

6GHz WiFi Packet Capture (control and center frequency configuration)

Goal: Capture 6Ghz WiFi packets.

Candela offers several radios that are capable of 6GHz WiFi packet capture (see note above), each with their own quirks. While the main approach to WiFi packet capture remains unchanged from 2.4GHz/5GHz packet capture, there are a few key differences that are easy to overlook:

- 6GHz APs must use WPA3 or OWE
 - Decrypting WPA3 network traffic is possible with Wireshark but requires additional steps compared to WPA/WPA2 traffic decryption
- 6GHz APs must use PMF (protected management frames)
 - Remember: the data portion of all PMFs after 4-way handshake are encrypted
 - This is to protect against malicious de-authentication attempts
 - Wireshark may support this, but we have not tested it
- Intel AX210 and BE200 radios will not sniff 6GHz until they detect that they are in a US regulatory domain
 - This is a limitation in Intel radio firmware
 - See the cookbook on the website or the manual setup below for doing so

GHz WiFi packet capture only relevant for tri-band radios, including the Intel AX210/BE200 and the MTK 7922, 7925, and 7996 radios.

Manual Setup (w/ LANforge GUI)

NOTE: The monitor in the **Port Mgr** tab may not display updated information on the monitor channel. Verify correct configuration by running iw moni0 info in a terminal, where moni0 is the name of your sniffer.

1. Select a radio to sniff with and ensure its channel is set to AUTO.

		wipny2 (ct5230	Status Informatio	ngure settings	000
Curren	t: LINK-DOWN NO	NE	- Status Informatic	A1	
Driver I	Info: WIFI-Radio Driver	r: iwlwifi (BE200) Bus: 0000:06	:00.0 Firmware: 94	4.62990553.0 gl-c0-fm-c0-94.uc, Features: 80	02.11abgn-BE
		Por	t Configurable	25	
Standar	rd Configuration	Extended Config	Firm <u>w</u> are		
		Gener	al Interface S	Settings	
		Down			
		A <u>l</u> ias:			
		MAC Addr	e4:60:17:65	:33:85	
		Rpt Timer:	medium (8 s)	
		-1-			
	This radio support	5:	wifi Settings		
		Virtual Stations	:	1	
		Associated Clien	ts:	1	
		Virtual APs:		0 802 11abon-BE	
		reactires.		002.1180gn-02	
	Country:	United States (840)			
	Channel/Freq:	AUTO (-1 Mhz)	✓ AP:	DEFAULT	
	Antenna:	All (2x2)	Tx-Po	ower: DEFAULT (-1)	-
	RTS:	DEFAULT	Frag	2346	
) a hura
	No Runtime				Jebug
		Ignore RADAR	on't Share Sc	an 📋 verbose Debug 📋 Use S	syslog
Print	Display Lo	gs <u>P</u> robe	e <u>S</u> ync	Apply <u>O</u> K	<u>C</u> ancel

2. Either create a station or use an existing station on the monitor radio and associate it to an AP. Ensure that it obtains an IP address.

							All	Network Interfaces	(Ports) for all Resources	5.				
Por	t Ø	î	Parent Dev	Channel	Alias	SSID	AP	IP	Mode	Signal	Device	MAC	Port Type	Hardware
1.3.1	0		wiphy2	339	wlan2	jrm1-6ghz-ch149e	38:F8:F6:8F:F6:46	10.41.0.7	802.11a-BE 320 2x2	-60 dBm	wlan2	e4:60:17:65:33:85	WIFI-STA	BE200
1.3.1	1		wiphy1	36	wlan1	jrm1-5ghz-ch36	38:F8:F6:5E:29:4A	10.41.0.5	802.11an-BE 80 2x2	-54 dBm	wlan1	e4:60:17:65:35:01	WIFI-STA	BE200
1.3.1	3		wiphy0	1	wlan0	jrm1-2ghz-ch6	38:F8:F6:07:5E:44	10.41.0.6	802.11bgn-BE 40 2x2	-42 dBm	wlan0	e4:60:17:64:e0:97	WIFI-STA	BE200

The ability to create a station validates that the parent radio is free to transmit on the 6ghz spectrum. If the radio refuses to associate a station, then there might be a mixture of regulatory domains being broadcast, or the channel is not a PSC channel.

- Admin-down the station if it is on the monitor radio.
 (Select the station and click the Down button [I] or Alt + S)
- 4. Set the monitor radio's channel to the channel you want to sniff.

O wiphy2 (ct523c-6e10) Cor	figure Settings 💿 📀 😣
Port Status Informat	ion
Current: LINK-DOWN NONE	
Driver Info: WIFI-Radio Driver: WWifi (BE200) Bust 0000:06:00.0 Firmware:	4.62990553.0 g+cu-tm-cu-94.uc, Features: 802.11 abgn-BE
Port Configurab	les
Standard Configuration Extended Config Firmware]
General Interface	Settings
Down	
Alias:	
MAC Addr: e4:60:17:6	5:33:85
Rpt_Timer: medium	(8 s) 🔻
WiFi Setting	5
This radio supports:	
Virtual Stations:	1
Associated Clients:	1
VIITUAL APS: Features:	0 802.11abon-BE
Country: United States (840)	
Channel/Freq: 339 149e (6695 Mhz)	DEFAULT
Antenna: All (2x2) Tx-F	ower: DEFAULT (-1)
RTS: DEFAULT Frag	p: 2346
🗌 No Runtime PM 📄 Extra TxStatus 📄 TXS Al	Extra RxStatus OFDMA Debug
Iqnore RADAR Don't Share S	can 🗌 Verbose Debug 🔲 Use Syslog
Print Display Logs Probe Sync	Apply <u>O</u> K <u>C</u> ancel

5. Set the monitor to the desired bandwidth.

()	moni0 (ct523c-6e10) Configure Settings 💿 📀 🗵
	Port Status Information
Current:	LINK-UP NONE
Driver In	fo: WIFI-MON Parent: wiphy2, Driver: iw/wifi, Features: 802.11abgn-BE wiphy2
	Port Configurables
Standard Configuration	DIN Extended Config
Enable	General Interface Settings
Set MAC	
Set TX Q Len	Down
Set MTU	Aliast
Set Offload	Alīds.
Set PROMISC	Rp <u>t</u> Timer: medium (8 s)
Low Level	
PROMISC	WiFi Settings
TSO Enabled	
UFO Enabled	AID 0 AP: DEFAULT
GSO Enabled	Bandwidth: 320Mbz (320 Mbz)
LRO Enabled	20Mbz (20 Mbz)
GRO Enabled	40Mhz (40 Mhz)
	80Mhz (80 Mhz)
	160Mhz (160 Mhz)
Print Display	<u>H320Mhz (320 Mhz)</u> <u>Apply</u> <u>OK</u> <u>Cancel</u>

6. With the monitor selected, click **Sniff Packets**.



Logged in to: 192.168.92.10:4002 as: Admin

Simultaneous Sniffing

Plenty of situations would require sniffing from multiple monitors at the same time. This can be done using the GUI or with some basic shell scripting.

Using the LANforge GUI

1. Set the center channel for each of the radios you want to sniff from.

• wiphy2 (ct523c-6e10) Configure Settings	\odot \otimes \otimes
Port Status Information	
Current: LINK-DOWN NONE	
Driver Into: WIFI-Radio Driver: WWith (BE200) Bus: 00000600.0 Firmware: 94.62990553.0 gFc0-tm-c0-94.0c, Features: 802	L11abgn-BE
Port Configurables	
Standard Configuration Extended Config Firm <u>w</u> are	
General Interface Settings	
Down	
Alias:	
MAC Addr: e4:60:17:65:33:85	
Rp <u>t</u> Timer: medium (8 s) 🔽	
WiFi Settings	
This radio supports:	
Virtual Stations: 1	
Associated Clients: 1	
Features: 802.11abon-BE	
Country United States (840)	
Channel/Freq: 339 149e (6695 Mhz)	
Antenna: All (2x2) Tx-Power: DEFAULT (-1)	-
RTS: DEFAULT Frag: 2346	
🗌 No Runtime PM 📄 Extra TxStatus 📄 TXS All 📄 Extra RxStatus 📄 OFDMA De	ebug
🗌 Ignore RADAR 📃 Don't Share Scan 📃 Verbose Debug 📃 Use Sy	yslog
Print Display Logs Probe Sync Apply OK	<u>C</u> ancel

2. You can select three radios (using shift-click-drag or ctrl-click select).

Status	F	Port	t Mgr 🛛 Exte	nded Port	Mgr RF-Ge	nerato	r	Resource Mgr D	UT Profiles T
					Disp: 192.168	3.92.19	4:1	Sniff P	ackets
					Rpt Timer: me	dium	(8	s) 🔻 Ap	ply 🗌
									All Network]
Port	ø	î	Parent Dev	Channel	Alias	SSID	AP	IP	Mode
1.2.18			rd0a		rd0b			10.40.0.251	
1.3.00					eth0			192.168.92.194	
1.3.01					eth1			0.0.00	
1.3.02				6	wiphy0			0.0.00	802.11abgn-BE
1.3.03				36	wiphy1			0.0.00	802.11abgn-BE
1.3.04				339	wiphy2			0.0.00	802.11abgn-BE
1.3.05				0	wiphy3			0.0.00	802.11abgn-BE
1.3.06				0	wiphy4			0.0.00	802.11abgn-BE
1.3.07				0	wiphy5			0.0.00	802.11abgn-BE
1.3.08				0	wiphv6			0.0.0.0	802.11abon-BF

3. Then click **Sniff Packets** and the LANforge server will create multiple monitor interfaces, then one (or more) Wireshark instances will appear sniffing traffic.

Status		Port	Mgr Ext	ended Port	Mgr RF	-Gener	ator	Reso	urce Mg	DUT	Prof	iles (Traffi	c-Profiles	Aler	ts Wa	rnings	Wifi-Me	ssages	; +	
					Disp: 192	168.92	.194:1		4	Sniff Packe	ets	[Do	wn 1	Clear	Counter	s	Reset Por	rt	Delete	
					Rpt Timer:	mediu	m (8	s)	•	Apply		[VR	f I	0	isp <u>l</u> ay		Cr <u>e</u> ate		Mo <u>d</u> ify	<u>B</u> atch Modif
						-					-All N	letwork	Inter	faces (Po	rts) for a	II Resour	rces. —				
		_				0					*n	noni2a	, mo	ni3a, ar	nd mon	i0 (as sı	perus	er)			\odot \land \times
Port	Ø	2 ↓ Parent Dev Channel		Alias	File	Edit	View	Go	Capture	Analy	ze Sta	tistics	Telepi	hony V	Vireless	Tools	Help				
1.2.18	_	-	rd0a		rd0b	_	_		-	_	_	-	0						~	~ ~	200
1.3.00					eth0			J	۲	0101 0310 0311	X	C	9				2 📃		Ð		2 4
1.3.01					eth1				<i>C</i> 1.	-											
1.3.02				6	wiphy0		oply a c	lisplay	/ filter	<ctrl-></ctrl->											
1.3.03				36	wiphy1	No.	Т	ime		Source			_	Destinat	ion		Protoc	ol Lengt	th Info		A
1.3.04				339	wiphy2	32	2957 1	0.993	3677368					Intel_8	Be:b0:e	8	802.1	1 6	2 Ackr	nowledger	ment, F
1.3.05				0	wiphy3	32	2958 1	0.993	3679973	Intel	_8e:b0	0:e8		ASUSTel	COMPU_	af:62:.	. 802.1	1 6	8 Requ	uest-to-s	send, F
1 2 07				0	wiphy4	32	2959 1	0.99	3680996					Intel_8	3e:b0:e	8	802.1	1 6	2 Clea	ar-to-ser	id, Fla
13.07				0	wiphy5	32	2900 1	0.994	1493023					Intel 8	Re:b0:e	8	802.1	1 6	2 Ackr	nowledger	ment. F
l anna d i		. 10	0.100.00.10	4002	A alas in	32	2962 1	0.994	4495647	ASUST	ekCOMF	V_af:0	62:	Broadca	ist	-	802.1	1 13	0 Tri	gger HĔ Đ	Basic,
Logged I	n to:	: 19	2.108.92.10	1:4002 as: /	Admin	32	2963 1	0.995	5220917	ASUST	ekCOMF	PU_af:0	52:	Intel_3	3c:29:7	7	802.1	1 8	2 802	.11 Block	Ack,
						32	2964 1 2065 1	0.99	5223444	ASUST	ekcomp	νυ_aτ:	52:		Se:D⊍:T (COMPII	2 af:62:	802.1	1 6	2 Cles	uest-to-se	3end, ⊢ nd Ela
						32	2966 1	0.995	5226532					ADDDIC		u1.02	WLAN	8	6 Radi	iotap Ca	oture v
						32	2967 1	0.914	4214595	Adtra	1_8f:f	6:46		Broadca	ast		802.1	1 32	6 Bead	con frame	e, SN=1
						32	2968 1	0.914	4219441	Hewle	tPack	(a_c5:	03:	Broadca	ist		802.1	1 14	6 Data	a, SN=292	23, FN=
						4															
						L Er	amo 1	· 68	hytes	on wire	(544	hits)	68	hytes c	anturo	d (544	hite)	on inte	rface	moni2a	id 0
						Ra	diota	. 00 р Неа	ader v0	, Lenath	1 48	DIC3),	00	bytes t	apeure	u (344	0103)	on The	Tace	ποπ12α,	10 0
						▶ 80	2.11	radio	o infor	mation											
						→ IE	EE 80	2.11	Reques	t-to-ser	nd, Fl	.ags: .		C							
_							Z w	iresha	rk_3_int	erfacesCK	0XY2.p	capng				Packet	ts: 3296	8 · Droppe	ed: 0 (0	.0%) Pro	ofile: Default

Saving and Finding the Capture

1. Stop the capture (click the **b**utton.



2. Save the capture(s) to files.

	ioni3a, and moni0 (as superuser) 💿 🛇 😣
<u>File E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatist	ics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp
Open Ctrl+O	← → ≝ 주 분
Open <u>R</u> ecent	
<u>M</u> erge	Destination Protocol Length Info
Import from Hex Dump	Intel_8e:b0:e8 802.11 62 Acknowledgement, F
<u>C</u> lose Ctrl+W	ASUSTekCOMPU_af:62:802.11 68 Request-to-send, F — Intel_8e:b0:e8 802.11 62 Clear-to-send, Fla
Save Ctrl+S	WLAN 74 Radiotap Capture v Intel 8e:b0:e8 802.11 62 Acknowledgement, F
Save <u>A</u> s Ctrl+Shift+S	Broadcast 802.11 130 Trigger HĔ Basic, Thtel 3c:29:77 802.11 82 802.11 Block Ack
File Set	Intel_8e:b0:f2 802.11 68 Request-to-send, F
Export Specified Packets	WLAN 86 Radiotap Capture v
Export Packet Dissections	Broadcast 802.11 326 Beacon Frame, SN=1 Broadcast 802.11 146 Data, SN=2923, FN=
Export Packet <u>B</u> ytes Ctrl+Shift+X	
Export PDUs to File	bytes captured (544 bits) on interface moni2a, id 0
Strip Headers	
Export TLS Session Keys	
Export Objects	▶ _
Print Ctrl+P	_
Quit Ctrl+Q	
wireshark_3_interfacesCK0XY2.pcapng	Packets: 32968 · Dropped: 0 (0.0%) Profile: Default
Wireshark · S	ave Capture File As (as superuser)
Look in: 📄 /home/lanforge/report-data	- 3 0 6 📰 🗏
Scomputer Name	 Size Type Date Modified
Computer Name	Size Type Date Modified
Computer	Size Type Date Modified
Computer Name / / File name: three-capture	▼ Size Type Date Modified
Computer Name Image:	Size Type Date Modified Size Type Image: Size Image: Size Image: Size Image: Size
Computer Name / / File name: three-capture Save as: Wireshark/ pcapng	

3. To view the capture later, use the command: \$ wireshark <filename>

O MATE Terminal	(
<pre>lanforge@ct523c-6e10:~\$ cd report-data/ lanforge@ct523c-6e10:~/report-data\$ wireshark tl</pre>	bree-capture pcappo

Using the _lf_sniff*radio.py* Script

The lf_sniff_radio.py (in *scripts/py-scripts*) can help automate packet capture by creating monitor interfaces on the desired radio and doing a sniff with tshark or dumpcap. Make sure that your parent radios are lacking stations or virtual APs.



You would save the script (E.G. /home/lanforge/scripts/py-scripts/my-sniffer.bash) and run the script from the current directory (as root):



Please refer to the help output from ./lf_sniff_radio.py --help | less.

Saving and Finding the Capture

Use wireshark on each of the resulting files specified on the --outfile parameters above.

Tips About Transmitting on the Channel

It is important to remember that radios in monitor mode are subject to the same power dynamics that stations and APs experience when transmit power is too strong. **Sending traffic from a radio in the same system as your monitor radio will be too strong a signal to capture all packets**.

- 1. Use a separate LANforge for stations
- 2. Use a separate LANforge system for monitoring/packet capture

If there are insufficient packets received, you might have at least one of these issues:

- 1. Your monitor system is too close to the AP, the station, or both. You might need to use *in-line attenuators* on the antennas of the system to not drop frames.
- 2. The antenna diversity does not match. When sniffing with an AX210 or BE200 radio, you have 2x2 diversity. This might only capture beacons and a few control frames. If the AP or the station negotiate to 3x3 or 4x4 diversity, a 2x2 monitor radio will be inadequate.

Manual Setup (w/o LANforge GUI)

First way is to bring up a station on the desired 6ghz ssid and allow it to fully connect. Once it is connected, highlight the station's parent radio and select the sniff packets button. This will create a monitor mode

interface on the same parent radio as the station and allow sniffing while the station is connected. The downside to this method is that the station must remain connected in order for the monitor mode interface to continue sniffing on the desired 6ghz channel.

The second way is to use another AX210 as an independent monitor mode interface, but you will need the following manual steps in order to get the frequency setup:

- admin up the wlan interface on a WiFi 6E radio and let it scan all bands (2, 5, 6ghz which takes a minute or two).
- highlight the wiphy 6E radio in **Port Mgr** and select **Sniff Packets** to create the monitor interface. Note the moni interface number such as *moni1a*, *moni2a*, etc...
- Stop the wireshark capture, but leave the window open
- Admin down the wlan interface, but leave the wiphy and moni interfaces up
- Open a terminal window and type the following commands:
 - o su -
 - cd /home/lanforge
 - . lanforge.profile (note there is a space between the first . and lanforge)
 - iw dev monila info (using the interface number noted previously)
 - iw dev monila set freq [6E channel frequency which is 6455]
 - iw dev monila info (checking that the 6E frequency was set)
- If the last step is successful, you should be able to re-start the wireshark capture and observe captured frames on the 6ghz band.

Understanding control frequency and center frequency

The control frequency will change base on settings. The center frequency will stay the same with in the bandwidth, For example for channel 7 with 80Mhz bw , here are the monitor commands possible:

- iw dev moni10a set freq 5955 80 5985
- iw dev monil0a set freq 5975 80 5985
- iw dev moni10a set freq 5995 80 5985
- iw dev monil0a set freq 6015 80 5985

The *iw* command syntax

iw dev monilOa set freq <control frequency> <Band width> <center frequency>

Usage:

```
iw [options] dev <devname> \
    set freq <freq> [NOHT|HT20|HT40+|HT40-|5MHz|10MHz|80MHz] \
    dev <devname> \
    set freq <control freq> [5|10|20|40|80|80+80|160] \
    [<center1_freq> [<center2_freq>]]
Options:
    --debug enable netlink debugging
```

Conversion between channel a Frequency

• Candela numbering system (starting 6e channel 191), note algorithm works for 5g

• 6e ch = (6e freq - 5000) / 5

• 6e freq = (ch 6e * 5) + 5000

Support description

- 1. The monitor port needs to be on the same radio as the station. So if the station is on wiphy1, the monitor port must also be on wiphy1. I was able to see some packets that way. Highlight the radio the station is on and click **Sniff Packets**. *The downside to this method is that the station must remain connected in order for the monitor mode interface to continue sniffing on the desired 6ghz channel.*
- 2. The second way is to use another AX210 as an independent monitor mode interface, but there are some manual steps in order to get the frequency setup:
 - 1. admin up the wlan interface on a wiphy 6E NIC and let it scan all bands (2, 5, 6ghz which takes a minute or two).
 - 2. highlight the wiphy 6E NIC in port mgr and select 'Sniff Packets' to create the monitor interface...note the moni interface number such as (moni1a, moni2a, etc...).
 - 3. stop the wireshark capture, but leave the window open
 - 4. admin down the station interface, but leave the wiphy and moni interfaces up
 - 5. open a terminal window and type the following commands:
 - su [Enter]
 - cd /home/lanforge [Enter]
 - lanforge.profile [Enter]
 - iw dev monila info Enter
 (replace monila with your monitor interface)
 - iw dev monila set freq <control-freq> <channel-width> <centerfrequency> Enter
 - iw dev monila info Enter (checking that the 6E frequency was set)
 - 6. Restart the wireshark capture and observe captured frames on the 6ghz band.

Candela Technologies, Inc., 2417 Main Street, Suite 201, Ferndale, WA 98248, USA www.candelatech.com | sales@candelatech.com | +1.360.380.1618