Published at https://www.packet6.com/802-11-state-machine on September 29, 2015

In the wired world, to connect to the network you would plug in your Ethernet cable into the switch. In the wifi world, you must connect to the access point. The process of connecting to an access point is called the 802.11 State Machine.

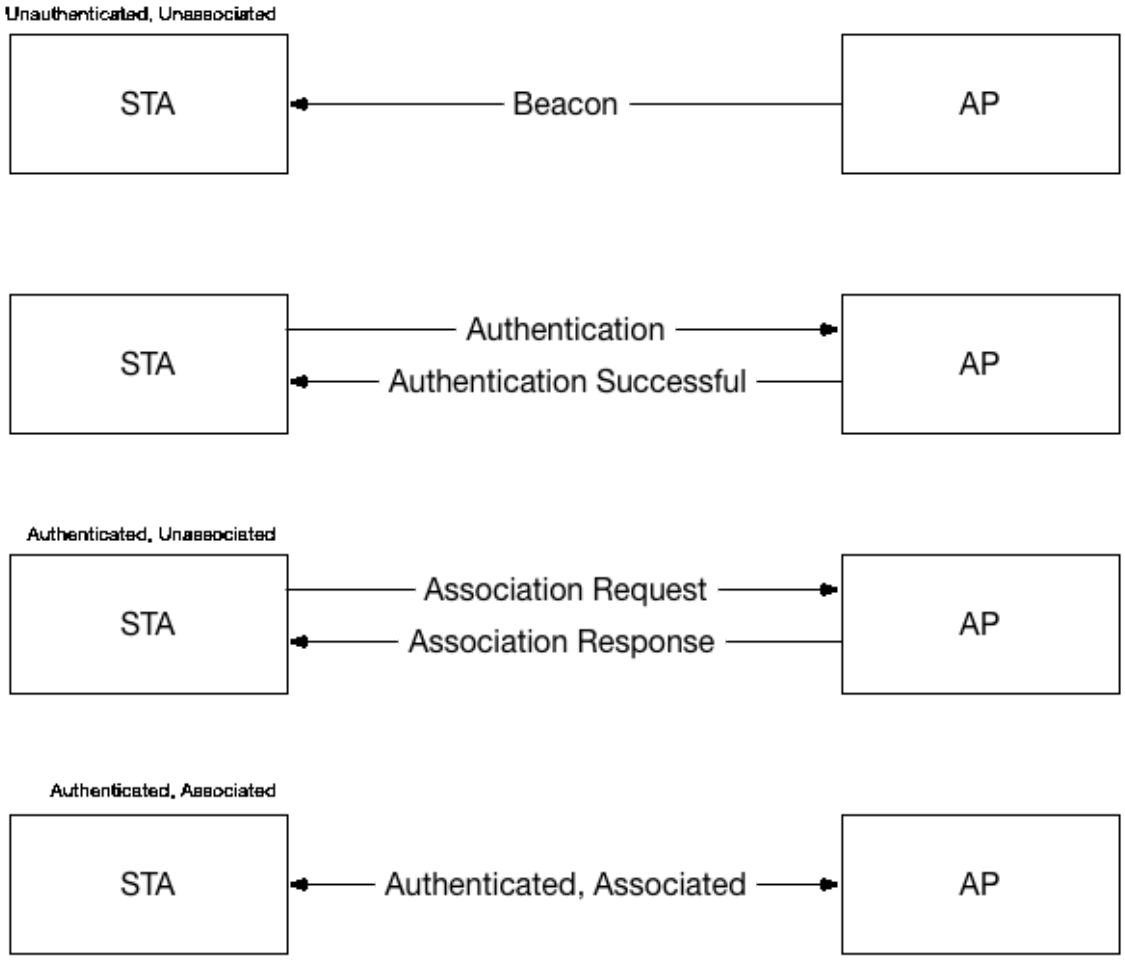
How does the station (STA) and access point agree to this connection?

I'm going to attempt to break it down step-by-step on this post.

802.11 State Machine

In my example, I have one STA connecting to an open SSID. The summary of it all is as follows:

1. STA is unauthenticated and unassociated
2. STA becomes authenticated and unassociated
3. STA becomes authenticated and associated
4. STA clears security requirements such as 802.1X, if required



PACKET6

Beacon/Probe

The STA begins the process by performing a passive or active scan. In the passive mode, the STA is listening for beacons from an access point. The beacon frame contains the BSSID which is the MAC address of the radio sourcing from the access point.

Source	Destination	Protocol	Length	Info
0c:68:03:d6:88:78	ff:ff:ff:ff:ff:ff	802.11	269	Beacon frame, SN=2154, FN=0, Flags=........C, BI=102, SSID=TEST
d8:bb:2c:1b:4f:05 (d8:bb:2c…	0c:68:03:d6:88:7d (0c:68:03:d6:88:…	802.11	45	Request-to-send, Flags=........C
	d8:bb:2c:1b:4f:05 (d8:bb:2c:1b:4f:…	802.11	39	Clear-to-send, Flags=........C

Wireshark capture of the beacon frame

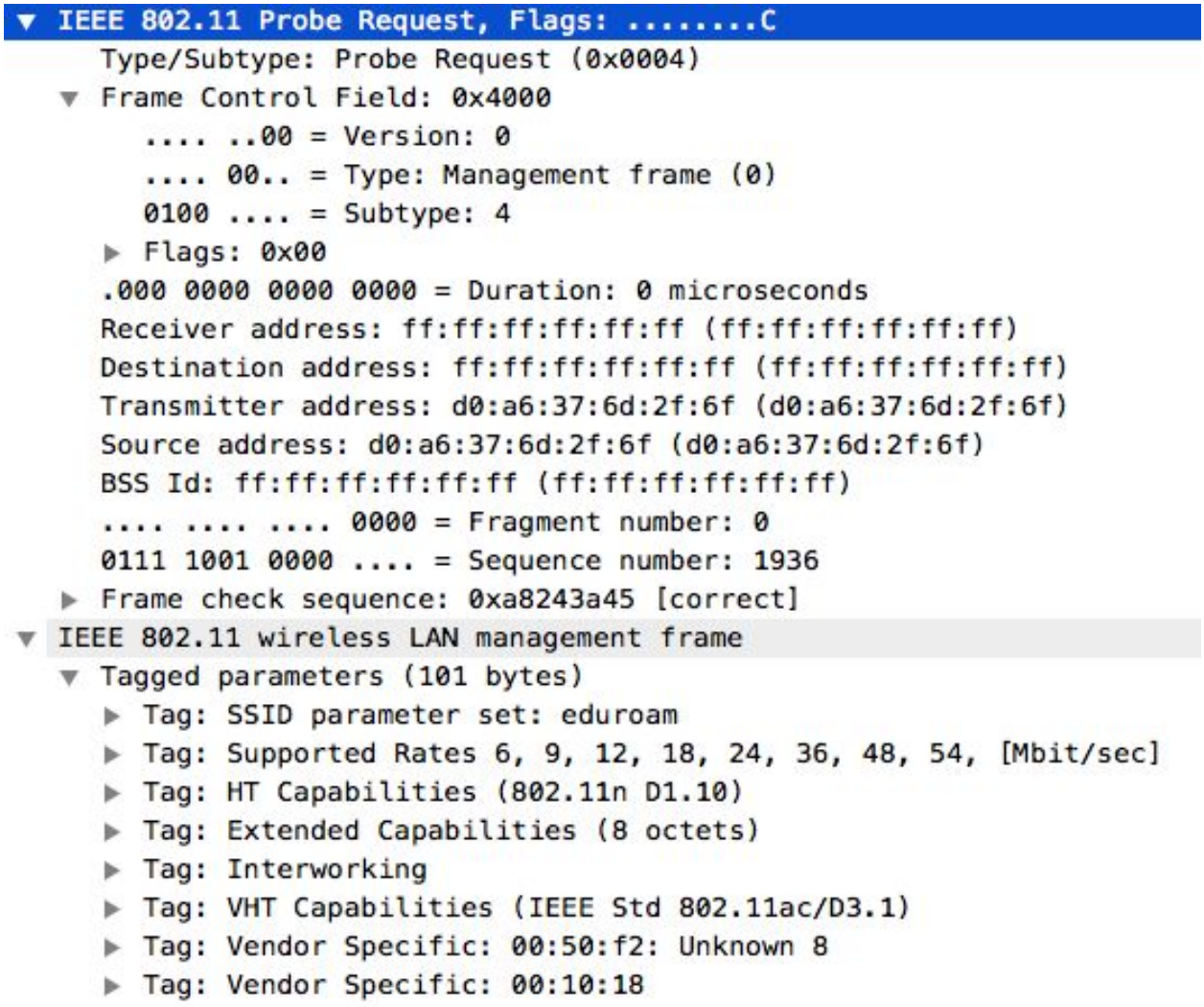
The beacon frame is a type of management frame defined in 802.11-2007. It includes capability information and parameters.

```
▼ IEEE 802.11 wireless LAN management frame
  ▼ Fixed parameters (12 bytes)
      Timestamp: 0x0000002b16995832
      Beacon Interval: 0.104448 [Seconds]
    ▼ Capabilities Information: 0x1001
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .0.. .... .... = Short Slot Time: Not in use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...1 .... .... .... = Radio Measurement: Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
  ▼ Tagged parameters (204 bytes)
    ▶ Tag: SSID parameter set: TEST
    ▶ Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: Country Information: Country Code US, Environment Any
    ▶ Tag: QBSS Load Element 802.11e CCA Version
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Extended Capabilities (6 octets)
    ▶ Tag: Cisco CCX1 CKIP + Device Name
    ▶ Tag: Vendor Specific: 00:40:96: Aironet DTPC Powerlevel 0x08
    ▶ Tag: Vendor Specific: 00:50:f2: WMM/WME: Parameter Element
    ▶ Tag: Vendor Specific: 00:40:96: Aironet Unknown (1) (1)
    ▶ Tag: Vendor Specific: 00:40:96: Aironet CCX version = 5
    ▶ Tag: Vendor Specific: 00:40:96: Aironet Unknown (11) (11)
    ▶ Tag: Vendor Specific: 00:40:96: Aironet Client MFP Disabled
```

Active Scan / Probe

A probe is sourced from the STA requesting to join a wireless network. This is a probe request management frame. The probe is responded by an access point using a probe response management frame.

In the probe request you will find the parameters as shown below. This is an example probe request from a STA broadcasted to any access point that can respond. The wireless network requested is eduroam.



Authentication

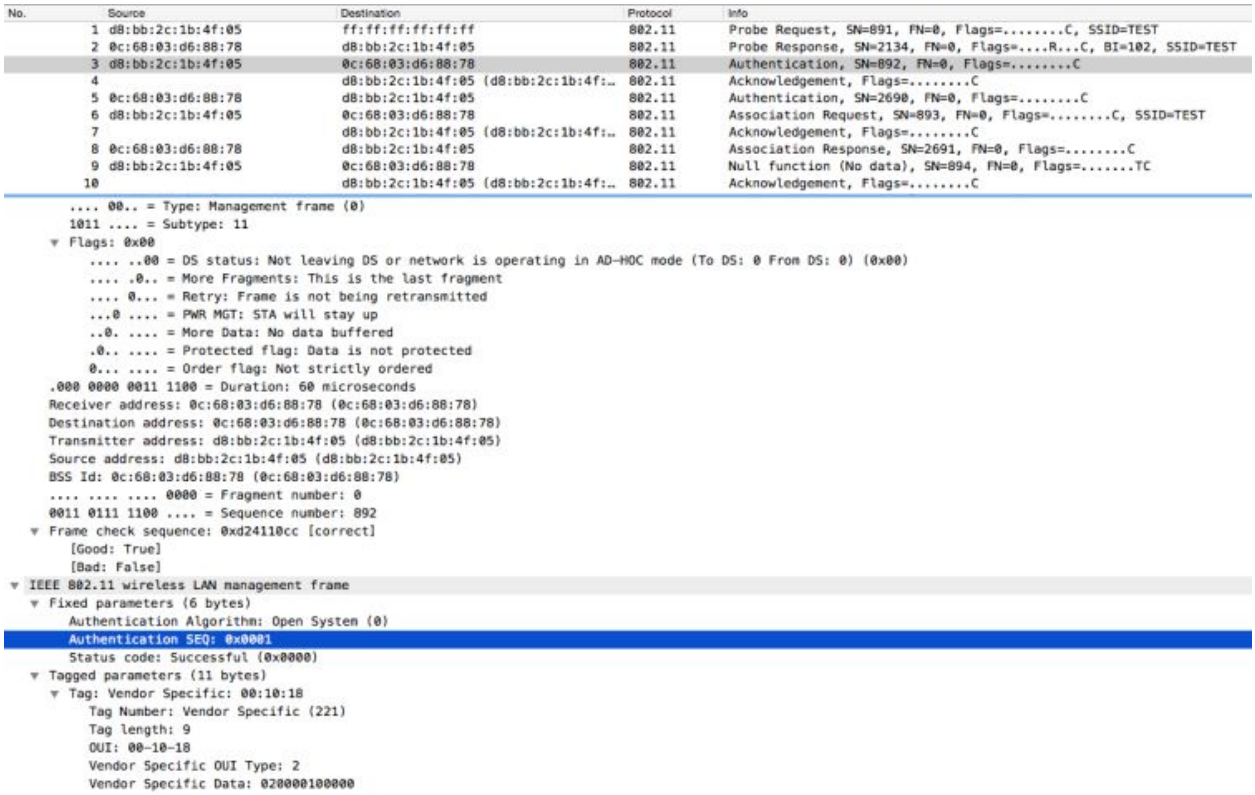
The probing/scanning phase is part of the unauthenticated and unassociated step. The STA has not authenticated with the access point and also is not associated with the access point. Think of authentication as plugging a computer into a port on a switch.

The STA must be authenticated to the access point *before* it is associated. It sounds backwards. These are the two states in this phase and it must be done in this order.

A STA can be in either two states in Authentication and Association:

- Unauthenticated or authenticated.
- Unassociated or associated.

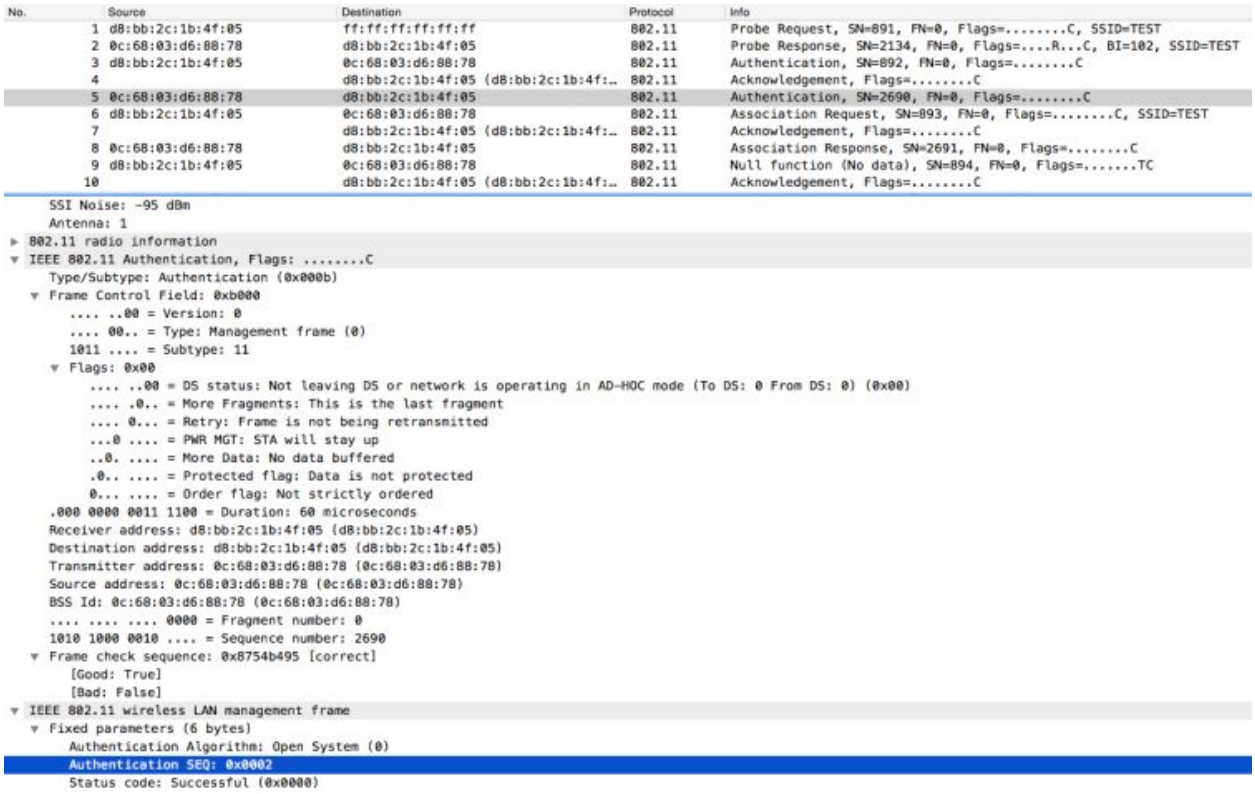
To begin the Authentication step, the STA sends an Authentication wireless management frame to the access point. The access point responds with an Acknowledgement frame.



Authentication frame sent to the AP.

Notice above, the Authentication Sequence is set to a state of 1.

The access point will acknowledge the Authentication frame from the STA and upon successful authentication, the access point will send an authentication frame to the STA with an Authentication Sequence with a **State of 2**, for success.



Access point sends an Authentication frame with a state of 2, for Successful.

Open System and Shared Key

If you noticed in the above successful authentication frame, the Authentication Algorithm was set to Open System. There are two types of methods for authentication.

- Open System
- Shared Key

Open System performs *no client verification*. This is the method used with SSIDs utilizing WPA, WPA2, and those with no password.

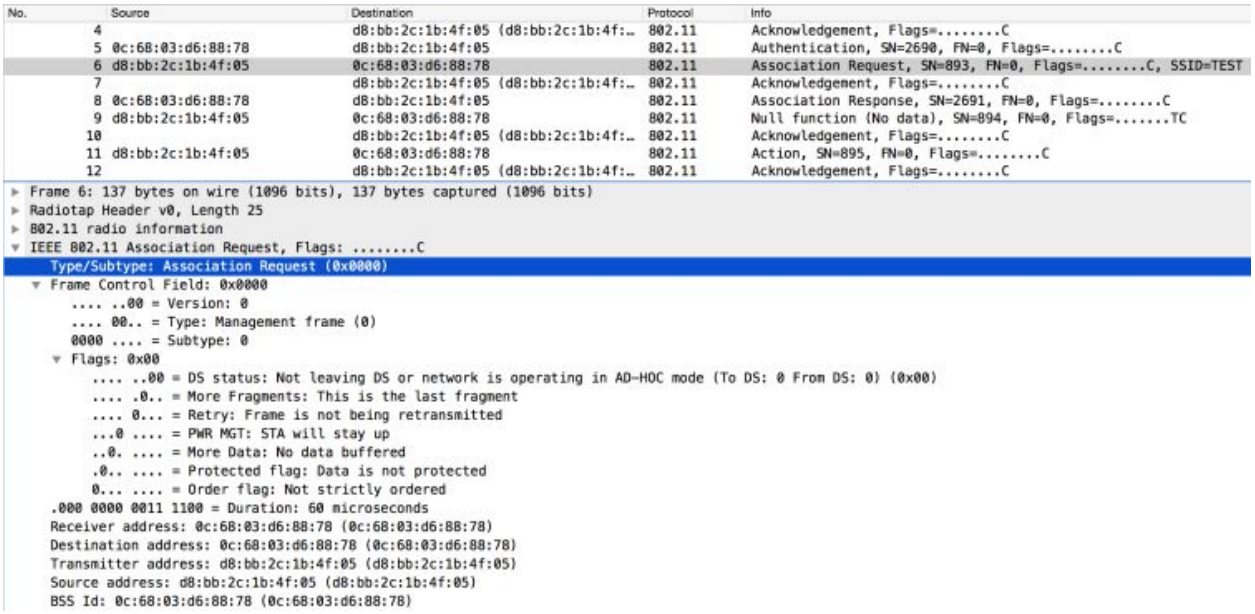
Shared Key uses a passphrase and contains a *4-way handshake* for authentication. The STA sends a request to authenticate, access point receives the request and sends back a cleartext challenge, the STA encrypts and sends another authentication request based on the cleartext challenge and then the access point compares the STA's challenge to the text. If successful, the STA is authenticated.

Association

Once the STA is authenticated to the access point, the next step is to become Associated. The Association occurs *after* the Shared Key Authentication or Open System Authentication

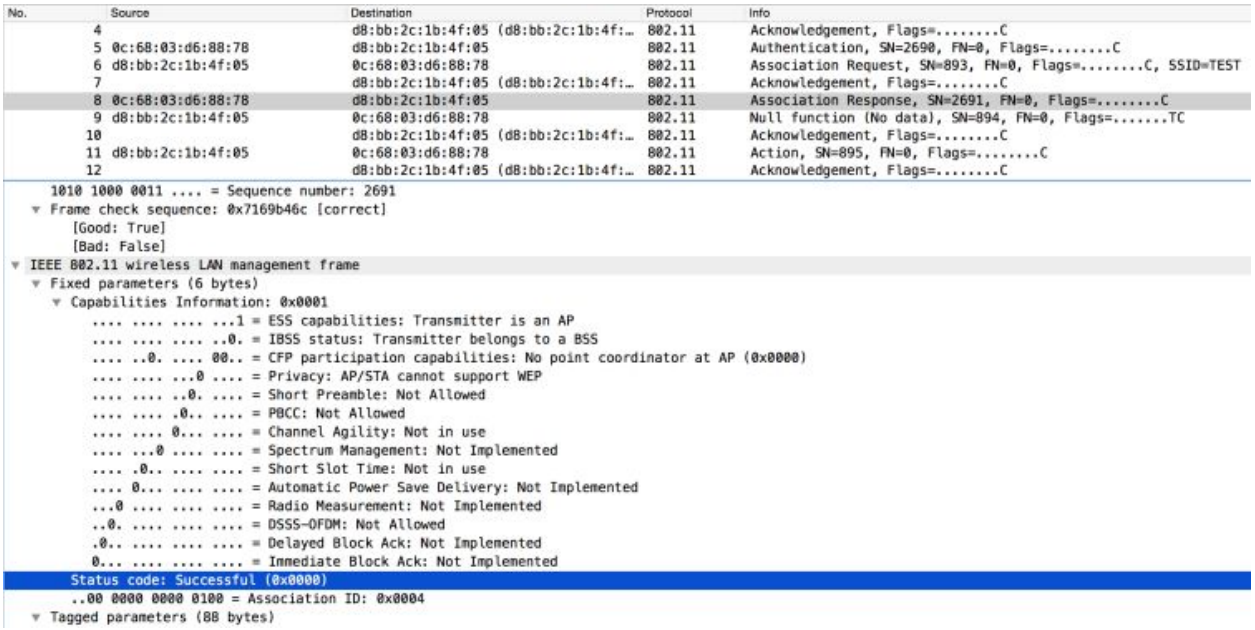
Algorithm. There cannot be a STA that is Associated but not Authenticated. If the STA fails Authentication, it does not move to Association.

After the the access point sends an Acknowledgement to the STA's Authentication Response, the STA sends an Association Request.



The Association Request is Acknowledged by the access point which then sends an Association Response frame to the STA.

If the association is successful, the access point's Association Response frame will contain a Status code: Successful.



The details within an Association Response include:

- Capabilities Information such as
    - Supported Data Rates
    - HT Capabilities
    - HT Information such as the Primary Channel
    - WMM information
- And more..

If the Status code is anything other than Successful, then the STA is deauthenticated.

Summary

The example above uses a STA that is trying to connect to a wireless network for the first time. The SSID is called TEST and does not have a password set up.

The STA probes for the SSID, moves into Authentication, transitions into Association, and is then successfully Authenticated and Associated. This last part indicates the STA can now send data wirelessly on the TEST network.

Below are the states a station cycles through to join a BSS:

1. Unauthenticated and Unassociated.
2. Authenticated but Unassociated.
3. Authenticated and Associated.