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

Wifi Roaming with Opportunistic Key Caching (OKC)

Goal: Show how LANforge can emulate an OKC VAP or OKC STA then observe the different results when OKC is enabled or not.
Opportunistic Key Caching (OKC) is a fast roaming solution that is one predecessor to 802.11r Fast BSS Transition. OKC is also referred to as Proactive Key Caching (PKC). Here we will demonstrate the following four scenarios with OKC:

1. OKC on VAP and NOT on STA
2. OKC on both VAP and STA
3. OKC disabled on both VAP and STA
4. OKC disabled on VAP but enabled on STA

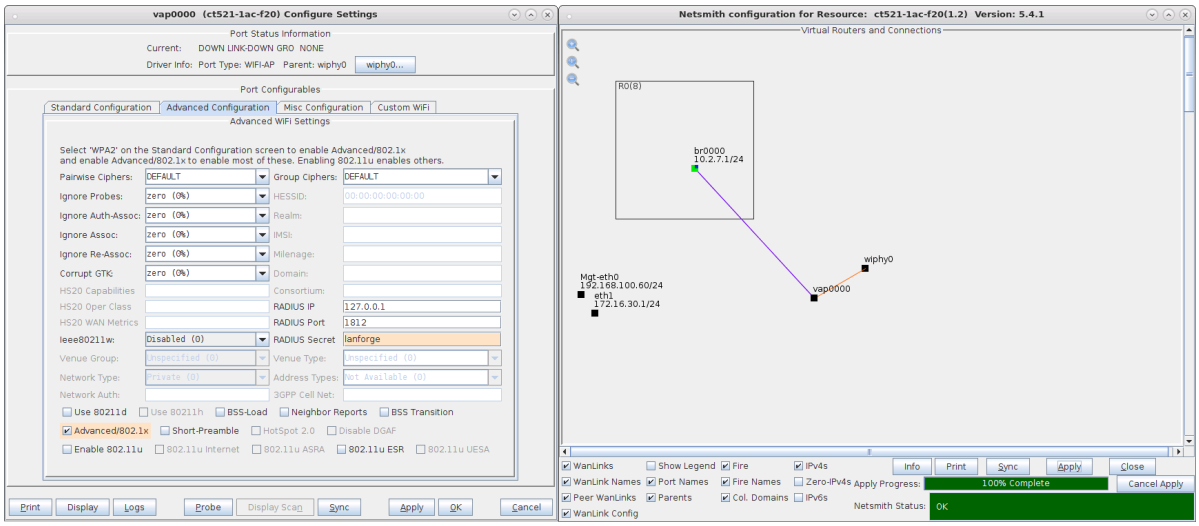
OKC Scenarios

OKC On VAP Only

STA roam result: Full RADIUS authentication plus 4-way handshake.

Using OKC on a VAP requires setting up a custom configuration file in LANforge to utilize the Multiple BSSID feature. In this scenario, the STA is not configured to use OKC and must do a full RADIUS authentication plus 4-way handshake when roaming to the next BSSID.

1. Setup a VAP using RADIUS and EAP-TTLS with a bridge in a virtual router.
   See Setting up a RADIUS Server for help with this step.



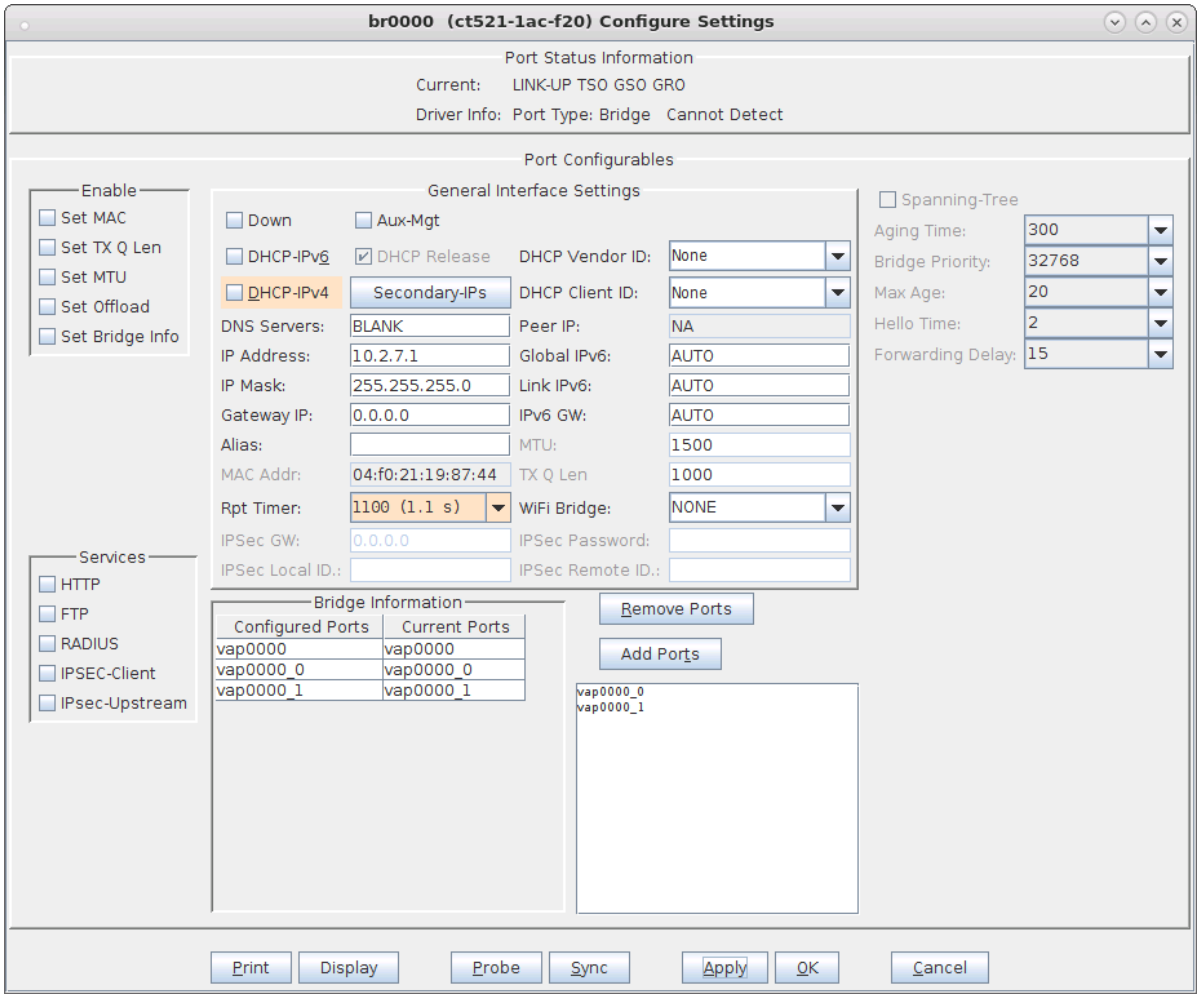
2. Add the following to the custom config section which will create two BSSIDs on the same hostapd process which is required for OKC to work on hostapd:

```
bss=vap0000_0
ssid=okctest1
bssid=04:f0:21:19:88:44
ieee8021x=1
own_ip_addr=127.0.0.1
auth_server_addr=127.0.0.1
auth_server_port=1812
auth_server_shared_secret=lanforge
wpa=2
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
wpa_key_mgmt=WPA-EAP WPA-EAP-SHA256
```

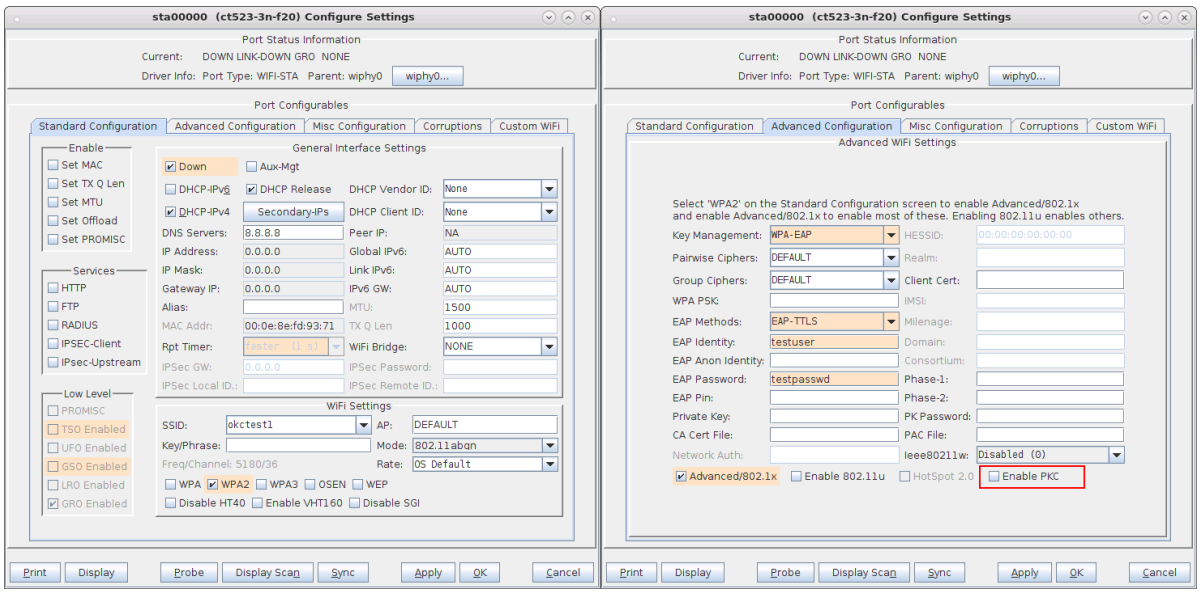
```
bss_load_update_period=100
chan_util_avg_period=600
rrm_neighbor_report=1
rrm_beacon_report=1
bss_transition=1
okc=1

bss=vap0000_1
ssid=okctest1
bssid=04:f0:21:19:89:44
ieee8021x=1
own_ip_addr=127.0.0.1
auth_server_addr=127.0.0.1
auth_server_port=1812
auth_server_shared_secret=lanforge
wpa=2
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
wpa_key_mgmt=WPA-EAP WPA-EAP-SHA256
bss_load_update_period=100
chan_util_avg_period=600
rrm_neighbor_report=1
rrm_beacon_report=1
bss_transition=1
okc=1
```

3. Reset the VAP to use the new configuration.
4. Modify the bridge to use the two new sub interfaces vap0000_0 and vap0000_1.



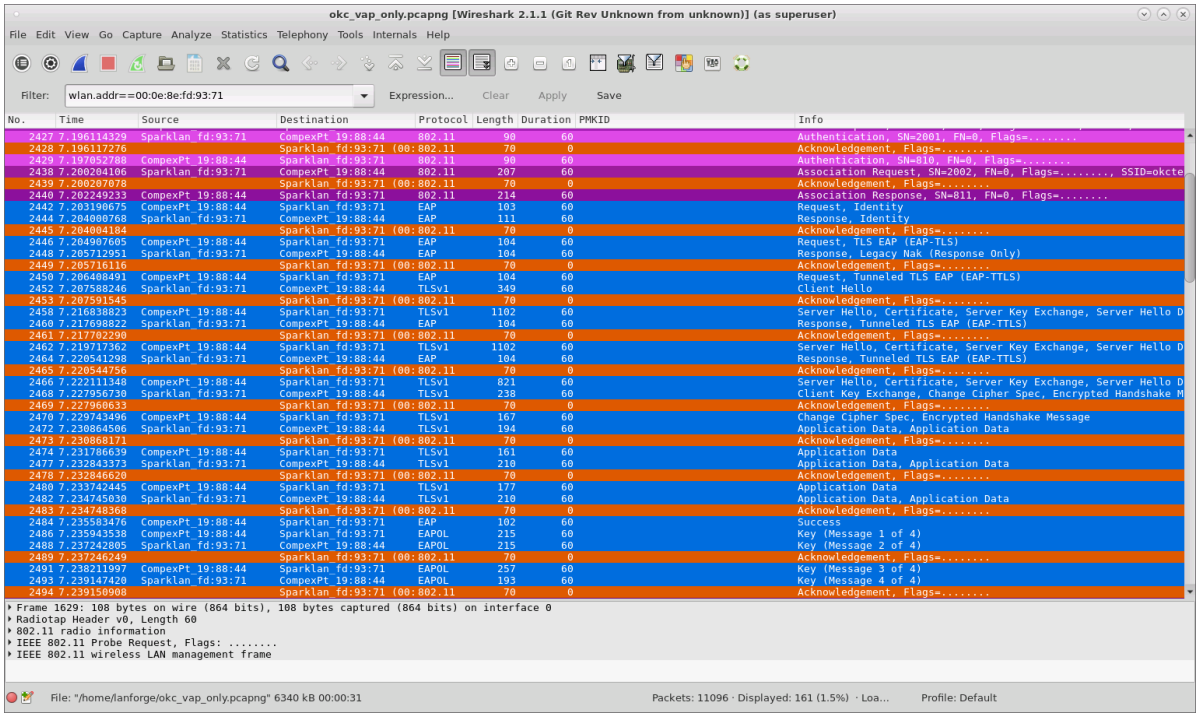
5. Modify a STA so that it is configured to connect to the SSID with 802.1X authentication for EAP-TTLS and with PKC disabled.



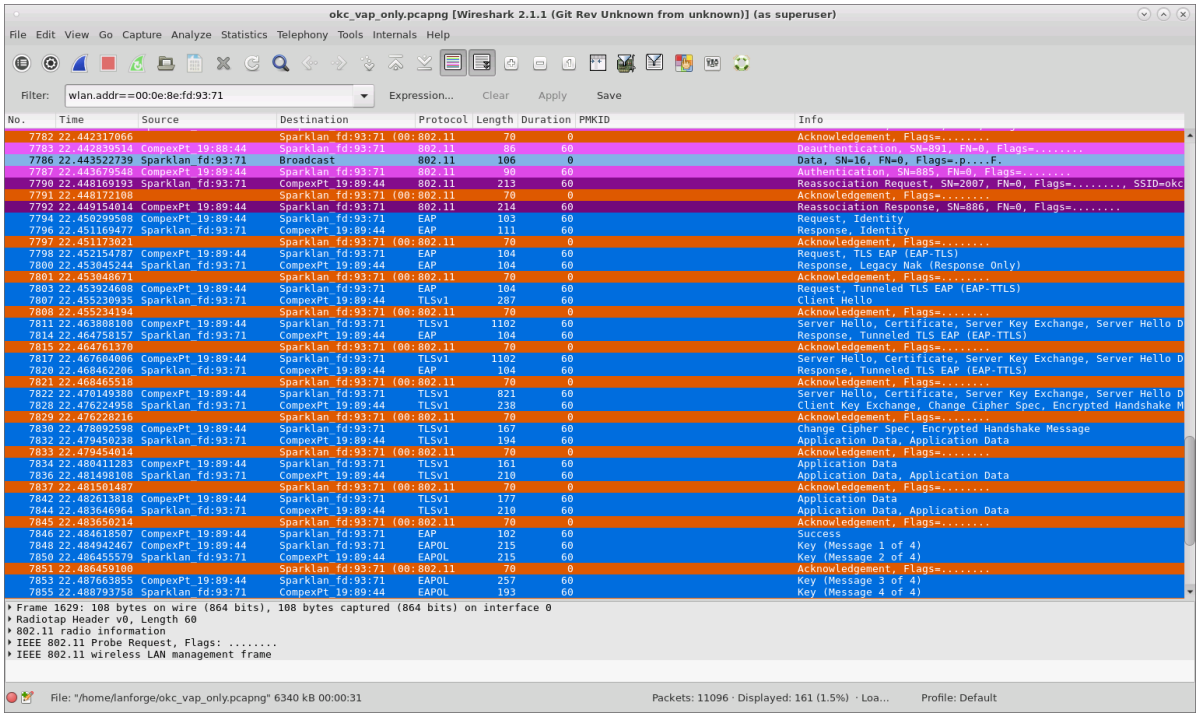
6. Start a packet capture then admin the STA up.
7. Use `wpa_cli` to force the STA to roam with the following terminal commands:

```
# cd /home/lanforge
# . lanforge.profile
# wpa_cli -i sta00000 scan
# wpa_cli -i sta00000 roam <next BSSID>
```

8. In the packet capture, the initial RADIUS authentication and 4-way handshake are shown:



9. Then the STA sends a Reassociation Request which is missing the PMKID and another full RADIUS authentication and 4-way handshake take place to associate to the new BSSID.

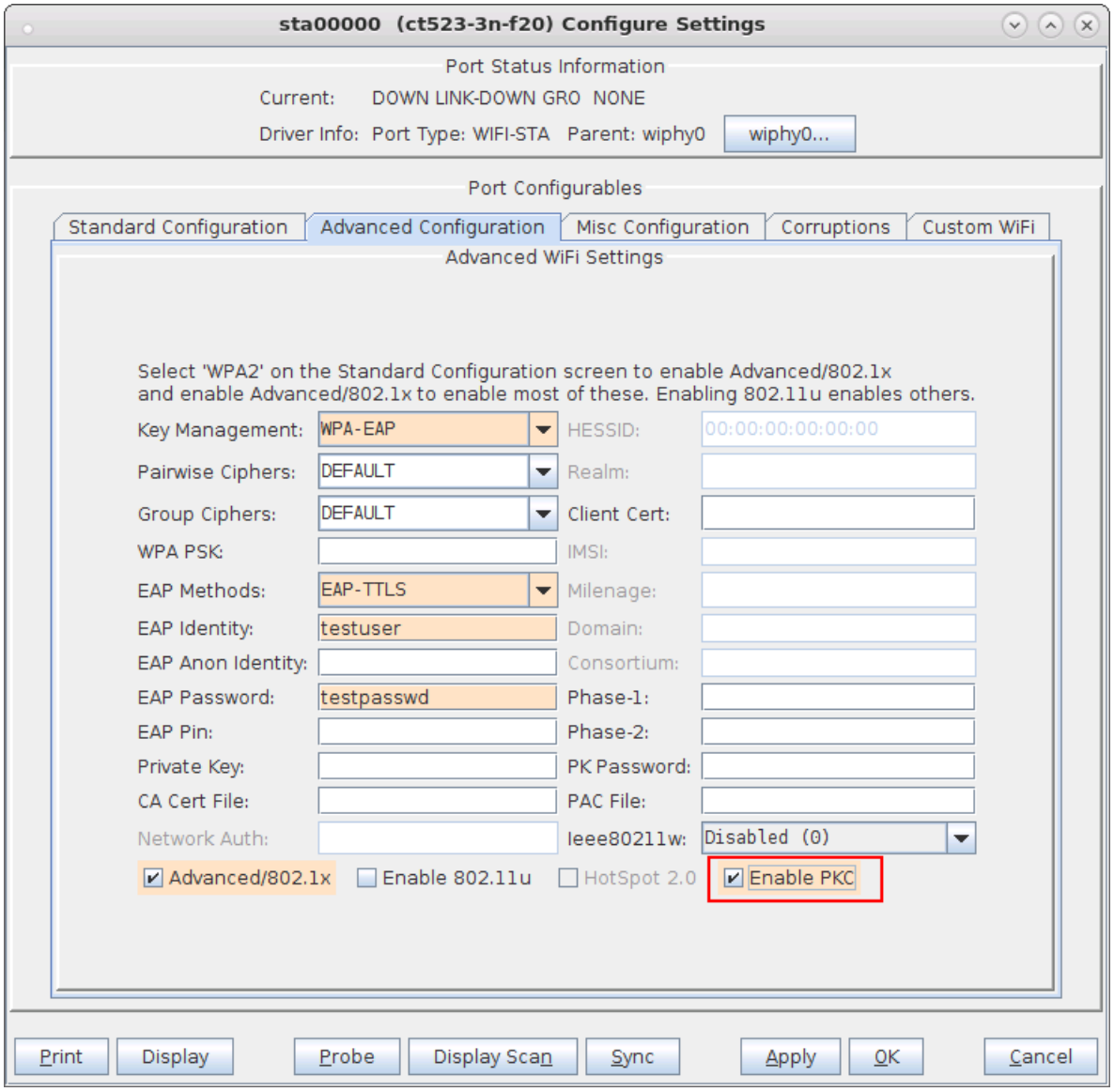


OKC On Both VAP and STA

STA roam result: PMKID is sent, then only 4-way handshake is required.

When both VAP and STA are using OKC, the STA sends its calculated PMKID in the Reassociation Request to the target AP which means the full RADIUS is not needed and only a 4-way handshake is sufficient to connect to the new VAP.

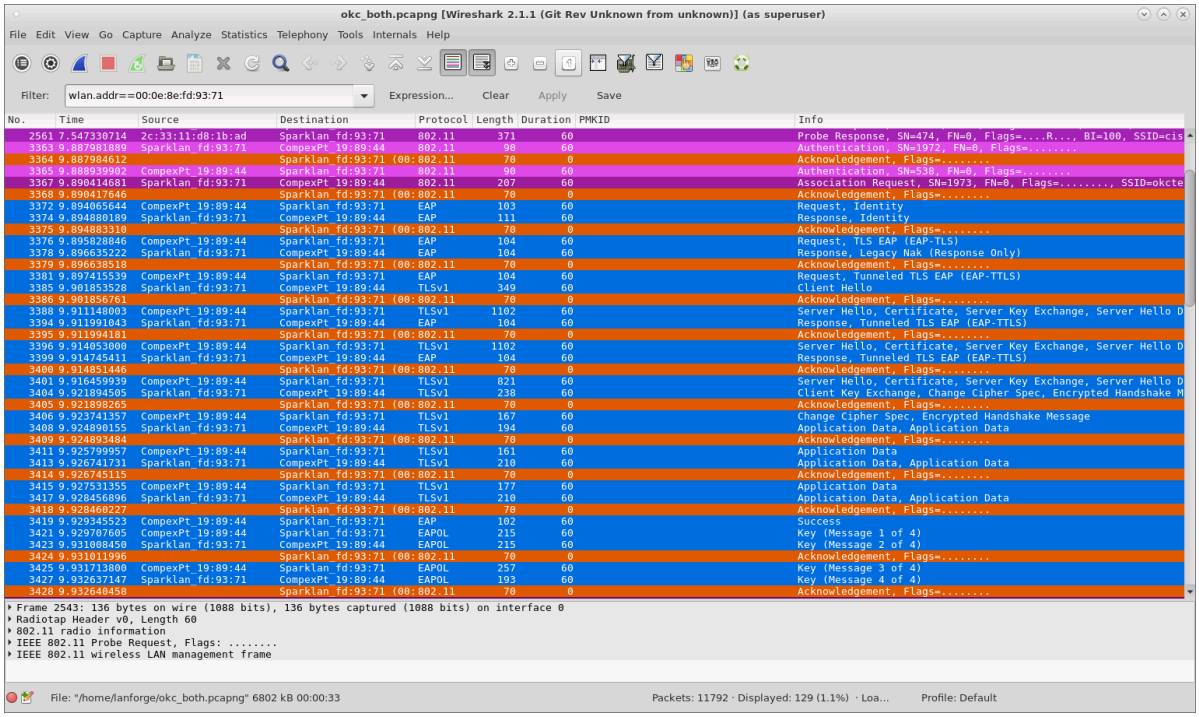
1. Admin the STA down , then modify the STA to enable PKC



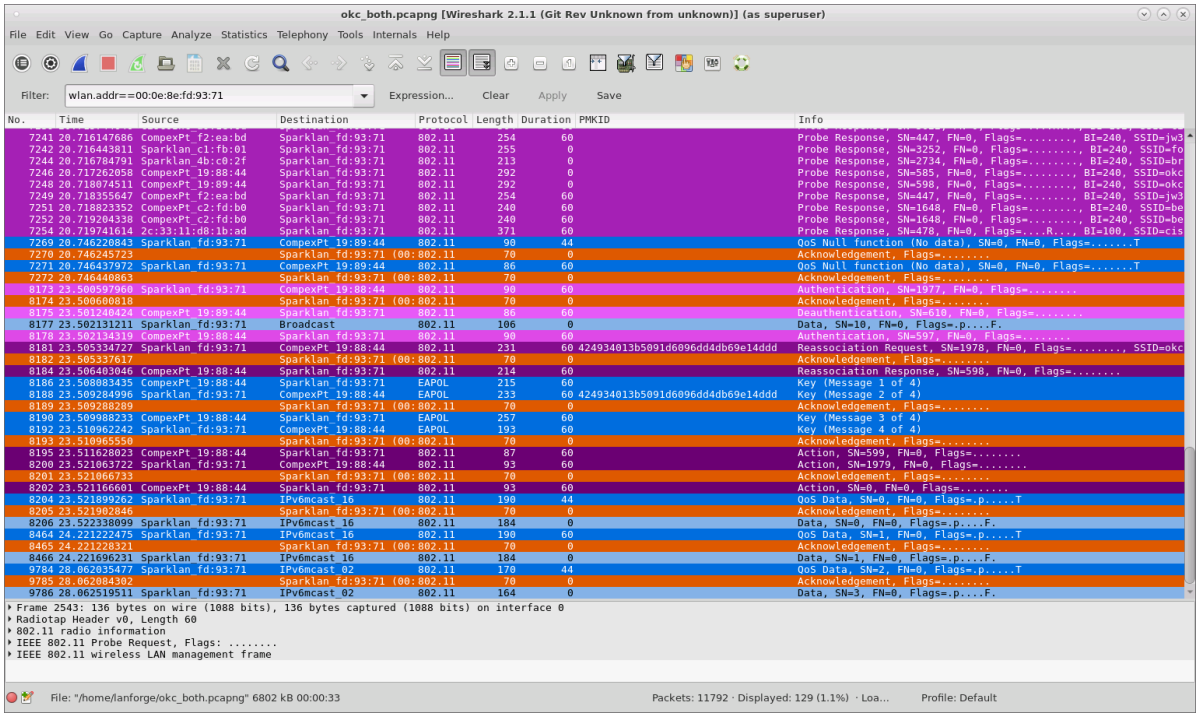
2. Start a packet capture then admin the STA up.
3. Use `wpa_cli` to force the STA to roam with the following terminal commands:

```
# wpa_cli -i sta00000 scan
# wpa_cli -i sta00000 roam <next BSSID>
```

4. In the packet capture, the initial RADIUS authentication and 4-way handshake are shown:



5. Then the STA sends a Reassociation Request which includes its PMKID and only the 4-way handshake is required to associate to the new BSSID.



OKC Disabled On VAP and STA

STA roam result: Full RADIUS authentication plus 4-way handshake.

Because neither is using OKC, a full RADIUS authentication plus 4-way handshake is required when the STA roams to the new VAP.

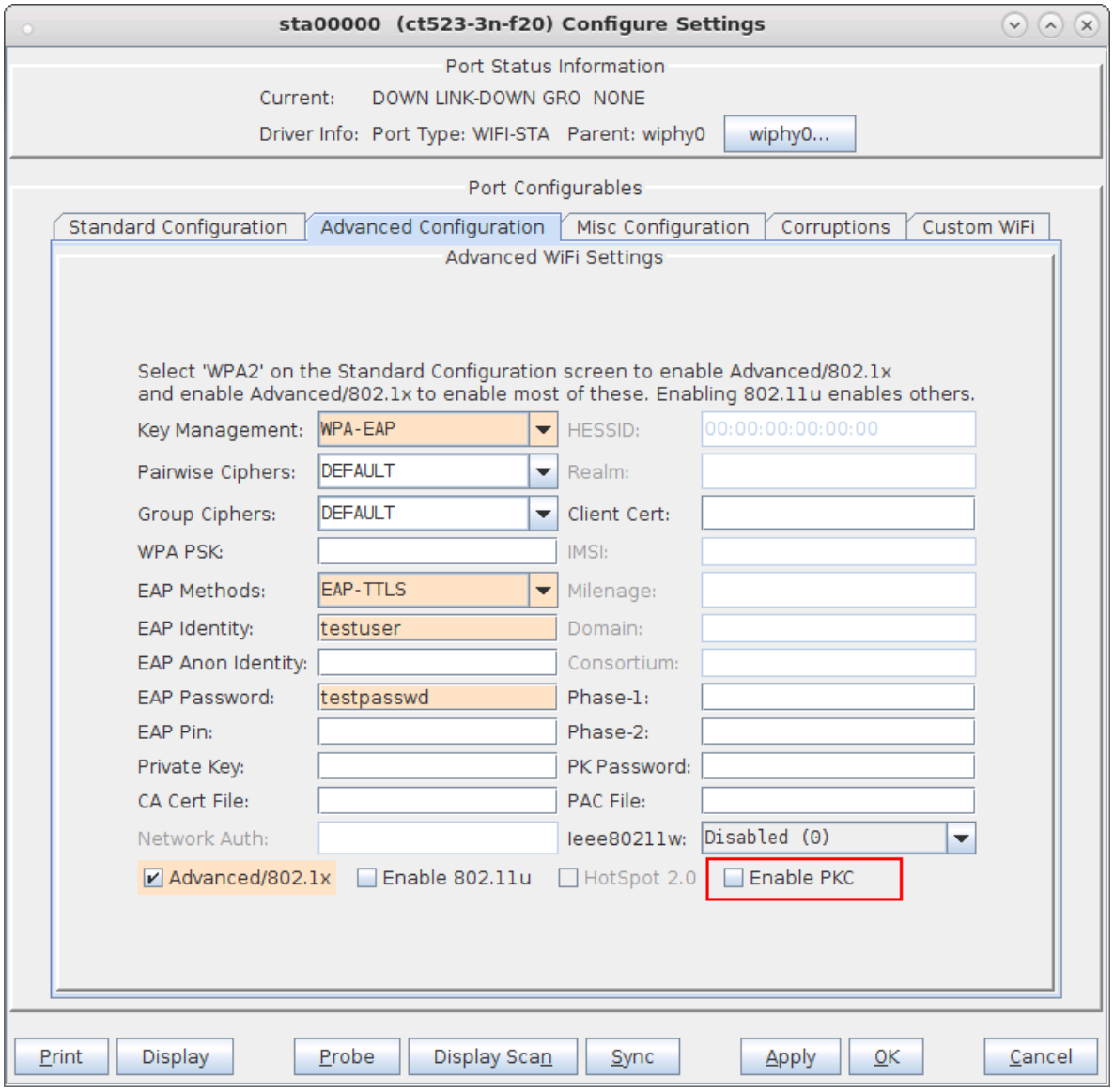
1. To disable OKC on the VAP, comment out the okc=1 lines in the VAP custom configuration, then reset the VAP.

```
bss=vap0000_0
ssid=okctest1
bssid=04:f0:21:19:88:44
ieee8021x=1
own_ip_addr=127.0.0.1
auth_server_addr=127.0.0.1
```

```
auth_server_port=1812
auth_server_shared_secret=lanforge
wpa=2
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
wpa_key_mgmt=WPA-EAP WPA-EAP-SHA256
bss_load_update_period=100
chan_util_avg_period=600
rrm_neighbor_report=1
rrm_beacon_report=1
bss_transition=1
#okc=1

bss=vap0000_1
ssid=okctest1
bssid=04:f0:21:19:89:44
ieee8021x=1
own_ip_addr=127.0.0.1
auth_server_addr=127.0.0.1
auth_server_port=1812
auth_server_shared_secret=lanforge
wpa=2
wpa_pairwise=TKIP CCMP
rsn_pairwise=CCMP
wpa_key_mgmt=WPA-EAP WPA-EAP-SHA256
bss_load_update_period=100
chan_util_avg_period=600
rrm_neighbor_report=1
rrm_beacon_report=1
bss_transition=1
#okc=1
```

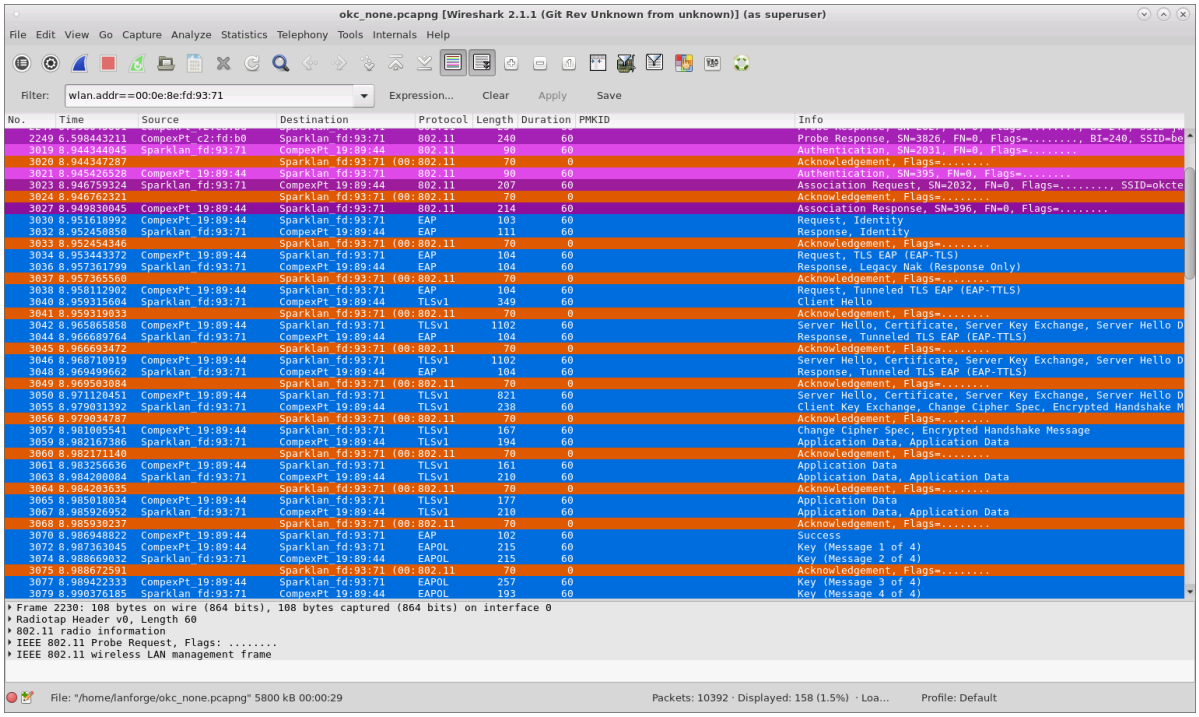
2. Admin the STA down , then modify the STA to disable PKC



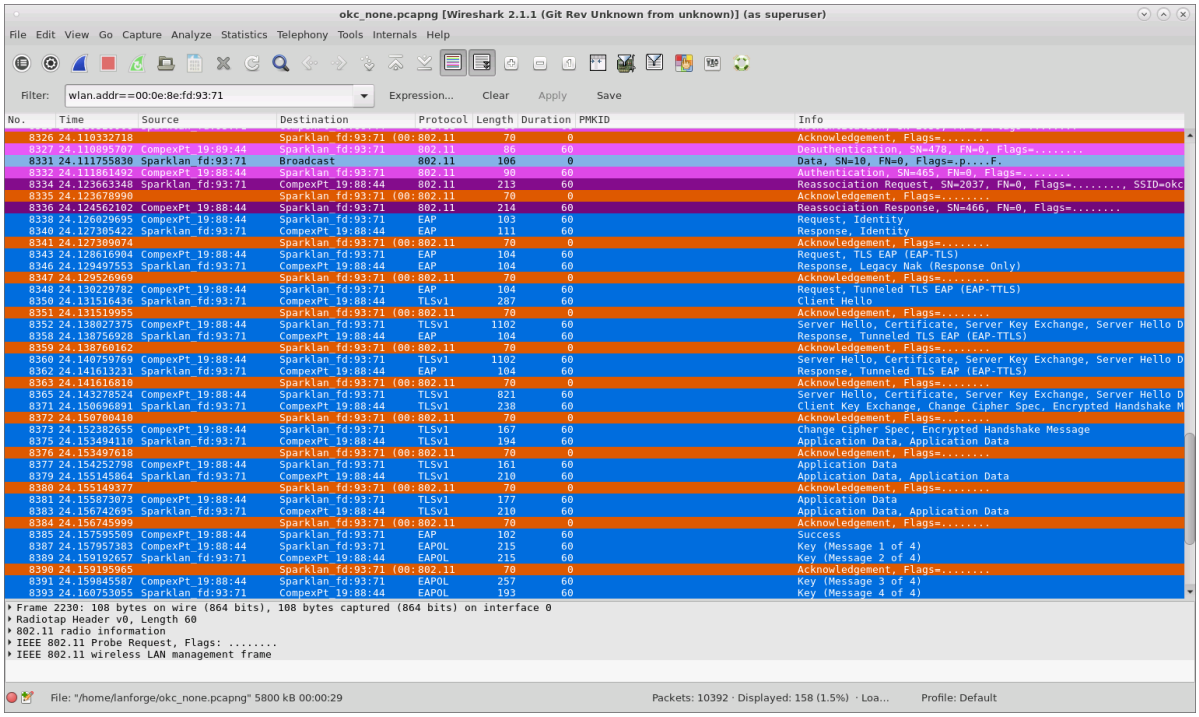
3. Start a packet capture then admin the STA up.
4. Use `wpa_cli` to force the STA to roam with the following terminal commands:

```
# wpa_cli -i sta00000 scan
# wpa_cli -i sta00000 roam <next BSSID>
```

5. In the packet capture, the initial RADIUS authentication and 4-way handshake are shown:



6. Then the STA sends a Reassociation Request which is missing the PMKID and another full RADIUS authentication and 4-way handshake take place to associate to the new BSSID.

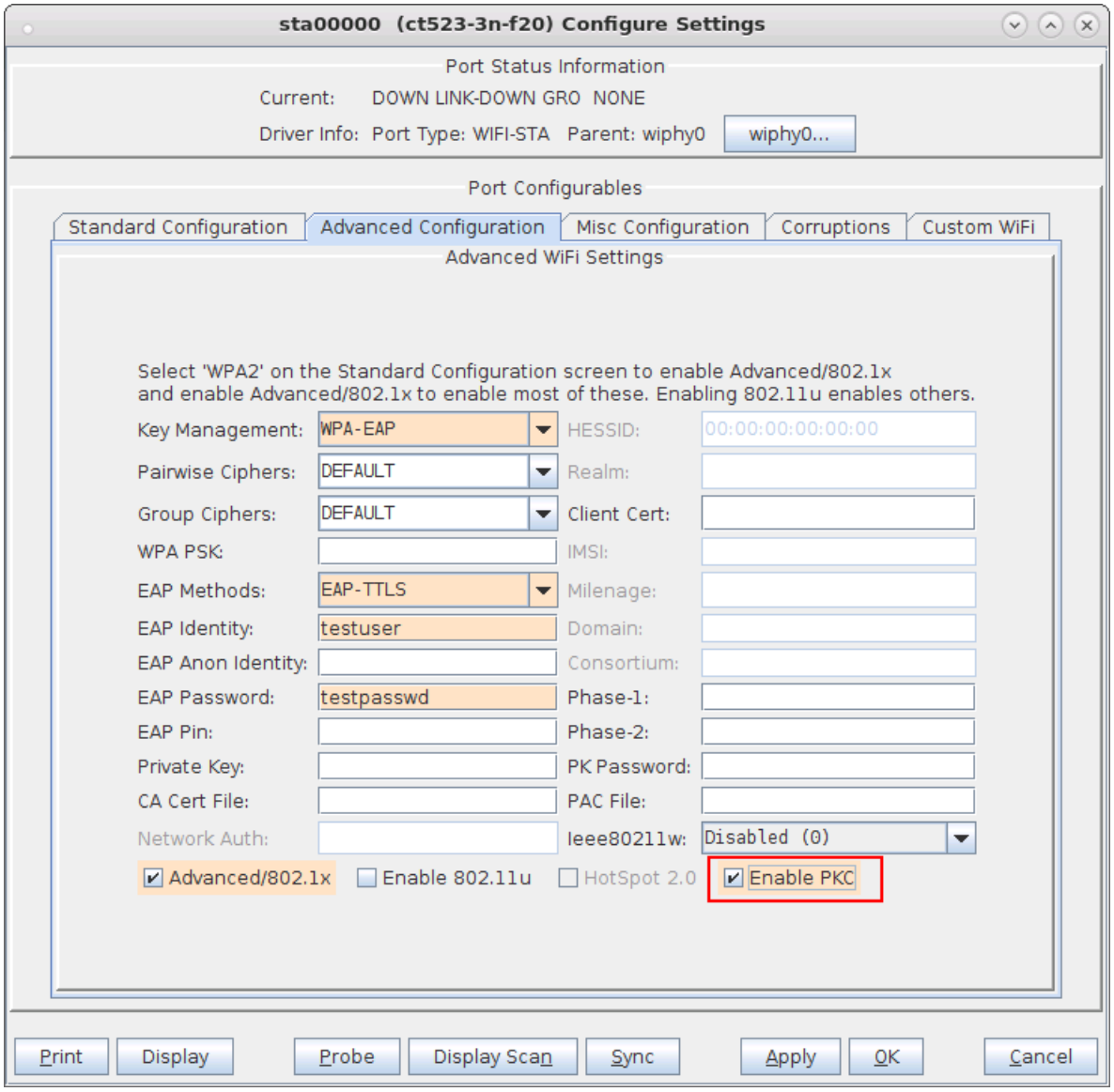


OKC Disabled On VAP and Enabled On STA

STA roam result: PMKID is sent, then full RADIUS authentication plus 4-way handshake.

If just the STA is using OKC, it will send its calculated PMKID in a Reassociation Request to the target AP, but the AP ignores it and the STA must perform a full RADIUS authentication plus 4-way handshake.

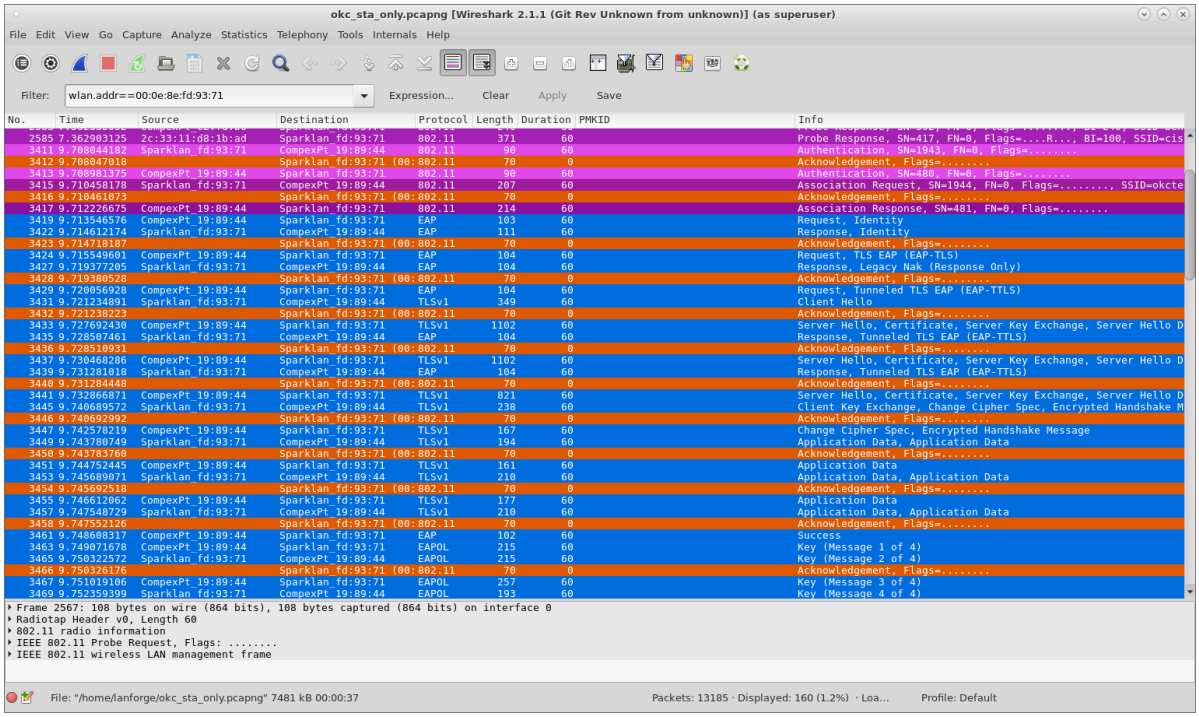
1. Admin the STA down , then modify the STA to enable PKC



2. Start a packet capture then admin the STA up.
3. Use `wpa_cli` to force the STA to roam with the following terminal commands:

```
# wpa_cli -i sta00000 scan
# wpa_cli -i sta00000 roam <next BSSID>
```

4. In the packet capture, the initial RADIUS authentication and 4-way handshake are shown:



5. Then the STA sends a Reassociation Request which includes its PMKID but the VAP ignores it and a full RADIUS authentication plus 4-way handshake are required.