

6GHz Packet Capture

Goal: 6GHz Packet Capture Using LANforge Radios in Monitor Mode.

Depending on the NIC, there are different steps required in order to capture on 6GHz frequencies.

Intel AX210/BE200 - Require a station on the parent interface to scan and determine that it is in a US regulatory domain before a monitor mode interface can be assigned a 6GHz frequency.

Mediatek 7921/7922 - No regulatory domain restriction at this time.

1. Clone and get latest copy of lanforge-scripts.

- A. `cd /home/lanforge`
- B. `git clone https://github.com/greearb/lanforge-scripts`
- C. `cd /home/lanforge/lanforge-scripts/py-scripts`

2. Run `lf_sniff_radio.py` script.

- A. Run the `lf_sniff_radio.py` script with the `--help` argument to understand your options or `pip install` any missing modules as needed.

```
[root@ibase-i5-f36 py-scripts]# ./lf_sniff_radio.py --help
usage: ./lf_sniff_radio.py
       --mgr localhost
       --mgr_port 8080
       --radio wiphy0
       --outfile /home/lanforge/test_sniff.pcap
       --duration 1
       --channel 36
       --channel_bw 40
       --center_freq 5190
       --radio_mode AUTO
       --monitor_name Sniffer0

AX210 sniff command
=====

./lf_sniff_radio.py
--mgr 192.168.0.104
--mgr_port 8080
--radio wiphy7
--outfile /home/lanforge/sniff_6G_80.pcap
--duration 20
/--channel 1e
--channel_bw 80
--channel_freq 5955
--center_freq 5985
--radio_mode AUTO
--monitor_name SNIFF_6G_80
```

- B. Run the script with arguments for your test case.

To sniff on 6GHz with an AX210 NIC on resource 1, wiphy2:

```
./lf_sniff_radio.py --mgr 192.168.101.197 --radio "1.wiphy2" \
--outfile sniff_6G-AX210.pcapng --duration 10 --channel 37e --ax210 \
--num_stations 1 --ssid test --ax210_scan_time 20
```

To sniff on 6GHz with an MTK7921/MTK7922 NIC on resource 6, wiphy0:

```
./lf_sniff_radio.py --mgr 192.168.100.193 --radio "6.wiphy0" \
--outfile sniff_6G-MTK.pcapng --duration 10 --channel 133e
```

- C. For more information, see this guide: [sniffer_manual.pdf](#)