# 使用本备忘单解决常见的无线问题

## 目录

# 简介

本文档介绍通过调试（通常为debug client <mac地址>）分析常见无线问题的备忘单。

# 先决条件

## 要求

本文档没有任何特定的要求。

## 使用的组件

本文档中的信息基于所有AireOS控制器。

- 控制器- 440x、5508、5520、75xx、85xx、2504、3504和vWLC，以及WISM。
- 虽然融合接入IOS® XE控制器和交换机的许多概念是相同的，但本文档不适用于这些概念，因为输出和调试是截然不同的。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# Show Client输出中的简要PEM状态

要通过show client和debug进行分析，首先需要了解某些电源输入模块(PEM)状态和APF状态。

- START — 新客户端条目的初始状态。
- AUTHCHECK - WLAN具有要强制执行的L2身份验证策略。
- 8021X_REQD -客户端必须完成802.1x认证。
- L2AUTHCOMPLETE -客户端已成功完成L2策略。该过程现在可以继续执行L3策略（地址学习、网络身份验证等）。如果这是同一移动组中的漫游客户端，控制器将发送移动通告以从其他控制器获取第3层信息。
- WEP_REQD — 客户端必须完成 WEP 认证。

- DHCP_REQD -控制器从客户端获取L3地址，这通过ARP请求、DHCP请求或更新完成，或通过从该移动组中的其他控制器获取的信息完成。如果 WLAN 上标记有 DHCP Required，则仅使用 DHCP 或移动信息。
- WEBAUTH_REQD — 客户端必须完成 Web 认证。（L3 策略）
- CENTRAL_WEBAUTH_REQD -客户端必须完成CWA登录。WLC等待接收CoA。
- RUN -客户端已成功完成所需的L2和L3策略，此时可以向网络传输流量。

给定场景显示了无线设置中常见错误配置的关键调试行，这些错误配置以粗体突出显示关键参数。

# 场景1：客户端上用于WPA/WPA2 PSK身份验证的口令配置错误

<#root>

```
(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 Received..... 0

Number of Data Rx Packets Dropped..... 0

Number of Data Bytes Received..... 0

Number of Data Rx Bytes Dropped..... 0

Number of Realtime Packets Received..... 0

Number of Realtime Rx Packets Dropped..... 0

Number of Realtime Bytes Received..... 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：

<#root>

```
(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
*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 Unas

*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' (AC
*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 0.0.0.0 START (0) Changing IPv6 ACL 'none' (AC
*apfMsConnTask_4: May 07 17:03:56.060: 24:77:03:19:fb:70 apfApplyWlanPolicy: Apply WLAN Policy over PMI
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 In processSsidIE:4795 setting Central switched
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 In processSsidIE:4798 apVapId = 5 and Split Ac
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Applying site-specific Local Bridging override
*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Applying Local Bridging Interface Policy for s
*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
*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
```

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

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

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 pemApfDeleteMobileStation2: APF_MS_PEM_WAIT_L2

*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

*apfMsConnTask_4: May 07 17:03:56.061: 24:77:03:19:fb:70 Updated location for station old AP ec:c8:82:a

*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

*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

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

***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 ru

*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 sta

*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfPemAddUser2:session timeout forstation 24:7

*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Stopping deletion of Mobile Station: (callerId

*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Func: apfPemAddUser2, Ms Timeout = 0, Session

*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 Sending Assoc Response to station on BSSID 08:

*apfMsConnTask_4: May 07 17:03:56.062: 24:77:03:19:fb:70 apfProcessAssocReq (apf_80211.c:8292) Changing

*spamApTask3: May 07 17:03:56.065: 24:77:03:19:fb:70 Sent 1x initiate message to multi thread task for

*Dot1x_NW_MsgTask_0: May 07 17:03:56.065: 24:77:03:19:fb:70 Creating a PKC PMKID Cache entry for statio

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 Resetting MSCB PMK Cache Entry 0 for statio

*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

*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 cac

*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

*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

*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 int

*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:

*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**

***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:**

***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**

**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**

**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 mo

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70 mscb->apfMsLwappLradNhMac = b0:fa:eb:b8:f5:

*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-

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70  dot1xcb->snapOrg = 00 00 00 dot1xcb->eapol

*Dot1x_NW_MsgTask_0: May 07 17:03:56.066: 24:77:03:19:fb:70  mscb->apfMsLwappMwarPort = 5246 mscb->apfM

*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:

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

*Dot1x_NW_MsgTask_0: May 07 17:03:56.069: 24:77:03:19:fb:70 Received EAPOL-key in PTK_START state (mess

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

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

```
 ***!--- 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 mobi
*dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70 mscb->apfMsLwappLradNhMac = b0:fa:eb:b8:f5:12 msc
*dot1xMsgTask: May 07 17:03:56.364: 24:77:03:19:fb:70  mscb->apfMsBssid = 08:cc:68:67:1f:f0 mscb->apfMs
*dot1xMsgTask: May 07 17:03:56.365: 24:77:03:19:fb:70  dot1xcb->snapOrg = 00 00 00 dot1xcb->eapolWepBit
*dot1xMsgTask: May 07 17:03:56.365: 24:77:03:19:fb:70  mscb->apfMsLwappMwarPort = 5246 mscb->apfMsLwapp
*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:
*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-key in PTK_START state (mess
*Dot1x_NW_MsgTask_0: May 07 17:03:56.366: 24:77:03:19:fb:70 Received EAPOL-key M2 with invalid MIC from
```

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

```
 ***!--- MIC error due to wrong preshared key
```

## 结论

虽然timeoutEvt for M2 key也可能是由于驱动程序/NIC错误引起的，但最常见的问题之一是用户为PSK密码输入了不正确的凭据（缺少区分大小写/特殊字符等），并且无法连接。

场景2：无线电话听筒(792x/9971)无法与无线“离开服务区”关联

参考：7925G话机无法关联到AP -呼叫失败：TSPEC QOS策略不匹配

**拓扑**

采用Cisco统一无线IP电话的WLAN。

问题详细资料

AIR-CT5508-50-K9 //升级的电话和无线控制器固件不接受电话注册。

调试和日志：

<#root>

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

*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

*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

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying site-specific Local Bridging override

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying Local Bridging Interface Policy for st

*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

*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

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

*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 4

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

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

*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

*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:x

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Scheduling deletion of Mobile Station:  (caller

**VoIP Call Failure: '1x:xx:1x:xx:xx:xx' client, detected by 'xx-xx-xx' AP on radio type '802.11b/g'. Rea**

.

***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**

结论

在WLC上的调试显示7925G关联失败，因为AP返回关联状态代码201。

这是因为WLAN配置导致听筒拒绝流量规范(TSPEC)请求。尝试连接的WLAN 7925G配置的QoS配置文件为银牌(UP 0,3)，而不是白金级(UP 6,7)（根据需要）。这会导致WLAN的听筒中语音流量/操作帧交换的TSPEC不匹配，并最终导致AP拒绝。

根据7925G部署指南中的定义，为7925G手机创建具有白金服务QoS配置文件的新WLAN：

思科统一无线IP电话7925G、7925G-EX和7926G部署指南

正确配置后，即可解决问题。

方案3：为WPA配置的客户端，但仅为WPA2配置AP

**debug client <mac addr>**：

<#root>

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 10:51:44 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 0.0.0.0 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 phas**

方案4：解析AAA返回或响应代码

**要收集**预期日志，需要运行以下调试：

(Cisco Controller) > **debug mac addr <mac>**

(Cisco Controller) > **debug aaa events enable**

(或者)

(Cisco Controller) > **debug client <mac>**

(Cisco Controller) > **debug aaa events enable**

(Cisco Controller) > **debug aaa errors enable**

如果启用了陷阱，则AAA连接失败会生成SNMP陷阱。

debug输出示例：

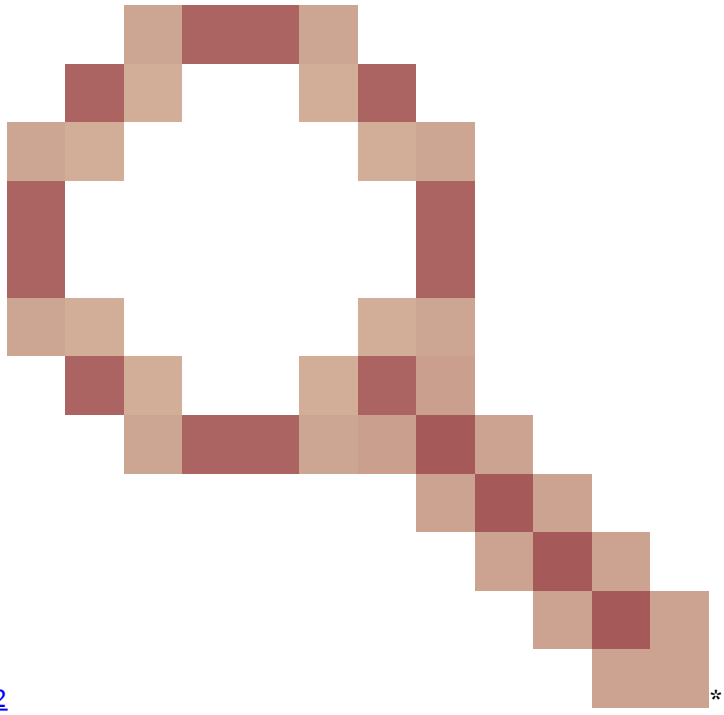
<#root>

*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
*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. Cisco bug ID CSCud12582 ***Proc

**Returning AAA Error 'Authentication Failed' (-4) for mobile**

***its the most common reason seen

可能的原因:

- 用户帐户和/或密码无效。
- 计算机不是域的成员，请在AD端出现问题。
- 证书服务无法正常工作。
- 服务器证书已过期或未使用。

    - RADIUS配置不正确。
- 访问密钥输入错误-它区分大小写（SSID也一样）。
- 更新Microsoft修补程序。
- EAP计时器。
- 客户端/服务器上配置的EAP方法不正确。
- 客户端证书已过期或未使用。

返回Mobile的AAA错误超时(-5)

AAA Server Unreachable（无法访问AAA服务器），然后是客户端取消身份验证。

示例：

<#root>

Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to 209.165.200.254 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**

**Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Processing AAA Error 'Timeout' (-5) for mobile 00:13:ce:1a:9**
**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 slo**

Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Scheduling deletion of Mobile Station: (callerId: 65) in 10

返回手机的AAA错误内部错误(-6)

属性不匹配。AAA发送不正确或不合适的属性（错误长度），这些属性与WLC不理解/不兼容。WLC发送Deauth消息，然后发送内部错误消息。示例：Cisco Bug ID CSCum83894 AAA Internal Error and auth fail with unknown attributes in access accept。

示例：

*radiusTransportThread: Feb 21 12:14:36.109: Aborting ATTR processing 599 (avp 26/6) *radiusTransportThread: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd

返回移动的AAA错误无服务器(-7)。

Radius配置不正确和/或使用不支持的配置。

示例：

*Jun 22 20:32:10.229: 00:21:e9:57:3c:bf Returning AAA Error 'No Server' (-7) for mobile 00:21:e9:57:3c:bf *Jun 22 20:32:10.229: AuthorizationResponse

场景5：客户端无法关联到AP

使用的调试：

**debug client <mac addr>**

要解析的日志：

向BSSID 00:26：cb：94:44：c0（状态0） ApVapId 1插槽0上的工作站发送关联响应

- 插槽0 = B/G(2.4)射频
- 插槽1 = A(5)无线电
- 发送Assoc响应状态0 =成功

除状态0以外的任何状态均为“失败”。

常见关联响应状态代码位于：802.11 Association Status，802.11 Deauth Reason Code

场景6：由于空闲超时客户端取消关联

使用的调试：

**debug client <mac addr>**

要解析的日志

从AP 00:26：cb：94:44：c0，插槽0接收空闲超时，适用于STA 00:1e：8c：0f：a4:57

apfMsDeleteByMscb Scheduling mobile for deletion with deleteReason 4， reasonCode 4

安排在1秒内删除移动站：（呼叫方ID： 30）

apfMsExpireCallback (apf_ms.c：608) Expiring Mobile！

已在BSSID 00:26：cb：94:44：c0 slot 0(caller apf_ms.c：5094)上将取消身份验证发送到移动设备

**条件**

在未收到来自客户端的流量时发生。

默认持续时间为300秒。

**解决方法**

从WLC全局增加空闲超时GUI>>Controller>>General，或者从WLC按WLAN增加空闲超时 **GUI>WLAN>ID>>Advanced**.

场景7：由于会话超时，客户端取消关联

使用的调试：

**debug client <mac addr>**

要解析的日志：

apfMsExpireCallback (apf_ms.c:608) Expiring Mobile! apfMsExpireMobileStation (apf_ms.c:5009) Changing state for mobile 00:1e:8c:0f:a4:57 on AP 00

**条件**

在计划的持续时间（默认1800秒）时发生。

它强制WEBAUTH用户再次进行WEBAUTH。

**解决方法**

增加或禁用每个WLAN在WLC上的会话超时 **GUI>WLAN>ID>Advanced**。

场景8：由于WLAN更改导致客户端取消关联

使用的调试：

**debug client <mac addr>**

要解析的日志：

apfSendDisAssocMsgDebug (apf_80211.c:1855) Changing state for mobile 00:1e:8c:0f:a4:57 on AP 00:26:cb:94:44:c0 from Associated to Disassociated S

**条件**

要以任何方式修改WLAN，请禁用和重新启用WLAN。

**解决方法**

这是预料之中的现象。当进行WLAN更改时，客户端会取消关联并重新关联。

情景9：由于手动从WLC中删除，客户端取消关联

使用的调试：

**debug client <mac addr>**

要解析的日志：

apfMsDeleteByMscb Scheduling mobile for deletion with deleteReason 6, reasonCode 1 Scheduling deletion of Mobile Station: (callerId: 30) in 1 seconds

**条件**

从GUI中：删除客户端

从CLI： **config client deauthenticate <mac address>**

场景10：由于身份验证超时客户端取消关联

使用的调试：

**debug client <mac addr>**

要解析的日志：

Retransmit failure for EAPOL-Key M3 to mobile 00:1e:8c:0f:a4:57, retransmit count 3, mscb deauth count 0 Sent Deauthenticate to mobile on BSSID 00:2

**条件**

已达到身份验证或密钥交换最大重新传输次数。

**解决方法**

检查/更新客户端驱动程序、安全配置、证书等。

场景11：由于AP无线电重置（电源/信道）导致客户端取消关联

使用的调试：

**debug client <mac addr>**

要解析的日志：

Cleaning up state for STA 00:1e:8c:0f:a4:57 due to event for AP 00:26:cb:94:44:c0(0) apfSendDisAssocMsgDebug (apf_80211.c:1855) Changing state for

**条件**

AP取消关联客户端，但WLC不删除条目。

**解决方法**

预期行为。

场景12:802.1X“timeoutEvt”的Symantec客户端问题

问题

对于站点和消息= M3，运行Symantec软件的客户端与消息802.1X timeoutEvt. 计时器超时取消关联

EAP/Eapol过程无法完成，无论Intel/Broadcom卡上使用的是A/G射频。使用wep、wpa-psk时没有问题。

**条件**

WLC代码并不重要。

AP -所有型号-全部在本地模式下。
wlan 3 - WPA2+802.1X PEAP + mshcapv2
广播SSID。

RADIUS服务器nps 2008。
所有PC上都安装了Symantec防病毒软件。

使用Asus、Broadcom、Intel - win7、win-xp。

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。

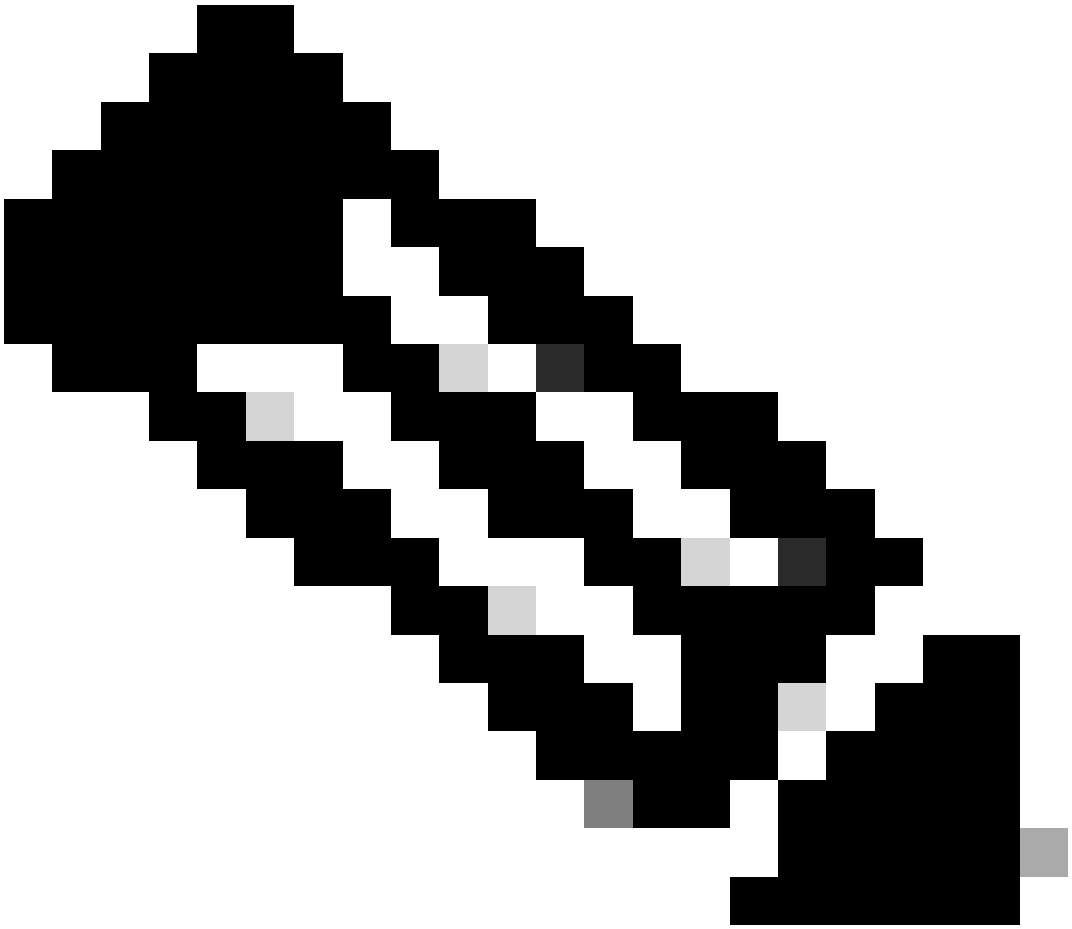
**修复/解决方法**

在win7和xp上禁用Symantec Network Protection and Firewall。这是Win 7和XP操作系统的Symantec问题。

调试输出:

*dot1xMsgTask: Apr 12 11:45:39.335: 84:3a:4b:7a:d5:ac Retransmit 1 of EAPOL-Key M3 (length 155) for mobile 84:3a:4b:7a:d5:ac *osapiBsnTimer: Ap
*dot1xMsgTask: Apr 12 11:45:44.336: 84:3a:4b:7a:d5:ac Retransmit 2 of EAPOL-Key M3 (length 155) for mobile 84:3a:4b:7a:d5:ac *osapiBsnTimer: Ap
*dot1xMsgTask: Apr 12 11:45:49.336: 84:3a:4b:7a:d5:ac Retransmit 3 of EAPOL-Key M3 (length 155) for mobile 84:3a:4b:7a:d5:ac *osapiBsnTimer: Ap

---



**注意**：15.2（在早期版本中也可见）中存在如下症状：
-client从AP获取M1
-client发送M2
-client从AP获取M3
-client在发出M4之前先填充新的成对密钥

---

- 客户端传输使用新密钥AP加密的M4，并将M4消息作为“解密错误”丢弃。

- WLC调试客户端显示您的M3重新传输超时。显然，这是Microsoft和Symantec之间的问题，而不是特定于Intel的问题。解决方法是删除Symantec。

- 这实际上是一个可能在Windows中由Symantec触发的Bug。调整EAP计时器无法解决此问题。

- 关于此问题，Cisco TAC将受影响的用户转发给Symantec和Microsoft。

场景13：Air Print Service未显示在启用了监听的mDNS的客户端上

打开mDNS监听时，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，带7.6.100.0。
在启用mDNS监听的情况下，在WLC的“服务”部分下列出了提供AirPrint服务的设备。
相应的mDNS配置文件已正确映射到WLAN和接口。
仍然无法看到客户端上的AirPrint设备。

使用的调试：

**debug client <mac addr>**

**debug mdns all enable**

*Bonjour_Msg_Task: Apr 15 15:29:35.640: b0:65:bd:df:f8:71 Query Service Name: _universal._sub._ipp._tcp.local., Type: C, Class: 1. *Bonjour_Msg_Ta
*Bonjour_Msg_Task: Apr 15 15:29:35.640: Sending Query Response bonjSpNameStr: _dns-sd._udp.YVG.local., bonjMsalServiceName: HP_Photosmart_

说明：

客户端会请求_universal._sub._ipps._tcp.local或_universal._sub._ipp._tcp.local而不是 **_ipp._tcp.local** 或_ipp._tcp.local字符串。
因此，添加的AirPrint服务不起作用。已标识该服务并将请求的服务字符串映射到 HP_Photosmart_Printer_1.
相同服务已添加到映射到WLAN的配置文件中，但没有为设备列出服务。

我们发现，由于附加了域名，并且添加了域名以执行dns-sd._udp.YVG local的客户端查询，WLC无法处理Bonjour数据包，因为dns-sd._udp.YVG.local在数据库中不存在。

已确定与相同漏洞相关的给定增强Bug - Cisco Bug ID 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设备在使用默认 fast SSID change disabled的相同Cisco WLC上面临从一个WLAN移动到另一个WLAN的问题。

设置导致控制器在客户端尝试关联到另一个客户端后，从存在的WLAN取消对客户端的身份验证。

通常的结果是iOS设备上的“nable to Join the Network" Umessage”。

Show client

(jk-2504-116) >显示网络摘要

<snip>

快速SSID更改.....禁用

使用的调试：

## <#root>

(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**

***Apple Client initiating switch from one wlan to another. *apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e

***apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Deleting client immediately since WLAN has chan**

*apfMsConnTask_7: Jan 30 21:33:14.544: 1c:e6:2b:cd:da:9d Scheduling deletion of Mobile Station: (calle

***apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Sent Deauthenticate to mobile on BSSID 00:21:a0:**

*apfReceiveTask: Jan 30 21:33:15.375: 1c:e6:2b:cd:da:9d Found an cache entry for BSSID 00:21:a0:e3:fd:

***pemReceiveTask: Jan 30 21:33:15.377: 1c:e6:2b:cd:da:9d 192.0.2.254 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 fast-ssid change disabled *apfMsConnTask_7: Jan 30 21:33:23.89

***apfMsConnTask_7: Jan 30 21:33:23.891: 1c:e6:2b:cd:da:9d Sending Assoc Response to station on BSSID 00:**

*apfMsConnTask_7: Jan 30 21:33:23.892: 1c:e6:2b:cd:da:9d apfProcessAssocReq (apf_80211.c:8292) Changin

**解决方法**

启用WLC的快速更改ssid GUI > Controller>General.

场景15：客户端LDAP关联成功

安全LDAP有助于保护控制器与使用TLS的LDAP服务器之间的连接。控制器软件版本7.6及更高版本支持此功能。

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，当客户端需要获得身份验证时，控制器会向LDAP服务器发送身份验证请求。LDAP服务器使用查询结果进行响应。在此交换时，包括客户端用户名/密码的所有信息均以明文发送。只要添加了绑定用户名/密码，LDAP服务器就会响应来自任何用户的查询。

2. 已验证

在此类型中，控制器配置有用于向LDAP服务器验证自身的用户名和密码。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。这有助于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，客户端详细信息仍以明文发送。

LDAP over TLS的真正需求源于这两种类型造成的安全漏洞，在这种漏洞中，客户端身份验证数据和事务的其他部分会以明文形式发生。

**要求**

WLC运行软件版本7.6及更高版本。

Microsoft服务器使用LDAP。

使用的调试：

**debug aaa ldap enable**

*LDAP DB Task 1: Feb 06 12:28:12.912: ldapAuthRequest [1] called lcapi_query base="CN=Users,DC=gceaaa,DC=com" type="person" attr="sAMAcco

场景16：LDAP上的客户端身份验证失败

使用的调试：

**debug aaa ldap enable**

*LDAP DB Task 1: Feb 07 17:19:46.535: LDAP_CLIENT: Received no referrals in search result msg *LDAP DB Task 1: Feb 07 17:19:46.535: LDAP_C

**解决方法**

检查LDAP服务器是否存在拒绝原因。

方案17：由于WLC上的LDAP配置错误导致的客户端关联问题

使用的调试：

**debug aaa ldap enable**

*LDAP DB Task 1: Feb 07 17:21:26.710: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success) *LDAP DB Task 1: Feb 07 17:21:26.712: ldapInitAndBi

**解决方法**

跨客户端/WLC和LDAP服务器验证凭证。

方案18：无法访问LDAP服务器时的客户端关联问题

使用的调试：

**debug aaa ldap enable**

*LDAP DB Task 2: Feb 07 17:26:45.874: ldapInitAndBind [2] configured Method Anonymous lcapi_bind (rc = 1005 - LDAP bind failed) *LDAP DB Tas

**解决方法**

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客户端漫游问题

**条件**

AIR-CT5508-K9 / 7.4.100.0

Apple设备会断开与以下无线网络的连接：

- WPA2策略
- WPA2加密AES
- 身份验证802.1X已启用

Cisco ISE的身份验证和授权。

Apple设备会定期断开与广播SSID的连接。例如，当同一位置的另一部电话保持连接时，iPhone会掉线。因此，这种情况是随机发生的（时间和电话）。

笔记本电脑客户端没有问题。它们连接到同一个SSID。

此问题发生在正常操作期间，没有漫游和备用模式。

WLAN已删除所有可能导致问题的可能设置(aironet ext)。

使用的调试：

**debug client <mac addr>**

<#root>

***apfMsConnTask_5: Jun 11 16:12:56.342: f0:d1:a9:bb:2d:fa Received RSN IE with 0 PMKIDs from mobile f0:d1**

```
 ***At 16:12:56 in the debugs we see a client re-association. From there the AP is expecting the client
***At this point it does not! 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
***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
***As we can see the client did not present a PMKID to use so we sent it through layer 2 security/EAP a
***The client then hits a snag in the EAP process where the client fails to respond to the EAP ID or re
***This is going to be normal and EXPECTED behavior currently with Sticky key cache clients.
```

**解决方法**

对于拥有粘滞密钥缓存(SKC)客户端并拥有WLC代码7.2及更高版本的客户，您现在所能做的就是为SKC启用漫游支持。默认情况下，WLC仅支持随机密钥缓存(OKC)。为了允许客户端使用其在每个AP上生成的旧PMKID，您必须通过WLC CLI启用它。

**config wlan security wpa wpa2 cache sticky enable <1>**

请记住，由于SKC的性质，这不会改善初始漫游；但是，它会改善对相同AP的后续漫游（本手册中最多可达8次）。想象一下有8个AP的走廊。第一个演练包含每个AP的完全关联，延迟大约为1-2秒。当您到达终点并走回终点时，客户端会显示8个唯一PMKID，同时返回到相同关联。

如果启用了SKC支持，则AP无需通过完全身份验证。这样可以消除延迟，并且客户端看起来可以保持连接。

场景20：使用CCKM验证快速安全漫游(FSR)

802.11 WLAN漫游和CUWN快速安全漫游

使用的调试：

**debug client <mac addr>**

<#root>

*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 mob

**CCKM: Mobile is using CCKM**

***The Reassociation Request is received from the client, which provides the CCKM information needed i

**CCKM: using HMAC MD5 to compute MIC**

***WLC computes the MIC used for this CCKM fast-roaming exchange. *apfMsConnTask_2: Jun 25 15:43:33.75

**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

**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 2

**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 informati

**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 clien

如图所示，执行快速安全漫游以避免EAP身份验证帧和更多的4次握手，因为新的加密密钥仍然是CCKM协商方案派生的。这通过漫游重新关联帧以及客户端和WLC之前缓存的信息来完成。

场景21：使用WPA2 PMKID缓存验证快速安全漫游(FSR)

使用的调试：

**debug client <mac addr>**

<#root>

*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:1

**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 reques

**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 00:26:40.7

**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:

**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

**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. *dot1xMsg

**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

**Including PMKID in M1(16)**

***The hashed PMKID is included on the Message-1 of the WPA/WPA2 4-Way handshake. *dot1xMsgTask: Jun 2

场景22：验证使用主动密钥缓存的快速安全漫游

使用的调试：

**debug client <mac addr>**

<#root>

*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:b
***However, since the client performs PKC/OKC and not SKC (as per the following messages), the WLC compu

如调试开始时所示，必须在收到来自客户端的重新关联请求后计算PMKID。验证PMKID并确认缓存的PMK与WPA2 4次握手一起使用来获取加密密钥并完成快速安全漫游时，需要执行此操作。请勿混淆调试中的CCKM条目；如前所述，这不是用于执行CCKM，而是PKC/OKC。在这里，CCKM只是WLC用于这些输出的名称，例如处理值以计算PMKID的函数的名称。

场景23：使用802.11r验证快速安全漫游(FSR)

使用的调试：

**debug client <mac addr>**

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32 Doing preauth for this client over the Air ***WLC begins FT fast-secure roaming over-the-A
because the client asks for this with FT on the Authentication frame that is sent to the new AP over-the-Air (before the Reassociation Request). *apfMsCon

.

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。