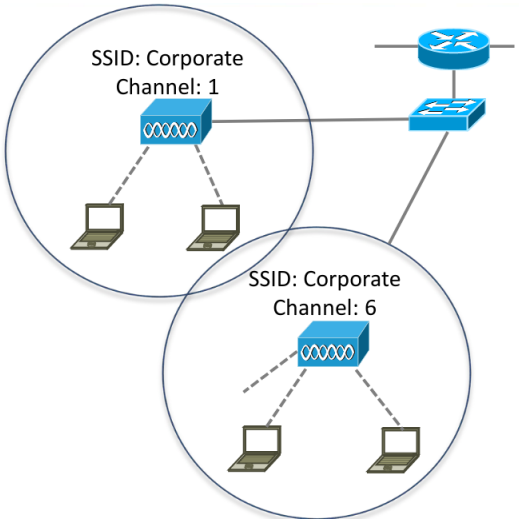
- Wireless Access Points broadcast information about their WLANs (including the SSID and authentication requirements) with beacon frames
- This can be disabled

ESS Extended Service Set



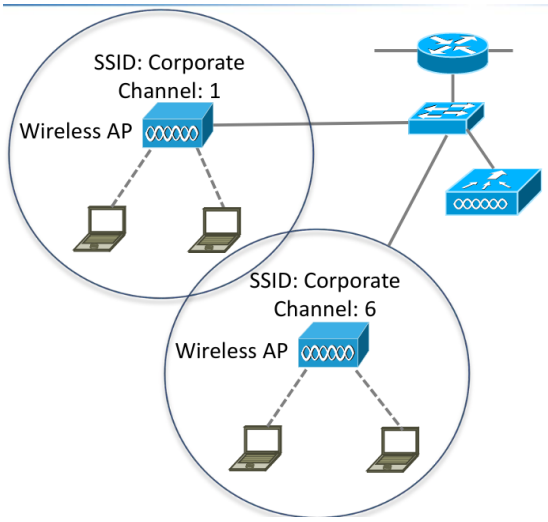
- The same SSID can be supported across multiple Access Points to give a larger coverage area

Roaming



- Wireless client stations can roam across Wireless APs supporting the same WLANs

WLC Wireless LAN Controllers



- In a large campus, configuring a large amount of Access Points one by one becomes unmanageable
- A Wireless LAN Controller can be used as a central point of management

Autonomous vs Lightweight Access Points

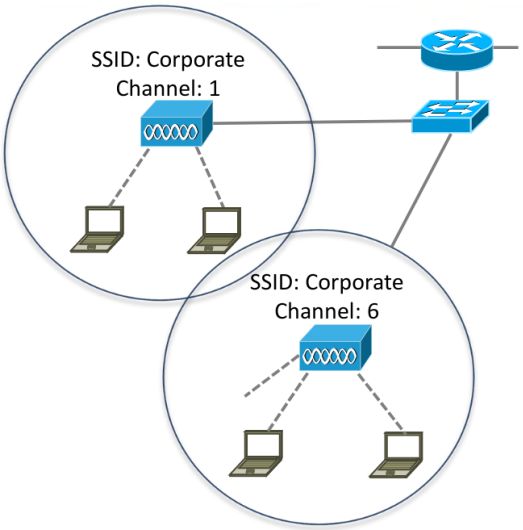
- Standalone Access Points are known as Autonomous Access Points
- Access Points with a WLC are known as Lightweight Access Points
- The installed software image determines whether an Access Point is Autonomous or Lightweight

Zero Touch Provisioning

- Lightweight Access Points support Zero Touch Provisioning
- They discover their Wireless LAN Controller via these options:
    - DHCP - option 43 gives the IP address of the WLC
    - DNS – ‘cisco-capwap-controller’ resolves the IP address of the WLC
    - Local subnet broadcast

- The lightweight Access Point downloads its configuration from the Wireless LAN Controller
- This includes what WLANs it should support and their settings
- The WLC also monitors the wireless quality and controls the channels and power of the Access Points
- It can also detect rogue APs

Roaming with Wireless LAN Controller



- Wireless stations can roam across Wireless APs supporting the same WLANs
- The infrastructure can be configured to make roaming seamless

CAPWAP

- Control And Provisioning of Wireless Access Points (CAPWAP) protocol is a standardized protocol that enables a Wireless LAN Controller to manage a collection of Wireless Access Points
- Communications are encrypted inside a DTLS CAPWAP tunnel
- It uses UDP ports 5246 and 5247

Split MAC

- Work is moved from the APs to the WLC which is why they are called Lightweight APs
- Real-Time traffic is still handled by the AP in order to provide suitable performance, the rest is handled by the WLC
- This is known as ‘Split MAC’

Split MAC – AP Operations

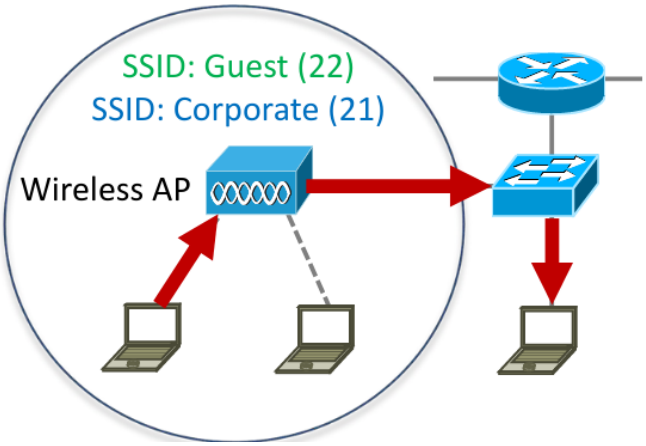
- Client handshake when connecting
- Beacons
- Performance monitoring
- Encryption and decryption
- Clients in power save

Split MAC – WLC Operations

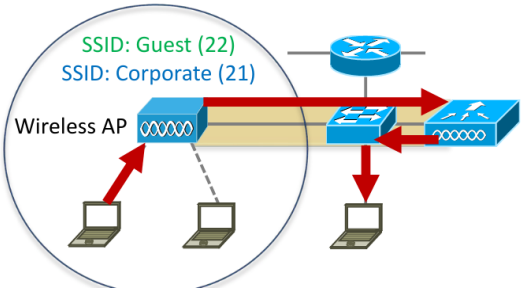
- Authentication

- Roaming control
- 802.11 to 802.3 communication
- Radio Frequency management
- Security management
- QoS management

Traffic Flow with Autonomous AP



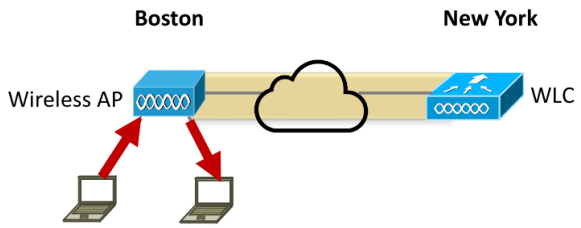
Traffic Flow with CAPWAP



- Management traffic between the AP and WLC also passes through the CAPWAP tunnel
- LAG Link Aggregation (Etherchannel) is often used on the WLC to switch link

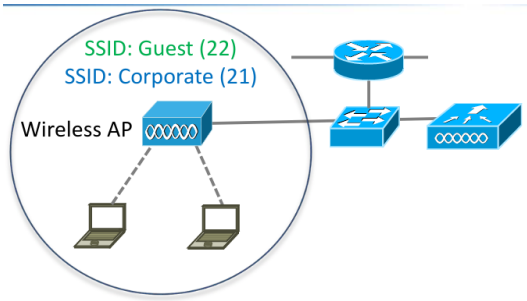
Flexconnect

FlexConnect

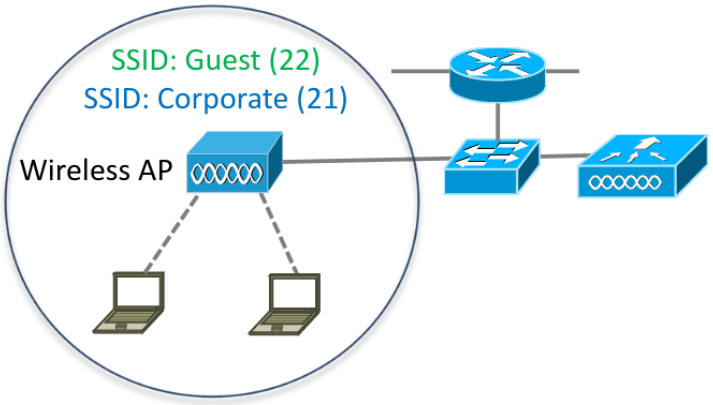


- Traffic is forwarded locally wher FlexConnect is configured
- This is useful for small branch offices without a Wireless LAN Controller

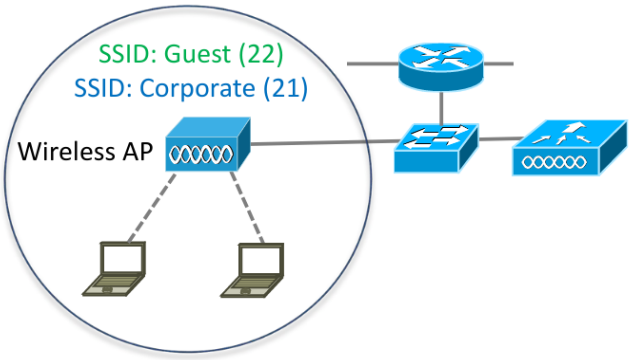
Autonomous AP Switch Configuration



- In this example two WLANs have been configured on the Autonomous AP
- The Corporate WLAN is mapped to VLAN 21
- The Guest WLAN is mapped to VLAN 22

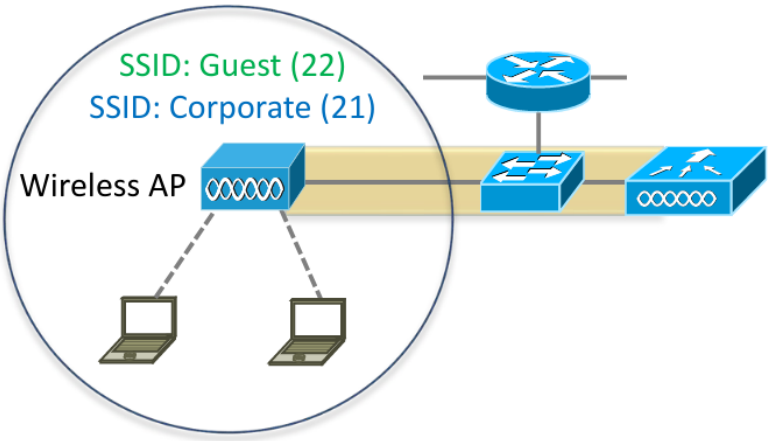



```
Switch(config)# vlan 21
Switch(config-vlan)# name Corporate
Switch(config)# vlan 22
Switch(config-vlan)# name Guest
```

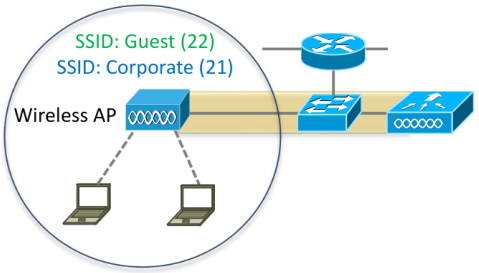



```
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# switchport trunk encap dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 21,22
```

Lightweight AP Switch Configuration

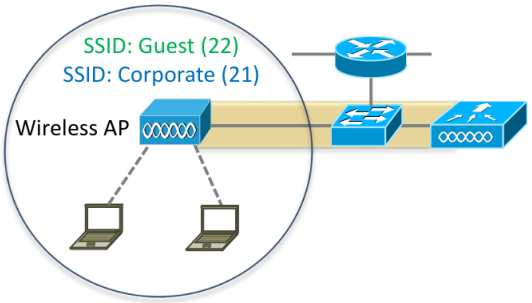



```
Switch(config)# vlan 21
Switch(config-vlan)# name Corporate
Switch(config)# vlan 22
Switch(config-vlan)# name Guest
```



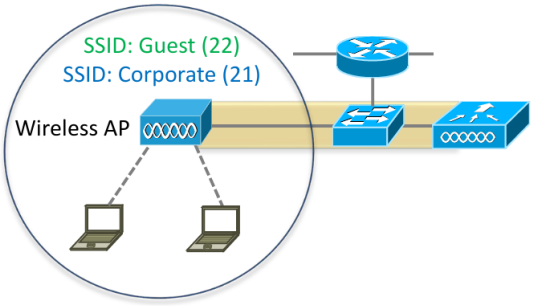
- In this example, VLAN 10 is for the administrator to manage the WLC
- VLAN 11 is for the WLC to manage the Access Points
- The same VLAN can optionally be used for both

```
Switch(config)# vlan 10
Switch(config-vlan)# name WLC-Management
Switch(config)# vlan 11
Switch(config-vlan)# name AP-Management
```



- Configure the interface connected to the WLC as a trunk for the management and WLAN VLANs
- Communication between the WLC and APs is tunneled inside a CAPWAP tunnel

```
Switch(config)# interface GigabitEthernet1/0/2
Switch(config-if)# switchport trunk encap dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,11,21,22
```



- Configure the interface connected to the APs as an access port in the AP management VLAN

```
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 11
```

Wifi Channels and Radio Frequencies

- WiFi services operate in the 2.4 GHz and 5 GHz frequency spectrum.
- This is allocated for ISM industrial, scientific, and medical use

- A radio operator's license is not required.
- ISM devices do not have regulatory protection against interference from other users of the band.

IEEE 802.11 Standards

	802.11	802.11a	802.11b	802.11g	802.11n	802.11ac
Year	1997	1999	1999	2003	2009	2013
Frequency	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz	2.4 & 5 GHz	5 GHz
Data Rate in Mbps & Backwards Compatibility	1, 2	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	1, 2, 5.5, 11 for backward compatibility with b. 6, 9, 12, 18, 24, 36, 48, 54	Up to 600 Backward compatible with a, b, g	Up to 3500 Backward compatible with a and n

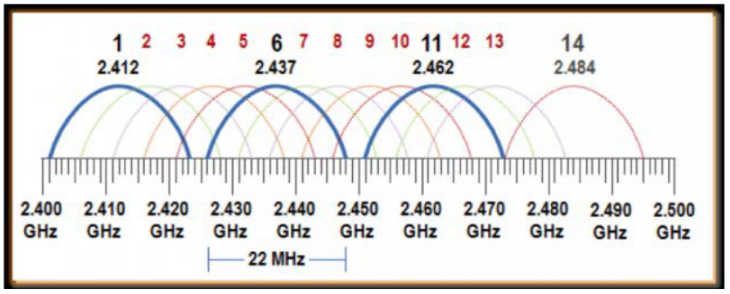
Cisco Access Points support all standards

You can choose which you want to enable per WLAN

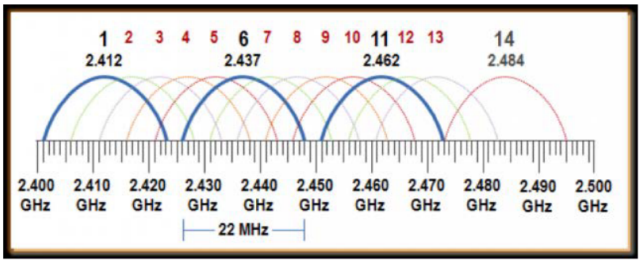
2.4 GHz Spectrum

2.4 GHz Spectrum

- The 2.4 GHz ISM spectrum ranges from 2.4 to 2.4835 GHz
- (2.4 to 2.497 GHz in Japan)
- The spectrum is divided into smaller (22 MHz) ranges of frequencies called channels



- Each AP operates in one channel
- Some channels overlap and can cause interference with each other
- Access Points with overlapping service areas should use non-overlapping channels



2.4 GHz Interference

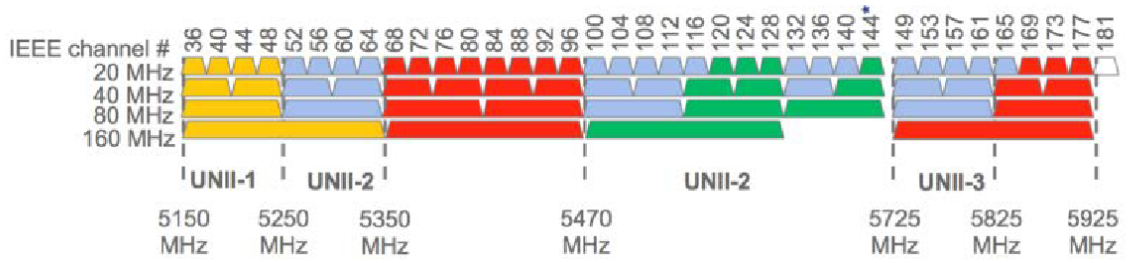
- The ISM band is unlicensed
- Many devices can cause interference in the 2.4 GHz range

5GHz Spectrum

5 GHz Spectrum

- 2.4 GHz channels are 22 MHz wide
- 5 GHz channels are 20 MHz wide
- They have less overlap than 2.4 GHz channels
- Neighboring APs should be separated by at least one channel
- Channels can be bonded (40, 80 or 160 MHz wide) to multiply data rates by 2, 4 or 8x

5 GHz Spectrum



2.4 vs 5 GHz

- 2.4 GHz has greater range and better propagation through obstacles
- 2.4 GHz is more crowded
- 5 GHz 802.11ac has higher throughput than is available with 2.4 GHz
- Your client stations may only be compatible with 2.4 GHz

Wireless Security

- WiFi coverage can leak outside the desired area
- End stations do not need physical access to join the network
- This can make it more vulnerable to attack
- Strong authentication and encryption techniques should be used

Wireless Security Standards

- **WEP** Wired Equivalent Privacy (1999) – RC4 encryption
- **WPA** WiFi Protected Access (2003) – RC4 encryption, TKIP Temporal Key Integrity Protocol
- **WPA2** (2004) – AES encryption, CCMP Counter Cipher Mode with Block Chaining Message Authentication Code protocol
- **WPA3** (2018) – AES encryption, CCMP, protection against KRACK attack

WPA Personal and WPA Enterprise

- **WPA Personal** uses pre-shared keys (PSKs)
- **WPA Enterprise** uses a AAA server