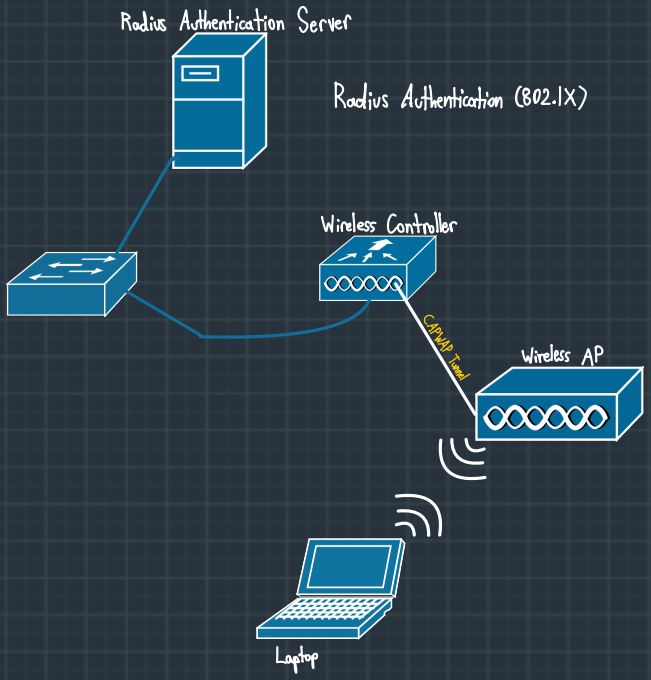
Wireless Notes:

Note: Page I copied from CBTNuggets Notes

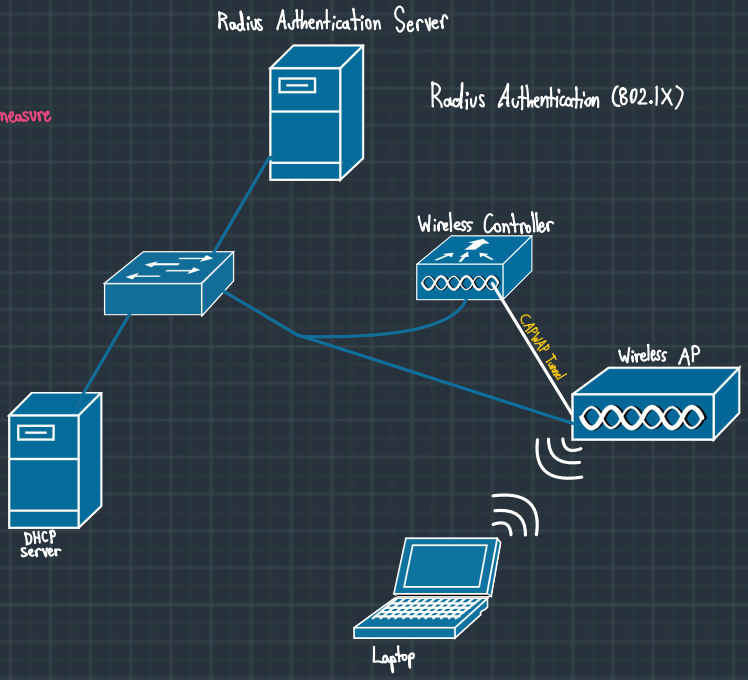
Cisco Wireless LAN Controller:

- Autonomous Wireless Access Point (WAP): Standalone access point that does not need a controller to function, they have their own configuration interfaces
- Lightweight WAP: Designed to be controlled by a controller, essentially a robot that needs commands passed to it to function
  - A configuration set on the controller autopopulates the configuration to the lightweight WAPs it controls
- CAPWAP Tunnel: The communication tunnel between the WAP and the controller that it sends its data to
- WAPs have a split MAC design where the controller handles the MAC addresses of the devices on the network instead of the AP itself
  - This is because with a centralized location, the MAC addresses of devices can be synonomously logged and authorized on multiple WAPs at once; as a user roams across the network and connects to different WAPs over one session, their connection will not be dropped and reestablished
- Interfaces: Can be configured as management/service ports or distribution (LAG) ports



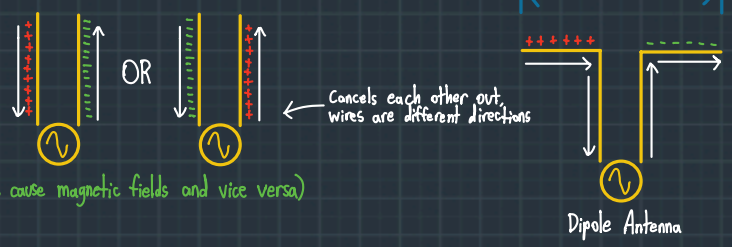
Wireless Security:

- WiFi Security options include:
  - Disabled/None/Open: Open network, anyone can connect can also use a vpn as a futher security measure
  - WEP: Broken security via small key space
  - WPA: Broken security
  - WPA2: Better than WPA
  - WPA3: Better than WPA2, and backwards compatible
- Personal: Uses preshared keys for authentication
- Enterprise: Uses a centralized AAA server for authentication (Radius/Kerberos)
- WPA2 PSK (password) used primarily in SOHO environments
- Autonomous AP: Access points off a switch
- Wireless Controllers: Overviewed above
- Implement Wifi devices with a PSK on Packet Tracer

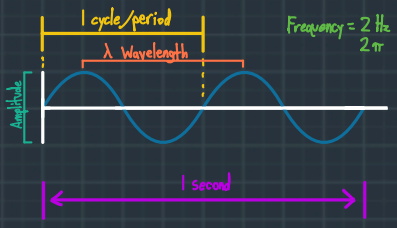


Wireless Networking Deep Dive:
Wireless LAN Design Options:
- Ad Hoc: Wireless device to wireless device without any infrastructure or APs present
- Infrastructure Wireless LAN: An AP running to a switch to provide internet to the rest of the world
- Mesh Wireless LAN: Uses a mesh of WAPs to regenerate signal and coverage around an area

Wireless Communication Theory:
- Electromagnetic Spectrum: There is a tight relationship between electricity and magnetism, electricity creates magnetism and magnetism creates electricity
- When radio waves are sent, an electric field is broadcast vertically and the magnetic field is orthogonal to that
  - Orthogonal: At right angles to (phase shifted 90°)
  - Transverse Wave: The electromagnetic radiation produced by a radio wave from an antenna
- Antenna Theory: How can an electromagnetic wave be transferred outside an antenna
  - A device generates positive and negative charges on 2 pieces of wire
  - Dipole Antenna: A type of antenna used to radiates EM waves
  - λ: Wavelength

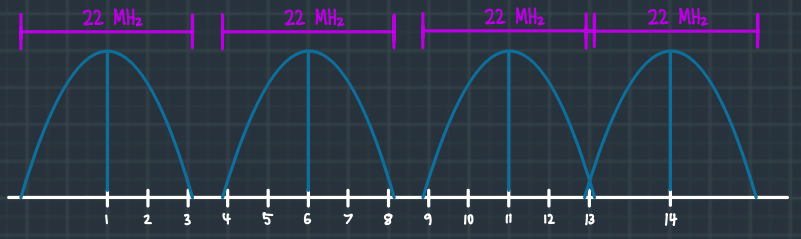


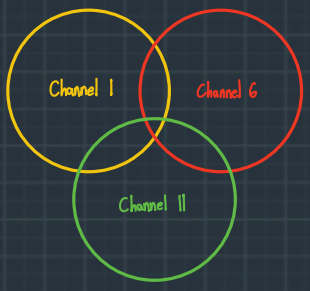
- Maxwells Equations: Governs light and radio waves on the electromagnetic spectrum (how electric fields cause magnetic fields and vice versa)
  - $\nabla \times D = \rho$
  - $\nabla \times B = 0$
  - $\nabla \times E = -\frac{\partial B}{\partial t}$
  - $\nabla \times H = J + \frac{\partial D}{\partial t}$
- Wireless Communication Theory Terms:
  - Frequency: The # of complete cycles per second (measured in Hertz)
  - Cycle: One complete sinθ wave
  - Hertz: The measurement of cycles per second (the measurement of the frequency)
  - Radio Frequency Range: Official Range within 3 kilohertz and 300 Gigahertz
    - Wireless communication is found between 2 ranges:
      - 2.4 GHz Band: 2.4-2.4835 GHz
      - 5 GHz Band: 5.15-5.85 GHz
    - Wireless Bands are subdivided into channels



λ and f are directly proportional: (inverse)
As λ↑ f↓
λ↓ f↑
Accordian
Same distance
Same amplitude

- WiFi Channels:
  - 2.4 Channels:
    - Usable channels in this range include: 1, 6, 11
    - 5 MHz between channels (there is 12 MHz between channel 13 and 14)
    - Channel 14 is only allowed in Japan with 802.11b
    - A honeycomb design means no overlapping channels
  - 5 GHz:
    - Not channel restricted
    - Wider channel ranges that won't overlap





- RF Signal Strength:
  - Measured in decibel milliwatts (dBm)
  - Transmitters range between 1-100 milliwatts (mW)
  - Milliwatt (mW) = $\frac{1}{1000}$ of a watt
  - mW to dBm relationship:
    - 1 mW = 0 dBm
    - 10 mW = 10 dBm
    - 100 mW = 20 dBm
    - 1 W = 1000 mW = 30 dBm
    - Logarithmic scaling, +10 dBm = ×10 mW
      -10 dBm = ÷10 mW
      +3 dBm = ×2 mW
      -3 dBm = ÷2 mW

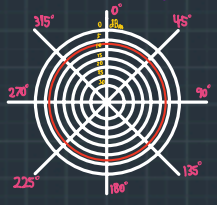
Transmit Power (TX) = Positive dBm
Receive Power (RX) = Negative dBm

- Signal to Noise Ratio: The difference in the background radio noise you have in an environment and the signal strength
  - * SNR = Received Signal - Noise Floor
  - A good SNR is ≥25 for VoIP or streaming and ≥20 for regular traffic

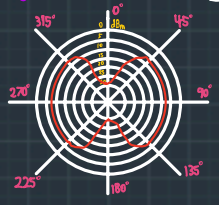
Antenna Types:

-Radiation Pattern: The measure of signal strength around an antenna

-Omnidirectional Antenna: Designed to propagate signal in all directions



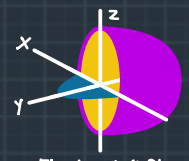
H Plane



E Plane

The coverage of an access point

Horizontal "H" Plane
Azimuth - top-down



Elevation "E" Plane
Elevation - Side-view

-Directional Antenna: Designed to propagate in a specific direction

-Patch Antenna: Propagates signal primarily in one general direction

H Plane

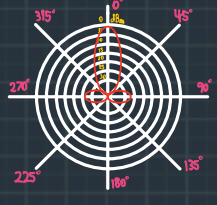
E Plane

$f = \frac{c}{\lambda}$ ← c

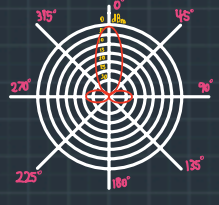
$\lambda = \frac{v}{f}$

$f = \frac{1}{T}$ ← period

-Yagi Antenna: Hyper-focused, very directional antenna over "short" distances



H Plane



E Plane

-Dish/Parabolic Antenna: Same as Yagi but longer distance due to its unique shape, Hyper-focused, very directional antenna over "long" distances

Access Point Operation:

-AP steps are as follows:

-Boot State: LAP boots from local IOS image & recieves addressing

-WLC Discovery State: LAP actively searches for a controller with CAPWAP discovery request messages

-WLC Discovery Process:

-CAPWAP discovery request messages are sent out as broadcast messages on the local subnet over UDP port 5246

-DHCP Option 43 information used, if configured on DHCP server

-LAP attempts to resolve a DNS request to CISCO-CAPWAP-CONTROLLER.localdomain

-If no controller is found, the LAP will reboot and go through the discovery process again

-At the end of discovery, the LAP will have a list of available WLCs on the network

-CAPWAP Tunnel State: CAPWAP tunnels are established between LAP and WLC

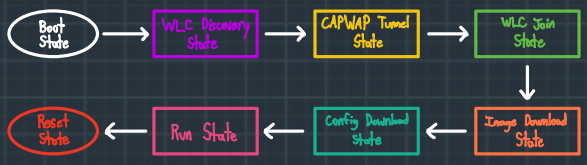
-WLC Join State: CAPWAP message exchange authenticates and associates LAP and WLC

-WLC Selection Process:

-Join a previous Known controller

-Join a master controller

-Join the least-loaded controller



-Image Download State: LAP compares local software image to the WLCs baseline image and updates if necessary

-Config Download State: LAP polls the WLC for configuration information

-Run State: LAP is fully operational and is providing network access via BSSID

-Reset State: LAP tears down CAPWAP tunnels, erases client associations, and restarts process

Wi-Fi Standards:

-Wi-Fi standards over the years are included in the table below

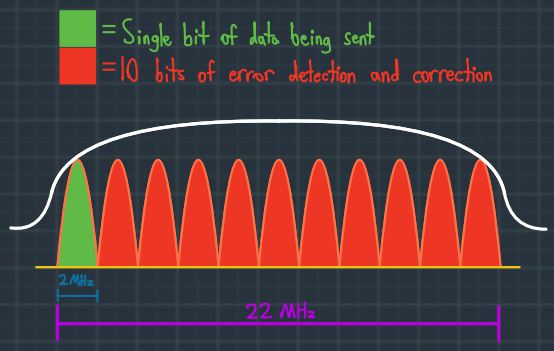
-Bandwidth = $f_H - f_L$

Wi-Fi (Phy) Standards Table:

Standard	Year Released	Frequency Band	Maximum Bandwidth	Transmission Method
802.11	1997	2.4 GHz	1-2 Mbps	DSSS or FHSS
802.11a	1999	5 GHz	54 Mbps	OFDM
802.11b	1999	2.4 GHz	11 Mbps	DSSS
802.11g	2003	2.4 GHz	54 Mbps	OFDM
802.11n	2009	2.4 and 5 GHz	600 Mbps	OFDM
802.11ac	2013	5 GHz	6.93 Gbps	OFDM
802.11ax	2021	2.4, 5, and 6 GHz	9.68 Gbps	OFDMA

FHSS not used after original standard

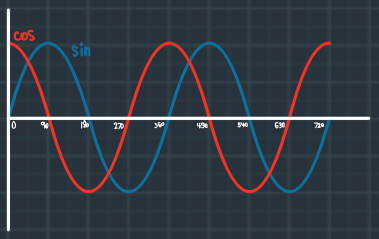
Note: WiFi 6E adds the 6 GHz band with 7 non-overlapping 160 MHz channels



Transmission Methods:

Direct-Sequence Spread Spectrum:

- A single bit can be sent using a 2 MHz frequency range
- Using Barker 11 Coding, 1 bit is transmitted along with 10 extra bit (called "chips"), which provide protection from interference
- A Symbol is the sequence of 11 bits being sent to encode a single bit
- Used in the older 802.11b wireless standard



Orthogonal Frequency Division Multiplexing:

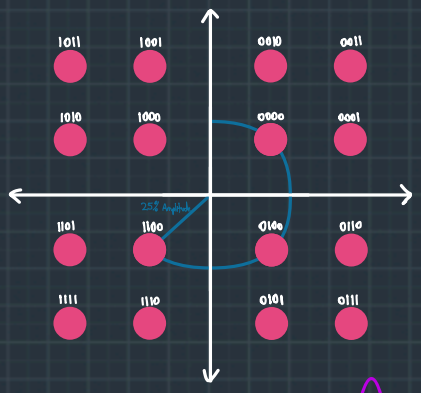
- Frequency Division Multiplexing: A 20 MHz band used to send 10 different bits of data at a time on 2 MHz subchannels
  - With all these subchannels directly adjacent, there is bound to be interference unless there is orthogonality
- Orthogonal: At right angles to (phase-shifted 90°)
- Definition: A data transmission technique that sends different signals using different subchannels (different frequencies), where adjacent subchannels are transmitted 90° to one another
  - When one wave is at peak power, the other is at 0 and vice versa so no interference will occur

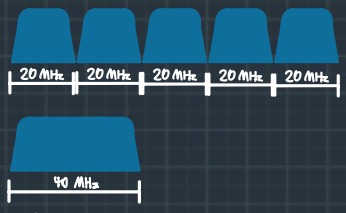
Quadrature Amplitude Modulation:

- A form of being able to send more bits using a single 2 MHz subchannel
- 16-QAM: Identifies 16 different targets in a constellation, each of which represents 4 bits

Example Table of Constellation Targets

Amplitude	Phase	Data
25%	225 degrees	1100
75%	135 degrees	1001
25%	315 degrees	0100
75%	247 degrees	1110
25%	225 degrees	1100
75%	337 degrees	0110
25%	225 degrees	1100
75%	225 degrees	1111

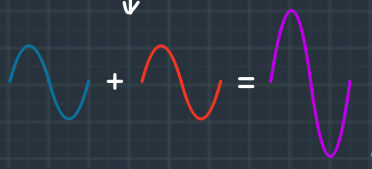


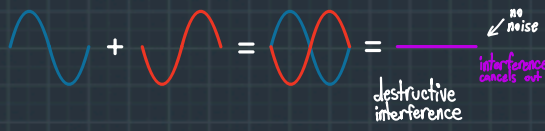


Channel Bonding: Putting channels together to provide even more throughput

Beamforming: Using constructive and destructive interference to affect amplitude and noise

- Waves are overlayed each other, increasing or decreasing amplitude
- Changes the phases of waves to focus on a specific client, by creating constructive and deconstructive interference
- Introduced in IEEE 802.11n





Single-User Multiple Input Multiple Output (SU-MIMO): An access point can only talk to one user at a time (can only send one spatial stream (1 ss))

Multiple-User Multiple Input Multiple Output (MU-MIMO): An access point can send 4 downstream spatial streams at a time but can only recieve one

Standard	QAM	Bits Represented	Supported Channel Widths	Spatial Streams
802.11n	64-QAM	6 bits	20 MHz 40 MHz	1 Downstream
802.11ac	256-QAM	8 bits	20 MHz 40 MHz 80 MHz 160 MHz	4 Downstream
802.11ax	1024-QAM	10 bits	20 MHz 40 MHz 80 MHz 160 MHz	2.4 GHz Band: 4 Upstream & Downstream 5 GHz Band: 8 Upstream & Downstream

? Theoretical 8 spatial streams

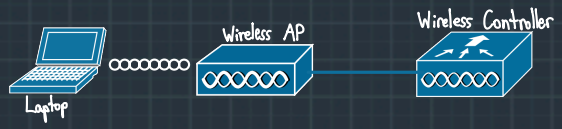
Orthogonal Frequency Division Multiple Access:

- Utilizes target wake time functionality to conserve power and minimize collisions, reduces further collisions caused by carrier sense multiple access with collision avoidance (CSMA/CA)
- Carrier Sense Multiple Access with Collision Avoidance:
  - Wireless network need collision avoidance over collision detection because most of their signal strength is used to send the data

- To avoid collisions, the client will probe to sense if there are any other transmissions happening to that access point
- If no transmissions are sensed, the client will send the data to the AP and wait for an acknowledgement; If one is not recieved, it will attempt to transmit the data again
- If a transmission is sensed, the client will wait a random amount of time before probing again

- Target Wake Time: When an access point connects out to clients, they give each client a timeslot, scheduling communication with each device connected to it
  - Used by a 802.11ax AP to schedule when a client can send and recieve, resulting in less latency and power saving (deterministic transmission)
  - Client devices might be configured to go into low power mode when not communicating with the AP
- Basic Service Set Coloring: Allows signals for one SSID on a specific channel to be distinguished from signals for a different SSID using the same channel by "coloring" the traffic

Pre-Shared Key Authentication:



- A way to set AP authentication for small deployment environments

Pre-Shared Key Theory:

- All WPA versions support personal mode (PSK) and enterprise mode (802.1x)
- In personal mode a PSK string must be configured on controller, APs, and clients

Temporal Key Integrity Protocol: Used by original WPA standard; Combines key string and SSID to generate unique encryption keys

Advanced Encryption Standard: Used by WPA2 and WPA3 as a more advanced encryption algorithm than TKIP, protecting against password attacks

Pre-Shared Key Benefits:

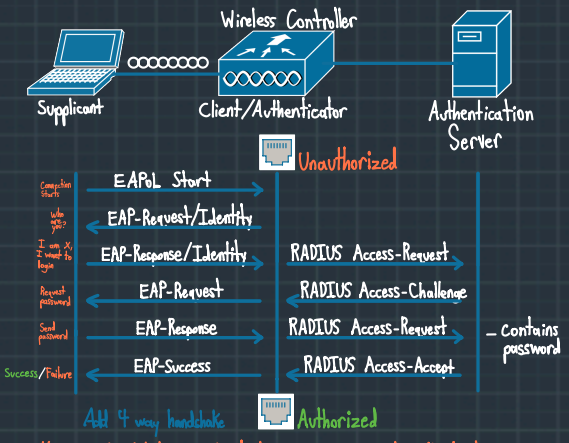
- Less complex than 802.1x deployments
- Legacy client support

Pre-Shared Key Limitations:

- Less secure
- More administrative burden
- Requires complex key creation

Extensible Authentication Protocol Authentication:

- 802.1x Authentication
  - IEEE standard which defines port-based network control/security
  - Uses EAP over LAN (EAPoL) to control access to the local area network
  - 3 parts to a 802.1x network:
    - Supplicant: The endpoint requesting access
    - Authenticator: Network device controlling physical access to the network
    - Authentication Server: Performs the actual authentication of the endpoint

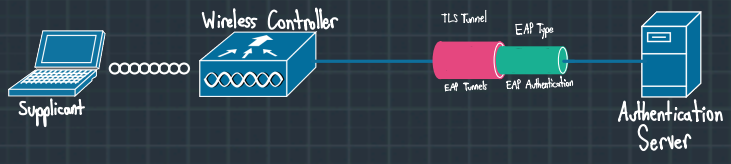


4-way handshake is only between supplicant and authenticator

retransmitted PSK?

EAP Types:

- Native EAP Types:
  - EAP-TLS:
    - One of the most secure EAP types
    - Uses X.509 certificates for mutual authentication
    - Highly regarded in BYOD deployments
  - EAP-MD5:
    - Hides credentials in a hash
    - Common in IP phones
  - EAP-MSCHAPv2:
    - Credentials encrypted within an MSCHAPv2 session
    - Simple transmission of credentials
    - Ability to communicate with Active Directory
  - EAP-GTC:
    - Cisco Alternate to MSCHAPv2
    - Enables more generic authentication
- Tunneled EAP Types:
  - Protected EAP (PEAP):
    - Originally proposed by Microsoft
    - Uses X.509 certificates
    - Uses an additional native EAP type for inner method
  - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST):
    - Created by Cisco as a PEAP Alternative
    - Faster re-authentication



-Faster wireless roaming

Wireless QoS: (802.11e)

-WiFi Multimedia (WMM)

-IEEE 802.1P markings map to WMM access categories

-Access category determines Interframe Space (IFS) and Random Backoff Timer

-To treat traffic with a higher priority differently there will be a more agressive IFS, so traffic is sent closer together and the random backoff timer will be shorter

4 Access Categories	802.1D
AC_VO (Voice)	6 & 7
AC_VI (Video)	4 & 5
AC_BE (Best Effort)	0 & 3
AC_BK (Background)	1 & 2

Wireless Troubleshooting:

-Successful Client WLAN Association:

-Client must be within access point RF range

-Client must properly authenticate to the WLAN

-Client should recieve a valid IP address on the subnet

Wireless Security & WiFi-Hacking:

Propagation: How the wave travels away from a source

Diffraction: How the wave gets wider as it travels away from a source