802.11 Association process explained

Access points are bridges that bridge traffic between mobile stations and other devices on the network. Before a mobile station can send traffic through an AP, it must be in the appropriate connection state.

The three 802.11 connection states are:

- Not authenticated or associated.
- Authenticated but not yet associated.
- Authenticated and associated.

A mobile station must be in an authenticated and associated state before bridging will occur.

The mobile station and AP will exchange a series of 802.11 management frames in order to get to an authenticated and associated state.
A mobile station starts out as not authenticated and associated.

1. A mobile station sends probe requests to discover 802.11 networks within its proximity. Probe requests advertise the mobile stations supported data rates and 802.11 capabilities such as 802.11n. Because the probe request is sent from the mobile station to the destination layer-2 address and BSSID of ff:ff:ff:ff:ff:ff all AP’s that receive it will respond.

2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP.

A mobile station chooses compatible networks from the probe responses it receives. Compatibility could be based on encryption type. Once compatible networks are discovered the mobile station will attempt low-level 802.11 authentication with compatible APs. Keep in mind that 802.11 authentication is not the same as WPA2 or 802.1X authentication mechanisms which occur after a mobile station is authenticated and associated. Originally 802.11 authentication frames were designed for WEP encryption however this security scheme has been proven to be insecure and therefore deprecated. Because of this 802.11 authentication frames are open and almost always succeed.

3. A mobile station sends a low-level 802.11 authentication frame to an AP setting the authentication to open and the sequence to 0x0001.

4. The AP receives the authentication frame and responds to the mobile station with authentication frame set to open indicating a sequence of 0x0002.

If an AP receives any frame other than an authentication or probe request from a mobile station that is not authenticated it will respond with a deauthentication frame placing the mobile into an unauthenticated and unassociated state. The station will have to begin the association process from the low level authentication step. At this point the mobile station is authenticated but not yet associated. Some 802.11 capabilities allow a mobile station to low-level authenticate to multiple APs. This speeds up the association process when moving between APs. A mobile station can be 802.11 authenticated to multiple APs however it can only be actively associated and transferring data through a single AP at a time.

5. Once a mobile station determines which AP it would like to associate to, it will send an association request to that AP. The association request contains chosen encryption types if required and other compatible 802.11 capabilities.

If an AP receives a frame from a mobile station that is authenticated but not yet associated, it will respond with a disassociation frame placing the mobile into an authenticated but unassociated state.

6. If the elements in the association request match the capabilities of the AP, the AP will create an Association ID for the mobile station and respond with an association response with a success message granting network access to the mobile station.

7. Now the mobile station is successfully associated to the AP and data transfer can begin.

Note: If WPA/WPA2 or 802.1X authentication is required on the wireless network, the mobile station will not be able to send data until dynamic keying and authentication have taken place after the 802.11 Association is complete.