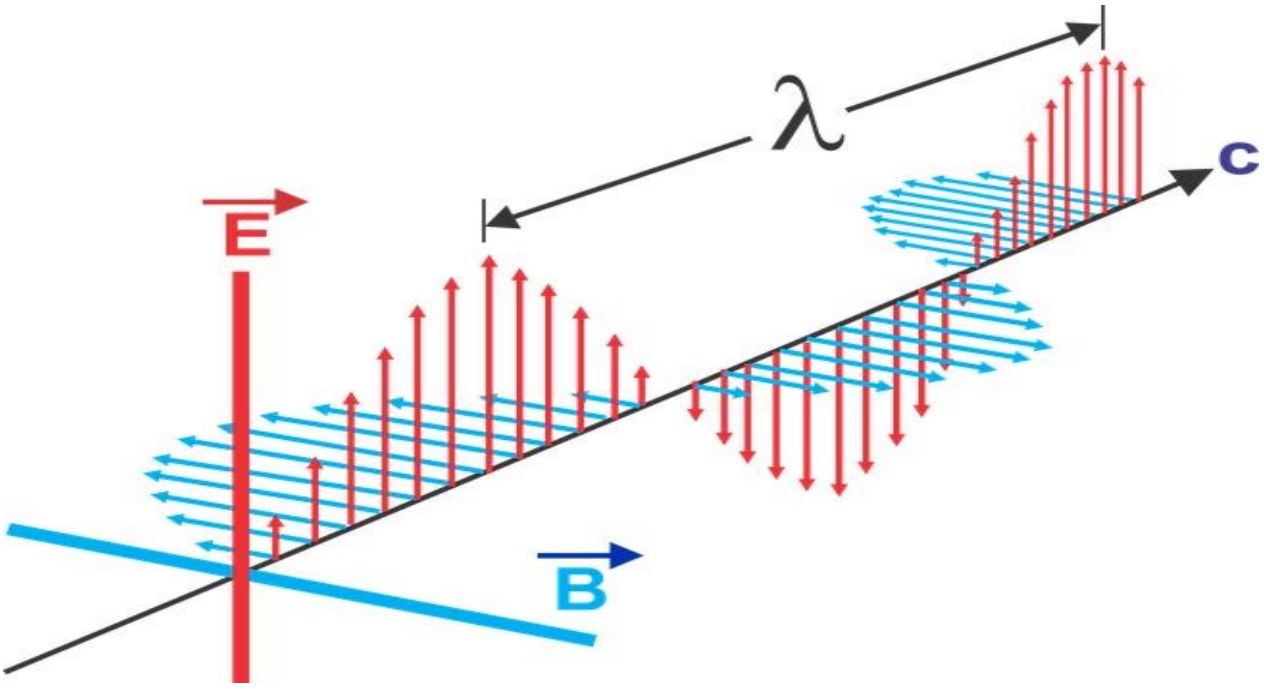
BASIC RF Theory

Electromagnetic Radiation (EMR) is simply a form of energy that carries signals from one point to another. It exhibits wave-like behavior, consists of both electric and magnetic fields, and travels at the speed of light (in a vacuum).

FREQUENCY	DESCRIPTION
30 GHZ - 300 GHZ	extremely high frequency
3 GHZ - 30 GHZ	superhigh frequency
300 MHZ - 3 GHZ	ultrahigh frequency
30 MHZ - 300 MHZ	very high frequency
3 MHZ - 30 MHZ	high frequency
300 KHZ - 3 MHZ	medium frequency
30 KHZ - 300 KHZ	low frequency
3 KHZ - 30 KHZ	very low frequency
300 HZ - 3 KHZ	voice frequency
Up to 300 HZ	extremely low frequency

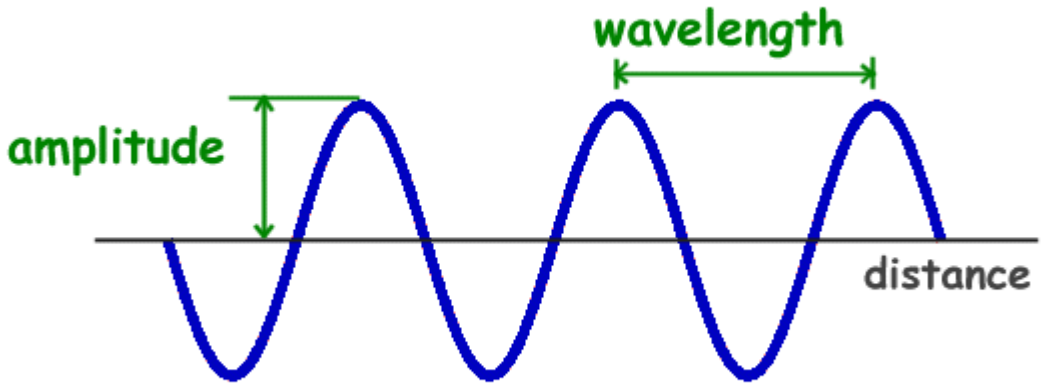
As can be seen above, the spectrum is broken down into several ranges. Although all are important in wireless communication, the ranges that are most important to us in terms of 802.11 communications are UHF and SHF. Specifically, we deal with the 2.4 GHz and 5.8 GHz frequency bands. But as all are part of the Electro-Magnetic Radiation (EMR) spectrum, let's get back to EMR in general.



EMR, depicted above, is the term that describes the propagation of radio signals. As the electric (E) field propagates, it gives up its energy to a companion magnetic (B) field. We see a gradual transfer of energy from one form to another, but no loss or gain in the total energy of the wave, at least in a vacuum.

Amplitude measures the magnitude of change of the oscillating variable within an oscillating system (think peaks and troughs).

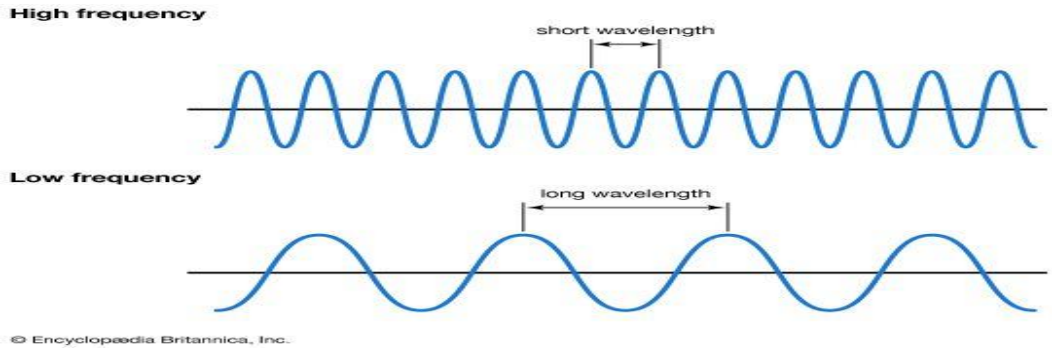
Wavelength is the measure of spatial distance over which the wave's shape repeats (the difference in the peaks).



The wavelength is especially important when dealing with antenna design, as an antenna is most efficient when its length is proportional to the signal's wavelength. An important formula to remember follows, which is for a quarter-wavelength antenna.

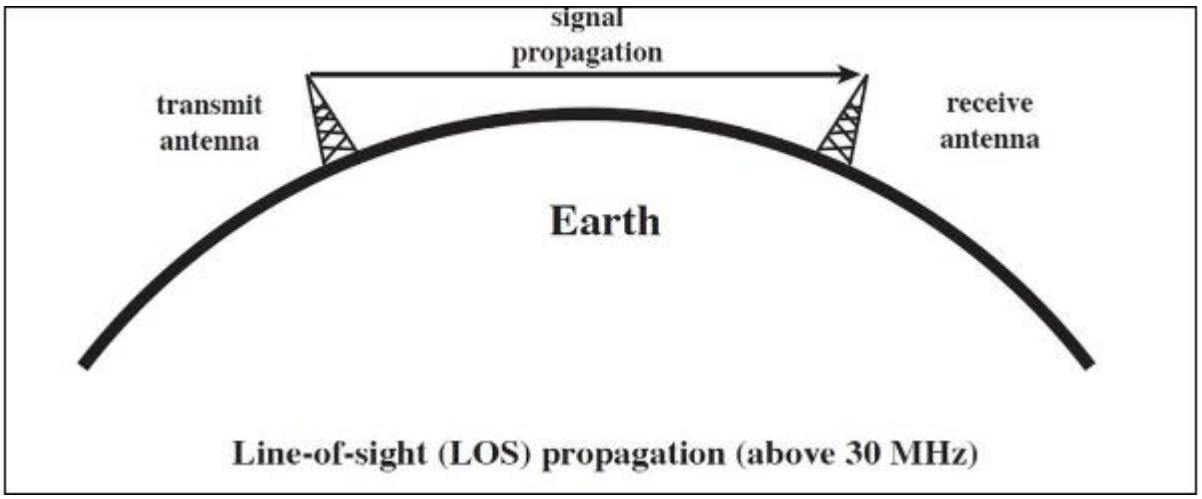
234 / Frequency (MHz) = Antenna Length (Ft)

Frequency refers to the number of occurrences of a repeating event per unit time. Full wavelength for 2.4ghz is 4.92126 inches and for 5ghz it is 2.035433 inches. (6ghz is 1.9685)



Frequency is measured in Hertz, but can also be referred to as Cycles Per Second (CPS). Frequency can be changed by modifying the voltage of the input signal.

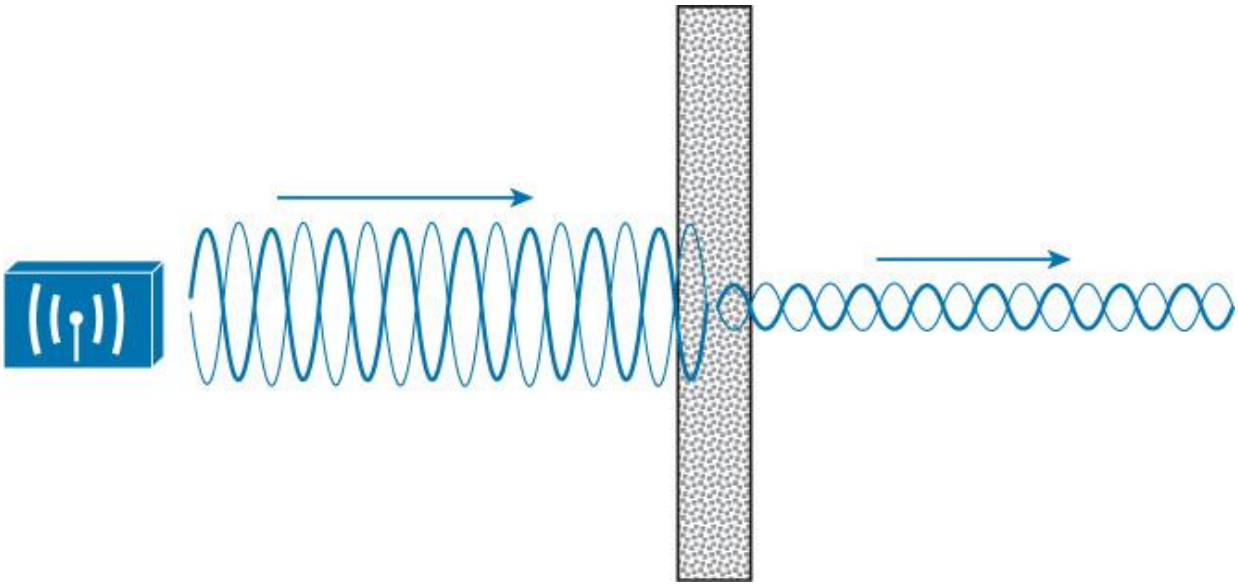
Radio line of sight is the clear path that a radio wave travels between two emitters.



Radio waves travel in a straight line. These waves may be absorbed, reflected, refracted, or diffracted. In addition, scattering and shadowing may affect the signal. For best results in transmission and reception, radio line-of-sight (LOS) is important. When degradation is caused, it is called free space loss.

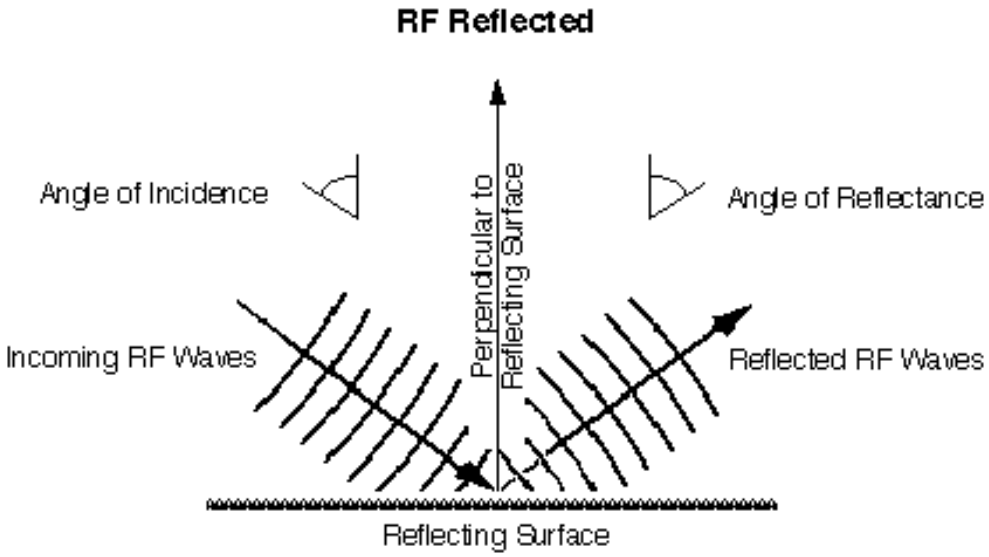
Signal Propagation Factors

Absorption is when an object traps incoming radio waves



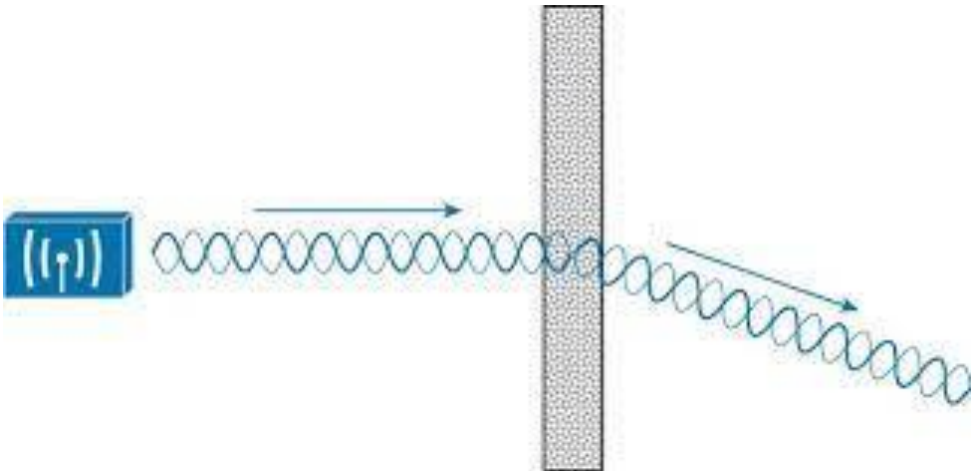
RF energy can be absorbed by various materials. Some materials absorb RF more than others. As signal frequency increases, so do the effects of absorption. The shorter the wavelength the greater the effects of absorption will be.

Reflection is when radio waves reflect off an object and have both equal angles of incidence and reflectance.

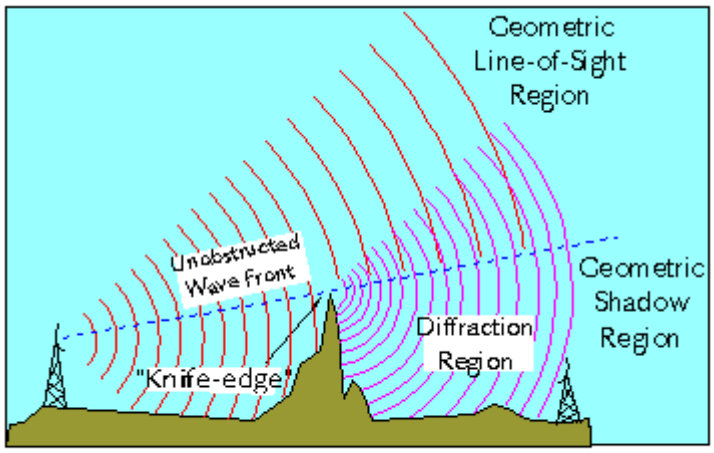


Buildings with metallic surfaces provide excellent reflectors of radio energy. Signals traveling to and from wireless access points often travel via a variety of paths.

Refraction occurs when RF waves cross from one medium to another of a different density; their speed and direction are altered.

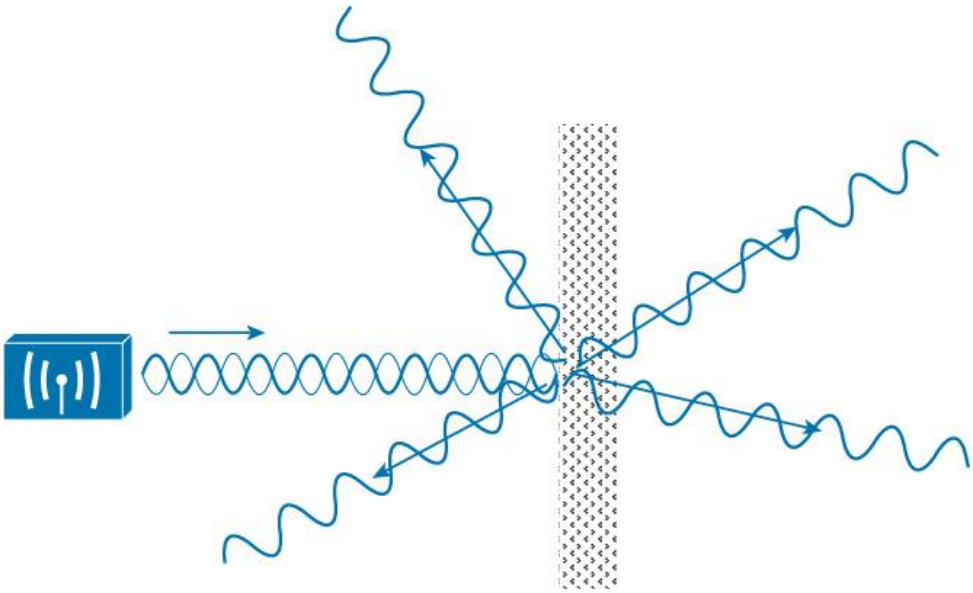


Diffraction is the bending of radio waves around small objects and openings.

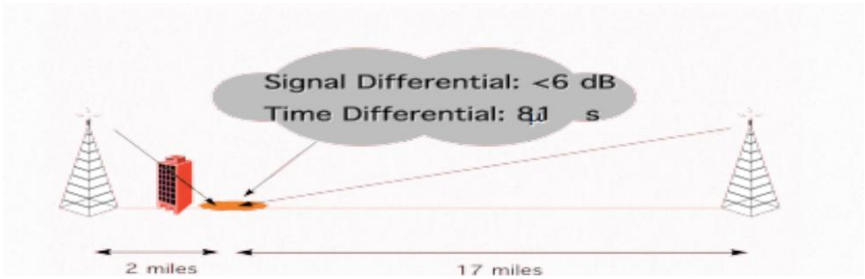


knife-edge effect

Scattering occurs when a radio wave strikes an uneven surface and reflects the waves in different directions.



Shadowing is an area in which no coverage is available due to terrain or other objects.



Multi-Path is when radio waves take multiple paths to reach the same receiving radio. Multipath in 802.11 is enhanced by using Multiple Input, Multiple Output (MIMO). MIMO was introduced in 802.11n, MIMO takes advantage of multipath by using multiple antennas. MIMO allows devices to identify the different paths the signals take to the receiver and sends unique streams of data, known as *spatial streams*, along different paths. Transmission across multiple spatial streams to a single client is known as single-user MIMO (SU-MIMO). Doubling the number of spatial streams effectively doubles the available throughput.

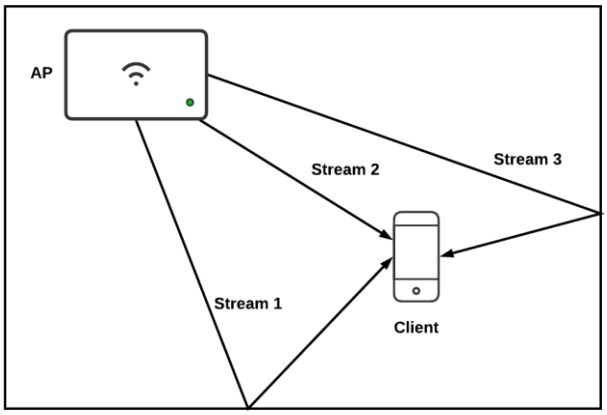


Figure 1 SU-MIMO

802.11ac expanded MIMO to allow the AP to use different spatial streams to transmit to multiple clients (up to four) simultaneously. This is known as downlink multiuser MIMO (DL-MU-MIMO).

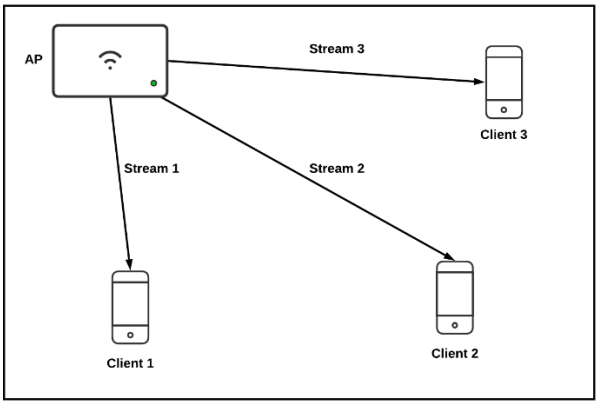


Figure 2 DL-MU-MIMO

MU-MIMO in 802.11ax allows up to eight clients across eight spatial streams and allows for clients to transmit to the AP simultaneously across different spatial streams (uplink, UL-MU-MIMO).

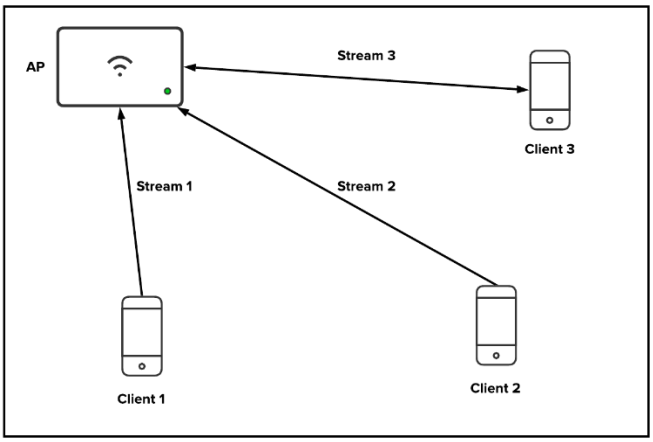
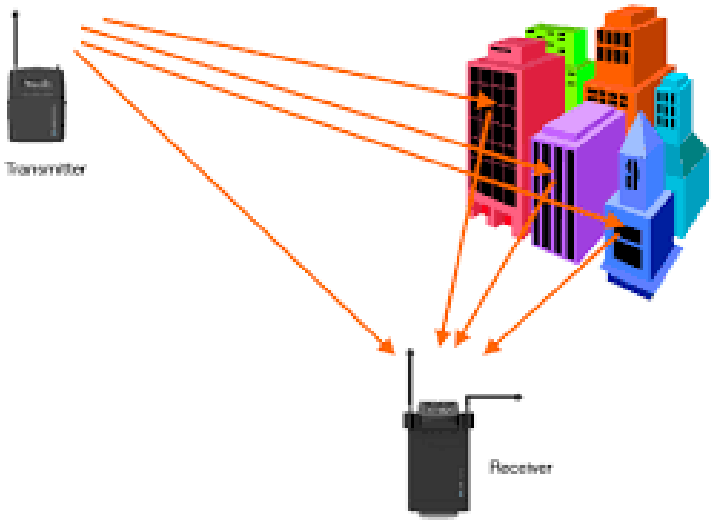


Figure 3 UL-MU-MIMO

The number of spatial streams a device supports varies by manufacturer and model. Antenna capabilities are typically written in the form *transmitters x receivers: spatial streams.* For example, an access point with antenna capabilities of 8x8:8, would have 8 transmit antennas, 8 receive antennas, and 8 spatial streams. Client devices do not have to be 802.11ax-capable to take advantage of APs with 8x8:8 antennas. Through techniques like maximal ratio combining (MRC), the AP can improve the strength of the signal it receives from its clients. Stronger signal strength means higher data rates and longer range for APs with 8x8:8 antennas over those with 4x4:4. [1]



Radio signals can reach the receiving antenna by multiple paths, caused by atmospheric ducting, ionospheric reflection, refraction, and reflection from water bodies and terrestrial objects such as mountains and buildings. Four important effects can occur as a result of multi-path:

[1] https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Wi-Fi_6_(802.11ax)_Technical_Guide

Upfade

The signal strength is increased at the receiver. This is due to the multiple signals arriving in phase or close to the primary wave. The signal will never be stronger than the original transmitted signal (free space path loss).

Downfade

Basically, this is the opposite of upfade - the multiple signals arrive significantly out of phase with the primary wave (more than 120 degrees), causing the signal strength to decrease

Nulling

This occurs when the multiple signals arrive 180 degrees out of phase with the primary wave, cancelling out the signal.

Data Corruption

Also known as Intersymbol Interference (ISI), this is caused when the multiple signals arrive at different times and cause bits to overlap with each other, confusing the demodulation.

Gain and Loss

In the end, all things add up to a signal's gain or loss. Gain describes a positive difference in amplitude and is obtained through amplification of the signal either intentionally (amplifier) or unintentionally (signal combination after reflection). Loss (or attenuation) describes a negative difference in amplitude. One can intentionally attenuate a signal using an attenuator while unintentional loss of signal can be caused by the many factors described above.

Modulation

Modulation is the process of conveying a message signal inside another signal that can be physically transmitted by modifying one or more of its properties. This "carrier signal" carries no information of its own. Three basic operations can be used to modulate this carrier signal: changing its amplitude, changing its frequency, and changing its phase. These modulations can be done for both analogue and digital transmissions. Analogue modulation includes Amplitude Modulation (AM), Frequency Modulation (FM), and Phase Modulation (PM).

WLAN's use digital modulation. Digital modulation types include Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), and Phase Shift Keying (PSK). Advantages of digital modulation include error correction, better use of bandwidth, and less power usage. Binary Phase Shift Keying (BPSK) which can be found in CDMA, WiMAX (16d, 16e), WLAN 11a, 11b, 11g, 11n, Satellite, and DVB. Quadrature Phase Shift Keying (QPSK) is used in various cellular wireless standards such as GSM, CDMA, LTE, 802.11 WLAN, 802.16 fixed and mobile WiMAX, Satellite and CABLE TV applications. An easy way to visualize how BPSK and QPSK fit into same wireless technologies, is BPSK is used for signaling and channel setup where QPSK is used for sending data. BPSK has a data rate of 3 Mbps and QPSK has 6 Mbps and more. Quadrature Amplitude modulation (QAM) is found in Wi-Fi 5 (256-QAM) and Wi-Fi 6(1024-QAM). QAM is also used in 5G modulation. QAM is a signal in which two carriers shifted in phase by 90 degrees (i.e., sine and cosine) are modulated and combined. At the receiving end the two carriers are then separated and interrupted. Normally the lowest order QAM encountered is 16QAM. The reason for this being the lowest order normally encountered is that 2QAM is the same as BPSK, and 4QAM is the same as QPSK. QAM is used for its ability to transmit higher data rates.

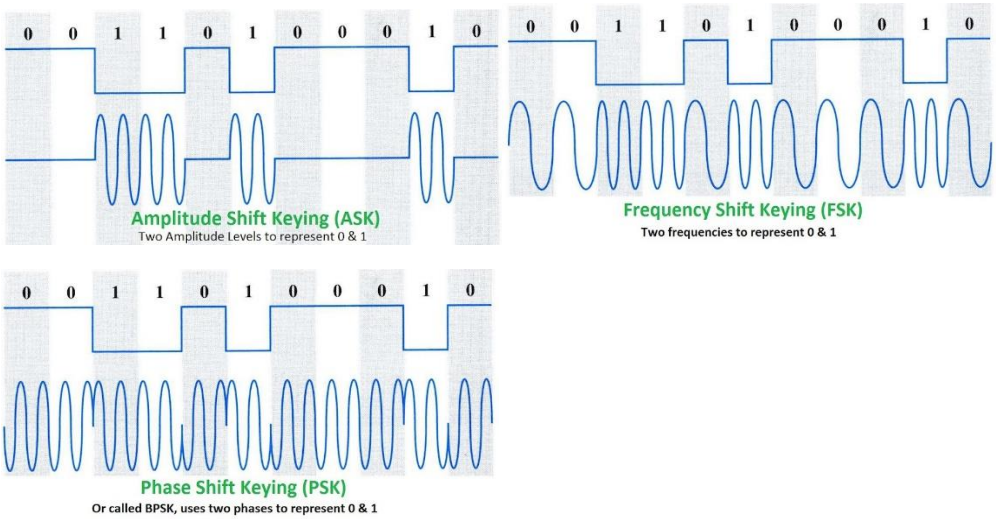


Figure 4 BPSK 180-degree Phase shift

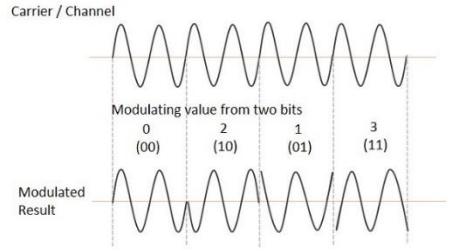


Figure 5 QPSK 90-degree phase shift

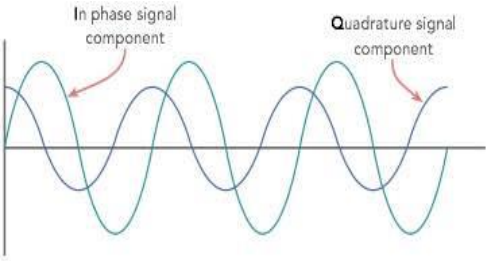


Figure 6 QAM Signal

Multiplexing

Also called “muxing”, this is a method by which multiple message signals can be combined into one carrier signal for transmission. There are many different types including the following examples. [2]

- Frequency Division Multiplexing (FDM)
- Time Division Multiplexing (TDM)
- Orthogonal Frequency Division Multiplexing (OFDM)

Antennas

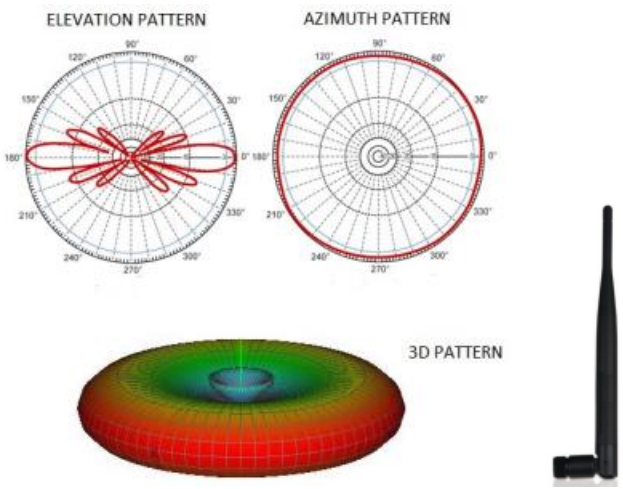
Gain and Loss:

Rule	Explanation	Percentage of Power Lost/Gained	Current Power Level	Example
-3 db	**Half the watt value**	**50% lost**	**Half of original**	**100mW -3db = 50mW**
+3 db	**Double the watt value**	**100% gained**	**Double the original**	**10mW + 3db = 20mW**
-10 db	**Decrease watt value to one tenth of original**	**90% lost**	**One-tenth of the original**	**300mW – 10db = 30mW**
+10 db	**Increase the watt value by ten-fold**	**1,000% gained**	**Ten times the original**	**10mW + 10db = 100mW**

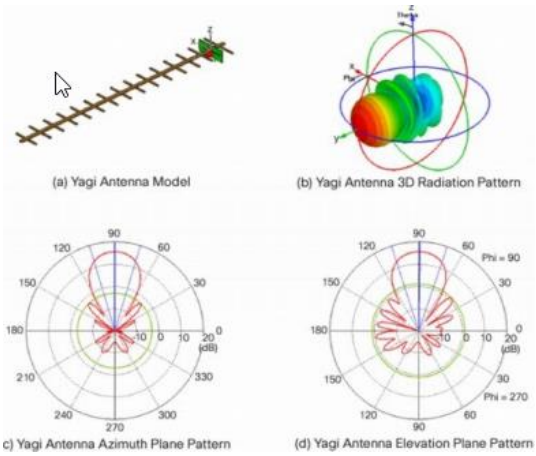
Antenna gain is measured in dBi (decibels isotropic) or dBd (decibels dipole). dBi measures the antenna gain against a true isotropic antenna. A non-existent antenna based on a perfect omni-directional radiator. dBd measures the antenna gain against a reference dipole antenna. dB, dBi, and dBd are all measurements of gain. You may also see dBm which is a measure of signal power. dBm is a standard unit for measuring levels of power in relation to a 1-milliwatt (mW) reference signal.

Omni Directional probably the most common antenna. For 802.11 they typically come in 3dbi or 6dbi and depending on the card are dual band.

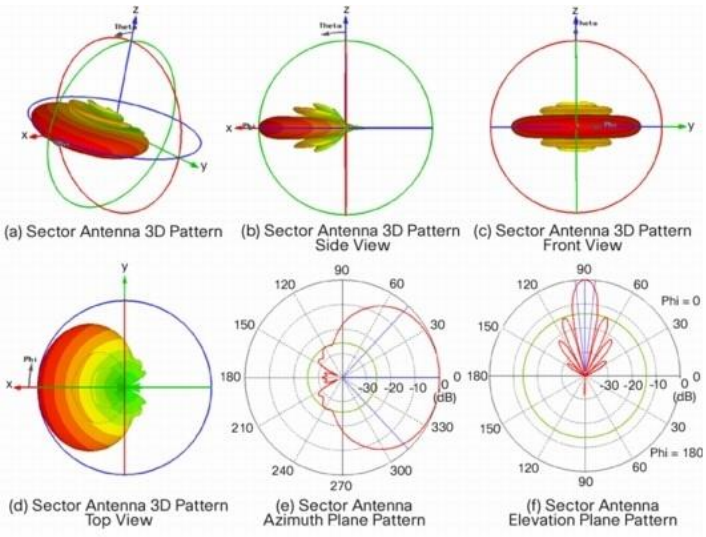
[2] https://www.electronics-notes.com/articles/radio/modulation/quadrature-amplitude-modulation-types-8qam-16qam-32qam-64qam-128qam-256qam.php



Directional: There are several types of directional antennas, but the example below is a Yagi. Directional antennas will have a lot more gain and you will typically use these when you must maintain some standoff. For example, you could setup in a parking garage across the street from the location and point it at your target. Be careful where you have a Yagi pointed. It is a highly directional antenna so make sure you are collecting against APs that you need to. Bottom line, confirm you are getting what you need.



Sector: These antennas are used often for cellular networks. They are also frequently used in Enterprise WLAN. Sector antennas are great for providing signal to specific areas and help minimize bleed over outside of your buildings.



Alfa has a couple different Sector antennas that fit on almost all their cards. This antenna should be part of your WiFi assessment load out. It useful for narrowing down the location potential Rogue APs. You can lock onto a channel and use this antenna as it is more directional. This antenna will also be helpful when collecting against the client's network because of its directionality. It will help minimize collecting against APs that are not in scope / don't belong to the client.



802.11 Basic Theory

Below are the current 802.11 Standards.

Generation/IEEE Standard	Maximum Linkrate	Adopted	Frequency
Wi-Fi 6E (802.11ax)	600 to 9608 Mbit/s	2019	6 GHz
Wi-Fi 6 (802.11ax)	600 to 9608 Mbit/s	2019	2.4/5 GHz
Wi-Fi 5 (802.11ac)	433 to 6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72 to 600 Mbit/s	2008	2.4/5 GHz
802.11g	6 to 54 Mbit/s	2003	2.4 GHz
802.11a	6 to 54 Mbit/s	1999	5 GHz
802.11b	1 to 11 Mbit/s	1999	2.4 GHz
802.11	1 to 2 Mbit/s	1997	2.4 GHz

Popularly referred to as Wi-Fi

- Currently has six specifications (A, B, G, N, AC, AX).
- Frequency Use
    - 2.4 GHz (B, G, N, AX) / 5 GHz (A/N, AC, AX).
    - Currently the WiFi6E 6 GHz band is still new.
    - Channels vary based on country regulations.

2.4 GHZ

22mhz wide channel 802.11B.

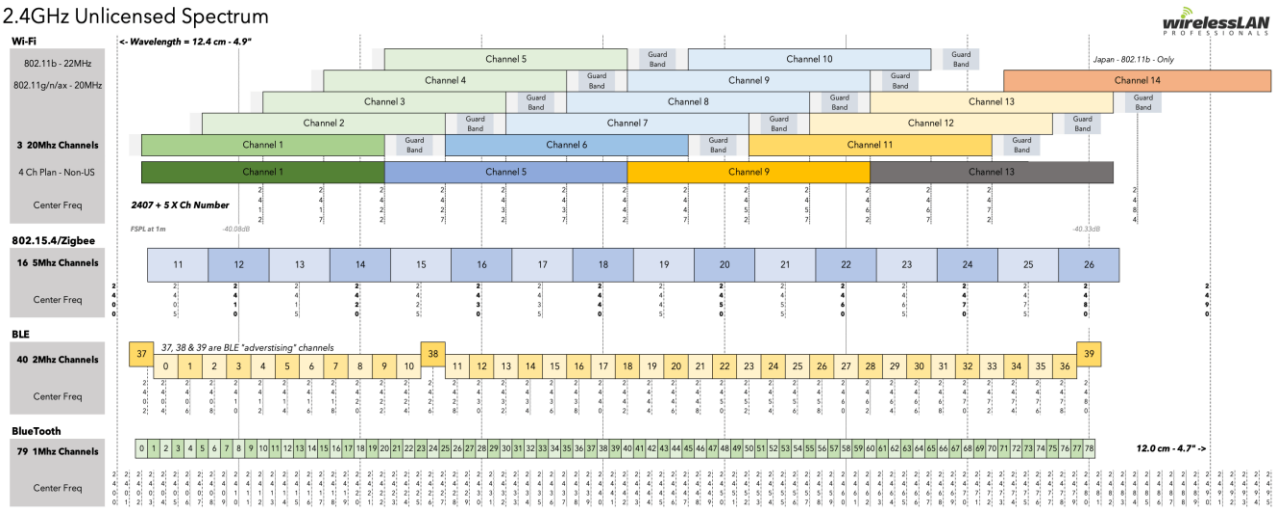
20mhz wide channels in use for 802.11g and above.

In the US only channels 1-11 are used.

Channels 1,6,11 are the only non-overlapping in 2.4 GHz.

Bluetooth, Zigbee, and BLE also operate in this band.

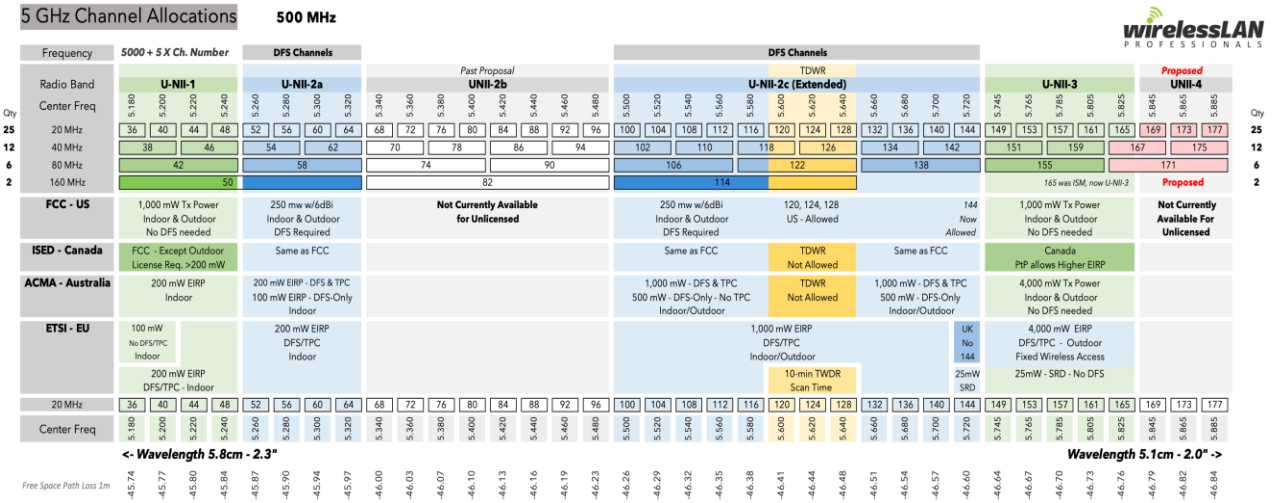
WiFi in this band will travel the farthest, about 300ft outdoors and around 150ft indoors (this is a estimate based on signal propagation). This is enviroment dependent.



5Ghz

Base channel is 20mhz wide channels. Channels can go all the way up to 160mhz wide. Transmission in this band will go about 150ft outdoors and 50 ft indoors. This is environment dependent.

5Ghz has Dynamic Frequency Shift (DFS) channels. These channels share spectrum with radar systems. If your device hears a radar event, it will stop using these channels and automatically move to another channel.

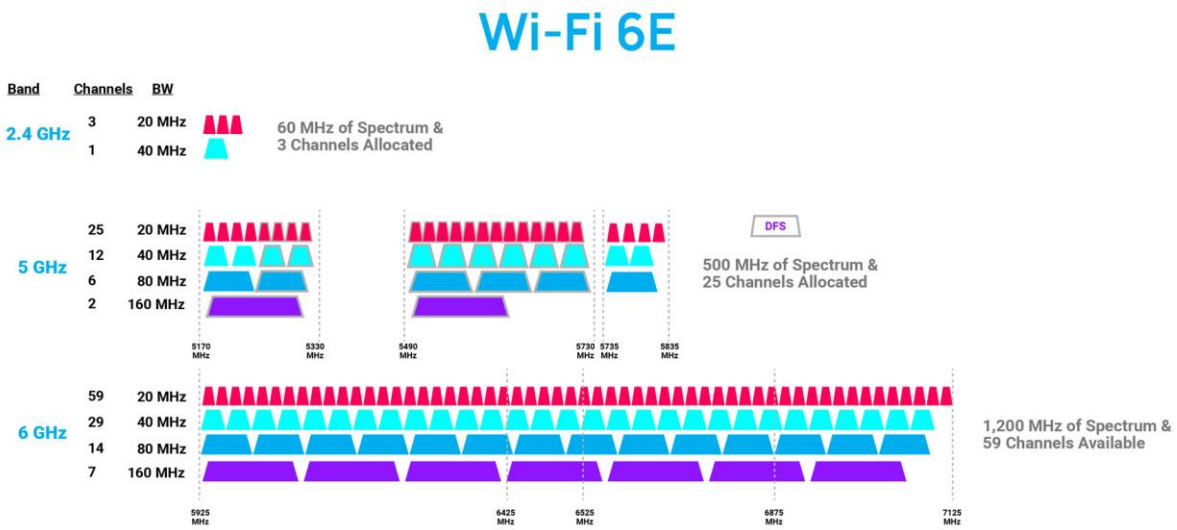


6GHz

Base channel is 20mhz wide channels. Channels can go all the way up to 160mhz wide.

This band was recently unlicensed. Transmission in this band will not travel very far, probably 90 ft outdoors and between 40-50ft indoors maximum. Although Wi-Fi6 is better at multiplexing because of

its implementation for bidirectional Multiple-User Multiple-Input/Multiple-Output (MU-MIMO), multiplexing can make signals travel farther then the estimated signal propagation distances.



802.11 Frame types

There are three types of 802.11 frames. Each type has several sub-types. Some of the relevant subtypes are described below:

- **Management Frames**: Enables stations to establish and maintain communications.
    - These include Authentication, Deauthentication, Association Request, Association Response, Reassociation Request, Reassociation Response, Disassociation, Beacon, Probe Request, Probe Response.
- **Control Frames**: Assist in the delivery of the data frames between stations.
    - These include Request to Send (RTS), Clear to Send (CTS), Acknowledgement (ACK).
- **Data Frames**: Carry actual data from higher layers, such as web pages, printer control data, etc. within the body of the frame.

PMF (Protected Management Frames): Provides protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging only. [3]

Management frames cannot be encrypted because Wi-Fi is a broadcast medium. PMF helps protect them against forgery. If the AP and client both support PMF there is additional key data added in the EAPOL exchange. It is important to note cryptographic protection of Deauthentication and Disassociation frames.

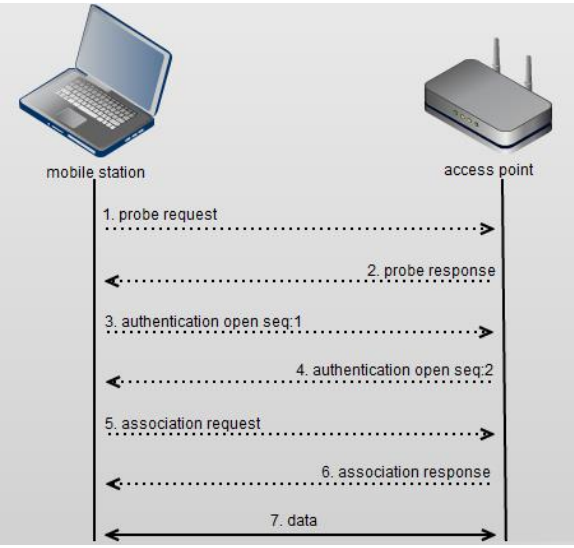
[3] https://www.wi-fi.org/knowledge-center/faq/what-are-protected-management-frames#:~:text=Protected%20Management%20Frames%20(PMF)%20provide,frames%20are%20protected%20from%20forging.

802.11 Discovery Phase

This phase is completed using Management Frames. This is where the device is trying to find a known network to connect or one with a better signal. The frames used for the discovery phase will generally be transmitted at the lowest possible transmission rate to ensure every station within the network coverage can hear what is going on. This should be 1mbps in 2.4GHZ and 6mpbs in 5GHZ. This allows for the maximum distance for the signal to travel. HT and VHT channels are generally not used for management frames.

- Active: During this exchange both the station and the AP are sharing information about their capabilities.
    - Probe Request: This is sent out by the client. There are two types of Probe Request. Probe Requests will go out on all channels the station can transmit and receive on.
        - Directed Probe Request: The station is looking for a specific network to connect. This network is in the preferred network list of the station. (These types of requests are less common these days)
        - Broadcast Probe Request: The station is looking for any network on the channel the probe request was broadcast.
    - Probe Response: This is sent out by the AP. The AP will respond to any probe request it receives. (Unless you have this turned off in the configurations).
- Passive:
    - Beacon Frames: These frames are sent by the AP on all channels the AP can transmit and receive on. Beacon frames are not directed towards any station and are a means for the AP to let all the stations in the coverage area know it is there and ready to communicate. In this frame the AP will broadcast its capabilities.

Authentication and Association



- Authentication: This is the 1st step in attaching to the network; the client must establish its identity. There are two types of authentication methods in the 802.11 standard.
    - Open system/authentication: Essentially a NULL authentication. The wireless client sends an authentication request, and the AP accepts without question. This does not mean there is not some other form of authentication higher up the OSI model. You are just not using the wireless authentication mechanism. This is common for Open Wi-Fi hotspots.
    - Shared Key: Allows anyone who has the key to authenticate to the wireless network. This is for WEP, WPA, WPA2
    - *Simultaneous Authentication of Equals (SAE): Is the new replacement for PSK. It uses forward security. No password is transmitted. This is a WiFi Alliance standard not in the 802.11 standard.*
- Association: 2nd step in attaching to the network. Here the client is registering with the network. This is where the capabilities of the client and the AP finalized. If they match the client will get a association success if not disassociation.

Note: 4-way handshakes and 802.1X authentication do not happen until after the association has taken place.

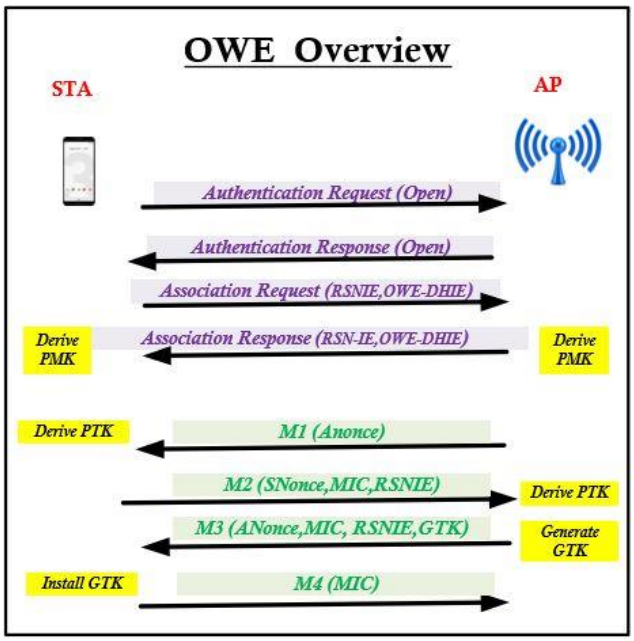
OPEN Networks:

These typically have a captive portal on them and there should be an acceptable use policy. If there is no AUP on the open network that should be a finding for an organization.

Open networks should have client Isolation turned on.

OWE (Opportunistic Wireless Encryption):

Is an extension to 802.11 that uses cryptographic handshake to encrypt the traffic from devices connecting to open network APs. In OWE, the key transfer happens in the Association frames. Both the AP and the client will transmit their public keys. The PMK is derived from its private key, the peer's public key, and the DH group. After the association frames are sent and both client and AP agree on OWE, a 4-way handshake is completed. OWE allows for PMK caching to speed up the process if a client has already associated to the AP. PMF is required for OWE.



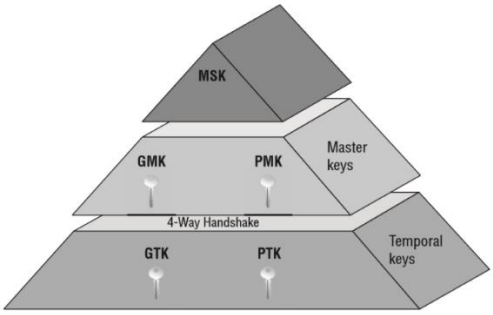
4-Way Handshake

Covered under 802.11i. The 4-way handshake is a process of exchanging messages which can be used to generate encryption keys.

Keys and terms used in the 4-way handshake:

- MSK (Master Session Key)
- PMK (Pairwise Master Key)
- GMK (Group Master Key)
- PTK (Pairwise Transient Key)
- GTK (Group Temporal Key)
- ANonce
- SNonce
- MIC

MSK: Master session key is the 1st key generated either from the 802.1X/EAP or derived from the PSK authentication.



PMK: Pairwise Master Key is generated from the Master Session Key. The PMK is used to help generate the PTK. In case of the WPA2/PSK the passphrase is converted into a 256-bit string and used as the PMK.

PMK = PBKDF2 (HMAC-SHA1, PSK, SSID, 4096, 256)

PMKID: This is used for roaming purposes. The networks will create the PMKID to ensure smooth roaming. This is vendor specific and not all ap will create the PMKID.

GMK: Group Master Key is used in a 4-way handshake to create the GTK.

PTK: is used to encrypt all unicast traffic between the client station and the ap. This key is unique for every client stations. To generate a PTK every client and ap need the following information:

PTK = PRF (PMK + ANonce + SNonce + AA(MAC) + SA(MAC))

ANonce: random number generated by the ap

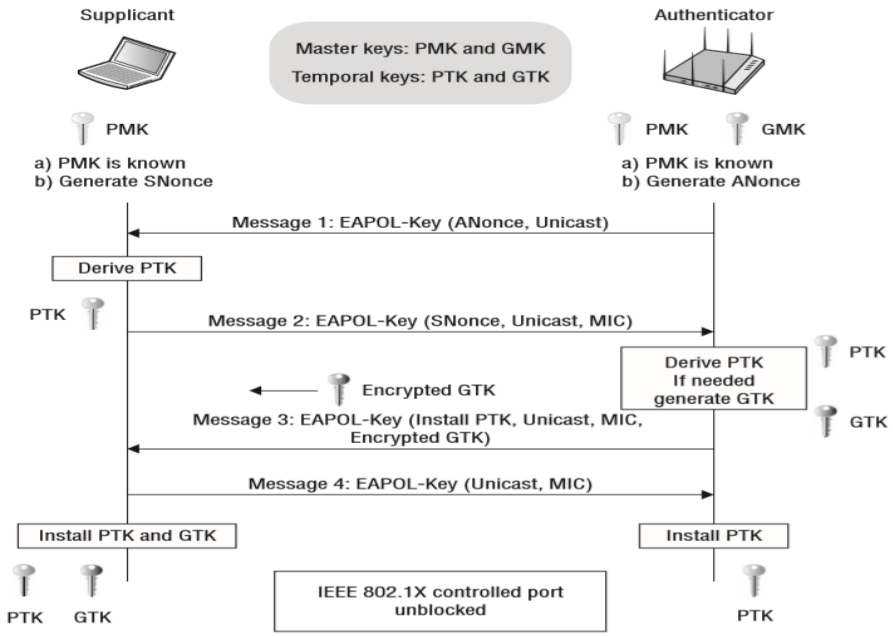
SNonce: random number generated by the supplicant (client station)

AA: Address of Authenticator (AP MAC)

SA: Address of Supplicant (Client station MAC)

PRF: pseudo-random function

PMK: Pairwise Master Key

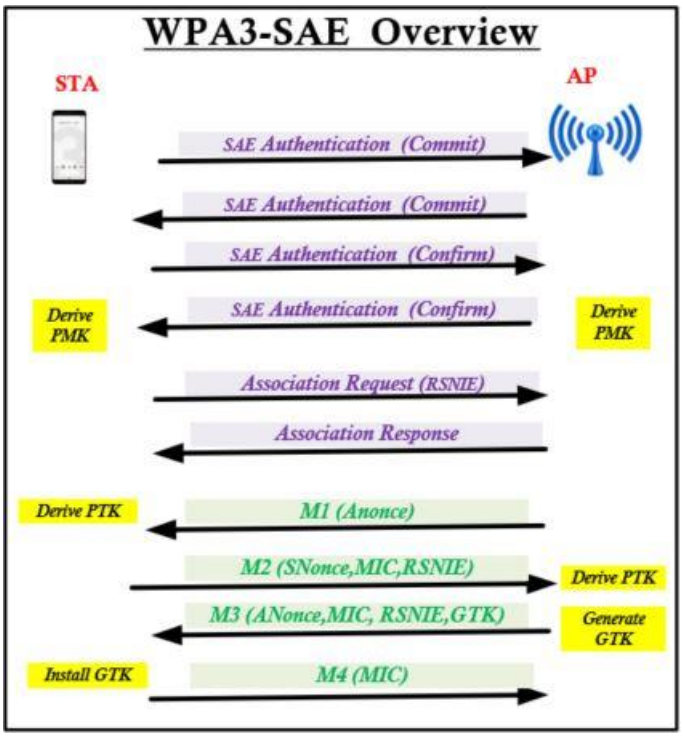


GTK: Group Temporal Key is used to encrypt all broadcast and multicast traffic between the ap and all the clients' devices on that specific ap. Every access point will create its own GTK. The **MIC (message integrity check)** is sent with the GTK to the client device. [4]

Simultaneous Authentication of Equals (SAE): In WPA2(4-way handshake), the PMK is dependent on the password. In WPA3(SAE) it is not. Another difference during authentication is that there are 4 authentication frames sent before the client is allowed to start the association process. Before the authentication process begins both sides will generate a PWE (password element) which is essential a public key. PMF is also required for SAE.

- Authentication: The first 2 authentication frames are called "Commits". The 1st commit is from the client and the second is from the AP. Both sides will transmit their Group ID, a Scalar, and a FFE (Finite Field Element). The FFE is "public key" and how the password is never transmitted. The next 2 authentication frames are "Confirm" frames. In these frames both a client and the AP send back a hash of the key to confirm they both have the same key. Once that is complete and successful the client will send an association request.
- Association: The request and the response are approximately the same
- 4-Way handshake: The 4-way handshake is very similar to the WPA2 version, the "Private Key" is the Passphrase both devices already known

[4] https://www.wifi-professionals.com/2019/01/4-way-handshake



Wi-Fi Security:

WEP 64 (risky): The old WEP protocol standard is vulnerable.

WEP 128 (risky): This is WEP, but with a larger encryption key size. It isn't any less vulnerable than WEP 64.

WPA-PSK (TKIP): This uses the original version of the WPA protocol (essentially WPA1). It has been superseded by WPA2 and is not secure. The password is 8-63 characters long or it can be entered in as a 64-bit hexadecimal key.

WPA-PSK (AES): This uses the original WPA protocol but replaces TKIP with the more modern AES encryption. It's offered as a stopgap, but devices that support AES will almost always support WPA2, while devices that require WPA will almost never support AES encryption. So, this option makes little sense. The password is 8-63 characters long or it can be entered in as a 64-bit hexadecimal key.

WPA2-PSK (TKIP): This uses the modern WPA2 standard with older TKIP encryption. This is not secure and is only a good idea if you have older devices that can't connect to a WPA2-PSK (AES) network. The password is 8-63 characters long or it can be entered in as a 64-bit hexadecimal key.

WPA2-PSK (AES): This is the most secure option. It uses WPA2, the latest Wi-Fi encryption standard, and the latest AES encryption protocol. On some devices, you'll just see the option "WPA2" or "WPA2-

PSK." If you do, it will probably just use AES, as that's a common-sense choice. The password is 8-63 characters long or it can be entered in as a 64-bit hexadecimal key.

WPAWPA2-PSK (TKIP/AES): Some devices offer—and even recommend—this mixed-mode option. This option enables both WPA and WPA2, with both TKIP and AES. This provides maximum compatibility with any ancient devices you might have, but also allows an attacker to breach your network by cracking the more vulnerable WPA and TKIP protocols.

WPA3-PSK(GCMP): Currently has a transition mode to make sure older devices can still access the AP. PMF is required in WPA3 and SAE protects the 4-way handshake even when a non-complex password is used.

EAP/802.1X: 802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server. The RADIUS server is able to do this by communicating with the organization's directory, typically over the LDAP or SAML protocol.

Common EAP types used with Wi-Fi:

EAP-TLS: client and server certificate required

TTLS(EAP-MSCHAP-v2): only server certificate, also normally requires a third-party application to be loaded on the clients using it.

PEAPv0(EAP-MSCHAP-v2): only server certificate

PEAPv0(EAP-TLS): client and server certificate required

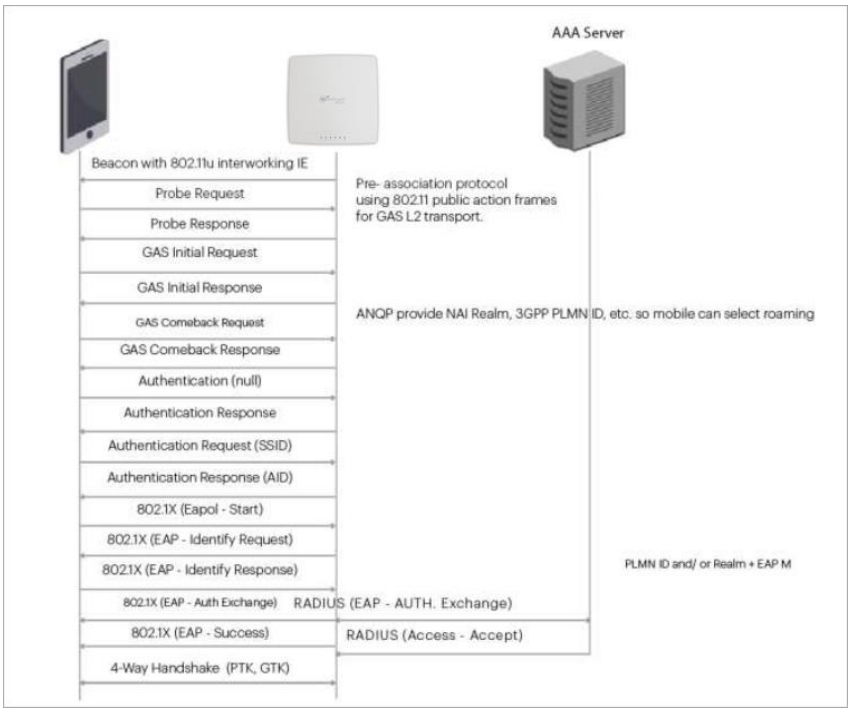
PEAPv1(EAP-GTC): used with token card and directory-based authentication systems and only server certificates required.

EAP-SIM: EAP for GSM Subscriber Identity Module- mobile communication

EAP-AKA: EAP for UMTS Subscriber Identity Module- mobile communication

Hotspot 2.0/ Wi-Fi Certified Pass point: Is a standard for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks. It is based on the IEEE 802.11u standard for interworking with external networks. With the advent of smart phones and tablets, the data consumption and strain on cellular networks has increased significantly. Hotspot 2.0 enables cellular network-like roaming that requires little or no manual intervention allowing users to automatically switch to a Wi-Fi network, whenever it is available, and free up the cellular network.[5]

[5] https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Wi-Fi-Cloud/manage_wirelessmanager/configuration/wifi_access/hotspot_2.0_settings.html


AAA Server
Beacon with 802.11u interworking IE
Probe Request
Probe Response
GAS Initial Request
GAS Initial Response
GAS Comeback Request
GAS Comeback Response
Authentication (null)
Authentication Response
Authentication Request (SSID)
Authentication Response (AID)
802.1X (Eapol - Start)
802.1X (EAP - Identify Request)
802.1X (EAP - Identify Response)
802.1X (EAP - Auth Exchange)
802.1X (EAP - Success)
4-Way Handshake (PTK, GTK)
Pre- association protocol
using 802.11 public action frames
for GAS L2 transport.
ANQP provide NAI Realm, 3GPP PLMN ID, etc. so mobile can select roaming
PLMN ID and/ or Realm + EAP M
RADIUS (EAP - AUTH. Exchange)
RADIUS (Access - Accept)

https://infocenter.nordicsemi.com/index.jsp?topic=%2Fug_nc_programmer%2FUG%2Fnrf_connect_programmer%2Fncp_programming_dongle.html

https://infocenter.nordicsemi.com/index.jsp?topic=%2Fug_sniffer_ble%2FUG%2Fsniffer_ble%2Fintro.html

References:

https://mrncciew.com/2019/11/29/wpa3-sae-mode/

https://tools.ietf.org/html/rfc8110

https://www.wi-fi.org/beacon/dan-harkins/wi-fi-certified-enhanced-open-transparent-wi-fi-protections-without-complexity

https://www.engeniustech.com/wi-fi-6e-how-the-unlicensed-6-ghz-spectrum-will-drive-innovation/

https://wificoops.com/2019/08/05/wi-fi-security-enhancements-part-2-enhanced-open-owe/

https://mrncciew.com/2019/11/21/enhanced-open-part-1/

https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11w_Management_Frame_Protection_MFP

https://www.mist.com/wpa3-just-the-essentials-on-the-latest-in-wi-fi-security/#:~:text=WPA3%20Personal%20(WPA%2D3%20SAE,personal%20authentication%20process%20of%20WPA3.

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Wi-Fi-Cloud/manage_wirelessmanager/configuration/wifi_access/hotspot_2.0_settings.html

https://github.com/s0lst1c3/s0lst1c3.github.io/blob/master/_posts/2019-09-10-eap-downgrade-attacks.md

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-get-anyones-wi-fi-password-without-cracking-using-wifiphisher-0165154/

https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wi-Fi_6_(802.11ax)_Technical_Guide

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Wi-Fi-Cloud/manage_wirelessmanager/configuration/wifi_access/hotspot_2.0_settings.html

https://mrncciew.com/2019/11/29/wpa3-sae-mode/

https://mrncciew.com/2014/10/03/cwap-mac-header-qos-control/

https://blogs.arubanetworks.com/industries/802-11-reason-codes-and-status-codes/

https://www.wi-fi.org/knowledge-center/faq/what-are-protected-management-frames#:~:text=Protected%20Management%20Frames%20(PMF)%20provide,frames%20are%20protected%20from%20forging.

https://www.elttam.com/blog/intro-sdr-and-rf-analysis/#content

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Wi-Fi_6_(802.11ax)_Technical_Guide

CWNA-107 Official Study Guide 5th Edition David D. Coleman, David A. Westcott

CWSP-206 Official Study Guide 1st Edition Tom Carpentar

802.11 Wireless Networks Definitive Guide 2nd Edition O'Reilly Matthew S. Gast

General Class License Manual For Ham Radio 9th Edition ARRL