

Diagnostic script for WiFi packet capture files.

Goal: Use a diagnostic script to parse a WiFi packet capture file and generate histograms, packet loss stats, and other helpful information for diagnosing WiFi behaviour.

LANforge will be used to create a WiFi capture file, and then we will run the diagnostic script to help understand the on-air behaviour.



1. Create capture file.

- A. If you already have your own capture file or know how to create them, then skip this section.
- B. Packet captures are created using WiFi Monitor interfaces. LANforge can automatically create and manage these for you. The simplest way to create a capture is to use the Port-Mgr tab in the LANforge GUI.

0				LANfo	orge Manag	ger Vers	ion(5.4.1)				\odot) (X)
<u>Control</u>	<u>Reporting</u> T	ear <u>O</u> ff <u>I</u> nfo	<u>P</u> lugins									
	Chamber View Stop All Restart Manager Refresh HELP											
File-IO	Generic F	Resource Mgr	VAP Statio	ns DUT	Profiles	Traffic-Profil	es Alerts	Messages	Warning	ıs + Wi	fi-Messages	7
Status	Port Mgr	Layer-3 L3	Endps La	ayer 4-7 🛛 🖌	Armageddon	WanLinks	S VolP/RTF	VolP/RTP	Endps 4	Attenuators	RF-Genera	ator
Disp:	192.168.10	0.195:0	Sniff Pac	kets	🕑 Down	1 Clear	Counters	Reset Po	rt Del	ete		
Rpt T	ïmer: mediur	n (8s) 🔻	Apply	/	VRF	1 D	isp <u>l</u> ay	Cr <u>e</u> ate	Mo	<u>d</u> ify <u>B</u> a	tch Modify	
	All Ethernet Interfaces (Ports) for all Resources.											
Port	Phanton	n Down	IP	SEC	Alias	Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	
1.2.04			192.168	0	eth4		6,900	115	0	0	26,702	
1.2.05			3.3.3.100	0	eth5		132,360,	984,645,	0	0	107,198,	4
1.2.06			0.0.0.0	0	wiphy0		0	0	0	0	0	=
1.2.07			0.0.0.0	0	wiphyl		47,341,5	10,649,187	5,044	179,019,	0	_
												Þ
Logged in	Logged in to: 192.168.100.238:4002 as: Admin											

C. Select WiFi radio that you wish to use and double-click it to bring up the modify window. Set the frequency to match the channel you wish to sniff and click OK to submit the changes and close the window.

• wiphy1 (lf0313-63e7) Configure Setting	s 📀 🔊 🗴					
Port Status Information						
Current: LINK-DOWN NONE						
Driver Info: Port Type: WIFI-Radio Driver: ath10k(9984) Bus: (0000:04:00.0					
Port Configurables						
Standard Configuration Firmware						
General Interface Settings	1					
Down						
Alias:						
MAC Addr: 04:f0:21:38:98:b0						
Rpt Timer: 1299 (1.299 s) 🔻						
WiFi Settings						
Max-VIFs: 4 Max-Stations: 28 Max-APs: 4 Supports: 802.11an-A	c III					
Country: United States (840)						
Channel/Freq: <mark>36 (5180 Mhz) </mark> AP: DEFAULT						
Antenna: All (4x4) Tx-Power: DEFAULT	(-1) 💌					
RTS: DEFAULT Frag: 2346						
🔲 Ignore RADAR 🔛 Don't Share Scan 🔽 Verbose Debug 🗔 Use Syslog						
Print Display Logs Probe Sync Apply	<u>O</u> K <u>C</u> ancel					

D. Make sure the radio is still selected, and click the 'Sniff Packets' button on the Port Mgr tab. You normally need to be connected to the LANforge system using remote-desktop or VNC for this to work properly. After you click 'Sniff Packets', a monitor interface will be created and Wireshark will start. When your capture is complete, stop the capture in Wireshark and save the capture file.

0	*moni7	[Wireshark 2.1.1 (Git Rev Ur	known from unknown)] (o	on lf0313-63e7)	\odot \otimes \otimes		
File E	dit View Go Capture Analyze Statistics	Telephony Tools Internals Help					
۰	• <u>/ / L x c</u>	•] 🍑 🗹 🎦 🚥 🙄			
Filte	er:	 Expression. 	Clear Apply	Save ibss ap-sta			
No.	Time Source	Destination	Protocol Length Info				
270	45 00.54.55.075520554 Compexit_12.ea.	d Compexit 41.44.15	002.11 4070 Q05 Dat	a, 3N-1100, FN-0, Flagsp			
270	50 08:54:53.075941353 CompexPt_T2:ea:0	d CompexPt_4T:a4:T3	802.11 4676 QOS Dat	a, SN=1181, FN=0, Flags=.p	F.		
270	52 08:54:53.075944484 CompexPt f2:ea:	d CompexPt 4f:a4:f3	802.11 4676 005 Dat	a, SN=1182, FN=0, Flags=.p	F.		
270	53 08:54:53.075946139 CompexPt f2:ea:	d CompexPt 4f:a4:f3	802.11 4676 0oS Dat	a. SN=1184. FN=0. Flags=.p	F.		
270	54 08:54:53.075947392 CompexPt_f2:ea:h	d CompexPt_4f:a4:f3	802.11 4676 QoS Dat	a, SN=1185, FN=0, Flags=.p	F.		
270	55 08:54:53.075948945 CompexPt_f2:ea:h	d CompexPt_4f:a4:f3	802.11 4676 QoS Dat	a, SN=1186, FN=0, Flags=.p	F.		
1 270	56 00.51.53 077070073 Composet f2.00.1	d Composet da-20-f3	202 11 4676 0os Dot	SN-3057 EN-0 Elage- p	·		
▶ Fram	e 1: 4676 bytes on wire (37408 bits).	4676 bytes captured (37408 b	its) on interface 0				
▶ Radi	otap Header v0, Length 64						
▶ 802.	* 802.11 radio information						
IEEE 802.11 QoS Data, Flags: .pF.							
Data	(4578 bytes)						
0000	00 00 40 00 2a 40 30 a0 20 08 00 a0	20 08 00 a0@.*@0					
0010	20 08 00 a0 20 08 00 00 40 00 3c 14	40 01 dd 00 @.<.@			0		
0020	00 00 00 00 72 e0 24 00 04 00 00 00	14 00 04 04r.\$D					
0030	94 00 00 00 00 00 00 00 d7 00 d9 01	12 02 d9 03					
0040	88 42 30 00 04 f0 21 da 2e f3 04 f0	21 f2 ea bd .B0!!					
0050	04 TU 21 T2 ea bd 50 71 80 00 e0 b8	90 20 1T 00!Pq	••				
• 💅	File: "/var/tmp/wireshark_moni Packe	ts: 27070 · Displayed: 27070 (100.	0%) · Dropped: 55281 (204.2%)	Profile: Default		

2. Use the do_wifi_diag.bash script to diagnose the capture file.

A. The LANforge scripts package is normally installed in /home/lanforge/scripts You can also clone the repository from github using this link: https://github.com/greearb/lanforge-scripts Assuming it is in the standard location, change to the wifi_diag directory: **cd /home/lanfore/scripts/wifi_diag**. The ./do_wifi_diag.bash script will be used to launch the wifi-diag script.

<pre>greearb@ben-dt4:~/btbits/x64_btbits/server/lf_scripts/wifi_diag</pre>	\odot \otimes \otimes
File Edit View Search Terminal Help	
<pre>[greearb@ben-dt4 wifi_diag]\$ [greearb@ben-dt4 wifi_diag]\$ [greearb@ben-dt4 wifi_diag]\$./do_wifi_diag.bash -h Usage: ./do_wifi_diag_bash -f {input-pcap-file} -o {output-directory} -d {DUT-bssid} ./do_wifi_diag_bash -f my.pcap -o report -d dc:ef:09:e3:b8:7d [greearb@ben-dt4 wifi_diag]\$ [greearb@ben-dt4 wifi_diag]\$ [greearb@ben-dt4 wifi_diag]\$./do_wifi_diag.bash -f ~/tmp/lf-dl-60sta.pcapng -o test -d 04:f0:21:f2:ea:bd - </pre>	-c

B. Run the do_wifi_diag.bash script with appropriate arguments to match your device-under-test (DUT) and pcap file. The diagnostic script can process around 300 packets per second on a fast machine, so it can take a while to process a big file.

greearb@ben-dt4:~/btbits/x64_btbits/server/lf_scripts/wifi_diag	
File Edit View Search Terminal Help	
[greearb@ben-dt4 wifi_diag]\$./do_wifi_diag.bash -f ~/tmp/lf-dl-60sta.pcapng -o test -d 04:f0:21:f2:ea:bd -C	-
Removing existing output directory: test	
Starting the wifi pcap diag.pl script, this can take a while	
NOTE: Processed 10000 packets and 5144163 input lines in 0:0:29 so far (344 pps).	
NOTE: Processed 20000 packets and 10501132 input lines in 0:1:2 so far (322 pps).	
NOTE: Processed 30000 packets and 15659389 input lines in 0:1:35 so far (315 pps).	
NOTE: Processed 40000 packets and 20895107 input lines in 0:2:8 so far (312 pps).	
NOTE: Processed 50000 packets and 26102736 input lines in 0:2:42 so far (308 pps).	
NOTE: Processed 60000 packets and 31360660 input lines in 0:3:17 so far (304 pps).	
NOTE: Processed 70000 packets and 36535836 input lines in 0:3:53 so far (300 pps).	
NOTE: Processed 80000 packets and 41700529 input lines in 0:4:26 so far (300 pps).	
NOTE: Processed 90000 packets and 46951889 input lines in 0:5:0 so far (300 pps).	
NOTE: Processed 96523 packets and 50262006 input lines in 0:5:22 so far (299 pps).	
Warning: empty y range [1:1], adjusting to [0.99:1.01]	
Warning: empty y range [1:1], adjusting to [0.99:1.0]]	
Warning: empty, range [0:0], adjusting to [-1:1]	
Warning: empty v range [0:0], adjusting to [-1:1]	
Warning empty v range [1:1] adjusting to [0.99:1.0]	
Warning empty y range [1.1], adjusting to [0.55.11]	
Panort sudd to tact (index thm]	
naport sarce to, test/index.num	
Toreasthe And A wife diagle	9
[Aiccain@ncu.ur4 mitTaraA]\$	

C. When the test is complete, you can open the [test]/index.html file to view the results, print to PDF, etc.



D. You can find the full report from this example here: examples/wifi-diag-report/index.html You can also view the report in PDF format: examples/wifi-diag-report.pdf

Candela Technologies, Inc., 2417 Main Street, Suite 201, Ferndale, WA 98248, USA www.candelatech.com | sales@candelatech.com | +1.360.380.1618