sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

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:

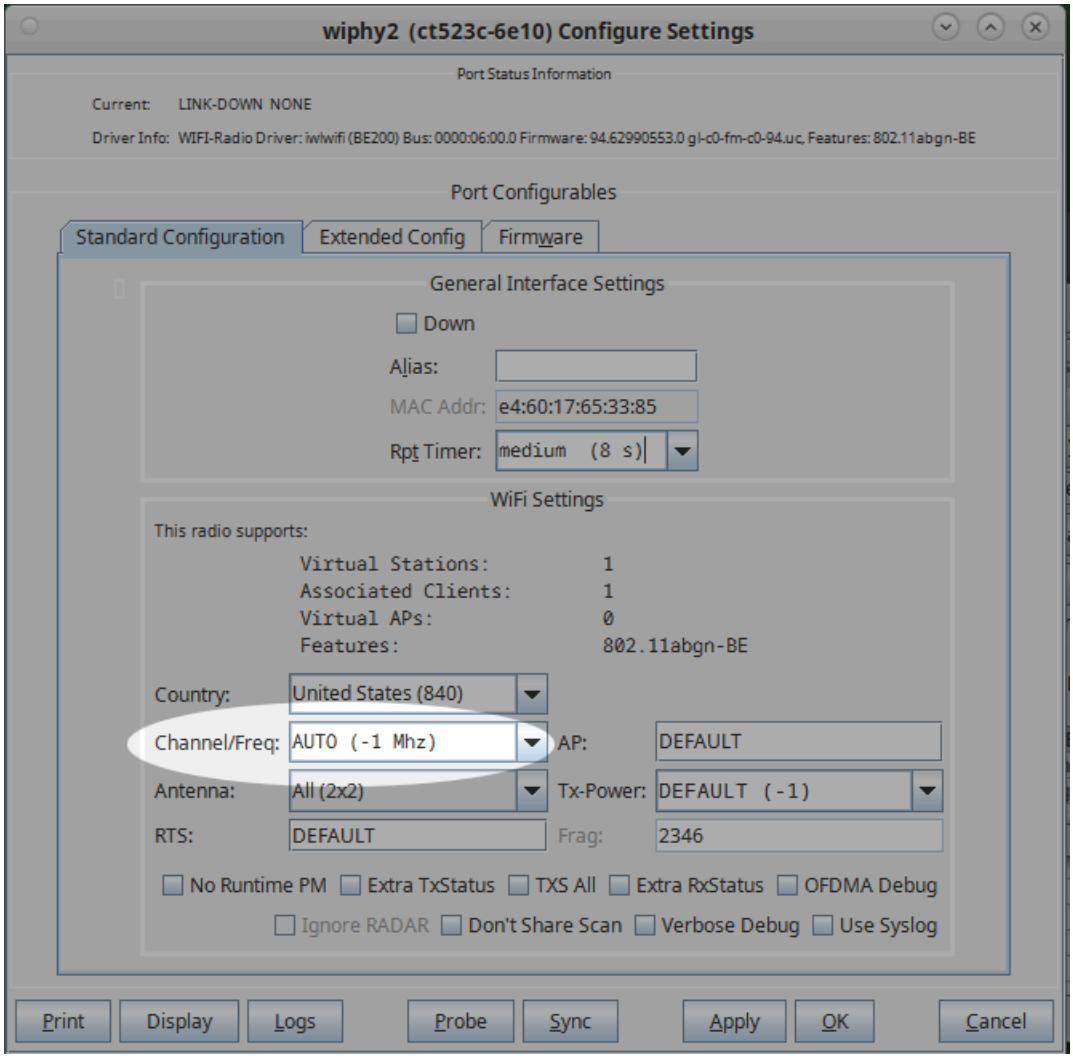
- **6GHz APs must use WPA3 or OWE**
  - Decrypting WPA3 network traffic is possible with Wireshark but requires additional steps compared to WPA/WPA2 traffic decryption
- **6GHz APs must use PMF (protected management frames)**
  - Remember: the data portion of all PMFs after 4-way handshake are*encrypted*
  - 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

i 6GHz WiFi packet capture only relevant for tri-band radios, including the **Intel AX210/BE200** and the **MTK 7922, 7925, and 7996** radios.

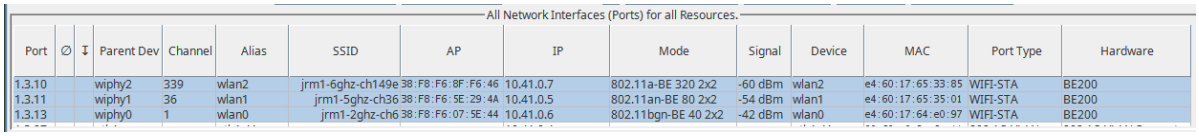
Manual Setup (w/ LANforge GUI)

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*.

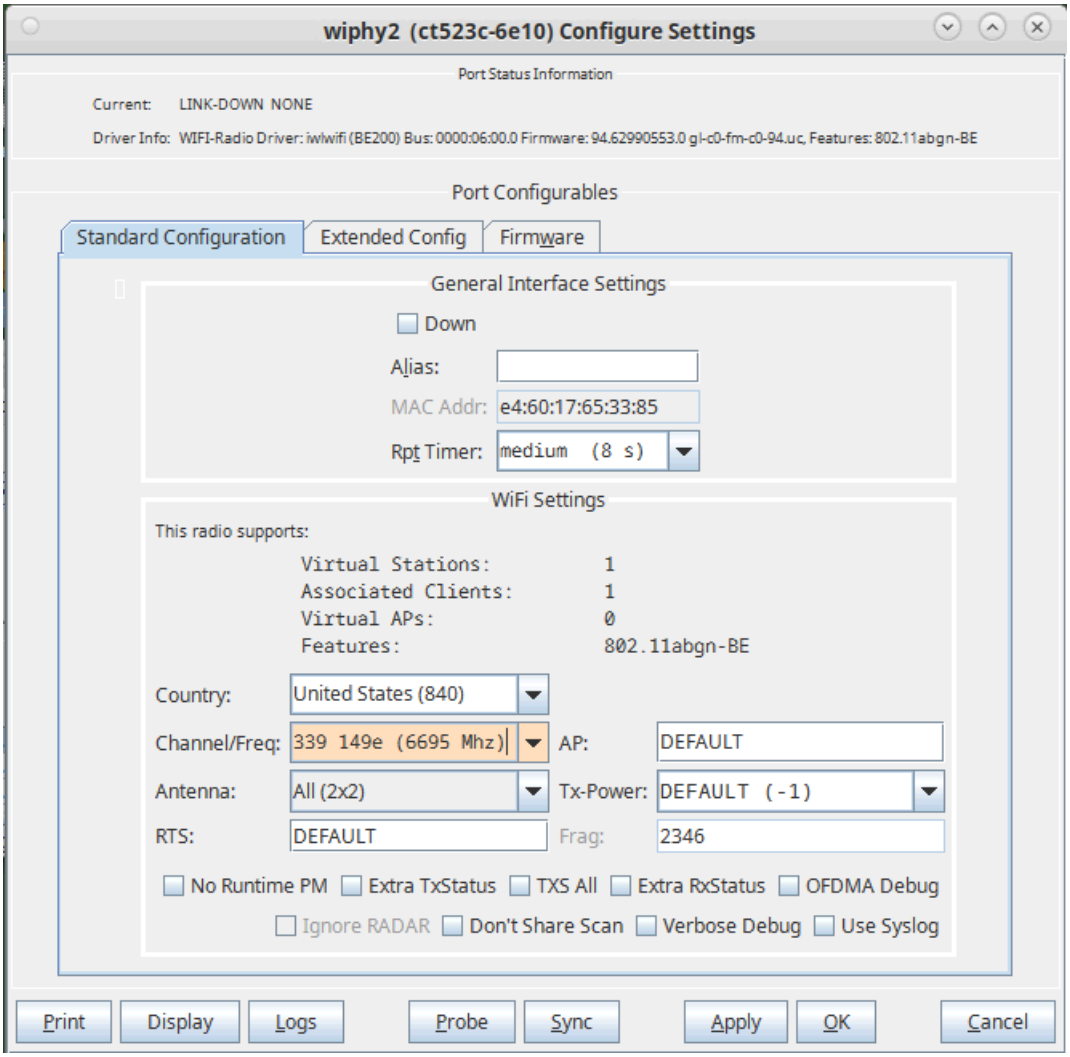


2. Either create a station or use an existing station on the monitor radio and associate it to an AP. Ensure that it obtains an IP address.

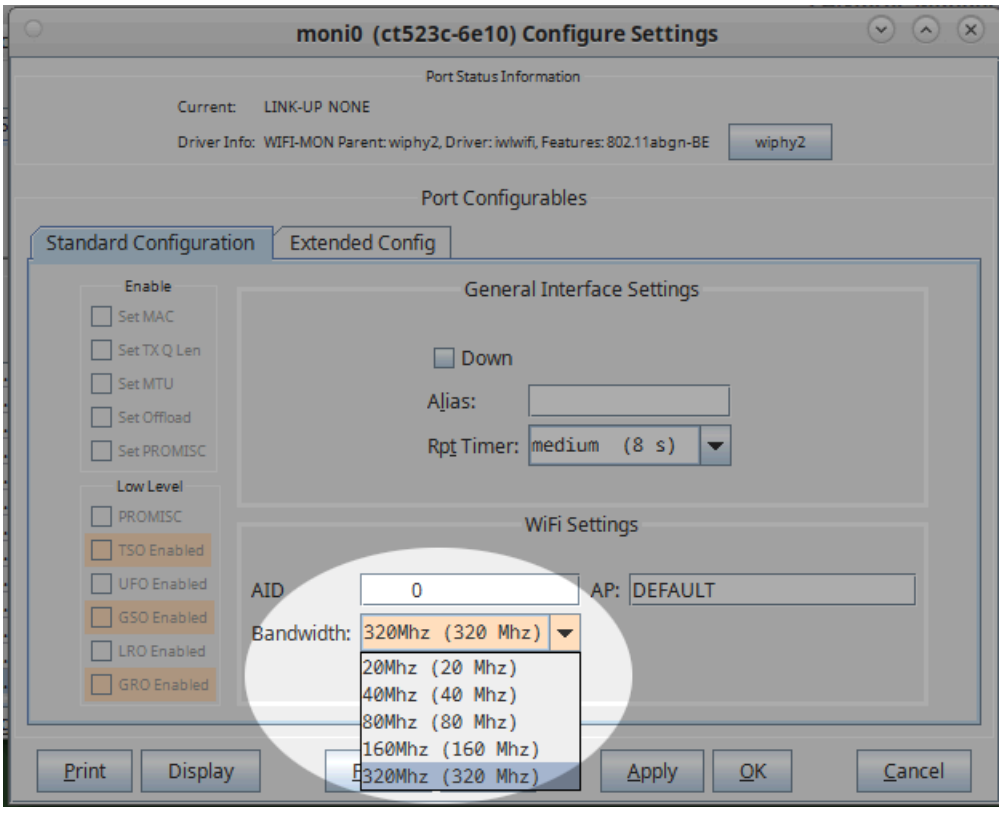


> ⚠ The ability to create a station validates that the parent radio is free to transmit on the 6ghz spectrum. If the radio refuses to associate a station, then there might be a mixture of regulatory domains being broadcast, or the channel is not a PSC channel.

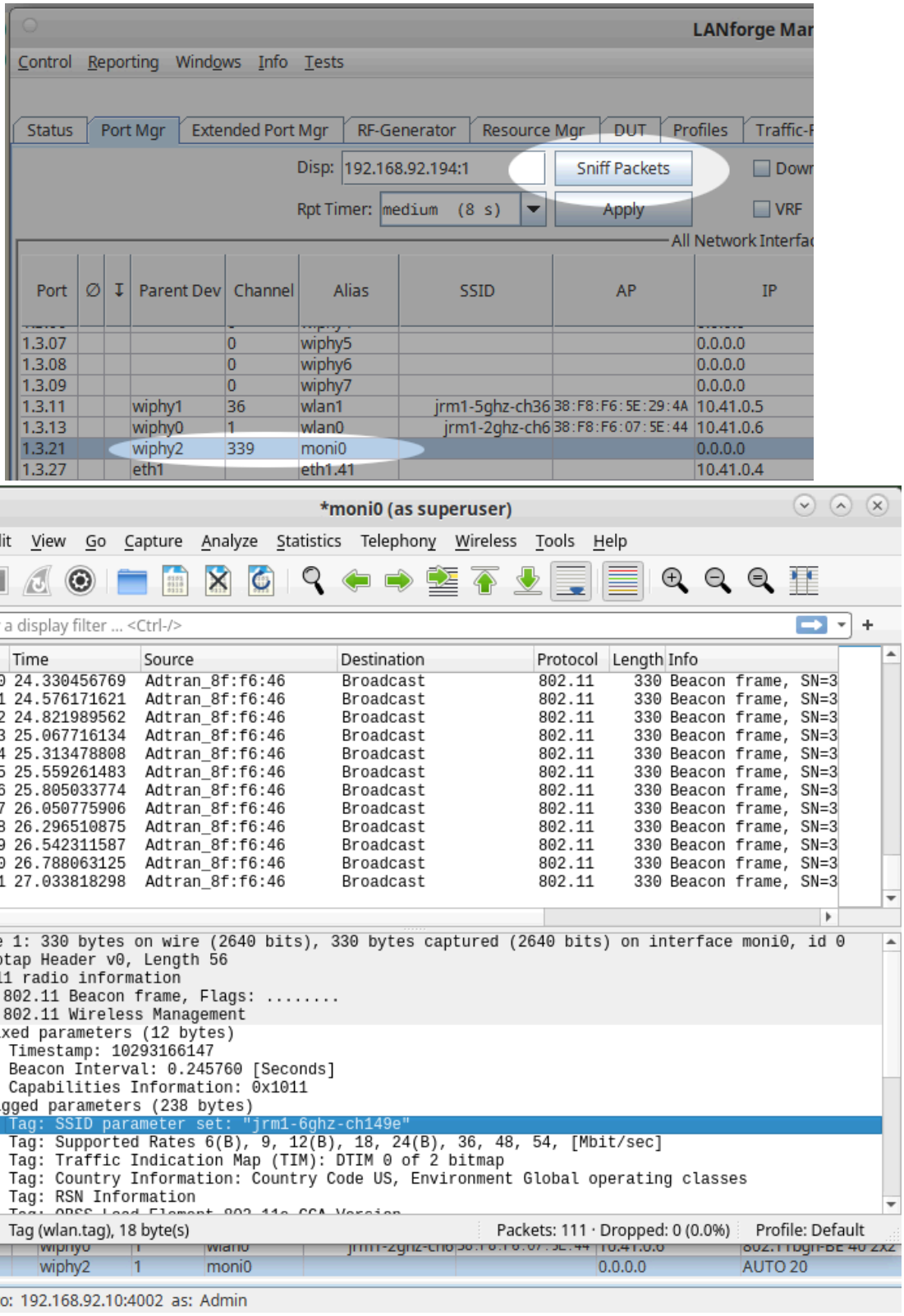
3. Admin-down the station if it is on the monitor radio.
   (Select the station and click the Down button [↧] or Alt + S)
4. Set the *monitor radio's* channel to the channel you want to sniff.



5. Set the monitor to the desired bandwidth.



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

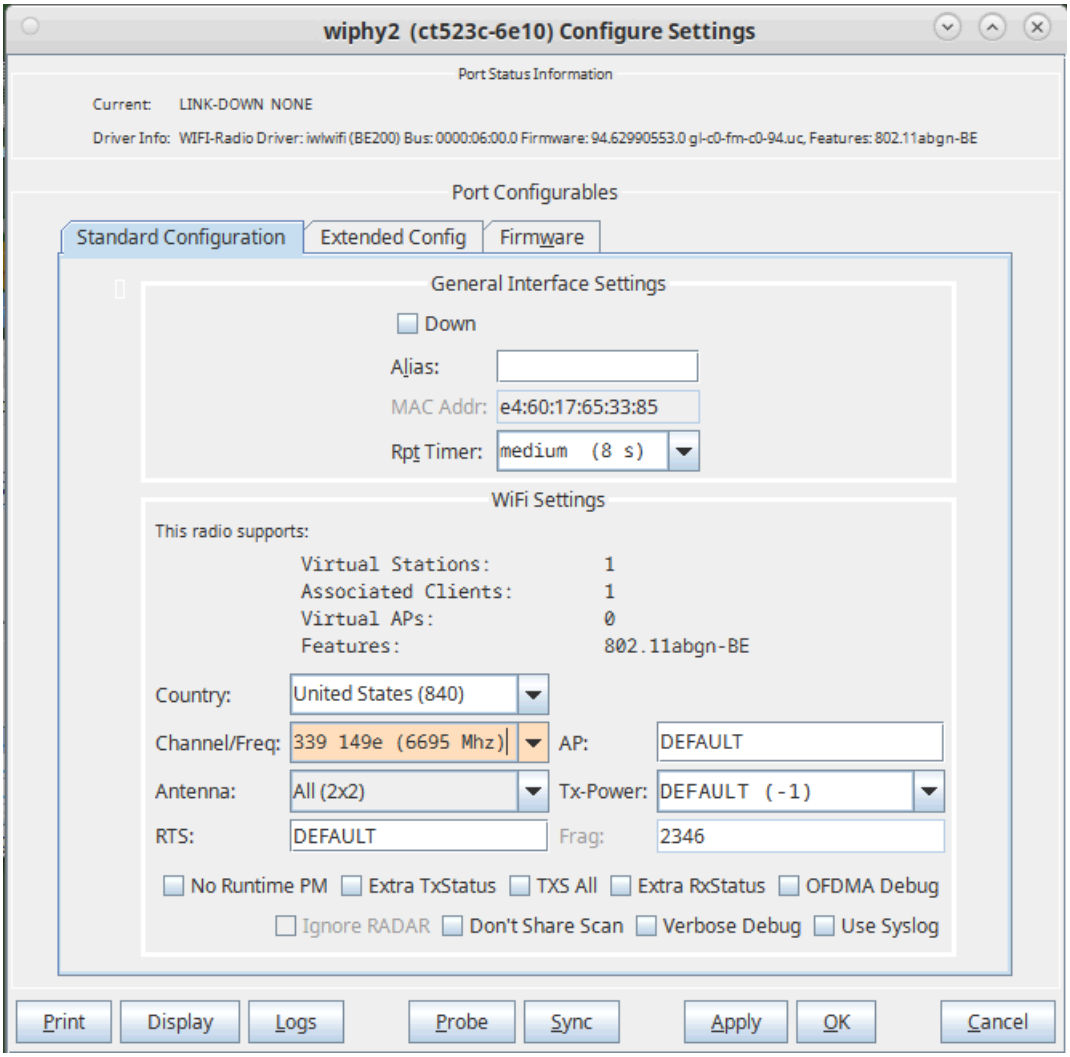


Simultaneous Sniffing

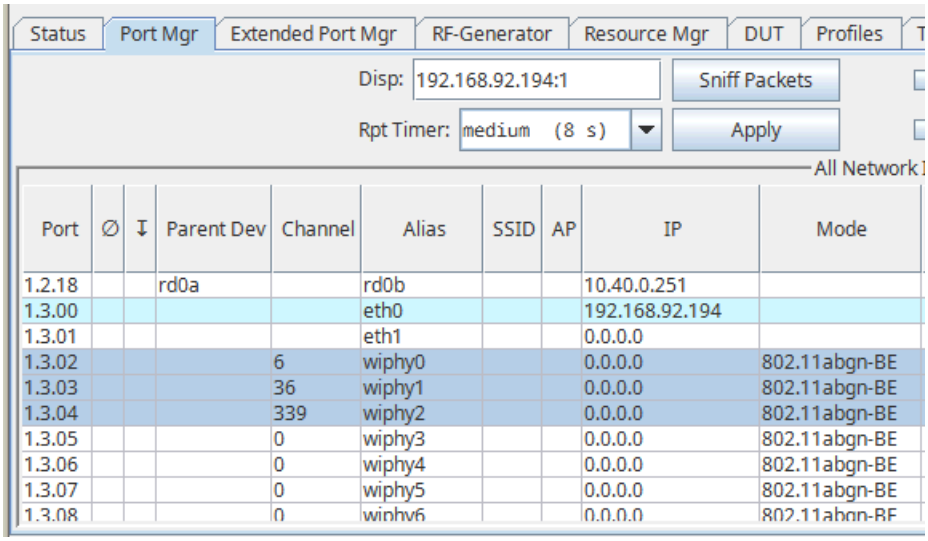
Plenty of situations would require sniffing from multiple monitors at the same time. This can be done using the GUI or with some basic shell scripting.

Using the LANforge GUI

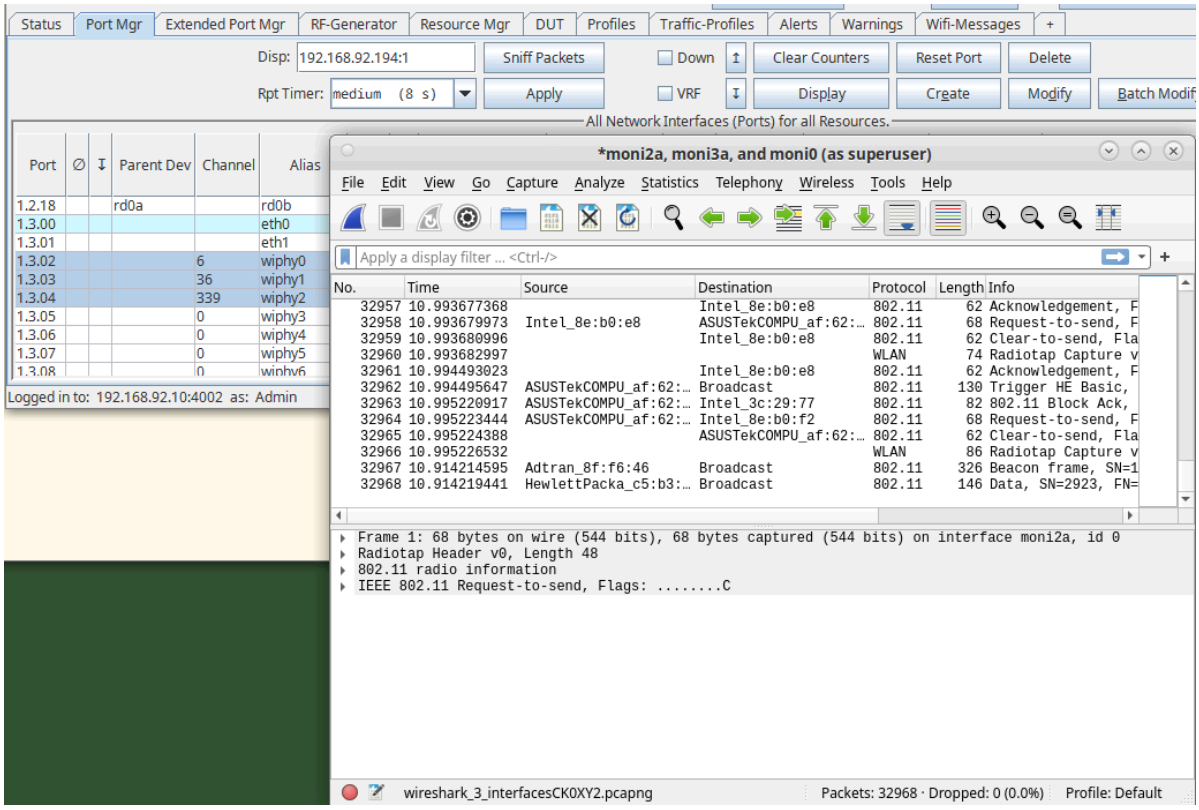
1. Set the center channel for each of the radios you want to sniff from.



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

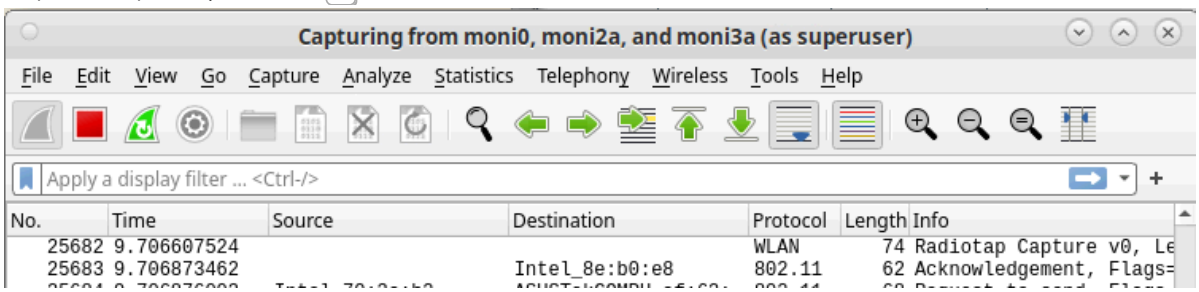


3. Then click **Sniff Packets** and the LANforge server will create multiple monitor interfaces, then one (or more) Wireshark instances will appear sniffing traffic.

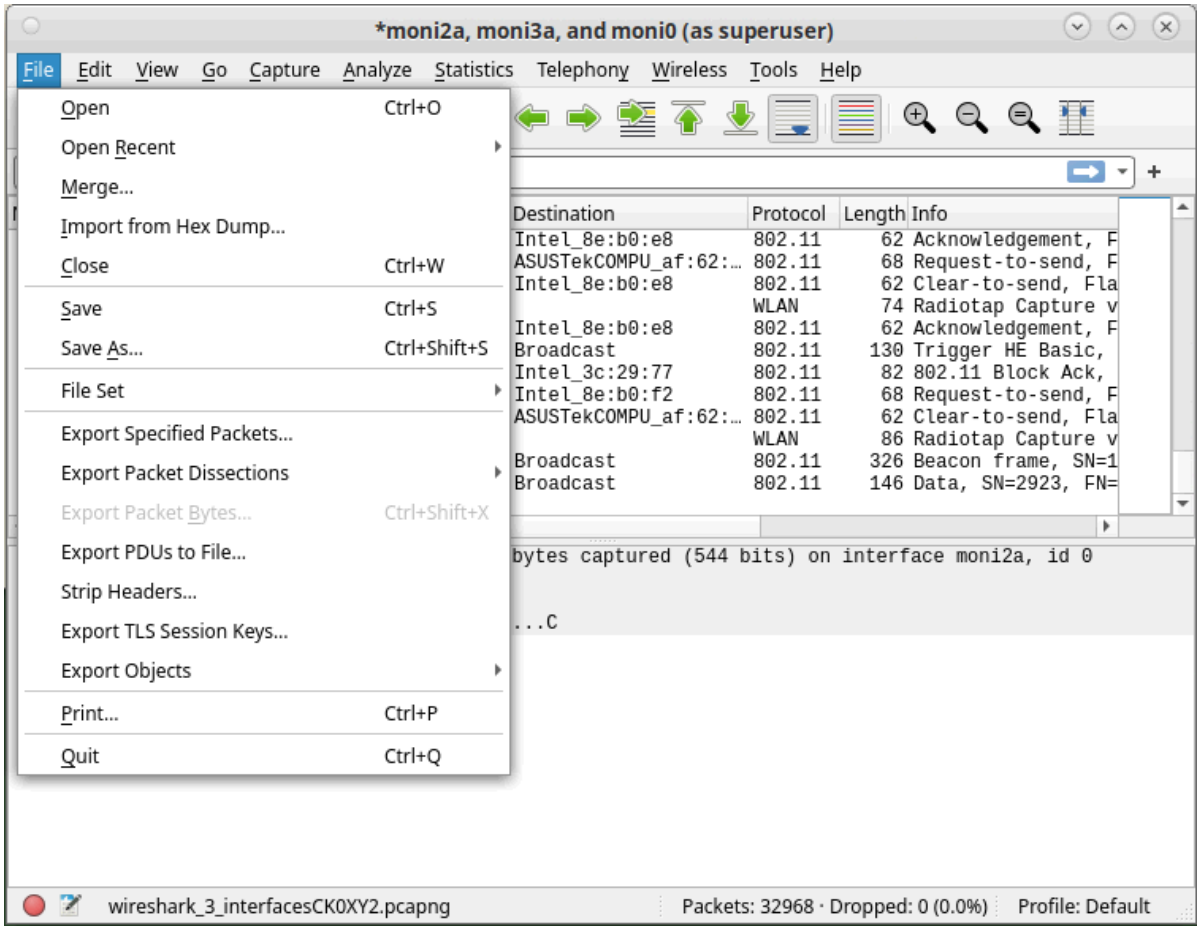


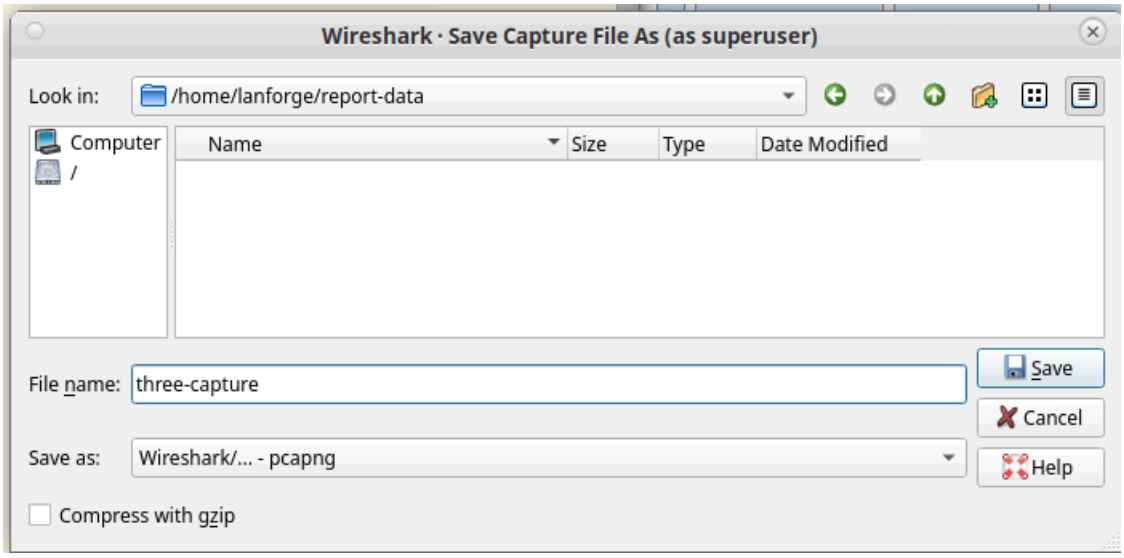
Saving and Finding the Capture

1. Stop the capture (click the ■ button.



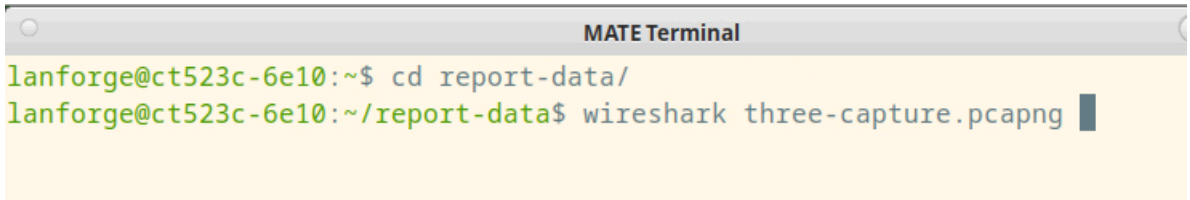
2. Save the capture(s) to files.





3. To view the capture later, use the command:

```
$ wireshark <filename>
```



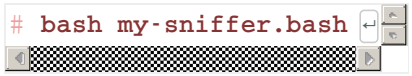
Using the _lf_sniff*radio.py* Script

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.

```
#!/bin/bash
cd /home/lanforge/scripts/py-scripts
./lf_sniff_radio.py --radio wiphy0 \
    --outfile /home/lanforge/report-data/2ghz.pcap \
    --duration 60 \
    --channel 6 \
    --channel_bw 40 \
    --radio_mode AUTO \
    --monitor_name moni0 &

./lf_sniff_radio.py --radio wiphy1 \
    --outfile /home/lanforge/report-data/5ghz.pcap \
    --duration 60 \
    --channel 36 \
    --channel_bw 80 \
    --radio_mode AUTO \
    --monitor_name moni1 &

./lf_sniff_radio.py --radio wiphy2 \
    --outfile /home/lanforge/report-data/6ghz.pcap \
    --duration 60 \
    --channel 339 \
    --channel_bw 360 \
    --radio_mode AUTO \
    --monitor_name moni2 &

wait
echo "done."
```

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:
  - `su -`
  - `cd /home/lanforge`
  - `. lanforge.profile` (note there is a space between the first `.` and `lanforge`)
  - `iw dev moni1a info` (using the interface number noted previously)
  - `iw dev moni1a set freq` [*6E channel frequency which is 6455*]
  - `iw dev moni1a 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 moni10a set freq 5975 80 5985`
- `iw dev moni10a set freq 5995 80 5985`
- `iw dev moni10a set freq 6015 80 5985`

The *iw* command syntax

```
iw dev moni10a 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 moni1a info` Enter
          (replace *moni1a* with your monitor interface)
        - `iw dev moni1a set freq <control-freq> <channel-width> <center-frequency>` Enter
        - `iw dev moni1a info` Enter
          (checking that the 6E frequency was set)
    6. Restart the wireshark capture and observe captured frames on the 6ghz band.