General WLAN Concepts

Wireless Standards are created by the IEEE. The IEEE is responsible for generating a variety of technology standards to include information technology standards. The first 802.11 standard was released in 1997. Amendments are modification to the original standard or define new technologies, features, or capabilities.

Wi-Fi Alliance is an organization that provides certifications for interoperability of wireless devices and adherence to the 802.11 IEEE standards. Several Wi-Fi Alliance certifications are defined here:

Wi-Fi Protected Access (WPA): Pre-802.11i certification in response to original 802.11 security vulnerabilities. WPA was an interim solution until the 802.11i security amendment was released. WPA uses TKIP/RC4 encryption mechanisms.

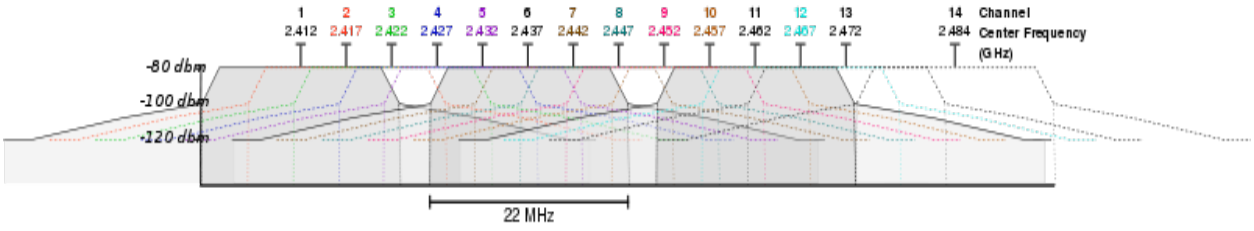
Wi-Fi Protected Access 2 (WPA2): Certification for 802.11i compliant wireless devices. WPA2 is backwards compatible with WPA and uses CCMP/AES encryption mechanisms.

Wi-Fi Multimedia (WMM): Certification for 802.11e amendment compliant devices which address Quality of Service (QoS) approaches to the delivery of time-sensitive, time-bounded applications such as voice and video.

Wi-Fi Multimedia Power Save (WMM-PS): Certification designed for mobile devices that require advanced power-save mechanisms to extend battery life in those mobile devices.

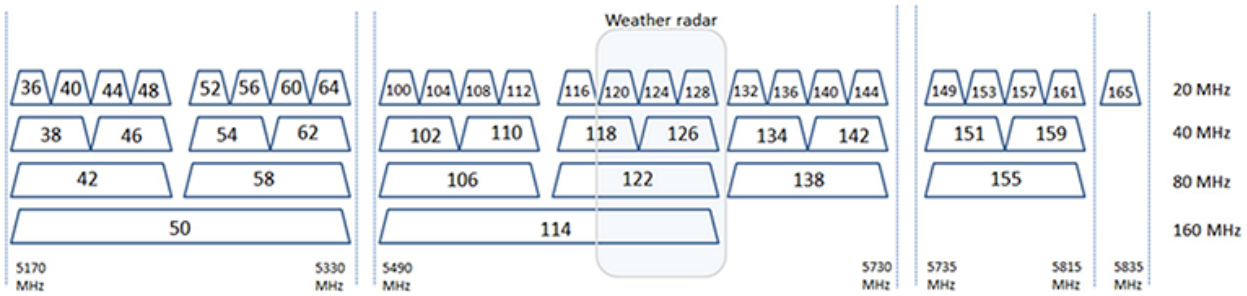
Wi-Fi Protected Setup (WPS): Certification for SOHO devices to ease connecting wireless devices to access points but still providing strong security with WPA/WPA2 mechanisms. WPS can be configured with a PIN-based or Push Button (PBC) configurations. Near Field Communications (NFC) is another option used with WPS.

2.4 GHz Spectrum



In the 2.4 GHz spectrum, channels 1, 6, and 11 do not overlap. Non-overlapping channels are those separated by at least 25 MHz. Each channel from 1-13 are separated by 5 MHz in this spectrum are 22 MHz wide.

5.0 GHz Spectrum



In the 5.0 GHz spectrum, all channels are 20 MHz wide and separated by 20 MHz on their center frequencies of each channel. Channel bonding allows for 40, 80, and 160 MHz wide channels in 802.11n and 802.11ac amendment technologies. Channel bonding increases throughput.

WLAN Terminology

Access Point (AP): device that allows wireless devices access to network resources. Access points can be configured or deployed by CLI or GUI.

Basic Service Set (BSS):

Extended Service Set (ESS):

Independent Basic Service Set (IBSS):

Basic Service Set Identifier (BSSID):

Service Set Identifier (SSID):

There are two main modes of operation for Wireless LANs, Infrastructure and Ad-hoc. *Ad-hoc* networks are also called a peer-to-peer or independent basic service set (IBSS). These ad-hoc networks consist of at least two stations communicating directly to each other without and access point. Both Ad-hoc and Infrastructure modes use a Service Set Identifier (SSID).

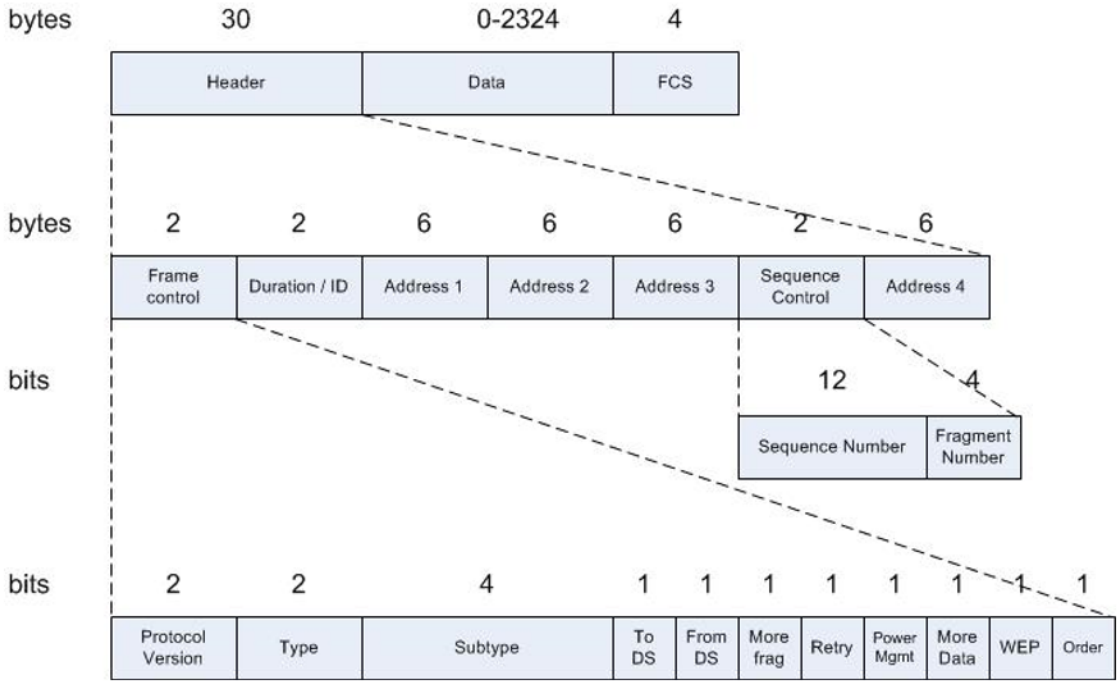
Infrastructure mode is a configuration that allows stations (STA) to connect to an access point (AP) which is in turn connected to a distribution system (DS). The DS connects to the network resources on the wired LAN side. The AP is also known as the portal to the DS. Client STAs connect to the DS and network resources through the AP. The DS can also provide a path to the Internet.

The Linux operating system has several utilities that allow the operating system and the wireless adapters to be configured in several modes. In infrastructure mode, a STA connecting to an AP is in *Managed* mode. When a Linux machine is configured to be an AP with other STAs connecting to it, it is referred to as being in *Master* mode.

Monitor mode allows a wireless card to monitor frames without filtering and can also sending raw 802.11 frames with some drivers. Monitor mode is the essentially the equivalent of *Promiscuous* mode on a wired network.

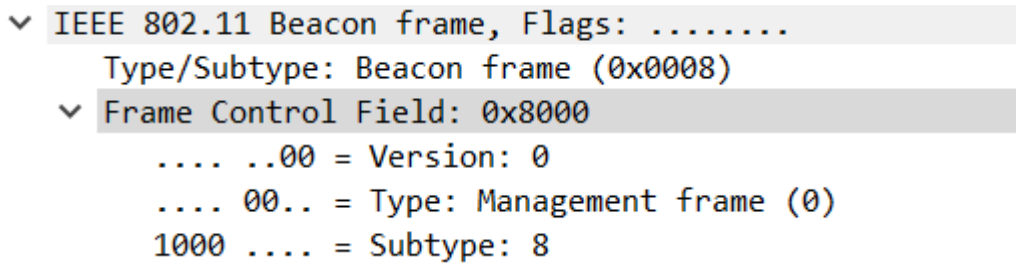
Frames

The following is a breakdown of a typical wireless frame. Each field is broken down further, here, beginning with the Frame Control field. An exemplar Beacon Frame is used to show the breakdown.



Frame Control (2 bytes in total):

> **Protocol Version (2 bits)** provides the version of the 802.11 protocol used. This value is currently 0.
>
> **Type and Subtype (6 bits)** determines the function of the frame. There are three different frame type fields: *control (value:1), data (value:2), and management (value:0)*. There are multiple subtype fields for each frame type and each subtype determines the specific function to perform for its associated frame type.



The next 8 bits are also known as the Flags and broken down here.

To DS and From DS (2 bits) indicates whether the frame is going into or exiting the distribution system.

More Fragments (1 bit) indicates whether more fragments of the frame are to follow.

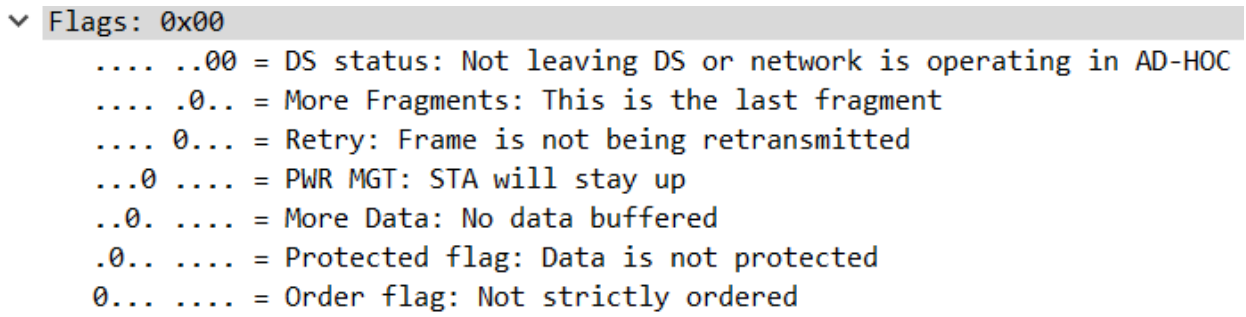
Retry (1 bit) indicates that the frame is being retransmitted.

Power Management (1 bit) indicates whether the sending STA is in active mode (value:0) or power-save mode (value:1).

More Data (1 bit) indicates to a STA in power-save mode that the AP has more frames to send. It is also used for APs to indicate that additional broadcast/multicast frames are to follow.

WEP/Privacy (1 bit) indicates whether or not encryption and authentication are used in the frame.

Order (1 bit) indicates that the frame is being sent using the Strictly-Ordered service class. Usually not set.



Duration/ID (2 bytes):

ID: Station Association ID (AID) used in Traffic Indicator Map (TIM) by an AP. When a STA associates with an AP, the STA is assigned an AID. The AID is used when data is buffered at the AP for a STA is in Power Save mode. A control beacon frame will use a TIM that will indicate which STAs by AID have data buffered at the AP.

Duration used for Network Allocation Vector (NAV) and also referred to as virtual carrier sense. When this section is used for a duration, it is the number of microseconds that the channel will allocated for successful transmission of the frame.

Addresses

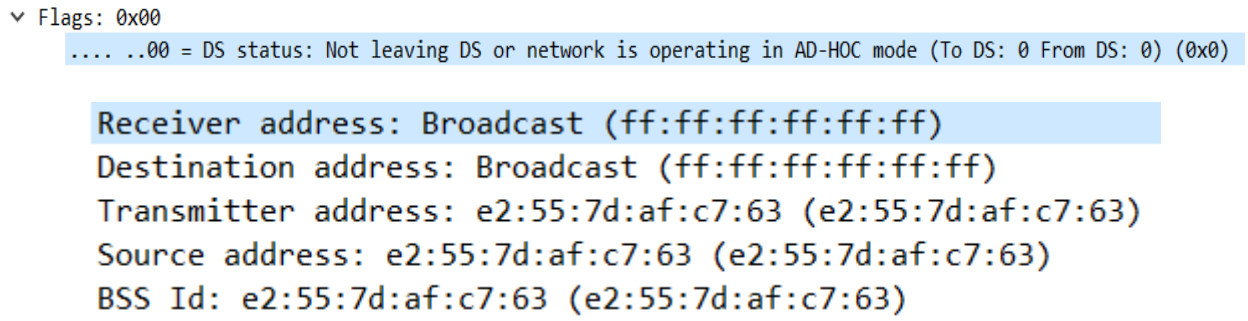
Two bits in four different combination will be used to identify how the addresses are used in the frame. These two bits are part of the Flags section when identified by a protocol analyzer. Up to four addresses can be used, but typically only three will be present. The fourth address is used in a wireless distribution system (WDS) configuration in a mesh design. In an ad-hoc network, there are no To DS or From DS addresses.

To DS	From DS	Address1	Address2	Address3	Address4
0	0	DA	SA	BSSID	X
0	1	DA	BSSID	SA	X
1	0	BSSID	SA	DA	X
1	1	RA	TA	DA	SA (WDS)

DA: Destination Address RA: Receiver Address

SA: Source Address TA: Transmitter Address

In the following frame, the Flags section indicates the first two bits are set as 00.



Sequence Control has two subfields:

Sequence number: can be any value from 0-4095 and used in a one-up manner, then repeats back at 0 after 4095 is used. The sequence number is the same for each frame sent in a fragmented frame.

Fragment number: Will be a value from 0-15 for each fragment in a fragmented frame.

```
.... .... .... 0000 = Fragment number: 0
0000 0110 1001 .... = Sequence number: 105
```

Data can be up to 2304 bytes in size + any encryption overhead. The Data is also referred to as the MAC Service Data Unit (MSDU).

WEP: 8 bytes of overhead

TKIP: 20 bytes of overhead

CCMP: 16 bytes of overhead

Frame Check Sequence (32 bits) is the Cyclic Redundancy Check of the frame.

More on Frames

There are three main types of wireless frames, Management, Control, and Data**.** Within each type are several subtypes and each subtype is dependent on the main type.

Management frames are used to manage STA access to the WLAN.

Control frames control access to the medium or in our case, the RF channel.

Data frames carry payload from upper layers 3-7 of the OSI model.

Acknowledgment frames contain only three fields. Frame Control, Duration, and Receiver Address. The Duration is set to 0 if acknowledging a complete frame or frame burst. The receiver address is the MAC address of the original sender or the frame or frame burst. If the original transmitter does not receive an acknowledgment, it is assumed the intended recipient never got it or was corrupted. The original transmitter will then retransmit the frame. Note that Acknowledgments are not used in response to broadcast or multicast frames.

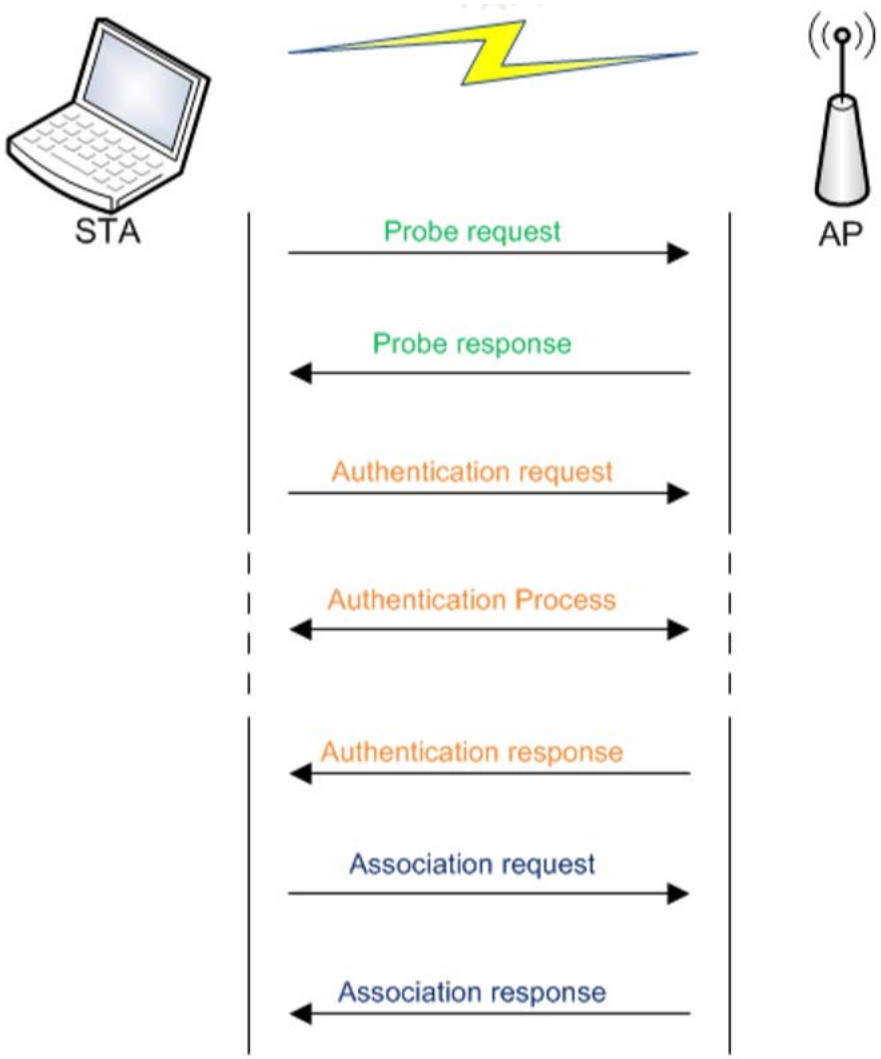
Beacon frames are very common frames seen in 802.11 frame traffic. They are used to broadcast the name of the WLAN, capabilities, data rates, and so on supported by the AP that STAs must also support if they are to associate. Beacons are sent out by default at about 10 per second. An AP that is hiding its SSID will not include the SSID. Beacons are one way that a STA can learn about nearby APs from the AP.

STAs can also learn about nearby WLANs by broadcasting a *probe request* with the destination address set as all FFs. APs in range of the probe request will respond with a *probe response* and information about the APs WLAN capabilities, data rates, and so on. A STA can also send out a broadcasted probe request but ask for a specific SSID. These probe requests for specific SSIDs are attempts to find WLANs that the STA was previously connected to once before. Keep in

mind that although a STA may be authenticated and associated with an AP and part of a BSS, the STA will go off channel looking for other WLANs. This off-channel behavior is what aids in roaming and searching for the strongest signal AP that meets the STA's capabilities.

Action frames are a result of the 802.11h amendment. Action frames are used for spectrum management in newer WLAN technologies such as 802.11ac.

Authentication and Association. The following is a simplification of the Authentication and Association steps.



Most modern wireless networks use WPA/WPA2 in either Personal or Enterprise configurations. Some networks will still WEP. Wired equivalent Privacy is often used where STAs do not support the more intensive WPA/WPA2 encryption algorithms because of hardware limitations. These WEP only STAs are often older devices such as scanners used in manufacturing and inventory control processes. Legacy WEP only voice handsets are still used out in the wild.

Authentication can take one of two forms, *Shared Key and Open System Authen*tication. Do not confuse Shared Key Authentication with the term Pre-Shared Key (PSK) or its use in WPA/WPA2 personal modes.

Open authentication is used in WPA/WPA2 networks and does not fail. An authentication response from the AP is successful if the AP and client are compatible. Open authentication relies on other mechanisms to generate encryptions keys used to encrypt WLAN 802.11 traffic.

This is followed by an *Association Request* from the STA to the AP. Again, if the two are compatible, the AP will respond with a successful *Association Response.*

From this point, the STA is assigned an IP address and provided other network information through the DHCP processes.

Encryption. Open WLAN traffic is easily eavesdropped upon because no encryption of traffic frames is occurring. Everything is in clear text; however, upper layer protocols can provide encryption if it is part of their protocol suite, e.g. HTTPS and SSH.

WEP uses and RC4 (ARC4) algorithm and was an attempt to provide the equivalent privacy or a wired infrastructure. WEP was part of the original legacy 802.11 standard. WEP uses either 64 or 128-bit length keys, however part of the key space uses an initialization vector (IV) or 24 bits. This essentially led to key lengths of 40 and 104 bits. The weakness with WEP involves the reuse of IV which can occur in about 10,000 frames. IV reuse allows an attacker to compare two cipher text outputs encrypted with the same IV and key. WEP can still be found out in the wild in networks that still use legacy devices that simply do not have the firmware to support the advance encryption algorithms.

WPA Personal still uses RC4 (ARC4) algorithms but in conjunction with Temporal Key Integrity Protocol (TKIP). As the name implies, TKIP, is time based. WPA is a pre-802.11i implementation to overcome WEP insecurity. *WPA Enterpri*se uses an 802.1X port-based access control mechanism, Extensible Authentication Protocol (EAP) in conjunction with an Authentication Server such as RADIUS (Remote Authentication and Dial-in User Service).

WPA2 Personal uses AES in conjunction with CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). AES is mandatory in WPA2 Personal networks, but TKIP is optional.

WPA2 Personal and Enterprise are full implementations of the 802.11i amendment and are considered Robust Security Networks (RSN).

After association, keys distribution and verification occur. Keys are created uniquely for each AP and STA pairing. This is referred to a the *4-way handshake*. During this handshake, the Pairwise Transient Key (PTK) and Group Temporal Key (GTK) are exchanged. The PTK is used for unicast frames and the GTK is used for multicast and broadcast data.

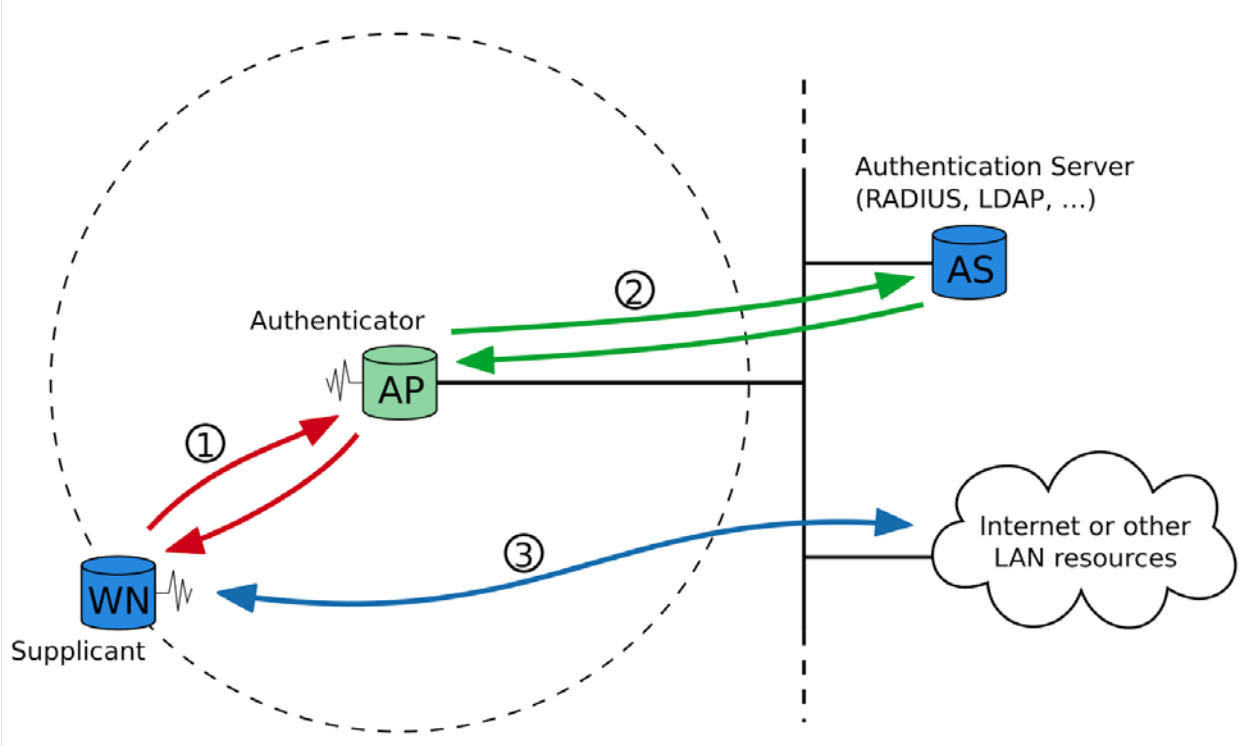
With regard to WPA and WPA2 networks, the *Supplicant* is the STA requesting access to the WLAN. The *Authenticator* is the device that attempts to authenticate the supplicant.

The generation of the PTK requires 5 pieces of data, the Pairwise Master Key (PMK), the Authenticator Nonce (*Anonce*), the Supplicant Nonce (*Snonce*), the STA MAC address, and the AP MAC address. Each nonce is a random number generated by the supplicant and authenticator, respectively. Using these 5 pieces of data leads to a unique STA-AP key pairing.

The PMK is the 256-bit key created from an 8-63 ASCII case-sensitive characters or 64 hexadecimal character WPA/WPA2 Personal pre-shared key.

Wi-Fi Protected Setup (WPS) and *Push Button Configuration (PBC)* are Small Office Home Office solutions to simplify the process of securing a wireless network. WPS uses an eight digit PIN to be entered on all devices that will be part of the same WLAN if WPS is used as the alternative to a pre-shared key. The PIN can be dynamically generated or pre-configured in the AP settings.

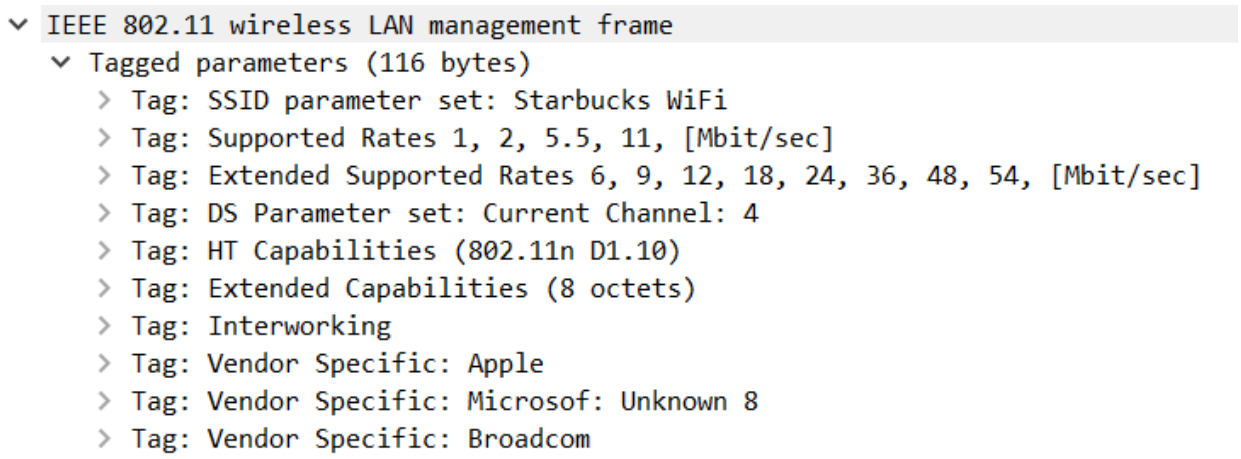
WPA Enterprise and WPA2 Enterprise uses *802.1X/EAP* port based authentication to authenticate users. A central *Authentication Server* is used to authenticate users, devices, or both. The authentication server can be a RADIUS or a AAA authentication server. AAA is Authentication, Authorization, and Accountability. The authentication server will authenticate the wireless client supplicant (STA) through the AP (authenticator). 802.1X is a framework that allows for an authentication process to occur. An Extensible Authentication Protocol (EAP) type is used to complete the authentication process. An example of an EAP types is EAP-Transport Layer Security (EAP-TLS). EAP types allow users to authenticate using credential such as username/password or certificates. After a user or device is authenticated, network resources can be accessed.



802.1X/EAP. The process begins after the STA associates to the AP. The supplicant begins the authentication process by sending an EAP Over LAN (EAPOL) Start message to the authenticator. The authenticator then sends an EAP Identity Request to the supplicant. The supplicant replies with an EAP Identity Response to the authenticator. The EAP Identity Response is forward from the AP to the authentication server in the proper protocol (e.g. RADIUS) to communicate with the authentication server in the form of an Access Request. An Access Challenge is sent from the authentication server back to the authenticator. From the authenticator, the challenge is sent to the supplicant in the form of a EAP Credentials Request. The supplicant responds to the authenticator (AP) with an EAP Credentials Response. The response is sent to the authentication server from the authenticator. The AAA or RADIUS server verifies the credentials or certificate. Verification can be accomplished with Windows Active Directory or another database. If verification is successful, the authentication server responds with an Access-Accept back to the authenticator. If verification fails, an Access-Reject is sent. The authenticator forwards an EAP Success to the supplicant. The authenticator then authorizes the port to send normal network traffic and allows the supplicant access to network resources.

Open Networks such as those found in public Wi-Fi hotspots use no encryption and rely on upper layer protocols for privacy and encryption, e.g. HTTPS and SSH.

More examples of probe requests sent out by a STA on all channels in a broadcast. An AP will respond in a unicast frame to the STA with its capabilities. The following is a probe request for “Starbucks WiFi” on channel 4.



The following is a probe request sent out to the broadcast address on channel 1 for any AP listening.

```
IEEE 802.11 wireless LAN management frame
  Tagged parameters (129 bytes)
    Tag: SSID parameter set: Broadcast
    Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
    Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 1
    Tag: HT Capabilities (802.11n D1.10)
    Tag: Extended Capabilities (4 octets)
    Tag: Vendor Specific: Apple
    Tag: Interworking
    Tag: Vendor Specific: Broadcom
    Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
```

And the **probe response** from “BaguetteCampus” to the previous request:

```
Tagged parameters (242 bytes)
  Tag: SSID parameter set: BaguetteCampus
  Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
  Tag: DS Parameter set: Current Channel: 1
  Tag: Country Information: Country Code US, Environment Any
  Tag: Power Constraint: 0
  Tag: TPC Report Transmit Power: 21, Link Margin: 0
  Tag: ERP Information
  Tag: ERP Information
  Tag: RSN Information
  Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
  Tag: AP Channel Report: Operating Class 12, Channel List : 1, 2, 6, 8, 11,
```

Null data frames contain no upper layer payloads and are used by a STA to inform the AP that it is going into PS mode or is awake (Continuous Aware Mode).

```
Flags: 0x11
    .... ..01 = DS status: Frame from STA to DS via an AP
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...1 .... = PWR MGT: STA will go to sleep
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0... .... = Order flag: Not strictly ordered
```

RF Measurements

There are two categories of RF measurements, absolute and relative.

Absolute: Absolute measurements are used to identify the actual power output of a device. The watt is the unit of measure for power. A dBm is a value compared to 1 milliwatt (mW). A milliwatt is another absolute power measurement and is one thousandths of a watt. Futhermore, 0 dBm is 1 mW and 30 dBm is 1,000 mW or 1 Watt.

Relative: Measurements that compare one power to another. A decibel (dB) is a relative measurement. A decibel isotropic (dBi) refers to the gain of an antenna as compared to a hypothetical isotropic antenna which distributes energy equally in all directions. A decibel dipole (dBd) refers to the gain of an antenna as compared to a half-wave dipole antenna.

dBi = dBd + 2.15

Rule of 3s and 10s. An increase in 3 dBm doubles the power output. An increase in 10 dBm is a 10-fold increase in power output. The opposite is also true: an drop in 3dBm halves the power output and a 10 dBm drop equates to 1/10 the original power output.

A 6 dB increase or decrease results in a doubling or halving of distance, respectively.

RF Math and Concepts

Each connector adds about 0.5 dB insertion loss. Minimize cable segments and opt for single lengths of cables. Use cable loss calculators to determine insertion loss based on cable type and length. Timesmicrowave.com/calculator.

Signal-to-noise ratio (SNR): Difference between the received signal and the noise floor or background noise. SNR of 25 dB is good. 10 dB or less is poor.

Received Signal Strength Indicator (RSSI): Vendor defined measurement of signal strength. Used by devices to make roaming decisions and dynamic rate switching.

Link budget: Sum of all losses and gains through the RF medium including air and free space path loss. All active and passive gains and insertion loss are accounted for in the budget. The goal is to determine if the received signal is above the receiver's sensitivity threshold.

Fade margin: expression of how much margin in dB there is between the received signal strength and the receiver's sensitivity threshold. Common practice is 10-25 dB above the receiver's threshold.

Less than 3 miles: 10 dB

From 3 to 5 miles: 15 dB

Greater than 5 miles: 25 dB

System operating margin (SOM): The actual measured buffer after the link budget is calculated and fade margin determined.

Fresnel zone: Football shape of RF in point-to-point links. Infinite concentric ellipsoids with the center or inner most one named the first Fresnel Zone. The first zone must be 60% or greater unobstructed. Based on frequency and distance and has no influence from the antenna beamwidth. Calculation of the Fresnel zone is used to determine minimum antenna height.

Free Space Path Loss (FSPL): Based on frequency and distance. It is a measure of signal strength loss as an electromagnetic wave travels through a free space, or air. FSPL is a component used in calculating a link budget.

Antennas

Omni-directional. Dipoles, rubber ducks. Used indoors on access points. Outdoor usage in P-t-M-P links. The higher the passive gain of an omni-directional, the narrower the elevation plane. Think of a flattened donut as opposed to an intact one.

Semi-directional. Planar (patch and panel), Yagi, Cantenna. Used in short to medium distances outdoors typically up to two miles. Indoor usage for coverage to help minimize MIMO effects, down long hallways, or in retail spaces with aisles or racks.

Highly directional. Parabolic dishes and grids. Used in P-t-P links in distances greater than a few miles typically up to 5 miles.

WLAN Network Discovery

Active Scanning: Consists of broadcasted probes across many channels or directed broadcast to specific SSIDs sent from the STA or device. Active scanning sends Probe Request in an attempt to elicit a Probe Response from an AP.

Passive Scanning: Listening in a monitor or managed mode on the interface adapter. Passive scanning is listening for Beacon frames.

Active and passive scanning occur all the time whether the STA is connected to an AP in a BSS. This is often referred to as off-channel scanning. Beacons and probes are management type frames.

Tools

Aircrack-ng: Aircrack-ng is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security: Monitoring, Attacking, Testing, and Cracking.

Airmon-ng: Is a script that can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. Entering the airmon-ng command without parameters will show the interfaces status.

Airodump-ng: Used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng. If you

have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points. Additionally, airodump-ng writes out several files containing the details of all access points and clients seen

Airgraph-ng: Creates a graphic of the wireless network.

Aireplay-ng: The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys. There are different attacks which can cause deauthentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection. With the packetforge-ng tool it's possible to create arbitrary frames.

GPSd: A daemon that receives data from a GPS receiver, and provides the data back to multiple applications such as Kismet or Airodump-ng.

Wash: Utility that will list APs by BSSID and list any WPS version information. In addition to the WPS information, the state of the WPS process on the AP can be determined as locked or not. The WPS version information can then be used to target APs for brute force WPS PIN attacks with Reaver.

Reaver: Command line tool that implements a brute force attack against Wifi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases.

Kismet: A wireless network detector, sniffer, and intrusion detection system. Kismet works predominately with Wi-Fi (IEEE 802.11) networks, but can be expanded via plug-ins to handle other network types. Kismet identifies networks by passively collecting packets and detecting networks, which allows it to detect (and given time, expose the names of) hidden networks and the presence of non-beaconing networks via data traffic.

Wireshark: Network protocol analyzer that can do live capture from a network interface or offline analysis from a variety of capture files.

Ettercap: A comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

WAIDPS: Wireless Auditing, Intrusion Detection & Prevention System is a tool that can help gather information about wireless networks and clients.

Foremost: File carving tool originally designed for extracting files from disk images used in forensics processes. Foremost can parse through reassembled data streams from TCPFlow.

TCPFlow: Utility that can parse a network capture for data streams and reassemble them into individual files.

Commands

View Network Interfaces and Wireless Interfaces

```
# ifconfig -a

# iwconfig
```

Changing the MAC address of a Network Interface

Sometimes it may be necessary to change the MAC address of an interface because a target has applied a legacy security practice of MAC filtering which should only allow specific MAC addresses on a white list to connect to the AP or network. Capturing raw 802.11 traffic frames will identify which STA MACs are connected to the AP are could be thought of as being on a whitelist. As a pentester, you can change the MAC address to spoof a legitimate MAC of the network.

```
# macchanger -m <MAC> <adapter>
```

Scanning for Access Points

In managed mode, you should be able to view nearby APs with iwlist.

```
# iwlist <wireless interface> scan
```

Enable Monitor Mode for a Wireless Interface

Monitor mode is equivalent to promiscuous mode on the wired side of networking. This will allow us to capture the 802.11 traffic but only at layer 1 and 2. The MSDU data payloads from layers 3-7 will not be captured.

To view the available wireless cards you can use airmon-ng:

```
# airmon-ng
```

You can enable monitor mode for a wireless card using airmon-ng. It will create a new interface from the original, e.g. wlan0mon from the original wlan0. Use the “check kill” arguments to kill off network services that will interfere with monitor mode.

```
# airmon-ng check kill

# airmon-ng start <wireless interface>
```

The resulting new interface will be used as the monitor interface with other tools.

Capturing Packets in Monitor Mode

Monitor mode allows the wireless interface card to capture raw layer 1 and 2 802.11 frames. Airodump-ng allow you to capture and save packets that can be analyzed later with other tools such as Wireshark.

```
# airmon-ng --channel <channel> --wps --write <output file
prefix> --manufacturer <wireless monitor mode interface>
```

To target a specific AP using its BSSID:

```
# airmon-ng --channel <channel> --write <output file prefix> --
BSSID <wireless monitor mode interface>
```

Exploitation

Wireless Cracking General Steps

WEP

- Use a monitor mode enabled adapter to identify a WEP supported access point with a client connected to it. Run `Airodump` which will display a "CIPHER" column that can show WEP, TKIP, and CCMP. In the lower portion of the `airodump` will be displayed "STATION" and "BSSID." Stations will be connected to BSSIDs if they are a part of the BSS.
- Use `airodump` to target the BSSID by MAC and channel and write the output to a file.
- To generate enough frames with reused IVs, use `aireplay` in a different terminal with `airodump` running. This will capture re-inject ARP packets from `aireplay`.
- Once a large amount, e.g. several thousand, of ARP data packets are captured, run `aircrack` and point it at the `.cap` capture file being written by `airodump`.

WPA/WPA2 Personal

- Ideally, capturing a 4-way handshake is the best. However, not all 4 parts are necessary. Use a monitor mode enabled adapter to identify a WPA supported access point with a client connected to it. Run `Airodump`, it will display a "CIPHER" column that can show WEP, TKIP, and CCMP. In the lower portion of the `airodump` will be displayed "STATION" and "BSSID." Stations will be connected to BSSIDs if they are a part of the BSS.
- Use `airodump` to target the BSSID by MAC and channel and write the output to a file.
- Wait for a client to connect to the AP so you can capture the 4-way handshake, or force an already connected client off momentarily with a deauthentication frame. This quick deauth will likely go unnoticed. The deauth can be accomplished in a different terminal other than the one running `airodump`.
- The `airodump` terminal should display at the top that a 4-way handshake was captured if successful.
- Stop the capture and open up the `.cap` file in Wireshark. Once in Wireshark, look for the EAPOL messages (1-4) to verify capturing a 4-way handshake.
- Use `aircrack` against the capture file and use a wordlist that may contain a passphrase used as the passphrase for the target network.

- Speeding up the process can be accomplished by pre-generating pre-shared keys using the passphrases in a list and the target SSID. Both are passed through a tool, `genpmk`.

WPS

- Use a monitor mode enabled adapter along with `airodump` to identify WPS enabled BSS. Targeting WPS version 1.0 access points works well. Another alternative to using airodump is `wash`. The key piece of information is the BSSID of a network we want to pentest.

- Once you have a target BSSID, use another tool, `reaver` to being the WPS PIN brute-force attack. Slowing down the attempts and putting `reaver` to sleep after 10 tries will help ensure your attack does not reboot the AP or lock the WPS feature.

- Be patient. This slow and low attack could take many hours or a few days. If successful, the Pre-shared key and PIN will be displayed to you. Note, that you can stop and resume `reaver` where it left off.

Attacks

Infrastructure Attacks

Evil Twin. Introduction of an attacker controlled AP in the hearing vicinity of a target WLAN. The attacker controlled AP is used to imitate a legitimate WLAN AP. In other words, to beacon and advertise the same SSID or ESSID as the target WLAN. An unsuspecting user could connect to the evil twin AP thinking it belongs the true target WLAN. Evil twins are used to further conduct man-in-the-middle attacks to relay traffic to and from the legitimate STA and WLAN while at the same time, trying to eavesdrop on the communications. `Airbase` is part of the `Aircrack` suite and facilitates the establishment of evil twins.

Rogue Access Points. An unauthorized access point connected to an authorized network. Rogue access points can allow unauthorized, unchecked, and/or uncontrolled access to an internal network. This type of device could then allow the bypassing of security controls such as encryption, firewalls, and intrusion detection systems. A laptop with both wired and wireless network interface adapters could bridge potential wireless STAs through the laptop into authorized network via a wired connection. `Airbase` is used to create the rogue access point and `bridge-utils` is used to bridge the interfaces. IP forwarding also has to be enabled.

Client Attacks

Dissassociation and Deauthentication. Although the 802.11w amendment introduce protected management frames, it is still possible to kick STAs off an AP with deauth and disassociation frames since neither frame types is a request. Aireplay is a tool that can generate such frames targeted STAs while masquerading as the legitimate AP and its BSSID.

Traffic Analysis

Wireshark is great tool to conduct traffic analysis. It can also be used to capture raw 802.11 frames and upper layer protocols real time or examine a variety of capture file formats. It is a best practice to not run Wireshark in a privileged or root context. Any code captured and reassembled during analysis could execute with the privileges of the user running Wireshark, e.g. malware.

Statistics can be viewed with Wireshark. Conversations between end points, addresses, and top protocol usage are just a few points that Wireshark can help aggregate for analysis.

Cracked encryption Pre-shared keys can be used to decrypt previous captures if the data was encrypted with the PSK. Files that were transferred over a medium such as RF can be carved out of reassembled frames and upper layer packets once decrypted with Wireshark as well. TShark is a companion command line tool for Wireshark. Wireshark has an "export object" selection under the File menu list which can export files from HTTP, SMB, and DICOM protocols. The alternative to file extraction is to select the correct data stream and save the "raw" interpretation of the stream.

Another tool that can visually display information about a network is `airgraph`. It can use a capture file to generate a visual network graphic which is helpful when compiling a final report on your activities and methods.

Wireshark Filters

Select only frames from a BSSID	wlan.bssid == <BSSID>
Sort on Frame Control Types	wlan.fc.type == #
Sort on Frame Control Subtypes	wlan.fc.type_subtype == #
Management frames	wlan.fc.type == 0
Control frames	wlan.fc.type == 1
Data frames	wlan.fc.type == 2
Association request	wlan.fc.type_subtype == 0
Association response	wlan.fc.type_subtype == 1
Reassociation request	wlan.fc.type_subtype == 2
Reassociation response	wlan.fc.type_subtype == 3
Probe request	wlan.fc.type_subtype == 4
Probe response	wlan.fc.type_subtype == 5
Beacon	wlan.fc.type_subtype == 8
Announcement traffic indication map (ATIM)	wlan.fc.type_subtype == 9
Disassociate	wlan.fc.type_subtype == 10
Authentication	wlan.fc.type_subtype == 11
Deauthentication	wlan.fc.type_subtype == 12
Action frames	wlan.fc.type_subtype == 13
Block ACK Request	wlan.fc.type_subtype == 24
Block ACK	wlan.fc.type_subtype == 25
Power-Save Poll	wlan.fc.type_subtype == 26
Request to Send	wlan.fc.type_subtype == 27
Clear to Send	wlan.fc.type_subtype == 28
ACK	wlan.fc.type_subtype == 29