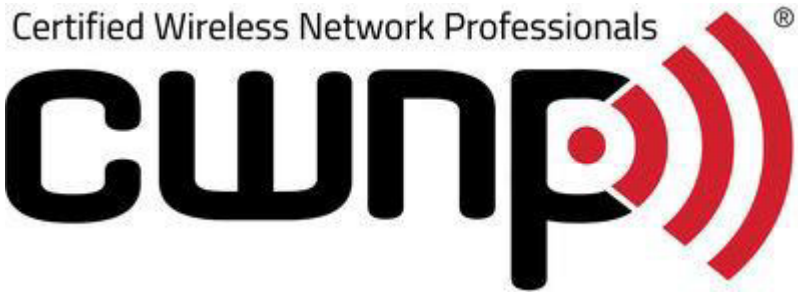


Network Discovery in the new Band of 6 GHz in Wi-Fi

Belal ALBaytar

CWNE

Candidate

Edited and reviewed for grammar and image use by CWNP.

Introduction:

Mobility is one of the key features of wireless networks, and while stations keep moving around access point service set areas (Basic Service Areas), stations must have the ability to discover all available networks or "SSIDs" to which they can connect. Unfortunately, this mechanism costs precious time and power from the station side or "mobile user." That's why we have to be efficient when introducing a standard method to do this.

In this article, I will discuss the methods that have been introduced for the 6 GHz band in Wi-Fi to help and improve efficient management and still able to discover the SSIDs in 6 GHz. But first I will briefly talk about discovery mechanisms in Wi-Fi networks in general (2.4GHz and 5GHz).

Network Discovery in 2.4 and 5 GHz:

Before I start, I would like to identify the acronyms of Service Set ID (SSID), which provides the network name, and Basic Service Set ID (BSSID), which stands for a virtual mac address that is unique for each Wi-Fi service set implemented by an AP. Many access points may broadcast the same SSID to form an Extended Service Set (ESS).

Also, if you have an access point that broadcasts two SSIDs on both bands, 2.4 and 5 GHz, let us say Home and Guest, those two SSIDs will have four BSSIDs in total - two for each band. Each implementation of an SSID in each band requires a radio for that implementation and will have a unique BSSID for each of the implemented SSIDs in all bands.

In the 2.4 and 5 GHz bands, Wi-Fi devices can discover specific service sets or BSSIDs through two primary methods. Here, I will discuss two methods to later explain how the standard for 6 GHz deals with the same requirement (locating a service set in the band).

Active Scanning, in this technique, stations are taking the lead to interact with any possible access point's BSSIDs in a channel by sending a Probe-Request frame. Stations will set a timer to await the answer(s) and then the station will jump into another channel and send a probe and so on until they have scanned the entire channel set that the transceiver supports. Stations can send Probe-Request frames for a specific SSID and it called a directed Probe-Request. They can also send Probe-Request frames for any available BSSID where it called a Null Probe-request. The latter allows for the location of SSIDs in a channel regardless of the name.

When the access points receive these Probe-Request frames, if they are not configured with a hidden SSID, they will respond in Probe-Response frames. These frames will contain details for operation parameters that concern connection parameters that I will not discuss here, but at least contain the central frequency of the primary channel.

Passive Scanning, here stations only listens for Beacon frames or Probe-Response frames (sent in response to other Probe-Request frames) transmitted in the air. The access points use Beacon frames to advertise their existence in intervals of 100-time units. A time unit is 1024 microseconds and is called the ***Target Beacon Transmission Time (TBTT).*** More time-units can be defined to decrease the overhead on the medium, but 100 is the default. Don't be confused, 100 time-units equals 100 times 1024, or 102,400 microseconds, which is equal to 102.4 milliseconds. This number is why many round to 100 milliseconds between Beacon frames. If you increase the number of time-units, Beacons may be delayed more due to the contention that happened in the medium and thus make the client wait more time than active scanning to discover a BSSID. Also, passive scanning can miss access point Beacon frames because it cannot wait a long time on a channel before moving to the next.

Beacon frames are transmitted at low speeds (data rates) of 1 or 2 Mbps for 2.4 GHz and 6 Mbps for 5 GHz and that allows them to be decoded by legacy devices.

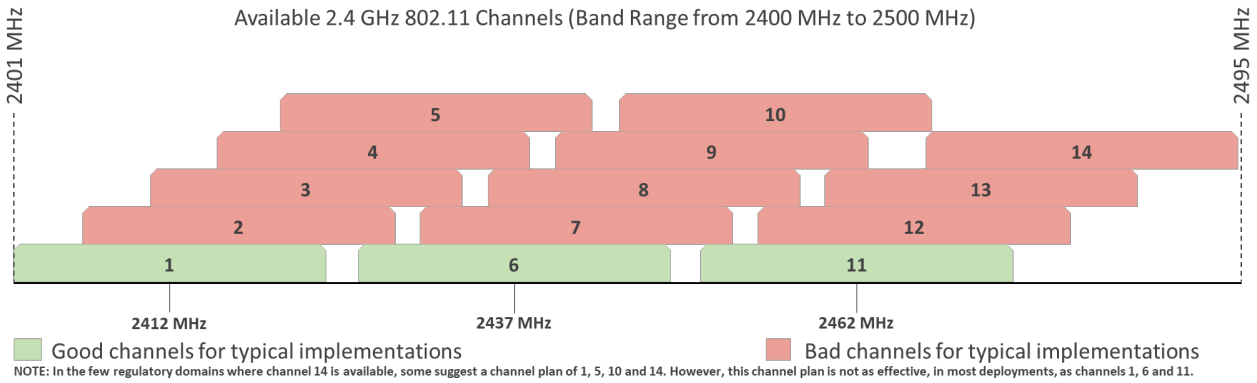
Stations mostly use active scanning to discover BSSIDs. In an ESS environment, a table of candidate AP-BSSIDs and corresponding supported channels must be created on stations to allow for roaming to another AP. Even if the station has a quality connection to an AP-BSSID, the station will do off-channel scanning. This action involves sending Probe-Request frames on

channels that are not the same channel used to communicate with the connected AP-BSSID. Off-channel scanning allows the stations to identify potential roaming targets.

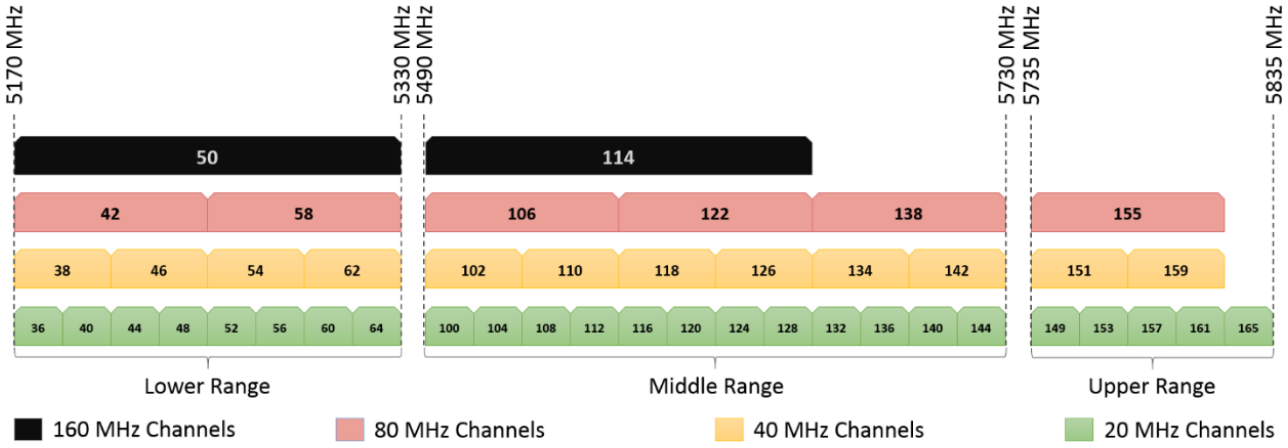
Using active scanning can drain the battery in the mobile device. In the 2.4 GHz band we only have three non-overlapping channels (1, 6, and 11) used in most networks and not much active scanning will have to be performed (assuming the clients scan only those channels, which many do not), giving better battery life. However, in the 5 GHz band, we have up to 25 channels and, if we exclude the DFS channels (here, I exclude the TDWR from CH 116 -132) we still have about 20 channels. The result is more probing of more channels, which means decreased battery life over that of 2.4 GHz devices. Keep in mind, however, that this battery drain is not an excessive amount in either case.

In the 6 GHz band with the existence of up to 59 channels (though many regulatory domains support only a small subset of these), this mechanism will not be as efficient as it was in the previous bands. Stations would stay busy scanning the channels and a significant amount of time would be used in this process and more power would be consumed as well.

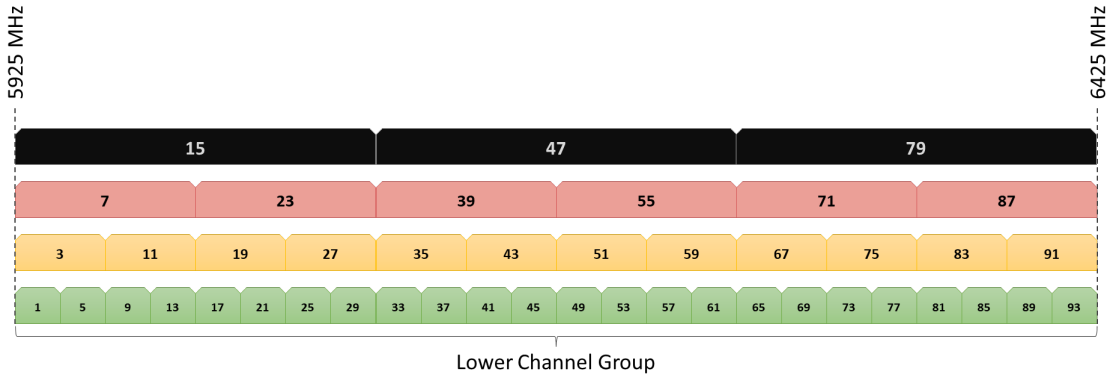
Channels used in 6, 5 and 2.4 GHz Wi-Fi solutions:

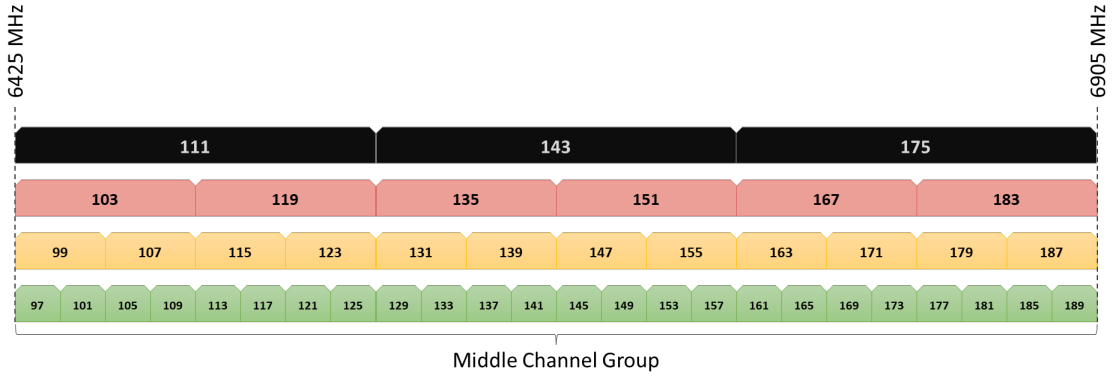


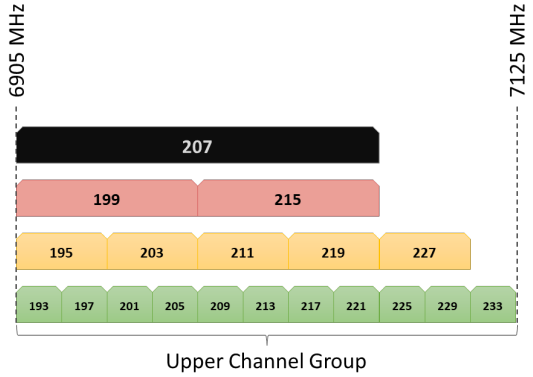
2.4 GHz Channels



5 GHz Channels







6 GHz Channels

Images Copyright CWNP. Used with permission.

To be clear DFS channels in the US such as 120, 124 and 128 are available for use based on specific rules, while some countries are not allowing use of those channels. In this topic, it is not our focal point, but whether it is 20 or 15 channels in 5 GHz, it's still applicable to the number of channels to scan using the probing mechanism compared with 59 channels in 6 GHz.

Network Discovery in 6 GHz:

In 6 GHz, the network discovery can't be done as the 2.4GHz and 5GHz bands allow. There are so many channels, 59 20MHz channels, that it will consume too much time, up to 6.04 seconds (stations normally wait about 100 ms to hear Probe Response frames), which is considered a very significant duration in the Wi-Fi world. Imagine a user who is making a voice call and moving inside the building. 6 seconds is a huge number to do roaming. It is a nonstarter. Also, power consumed in this operation is another reason not to use the old way.

Wi-Fi stations operating in the 6 GHz band use two methods to discover networks: In-Band and Out-Band discovery. Let us see the how they work.

In-Band Discovery:

With in-band discovery in 6 GHz, the station may do both scanning techniques with restrictions on active scanning. Active scanning must be performed in an organized manner where it does a preferred channel scan on what are called preferred scanning channels (PSCs). I will discuss PSCs more later. First, let's discuss the passive scanning methods in 6 GHz.

Access points operating in the 6 GHz band may use ***Fast-Initial Link Setup*** **(FILS)** that is included in the 802.11 standard. FILS is designed to improve dense environment discovery, authentication, and fast roaming. It is a similar to the Beacon frames but consume less airtime to reduce overhead.

In the FILS method APs, send the information as a broadcast containing the SSID, BSSID, and primary channel every 20 ms based on channel availability. These broadcasts are known as discovery announcement frames. The Beacon frames are also still transmitted as normal for the other bands. Compatible stations can listen for these discovery announcement frames and use them to identify and possibly connect to an AP.

NOTE: FILS goes well beyond just the discovery phase of Wi-Fi connection. When fully used, it can improve connection times related to AP discovery as well as authentication and association to the network.

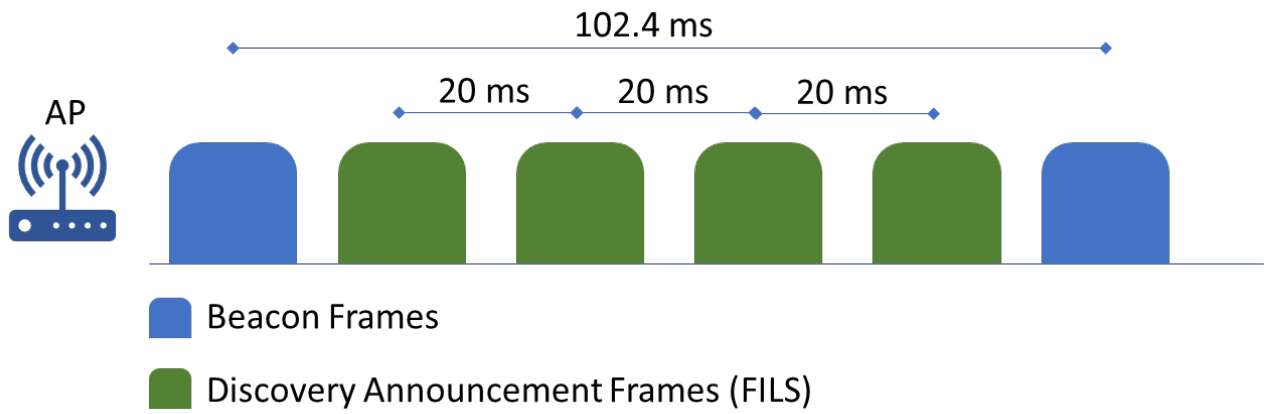


Image Copyright CWNP. Used with permission.

The characteristics of the FILS Discovery Announcement frame:

- Transmitted every 20 ms
- Broadcast Action Frame
- Contain Short SSID, Primary Channel, TBTT, and more depending on configuration

Another method of passive discovery is the ***Unsolicited Probe-Response Frames (UPR),*** also designed to reduce probe request overhead. It uses the same interval time as FILS of 20 ms and also contains detailed information as a Probe Response frame It is mainly used to support avoiding probe request storms.

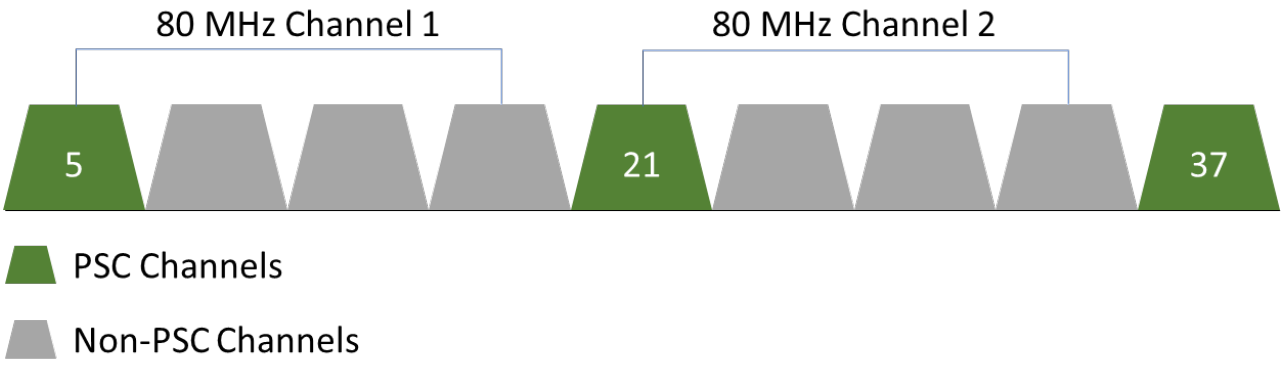
Characteristics of UPR Frames:

- Broadcast frames, unlike normal Probe Response frames
- Transmitted every 20 ms
- Contain all information needed for association
- It can carry multiple BSSIDs

Both the FILS discovery method and UPRs reduce the time a station needs to listen on a channel significantly. The station can listen for an average of just 10 ms and determine if there is an active AP on the channel that would be a good connection candidate. With a Beacon frame, the station would need to listen an average of 50 ms. This is a five-factor improvement.

The two passive methods I have mentioned above are limited listening or passive scanning activity. While both are able to be used on all 59 20MHz channels, the interval time of both methods are well designed for voice applications over Wi-Fi.

In the Active Discovery option, we have the ***Preferred Scanning Channels (PCS)***. The stations send probe requests on the PSC channels only. If the network is designed for 80 MHz channels and the primary 20 MHz channel is on a PSC, the stations will always be able to find the active APs by scanning only 15 total channels. This will not work if narrower channels are used or, at least, the stations will not be able to find APs that do not have a primary channel on a PSC.



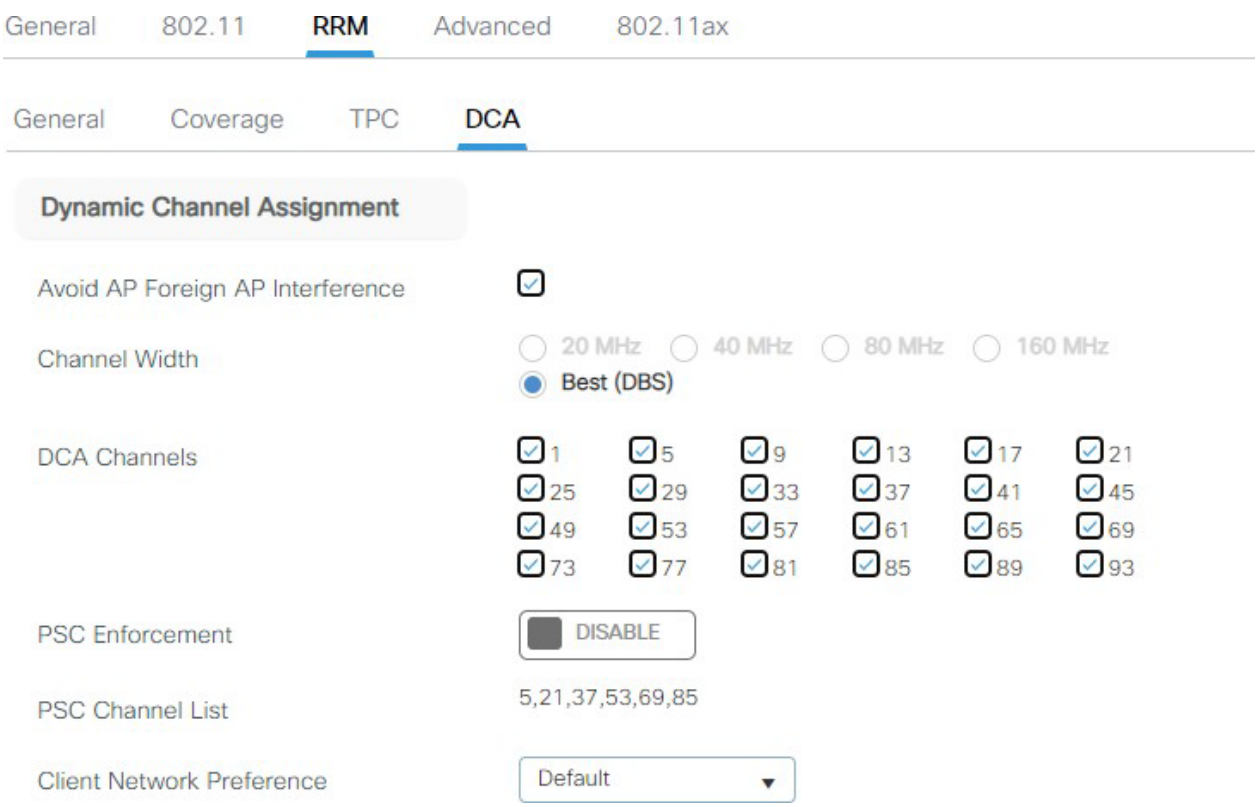
The PSC channel list is:

```
5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213 and 229
```

PSC is not likely to become the primary discovery method as out-of-band methods will be used by most traditional Wi-Fi clients (laptops, tablets, mobile phones, etc.). However, it may find a use in 6 GHz-only deployments, which would be rare for traditional access but may be valuable in specific and unique implementations. In the same way, FILS and UPR are likely to be less common in traditional deployments.

Because PSC is part of the standard and APs and clients must support it, vendors are implementing PSC parameters in their automatic configuration solutions, such as Cisco's RRM shown in the image below. Here, when PSC Enforcement is enabled, the Dynamic Channel Assignment (DCA) algorithm will only assign PSC channels as primary channels. The PSC channel list will be based on the region.

In my opinion, the introduction of the new 6 GHz band is still in need of more development in upcoming amendments or the new PHYs such Wi-Fi 7 IEEE 802.11be. I think more techniques may be developed to enhance network discovery in the 6 GHz band or existing techniques may be enhanced.



Cisco PSC Configuration for RRM

Out-of-Band Discovery:

By the name, you can understand stations will not use the 6 GHz band for discovery process when performing out-of-band discovery. Instead, they use the other bands of 2.4 Ghz and 5 GHz. In this method, the station learns about available networks by processing information from the following method:

- Reduced Neighbor Report (RNR).

With ***Reduced Neighbor Report (RNR),*** the method is not new. It was introduced in the 802.11v amendment in 2011. The part of RNR info element used to show data about neighbor APs, information such primary channel and channel width, can help the station to identify available networks that could be used for connection. When a device is connected on channel 5 in 6 GHz, for example, and it want to roam to another AP in 6 GHz, the device will probe the 5 GHz or 2.4 GHz **bands to resolve candidate 6 GHz channels to roam on.**

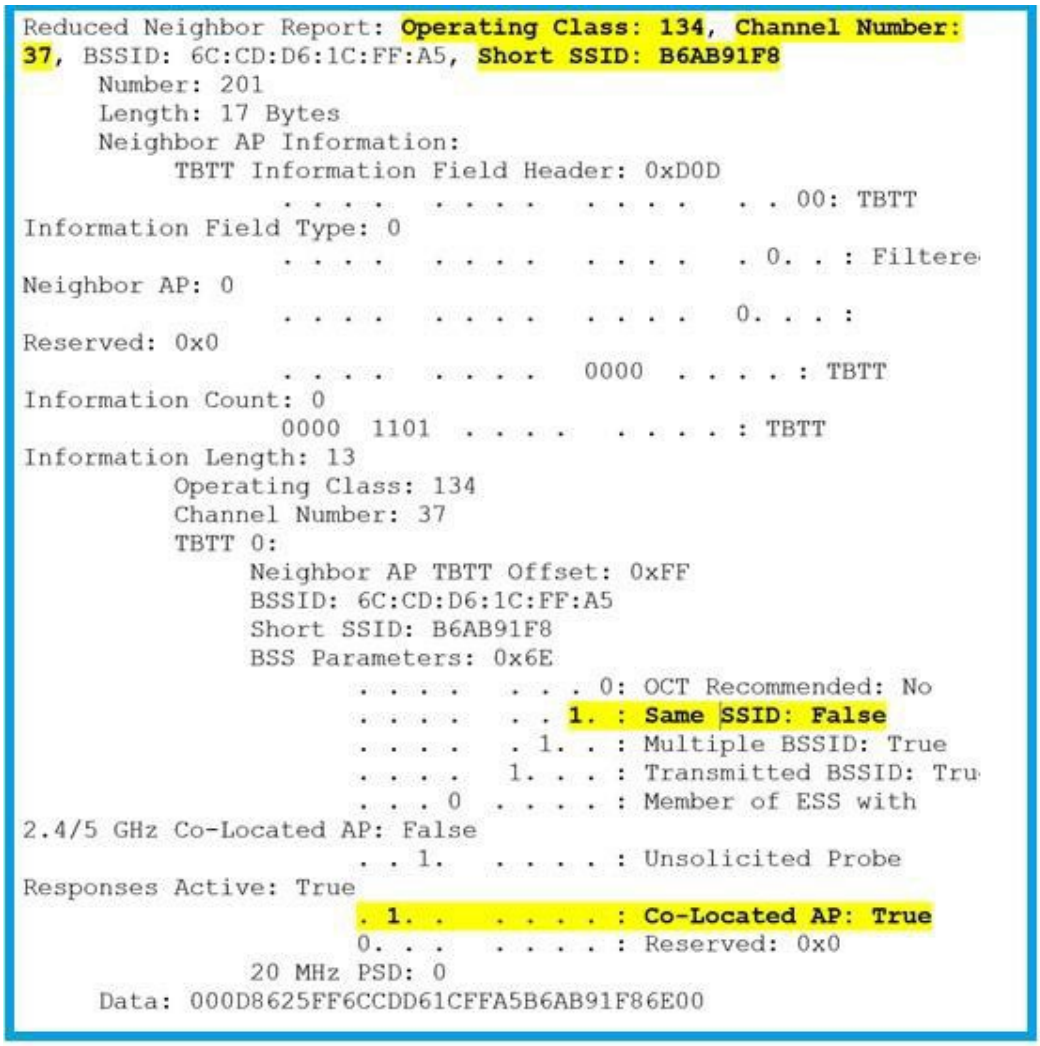


Image credited to https://www.accessagility.com/blog/how-to-detect-6-ghz-Wi-Fi-networks-using-2.4-or-5-ghz-adapters

In this method, stations and APs can use the entire 20 MHz 59 channels (if supported in the operating region) to use as primary channels with no need to send probing and increase the overhead of 6 GHz band. Of course, the network must be designed to support it and the clients must also support the behavior.

The RNR includes the BSSID and a short SSID, which is effectively a 4-byte encoding using the SSID as the input. It cannot be decoded to an exact SSID (it is not directly reversible), but the same SSID will always generate the same short SSID. The station may send a probe request in the 6 GHz channel using the short SSID (even if it is not a PSC) according to the standard. The standard says that you can send a probe request on any 6 GHz channel after waiting for the FILS delay (so that you have the opportunity to receive a broadcast frame containing the information you need without probing) if you know the BSSID, SSID, or short SSID from some other source (either RNRs from 2.4/5 GHz or some other out-of-band method).

In the ***Multiple BSSID Beacon frames and Probe Response frames***, the AP transmits information about the primary SSID it is running in the channel and additionally provides information about other SSIDs that may be accessed by the station. Let us says Employees and Guests SSIDs, it is more efficient to send information about two or more SSIDs in one response rather than respond individually. In the 802.11v the standard was aware of this to reduce overhead on management frames. Stations can passively hear probe responses and learn about neighboring SSIDs. For 6 GHz stations associated with a 6 GHz AP, they may learn of other desired SSIDs in the same AP from this method.

The picture on the following page shows that.

NOTE: Access Network Query Protocol (ANQP) messages may also be used to locate a 6 GHz AP through 2.4 or 5 GHz radios; however, RNRs are likely to become the most common method.

Conclusion:

Wi-Fi has played a successful role for keeping us connected, and realizing that importance has push us to develop more int this technology. Introducing the 6 GHz in my humbled opinion is a major shift in this technology for both industrial aspect and the life we live.

More options and services will be available, imaginary application will be witnessed, and in this matter a lot of efforts has to be done to keep the successful of Wi-Fi keep up in the new band of 6 GHz.

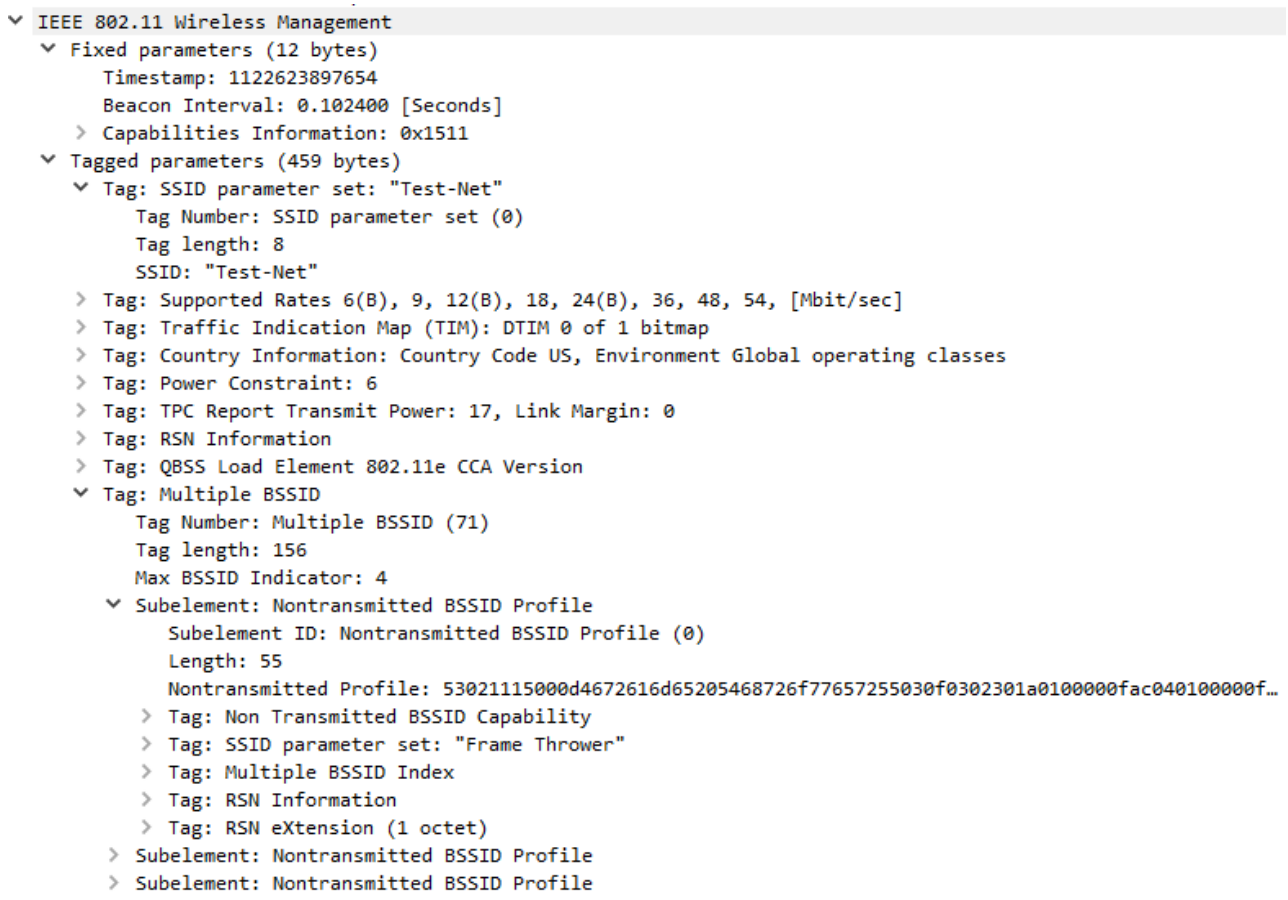


Image captured from a capture file shared by https://rowelldionicio.com/how-multiple-bssid-helps-wi-fi-6/