5557x Wi-Fi 6/6E User Guide

Usage, How To & FAQs

About this document

Scope and purpose

This document serves as a Usage and configuration Guide for the 802.11ax, 6GHz features supported in the Infineon Wi-Fi 6/6E Solutions. Also helps as a quick reference for the some of the frequently asked questions.

Intended audience

This document is primarily intended for those using Infineon Wi-Fi solutions with the Linux host of their choice. It is recommended that the reader have prior experience with Linux kernel wireless networking.

Table of contents

Contents

1 Configure & use 802.11ax features

1.1 SoftAP bringup in 802.11ax

To enable 802.11ax operation in the SoftAP, set the following hostapd.conf params with the appropriate values as shown below for each wireless network type.

S.NO	Description	hostapd.conf parameter
1	Enable the 802.11ax support in SoftAP	ieee80211ax=1
2	Set the channel width as 20/40/80 MHz	he_oper_chwidth=<0/1>
3	Specify the center frequency of the 80MHz channel	he_oper_centr_freq_seg0_idx=39

Reference hostapd.conf for each desired security type and wireless channel config:

SoftAP hostapd conf	OPEN	WPA2	WPA3 SAE

2G Band
CH 6
20 MHz
 	
Primary
CH 6
	ctrl_interface=/var/run/hostapd
	interface=wlan0
	driver=nl80211
	ssid=IFX-AX-OPEN-20MHz-2G
	channel=6
	hw_mode=g
	wmm_enabled=1
	ieee80211n=1
	ht_capab=[SHORT-GI-20]
	ieee80211ac=1
	vht_oper_chwidth=0
	vht_oper_centr_freq_seg0_idx=6
	
	# HE confs
	ieee80211ax=1
	he_oper_chwidth=0
	he_oper_centr_freq_seg0_idx=6
		ctrl_interface=/var/run/hostapd
		interface=wlan0
		driver=nl80211
		ssid=IFX-AX-WPA2-20MHz-2G
		channel=6
		hw_mode=g
		wmm_enabled=1
		ieee80211n=1
		ht_capab=[SHORT-GI-20]
		ieee80211ac=1
		vht_oper_chwidth=0
		vht_oper_centr_freq_seg0_idx=6
		
		# HE confs
		ieee80211ax=1
		he_oper_chwidth=0
		he_oper_centr_freq_seg0_idx=6
		
		# WPA2 confs
		wpa=2
		rsn_pairwise=CCMP
		wpa_key_mgmt=WPA-PSK
		wpa_passphrase=1234567890
			ctrl_interface=/var/run/hostapd
			interface=wlan0
			driver=nl80211
			ssid=IFX-AX-WPA3-20MHz-2G
			channel=6
			hw_mode=g
			wmm_enabled=1
			ieee80211n=1
			ht_capab=[SHORT-GI-20]
			ieee80211ac=1
			vht_oper_chwidth=0
			vht_oper_centr_freq_seg0_idx=6
			
			# HE confs
			ieee80211ax=1
			he_oper_chwidth=0
			he_oper_centr_freq_seg0_idx=6
			
			# WPA3 confs
			wpa=2
			sae_pwe=2
			sae_groups=19
			ieee80211w=2
			rsn_pairwise=CCMP
			wpa_key_mgmt=SAE
			sae_password=1234567890

5G Band
CH 36
20 MHz
 	
Primary
CH 36
	ctrl_interface=/var/run/hostapd
	interface=wlan0
	driver=nl80211
	ssid=IFX-AX-OPEN-20MHz-5G
	channel=36
	hw_mode=a
	wmm_enabled=1
	ieee80211n=1
	ht_capab=[SHORT-GI-20]
	ieee80211ac=1
	vht_oper_chwidth=0
	vht_oper_centr_freq_seg0_idx=36
	
	# HE confs
	ieee80211ax=1
	he_oper_chwidth=0
	he_oper_centr_freq_seg0_idx=36
		ctrl_interface=/var/run/hostapd
		interface=wlan0
		driver=nl80211
		ssid=IFX-AX-WPA2-20MHz-5G
		channel=36
		hw_mode=a
		wmm_enabled=1
		ieee80211n=1
		ht_capab=[SHORT-GI-20]
		ieee80211ac=1
		vht_oper_chwidth=0
		vht_oper_centr_freq_seg0_idx=36
		
		# HE confs
		ieee80211ax=1
		he_oper_chwidth=0
		he_oper_centr_freq_seg0_idx=36
			ctrl_interface=/var/run/hostapd
			interface=wlan0
			driver=nl80211
			ssid=IFX-AX-WPA3-20MHz-5G
			channel=36
			hw_mode=a
			wmm_enabled=1
			ieee80211n=1
			ht_capab=[SHORT-GI-20]
			ieee80211ac=1
			vht_oper_chwidth=0
			vht_oper_centr_freq_seg0_idx=36
			
			# HE confs
			ieee80211ax=1
			he_oper_chwidth=0
			he_oper_centr_freq_seg0_idx=36

SoftAP hostapd conf	OPEN	WPA2	WPA3 SAE

		# WPA2 confs
		wpa=2
		rsn_pairwise=CCMP
		wpa_key_mgmt=WPA-PSK
		wpa_passphrase=1234567890
			# WPA3 confs
			wpa=2
			sae_pwe=2
			sae_groups=19
			ieee80211w=2
			rsn_pairwise=CCMP
			wpa_key_mgmt=SAE
			sae_password=1234567890

5G Band
CH 46
40 MHz
 	
Primary
CH 48
	ctrl_interface=/var/run/hostapd
	interface=wlan0
	driver=nl80211
	ssid=IFX-AX-OPEN-40MHz-5G
	channel=48
	hw_mode=a
	wmm_enabled=1
	ieee80211n=1
	ht_capab=[HT40-]
	ieee80211ac=1
	vht_oper_chwidth=0
	vht_oper_centr_freq_seg0_idx=46
	
	# HE confs
	ieee80211ax=1
	he_oper_chwidth=0
	he_oper_centr_freq_seg0_idx=46
		ctrl_interface=/var/run/hostapd
		interface=wlan0
		driver=nl80211
		ssid=IFX-AX-WPA2-40MHz-5G
		channel=48
		hw_mode=a
		wmm_enabled=1
		ieee80211n=1
		ht_capab=[HT40-]
		ieee80211ac=1
		vht_oper_chwidth=0
		vht_oper_centr_freq_seg0_idx=46
		
		# HE confs
		ieee80211ax=1
		he_oper_chwidth=0
		he_oper_centr_freq_seg0_idx=46
		
		# WPA2 confs
		wpa=2
		rsn_pairwise=CCMP
		wpa_key_mgmt=WPA-PSK
		wpa_passphrase=1234567890
			ctrl_interface=/var/run/hostapd
			interface=wlan0
			driver=nl80211
			ssid=IFX-AX-WPA3-40MHz-5G
			channel=48
			hw_mode=a
			wmm_enabled=1
			ieee80211n=1
			ht_capab=[HT40-]
			ieee80211ac=1
			vht_oper_chwidth=0
			vht_oper_centr_freq_seg0_idx=46
			
			# HE confs
			ieee80211ax=1
			he_oper_chwidth=0
			he_oper_centr_freq_seg0_idx=46
			
			# WPA3 confs
			wpa=2
			sae_pwe=2
			sae_groups=19
			ieee80211w=2
			rsn_pairwise=CCMP
			wpa_key_mgmt=SAE
			sae_password=1234567890

5G Band
CH 42
80 MHz
 	
Primary
CH 36
	ctrl_interface=/var/run/hostapd
	interface=wlan0
	driver=nl80211
	ssid=IFX-AX-OPEN-80MHz-5G
	channel=36
	hw_mode=a
	wmm_enabled=1
	ieee80211n=1
	ht_capab=[HT40+][HT40-]
	ieee80211ac=1
	vht_oper_chwidth=1
	vht_oper_centr_freq_seg0_idx=42
	
	# HE confs
	ieee80211ax=1
	he_oper_chwidth=1
	he_oper_centr_freq_seg0_idx=42
		ctrl_interface=/var/run/hostapd
		interface=wlan0
		driver=nl80211
		ssid=IFX-AX-WPA2-80MHz-5G
		channel=36
		hw_mode=a
		wmm_enabled=1
		ieee80211n=1
		ht_capab=[HT40+][HT40-]
		ieee80211ac=1
		vht_oper_chwidth=1
		vht_oper_centr_freq_seg0_idx=42
		
		# HE confs
		ieee80211ax=1
		he_oper_chwidth=1
		he_oper_centr_freq_seg0_idx=42
		
		# WPA2 confs
		wpa=2
		rsn_pairwise=CCMP
		wpa_key_mgmt=WPA-PSK
		wpa_passphrase=1234567890
			ctrl_interface=/var/run/hostapd
			interface=wlan0
			driver=nl80211
			ssid=IFX-AX-WPA3-80MHz-5G
			channel=36
			hw_mode=a
			wmm_enabled=1
			ieee80211n=1
			ht_capab=[HT40+][HT40-]
			ieee80211ac=1
			vht_oper_chwidth=1
			vht_oper_centr_freq_seg0_idx=42
			
			# HE confs
			ieee80211ax=1
			he_oper_chwidth=1
			he_oper_centr_freq_seg0_idx=42
			
			# WPA3 confs
			wpa=2
			sae_pwe=2
			sae_groups=19
			ieee80211w=2
			rsn_pairwise=CCMP
			wpa_key_mgmt=SAE
			sae_password=1234567890

1.2 STA association in 802.11ax

To discover the available APs using scan and to connect with a desired 802.11ax AP, use the following sample wpa_supplicant.conf files corresponding to each of the SoftAP Conf files mentioned in the previous section.

STA wpa_supplicant conf	OPEN	WPA2	WPA3 SAE	WPA3 OWE

2G Band
CH 6
20 MHz
 	
Primary
CH 6
	ctrl_interface=/var/run/wpa_supplicant
	
	network={
	ssid="IFX-AX-OPEN-20MHz-2G"
	key_mgmt=NONE
	
	}
		ctrl_interface=/var/run/wpa_supplicant
		
		network={
		ssid="IFX-AX-WPA2-20MHz-2G"
		proto=WPA2
		pairwise=CCMP
		key_mgmt=WPA-PSK
		psk="1234567890"
		
		}
			ctrl_interface=/var/run/wpa_supplicant
			sae_groups=19
			sae_pwe=2
			network={
			ssid="IFX-AX-WPA3-20MHz-2G"
			proto=RSN
			pairwise=CCMP
			ieee80211w=2
			key_mgmt=SAE
			sae_password="1234567890"
			}
				ctrl_interface=/var/run/wpa_supplicant
				
				network={
				ssid="IFX-AX-OWE-20MHz-2G"
				ieee80211w=2
				key_mgmt=OWE
				}

5G Band
CH 36
20 MHz
 	
Primary
CH 36
	ctrl_interface=/var/run/wpa_supplicant
	
	network={
	ssid="IFX-AX-OPEN-20MHz-5G"
	key_mgmt=NONE
	
	}
		ctrl_interface=/var/run/wpa_supplicant
		
		network={
		ssid="IFX-AX-WPA2-20MHz-5G"
		proto=WPA2
		pairwise=CCMP
		key_mgmt=WPA-PSK
		psk="1234567890"
		
		}
			ctrl_interface=/var/run/wpa_supplicant
			sae_groups=19
			sae_pwe=2
			network={
			ssid="IFX-AX-WPA3-20MHz-5G"
			proto=RSN
			pairwise=CCMP
			ieee80211w=2
			key_mgmt=SAE
			sae_password="1234567890"
			}
				ctrl_interface=/var/run/wpa_supplicant
				
				network={
				ssid="IFX-AX-OWE-20MHz-5G"
				ieee80211w=2
				key_mgmt=OWE
				}

5G Band
CH 46
40 MHz
 	
Primary
CH 48
	ctrl_interface=/var/run/wpa_supplicant
	
	network={
	ssid="IFX-AX-OPEN-40MHz-5G"
	key_mgmt=NONE
	
	}
		ctrl_interface=/var/run/wpa_supplicant
		
		network={
		ssid="IFX-AX-WPA2-40MHz-5G"
		proto=WPA2
		pairwise=CCMP
		key_mgmt=WPA-PSK
		psk="1234567890"
		
		}
			ctrl_interface=/var/run/wpa_supplicant
			sae_groups=19
			sae_pwe=2
			network={
			ssid="IFX-AX-WPA3-40MHz-5G"
			proto=RSN
			pairwise=CCMP
			ieee80211w=2
			key_mgmt=SAE
			sae_password="1234567890"
			}
				ctrl_interface=/var/run/wpa_supplicant
				
				network={
				ssid="IFX-AX-OWE-40MHz-5G"
				ieee80211w=2
				key_mgmt=OWE
				}

5G Band
CH 42
80 MHz
 	
Primary
CH 36
	ctrl_interface=/var/run/wpa_supplicant
	
	network={
	ssid="IFX-AX-OPEN-80MHz-5G"
	key_mgmt=NONE
	
	}
		ctrl_interface=/var/run/wpa_supplicant
		
		network={
		ssid="IFX-AX-WPA2-80MHz-5G"
		proto=WPA2
		pairwise=CCMP
		key_mgmt=WPA-PSK
		psk="1234567890"
		
		}
			ctrl_interface=/var/run/wpa_supplicant
			sae_groups=19
			sae_pwe=2
			network={
			ssid="IFX-AX-WPA3-80MHz-5G"
			proto=RSN
			pairwise=CCMP
			ieee80211w=2
			key_mgmt=SAE
			sae_password="1234567890"
			}
				ctrl_interface=/var/run/wpa_supplicant
				
				network={
				ssid="IFX-AX-OWE-80MHz-5G"
				ieee80211w=2
				key_mgmt=OWE
				}

1.3 Target Wake Time (TWT) in STA

The Target Wake Time feature part of the 802.11ax standard address few of the drawbacks in the existing power save mechanisms by having a wake schedule agreement with the AP. There are two types of TWT agreements: individual (iTWT) and broadcast (bTWT). Individual TWT agreement is an agreement negotiated between an AP and an individual STA. Wheras, in Broadcast TWT agreement, the AP Sets up a TWT SP with multiple STAs and advertises the existing broadcast TWT agreement params in beacons.

1.3.1 Auto iTWT session Setup & Teardown in STA

Enabling Auto/Default iTWT session helps in establishing an iTWT session, after the STA successfully associated with a TWT capable AP. This feature can be controlled using the following wpa_supplicant.conf global parameter “twt_def_algo”.

twt_def_algo=<0/1/2>	Description	TWT parameters chosen implicitly for the Auto iTWT session		
		2G Band	5G Band	6G Band
0	No Default iTWT	NA	NA	NA
1	Default iTWT session suitable for a connection with “idle” traffic	SP: 2 ms | SI: 614.4 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced	SP: 512 us | SI: 614.4 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced	SP: 512 us | SI: 614.4 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced
2	Default iTWT session suitable for a connection with “active” traffic	SP: 8 ms | SI: 50 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced	SP: 8 ms | SI: 50 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced	SP: 8 ms | SI: 50 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced

After association, the default iTWT session is established automatically and post Disassociation, all the iTWT sessions established by the STA gets teardowned.

1.3.2 Manual iTWT Session Setup in STA

In the case when Auto iTWT session is disabled, the iTWT sessions can be manually setup using wpa_cli cmds listed below.

S.NO	Desired iTWT session	wpa_cli cmd to run on STA
1	SP: 2 ms | SI: 614.4 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced	`wpa_cli >`**`twt_setup setup_cmd=2 min_twt=8 mantissa=600 exponent=10 trigger=1 implicit=1 flow_type=1`**
2	SP: 512 us | SI: 614.4 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced Specific TWT (in TSF 81549894459)	`wpa_cli >` **`twt_setup setup_cmd=2 min_twt=2 mantissa=600 exponent=10 trigger=1 implicit=1 flow_type=1 twt=81549894459`**
3	SP: 512 us | SI: 614.4 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced Specific TWT (in TSF Offset 20.48 ms)	`wpa_cli >` **`twt_setup setup_cmd=2 min_twt=2 mantissa=600 exponent=10 trigger=1 implicit=1 flow_type=1 twt_offset=204800`**
4	SP: 8 ms | SI: 50 ms Setup cmd: Demand Trigger Enabled Implicit Un-Announced With Specific Flow ID 5	`wpa_cli >`**`twt_setup setup_cmd=2 min_twt=31 mantissa=50000 exponent=0 trigger=1 implicit=1 flow_type=1 flow_id=5`**

S.NO	Desired iTWT session	wpa_cli cmd to run on STA
5	SP: 8 ms | SI: 50 ms Setup cmd: Suggest Trigger Enabled Implicit Un-Announced	wpa_cli >**twt_setup setup_cmd=1 min_twt=31 mantissa=50000 exponent=0 trigger=1 implicit=1 flow_type=1**
6	SP: 8 ms | SI: 50 ms Setup cmd: Request Trigger Enabled Implicit Un-Announced	wpa_cli >**twt_setup setup_cmd=0 min_twt=31 mantissa=50000 exponent=0 trigger=1 implicit=1 flow_type=1**

1.3.3 Manual iTWT Session Teardown in STA

Irrespective of Auto iTWT session being enabled/disabled, the current active iTWT sessions can be manually teardowned using wpa_cli cmds listed below.

S.NO	iTWT session to be Teardowned	wpa_cli cmd to run on STA
1	iTWT session Flow ID 3 on the STA	wpa_cli > **twt_teardown flags=03**
2	Teardown all the active iTWT session on the STA	wpa_cli > **twt_teardown flags=128**

1.4 Basic Service Set Color (BSS Color) in SoftAP

With this 802.11ax feature, the AP & STAs can classify whether the received HE PPDU frames are intra/inter BSS transmission frames. This helps the devices to avoid decoding specific inter BSS PPDUs and go ahead with the frame transmission under specific scenarios.

In a SoftAP to select a specific BSS color between "1-63", use the following hostapd.conf param(s)

```
ieee80211ax=1
he_bss_color=<1-63>
```

1.5 Multi User – Enhanced Distributed Channel Access (MU-EDCA) in STA

In an 802.11ax network, for the STAs to do an Uplink Multi User transmission, the medium must be reserved by the AP using contention and then a Multi User Ready to Send (MU-RTS) or Trigger frame has to be sent to the STAs. For the 802.11ax AP to have a granular control over the medium contention, few MU EDCA parameters are newly introduced and advertised by the AP to STAs using the beacon IEs.

The MU-EDCA functionality in the STA can be toggled with an IFX Vendor NL80211 subcmd using the "iw" utility

S.NO	Description	iw utility cmd to run on STA
1	Check if MU-EDCA is enabled	$ **iw dev** <iface> **vendor recv 0x000319 0xb 0xa**
2	Enable MU-EDCA functionality	$ **iw dev** <iface> **vendor send 0x000319 0xb 0x1**
3	Disable MU-EDCA functionality	$ **iw dev** <iface> **vendor send 0x000319 0xb 0x0**

2 Configure & Use 6GHz Band Support

The 55573 chip has the triband capability and can operate in the 6GHz Band from CH 1 to CH 233 with 20, 40 & 80MHz Bandwidth.

2.1 Disable the 6GHz operation

To restrict the 6GHz band support in a Triband capable chip for all modes of operation, use the kernel module param “disable_6ghz” available in brcmfmac driver.

Description	Kernel module param to use during insmod in SoftAP / STA
Disable 6GHz band support	`$ insmod ./brcmfmac.ko` **`disable_6ghz=1`** `<other module params>`

Enable 6GHz band support.
Default if the chip supports it.
	`$ insmod ./brcmfmac.ko <other module params>`
	(OR)
	`$ insmod ./brcmfmac.ko` **`disable_6ghz=0`** `<other module params>`

Once the 6GHz support is disabled, check the output of “**$ iw phy**” cmd and confirm that **“Band 4”** is not listed under supported bands list.

2.2 SoftAP bringup in 6GHz

Open & WPA2 security modes are restricted in 6GHz Band, so the following hostapd conf sample is only specific to WPA3 security.

6G Band CH 1 20 MHz WPA3 SAE Primary CH 1	6G Band CH 3 40 MHz WPA3 SAE Primary CH 5	6G Band CH 7 80 MHz WPA3 SAE Primary CH 13

ctrl_interface=/var/run/hostapd
interface=wlan0
driver=nl80211
ssid=IFX-AX-WPA3-20MHz-6G
channel=1
op_class=131
hw_mode=a
wmm_enabled=1
 	
# HE confs 	
ieee80211ax=1
he_oper_chwidth=0
he_oper_centr_freq_seg0_idx=1
he_6ghz_rx_ant_pat=0
he_6ghz_tx_ant_pat=0
 	
# WPA3 confs 	
wpa=2
sae_pwe=2
sae_groups=19
ieee80211w=2
rsn_pairwise=CCMP
wpa_key_mgmt=SAE
sae_password=1234567890
	ctrl_interface=/var/run/hostapd
	interface=wlan0
	driver=nl80211
	ssid=IFX-AX-WPA3-40MHz-6G
	channel=5
	op_class=132
	hw_mode=a
	wmm_enabled=1
	
	# HE confs
	ieee80211ax=1
	he_oper_chwidth=0
	he_oper_centr_freq_seg0_idx=3
	he_6ghz_rx_ant_pat=0
	he_6ghz_tx_ant_pat=0
	
	# WPA3 confs
	wpa=2
	sae_pwe=2
	sae_groups=19
	ieee80211w=2
	rsn_pairwise=CCMP
	wpa_key_mgmt=SAE
	sae_password=1234567890
		ctrl_interface=/var/run/hostapd
		interface=wlan0
		driver=nl80211
		ssid=IFX-AX-WPA3-80MHz-6G
		channel=13
		op_class=133
		hw_mode=a
		wmm_enabled=1
		
		# HE confs
		ieee80211ax=1
		he_oper_chwidth=1
		he_oper_centr_freq_seg0_idx=7
		he_6ghz_rx_ant_pat=0
		he_6ghz_tx_ant_pat=0
		
		# WPA3 confs
		wpa=2
		sae_pwe=2
		sae_groups=19
		ieee80211w=2
		rsn_pairwise=CCMP
		wpa_key_mgmt=SAE
		sae_password=1234567890

2.3 STA association in 6GHz

To discover the available APs using scan and connect to a desired 6GHz AP, use the following sample wpa_supplicant.conf files. Open & WPA2 security modes are restricted in 6GHz Band, so the following sample is only specific to WPA3 security.

STA wpa_supplicant conf	WPA3 SAE	WPA3 OWE

To discover a desired AP by initiating a scan on all 2G, all 5G & all 6G channels and associate with it in WPA3 security	ctrl_interface=/var/run/wpa_supplicant
	sae_groups=19
	sae_pwe=2
	
	network={
	        ssid="IFX-AX-WPA3-80MHz-6G”
	        proto=RSN
	        pairwise=CCMP
	        ieee80211w=2
	        key_mgmt=SAE
	        sae_password="1234567890"
	}
		ctrl_interface=/var/run/wpa_supplicant
		
		network={
		        ssid="IFX-AX-OWE-80MHz-6G”
		        ieee80211w=2
		        key_mgmt=OWE
		}

To discover a desired AP by initiating a scan on all 2G, all 5G & only 15 6G PSC channels and associate with it in WPA3 security.
 	
Only the frequencies passed on the “scan_freq” wpa_supplicant conf param will be included in the first scan triggered after the wpa_supplicant process init. This helps in avoiding scanning all the 6G non-PSC channels and effectively reduces initial STA discover an associate duration.
	ctrl_interface=/var/run/wpa_supplicant
	sae_groups=19
	sae_pwe=2
	
	network={
	        ssid="IFX-AX-WPA3-80MHz-6G”
	        proto=RSN
	        pairwise=CCMP
	        ieee80211w=2
	        key_mgmt=SAE
	        sae_password="1234567890"
	
	        scan_freq=2412 2417 2422 2427 2432 2437 2442 2447 2452 2457 2462 5180 5200 5220 5240 5260 5280 5300 5320 5500 5520 5540 5560 5580 5600 5620 5640 5660 5680 5700 5720 5745 5765 5785 5805 5825 5975 6055 6135 6215 6295 6375 6455 6535 6615 6695 6775 6855 6935 7015 7095
	}
		ctrl_interface=/var/run/wpa_supplicant
		
		network={
		        ssid="IFX-AX-OWE-80MHz-6G”
		        ieee80211w=2
		        key_mgmt=OWE
		
		        scan_freq=2412 2417 2422 2427 2432 2437 2442 2447 2452 2457 2462 5180 5200 5220 5240 5260 5280 5300 5320 5500 5520 5540 5560 5580 5600 5620 5640 5660 5680 5700 5720 5745 5765 5785 5805 5825 5975 6055 6135 6215 6295 6375 6455 6535 6615 6695 6775 6855 6935 7015 7095
		}

2.3.1 Trigger a 6GHz scan in STA

To Trigger a scan on the 15 6G PSC channels

```
$ wpa_cli > scan freq=5975,6055,6135,6215,6295,6375,6455,6535,6615,6695,6775,6855,6935,7015,7095
```

To Trigger a scan on all the 59 6G PSC & Non-PSC channels

```
$ wpa_cli > scan freq=5935-7115
```

2.3.2 Trigger a Triband scan in STA

To Trigger a scan on the all 2G, all 5G & only 15 6G PSC channels

```
$ wpa_cli > scan freq=2400-2500,5100-5900,5975,6055,6135,6215,6295,6375,6455,6535,6615,6695,6775,6855,6935,
7015,7095
```

To Trigger a scan on all 2G, all 5G & all 6G channels

```
$ wpa cli > scan
```

3 Configure & use other features

3.1 Optimized Connectivity Experience (OCE)

OCE helps in reducing the time taken for the discovering the desired network and roaming using FILS. And with this, a relatively better BSS can be selected based on the link quality metric assessment.

The OCE functionality in the STA can be toggled with an IFX Vendor NL80211 subcmd using the "iw" utility

S.NO	Description	Iw utility cmd to run on STA
1	Check if OCE is enabled	`$ iw dev <iface> vendor recv 0x000319 0xf 0xa`
2	Enable OCE functionality	`$ iw dev <iface> vendor send 0x000319 0xf 0x1`
3	Disable OCE functionality	`$ iw dev <iface> vendor send 0x000319 0xf 0x0`

3.2 Multi Band Operation (MBO)

MBO also knows as Agile Multiband helps in the efficient usage of the available spectrum. This feature certifies the interoperability of a bundle of features that are defined by the IEEE standard amendments 802.11k, 802.11v, and 802.11u, as well as the Wi-Fi-Alliance defined specifications. These technologies are used to exchange access points (AP), band, and channel preferences, link quality, and status information between AP and client device.

Usage of "wpa_cli mbo" cmd:

```
$ wpa_cli mbo [cmd_id=1|2|4] [oper_class=<value defined by IEEE>] [pref_val=0|1|255]
[reason_code=<reason-u8>] [chan=<channel id>] [cell_cap=1|2] [enable=0|1]
[notif_type=2|3]
```

3.2.1 Add Band/Channel Preference

Command to add band/channel preference. Each unique combination considered as one entry and duplicate entry are ignored. This is a BSS specific command. "Preference" & "reason code" of the command executed at the latest will override earlier one.

Pref_val	Description
1	non-operable band/chan
2	non-operable band/chan
3	preferred band/chan

reason_code	Description
0	Unspecified
1	Beacon Strength
2	Co-located Interference
3	In-device Interference
4-255	Reserved

```
$ wpa_cli -i wlan0 mbo cmd_id=1 oper_class=115 chan=44 pref_val=0 reason_code=0
```

3.2.2 Delete Band/Channel Preference

Command to delete configured band/channel entries. This is a BSS specific command.

```
$ wpa_cli -i wlan0 mbo cmd_id=2 oper_class=115 chan=44
```

4 Frequently Asked Questions (FAQs)

4.1

Q: How to find if the STA associated to the AP is in fact operating in 802.11ax mode?

A: In the "$ wpa_cli status", look for a parameter named "wifi_generation" and this would be set to a value "6".

```
$ wpa_cli > status
bssid=<bssid>
freq=5180
ssid=IFX-AX-WPA3-80MHz-5G
id=0
mode=station
wifi_generation=6
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=SAE
pmf=2
mgmt_group_cipher=BIP
sae_group=19
sae_h2e=1
sae_pk=0
wpa_state=COMPLETED
p2p_device_address=<p2p dev address>
address=<address>
uuid=<uuid>
ieee80211ax=1
```

4.2

Q: How to verify whether the selected BSS color value is successfully set in the 802.11ax SoftAP

A: Query the currently set BSS color value using the "iw" utility in the STA & SoftAP.

```
$ iw dev <iface> vendor recv 0x000319 0x10 0xa
vendor response: 32 00 00 00
```

The received response is 32, so the correspondnig BSS color value in Decimal is "50". The other option is to check the BSS color advertised by the SoftAP in the "HE Operation" IE of the HE Beacon.

4.3

Q: When operating as a 6GHz STA, sometimes the STA disconnects with the AP automatically.

A: This could be because of the change in the regulatory domain. And this happens when the regulatory Database files installed in the Host System is very old and incompatible with the cfg80211 that is being used. Avoid this issue by removing/renaming the following files from the Host platform.

```
/lib/firmware/regulatory.db
/lib/firmware/regulatory.db.p7s
/usr/lib/crda/regulatory.bin
```

Revision history

Document version	Date of release	Description of changes
1.0	2023-02-17	Initial Release

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2023-02-17
Published by
Infineon Technologies AG
81726 München, Germany

Do you have a question about this document?
Email: erratum@infineon.com

Document reference
002-37098 Rev 1.1

IMPORTANT NOTICE
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.