

LANforge WiFi Degraded vAP Testing

Goal: Create 1 vAP on a single a/b/g/n/AC radio and configure it to drop 50% of management frames to test that station devices can handle lost management frames properly.

Requires LANforge 5.3.2 or later. Configure 1 vAP, add the vAP to a bridge and set up DHCP. The Device Under Test (DUT) in this case is a mobile handset or other wifi station device. Verify that station can handle associating with an AP that drops many management frames. This example uses a LANforge CT523 system but the procedure should work on all CT520, CT521, CT522, CT523 and CT525 systems.

1. In the **Ports** tab, select the radio **wiphy2** and click **Create.** Configure the values appropriately and click create.

•			Create VLANs on Port: 1.2.04	\odot \otimes \times
0	○ MAC-VLAN ○ WiFi STA	○ 802.1Q-VLAN ○ ⑧ WiFi VAP ○ WiFi	Redirect O Bridge O GRE Tunnel Monitor O WiFi Virtual Radio	
2	Shelf:	1 💌	Resource: 2 (ben-ota2) Port: 4 (wiphy2)	-
B	VLAN ID:		DHCP-IPv4	
	Parent MAC:	04:f0:21:11:e7:3b	DHCP Client ID: None	
	MAC Addr:	XX:XX:XX:*:*:XX 💌	IP Address: Global IPv6: AUTO	
	Quantity:		IP Mask or Bits: Link IPv6: AUTO	
			Gateway IP: IPv6 GW: AUTO	
	#1 Redir Name:		#2 Redir Name:	
	STA ID:	200	SSID: ben-ota-w2-1-a	
	WiFi AP:		Key/Phrase:	
	WPA	WPA2	WEP	
A	Down			
	<u>A</u> pply	<u>C</u> ancel		

2. In the **Ports** tab you will see the new WiFi vAP:

LANforge Manager Version(5.3.3) ben-title														
<u>C</u> ontrol <u>R</u> eporting <u>T</u> ear-Off <u>I</u> nfo <u>P</u> lugins														
	Stop All Restart Manager Refresh HELP													
File-IO	File-IO Layer-4 Generic Test Mgr Test Group Resource Mgr Event Log Alerts Port Mgr Messages													
D	Disp: 192.168.100.149:0.0 Sniff Packets Clear Counters Reset Port Delete													
R	pt Tim	er: me	edium (8 s) 🔻		Apply	/	<u>V</u> iew	Details	Cr <u>e</u>	ate	<u>M</u> odify	<u>B</u> atch Me	odify
						-All Et	hernet Ir	nterfaces (Po	rts) for all	Resource	s. —			
Port	Pha	Down		IP	SEC	Alias	Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	TX Pkts	Pps TX
1.2.07		V	0.0.0.0		0	wlan2	wiphy2	0	0	0	0	0	0	0
1.2.08		~	0.0.0.0		0	vapl	wiphyl	0	0	0	0	312	3	0
1.2.09		~	0.0.0.0		0	vap2	wiphyl	0	0	0	0	216	2	0 =
1.2.10			0.0.0.0		0	vap200	wiphy2	93,751,752	61,990	0	0	1,972,450	22,802	0 🖵
Logged in to: ben-ota-1:4002 as: Admin														

3. Select the **Status** panel in the LANforge GUI, and click the Netsmith button for the appropriate resource. Rightclick and select the 'New Bridge' option. In this example, I selected 'br2' as the bridge name. After creating the bridge, click Sync to show the new bridge device. Right-click on br2 and select Modify Port. Add the vAP you just created to the bridge with the Add Ports button and then apply:

br2 (ben-ota2) Configure Settings									
Port Status Information Current: LINK-UP PROBE-ERROR TSO UFO GSO GRO Driver Info: Port Type: Bridge Driver: bridge(2.3) Bus: N/A									
Port Configurables									
Enable ——		1	Spanning-Tree						
Set IF Down	Down	Aux-Mgt			Aging Time:	300			
Set MAC	DHCP-IPv6	DHCP Release	DHCP Vendor ID: None		Bridge Priority:	32768			
Set TX Q Len	DHCP-IPv4	Secondary-IPs	DHCP Client ID:	None	Max Age:	20	-		
Set MIU	DNS Servers:	BLANK	Peer IP:	NA	Hello Time:	2	-		
Set Bridge Info	IP Address:	88.1.1.1	Global IPv6:	AUTO	Forwarding Delay:	15	-		
Jet bridge mit	IP Mask:	255.255.255.0	Link IPv6:	AUTO					
	Gateway IP:	0.0.0.0	IPv6 GW:	AUTO					
	Alias:		MTU:	1500					
	MAC Addr:	04:f0:21:7b:11:3b	TX Q Len	0					
	Rpt Timer:	medium (8 s) 🔻	WiFi Bridge:	NONE					
	Bridg	je Information	Remov						
Services —	Configured Po	rts Current Ports							
	449200	100200		orts					
FTP			vap200						
	,								
Print View Details Probe Sync Apply OK Cancel									

4. Create a virtual router in Netsmith and add br2, and optionally a wired port (eth1) to the router. Double-click the br2 port and configure DHCP to match its IP address. When complete, Netsmith should look something like this:



5. Now, we should have 1 vAP able to accept stations and give out DHCP addresses. For an initial test, make sure the DUT can connect to the vAP and get an IP address. Once that is verified, right-click and choose Port Modify on the vap200 vAP. We will now configure it to not respond to 50% of the management frames sent to it:

•	vap200 (ben-ota2	?) Configure Settin	gs	\odot \land \times					
	Port Status Information								
Current: LINK-UP GRO NONE									
Driver Info: Port Type: WIFI-AP Parent: wiphy2									
Port Configurables									
Standard Configuration	Advanced Configura	tion Misc Configu	Iration Custom WiFi						
	Advanc	ed WiFi Settings							
Select 'WPA2' on the and enable Advanced	Standard Configuratio d/802.1x to enable mos	on screen to enable t of these. Enablin	e Advanced/802.1x g 802.11u enables others.						
Ignore Probes:	50% (50%)	▼ HESSID:							
Ignore Auth-Assoc:	50% (50%)	Realm:							
Ignore Assoc:	50% (50%)	▼ IMSI:							
Ignore Re-Assoc:	50% (50%)	 Milenage: 							
Corrupt GTK:	50% (50%)	▼ Domain:							
HS20 Capabilities		Consortium:							
HS20 Oper Class		RADIUS IP	127.0.0.1						
HS20 WAN Metrics		RADIUS Port	1812						
leee80211w:	Disabled (O)	RADIUS Secret							
Venue Group:	Jnspecified (0)	 Venue Type: 	Unspecified (0) 🔻						
Network Type:	Private (O)	Address Types:	Not Available (0) 🗸						
Network Auth:		3GPP Cell Net:							
🗌 Use 80211d 🗌 U	se 80211h 🗌 Short-P	reamble							
Advanced/802.1x	HotSpot 2.0 Di	sable DGAF							
Enable 802.11u	🗌 Enable 802.11u 🔄 802.11u Internet 🔄 802.11u ASRA 🔄 802.11u ESR 🔄 802.11u UESA								
Print View Details Logs	Probe	Display Scan	Sync Apply OK	Cancel					

- 6. In this case, we are using open authentication, but it would also be good to test with encryption (WPA2 PSK, for instance) to make sure that the DUT can handle failures of the 4-way authentication handshake, for instance.
- 7. To verify the results, use a sniffer to watch the association requests and responses. A LANforge radio configured for monitor mode could verify this, as could third-party sniffers. In the capture below you can see that the station had to make two Authentication requests before the AP would answer (because the AP is set to randomly ignore 50% of the association requests):

•	*moni5a [Wiresh	ark 1.10.14 (Git Rev Unknow	n from unl	known)] (on ben-ota-1)	\odot \otimes \times			
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help								
🕒 🛛 🧹 🖿 🖉 🖿 🖉 X G	Q 🔄 📎 😓		1	🕁 🗹 ங 🙁				
Filter: wlan.addr == 04:f0:21:11:e7:3a	Å	Expression Clear Apply	Save	bss-cross ibss-10k sta1000 vap50 wlan2-o1				
No. Time 2992 2015-10-13 10:03:20.735583060 2992 2015-10-13 10:03:20.735982060 301 2015-10-13 10:03:20.736849060 302 2015-10-13 10:03:20.737249060 303 2015-10-13 10:03:20.785202060 304 2015-10-13 10:03:20.785597060 305 2015-10-13 10:03:20.785597060	Source Netgear_11:0a:78 Netgear_11:0a:78 Netgear_11:0a:78 Netgear_11:0a:78 Netgear_11:0a:78 Netgear_11:0a:78	Destination CompexPt_11:e7:3a CompexPt_11:e7:3a CompexPt_11:e7:3a CompexPt_11:e7:3a CompexPt_11:e7:3a CompexPt_11:e7:3a	Protocol 802.11 802.11 802.11 802.11 802.11 802.11 802.11	Length Info 250 Probe Response, SN=3350, FN=0, Flags=R, BI= 250 Probe Response, SN=3350, FN=0, Flags=R, BI= 250 Probe Response, SN=3351, FN=0, Flags=R, BI= 250 Probe Response, SN=3351, FN=0, Flags=, BI= 250 Probe Response, SN=3352, FN=0, Flags=, BI= 250 Probe Response, SN=3352, FN=0, Flags=, R, BI= 250 Probe Response, SN=3352, FN=0, Flags=, R, BI=	100, SSI 100, SSI 100, SSI 100, SSI 100, SSI 100, SSI 100, SSI			
306 2015-10-13 10:03:20.787151000	Netgear 11:0a:78	CompexPt 11:e7:3a	802.11	250 Probe Response, SN=3352, FN=0, Flags=R, BI=	100, SSI			
307 2015-10-13 10:03:20.787541000 309 2015-10-13 10:03:20.903128000 310 2015-10-13 10:03:20.903177000 313 2015-10-13 10:03:21.004169000 314 2015-10-13 10:03:21.004215000 315 2015-10-13 10:03:21.004593000 317 2015-10-13 10:03:21.01156000 318 2015-10-13 10:03:21.011254000	Netgear_11:0a:78 CompexPt_11:e7:3a CompexPt_11:e7:3a CompexPt_7b:11:3b CompexPt_11:e7:3a	CompexPt_11:e7:3a CompexPt_7b:11:3b CompexPt_11:e7:3a (RA) CompexPt_11:e7:3a (RA) CompexPt_11:e7:3a (RA) CompexPt_11:e7:3a (RA) CompexPt_11:e7:3a (RA)	802.11 802.11 802.11 802.11 802.11 802.11 802.11 802.11	 250 Probe Response, SN=3352, FN=0, Flags=	100, SSI SSID=be			
٩ (<u> </u>				
Frame 309: 48 bytes on wire (384 bits Radiotap Header v0, Length 18 Header revision: 0 Header length: 18 Present flags Flags: 0x00 Data Rate: 6.0 Mb/s Channel trequency: 5745 [A 149] Channel type: 802.11a (0x0140) SSI Signal: -11 dBm Antenna: 0 RX flags: 0x0000 Tref enderset Tref enderset In the set of the set), 48 bytes captured	(384 bits) on interface 0			Ĵ			
▶ IEEE 802.11 Authentication, Flags:					Ψ			
0000 00 00 12 00 2e 48 00 00 00 0c 72 0010 00 00 0b 00 03 co 00 44 f0 21 7b 11 0020 e7 3a 04 f0 21 7b 11 3b 40 10 00	L 16 40 01 f5 00 L 3b 04 f0 21 11 0 00 01 00 00 00:	Hq.@ {;!.<br !{.;@						

A. Also in Wireshark, go to the **Statistics** menu and select **IO Graphs** to display up to 5 graphs based on the available frames in the capture file.

•	Wireshark IO Graphs: impaired	ap-test-0-50-75-100-0.pcapng	(as superuser)	\odot \otimes \otimes
0% impairment	50% impairment	75% impairment	100%	0%
_,,				- 100
11:45:05 11:46:45	11:48:25 11:50:05 11	:51:45 11:53:25 11:55:	05 11:56:45	11:58:25 12:00:05
Graphs				X Axis
Graph 1 Color 🗹 Filter: wlan	.fc.type_subtype==0x04	Probe Requests s	style: Line 🍦 🗹 S	Smooth Tick interval: 10 sec 🛔
Graph 2 Color Filter: wlan	.fc.type_subtype==0x05	Probe Responses	style: Dot 🛔 🗹 s	Smooth Pixels per tick: 10 🛔
Graph 3 Color 🗹 Filter: wlan	.fc.type_subtype==0x00	S	style: Line 🛔 🗹 s	Smooth 🗹 View as time of day
Graph 4 Color Filter: wlan	.fc.type_subtype==0x01	S	style: Dot 🛔 🗹 s	Smooth Y Axis
Graph 5 Color Filter: wlan	.fc.retry==1	s	style: Impulse 🛔 🗹 s	Smooth
				Scale: Auto * Smooth: No filter *
😲 Help 🛛 📳 Copy				🗶 Close 🛛 🛃 Save

B. The two images below have been annotated to show the behavior of 10 stations being reset every 30 seconds while their vAP has increasing impairment of management frames.

•	Wireshark IO Graphs: impaired-	ap-test-0-50-75-100-0.pcapng	(as superuser)	\odot \otimes \otimes
0% impairment	50% impairment	75% impairment	100%	0%
	MAAAAA			-25
11:45:05 11:46:45	11:48:25 11:50:05 11	1:51:45 11:53:25 11:55	:05 11:56:45	11:58:25 12:00:05
Graphs Graph 1 Color ☑ Filter: Wlan.1 Graph 2 Color ☑ Filter: Wlan.1 Graph 3 Color ☑ Filter: Wlan.1 Graph 4 Color ☑ Filter: Wlan.1 Graph 5 Color ☑ Filter: Wlan.1	fc.type_subtype==0x04 fc.type_subtype==0x05 fc.type_subtype==0x00 fc.type_subtype==0x01 fc.retry==1	s Association Requests Association Responses s	tyle: Line 🕴 🖉 S tyle: Dot 🛊 🖉 S tyle: Line 🛊 🖉 S tyle: Dot 🛊 🖉 S tyle: Impulse 🛊 🖉 S	X Axis Tick interval: 10 sec Pixels per tick: 10 Wiew as time of day Y Axis Unit: Packets/Tick Scale: Auto Smooth: No filter Packets
Copy				🗶 Close 🕹 Save

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