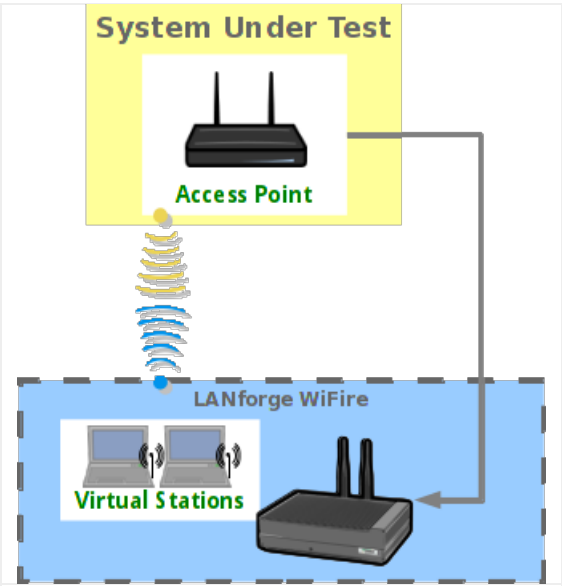
sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

Using LANforge python script to do packet captures then analyze to determine if the traffic was OFDMA, MU-MIMO or Single User

Goal: Sniff wireless traffic to/from LANforge stations using additional LANforge Radios in monitor mode. This script automates creating WiFi monitor devices correctly configured for the station's channel, and in the case of OFDMA, the AID and BSSID will also be configured in the sniffing radio. The OFDMA vs MU-MIMO analysis is performed by the wifi diagnostics script. Both of these scripts require LANforge 5.4.2 or higher and an appropriate set of WiFi radios.



1. Create and configure stations to talk to your DUT. You may create these through Chamber View scenarios or other methods. Please refer to introductory cookbooks for more information on this if you have questions.

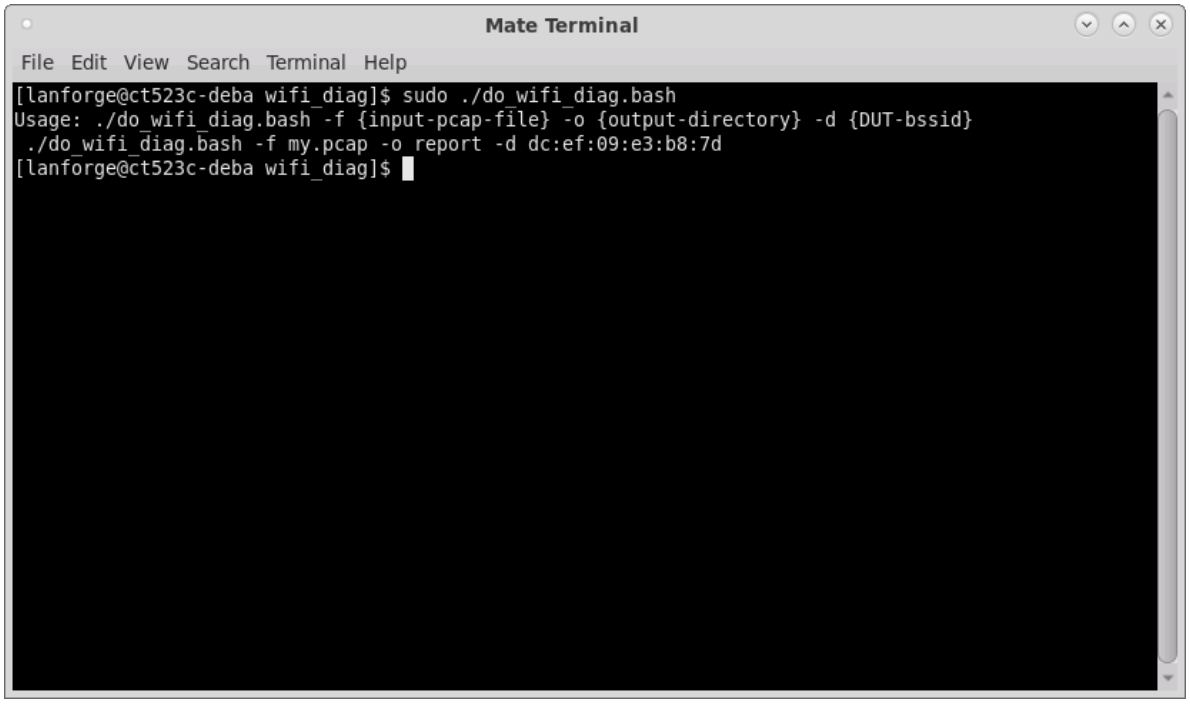
2. Run lf_sniff.py script.
   A. Change directory to the /home/lanforge/scripts directory (or other location if you have installed scripts elsewhere), and run the lf_sniff.py script with the --help argument to understand your options..

   B. Run the script with arguments for your test case. The basic idea is to provide a list of stations you wish to sniff, and a list of matching radios that you wish to use as sniffers. The script will query the station to find the channel, AID and BSSID and will then create WiFi monitor devices on the sniffer radios. A command-line packet capture tool will then be started and write the captured packets to disk for the requested duration. When the duration is complete, the packet capture process will exit. You can then post-process the packet captures, open them with wireshark, etc.
   Examples
   Sniff sta00000 on LANforge resource 1 using radio wiphy0 on LANforge resource 2 for 15 seconds:

```
./lf_sniff.py --lfmgr 192.168.100.238 --station "1.sta00000" \
--sniffer_radios "2.wiphy0" --duration 0.25
```

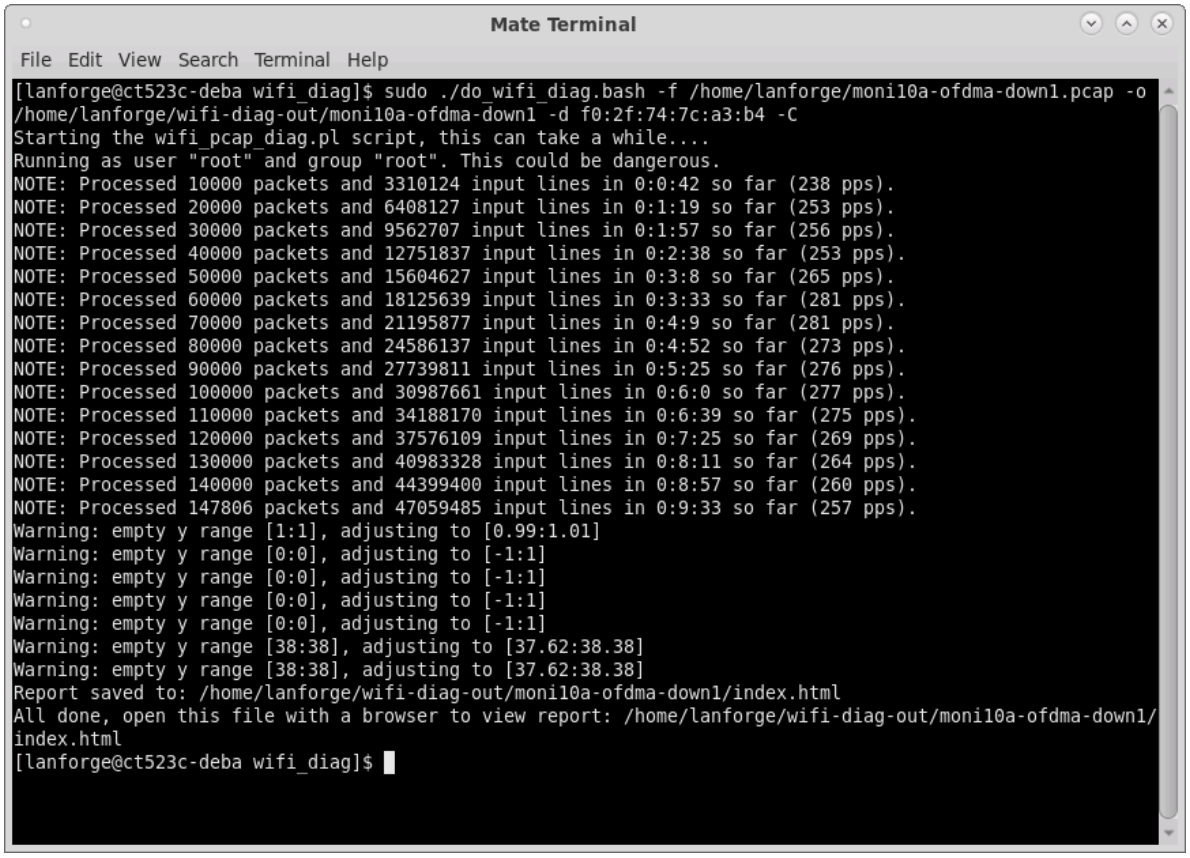
3. Run do_wifi_diag.bash script.

A. Change directory to the /home/lanforge/scripts/wifi_diag directory, and run the bash script without any arguments to view the usage help.



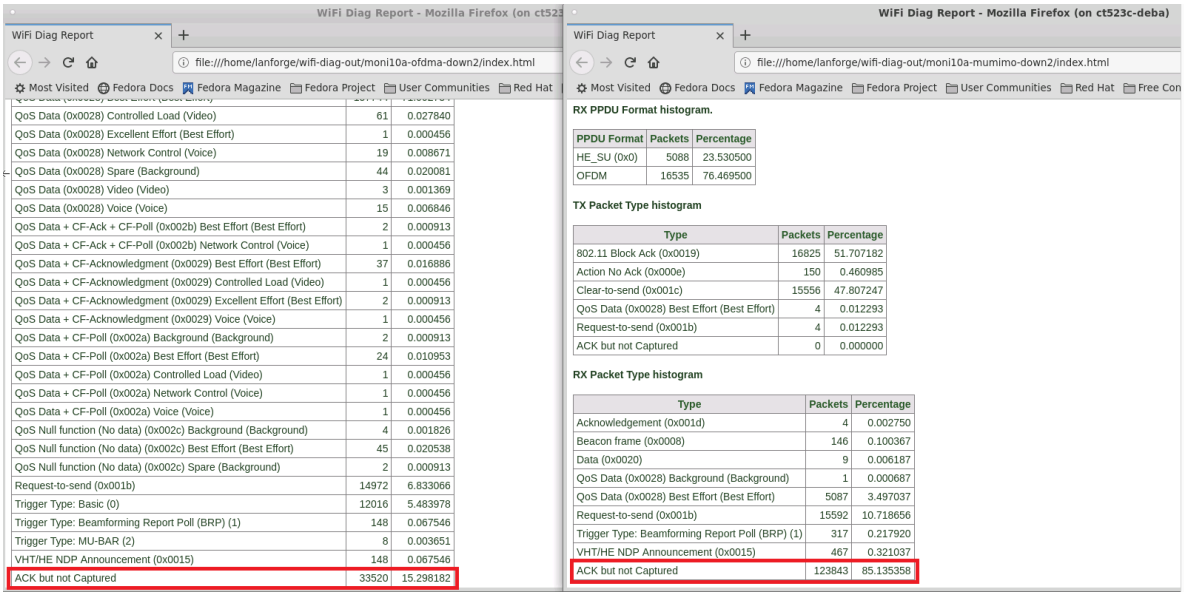
B. Run the bash script with correct location of the pcap file obtained with lf_sniff.py and with the correct BSSID of the AP used as the DUT. Depending on your system processing power and the pcap file size, the wifi diag script will take some time to complete.

C. When the wifi diag script is complete, you can open the index.html file to view the results.



4. Interpreting the report for OFDMA or MU-MIMO operation.

A. To determine if the packet capture contains OFDMA or MU-MIMO operation, scroll down in the report to the table labeled "RX Packet Type Histogram" and the element "ACK but not captured" which is a count of the number of Block ACKs captured without capturing the corresponding Data frames. If the report shows a large percentage of "ACK but not captured", this indicates MU-MIMO operation because the data frames are not able to be captured. If there is a lower percentage, than the traffic is likely OFDMA.



QoS Data (0x0028) Controlled Load (Video)	61	0.027840
QoS Data (0x0028) Excellent Effort (Best Effort)	1	0.000456
QoS Data (0x0028) Network Control (Voice)	19	0.008671
QoS Data (0x0028) Spare (Background)	44	0.020081
QoS Data (0x0028) Video (Video)	3	0.001369
QoS Data (0x0028) Voice (Voice)	15	0.006846
QoS Data + CF-Ack + CF-Poll (0x002b) Best Effort (Best Effort)	2	0.000913
QoS Data + CF-Ack + CF-Poll (0x002b) Network Control (Voice)	1	0.000456
QoS Data + CF-Acknowledgment (0x0029) Best Effort (Best Effort)	37	0.016886
QoS Data + CF-Acknowledgment (0x0029) Controlled Load (Video)	1	0.000456
QoS Data + CF-Acknowledgment (0x0029) Excellent Effort (Best Effort)	2	0.000913
QoS Data + CF-Acknowledgment (0x0029) Voice (Voice)	1	0.000456
QoS Data + CF-Poll (0x002a) Background (Background)	2	0.000913
QoS Data + CF-Poll (0x002a) Best Effort (Best Effort)	24	0.010953
QoS Data + CF-Poll (0x002a) Controlled Load (Video)	1	0.000456
QoS Data + CF-Poll (0x002a) Network Control (Voice)	1	0.000456
QoS Data + CF-Poll (0x002a) Voice (Voice)	1	0.000456
QoS Null function (No data) (0x002c) Background (Background)	4	0.001826
QoS Null function (No data) (0x002c) Best Effort (Best Effort)	45	0.020538
QoS Null function (No data) (0x002c) Spare (Background)	2	0.000913
Request-to-send (0x001b)	14972	6.833066
Trigger Type: Basic (0)	12016	5.483978
Trigger Type: Beamforming Report Poll (BRP) (1)	148	0.067546
Trigger Type: MU-BAR (2)	8	0.003651
VHT/HE NDP Announcement (0x0015)	148	0.067546
ACK but not Captured	33520	15.298182

RX PPDU Format histogram.

PPDU Format	Packets	Percentage
HE_SU (0x0)	5088	23.530500
OFDM	16535	76.469500

TX Packet Type histogram

Type	Packets	Percentage
802.11 Block Ack (0x0019)	16825	51.707182
Action No Ack (0x000e)	150	0.460985
Clear-to-send (0x001c)	15556	47.807247
QoS Data (0x0028) Best Effort (Best Effort)	4	0.012293
Request-to-send (0x001b)	4	0.012293
ACK but not Captured	0	0.000000

RX Packet Type histogram

Type	Packets	Percentage
Acknowledgement (0x001d)	4	0.002750
Beacon frame (0x0008)	146	0.100367
Data (0x0020)	9	0.006187
QoS Data (0x0028) Background (Background)	1	0.000687
QoS Data (0x0028) Best Effort (Best Effort)	5087	3.497037
Request-to-send (0x001b)	15592	10.718656
Trigger Type: Beamforming Report Poll (BRP) (1)	317	0.217920
VHT/HE NDP Announcement (0x0015)	467	0.321037
ACK but not Captured	123843	85.135358

B. "ACK but not captured" is also represented in the graph later in the report labeled "RX Dummy Packets".

C. The graph labeled "RX RU Alloc over time" also indicates OFDMA operation because it shows when frames were assigned a Resource Unit allocation which is the main trait of OFDMA operation.