

Using Wireshark to Sniff WiFi Monitors

Goal: Sniff wireless traffic from a LANforge radio using Wireshark and a WiFi Monitor port. The best way to sniff wireless packets via Wireshark in LANforge is from a monitor port that is on its own radio (no other AP, STAs, etc.). This example will walk through the monitor port creation, sniffing the monitor port, as well as Wireshark filter recommendations.

This example uses a LANforge CT523 system but the procedure should work on a CT522, CT525, or similar system.





- 1. Create a monitor port.
 - A. In the **Port Mgr** tab, select a wiphy device that you wish to sniff with (this example will use wiphy1, an ath10k radio).
 - B. If the wiphy device is down, click the up arrow to enable it.

🛃 LANforge Manager Version(5.3.5) 📃 🖂 🖂								
Control Reporting Tear-Off Info Plugins								
Stop All Restart Manager Refresh HELP								HELP
Layer-4 Generic Test Mgr Test Group Resource Mgr Event Log Alerts Port Mgr VAP Stations Messages								
Status Layer-5 L5 Enups V			Anna	geuuon	wan	LITIKS AL	tendators	1110-10
Disp: 192.168.100.206:0 S	niff Packets	Clear	r Counters	Reset	Port	Delete		
Rpt Timer: medium (8 s) 🔻	Apply	Ų <u>V</u> ie	w Details	Cr <u>e</u>	ate	Mo <u>d</u> ify	<u>B</u> atch Modi	fy
	All Ethernet	nterfaces (Por	ts) for all Re	esources				
Port Pha Down IP SEC	Alias Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	TX Pkts	Pps TX
1.1.0	eth0	28,204,301	78,708	4	3,995	138,989,512	119,168	3
1.1.1 0.0.0.0 0	eth1	0	0	0	0	0	0	0
1.1.2 0.0.0.0 0	wiphy0	119,166,145	546,717	14	23,808	234,792	1,431	0
1.1.3 0.0.0.0 0	wiphy1	0	0	0	0	0	0	0
1.1.4 0.0.0.0 0	wiphy2	92,304,964	438,217	16	26,589	77,221	2,413	0
								•••••
Logged in to: brent-523:4002 as: Admin								

C. Click Modify.

٠ ٤	wiphy1 (brent-523) Configure Settings							
	Port Status Information	1						
Current: LINK-DOWN NONE								
Driver Info: Port Type: WIFI-Radio Driver: ath10k(988x) Bus: 0000:06:00.0								
	Port Configurables							
Standard Configura	tion RF Patterns Firmware							
Enable —	General Interface Settings	1						
	Allas:							
	MAC Addr: 04:T0:21:11:07:36 IX Q Len 0							
	Rpt Timer: medium (8 s)							
	WiFi Settings							
	Max-VIFs: 64 Max-Stations: 64 Max-APs: 7 Supports: 802.11abgn-AC							
	Country: United States (840)							
	Channel/Freq: 36 (5180 Mhz)							
	Antenna: All (3x3) Tx-Power: DEFAULT (-1)	-						
	RTS: DEFAULT Frag: 2346							
	Verbose Debug							
Print View Details	Logs Probe Sync Apply OK	<u>C</u> ancel						

- A. Select the channel you wish to sniff. Channel 36 will be used for this test.
- B. Click OK.
- D. Back in the Port Mgr tab, with the wiphy device still selected, click Create.

\$			Create VLANs of	on Port: 1.1.3		_ O X
1	○ MAC-VLAN ○ WiFi STA	○ 802.1Q-VLAN ○ Red ⊃ WiFi VAP	irect 🔾 Bridge or 🔾 WiFi Virtua	⊖ GRE Tunnel al Radio		
2	Shelf:	1	Resource:	1 (brent-523) 🔻	Port: 3 (v	wiphyl)
B	VLAN ID:		DHCP-IPv4			
	Parent MAC:	04:f0:21:11:e7:36	DHCP Client ID:	None	-	
	MAC Addr:	XX:XX:XX:*:*:XX	IP Address:		Global IPv6:	
	Quantity:	1	IP Mask or Bits:		Link IPv6:	AUTO
			Gateway IP:		IPv6 GW:	
	#1 Redir Name:		#2 Redir Name:			
	STA ID:	0	SSID:			
	WiFi AP:		Key/Phrase:			
	WPA	WPA2	WEP			
4	Down					
	Apply 📐	<u>C</u> ancel			Ready	

- A. Select the WiFi Monitor option at the top.
- B. Set the $\ensuremath{\textbf{Quantity}}$ to 1.
- C. Set the $\ensuremath{\text{STA ID}}$ to $\ensuremath{\text{0}}.$
- D. Click **Apply** and close the Create Port window.

E. In the Port Mgr tab again, modify moni0.

🔮 moni0 (brent-5	23) Configure Settings							
Port Status Information								
Current: LINK-UP GRO NONE								
Driver Info: Port Type: WIFI-MON Parent: wiphy1								
P	ort Configurables							
Enable ——	General Interface Settings							
🗌 Set IF Down								
Set MAC								
🗌 Set TX Q Len	Down							
Set MTU	Alias:							
🗌 Set Offload	Rpt Timer: medium (8 s) 💌							
Set PROMISC								
Low Level								
PROMISC	WiFi Settings							
TSO Enabled								
UFO Enabled								
GSO Enabled	🗌 Disable HT40 🔲 Disable HT80							
LRO Enabled								
GRO Enabled								
,								
Print View Details Probe	e Sync <u>Apply OK</u> <u>Cancel</u>							

A. You can disable HT40 and HT80 here if needed.

B. Click **OK** to close the window.

- 2. For this current setup, traffic will be generated with a layer 3 UDP connection between two stations. For more information see Generating Traffic for WLAN Testing
- 3. Use Wireshark to sniff **moni0**.
 - A. If you are running the LANforge GUI from a Windows machine without x server installed, you will need to connect remotely to the LANforge system via **rdesktop** or **vnc**.

A. To connect via **rdesktop**, type the following command into a console (replace LANforge-IP with the IP of your LANforge system):



- I. The login info is username/password lanforge/lanforge
- B. To connect via vnc, type the following command into a console (replace LANforge-IP with the IP of your LANforge system. Don't forget to add the ':1' after the IP:

vncviewer [LANforge-IP]:1 The password is lanforge.

Applications Places System Tue Feb 21, 12:43 Ianforge@brent-523:~ Ianforge@brent-523:~ Trash Ianforge@brent-523:~ File Edit Computer Computer
Ianforge@brent-523:~ Ianforge@brent-523:~ • Irash Ianforge@brent-523:~ File Edit View Search Terminal Help Computer Ianforge@brent-523 ~15
Trash Ianforge@brent-523:~ • • • • • • • • • • • • • • • • • • •
Configure LANforge
LANforge-FIRE GUI
LANforge-ICE GUI
k.

C. Once you have accessed the LANforge system via rdesktop or vnc, open the LANforge GUI with the desktop icon shown below.



- B. Select **moni0** in the **Port Mgr** tab.
- C. Click the **Sniff Packets** button. Wireshark will now open and automatically start scanning for packets. If you get a window that warns about running as user root, click **OK**.

🛃 LANforge Manager Version(5.3.5) 🗕 🗆 🗶														
<u>C</u> ontrol	Control Reporting Tear-Off Info Plugins													
	Stop All Restart Manager Refresh HELP													
Layer-4 Status	Layer-4 Generic Test Mgr Test Group Resource Mgr Event Log Alerts Port Mgr vAP Stations Messages Status Layer-3 L3 Endps VolP/RTP VolP/RTP Endps Armageddon WanLinks Attenuators File-10													
	Disp: 192.168.100.206:0 Sniff Packets 1 Clear Counters Reset Port Delete													
	Rpt Ti	mer: I	medium	(8s) 🔻	·	Apply		Į ⊻ie	w Details	Cre	ate	Mo <u>d</u> ify	<u>B</u> atch Modi	fy
						All Et	hernet	nterfaces (Por	ts) for all R	esources				
Port	Pha	Down	n	IP	SEC	Alias	Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	TX Pkts	Pps TX
1.1.0			192.16	8.100.192	0	eth0		32,194,714	116,445	8	7,335	171,859,002	151,077	11
1.1.1			0.0.0.0)	0	eth1		0	0	0	0	0	0	0
1.1.2			0.0.0.0)	0	wiphy0		123,232,035	564,287	65	102,061	405,468	1,640	0
1.1.3			0.0.0.0)	0	wiphy1		45,873,427	261,958	377	503,771	0	0	0
1.1.4			0.0.0.0)	0	wiphy2		94,805,676	449,422	73	108,605	238,501	2,630	0
1.1.5			0.0.0.0	1	0	moni0	wiphy1	50,788,788	215,406	307	564,049	0	0	0
1.1.6			86.1.1.	1	0	vap0	wiphy0	153,800	134	0	0	168,050	190	0
1.1.7			86.1.1.	10	0	sta0	wiphy2	81,096	84	0	0	78,476	68	0
1.1.8			86.1.1.	11	0	stal	wiphy2	80,594	81	0	0	78,114	67	0
														Þ
Logged i	Logged in to: brent-523:4002 as: Admin													

A. To use a filter, simply add the filter constraints to the filter text box as seen below and click**Apply** to the right. The below screenshot has wireshark filtering on a specific IP.

🔏 🔹 Capturing from moni0 [Wireshark 2.1.1 (Git Rev Unknown from unknown)] (on brent-523) 📃 🗖 🔍
File Edit View Go Capture Analyze Stat	tistics Telephony Tools Internals Help
Filter: ip.addr==86.1.1.10	Expression Clear Apply Save
No. Time Source	Destination Protocol Length Info
20957 00.58598743 80.1.1.11	80.1.1.10 LANFORGE 1503 Seq: 259
21000 00.79451758 80.1.1.10	86.1.1.11 LANForge 1563 Seq: 260
21002 00.79527032 80.1.1.10	86 1 1 10 LANForge 1563 Seq: 260
21006 60.79642158 86.1.1.11	86.1.1.10 LANforge 1563 Seq: 260
21060 61.00557988; 86.1.1.10	86.1.1.11 LANforge 1563 Seq: 261
21062 61.00633398 86.1.1.10	86.1.1.11 LANforge 1563 Seq: 261
21064 61.00672896 86.1.1.11	86.1.1.10 LANforge 1563 Seq: 261
21066 61.00751672 86.1.1.11	86.1.1.10 LANforge 1563 Seq: 261
21117 61.21560615 [,] 86.1.1.10	86.1.1.11 LANforge 1563 Seq: 262
21119 61.21597788 86.1.1.11	86.1.1.10 LANforge 1563 Seq: 262
21121 61.21674900! 86.1.1.10	86.1.1.11 LANforge 1563 Seq: 262
21123 61.21706741 86.1.1.11	86.1.1.10 LANforge 1563 Seq: 262
21169 61.42599177 [,] 86.1.1.10	86.1.1.11 LANforge 1563 Seq: 263
21171 61.42621316 86.1.1.11	86.1.1.10 LANforge 1563 Seq: 263
21173 61.42700193 86.1.1.10	86.1.1.11 LANforge 1563 Seq: 263
21175 61.42722277 86.1.1.11	86.1.1.10 LANforge 1563 Seq: 263
21227 61.63506546 86.1.1.10	86.1.1.11 LANTorge 1563 Seq: 264
21229 61.63581659! 86.1.1.10	86.1.1.11 LANForge 1563 Seq: 264
21231 01.03021495 80.1.1.11	86.1.1.10 LANForgo 1563 Seq: 264
21234 01.03039300 80.1.1.11	80.1.1.10 LANTOIGE 1505 Seq. 204
Frame 1586: 1563 bytes on wire (12504 bi	its), 1563 bytes captured (12504 bits) on interface 0
 Radiotap Header v0. Length 29 	
802.11 radio information	
▶ IEEE 802.11 QoS Data, Flags:T	
Logical-Link Control	
Internet Protocol Version 4, Src: 86.1.1	1.11, Dst: 86.1.1.10
 User Datagram Protocol, Src Port: 33003, 	, Dst Port: 33002
LANforge Traffic Generator	
0000 00 00 1d 00 2b 48 08 00 b6 52 12 48	3 00 00 00 00+HR.H
0010 00 00 3c 14 40 01 ea 00 00 00 07 04	4 12 88 01 30
0020 00 00 00 88 10 D7 2T 00 08 88 45 37	7 43 00 0e 8e/E/C
0040 00 05 dc a3 2a 40 00 40 11 e3 cf 56	5 01 01 0b 56*@.@VV
0050 01 01 0a 80 eb 80 ea 05 c8 0e 0e 00	0 00 00 1a
0070 20 bc 32 10 06 66 d8 00 00 00 00 00	0 00 00 00 00 + <m< td=""></m<>
0080 01 02 03 04 05 06 07 08 09 0a 0b 0c	0d 0e 0f 10
AAAA 11 12 13 14 15 16 17 18 10 1a 1b 1c	- 1d 1e 1f 20
moni0: <live capture="" in="" progress=""> File: /va</live>	Profile: Default

B. If you'd like to only see traffic to/from a single AP use the filterwlan.addr == [bssid]

4	*moni	4a [Wiresh	ark 1.12.6 (0	Git Rev Unknown fro	m unknown)] (or	brent-523) 🗕 🗖
File Edit	t View Go	Capture	Analyze S	tatistics Telephon	y Tools Intern	als Help
• •			🗋 🗙 C	Q ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	° ⊼ ⊻ [
Filter: w	lan.addr =:	= 00:0e:8e	:d4:53:2f	E E	xpression Cl	ear Apply Save
No.	Time	Source		Destination	Protocol L	ength Info
547 3 556 4 557 4 605 4 646 4 664 5 684 5 712 5 713 5 721 5	3.971028000 4.018318000 4.018336000 4.134191000 4.379931000 4.379931000 5.4871490000 5.117305000 5.362999000 5.444919000 5.444937000 5.479387000 5.608776000	Sparklan_d Sparklan_d Sparklan_d Sparklan_d Sparklan_d Sparklan_d Sparklan_d Sparklan_d Sparklan_d Sparklan_d	14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f 14:53:2f	CompexPt_9e:26:00 CompexPt_9e:26:00 Sparklan_d4:53:21 Broadcast Broadcast Broadcast Broadcast Broadcast Broadcast Sparklan_da:79:9b Sparklan_d4:53:21 Sparklan_34:96:a0 Broadcast	802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11	213 Probe Response, SN=55 213 Probe Response, SN=55 62 Acknowledgement, Flag 219 Beacon frame, SN=558, 219 Beacon frame, SN=560, 219 Beacon frame, SN=561, 219 Beacon frame, SN=561, 219 Beacon frame, SN=563, 213 Probe Response, SN=56 62 Acknowledgement, Flag 213 Probe Response, SN=566 219 Beacon frame, SN=566.
<pre> Frame : Radiota Radiota Field 80 IEEE 80 0000 00 0010 20 0020 10 0030 80 0040 00 </pre>	74: 219 byt ap Header v 02.11 Beaco 02.11 wirel 00 30 00 2 08 00 00 0 02 85 09 ad 00 00 00 f 0e 8e d4 5:	es on wire 0, Length 4 n frame, Fi ess LAN mar f 40 00 a0 0 00 00 00 0 00 f8 00 0 00 ff ff ff 3 2f 00 21	(1752 bits 48 Lags: 20 08 00 a 92 b2 31 6 00 00 e8 6f ff 00 6 80 41 08 6), 219 bytes captu C ame 0 20 08 00 a0 . 0 00 00 00 00 0 f8 01 eb 02 . e 8e d4 53 2f . i 80 00 00 00 .	red (1752 bits) 0./@ 	<pre>> on interface 0</pre>

D. There are many filters that can be used in Wireshark. Some handy ones include:

```
IP: ip.addr==x.x.x.x
wlan MAC: wlan.addr==xx:xx:xx:xx:xx
Association request wlan.fc.type_subtype eq 0
Association response wlan.fc.type_subtype eq 1
Probe request wlan.fc.type_subtype eq 4
Probe response wlan.fc.type_subtype eq 5
Beacon wlan.fc.type_subtype eq 8
Authentication wlan.fc.type_subtype eq 11
Deauthentication wlan.fc.type_subtype eq 12
```

- E. Filters can be combined to specify if packets should match all filters (with &&) or any filters (with | |).
 For example, if you wanted to view packets that only contain both IPs 1.1.1.1 and 2.2.2.2 you could use the following: ip.addr==1.1.1.1 && ip.addr==2.2.2.2
 Or, if you want to see all packets containing 1.1.1.1 and all packets containing 2.2.2.2, you could use the following: ip.addr=1.1.1.1 || ip.addr==2.2.2.2
- F. You can visit https://wiki.wireshark.org/DisplayFilters for more tips on filters. A handy 'cheat sheet' with most filters can be found here.

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