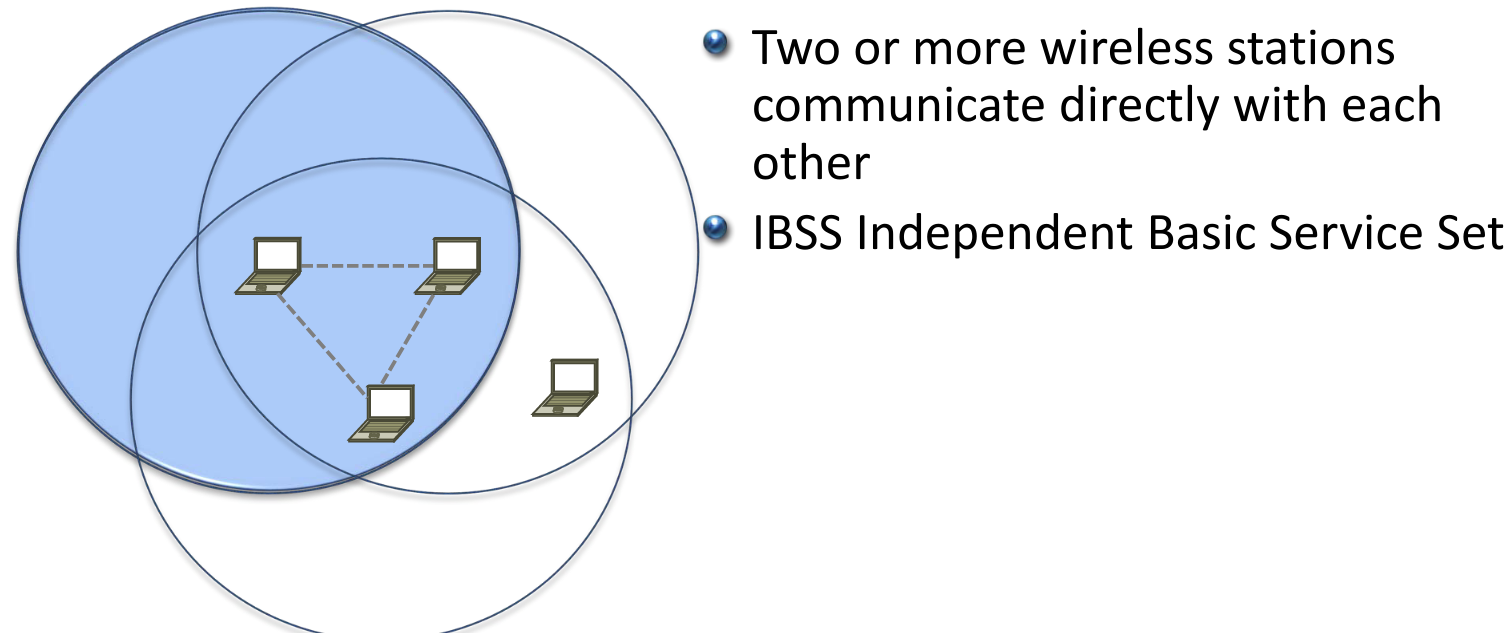
# **802.11 WiFi**

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

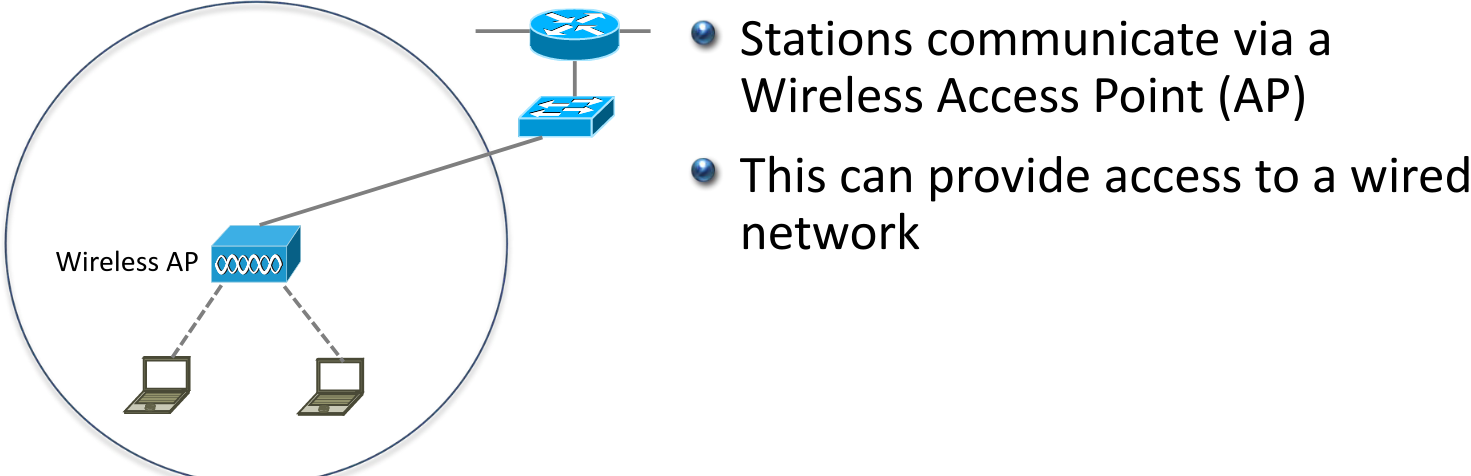
# **Wireless Network Types**

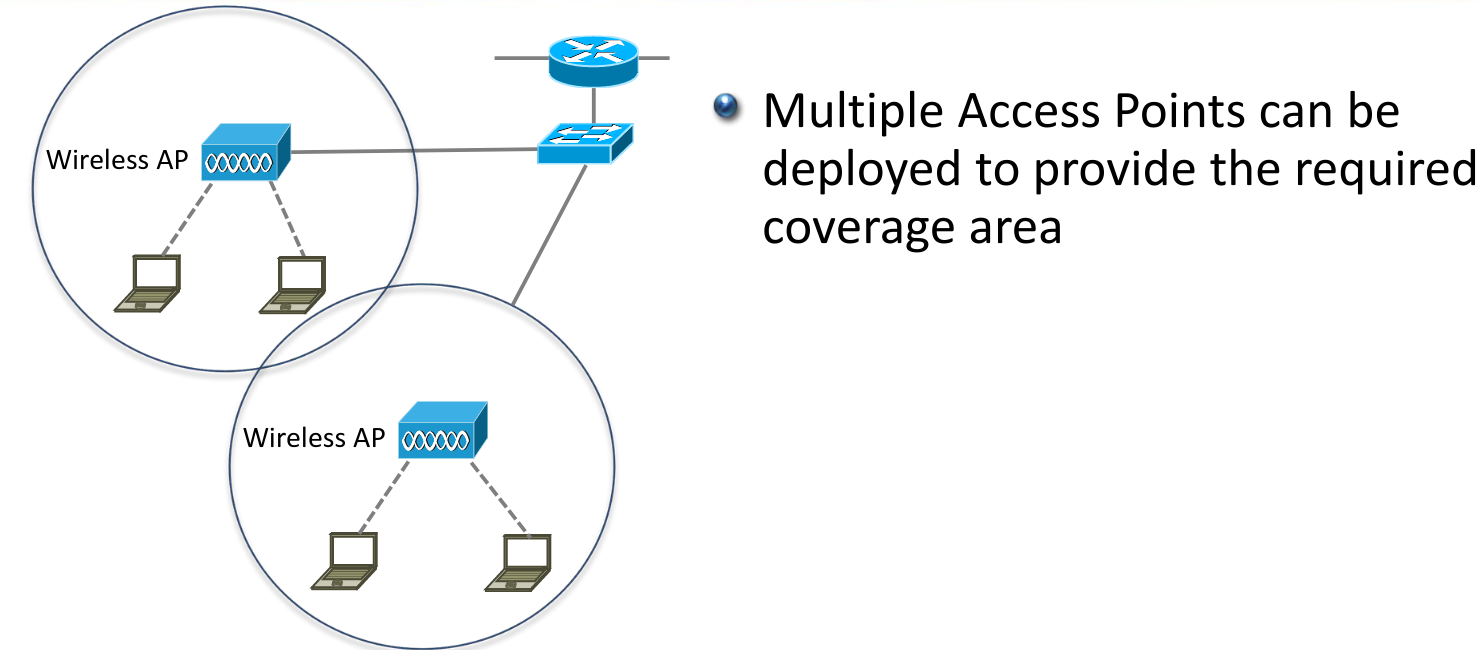
* **WPAN**: Wireless Personal Area Network
  + Devices are within 10 meters of each other
  + Bluetooth is often used
* **WLAN**: Wireless Local Area Network
  + Provides access to a campus (typically wired) network, without the need for a cable
  + Devices within 100m of a Wireless Access Point
* **WMAN**: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

## **Ad Hoc Networks**



## **Infrastructure Mode**





**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

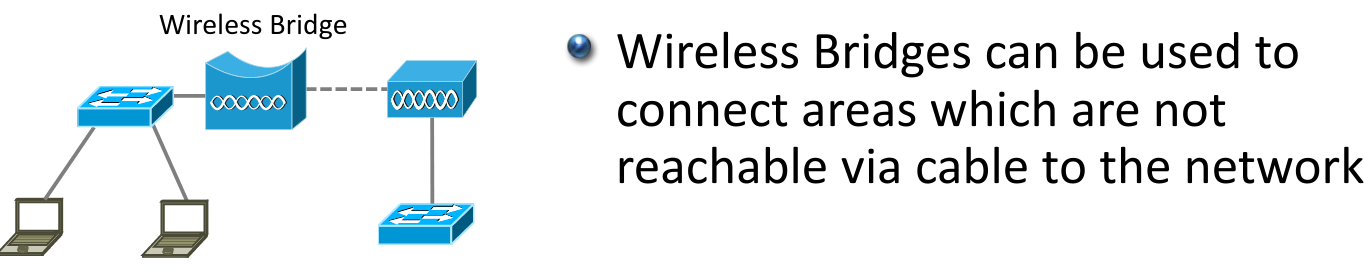
## **WiFi Direct**

* 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**



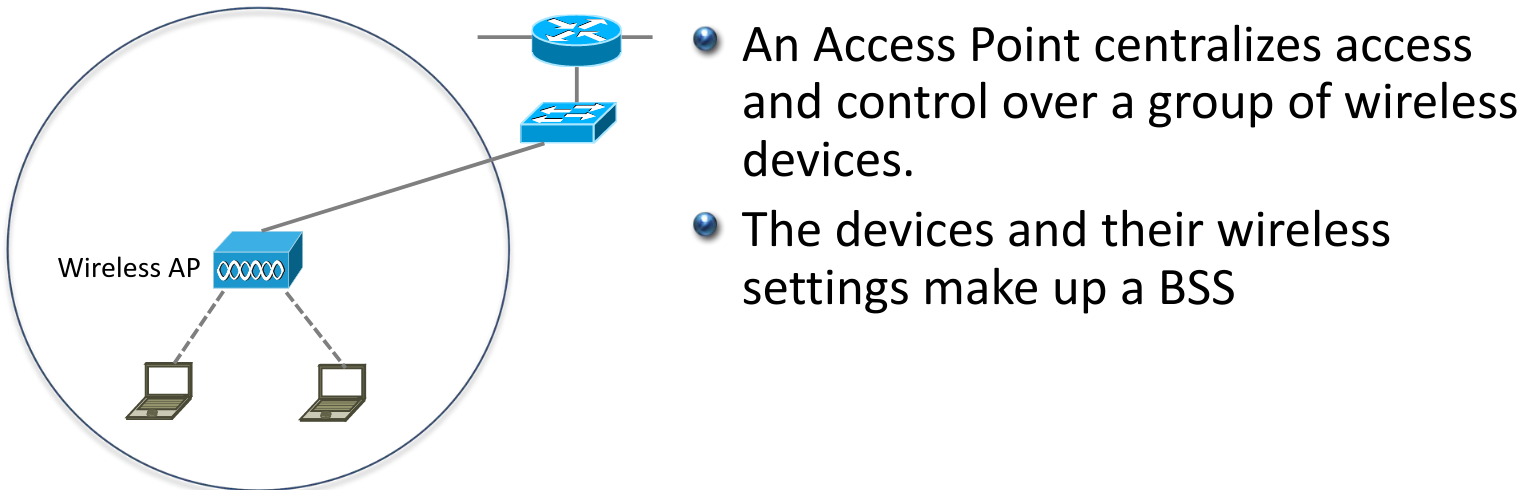
## **Mesh Networks**



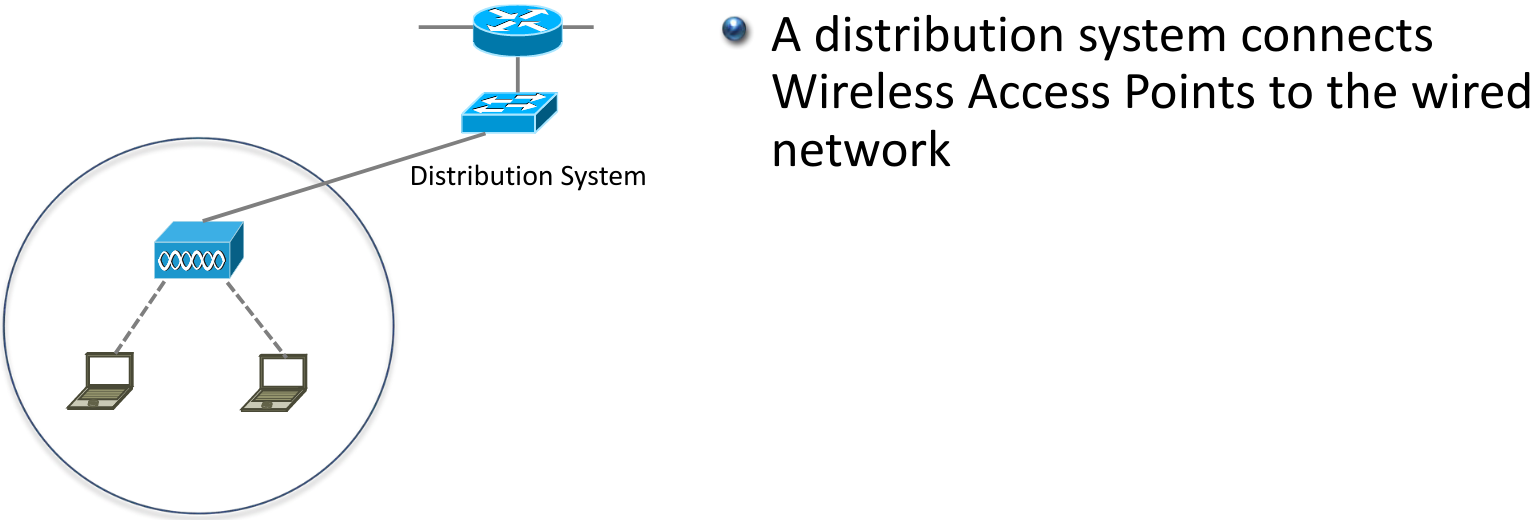
# **Wireless Access Points**

* 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

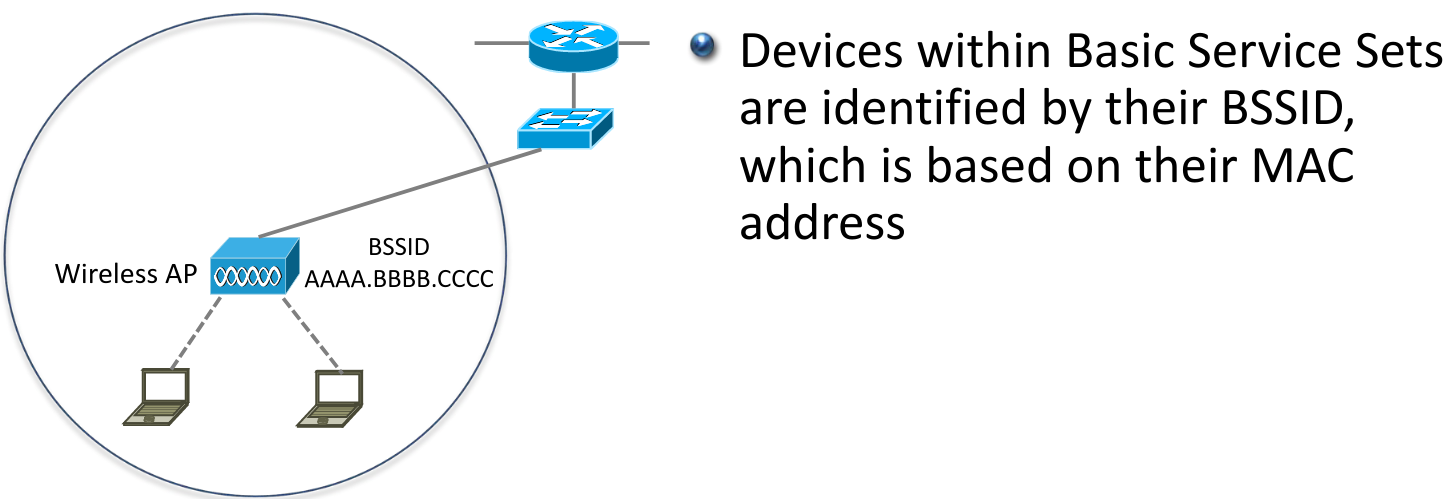
## **BSS Basic Service Set**



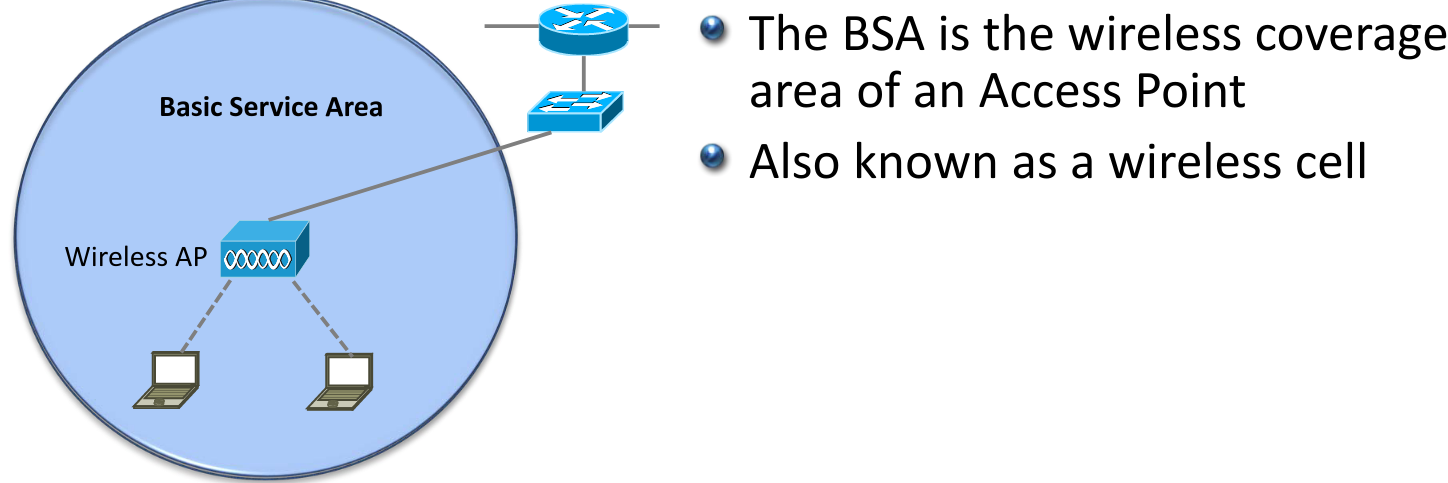
## **DS Distribution System**



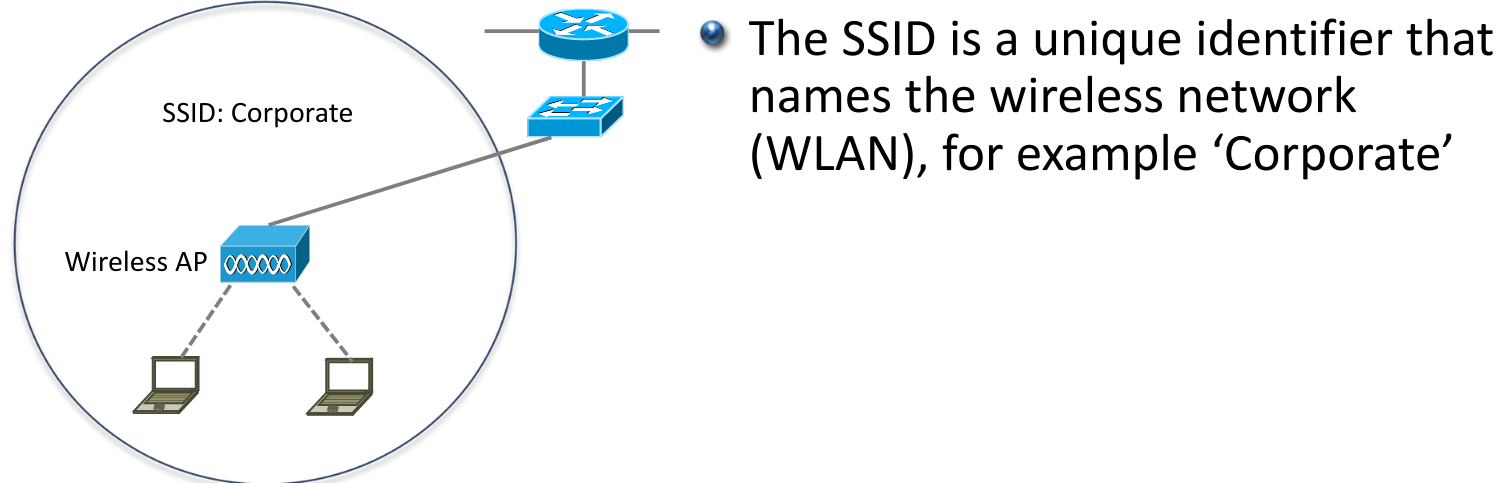
## **BSSID Basic Service Set Identifier**



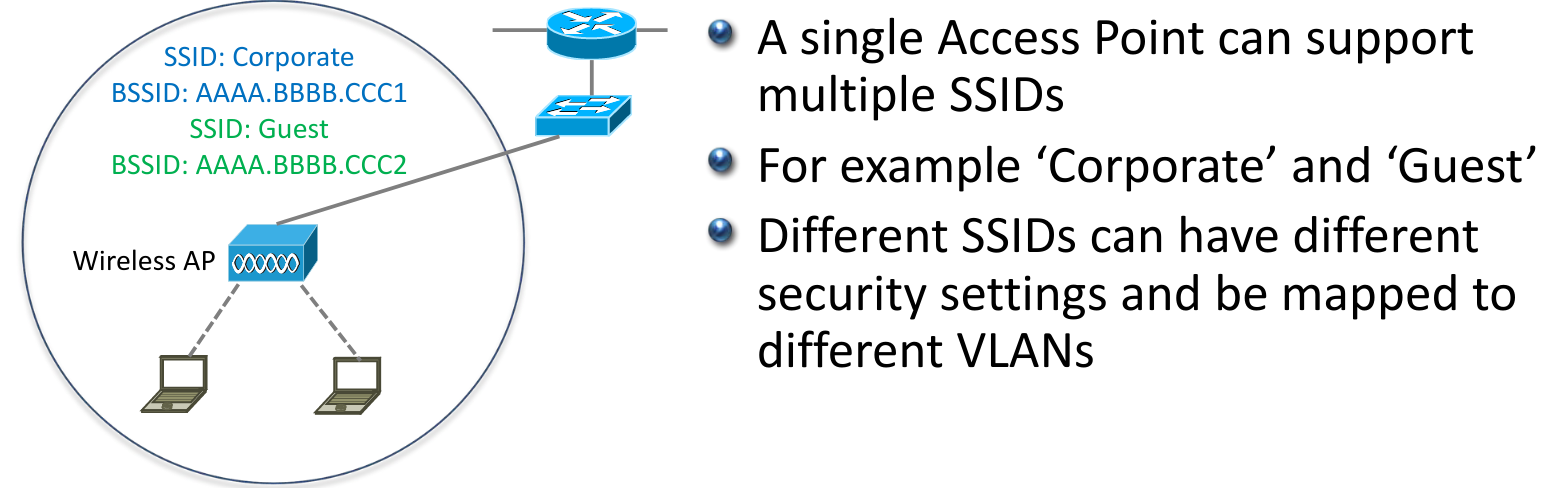
## **BSA Basic Service Area**



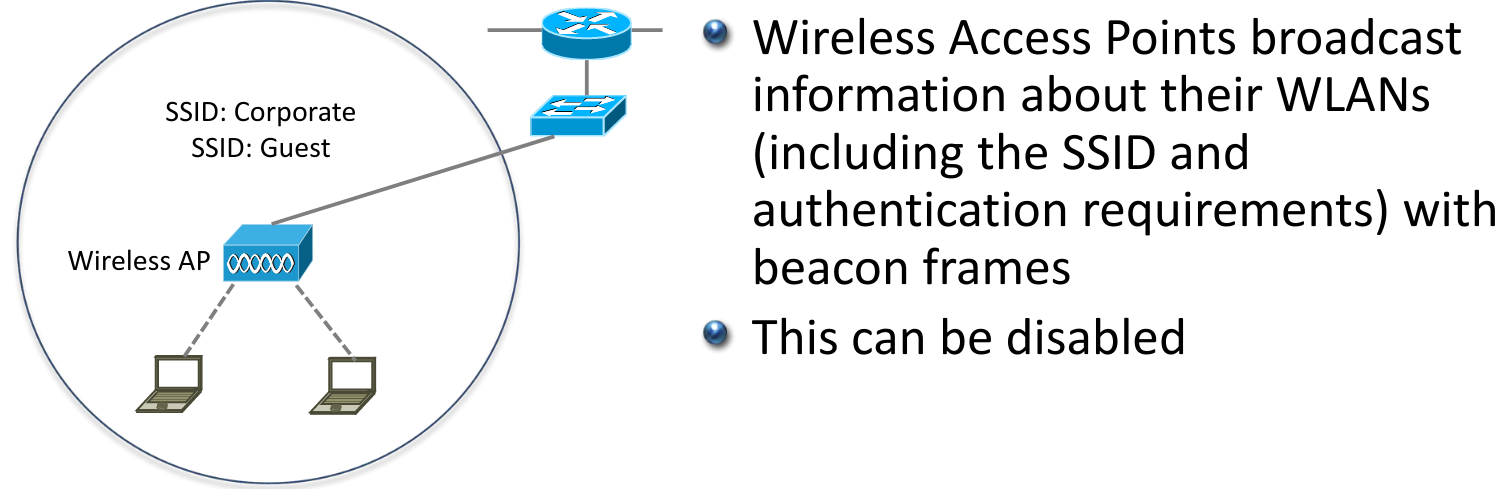
## **SSID Service Set Identifier**



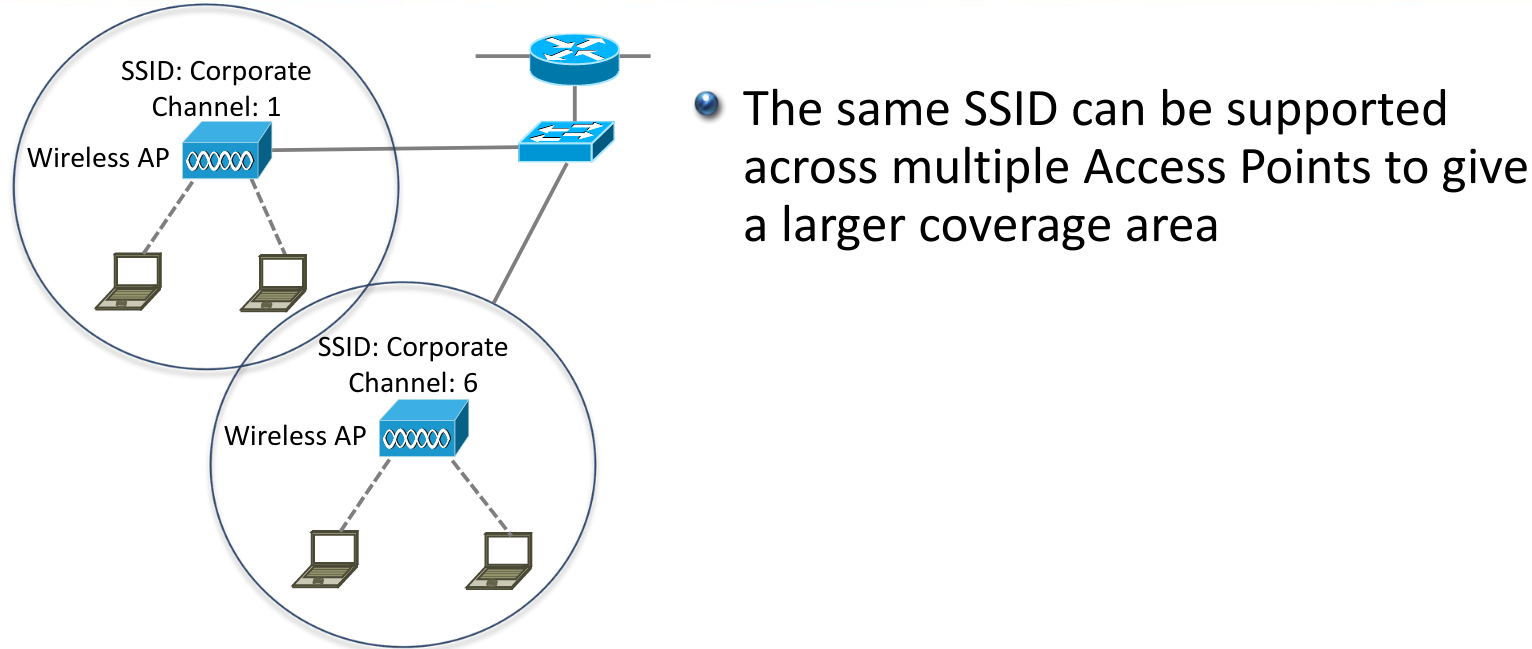
## **Multiple SSID Service Set Identifiers**



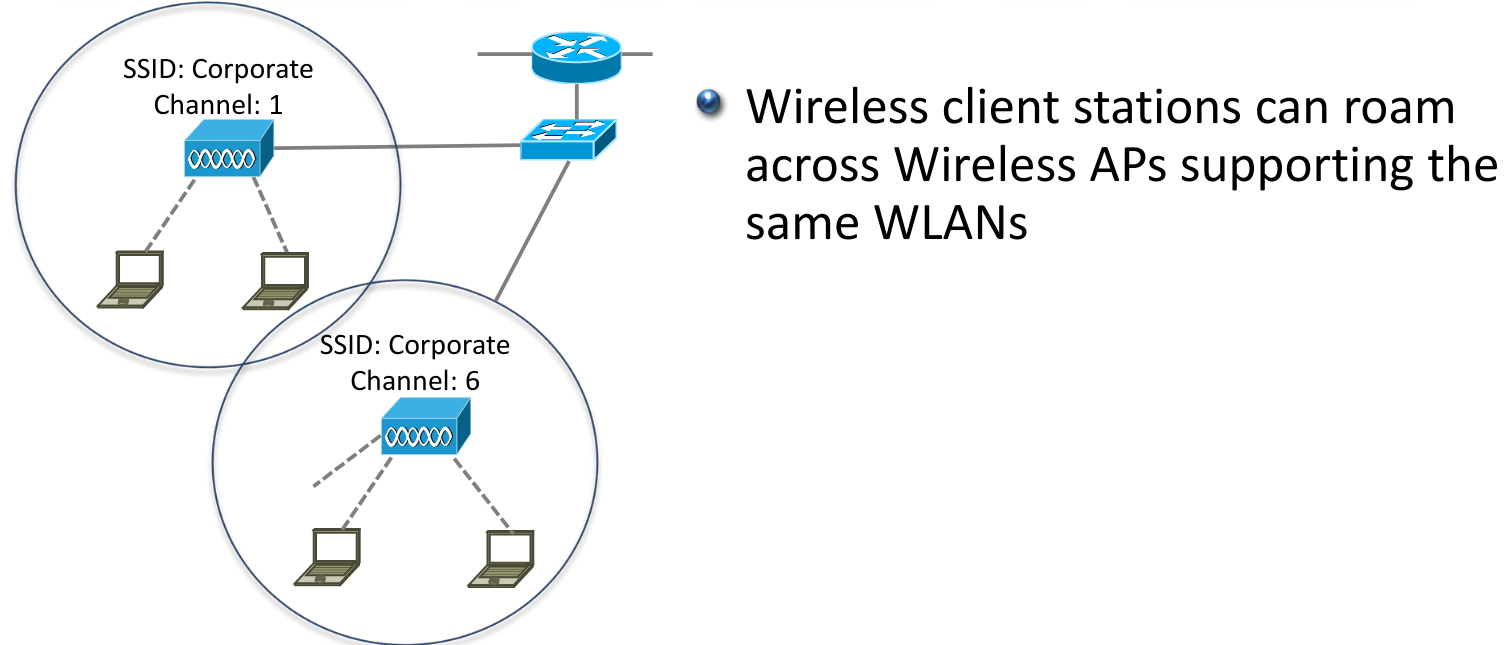
## **Beacons**



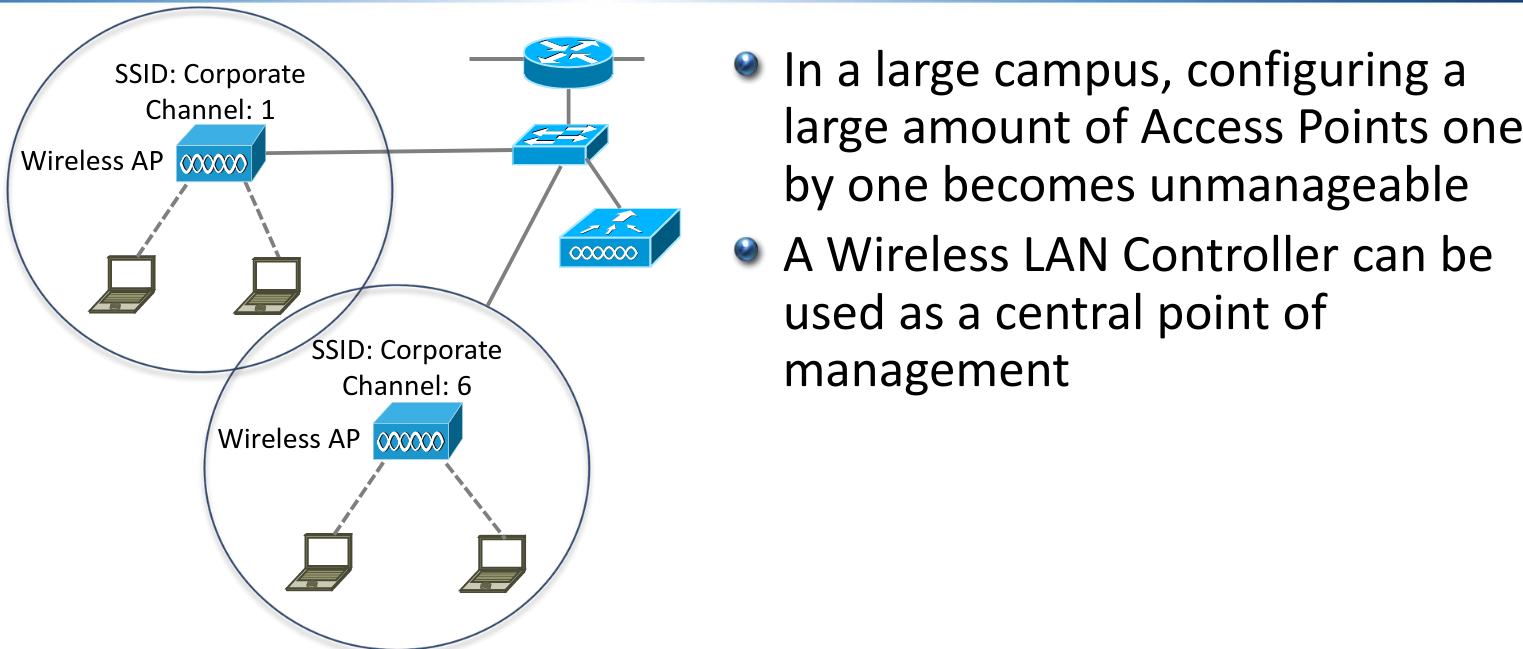
## **ESS Extended Service Set**



## **Roaming**



# **WLC Wireless LAN Controllers**



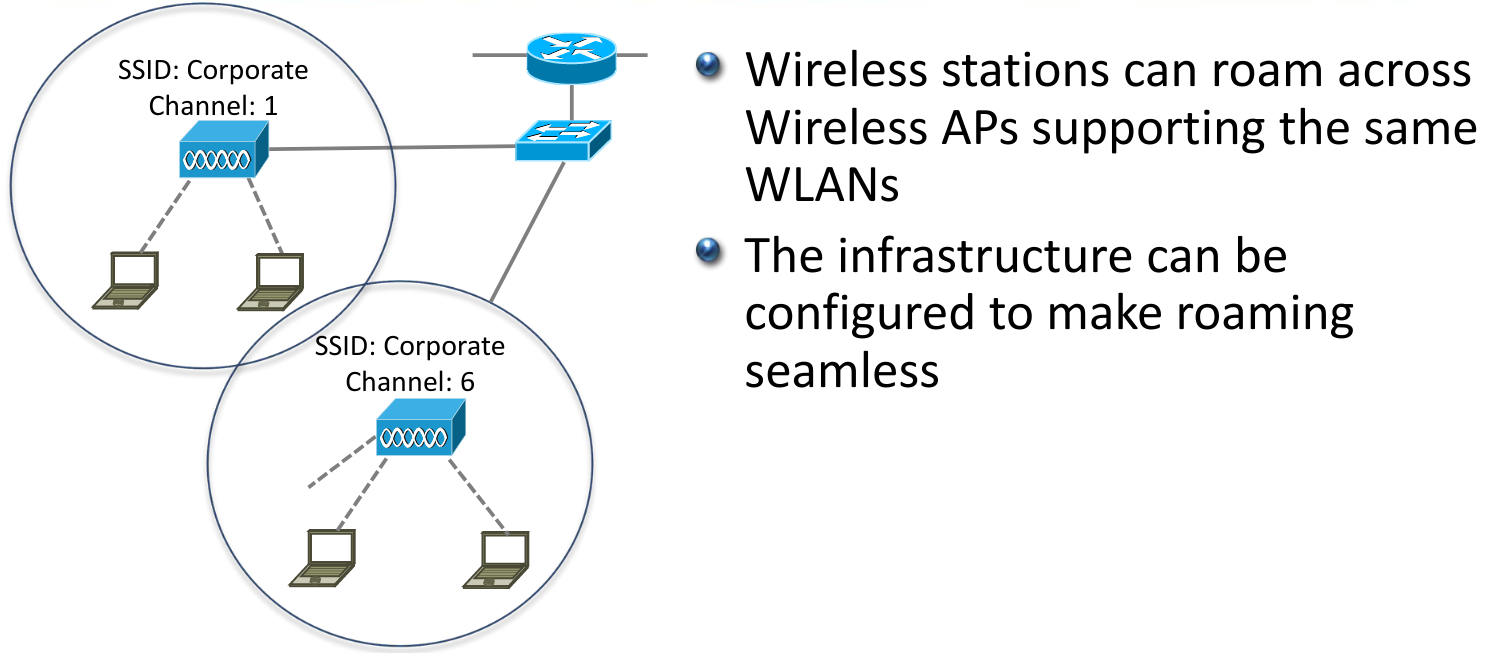
## **Autonomous vs Lightweight Access Points**

* 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**



## **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**

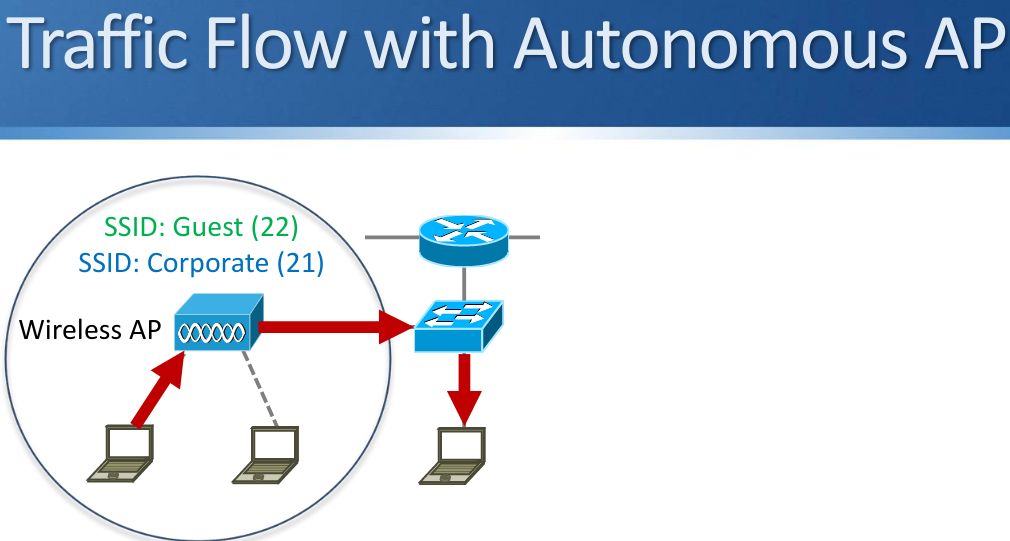
* Work is moved from the APs to the WLC which is why they are called Lightweight APs
* Real-Time traffic is still handled by the AP in order to provide suitable performance, the rest is handled by the WLC
* This is known as ‘Split MAC’

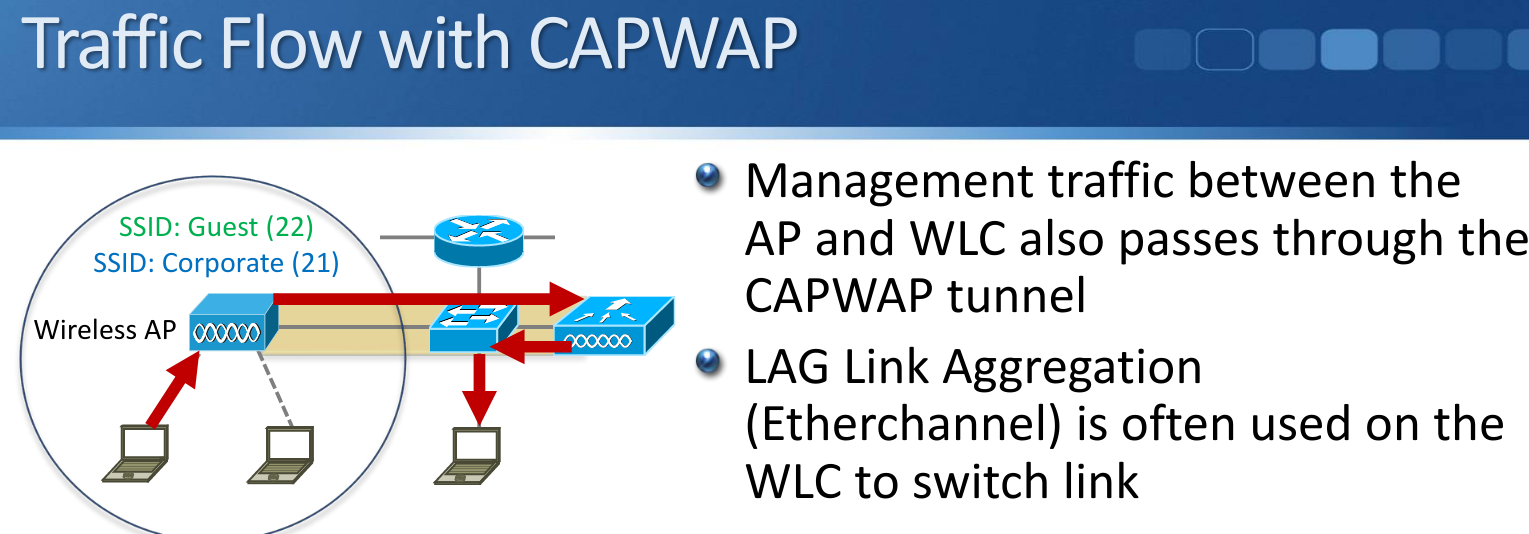
Split MAC – AP Operations

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

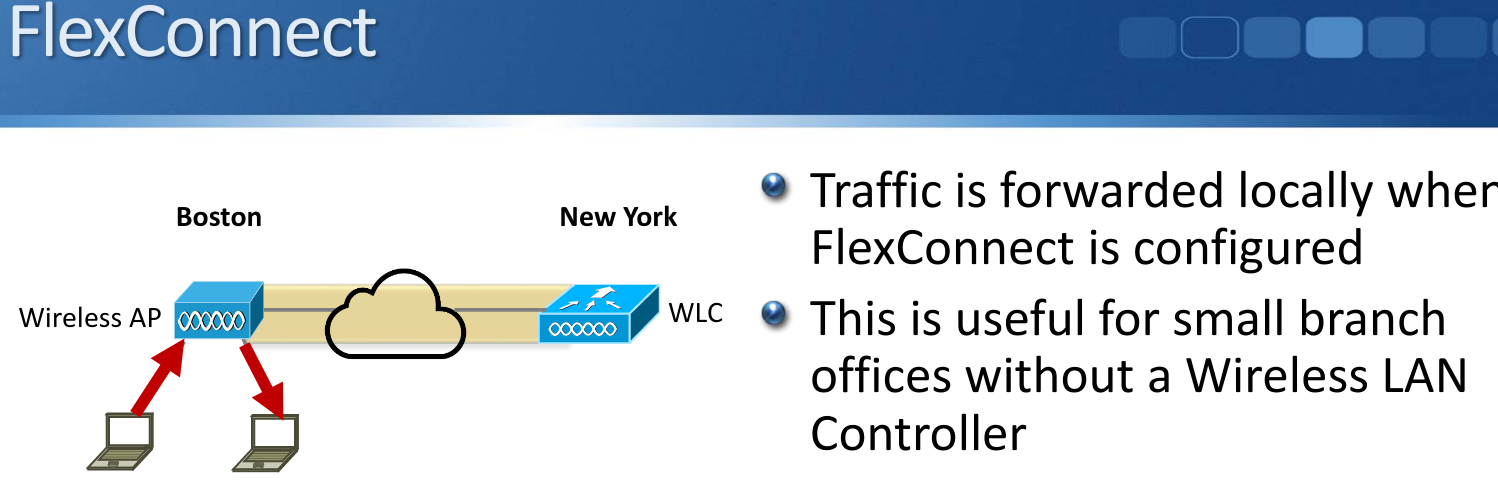
Split MAC – WLC Operations

* Authentication
* Roaming control
* 802.11 to 802.3 communication
* Radio Frequency management
* Security management
* QoS management

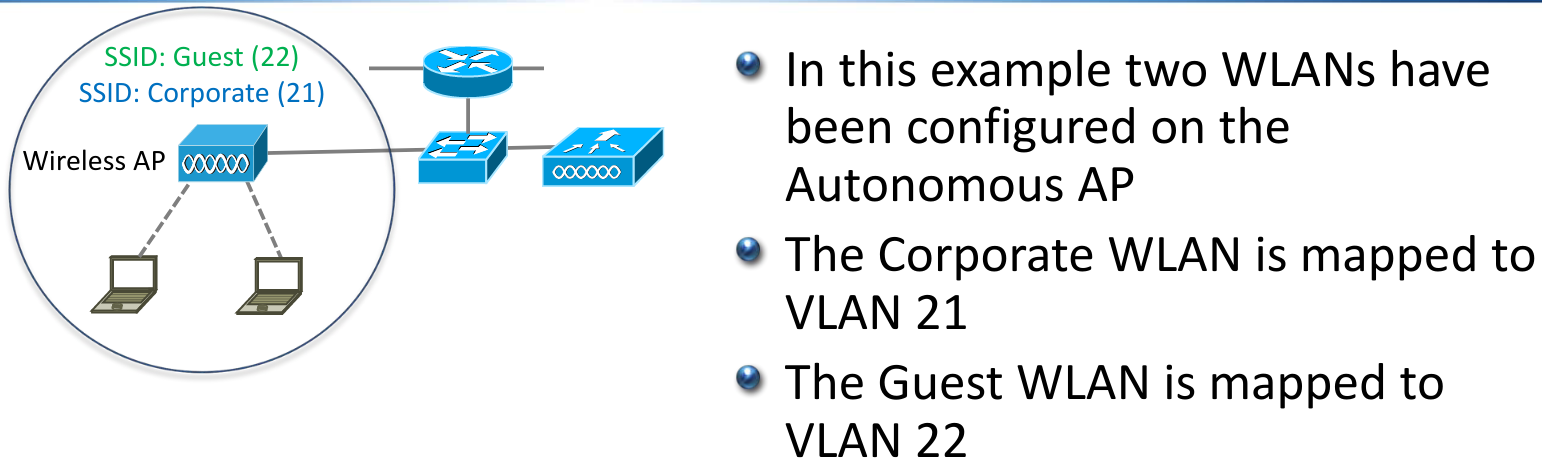


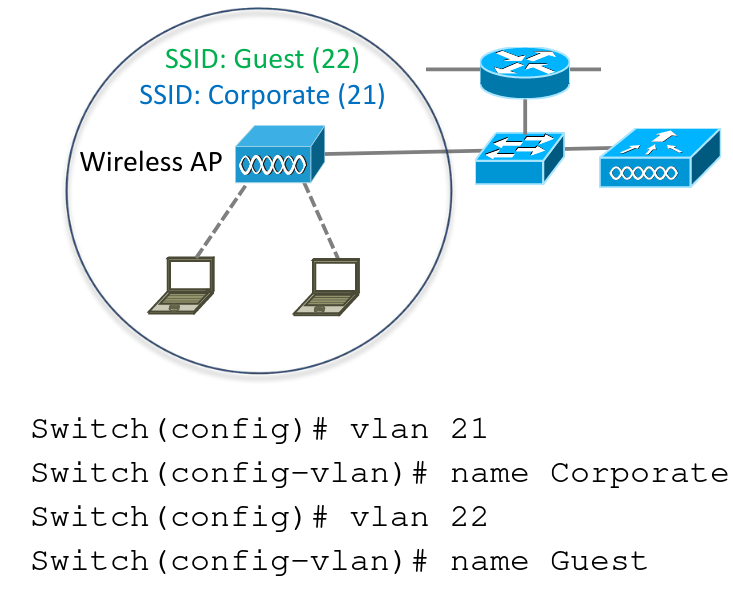


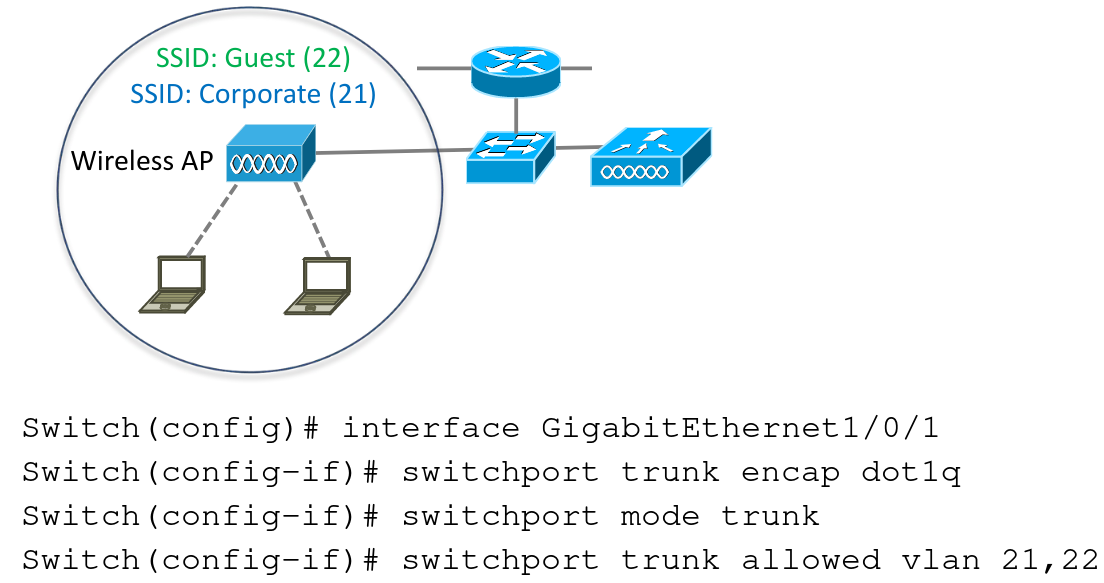
## **Flexconnect**



# **Autonomous AP Switch Configuration**

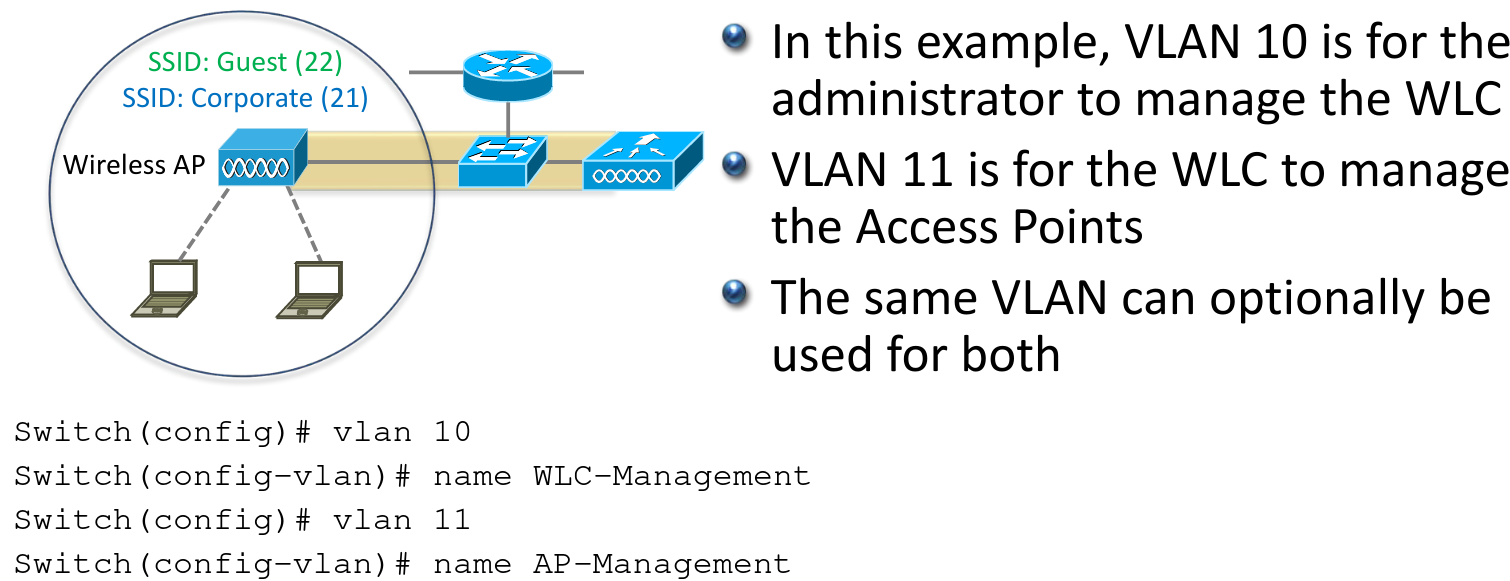


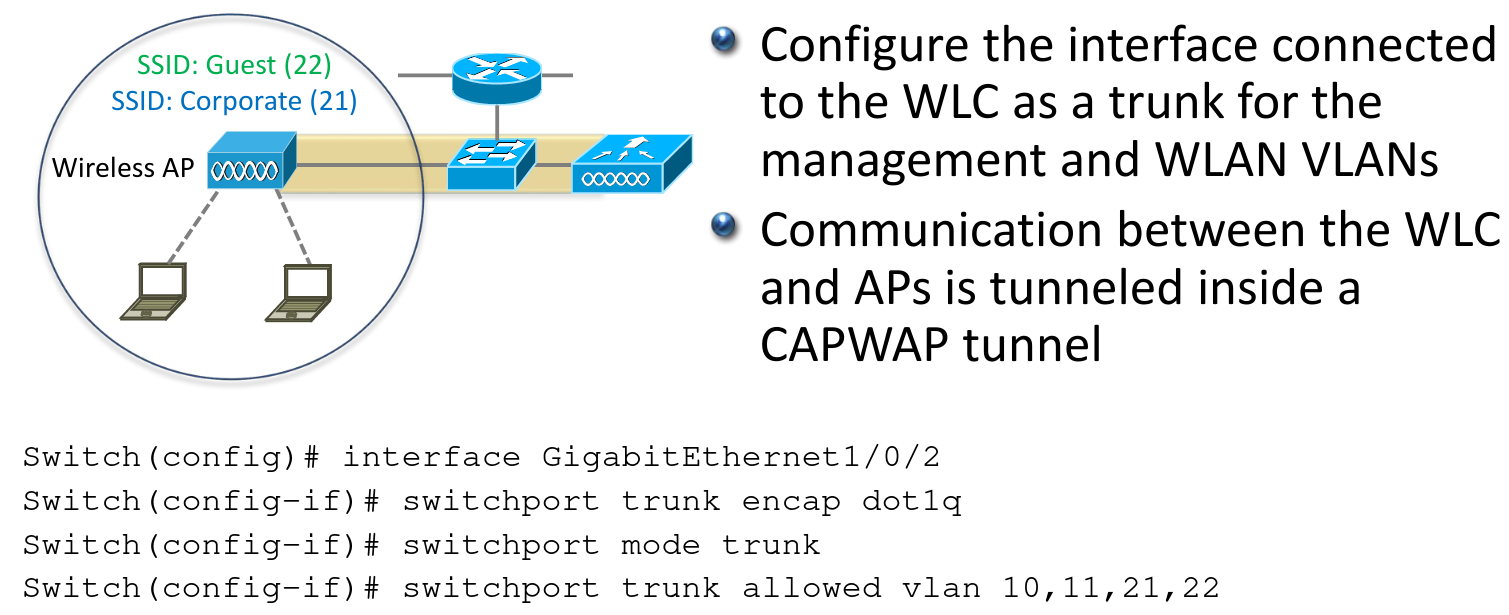


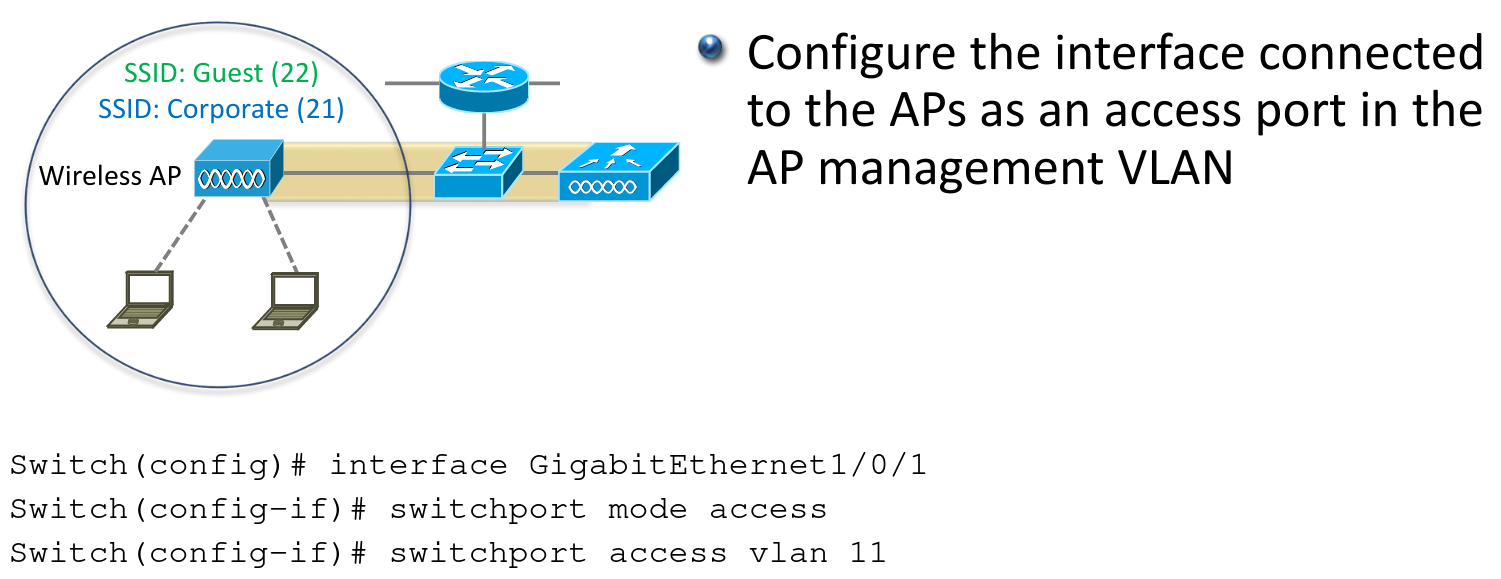


# **Lightweight AP Switch Configuration**



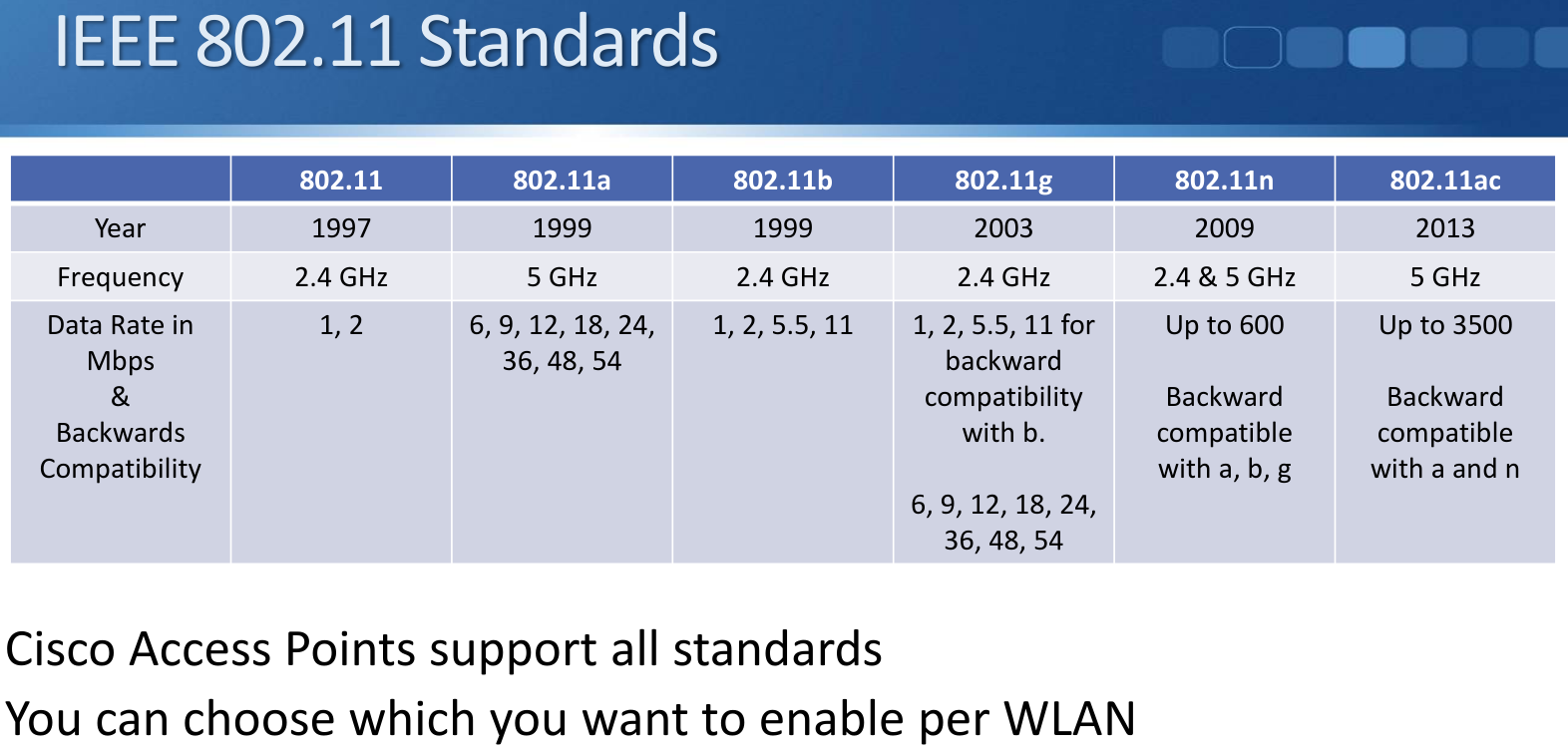




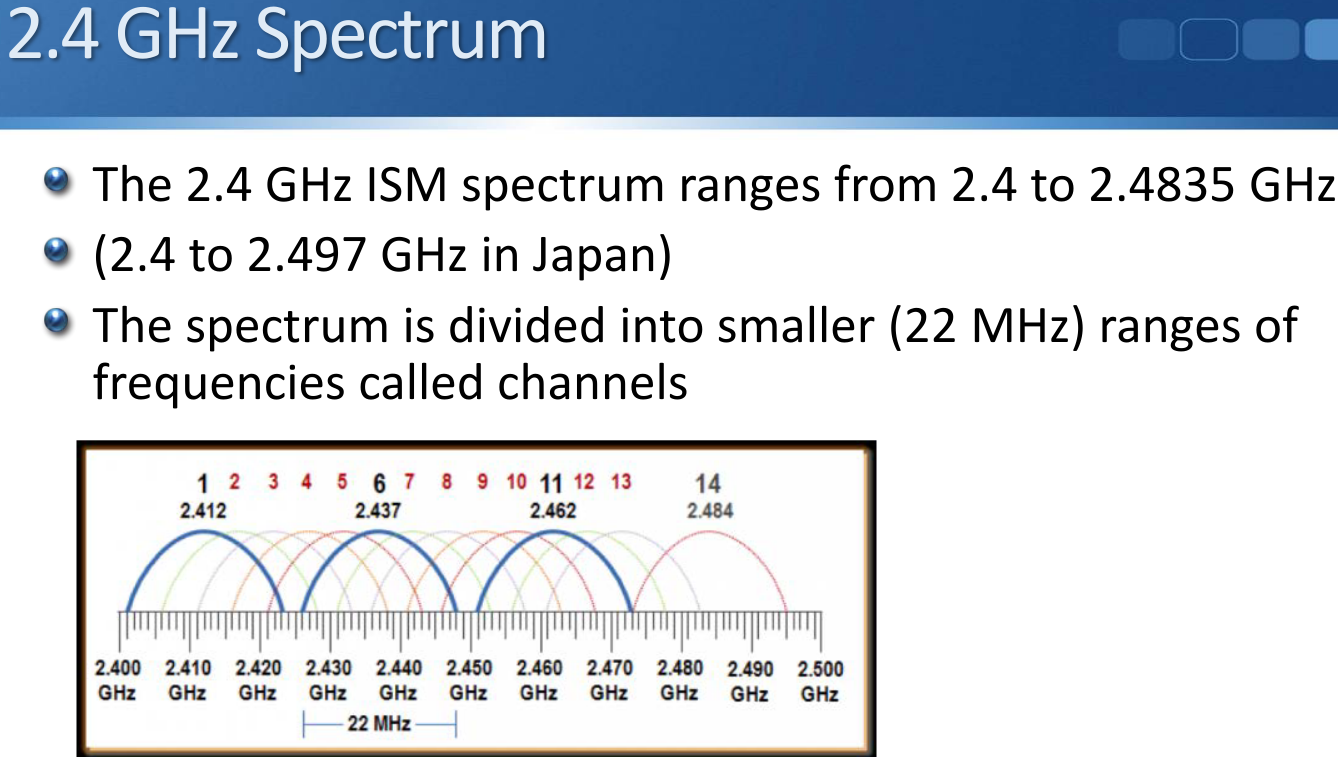


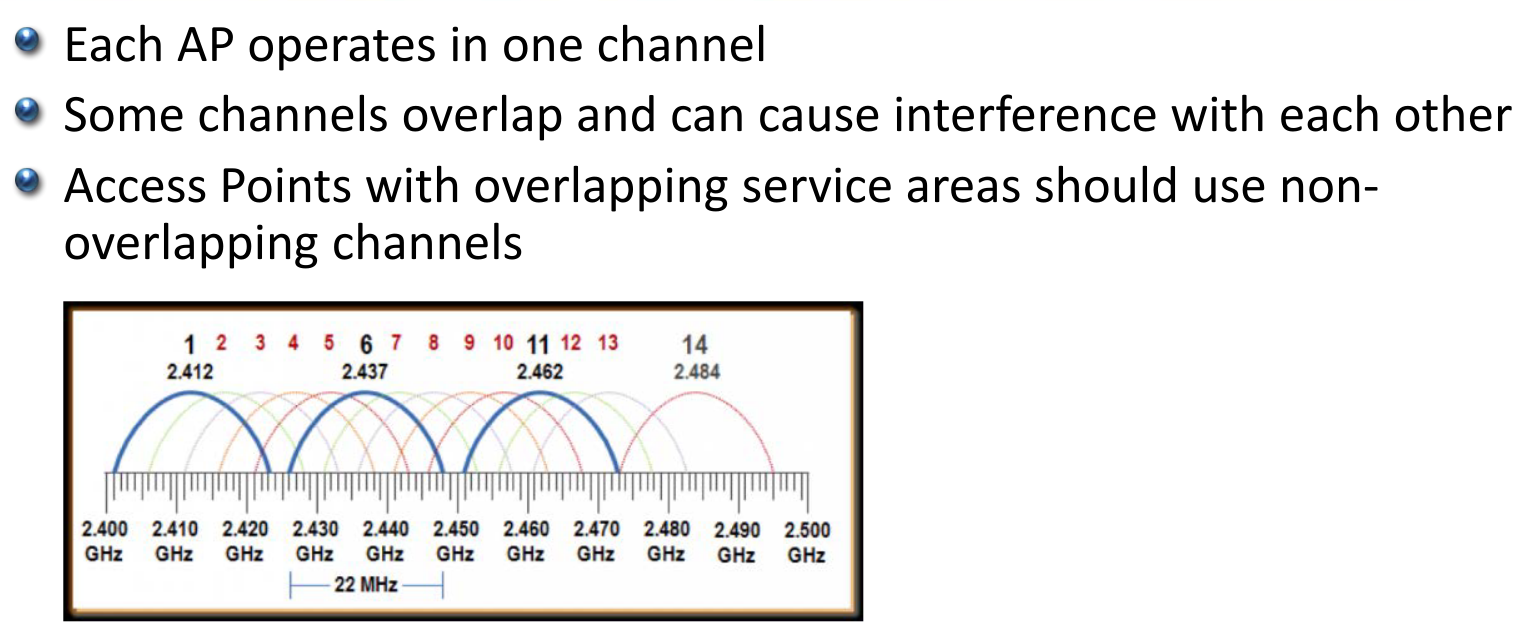
# **Wifi Channels and Radio Frequencies**

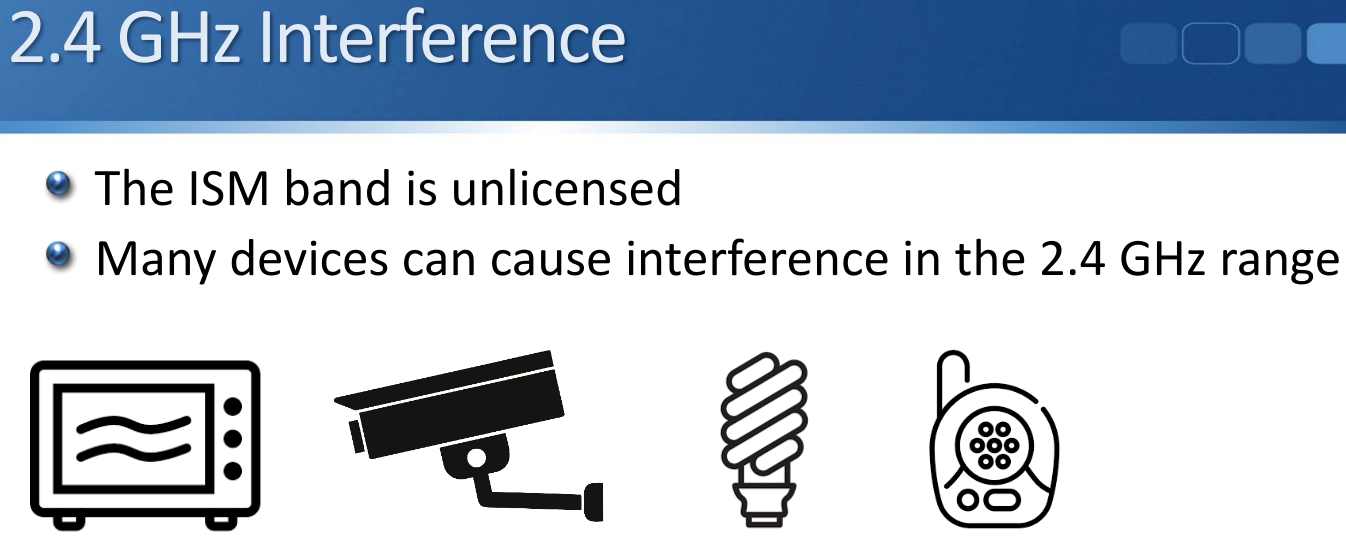
* WiFi services operate in the 2.4 GHz and 5 GHz frequency spectrum.
* This is allocated for ISM industrial, scientific, and medical use
* A radio operator's license is not required.
* ISM devices do not have regulatory protection against interference from other users of the band.



# **2.4 GHz Spectrum**

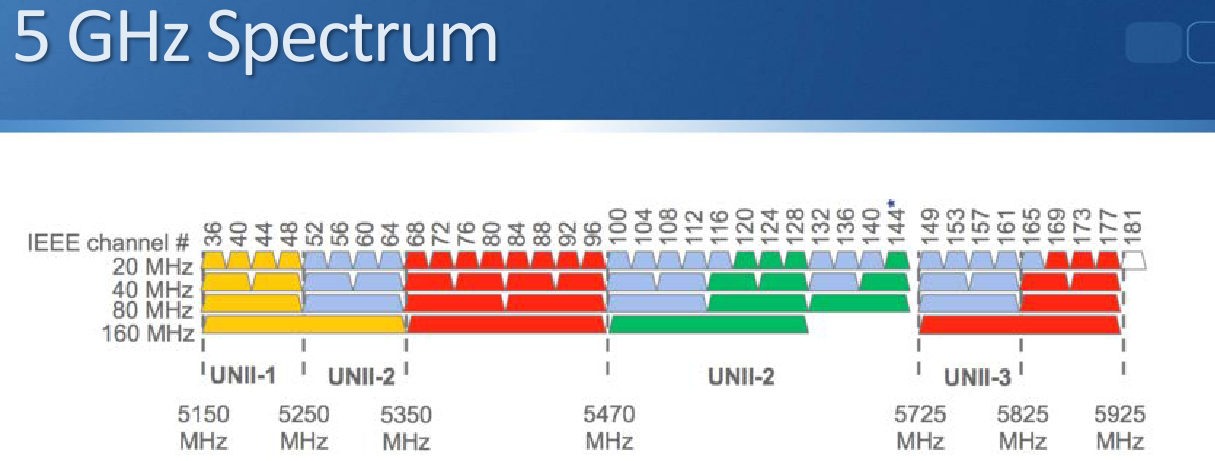


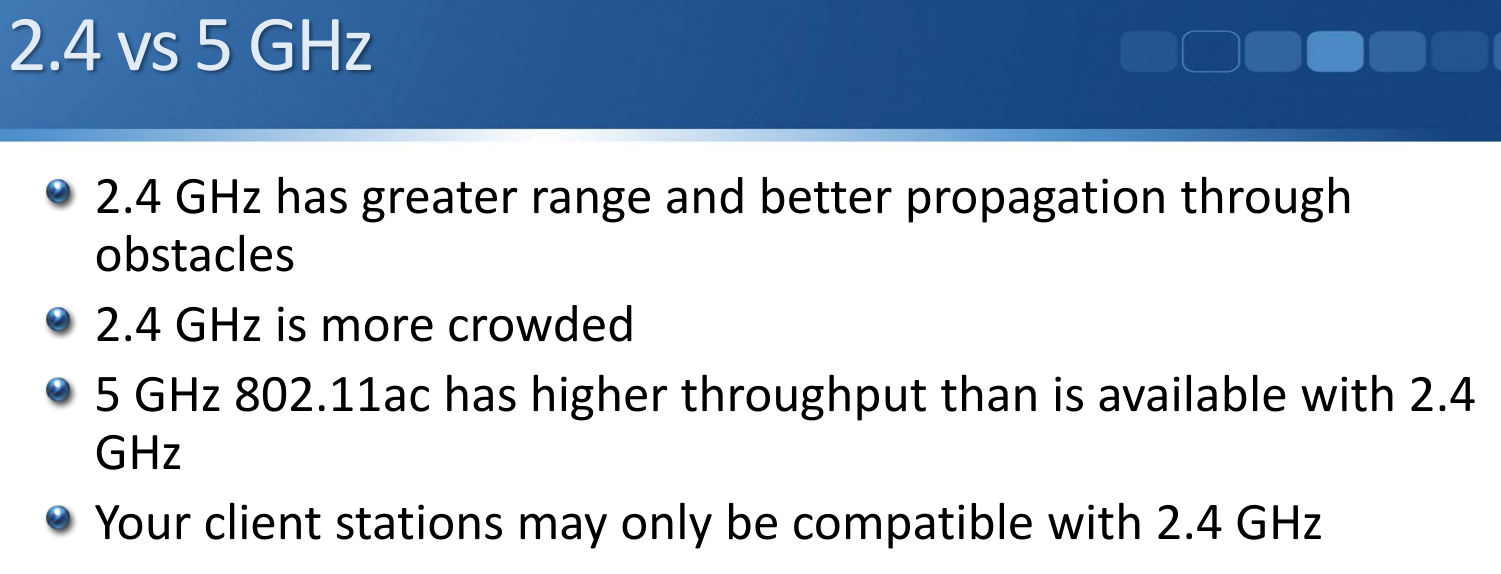




# **5GHz Spectrum**







# **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**

