

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

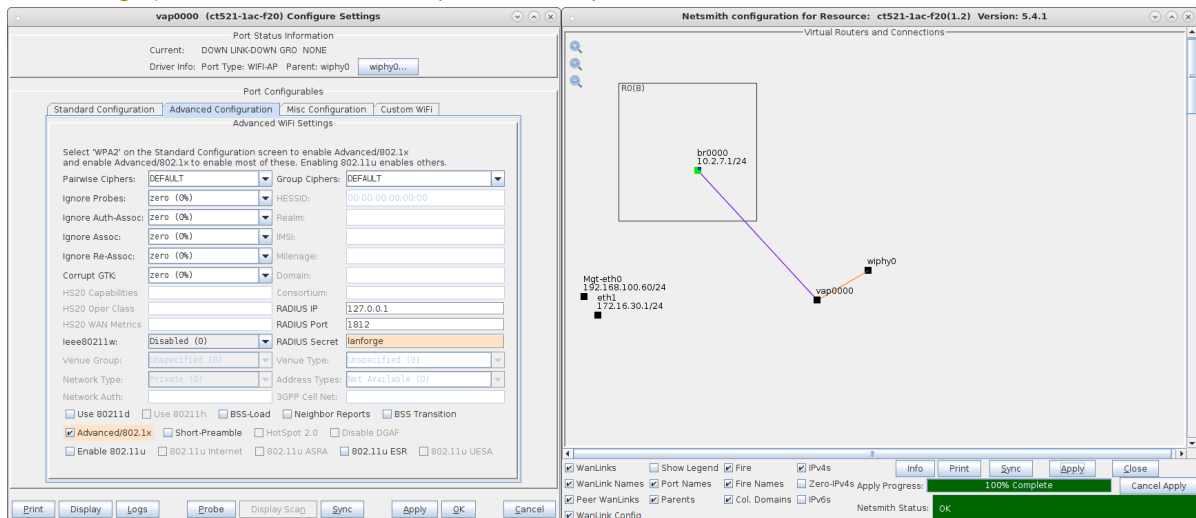
OKC Scenarios

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
ieee80211x=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.

br0000 (ct521-lac-f20) Configure Settings

Port Status Information
Current: LINK-UP TSO GSO GRO
Driver Info: Port Type: Bridge Cannot Detect

Port Configurables

Enable

- ☐ Set MAC
- ☐ Set TX Q Len
- ☐ Set MTU
- ☐ Set Offload
- ☐ Set Bridge Info

General Interface Settings

☐ Down ☐ Aux-Mgt

☐ DHCP-IPv6 ☒ DHCP Release DHCP Vendor ID: None

☐ DHCP-IPv4 DHCP Client ID: None

DNS Servers: BLANK Peer IP: NA

IP Address: 10.2.7.1 Global IPv6: AUTO

IP Mask: 255.255.255.0 Link IPv6: AUTO

Gateway IP: 0.0.0.0 IPv6 GW: AUTO

Alias: MTU: 1500

MAC Addr: 04:f0:21:19:87:44 TX Q Len: 1000

Rpt Timer: 1100 (1.1 s) WiFi Bridge: NONE

IPSec GW: 0.0.0.0 IPSec Password:

IPSec Local ID.: IPSec Remote ID.:

Spanning-Tree ☐

Aging Time: 300

Bridge Priority: 32768

Max Age: 20

Hello Time: 2

Forwarding Delay: 15

Services

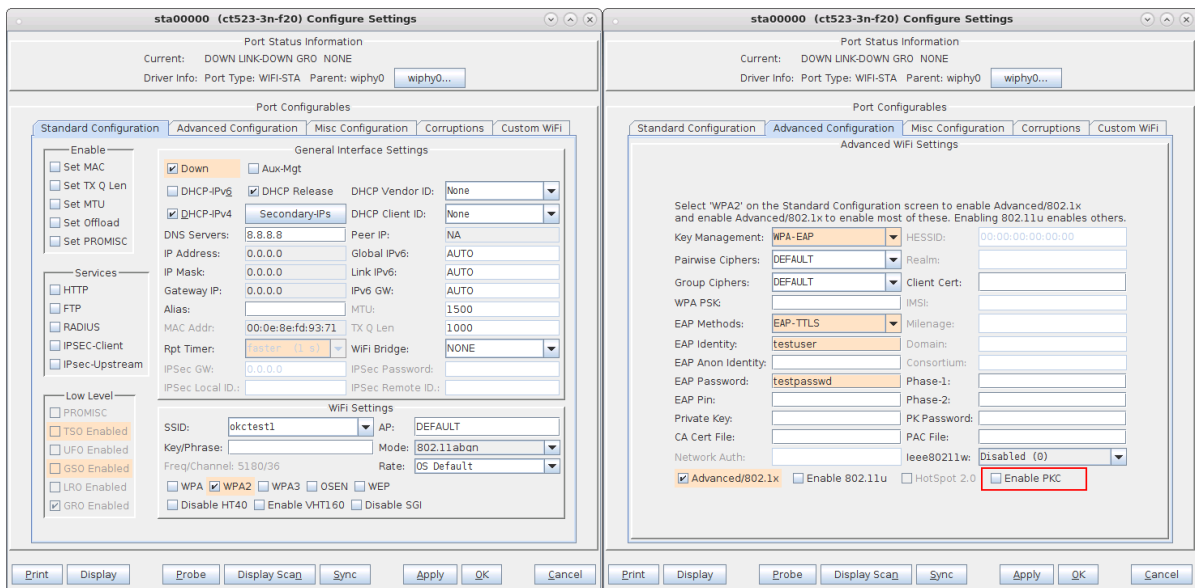
- ☐ HTTP
- ☐ FTP
- ☐ RADIUS
- ☐ IPSEC-Client
- ☐ IPsec-Upstream

Bridge Information

| Configured Ports | Current Ports |
|------------------|---------------|
| vap0000 | vap0000 |
| vap0000_0 | vap0000_0 |
| vap0000_1 | vap0000_1 |

vap0000_0
vap0000_1

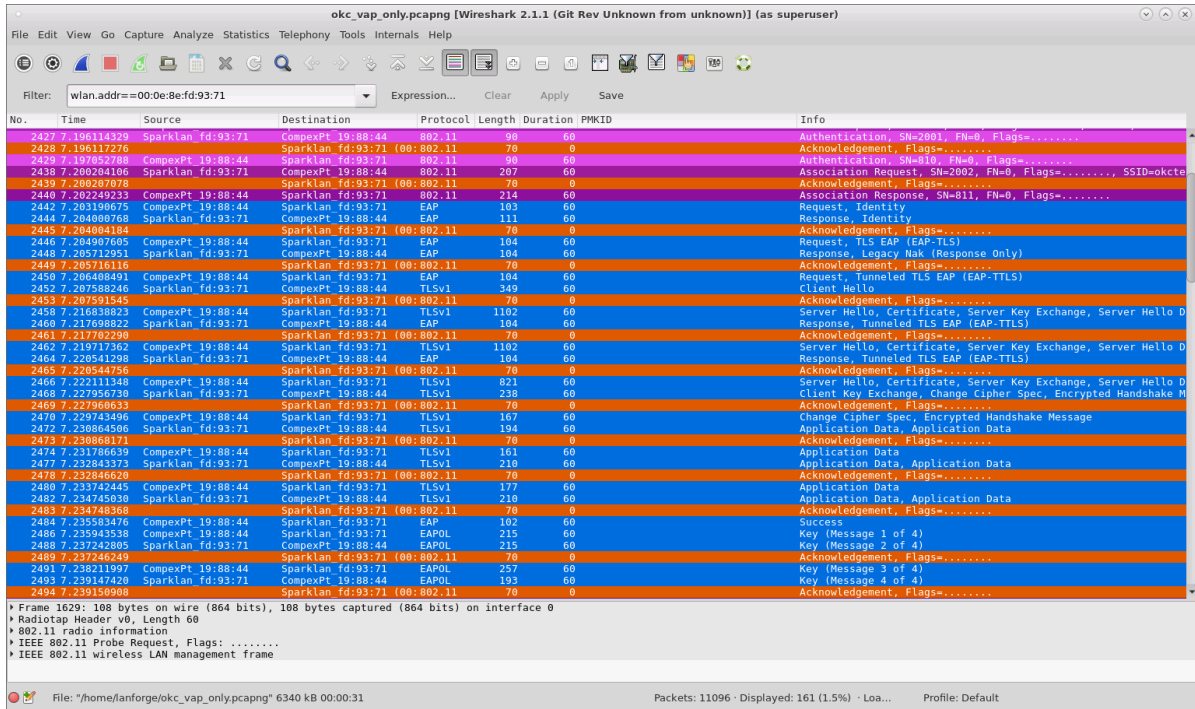
5. Modify a STA so that it is configured to connect to the SSID with 802.1X authentication for EAP-TTLS and with PKC disabled.



- Start a packet capture then admin the STA up.
- 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>
```

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



- 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_vap_only.pcapng [Wireshark 2.1.1 (Git Rev Unknown from unknown)] (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.addr==00:0e:8e:fd:93:71 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Duration | PMKID | Info |
|------|--------------|-------------------|-------------------------------|----------|--------|----------|-------|--|
| 7782 | 22.442317066 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7783 | 22.44239514 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 86 | 60 | | Deauthentication, SN=491, PN=0, Flags=..... |
| 7786 | 22.443522739 | Sparklan fd:93:71 | Broadcast | 802.11 | 106 | 0 | | Data, SN=16, PN=0, Flags=p....F. |
| 7789 | 22.44369254 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 96 | 60 | | Authentication, SN=2007, PN=0, Flags=..... |
| 7790 | 22.448169193 | Sparklan fd:93:71 | CompeXPT 19:89:44 | 802.11 | 213 | 60 | | Reassociation Request, SN=2007, FN=0, Flags=..... SSID=okc |
| 7791 | 22.448172108 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7792 | 22.449154014 | CompeXPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 214 | 60 | | Reassociation Response, SN=806, FN=0, Flags=..... |
| 7794 | 22.450239958 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 103 | 60 | | Request, Identity |
| 7796 | 22.451169477 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAP | 111 | 60 | | Response, Identity |
| 7797 | 22.451173021 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7798 | 22.452114787 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, TLS EAP (EAP-TLS) |
| 7800 | 22.453045244 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAP | 104 | 60 | | Response, Legacy Nak (Response Only) |
| 7801 | 22.453848671 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7803 | 22.453924608 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, Tunneled TLS EAP (EAP-TTLS) |
| 7807 | 22.455230935 | Sparklan fd:93:71 | CompeXPT 19:89:44 | TLSv1 | 287 | 60 | | Client Hello |
| 7808 | 22.455234194 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7811 | 22.463888108 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 7814 | 22.464758157 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAP | 104 | 60 | | Response, Tunneled TLS EAP (EAP-TTLS) |
| 7815 | 22.464761376 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7817 | 22.467604096 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 7820 | 22.468462206 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAP | 104 | 60 | | Response, Tunneled TLS EAP (EAP-TTLS) |
| 7821 | 22.468465518 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7822 | 22.470149388 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 821 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 7828 | 22.476224958 | Sparklan fd:93:71 | CompeXPT 19:89:44 | TLSv1 | 238 | 60 | | Client Key Exchange, Change Cipher Spec, Encrypted Handshake M |
| 7829 | 22.476228216 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7838 | 22.478692598 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 167 | 60 | | Change Cipher Spec, Encrypted Handshake Message |
| 7832 | 22.479450238 | Sparklan fd:93:71 | CompeXPT 19:89:44 | TLSv1 | 194 | 60 | | Application Data, Application Data |
| 7833 | 22.479454014 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7834 | 22.480411283 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 161 | 60 | | Application Data |
| 7836 | 22.481493188 | Sparklan fd:93:71 | CompeXPT 19:89:44 | TLSv1 | 210 | 60 | | Application Data, Application Data |
| 7837 | 22.481591487 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7842 | 22.482613818 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 177 | 60 | | Application Data |
| 7844 | 22.483646964 | Sparklan fd:93:71 | CompeXPT 19:89:44 | TLSv1 | 210 | 60 | | Application Data, Application Data |
| 7845 | 22.483650214 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7846 | 22.484618507 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 102 | 60 | | Success |
| 7848 | 22.484942467 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 215 | 60 | | Key (Message 1 of 4) |
| 7858 | 22.486455379 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAPOL | 215 | 60 | | Key (Message 2 of 4) |
| 7851 | 22.486459108 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | EAP | 70 | 0 | | Acknowledgement, Flags=..... |
| 7853 | 22.487663855 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 257 | 60 | | Key (Message 3 of 4) |
| 7855 | 22.488793758 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAPOL | 193 | 60 | | Key (Message 4 of 4) |

▶ Frame 1629: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
 ▶ Radiotap Header v0, Length 60
 ▶ 802.11 radio information
 ▶ IEEE 802.11 Probe Request, Flags:
 ▶ IEEE 802.11 Wireless LAN management frame

File: "/home/lanforge/okc_vap_only.pcapng" 6340 kB 00:00:31 Packets: 11096 · Displayed: 161 (1.5%) · Load... Profile: Default

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

sta00000 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: DOWN LINK-DOWN GRO NONE
 Driver Info: Port Type: WIFI-STA Parent: wiphy0 [wiphy0...](#)

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

| | | | |
|--------------------|-------------------|--------------|-------------------|
| Key Management: | WPA-EAP | HESSID: | 00:00:00:00:00:00 |
| Pairwise Ciphers: | DEFAULT | Realm: | |
| Group Ciphers: | DEFAULT | Client Cert: | |
| WPA PSK: | | IMSI: | |
| EAP Methods: | EAP-TTLS | Milenage: | |
| EAP Identity: | testuser | Domain: | |
| EAP Anon Identity: | | Consortium: | |
| EAP Password: | testpasswd | Phase-1: | |
| EAP Pin: | | Phase-2: | |
| Private Key: | | PK Password: | |
| CA Cert File: | | PAC File: | |
| Network Auth: | | ieee80211w: | Disabled (0) |

☒ **Advanced/802.1x**
☐ Enable 802.11u
 ☐ HotSpot 2.0
 ☒ **Enable PKC**

[Print](#)
[Display](#)
[Probe](#)
[Display Scan](#)
[Sync](#)
[Apply](#)
[OK](#)
[Cancel](#)

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:

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.addr==00:0e:8e:fd:93:71 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Duration | PMKID | Info |
|------|-------------|-------------------|-------------------------------|----------|--------|----------|-------|---|
| 2561 | 7.547330714 | 2c:33:11:d8:1b:ad | Sparklan fd:93:71 | 802.11 | 371 | 60 | | Probe Response, SN=474, FN=0, Flags=.....R.... BI=180, SSID=cis |
| 3363 | 9.887981889 | Sparklan fd:93:71 | ComexPT 19:89:44 | 802.11 | 98 | 60 | | Authentication, SN=1972, FN=0, Flags=..... |
| 3364 | 9.887984612 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3365 | 9.888039951 | ComexPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 98 | 60 | | Authentication, SN=58, FN=0, Flags=..... |
| 3367 | 9.890414681 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 207 | 60 | | Association Request, SN=1973, FN=0, Flags=....., SSID=okct |
| 3368 | 9.890417646 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3372 | 9.894065644 | ComexPT 19:89:44 | Sparklan fd:93:71 | EAP | 103 | 60 | | Request, Identity |
| 3374 | 9.894880189 | Sparklan fd:93:71 | ComexPT 19:89:44 | EAP | 111 | 60 | | Response, Identity |
| 3375 | 9.894883310 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3376 | 9.895828846 | ComexPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, TLS EAP (EAP-TLS) |
| 3378 | 9.896615529 | Sparklan fd:93:71 | ComexPT 19:89:44 | EAP | 104 | 60 | | Response, Legacy Nak (Response Only) |
| 3379 | 9.896618518 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3381 | 9.897415539 | ComexPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, Tunnelled TLS EAP (EAP-TTLS) |
| 3385 | 9.901853528 | Sparklan fd:93:71 | ComexPT 19:89:44 | TLSv1 | 349 | 60 | | Client Hello |
| 3386 | 9.901856761 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3388 | 9.911148003 | ComexPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3394 | 9.911991043 | Sparklan fd:93:71 | ComexPT 19:89:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 3395 | 9.911994181 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3396 | 9.914853000 | ComexPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3399 | 9.914745411 | Sparklan fd:93:71 | ComexPT 19:89:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 3400 | 9.914851446 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3401 | 9.914853000 | ComexPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 821 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3404 | 9.921894505 | Sparklan fd:93:71 | ComexPT 19:89:44 | TLSv1 | 238 | 60 | | Client Key Exchange, Change Cipher Spec, Encrypted Handshake M |
| 3405 | 9.921898265 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3406 | 9.923741357 | ComexPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 167 | 60 | | Change Cipher Spec, Encrypted Handshake Message |
| 3408 | 9.924890155 | Sparklan fd:93:71 | ComexPT 19:89:44 | TLSv1 | 194 | 60 | | Application Data |
| 3409 | 9.924893484 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3411 | 9.925799957 | ComexPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 161 | 60 | | Application Data |
| 3413 | 9.926741731 | Sparklan fd:93:71 | ComexPT 19:89:44 | TLSv1 | 210 | 60 | | Application Data, Application Data |
| 3414 | 9.926745315 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3415 | 9.927531355 | ComexPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 177 | 60 | | Application Data |
| 3417 | 9.928456896 | Sparklan fd:93:71 | ComexPT 19:89:44 | TLSv1 | 210 | 60 | | Application Data, Application Data |
| 3418 | 9.928460827 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3419 | 9.929345513 | ComexPT 19:89:44 | Sparklan fd:93:71 | EAP | 102 | 60 | | Success |
| 3421 | 9.929707605 | ComexPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 215 | 60 | | Key (Message 1 of 4) |
| 3423 | 9.931088450 | Sparklan fd:93:71 | ComexPT 19:89:44 | EAPOL | 215 | 60 | | Key (Message 2 of 4) |
| 3424 | 9.931091806 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3425 | 9.931713800 | ComexPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 257 | 60 | | Key (Message 3 of 4) |
| 3427 | 9.932637147 | Sparklan fd:93:71 | ComexPT 19:89:44 | EAPOL | 193 | 60 | | Key (Message 4 of 4) |
| 3428 | 9.932640458 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |

File: "/home/anforge/okc_both.pcapng" 6802 kB 00:00:33 Packets: 11792 · Displayed: 129 (1.1%) · Loa... Profile: Default

- 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.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.addr==00:0e:8e:fd:93:71 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Duration | PMKID | Info |
|------|--------------|-------------------|-------------------------------|----------|--------|----------|----------------------------------|---|
| 7241 | 20.716147686 | ComexPT f2:ea:bd | Sparklan fd:93:71 | 802.11 | 254 | 60 | | Probe Response, SN=447, FN=0, Flags=..... BI=240, SSID=jw3 |
| 7242 | 20.716443811 | Sparklan c1:fb:01 | Sparklan fd:93:71 | 802.11 | 255 | 0 | | Probe Response, SN=3252, FN=0, Flags=..... BI=240, SSID=fo |
| 7244 | 20.716784791 | Sparklan 4b:c8:2f | Sparklan fd:93:71 | 802.11 | 213 | 0 | | Probe Response, SN=2734, FN=0, Flags=..... BI=240, SSID=br |
| 7246 | 20.717626058 | ComexPT 19:88:44 | Sparklan fd:93:71 | 802.11 | 292 | 0 | | Probe Response, SN=585, FN=0, Flags=..... BI=240, SSID=okc |
| 7248 | 20.718074511 | ComexPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 292 | 0 | | Probe Response, SN=598, FN=0, Flags=..... BI=240, SSID=okc |
| 7249 | 20.718355647 | ComexPT f2:ea:bd | Sparklan fd:93:71 | 802.11 | 254 | 60 | | Probe Response, SN=447, FN=0, Flags=..... BI=240, SSID=jw3 |
| 7251 | 20.718823352 | ComexPT c2:fd:b0 | Sparklan fd:93:71 | 802.11 | 248 | 60 | | Probe Response, SN=1648, FN=0, Flags=..... BI=240, SSID=be |
| 7252 | 20.719204338 | ComexPT c2:fd:b0 | Sparklan fd:93:71 | 802.11 | 248 | 60 | | Probe Response, SN=1648, FN=0, Flags=..... BI=240, SSID=be |
| 7254 | 20.719741614 | 2c:33:11:d8:1b:ad | Sparklan fd:93:71 | 802.11 | 371 | 60 | | Probe Response, SN=478, FN=0, Flags=.....R.... BI=180, SSID=cis |
| 7269 | 20.746220843 | Sparklan fd:93:71 | ComexPT 19:89:44 | 802.11 | 98 | 44 | | QoS Null function (No data), SN=0, FN=0, Flags=.....T |
| 7270 | 20.746249459 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 7271 | 20.746437972 | Sparklan fd:93:71 | ComexPT 19:89:44 | 802.11 | 86 | 60 | | QoS Null function (No data), SN=0, FN=0, Flags=.....T |
| 7272 | 20.746440863 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8171 | 23.500839768 | Sparklan fd:93:71 | ComexPT 19:88:44 | 802.11 | 98 | 60 | | Authentication, SN=1977, FN=0, Flags=..... |
| 8174 | 23.500600010 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8175 | 23.501240424 | ComexPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 86 | 60 | | Deauthentication, SN=410, FN=0, Flags=..... |
| 8177 | 23.502131211 | Sparklan fd:93:71 | Broadcast | 802.11 | 106 | 0 | | Data, SN=10, FN=0, Flags=p....F. |
| 8178 | 23.502131211 | ComexPT 19:88:44 | Sparklan fd:93:71 | 802.11 | 231 | 60 | 424934013b5091d6096dd4db69e14ddd | Authentication, SN=572, FN=0, Flags=..... |
| 8181 | 23.505314727 | Sparklan fd:93:71 | ComexPT 19:88:44 | 802.11 | 231 | 60 | 424934013b5091d6096dd4db69e14ddd | Reassociation Request, SN=1978, FN=0, Flags=....., SSID=okc |
| 8182 | 23.505337617 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8184 | 23.506409346 | ComexPT 19:88:44 | Sparklan fd:93:71 | 802.11 | 214 | 60 | | Reassociation Response, SN=598, FN=0, Flags=..... |
| 8186 | 23.506883435 | Sparklan fd:93:71 | ComexPT 19:88:44 | EAPOL | 215 | 60 | | Key (Message 1 of 4) |
| 8188 | 23.509284996 | Sparklan fd:93:71 | ComexPT 19:88:44 | EAPOL | 233 | 60 | 424934013b5091d6096dd4db69e14ddd | Key (Message 2 of 4) |
| 8189 | 23.509288289 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8190 | 23.509988233 | ComexPT 19:88:44 | Sparklan fd:93:71 | EAPOL | 257 | 60 | | Key (Message 3 of 4) |
| 8192 | 23.510622242 | Sparklan fd:93:71 | ComexPT 19:88:44 | EAPOL | 193 | 60 | | Key (Message 4 of 4) |
| 8193 | 23.510965550 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8195 | 23.511628023 | ComexPT 19:88:44 | Sparklan fd:93:71 | 802.11 | 87 | 60 | | Action, SN=599, FN=0, Flags=..... |
| 8200 | 23.521863722 | Sparklan fd:93:71 | ComexPT 19:88:44 | 802.11 | 93 | 60 | | Action, SN=1979, FN=0, Flags=..... |
| 8201 | 23.521866733 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8202 | 23.521166601 | ComexPT 19:88:44 | Sparklan fd:93:71 | 802.11 | 93 | 60 | | Action, SN=0, FN=0, Flags=..... |
| 8204 | 23.521899262 | Sparklan fd:93:71 | IPv6cast 16 | 802.11 | 190 | 44 | | QoS Data, SN=0, FN=0, Flags=p....T |
| 8205 | 23.521899246 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8206 | 23.522338099 | Sparklan fd:93:71 | IPv6cast 16 | 802.11 | 184 | 0 | | Data, SN=0, FN=0, Flags=p....F. |
| 8464 | 24.221222475 | Sparklan fd:93:71 | IPv6cast 16 | 802.11 | 190 | 60 | | QoS Data, SN=1, FN=0, Flags=p....T |
| 8465 | 24.221220521 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8466 | 24.221604231 | Sparklan fd:93:71 | IPv6cast 16 | 802.11 | 184 | 0 | | Data, SN=1, FN=0, Flags=p....F. |
| 9784 | 28.062935477 | Sparklan fd:93:71 | IPv6cast 02 | 802.11 | 170 | 44 | | QoS Data, SN=2, FN=0, Flags=p....T |
| 9785 | 28.062884302 | Sparklan fd:93:71 | Sparklan fd:93:71 (00:802.11) | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 9786 | 28.062519511 | Sparklan fd:93:71 | IPv6cast 02 | 802.11 | 164 | 0 | | Data, SN=3, FN=0, Flags=p....F. |

File: "/home/anforge/okc_both.pcapng" 6802 kB 00:00:33 Packets: 11792 · Displayed: 129 (1.1%) · Loa... Profile: Default

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.

- 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

sta00000 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: DOWN LINK-DOWN GRO NONE
 Driver Info: Port Type: WIFI-STA Parent: wiphy0 [wiphy0...](#)

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

| | | | |
|--------------------|-----------------|--------------|-------------------|
| Key Management: | WPA-EAP | HESSID: | 00:00:00:00:00:00 |
| Pairwise Ciphers: | DEFAULT | Realm: | |
| Group Ciphers: | DEFAULT | Client Cert: | |
| WPA PSK: | | IMSI: | |
| EAP Methods: | EAP-TTLS | Milenage: | |
| EAP Identity: | testuser | Domain: | |
| EAP Anon Identity: | | Consortium: | |
| EAP Password: | testpasswd | Phase-1: | |
| EAP Pin: | | Phase-2: | |
| Private Key: | | PK Password: | |
| CA Cert File: | | PAC File: | |
| Network Auth: | | ieee80211w: | Disabled (0) |

☒ **Advanced/802.1x**
☐ Enable 802.11u
 ☐ HotSpot 2.0
 ☐ **Enable PKC**

[Print](#)
[Display](#)
[Probe](#)
[Display Scan](#)
[Sync](#)
[Apply](#)
[OK](#)
[Cancel](#)

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:

okc_none.pcapng [Wireshark 2.1.1 (Git Rev Unknown from unknown)] (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.addr==00:0e:8e:fd:93:71 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Duration | PMKID | Info |
|------|-------------|-------------------------------|-------------------------------|----------|--------|----------|-------|--|
| 2249 | 6.598443211 | CompexPT c2:fd:b0 | Sparklan fd:93:71 | 802.11 | 240 | 60 | | Probe Response, SN=3826, FN=0, Flags=....., BI=240, SSID=okc |
| 3019 | 8.944344845 | Sparklan fd:93:71 | CompexPT 19:89:44 | 802.11 | 98 | 0 | | Authentication, SN=2031, FN=0, Flags=..... |
| 3020 | 8.944347287 | CompexPT 19:89:44 | Sparklan fd:93:71 (00:802.11) | 70 | 0 | | | Acknowledgement, Flags=..... |
| 3021 | 8.946759324 | Sparklan fd:93:71 | CompexPT 19:89:44 | 802.11 | 207 | 0 | | Authentication, SN=395, FN=0, Flags=..... |
| 3024 | 8.946762321 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Association Request, SN=2032, FN=0, Flags=....., SSID=okc |
| 3027 | 8.949838045 | CompexPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 214 | 60 | | Acknowledgement, Flags=..... |
| 3030 | 8.951618992 | Sparklan fd:93:71 | CompexPT 19:89:44 | EAP | 103 | 60 | | Association Response, SN=396, FN=0, Flags=..... |
| 3032 | 8.952458850 | Sparklan fd:93:71 | CompexPT 19:89:44 | EAP | 111 | 60 | | Response, Identity |
| 3033 | 8.952454346 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3034 | 8.953443372 | CompexPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, TLS EAP (EAP-TLS) |
| 3036 | 8.953671709 | Sparklan fd:93:71 | CompexPT 19:89:44 | EAP | 104 | 60 | | Response, Legacy Nak (Response Only) |
| 3037 | 8.957365560 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3038 | 8.958112982 | CompexPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, Tunnelled TLS EAP (EAP-TTLS) |
| 3040 | 8.959115041 | Sparklan fd:93:71 | CompexPT 19:89:44 | TLV1 | 349 | 60 | | Client Hello |
| 3041 | 8.959319893 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3042 | 8.965865858 | CompexPT 19:89:44 | Sparklan fd:93:71 | TLV1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3044 | 8.966689764 | Sparklan fd:93:71 | CompexPT 19:89:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 3045 | 8.966993492 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3046 | 8.968718910 | CompexPT 19:89:44 | Sparklan fd:93:71 | TLV1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3048 | 8.969496662 | Sparklan fd:93:71 | CompexPT 19:89:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 3049 | 8.969583084 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3050 | 8.971110441 | CompexPT 19:89:44 | Sparklan fd:93:71 | TLV1 | 821 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3055 | 8.979031392 | Sparklan fd:93:71 | CompexPT 19:89:44 | TLV1 | 238 | 0 | | Client Key Exchange, Change Cipher Spec, Encrypted Handshake M |
| 3056 | 8.979034787 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3057 | 8.981005541 | CompexPT 19:89:44 | Sparklan fd:93:71 | TLV1 | 167 | 60 | | Change Cipher Spec, Encrypted Handshake Message |
| 3059 | 8.982167386 | Sparklan fd:93:71 | CompexPT 19:89:44 | TLV1 | 194 | 60 | | Application Data, Application Data |
| 3060 | 8.982171140 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3061 | 8.983256636 | CompexPT 19:89:44 | Sparklan fd:93:71 | TLV1 | 161 | 60 | | Application Data |
| 3063 | 8.984260084 | Sparklan fd:93:71 | CompexPT 19:89:44 | TLV1 | 210 | 60 | | Application Data, Application Data |
| 3064 | 8.984283635 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3065 | 8.985018034 | CompexPT 19:89:44 | Sparklan fd:93:71 | TLV1 | 177 | 60 | | Application Data |
| 3067 | 8.985926352 | Sparklan fd:93:71 | CompexPT 19:89:44 | TLV1 | 210 | 60 | | Application Data, Application Data |
| 3068 | 8.985930237 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3070 | 8.986948822 | CompexPT 19:89:44 | Sparklan fd:93:71 | EAP | 102 | 60 | | Success |
| 3072 | 8.987363045 | CompexPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 215 | 60 | | Key (Message 1 of 4) |
| 3074 | 8.988669032 | Sparklan fd:93:71 | CompexPT 19:89:44 | EAPOL | 215 | 60 | | Key (Message 2 of 4) |
| 3075 | 8.988672591 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3077 | 8.989422333 | CompexPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 257 | 60 | | Key (Message 3 of 4) |
| 3079 | 8.990376185 | CompexPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 193 | 60 | | Key (Message 4 of 4) |

Frame 2230: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
 Radiotap Header v0, Length 60
 802.11 radio information
 IEEE 802.11 Probe Request, Flags:
 IEEE 802.11 wireless LAN management frame

File: "/home/fanforge/okc_none.pcapng" 5800 kB 00:00:29 Packets: 10392 · Displayed: 158 (1.5%) · Load... Profile: Default

- 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_none.pcapng [Wireshark 2.1.1 (Git Rev Unknown from unknown)] (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.addr==00:0e:8e:fd:93:71 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Duration | PMKID | Info |
|------|--------------|-------------------------------|-------------------|----------|--------|----------|-------|--|
| 8326 | 24.110332718 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8327 | 24.110895787 | CompexPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 86 | 60 | | Deauthentication, SN=478, FN=0, Flags=..... |
| 8331 | 24.111755830 | Sparklan fd:93:71 | Broadcast | 802.11 | 106 | 0 | | Data, SN=10, FN=0, Flags=..... |
| 8332 | 24.111816192 | CompexPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 90 | 60 | | Authentication, SN=478, FN=0, Flags=..... |
| 8334 | 24.123663348 | Sparklan fd:93:71 | CompexPT 19:88:44 | 802.11 | 213 | 60 | | Reassociation Request, SN=2037, FN=0, Flags=....., SSID=okc |
| 8335 | 24.123678990 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8336 | 24.124562109 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAP | 103 | 60 | | Reassociation Response, SN=466, FN=0, Flags=..... |
| 8338 | 24.126028695 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAP | 103 | 60 | | Request, Identity |
| 8340 | 24.127385422 | Sparklan fd:93:71 | CompexPT 19:88:44 | EAP | 111 | 60 | | Response, Identity |
| 8341 | 24.127399874 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8343 | 24.128616192 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, TLS EAP (EAP-TLS) |
| 8346 | 24.129497553 | Sparklan fd:93:71 | CompexPT 19:88:44 | EAP | 104 | 60 | | Response, Legacy Nak (Response Only) |
| 8347 | 24.129526969 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8348 | 24.130229782 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, Tunnelled TLS EAP (EAP-TTLS) |
| 8350 | 24.131161436 | Sparklan fd:93:71 | CompexPT 19:88:44 | TLV1 | 297 | 60 | | Client Hello |
| 8351 | 24.131519955 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8352 | 24.138027375 | CompexPT 19:88:44 | Sparklan fd:93:71 | TLV1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 8358 | 24.138756028 | Sparklan fd:93:71 | CompexPT 19:88:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 8359 | 24.138760162 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8360 | 24.140759769 | CompexPT 19:88:44 | Sparklan fd:93:71 | TLV1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 8362 | 24.141613231 | Sparklan fd:93:71 | CompexPT 19:88:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 8363 | 24.141616192 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8365 | 24.143278524 | CompexPT 19:88:44 | Sparklan fd:93:71 | TLV1 | 821 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 8371 | 24.150696891 | Sparklan fd:93:71 | CompexPT 19:88:44 | TLV1 | 238 | 60 | | Client Key Exchange, Change Cipher Spec, Encrypted Handshake M |
| 8372 | 24.150700410 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8373 | 24.152381535 | CompexPT 19:88:44 | Sparklan fd:93:71 | TLV1 | 167 | 60 | | Change Cipher Spec, Encrypted Handshake Message |
| 8375 | 24.153494110 | Sparklan fd:93:71 | CompexPT 19:88:44 | TLV1 | 194 | 60 | | Application Data, Application Data |
| 8376 | 24.153497618 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8377 | 24.154252798 | CompexPT 19:88:44 | Sparklan fd:93:71 | TLV1 | 161 | 60 | | Application Data |
| 8379 | 24.155145864 | Sparklan fd:93:71 | CompexPT 19:88:44 | TLV1 | 210 | 60 | | Application Data, Application Data |
| 8380 | 24.155149377 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8381 | 24.155873873 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAPOL | 177 | 60 | | Application Data |
| 8383 | 24.156742695 | Sparklan fd:93:71 | CompexPT 19:88:44 | EAPOL | 215 | 60 | | Application Data, Application Data |
| 8384 | 24.156745999 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8385 | 24.157595509 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAP | 102 | 60 | | Success |
| 8387 | 24.157957383 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAPOL | 215 | 60 | | Key (Message 1 of 4) |
| 8389 | 24.159192657 | Sparklan fd:93:71 | CompexPT 19:88:44 | EAPOL | 215 | 60 | | Key (Message 2 of 4) |
| 8390 | 24.159195965 | Sparklan fd:93:71 (00:802.11) | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8391 | 24.159845587 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAPOL | 257 | 60 | | Key (Message 3 of 4) |
| 8392 | 24.160753055 | CompexPT 19:88:44 | Sparklan fd:93:71 | EAPOL | 193 | 60 | | Key (Message 4 of 4) |

Frame 2230: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
 Radiotap Header v0, Length 60
 802.11 radio information
 IEEE 802.11 Probe Request, Flags:
 IEEE 802.11 wireless LAN management frame

File: "/home/fanforge/okc_none.pcapng" 5800 kB 00:00:29 Packets: 10392 · Displayed: 158 (1.5%) · Load... Profile: Default

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.

- Admin the STA down, then modify the STA to enable PKC

sta00000 (ct523-3n-f20) Configure Settings

Port Status Information
 Current: DOWN LINK-DOWN GRO NONE
 Driver Info: Port Type: WIFI-STA Parent: wiphy0 [wiphy0...](#)

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

| | | | |
|--------------------|-----------------|--------------|-------------------|
| Key Management: | WPA-EAP | HESSID: | 00:00:00:00:00:00 |
| Pairwise Ciphers: | DEFAULT | Realm: | |
| Group Ciphers: | DEFAULT | Client Cert: | |
| WPA PSK: | | IMSI: | |
| EAP Methods: | EAP-TTLS | Milenage: | |
| EAP Identity: | testuser | Domain: | |
| EAP Anon Identity: | | Consortium: | |
| EAP Password: | testpasswd | Phase-1: | |
| EAP Pin: | | Phase-2: | |
| Private Key: | | PK Password: | |
| CA Cert File: | | PAC File: | |
| Network Auth: | | ieee80211w: | Disabled (0) |

☒ **Advanced/802.1x**
☐ Enable 802.11u
 ☐ HotSpot 2.0
 ☒ **Enable PKC**

[Print](#)
[Display](#)
[Probe](#)
[Display Scan](#)
[Sync](#)
[Apply](#)
[OK](#)
[Cancel](#)

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:

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.addr==00:0e:8e:fd:93:71 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Duration | PMKID | Info |
|------|-------------|-------------------|-------------------|----------|--------|----------|-------|--|
| 2585 | 9.362983125 | 2c:53:11:d0:1b:ad | Sparklan fd:93:71 | 802.11 | 371 | 60 | | Probe Response, SN=417, FN=0, Flags=.....R....BI=100, SSID=cis |
| 3411 | 9.788844102 | Sparklan fd:93:71 | CompeXPT 19:89:44 | 802.11 | 98 | 0 | | Authentication, SN=1943, FN=0, Flags=..... |
| 3412 | 9.788847018 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3413 | 9.788848125 | CompeXPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 98 | 0 | | Authentication, SN=481, FN=0, Flags=..... |
| 3415 | 9.710458178 | Sparklan fd:93:71 | CompeXPT 19:89:44 | 802.11 | 207 | 0 | | Association Request, SN=1944, FN=0, Flags=....., SSID=okcte |
| 3416 | 9.710461073 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3417 | 9.712226675 | CompeXPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 214 | 60 | | Association Response, SN=481, FN=0, Flags=..... |
| 3419 | 9.712354576 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 103 | 60 | | Request, Identity |
| 3422 | 9.714612174 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAP | 111 | 60 | | Response, Identity |
| 3423 | 9.714718187 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3424 | 9.715549681 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, TLS EAP (EAP-TLS) |
| 3427 | 9.710377205 | Sparklan fd:93:71 | Sparklan fd:93:71 | EAP | 104 | 60 | | Response, Legacy Nak (Response Only) |
| 3428 | 9.710389528 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3429 | 9.720056928 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, Tunnelled TLS EAP (EAP-TTLS) |
| 3431 | 9.721218021 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 349 | 60 | | Client Hello |
| 3432 | 9.721223823 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3433 | 9.727692430 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3436 | 9.728507461 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 3437 | 9.728508286 | CompeXPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3439 | 9.731281018 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAP | 104 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 3440 | 9.731284448 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 3441 | 9.732866671 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 821 | 60 | | Acknowledgement, Flags=..... |
| 3445 | 9.740689572 | Sparklan fd:93:71 | CompeXPT 19:89:44 | TLSv1 | 238 | 60 | | Client Key Exchange, Change Cipher Spec, Encrypted Handshake M |
| 3446 | 9.740692992 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3447 | 9.742578210 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 167 | 60 | | Change Cipher Spec, Encrypted Handshake Message |
| 3449 | 9.743709749 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 194 | 60 | | Application Data, Application Data |
| 3450 | 9.743783760 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3451 | 9.744752445 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 161 | 60 | | Application Data |
| 3453 | 9.745689071 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAPOL | 215 | 60 | | Application Data |
| 3454 | 9.745692518 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3455 | 9.746612062 | CompeXPT 19:89:44 | Sparklan fd:93:71 | TLSv1 | 177 | 60 | | Application Data |
| 3457 | 9.747548729 | Sparklan fd:93:71 | CompeXPT 19:89:44 | TLSv1 | 210 | 60 | | Application Data, Application Data |
| 3458 | 9.747552126 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3461 | 9.748608317 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAP | 102 | 60 | | Success |
| 3463 | 9.749071678 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 215 | 60 | | Key (Message 1 of 4) |
| 3465 | 9.750322572 | Sparklan fd:93:71 | CompeXPT 19:89:44 | EAPOL | 215 | 60 | | Key (Message 2 of 4) |
| 3466 | 9.750326103 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 3467 | 9.751019106 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 257 | 60 | | Key (Message 3 of 4) |
| 3469 | 9.752359399 | CompeXPT 19:89:44 | Sparklan fd:93:71 | EAPOL | 193 | 60 | | Key (Message 4 of 4) |

Frame 2567: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
 Radiotap Header v0, Length 60
 802.11 radio information
 IEEE 802.11 Probe Request, Flags:
 IEEE 802.11 wireless LAN management frame

File: "/home/anforge/okc_sta_only.pcapng" 7481 kB 00:00:37 Packets: 13185 · Displayed: 160 (1.2%) · Loa... Profile: Default

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.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.addr==00:0e:8e:fd:93:71 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Duration | PMKID | Info |
|------|---------------|-------------------|-------------------|----------|--------|----------|--------------------------------|--|
| 8680 | 24.829069678 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8681 | 24.838223641 | CompeXPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 86 | 60 | | Deauthentication, SN=559, FN=0, Flags=..... |
| 8683 | 24.8390935248 | Sparklan fd:93:71 | Broadcast | 802.11 | 106 | 0 | | Data, SN=11, FN=0, Flags=..... |
| 8684 | 24.839101535 | CompeXPT 19:89:44 | Sparklan fd:93:71 | 802.11 | 60 | 0 | | Authentication, SN=246, FN=0, Flags=..... |
| 8686 | 24.834493647 | Sparklan fd:93:71 | CompeXPT 19:88:44 | 802.11 | 231 | 60 | dc66e86bde24f862297e94fa2b39b4 | Reassociation Request, SN=1949, FN=0, Flags=....., SSID=okcte |
| 8687 | 24.834496522 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8688 | 24.835456451 | CompeXPT 19:88:44 | Sparklan fd:93:71 | 802.11 | 214 | 60 | | Reassociation Response, SN=547, FN=0, Flags=..... |
| 8690 | 24.837133923 | Sparklan fd:93:71 | Sparklan fd:93:71 | EAP | 103 | 60 | | Request, Identity |
| 8692 | 24.838297278 | Sparklan fd:93:71 | CompeXPT 19:88:44 | EAP | 111 | 60 | | Response, Identity |
| 8693 | 24.838390732 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8694 | 24.839225546 | CompeXPT 19:88:44 | Sparklan fd:93:71 | EAP | 103 | 60 | | Request, TLS EAP (EAP-TLS) |
| 8696 | 24.840063365 | Sparklan fd:93:71 | CompeXPT 19:88:44 | EAP | 104 | 60 | | Response, Legacy Nak (Response Only) |
| 8697 | 24.840067805 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8698 | 24.840764926 | CompeXPT 19:88:44 | Sparklan fd:93:71 | EAP | 104 | 60 | | Request, Tunnelled TLS EAP (EAP-TTLS) |
| 8700 | 24.842407557 | Sparklan fd:93:71 | CompeXPT 19:88:44 | TLSv1 | 287 | 60 | | Client Hello |
| 8701 | 24.842411011 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8703 | 24.848955037 | CompeXPT 19:88:44 | Sparklan fd:93:71 | TLSv1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 8705 | 24.848956212 | Sparklan fd:93:71 | CompeXPT 19:88:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 8706 | 24.849268403 | Sparklan fd:93:71 | CompeXPT 19:88:44 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8707 | 24.851981053 | CompeXPT 19:88:44 | Sparklan fd:93:71 | TLSv1 | 1102 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 8709 | 24.852888129 | Sparklan fd:93:71 | CompeXPT 19:88:44 | EAP | 104 | 60 | | Response, Tunnelled TLS EAP (EAP-TTLS) |
| 8710 | 24.852881803 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8711 | 24.854460327 | CompeXPT 19:88:44 | Sparklan fd:93:71 | TLSv1 | 821 | 60 | | Server Hello, Certificate, Server Key Exchange, Server Hello D |
| 8714 | 24.859616192 | Sparklan fd:93:71 | CompeXPT 19:88:44 | TLSv1 | 238 | 60 | | Client Key Exchange, Change Cipher Spec, Encrypted Handshake M |
| 8715 | 24.859641877 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8716 | 24.861510226 | CompeXPT 19:88:44 | Sparklan fd:93:71 | TLSv1 | 167 | 60 | | Change Cipher Spec, Encrypted Handshake Message |
| 8718 | 24.862355999 | Sparklan fd:93:71 | CompeXPT 19:88:44 | TLSv1 | 194 | 60 | | Application Data, Application Data |
| 8719 | 24.862560787 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8720 | 24.864889838 | CompeXPT 19:88:44 | Sparklan fd:93:71 | TLSv1 | 161 | 60 | | Application Data |
| 8723 | 24.865819979 | Sparklan fd:93:71 | CompeXPT 19:88:44 | TLSv1 | 210 | 60 | | Application Data, Application Data |
| 8724 | 24.865823366 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8725 | 24.866669154 | CompeXPT 19:88:44 | Sparklan fd:93:71 | TLSv1 | 177 | 60 | | Application Data |
| 8727 | 24.867571529 | Sparklan fd:93:71 | CompeXPT 19:88:44 | TLSv1 | 210 | 60 | | Application Data, Application Data |
| 8728 | 24.867575842 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8729 | 24.868578312 | CompeXPT 19:88:44 | Sparklan fd:93:71 | EAP | 102 | 60 | | Success |
| 8731 | 24.868903422 | CompeXPT 19:88:44 | Sparklan fd:93:71 | EAPOL | 215 | 60 | | Key (Message 1 of 4) |
| 8733 | 24.870254506 | Sparklan fd:93:71 | CompeXPT 19:88:44 | EAPOL | 233 | 60 | dc66e86bde24f862297e94fa2b39b4 | Key (Message 2 of 4) |
| 8734 | 24.870257998 | Sparklan fd:93:71 | Sparklan fd:93:71 | 802.11 | 70 | 0 | | Acknowledgement, Flags=..... |
| 8735 | 24.870977518 | CompeXPT 19:88:44 | Sparklan fd:93:71 | EAPOL | 257 | 60 | | Key (Message 3 of 4) |
| 8737 | 24.871882955 | Sparklan fd:93:71 | CompeXPT 19:88:44 | EAPOL | 193 | 60 | | Key (Message 4 of 4) |

Frame 2567: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0
 Radiotap Header v0, Length 60
 802.11 radio information
 IEEE 802.11 Probe Request, Flags:
 IEEE 802.11 wireless LAN management frame

File: "/home/anforge/okc_sta_only.pcapng" 7481 kB 00:00:37 Packets: 13185 · Displayed: 160 (1.2%) · Loa... Profile: Default