



Active Expert Bench Testing  
Subject: Apple Mac Roaming  
Date: 7/25/2017  
Author: George Stefanick

Mac Book - 2016 model  
OS: Sierra

In this exercise we will examine two roaming events with a Mac Book Pro confirming roaming behavior. Since the Mac Book Pro doesn't support advance roaming algorithms, you will observe full 802.1X authentications, whereby the Mac Book will communicate to the WLC, WLC will communicate to Radius, Radius then communicates to AD. The proverbial pulling the cable from the wall and plugging to back in during each roam. The lack of advance roaming keys can cause blips with realtime applications.

Mac Books do support SKC which we will examine as well. SKC is also called sticky key, fast roam back, PMK cache, and static PMKID. SKC is not a recommend approach for enterprise deployments. The Mac Book will do full 802.1X roams initially to the access point and fast roam back during reassociations.

<https://support.apple.com/en-us/HT206207>

APPLE:

Roam performance

Roam performance describes how long a client needs to authenticate successfully to a new BSSID.

Finding a valid network and AP is only part of the process. The client must complete the roam process quickly and without interruption, so the user doesn't experience downtime. Roaming involves the client authenticating against the new BSSID and deauthenticating from the current BSSID. The security and authentication method determines how quickly this can happen.

First, 802.1X-based authentication requires the client to complete the entire EAP key exchange. Then, it can deauthenticate from the current BSSID. Depending on the environment's authentication infrastructure, this might take several seconds. End users could experience interrupted service in the form of dead air.

macOS supports static PMKID (Pairwise Master Key identifier) caching to help optimize roaming between BSSIDs in the same ESSID. macOS doesn't support Fast BSS Transition, also known as 802.11r. You don't have to deploy additional SSIDs to support macOS because macOS interoperates with 802.11r.

## MAC BOOK PRO ROAMING EXAMINED - OKC

Roaming Event #1 - 11:03 - BSSID: Cisco96:80:E5

```
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Processing assoc-req station:98:01:a7:a0:96:b7 AP:7c:95:f3:96:80:e0-01 thread:1a6c8558
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 trying to join WLAN with RSSI 205. Checking for XOR roam conditions on AP: 7C:95:F3:96:80:E0 Slot: 1
```

### \* Here you see the mac book doing a new association to access point 96:80:e0

```
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 is associating to AP 7C:95:F3:96:80:E0 which is not XOR roam capable
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Reassociation received from mobile on BSSID 7c:95:f3:96:80:e5 AP TEST-HHDC-122-A-36021
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 trying to join WLAN with RSSI 205. Checking for XOR roam conditions on AP: 7C:95:F3:96:80:E0 Slot: 1
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 is associating to AP 7C:95:F3:96:80:E0 which is not XOR roam capable
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Global 200 Clients are allowed to AP radio
*apfMsConnTask_4: Jul 18 11:03:54.917: 98:01:a7:a0:96:b7 Max Client Trap Threshold: 0 cur: 7
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 override for default ap group, marking intgrp NULL
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Applying Interface(production_data) policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 246
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Re-applying interface policy for client
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2931)
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing Uri ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2951)
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv6 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2972)
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 apfApplyWlanPolicy: Retaining (ACL [255] / Flexconnect ACL [65535]) received in AAA attributes on mobile
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type, Tunnel User - 0
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Setting the NAS Id to WLAN specific Id 'HH-5508-A'
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 In processSsidIE:6458 setting Central switched to TRUE
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 In processSsidIE:6461 apVapId = 11 and Split Acl Id = 65535
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Applying site-specific Local Bridging override for station 98:01:a7:a0:96:b7 - vapId 11, site 'TEST_OFFNET', interface 'production_data'
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Applying Local Bridging Interface Policy for station 98:01:a7:a0:96:b7 - vlan 246, interface id 14, interface 'production_data'
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 override from ap group, removing intf group from mscb
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Applying site-specific override for station 98:01:a7:a0:96:b7 - vapId 11, site 'TEST_OFFNET', interface 'production_data'
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Applying Interface(production_data) policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 246
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Re-applying interface policy for client
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2931)
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing Uri ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2951)
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 Setting the NAS Id to AP group specific Id 'HHDC-5508-TEST-B'
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 processSsidIE statusCode is 0 and status is 0
*apfMsConnTask_4: Jul 18 11:03:54.918: 98:01:a7:a0:96:b7 processSsidIE ssid_done_flag is 0 finish_flag is 0
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 STA - rates (B): 140 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 suppRates statusCode is 0 and gotSuppRatesElement is 1
*apfMsConnTask_4: Jul 18 11:03:54.919: RSNIE in Assoc. Req.: (38)
*apfMsConnTask_4: Jul 18 11:03:54.919: [0000] 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f
*apfMsConnTask_4: Jul 18 11:03:54.919: [0016] ac 01 00 00 01 00 87 37 9b 53 f0 1b 03 3e bd e1
*apfMsConnTask_4: Jul 18 11:03:54.919: [0032] 5b 0f fb 9a 3e ea
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Processing RSN IE type 48, length 38 for mobile 98:01:a7:a0:96:b7
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Received 802.11i 802.1X key management suite, enabling dot1x Authentication
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 RSN Capabilities: 0
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Marking Mobile as non-11w Capable
```

### \* During the Mac Book's first authentication it created a PMKID. During reassociation the Mac Book presents this PMKID to the new access point. This is what you are seeing here:

```
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Received RSN IE with 1 PMKIDs from mobile 98:01:a7:a0:96:b7
*apfMsConnTask_4: Jul 18 11:03:54.919: Received PMKID: (16)
```

```
*apfMsConnTask_4: Jul 18 11:03:54.919: [0000] 87 37 9b 53 f0 1b 03 3e bd e1 5b 0f fb 9a 3e ea
```

### \* The controller searches for the PMKID in cache, but there is no valid PMKID in cache. The reason for this because the Mac Book doesn't support OKC or 802.11r.

```
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Searching for PMKID in MSCB PMKID cache for mobile 98:01:a7:a0:96:b7
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 No valid PMKID found in the MSCB PMKID cache for mobile 98:01:a7:a0:96:b7
*apfMsConnTask_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Trying to compute a PMKID from MSCB PMK cache for mobile 98:01:a7:a0:96:b7
*apfMsConnTask_4: Jul 18 11:03:54.919: CCKM: Find PMK in cache: BSSID = (6)
*apfMsConnTask_4: Jul 18 11:03:54.919: [0000] 7c 95 f3 96 80 e0
*apfMsConnTask_4: Jul 18 11:03:54.919: CCKM: Find PMK in cache: realAA = (6)
*apfMsConnTask_4: Jul 18 11:03:54.919: [0000] 7c 95 f3 96 80 e5
*apfMsConnTask_4: Jul 18 11:03:54.919: CCKM: Find PMK in cache: PMKID = (16)
```

\*apfMsConnTask\_4: Jul 18 11:03:54.919: [0000] 87 37 9b 53 f0 1b 03 3e bd e1 5b 0f fb 9a 3e ea

\*apfMsConnTask\_4: Jul 18 11:03:54.919: CCKM: AA (6)

\*apfMsConnTask\_4: Jul 18 11:03:54.919: [0000] 7c 95 f3 96 80 e5

\*apfMsConnTask\_4: Jul 18 11:03:54.919: CCKM: SPA (6)

\*apfMsConnTask\_4: Jul 18 11:03:54.919: [0000] 98 01 a7 a0 96 b7

## \* The controller then tries to compute the PMKID PMK cache. There is no record of the PMK cache.

\*apfMsConnTask\_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Unable to compute a valid PMKID from MSCB PMK cache for mobile 98:01:a7:a0:96:b7

\*apfMsConnTask\_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Searching for PMK in global PMK cache for mobile 98:01:a7:a0:96:b7

\*apfMsConnTask\_4: Jul 18 11:03:54.919: 98:01:a7:a0:96:b7 Found an entry in the global PMK cache for station 98:01:a7:a0:96:b7

\*apfMsConnTask\_4: Jul 18 11:03:54.919: CCKM: AA (6)

\*apfMsConnTask\_4: Jul 18 11:03:54.919: [0000] 7c 95 f3 96 80 e5

\*apfMsConnTask\_4: Jul 18 11:03:54.920: CCKM: SPA (6)

\*apfMsConnTask\_4: Jul 18 11:03:54.920: [0000] 98 01 a7 a0 96 b7

\*apfMsConnTask\_4: Jul 18 11:03:54.920: dot1xDoesPmkIdMatchPmk2, Received 11w Flag: 0

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 Unable to compute a valid PMKID from global PMK cache for mobile 98:01:a7:a0:96:b7

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 Setting active key cache index 0 --> 8

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 unsetting PmkIdValidatedByAp

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 pemApfDeleteMobileStation2: APF\_MS\_PEM\_WAIT\_L2\_AUTH\_COMPLETE = 0.

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Deleted mobile LWAPP rule on AP [6c:50:4d:ab:2a:20]

\*pemReceiveTask: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 10.246.36.69 Removed NPU entry.

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 Updated location for station old AP 6c:50:4d:ab:2a:20-1, new AP 7c:95:f3:96:80:e0-1

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 apfMsRunStateDec

\*spamApTask5: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 Delete Mobile request sent to the AP 10.101.1.113:37772

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 apfMs1xStateDec

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Change state to START (0) last state RUN (20)

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 pemApfAddMobileStation2: APF\_MS\_PEM\_WAIT\_L2\_AUTH\_COMPLETE = 0.

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 10.246.36.69 START (0) Initializing policy

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 10.246.36.69 START (0) Change state to AUTHCHECK (2) last state START (0)

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 10.246.36.69 AUTHCHECK (2) Change state to 8021X\_REQD (3) last state AUTHCHECK (2)

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 Encryption policy is set to 0x80000001

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 Not Using WMM Compliance code qosCap 00

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 10.246.36.69 8021X\_REQD (3) Plumbed mobile LWAPP rule on AP 7c:95:f3:96:80:e0 vapid11 apVapId 11 flex-acl-name:

\*apfMsConnTask\_4: Jul 18 11:03:54.920: 98:01:a7:a0:96:b7 apfPemAddUser2 (apf\_policy.c:437) Changing state for mobile 98:01:a7:a0:96:b7 on AP 7c:95:f3:96:80:e0 from Associated to Associated

\*apfMsConnTask\_4: Jul 18 11:03:54.921: 98:01:a7:a0:96:b7 apfPemAddUser2:session timeout forstation 98:01:a7:a0:96:b7 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0

\*apfMsConnTask\_4: Jul 18 11:03:54.921: 98:01:a7:a0:96:b7 Stopping deletion of Mobile Station: callerId: 48

\*apfMsConnTask\_4: Jul 18 11:03:54.921: 98:01:a7:a0:96:b7 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

\*apfMsConnTask\_4: Jul 18 11:03:54.921: 98:01:a7:a0:96:b7 Sending assoc-resp with status 0 station:98:01:a7:a0:96:b7 AP:7c:95:f3:96:80:e0-01 on apVapId 11

\*apfMsConnTask\_4: Jul 18 11:03:54.923: 98:01:a7:a0:96:b7 Sending Assoc Response to station on BSSID 7c:95:f3:96:80:e5 (status 0) ApVapId 11 Slot 1

\*apfMsConnTask\_4: Jul 18 11:03:54.921: 98:01:a7:a0:96:b7 apfProcessAssocReq (apf\_80211.c:10884) Changing state for mobile 98:01:a7:a0:96:b7 on AP 7c:95:f3:96:80:e0 from Associated to Associated

\*spamApTask6: Jul 18 11:03:54.921: 98:01:a7:a0:96:b7 Successful transmission of LWAPP Add-Mobile to AP 7c:95:f3:96:80:e0

\*spamApTask6: Jul 18 11:03:54.923: 98:01:a7:a0:96:b7 Received ADD\_MOBILE ack - Initiating 1x to STA 98:01:a7:a0:96:b7 (idx 60)

\*spamApTask6: Jul 18 11:03:54.923: 98:01:a7:a0:96:b7 Sent dot1x auth initiate message for mobile 98:01:a7:a0:96:b7

## \* What you observe next is a full 802.1X authentication.

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.923: 98:01:a7:a0:96:b7 reauth\_sm state transition 0 --> 0 for mobile 98:01:a7:a0:96:b7 at 1x\_reauth\_sm.c:53

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.923: 98:01:a7:a0:96:b7 EAP-PARAM Debug - eap-params for Wan-Id :11 is disabled - applying Global eap timers and retries

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.924: 98:01:a7:a0:96:b7 Disable re-auth, use PMK lifetime.

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.924: 98:01:a7:a0:96:b7 dot1x - moving mobile 98:01:a7:a0:96:b7 into Connecting state

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.924: 98:01:a7:a0:96:b7 Sending EAP-Request/Identity to mobile 98:01:a7:a0:96:b7 (EAP Id 1)

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.934: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.934: 98:01:a7:a0:96:b7 Received Identity Response (count=1) from mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.934: 98:01:a7:a0:96:b7 Reseting reauth count 1 to 0 for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.934: 98:01:a7:a0:96:b7 EAP State update from Connecting to Authenticating for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.934: 98:01:a7:a0:96:b7 dot1x - moving mobile 98:01:a7:a0:96:b7 into Authenticating state

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.937: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.937: 98:01:a7:a0:96:b7 Processing Access-Challenge for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.937: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=77) for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.937: 98:01:a7:a0:96:b7 WARNING: updated EAP-Identifier 1 ==> 77 for STA 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.937: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 77)

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.943: 98:01:a7:a0:96:b7 Allocating EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.943: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.943: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 77, EAP Type 25)

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.943: 98:01:a7:a0:96:b7 Reseting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.943: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.945: 98:01:a7:a0:96:b7 Processing Access-Challenge for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.945: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=78) for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.945: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 78)

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.955: 98:01:a7:a0:96:b7 Reusing allocated memory for EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.955: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.955: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 78, EAP Type 25)

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.955: 98:01:a7:a0:96:b7 Reseting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.955: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.960: 98:01:a7:a0:96:b7 Processing Access-Challenge for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.960: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=79) for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.960: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 79)

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.962: 98:01:a7:a0:96:b7 Reusing allocated memory for EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.962: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.962: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 79, EAP Type 25)

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.962: 98:01:a7:a0:96:b7 Reseting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.962: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.968: 98:01:a7:a0:96:b7 Processing Access-Accept for mobile 98:01:a7:a0:96:b7

\*Dot1x\_NW\_MsgTask\_7: Jul 18 11:03:54.968: 98:01:a7:a0:96:b7 Reseting web IPv4 acl from 255 to 255

## Roaming Event #2 - 11:05 - BSSID: CiscoAA:E1:A0

### \* Here you see the Mac Book does a new association to access point AA:E1:A0

```
*apfMsConnTask_2: Jul 18 11:05:52.730: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 is associating to AP 6C:50:4D:AA:E1:A0 which is not XOR roam capable
*apfMsConnTask_2: Jul 18 11:05:52.730: 98:01:a7:a0:96:b7 Reassociation received from mobile on BSSID 6c:50:4d:aa:e1:a5 AP HH-DC-3-3502f
*apfMsConnTask_2: Jul 18 11:05:52.730: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 trying to join WLAN with RSSI 207. Checking for XOR roam conditions on AP: 6C:50:4D:AA:E1:A0 Slot: 1
*apfMsConnTask_2: Jul 18 11:05:52.730: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 is associating to AP 6C:50:4D:AA:E1:A0 which is not XOR roam capable
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Global 200 Clients are allowed to AP radio
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Max Client Trap Threshold: 0 cur: 4
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Rf profile 600 Clients are allowed to AP wlan
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 override for default ap group, marking intgrp NULL
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Applying Interface(production_data) policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 246
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Re-applying interface policy for client
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2931)
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing Url ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apt_policy.c:2951)
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv6 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2972)
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 apfApplyWlanPolicy: Retaining ACL [255] / Flexconnect ACL [65535] received in AAA attributes on mobile
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type, Tunnel User - 0
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Setting the NAS Id to WLAN specific Id 'HH-5508-A'
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 In processSsidE:6469 setting Central switched to TRUE
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 In processSsidE:6461 apVapId = 11 and Split Acl Id = 65535
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Applying site-specific Local Bridging override for station 98:01:a7:a0:96:b7 - vapId 11, site 'TEST_OFFNET', interface 'production_data'
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Applying Local Bridging Interface Policy for station 98:01:a7:a0:96:b7 - vlan 246, interface id 14, interface 'production_data'
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 override from ap group, removing intf group from mscb
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Applying site-specific override for station 98:01:a7:a0:96:b7 - vapId 11, site 'TEST_OFFNET', interface 'production_data'
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Applying Interface(production_data) policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 246
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 Re-applying interface policy for client
```

```
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2931)
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing Url ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apt_policy.c:2951)
*apfMsConnTask_2: Jul 18 11:05:52.731: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv6 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2972)
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 Setting the NAS Id to AP group specific Id 'HHDC-5508-TEST-B'
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 processSsidE statusCode is 0 and status is 0
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 processSsidE ssid_done_flag is 0 finish_flag is 0
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 STA - rates (B): 140 18 24 36 48 72 96 108 0 0 0 0 0 0 0
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 suppRates statusCode is 0 and gotSuppRatesElement is 1
*apfMsConnTask_2: Jul 18 11:05:52.732: RSNIE in Assoc. Req.: (38)
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0000] 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0016] ac 01 00 00 01 00 51 33 11 cd c4 9e 40 1f 56 50
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0032] 8a 95 a0 04 29 c5
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 Processing RSN IE type 48, length 38 for mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7
```

```
comp128 is enabled
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 Received 802.11i 802.1X key management suite, enabling dot1x Authentication
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 RSN Capabilities: 0
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 Marking Mobile as non-11w Capable
```

### \* Again the Mac Book presents the PMKID in the association phase.

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 Received RSN IE with 1 PMKIDs from mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: Received PMKID: (16)
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0000] 51 33 11 cd c4 9e 40 1f 56 50 8a 95 a0 04 29 c5
```

### \* The controller searches for the PMKID in cache, but there is no validate PMKID in cache. The reason for this is the Mac Book doesn't support OKC or 802.11r.

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 Searching for PMKID in MSCB PMKID cache for mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 No valid PMKID found in the MSCB PMKID cache for mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: 98:01:a7:a0:96:b7 Trying to compute a PMKID from MSCB PMK cache for mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: CCKM: Find PMK in cache: BSSID = (6)
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0000] 6c 50 4d aa e1 a0
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: CCKM: Find PMK in cache: realAA = (6)
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0000] 6c 50 4d aa e1 a5
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: CCKM: Find PMK in cache: PMKID = (16)
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0000] 51 33 11 cd c4 9e 40 1f 56 50 8a 95 a0 04 29 c5
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: CCKM: AA (6)
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0000] 6c 50 4d aa e1 a5
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: CCKM: SPA (6)
```

```
*apfMsConnTask_2: Jul 18 11:05:52.732: [0000] 98 01 a7 a0 96 b7
```

## \* The controller then tries to compute the PMKID PMK cache. There is no record of the PMK cache.

```
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Unable to compute a valid PMKID from MSCB PMK cache for mobile 98:01:a7:a0:96:b7
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Searching for PMK in global PMK cache for mobile 98:01:a7:a0:96:b7
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Found an entry in the global PMK cache for station 98:01:a7:a0:96:b7
*apfMsConnTask_2: Jul 18 11:05:52.733: CCKM: AA (6)

*apfMsConnTask_2: Jul 18 11:05:52.733: [0000] 6c 50 4d aa e1 a5

*apfMsConnTask_2: Jul 18 11:05:52.733: CCKM: SPA (6)

*apfMsConnTask_2: Jul 18 11:05:52.733: [0000] 98 01 a7 a0 96 b7

*apfMsConnTask_2: Jul 18 11:05:52.733: dot1xDoesPmkIdMatchPmk2, Received 11w Flag: 0
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Unable to compute a valid PMKID from global PMK cache for mobile 98:01:a7:a0:96:b7
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Setting active key cache index 0 ---> 8
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 unsetting PmkIdValidatedByAp
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Deleted mobile LWAPP rule on AP [dc:a5:f4:9d:e0:90]
*pemReceiveTask: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 10.246.36.69 Removed NPU entry.
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Updated location for station old AP dc:a5:f4:9d:e0:90-1, new AP 6c:50:4d:aa:e1:a0-1
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 apfMsRunStateDec
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 apfMs1xStateDec
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Change state to START (0) last state RUN (20)

*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 pemApfAddMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 10.246.36.69 START (0) Initializing policy
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 10.246.36.69 START (0) Change state to AUTHCHECK (2) last state START (0)

*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 10.246.36.69 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Encryption policy is set to 0x80000001
*apfMsConnTask_2: Jul 18 11:05:52.733: 98:01:a7:a0:96:b7 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 10.246.36.69 8021X_REQD (3) Plumbed mobile LWAPP rule on AP 6c:50:4d:aa:e1:a0 vapld 11 apVapld 11 flex-acl-name:
*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 apfPemAddUser2 (apf_policy.c:437) Changing state for mobile 98:01:a7:a0:96:b7 on AP 6c:50:4d:aa:e1:a0 from Associated to Associated

*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 apfPemAddUser2:session timeout for station 98:01:a7:a0:96:b7 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0
*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 Stopping deletion of Mobile Station: (callerId: 48)
*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0

*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 Sending assoc-req with status 0 station:98:01:a7:a0:96:b7 AP:6c:50:4d:aa:e1:a0-01 on apVapld 11
*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 Sending Assoc Response to station on BSSID 6c:50:4d:aa:e1:a5 (status 0) ApVapld 11 Slot 1
*apfMsConnTask_2: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 apfProcessAssocReq (apf_80211.c:10884) Changing state for mobile 98:01:a7:a0:96:b7 on AP 6c:50:4d:aa:e1:a0 from Associated to Associated

*spamApTask3: Jul 18 11:05:52.734: 98:01:a7:a0:96:b7 Delete Mobile request sent to the AP 10.101.1.80:41603

*spamApTask3: Jul 18 11:05:52.735: 98:01:a7:a0:96:b7 Successful transmission of LWAPP Add-Mobile to AP 6c:50:4d:aa:e1:a0
*spamApTask3: Jul 18 11:05:52.737: 98:01:a7:a0:96:b7 Received ADD_MOBILE ack - Initiating 1x to STA 98:01:a7:a0:96:b7 (idx 48)
*spamApTask3: Jul 18 11:05:52.737: 98:01:a7:a0:96:b7 Sent dot1x auth initiate message for mobile 98:01:a7:a0:96:b7
```

## \* What you observe next, again is a full 802.1X authentication.

```
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.737: 98:01:a7:a0:96:b7 reauth_sm state transition 0 ---> 0 for mobile 98:01:a7:a0:96:b7 at 1x_reauth_sm.c:53
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.737: 98:01:a7:a0:96:b7 EAP-PARAM Debug - eap-params for Wlan-Id :11 is disabled - applying Global eap timers and retries
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.737: 98:01:a7:a0:96:b7 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.737: 98:01:a7:a0:96:b7 dot1x - moving mobile 98:01:a7:a0:96:b7 into Connecting state
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.737: 98:01:a7:a0:96:b7 Sending EAP-Request/Identity to mobile 98:01:a7:a0:96:b7 (EAP Id 1)
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.744: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.744: 98:01:a7:a0:96:b7 Received Identity Response (count=1) from mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.744: 98:01:a7:a0:96:b7 Resetting reauth count 1 to 0 for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.744: 98:01:a7:a0:96:b7 EAP State update from Connecting to Authenticating for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.744: 98:01:a7:a0:96:b7 dot1x - moving mobile 98:01:a7:a0:96:b7 into Authenticating state
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.744: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.747: 98:01:a7:a0:96:b7 Processing Access-Challenge for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.747: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=154) for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.747: 98:01:a7:a0:96:b7 WARNING: updated EAP-Identifier 1 ==> 154 for STA 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.747: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 154)
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.747: 98:01:a7:a0:96:b7 Allocating EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.749: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.750: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 154, EAP Type 25)
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.750: 98:01:a7:a0:96:b7 Resetting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.750: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.751: 98:01:a7:a0:96:b7 Processing Access-Challenge for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.751: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=155) for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.752: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 155)
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.752: 98:01:a7:a0:96:b7 Reusing allocated memory for EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.755: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.755: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 155, EAP Type 25)
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.755: 98:01:a7:a0:96:b7 Resetting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.755: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.760: 98:01:a7:a0:96:b7 Processing Access-Challenge for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.760: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=156) for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.760: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 156)
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.760: 98:01:a7:a0:96:b7 Reusing allocated memory for EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.762: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.762: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 156, EAP Type 25)
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.762: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.762: 98:01:a7:a0:96:b7 Resetting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.762: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.768: 98:01:a7:a0:96:b7 Processing Access-Accept for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 11:05:52.768: 98:01:a7:a0:96:b7 Resetting web IPv4 acl from 255 to 255
```





```
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.219: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=136) for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.219: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 136)
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.219: 98:01:a7:a0:96:b7 Reusing allocated memory for EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.220: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.220: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 136, EAP Type 25)
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.220: 98:01:a7:a0:96:b7 Reseting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.220: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.222: 98:01:a7:a0:96:b7 Processing Access-Challenge for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.222: 98:01:a7:a0:96:b7 Entering Backend Auth Req state (id=137) for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.222: 98:01:a7:a0:96:b7 Sending EAP Request from AAA to mobile 98:01:a7:a0:96:b7 (EAP Id 137)
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.222: 98:01:a7:a0:96:b7 Reusing allocated memory for EAP Pkt for retransmission to mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.227: 98:01:a7:a0:96:b7 Received EAPOL EAPPKT from mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.227: 98:01:a7:a0:96:b7 Received EAP Response from mobile 98:01:a7:a0:96:b7 (EAP Id 137, EAP Type 25)
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.227: 98:01:a7:a0:96:b7 Reseting reauth count 0 to 0 for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.227: 98:01:a7:a0:96:b7 Entering Backend Auth Response state for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.234: 98:01:a7:a0:96:b7 Processing Access-Accept for mobile 98:01:a7:a0:96:b7
*Dot1x_NW_MsgTask_7: Jul 18 13:24:24.234: 98:01:a7:a0:96:b7 Reseting web IPv4 acl from 255 to 255
```

## \* Next we roamed the Mac Book to other access points and then back to access point 96:80:e0. This is what you observe here.

```
*apfMsConnTask_4: Jul 18 13:30:27.517: 98:01:a7:a0:96:b7 Reassociation received from mobile on BSSID 7c:95:f3:96:80:e2 AP TEST-HHDC-122-A-3602i
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 trying to join WLAN with RSSI 200. Checking for XOR roam conditions on AP: 7C:95:F3:96:80:E0 Slot: 1
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Station: 98:01:A7:A0:96:B7 is associating to AP 7C:95:F3:96:80:E0 which is not XOR roam capable
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Global 200 Clients are allowed to AP radio
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Max Client Trap Threshold: 0 cur: 7
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Rf profile 600 Clients are allowed to AP wlan
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 override for default ap group, marking intgrp NULL
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Applying Interface(production_data) policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 246
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Re-applying interface policy for client
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2931)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing Url ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2951)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv6 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2972)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type, Tunnel User - 0
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Setting the NAS Id to WLAN specific Id 'HH-5508-A'
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 In processSsidIE:6458 setting Central switched to TRUE
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 In processSsidIE:6461 apVapId = 12 and Split Acl Id = 65535
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Applying site-specific Local Bridging override for station 98:01:a7:a0:96:b7 - vapId 14, site 'TEST_OFFNET', interface 'production_data'
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Applying Local Bridging Interface Policy for station 98:01:a7:a0:96:b7 - vlan 246, interface id 14, interface 'production_data'
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 override from ap group, removing intf group from mscb
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Applying site-specific override for station 98:01:a7:a0:96:b7 - vapId 14, site 'TEST_OFFNET', interface 'production_data'
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Applying Interface(production_data) policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 246
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Re-applying interface policy for client
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv4 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2931)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing Url ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2951)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Changing IPv6 ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2972)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Setting the NAS Id to AP group specific Id 'HHDC-5508-TEST-B'
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 processSsidIE statusCode is 0 and status is 0
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 processSsidIE ssid_done_flag is 0 finish_flag is 0
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 STA - rates (B): 140 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 suppRates statusCode is 0 and gotSuppRatesElement is 1
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: RSNIE in Assoc. Req.: (38)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: [0000] 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: [0016] ac 01 00 00 01 00 19 3f 85 7a 62 ee 3e ff b7 c6
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: [0032] f2 f4 cd 3e e2 b5
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Processing RSN IE type 48, length 38 for mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7
```

```
ccmp128 is enabled
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Received 802.11i 802.1X key management suite, enabling dot1x Authentication
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 RSN Capabilities: 0
```

```
*apfMsConnTask_4: Jul 18 13:30:27.518: 98:01:a7:a0:96:b7 Marking Mobile as non-11w Capable
```

## \* Mac Book presents the PMKID to the access point:

```
*apfMsConnTask_4: Jul 18 13:30:27.519: 98:01:a7:a0:96:b7 Received RSN IE with 1 PMKIDs from mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_4: Jul 18 13:30:27.519: Received PMKID: (16)
```

```
*apfMsConnTask_4: Jul 18 13:30:27.519: [0000] 19 3f 85 7a 62 ee 3e ff b7 c6 f2 f4 cd 3e e2 b5
```

## \* The WLC is able to locate the PMKID which is stored on the access point from the first association.

```
*apfMsConnTask_4: Jul 18 13:30:27.519: 98:01:a7:a0:96:b7 Searching for PMKID in MSCB PMKID cache for mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_4: Jul 18 13:30:27.519: 98:01:a7:a0:96:b7 Found an cache entry for BSSID 7c:95:f3:96:80:e4 in PMKID cache at index 0 of station 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_4: Jul 18 13:30:27.519: 98:01:a7:a0:96:b7 Found a valid PMKID in the MSCB PMKID cache for mobile 98:01:a7:a0:96:b7
```

```
*apfMsConnTask_4: Jul 18 13:30:27.519: 98:01:a7:a0:96:b7 Setting active key cache index 1 --> 0
```

```
*apfMsConnTask_4: Jul 18 13:30:27.519: 98:01:a7:a0:96:b7 pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
```

```
*apfMsConnTask_4: Jul 18 13:30:27.519: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Deleted mobile LWAPP rule on AP [6c:50:4d:ab:2b:d0]
```

```
*pemReceiveTask: Jul 18 13:30:27.520: 98:01:a7:a0:96:b7 10.246.36.69 Removed NPU entry.
```

```
*apfMsConnTask_4: Jul 18 13:30:27.520: 98:01:a7:a0:96:b7 Updated location for station old AP 6c:50:4d:ab:2b:d0-1, new AP 7c:95:f3:96:80:e0-1
```

```
*apfMsConnTask_4: Jul 18 13:30:27.520: 98:01:a7:a0:96:b7 apfMsRunStateDec
```

```
*spamApTask7: Jul 18 13:30:27.520: 98:01:a7:a0:96:b7 Delete Mobile request sent to the AP 10.101.1.31:31608
```

```
*apfMsConnTask_4: Jul 18 13:30:27.520: 98:01:a7:a0:96:b7 apfMs1xStateDec
```





\*Dot1x\_NW\_MsgTask\_7: Jul 18 13:30:27.538: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Fast Path rule (contd...) 802.1P = 4, DSCP = 0, TokenID = 15206, IntfId = 14 Local Bridging Vlan = 246, Local Bridging intf id = 14  
\*Dot1x\_NW\_MsgTask\_7: Jul 18 13:30:27.538: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 0, AppToken = 15206 AverageRate = 0, BurstRate = 0  
\*Dot1x\_NW\_MsgTask\_7: Jul 18 13:30:27.538: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 0, AppToken = 15206 AverageRate = 0, BurstRate = 0  
\*Dot1x\_NW\_MsgTask\_7: Jul 18 13:30:27.538: 98:01:a7:a0:96:b7 10.246.36.69 RUN (20) Fast Path rule (contd...) AVC Ratelimit: AppID = 0 ,AppAction = 0, AppToken = 15206 AverageRate = 0, BurstRate = 0

# CISCO:

## Information About Sticky Key Caching

The controller supports sticky key caching (SKC). With sticky key caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client.

In SKC, the client stores each Pairwise Master Key ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

## Restrictions for Sticky Key Caching

- The controller supports SKC for up to eight APs per client. If a client roams to more than 8 APs per session, the old APs are removed to store the newly cached entries when the client roams. We recommend that you do not use SKC for large scale deployments.
- SKC works only on WPA2-enabled WLANs.
- SKC does not work across controllers in a mobility group.
- SKC works only on local mode APs.

# APPLE:

## macOS wireless roaming for enterprise customers

<https://support.apple.com/en-us/HT206207>

Learn how macOS supports roaming between access points within a wireless network.

For system administrators, macOS roaming helps your Mac stay connected as it moves between different places within your office network.

## Trigger threshold

The trigger threshold is the minimum signal level a client requires to maintain the current connection.

macOS clients monitor and maintain the current BSSID's connection until the RSSI crosses the -75 dBm threshold. After RSSI crosses that threshold, macOS scans for roam candidate BSSIDs for the current ESSID.

Consider this threshold in view of the signal overlap between your wireless cells. macOS maintains a connection until the -75 dBm threshold, but 5 GHz cells are designed with a -67 dBm overlap. Those clients will remain connected to the current BSSID longer than you expect.

Also consider how the cell overlap is measured. The antennas on computers vary from model to model, and they see different cell boundaries than expected. It's always best to use the target device when you measure cell overlap.

## Selection criteria for band, network, and roam candidates

macOS always defaults to the 5 GHz band over the 2.4 GHz band. This happens as long as the RSSI for a 5 GHz network is -68 dBm or better.

If multiple 5 GHz SSIDs meet this level, macOS chooses a network based on these criteria:

- 802.11ac is preferred over 802.11n or 802.11a.
- 802.11n is preferred over 802.11a.
- 80 MHz channel width is preferred over 40 MHz or 20 MHz.
- 40 MHz channel width is preferred over 20 MHz.

macOS doesn't support 802.11k. macOS does interoperate with SSIDs that have 802.11k enabled. But, macOS doesn't limit roam scans of the environment based on the neighbor report. A roam scan is when stations check the available channels in a given band (either 2.4 or 5 GHz) for access points (APs) that support the current ESSID. macOS selects a target BSSID whose reported RSSI is 12 dB or greater than the current BSSID's RSSI. This is true even if the macOS client is idle or transmitting/receiving data.

## Roam performance

Roam performance describes how long a client needs to authenticate successfully to a new BSSID.

Finding a valid network and AP is only part of the process. The client must complete the roam process quickly and without interruption, so the user doesn't experience downtime. Roaming involves the client authenticating against the new BSSID and deauthenticating from the current BSSID. The security and authentication method determines how quickly this can happen.

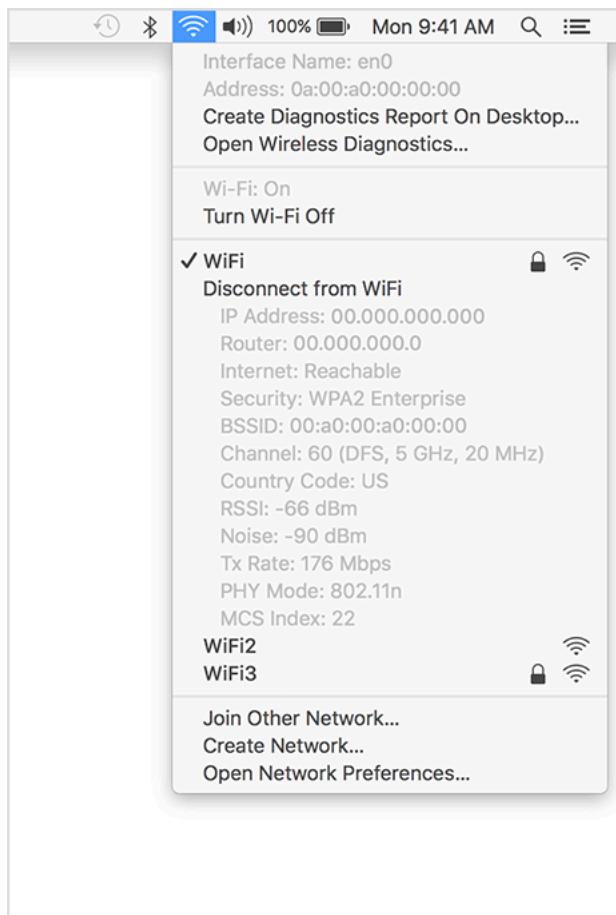
First, 802.1X-based authentication requires the client to complete the entire EAP key exchange. Then, it can deauthenticate from the current BSSID. Depending on the environment's authentication infrastructure, this might take several seconds. End users could experience interrupted service in the form of dead air.

macOS supports static PMKID (Pairwise Master Key identifier) caching to help optimize roaming between BSSIDs in the same ESSID. macOS doesn't support Fast BSS Transition, also known as 802.11r. You don't have to deploy additional SSIDs to support macOS because macOS interoperates with 802.11r.

## Measure Client RSSI

macOS offers a few built-in tools that scan to measure RSSI.

To learn the RSSI for the associated network, hold the Option key while you click the



To learn the RSSI for networks in the client's environment, use Wireless Diagnostics.



To open Wireless Diagnostics, Option-click on the Wi-Fi menu, select Open Wireless Diagnostic, and choose Scan. Click the Scan Now button to find all nearby wireless networks and measure their RSSI.

Summary		Network Name	BSSID	Security	Protocol	RSSI
Total	24	WiFi2	00:00:00:00:aa:00	WPA/WPA2 Personal	802.11a/n	-53
2.4 GHz Count	4	WiFi3	00:00:00:00:aa:0a	WPA2 Personal	802.11a/n	-59
5 GHz Count	20	WiFi4	00:00:00:aa:00:00	Open	802.11a/n	-83
Current Channel Count	4	WiFi5	00:00:aa:00:00:00	WPA2 Personal	802.11b/g/n	-73
Best 2.4 GHz	11, 2	WiFi6	0a:00:00:a0:00:00	Open	802.11a/n	-83
Best 5 GHz	40, 44	WiFi7	00:00:0a:00:00:0a	WPA2 Enterprise	802.11a/n	-81
		WiFi8	00:00:a0:00:00:0a	Open	802.11b/g/n	-66

In addition to this graphic tool, you can also use the command-line utility "airport" to get the same data. This is found in /System/Library/PrivateFrameworks/Apple80211.framework/Versions/A/Resources/.

The '-s' flag scans the current environment for available networks and lists the RSSI.

```
>>> % airport -s

SSID BSSID          RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
WiFi 00:a0:00:00:0a:00 -77  1    Y  -- NONE
work a0:00:00:a0:00:00 -88  2    Y  -- WPA2(PSK/AES/AES)
WiFi 00:00:00:0a:00:a0 -76  11   Y  -- NONE
WiFi 00:0a:0a:00:00:00 -75  52   Y  US NONE
home 00:00:00:aa:00:00 -76  52   Y  US WPA(PSK/AES/AES) WPA2(PSK,FT-PSK/AES/AES)
WiFi 00:a0:00:00:00:00 -77  140  Y  US NONE
home 00:aa:00:00:00:00 -76  140  Y  US WPA(PSK/AES/AES) WPA2(PSK,FT-PSK/AES/AES)
work a0:00:00:00:00:0a -85  11   Y  -- WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
WiFi 00:a0:00:00:0a:00 -56  11   Y  -- NONE
home aa:00:00:00:00:00 -56  11   Y  US WPA(PSK/AES/AES) WPA2(PSK,FT-PSK/AES/AES)
work 00:00:a0:00:00:00 -59  11   N  -- WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
work 00:a0:0a:00:00:00 -75  9    N  US WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
WiFi 00:00:00:00:00:aa -28  1    Y  -- NONE
home 0a:00:00:0a:00:00 -28  1    Y  US WPA(PSK/AES/AES) WPA2(PSK,FT-PSK/AES/AES)
home 00:00:aa:00:00:00 -76  1    Y  US WPA(PSK/AES/AES) WPA2(PSK,FT-PSK/AES/AES)
work 00:00:00:a0:00:0a -54  165  Y  US NONE
work 00:00:0a:00:a0:00 -53  165  Y  US WPA2(802.1x,FT-802.1x/AES/AES)
work 00:00:00:00:aa:00 -40  161,-1 Y  -- WPA(802.1x/AES/AES) WPA2(802.1x/AES/AES)
WiFi 00:a0:00:a0:00:00 -33  132  Y  US NONE
home 00:0a:00:00:0a:00 -33  132  Y  US WPA(PSK/AES/AES) WPA2(PSK,FT-PSK/AES/AES)

>>> %
```

Starting with OS X El Capitan, you can turn on Wi-Fi Monitor on the desktop. This displays signal strength and other environment details. Hold down Option and



Shift-click on the Wi-Fi menu to reveal the Debug menu.

Then choose Show Wi-Fi Monitor.

The screenshot shows the Wi-Fi Monitor window with the following details:

- WiFi**
- 00.000.000.00
- WPA2 Enterprise
- 60 / 20 MHz / US
- 67 dBm / -90 dBm
- 11n / 176 Mbps

Two graphs are visible:

- The top graph shows signal strength in dBm, with a scale from -60 to -100. The signal fluctuates around -70 dBm.
- The bottom graph shows a metric (likely channel width or power) with a scale from 160 to 200. The value is mostly at 176, with a step up to 196.

Additional information at the bottom of the window:

- Enabled [Auto]
- 149++ 0 0 0 0 0 0 0 149++ 149++ 0 0 0 0 0
- LowPower (260.875 s)
- Master [00:0A:00:00:A0:00] / 0 [00:0A:00:00:A0:00] / 0
- 6 peers
- AWDL

Published Date: Apr 4, 2017