Define Wi-Fi 6E Band Operations and Client Connectivity

Contents

- **Introduction**
- **Prerequisites**
  - Requirements
  - Components Used
- **Background Information**
  - Wi-Fi 6E Security
    - Cisco Catalyst Wi-Fi 6E APs
- **Configure**
  - Network Diagram
  - Configurations
- **Verify**
  - Beacon Changes
    - Verification
  - Multiple Basic Service Set Identifier (BSSID)
    - Configure Multi BSSID Profile (GUI)
    - Configure Multi BSSID Profile (CLI)
    - Configure Multi-BSSID in the RF Profile (GUI)
    - Configure Multi-BSSID in the RF Profile (CLI)
    - Creation of Multiple SSIDs
    - Verification
  - AP Discovery by Wireless Clients
    - Out-of-Band
    - In-Band
  - FILS
    - Configure FILS Discovery Frames in the RF Profile (GUI)
    - Configure FILS Discovery Frames in the RF Profile (CLI)
    - Verification
  - UPR
    - Configure Broadcast Probe Response in RF Profile (GUI)
    - Configure Broadcast Probe Response in RF Profile (CLI)
    - Verification
  - PSC
    - Configure Preferred Scanning Channels in the RF Profile (GUI)
    - Configure Preferred Scanning Channels in the RF Profile (CLI)
    - Verification
  - 6-GHz Client Steering
    - Configuring 6-GHz Client Steering in the Global Configuration Mode (GUI)
    - Configuring 6-GHz Client Steering in the Global Configuration Mode (CLI)
    - Configure 6-GHz Client Steering on the WLAN (GUI)
    - Configure 6-GHz Client Steering on the WLAN (CLI)
    - Verification

Client Connectivity
Tests with AP 9166
Troubleshoot
Related Information

Introduction

This document describes how to configure Wi-Fi 6E Band Operations and what to expect on different clients.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless Lan Controllers (WLC) 9800
- Cisco Access Points (APs) that support Wi-Fi 6E.
- IEEE Standard 802.11ax.
- Network tools: Wireshark

Components Used

The information in this document is based on these software and hardware versions:

- WLC 9800-CL with Cisco IOS® XE 17.9.3.
- APs C9136, CW9162 and CW9166.
- Wi-Fi 6E Clients:
  - Lenovo X1 Carbon Gen11 with Intel AX211 Wi-Fi 6 and 6E Adapter with driver version 22.200.2(1).
  - Netgear A8000 Wi-Fi 6 and 6E Adapter with driver v1(0.0.108);
  - Mobile Phone Pixel 6a with Android 13;
  - Mobile Phone Samsung S23 with Android 13.
- Wireshark v4.0.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The key thing to know is that Wi-Fi 6E is not an entirely new standard, but an extension. At its base, Wi-Fi 6E is an extension of the Wi-Fi 6 (802.11ax) wireless standard into the 6-GHz radio-frequency band.

Wi-Fi 6E builds on Wi-Fi 6, which is the latest generation of the Wi-Fi standard, but only Wi-Fi 6E devices and applications can operate in the 6-GHz band.

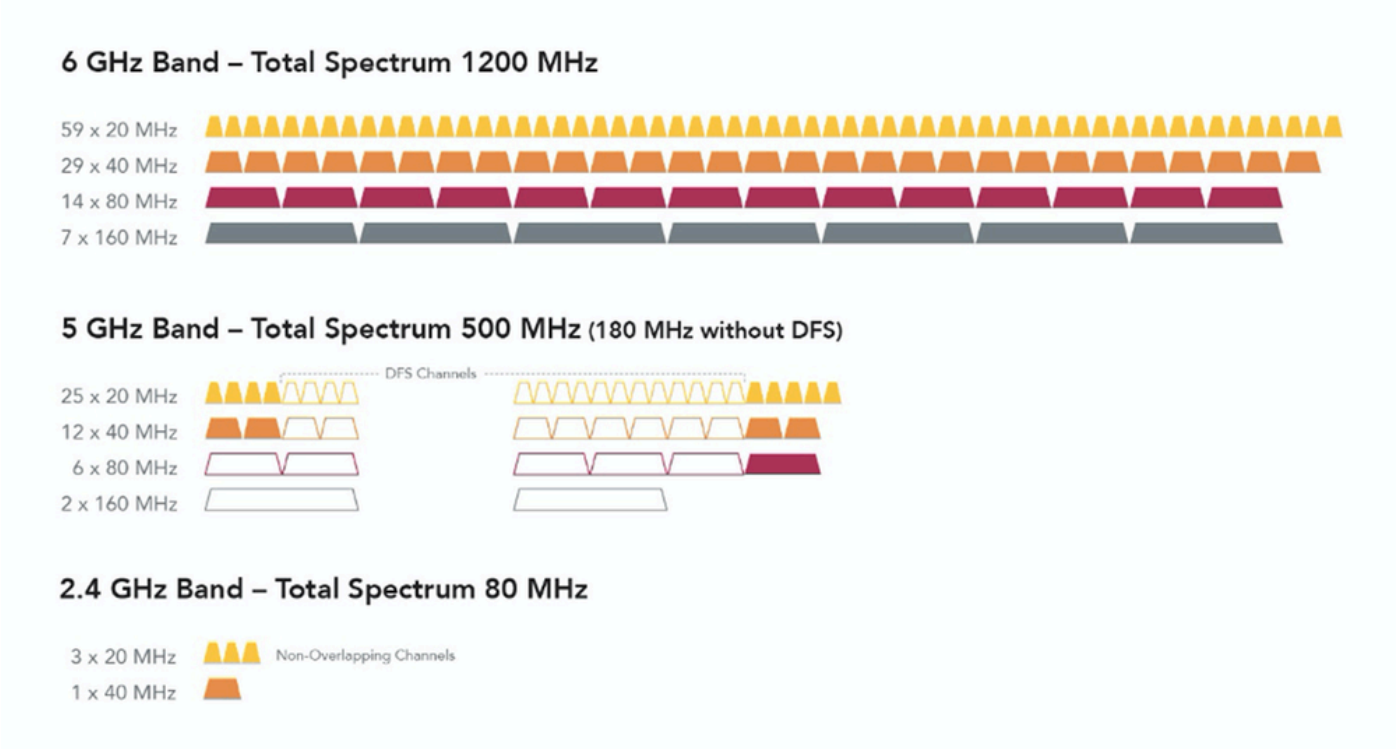
Since the 6-GHz spectrum is new and accepts only Wi-Fi 6E devices, it does not have any of the old issues that clogg up current networks.

It offers better:

- **Capacity:** In US defined by FCC, there is additional spectrum of 1200 MHz worth or 59 new channels. The new 6-GHz band employs fourteen 80-MHz and seven 160-MHz channels. Other countries can have different spectrum amount allocated for WiFi 6E. Please check Countries Enabling Wi-Fi in 6 GHz (Wi-Fi 6E) for updated info on country adoption of WiFi 6E.

- **Reliability:**Wi-Fi 6E provides a new standard of reliability and predictability of connection that shortens the gap between wireless and wired connections. Devices from Wi-Fi 1 (802.11b) through Wi-Fi 6 (802.11ax) are not supported on 6 GHz.

- **Security:**Wi-Fi Protected Access 3 (WPA3) is a mandatory requirement for the Wi-Fi 6E network and secures the network better than ever. And since only Wi-Fi 6 products are to use this network, there are no legacy security issues to deal with. WPA3 provides new authentication and encryption algorithms for networks and furnishes fixes for issues that were missed by WPA2. It also implements an additional layer of protection from deauthentication and disassociation attacks.



Comparizon of 2.4, 5 and 6 GHz wifi spectrum and channels

For additional background information about Wi-Fi 6E, please check our Wi-Fi 6E: The Next Great Chapter in Wi-Fi White Paper .

There are various managements and changes in Wi-Fi 6E. In the Verification section of this document, there is a small description of some of these enhancements accompanied by the verification in the real environment.

Wi-Fi 6E Security

Wi-Fi 6E uplevels security with Wi-Fi Protected Access 3 (WPA3) and Opportunistic Wireless Encryption (OWE) and there is no backward compatibility with Open and WPA2 security.

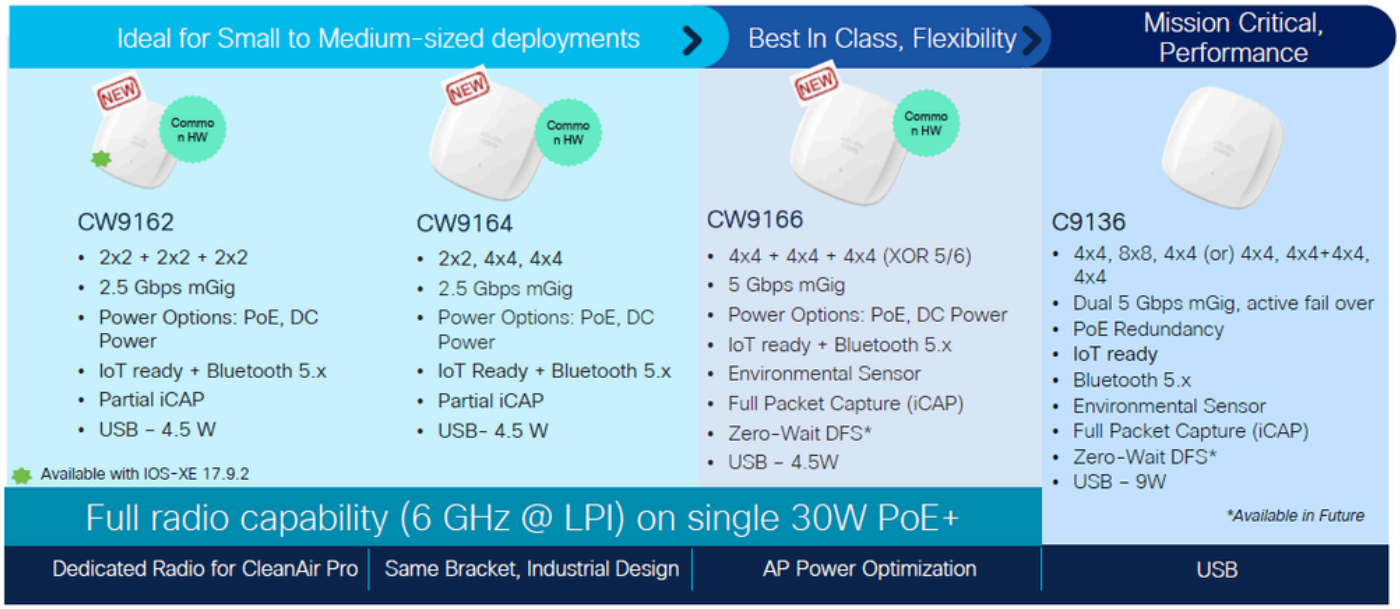
WPA3 and Enhanced Open Security are now mandatory for Wi-Fi 6E certification and Wi-Fi 6E also requires Protected Management Frame (PMF) in both AP and Clients.

When configuring a 6GHz SSID there are certain security requirements that must be met:

- WPA3 L2 security with OWE, SAE or 802.1x-SHA256
- Protected Management Frame Enabled;
- Any other L2 security method is not allowed, that is, no mixed mode possible.

To know more about detailed information about WPA3 implementation in Cisco WLANs, including client security compatibility matrix, please feel free to check the WPA3 Deployment Guide.

Cisco Catalyst Wi-Fi 6E APs

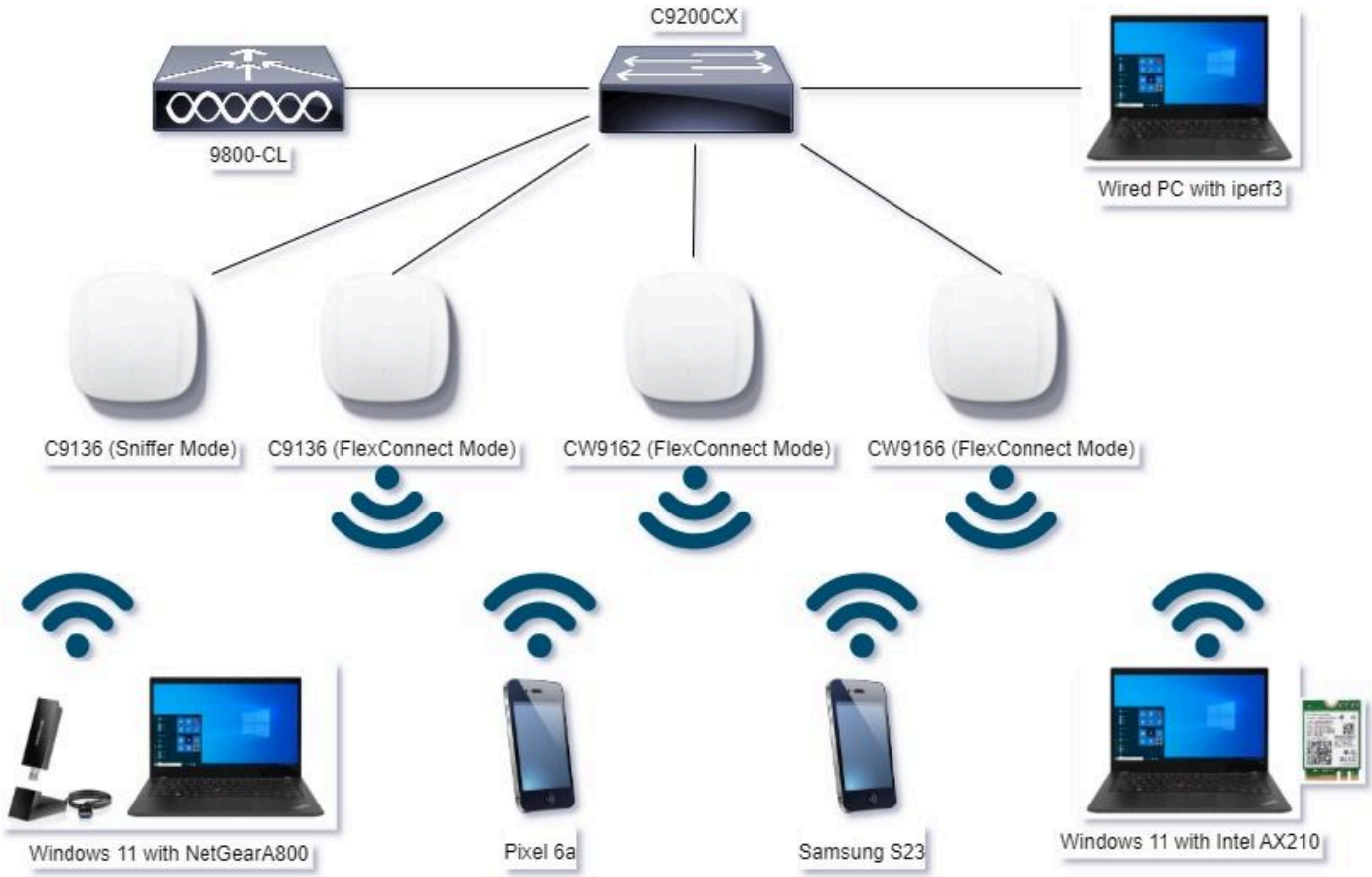


Wi-Fi 6E Access Points

Configure

In this section, it is shown the basic WLAN configuration. Later in the doc, it is shown how to configure each Wi-Fi 6E elements and how to verify the configuration and expected behavior.

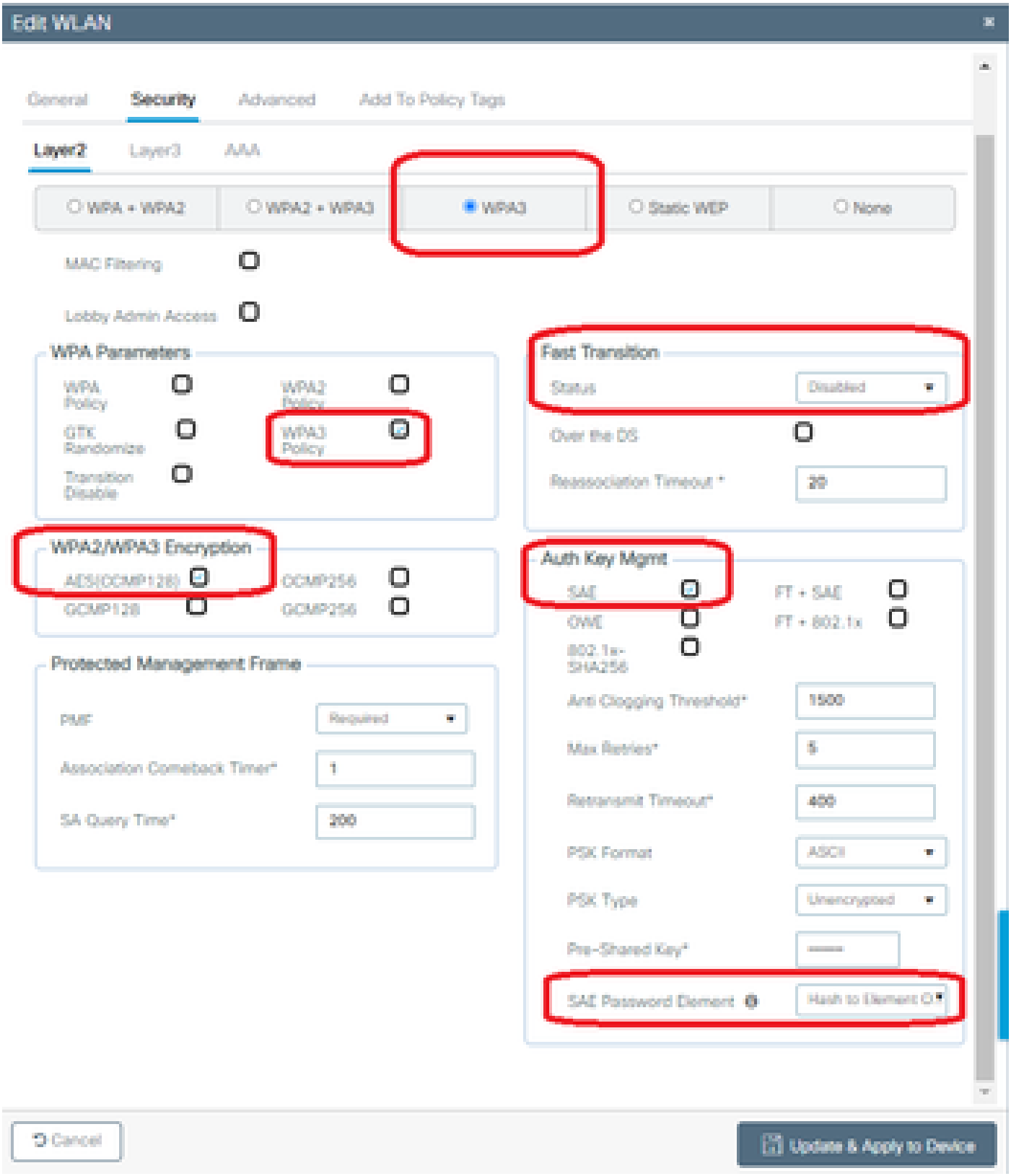
Network Diagram



Network Diagram

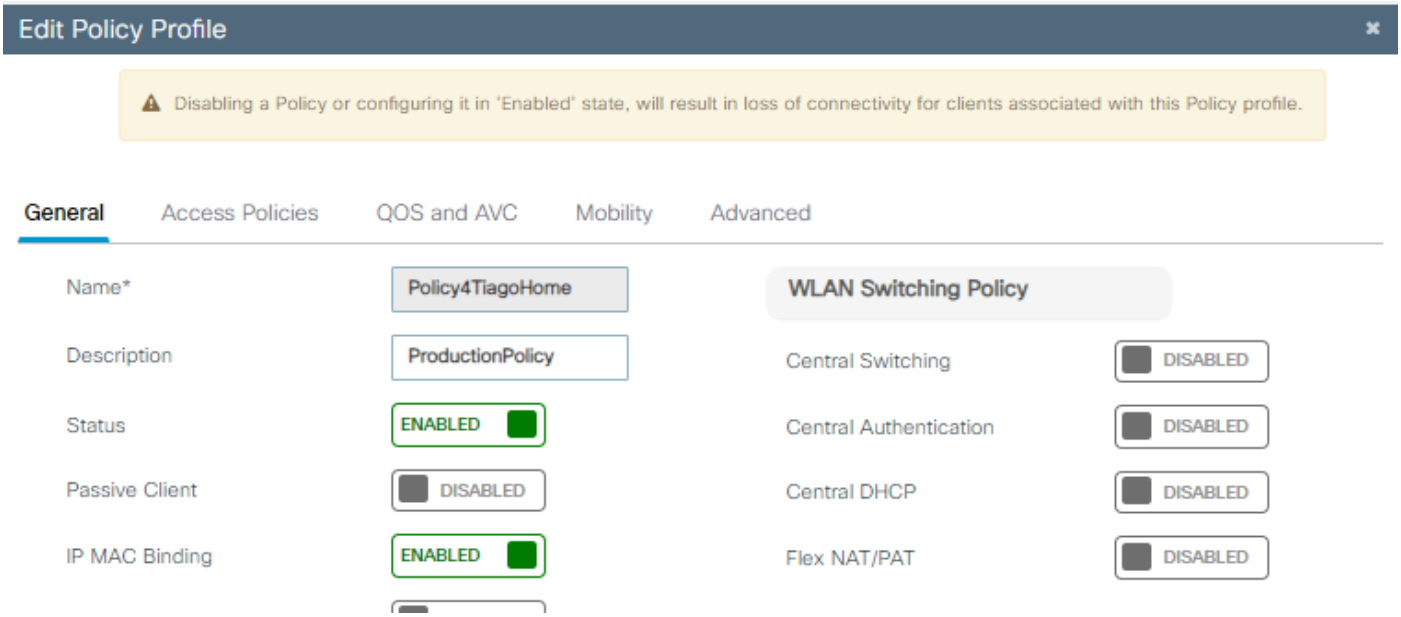
Configurations

In this document, the initial WLAN base security configuration is WPA3+AES+SAE with H2E as shown here:



The WLAN configuration and push to APs is done as per the steps in the section: How to Configure WLANs from the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS® XE Cupertino 17.9.x.

The WLAN is mapped to a locally switched policy profile with switching and authentication policy as shown here:



Verify

Use this section to confirm that your configuration works properly.

The verification section is divided in new changes or features introduced and observations per client type if applicable.

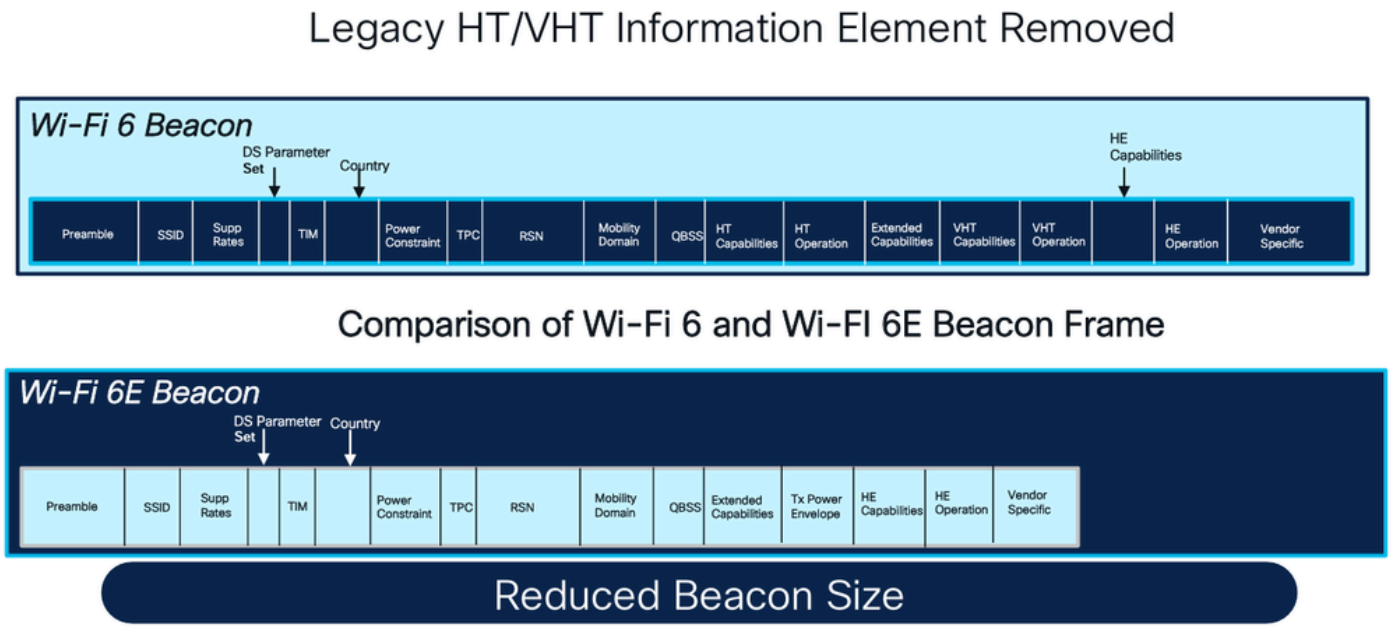
There is a Configuration and Verification section per feature.

In these tests and verifications, the Over the Air Captures (OTAs) were performed with an AP in sniffer mode.

You can check this article to find how to setup an AP in sniffer mode: APs Catalyst 91xx in Sniffer Mode.

Beacon Changes

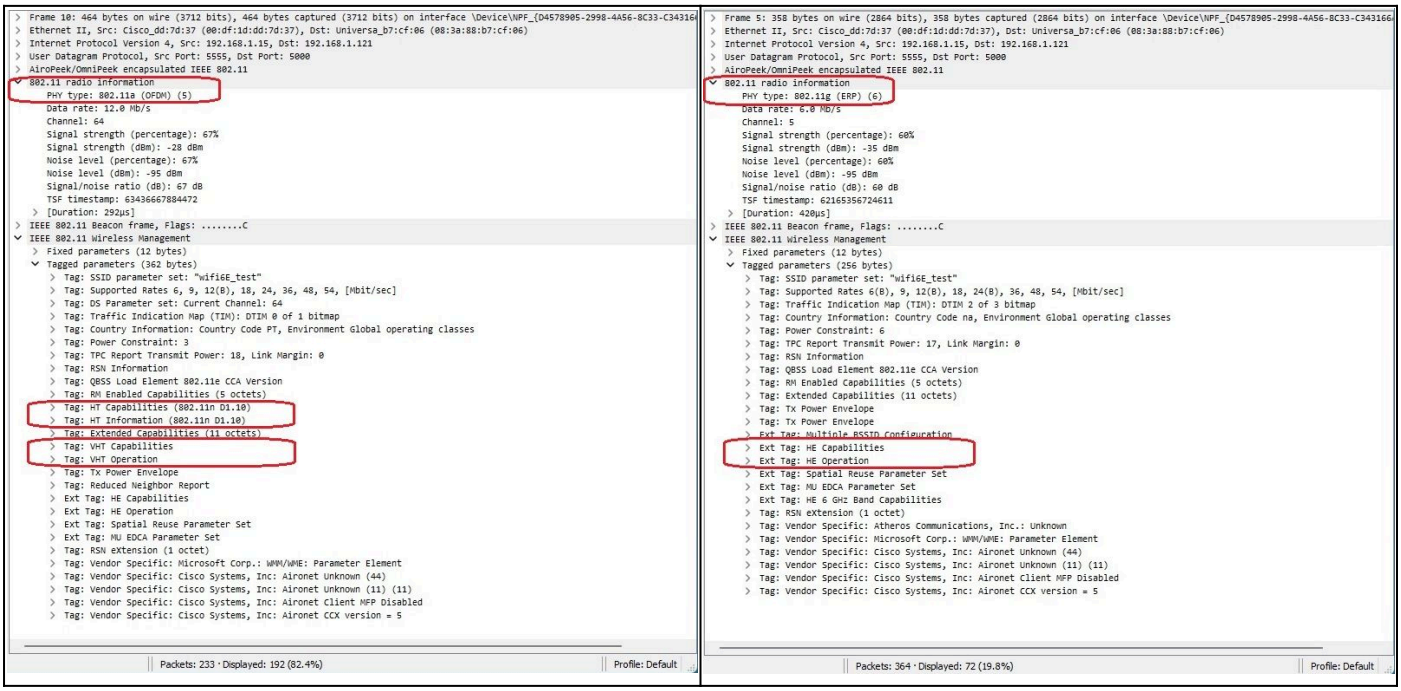
Beacons still exist on Wi-Fi 6E, and are sent every 100ms by default, however they are a bit different from the Wi-Fi 6 (2.4GHz or 5GHz) beacons. In Wi-Fi 6 the beacon contains HT and VHT Information Elements, however in Wi-Fi 6E, those elements are removed and there is only HE Information element.

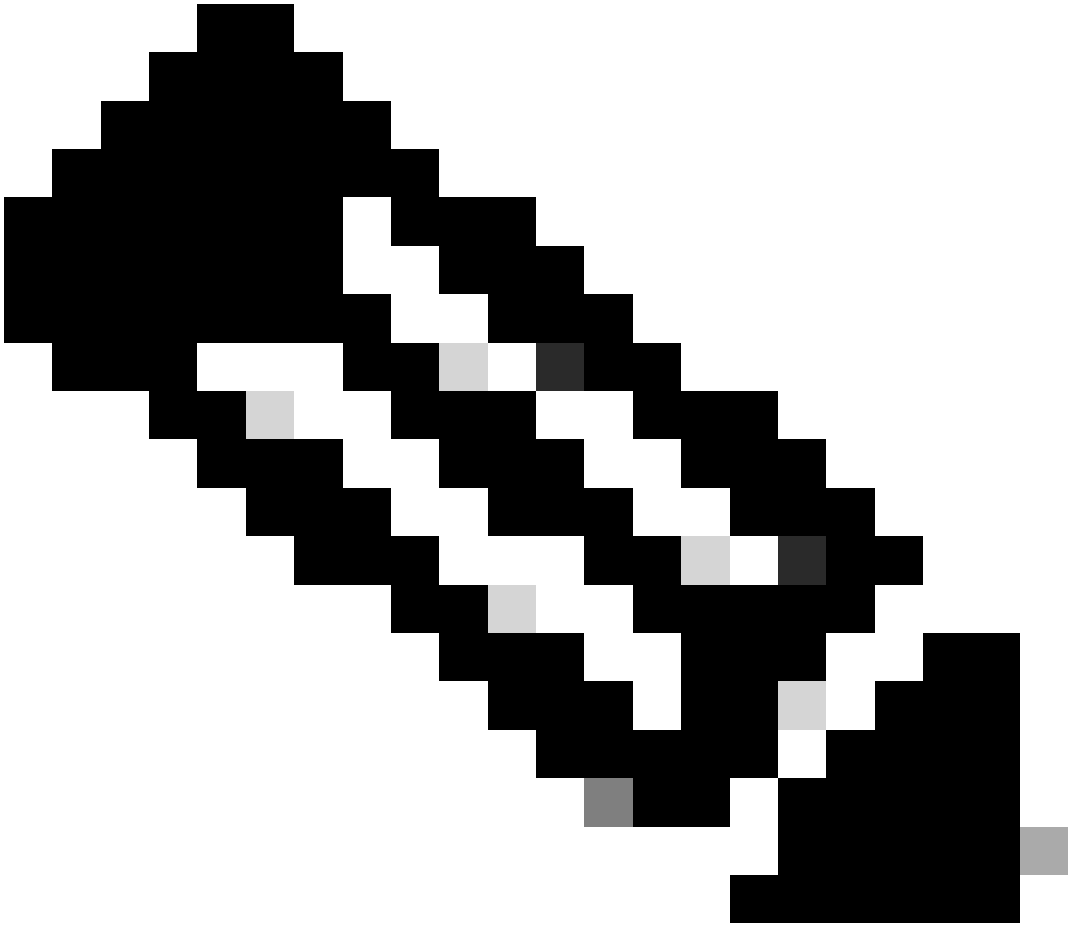


Comparison of Wi-Fi 6 and Wi-Fi 6E Beacon Frames

Verification

Here is what we can see in the OTA:





Note: DS Parameter set is an optional field and can be not included in the beacon frames.

Multiple Basic Service Set Identifier (BSSID)

Multiple BSSID is a capability originally specified in 802.11v. It Combines multiple SSID information in a single beacon frame, that is, instead of a beacon for each SSID, it sends a single beacon that contains various BSSIDs.

This is mandated in Wi-Fi 6E and the main goal is to conserve Air Time.

Configure Multi BSSID Profile (GUI)

Step 1 - Choose Configuration > Tags & Profiles > Multi BSSID.

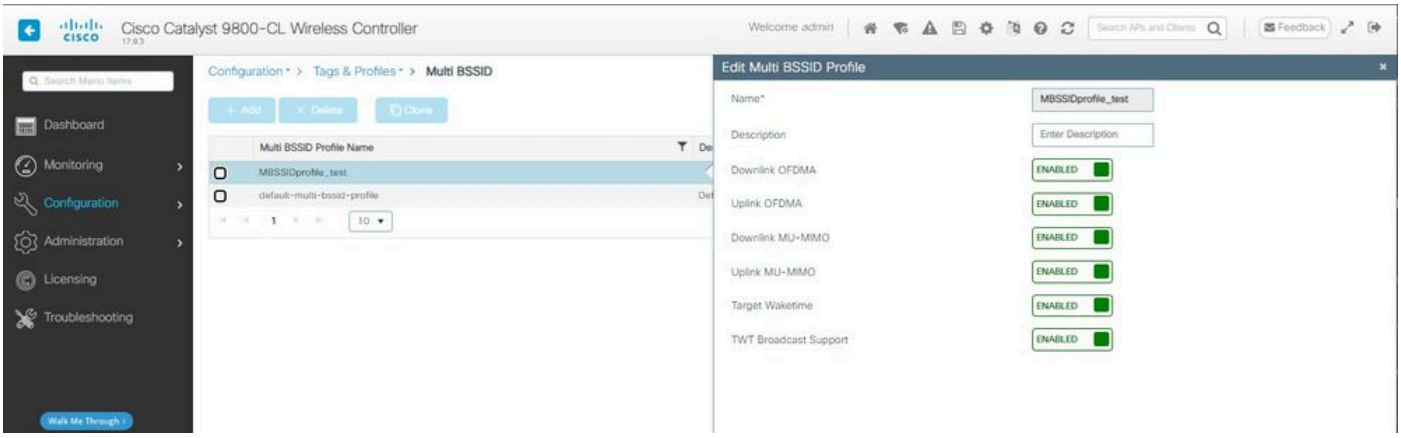
Step 2 - Click Add. The Add Multi BSSID Profile page is displayed.

Step 3 - Enter the name and the description of the BSSID profile.

Step 4 - Enable the these 802.11ax parameters:

- **Downlink OFDMA**
- **Uplink OFDMA**
- **Downlink MU-MIMO**
- **Uplink MU-MIMO**
- **Target Waketime**
- **TWT Broadcast Support**

Step 5 - Click **Apply to Device**.



Configure Multi BSSID Profile (CLI)

```
Device# configure terminal
Device (config)# wireless profile multi-bssid multi-bssid-profile-name
Device (config-wireless-multi-bssid-profile)# dot11ax downlink-mumimo
```

Configure Multi-BSSID in the RF Profile (GUI)

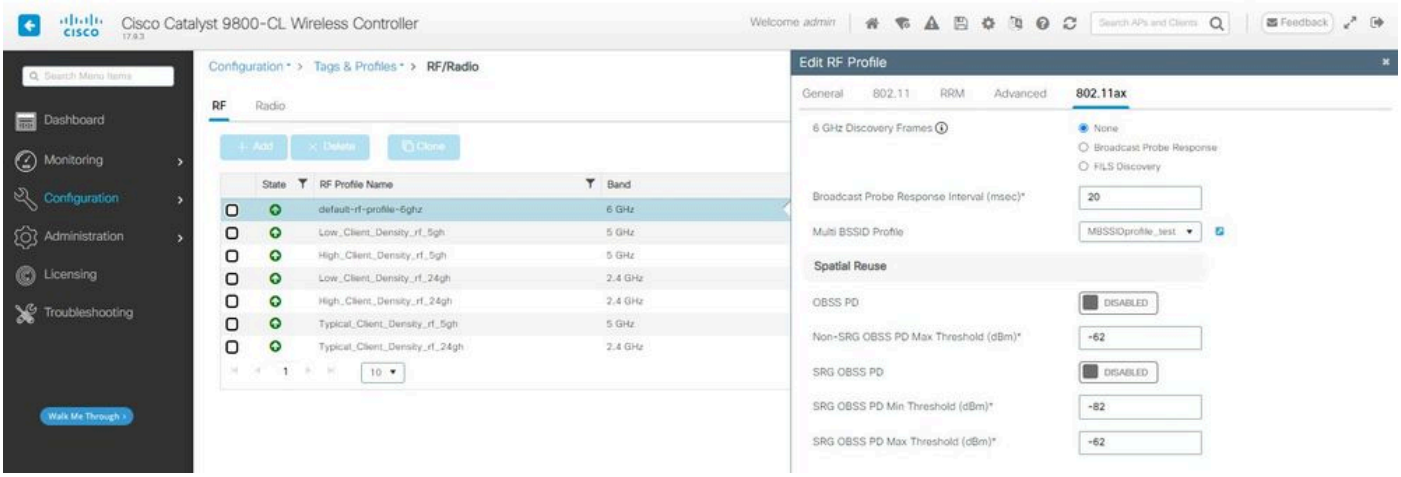
Step 1 - Choose Configuration > Tags & Profiles > RF/Radio.

Step 2 - In the **RF** tab, click **Add.** The Add RF Profile page is displayed.

Step 3 - Choose the **802.11ax** tab.

Step 4 - In the **Multi BSSID Profile** field, choose the profile from the drop-down list.

Step 5 - Click **Apply to Device**.

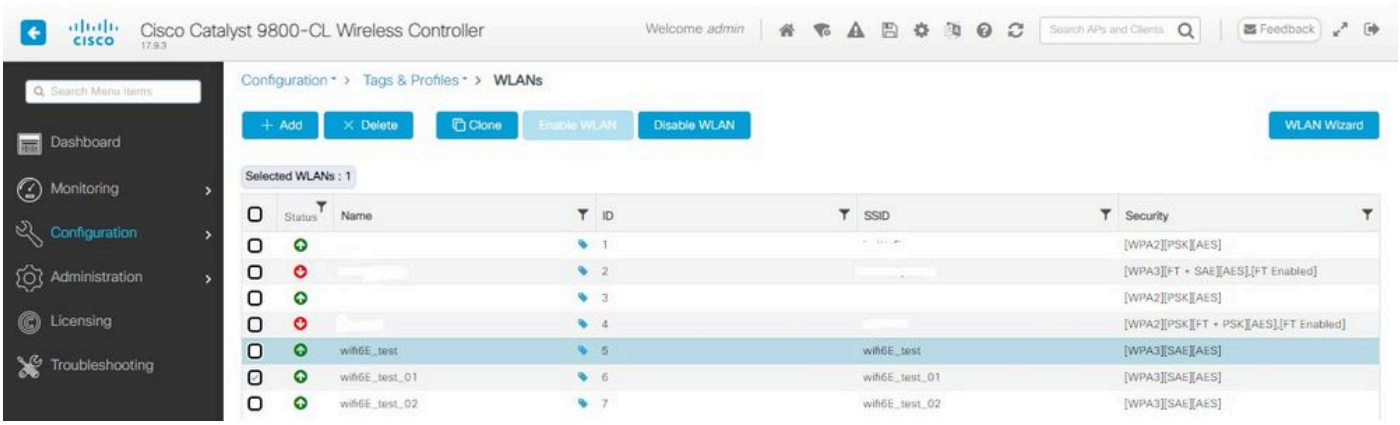


Configure Multi-BSSID in the RF Profile (CLI)

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax multi-bssid-profile multi-bssid-profile-name
```

Creation of Multiple SSIDs

To verify the MBSSID feature, you must have various SSIDs enabled and pushed to the APs. In this verification, three SSIDs are used:



Verification

To verify if the configuration is in place issue the commands shown here:

<#root>

WLC9800#

show ap rf-profile name *default-rf-profile-6ghz* detail | b 802.11ax

```
802.11ax
 OBSS PD : Disabled
```

```
 Non-SRG OBSS PD Maximum : -62 dBm
 SRG OBSS PD : Disabled
 SRG OBSS PD Minimum : -82 dBm
 SRG OBSS PD Maximum : -62 dBm
 Broadcast Probe Response : Disabled
 FILS Discovery : Disabled
 Multi-BSSID Profile Name :
```

MBSSIDprofile_test

```
NDP mode : Auto
Guard Interval : 800ns
PSC Enforcement : Disabled

WLC9800#
WLC9800#
```

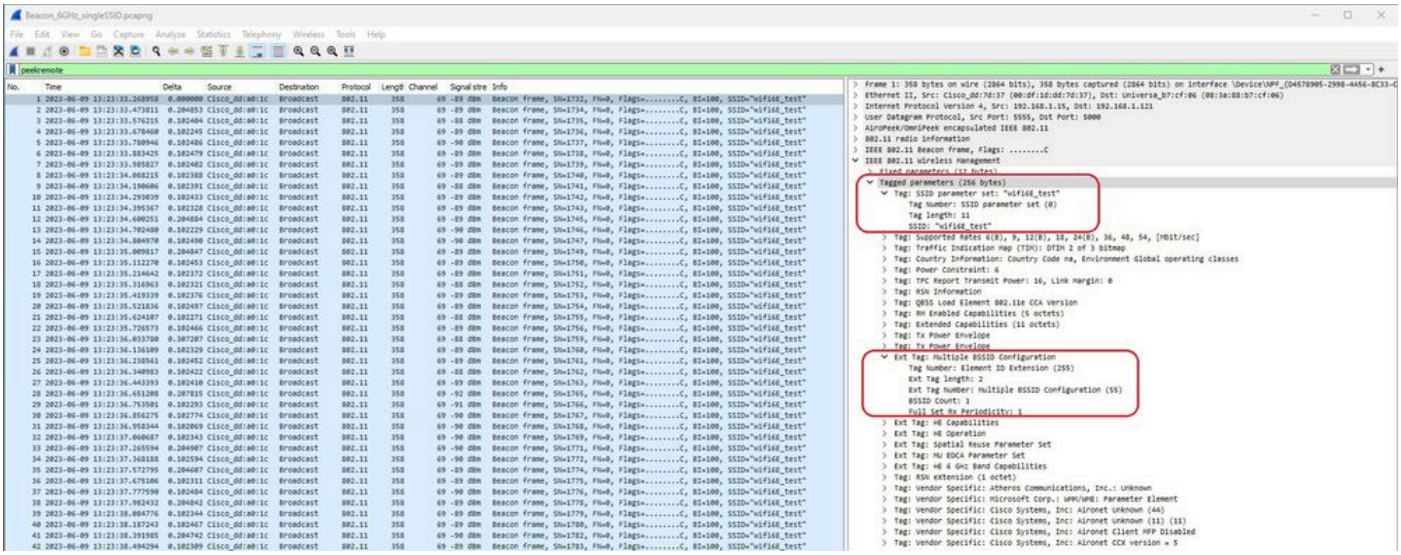
show wireless profile multi-bssid detailed *MBSSIDprofile_test*

Multi bssid profile name :

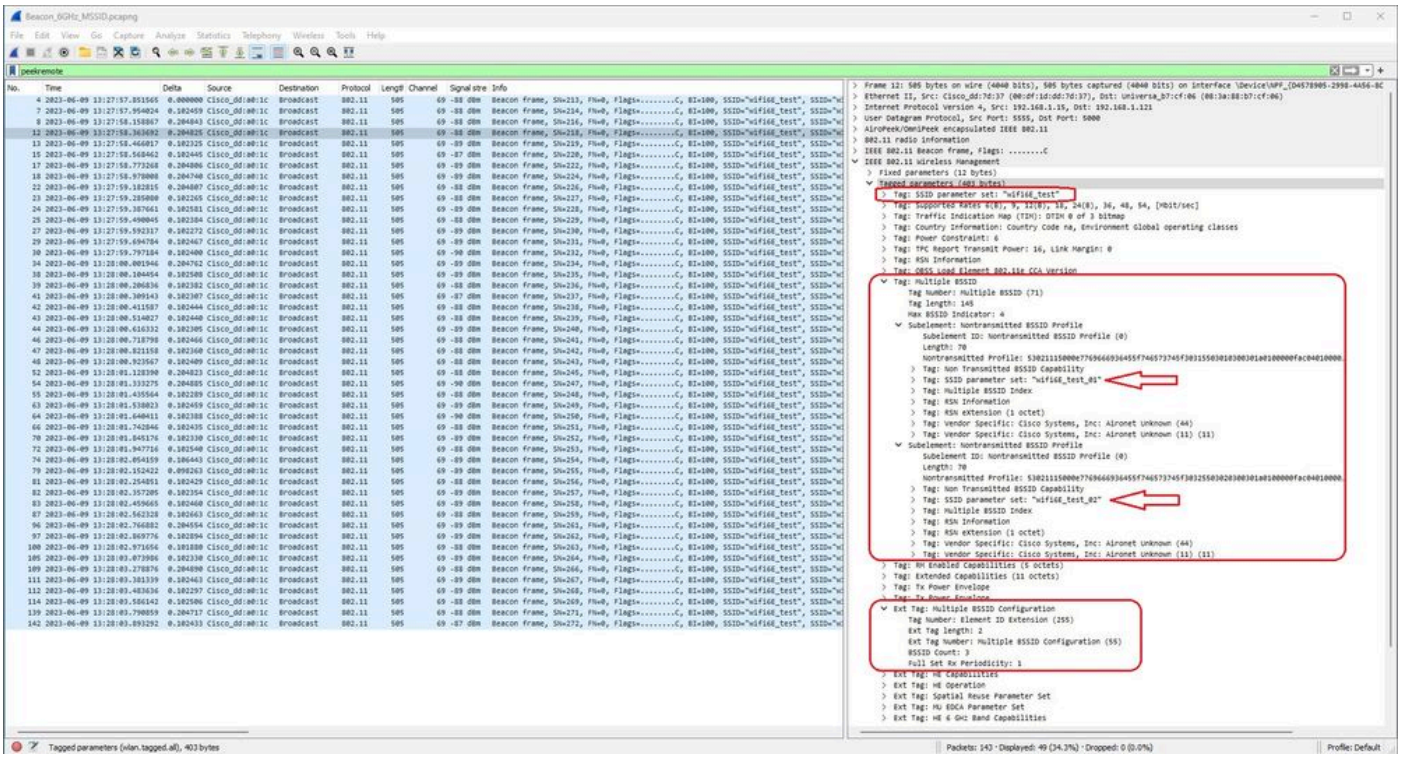
MBSSIDprofile_test

```
-------------------------------------------------
Description :
802.11ax parameters
OFDMA Downlink : Enabled
OFDMA Uplink : Enabled
MU-MIMO Downlink : Enabled
MU-MIMO Uplink : Enabled
Target Waketime : Enabled
TWT broadcast support : Enabled

WLC9800#
```

Here is what you can see in the OTA captures when using Single BSSID:



Here is what you can see in the OTA captures when using Multiple BSSIDs:



AP Discovery by Wireless Clients

Discovery is the process where a client device, on power-up or when it enters a building, finds a suitable access point to connect to.

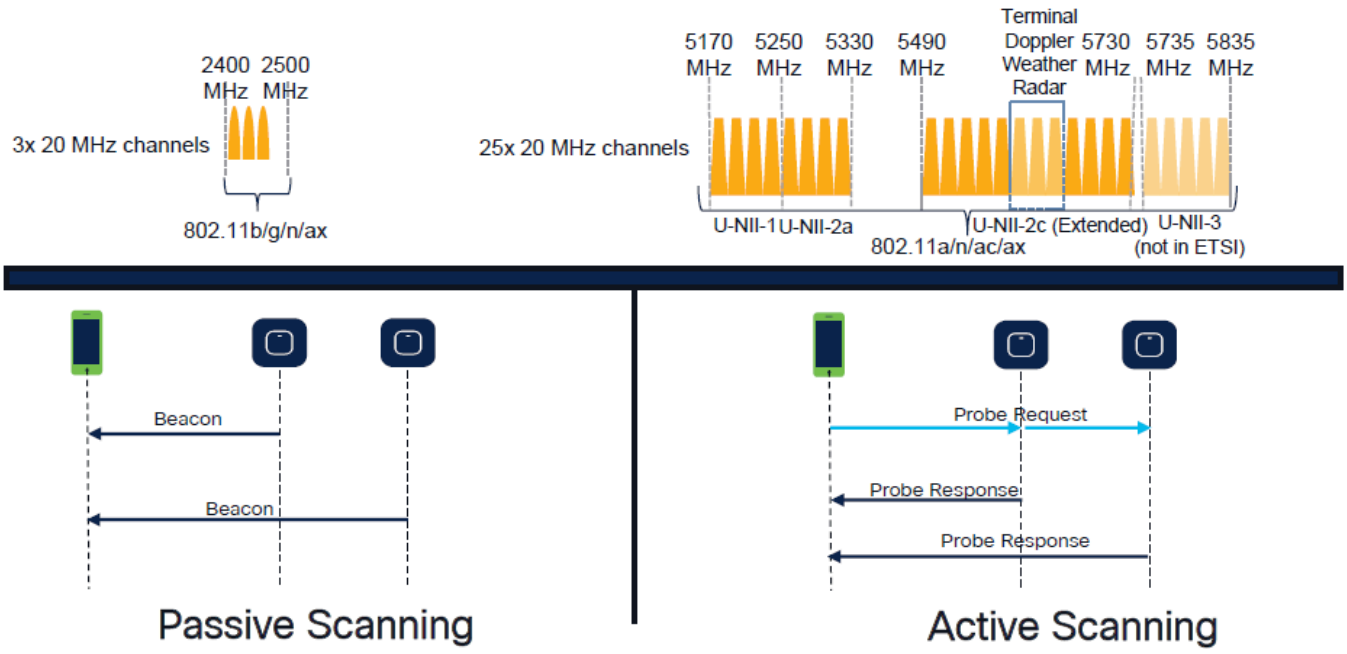
The simplest way to perform discovery, used by most client devices today, is to scan channels in turn by the transmission of one or more probe requests, it then listens for responses from access points in the area, examines the probe responses to see if any of the SSIDs match profiles in the client, then steps to the next channel.

This has three drawbacks:

- it takes significant time, which can affect application performance while the radio is away from its serving channel;
- it requires many probe request and response frames on the air, which reduces airtime efficiency;
- it affects client battery life.

The time – in the order of 20 msec per non-DFS channel or up to 100ms on DFS channel – is already an issue in the 5 GHz band. It becomes more significant when we realize that a Wi-Fi 6E client can have to scan every one of the 59 possible 20 MHz channels in the band to discover all available access points.

The legacy methods aka Passive Scanning and Active Scanning, do not scale on 6GHz. On 2.4 and 5Ghz, it is used the "hunt-and-seek" method to scan BSSIDs or for APs, either by Passive Scanning or Active Scanning:



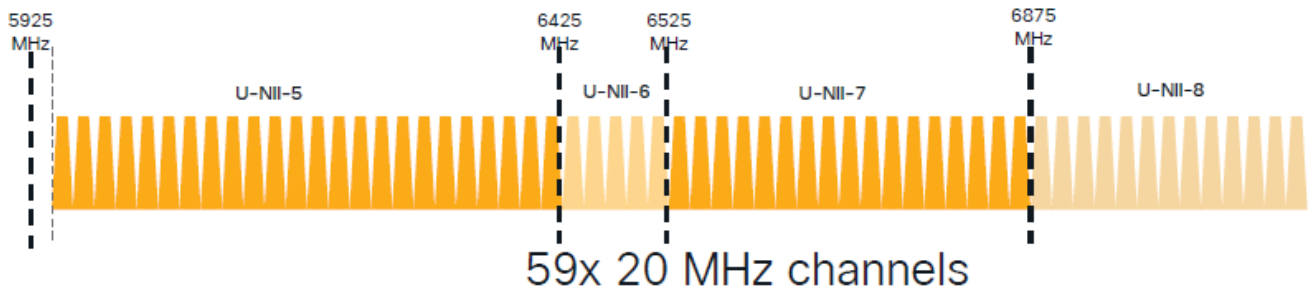
Traditionally, wireless devices communicate with access points in a specific exchange of information. Client devices use an active “hunt-and-seek” approach to scan for nearby APs.

This active scanning approach involves the send of ***probe request*** frames along the 2.4 GHz and 5 GHz frequency spectrum. An AP would respond with a ***probe response*** frame that contains all the necessary basic service set (BSS) information to connect to the network.

This information would consist of SSID, BSSID, channel width, and security information among other things.

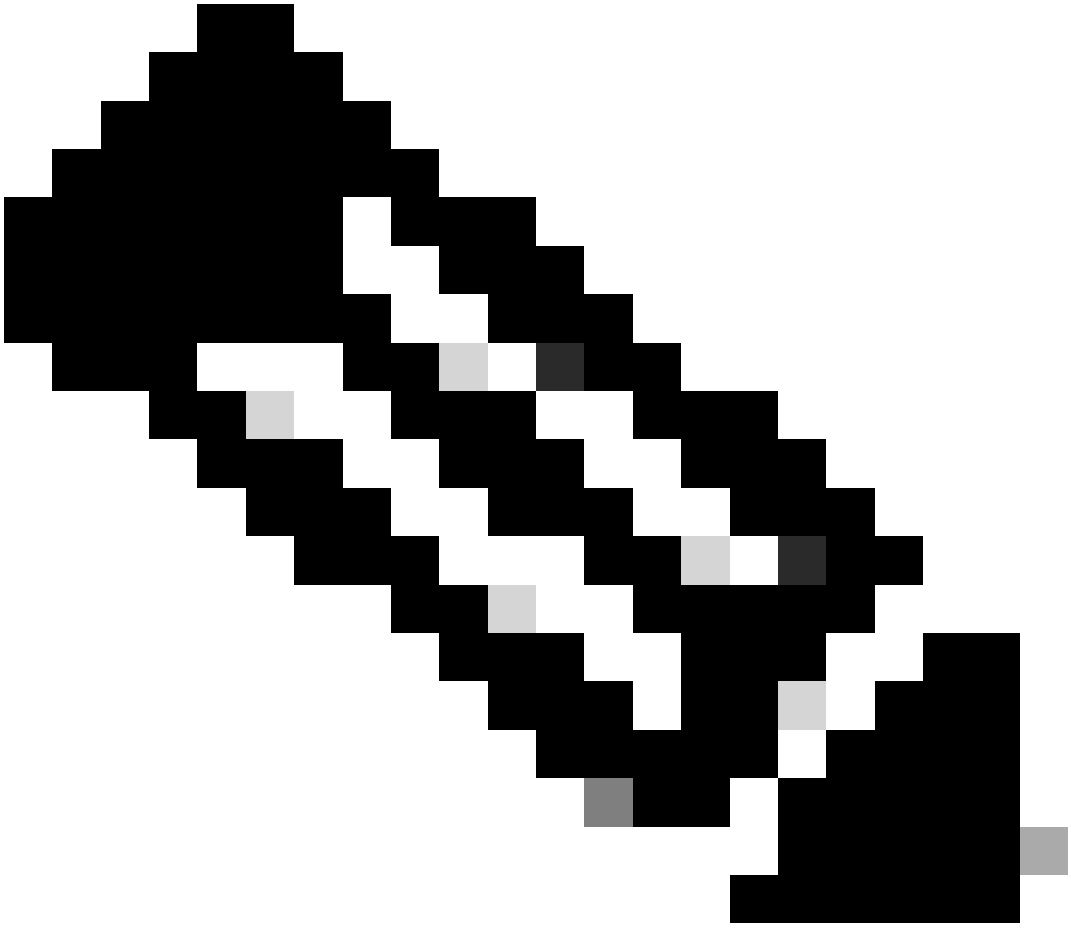
This active “hunt-and-seek" approach to network connectivity is no longer necessary and is actually discouraged in Wi-Fi 6E on the 6 GHz band because it is now inefficient to broadcast the same probe requests over so many channels.

Wifi clients can send only Probe Requests on 20 MHz channels, and on 6Ghz there are up to 59x20MHz, which means that the client would need to scan all 59 channels that sums to ~6 seconds to passive scan all 59 channels:



On Wi-Fi 6E, there are new AP Discovery Mechanisms:

At the time of writing this document, the windows/intel and android clients tested supported FILS and broadcast probe responses, however it was not the same across Apple and some Android clients which can possibly not support FILS or broadcast probe responses.
Due to this problem a preferred scanning channel (PSC) is considered more relevant. However as currently different wireless client vendors are possible to not be fully compatible with wifi 6 scanning, it can not be an ideal approach to configure only 6ghz wlan/ssid.



Note: If you want to make sure to know what discovery mechanism each client supports, you must reach to wireless client vendor support.

So based on wireless client vendor support, currently it is possible to be relevant to have an out-of-band discovery with 2.4/5Ghz enabled for a RNR /Reduced Neighbor Report option wherein wireless clients can discover a 6Ghz SSID on an AP by listening to RNR Information Element included in the 2.4/5Ghz beacons from that AP.

It very unlikely that you have a WLC and AP providing ONLY 6GHz WLAN, and most likely there are other WLANs beeing broadcasted. Taking this into account its recommended to use those legacy bands to advertise the 6GHz only WLANs, in the RNR information element, for client devices that do not support In-Band discovery mechanisms.

In the end there is no added configuration burden because the RNR is a feature already supported by Wi-Fi 6E devices and therefore Wi-Fi 6E devices support it.

Out-of-Band

Out-of-band discovery is used for cross-communication on all 3 frequency bands (2.4, 5, and 6 GHz). This method, introduced in 802.11v is known as Reduced Neighbor Reporting (RNR).

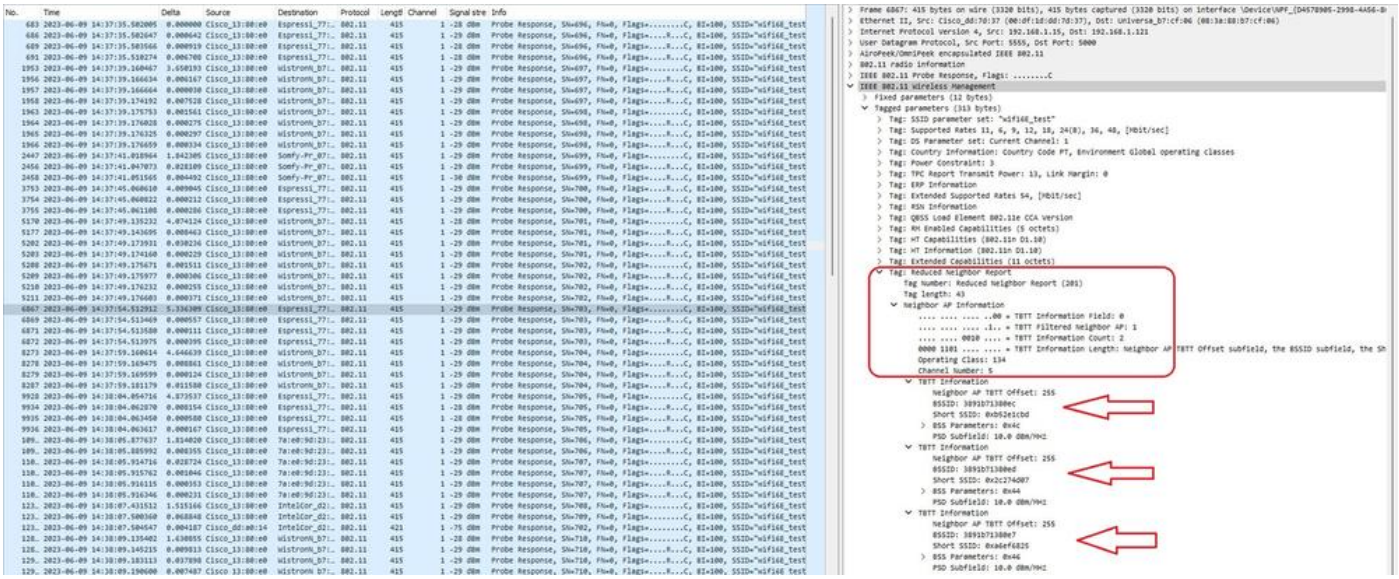
Essentially, when a Wi-Fi 6E-capable AP sends a probe response frame it includes, (along with basic service set (BSS) information for the 2.4 or 5 GHz band) RNR information about its 6 GHz radio.

This RNR serves as enough information for the client device to roam between 6 GHz and 2.4 or 5 GHz networks.

In summary: Clients use only RNR to discover WLANs in 6 GHz through legacy bands. They do not scan 6 GHz straight away.

If we capture the traffic on 2.4 or 5GHz over the air, and observe the Probe Responses.

This is what is expected to be seen for example in an OTA capture of a Probe Response on channel 1 (2.4GHz) for an SSID broadcast on 2.4, 5 and 6GHz:



You can see the RNR reporting the same SSID on 6GHz channel 5 and 2 other BSSIDs.

This is for the same SSID, but a Probe response on 5GHz:

In-Band

In-band discoveryis used for communication between 6 GHz devices, and there are three methods of in-band discovery:

- **Fast Initial Link Setup** (FILS) and **unsolicited probe response** (UPR) frames are two passive methods of in-band discovery. It is FILS or UPR and not both. 6 GHz Discovery Frames are needed only if 6 GHz is the only radio that is operational.
- **Preferred Scanning Channels** (PSC) is an active method of in-band discovery. Wireless clients probe only PSC channels; scans Non PSC if it detects from RNR.

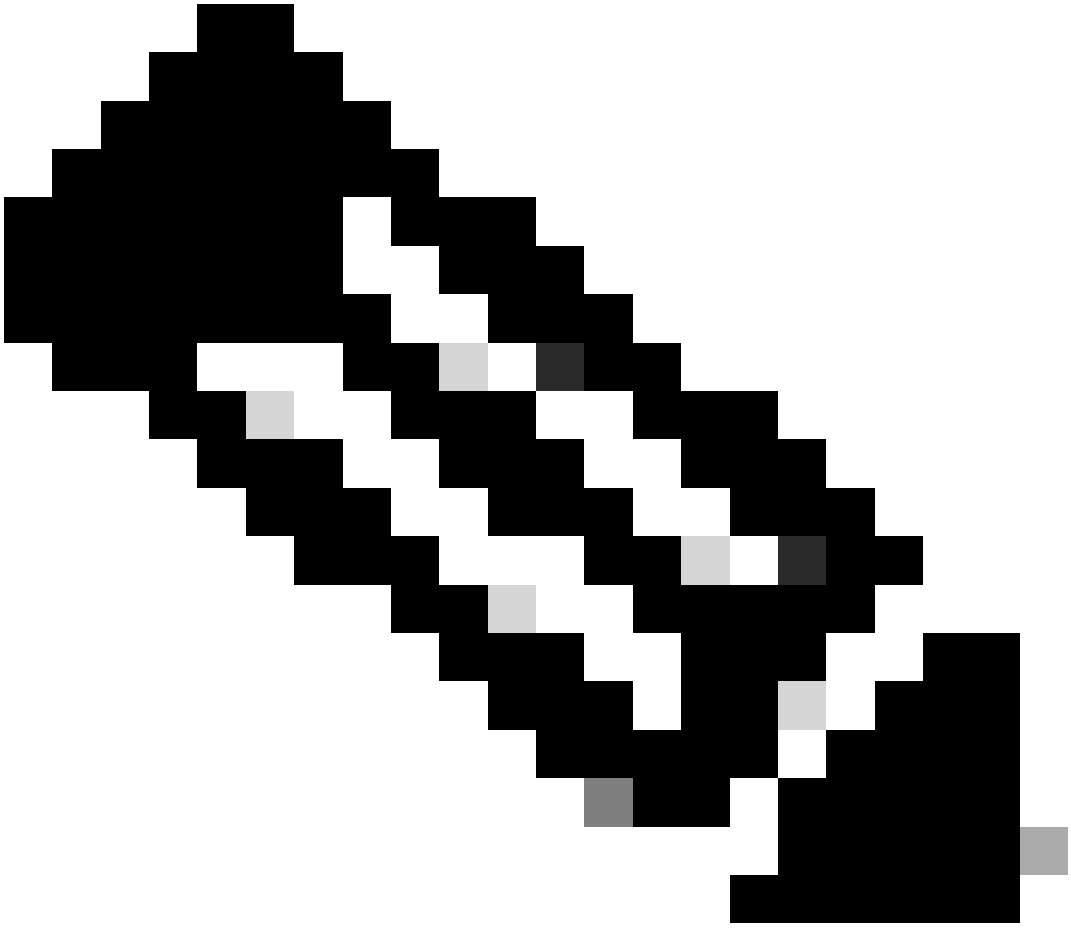
Remember that these are in-band discovery methods, which means that this only applies to Wi-Fi 6E clients that connect to wireless networks on the 6 GHz band.

FILS

FILS is part of IEEE 802.11ai Standard and addresses improvements in Network and BSS Discovery, Authentication and Association, DHCP and IP address setup.

FILS uses “discovery announcement frames” which are essentially condensed beacon frames. Only crucial information is sent in a FILS frame: Short SSID, BSSID, and channel, for the AP to decide on the AP to connect.

If FILS is configured, the 6 GHz AP broadcasts an announcement discovery frame approximately every 20 milliseconds which consumes less air time and reduces probe request overhead.



Note: 6 GHz Discovery Frames are needed only if 6 GHz is the only radio that is operational. When other radios (2.4/5 GHz) are operational, clients detect 6 GHz presence from RNR IE.

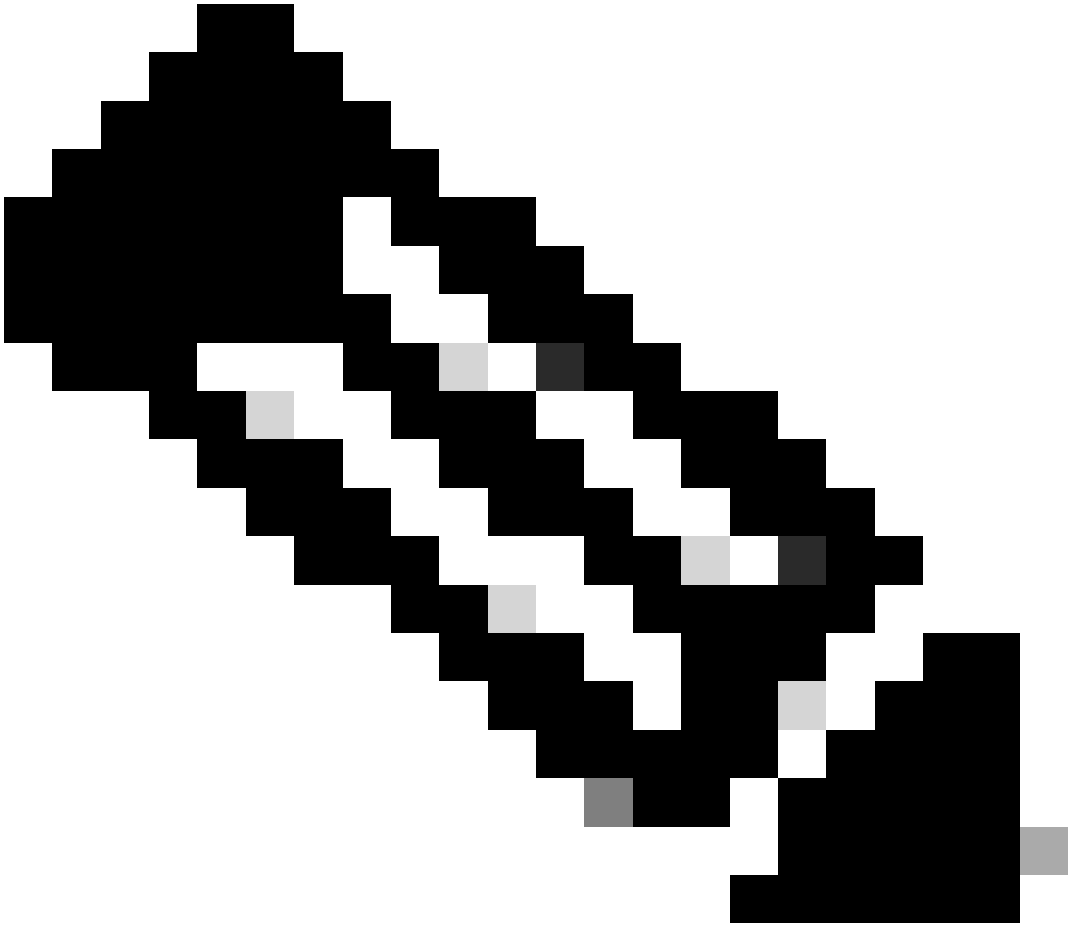
Configure FILS Discovery Frames in the RF Profile (GUI)

Step 1 - Choose Configuration > Tags & Profiles > RF/Radio.

Step 2 - In the **RF** tab, click **Add.** The Add RF Profile page is displayed.

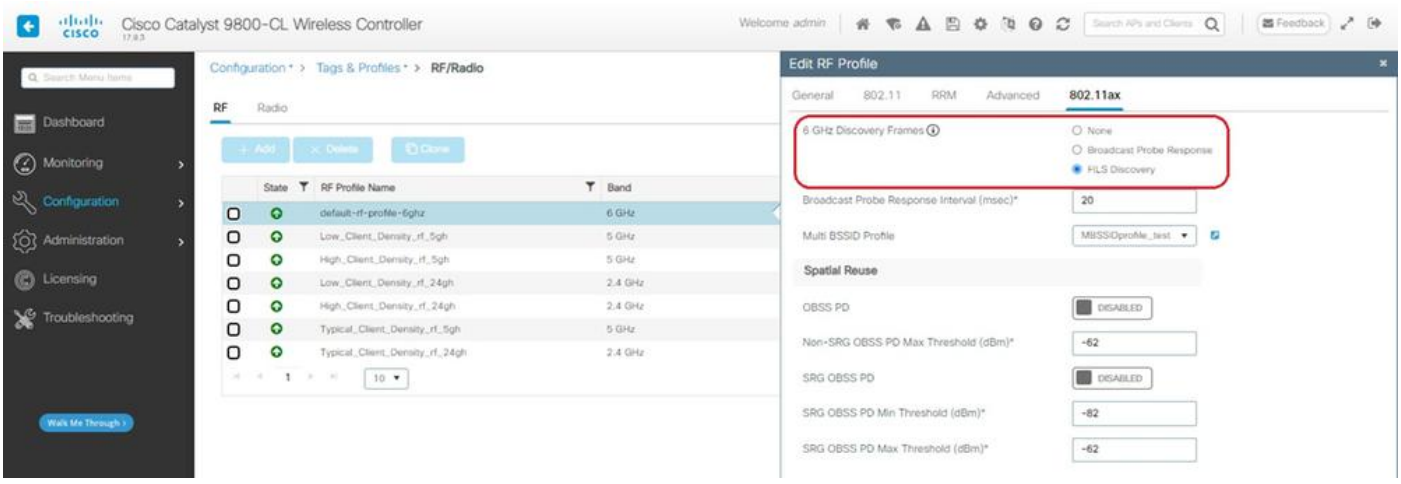
Step 3 - Choose the **802.11ax** tab.

Step 4 - In the **6 GHz Discovery Frames** section, click the **FILS Discovery** option.



Note: To prevent the transmission of discovery FILS frames when the discovery frames are set to **None** in the RF profile, ensure that you disable FILS discovery frames by either switch to the 5-GHz or the 2.4-GHz bands on the AP or by selection of the Broadcast Probe Response option.

Step 5 - Click **Apply to Device**.



Configure FILS Discovery Frames in the RF Profile (CLI)

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax fils-discovery
```

Verification

To verify if the configuration is in place issue the **show** command as shown here:

<#root>

WLC9800#

show ap rf-profile name *default-rf-profile-6ghz* detail | b 802.11ax

```
802.11ax
 OBSS PD : Disabled
 Non-SRG OBSS PD Maximum : -62 dBm
 SRG OBSS PD : Disabled
 SRG OBSS PD Minimum : -82 dBm
 SRG OBSS PD Maximum : -62 dBm
 Broadcast Probe Response : Disabled
```

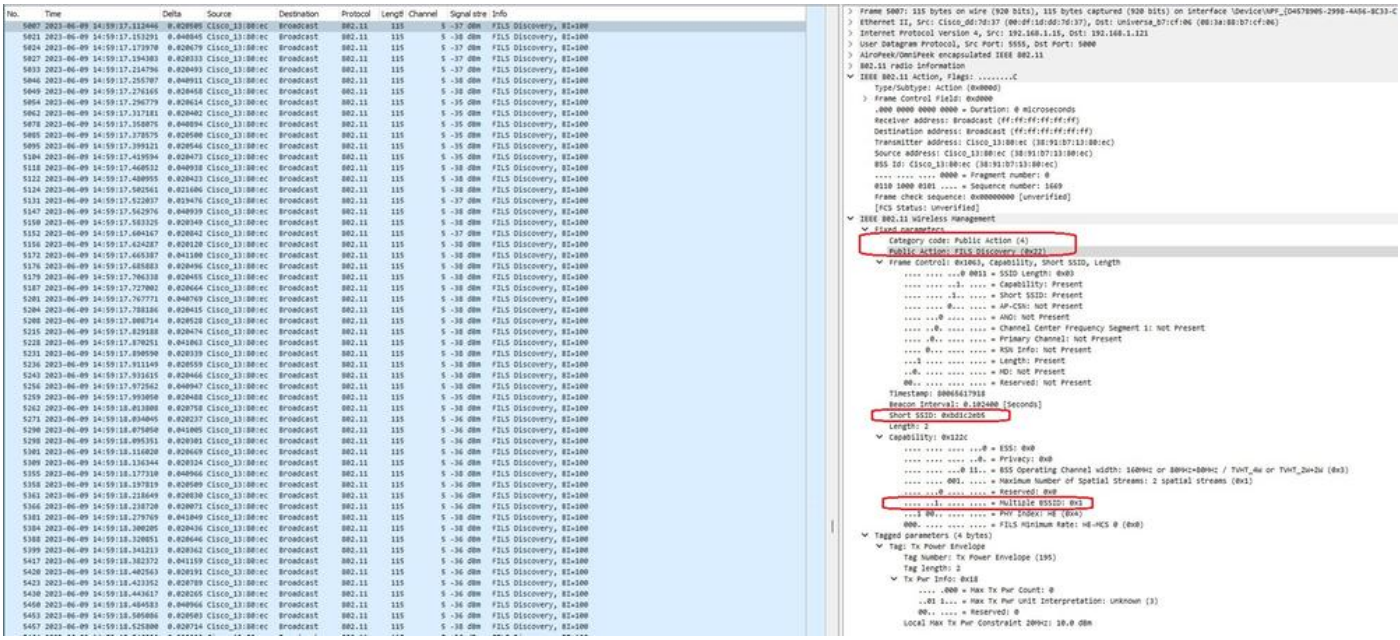
FILS Discovery : Enabled

```
 Multi-BSSID Profile Name :
```

MBSSIDprofile_test

```
NDP mode : Auto
Guard Interval : 800ns
PSC Enforcement : Disabled
```

Here is what we expect to see if we capture the wireless traffic over the air:



You can observe that the delta between frames is most of the times ~20ms, however sometimes you see ~40ms. After checking the frame sequence it was concluded that the sniffer AP was missing the capture of FILS frames sporadically.

UPR

An unsolicited probe response (UPR) frame contains*all*the same information sent in a beacon, that is, it carries multiple BSSIDs and contains all information needed for association.

If used, the 6 GHz AP broadcasts a full probe response frame every 20 milliseconds which helps avoid probe storms.

In 6GHz there are new probe restrictions:

- Clients cannot do blind probe, that is, broadcast destination address using wildcard SSID and BSSID are no allowed because broadcast probe requests and probes with wildcard SSID create probe storm and impacts performance;
- Clients must wait at least the duration of minimum probe delay interval (~20 msec);
- Probe Responses are always broadcast.

UPR is also known as Broadcast Probe Response and in the next section, you can see how to enable it.

Configure Broadcast Probe Response in RF Profile (GUI)

Step 1 - Choose Configuration > Tags & Profiles > RF/Radio.

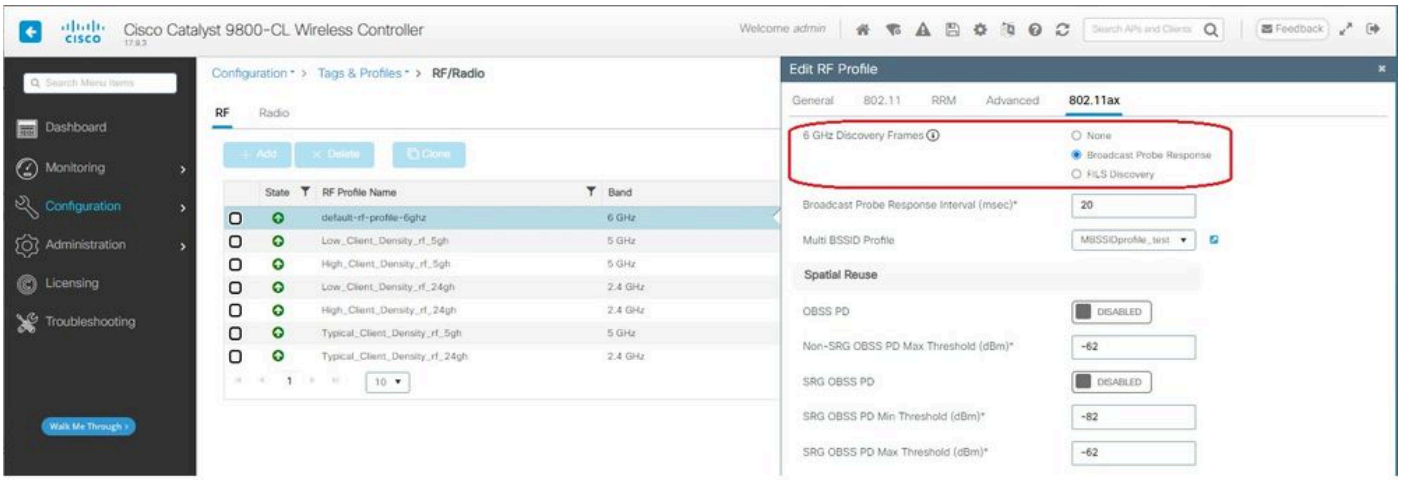
Step 2 - In the RF tab, click **Add.** The Add RF Profile page is displayed.

Step 3 - Choose the **802.11ax** tab.

Step 4 - In the **6 GHz Discovery Frames** section, click the **Broadcast Probe Response** option.

Step 5 - In the **Broadcast Probe Response Interval** field, enter the broadcast probe response time interval in milli-seconds (ms). The value range is between 5 ms and 25 ms. The default value is 20 ms.

Step 6 - Click **Apply to Device**.



Configure Broadcast Probe Response in RF Profile (CLI)

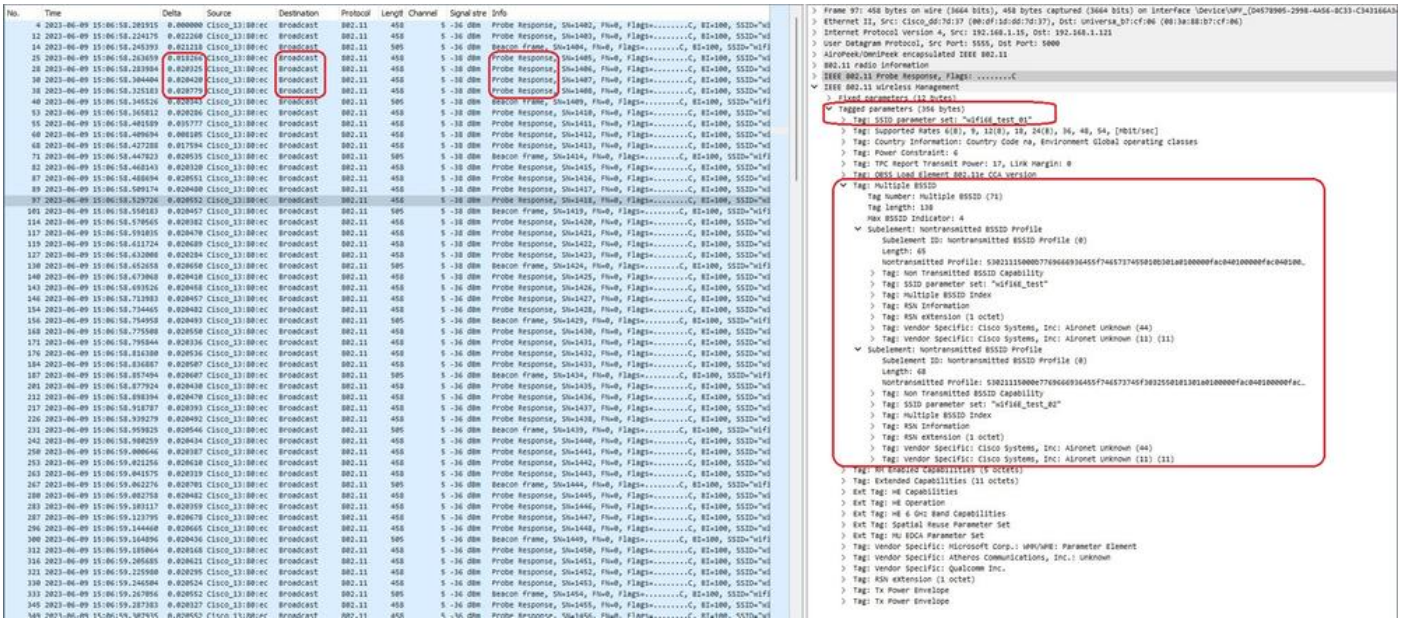
```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax bcast-probe-response
Device(config-rf-profile)# dot11ax bcast-probe-response time-interval 20
```

Verification

To verify if the configuration is in place issue the **show** command as shown here:

```
<#root>

WLC9800#

show ap rf-profile name default-rf-profile-6ghz detail | b 802.11ax


802.11ax
 OBSS PD : Disabled
 Non-SRG OBSS PD Maximum : -62 dBm
 SRG OBSS PD : Disabled
 SRG OBSS PD Minimum : -82 dBm
 SRG OBSS PD Maximum : -62 dBm


Broadcast Probe Response : Enabled
 Broadcast Probe Response Interval : 20 msec


 FILS Discovery : Disabled
 Multi-BSSID Profile Name :

MBSSIDprofile_test


NDP mode : Auto
Guard Interval : 800ns
PSC Enforcement : Disabled
```

When UPR (Broadcast Probe Response) is used this is how it looks over the air:



PSC

The third discovery method in Wi-Fi 6E, which is active, is Preferred Channel Scanning (PSC). This is actually the only method by which Wi-Fi 6E client devices are allowed to send probe requests.

With 1200 MHz of spectrum and 59 new 20 MHz channels, a station with a dwell time of 100 ms per channel would require almost 6 seconds to complete a passive scan of the entire band.

With PSC, client devices are limited to send probe requests on every fourth 20 MHz channel. PSCs are spaced 80 MHz apart, so a client would only need to scan 15 channels instead of 59.

The full list of 6 GHz PSC channels is 5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, and 229.

PSC channels

Configure Preferred Scanning Channels in the RF Profile (GUI)

Step 1 - Choose Configuration > Tags & Profiles > RF/Radio.

Step 2 - In the **RF** tab, click **Add.** The Add RF Profile page is displayed.

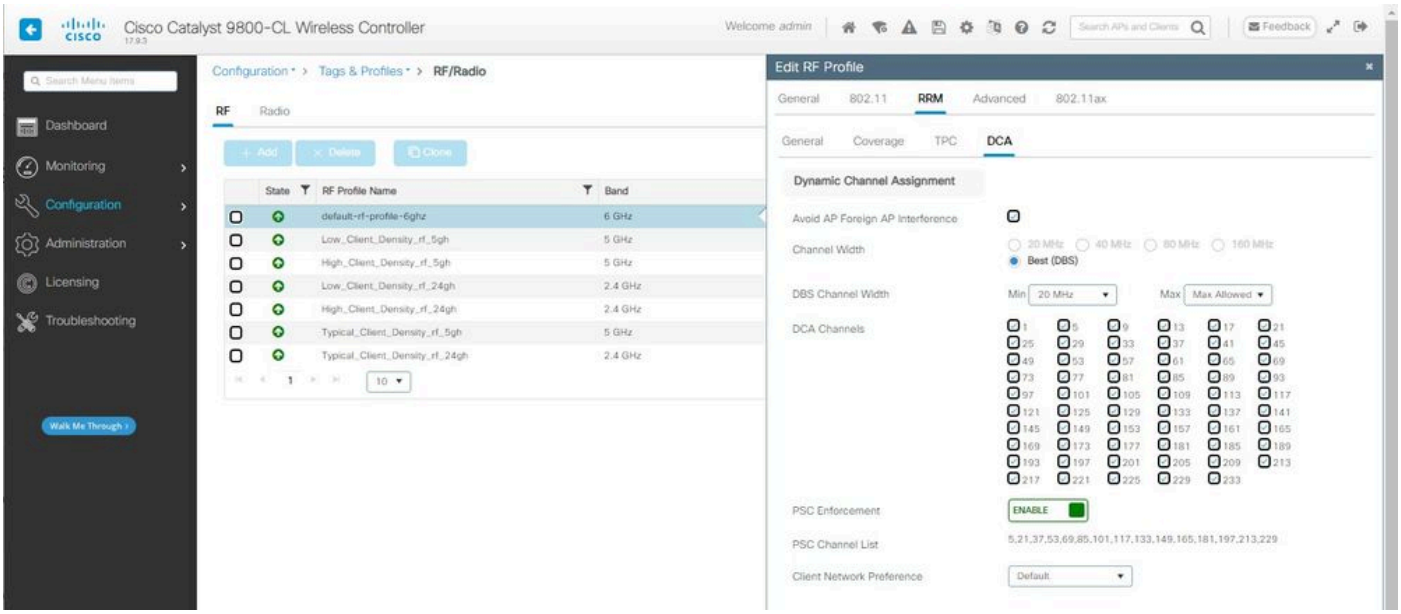
Step 3 - Choose the **RRM** tab.

Step 4 - Choose the **DCA** tab.

Step 5 - In the **Dynamic Channel Assignment** section, select the required channels in **DCA Channels** section.

Step 6 - In the **PSC Enforcement** field, click the toggle button to enable the preferred scanning channel enforcement for DCA.

Step 7 - Click **Apply to Device**.



Configure Preferred Scanning Channels in the RF Profile (CLI)

```
Device# configure terminal
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# channel psc
```

Verification

To verify if the configuration is in place issue the command as shown here:

<#root>

```
WLC9800#
```

show ap rf-profile name *default-rf-profile-6ghz* detail | b DCA

```
DCA Channel List : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93,97,101,105,109,
Unused Channel List :
```

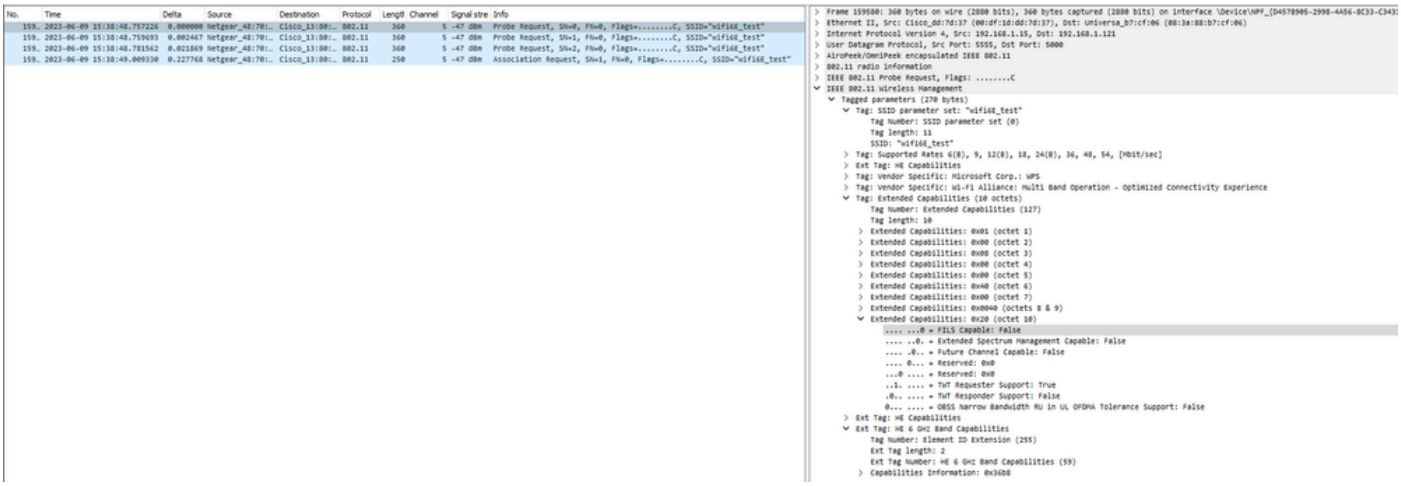
PSC Channel List : 5,21,37,53,69,85,101,117,133,149,165,181,197,213,229

```
DCA Bandwidth : best
DBS Min Channel Width : 20 MHz
DBS Max Channel Width : MAX ALLOWED
DCA Foreign AP Contribution : Enabled
[...]
```

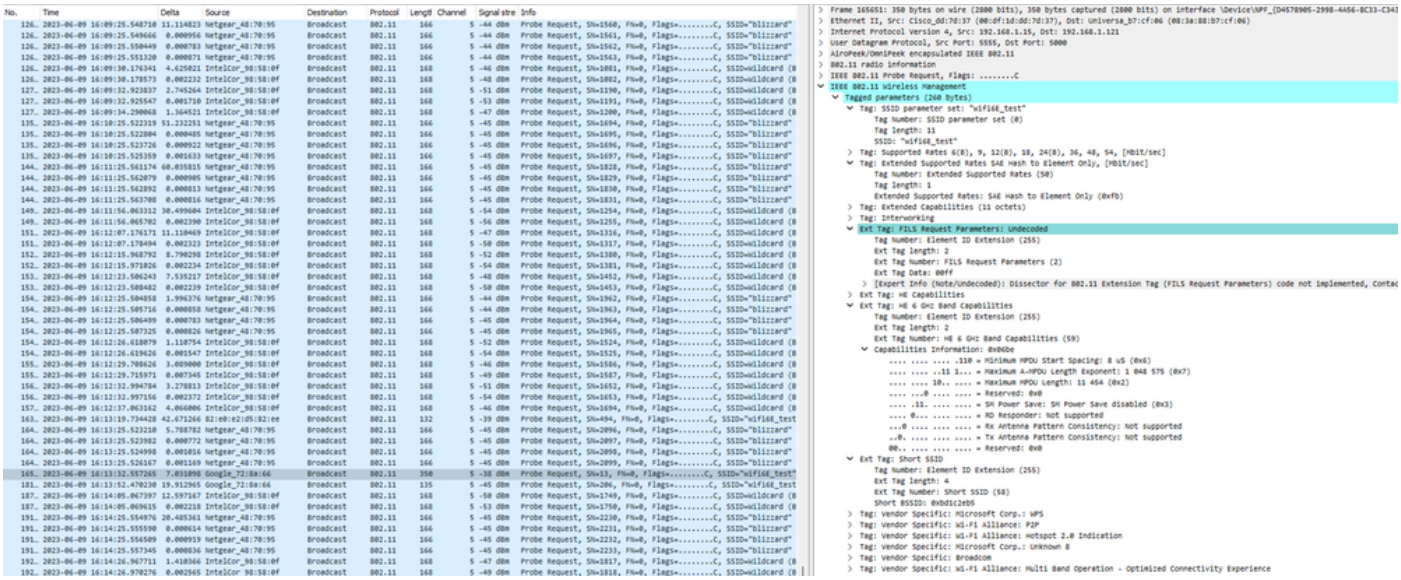
PSC Enforcement : Enabled

Here we can observe Wi-Fi 6E clients that send probe requests on PSC channel 5:

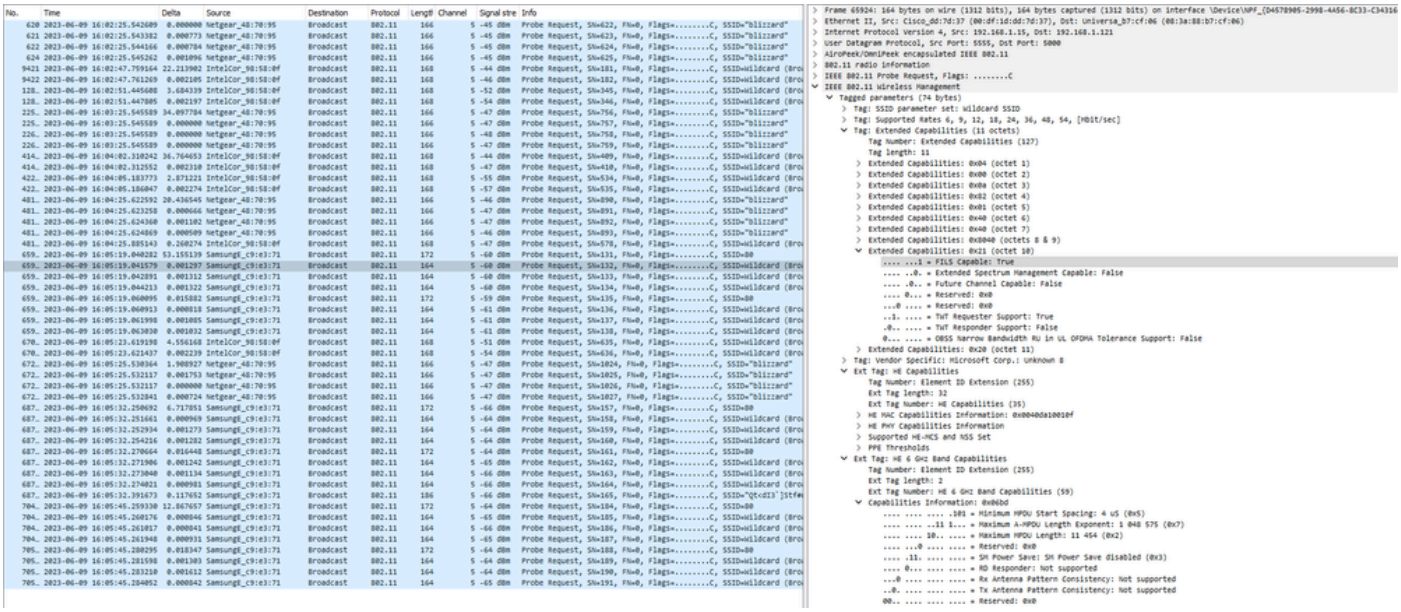
NetGear A8000



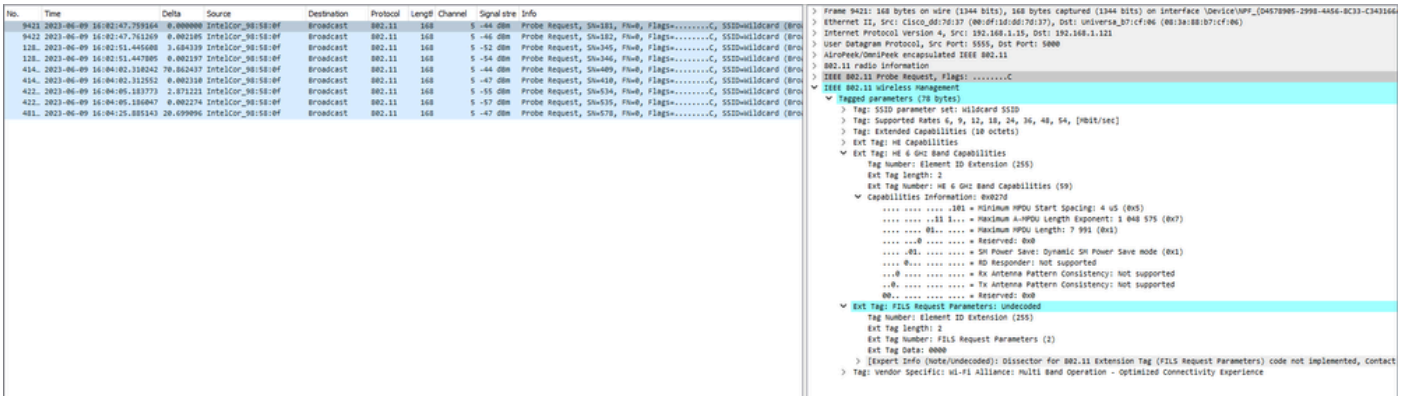
Pixel 6a



Samsung S23



Intel AX211



6-GHz Client Steering

The 6-GHz band provides more channels, more bandwidth, and has less network congestion when compared to the existing 2.4-GHz and 5-GHz bands.

As a result, wireless clients that are 6-GHz capable connect to the 6-GHz radio to take advantage of these benefits.

This topic provides details about 6-GHz client steering for APs supporting 6-GHz band.

The 6-GHz client steering takes place when the controller receives a periodic client statistics report from the 2.4-GHz band or the 5-GHz band.

The client steering configuration is enabled under WLAN, and is configured only for clients that are 6-GHz capable.

If a client in the report is 6-GHz capable, then client steering is triggered, and the client is steered to the 6-GHz band.

Please find more about Band-Steering for Dual-Band Wi-Fi Access Points in the document *Qualcomm Research Band-Steering for Dual-Band Wi-Fi Access Points.*

The Steering Mechanism

To start steering a client, the AP first disassociates with the client on a particular band, and then blocks that client from re-associating on that band for a period of time.

Once disassociated, the client briefly tries to reassociate with the AP on the same SSID and on the same band as the last association before scanning for other AP or band options.

Most Wi-Fi clients scan both bands by sending Probe Requests and estimate the downlink signal strength from the Probe Responses which also indicate the AP’s readiness to re-associate.

Since this scanning and re-association behavior is completely client implementation dependent, some clients can steer faster than others.

It is possible that some clients do not steer, and keep trying to re-associate with the original (blocked) band or just choose to disassociate from Wi-Fi altogether and attempt to re-associate only when they have packets to send.

Steering Caution

Care needs to be taken at the AP to prevent such steering-unfriendly clients from getting blocked at the AP, in which case user intervention can be needed to restore the Wi-Fi connection.

User intervention can be as simple as toggling the Wi-Fi on/off. Clearly such user interventions are not desirable. Therefore, the design errs on the conservative side.

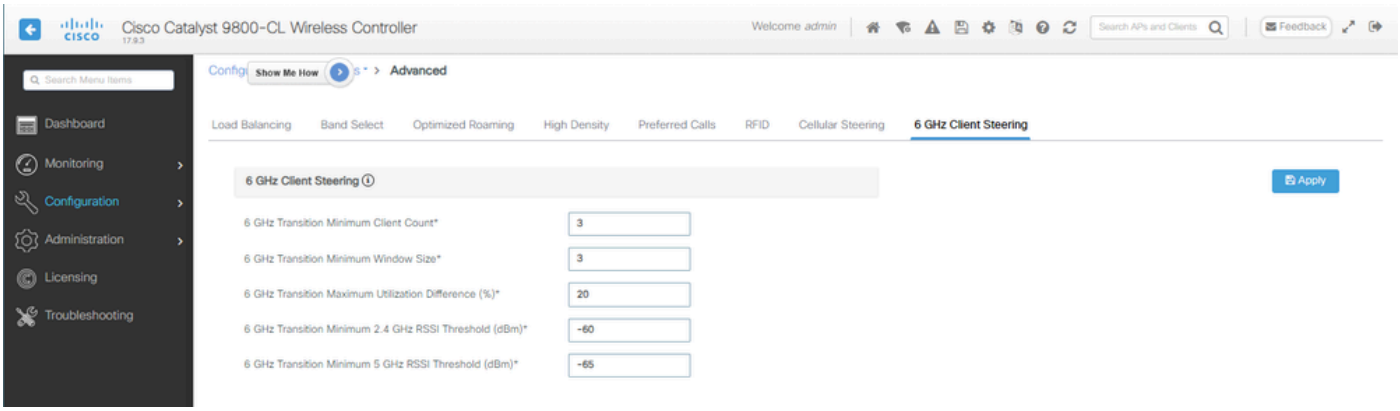
If a client cannot be steered or a steering attempt fails, the AP lets the client re-associate with the original band as opposed to risking the client being blocked from the AP for an extended period of time.

Since the client is only steered when idle, there is no interruption to the user traffic.

Configuring 6-GHz Client Steering in the Global Configuration Mode (GUI)

Step 1 - Choose Configuration > Wireless > Advanced.
Step 2 - Click the **6 GHz Client Steering** tab. Client steering is configurable per WLAN.
Step 3 - In the **6 GHz Transition Minimum Client Count** field, enter a value to set the minimum number of clients for client steering. The default value is three clients. The value range is between 0 and 200 clients.

Step 4 - In the **6 GHz Transition Minimum Window Size** field, enter a value to set the minimum window size of client steering. The default value is three clients. The value range is between 0 and 200 clients.
Step 5 - In the **6 GHz Transition Maximum Utilization Difference** field, enter a value to set the maximum utilization difference for steering. The value range is between 0 percent to 100 percent. The default value is 20.
Step 6 - In the **6 GHz Transition Minimum 2.4 GHz RSSI Threshold** field, enter a value to set the minimum value for client steering 2.4-GHz RSSI threshold.
Step 7 - In the **6 GHz Transition Minimum 5 GHz RSSI Threshold** field, enter a value to set the minimum value for client steering 5-GHz RSSI threshold.
Step 8 - Click **Apply.**

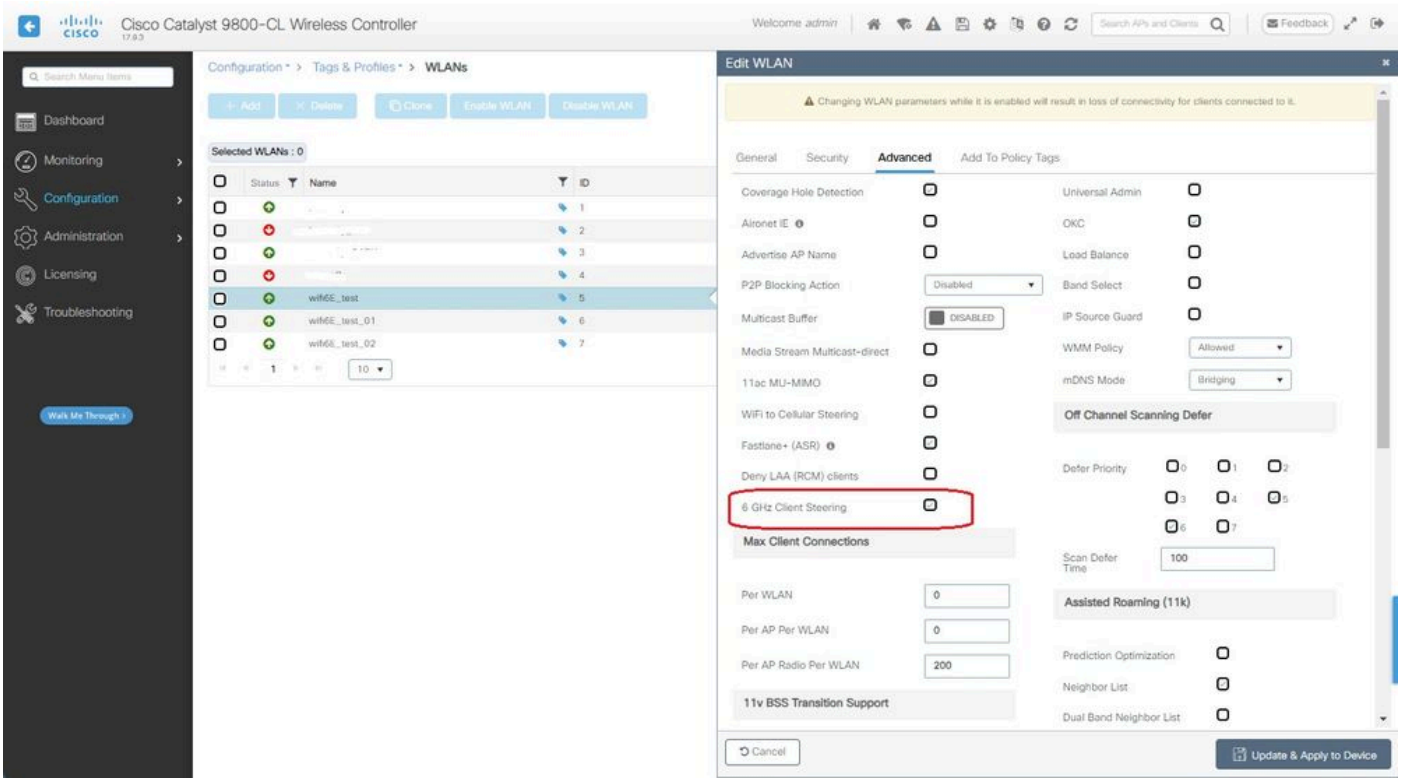


Configuring 6-GHz Client Steering in the Global Configuration Mode (CLI)

```
Device# configure terminal
Device(config)# client-steering client-count 3
Device(config)# client-steering window-size 5
Device(config)# wireless client client-steering util-threshold 25
Device(config)# wireless client client-steering min-rssi-24ghz -70
Device(config)# wireless client client-steering min-rssi-5ghz -75
```

Configure 6-GHz Client Steering on the WLAN (GUI)

Step 1 - Choose Configuration > Tags & Profiles > WLANs.
Step 2 - Click Add.The Add WLAN page is displayed.
Step 3 - Click the **Advanced** tab.
Step 4 - Check the **6 GHz Client Steering** check box to enable client steering on the WLAN.
Step 5 - Click **Apply to Device**.



Configure 6-GHz Client Steering on the WLAN (CLI)

```
Device# configure terminal
Device(config)# wlan wlan-name id ssid-name
Device(config-wlan)# client-steering
```

Verification

To verify if the configuration is in place issue the command as shown here:

<#root>

```
WLC9800#
```

show wireless client steering

```
Client Steering Configuration Information
  Macro to micro transition threshold : -55 dBm
  Micro to Macro transition threshold : -65 dBm
  Micro-Macro transition minimum client count : 3
```

```
  Micro-Macro transition client balancing window : 3
  Probe suppression mode : Disabled
  Probe suppression transition aggressiveness : 3
  Probe suppression hysteresis : -6 dB
  6Ghz transition minimum client count : 3
  6Ghz transition minimum window size : 3
  6Ghz transition maximum channel util difference : 20%
  6Ghz transition minimum 2.4Ghz RSSI threshold : -60 dBm
  6Ghz transition minimum 5Ghz RSSI threshold : -65 dBm

WLAN Configuration Information

WLAN Profile Name     11k Neighbor Report    11v BSS Transition
------------------------------------------------------------------------------------------
5    wifi6E_test      Enabled                Enabled
6    wifi6E_test_01   Enabled                Enabled
7    wifi6E_test_02   Enabled                Enabled

WLC9800#
```

`show wlan id 5 | i Client Steering`

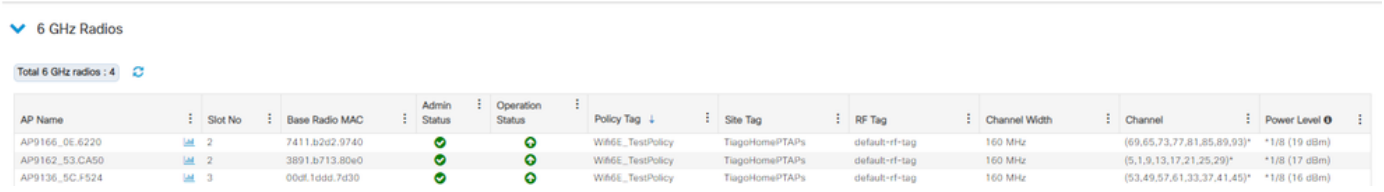
```
6Ghz Client Steering : Enabled
```

Client Connectivity

In this section it is shown the process OTA of each client connecting to the WLAN.

The lab was with these conditions:

- Clients and APs were ~1 meter in line of sight without obstructions.
- All APs broadcasting WLAN with Channel Width of 160MHz and power level 1.
- The client devices were switched on the same VLAN as the iperf server.
- All APs connected via 1Gbps link.



Tests with AP 9166

NetGear A8000

Client details in WLC:

<#root>

```
#show wireless client mac-address 9418.6548.7095 detail

Client MAC Address : 9418.6548.7095
[...]
Client IPv4 Address : 192.168.1.163
[...]
```

AP MAC Address : 7411.b2d2.9740
AP Name: AP9166_0E.6220
AP slot : 2
Client State : Associated
Policy Profile : Policy4TiagoHome
Flex Profile : TiagoHomeFlexProfile
Wireless LAN Id: 5
WLAN Profile Name: wifi6E_test
Wireless LAN Network Name (SSID): wifi6E_test
BSSID : 7411.b2d2.9747
Connected For : 1207 seconds

Protocol : 802.11ax - 6 GHz

Channel : 69

[...]
Current Rate : m11 ss2
Supported Rates : 54.0
[...]

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

Authentication Key Management : SAE

AAA override passphrase : No

SAE PWE Method : Hash to Element(H2E)

[...]

Protected Management Frame - 802.11w : Yes

EAP Type : Not Applicable
[...]
[...]
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
Number of Bytes Received from Client : 1026751751
Number of Bytes Sent to Client : 106125429
Number of Packets Received from Client : 793074
Number of Packets Sent to Client : 184944
Number of Policy Errors : 0

Radio Signal Strength Indicator : -44 dBm

Signal to Noise Ratio : 49 dB

```
[...]
Device Classification Information:

Device Type : Microsoft-Workstation


Device Name : CSCO-W-xxxxxxx


Protocol Map : 0x000029 (OUI, DHCP, HTTP)
Device OS : Windows NT 10.0; Win64; x64
```

Pixel 6a

Client details in WLC:

<#root>

```
#show wireless client mac-address 2495.2f72.8a66 detail

Client MAC Address : 2495.2f72.8a66
[...]
Client IPv4 Address : 192.168.1.162
[...]
AP MAC Address : 7411.b2d2.9740
AP Name: AP9166_OE.6220
AP slot : 2
Client State : Associated
Policy Profile : Policy4TiagoHome
Flex Profile : TiagoHomeFlexProfile
Wireless LAN Id: 5
WLAN Profile Name: wifi6E_test
Wireless LAN Network Name (SSID): wifi6E_test
BSSID : 7411.b2d2.9747
Connected For : 329 seconds
Protocol : 802.11ax - 6 GHz
Channel : 69
Client IIF-ID : 0xa000000a
Association Id : 33
Authentication Algorithm : Open System
[...]
Current Rate : 6.0
Supported Rates : 61.0
[...]

Policy Type : WPA3


Encryption Cipher : CCMP (AES)


Authentication Key Management : SAE


AAA override passphrase : No
```

SAE PWE Method : Hash to Element(H2E)

[...]

Protected Management Frame - 802.11w : Yes

EAP Type : Not Applicable
[...]
Session Manager:
Point of Attachment : capwap_90000025
IIF ID : 0x90000025
Authorized : TRUE
Session timeout : 86400
Common Session ID: 000000000000171BC51FF477
Acct Session ID : 0x00000000
Auth Method Status List
Method : SAE
Local Policies:
Service Template : wlan_svc_Policy4TiagoHome (priority 254)
VLAN : default
Absolute-Timer : 86400
Server Policies:
Resultant Policies:
VLAN Name : default
VLAN : 1
Absolute-Timer : 86400
[...]
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
Number of Bytes Received from Client : 603220312
Number of Bytes Sent to Client : 72111916
Number of Packets Received from Client : 461422
Number of Packets Sent to Client : 107888
Number of Policy Errors : 0

Radio Signal Strength Indicator : -45 dBm

Signal to Noise Ratio : 48 dB

[...]
Device Classification Information:

Device Type : Android-Google-Pixel

Device Name : Pixel-6a

Protocol Map : 0x000029 (OUI, DHCP, HTTP)
Device OS : X11; Linux x86_64

Samsung S23

Client details in WLC:

<#root>

#show wireless client mac-address 0429.2ec9.e371 detail

Client MAC Address : 0429.2ec9.e371
[...]
Client IPv4 Address : 192.168.1.160
[...]
AP MAC Address : 7411.b2d2.9740
AP Name: AP9166_0E.6220
AP slot : 2
Client State : Associated
Policy Profile : Policy4TiagoHome
Flex Profile : TiagoHomeFlexProfile
Wireless LAN Id: 5
WLAN Profile Name: wifi6E_test
Wireless LAN Network Name (SSID): wifi6E_test
BSSID : 7411.b2d2.9747
Connected For : 117 seconds

Protocol : 802.11ax - 6 GHz

Channel : 69

Client IIF-ID : 0xa0000002
Association Id : 33
Authentication Algorithm : Open System
[...]
Current Rate : 6.0
Supported Rates : 54.0
[...]

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

Authentication Key Management : SAE

AAA override passphrase : No

SAE PWE Method : Hash to Element(H2E)

[...]

Protected Management Frame - 802.11w : Yes

EAP Type : Not Applicable
[...]
Session Manager:
Point of Attachment : capwap_90000025
IIF ID : 0x90000025
Authorized : TRUE
Session timeout : 86400

```
Common Session ID: 0000000000001713C518E305
Acct Session ID : 0x00000000
Auth Method Status List
Method : SAE
Local Policies:
Service Template : wlan_svc_Policy4TiagoHome (priority 254)
VLAN : default
Absolute-Timer : 86400
Server Policies:
Resultant Policies:
VLAN Name : default
VLAN : 1
Absolute-Timer : 86400
[...]
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
Number of Bytes Received from Client : 550161686
Number of Bytes Sent to Client : 5751483
Number of Packets Received from Client : 417388
Number of Packets Sent to Client : 63427
Number of Policy Errors : 0
```

Radio Signal Strength Indicator : -52 dBm

Signal to Noise Ratio : 41 dB

```
[...]
Device Classification Information:
```

Device Type : Android-Device

Device Name : Galaxy-S23

```
Protocol Map : 0x000029 (OUI, DHCP, HTTP)
```

Intel AX211

Client details in WLC:

<#root>

```
#show wireless client mac-address 286b.3598.580f detail

Client MAC Address : 286b.3598.580f
[...]
Client IPv4 Address : 192.168.1.159
[...]
AP MAC Address : 7411.b2d2.9740
AP Name: AP9166_0E.6220
AP slot : 2
Client State : Associated
Policy Profile : Policy4TiagoHome
Flex Profile : TiagoHomeFlexProfile
```

Wireless LAN Id: 5
WLAN Profile Name: wifi6E_test
Wireless LAN Network Name (SSID): wifi6E_test
BSSID : 7411.b2d2.9747
Connected For : 145 seconds

Protocol : 802.11ax - 6 GHz

Channel : 69

Client IIF-ID : 0xa0000001
Association Id : 35
Authentication Algorithm : Open System
[...]
Current Rate : 6.0
Supported Rates : 54.0
AAA QoS Rate Limit Parameters:
QoS Average Data Rate Upstream : (kbps)
QoS Realtime Average Data Rate Upstream : (kbps)
QoS Burst Data Rate Upstream : (kbps)
QoS Realtime Burst Data Rate Upstream : (kbps)
QoS Average Data Rate Downstream : (kbps)
QoS Realtime Average Data Rate Downstream : (kbps)
QoS Burst Data Rate Downstream : (kbps)
QoS Realtime Burst Data Rate Downstream : (kbps)
[...]

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

Authentication Key Management : SAE

AAA override passphrase : No

SAE PWE Method : Hash to Element(H2E)

[...]

Protected Management Frame - 802.11w : Yes

[...]
Session Manager:
Point of Attachment : capwap_90000025
IIF ID : 0x90000025
Authorized : TRUE
Session timeout : 86400
Common Session ID: 000000000000171CC520478F
Acct Session ID : 0x00000000
Auth Method Status List
Method : SAE
Local Policies:
Service Template : wlan_svc_Policy4TiagoHome (priority 254)

```
VLAN : default
Absolute-Timer : 86400
Server Policies:
Resultant Policies:
VLAN Name : default
VLAN : 1
Absolute-Timer : 86400
[...]
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
Number of Bytes Received from Client : 335019921
Number of Bytes Sent to Client : 3315418
Number of Packets Received from Client : 250583
Number of Packets Sent to Client : 38960
Number of Policy Errors : 0
```

Radio Signal Strength Indicator : -54 dBm

Signal to Noise Ratio : 39 dB

```
[...]
Device Classification Information:
```

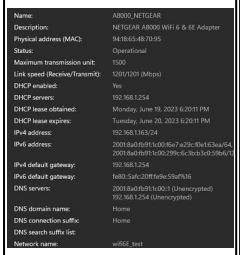
Device Type : LENOVO 21CCS43W0T

Device Name : CSCO-W-xxxxxxxx

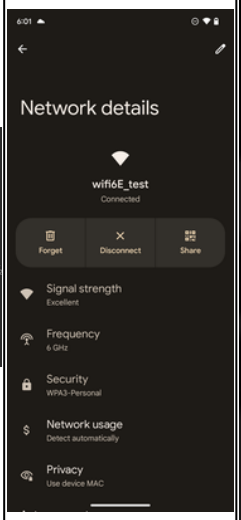
```
Protocol Map : 0x000429 (OUI, DOT11, DHCP, HTTP)
Device OS : Windows 10
```

Here you can observe the network details provided by each client:

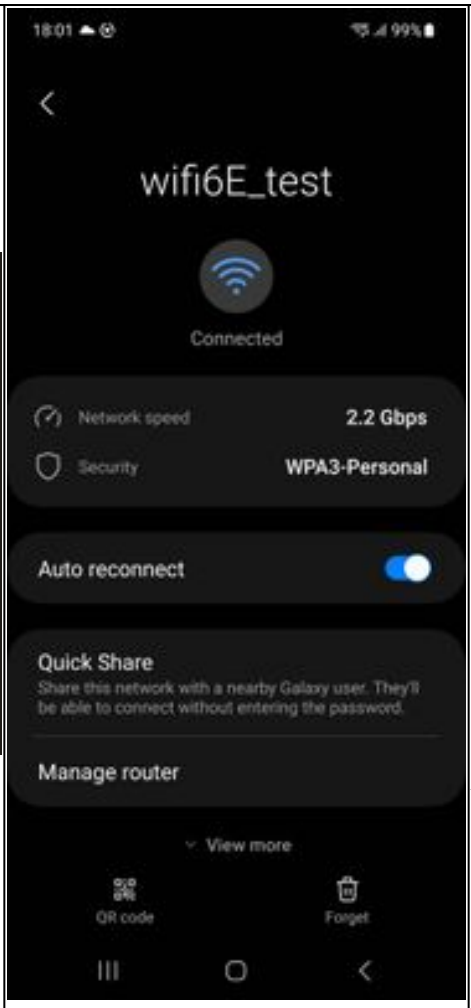
NetGearA8000	Pixel 6a	Samsung S23	Intel AX211



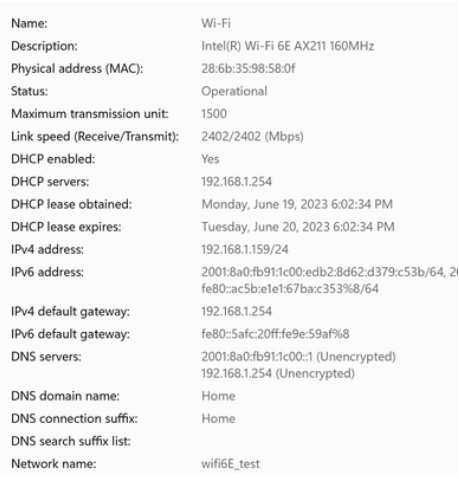
NetGearA8000 Client Details



Pixel6a Client Details



S23 Client Details



AX211 Client Details

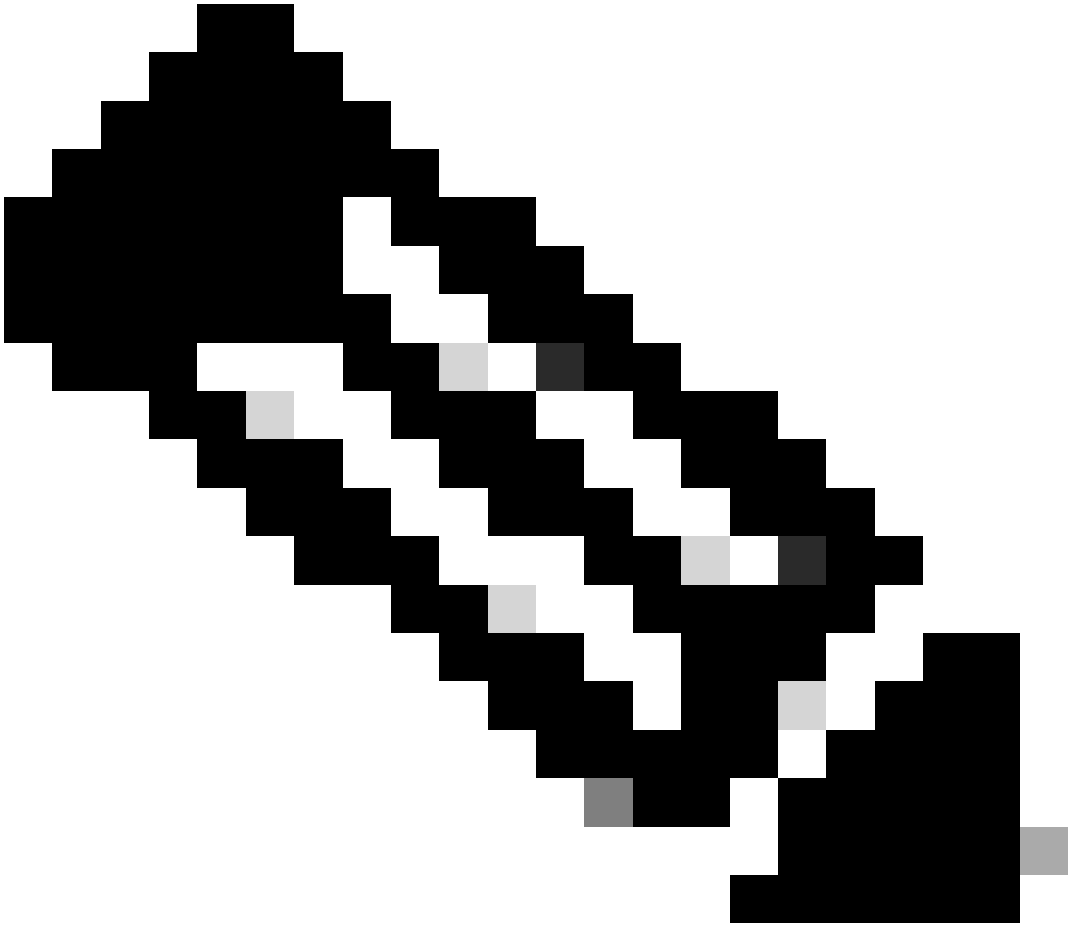
Troubleshoot

The troubleshooting section of this document is aimed to provide general guidance on troubleshooting WLAN broadcasting issues rather then client specific problems that can occur when using any of the band operations explained in this document.

Troubleshooting on the client-side depends a lot on the client operating system. Windows allows to scan for networks and identify if the 6GHz BSSIDs are being heard by the laptop. The section about colocated APs show you what other BSSID from the same APs were learned through RNR report.

```
C:\Windows\System32>netsh wlan show networks mode=Bssid

Interface name : A8000_NETGEAR
There are 4 networks currently visible.
(...)

SSID 3 : Darchis6
    Network type            : Infrastructure
    Authentication          : WPA3-Personal
    Encryption              : CCMP
    BSSID 1                 : 10:a8:29:30:0d:07
         Signal             : 6%
         Radio type         : 802.11ax
         Band               : 6 GHz
```

```
     Channel            : 69
     Hash-to-Element:   : Supported
     Bss Load:
         Connected Stations:         0
         Channel Utilization:        2 (0 %)
         Medium Available Capacity:  23437 (749984 us/s)
     Colocated APs:     : 3
        BSSID: 10:a8:29:30:0d:01,  Band: 2.4 GHz,  Channel: 1
        BSSID: 10:a8:29:30:0d:0f,  Band: 5 GHz  ,  Channel: 36
        BSSID: 10:a8:29:30:0d:0e,  Band: 5 GHz  ,  Channel: 36
     Basic rates (Mbps) : 6 12 24
     Other rates (Mbps) : 9 18 36 48 54
BSSID 2                 : 10:a8:29:30:0d:0f
     Signal             : 57%
     Radio type         : 802.11ax
     Band               : 5 GHz
     Channel            : 36
     Hash-to-Element:   : Supported
     Bss Load:
         Connected Stations:         0
         Channel Utilization:        9 (3 %)
         Medium Available Capacity:  23437 (749984 us/s)
     Colocated APs:     : 1
        BSSID: 10:a8:29:30:0d:07,  Band: 6 GHz  ,  Channel: 69
     Basic rates (Mbps) : 6 12 24
     Other rates (Mbps) : 9 18 36 48 54
BSSID 3                 : 18:f9:35:4d:9d:67
     Signal             : 79%
     Radio type         : 802.11ax
     Band               : 6 GHz
     Channel            : 37
     Hash-to-Element:   : Supported
     Bss Load:
         Connected Stations:         0
         Channel Utilization:        2 (0 %)
         Medium Available Capacity:  23437 (749984 us/s)
     Colocated APs:     : 3
        BSSID: 18:f9:35:4d:9d:6f,  Band: 5 GHz  ,  Channel: 52
        BSSID: 18:f9:35:4d:9d:6e,  Band: 5 GHz  ,  Channel: 52
        BSSID: 18:f9:35:4d:9d:61,  Band: 2.4 GHz,  Channel: 11
     Basic rates (Mbps) : 6 12 24
     Other rates (Mbps) : 9 18 36 48 54
```



Note: Refer to Important Information on Debug Commands before you use **debug** commands.

To troubleshoot client connectivity issues, it is recommended to use these documents:

Troubleshoot Catalyst 9800 Client Connectivity Issues Flow .

Understand Wireless Debugs and Log Collection on Catalyst 9800 Wireless LAN Controllers .

For AP troubleshooting it is recommended to use this document:

Troubleshoot COS APs

For throughput calculation and validation, please check this guide:

802.11ac wireless throughput testing and validation guide .

Even though it was created when 11ac was released, the same calculations apply for 11ax.

Related Information

What is Wi-Fi 6E?

What Is Wi-Fi 6 vs. Wi-Fi 6E?

Wi-Fi 6E At-a-Glance

Wi-Fi 6E: The Next Great Chapter in Wi-Fi White Paper

Cisco Live - Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points

Countries Enabling Wi-Fi in 6 GHz (Wi-Fi 6E)

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide 17.9.x

WPA3 Deployment Guide