wifi-bond

Welcome to the world of wireless networks !!!

802.11 Association process

Posted on April 8, 2017August 17, 2017 by wifibond
An access point acts as hub between station(client device) and other devices on the network. Before the station can send traffic through an access point, it must have established a connection state.

There are three 802.11 connection states:

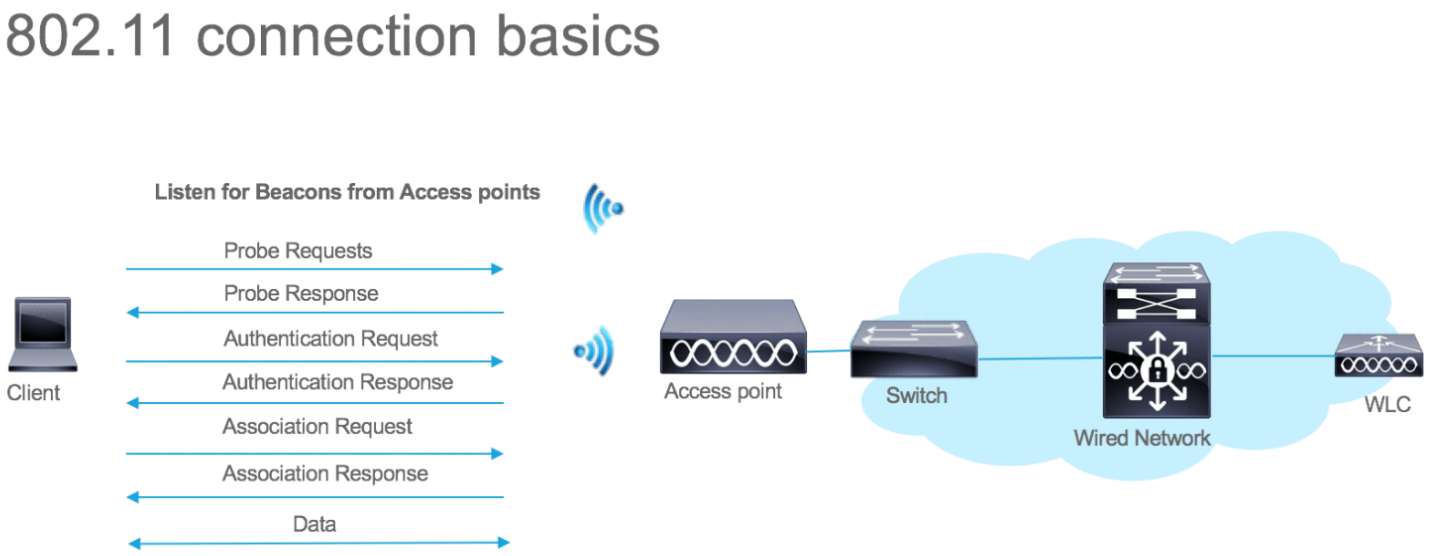
State 1: Unauthenticated and Unassociated

State 2: Authenticated, Unassociated

State 3: Authenticated, Associated

The station must be in an authenticated and associated state before connection is established.

The station and AP will exchange a series of 802.11 management frames in order to get to an authenticated and associated state.



Beacons: The access point periodically sends a beacon frame to announce its presence and relay many information that is required by the stations to connect to the wireless network

Probe Request: A station sends probe requests to discover 802.11 networks within its proximity. Probe requests advertise the stations supported data rates and 802.11 capabilities such as 802.11n.

Probe Response: Access point receiving the probe request check to see if the station has at least one common supported data rate. If they share a common data rate, a probe response is sent advertising the SSID, supported data rates, encryption types if required, and other 802.11 capabilities of the access point.

Authentication Request: The station chooses a SSID/network from the probe responses it receives. It also checks the compatibility on encryption type. Once compatible networks are discovered the station will attempt low-level 802.11 authentication with compatible access points. The station sends a low-level 802.11 authentication frame to an AP setting the authentication to open and the sequence to 0x0001.

Authentication Response: The access point receives the authentication frame and responds to the station with authentication frame set to open indicating a sequence, If an access point receives any frame other than an authentication or probe request from a station that is not authenticated it will respond with a deauthentication frame placing the mobile into an unauthenticated an unassociated state. The station will have to begin the association process from the low level authentication step. At this point the station is authenticated but not yet associated.

Association Request : Once the station determines which access point it would like to associate to, it will send an association request to that access point.The association request contains chosen encryption types and other compatible 802.11 capabilities.

Association Response: If the elements of association request match the capabilities of the access point, it 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.

Data: At this stage the connection is established and the station is successfully associated to the access point and is ready for data transfer

---

2 thoughts on “802.11 Association process”

1. ***Billy Tseng*** says: May 16, 2018 at 6:41 pm
   Hi. What could prevent a STA(Android) device from sending an authentication request after receiving probe response from the AP? There were forty something identical STAs(all Android with the same model/hardware) connected to an SSID and all of a sudden they all disconnected from the AP with “Authentication problem”. Packet capture result shows there were only 802.11 probe request and response frames without any authentication frames followed. Both request and response frames have the same bitrate (1Mbps). Restarting WiFi or restarting the STAs didn’t fix the issue. Even forgetting the network on the STAs didn’t work. However, a completely different Android device,

which was not connected previously, was able to associate the same SSID (with WPA2 password).

Interestingly, as soon as I restarted the AP, all forty STAs reconnected to the AP. Authentication frames started to show up after AP got rebooted. At this point, I really have no idea if the issue is on the AP or on the Android devices.

Reply

wifibond says: October 26, 2018 at 7:03 pm

Hi Billy, Apologies
For the delay in responding. I didn't receive an alert until I logged into the site for some editing.
I have seen this happen before and often it can be either the STA or the AP.
In your case, I suspect something in the wifi infrastructure blocking the station from Connecting.
Are you using controller based wireless network ? If yes, is there a possibility of client being excluded /blacklisted for certain duration?
I have also seen instances where probe
Requests are not sent by STA's until the wifi connection is reset.

Reply