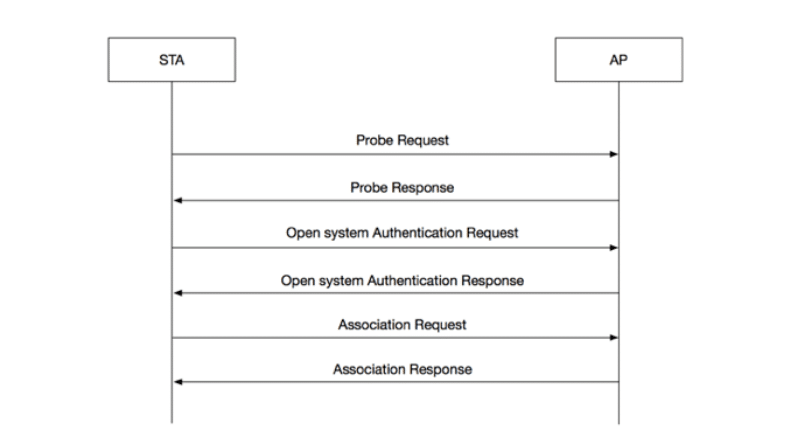
WiFi connections happen in a matter of microseconds. Within that small time frame, there are many frame exchanges occurring between a station and access point. Beacon frames are transmitted at an interval to allow passive or active scanning stations to join a particular WiFi network.

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:

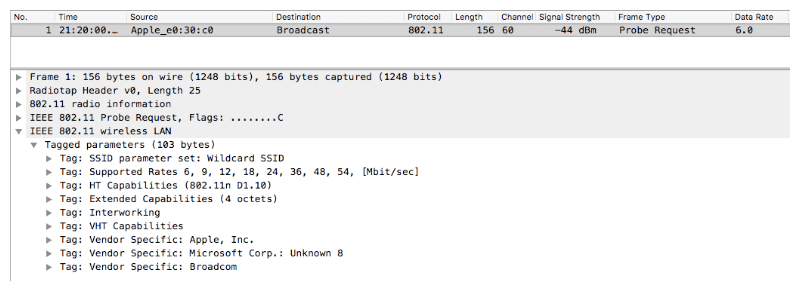
* Probe Request
* Probe Response
* Authentication Request
* Authentication Response
* Association Request
* Association Response

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



#### 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.

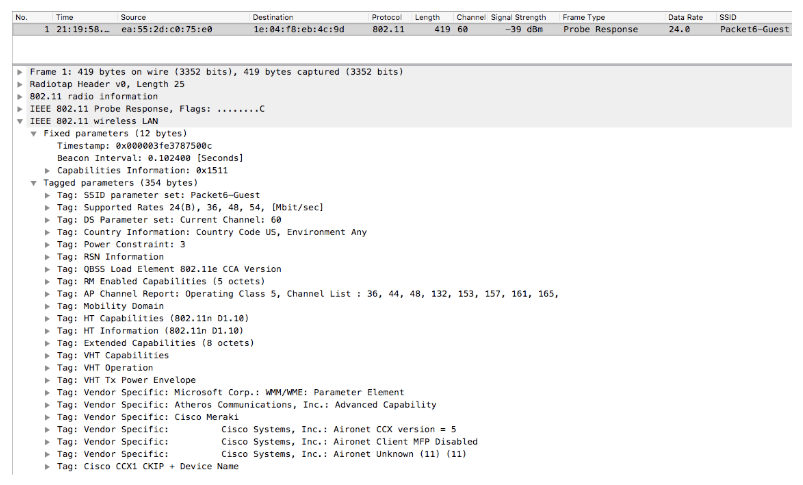


Sample Probe Request Frame

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.

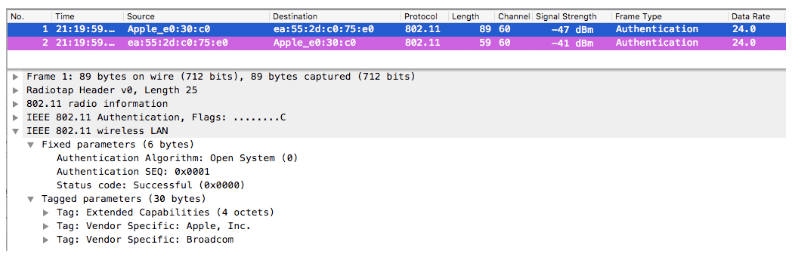
**NOTE:** This is not a security authentication process that you’d see with role PSK or 802.1X. This authentication frame starts the Open System authentication for joining the WiFi network. Any security methods, such as 802.1X, will occur after the 802.11 state machine.



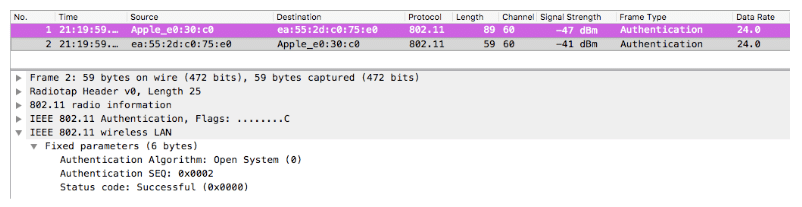
Sample Probe Response Frame

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.



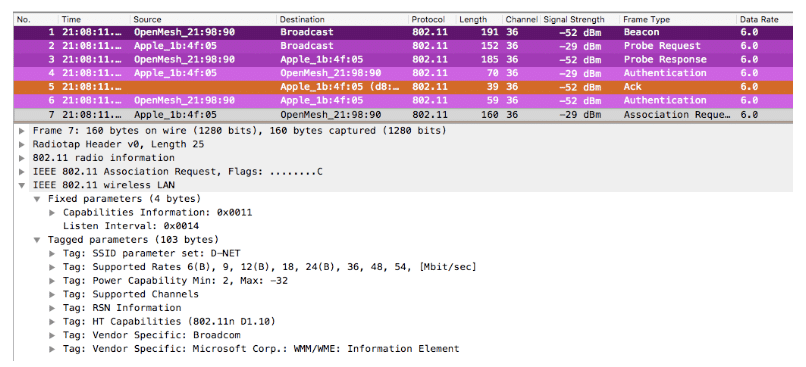
Sample Authentication Request Frame



Sample Authentication Response Frame

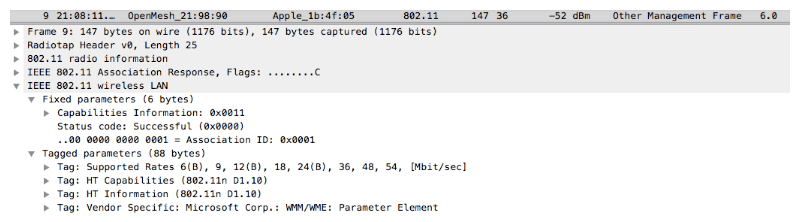
#### Association

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.