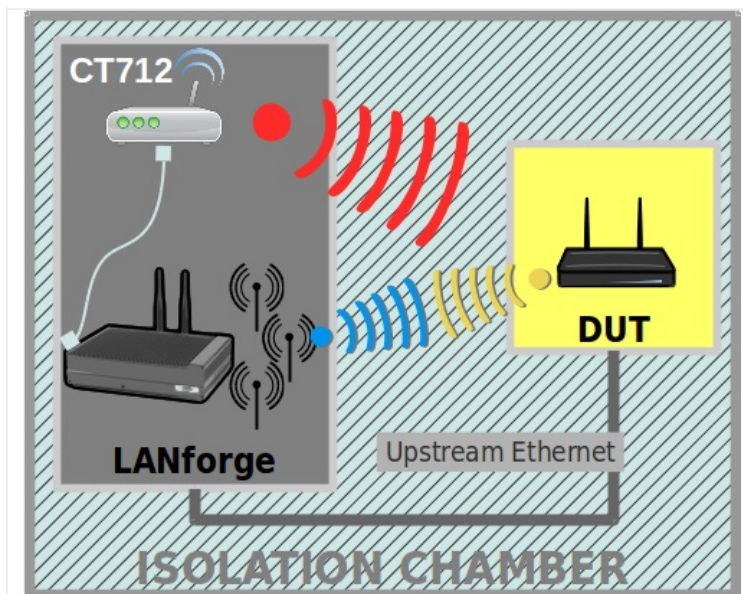


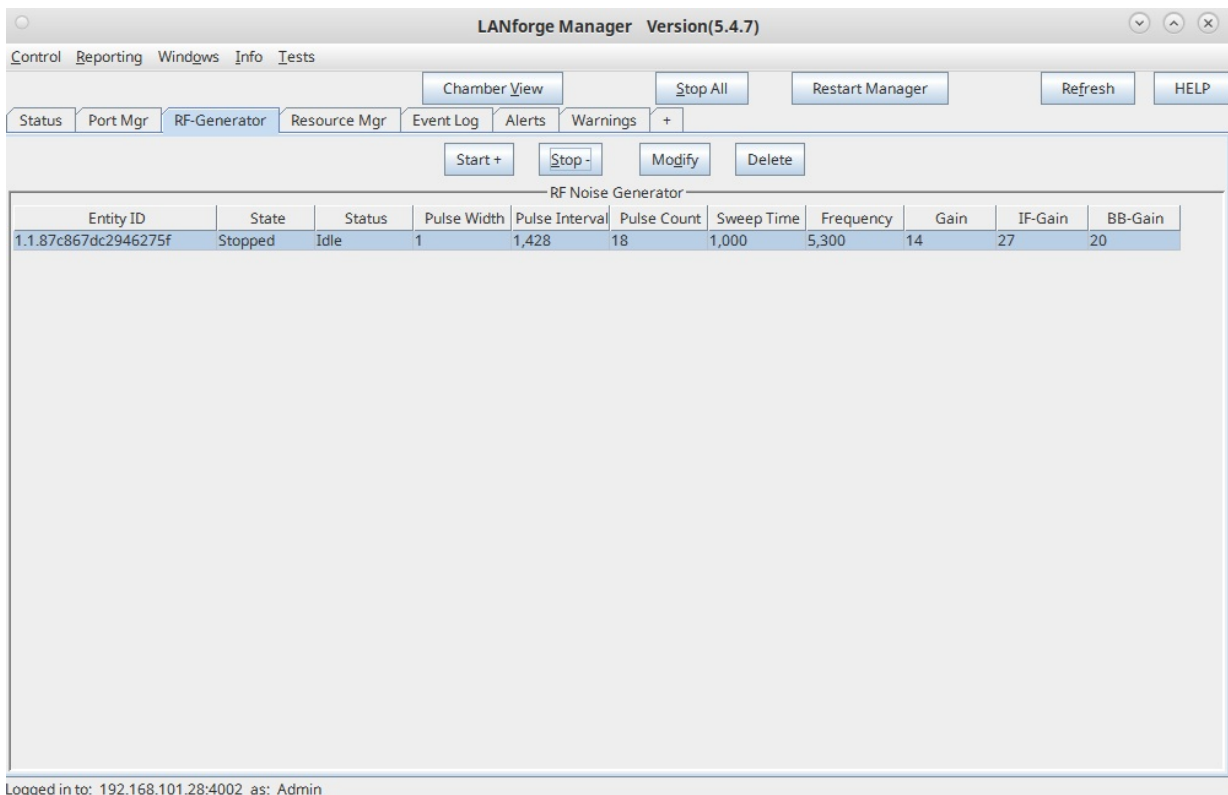
Using CT712 RF Noise Generator and RADAR Simulator to test DFS channels

Goal: Generate RF pulses that simulate RADAR and cause an AP using DFS to exercise its detection and response abilities.

DFS (Dynamic Frequency Selection) allows an AP to use channels in the same spectrum that some RADAR systems use and provide a method of changing channels when RADAR signals are detected. In this example, we will use a LANforge CT712 which is our customized script and integrated GUI control for the HackRF-One Software-Defined Radio (SDR) to generate the RF pulses that simulate RADAR signals and cause a third-party AP under test to detect and change channels. It is recommended that this type of testing be done in a RF isolation chamber to limit interference to production WLAN and RADAR systems in use.



1. Verify a client is connected to a third-party AP using a DFS channel.
For more information see
[Wikipedia: 5GHz Channels](#)
[WLAN Pros WiFi Channel Reference](#)
2. On the RF Generator tab, modify the device that corresponds to the CT712 USB device to set the desired channel and pulse characteristics.
NOTE: The different RADAR types are defined as described in the document [FCC DFS Compliance Procedures](#). RF pulses defined outside of these parameters can be used for other RF noise and interference tests.



3. Select a FCC RADAR type preset button or enter specific values to set the desired pulse characteristics, then set the transmit frequency, then select OK.

Modify RF Generator

Name: 1.1.87c867dc2946275f

Radar Type: FCC0 (0)

Pulse Width: 1us, FCC[0,1,2,6], W[53,56], KOREA[1,2,4], CHINA0 (2)

Pulse Interval: 1428us, FCC0 (1.428 ms)

Pulse Count: 18, FCC[0,3], ETSI4, W[53,56], KOREA1 (18)

Pulse Repetition Frequency 1: 0 (0)

Pulse Repetition Frequency 2: 0 (0)

Pulse Repetition Frequency 3: 0 (0)

Frequency Modulation: 5 (5)

UUT Channel: 20 (20)

Burst Offset: 0 (0 us)

Long Pulse Width: 30us (30 us)

Chirp Width: 0 (0)

☒ One Burst ☐ Trials Low ☐ Trials Center ☐ Trials High

Sweep Time: 1 second (1 s)

Frequency: Channel 60: 5300 (5,300,000)

OFDM Header Modulation: BPSK (0)

OFDM Payload Modulation: BPSK (0)

Time period 1 on: 0us (0 us)

Time period 1 off: 0us (0 us)

Time period 2 on: 0us (0 us)

Time period 2 off: 0us (0 us)

Time period 3 on: 0us (0 us)

Time period 3 off: 0us (0 us)

Duration: 0us (0 us)

Trigger dBm: 0 (0)

Trigger AMP: 0 (0)

Gain: On (+14dB) (14)

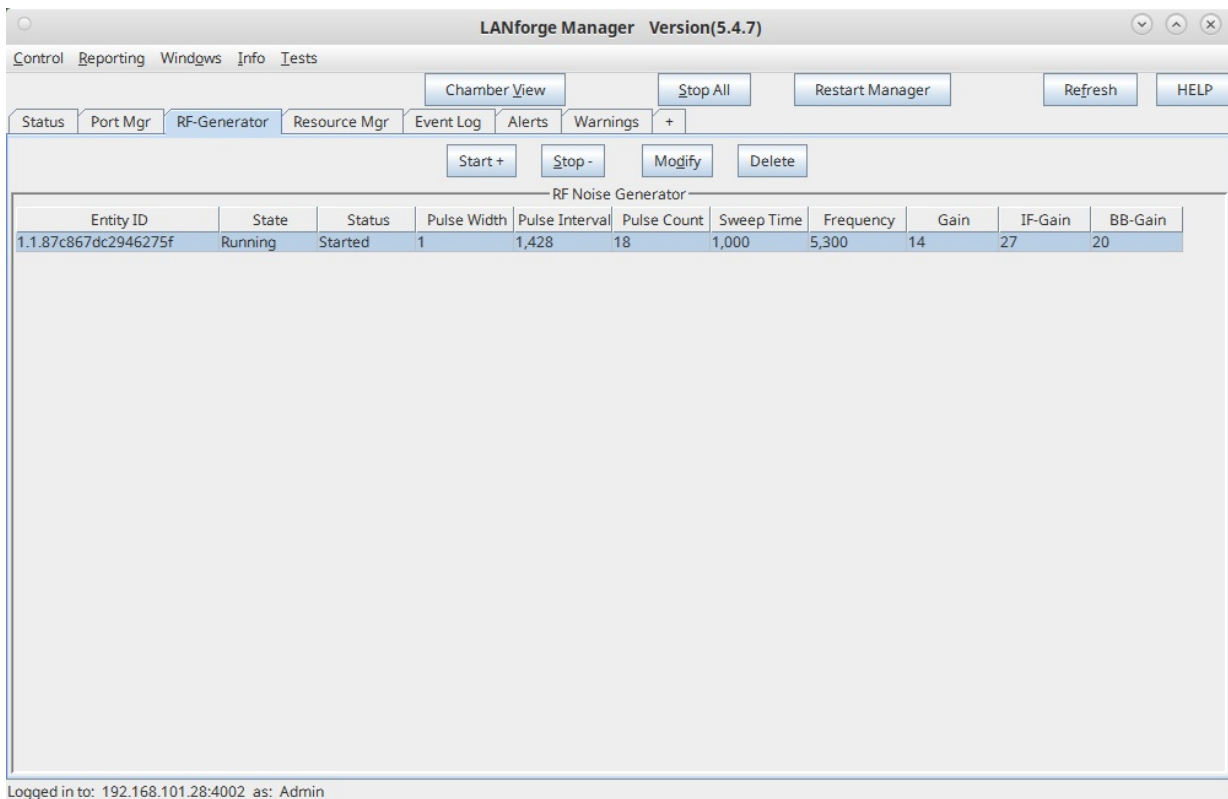
IF-Gain: Medium (27)

BB-Gain: Normal (20)

Sample Rate: DEFAULT

Buttons: Sync, Apply, OK, Cancel

4. Highlight the RF Generator entry and select the Start+ button to start transmitting. In some versions, you may have to select Start+ twice in order to start transmitting



Logged in to: 192.168.101.28:4002 as: Admin

5. When the CT712 is activated, the Status will show Started and the HackRF-One device's TX LED should show a red light. The AP under test should detect RADAR within 10 seconds, change to an available channel and not be able to use the previous channel again for 30 minutes.

For more information see

[WiFi Alliance: DFS Best Practices](#)

6. An alternate method of controlling the CT712 HackRF-One device is to use the lf_hackrf_dfs.py script in the /home/lanforge directory:

- A. Open a terminal window on the LANforge system.

- B. cd to /home/lanforge

- C. To show the script usage, type: ./lf_hackrf_dfs.py --help

```
usage: lf_hackrf_dfs.py [-h] [--lf_hackrf LF_HACKRF] [--pulse_width PULSE_WIDTH]
                        [--pulse_interval PULSE_INTERVAL] [--pulse_count PULSE_COUNT]
                        [--one_burst] [--bursts BURSTS] [--rf_type RF_TYPE]
                        [--uut_channel UUT_CHANNEL] [--sweep_time SWEEP_TIME] [--freq FREQ]
                        [--daemon DAEMON] [--pid_file PID_FILE] [--gain GAIN] [--if_gain IF_GAIN]
                        [--bb_gain BB_GAIN] [--log_level LOG_LEVEL] [--mgt_pipe MGT_PIPE]
                        [--no_repeat] [--sample_mod SAMPLE_MOD]
                        [--host_perf_adjust HOST_PERF_ADJUST] [--tx_sample_rate TX_SAMPLE_RATE]
dfs testing , FCC0-6, ETSI0-6
Note: some systems will need to preface command with sudo nice -19
```

options:

```
-h, --help            show this help message and exit
--lf_hackrf LF_HACKRF
                        --lf_hackrf { last 4 bytes of serial num from hackrf_info }
--pulse_width PULSE_WIDTH
                        --pulse_width { usecs } default: 1
--pulse_interval PULSE_INTERVAL
                        --pulse_interval { usecs } default: 1
--pulse_count PULSE_COUNT
                        --pulse_count { number } default: 1
--one_burst            --one_burst store_true default: False
--bursts BURSTS        --bursts provide a number of bursts
--rf_type RF_TYPE, --radar_type RF_TYPE
                        Note: .lower used so upper case or lower case may be entered.
```