Wireless Fundamentals

Differences Between WLAN and LAN

- WLANs use radio waves as the physical layer.
  - WLANs use CSMA/CA instead of CSMA/CD for media access.
  - Two-way radio (half-duplex) communication.
- Radio waves have problems that are not found on wires.
  - Connectivity issues:
    - Coverage problems
    - Interference, noise
  - Privacy issues
- Access points are shared devices similar to an Ethernet hub for shared bandwidth.
- WLANs must meet country-specific RF regulations.

Benefits of Wireless

Mobility

Scalability

- can be added to a network easily
- use of “hotspots”

Flexibility

- anytime, anywhere connectivity

Cost

- inexpensive to install
- reduced installation costs

Limitations/Risks of Wireless

Uses unlicensed regions of the RF spectrum

- used by many different devices

Interference

- cordless phones
- microwaves

Security

- easy access to the network
- encryption/authentication helps with security issues

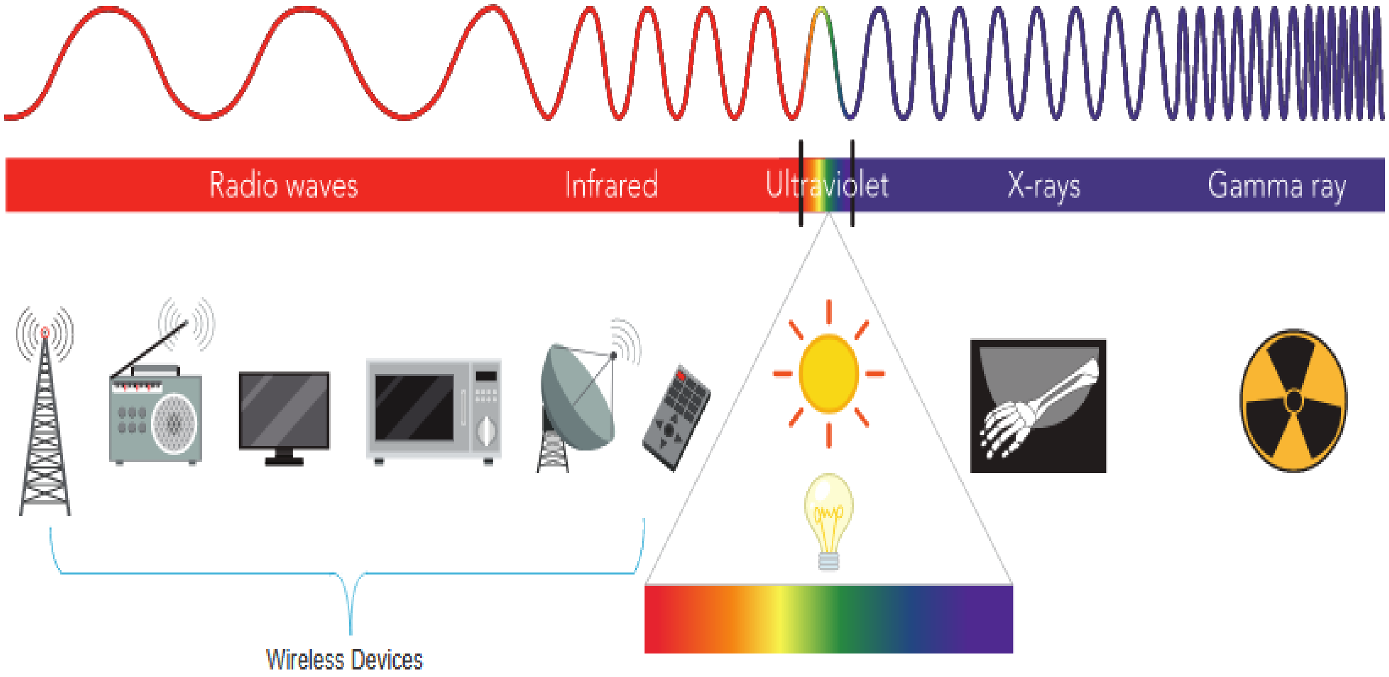
Types of Wireless Networks

- Wireless Personal-Area Network (**WPAN**) – Low power and short-range (20-30ft or 6-9 meters). Based on IEEE 802.15 standard and 2.4 GHz frequency. Bluetooth and Zigbee are WPAN examples.
- Wireless LAN (**WLAN**) – Medium sized networks up to about 300 feet. Based on IEEE 802.11 standard and 2.4 or 5.0 GHz frequency.
- Wireless MAN (**WMAN**) – Large geographic area such as city or district. Uses specific licensed frequencies.
- Wireless WAN (**WWAN**) – Extensive geographic area for national or global communication. Uses specific licensed frequencies.

Radio Frequencies

All wireless devices operate in the range of the electromagnetic spectrum. WLAN networks operate in the 2.4 and 5 GHz frequency bands.

- **2.4 GHz** (**UHF**) – 802.11b/g/n/ax
- **5 GHz** (**SHF**) – 802.11a/n/ac/ax



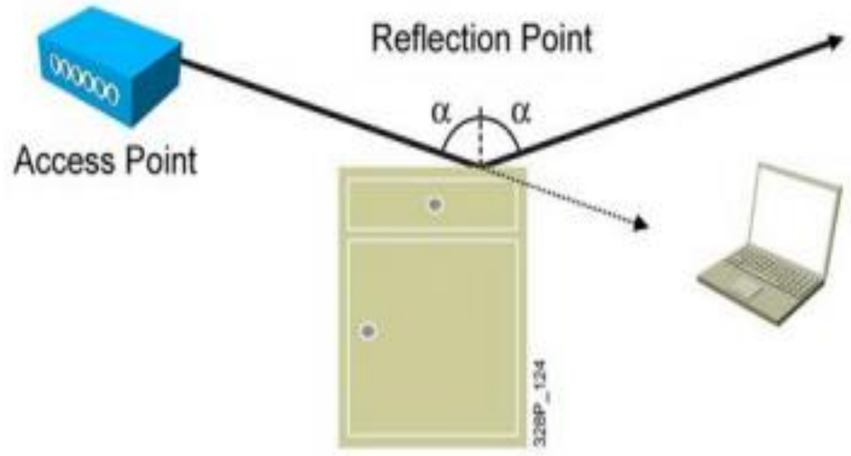
Radio Frequency (RF)

- Signal able to transmit through walls
- RF bands set aside for wireless devices, including cordless phones and computer peripherals
- 900 MHz – used by cell phones
- 2.4 GHz
  - Bluetooth technology
  - low speed, short range
  - can communicate with many devices at once
- 5 GHz
  - Wireless LAN
  - transmit at a higher level = greater distance
  - conform to 802.11 standards

RF Principles

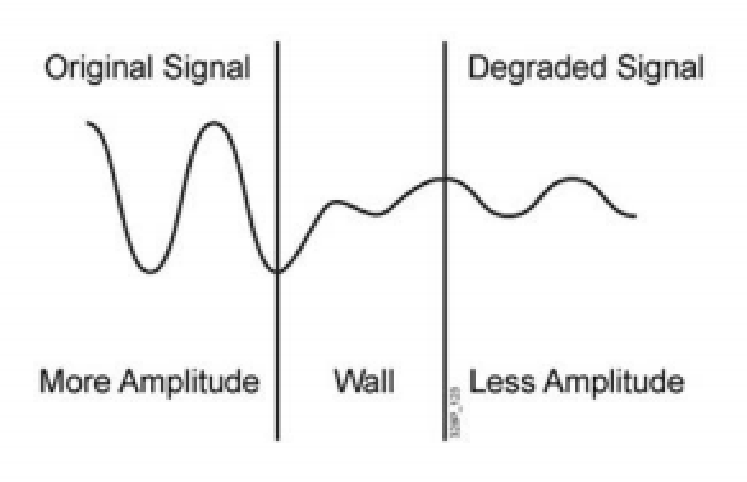
- **Reflections:** When the radio wave hits the obstacle at a low angle, the wave (the entire wave, or part of it) might bounce on the obstacle. This phenomenon is called reflection.

- **Refraction:** Refraction occurs when a wave changes direction. This change in direction usually happens when a wave passes from one medium to another (from air to water, for example).

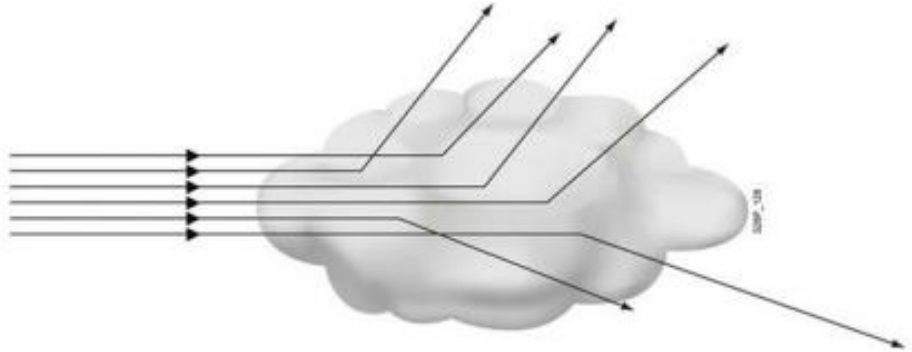


RF Principles

- **Absorption:** When radio waves go through 'something' (some material), they generally get weakened or dampened. How much they lose in power will depend on the material.



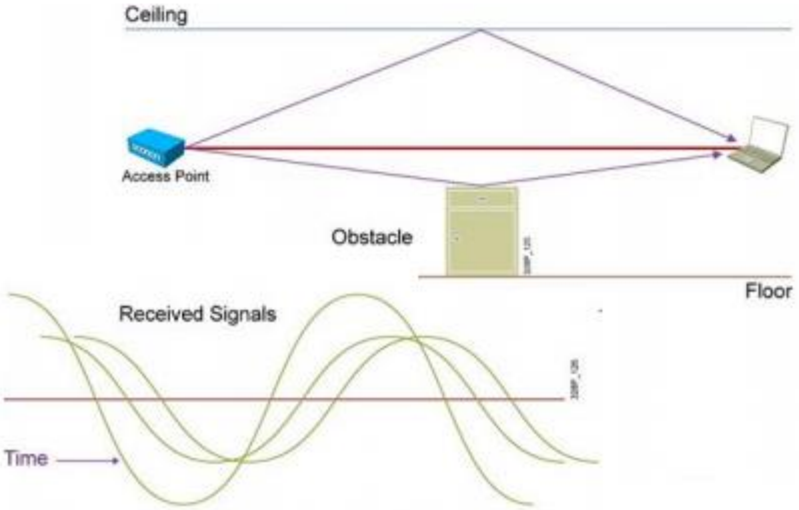
- **Scattering:** Reflection also occurs in the air itself, bouncing on dust or micro drops of water (humidity). These multiple reflections are described as scattering.

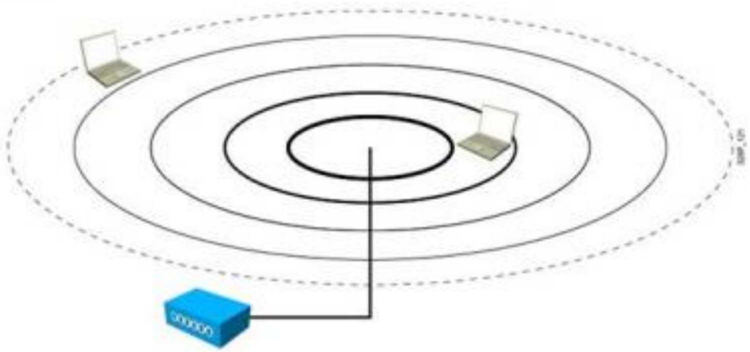


RF Principles

- **Multipath:** A signal sent to a station travels in a straight line and reaches the destination. A few microseconds later, copies of the same signal reflected on walls, ceiling, and obstacles also reach the destination.

- **Free Path Loss:** Even without obstacles, a radio wave gets weaker as it moves away from the emitting source because the energy of the wave spreads.





Frequency Channel Saturation

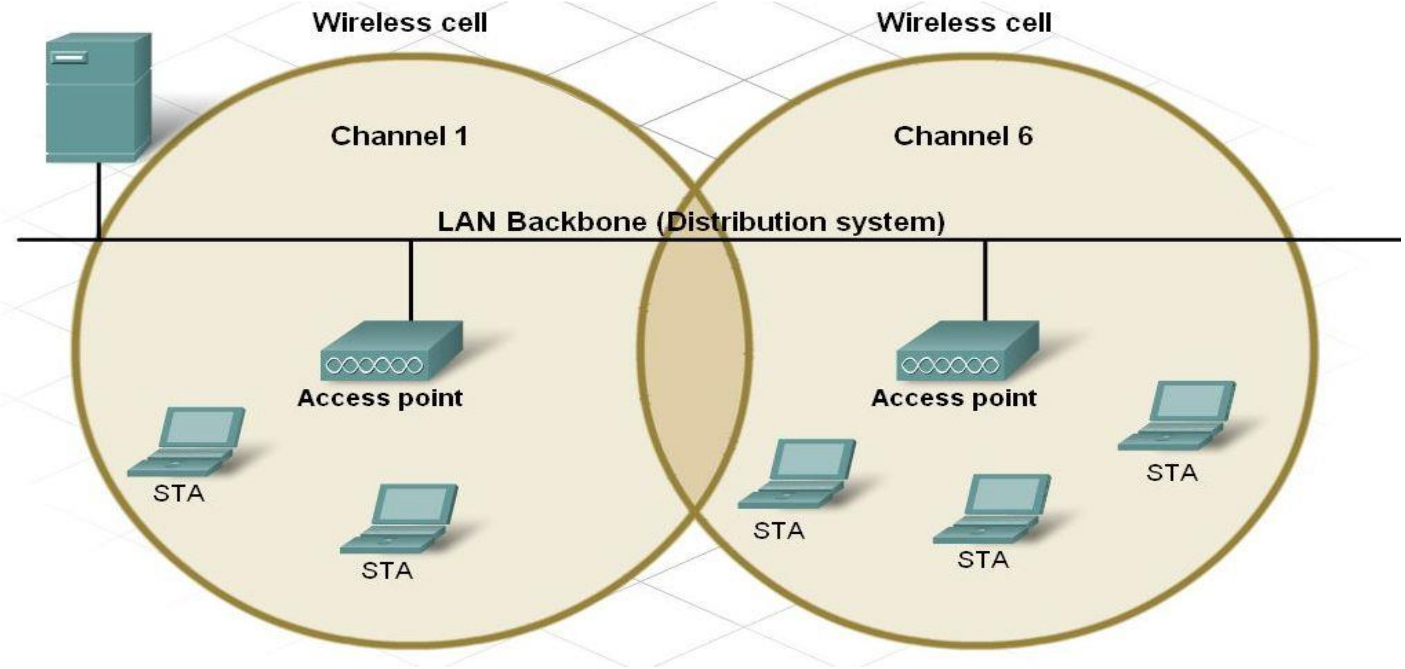
If the demand for a specific wireless channel is too high, the channel may become oversaturated, degrading the quality of the communication.

Channel saturation can be mitigated using techniques that use the channels more efficiently.

- Direct-Sequence Spread Spectrum (**DSSS**) - A modulation technique designed to spread a signal over a larger frequency band. Used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.
- Frequency-Hopping Spread Spectrum (**FHSS**) - Transmits radio signals by rapidly switching a carrier signal among many frequency channels. Sender and receiver must be synchronized to “know” which channel to jump to. Used by the original 802.11 standard.
- Orthogonal Frequency-Division Multiplexing (**OFDM**) - A subset of frequency division multiplexing in which a single channel uses multiple sub-channels on adjacent frequencies. OFDM is used by a number of communication systems including 802.11a/g/n/ac.

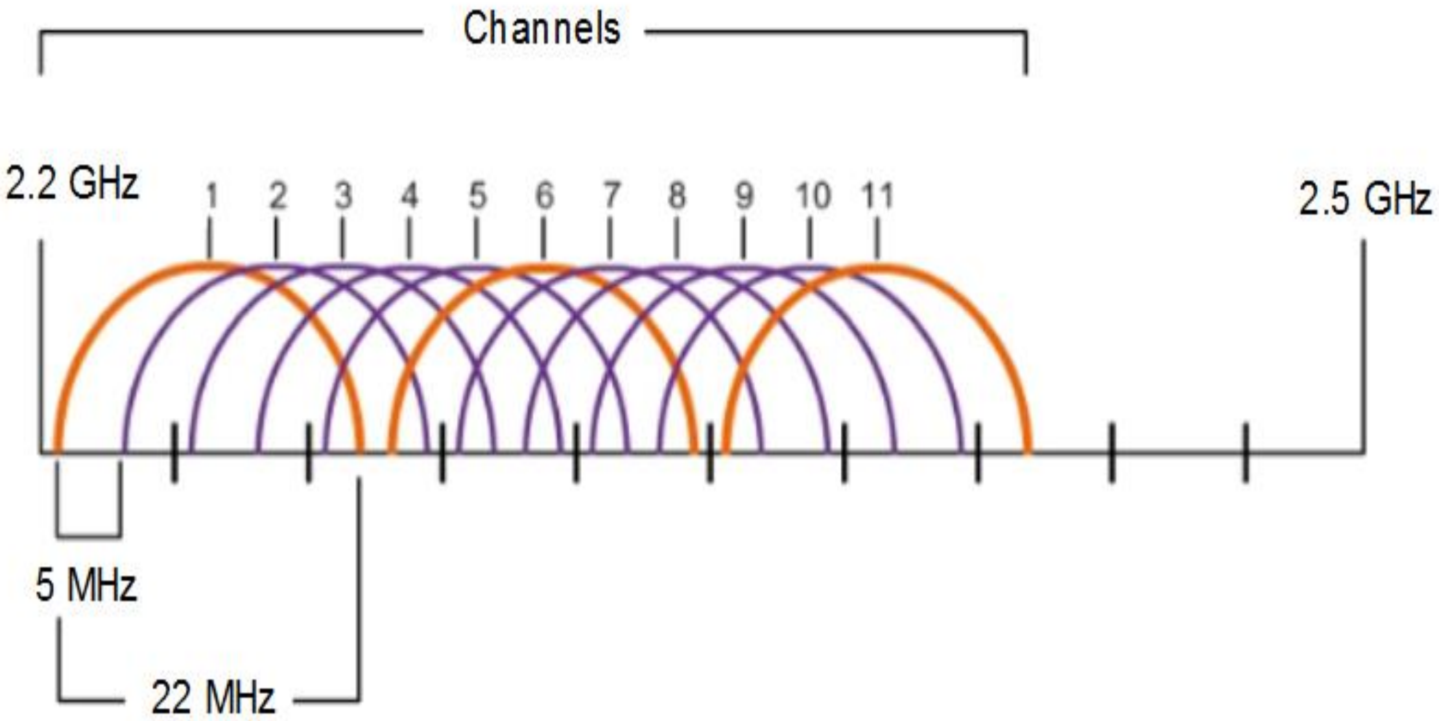
Channels in a WLAN

- Use of channels help to control conversations
  - allows multiple Access Points close to one another to function
  - each AP must be on different channel
- Each channel capable of carrying a different conversation



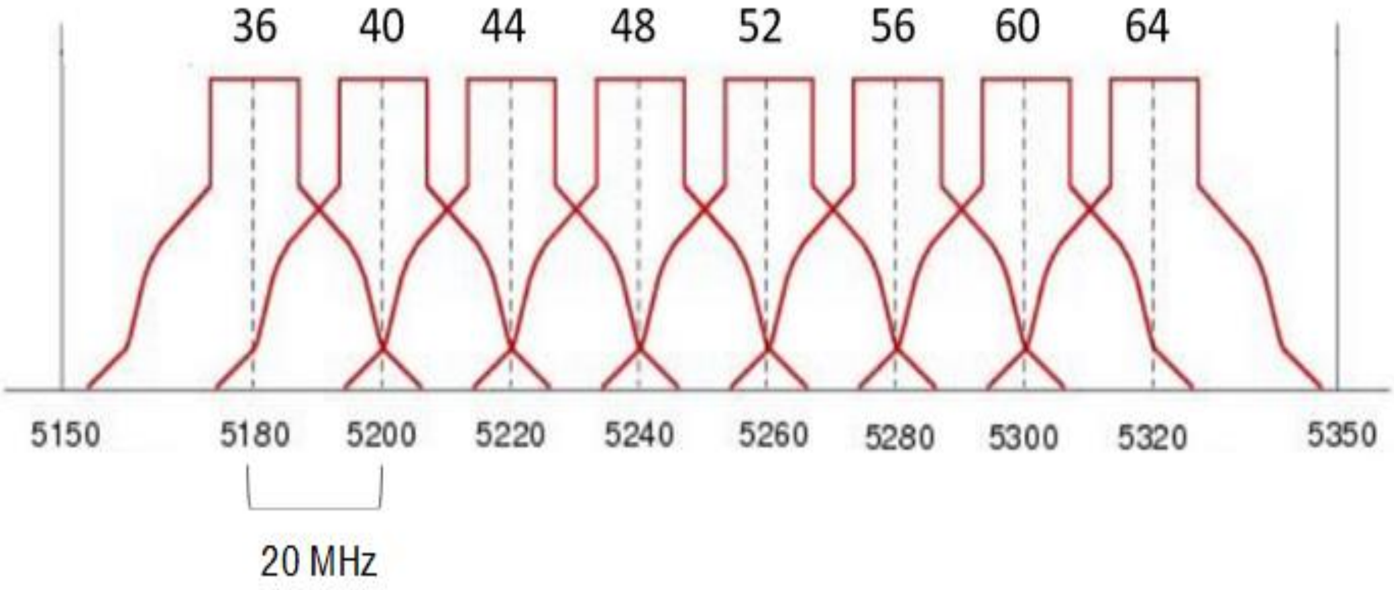
Channel Selection

- The 2.4 GHz band is subdivided into multiple channels each allotted 22 MHz bandwidth and separated from the next channel by 5 MHz.
- A best practice for 802.11b/g/n WLANs requiring multiple APs is to use non-overlapping channels such as 1, 6, and 11.



Channel Selection (Cont.)

- For the 5GHz standards 802.11a/n/ac, there are 24 channels. Each channel is separated from the next channel by 20 MHz.
- Non-overlapping channels are 36, 48, and 60.



802.11 Standards

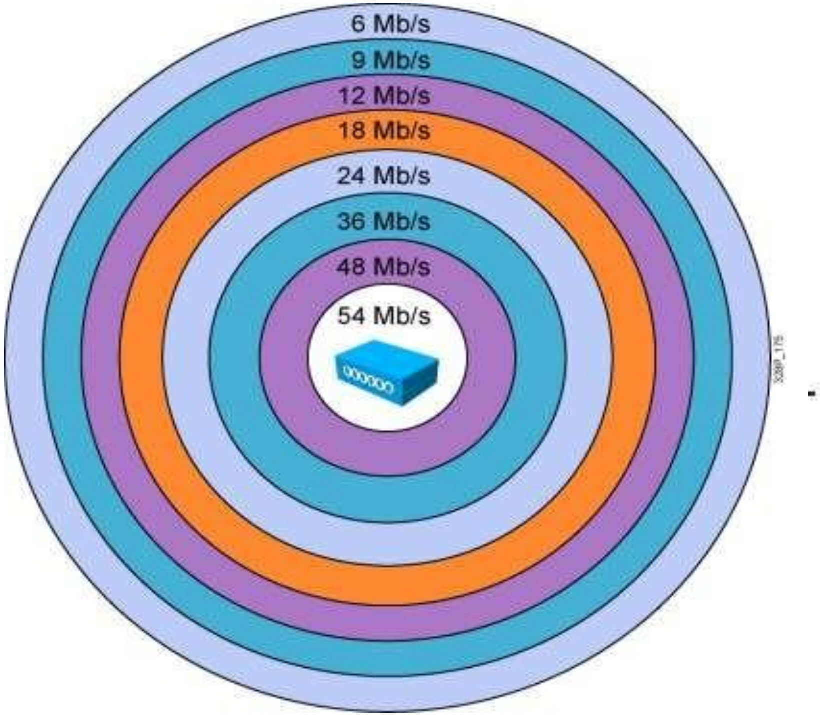
802.11 WLAN standards define how radio frequencies are used for wireless links.

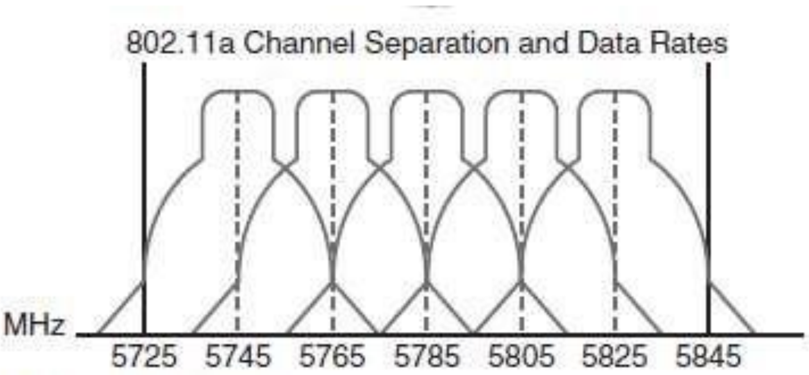
IEEE Standard	Radio Frequency	Description
802.11	2.4 GHz	Data rates up to 2 Mb/s
802.11a	5 GHz	Data rates up to 54 Mb/s Not interoperable with 802.11b or 802.11g
802.11b	2.4 GHz	Data rates up to 11 Mb/s Longer range than 802.11a and better able to penetrate building structures
802.11g	2.4 GHz	Data rates up to 54 Mb/s Backward compatible with 802.11b
802.11n	2.4 and 5 GHz	Data rates 150 – 600 Mb/s Require multiple antennas with MIMO technology
802.11ac	5 GHz	Data rates 450 Mb/s – 1.3 Gb/s Supports up to eight antennas
802.11ax	2.4 and 5 GHz	High-Efficiency Wireless (HEW) Capable of using 1 GHz and 7 GHz frequencies

continue...

802.11a Standard

- The 802.11a amendment was published in 1999.
- 802.11a uses OFDM only (6 Mbps to 54 Mbps).
- 802.11a offers up to 23 nonoverlapping channels.(36, 44, 52, 60)
- Operates in the 5-GHz band.



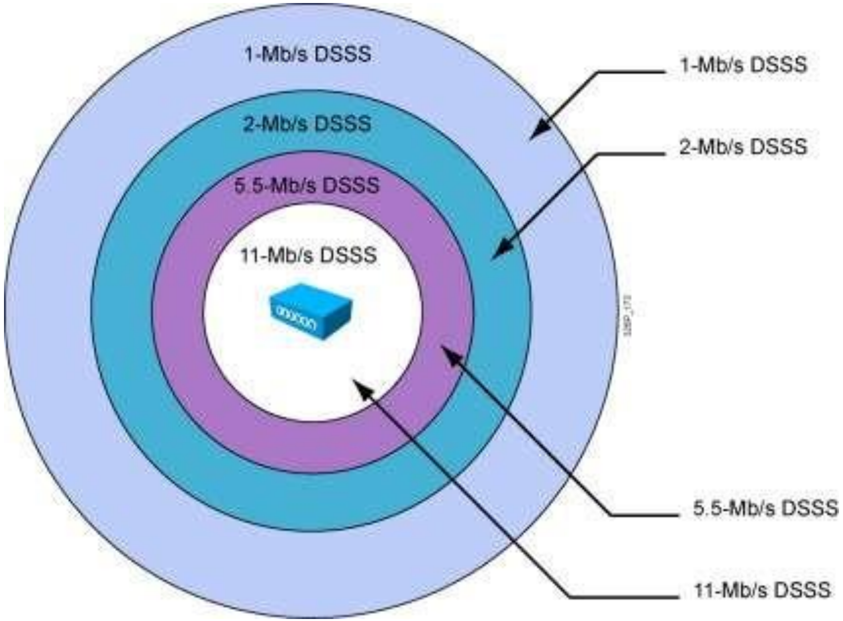


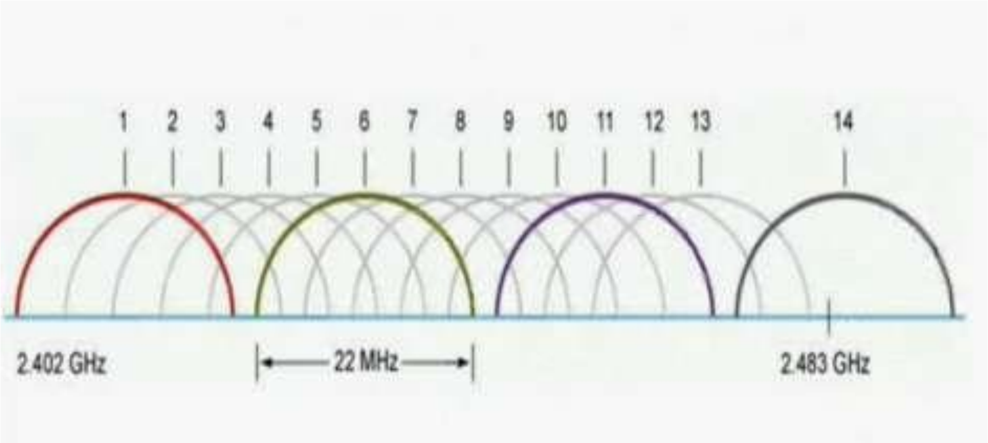
802.11a Channel List:
UNII-1: 36, 40, 44, 48
UNII-2: 52, 56, 60, 64
UNII-2e: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
UNII-3: 149, 153, 157, 161

continue...

802.11b Standard

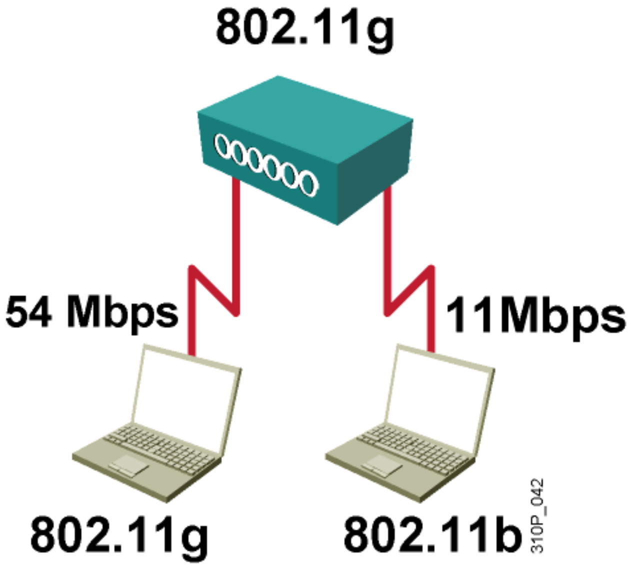
- The 802.11b was published in 1999 and modified almost as soon as it was created to allow for faster speeds.
- Data rate to 5.5 Mbps and 11 Mbps.
- There are 3 nonoverlapping channels: 1, 6, 11.
- Operates in the 2.4-GHz band.



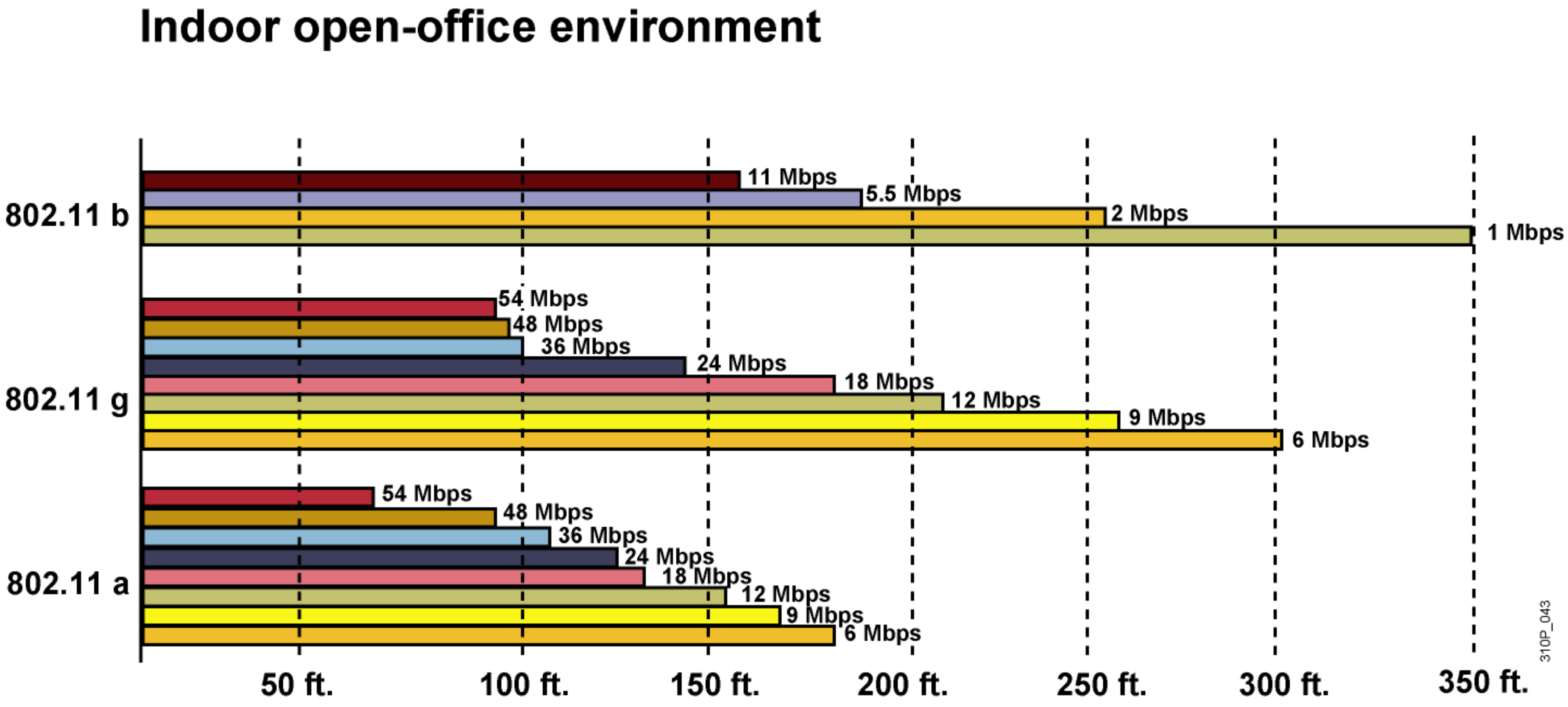


802.11g Standard

- Standard was ratified June 2003
- Operates in the 2.4-GHz band
- Same three nonoverlapping channels: 1, 6, 11
- 12 data rates of up to 54 Mbps
  - 1, 2, 5.5, 11 Mbps (DSSS / 802.11b)
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbps (OFDM)
- Full backward compatiblity to 802.11b standard but 802.11b stations cannot decode 802.11g radio signals.



Range Comparisons

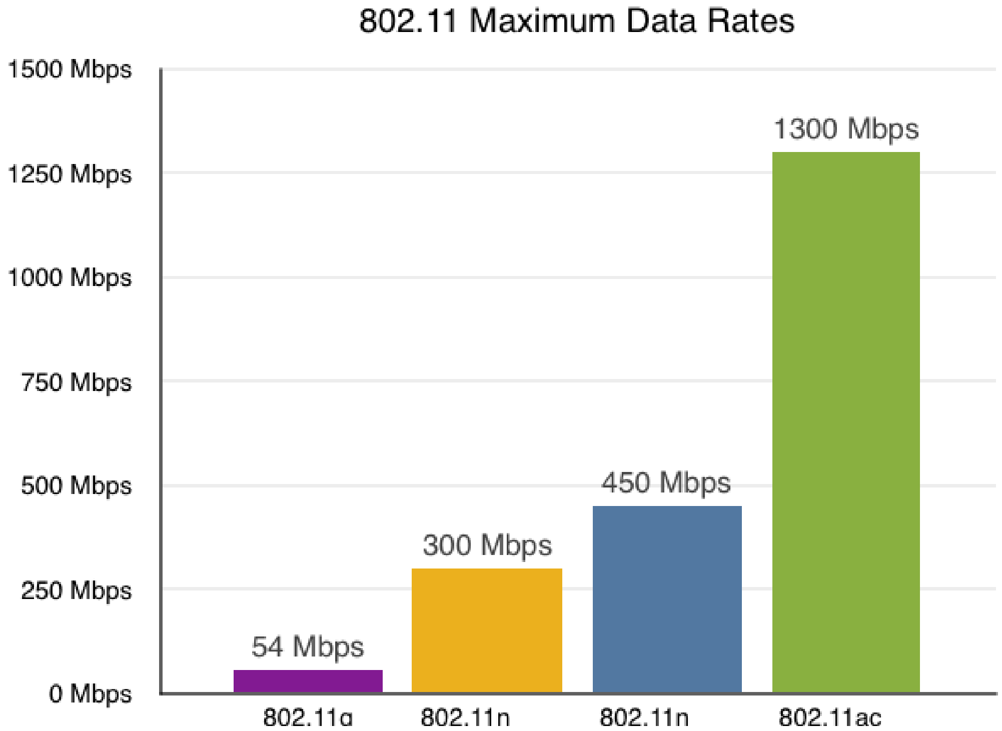


802.11n Standard

- The 802.11n was published in 2009
- Operates at the 2.4 GHz or less than 5GHz Bands. Great in 5GHz, not so good in 2.4 GHz
- 9 to 11 non-overlapping 40 MHz channels in 5GHz
- 1.5 non-overlapping channels in 2.4GHz
- Data rates from 54 Mbit/s to 450 Mbit/s

802.11ac Standard

- Release in December 2013
- It is an amendment to IEEE 802.11
- Operates at 5GHz band with Data rates up to 1300 Mbit/s



WLAN Components

Wireless NICs

•To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver.

•If a device does not have an integrated wireless NIC, then a USB wireless adapter can be used.

Wireless Home Router

•A home user typically interconnects wireless devices using a small, wireless router.

•Wireless routers serve as the following:

- –Access point – To provide wires access
- –Switch – To interconnect wired devices
- –Router - To provide a default gateway to other networks and the Internet

WLAN Components (Cont).

Wireless Access Point

•Wireless clients use their wireless NIC to discover nearby access points (APs).

•Clients then attempt to associate and authenticate with an AP.

•After being authenticated, wireless users have access to network resources.

Wireless Antennas

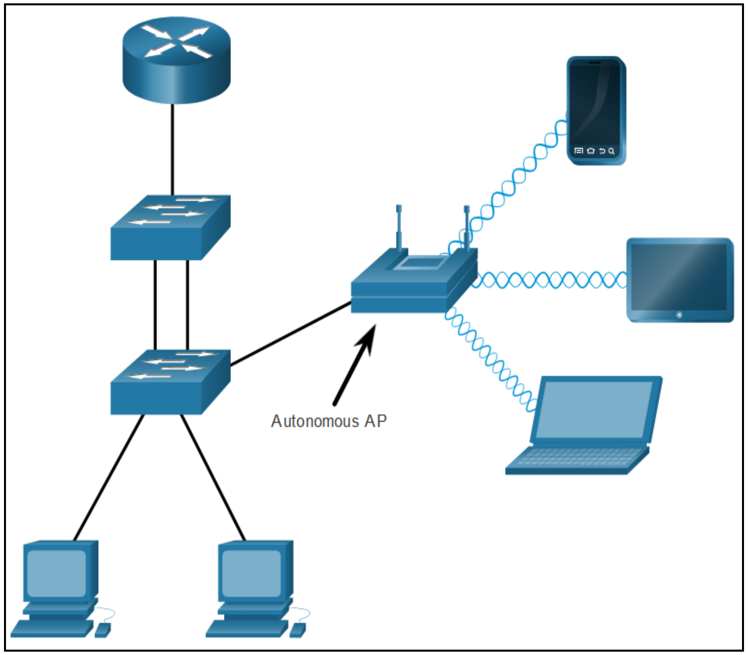
•Types of external antennas:

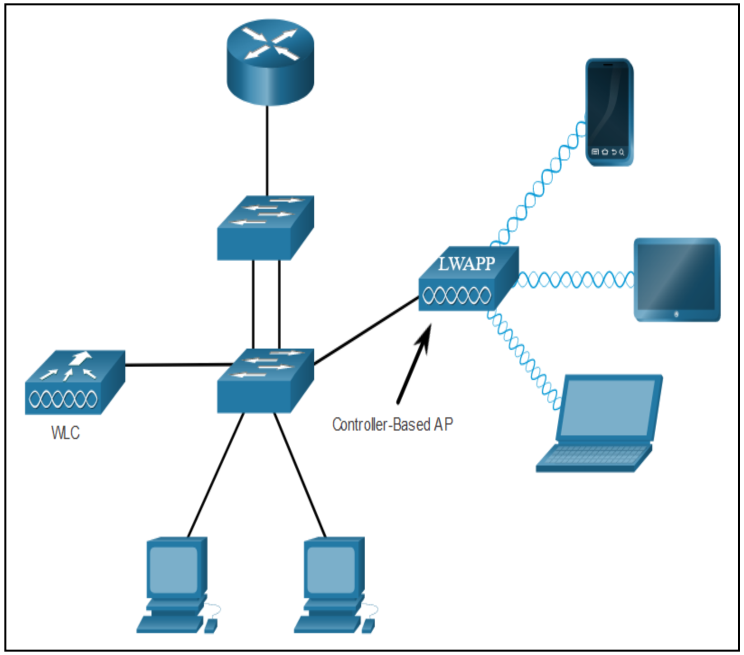
- Omnidirectional – Provide 360-degree coverage. Ideal in houses and office areas.
- Directional – Focus the radio signal in a specific direction. Examples are the Yagi and parabolic dish.
- Multiple Input Multiple Output (MIMO) – Uses multiple antennas (Up to eight) to increase bandwidth.

AP Categories

APs can be categorized as either autonomous APs or controller-based APs.

- **Autonomous APs** – Standalone devices configured through a command line interface or GUI. Each autonomous AP acts independently of the others and is configured and managed manually by an administrator.
- **Controller-based APs** – Also known as lightweight APs (LAPs). Use Lightweight Access Point Protocol (LWAPP) to communicate with a LWAN controller (WLC). Each LAP is automatically configured and managed by the

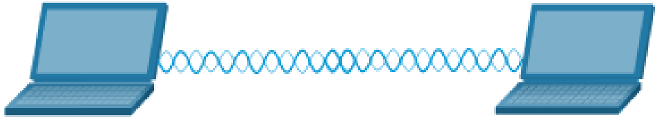




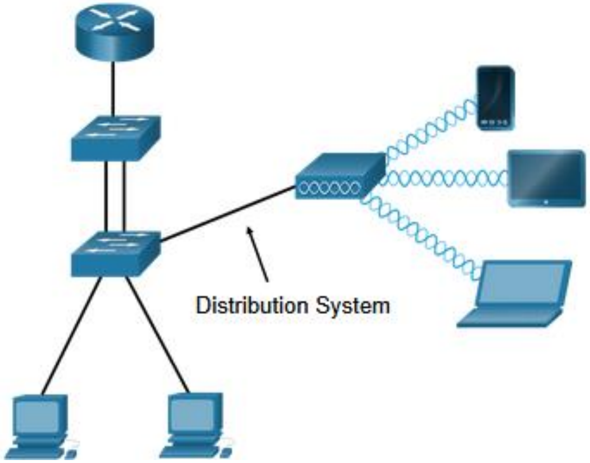
WLAN Operation

Wireless Topology Modes

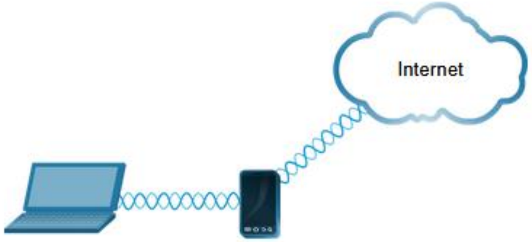
Ad hoc mode - Used to connect clients in peer-to-peer manner without an AP.



Infrastructure mode - Used to connect clients to the network using an AP.



Tethering - Variation of the ad hoc topology is when a smart phone or tablet with cellular data access is enabled to create a personal hotspot.



BSS and ESS

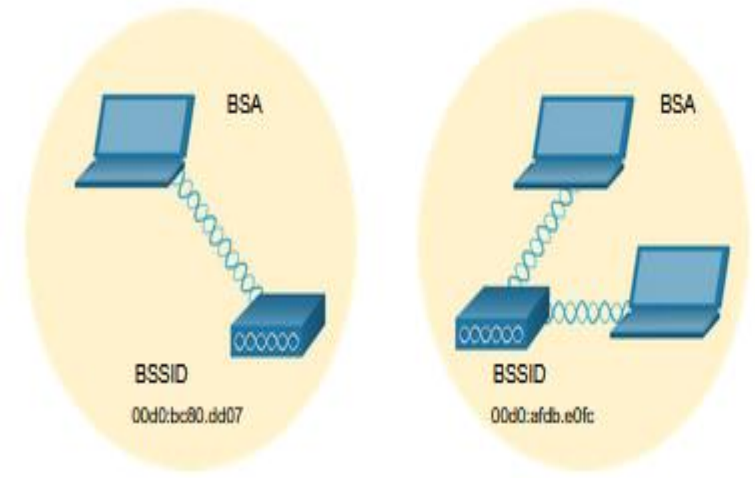
Infrastructure mode defines two topology blocks:

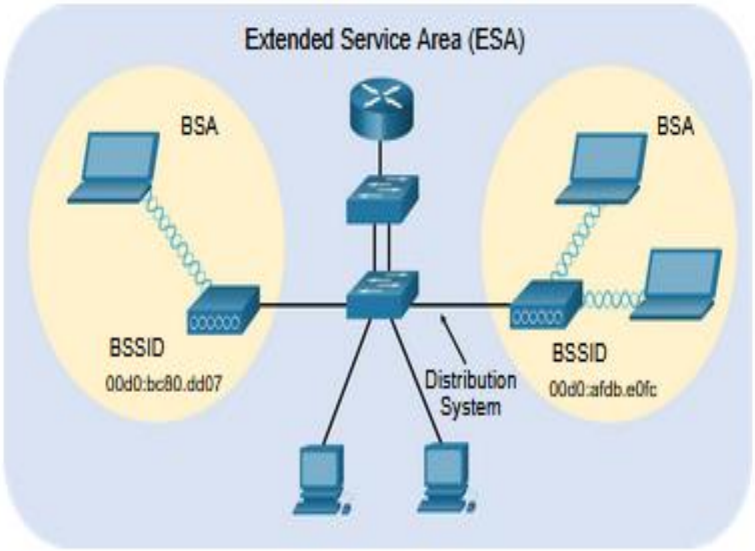
Basic Service Set (**BSS**)

- Uses single AP to interconnect all associated wireless clients.
- Clients in different BSSs cannot communicate.

Extended Service Set (**ESS**)

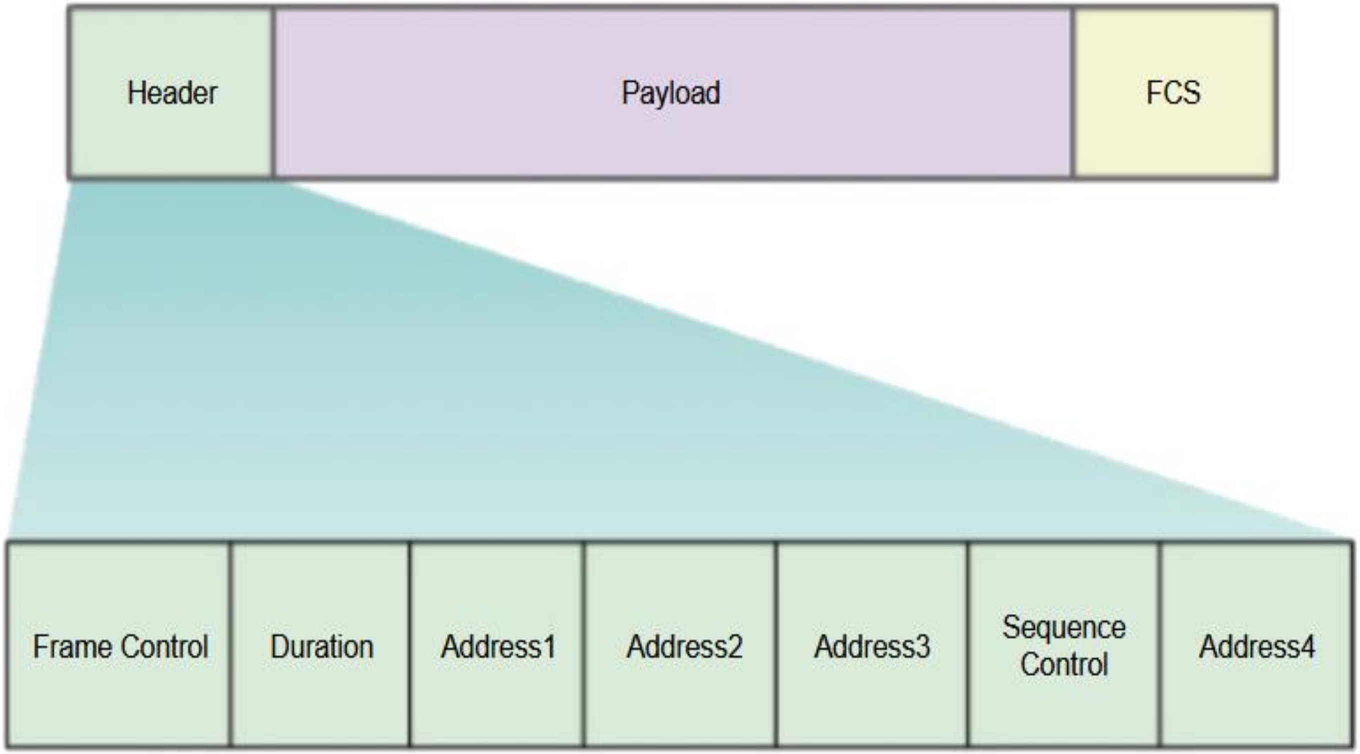
- A union of two or more BSSs interconnected by a wired distribution system.
- Clients in each BSS can communication through the ESS.





802.11 Frame Structure

The 802.11 frame format is similar to the Ethernet frame format, except that it contains more fields.



CSMA/CA

WLANs are half-duplex and a client cannot “hear” while it is sending, making it impossible to detect a collision.

WLANs use carrier sense multiple access with collision avoidance (**CSMA/CA**) to determine how and when to send data. A wireless client does the following:

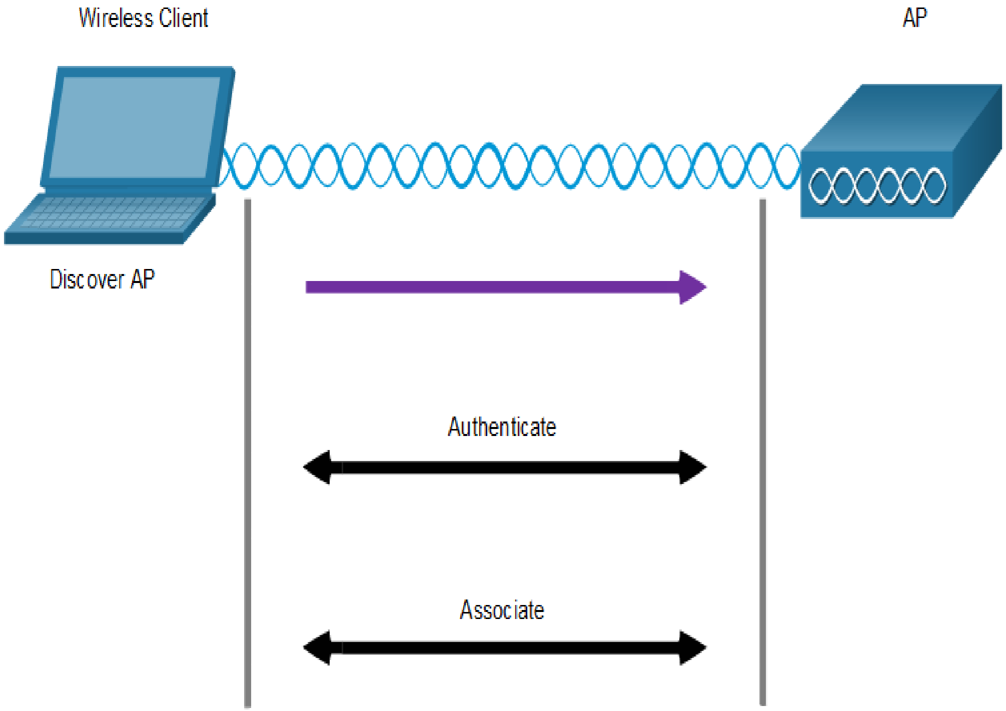
1. Listens to the channel to see if it is idle, i.e. no other traffic currently on the channel.
2. Sends a ready to send (**RTS**) message the AP to request dedicated access to the network.
3. Receives a clear to send (**CTS**) message from the AP granting access to send.
4. Waits a random amount of time before restarting the process if no CTS message received.
5. Transmits the data.
6. Acknowledges all transmissions. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process

Wireless Client and AP Association

For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

Wireless devices complete the following three stage process:

- Discover a wireless AP
- Authenticate with the AP
- Associate with the AP



Wireless Client and AP Association (Cont.)

To achieve successful association, a wireless client and an AP must agree on specific parameters:

- **SSID** – The client needs to know the name of the network to connect.
- **Password** – This is required for the client to authenticate to the AP.
- **Network mode** – The 802.11 standard in use.
- **Security mode** – The security parameter settings, i.e. WEP, WPA, or WPA2.
- **Channel settings** – The frequency bands in use.

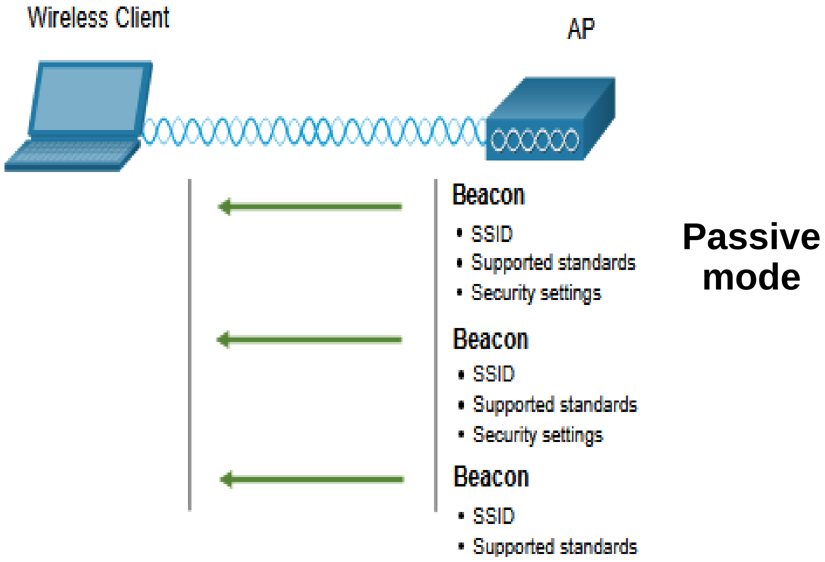
Purpose of SSID

- Allows wireless components to connect to the WLAN
  - tells wireless devices which WLAN they belong to
  - tells devices whom then can talk to
- All wireless devices must have same SSID to communicate with each other
- Characteristics
  - case sensitive
  - alphanumeric characters
  - sent in the header of the frame

Passive and Active Discover Mode

Wireless clients connect to the AP using a passive or active scanning (probing) process.

- Passive mode – AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings.
- Active mode – Wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels.



Wireless Client

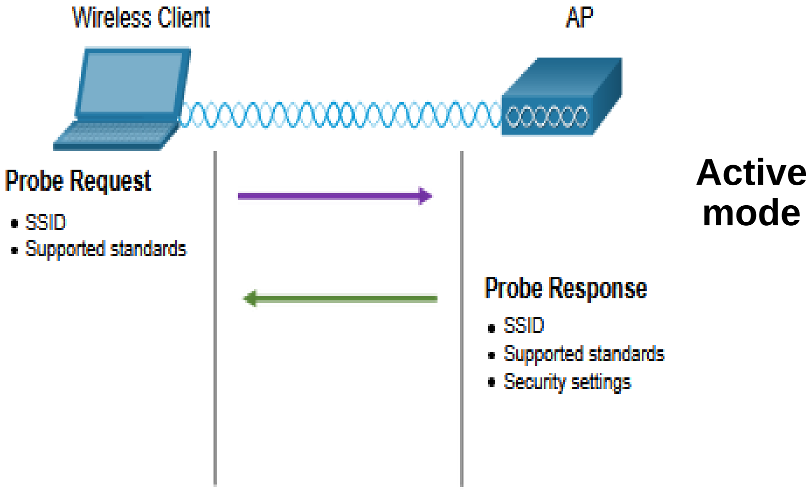
AP

Beacon
- SSID
- Supported standards
- Security settings

Beacon
- SSID
- Supported standards
- Security settings

Beacon
- SSID
- Supported standards

Passive mode



Wireless Client

AP

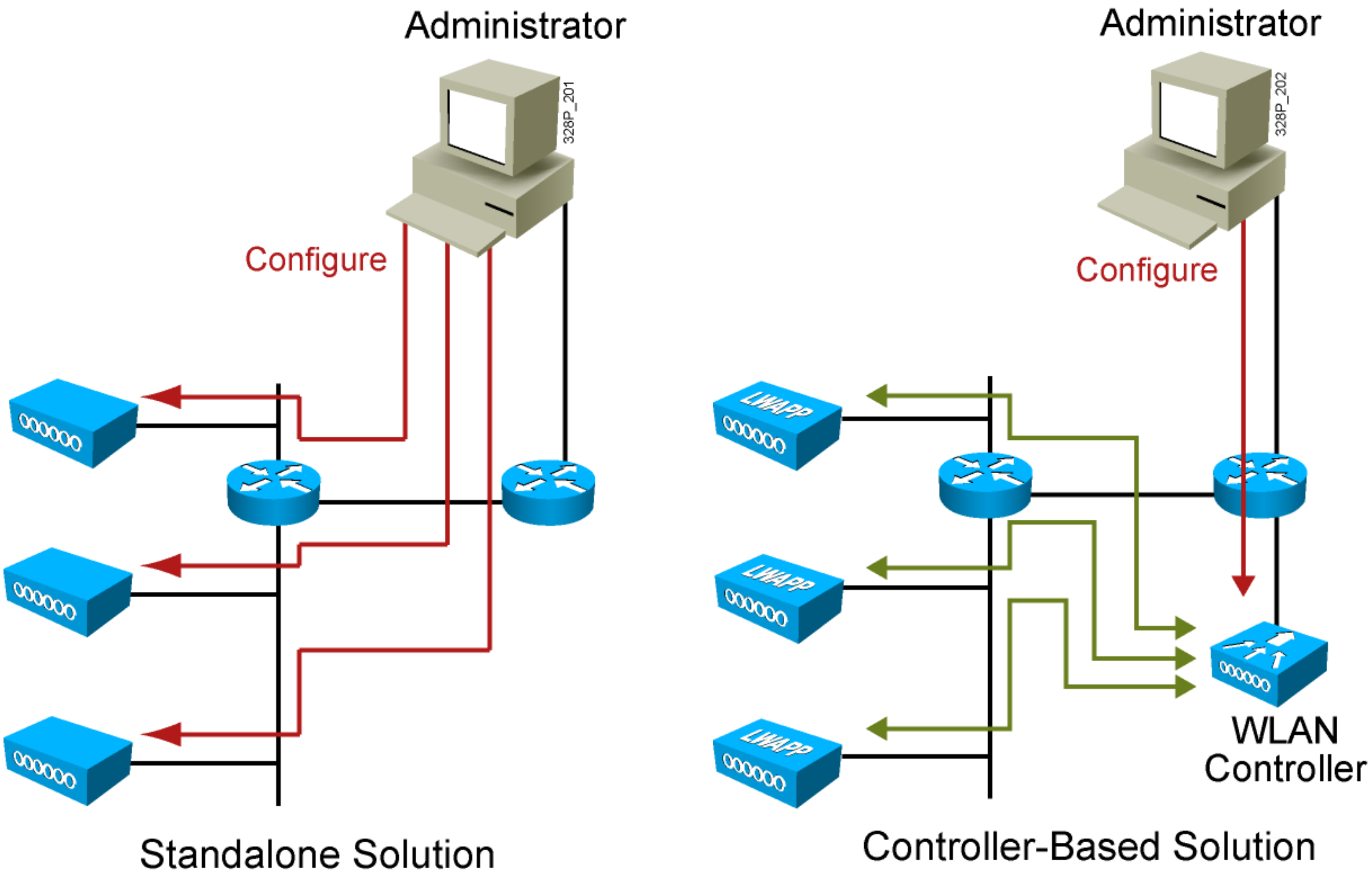
Probe Request
- SSID
- Supported standards

Probe Response
- SSID
- Supported standards
- Security settings

Active mode

Wireless Network Basic Architecture

Standalone and Lighweight AP



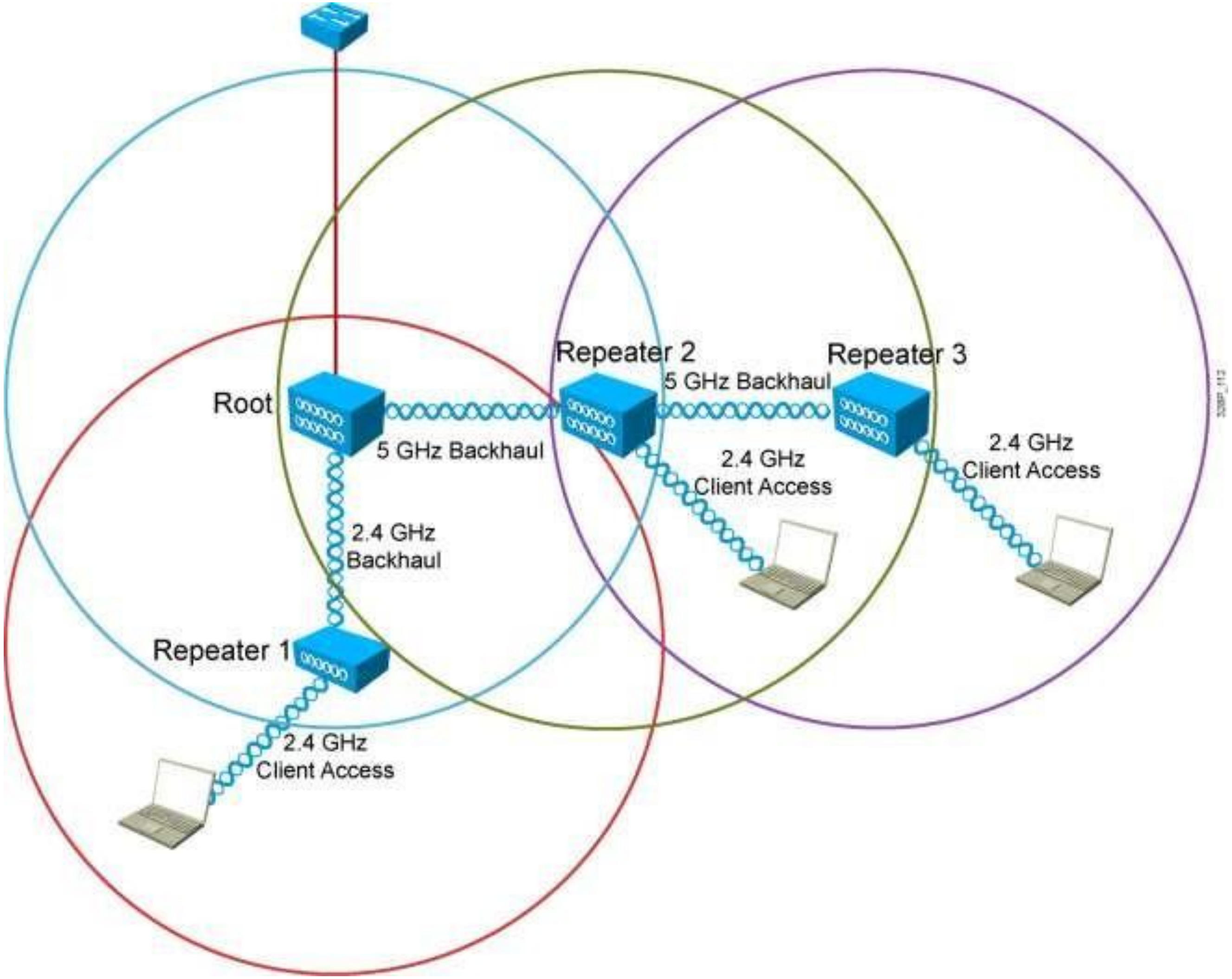
Repeater

Extends the AP coverage

Dual radio can create dual half-duplex

Overlap of 50% required

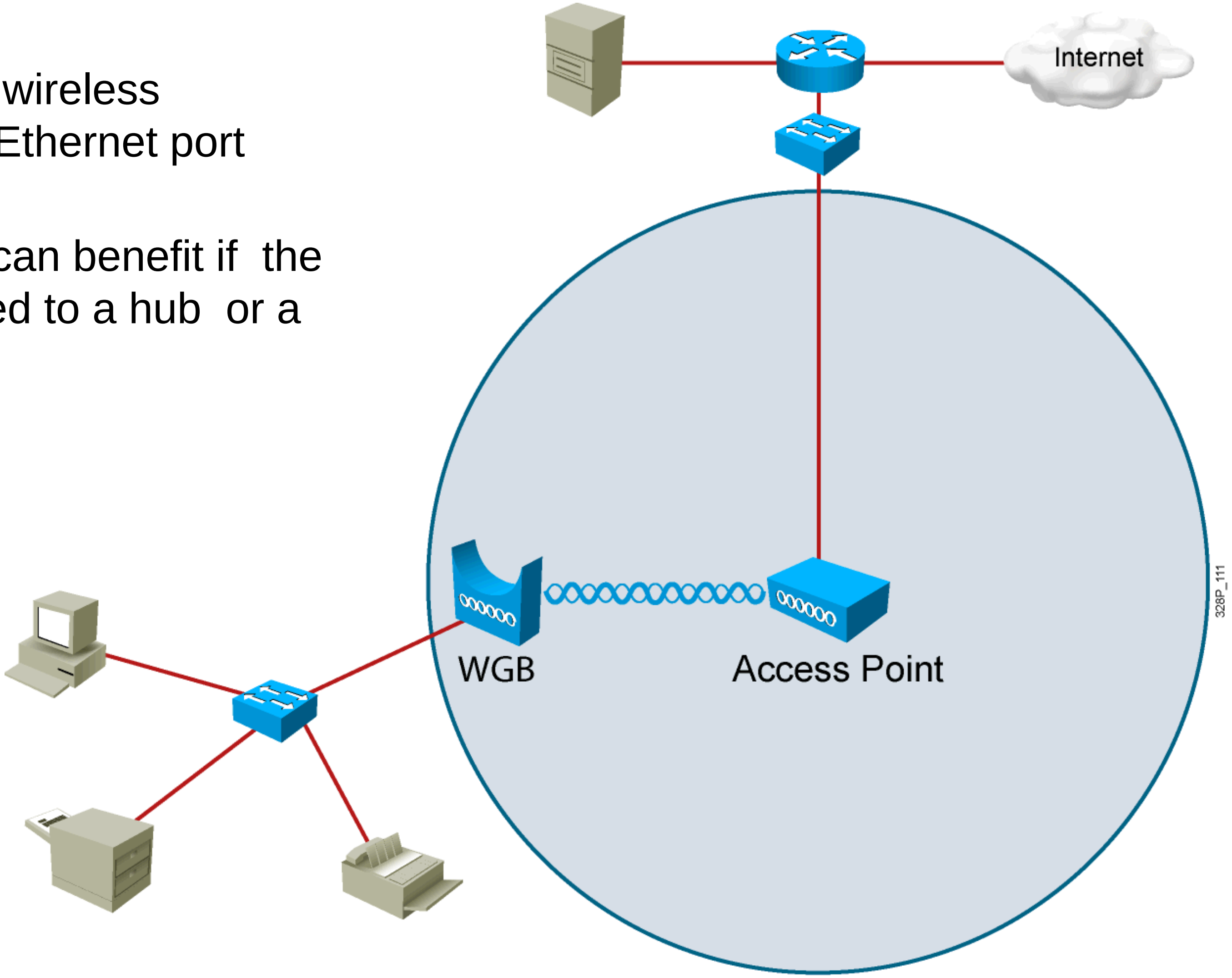
Throughput impacted when single frequency used



Workgroup Bridge

A WGB provides wireless connection from Ethernet port

Several devices can benefit if the WGB is connected to a hub or a switch.

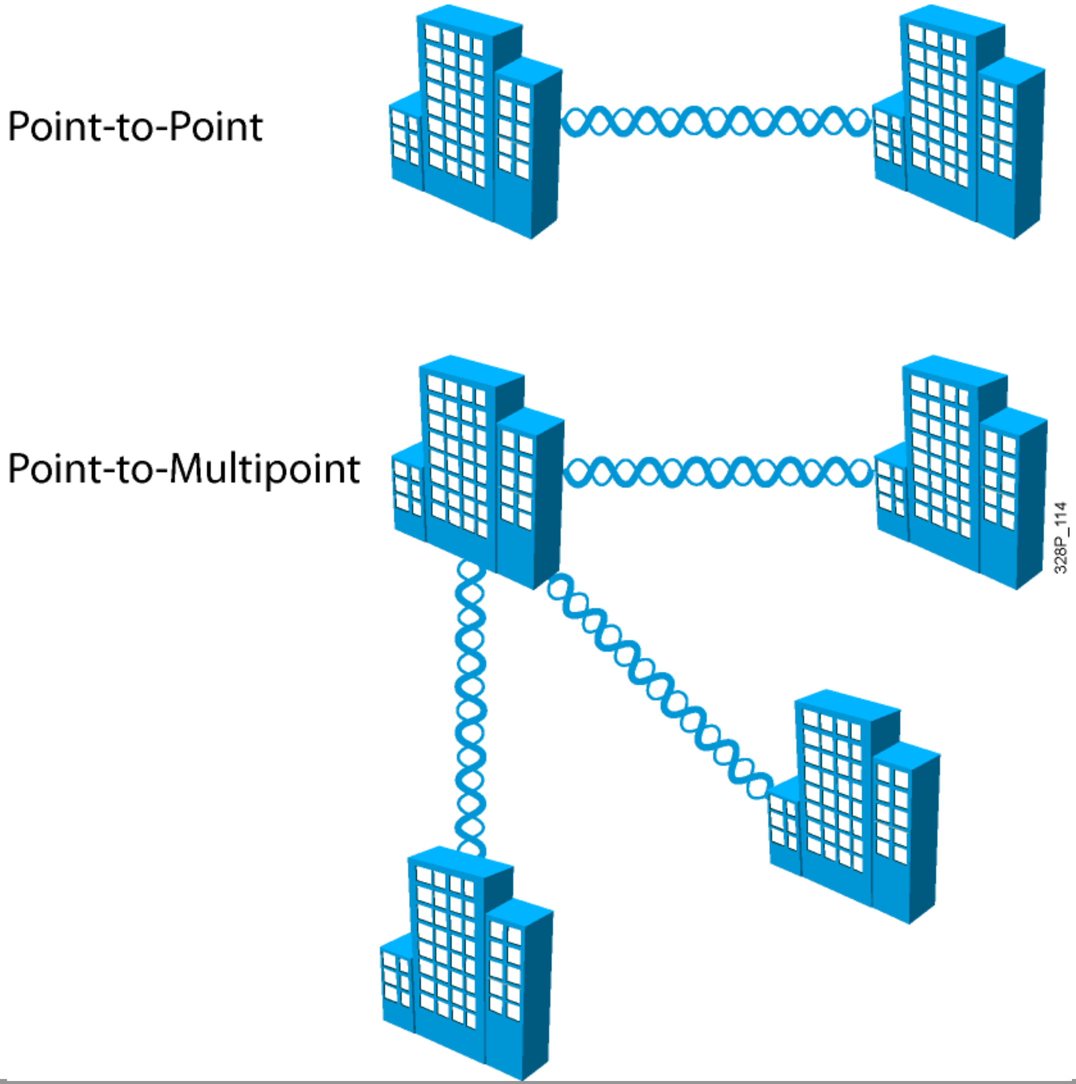


Outdoor Wireless Bridge

Extend the LAN by linking LANs

Usually a few miles Range

Point to point or hub and spoke



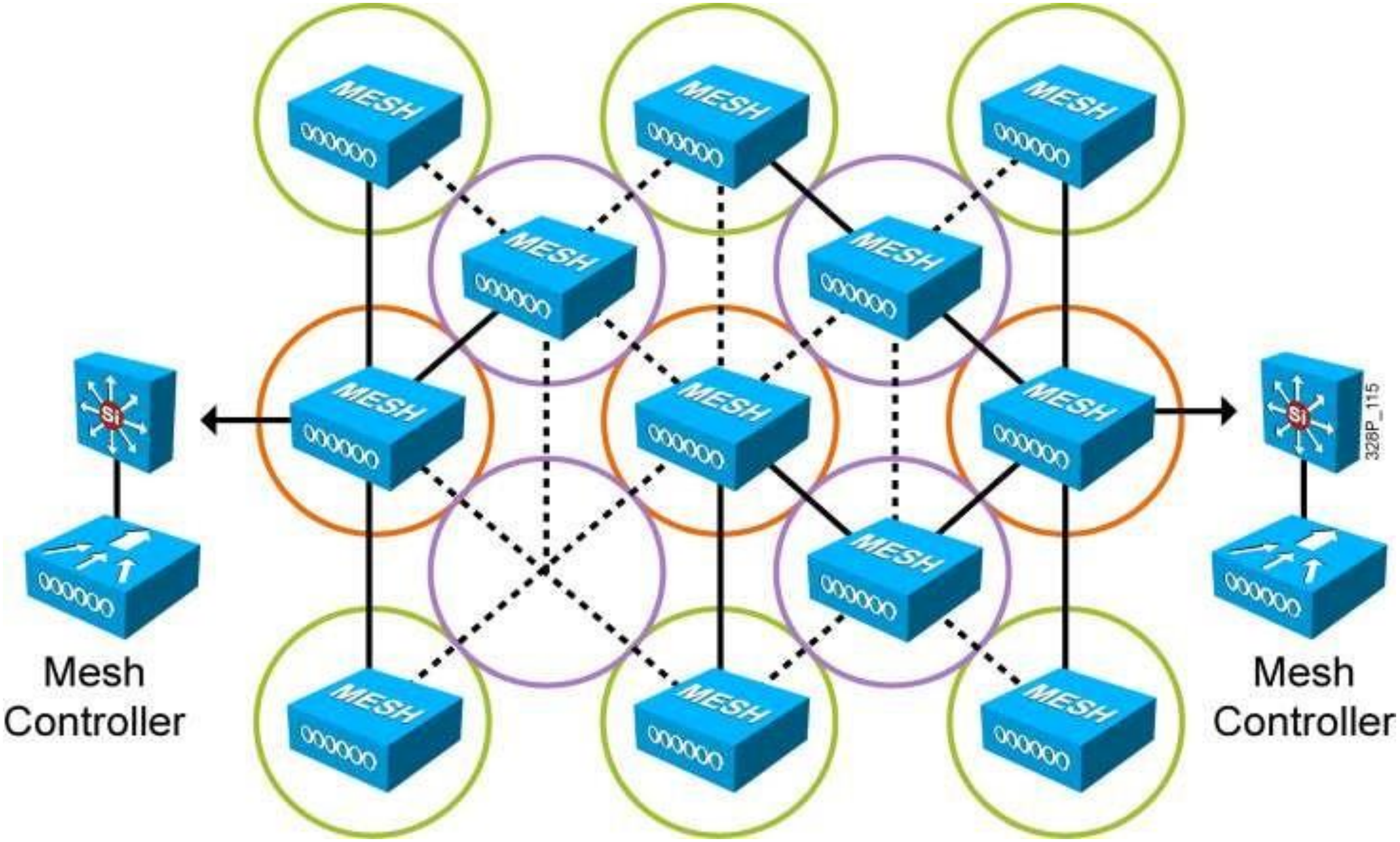
Point-to-Point

Point-to-Multipoint

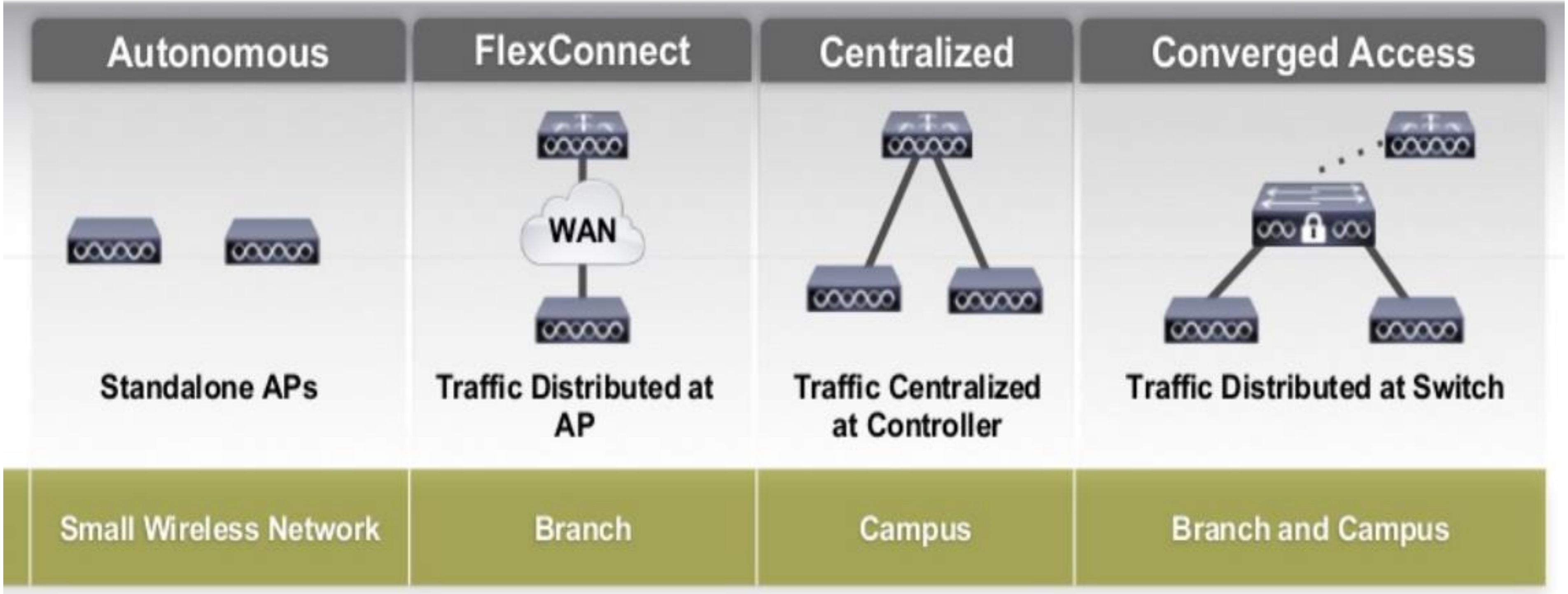
Mesh Networks

Devices are connected with redundant connection between nodes

No single point of failure



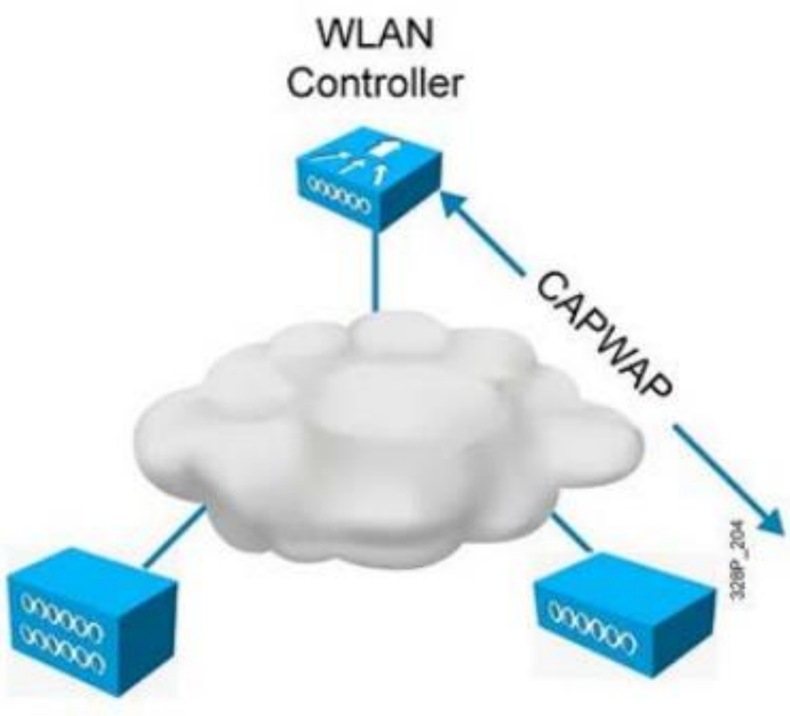
Wireless Architectures



Autonomous	FlexConnect	Centralized	Converged Access
Standalone APs	Traffic Distributed at AP	Traffic Centralized at Controller	Traffic Distributed at Switch
Small Wireless Network	Branch	Campus	Branch and Campus

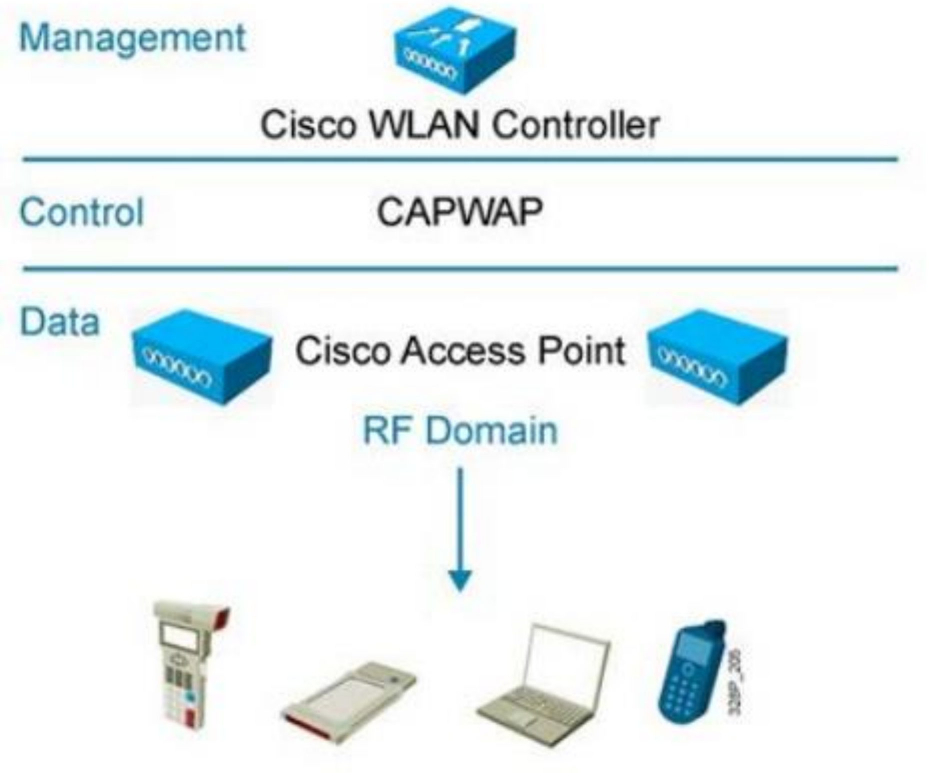
Cisco Split MAC Design

- Cisco WLAN Controller
  - Security policies
  - QoS policies
  - RF managemenr
  - Mobility management
- Cisco controller-based access point
  - Remote RF interface
  - Encryption downstream
  - Decryption upstream



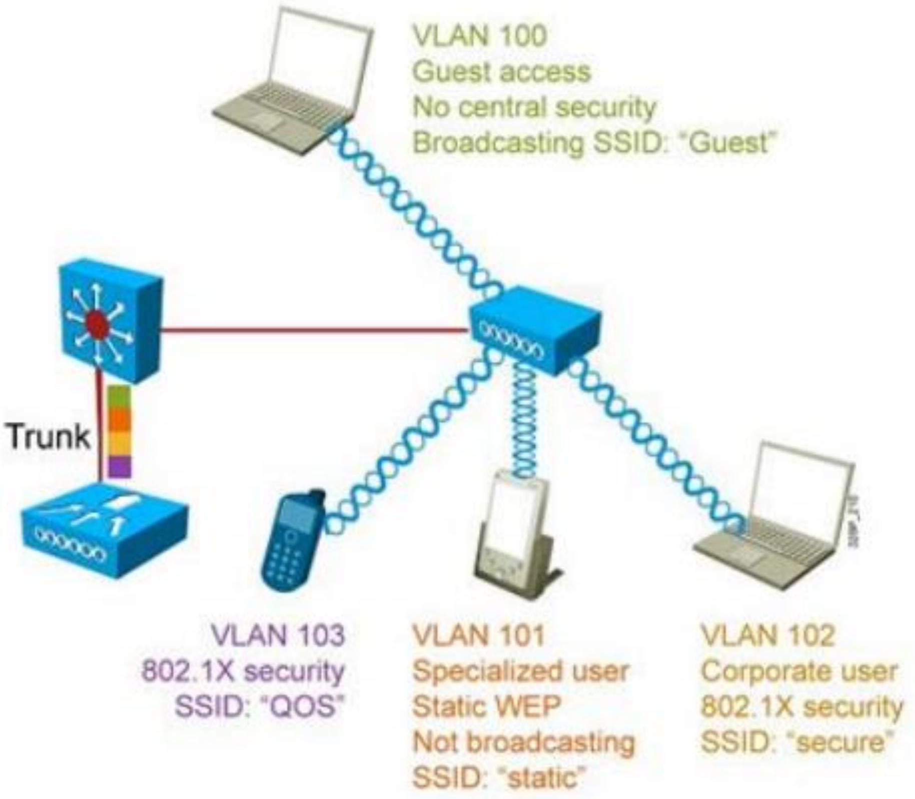
Dynamic RF management

- Channel assignment
- Transmit power adjustment
- Interference avoidance
- Coverage hole management
- Load balancing
- Capacity management



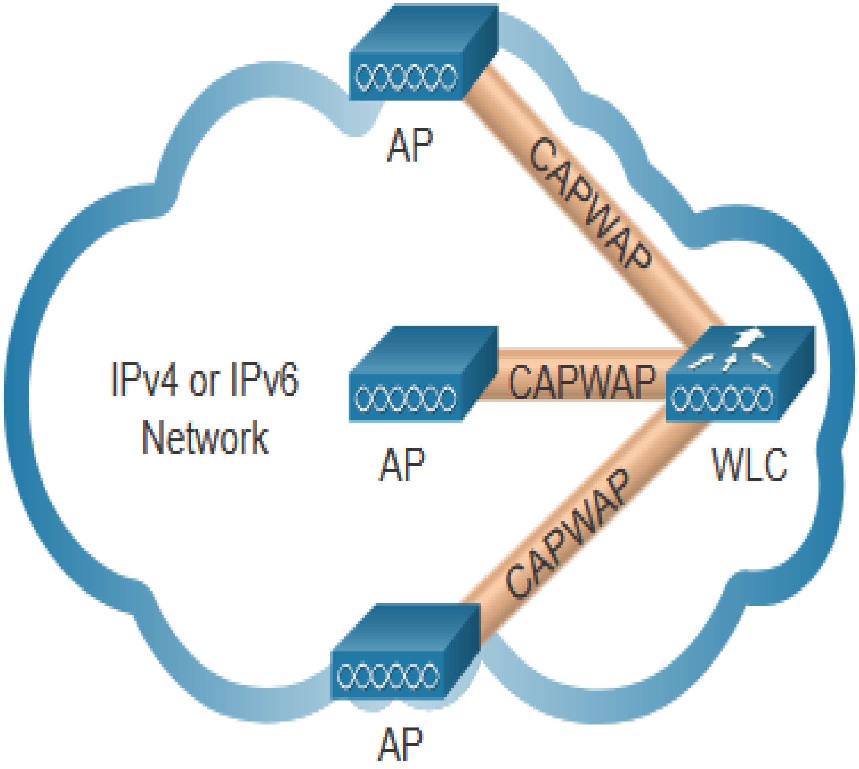
Wireless Virtual LAN Support

- Multiple SSIDs
- Multiple security types
- Supports multiple VLANs from switches
- IEEE 802.1Q Trunking protocol



Introduction to CAPWAP

- CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs.
- Based on LWAPP but adds additional security with Datagram Transport Layer Security (DLTS).
- Encapsulates and forwards WLAN client traffic between an AP and a WLC over tunnels using UDP ports 5246 and 5247.
- Operates over both IPv4 and IPv6. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.



Split MAC Architecture

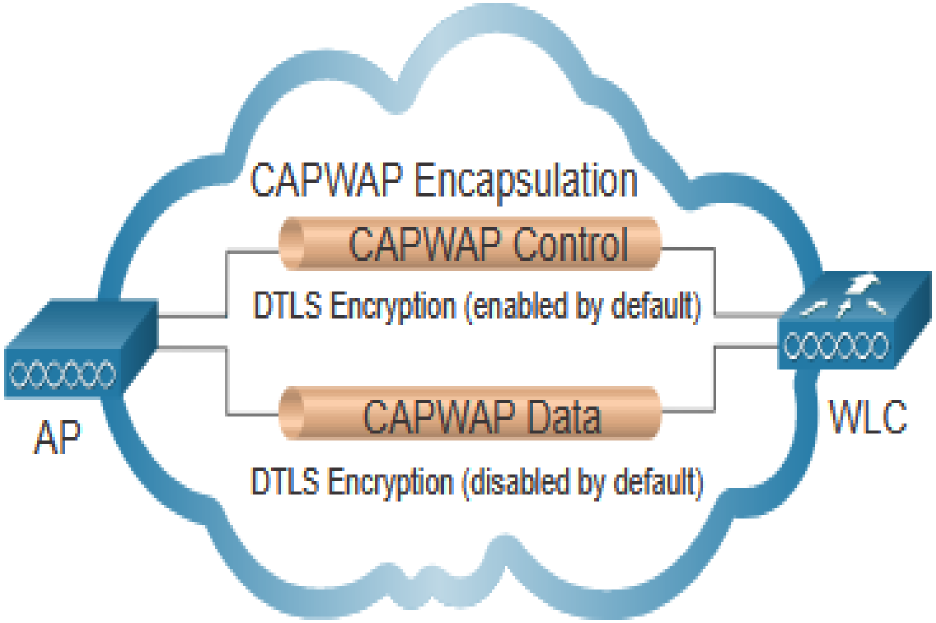
The CAPWAP split MAC concept does all the functions normally performed by individual APs and distributes them between two functional components:

- AP MAC Functions
- WLC MAC Functions

AP MAC Functions	WLC MAC Functions
Beacons and probe responses	Authentication
Packet acknowledgements and retransmissions	Association and re-association of roaming clients
Frame queueing and packet prioritization	Frame translation to other protocols
MAC layer data encryption and decryption	Termination of 802.11 traffic on a wired interface

DTLS Encryption

- DTLS provides security between the AP and the WLC.
- It is enabled by default to secure the CAPWAP control channel and encryp all management and control traffic between AP and WLC.
- Data encryption is disabled by default and requires a DTLS license to be installed on the WLC before it can be enabled on the AP.

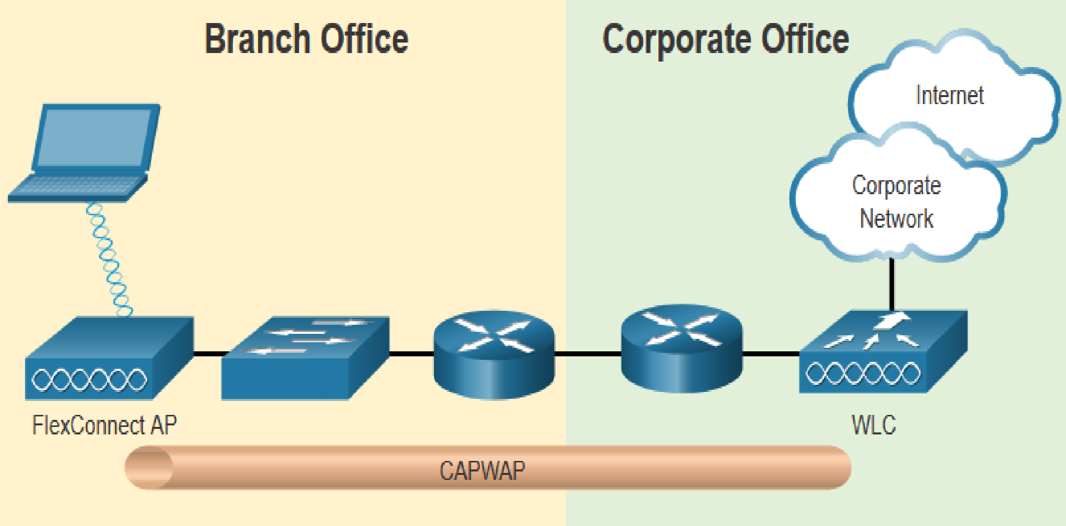

CAPWAP Encapsulation
CAPWAP Control
DTLS Encryption (enabled by default)
CAPWAP Data
DTLS Encryption (disabled by default)
AP
WLC

Flex Connect APs

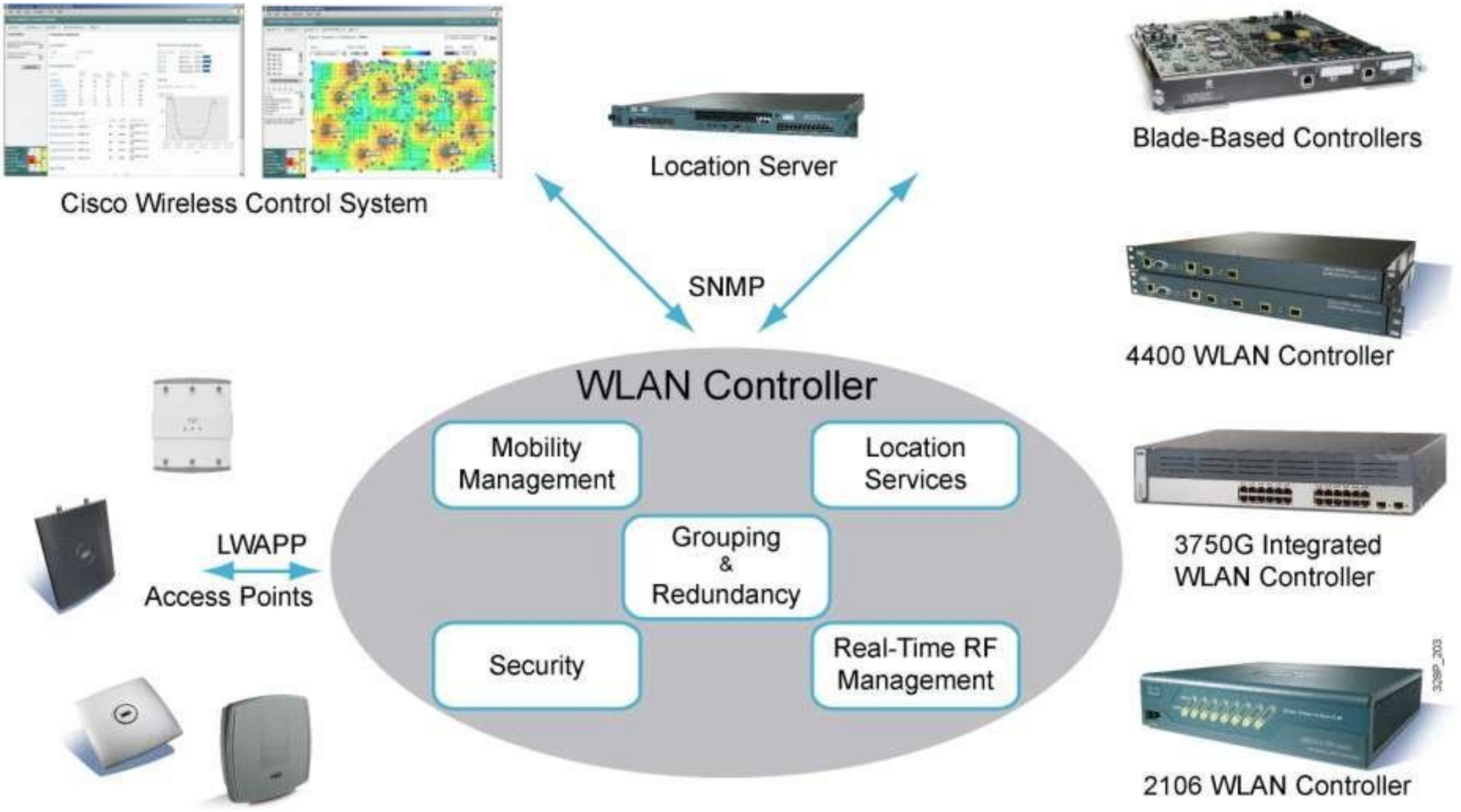
FlexConnect enables the configuration and control of Aps over a WAN link.

There are two modes of option for the FlexConnect AP:

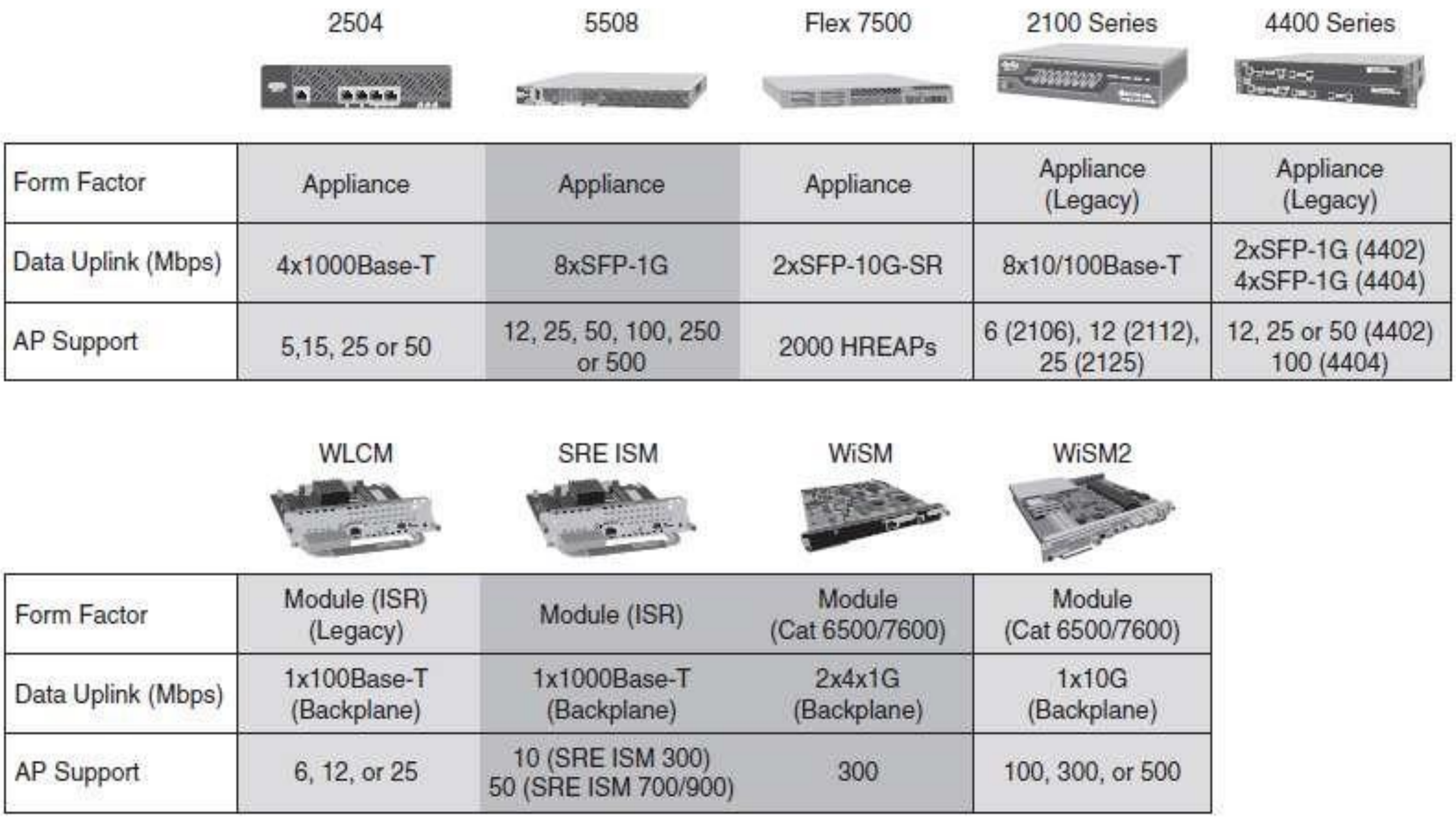
- **Connected mode** – The WLC is reachable. The FlexConnect AP has CAPWAP connectivity with the WLC through the CAPWAP tunnel. The WLC performs all CAPWAP functions.
- **Standalone mode** – The WLC is unreachable. The FlexConnect AP has lost CAPWAP connectivity with the WLC. The FlexConnect AP can assume some of the WLC functions such as switching client data traffic locally and performing client authentication locally.



Controller-based Solution



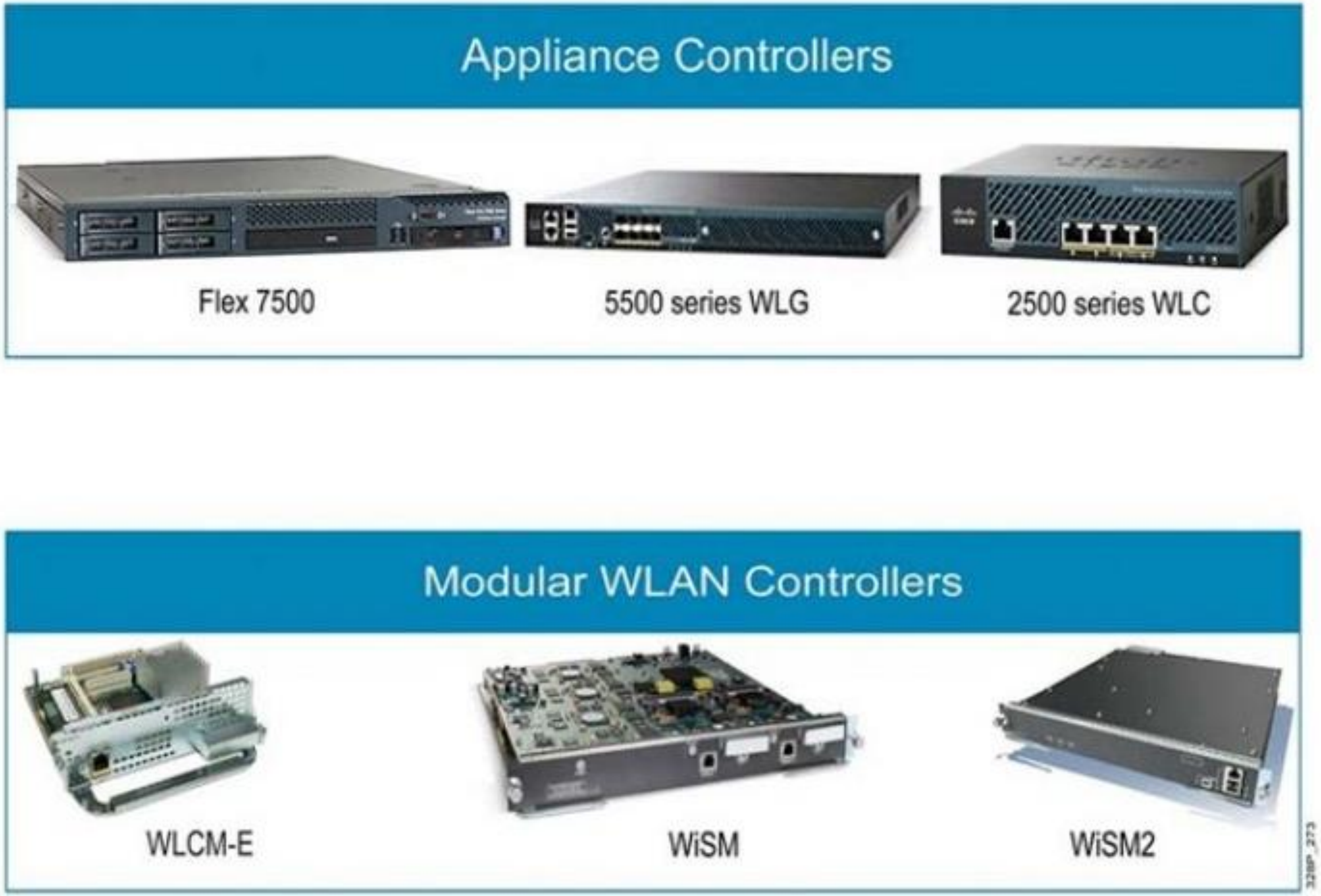
Controller Models



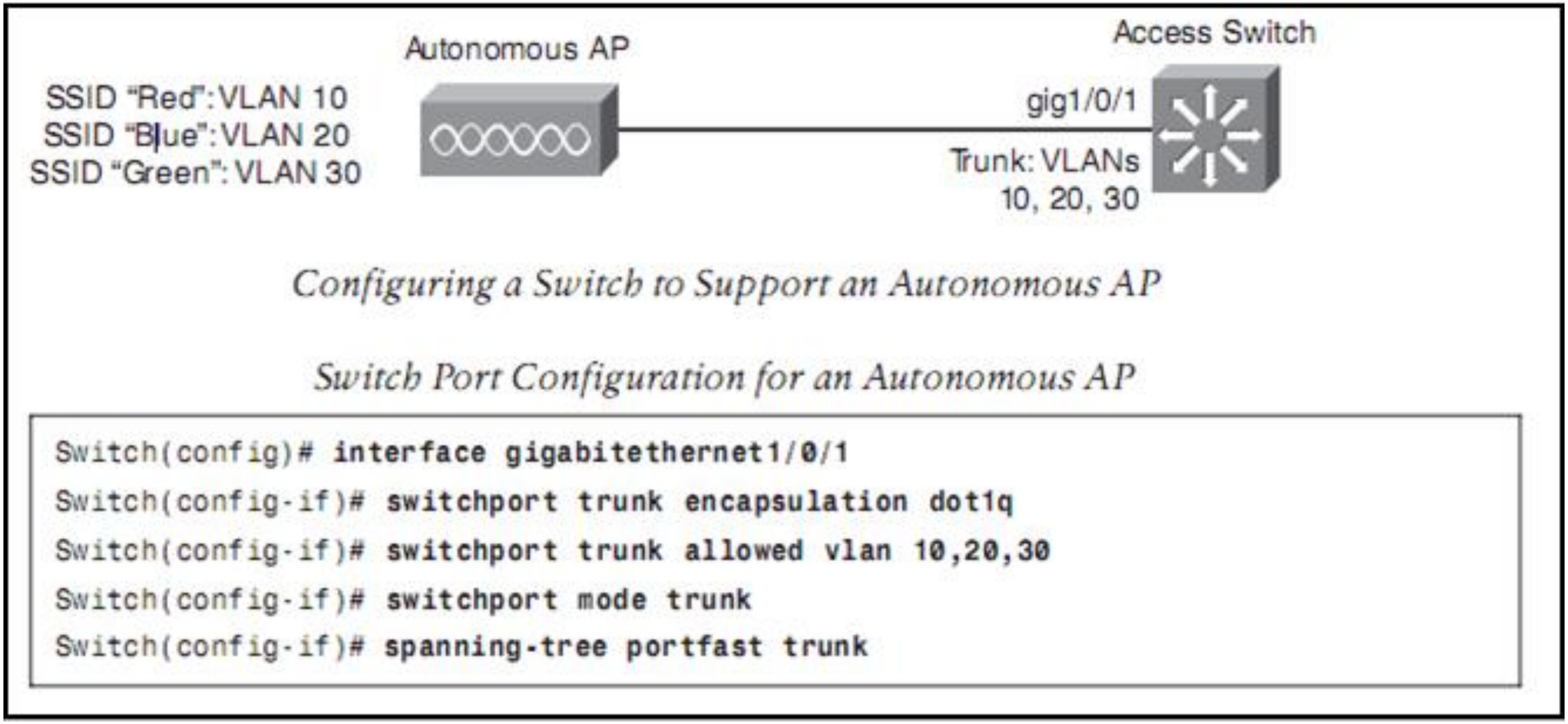
	2504	5508	Flex 7500	2100 Series	4400 Series
Form Factor	Appliance	Appliance	Appliance	Appliance (Legacy)	Appliance (Legacy)
Data Uplink (Mbps)	4x1000Base-T	8xSFP-1G	2xSFP-10G-SR	8x10/100Base-T	2xSFP-1G (4402) 4xSFP-1G (4404)
AP Support	5,15, 25 or 50	12, 25, 50, 100, 250 or 500	2000 HREAPs	6 (2106), 12 (2112), 25 (2125)	12, 25 or 50 (4402) 100 (4404)

	WLCM	SRE ISM	WiSM	WiSM2
Form Factor	Module (ISR) (Legacy)	Module (ISR)	Module (Cat 6500/7600)	Module (Cat 6500/7600)
Data Uplink (Mbps)	1x100Base-T (Backplane)	1x1000Base-T (Backplane)	2x4x1G (Backplane)	1x10G (Backplane)
AP Support	6, 12, or 25	10 (SRE ISM 300) 50 (SRE ISM 700/900)	300	100, 300, or 500

Controller Models



Configuring Switch Ports for Autonomous AP

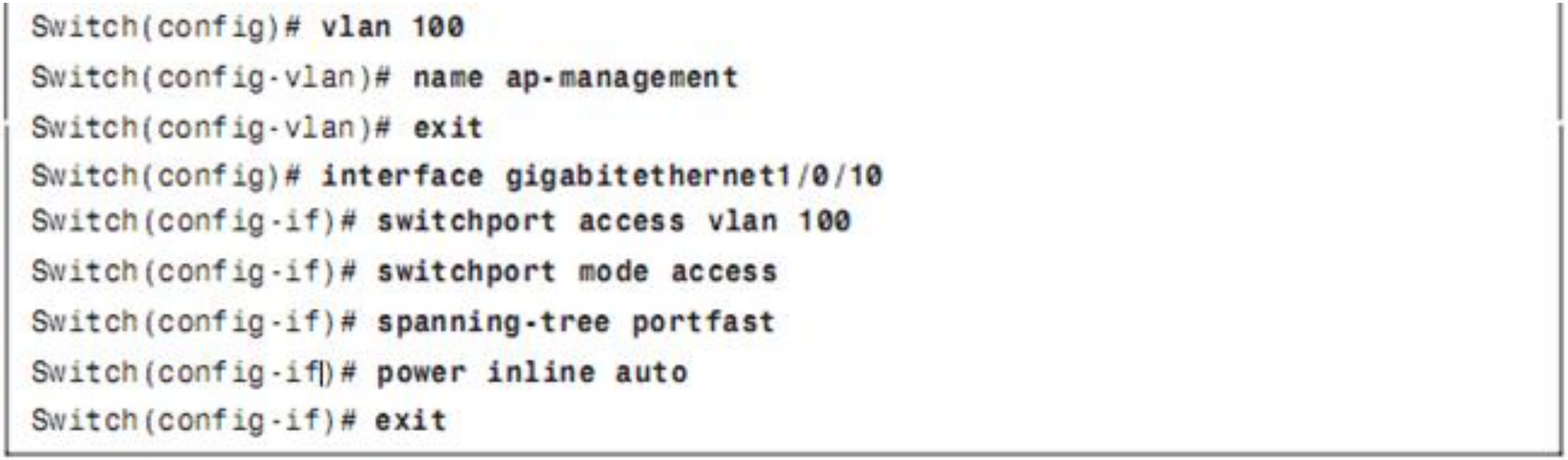


Configuring a Switch to Support an Autonomous AP

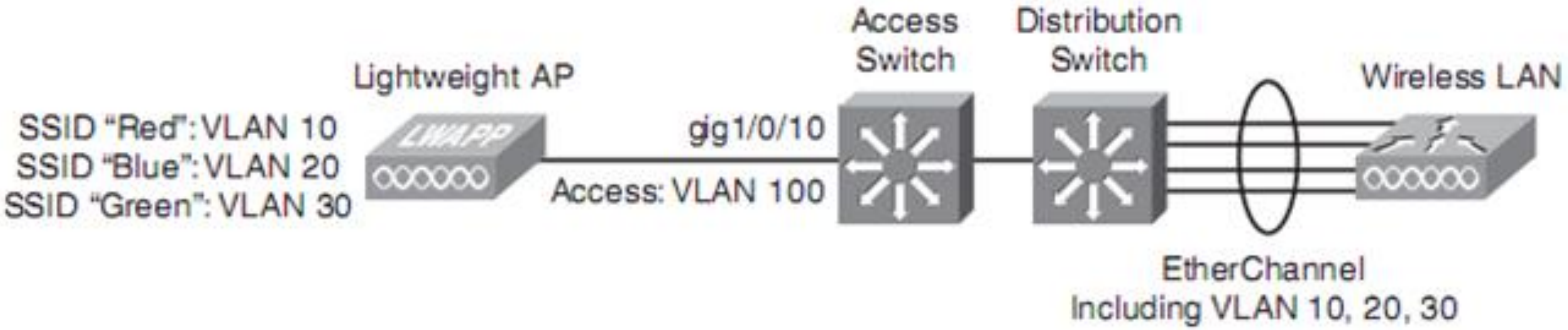
Switch Port Configuration for an Autonomous AP

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)# switchport mode trunk
Switch(config-if)# spanning-tree portfast trunk
```

Configuring Switch Ports for Lightweight AP



```
Switch(config)# vlan 100
Switch(config-vlan)# name ap-management
Switch(config-vlan)# exit
Switch(config)# interface gigabitethernet1/0/10
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport mode access
Switch(config-if)# spanning-tree portfast
Switch(config-if|)# power inline auto
Switch(config-if)# exit
```



CISCO