目录

简介

本文档是通过调试（通常采用“debug client <mac address>”命令）对常见无线问题进行解析的速查手册。通过“show client”和调试进行解析要求用户先了解一些 PEM 状态和 APF 状态。

使用的组件

本文档同样适用于所有“AireOS”控制器。在编写本文档时，这些控制器包括 440x、5508、5520、75xx、85xx、2504 和 vWLC 以及 Wisms。虽然许多概念在融合接入 IOS-XE 控制器和交换机中完全相同，但由于输出和调试截然不同，因此本文档对其并不适用。

show client 输出中的简要 PEM 状态

- **START** - 新客户端条目的初始状态。
- **AUTHCHECK** - WLAN 具有要执行的 L2 身份验证策略。
- **8021X_REQD** - 客户端必须完成 802.1x 身份验证。
- **L2AUTHCOMPLETE** - 客户端已成功实施 L2 策略。该过程现在可以继续执行 L3 策略（地址获知和 Web 身份验证等）。如果控制器是同一移动组中的漫游客户端，则该控制器会在此处发送移动通告，以从其他控制器获知 L3 信息。
- **WEP_REQD** - 客户端必须完成 WEP 身份验证。
- **DHCP_REQD** - 控制器需要从客户端获知 L3 地址，这是通过 ARP 请求、DHCP 请求或续订，或者通过从移动组中的另一个控制器获知的信息来完成。如果在 WLAN 上标记了“需要 DHCP”(DHCP Required)，则仅使用 DHCP 或移动信息。
- **WEBAUTH_REQD** - 客户端必须完成 Web 身份验证。（L3 策略）
- **CENTRAL_WEBAUTH_REQD -** 客户端必须完成 CWA 登录，WLC 正在等待接收 CoA。
- **RUN** - 客户端已成功实施所需的 L2 和 L3 策略，并且现在可以将流量传输到网络。

以下情景将显示无线设置中常见配置不当情况的关键调试行，以**粗体**突出显示关键参数。

情景 1：用于客户端上的 WPA/WPA2 PSK 身份验证的口令配置不当

```
(Cisco Controller) >show client detail 24:77:03:19:fb:70

Client MAC Address..............................24:77:03:19:fb:70

Client Username ................................N/A

AP MAC Address..................................ec:c8:82:a4:5b:c0

AP Name.....................................Shankar_AP_1042

AP radio slot Id................................1

Client State....................................Associated

Client NAC OOB State............................Access

Wireless LAN Id.................................5

Hotspot (802.11u)...............................Not Supported

BSSID...........................................ec:c8:82:a4:5b:cb

Connected For ..................................0 secs

Channel.........................................44

IP Address......................................Unknown
```

Gateway Address..... Unknown

Netmask..... Unknown

Association Id..... 1

Authentication Algorithm..... Open System

Reason Code..... 1

Status Code..... 0

Session Timeout..... 0

Client CCX version..... 4

Client E2E version..... 1

QoS Level..... Silver

Avg data Rate..... 0

Burst data Rate..... 0

Avg Real time data Rate..... 0

Burst Real Time data Rate..... 0

802.1P Priority Tag..... 2

CTS Security Group Tag..... Not Applicable

KTS CAC Capability..... No

WMM Support..... Enabled

  APSD ACs..... BK BE VI VO

Power Save..... OFF

Current Rate..... m15

Supported Rates..... 6.0,9.0,12.0,18.0,24.0,36.0,

      ..... 48.0,54.0

Mobility State..... None

Mobility Move Count..... 0

Security Policy Completed..... No

Policy Manager State..... 8021X_REQD
//This proves client is struggling to clear Layer-2 authentication.
It means we have to move to debug to understand where in L-2 we are failing Policy Manager Rule Created.....Yes Audit Session ID..... none AAA Role Type..... none Local Policy Applied..... none IPv4 ACL Name..... none FlexConnect ACL Applied Status.....Unavailable IPv4 ACL Applied Status.....Unavailable IPv6 ACL Name..... none IPv6 ACL Applied Status.....Unavailable Layer2 ACL Name..... none Layer2 ACL Applied Status..... Unavailable mDNS Status.....Enabled mDNS Profile Name..... default-mdns-profile No. of mDNS Services

```
Advertised.................0 Policy Type.....................................WPA2
Authentication Key Management...................PSK Encryption
Cipher.............................CCMP (AES) Protected Management Frame
.....................No Management Frame Protection.....................No EAP
Type.....................................Unknown
Interface..................................... vlan21
VLAN.......................................... 21 Quarantine
VLAN.................................0 Access VLAN. ..................................... 21
Client Capabilities: CF Pollable.............................Not implemented CF Poll
Request..........................Not implemented Short Preamble.............................
Not implemented PBCC.....................................Not implemented Channel
Agility..........................Not implemented Listen Interval.............................
10 Fast BSS Transition.......................Not implemented Client Wifi Direct Capabilities:
WFD capable.................................No Manged WFD capable.........................No
Cross Connection Capable...................No Support Concurrent Operation..............No
Fast BSS Transition Details: Client Statistics: Number of Bytes Received. .................. 423
Number of Bytes Sent.......................429 Number of Packets Received. ................. 3
Number of Packets Sent.....................4 Number of Interim-Update Sent. .............. 0
Number of EAP Id Request Msg Timeouts......0 Number of EAP Id Request Msg Failures. ...... 0
Number of EAP Request Msg Timeouts.........0 Number of EAP Request Msg Failures. ......... 0
Number of EAP Key Msg Timeouts.............0 Number of EAP Key Msg Failures. ............. 0
Number of Data Retries.....................0 Number of RTS Retries. ...................... 0
Number of Duplicate Received Packets.......0 Number of Decrypt Failed Packets. ............ 0
Number of Mic Failured Packets.............0 Number of Mic Missing Packets. ............... 0
Number of RA Packets Dropped...............0 Number of Policy Errors. ..................... 0
Radio Signal Strength Indicator.............-18 dBm Signal to Noise Ratio.....................
40 dB Client Rate Limiting Statistics: Number of Data Packets Recieved.............0 Number of
Data Rx Packets Dropped..........0 Number of Data Bytes Recieved..............0 Number of Data
Rx Bytes Dropped............0 Number of Realtime Packets Recieved.........0 Number of Realtime
Rx Packets Dropped......0 Number of Realtime Bytes Recieved..........0 Number of Realtime Rx
Bytes Dropped........0 Number of Data Packets Sent................0 Number of Data Tx Packets
Dropped..........0 Number of Data Bytes Sent..................0 Number of Data Tx Bytes
Dropped............0 Number of Realtime Packets Sent............0 Number of Realtime Tx
Packets Dropped......0 Number of Realtime Bytes Sent..............0 Number of Realtime Tx
Bytes Dropped........0 Nearby AP Statistics: Shankar_AP_1602(slot 0) antenna0: 0 secs
ago......................-25 dBm antenna1: 0 secs ago......................-40 dBm
Shankar_AP_1602(slot 1) antenna0: 1 secs ago......................-41 dBm antenna1: 1 secs
ago......................-27 dBm Shankar_AP_3502(slot 0) antenna0: 0 secs
ago......................-90 dBm antenna1: 0 secs ago......................-83 dBm
Shankar_AP_1042(slot 0) antenna0: 0 secs ago......................-32 dBm antenna1: 0 secs
ago......................-41 dBm Shankar_AP_1042(slot 1) antenna0: 0 secs
ago......................-50 dBm antenna1: 0 secs ago......................-42 dBm DNS Server
details: DNS server IP ..............................0.0.0.0 DNS server IP
..............................0.0.0.0 Assisted Roaming Prediction List details: Client Dhcp
Required: False Allowed (URL)IP Addresses ------------------------
```

调试客户端分析

```
(Cisco Controller) >debug client 24:77:03:19:fb:70
```

***apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Association received from mobile on BSSID 08:cc:68:67:1f:fb //Client has initiated association for AP with BSSID 08:cc:68:67:1f:fb**

```
*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Global 200 Clients are allowed to AP
radio
```

```
*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Max Client Trap Threshold: 0  cur: 0
```

*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Rf profile 600 Clients are allowed to AP wlan

*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Applying Interface policy on Mobile, role Unassociated.Ms NAC State 2 Quarantine Vlan 0 Access Vlan 21

*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 Re-applying interface policy for client

*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2202)

*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2223)

*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 apfApplyWlanPolicy: Apply WLAN Policy over PMIPv6 Client Mobility Type

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 In processSsidIE:4795 setting Central switched to TRUE

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 In processSsidIE:4798 apVapId = 5 and Split Acl Id = 65535

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Applying site-specific Local Bridging override for station 24:77:03:19:fb:70 - vapId 5, site 'default-group', interface 'vlan21'

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Applying Local Bridging Interface Policy for station 24:77:03:19:fb:70 - vlan 21, interface id 14, interface 'vlan21'

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 processSsidIE statusCode is 0 and status is 0

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 processSsidIE ssid_done_flag is 0 finish_flag is 0

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 STA - rates (8): 140 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 suppRates statusCode is 0 and gotSuppRatesElement is 1

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Processing RSN IE type 48, length 22 for mobile 24:77:03:19:fb:70

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 START (0) Deleted mobile LWAPP rule on AP [ec:c8:82:a4:5b:c0]

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Updated location for station old AP ec:c8:82:a4:5b:c0-1, new AP 08:cc:68:67:1f:f0-1

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Updating AID for REAP AP Client 08:cc:68:67:1f:f0 - AID ===> 1

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 START (0) Initializing policy

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

***apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)//**

Client entering L2 authentication stage *apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Central switch is TRUE *apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Not Using WMM Compliance code qosCap 00 *apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rule on AP 08:cc:68:67:1f:f0 vapId 5 apVapId 5 flex-acl-name: *apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfMsAssoStateInc *apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfPemAddUser2 (apf_policy.c:333) Changing state for mobile 24:77:03:19:fb:70 on AP 08:cc:68:67:1f:f0 from Disassociated to Associated *apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfPemAddUser2:session timeout forstation 24:77:03:19:fb:70 - Session Tout 0, apfMsTimeOut '0' and sessionTimerRunning flag is 0 *apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Stopping deletion of Mobile Station: (callerId: 48) *apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Func: apfPemAddUser2, Ms Timeout = 0, Session Timeout = 0 *apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Sending Assoc Response to station on BSSID 08:cc:68:67:1f:fb (status 0) ApVapId 5 Slot 1 *apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfProcessAssocReq (apf_80211.c:8292) Changing state for mobile 24:77:03:19:fb:70 on AP 08:cc:68:67:1f:f0 from Associated to Associated *spamApTask3: May 07 17:03:56.065: 24:77:03:19:fb:70 Sent 1x initiate message to multi thread task for mobile 24:77:03:19:fb:70 *Dot1x_NW_MsgTask_0: May 07 17:03:56.065: 24:77:03:19:fb:70 Creating a PKC PMKID Cache entry for station 24:77:03:19:fb:70 (RSN 2) *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Resetting MSCB PMK Cache Entry 0 for station 24:77:03:19:fb:70 *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Removing BSSID ec:c8:82:a4:5b:cb from PMKID cache of station 24:77:03:19:fb:70 *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Setting active key cache index 0 ---> 8 *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Setting active key cache index 8 ---> 0 *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Adding BSSID 08:cc:68:67:1f:fb to PMKID cache at index 0 for station 24:77:03:19:fb:70 *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: New PMKID: (16) *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: [0000] d7 57 8e ff 2b 27 01 4e 93 39 0b 1c 1f 46 d2 da *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Initiating RSN PSK to mobile 24:77:03:19:fb:70 *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 EAP-PARAM Debug - eap-params for Wlan-Id :5 is disabled - applying Global eap timers and retries *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 dot1x - moving mobile 24:77:03:19:fb:70 into Force Auth state *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 EAPOL Header: *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 00000000: 02 03 00 5f ..._ *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Found an cache entry for BSSID 08:cc:68:67:1f:fb in PMKID cache at index 0 of station 24:77:03:19:fb:70 *Dot1x_NW_MsgTask_0: May 07 17:03:56.066: **24:77:03:19:fb:70 Found an cache entry for BSSID 08:cc:68:67:1f:fb in PMKID cache at index 0 of station 24:77:03:19:fb:70**

***Dot1x_NW_MsgTask_0: May 07 17:03:56.066: Including PMKID in M1 (16)**

***Dot1x_NW_MsgTask_0: May 07 17:03:56.066: [0000] d7 57 8e ff 2b 27 01 4e 93 39 0b 1c 1f 46 d2 da**

***Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Starting key exchange to mobile 24:77:03:19:fb:70, data packets will be dropped**

***Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Sending EAPOL-Key Message to mobile 24:77:03:19:fb:70**

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

***Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Sending EAPOL-Key Message to mobile 24:77:03:19:fb:70**

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Allocating EAP Pkt for retransmission to mobile 24:77:03:19:fb:70

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 mscb->apfMsLwappLradNhMac = b0:fa:eb:b8:f5:12 mscb->apfMsLradSlotId = 1 mscb->apfMsLradJumbo = 0 mscb->apfMsintIfNum = 1

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 mscb->apfMsBssid = 08:cc:68:67:1f:f0 mscb->apfMsAddress = 24:77:03:19:fb:70 mscb->apfMsApVapId = 5

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 dot1xcb->snapOrg = 00 00 00 dot1xcb->eapolWepBit = 0 mscb->apfMsLwappLradVlanId = 0 mscb->apfMsLwappMwarInet.ipv4.addr = 181004965

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 mscb->apfMsLwappMwarPort = 5246 mscb->apfMsLwappLradInet.ipv4.addr = 181004985 mscb->apfMsLwappLradPort = 36690

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Received EAPOL-Key from mobile 24:77:03:19:fb:70

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Ignoring invalid EAPOL version (1) in EAPOL-key message from mobile 24:77:03:19:fb:70

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Received EAPOL-key in PTK_START state (message 2) from mobile 24:77:03:19:fb:70

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Received EAPOL-key M2 with invalid MIC from mobile 24:77:03:19:fb:70 version 2

***osapiBsnTimer: May 07 17:03:56.364: 24:77:03:19:fb:70 802.1x 'timeoutEvt' Timer expired for station 24:77:03:19:fb:70 and for message = M2**

!--- MIC error due to wrong preshared key

***dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70 Retransmit 1 of EAPOL-Key M1 (length 121) for mobile 24:77:03:19:fb:70**

*dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70 mscb->apfMsLwappLradNhMac = b0:fa:eb:b8:f5:12 mscb->apfMsLradSlotId = 1 mscb->apfMsLradJumbo = 0 mscb->apfMsintIfNum = 1

*dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70 mscb->apfMsBssid = 08:cc:68:67:1f:f0 mscb->apfMsAddress = 24:77:03:19:fb:70 mscb->apfMsApVapId = 5

*dot1xMsgTask: May 07 17:03:56.365: 24:77:03:19:fb:70 dot1xcb->snapOrg = 00 00 00 dot1xcb->eapolWepBit = 0 mscb->apfMsLwappLradVlanId = 0 mscb->apfMsLwappMwarInet.ipv4.addr = 181004965

*dot1xMsgTask: May 07 17:03:56.365: 24:77:03:19:fb:70 mscb->apfMsLwappMwarPort = 5246 mscb->apfMsLwappLradInet.ipv4.addr = 181004985 mscb->apfMsLwappLradPort = 36690

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-Key from mobile 24:77:03:19:fb:70

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Ignoring invalid EAPOL version (1) in EAPOL-key message from mobile 24:77:03:19:fb:70

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-key in PTK_START state (message 2) from mobile 24:77:03:19:fb:70

*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-key M2 with invalid MIC from mobile 24:77:03:19:fb:70 version 2

***osapiBsnTimer: May 07 17:03:56.764: 24:77:03:19:fb:70 802.1x 'timeoutEvt' Timer expired for station 24:77:03:19:fb:70 and for message = M2**

!--- MIC error due to wrong preshared key

结论

虽然 M2 密钥的“timeoutEvt”也可能是由于驱动程序/NIC 错误导致，但是最常见的问题之一是用户为 PSK 密码输入的凭证（缺少大小写区分/特殊字符等）不正确且无法连接。

情景 2：无线电话听筒 (792x/9971) 未能与无线“离开服务区”关联

参考：https://supportforums.cisco.com/document/12068061/7925g-handsets-failing-association-ap-call-failed-tspec-qos-policy-does-not-match

拓扑

带有思科统一无线 IP 电话的 WLAN

问题详细信息

AIR-CT5508-50-K9 // 电话和无线控制器的已升级固件将不接受电话注册

调试和日志

```
apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Association received from mobile on AP
3x:xx:cx:9x:x0:x0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx 0.0.0.0 START (0) Changing IPv4 ACL
'none' (ACL ID xxx) ===> 'none' (ACL ID xxx) --- (caller apf_policy.c:1x09)

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx 0.0.0.0 START (0) Changing IPv6 ACL
'none' (ACL ID xxx5) ===> 'none' (ACL ID xxx) --- (caller apf_policy.c:18x6)

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying site-specific Local Bridging
override for station 1x:xx:1x:xx:xx:xx - vapId 1, site 'default-group', interface 'xwirex'

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying Local Bridging Interface Policy
for station 1x:xx:1x:xx:xx:xx - vlan 510, interface id 12, interface 'xwirex'

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx processSsidIE  statusCode is 0 and
status is 0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx processSsidIE  ssid_done_flag is 0
finish_flag is 0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx STA - rates (4): 130 132 139 150 0 0 0 0
0 0 0 0 0 0 0 0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx suppRates  statusCode is 0 and
gotSuppRatesElement is 1

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx STA - rates (12): 130 132 139 150 12 18
24 36 48 72 96 108 0 0 0 0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx extSuppRates  statusCode is 0 and
gotExtSuppRatesElement is 1

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Processing RSN IE type 48, length 22 for
mobile 1x:xx:1x:xx:xx:xx
```

```
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx CCKM: Mobile is using CCKM

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Received RSN IE with 0 PMKIDs from
mobile 1x:xx:1x:xx:xx:xx

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Setting active key cache index 8 ---> 8

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx unsetting PmkIdValidatedByAp

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Sending Assoc Response to station on
BSSID 3x:xx:cx:9x:x0:x0 (status 201) ApVapId 1 Slot 0

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Scheduling deletion of Mobile Station:
(callerId: 22) in 3 seconds

VoIP Call Failure: '1x:xx:1x:xx:xx:xx' client, detected by 'xx-xx-xx' AP on radio type
'802.11b/g'.Reason: 'Call failed: TSPEC QOS Policy does not match'.
Means platinum QoS was not configured on WLAN 1x:xx PM Client Excluded:
MACAddress:1x:xx:1x:xx:xx:xx Base Radio MAC :3x:xx:cx:9x:x0:x0 Slot: 1 User Name: dwpv\mtl7925
Ip Address: xx.xx.x.xx Reason:802.11 Association failed repeatedly. ReasonCode: 2
```

结论

WLC 上的调试显示，由于 AP 返回关联状态代码 201，7925G 关联失败。

这是由于来自听筒的 TSPEC（流量规范）请求因 WLAN 配置而遭到拒绝。7925G 尝试连接的 WLAN 使用白银级 (UP 0,3) QoS 配置文件进行配置，而不是按要求使用白金级 (UP 6,7) 配置文件进行配置。这导致对于通过 WLAN 从听筒进行的语音流量/操作帧交换，TSPEC 不匹配，并最终遭到 AP 拒绝。

使用 7925G 听筒专用的白金级 QoS 配置文件创建新的 WLAN 并根据已建立的最佳实践配置和 7925G 部署指南中的定义进行配置，7925G 部署指南访问地址为：

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7925g/7_0/english/deployment/guide/7925dply.pdf

配置后，问题应得到解决。

情景 3：为 WPA 配置客户端，但仅为 WPA2 配置 AP

Debug client <mac addr>

```
Wed May 7 10:51:37 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile

    Station:  (callerId: 23) in 5 seconds

Wed May 7 10:51:37 2014: xx.xx.xx.xx.xx.xx apfProcessProbeReq

    (apf_80211.c:4057) Changing state for mobile xx.xx.xx.xx.xx.xx on AP

     from Idle to Probe
```

Controller adds the new client, moving into probing status Wed May 7 10:51:37 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:38 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:38 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds AP is reporting probe activity every 500 ms as configured Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:41 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:44 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:44 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:44 2014: xx.xx.xx.xx.xx.xx Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed May 7 10:51:49 2014: xx.xx.xx.xx.xx.xx apfMsExpireCallback (apf_ms.c:433) Expiring Mobile!Wed May 7 10:51:49 2014: xx.xx.xx.xx.xx.xx 1.1.1.1 START (0) Deleted mobile LWAPP rule on AP [] Wed May 7 10:51:49 2014: xx.xx.xx.xx.xx.xx Deleting mobile on AP (0) After 5 seconds of inactivity, client is deleted, never moved into authentication or association phases.

情景 4：解析 AAA 返回或响应代码。

为收集预期日志而要运行的必要调试：

（思科控制器）>debug mac addr <mac>
（思科控制器）>debug aaa events enable
（或）
（思科控制器）>debug client <mac>
（思科控制器）>debug aaa events enable
（思科控制器）>debug aaa errors enable

如果启用陷阱，则 AAA 连接故障将生成 SNMP 陷阱。

调试输出示例 <部分内容已删减>

```
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS
message authenticator for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification
failed from server 10.50.0.74 with id=213.Possible secret mismatch for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Returning AAA Error
'Authentication Failed' (-4) for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: AuthorizationResponse: 0x4259f944
```

Returning AAA Error 'Success' (0) for mobile
Successful Authentication happened, AAA returns access-accept prior to Success (0) to confirm the same. **Returning AAA Error 'Out of Memory' (-2) for mobile**
it's the rare reason. CSCud12582 Processing AAA Error 'Out of Memory' **Returning AAA Error 'Authentication Failed' (-4) for mobile**
its the most common reason seen

可能原因：

1. 用户帐户和/或密码无效
2. 计算机不是域的成员，AD 端发生问题
3. 证书服务未正常工作
4. 服务器证书已到期或未使用
5. 未正确配置 RADIUS

6. 未正确输入访问密钥，密钥区分大小写（SSID 同样如此）
7. 更新 Microsoft 补丁
8. EAP 计时器
9. 在客户端/服务器上配置的 EAP 方法不正确
10. 客户端证书已到期或未使用。针对手机返回

AAA 错误“超时”(-5) ("Timeout" [-5])

AAA 服务器无法访问，然后客户端取消身份验证。

示例：

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

针对手机返回 AAA 错误“内部错误”(-6) ("Internal Error" [-6])

属性不匹配。AAA 发送无法理解/与 WLC 不兼容的错误/不当属性（长度错误）。WLC 发送“取消身份验证”(Deauth) 消息，随后发送“内部错误”(internal error) 消息 示例：

CSCum83894 AAA“内部错误”(internal error)，并且由于 Access-Accept 消息中包含未知属性，身份验证失败

示例：

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

针对手机返回 AAA 错误“无服务器”(-7) ("No Server" [-7])

Radius 配置错误和/或正在使用的配置不受支持

示例：

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

情景 5：客户端未能关联 AP

运行的调试

debug client <mac addr>

要解析的日志

Sending Assoc Response to station on BSSID 00:26:cb:94:44:c0 **(status 0)** ApVapId 1 **Slot 0**

- **Slot 0** = B/G(2.4) Radio

Slot 1 = A(5) Radio

- Sending Assoc Response **Status 0** = Success

Anything other than Status 0 is Failure

常见关联响应状态代码可在 https://supportforums.cisco.com/document/141136/80211-association-status-80211-deauth- reason-codes 中找到。

情景 6：由于空闲超时，客户端取消关联

运行的调试

debug client <mac addr>

要解析的日志

Received Idle-Timeout from AP 00:26:cb:94:44:c0, slot 0 for STA 00:1e:8c:0f:a4:57

apfMsDeleteByMscb Scheduling mobile for deletion with deleteReason 4, **reasonCode 4**

Scheduling deletion of Mobile Station: (callerId: 30) in 1 seconds

apfMsExpireCallback (apf_ms.c:608) Expiring Mobile!

Sent Deauthenticate to mobile on BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

条件

未从客户端收到流量后发生

默认持续时间为 300 秒

解决方法

从 WLC GUI>>“控制器”(Controller)>>“常规”(General) 以全局方式或从 WLC GUI>>WLAN>>ID>>“高级”(Advanced) 为每个 WLAN 增大空闲超时

情景 7：由于会话超时，客户端取消关联

```
DdLWeoeedgbbsuOugcgttocralp2ie6nanr2st0e<:m08a:c50ad20d1r1>: 00:13:ce:1a:92:41 Max
retransmission of Access-Request (id 100) to 155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

条件

在达到计划持续时间（默认为 1800 秒）时发生

将强制 WEBAUTH 用户再次执行 WEBAUTH 操作

解决方法

从 WLC GUI>>WLAN>>ID>>“高级”(Advanced) 为每个 WLAN 增大或禁用会话超时

情景 8：由于 WLAN 更改，客户端取消关联

运行的调试

debug client <mac addr>

要解析的日志

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

条件

以任意方式修改 WLAN 禁用并重新启用 WLAN

解决方法

这是预期行为。进行 WLAN 更改后，客户端将在取消关联后重新关联。

情景 9：由于从 WLC 手动删除，客户端取消关联

运行的调试

debug client <mac addr>

要解析的日志

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

条件

从 GUI：“删除客户端”(Remove Client)

从 CLI：config client deauthenticate <mac address>

情景 10：由于身份验证超时，客户端取消关联

运行的调试

debug client <mac addr>

要解析的日志

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

条件

达到身份验证或密钥交换最大重新传输数

解决方法

检查/更新客户端驱动程序、安全配置、证书等。

情景 11：由于 AP 无线电重置（电源/通道），客户端取消关联

运行的调试

debug client <mac addr>

要解析的日志

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

条件

AP 与客户端取消关联，但是 WLC 未删除条目

解决方法

预期行为。

情景 12：Symantec 客户端发生 802.1X“timeoutEvt”问题

问题

运行 Symantec 软件的客户端与消息 802.1X 'timeoutEvt' Timer expired for station and for message = M3 取消关联。

无论是否在 intel/Broadcom 卡上使用 A/G 无线电，EAP/Eapol 进程都未完成。使用 wep 或 wpa-psk 时没有任何问题。

条件

WLC 代码无关紧要。

APs -all model - 全部处于本地模式。
wlan 3 - WPA2+802.1X PEAP + mshcapv2
ssid 进行广播。
Radius 服务器 nps 2008
在使用 Asus、Braodcom、Intel - win7 或 win-xp 的所有 PC 上都安装 Symantec 防病毒软件

受影响的操作系统 - Windows 7 和 xp

受影响的无线适配器 - Intel(6205) 和 Broadcom

受影响的驱动程序/请求方 - 15.2.0.19，使用本地请求方。

修复/解决方法：在 win7 和 xp 上禁用 Symantec 网络保护和防火墙。这是 Symantec 用于 Win 7 和 XP 操作系统时产生的问题。

调试输出

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011:
00:13:ce:1a:92:41 Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

注意：

15.2 版本中存在如下特征（也出现在早期版本中）：

- 客户端从 AP 获取 M1

- 客户端发送 M2

- 客户端从 AP 获取 M3

- 客户端在发出 M4 之前搜寻新的成对密钥

- 客户端传输使用新密钥 AP 加密的 M4，将 M4 消息作为“解密错误”(decrypt error) 丢弃

- WLC“debug client”显示 M3 重新传输即将超时。显然，这是 Microsoft 和 Symantec 之间的问题，而与 Intel 无关。解决方法是删除 Symantec。这实际是 Windows 中可能存在而由 Symantec 触发的漏洞。调整 EAP 计时器无法解决此问题

关于此问题，Cisco TAC 会将受影响的客户转发给 Symantec 和 Microsoft。

情景 13：对于已开启 mDNS 监听的客户端未显示 Air Print 服务

开启 mDNS 监听后，客户端无法看到在 Apple 手持客户端设备上提供 AirPrint 服务的设备。

条件

5508 WLC 运行 7.6.100.0。
在开启 mDNS 监听的情况下，我们会在 WLC 上的“服务”(services) 部分下列出提供 AirPrint 服务的设备。

各个 mDNS 配置文件正确映射到 WLAN 和接口。
仍然无法在客户端上看到 AirPrint 设备。

运行的调试

debug client <mac addr>

debug mdns all enable

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to
155.43.129.216 reached for mobile 00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile
00:13:CE:1A:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Returning AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile
00:13:ce:1a:92:41
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Sent Deauthenticate to mobile on BSSID
00:0b:85:76:d3:e0 slot 1(caller 1x_auth_pae.c:1033) Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41
Scheduling deletion of Mobile Station: (callerId: 65) in 10 seconds
```

说明

客户端会请求“_universal._sub._ipps._tcp.local.”或“_universal._sub._ipp._tcp.local.”字符串，而不是“_ipp._tcp.local”或“_ipp._tcp.local.”字符串。
因此，添加 AirPrint 服务不起作用。已确定所请求的服务字符串将映射到“HP_Photosmart_Printer_1”
同一服务已添加在映射到 WLAN 的配置文件中，并且仍然没有为设备列出任何服务。

结果发现，由于附加域名且客户端查询**已附加域名的“dns- sd._udp.YVG.local.”，WLC 无法处理 Bonjour 包，原因是“dns-sd._udp.YVG.local.”在数据库中不存在。**

已确定有关相同内容的以下增强功能漏洞 -CSCuj32157

解决方法

唯一的解决方法是禁用 DHCP 选项 15（域名）或从客户端删除域名。

情景 14：由于已禁用快速 SSID 更改，Apple IOS 客户端“无法加入网络”

条件

大多数 Apple iOS 设备在默认设置为“禁用快速 ssid 更改”(fast ssid change disabled) 的同一思科 WLC 上从一个 WLAN 移至另一个 WLAN 时都会发生问题。

该设置导致在客户端尝试关联到另一个 WLAN 后，控制器便会从现有 WLAN 取消对客户端进行身份验证。

典型结果是在 iOS 设备上显示“无法加入网络”(unable to join the network) 消息

Show client

(jk-2504-116) >show network summary

<snip>

快速 SSID 更改 (Fast SSID Change) .....已禁用
运行的调试

```
(jk-2504-116) >debug client 1c:e6:2b:cd:da:9d


(jk-2504-116) >*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Association received
from mobile on BSSID 00:21:a0:e3:fd:be
Apple Client initiating switch from one wlan to another. *apfMsConnTask_7: Jan 30 21:33:14.544:
1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio *apfMsConnTask_7: Jan 30
21:33:14.544: 1c:e6:2b:cd:da:9d Max Client Trap Threshold: 0 cur: 1 *apfMsConnTask_7: Jan 30
21:33:14.544: 1c:e6:2b:cd:da:9d Rf profile 600 Clients are allowed to AP wlan *apfMsConnTask_7:
Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Deleting client immediately since WLAN has changed //WLC
removing apple client from original WLAN

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Scheduling deletion of Mobile Station:
(callerId: 50) in 1 seconds

*osapiBsnTimer: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireCallback (apf_ms.c:625)
Expiring Mobile!

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6632)
Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to
Disassociated



*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Sent Deauthenticate to mobile on BSSID
00:21:a0:e3:fd:b0 slot 1(caller apf_ms.c:6726)

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Found an cache entry for BSSID
00:21:a0:e3:fd:bf in PMKID cache at index 0 of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Removing BSSID 00:21:a0:e3:fd:bf from
PMKID cache of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Resetting MSCB PMK Cache Entry 0 for
station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Setting active key cache index 0 ---> 8

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Deleting the PMK cache when de-
authenticating the client.

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Global PMK Cache deletion failed.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsAssoStateDec

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6764)
Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Disassociated to Idle
```

```
*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d pemApfDeleteMobileStation2:
APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d 192.168.165.31 START (0) Deleted mobile
LWAPP rule on AP [00:21:a0:e3:fd:b0]

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d Deleting mobile on AP
00:21:a0:e3:fd:b0(1)

*pemReceiveTask: Jan 30 21:33:15.377: 1c:e6:2b:cd:da:9d 192.168.165.31 Removed NPU entry.
*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Adding mobile on LWAPP AP
00:21:a0:e3:fd:b0(1)
No client activity for > 7 sec due to fat-ssid change disabled *apfMsConnTask_7: Jan 30
21:33:23.890: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:bf
*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP
radio <Snip>  *apfMsConnTask_7: Jan 30 21:33:23.891: 1c:e6:2b:cd:da:9d Sending Assoc Response
to station on BSSID 00:21:a0:e3:fd:bf (status 0) ApVapId 1 Slot 1

*apfMsConnTask_7: Jan 30 21:33:23.892: 1c:e6:2b:cd:da:9d apfProcessAssocReq (apf_80211.c:8292)
Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to
Associated
```

解决办法

从 WLC GUI>>“控制器”(Controller)>>“常规”(General) 启用快速 ssid 更改

情景 15：客户端 LDAP 关联成功

安全 LDAP 使用 TLS 帮助保护控制器和 LDAP 服务器之间的连接。V7.6 和更高版本的控制器软件支持此功能。

控制器可以向 LDAP 服务器发送两种类型的查询：

1. 匿名：

在此类型中，当客户端需要进行身份验证时，控制器向 LDAP 服务器发送身份验证请求。然后，LDAP 服务器使用查询的结果进行响应。在此交换期间，包括客户端用户名/密码在内的所有信息都以明文形式发送。只要添加绑定用户名/密码，LDAP 服务器就将对来自任何人员的查询做出响应。

2. 经过身份验证：

在此方法中，控制器使用用于向 LDAP 服务器对自身进行身份验证的用户名和密码来进行配置。密码使用 MD5 SASL 进行加密，并在身份验证过程中发送到 LDAP 服务器。这可帮助 LDAP 服务器正确识别身份验证请求的来源。但是，即使控制器的身份受到保护，客户端详细信息仍会以明文形式发送。

这两种方法的客户端身份验证数据以及事务的其余内容均以明文形式处理，从而产生安全漏洞，因此确实需要使用基于 TLS 的 LDAP。

要求

WLC 运行 V7.6 和更高版本的软件

Microsoft 服务器执行 LDAP

运行的调试

debug aaa ldap enable

(jk-2504-116) >debug client 1c:e6:2b:cd:da:9d
(jk-2504-116) >***apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:be**
Apple Client initiating switch from one wlan to another. *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Max Client Trap Threshold: 0 cur: 1 *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Rf profile 600 Clients are allowed to AP wlan ***apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Deleting client immediately since WLAN has changed //WLC removing apple client from original WLAN**

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Scheduling deletion of Mobile Station: (callerId: 50) in 1 seconds

*osapiBsnTimer: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireCallback (apf_ms.c:625) Expiring Mobile!

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6632) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to Disassociated

***apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Sent Deauthenticate to mobile on BSSID 00:21:a0:e3:fd:b0 slot 1(caller apf_ms.c:6726)**

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Found an cache entry for BSSID 00:21:a0:e3:fd:bf in PMKID cache at index 0 of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Removing BSSID 00:21:a0:e3:fd:bf from PMKID cache of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Resetting MSCB PMK Cache Entry 0 for station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Setting active key cache index 0 ---> 8

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Deleting the PMK cache when de-authenticating the client.

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Global PMK Cache deletion failed.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsAssoStateDec

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6764) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Disassociated to Idle

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d 192.168.165.31 START (0) Deleted mobile LWAPP rule on AP [00:21:a0:e3:fd:b0]

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d Deleting mobile on AP 00:21:a0:e3:fd:b0(1)

***pemReceiveTask: Jan 30 21:33:15.377: 1c:e6:2b:cd:da:9d 192.168.165.31 Removed NPU entry.**

*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Adding mobile on LWAPP AP 00:21:a0:e3:fd:b0(1)
No client activity for > 7 sec due to fat-ssid change disabled *apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:bf

*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio <Snip> ***apfMsConnTask_7: Jan 30 21:33:23.891: 1c:e6:2b:cd:da:9d Sending Assoc Response to station on BSSID 00:21:a0:e3:fd:bf (status 0) ApVapId 1 Slot 1**

*apfMsConnTask_7: Jan 30 21:33:23.892: 1c:e6:2b:cd:da:9d apfProcessAssocReq (apf_80211.c:8292) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to Associated

情景 16：对 LDAP 的客户端身份验证失败

运行的调试

debug aaa ldap enable

(jk-2504-116) >debug client 1c:e6:2b:cd:da:9d

(jk-2504-116) >***apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:be**
Apple Client initiating switch from one wlan to another. *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Max Client Trap Threshold: 0 cur: 1 *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Rf profile 600 Clients are allowed to AP wlan ***apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Deleting client immediately since WLAN has changed //WLC removing apple client from original WLAN**

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Scheduling deletion of Mobile Station: (callerId: 50) in 1 seconds

*osapiBsnTimer: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireCallback (apf_ms.c:625) Expiring Mobile!

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6632) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to Disassociated

***apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Sent Deauthenticate to mobile on BSSID 00:21:a0:e3:fd:b0 slot 1(caller apf_ms.c:6726)**

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Found an cache entry for BSSID 00:21:a0:e3:fd:bf in PMKID cache at index 0 of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Removing BSSID 00:21:a0:e3:fd:bf from PMKID cache of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Resetting MSCB PMK Cache Entry 0 for station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Setting active key cache index 0 ---> 8

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Deleting the PMK cache when de-authenticating the client.

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Global PMK Cache deletion failed.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsAssoStateDec

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6764) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Disassociated to Idle

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d 192.168.165.31 START (0) Deleted mobile LWAPP rule on AP [00:21:a0:e3:fd:b0]

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d Deleting mobile on AP 00:21:a0:e3:fd:b0(1)

***pemReceiveTask: Jan 30 21:33:15.377: 1c:e6:2b:cd:da:9d 192.168.165.31 Removed NPU entry.**

*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Adding mobile on LWAPP AP 00:21:a0:e3:fd:b0(1)
No client activity for > 7 sec due to fat-ssid change disabled *apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:bf
*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio <Snip> ***apfMsConnTask_7: Jan 30 21:33:23.891: 1c:e6:2b:cd:da:9d Sending Assoc Response to station on BSSID 00:21:a0:e3:fd:bf (status 0) ApVapId 1 Slot 1**

*apfMsConnTask_7: Jan 30 21:33:23.892: 1c:e6:2b:cd:da:9d apfProcessAssocReq (apf_80211.c:8292) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to Associated

解决办法

检查 LDAP 服务器以查找拒绝原因。

情景 17：由于 LDAP 在 WLC 上配置不当，发生客户端关联问题

运行的调试

debug aaa ldap enable

(jk-2504-116) >debug client 1c:e6:2b:cd:da:9d

(jk-2504-116) >***apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:be**
Apple Client initiating switch from one wlan to another. *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Max Client Trap Threshold: 0 cur: 1 *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Rf profile 600 Clients are allowed to AP wlan ***apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Deleting client immediately since WLAN has changed //WLC removing apple client from original WLAN**

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Scheduling deletion of Mobile Station: (callerId: 50) in 1 seconds

*osapiBsnTimer: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireCallback (apf_ms.c:625) Expiring Mobile!

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6632) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to Disassociated

***apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Sent Deauthenticate to mobile on BSSID 00:21:a0:e3:fd:b0 slot 1(caller apf_ms.c:6726)**

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Found an cache entry for BSSID 00:21:a0:e3:fd:bf in PMKID cache at index 0 of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Removing BSSID 00:21:a0:e3:fd:bf from PMKID cache of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Resetting MSCB PMK Cache Entry 0 for station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Setting active key cache index 0 ---> 8

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Deleting the PMK cache when de-authenticating the client.

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Global PMK Cache deletion failed.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsAssoStateDec

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6764) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Disassociated to Idle

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d 192.168.165.31 START (0) Deleted mobile LWAPP rule on AP [00:21:a0:e3:fd:b0]

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d Deleting mobile on AP 00:21:a0:e3:fd:b0(1)

***pemReceiveTask: Jan 30 21:33:15.377: 1c:e6:2b:cd:da:9d 192.168.165.31 Removed NPU entry.**

*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Adding mobile on LWAPP AP 00:21:a0:e3:fd:b0(1)
No client activity for > 7 sec due to fat-ssid change disabled *apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:bf
*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio <Snip> ***apfMsConnTask_7: Jan 30 21:33:23.891: 1c:e6:2b:cd:da:9d Sending Assoc Response to station on BSSID 00:21:a0:e3:fd:bf (status 0) ApVapId 1 Slot 1**

*apfMsConnTask_7: Jan 30 21:33:23.892: 1c:e6:2b:cd:da:9d apfProcessAssocReq (apf_80211.c:8292) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to Associated

解决办法

跨客户端/WLC 和 LDAP 服务器验证凭证。

情景 18：当 LDAP 服务器无法访问时，发生客户端关联问题

运行的调试

debug aaa ldap enable

```
(jk-2504-116) >debug client 1c:e6:2b:cd:da:9d
(jk-2504-116) >*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:be
Apple Client initiating switch from one wlan to another. *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP radio *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Max Client Trap Threshold: 0 cur: 1 *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Rf profile 600 Clients are allowed to AP wlan *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Deleting client immediately since WLAN has changed //WLC removing apple client from original WLAN

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Scheduling deletion of Mobile Station: (callerId: 50) in 1 seconds

*osapiBsnTimer: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireCallback (apf_ms.c:625) Expiring Mobile!

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6632) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to Disassociated

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Sent Deauthenticate to mobile on BSSID 00:21:a0:e3:fd:b0 slot 1(caller apf_ms.c:6726)

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Found an cache entry for BSSID 00:21:a0:e3:fd:bf in PMKID cache at index 0 of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Removing BSSID 00:21:a0:e3:fd:bf from PMKID cache of station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Resetting MSCB PMK Cache Entry 0 for station 1c:e6:2b:cd:da:9d

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Setting active key cache index 0 ---> 8

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Deleting the PMK cache when de-authenticating the client.

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Global PMK Cache deletion failed.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsAssoStateDec

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d apfMsExpireMobileStation (apf_ms.c:6764) Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Disassociated to Idle

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.

*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d 192.168.165.31 START (0) Deleted mobile LWAPP rule on AP [00:21:a0:e3:fd:b0]
```

```
*apfReceiveTask: Jan 30 21:33:15.376: 1c:e6:2b:cd:da:9d Deleting mobile on AP
00:21:a0:e3:fd:b0(1)

*pemReceiveTask: Jan 30 21:33:15.377: 1c:e6:2b:cd:da:9d 192.168.165.31 Removed NPU entry.

*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Adding mobile on LWAPP AP
00:21:a0:e3:fd:b0(1)
No client activity for > 7 sec due to fat-ssid change disabled *apfMsConnTask_7: Jan 30
21:33:23.890: 1c:e6:2b:cd:da:9d Association received from mobile on BSSID 00:21:a0:e3:fd:bf
*apfMsConnTask_7: Jan 30 21:33:23.890: 1c:e6:2b:cd:da:9d Global 200 Clients are allowed to AP
radio <Snip>  *apfMsConnTask_7: Jan 30 21:33:23.891: 1c:e6:2b:cd:da:9d Sending Assoc Response to
station on BSSID 00:21:a0:e3:fd:bf (status 0) ApVapId 1 Slot 1

*apfMsConnTask_7: Jan 30 21:33:23.892: 1c:e6:2b:cd:da:9d apfProcessAssocReq (apf_80211.c:8292)
Changing state for mobile 1c:e6:2b:cd:da:9d on AP 00:21:a0:e3:fd:b0 from Associated to
Associated
```

解决办法

检查 WLC 和 LDAP 服务器网络连接问题。

情景 19：由于缺少粘性漫游配置，Apple 客户端发生漫游问题

条件

AIR-CT5508-K9 / 7.4.100.0

Apple 设备正在与使用以下配置的无线网络断开连接：

WPA2 策略
WPA2 加密 AES
已启用身份验证 802.1X

通过 Cisco ISE 进行身份验证和授权。

Apple 设备将定期与广播的 SSID 断开连接。例如，某个 iphone 将丢弃连接，而同一位置的另一个电话将保持连接。因此，此情况会随机发生（时间和电话都不定）。

笔记本电脑客户端没有问题。它们连接到同一 SSID。

此问题会在正常操作、无漫游、无备用模式期间发生。

WLAN 已经删除可能导致问题的所有可能设置 (aironet ext) 。

运行的调试

debug client <mac addr>

```
*apfMsConnTask_5: Jun 11 16:12:56.342: f0:d1:a9:bb:2d:fa Received RSN IE with 0 PMKIDs from
mobile f0:d1:a9:bb:2d:fa
At 16:12:56 in the debugs we see a client re-association.From there the AP is expecting the
client to present its old PMKID (Pairwise Master Key Identifiers).
At this point it doesn't!From the above message the AP/WLC didn’t receive a PMKID from the
iPhone.
This is kind of expected from this type of client.
```

Apple devices do not use the opportunistic key caching which allows clients to use the SAME PMKID at all Aps.
Apple devices use a key cache method of Sticky Key Caching.
This in turn means that the client has to build a PMKID at EACH AP in order to successfully roam to the AP.
As we can see the client didn't present a PMKID to use so we sent it through layer 2 security/EAP again.

The client then hits a snag in the EAP process where the client fails to respond to the EAP ID or request for credentials until the second attempt *dot1xMsgTask: Jun 11 16:12:56.345: f0:d1:a9:bb:2d:fa Sending EAP-Request/Identity to mobile f0:d1:a9:bb:2d:fa (EAP Id 1) *osapiBsnTimer: Jun 11 16:13:26.288: f0:d1:a9:bb:2d:fa 802.1x 'txWhen' Timer expired for station f0:d1:a9:bb:2d:fa and for message = M0 After this snag the client is allowed back onto the network all in approx. 1.5 seconds.
This is going to be normal and EXPECTED behavior currently with Sticky key cache clients.

解决办法

对于具有 SKC（粘性密钥缓存）客户端以及具有 WLC 代码 7.2 和更高版本的客户，我们现在可为其启用 SKC（粘性密钥缓存）漫游支持。
默认情况下，WLC 仅支持 OKC（机会性密钥缓存）。为允许客户端使用其在每个 AP 生成的旧 PMKID，必须通过 WLC CLI 将其启用。

config wlan security wpa wpa2 cache sticky enable <1>

请注意，由于 SKC 的性质，这不会改善初始漫游，但会改善同一 AP（根据本手册说明，最多支持 8 个 AP）的后续漫游。想像一下穿行一条具有 8 个 AP 的走廊。第一次穿行将由延迟约为 1-2 秒的每个 AP 上的完全关联组成。当您到达终点并返回时，客户端将最多提供 8 个唯一的 PMKID，因为其会移回到相同的 AP，并且在启用了 SKC 支持的情况下，将不必通过完整的身份验证。从而可消除延迟，并且客户端将显示为保持连接。

情景 20：通过 CCKM 验证快速安全漫游 (FSR)

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote- technology-00.html

运行的调试

debug client <mac addr>

*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c **CCKM: Received REASSOC REQ IE**
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c **Reassociation received from mobile on BSSID 84:78:ac:f0:2a:93**
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c

Processing WPA IE type 221, length 22 for mobile 00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
CCKM: Mobile is using CCKM
The Reassociation Request is received from the client, which provides the CCKM information needed in order to derive the new keys with a fast-secure roam. *apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c Setting active key cache index 0 ---> 8 *apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c CCKM: Processing REASSOC REQ IE *apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c **CCKM: using HMAC MD5 to compute MIC**
WLC computes the MIC used for this CCKM fast-roaming exchange. *apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c CCKM: Received a valid REASSOC REQ IE *apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c **CCKM: Initializing PMK cache entry with a new PTK**
The new PTK is derived.*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c Setting active key cache index 8 ---> 8 *apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c Setting active key cache index 8 ---> 8 *apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c Setting active

key cache index 8 ---> 0 *apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c **Creating a PKC PMKID Cache entry for station 00:40:96:b7:ab:5c (RSN 0) on BSSID 84:78:ac:f0:2a:93**
The new PMKID cache entry is created for this new AP-to-client association. *apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c CCKM: using HMAC MD5 to compute MIC *apfMsConnTask_2: Jun
25 15:43:33.751: 00:40:96:b7:ab:5c Including CCKM Response IE (length 62) in Assoc Resp to mobile *apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c **Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:93 (status 0) ApVapId 4 Slot 0**
The Reassociation Response is sent from the WLC/AP to the client, which includes the CCKM information required in order to confirm the new fast-roam and key derivation.*dot1xMsgTask: Jun 25 15:43:33.757: 00:40:96:b7:ab:5c **Skipping EAP-Success to mobile 00:40:96:b7:ab:5c**
EAP is skipped due to the fast roaming, and CCKM does not require further key handshakes. The client is now ready to pass encrypted data frames on the new AP.

如上所示，在避免 EAP 身份验证帧乃至 4 次握手的同时执行了快速安全漫游，因为新的加密密钥仍会派生，但基于 CCKM 协商方案派生。这是通过漫游重新关联帧以及客户端和 WLC 先前缓存的信息来完成的。

情景 21：通过 WPA2 PMKID 缓存验证快速安全漫游 (FSR)

运行的调试

debug client <mac addr>

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32 **Reassociation received from mobile on BSSID 84:78:ac:f0:68:d2**
This is the Reassociation Request from the client. *apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32 **Processing RSN IE type 48, length 38 for mobile ec:85:2f:15:39:32**
The WLC/AP finds an Information Element that claims PMKID Caching support on the Association request that is sent from the client. *apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32 **Received RSN IE with 1 PMKIDs from mobile ec:85:2f:15:39:32**
The Reassociation Request from the client comes with one PMKID.*apfMsConnTask_0: Jun 22 00:26:40.787: Received PMKID: (16) *apfMsConnTask_0: Jun 22 00:26:40.788: [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5 This is the PMKID that is received *apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32 **Searching for PMKID in MSCB PMKID cache for mobile ec:85:2f:15:39:32**
WLC searches for a matching PMKID on the database. *apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32 Found an cache entry for BSSID 84:78:ac:f0:68:d2 in PMKID cache at index 0 of station ec:85:2f:15:39:32 *apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32 **Found a valid PMKID in the MSCB PMKID cache for mobile ec:85:2f:15:39:32**
The WLC validates the PMKID provided by the client, and confirms that it has a valid PMK cache for this client-and-AP pair. *apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32 Setting active key cache index 1 ---> 0 *apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32 **Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d2(status 0) ApVapId 3 Slot 0**
The Reassociation Response is sent to the client, which validates the fast-roam with SKC. *dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32 **Initiating RSN with existing PMK to mobile ec:85:2f:15:39:32**
WLC initiates a Robust Secure Network association with this client-and-AP pair based on the cached PMK found.Hence, EAP is avoided as per the next message. *dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32 Skipping EAP-Success to mobile ec:85:2f:15:39:32 *dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32 Found an cache entry for BSSID 84:78:ac:f0:68:d2 in PMKID cache at index 0 of station ec:85:2f:15:39:32 *dot1xMsgTask: Jun 22 00:26:40.795: **Including PMKID in M1(16)**
The hashed PMKID is included on the Message-1 of the WPA/WPA2 4-Way handshake.*dot1xMsgTask: Jun 22 00:26:40.795: [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5 The PMKID is hashed.
The next messages are the same WPA/WPA2 4-Way handshake messages described thus far that are used in order to finish the encryption keys generation/installation. *dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32 Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00 *Dot1x_NW_MsgTask_2: Jun 22 00:26:40.811: ec:85:2f:15:39:32 Received EAPOL-Key from mobile ec:85:2f:15:39:32 *Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32 Received EAPOL-key in PTK_START state (message 2) from mobile ec:85:2f:15:39:32 *Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812:

ec:85:2f:15:39:32 PMK: Sending cache add *Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32 Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01 *Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32 Received EAPOL-Key from mobile ec:85:2f:15:39:32 *Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile ec:85:2f:15:39:32

情景 22：通过主动密钥缓存验证快速安全漫游 (FSR)

运行的调试

debug client <mac addr>

*apfMsConnTask_2: Jun 21 21:48:50.562: 00:40:96:b7:ab:5c **Reassociation received from mobile on BSSID 84:78:ac:f0:2a:92**
This is the Reassociation Request from the client. *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Processing RSN IE type 48, length 38 for mobile 00:40:96:b7:ab:5c The WLC/AP finds and Information Element that claims PMKID Caching support on the Association request that is sent from the client. *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Received RSN IE with 1 PMKIDs from mobile 00:40:96:b7:ab:5c The Reassociation Request from the client comes with one PMKID. *apfMsConnTask_2: Jun 21 21:48:50.563:Received PMKID: (16) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Searching for PMKID in MSCB PMKID cache for mobile 00:40:96:b7:ab:5c *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c No valid PMKID found in the MSCB PMKID cache for mobile 00:40:96:b7:ab:5 As the client has never authenticated with this new AP, the WLC cannot find a valid PMKID to match the one provided by the client. However, since the client performs PKC/OKC and not SKC (as per the following messages), the WLC computes a new PMKID based on the information gathered (the cached PMK,the client MAC address, and the new AP MAC address). *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Trying to compute a PMKID from MSCB PMK cache for mobile 00:40:96:b7:ab:5c *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: BSSID = (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 90 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: realAA = (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 92 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: PMKID = (16) *apfMsConnTask_2: Jun 21 21:48:50.563 : [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: AA (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 92 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: SPA (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 00 40 96 b7 ab 5c *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Adding BSSID 84:78:ac:f0:2a:92 to PMKID cache at index 0 for station 00:40:96:b7:ab:5c *apfMsConnTask_2: Jun 21 21:48:50.563: New PMKID: (16) *apfMsConnTask_2: Jun 21 21:48:50.563:[0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Computed a valid PMKID from MSCB PMK cache for mobile 00:40:96:b7:ab:5c The new PMKID is computed and validated to match the one provided by the client, which is also computed with the same information. Hence, the fast-secure roam is possible. *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Setting active key cache index 0 ---> 0 *apfMsConnTask_2: Jun 21 21:48:50.564: 00:40:96:b7:ab:5c Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:92 (status 0) ApVapId 3 Slot The Reassociation response is sent to the client, which validates the fast-roam with PKC/OKC. *dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Initiating RSN with existing PMK to mobile 00:40:96:b7:ab:5c WLC initiates a Robust Secure Network association with this client-and AP pair with the cached PMK found. Hence, EAP is avoided, as per the the next message. *dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Skipping EAP-Success to mobile 00:40:96:b7:ab:5c *dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Found an cache entry for BSSID 84:78:ac:f0:2a:92 in PMKID cache at index 0 of station 00:40:96:b7:ab:5c *dot1xMsgTask: Jun 21 21:48:50.570: Including PMKID in M1 (16) The hashed PMKID is included on the Message-1 of the WPA/WPA2 4-Way handshake. *dot1xMsgTask: Jun 21 21:48:50.570: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 The PMKID is hashed. The next messages are the same WPA/WPA2 4-Way handshake messages described thus far, which are used in order to finish the encryption keys generation/installation.
*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00 *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5 Received EAPOL-Key from mobile 00:40:96:b7:ab:5c *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c Received EAPOL-key in PTK_START state (message 2) from mobile 00:40:96:b7:ab:5c *Dot1x_NW_MsgTask_4: Jun 21

21:48:50.589: 00:40:96:b7:ab:5cPMK: Sending cache add *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.590: 00:40:96:b7:ab:5c Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01 *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c Received EAPOL-Key from mobile 00:40:96:b7:ab:5c *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:b7:ab:5c

如上所示，在调试开始时，必须在收到来自客户端的重新关联请求后计算 PMKID。需要满足此条件，以便验证 PMKID 并确认缓存的 PMK 与 WPA2 4 次握手配合使用，以派生加密密钥并完成快速安全漫游。请勿混淆调试中的 CCKM 条目；如前所述，为执行 CCKM 未使用此类条目，而是使用 PKC/OKC。CCKM 在此处只是 WLC 针对这些输出使用的名称，例如，用于处理值以便计算 PMKID 的函数的名称。

情景 23：通过 802.11r 验证快速安全漫游 (FSR)

运行的调试

debug client <mac addr>

*apfMsConnTask_2: Jun 21 21:48:50.562: 00:40:96:b7:ab:5c **Reassociation received from mobile on BSSID 84:78:ac:f0:2a:92**
This is the Reassociation Request from the client. *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Processing RSN IE type 48, length 38 for mobile 00:40:96:b7:ab:5c The WLC/AP finds and Information Element that claims PMKID Caching support on the Association request that is sent from the client. *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Received RSN IE with 1 PMKIDs from mobile 00:40:96:b7:ab:5c The Reassociation Request from the client comes with one PMKID. *apfMsConnTask_2: Jun 21 21:48:50.563:Received PMKID: (16) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Searching for PMKID in MSCB PMKID cache for mobile 00:40:96:b7:ab:5c *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c No valid PMKID found in the MSCB PMKID cache for mobile 00:40:96:b7:ab:5 As the client has never authenticated with this new AP, the WLC cannot find a valid PMKID to match the one provided by the client. However, since the client performs PKC/OKC and not SKC (as per the following messages), the WLC computes a new PMKID based on the information gathered (the cached PMK,the client MAC address, and the new AP MAC address). *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Trying to compute a PMKID from MSCB PMK cache for mobile 00:40:96:b7:ab:5c *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: BSSID = (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 90 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: realAA = (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 92 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: Find PMK in cache: PMKID = (16) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: AA (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 84 78 ac f0 2a 92 *apfMsConnTask_2: Jun 21 21:48:50.563: CCKM: SPA (6) *apfMsConnTask_2: Jun 21 21:48:50.563: [0000] 00 40 96 b7 ab 5c *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Adding BSSID 84:78:ac:f0:2a:92 to PMKID cache at index 0 for station 00:40:96:b7:ab:5c *apfMsConnTask_2: Jun 21 21:48:50.563: New PMKID: (16) *apfMsConnTask_2: Jun 21 21:48:50.563:[0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Computed a valid PMKID from MSCB PMK cache for mobile 00:40:96:b7:ab:5c The new PMKID is computed and validated to match the one provided by the client, which is also computed with the same information. Hence, the fast-secure roam is possible. *apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c Setting active key cache index 0 ---> 0 *apfMsConnTask_2: Jun 21 21:48:50.564: 00:40:96:b7:ab:5c Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:92 (status 0) ApVapId 3 Slot The Reassociation response is sent to the client, which validates the fast-roam with PKC/OKC. *dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Initiating RSN with existing PMK to mobile 00:40:96:b7:ab:5c WLC initiates a Robust Secure Network association with this client-and AP pair with the cached PMK found. Hence, EAP is avoided, as per the the next message. *dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Skipping EAP-Success to mobile 00:40:96:b7:ab:5c *dot1xMsgTask:

Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Found an cache entry for BSSID 84:78:ac:f0:2a:92 in PMKID cache at index 0 of station 00:40:96:b7:ab:5c *dot1xMsgTask: Jun 21 21:48:50.570: Including PMKID in M1 (16) The hashed PMKID is included on the Message-1 of the WPA/WPA2 4-Way handshake. *dot1xMsgTask: Jun 21 21:48:50.570: [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9 The PMKID is hashed. The next messages are the same WPA/WPA2 4-Way handshake messages described thus far, which are used in order to finish the encryption keys generation/installation. *dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00 *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5 Received EAPOL-Key from mobile 00:40:96:b7:ab:5c *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c Received EAPOL-key in PTK_START state (message 2) from mobile 00:40:96:b7:ab:5c *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5cPMK: Sending cache add *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.590: 00:40:96:b7:ab:5c Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01 *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c Received EAPOL-Key from mobile 00:40:96:b7:ab:5c *Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:b7:ab:5c