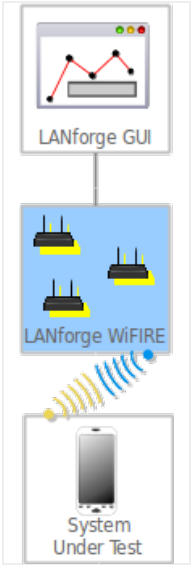
sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

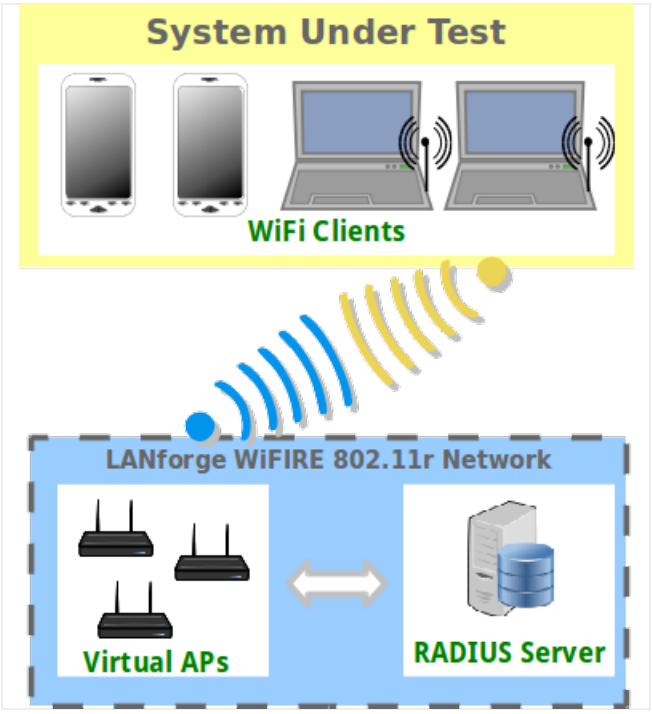
LANforge WiFi Access Point Network with 802.11r

Goal: Configure a virtual AP network with 802.11r to allow testing fast transition (FT) clients. Configure virtual Access Points to use 802.11r with FT-EAP. This example uses a LANforge CT523 system but the procedure will work on all CT522, CT523 and CT525 multi-radio systems.



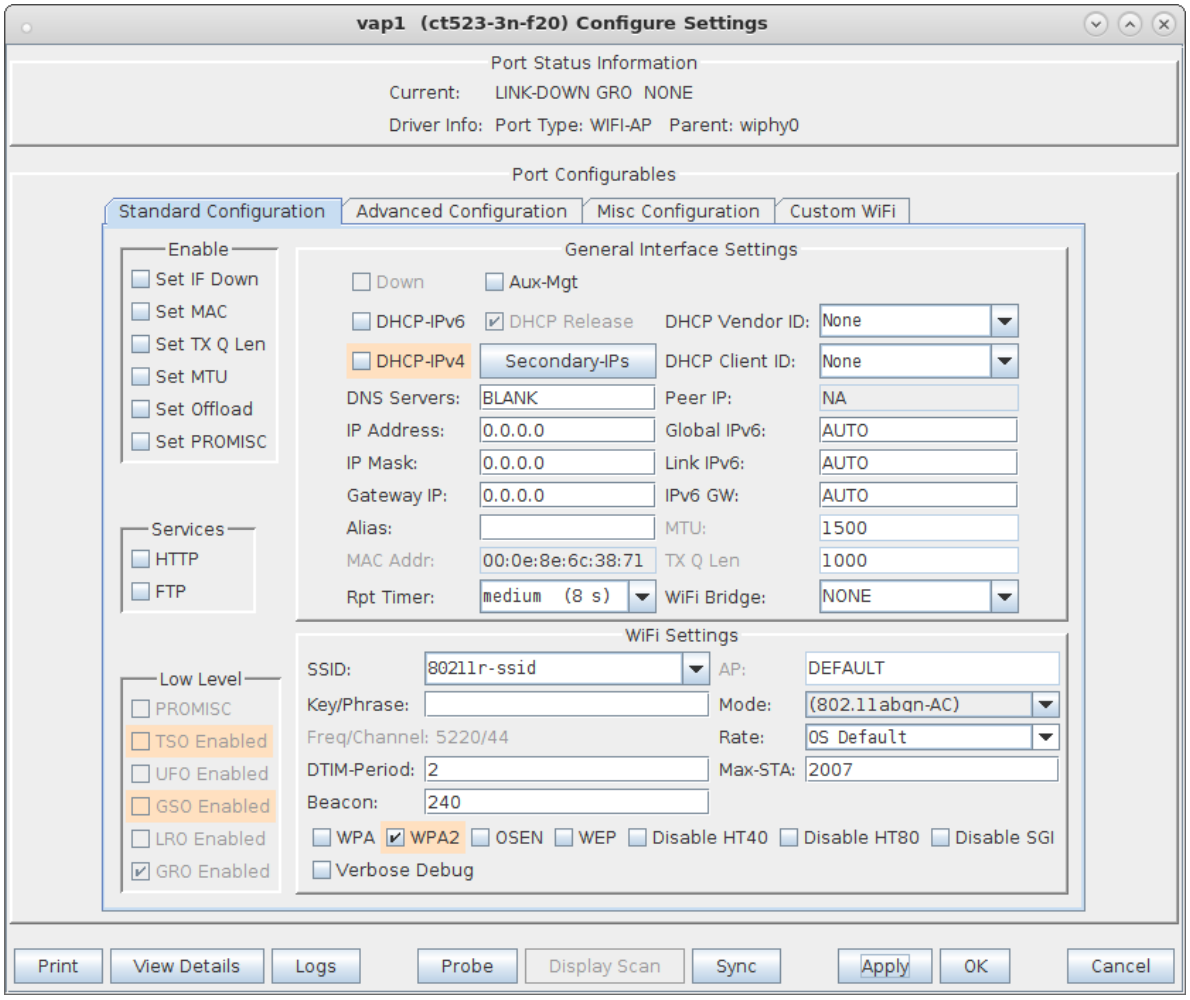
The wifi clients under test are also 802.11r enabled so that they can initiate FT Requests and roam. Here we are using another LANforge WiFire as the system under test to emulate 802.11r stations and force them to roam.

In LANforge, each virtual access point will be running its own hostapd process configured to enable 802.11r and bridged to other virtual access points. The bridged VAP network will emulate the Distributed System (DS) for FT over-the-DS roaming.

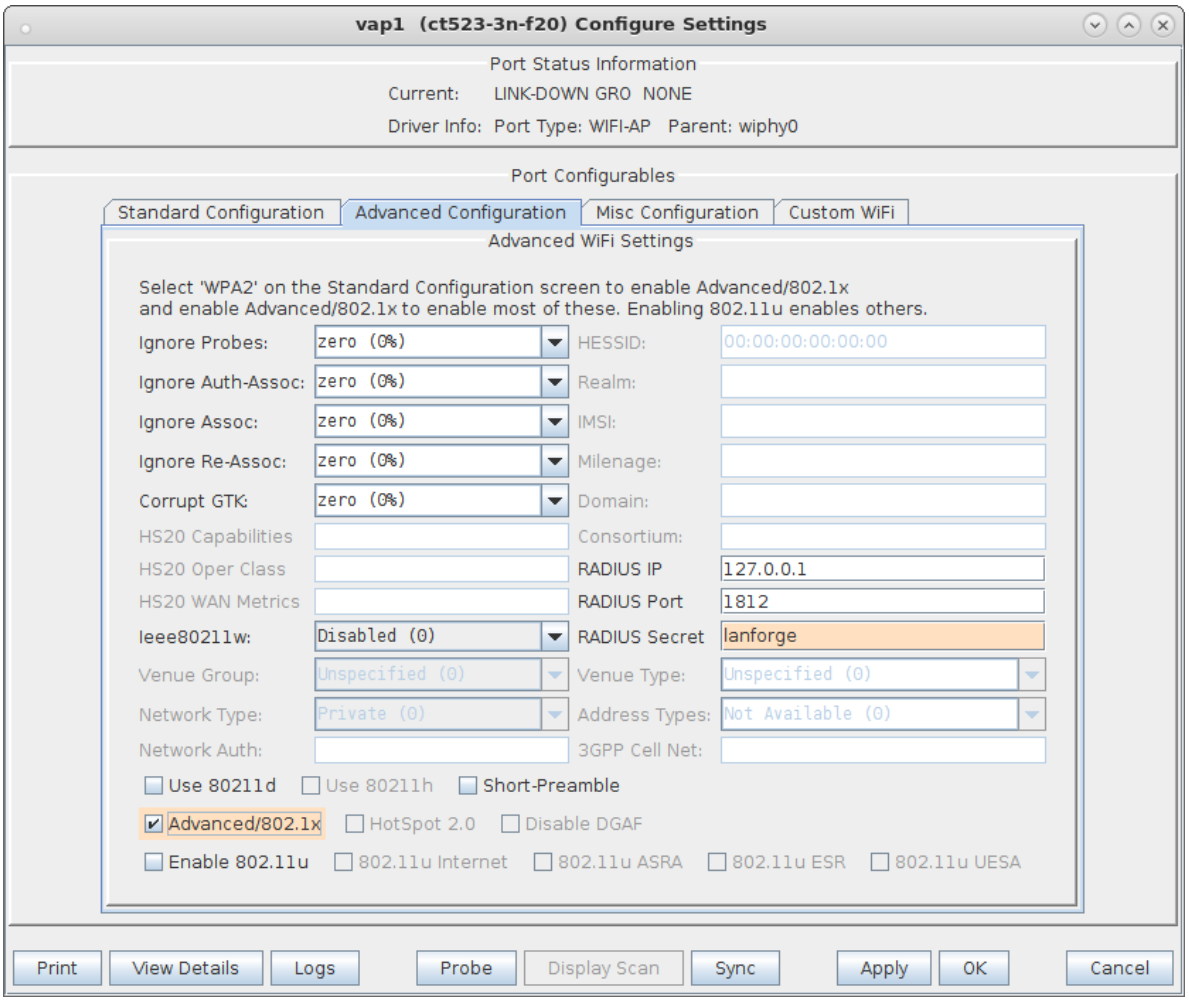


1. Setup a single virtual access point on each wifi NIC for at least two NICs and configure them for the same channel and SSID.
   A. Go to the Port Manager tab, select the parent device such as wiphy0, click Modify, set a specific channel/frequency. Repeat for wiphy1.
   B. Select wiphy0, click Create, fill out appropriate information and create a virtual access point. Repeat for wiphy1.

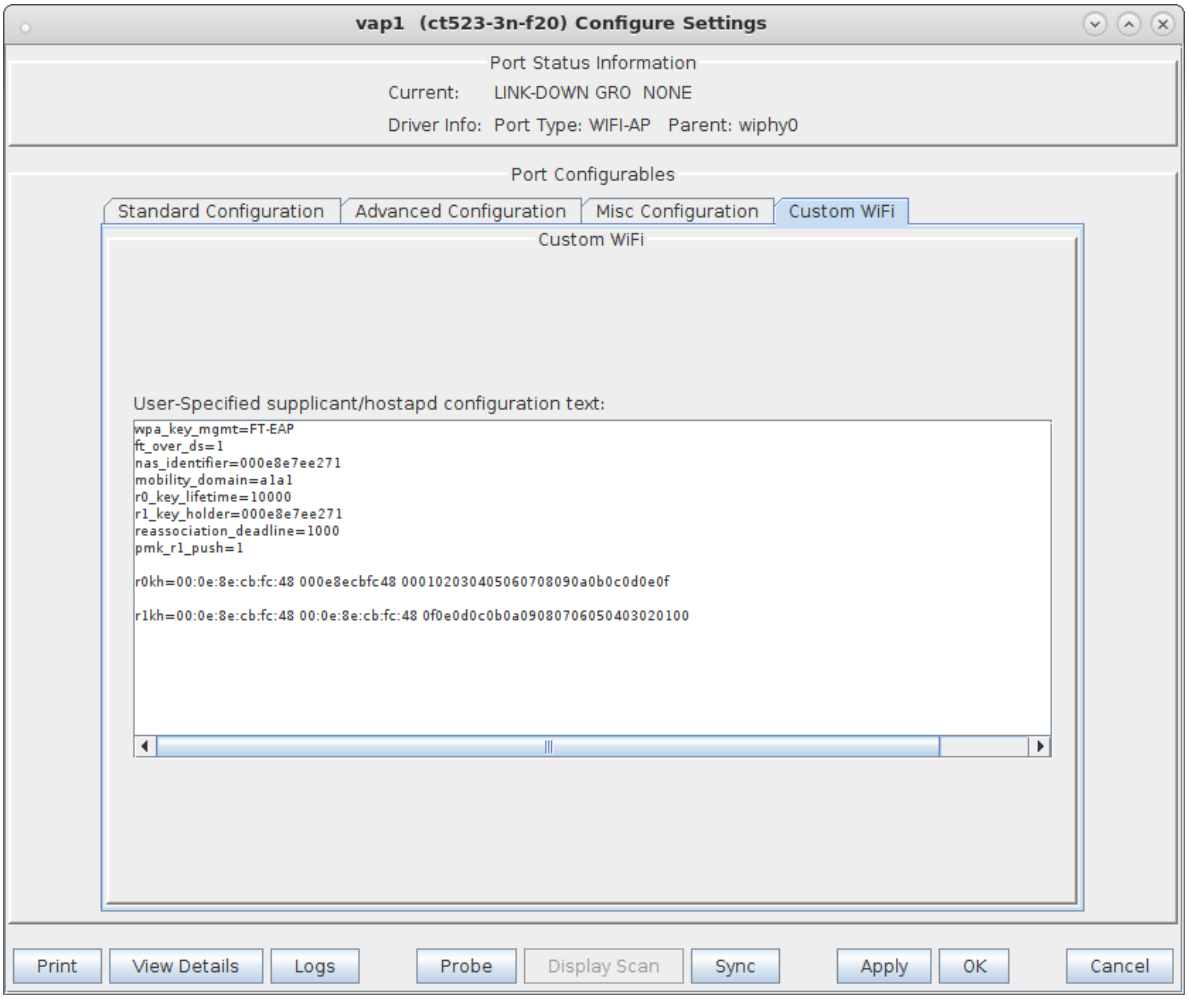
C. The new vap should appear in the Port-Mgr table. Double-click to modify. Configure SSID and select WPA2 but do not fill in the Key/Phrase:



D. Select the **Advanced Configuration** tab in the Port-Modify window and check the box Advanced/802.1x and fill in the RADIUS IP/Port/Secret. Here the RADIUS server will be another instance of hostapd configured on a bridge interface and accessible via localhost.



E. Select the **Custom WiFi** tab in the Port-Modify window to fill in the additional hostapd options to enable and configure 802.11r. These lines will be appended to the end of the LANforge generated hostapd configuration file located in /home/lanforge/wifi of the resource in use.



vap1 00:0e:8e:7e:e2:71 - Your MAC will be different.

```
wpa_key_mgmt=FT-EAP
ft_over_ds=1
nas_identifier=000e8e7ee271   #vap1 MAC without colon delimiters, yours will differ.
mobility_domain=a1a1
r0_key_lifetime=10000
r1_key_holder=000e8e7ee271   #vap1 MAC without colon delimiters, yours will differ.
reassociation_deadline=1000
pmk_r1_push=1

#r0kh is vap2 MAC address, vap2 nas identifier, AES key
r0kh=00:0e:8e:cb:fc:48 000e8ecbfc48 000102030405060708090a0b0c0d0e0f

#r1kh is vap2 MAC address, vap2 r1 key holder MAC, AES key
r1kh=00:0e:8e:cb:fc:48 00:0e:8e:cb:fc:48 0f0e0d0c0b0a09080706050403020100
```

full configuration file: hostapd_vap1.conf

vap2 00:0e:8e:cb:fc:48 - Your MAC will be different.

```
wpa_key_mgmt=FT-EAP
ft_over_ds=1
nas_identifier=000e8ecbfc48   #vap2 MAC without colon delimeters, yours will differ.
mobility_domain=a1a1
r0_key_lifetime=10000
r1_key_holder=000e8ecbfc48   #vap2 MAC without colon delimeters, yours will differ.
reassociation_deadline=1000
pmk_r1_push=1

#r0kh is vap1 MAC address, vap1 nas identifier, AES key
r0kh=00:0e:8e:7e:e2:71 000e8e7ee271 0f0e0d0c0b0a09080706050403020100

#r1kh is vap1 MAC address, vap1 r1 key holder MAC, AES key
r1kh=00:0e:8e:7e:e2:71 00:0e:8e:7e:e2:71 000102030405060708090a0b0c0d0e0f
```

full configuration file: hostapd_vap2.conf

If you wanted to add FT-PSK capability, add the following to the hostapd configuration file:

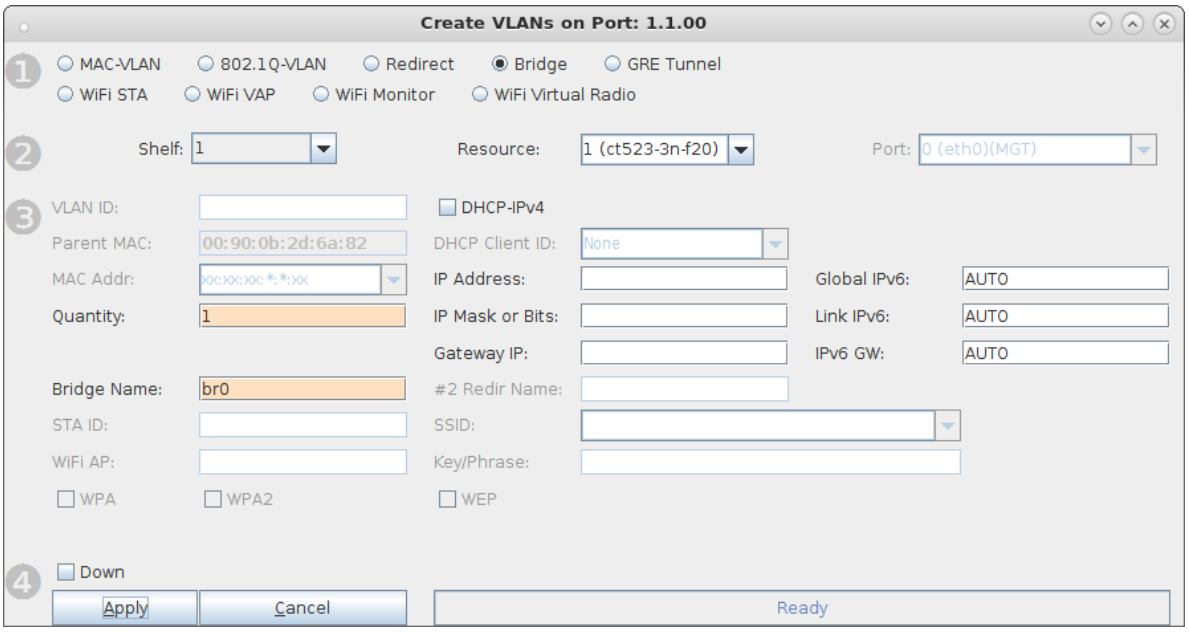
```
wpa_key_mgt=FT-EAP FT-PSK
wpa_passphrase=1234567890
```

In this example, we are configuring push mode key distribution where the master key holder, R0KH, derives the R1 key for all secondary key holders, R1KH, listed in the configuration file and sends it to them over the DS via bridge interfaces. The R0KH and R1KH entries must be configured for all virtual access points in the 802.11r network.

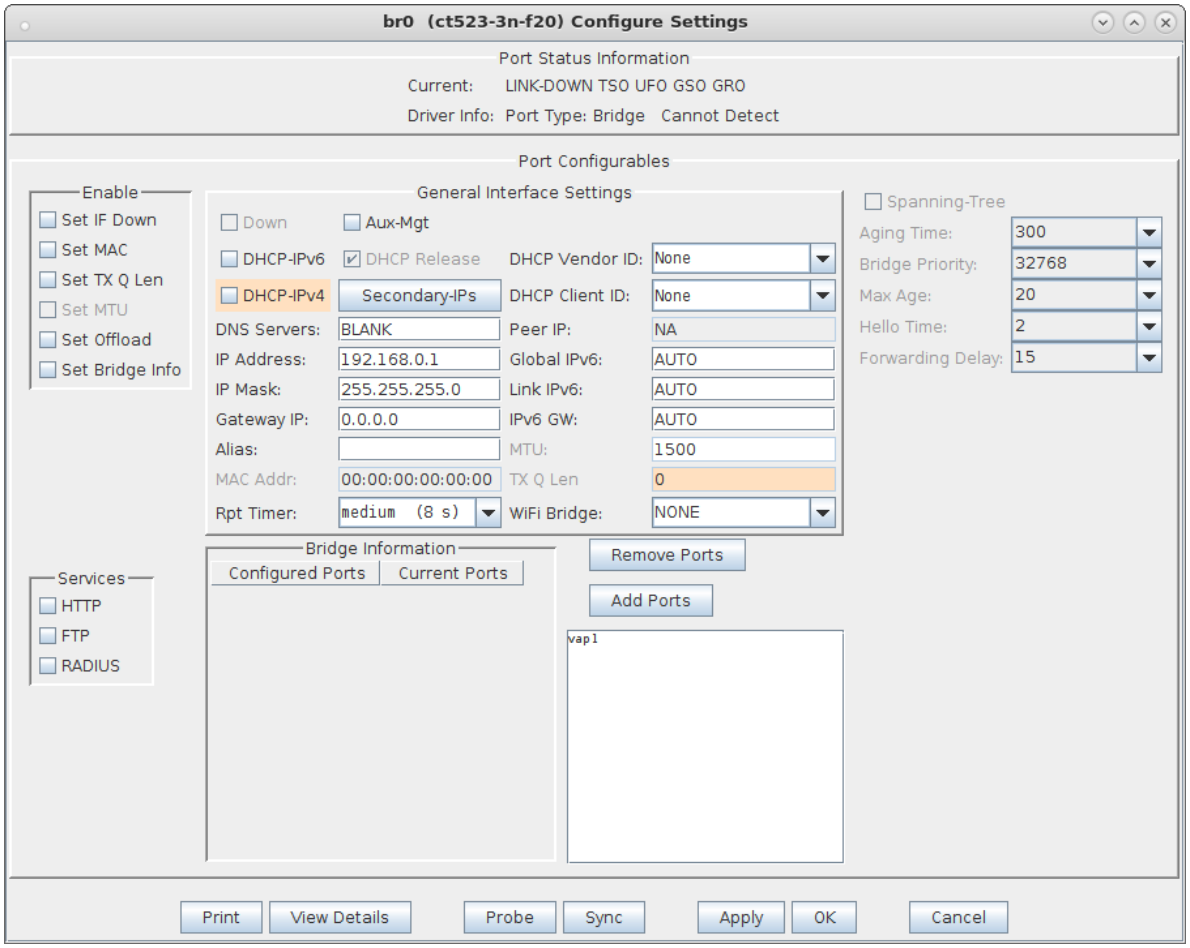
For more information on hostapd 802.11r configuration, see:
general hostapd configuration
https://www.w1.fi/cgit/hostap/plain/hostapd/hostapd.conf
how to enable wifi roaming
https://blog.fem.tu-ilmenau.de/archives/1002-HowTo-enable-WiFi-roaming-with-hostapd-and-VLANs.html
802.11r hostapd example
ftp://ftp.raspberry-pi-geek.com/pub/listings/rasp-pi-geek.com/04/AccessPoint/Listing04.txt

F. Repeat above steps A-E for vap2 on wiphy1.

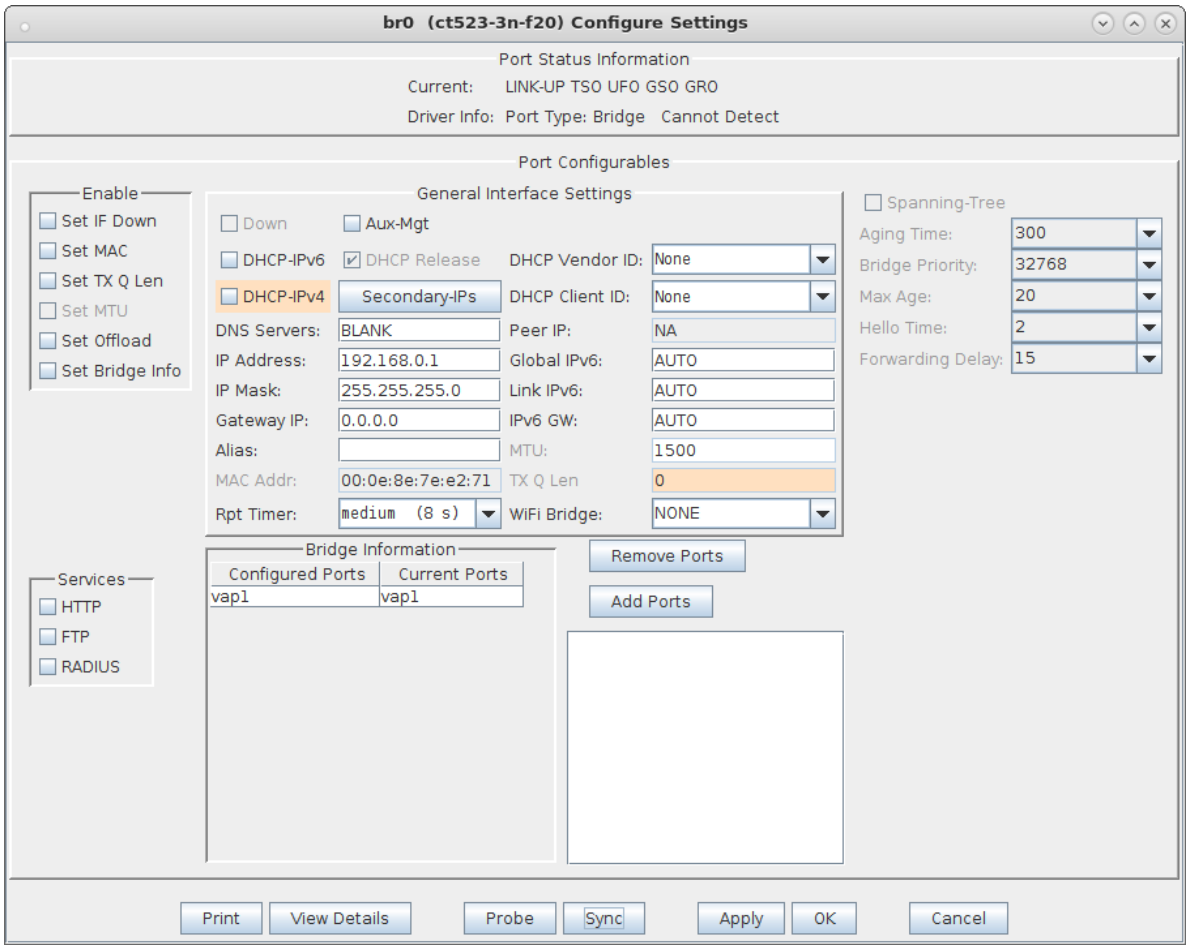
2. Create a bridge device for the first virtual access point, vap1. This bridge will be placed inside a virtual router so that it can serve DHCP requests and act as a RADIUS authentication server.
   A. Go to the port manager tab, select Create, then select Bridge and enter Quantity 1 and a Bridge Name, then Apply to create the bridge.



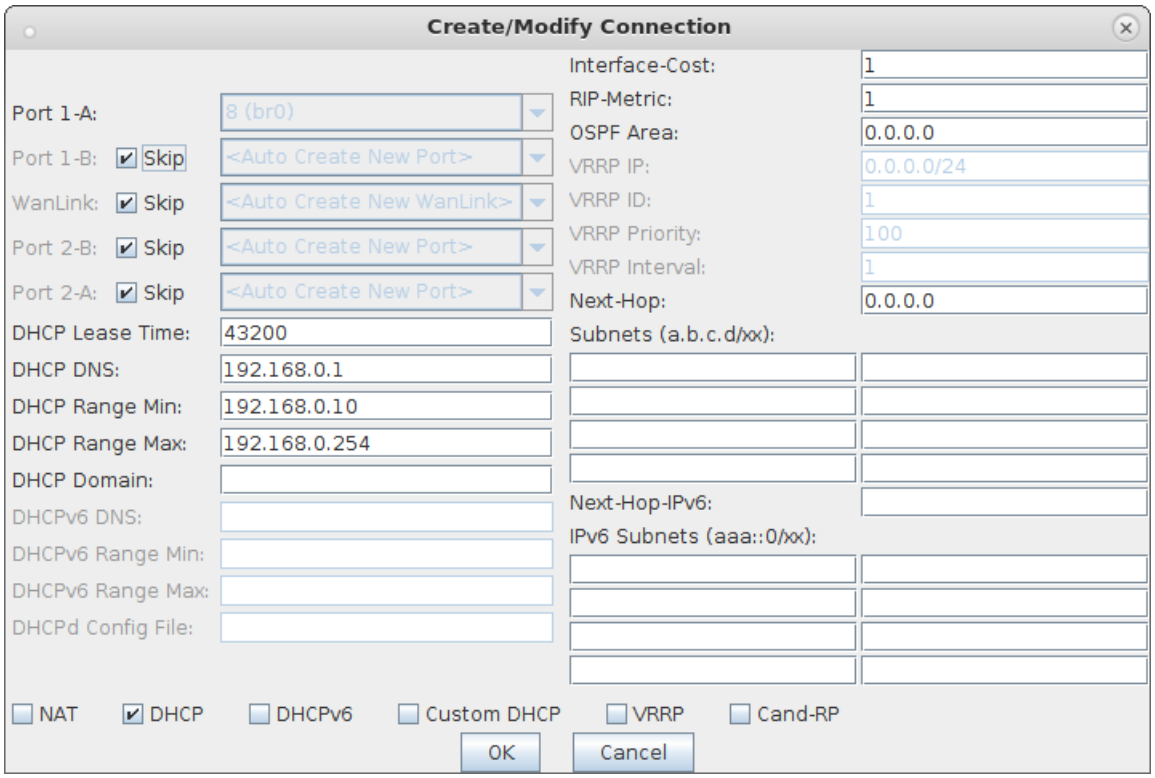
B. Modify the new bridge device to add vap1. Type vap1 in the text entry box, then select Add Ports, then select Apply.



C. Select Sync to verify vap1 is a configured and current bridge member.



D. Go to Netsmith, right-click the bridge and select Modify to add DHCP service. Select the DHCP checkbox at the bottom, then fill in the DHCP Lease Time, DHCP DNS, DHCP Range Min, DHCP Range Max and DHCP Domain if needed, then select OK.

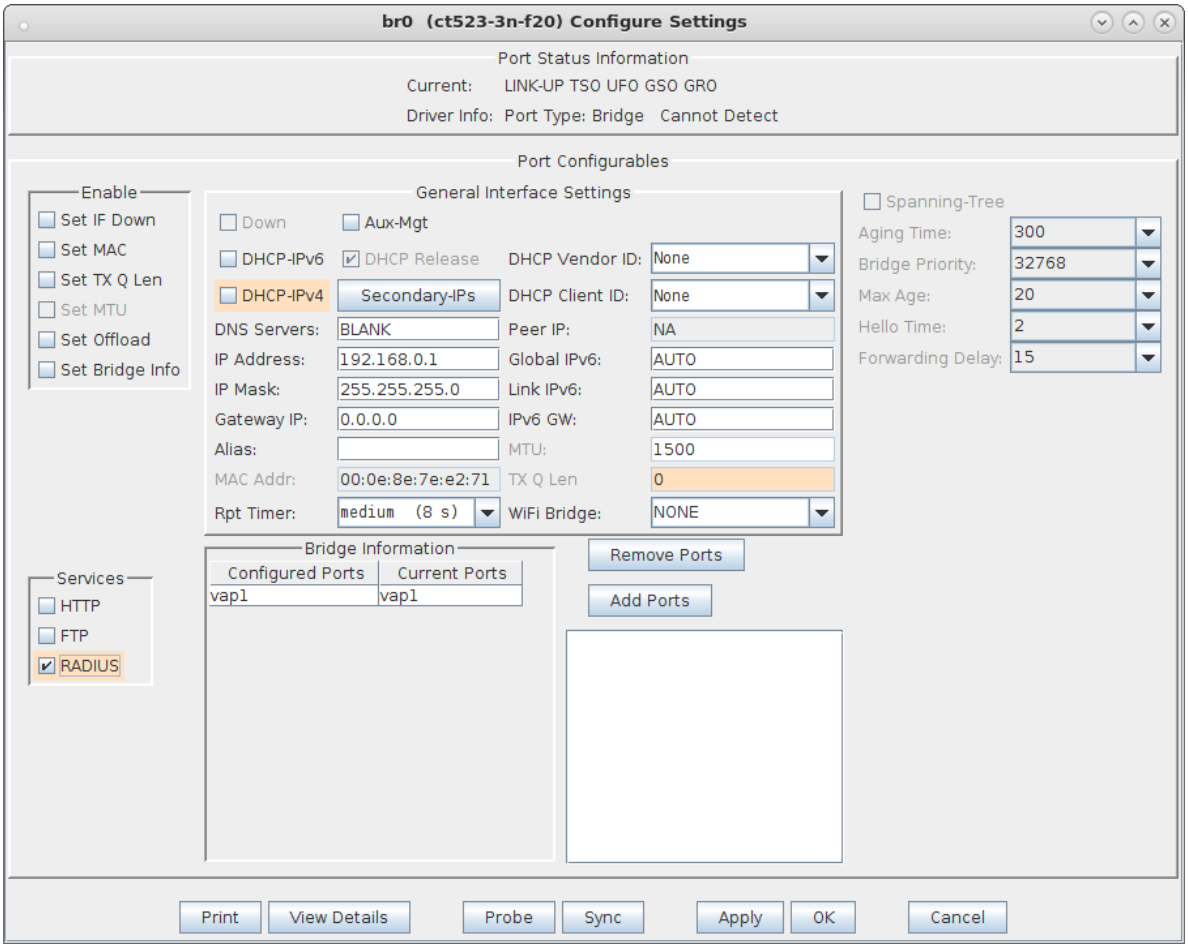


E. Go to Netsmith, right-click in a free area and select New Router and select OK. Then drag the bridge br0 into the virtual router and select Netsmith Apply.

For more information see Virtual Router with DHCP Cookbook (skip the wanlink portion)

3. Add a RADIUS server to the bridge device.
   A. Go to Netsmith, right-click the bridge and select Modify Port to add RADIUS service.

B. Select the RADIUS checkbox, then select OK.



C. Setup the following configuration files to start the RADIUS service. You will need to create these files, but the certificate files can be created by running the lf_kinstall script with the --do_radius option.

/etc/hostapd.radius_clients

```
0.0.0.0/0 lanforge
```

/etc/hostapd.eap_user

```
"dot11r.user" PEAP
"dot11r.user" MSCHAPV2 "!!dot11r123" [2]
```

/home/lanforge/wifi/hostapd_br0.conf

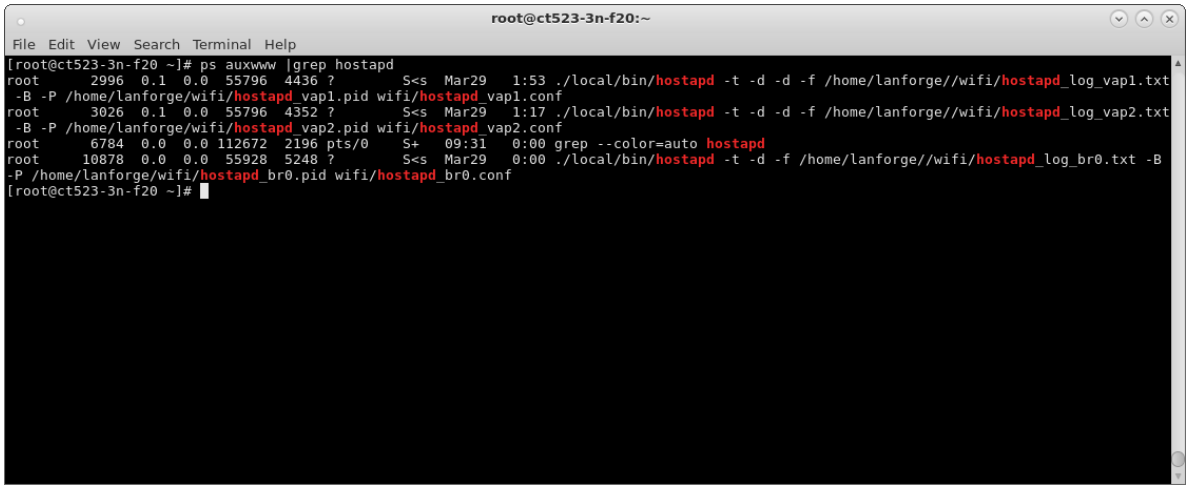
```
interface=br0
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/etc/hostapd.eap_user
server_id=ct523-3n-f20   #Your server_id will be different.
radius_server_auth_port=1812
radius_server_clients=/etc/hostapd.radius_clients

ca_cert=/etc/raddb/certs/ca.pem
server_cert=/etc/raddb/certs/server.pem
private_key=/etc/raddb/certs/server.key
private_key_passwd=lanforge
```

D. Verify that there are three hostapd processes running with the command:

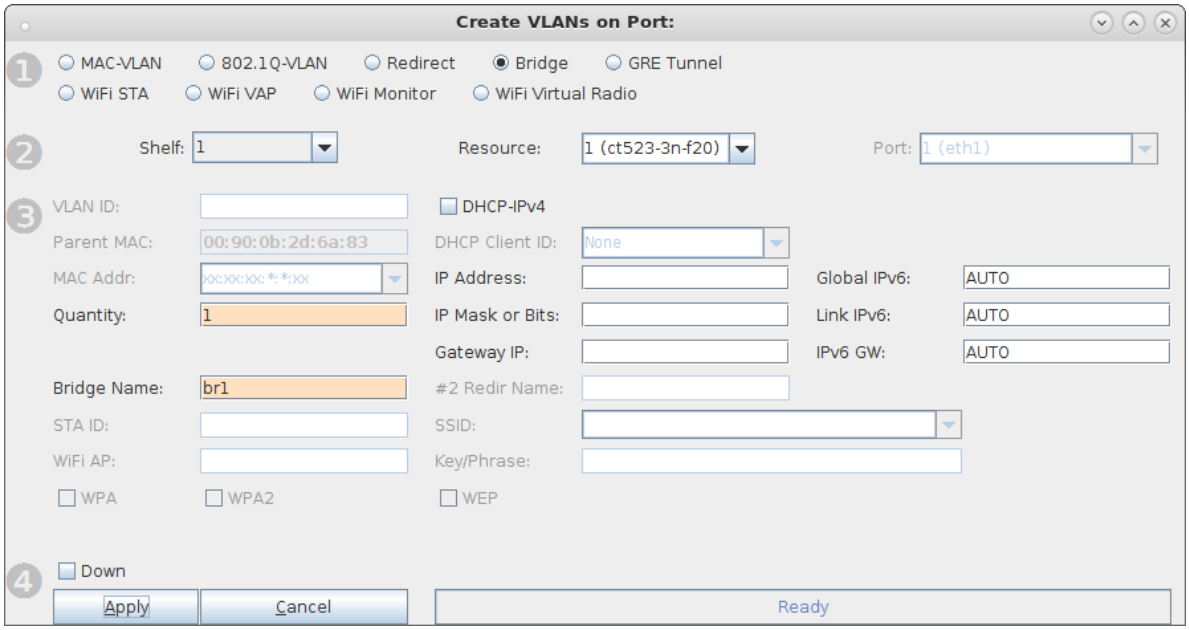
```
ps auxwww |grep hostapd
```

which should show something similar to the following:

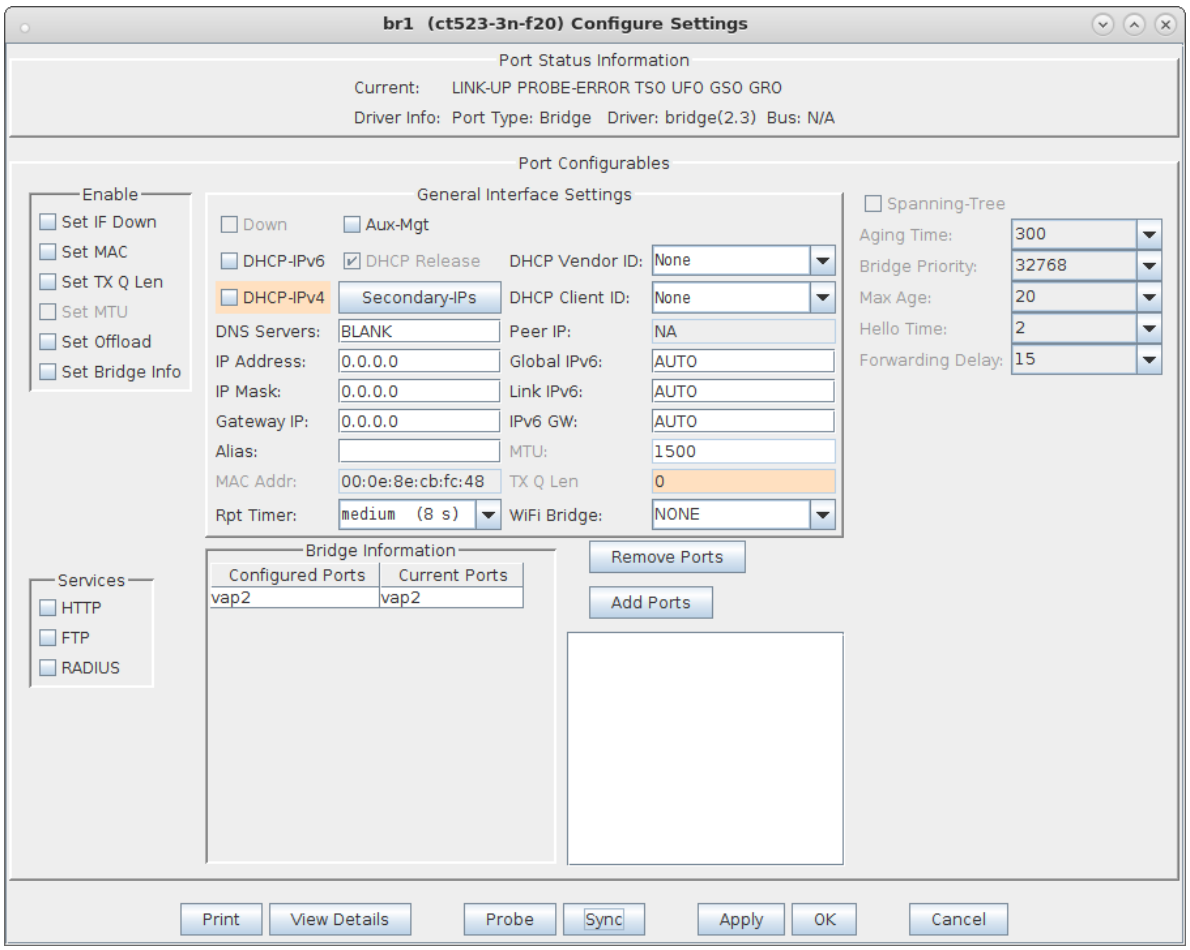


4. Create a second bridge device for the second virtual access point, vap2.
Each vap in the 802.11r network requires its own bridge so that the bridge device receive logic can correctly process packets from each vap during fast-transition client roaming.

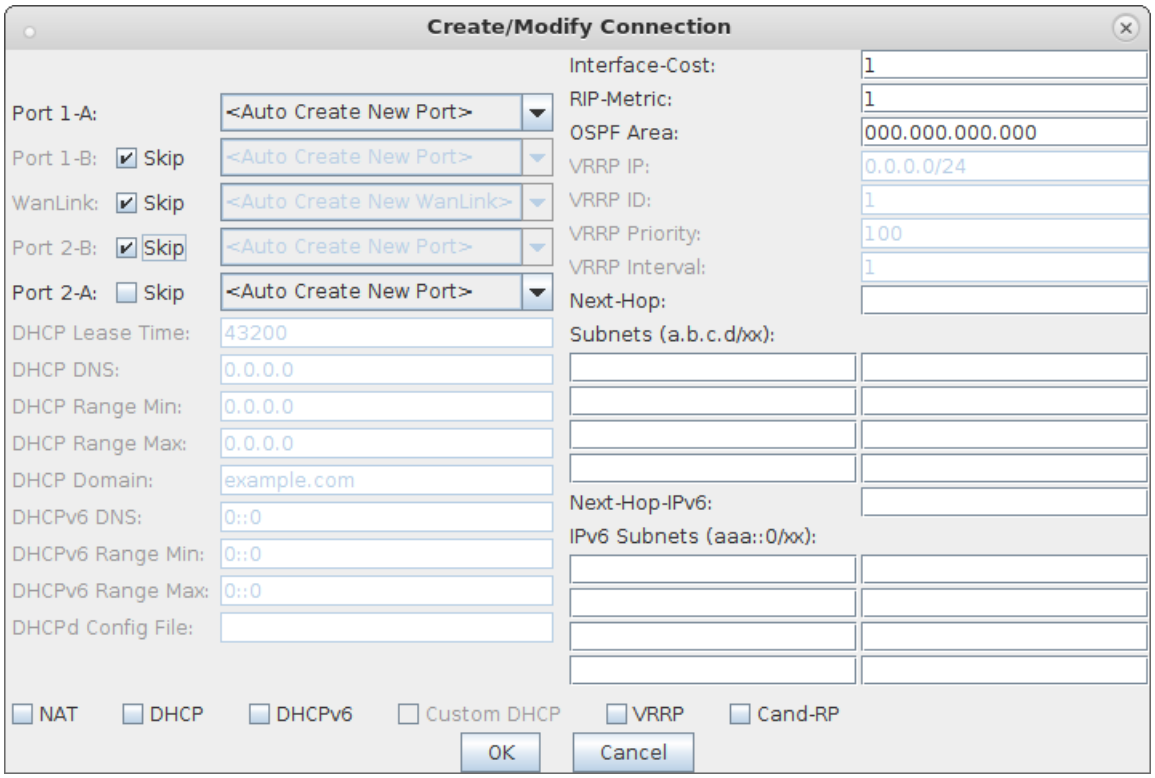
A. Go to Netsmith, right-click in a free area, select New Bridge, enter Quantity 1 and a Bridge Name, then select Apply. Sync Netsmith to view the new bridge.



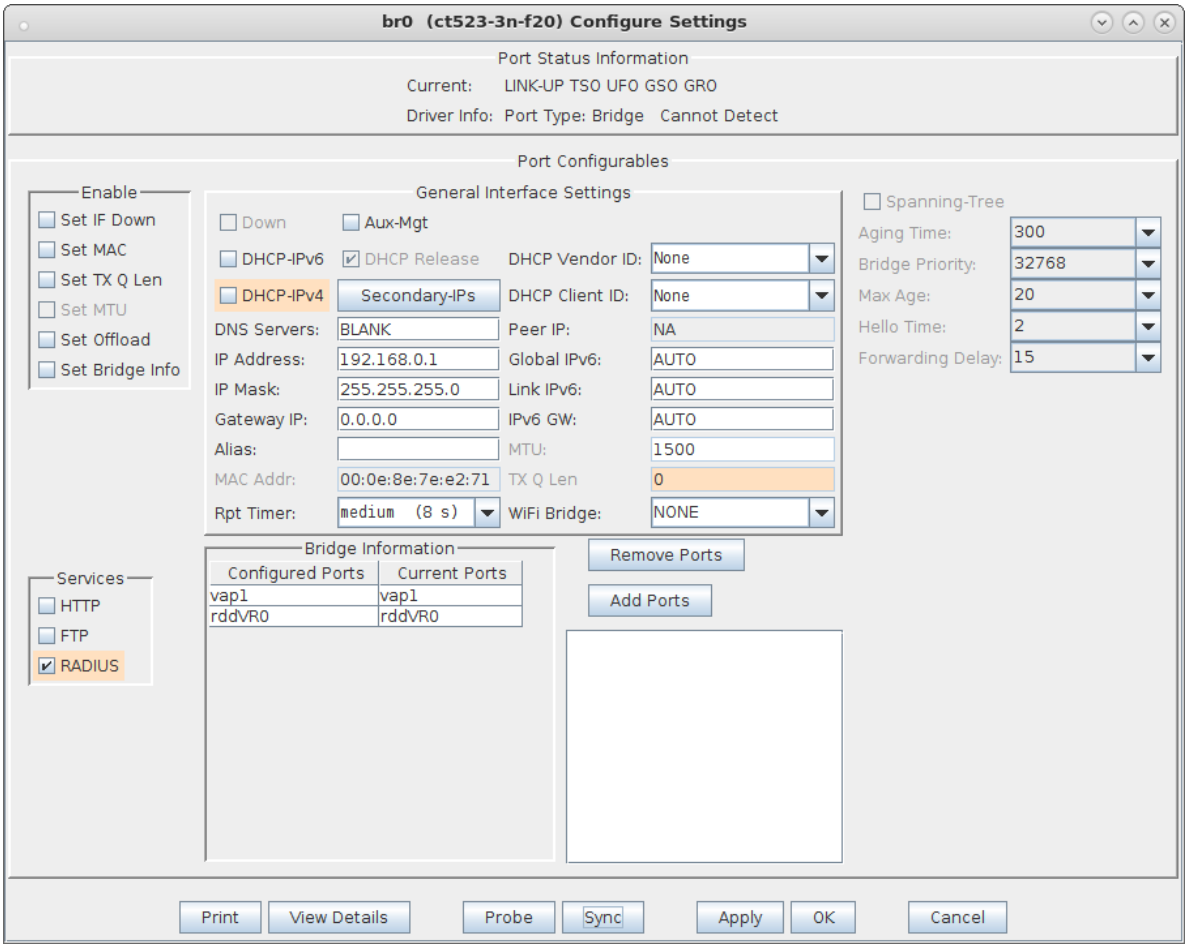
B. Right-click the new bridge and select Modify Port to add vap2 as a bridge member.



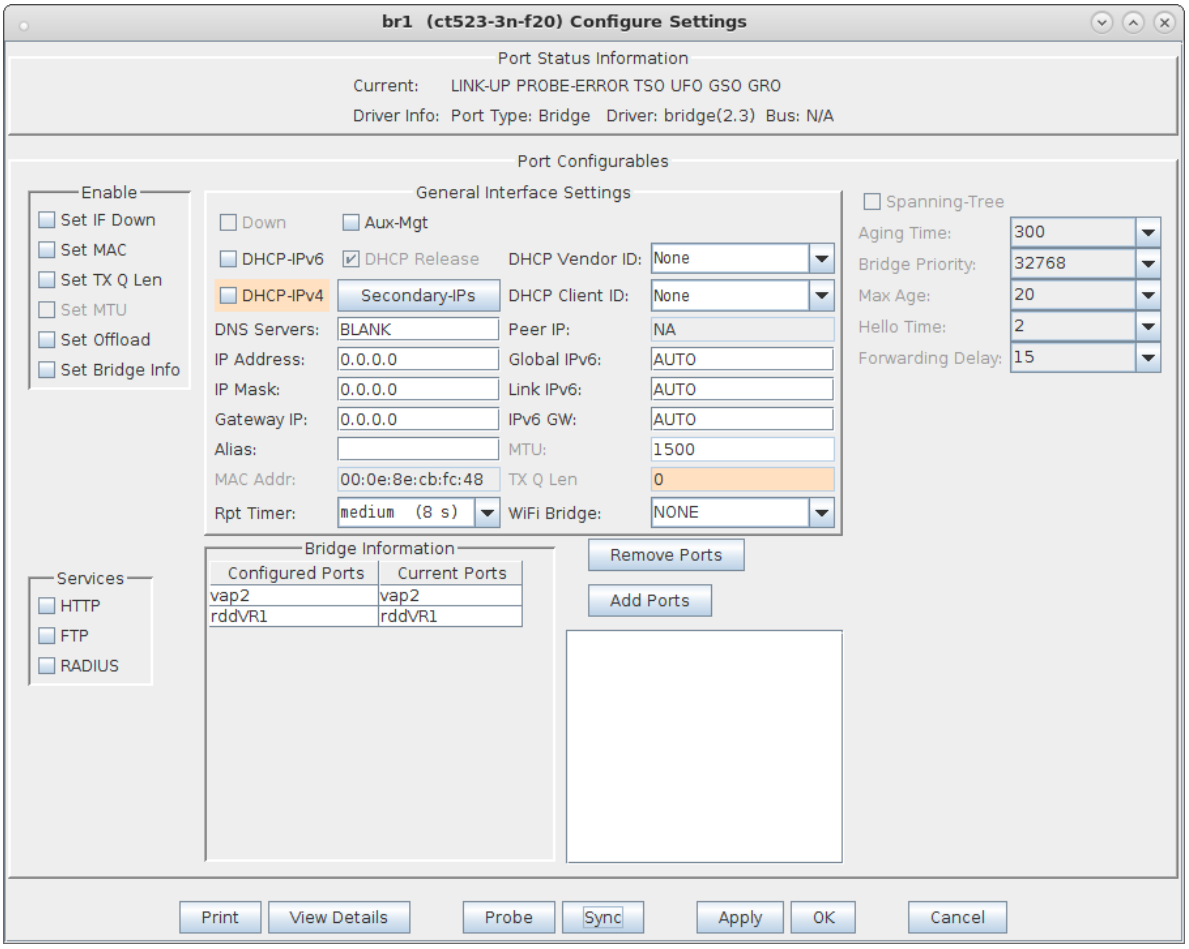
5. Each bridge will share a connection to a redirect device (rdd) pair so that FT messages can be sent and received.
   A. In Netsmith, right-click in a free area and select New Connection to create an rdd pair. Select **Skip** for Port 1-B, WanLink and Port 2-B then select OK. Select Netsmith Apply after creating the new connection.



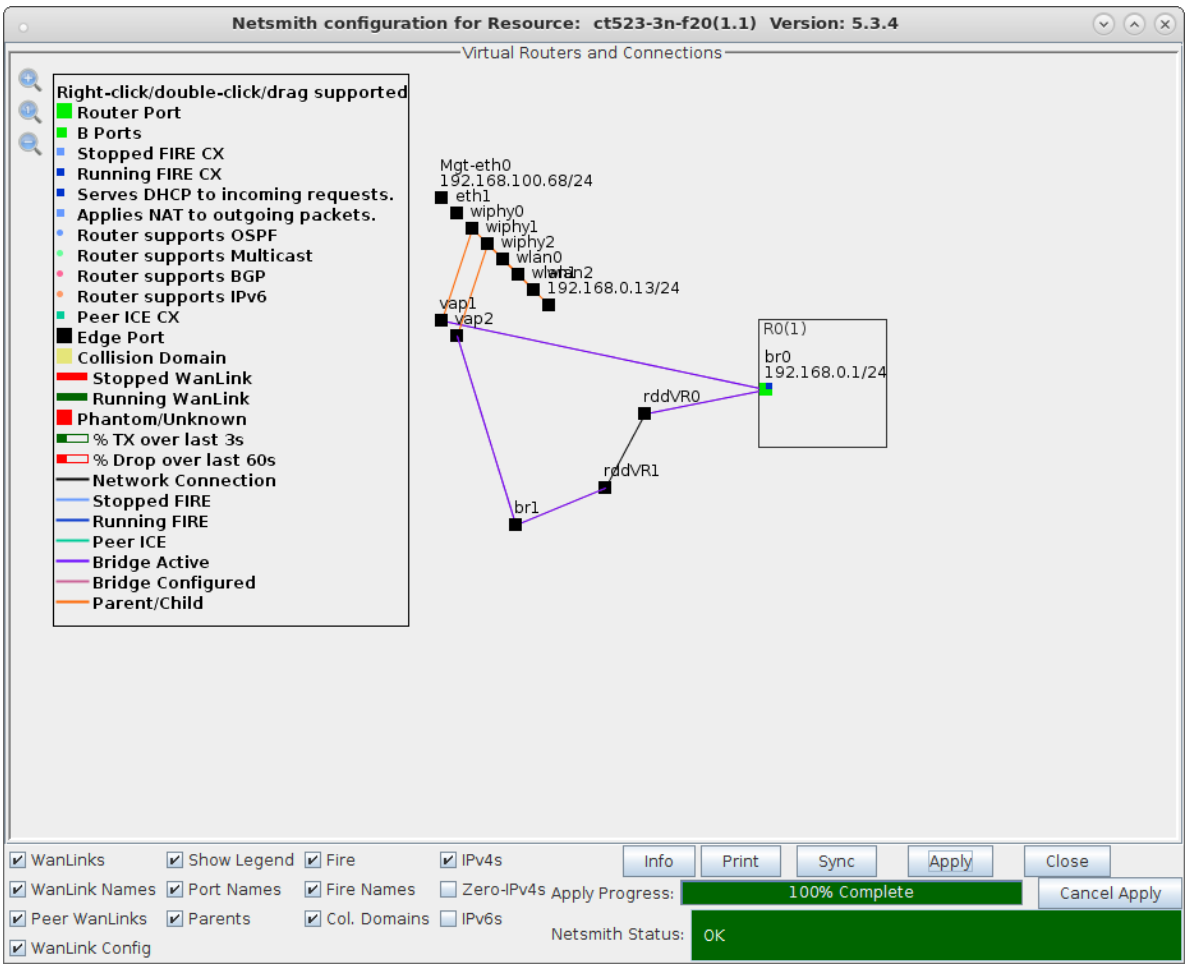
B. Right-click and select Modify Port br0, then add rddVR0 to br0, select Add Ports then select Apply. Your rddVRX numbering may differ depending on what other Netsmith objects are created.



C. Right-click and select Modify Port br1, then add rddVR1 to br1, select Add Ports then select Apply. Your rddVRX numbering may differ depending on what other Netsmith objects are created.

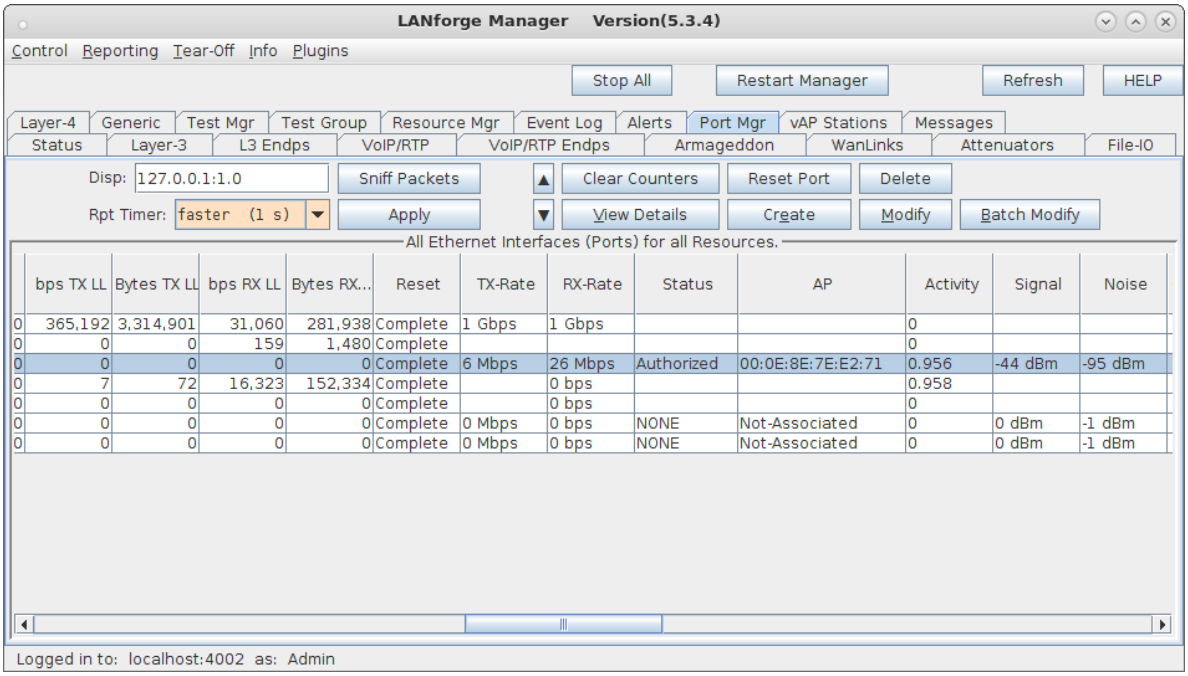


D. The final Netsmith display should show the two bridged virtual access points connected by a rdd pair

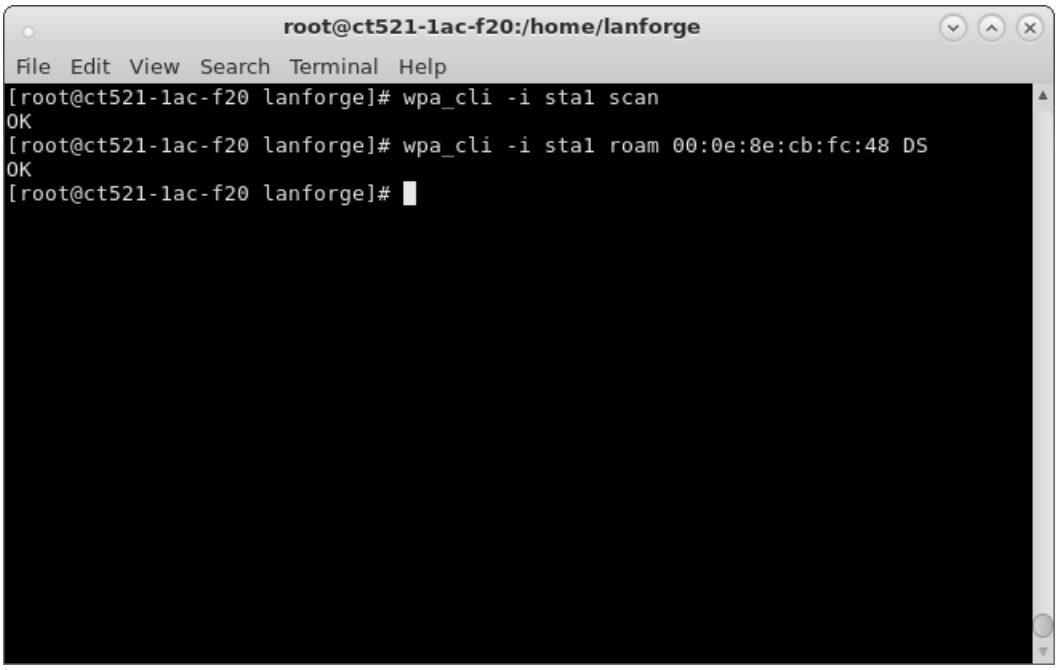


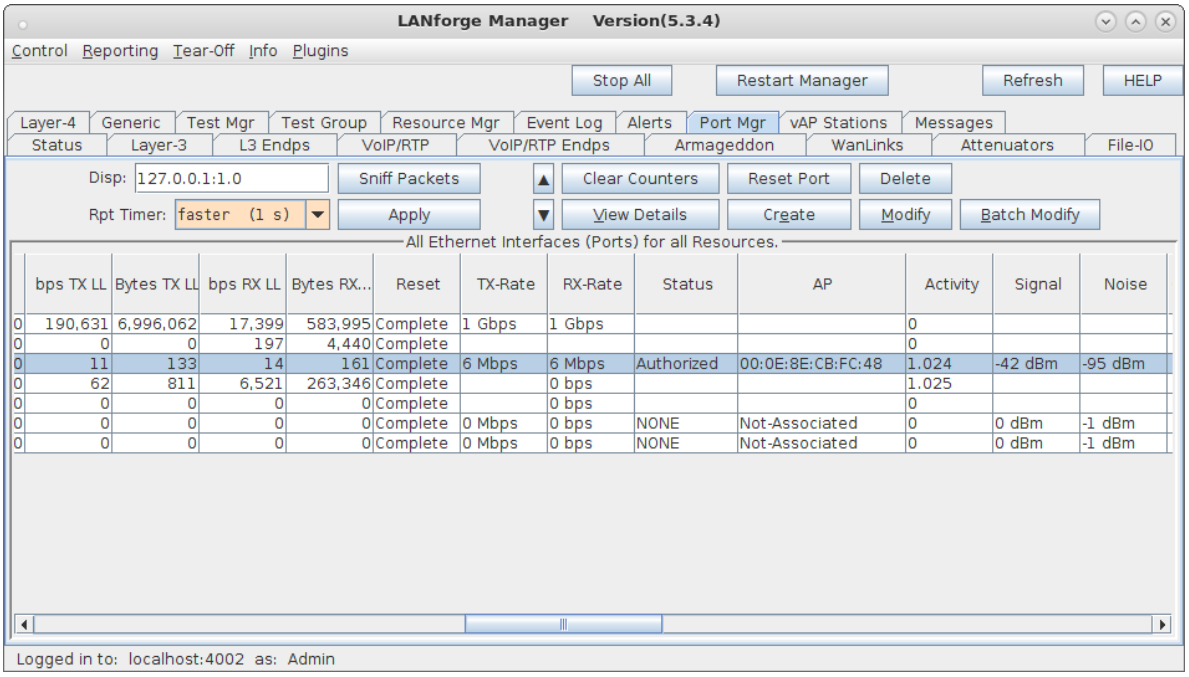
6. Connect clients and force them to roam from vap to vap. This can be accomplished with a wpa_cli command for one or two clients or the Mobility Plugin Script for many clients. If the system under test is not able to force a roam, a variable attenuator on each vap radio may help induce a client to roam as the signal strength from vap to vap is varied.

A. Client connected to vap1.

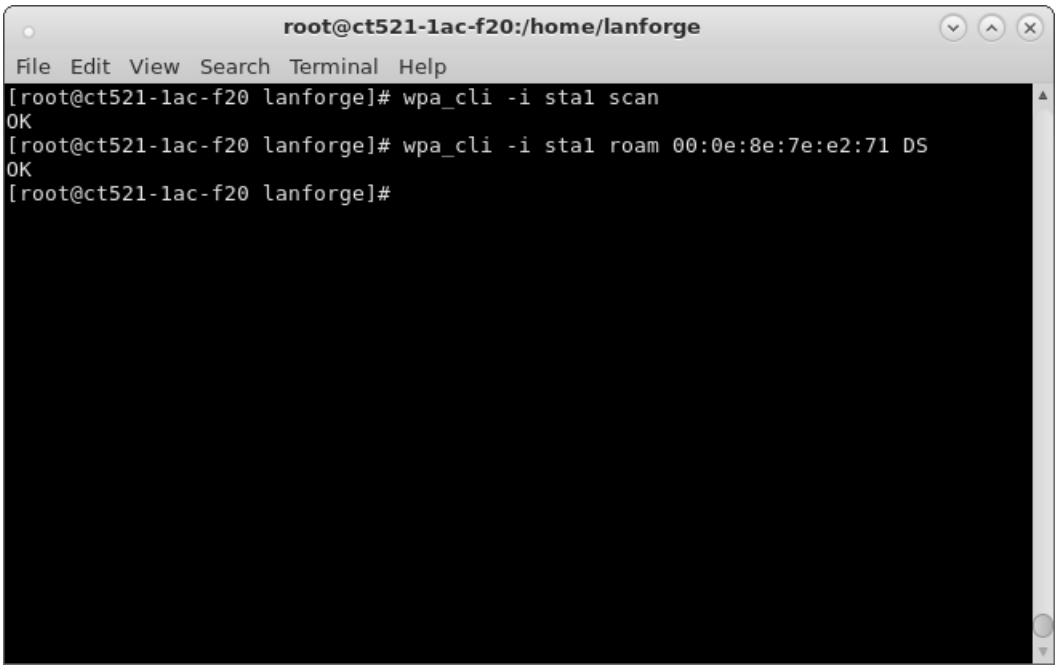


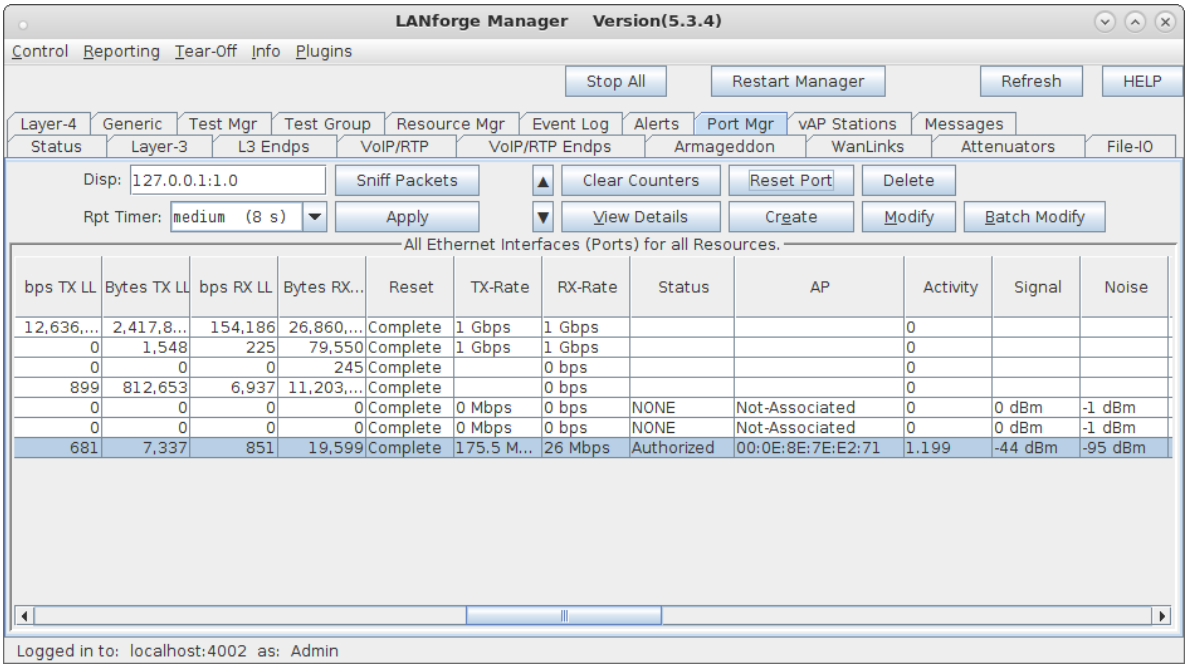
B. Client roams to vap2.



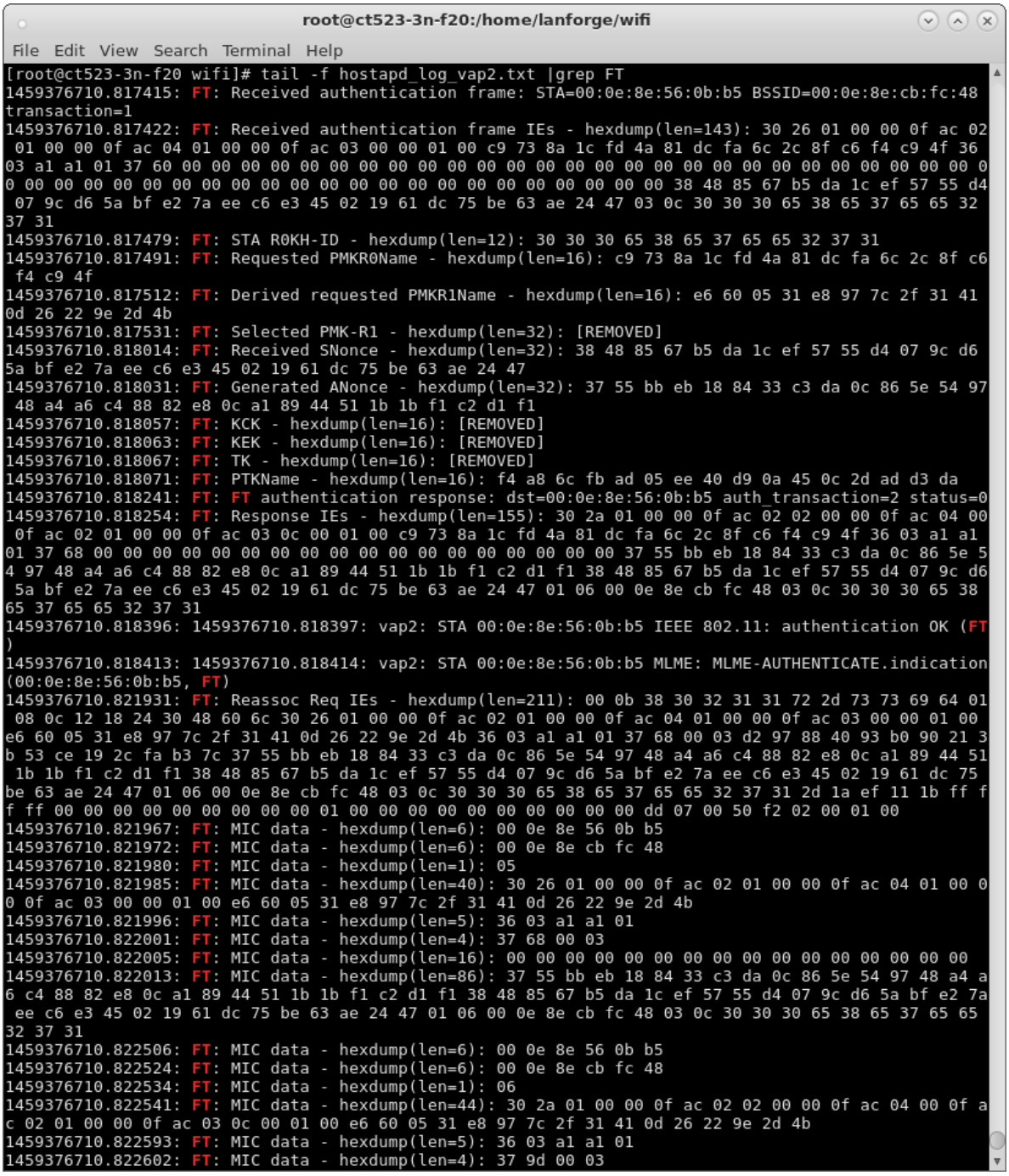


C. Client roams back to vap1.

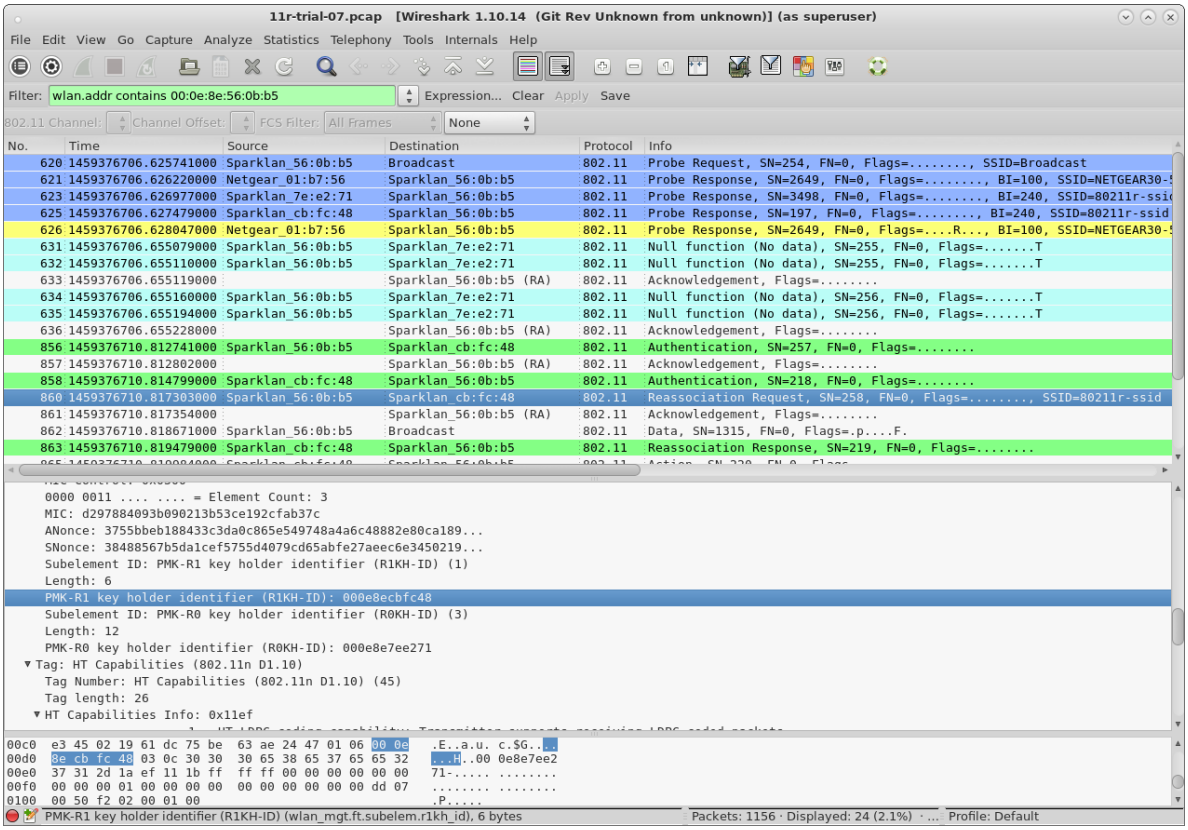




D. FT messaging in hostapd logs.



E. A wireless capture of over-the-air packets shows the transition.



F. Output graph of the Mobility Plugin script of several roaming stations.