

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

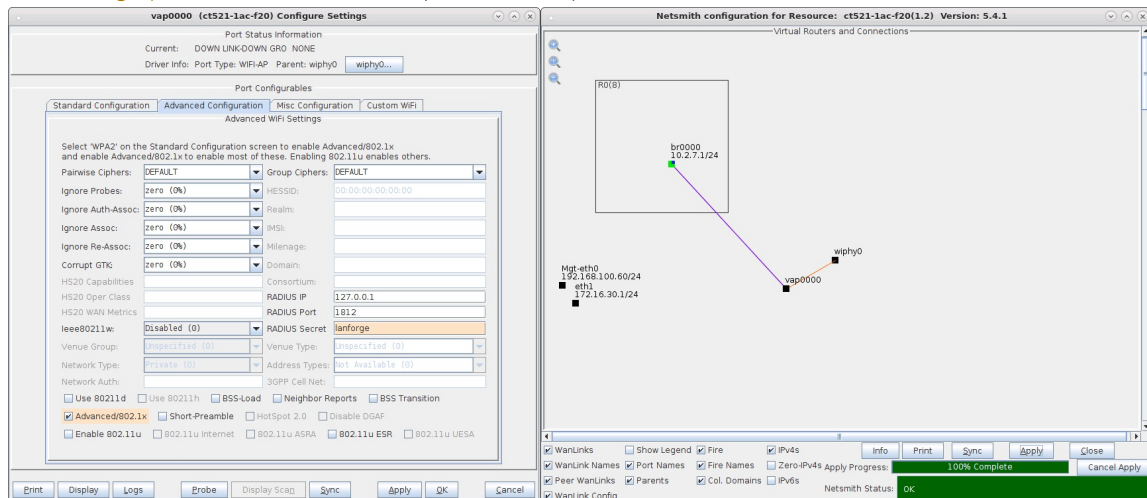
OKC Scenarios

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.

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

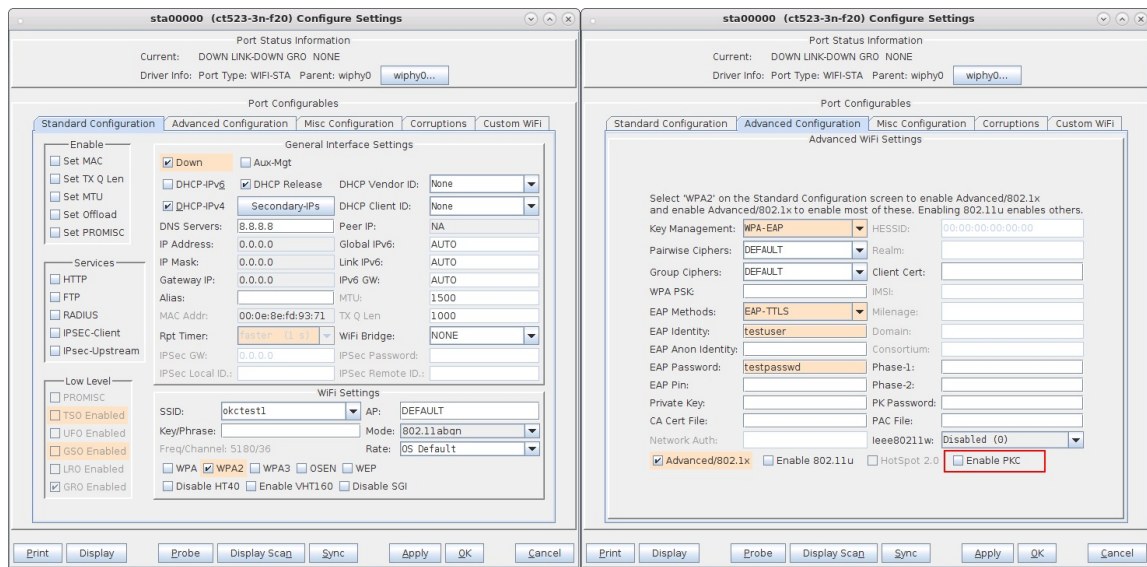
- ☐ HTTP
- ☐ FTP
- ☐ RADIUS
- ☐ IPSEC-Client
- ☐ IPsec-Upstream

Bridge Information

Configured Ports	Current Ports
vap0000	vap0000
vap0000_0	vap0000_0
vap0000_1	vap0000_1

vap0000_0
vap0000_1

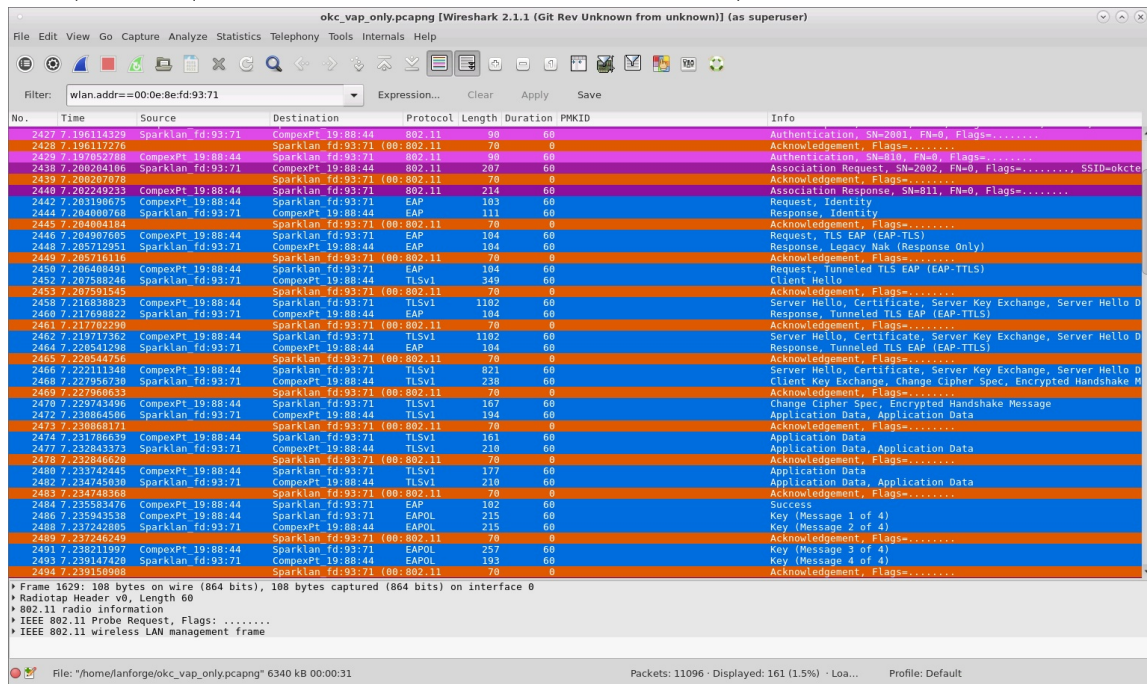
5. Modify a STA so that it is configured to connect to the SSID with 802.1X authentication for EAP-TTLS and with PKC disabled.



- 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	22.442317866		Sparklan fd:93:71 (00:802.11)		70	0		Acknowledgement, Flags=.....
7783	22.44333516	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	EAP	103	60		Deauthentication, SN=801, FN=0, Flags=.....
7786	22.443522930	Sparklan fd:93:71	Broadcast	802.11	106	0		Data, SrcIfs, Prio, Flags=.....
7787	22.443679548	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	EAP	98	60		Authentication, SN=885, FN=0, Flags=.....
7790	22.448169193	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	EAP	213	60		Reassociation Request, SN=2007, FN=0, Flags=....., SSID=okc
7791	22.448172100	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 (00:802.11)	EAP	214	60		Reassociation Response, SN=886, FN=0, Flags=.....
7794	22.450299508	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	EAP	103	60		Request, Identity
7796	22.451169477	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	EAP	111	60		Response, Identity
7797	22.451172921	Sparklan fd:93:71	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7798	22.452154787	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	EAP	104	60		Request, TLS EAP (EAP-TLS)
7800	22.453045244	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	EAP	104	60		Response, Legacy Nak (Response Only)
7801	22.453046071	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 (00:802.11)	EAP	104	60		Request, Tunnelled TLS EAP (EAP-TTLS)
7807	22.455230935	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	TLSv1	287	60		Client Hello
7808	22.455232190	Sparklan fd:93:71	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7811	22.463808109	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	TLSv1	1102	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
7814	22.464758157	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	EAP	104	60		Response, Tunnelled TLS EAP (EAP-TTLS)
7815	22.464761370	Sparklan fd:93:71	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7817	22.467604000	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	TLSv1	1102	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
7820	22.468462206	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	EAP	104	60		Response, Tunnelled TLS EAP (EAP-TTLS)
7821	22.468465518	Sparklan fd:93:71	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7822	22.470149380	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	TLSv1	821	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
7828	22.470224958	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	TLSv1	238	60		Client Key Exchange, Change Cipher Spec, Encrypted Handshake M
7829	22.470228216	Sparklan fd:93:71 (00:802.11)	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7830	22.470092590	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	TLSv1	167	60		Change Cipher Spec, Encrypted Handshake Message
7832	22.479450238	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	TLSv1	194	60		Application Data, Application Data
7833	22.479454014	Sparklan fd:93:71 (00:802.11)	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7834	22.480411283	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	TLSv1	161	60		Application Data
7836	22.481608100	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	TLSv1	210	60		Application Data, Application Data
7837	22.481501407	Sparklan fd:93:71 (00:802.11)	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7842	22.482613018	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	TLSv1	177	60		Application Data
7844	22.483640964	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	TLSv1	210	60		Application Data, Application Data
7845	22.483650214	Sparklan fd:93:71 (00:802.11)	Sparklan fd:93:71 (00:802.11)	EAP	70	0		Acknowledgement, Flags=.....
7846	22.484618507	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	EAP	102	60		Success
7848	22.484942407	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	EAPOL	215	60		Key (Message 1 of 4)
7850	22.486455579	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	EAPOL	215	60		Key (Message 2 of 4)
7851	22.486459100	Sparklan fd:93:71 (00:802.11)	Sparklan fd:93:71 (00:802.11)	EAPOL	70	0		Acknowledgement, Flags=.....
7853	22.487663855	CompexPT 19:89:44	Sparklan fd:93:71 (00:802.11)	EAPOL	257	60		Key (Message 3 of 4)
7855	22.489793750	Sparklan fd:93:71	CompexPT 19:89:44 (00:802.11)	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=..., BI=100, SSID=cis
3362	8.887981831	Sparklan fd:93:71	ComexPT 19:89:44	802.11	98	60		Authentication, SN=1972, FN=0, Flags=...
3363	9.807946412	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3365	9.888939802	ComexPT 19:89:44	Sparklan fd:93:71	802.11	98	60		Authentication, SN=538, FN=0, Flags=...
3367	9.898414681	Sparklan fd:93:71	ComexPT 19:89:44	802.11	297	60		Association Request, SN=1973, FN=0, Flags=..., SSID=okcte
3368	9.898417644	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3372	9.894065644	ComexPT 19:89:44	Sparklan fd:93:71	EAP	103	60		Request, Identity
3374	9.89480189	Sparklan fd:93:71	ComexPT 19:89:44	EAP	111	60		Response, Identity
3375	9.894803319	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3376	9.895820840	ComexPT 19:89:44	Sparklan fd:93:71	EAP	104	60		Request, TLS EAP (EAP-TLS)
3378	9.896635222	Sparklan fd:93:71	ComexPT 19:89:44	EAP	104	60		Response, Legacy Nak (Response Only)
3379	9.896635818	Sparklan fd:93:71	ComexPT 19:89:44	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	9.901835328	Sparklan fd:93:71	ComexPT 19:89:44	TLV1	349	60		Client Hello
3386	9.901856761	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3388	9.914833088	ComexPT 19:89:44	Sparklan fd:93:71	TLV1	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	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3396	9.914833088	ComexPT 19:89:44	Sparklan fd:93:71	TLV1	1102	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
3398	9.914745411	Sparklan fd:93:71	ComexPT 19:89:44	EAP	104	60		Response, Tunnelled TLS EAP (EAP-TTLS)
3400	9.914831446	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3401	9.916459939	ComexPT 19:89:44	Sparklan fd:93:71	TLV1	821	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
3404	9.921804305	Sparklan fd:93:71	ComexPT 19:89:44	TLV1	730	60		Client Key Exchange, Change Cipher Spec, Encrypted Handshake M
3405	9.921808265	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3406	9.923741357	ComexPT 19:89:44	Sparklan fd:93:71	TLV1	167	60		Change Cipher Spec, Encrypted Handshake Message
3408	9.924809155	Sparklan fd:93:71	ComexPT 19:89:44	TLV1	194	60		Application Data: Application Data
3409	9.924803484	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3411	9.925799957	ComexPT 19:89:44	Sparklan fd:93:71	TLV1	161	60		Application Data
3413	9.926571821	Sparklan fd:93:71	ComexPT 19:89:44	TLV1	218	60		Application Data: Application Data
3414	9.926745115	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3415	9.927531355	ComexPT 19:89:44	Sparklan fd:93:71	TLV1	177	60		Application Data
3417	9.928456896	Sparklan fd:93:71	ComexPT 19:89:44	TLV1	218	60		Application Data: Application Data
3418	9.928486922	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3419	9.929345523	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	9.931800405	Sparklan fd:93:71	ComexPT 19:89:44	EAPOL	215	60		Key (Message 2 of 4)
3424	9.931811596	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
3425	9.931713880	ComexPT 19:89:44	Sparklan fd:93:71	EAPOL	257	60		Key (Message 3 of 4)
3427	9.932607149	Sparklan fd:93:71	ComexPT 19:89:44	EAPOL	193	60		Key (Message 4 of 4)
3428	9.932604058	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...

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

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.

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=jw
7242	20.716443811	Sparklan c1:fb:01	Sparklan fd:93:71	802.11	255	0		Probe Response, SN=3232, FN=0, Flags=..., BI=240, SSID=f
7244	20.716748791	Sparklan 4b:c0:2f	Sparklan fd:93:71	802.11	213	0		Probe Response, SN=2734, FN=0, Flags=..., BI=240, SSID=br
7246	20.717262058	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	20.71835647	ComexPT f2:ea:bd	Sparklan fd:93:71	802.11	254	60		Probe Response, SN=447, FN=0, Flags=..., BI=240, SSID=jw
7251	20.718823352	ComexPT c2:fd:b0	Sparklan fd:93:71	802.11	240	60		Probe Response, SN=1648, FN=0, Flags=..., BI=240, SSID=be
7252	20.719284338	ComexPT c2:fd:b0	Sparklan fd:93:71	802.11	240	60		Probe Response, SN=1648, FN=0, Flags=..., BI=240, SSID=be
7254	20.719741412	2c:33:11:d8:1b:ad	Sparklan fd:93:71	802.11	371	60		Probe Response, SN=478, FN=0, Flags=..., BI=100, SSID=cis
7259	20.746228843	Sparklan fd:93:71	ComexPT 19:89:44	802.11	90	44		QoS Null function (No data), SN=0, FN=0, Flags=..., T
7270	20.746245723	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
7271	20.746457972	Sparklan fd:93:71	ComexPT 19:89:44	802.11	86	60		QoS Null function (No data), SN=0, FN=0, Flags=..., T
7272	20.746440083	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=...
8173	23.580597968	Sparklan fd:93:71	ComexPT 19:88:44	802.11	98	60		Authentication, SN=1977, FN=0, Flags=...
8174	23.580608910	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=...
8175	23.580610000	ComexPT 19:88:44	Sparklan fd:93:71	802.11	70	0		Authentication, SN=597, FN=0, Flags=...
8177	23.582131211	Sparklan fd:93:71	Broadcast	802.11	106	0		Data, SN=10, FN=0, Flags=p...F.
8178	23.582134319	ComexPT 19:88:44	Sparklan fd:93:71	802.11	98	60		Authentication, SN=597, FN=0, Flags=...
8181	23.585334727	Sparklan fd:93:71	ComexPT 19:88:44	802.11	231	60	424934013b5091d609edd4db69e14dd	Reassociation Request, SN=1978, FN=0, Flags=..., SSID=okc
8182	23.595373617	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=...
8184	23.596403046	ComexPT 19:88:44	Sparklan fd:93:71	802.11	214	60		Reassociation Response, SN=598, FN=0, Flags=...
8186	23.580883435	ComexPT 19:88:44	Sparklan fd:93:71	EAPOL	215	60		Key (Message 1 of 4)
8188	23.590784906	Sparklan fd:93:71	ComexPT 19:88:44	EAPOL	233	60	424934013b5091d609edd4db69e14dd	Key (Message 2 of 4)
8189	23.590788289	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=...
8190	23.589980223	ComexPT 19:88:44	Sparklan fd:93:71	EAPOL	257	60		Key (Message 3 of 4)
8192	23.510862242	Sparklan fd:93:71	ComexPT 19:88:44	EAPOL	193	60		Key (Message 4 of 4)
8193	23.510965550	Sparklan fd:93:71	ComexPT 19:88:44	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	23.521063722	Sparklan fd:93:71	ComexPT 19:88:44	802.11	93	60		Action, SN=1979, FN=0, Flags=...
8201	23.521066725	Sparklan fd:93:71	ComexPT 19:88:44	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	IPv6mcast 16	802.11	190	44		QoS Data, SN=0, FN=0, Flags=p...T
8205	23.521902846	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=...
8206	23.522338099	Sparklan fd:93:71	IPv6mcast 16	802.11	184	0		Data, SN=0, FN=0, Flags=p...F.
8464	24.221222475	Sparklan fd:93:71	IPv6mcast 16	802.11	190	60		QoS Data, SN=1, FN=0, Flags=p...T
8465	24.221224323	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=...
8466	24.221696231	Sparklan fd:93:71	IPv6mcast 16	802.11	184	0		Data, SN=1, FN=0, Flags=p...F.
9784	28.062035477	Sparklan fd:93:71	IPv6mcast 02	802.11	170	44		QoS Data, SN=2, FN=0, Flags=p...T
9785	28.062043402	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=...
9786	28.062519511	Sparklan fd:93:71	IPv6mcast 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%) · Load... 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.

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

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:

The screenshot shows a Wireshark packet capture of a network interface. The filter is set to `wlan.addr==00:0e:8e:fd:93:71`. The packet list shows a series of frames from the Sparklan interface to the wlan0 interface. The packet details pane shows the following information for the selected packet (No. 2249):

- Frame 2249: 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

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.

The screenshot shows a Wireshark packet capture of a network interface. The filter is set to `wlan.addr==00:0e:8e:fd:93:71`. The packet list shows a series of frames from the Sparklan interface to the wlan0 interface. The packet details pane shows the following information for the selected packet (No. 8331):

- Frame 8331: 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

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

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:

okc_sta_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
2588	9.362903125	2c:33:11:d8:1b:ad	Sparklan fd:93:71	802.11	371	60		Probe Response, SN=417, FN=0, Flags=....., BI=100, SSID=okcte
3411	9.708844182	Sparklan fd:93:71	ComexPT 19:89:44	802.11	98	60		Authentication, SN=1943, FN=0, Flags=.....
3412	9.708847018	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3413	9.708901375	ComexPT 19:89:44	Sparklan fd:93:71	802.11	98	60		Authentication, SN=480, FN=0, Flags=.....
3415	9.710450178	Sparklan fd:93:71	ComexPT 19:89:44	802.11	207	60		Association Request, SN=1944, FN=0, Flags=....., SSID=okcte
3416	9.710461023	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3417	9.712226675	ComexPT 19:89:44	Sparklan fd:93:71	802.11	214	60		Association Response, SN=481, FN=0, Flags=.....
3419	9.713546576	ComexPT 19:89:44	Sparklan fd:93:71	EAP	103	60		Request, Identity
3422	9.714612174	Sparklan fd:93:71	ComexPT 19:89:44	EAP	111	60		Response, Identity
3423	9.714710107	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3424	9.715549601	ComexPT 19:89:44	Sparklan fd:93:71	EAP	104	60		Request, TLS EAP (EAP-TLS)
3427	9.719377205	Sparklan fd:93:71	ComexPT 19:89:44	EAP	104	60		Response, Legacy Nak (Response Only)
3428	9.720308028	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3429	9.720956928	ComexPT 19:89:44	Sparklan fd:93:71	EAP	104	60		Request, Tunnelled TLS EAP (EAP-TTLS)
3431	9.721234891	Sparklan fd:93:71	ComexPT 19:89:44	TLVsv1	349	60		Client Hello
3432	9.722238223	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3433	9.722762430	ComexPT 19:89:44	Sparklan fd:93:71	TLVsv1	102	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
3435	9.728597461	Sparklan fd:93:71	ComexPT 19:89:44	EAP	104	60		Response, Tunnelled TLS EAP (EAP-TTLS)
3436	9.728510931	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3437	9.728484806	ComexPT 19:89:44	Sparklan fd:93:71	TLVsv1	102	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
3439	9.731281018	Sparklan fd:93:71	ComexPT 19:89:44	EAP	104	60		Response, Tunnelled TLS EAP (EAP-TTLS)
3440	9.731284448	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3441	9.732261692	ComexPT 19:89:44	Sparklan fd:93:71	TLVsv1	221	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
3445	9.740608952	Sparklan fd:93:71	ComexPT 19:89:44	TLVsv1	238	60		Client Key Exchange, Change Cipher Spec, Encrypted Handshake M
3446	9.740692992	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3447	9.742578219	ComexPT 19:89:44	Sparklan fd:93:71	TLVsv1	167	60		Change Cipher Spec, Encrypted Handshake Message
3449	9.743700740	Sparklan fd:93:71	ComexPT 19:89:44	TLVsv1	194	60		Application Data, Application Data
3450	9.743783760	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3451	9.744752445	ComexPT 19:89:44	Sparklan fd:93:71	TLVsv1	161	60		Application Data
3453	9.745609071	Sparklan fd:93:71	ComexPT 19:89:44	TLVsv1	210	60		Application Data, Application Data
3454	9.745692518	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3455	9.746612062	ComexPT 19:89:44	Sparklan fd:93:71	TLVsv1	177	60		Application Data
3459	9.747548729	Sparklan fd:93:71	ComexPT 19:89:44	TLVsv1	210	60		Application Data, Application Data
3459	9.747552126	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3461	9.748608317	ComexPT 19:89:44	Sparklan fd:93:71	EAP	102	60		Success
3462	9.749071678	ComexPT 19:89:44	Sparklan fd:93:71	EAPOL	215	60		Key (Message 1 of 4)
3465	9.750372572	Sparklan fd:93:71	ComexPT 19:89:44	EAPOL	215	60		Key (Message 2 of 4)
3466	9.750326176	Sparklan fd:93:71	ComexPT 19:89:44	802.11	70	0		Acknowledgement, Flags=.....
3467	9.751019106	ComexPT 19:89:44	Sparklan fd:93:71	EAPOL	257	60		Key (Message 3 of 4)
3469	9.752339109	Sparklan fd:93:71	ComexPT 19:89:44	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

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.

okc_sta_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
8680	24.829669678	ComexPT 19:89:44	Sparklan fd:93:71	802.11	70	0		Acknowledgement, Flags=.....
8681	24.830093528	ComexPT 19:89:44	Sparklan fd:93:71	802.11	60	60		Authentication, SN=550, FN=0, Flags=.....
8682	24.830093528	Sparklan fd:93:71	Broadcast	802.11	106	60		Authentication, SN=550, FN=0, Flags=.....
8684	24.830938568	ComexPT 19:88:44	Sparklan fd:93:71	802.11	98	60		Authentication, SN=548, FN=0, Flags=.....
8686	24.834493647	Sparklan fd:93:71	ComexPT 19:88:44	802.11	231	60	dc60e086ded24f862297e94fa2b39b4	Reassociation Request, SN=1949, FN=0, Flags=....., SSID=okcte
8687	24.834496922	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8688	24.835456431	ComexPT 19:88:44	Sparklan fd:93:71	802.11	214	60		Reassociation Response, SN=547, FN=0, Flags=.....
8690	24.837139203	ComexPT 19:88:44	Sparklan fd:93:71	EAP	103	60		Request, Identity
8692	24.838297278	Sparklan fd:93:71	ComexPT 19:88:44	EAP	111	60		Response, Identity
8693	24.838300125	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8694	24.839225546	ComexPT 19:88:44	Sparklan fd:93:71	EAP	104	60		Request, TLS EAP (EAP-TLS)
8696	24.840603305	Sparklan fd:93:71	ComexPT 19:88:44	EAP	104	60		Response, Legacy Nak (Response Only)
8697	24.840607005	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8698	24.840764926	ComexPT 19:88:44	Sparklan fd:93:71	EAP	104	60		Request, Tunnelled TLS EAP (EAP-TTLS)
8700	24.842407557	Sparklan fd:93:71	ComexPT 19:88:44	TLVsv1	287	60		Client Hello
8701	24.842411011	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8703	24.840955037	ComexPT 19:88:44	Sparklan fd:93:71	TLVsv1	1102	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
8705	24.849765212	Sparklan fd:93:71	ComexPT 19:88:44	EAP	104	60		Response, Tunnelled TLS EAP (EAP-TTLS)
8706	24.849768405	ComexPT 19:88:44	Sparklan fd:93:71	802.11	70	0		Acknowledgement, Flags=.....
8707	24.851081053	ComexPT 19:88:44	Sparklan fd:93:71	TLVsv1	102	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
8709	24.852808129	Sparklan fd:93:71	ComexPT 19:88:44	EAP	104	60		Response, Tunnelled TLS EAP (EAP-TTLS)
8710	24.852811503	ComexPT 19:88:44	Sparklan fd:93:71	802.11	70	0		Acknowledgement, Flags=.....
8711	24.854466327	ComexPT 19:88:44	Sparklan fd:93:71	TLVsv1	821	60		Server Hello, Certificate, Server Key Exchange, Server Hello D
8714	24.859616192	Sparklan fd:93:71	ComexPT 19:88:44	TLVsv1	238	60		Client Key Exchange, Change Cipher Spec, Encrypted Handshake M
8715	24.859641877	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8716	24.861310220	ComexPT 19:88:44	Sparklan fd:93:71	TLVsv1	167	60		Change Cipher Spec, Encrypted Handshake Message
8718	24.862535899	Sparklan fd:93:71	ComexPT 19:88:44	TLVsv1	194	60		Application Data, Application Data
8719	24.862568787	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8720	24.864889838	ComexPT 19:88:44	Sparklan fd:93:71	TLVsv1	161	60		Application Data
8723	24.865018070	Sparklan fd:93:71	ComexPT 19:88:44	TLVsv1	210	60		Application Data, Application Data
8724	24.865823366	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8725	24.866660154	ComexPT 19:88:44	Sparklan fd:93:71	TLVsv1	177	60		Application Data
8727	24.867571520	Sparklan fd:93:71	ComexPT 19:88:44	TLVsv1	210	60		Application Data, Application Data
8728	24.867575842	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8729	24.868578312	ComexPT 19:88:44	Sparklan fd:93:71	EAP	102	60		Success
8731	24.868083422	ComexPT 19:88:44	Sparklan fd:93:71	EAPOL	215	60		Key (Message 1 of 4)
8733	24.870254506	Sparklan fd:93:71	ComexPT 19:88:44	EAPOL	233	60	dc60e086ded24f862297e94fa2b39b4	Key (Message 2 of 4)
8734	24.870257998	Sparklan fd:93:71	ComexPT 19:88:44	802.11	70	0		Acknowledgement, Flags=.....
8735	24.870877518	ComexPT 19:88:44	Sparklan fd:93:71	EAPOL	257	60		Key (Message 3 of 4)
8737	24.871892955	Sparklan fd:93:71	ComexPT 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