針對常見無線問題使用此備忘單

目錄

簡介

必要條件

- 需求
- 採用元件

Show Client輸出中的簡要PEM狀態

案例1：使用者端上針對WPA/WPA2 PSK驗證設定的密碼短語錯誤

- 結論

場景2：無線電話聽筒(792x/9971)無法與無線「離開服務區」關聯

- 拓撲
- 問題詳細資料
- 結論

方案3：客戶端配置了WPA，但AP僅配置了WPA2

案例4：剖析AAA傳回或回應代碼

方案5：客戶端無法與AP關聯

案例6：因閒置逾時而取消從屬端關聯

- 狀況
- 因應措施

方案7：由於會話超時客戶端取消關聯

- 狀況
- 因應措施

方案8：由於WLAN更改而取消客戶端關聯

- 狀況
- 因應措施

方案9：由於手動從WLC刪除而取消客戶端關聯

- 狀況

方案10：由於身份驗證超時客戶端取消關聯

- 狀況
- 因應措施

方案11：由於AP無線電重置（電源/通道）導致客戶端取消關聯

- 狀況
- 因應措施

場景12：Symantec客戶端與802.1X「timeoutEvt」有關的問題

- 問題
- 狀況
- 修復/解決方法

場景13：Air Print Serviceid未顯示啟用監聽的mDNS客戶端

- 狀況
- 因應措施

方案14：由於停用了快速SSID更改，Apple iOS客戶端「無法加入網路」

- 狀況
- 因應措施

案例15：成功建立使用者端LDAP關聯

方案16：LDAP上的客戶端身份驗證失敗
因應措施
方案17：由於WLC上的LDAP配置錯誤而出現的客戶端關聯問題
因應措施
案例18：無法連線至LDAP伺服器時的使用者端關聯問題
因應措施
方案19：由於缺少粘滯漫遊配置，Apple客戶端漫遊問題
狀況
因應措施
案例20：使用CCKM驗證快速安全漫遊(FSR)
案例21：使用WPA2 PMKID快取驗證快速安全漫遊(FSR)
方案22：使用主動金鑰快取驗證快速安全漫遊
案例23：驗證使用802.11r的快速安全漫遊(FSR)

簡介

本檔案介紹透過偵錯（通常為debug client <mac address>）來剖析常見無線問題的備忘單。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於所有AireOS控制器。

- 控制器- 440x、5508、5520、75xx、85xx、2504、3504和vWLC以及WISM。
- 雖然許多概念在融合接入IOS® XE控制器和交換機中是相同的，但由於輸出和調試完全不同，本文檔不適用於這些概念。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

Show Client輸出中的簡要PEM狀態

要透過show client和debug進行剖析，首先需要瞭解某些Power Entry Module (PEM)狀態和APF狀態。

- START -新客戶端條目的初始狀態。
- AUTHCHECK - WLAN具有要強制執行的L2身份驗證策略。
- 8021X_REQD -客戶端必須完成802.1x認證。
- L2AUTHCOMPLETE -客戶端已成功完成L2策略。此過程現在可以繼續執行L3策略（地址學習、Web身份驗證等）。如果這是同一移動組中的漫遊客戶端，控制器會傳送移動通告以從其他控制器獲取L3資訊。

- WEP_REQD -客戶端必須完成WEP認證。
- DHCP_REQD -控制器從客戶端獲取L3地址，這透過ARP請求、DHCP請求或更新完成，或透過從該移動組中的其他控制器獲取的資訊完成。如果在WLAN上標籤「DHCP必需」，則僅使用DHCP或移動性資訊。
- WEBAUTH_REQD -客戶端必須完成Web身份驗證。（L3策略）
- CENTRAL_WEBAUTH_REQD -客戶端必須完成CWA登入。WLC等待接收CoA。
- RUN -客戶端已成功完成所需的L2和L3策略，此時可以向網路傳輸流量。

給定場景顯示了無線設定中常見錯誤配置的主要調試行，這些錯誤配置以粗體突出顯示關鍵引數。

案例1：使用者端上針對WPA/WPA2 PSK驗證設定的密碼短語錯誤

<#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
-------------------------
```

調試客戶端分析：

<#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
```

結論

雖然M2金鑰的timeoutEvt也可能是由於驅動程式/NIC錯誤所致，但最常見的問題之一是使用者為PSK密碼輸入了不正確的憑據（缺少區分大小寫/特殊字元等），並且無法連線。

場景2：無線電話聽筒(792x/9971)無法與無線「離開服務區」關聯

參考：7925G手機無法關聯到AP -呼叫失敗：TSPEC QOS策略不匹配

拓撲

WLAN和Cisco Unified Wireless IP電話。

問題詳細資料

AIR-CT5508-50-K9 //升級的電話和無線控制器韌體不接受電話註冊。

調試和日誌：

<#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

結論

在WLC上的調試顯示，當AP返回關聯狀態代碼201時，7925G關聯失敗。

這是由於WLAN配置導致手機拒絕流量規範(TSPEC)請求所致。嘗試連線的WLAN 7925G的QoS配置檔案配置為Silver (UP 0,3)，而不

是根據需要配置Platinum (UP 6,7)。這會導致WLAN從手機交換語音流量/操作幀的TSPEC不匹配，並最終導致來自AP的拒絕。

建立一個新的WLAN，其中的QoS配置檔案為Platinum，專門用於7925G手持裝置，並且根據已建立的最佳實踐和《7925G部署指南》中的定義進行配置：

Cisco統一無線IP電話7925G、7925G-EX和7926G部署指南

正確配置後，即可解決問題。

方案3：客戶端配置了WPA，但AP僅配置了WPA2

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**

案例4：剖析AAA傳回或回應代碼

要執行以收集預期記錄檔所需的偵錯：

（思科控制器）**> debug mac addr <mac>**

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

(或)

（思科控制器）**> debug client <mac>**

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

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

如果啟用了陷阱，AAA連線失敗會生成SNMP陷阱。

調試輸出示例<snipped>：

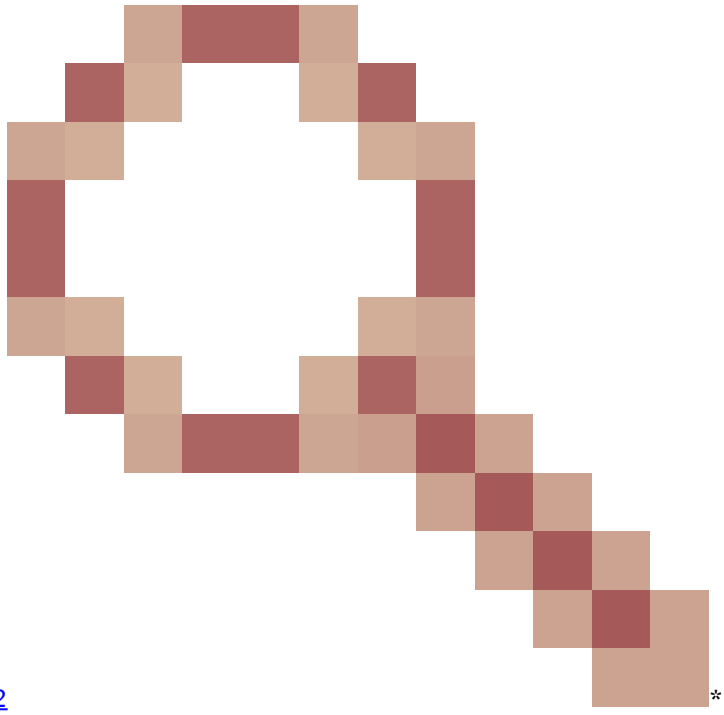
<#root>

*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：

- 使用者帳戶和/或密碼無效。

- 電腦不是網域成員，請在AD端發生問題。
- 憑證服務無法正常運作。
- 伺服器憑證已過期或未使用。
- RADIUS配置不正確。
- 訪問金鑰輸入錯誤-它區分大小寫（SSID也是如此）。
- 更新Microsoft修補程式。
- EAP計時器。
- 使用者端/伺服器上設定的EAP方法不正確。
- 使用者端憑證已過期或未使用。

傳回行動裝置的AAA錯誤逾時(-5)

AAA Server Unreachable，然後是客戶端deauth。

範例：

<#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

返回移動的AAA錯誤內部錯誤(-6)

屬性不匹配。AAA傳送的與WLC不瞭解/相容的不正確/不適當的屬性（錯誤長度）。WLC傳送Deauth消息，後跟內部錯誤消息。示例：思科漏洞ID CSCum83894 AAA Internal Error 和auth失敗，且訪問接受中的屬性未知。

範例：

*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

返回移動的AAA錯誤無伺服器(-7)。
Radius配置不正確和/或使用不支援的配置。

範例：

*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

方案5：客戶端無法與AP關聯

使用的調試：

debug client <mac addr>

要解析的日誌：

向BSSID 00:26：cb：94:44：c0（狀態0） ApVapId 1插槽0上的工作站傳送Assoc響應

- 插槽0 = B/G(2.4)無線電
- 插槽1 = A(5)無線電
- 傳送Assoc響應狀態0 =成功

除狀態0以外的任何狀態均為失敗。

常見關聯響應狀態代碼位於：802.11 Association Status、802.11 Deauth Reason Codes

案例6：因閒置逾時而取消從屬端關聯

使用的調試：

debug client <mac addr>

要解析的日誌

從AP 00:26：cb：94:44：c0，插槽0接收STA 00:1e：8c：0f：a4:57的空閒超時

apfMsDeleteByMscb Scheduling mobile for deletion with deleteReason 4， reasonCode 4

正在排程1秒內刪除行動工作站： (callerId： 30)

apfMsExpireCallback (apf_ms.c：608) Expiring Mobile！

在BSSID 00:26：cb：94:44：c0插槽0（呼叫方apf_ms.c：5094）上將取消身份驗證傳送到流動裝置

狀況

在未收到來自客戶端的流量之後發生。

預設持續時間為300秒。

因應措施

從WLC全局增加空閒超時GUI>>Controller>>General，或從WLC按WLAN增加空閒超時 **GUI>WLAN>ID>>Advanced**.

方案7：由於會話超時客戶端取消關聯

使用的調試：

debug client <mac addr>

要解析的日誌：

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

狀況

在排定的持續時間內發生（預設為1800秒）。

它會再次強制WEBAUTH使用者執行WEBAUTH。

因應措施

從WLC增加或停用每個WLAN的會話超時 **GUI>WLAN>ID>Advanced**。

方案8：由於WLAN更改而取消客戶端關聯

使用的調試：

debug client <mac addr>

要剖析的記錄：

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

狀況

要以任何方式修改WLAN，請停用和重新啟用WLAN。

因應措施

這是預期行為。當進行WLAN更改時，客戶端會取消關聯並重新關聯。

方案9：由於手動從WLC刪除而取消客戶端關聯

使用的調試：

debug client <mac addr>

要剖析的記錄：

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

狀況

從GUI：移除使用者端

在 CLI 上： **config client deauthenticate <mac address>**

方案10：由於身份驗證超時客戶端取消關聯

使用的調試：

debug client <mac addr>

要剖析的記錄：

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

狀況

已達到身份驗證或金鑰交換最大重新傳輸次數。

因應措施

檢查/更新客戶端驅動程式、安全配置、證書等。

方案11：由於AP無線電重置（電源/通道）導致客戶端取消關聯

使用的調試：

debug client <mac addr>

要剖析的記錄：

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

狀況

AP取消關聯客戶端，但WLC不刪除條目。

因應措施

預期行為。

場景12：Symantec客戶端與802.1X「timeoutEvt」有關的問題

問題

運行Symantec軟體的客戶端與消息802.1X的 timeoutEvt. 計時器取消關聯對於站點和消息= M3

EAP/Eapol程式無法完成，無論Intel/Broadcom卡上使用的A/G無線電為何。使用wep、wpa-psk時沒有問題。

狀況

WLC程式碼並不重要。

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

RADIUS伺服器nps 2008。
所有PC上都安裝了Symantec防病毒軟體。

使用Asus、Broadcom、Intel - win7、win-xp。

受影響的作業系統- Windows 7和xp

受影響的無線介面卡- Intel(6205)和Broadcom

受影響的驅動程式/請求方- 15.2.0.19，使用本地請求方。

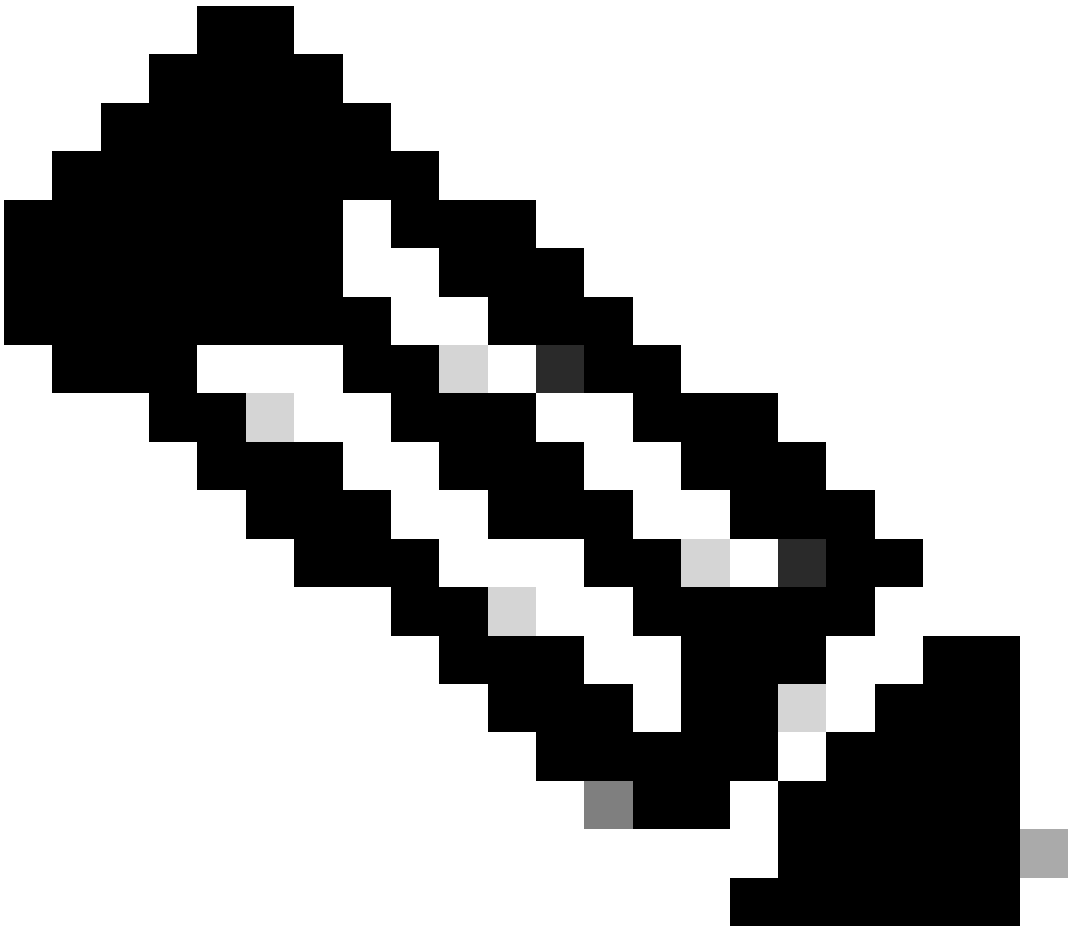
修復/解決方法

在win7和xp上停用Symantec Network Protection and Firewall。它是Win 7和XP作業系統的Symantec問題。

調試輸出：

*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（在早期版本中也看到）中存在如下症狀：

-client從AP獲取M1
-client傳送M2
-client從AP獲取M3
-client在傳送出M4之前插入新的成對金鑰

- 客戶端傳輸使用新金鑰AP加密的M4，並將M4消息作為「解密錯誤」丟棄。

- WLC調試客戶端顯示您M3重新傳輸超時。顯然，這是Microsoft和Symantec之間的問題，並不針對Intel。解決方法是刪除Symantec。

- 這實際上是Symantec在Windows中觸發的Bug。調整EAP計時器無法解決此問題。

- 關於此問題，Cisco TAC將受影響的使用者轉發給Symantec和Microsoft。

場景13：Air Print Service未顯示啟用監聽的mDNS客戶端

打開mDNS監聽時，客戶端無法看到在Apple手持客戶端裝置上提供AirPrint服務的裝置。

狀況

使用7.6.100.0的5508 WLC。
啟用mDNS監聽後，您就可以將提供AirPrint服務的裝置列在WLC的服務部分下。
相應的mDNS配置檔案已正確對映到WLAN和介面。
仍然無法看到客戶端上的AirPrint裝置。

使用的調試：

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_

說明:

客戶端將請求_universal._sub._ipps._tcp.local或_universal._sub._ipp._tcp.local而不是 **_ipp._tcp.local** 或_ipp._tcp.local字串。
因此，新增的AirPrint服務將無法運作。已辨識它，且請求的服務字串將對映到 HP_Photosmart_Printer_1.
相同服務已新增到對應至WLAN的設定檔中，但裝置沒有列出任何服務。

發現，由於增加了域名，並且客戶端在增加了域名的情況下查詢了dns-sd._udp.YVG local，因此WLC無法處理Bonjour資料包，因為dns-sd._udp.YVG.local不存在於資料庫中。

已辨識與同一相關的給定增強型漏洞-思科漏洞ID CSCuj32157。

因應措施

唯一的解決方法是停用DHCP選項15（域名）或從客戶端刪除域名。

方案14：由於停用了快速SSID更改，Apple iOS客戶端「無法加入網路」

狀況

大多數Apple iOS裝置在使用預設 fast SSID change disabled的相同Cisco WLC上從一個WLAN移動到另一個WLAN時遇到問題。

該設定會導致在客戶端嘗試關聯到另一個客戶端後，控制器從存在的WLAN中取消對客戶端的身份驗證。

通常的結果是iOS裝置上的「nable to Join the Network" Umessage」。

顯示客戶端

(jk-2504-116) >**顯示網路摘要**

<snip>

快速SSID變更.....停用

使用的調試：

<#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 char**

*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

因應措施

從WLC啟用快速ssid更改 GUI > Controller>General.

案例15：成功建立使用者端LDAP關聯

安全LDAP有助於保護控制器與使用TLS的LDAP伺服器之間的連線。控制器軟體版本7.6及更新版本支援此功能。

控制器可以向LDAP伺服器傳送兩種型別的查詢：

1. 匿名

在這種型別中，當客戶端需要獲得身份驗證時，控制器向LDAP伺服器傳送身份驗證請求。LDAP伺服器會以查詢結果回應。進行此交換時，包括客戶端使用者名稱/口令的所有資訊都以明文傳送。只要增加了繫結使用者名稱/密碼，LDAP伺服器就會響應來自任何人的查詢。

2. 已驗證

在此型別中，控制器配置了一個使用者名稱和密碼，用於透過LDAP伺服器進行身份驗證。密碼將使用MD5 SASL加密，並在身份驗證過程中傳送到LDAP伺服器。這可以幫助LDAP伺服器正確辨識身份驗證請求的來源。但是，即使控制器的標識受到保護，客戶端詳細資訊仍以明文傳送。

對基於TLS的LDAP的真正需求源於這兩種型別造成的安全漏洞，其中客戶端身份驗證資料和事務的其他部分以明文形式發生。

需求

WLC運行軟體版本7.6及更高版本。

Microsoft伺服器使用LDAP。

使用的調試：

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

方案16：LDAP上的客戶端身份驗證失敗

使用的調試：

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

因應措施

檢查LDAP伺服器是否拒絕原因。

方案17：由於WLC上的LDAP配置錯誤而出現的客戶端關聯問題

使用的調試：

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

因應措施

跨客戶端/WLC和LDAP伺服器驗證憑據。

案例18：無法連線至LDAP伺服器時的使用者端關聯問題

使用的調試：

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

因應措施

檢查WLC和LDAP伺服器的網路連線問題。

方案19：由於缺少粘滯漫遊配置，Apple客戶端漫遊問題

狀況

AIR-CT5508-K9 / 7.4.100.0

Apple裝置斷開與無線網路的連線，該無線網路使用：

- WPA2策略
- WPA2加密AES
- 啟用802.1X驗證

Cisco ISE的身份驗證和授權。

Apple裝置會定期從廣播SSID斷開連線。例如，當同一位置中的另一部電話保持連線時，iPhone會掉線。因此，這種情況是隨機發生的（時間和電話）。

筆記型電腦使用者端沒有問題。它們連線到同一個SSID。

此問題發生在正常操作期間，沒有漫遊和備用模式。

WLAN已刪除所有可能導致問題的可能設定(aironet ext)。

使用的調試：

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.
```

因應措施

對於具有粘滯金鑰快取(SKC)客戶端並具有WLC代碼7.2及更高版本的客戶，您現在可執行的操作是啟用SKC的漫遊支援。預設情況下，WLC僅支援機會金鑰快取(OKC)。為了允許客戶端使用它在每個AP上生成的舊PMKID，您必須透過WLC CLI啟用它。

config wlan security wpa wpa2 cache sticky enable <1>

請記住，由於SKC的性質，這不會改善初始漫遊；但是，它會改善對相同AP的後續漫遊（本手冊中最多8次）。想象一下有8個AP的走廊。第一個逐步解說包括每個AP的完全關聯，延遲大約1-2秒。當您到達終點並往回走時，客戶端會在返回相同關聯時顯示8個唯一PMKID。

如果啟用了SKC支援，則AP無需透過完全身份驗證。這樣可以消除延遲，並且客戶端看起來保持連線。

案例20：使用CCKM驗證快速安全漫遊(FSR)

802.11 WLAN漫遊和CUWN上的快速安全漫遊

使用的調試：

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

如圖所示，執行快速安全漫遊以避免EAP身份驗證幀和更多的4向握手，因為新的加密金鑰仍然派生，但基於CCKM協商方案。這可透過漫遊重新關聯幀以及客戶端和WLC之前快取的資訊完成。

案例21：使用WPA2 PMKID快取驗證快速安全漫遊(FSR)

使用的調試：

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

方案22：使用主動金鑰快取驗證快速安全漫遊

使用的調試：

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

如調試開始時所示，PMKID必須在收到來自客戶端的重新關聯請求之後計算。驗證PMKID並確認快取的PMK與WPA2 4向握手一起使用以導出加密金鑰並完成快速安全漫遊時，需要執行此操作。請勿混淆調試中的CCKM條目；這並非用於執行CCKM，而是PKC/OKC，如前所述。這裡，CCKM只是WLC用於這些輸出的名稱，例如處理值以計算PMKID的函式的名稱。

案例23：驗證使用802.11r的快速安全漫遊(FSR)

使用的調試：

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

.

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。