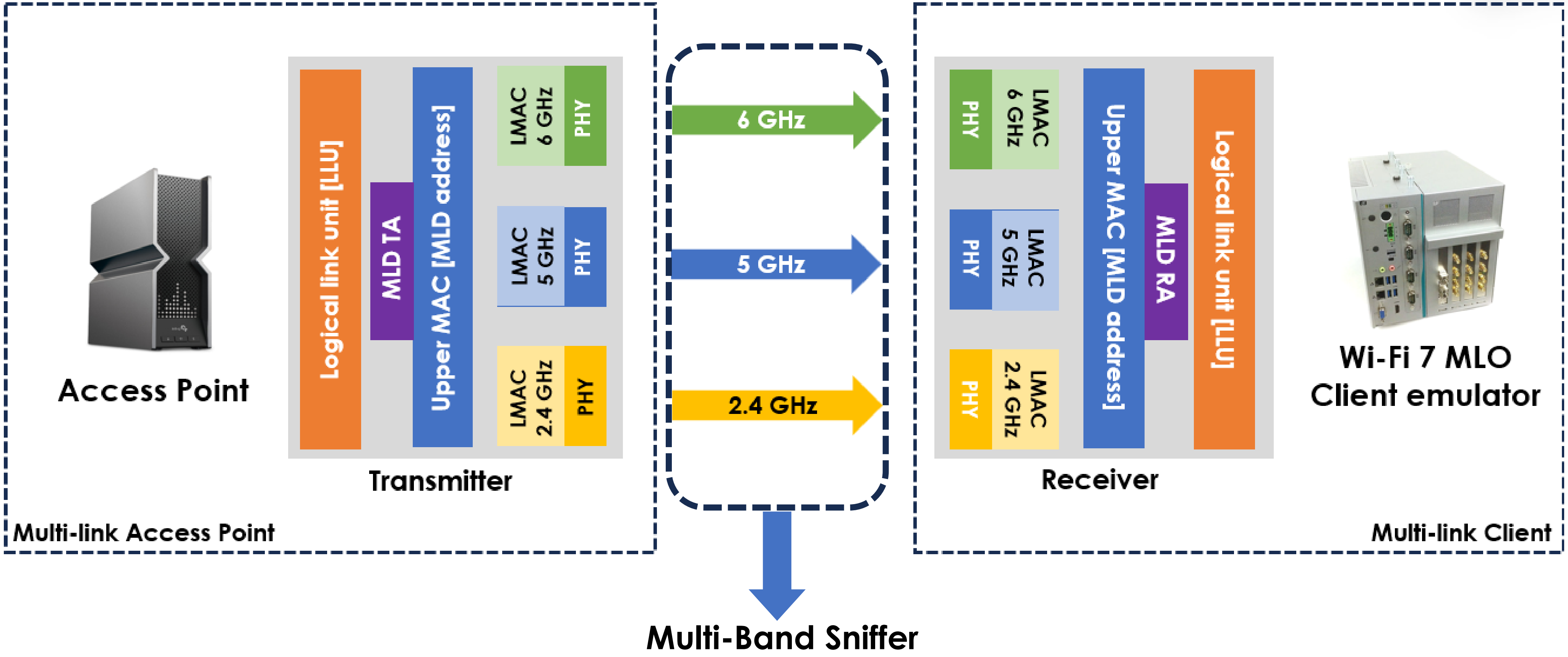
Network Testing & Emulation Solutions

Tri-Band sniffing using LANforge

✉ sales@candelatech.com
☎ 1-360-380-1618

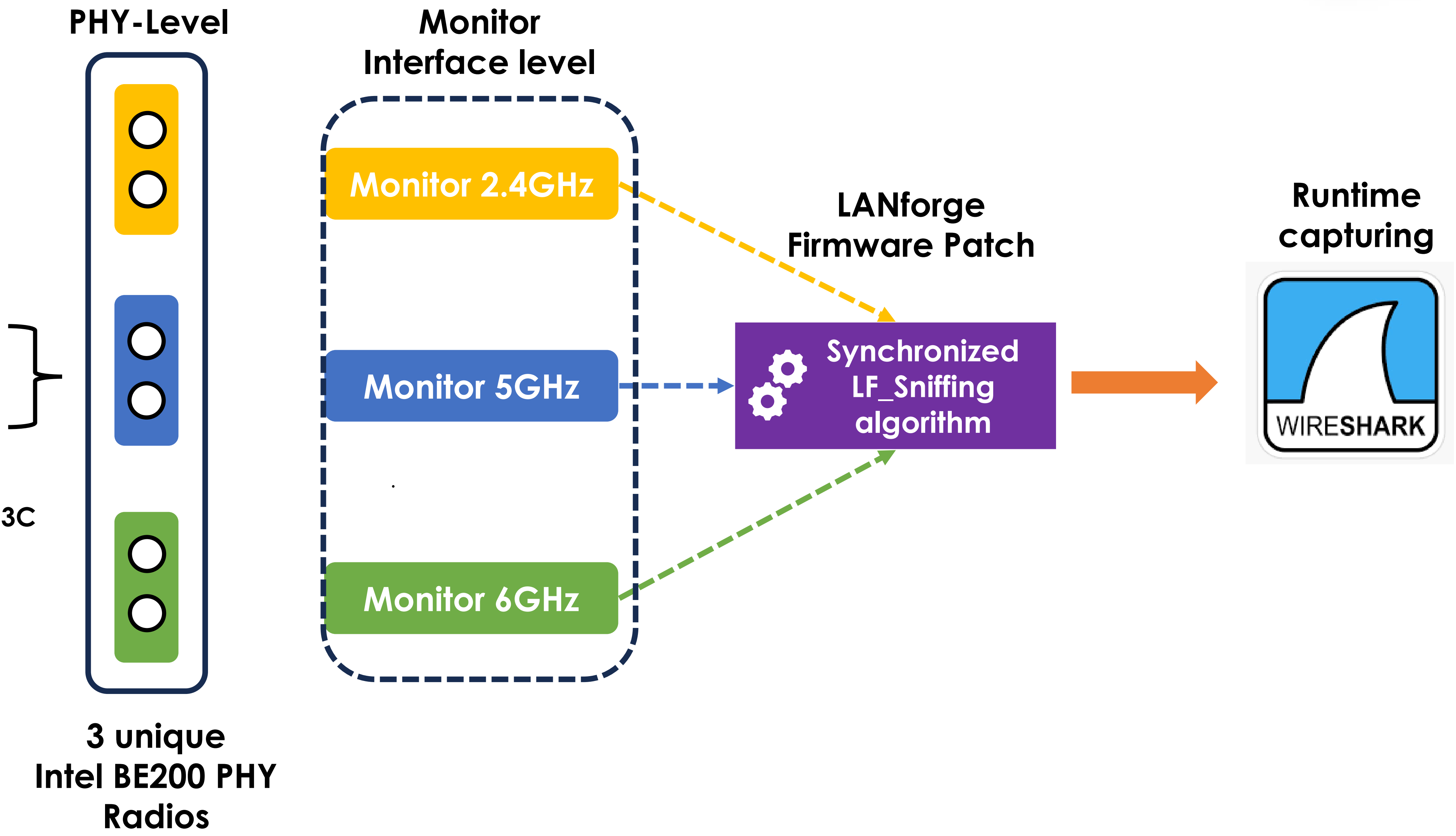
Multi-link sniffing:



- The multi-link sniffer will try to capture all the frames and layer-2 information that is being transmitted or received in all the bands available.
- It will synchronize the time stamps and capture all the frames parallelly at one instance.

Multi-band Sniffing PHY-level architecture:

LANFORGE CT-523C
Wi-Fi 7 Sniffer



PHY-Level

Monitor
Interface level

Monitor 2.4GHz

Monitor 5GHz

Monitor 6GHz

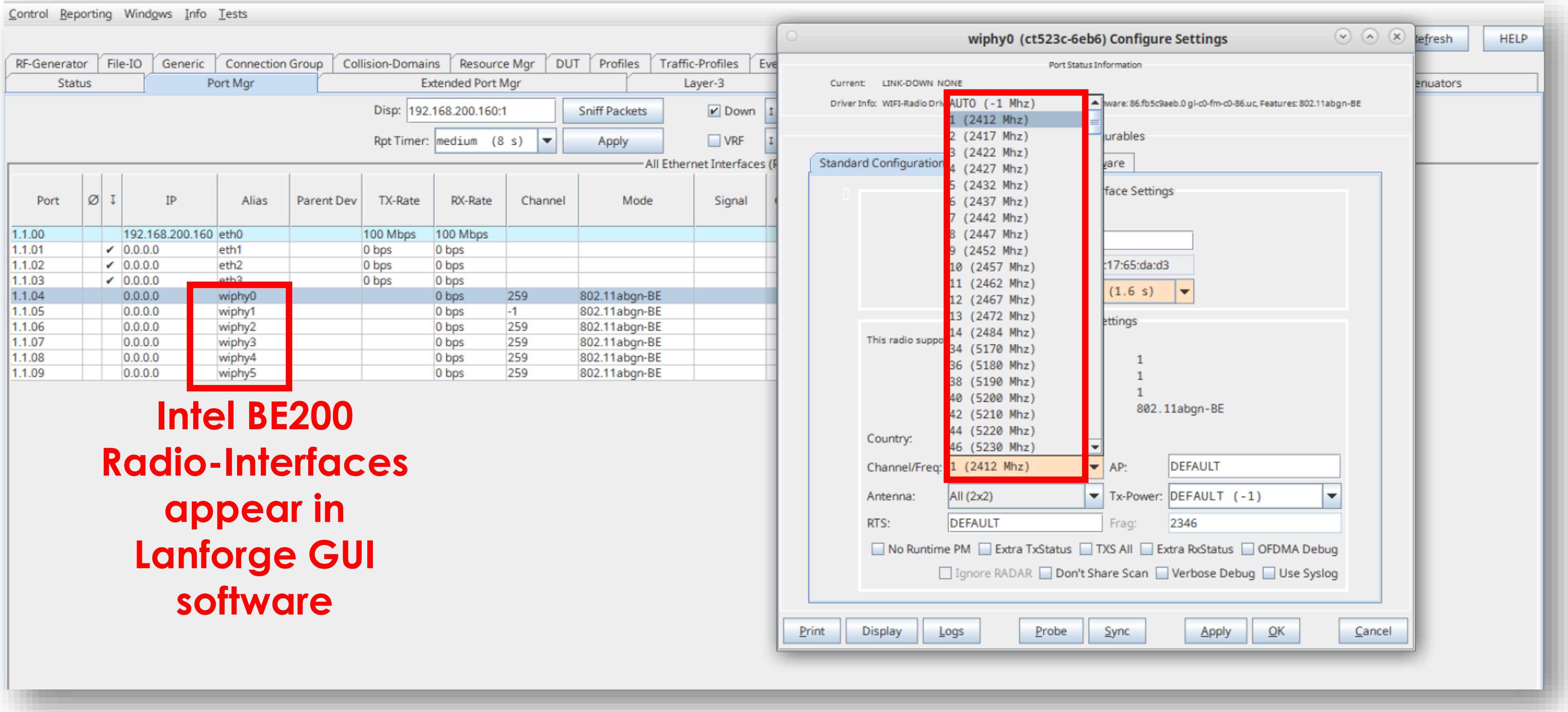
LANforge
Firmware Patch

Synchronized
LF_Sniffing
algorithm

Runtime
capturing

3 unique
Intel BE200 PHY
Radios

Multi-band Sniffing:



Disp: 192.168.200.160:1

Rpt Timer: medium (8 s)

☑ Down

☐ VRF

Port	Ø	↧	IP	Alias	Parent Dev	TX-Rate	RX-Rate	Channel	Mode	Signal
1.1.00			192.168.200.160	eth0		100 Mbps	100 Mbps			
1.1.01		✓	0.0.0.0	eth1		0 bps	0 bps			
1.1.02		✓	0.0.0.0	eth2		0 bps	0 bps			
1.1.03		✓	0.0.0.0	eth3		0 bps	0 bps			
1.1.04			0.0.0.0	wiphy0			0 bps	259	802.11abgn-BE	
1.1.05			0.0.0.0	wiphy1			0 bps	-1	802.11abgn-BE	
1.1.06			0.0.0.0	wiphy2			0 bps	259	802.11abgn-BE	
1.1.07			0.0.0.0	wiphy3			0 bps	259	802.11abgn-BE	
1.1.08			0.0.0.0	wiphy4			0 bps	259	802.11abgn-BE	
1.1.09			0.0.0.0	wiphy5			0 bps	259	802.11abgn-BE	

wiphy0 (ct523c-6eb6) Configure Settings

Port Status Information

Current: LINK-DOWN NONE

Driver Info: WIFI-Radio Dri… …ware: 86.fb5c9aeb.0 gl-c0-fm-c0-86.uc, Features: 802.11abgn-BE

…urables

Standard Configuration … …are

…face Settings

…:17:65:da:d3

(1.6 s)

…ettings

This radio suppo…

1
1
1
802.11abgn-BE

```
AUTO (-1 Mhz)
1 (2412 Mhz)
2 (2417 Mhz)
3 (2422 Mhz)
4 (2427 Mhz)
5 (2432 Mhz)
6 (2437 Mhz)
7 (2442 Mhz)
8 (2447 Mhz)
9 (2452 Mhz)
10 (2457 Mhz)
11 (2462 Mhz)
12 (2467 Mhz)
13 (2472 Mhz)
14 (2484 Mhz)
34 (5170 Mhz)
36 (5180 Mhz)
38 (5190 Mhz)
40 (5200 Mhz)
42 (5210 Mhz)
44 (5220 Mhz)
46 (5230 Mhz)
```

Country:

Channel/Freq: 1 (2412 Mhz)

AP: DEFAULT

Antenna: All (2x2)

Tx-Power: DEFAULT (-1)

RTS: DEFAULT

Frag: 2346

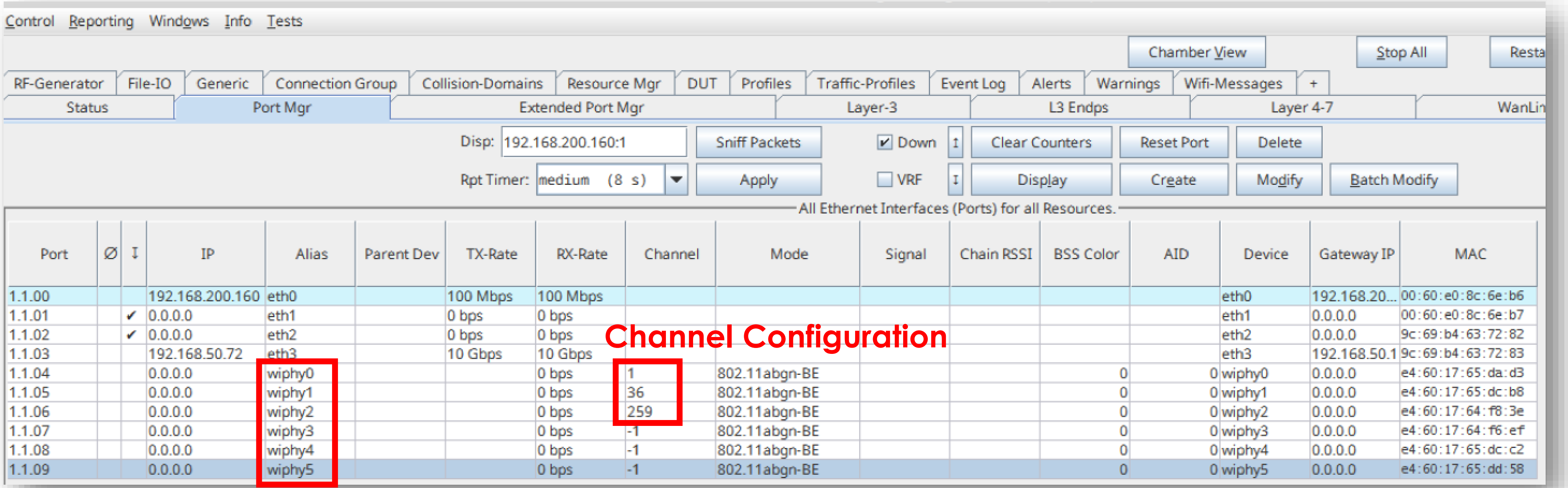
☐ No Runtime PM ☐ Extra TxStatus ☐ TXS All ☐ Extra RxStatus ☐ OFDMA Debug

☐ Ignore RADAR ☐ Don't Share Scan ☐ Verbose Debug ☐ Use Syslog

Intel BE200 Radio-Interfaces appear in Lanforge GUI software

- In LANforge, we have multiple radios available to work in Management and monitor modes.
- These radio interfaces can be configured to various channels that can operate a various AP bands.
- We can create a monitor mode on the radio interface to sniff packets.

Multi-band Sniffing:



Disp: 192.168.200.160:1

Rpt Timer: medium (8 s)

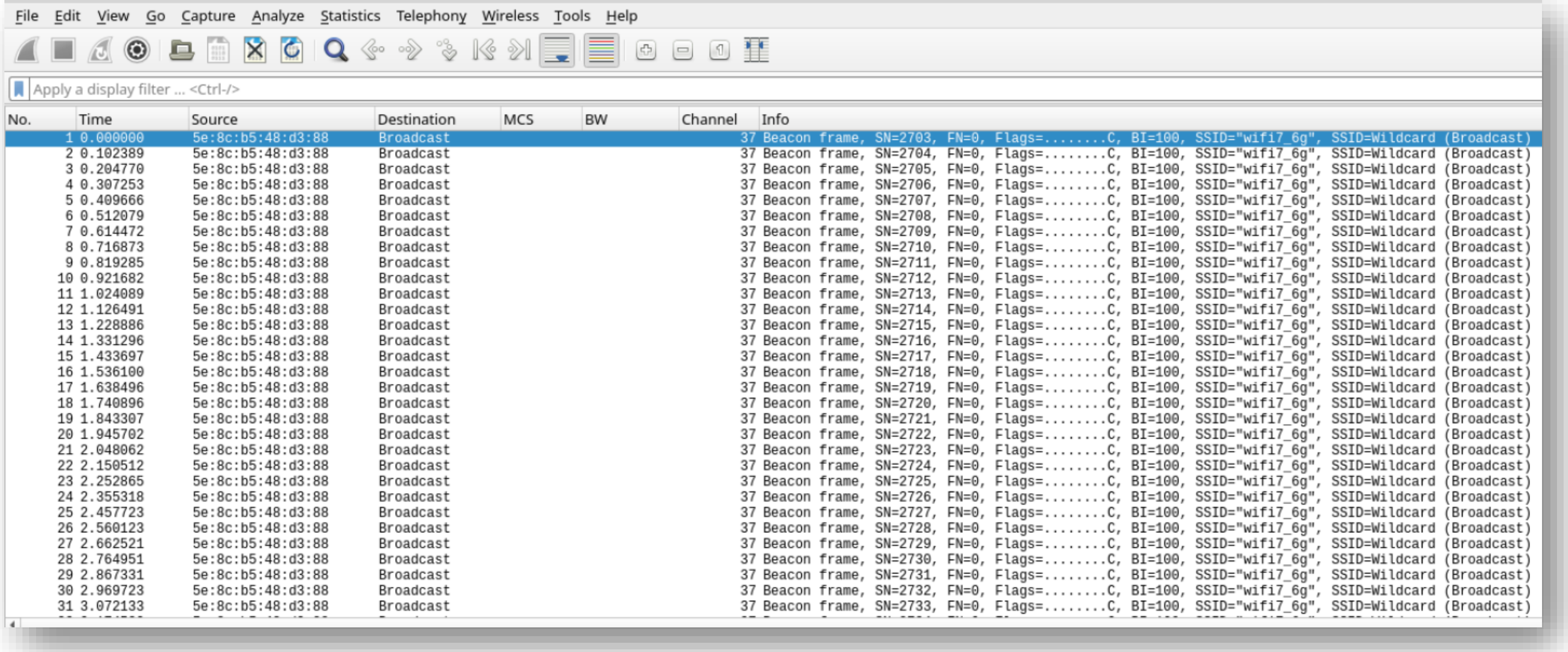
Port	Ø	↧	IP	Alias	Parent Dev	TX-Rate	RX-Rate	Channel	Mode	Signal	Chain RSSI	BSS Color	AID	Device	Gateway IP	MAC
1.1.00			192.168.200.160	eth0		100 Mbps	100 Mbps							eth0	192.168.20...	00:60:e0:8c:6e:b6
1.1.01		✔	0.0.0.0	eth1		0 bps	0 bps							eth1	0.0.0.0	00:60:e0:8c:6e:b7
1.1.02		✔	0.0.0.0	eth2		0 bps	0 bps							eth2	0.0.0.0	9c:69:b4:63:72:82
1.1.03			192.168.50.72	eth3		10 Gbps	10 Gbps							eth3	192.168.50.1	9c:69:b4:63:72:83
1.1.04			0.0.0.0	wiphy0			0 bps	1	802.11abgn-BE			0	0	wiphy0	0.0.0.0	e4:60:17:65:da:d3
1.1.05			0.0.0.0	wiphy1			0 bps	36	802.11abgn-BE			0	0	wiphy1	0.0.0.0	e4:60:17:65:dc:b8
1.1.06			0.0.0.0	wiphy2			0 bps	259	802.11abgn-BE			0	0	wiphy2	0.0.0.0	e4:60:17:64:f8:3e
1.1.07			0.0.0.0	wiphy3			0 bps	-1	802.11abgn-BE			0	0	wiphy3	0.0.0.0	e4:60:17:64:f6:ef
1.1.08			0.0.0.0	wiphy4			0 bps	-1	802.11abgn-BE			0	0	wiphy4	0.0.0.0	e4:60:17:65:dc:c2
1.1.09			0.0.0.0	wiphy5			0 bps	-1	802.11abgn-BE			0	0	wiphy5	0.0.0.0	e4:60:17:65:dd:58

Radio’s Available

We have forced 3 different PHY-radios to 3 different channels which operate respectively:

- 2.4 GHz: Channel 1
- 5 GHz: Channel 36
- 6 GHz: Channel 37

Multi-band Sniffing:



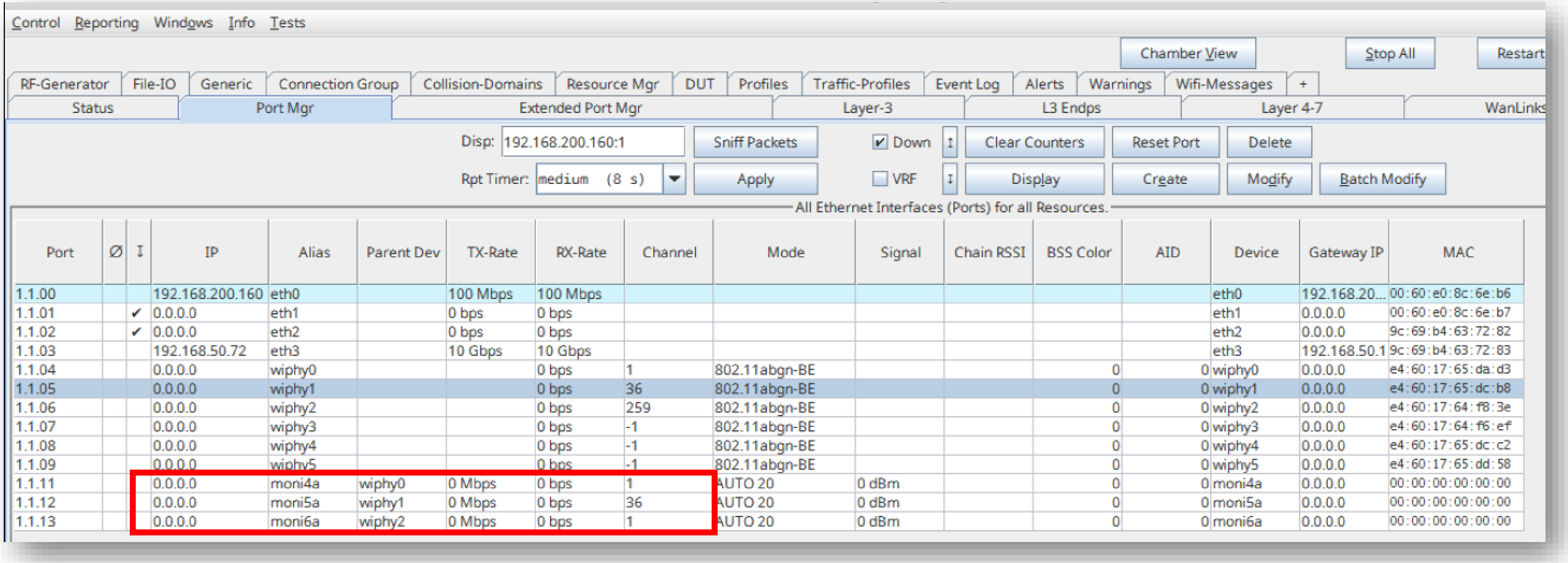
No.	Time	Source	Destination	MCS	BW	Channel	Info
1	0.000000	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2703, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
2	0.102389	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2704, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
3	0.204770	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2705, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
4	0.307253	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2706, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
5	0.409666	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2707, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
6	0.512079	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2708, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
7	0.614472	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2709, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
8	0.716873	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2710, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
9	0.819285	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2711, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
10	0.921682	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2712, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
11	1.024089	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2713, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
12	1.126491	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2714, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
13	1.228886	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2715, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
14	1.331296	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2716, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
15	1.433697	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2717, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
16	1.536100	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2718, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
17	1.638496	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2719, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
18	1.740896	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2720, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
19	1.843307	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2721, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
20	1.945702	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2722, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
21	2.048062	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2723, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
22	2.150512	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2724, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
23	2.252865	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2725, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
24	2.355318	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2726, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
25	2.457723	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2727, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
26	2.560123	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2728, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
27	2.662521	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2729, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
28	2.764951	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2730, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
29	2.867331	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2731, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
30	2.969723	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2732, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)
31	3.072133	5e:8c:b5:48:d3:88	Broadcast			37	Beacon frame, SN=2733, FN=0, Flags=........C, BI=100, SSID="wifi7_6g", SSID=Wildcard (Broadcast)

- To sniff on 6GHz channels we need to use some terminal commands for forcing the channel on respective PHY-interface available.

Here are the list of commands:

- su (Root login)
- . lanforge.profile
- iw dev moni6a info [any monitor interface]
- iw dev monia6a set freq 6295 320MHz [center frequency and Bandwidth information]

Multi-band Sniffing:



Disp: 192.168.200.160:1

Rpt Timer: medium (8 s)

☑ Down

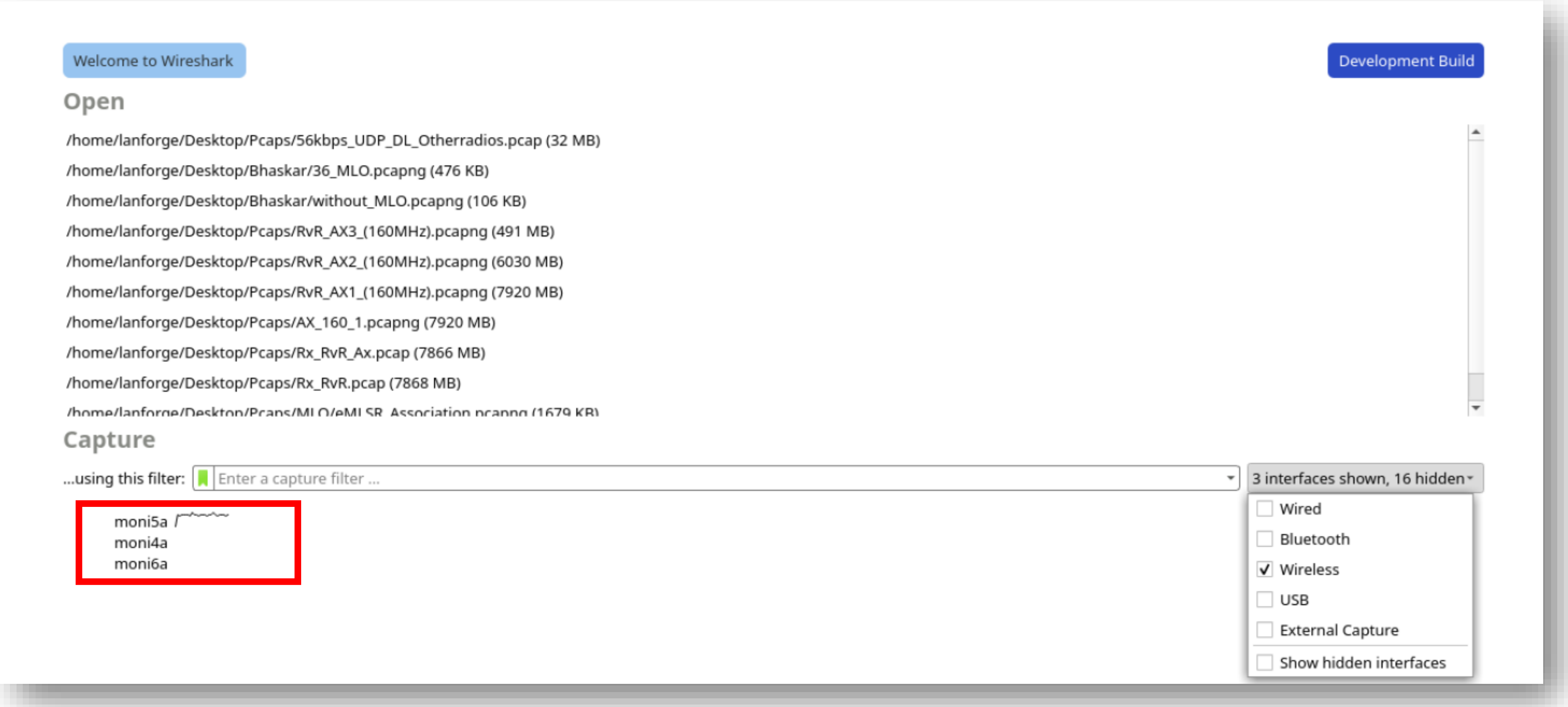
☐ VRF

All Ethernet Interfaces (Ports) for all Resources.

Port	Ø	↕	IP	Alias	Parent Dev	TX-Rate	RX-Rate	Channel	Mode	Signal	Chain RSSI	BSS Color	AID	Device	Gateway IP	MAC
1.1.00			192.168.200.160	eth0		100 Mbps	100 Mbps							eth0	192.168.20...	00:60:e0:8c:6e:b6
1.1.01		✔	0.0.0.0	eth1		0 bps	0 bps							eth1	0.0.0.0	00:60:e0:8c:6e:b7
1.1.02		✔	0.0.0.0	eth2		0 bps	0 bps							eth2	0.0.0.0	9c:69:b4:63:72:82
1.1.03			192.168.50.72	eth3		10 Gbps	10 Gbps							eth3	192.168.50.1	9c:69:b4:63:72:83
1.1.04			0.0.0.0	wiphy0			0 bps	1	802.11abgn-BE			0	0	wiphy0	0.0.0.0	e4:60:17:65:da:d3
1.1.05			0.0.0.0	wiphy1			0 bps	36	802.11abgn-BE			0	0	wiphy1	0.0.0.0	e4:60:17:65:dc:b8
1.1.06			0.0.0.0	wiphy2			0 bps	259	802.11abgn-BE			0	0	wiphy2	0.0.0.0	e4:60:17:64:f8:3e
1.1.07			0.0.0.0	wiphy3			0 bps	-1	802.11abgn-BE			0	0	wiphy3	0.0.0.0	e4:60:17:64:f6:ef
1.1.08			0.0.0.0	wiphy4			0 bps	-1	802.11abgn-BE			0	0	wiphy4	0.0.0.0	e4:60:17:65:dc:c2
1.1.09			0.0.0.0	wiphy5			0 bps	-1	802.11abgn-BE			0	0	wiphy5	0.0.0.0	e4:60:17:65:dd:58
1.1.11			0.0.0.0	moni4a	wiphy0	0 Mbps	0 bps	1	AUTO 20	0 dBm		0	0	moni4a	0.0.0.0	00:00:00:00:00:00
1.1.12			0.0.0.0	moni5a	wiphy1	0 Mbps	0 bps	36	AUTO 20	0 dBm		0	0	moni5a	0.0.0.0	00:00:00:00:00:00
1.1.13			0.0.0.0	moni6a	wiphy2	0 Mbps	0 bps	1	AUTO 20	0 dBm		0	0	moni6a	0.0.0.0	00:00:00:00:00:00

We have created 3 different monitor interfaces on the different radios and using these monitor interfaces we can sniff on multiple-links.

Multi-band Sniffing:



Open

/home/lanforge/Desktop/Pcaps/56kbps_UDP_DL_Otherradios.pcap (32 MB)
/home/lanforge/Desktop/Bhaskar/36_MLO.pcapng (476 KB)
/home/lanforge/Desktop/Bhaskar/without_MLO.pcapng (106 KB)
/home/lanforge/Desktop/Pcaps/RvR_AX3_(160MHz).pcapng (491 MB)
/home/lanforge/Desktop/Pcaps/RvR_AX2_(160MHz).pcapng (6030 MB)
/home/lanforge/Desktop/Pcaps/RvR_AX1_(160MHz).pcapng (7920 MB)
/home/lanforge/Desktop/Pcaps/AX_160_1.pcapng (7920 MB)
/home/lanforge/Desktop/Pcaps/Rx_RvR_Ax.pcap (7866 MB)
/home/lanforge/Desktop/Pcaps/Rx_RvR.pcap (7868 MB)
/home/lanforge/Desktop/Pcaps/MLO/eMLSR_Association.pcapng (1679 KB)

Capture

...using this filter: Enter a capture filter ...

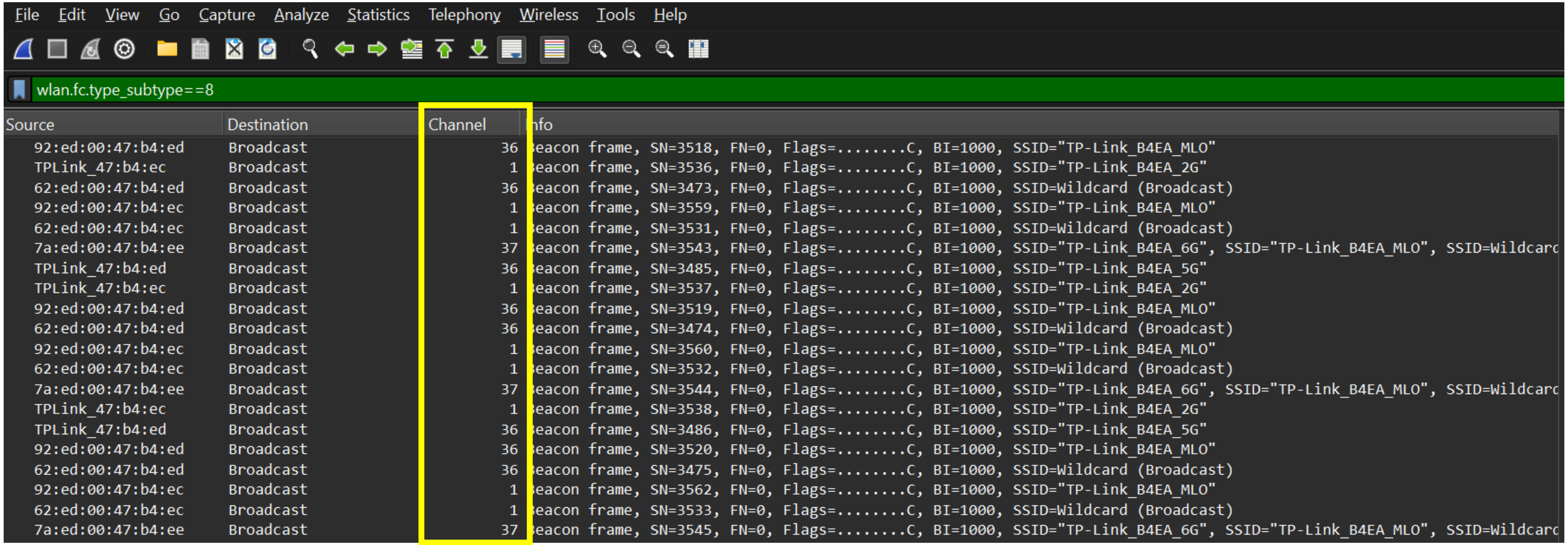
3 interfaces shown, 16 hidden

moni5a
moni4a
moni6a

- ☐ Wired
- ☐ Bluetooth
- ☑ Wireless
- ☐ USB
- ☐ External Capture
- ☐ Show hidden interfaces

- Now open terminal and login for the root.
- Open Wireshark and you can see lot of interfaces available for you to sniff.
- In the wireless interface available multi-select on all the monitor interfaces which we have created earlier.

Multi-band Sniffing:



wlan.fc.type_subtype==8

```
Source               Destination           Channel  Info
   92:ed:00:47:b4:ed    Broadcast                 36  Beacon frame, SN=3518, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_MLO"
   TPLink_47:b4:ec      Broadcast                  1  Beacon frame, SN=3536, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_2G"
   62:ed:00:47:b4:ed    Broadcast                 36  Beacon frame, SN=3473, FN=0, Flags=........C, BI=1000, SSID=Wildcard (Broadcast)
   92:ed:00:47:b4:ec    Broadcast                  1  Beacon frame, SN=3559, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_MLO"
   62:ed:00:47:b4:ec    Broadcast                  1  Beacon frame, SN=3531, FN=0, Flags=........C, BI=1000, SSID=Wildcard (Broadcast)
   7a:ed:00:47:b4:ee    Broadcast                 37  Beacon frame, SN=3543, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_6G", SSID="TP-Link_B4EA_MLO", SSID=Wildcarc
   TPLink_47:b4:ed      Broadcast                 36  Beacon frame, SN=3485, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_5G"
   TPLink_47:b4:ec      Broadcast                  1  Beacon frame, SN=3537, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_2G"
   92:ed:00:47:b4:ed    Broadcast                 36  Beacon frame, SN=3519, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_MLO"
   62:ed:00:47:b4:ed    Broadcast                 36  Beacon frame, SN=3474, FN=0, Flags=........C, BI=1000, SSID=Wildcard (Broadcast)
   92:ed:00:47:b4:ec    Broadcast                  1  Beacon frame, SN=3560, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_MLO"
   62:ed:00:47:b4:ec    Broadcast                  1  Beacon frame, SN=3532, FN=0, Flags=........C, BI=1000, SSID=Wildcard (Broadcast)
   7a:ed:00:47:b4:ee    Broadcast                 37  Beacon frame, SN=3544, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_6G", SSID="TP-Link_B4EA_MLO", SSID=Wildcarc
   TPLink_47:b4:ec      Broadcast                  1  Beacon frame, SN=3538, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_2G"
   TPLink_47:b4:ed      Broadcast                 36  Beacon frame, SN=3486, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_5G"
   92:ed:00:47:b4:ed    Broadcast                 36  Beacon frame, SN=3520, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_MLO"
   62:ed:00:47:b4:ed    Broadcast                 36  Beacon frame, SN=3475, FN=0, Flags=........C, BI=1000, SSID=Wildcard (Broadcast)
   92:ed:00:47:b4:ec    Broadcast                  1  Beacon frame, SN=3562, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_MLO"
   62:ed:00:47:b4:ec    Broadcast                  1  Beacon frame, SN=3533, FN=0, Flags=........C, BI=1000, SSID=Wildcard (Broadcast)
   7a:ed:00:47:b4:ee    Broadcast                 37  Beacon frame, SN=3545, FN=0, Flags=........C, BI=1000, SSID="TP-Link_B4EA_6G", SSID="TP-Link_B4EA_MLO", SSID=Wildcarc
```

- Now we can clearly see the beacons coming from various AP bands and this is how do Multi-band sniffing using LANforge box.
- Using this we can validate various kinds of Multi-link testcases.