CHAPTER 12

802.11 Fundamentals

September 4, 2014

This part of the CVD discusses 802.11 Fundamentals, namely the role of beacons, probe requests, and probe responses.

Before discussing details about a location ready WLAN design, it is important to understand how an Access Point and wireless client start their initial communication. Once the wireless network is up and running, WLAN clients connect to an Access Point that provides it the best connection and data rate possible. Before a client connects to an AP, the client must first figure out to which AP it should connect.

802.11 WLANs consist of multiple elements and behaviors which make up the foundation of the 802.11 protocol. A key part of the protocol discovers the appropriate WLAN and establishes a connection with that WLAN. The primary components of this process are:

- Beacons—Used by the WLAN network to advertise its presence.
- Probes—Used by WLAN clients to find their networks.
- Authentication—An artifact from the original 802.11 standard.
- Association—Establishes the data link between an AP and a WLAN client.

Beacons

Although beacons are regularly broadcast by an AP, the probe, authentication, and association frames are generally used only during the association and re-association process. In a CUWN network, the APs advertise their presence in the network by sending out Beacon frames, which includes the SSID and BSSID information. The Beacon frame also contains information about the supported rates, parameter sets that indicate channel number, security requirements (WEP or WPA, etc.), and optionally Traffic Indication Map (TIM) that APs can send periodically to poll stations that use power save mode but have data frames waiting for them at the Access Point. Typically APs transmit beacon frames every 100ms.

Note Many WLAN security documents suggest that sending beacons without the service set identifier (SSID) is a security best practice that prevents potential hackers from learning the SSID of a WLAN network. All WLAN solutions offer this as an option. However given that the SSID can be easily discovered while sniffing a WLAN client during the association phase, this option has little security value. For a Cisco Connected Mobile Experience (CMX) Solution, SSID can be broadcast or hidden based on the use case. Generally Connect & Engage or Analytics services would presume that SSID be broadcast to get maximum results, it is not a must. For operational and client support issues, it is often better to allow the SSID to be broadcast. The SSID should be chosen to represent to the identity of the company/venue/mall

or the purpose of the WLAN, while at the same time being as unique as possible; the SSID should not give away the purpose or the owner of the WLAN. Creating long random strings as SSIDs is not recommended because this simply adds to the operations and maintenance overhead without an appreciable security improvement; a simple word is often the best choice. Common WLAN-related words should be avoided because there is no process or standard to prevent accidental or intentional SSID duplication.

The following is an 802.11 beacon example:

```
Type/Subtype: Beacon frame (8)
...
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    ...
    Sequence number: 2577IEEE 802.11 wireless LAN management frame
    ...
        SSID parameter set: "wpa1"
            Tag Number: 0 (SSID parameter set)
            Tag length: 4
            Tag interpretation: wpa1
        Supported Rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
[Mbit/sec]
...
        Vendor Specific: WPA
            Tag Number: 221 (Vendor Specific)
            Tag length: 28
            Tag interpretation: WPA IE, type 1, version 1
            Tag interpretation: Multicast cipher suite: TKIP
            Tag interpretation: # of unicast cipher suites: 2
            Tag interpretation: Unicast cipher suite 1: TKIP
            Tag interpretation: # of auth key management suites: 1
            Tag interpretation: auth key management suite 1: WPA
            Tag interpretation: Not interpreted
...
```

802.11 Join Process—Association

Before an 802.11 client can send data over a WLAN network (Fast Roaming is an exception to this process, but is not discussed in this guide), it goes through the following three-stage process:

- 802.11 probing—802.11 networks make use of a number of options, but for an enterprise deployment the search for a specific network involves sending a probe request out on multiple channels that specifies the network name (SSID) and bit rates.
- 802.11 authentication—802.11 was originally developed with two authentication mechanisms. The first one, called “open authentication”, is fundamentally a NULL authentication where the client says “authenticate me” and the AP responds with “yes”. This is the mechanism used in almost all 802.11 deployments. Open authentication is the recommended choice for a Cisco Connected Mobile Experience (CMX) Analytics deployment, but not a must. Likewise it may not be necessary to have Open Authentication mechanism for Connect & Engage or Mobile App engagement. The second type of authentication, namely the WEP/WPA/WPA2, is a shared key mechanism that is widely used in home networks or small Wi-Fi deployments. If needed be, these authentication mechanisms may also be used in a CMX deployment where an open network is not desired, but analytics is still preferred (for example, a hotel or lobby environment). Enterprise authentication is achieved by using 802.1X/EAP authentication mechanisms and is not discussed as part of this solution guide.

- 802.11 association—This stage finalizes the security and bit rate options and establishes the data link between the WLAN client and the AP. If a client has joined a network and roams from one AP to another within the network, the association is called a re-association. The primary difference between an association and a re-association event is that a re-association frame sends the MAC address (BSSID) of the previous AP in its re-association request to provide roaming information to the extended WLAN network.

In conventional WLANs, APs advertise their presence by sending out beacon frames which include their SSID and BSSID. Prior to association, clients gather information about the APs by scanning the channels one by one either through passive scanning or active scanning. In passive scanning mode the client station moves the radio into each channel and waits to listen for beacons on the channel. The client station listens for beacons containing SSID that it may have already connected to before. If the client receives beacons from multiple APs for the same SSID, it attempts to connect to the AP with the best RSSI (receiver signal strength indicator).

The clients also perform active scanning, wherein the client stations send out probe request frames on each channel. These probe requests may contain SSID of a specific WLAN that the station is looking for or the probe requests can also look for "any" SSID to find out all the SSIDs in the proximity of the client. These are requests for APs to send out information about themselves. APs respond to Probe Requests with probe response frames, the contents of which are similar to Beacon frames. The APs operating on a particular channel responds back to probe request with a probe response with its SSID, supported rates, and security rates.

If a client station receives probe responses from multiple APs (and/or multiple SSIDs), the client station uses RSSI of the AP as a judge to connect to an AP with best signal strength.

The following shows a segment of a sample probe request, where the WLAN client sends out a request for a particular SSID (wpa1).

```
IEEE 802.11 wireless LAN management frame
    Tagged parameters (31 bytes)
        SSID parameter set: "wpa1"
            ...
        Supported Rates: 1.0(B) 2.0(B) 5.5 11.0 6.0 9.0 12.0 18.0
           ...
        Extended Supported Rates: 24.0 36.0 48.0 54.0
            ...
```

The following shows a portion of a sample probe response, where an AP using the specified SSID responds with supported rate and security properties for that WLAN SSID.

```
...
IEEE 802.11 wireless LAN management frame
...
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
[Mbit/sec]
   ...
            Tag interpretation: WPA IE, type 1, version 1
            Tag interpretation: Multicast cipher suite: TKIP
            Tag interpretation: # of unicast cipher suites: 1
            Tag interpretation: Unicast cipher suite 1: TKIP
            Tag interpretation: # of auth key management suites: 1
            Tag interpretation: auth key management suite 1: WPA
            Tag interpretation: Not interpreted
...
```

Note The user has to connect to an SSID irrespective of the type of authentication method used on the WLAN. Most of the client stations present the user with a list of SSIDs to join based on the best signal strength they receive. Once the user instructs a client to join a particular SSID, the client software usually stores this information in its cache; this info is then used by the client station to probe for the same SSID when it tries to connect again after a disassociation.

It is also fairly common for client station that is already associated with an AP to send probe requests every few seconds across other channels. The client station does this to maintain an updated list of known APs with best signal strength. When the client can no longer maintain a good connection with the AP, the client can roam to another AP with better signal strength. With newer improvements on the Cisco Wireless LAN Controllers, APs may force the client to disassociate so that the client can enter the 802.11 join phase again to connect to a better AP. Once the client station decides to join a particular SSID to the strongest AP, it follows through with the 802.11 authentication and 802.11 association phases to connect to the network.

Note More detail on the 802.11 authentication frames and association frames are can be found at: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/ch3_2_SPMb.html#wp1056095.

This method of actively scanning by sending probe requests and receiving probe responses on different channels, irrespective of an on-going connection between an AP and client, makes it possible for a client and APs to know about each other constantly. The WLC and MSE make use of this information to locate a Wi-Fi client and form the basis for a location aware client design. Chapter 13, “Location Fundamentals” covers location awareness in more detail.