

Wireless LAN Networks : Access Point Association

Vinh Ho (9 mins)

This is a three-phase: discover the AP, and then you have the authentication, and then the association. This is called the three-stage process for the wireless client and Access Point association.

Recall that the media contention method is the method in which devices determine how to access the media when traffic must be forwarded across the network. The IEEE 802.11 Wireless LAN use the MAC protocol CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance). While the name is similar to the Ethernet CSMA/CD, the operating concept is completely different.

When a wireless client sends data, it first senses the media to determine if other devices are transmitting. If not, it then sends an RTS (Request-to-Send) frame to the Access Point (AP). The AP receives the frame and, if available, grants the wireless client the access to the RF (Radio Frequency) medium by sending a CTS (Clear-to-Send) frame of the same time duration. All other wireless devices observing the CTS frame relinquish the media to the transmitting node for transmission. The CTS control frame includes the time duration that the transmitting node is allowed to transmit. Other wireless clients withhold transmissions for, at least, a specified duration.

For wireless devices to communicate over a network, they must first associate with an AP or wireless router. An important part of the 802.11 process is discovering a Wireless LAN and subsequently connecting to it. The management frames are used by wireless devices to complete the following three-stage process:

- Discover new wireless AP.
- Authenticate with the wireless AP.
- Associate with the wireless AP.

To associate the wireless client to an Access Point, must agree on specific parameters. Parameters must be configured on the AP and subsequently on the client to enable the negotiation of these processes.

What are the associate parameters? Common configuration wireless parameters include:

- SSID, you remember, is the Service Set Identifier, is a unique identifier that wireless clients use to distinguish between multiple wireless networks in the same vicinity. The SSID name appears in the list of available wireless networks on a client. Depending on the network configuration, several APs on a network can share an SSID. Names are usually 2 to 32 characters long.

- The next parameter is Password. Password is required for the wireless client to authenticate to the AP. A Password is sometimes called the security key. It prevents intruders and other unwanted users from accessing the wireless network.
- Network mode - refers to the 802.11a/b/g/n/ac/ad WLAN standards. APs and wireless routers can operate in a “Mixed” mode, meaning that it can simultaneously use multiple standards.
- Security Mode - refers to the security parameter settings, such as WEP, WPA/WPA2. Always enable the highest security level supported.
- Channel Setting is the last of the association parameter. Refers to the frequency band used to transmit wireless data. Wireless routers and AP can choose the Channel Setting or it can be set manually if there is interference with another AP or wireless device.

In Network mode, it can support Mixed, Wireless-N only, or Wireless-G only. The Mixed setting provides more flexibility, but it can also slow down communication. For example, if all the wireless clients connecting to the router are using 802.11n, then they all enjoy the better data rates provided. But, if 802.11g wireless client associate with the AP, then all of the faster wireless clients contending for the channel must wait for the 802.11g clients to clear the channel before transmitting. However, if all wireless clients support 802.11n, then select Wireless-N only for best performance.

So after you configure all the association parameters, now we talk about discovering the Access Point.


There are two modes: the Passive Mode and Active Mode. Wireless devices must discover and connect to an AP or wireless router. Wireless clients connect to the AP using a scanning or we call it, probing process. This process can be Passive Mode or Active Mode.

In Passive Mode, the AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings. The primary purpose of the beacon is to allow wireless clients to learn which networks and APs are available in a given area, thereby allowing them to choose which network and AP to use.

In Active mode, wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels. The Probe Request includes the SSID name and standards supported.

Active mode may be required if an AP or wireless router is configured not to broadcast Beacon frames, which is more secure. Wireless client could also send a Probe Request without an SSID to discover nearby WLAN networks. APs configured to broadcast Beacon frames would respond to the wireless client with a Probe Response and provide the SSID name. APs with the broadcast SSID feature disabled do not respond, this is one of the secure features.

Look at the figure you can see that the Access Point send out a lot of beacons, and advertising its SSID, its supported standards, its secure settings. The client, or sender, send a Probe Request with a known SSID, and supporting standard, and the Access Point with the same SSID will respond, and they call it a Probe Response frame.



Authentication - the 802.11 standard was originally developed with two authentication mechanisms: either Open Authentication or Shared key Authentication.

Open Authentication - fundamentally a NULL authentication where the wireless client says “authenticate me” and the AP responds with “yes”. Open Authentication provides wireless connectivity to any wireless device and should only be used in situations where security is of no concerns.

Shared key Authentication is a technique based on a key that is pre-shared between the client and the AP. Figure provides a simple overview of the authentication process. However, in most Shared Key Authentication installations, the exchange is as follows:

1. The wireless client sends an authentication frame to the AP.
2. The AP responds with a challenge text to the client.
3. The client encrypts the message using its pre-shared key and returns the encrypted text back to the AP.
4. The AP then decrypts the encrypted text using its shared key.
5. If the decrypted text matches the challenge text, the AP authenticates the client. If the messages do not match, the wireless client is not authenticated and wireless access is denied.

After a wireless client has been authenticated, the AP proceeds to the association stage. The association stage initialises settings. As part of this stage,

- The wireless client forwards an Association Request frame that includes its MAC address.
- AP responds with an Associate Response that includes the AP BSSID (Basic Set ID), which is the AP MAC address.
- The AP maps a logical port known as the Association Identifier (AID) to the wireless client. The AID is equivalent to a port on a switch and allows the infrastructure switch to keep track of frames destined for the wireless client to be forwarded.

After a wireless client has associated with an Access Point, traffic is now able to flow between the client and the AP.