# How WiFi Connection Works

By [Stefano Gridelli](https://netbeez.net/blog/author/stefano/" \o "Posts by Stefano Gridelli)June 26, 2019[NetBeez](https://netbeez.net/blog/category/netbeez/), [Network Monitoring](https://netbeez.net/blog/category/network-monitoring/)

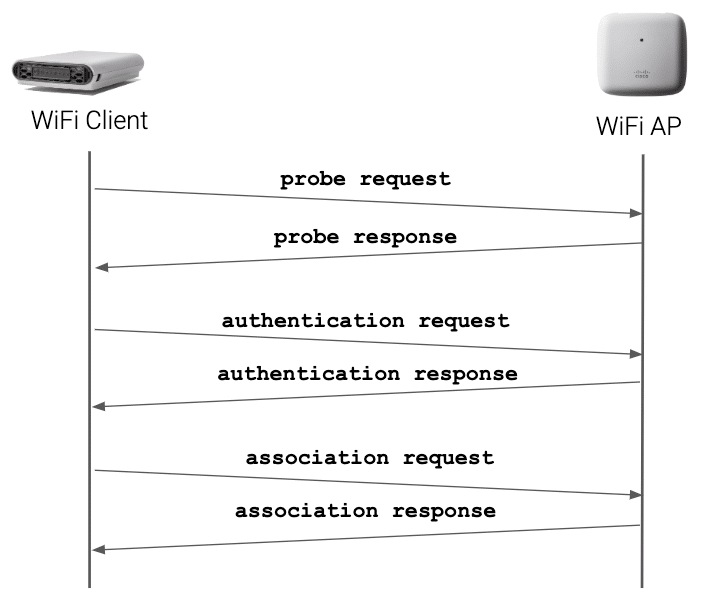
## WiFi Connections

To better understand how a WiFi client connects to a wireless network, it’s worth familiarizing yourself with two client processes. The first one being WPA supplicant.  WPA stands for ‘WiFi Protected Access’. The second one is the DHCP client, in which DHCP stands for ‘Dynamic Host Configuration Protocol’. Let’s see how these two system processes come into play.

The WPA supplicant process handles the *802.11 Authentication and Association* of the client with a BSSID. The *802.11 Authentication and Association* is then followed by the 4-way handshake, which establishes a secure and authenticated channel between the client and the access point. Once that step is completed, the DHCP client requests a dynamic IP address that is used to connect to the network and exchange communication with the outside world.

## 802.11 Authentication and Association

At the beginning of the 802.11 Authentication and Association process, the client scans all of the available frequencies in search of SSIDs to join. The client sends probe request frames which contain supported data rates and 802.11 capabilities. Access points in proximity reply with probe response frames that contain the SSID and BSSID, which corresponds to the access point’s MAC address.



When the client finds an SSID that matches its configuration, it will send an authentication request probe. Important to note is that the authentication request and response probes exchanged in this phase don’t provide encryption. That function is implemented by the 4-way handshake. Here, the authentication request and response exchange is only used to register the client’s MAC address. This information is also used in case MAC filtering is implemented. If the client is allowed to connect to the network, it will associate to the access point with the stronger signal.

Our friend, Rowell Dionicio (host of ‘Clear to Send’ podcast), wrote a more detailed article on the [802.11 Authentication and Association](https://netbeez.net/blog/station-authentication-association/" \t "/home/bleach/Documents\\x/_blank) process. Once the 802.11 Authentication and Association process is completed, the WPA supplicant client initiates the 4-way handshake.

## The 4-way Handshake Phase

The 4-way handshake is used to authenticate the WiFi client and encrypt all communications with the access point. The handshake is established by exchanging EAPoL frames between the WPA supplicant running on the client and the authenticator running on the access point.

If the SSID is configured with WPA2-Personal, the 4-way handshake uses a pre-shared key. If the SSID is configured with WPA2-Enterprise, the client will also execute an EAP transaction with an 802.1x authentication server (Radius). Here, I won’t cover in detail how the 4-way handshake process works, but if you want to learn more about the [4-way handshake](https://netbeez.net/blog/secure-network-4-way-handshake/" \t "/home/bleach/Documents\\x/_blank), I have linked another article written by Rowell Dionicio. If you want to learn more about 802.1x, check out the [802.1x Wikipedia page](https://en.wikipedia.org/wiki/IEEE_802.1X" \t "/home/bleach/Documents\\x/_blank), and the page [on the IANA website about EAP methods](https://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml" \l "eap-numbers-4" \t "/home/bleach/Documents\\x/_blank).

Once the 4-was handshake is completed, the client can now request an IP address to complete the WiFi connection.

## Reading WPA Supplicant Logs

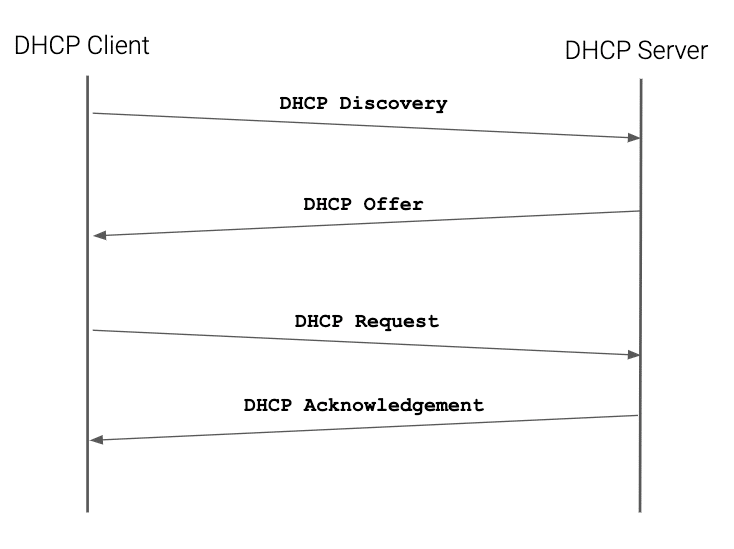
In Linux, the 802.11 Authentication and Association and the 4-way handshake are handled by the WPA supplicant process. The following table reports the different stage transitions that are logged by WPA supplicant. The default location of the file on many Linux distributions is /var/log/wpa\_supplicant/wpa\_supplicant.log.

|  |  |
| --- | --- |
| **State transition logged** | **Meaning** |
| SCANNING -> ASSOCIATING | The WiFi client has completed the scan and has initiated the 802.11 Authentication and Association |
| ASSOCIATING -> ASSOCIATED | The 802.11 Authentication and Association process is completed |
| ASSOCIATED -> 4WAY\_HANDSHAKE | The WiFi client has begun the 4-way handshake |
| 4WAY\_HANDSHAKE -> 4WAY\_HANDSHAKE | The 4-way handshake is occurring |
| 4WAY\_HANDSHAKE -> GROUP\_HANDSHAKE | The 4-way handshake is completed and the exchange of the group keys has begun |
| GROUP\_HANDSHAKE -> COMPLETED | The group keys exchange is completed |

If you want to learn more about [reading WPA logs](https://netbeez.net/blog/linux-wireless-engineers-read-wpa-supplicant-logs/" \t "/home/bleach/Documents\\x/_blank) in Linux, check out the article I have linked written by Panos Vouzis.

## Getting a DHCP address via D-O-R-A

Once the 4-way handshake is completed, the client moves to the “network phase” of the connection to request a dynamic IP address. Getting a DHCP address for WiFi clients is the same process as it is for Ethernet ones. The DHCP transaction between the DHCP client and the server is called D-O-R-A. This acronym relates to the frames exchanged during the transaction between client and server (see below image).

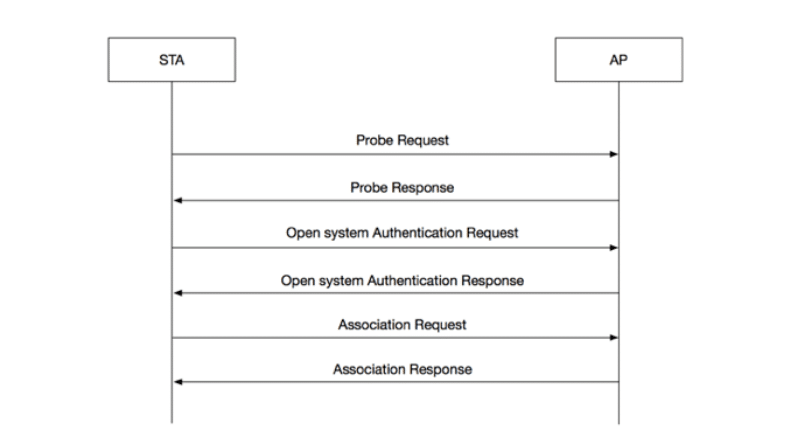


WiFi connections happen in a matter of microseconds. Within that small time frame, there are many frame exchanges occurring between a station and access point. Beacon frames are transmitted at an interval to allow passive or active scanning stations to join a particular WiFi network.

For a station to successfully join a WiFi network, a series of frame exchanges must occur which make up the Authentication and Association process, the 802.11 State Machine. The frames part of this transaction are as follows:

* Probe Request
* Probe Response
* Authentication Request
* Authentication Response
* Association Request
* Association Response

The sequence of frames exchanged are displayed in the graphic below:



The transaction begins with a DHCP discovery frame. Here, the DHCP client sends broadcasts to all the hosts in the local subnet. If a DHCP server is available, it will reply with a DHCP offer containing an IP address available for use. The client then verifies with an ARP lookup that no other hosts are improperly using the address offered by the server. If no other host replies to the ARP request, the client confirms the intent to use that IP with a DHCP request. The DHCP server acknowledges the IP address confirming with a DHCP acknowledgement. That marks the end of the D-O-R-A transaction.

## Reading DHCP logs

This section will help you troubleshoot DHCP issues on a WiFi client running Linux. If it’s not enabled yet, it’s recommended that you can configure the dhclient to log messages on /var/log/dhcpd.log rather than sending them to syslog. This way, it will be easier to review DHCP logs. In the dhcpd.log, you’ll find messages containing the following strings for the D-O-R-A transaction:

* DHCPDISCOVER
* DHCPOFFER
* DHCPREQUEST
* DHCPACK

Another important thing to notice is that these messages are exchanged when the DHCP state machine is between the PREINIT and BOUND stage. Here’s a list of the most important DHCP stages that will help you troubleshoot what’s going with the DHCP process.

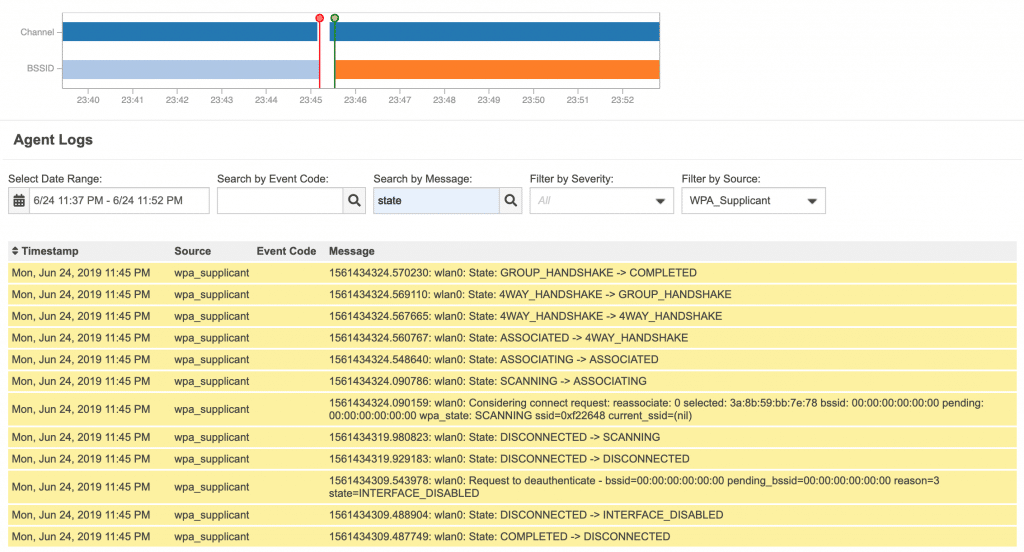
|  |  |
| --- | --- |
| **Stage** | **Meaning** |
| PREINIT | In this state, the DHCP client is initializing. |
| BOUND | The client has obtained a DHCP lease. |
| RENEW | The client is trying to renew its DHCP lease. |
| REBIND | The client didn’t renew the lease on time and requests a lease extension to any available server. |
| TIMEOUT | The client timed out and didn’t get a DHCP lease from a server. |
| FAIL | The client failed to obtain a DHCP lease for some other reasons. |

If you want to learn more about DHCP messages, check out the [IANA page on DHCP](https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml" \l "message-type-53" \t "/home/bleach/Documents\\x/_blank). For more information about the DHCP stages, check out the online [TCP/IP guide on DHCP](http://www.tcpipguide.com/free/t_DHCPGeneralOperationandClientFiniteStateMachine.htm" \t "/home/bleach/Documents\\x/_blank).

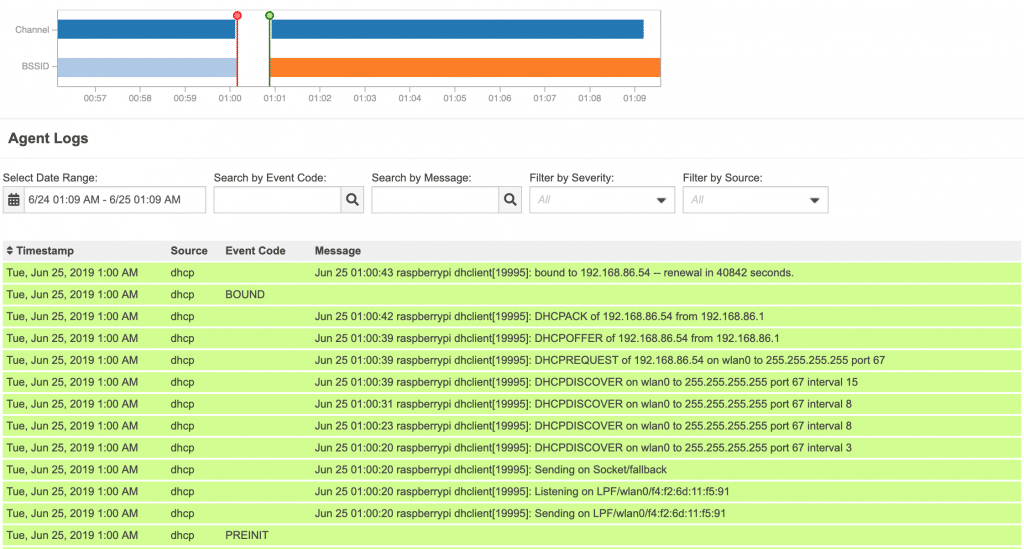
## Troubleshooting WiFi Connection Testing with NetBeez

NetBeez exposes the WPA supplicant and DHCP client logs of its WiFi agents (called Beez) on the dashboard. This feature helps engineers easily troubleshoot WiFi connection issues when they occur. By setting a connection timer on the monitored WiFi network profile, the WiFi Beez will periodically reconnect to the SSID, testing 802.11 association and authentication. This is a good way to proactively detect misconfigured access points, exhausted DHCP pools, and so on. Let’s see how we have implemented this functionality.

On the NetBeez dashboard, the user has to navigate to the Agents tab, then click on the WiFi agent deployed. In the wireless section of the agent details view, the user can access all WiFi metrics related to that particular agent, including logs. The following screenshot shows the filtered log messages from the WPA supplicant process running on the WiFi Beez:



In the next screenshot, I have filtered the DHCP messages logged when a WiFi Beez is requesting a DHCP address. You can easily identify the D-O-R-A transaction between the Beez and the access point.



If you want to see this in action, I have recorded a live demo on our YouTube channel.

**Conclusion**

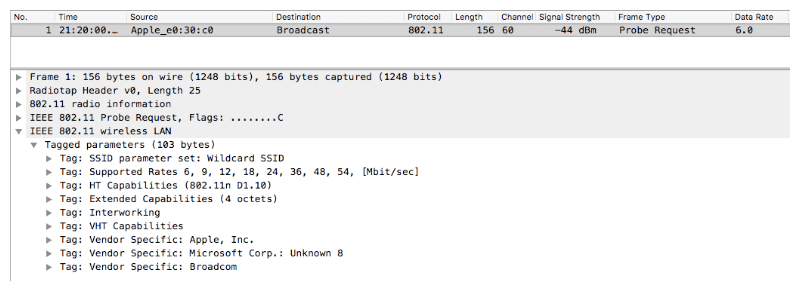
Familiarizing yourself with the WPA supplicant and DHCP client processes is important to understand how 802.11 networks work. To proactively detect problems on WiFi networks, engineers can configure dedicated WLAN agents to periodically reconnect to the network, testing 802.11 authentication and association, as well as DHCP.

# Station Authentication and Association

By [Rowell Dionicio](https://netbeez.net/blog/author/rowell/" \o "Posts by Rowell Dionicio)July 25, 2018[Network Troubleshooting](https://netbeez.net/blog/category/network-engineering/network-troubleshooting/), [WiFi Monitoring](https://netbeez.net/blog/category/wifi-monitoring/)

#### Authentication

In a station’s WiFi network discovery process, a Probe Request will be sent from the station to the BSSID listed in a Beacon frame the station received. This is the beginning of the 802.11 State Machine.

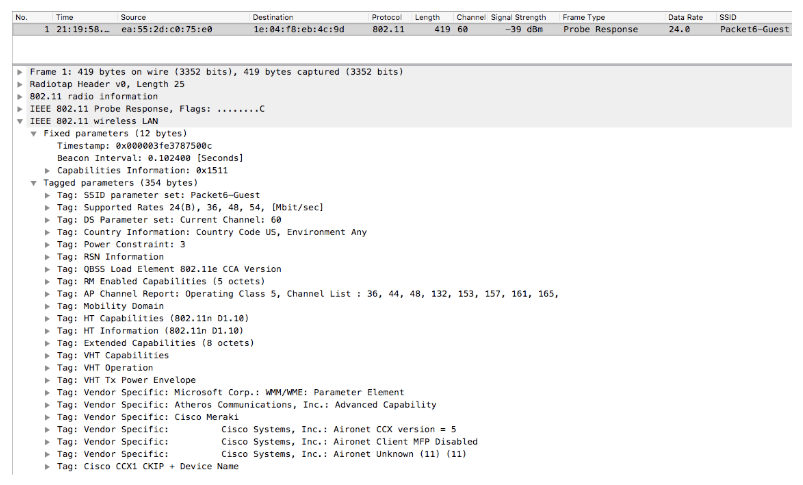


Sample Probe Request Frame

The access point responds with a Probe Response frame. After the station receives the Probe Response frame, it acknowledges the receipt of the frame with an Acknowledgement Frame.

Next, the station transmits an Authentication Request frame; this frame is also responded with an Acknowledgement Frame from the access point.

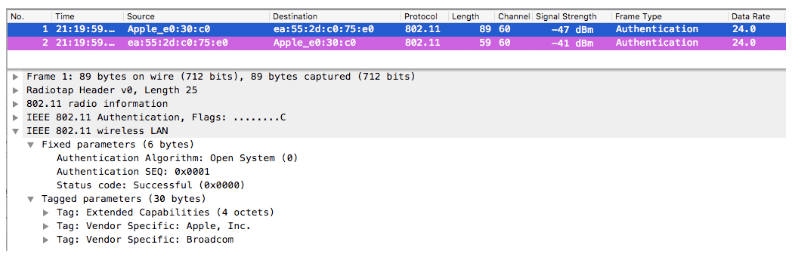
**NOTE:** This is not a security authentication process that you’d see with role PSK or 802.1X. This authentication frame starts the Open System authentication for joining the WiFi network. Any security methods, such as 802.1X, will occur after the 802.11 state machine.



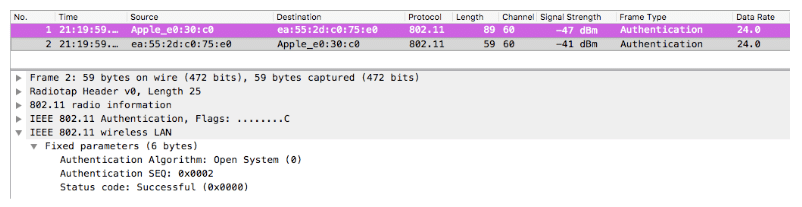
Sample Probe Response Frame

Open System authentication is a null authentication algorithm. Any station can request Open System authentication and be authenticated if the receiver has the authentication algorithm set to true, which is usually the case.

There are only two messages that are part of the Authentication frame transaction. The access point responds with an Authentication Response frame. If the response frame is “successful” then the station has been authenticated.



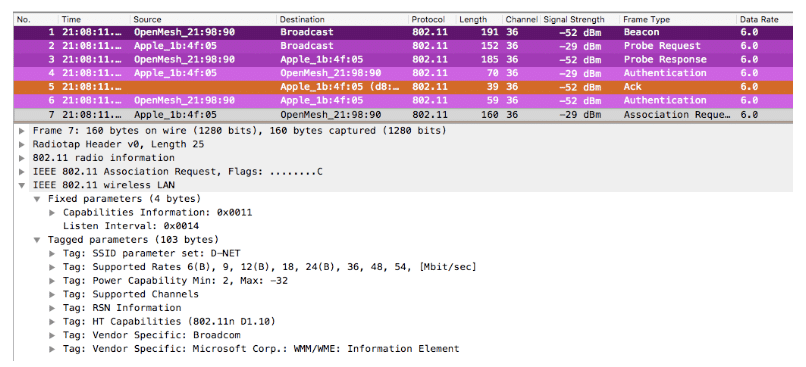
Sample Authentication Request Frame



Sample Authentication Response Frame

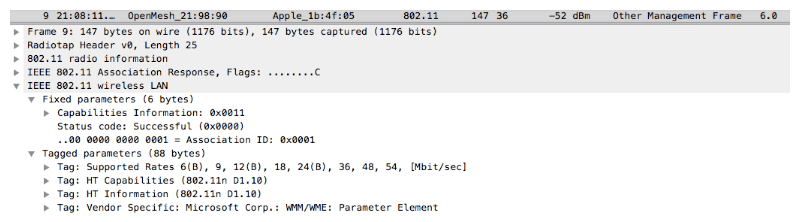
#### Association

Upon completion of successful Authentication frame exchanges, the station moves forward with associating. The station transmits an Association Request frame containing the station’s capabilities within fields and information elements of the frame.



Sample Association Request Frame

When the access point receives the Association Request frame, it responds with an Acknowledgement Frame and transmits an Association Response frame with the result of successful or unsuccessful. The station must support the required parameters defined by the WiFi network. If successful, the station will be assigned an Association ID which can be identified within the Association Response frame.



Sample Association Response Frame

The station responds to the Association Response frame with an Acknowledgement Frame which completes the 802.11 State Machine.

At this point, if there is a PSK or 802.1X configured on the WiFi network, it would begin completing that process with the necessary frame exchanges.

When troubleshooting any WiFi network, knowing how stations and access points communicate with each other can be beneficial to the process. The type of frames exchanged can assist in troubleshooting issues such as bad PSKs or failed 802.1X authentication. The frames tell the exact story happening within 802.11 wireless.

If you want to see this with your own eye, you can use [wireshark](https://www.wireshark.org" \t "/home/bleach/Documents\\x/_blank) packet capture and apply the following filters to your wifi network interface:

Probe Request: wlan.fc.type\_subtype == 0x0004  
Probe Response: wlan.fc.type\_subtype == 0x0005  
Authentication frame: wlan.fc.type\_subtype == 0x000b  
Association Request: wlan.fc.type\_subtype == 0x0000  
Association Response: wlan.fc.type\_subtype == 0x0001

**About the Author:**

Rowell Dionicio is a network engineer for a west coast university specializing in Wi-Fi design, deployment, and troubleshooting. He supports a WLAN infrastructure with over 40k concurrent Wi-Fi devices in higher education. He is the co-host to a Wi-Fi focused podcast, [https://cleartosend.net](https://cleartosend.net/" \t "/home/bleach/Documents\\x/_blank) and is co-host on a YouTube show ‘WiFi of Everything’. You can engage with him on Twitter @rowelldionicio where he encourages open communication.

# Securing Your Network with the 4-Way Handshake

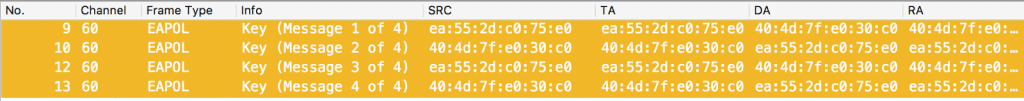
By [Rowell Dionicio](https://netbeez.net/blog/author/rowell/" \o "Posts by Rowell Dionicio)September 5, 2018[Network Engineering](https://netbeez.net/blog/category/network-engineering/), [Security](https://netbeez.net/blog/category/security/), [WiFi Monitoring](https://netbeez.net/blog/category/wifi-monitoring/)

Open networks are highly insecure and can lead to eavesdropping on communications. Additionally, there’s no mutual authentication in an open network to depict which access point a client is connecting to. How does one know if the access point that is accepting connections is actually trustworthy and not a rogue access point?

Secure communications between a client and access point require authentication and encryption. An access point broadcasting a secure SSID will advertise its security capabilities in the Robust Security Network Association (RSNA) Information Element.

The RSNA is used in either a pre-shared key (PSK) or 802.1X SSID, in other words,  WPA2-Personal or WPA2-Enterprise.

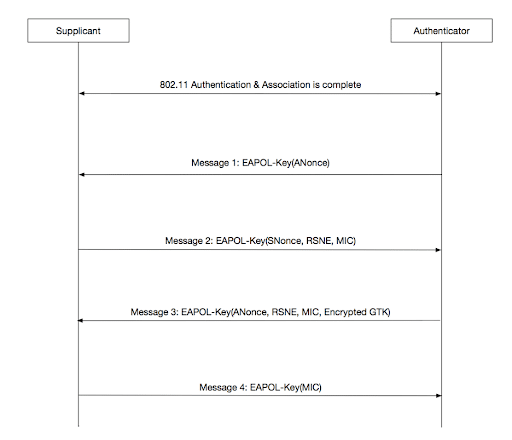
The 4-Way Handshake utilizes an exchange of four EAPOL-Key frames between the client and access point. In a PSK network, the exchange of frames occurs after the Open System Authentication and Association. In an 802.1X network, the 4-Way Handshake occurs after EAP authentication.



From the image above, there are four messages exchanged between the client and access point. Each message has a specific purpose:

The client and access point will derive their own separate pairwise transient key (PTK). The PTK is derived from each device’s pairwise master key (PMK). The PTK is comprised of the access point’s ANonce, client’s SNonce, and the MAC addresses of the access point and client.

To follow the frame exchanges, the graphic is presented below:

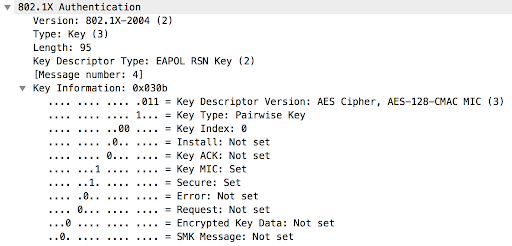


In message 1, the access point sends an EAPOL-Key frame to the client, containing the its ANonce which will be used to generate a PTK. This frame also contains other fields in the information element describing the type of encryption that is being used, such as AES cipher.

In message 2, the client sends its EAPOL-Key frame to the access point. This frame contains the SNonce, RSN Element, and the MIC (Message Integrity Code), allowing the client to derive a PTK from the SNonce and ANonce.

Message 3 (which is sent by the access point) contains an ANonce, RSN Element, and a MIC. What’s important about message 3 is the transportation of the Group Temporal Key (GTK) which is used to protect broadcast and multicast frames.

Message 4 is sent by the client which and contains a MIC. It is the final frame from the 4-Way Handshake. This final message notifies the access point of whether the temporal keys were installed successfully or not. This can be identified by the subfields of Key MIC: Set and Secure: Set.



## Vulnerabilities of the 4-Way Handshake

In 2018, it was announced there was a vulnerability within the 4-Way Handshake. The “KRACK Attack” proved to be able to target the weaknesses in the key re-installation process. Shortly after, another technique was identified through the use of a single EAPOL-Key frame.

The future of the 4-Way Handshake lies within WPA3 – the change involves the use of Simultaneous Authentication of Equals (SAE). Instead, a fresh PMK is negotiated in an SAE handshake. Following the 4-Way Handshake will be the formation of the fresh PMK with the SAE process. The result is protected against the previous two vulnerabilities that I had described above.

**About the Author:**

Rowell Dionicio is a network engineer for a west coast university specializing in Wi-Fi design, deployment, and troubleshooting. He supports a WLAN infrastructure with over 40k concurrent Wi-Fi devices in higher education. He is the co-host to a Wi-Fi focused podcast, [https://cleartosend.net](https://cleartosend.net/" \t "/home/bleach/Documents\\x/_blank) and is co-host on a YouTube show ‘WiFi of Everything’. You can engage with him on Twitter @rowelldionicio where he encourages open communication.