このチートシートをワイヤレスに関する一般的な問題に使用する

内容

はじめに

このドキュメントでは、一般的なワイヤレスの問題をデバッグ（通常はdebug client <mac address>）で解析したチートシートについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、すべてのAireOSコントローラに基づくものです。

- コントローラ：440x、5508、5520、75xx、85xx、2504、3504、およびvWLC、WISM。
- Converged Access IOS® XEコントローラおよびスイッチでは多くの概念が同じですが、出力とデバッグが根本的に異なるため、このドキュメントの対象外です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

show client の出力における PEM 状態の概要

show clientとデバッグで解析するには、まず電源入力モジュール(PEM)の状態とAPFの状態を理解する必要があります。

- START：新しいクライアント エントリの初期ステータス。
- AUTHCHECK：実施する L2 認証ポリシーが WLAN にあります。
- 8021X_REQD：クライアントは 802.1x 認証を完了する必要があります。
- L2AUTHCOMPLETE：クライアントはL2ポリシーを正常に終了しました。プロセスはL3ポリシー（アドレス学習、Web認証など）に進むことができます。これが同じモビリティグループ内のローミングクライアントである場合、コントローラはモビリティアナウンスを送信して、他のコントローラからL3情報を学習します。
- WEP_REQD：クライアントは WEP 認証を完了する必要があります。
- DHCP_REQD：コントローラは、L3アドレスをクライアントから学習します。これは、ARP要求、DHCP要求、更新、またはモビリティグループ内の他のコントローラから学習した情報によって実行されます。必要な DHCP が WLAN でマークされている場合は、DHCP またはモビリティ情報のみが使用されます。
- WEBAUTH_REQD：クライアントは Web 認証を完了する必要があります（L3 ポリシー）。
- CENTRAL_WEBAUTH_REQD：クライアントはCWAログインを完了する必要があります。WLCはCoAの受信を待機します。
- RUN：クライアントは必要な L2 および L3 ポリシーを正常に完了し、トラフィックをネットワークに送信できるようになりました。

以下のシナリオでは、ワイヤレスのセットアップで起こりがちな設定ミスに対するデバッグの重要な行を示しています。特に、重要なパラメータは太字で示しています。

シナリオ1：クライアントでのWPA/WPA2 PSK認証のパスフレーズの誤設定

<#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

-------------------------
```

debug client の分析:

<#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

M2キーのtimeoutEvtはドライバまたはNICのエラーが原因である可能性がありますが、最も一般的な問題の1つは、PSKパスワ

ードの誤ったクレデンシャル（大文字と小文字を区別しない、特殊文字を含む）を入力したユーザが接続できないことです。

シナリオ2：ワイヤレス電話ハンドセット(792x/9971)がワイヤレス「サービスエリアから離脱」との関連付けに失敗する

参考：7925G受話器がAPへのアソシエーションに失敗する – コールが失敗する：TSPEC QOSポリシーが一致しない

トポロジ

Cisco Unified Wireless IP Phone を使用した WLAN.

問題の詳細

AIR-CT5508-50-K9 //電話機とワイヤレスコントローラのファームウェアをアップグレードしても、電話機の登録が受け付けられません。

デバッグとログ:

<#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 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

WLCのデバッグでは、APがアソシエーションステータスコード201を返すため、7925Gがアソシエーションに失敗したことが示されます。

これは、WLAN設定に起因するハンドセット拒否からのトラフィック仕様(TSPEC)要求によるものです。接続を試行するWLAN 7925Gは、必要に応じてPlatinum(UP 6,7)ではなく、Silver(UP 0,3)のQoSプロファイルで設定されます。これは、WLANによるハンドセットからの音声トラフィックとアクションフレームの交換に対してTSPECの不一致を引き起こし、最終的にはAPから拒否されます。

7925Gハンドセット専用のQoSプロファイルPlatinumを使用して新しいWLANを作成し、確立されたベストプラクティスに従って、および『7925G Deployment Guide』の定義に従って設定します。

Cisco Unified Wireless IP Phone 7925G/7925G-EX/7926G 導入ガイド

正しく設定すると、問題は解決します。

シナリオ3：クライアントはWPA用に設定されるが、APはWPA2専用に設定される

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
```

シナリオ4:AAAのリターンコードまたは応答コードの解析

必要なログを収集するために実行する必要があるデバッグ：

（シスコ コントローラ）>debug mac addr <mac>
（シスコ コントローラ）>debug aaa events enable
（または）
（シスコ コントローラ）>debug client <mac>
（シスコ コントローラ）>debug aaa events enable
（シスコ コントローラ）>debug aaa errors enable

トラップが有効な場合、AAA接続障害によりSNMPトラップが生成されます。

デバッグ出力例（抜粋）:

```
   <#root>
```

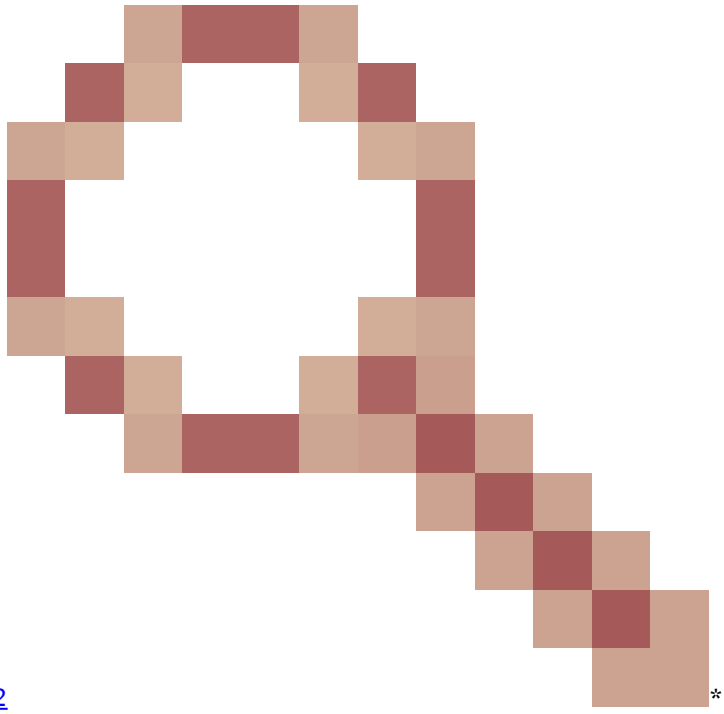
```
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for
```

```
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Returning AAA Error 'Authentication Fail
*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

考えられる理由：

1. ユーザ アカウントまたはパスワード（またはその両方）が無効.
2. コンピュータがドメインのメンバーになっていない（AD 側の問題）
3. 証明書サービスが正しく動作しません。
4. サーバ証明書が期限切れ、または使用されていない.
5. RADIUS の設定が不適切.
6. アクセスキーが誤って入力されました。大文字と小文字が区別されます（SSIDも同様）。
7. Microsoft の修正プログラムの更新が必要
8. EAP タイマー
9. クライアント/サーバに設定された EAP 方法が不適切
10. クライアント証明書が期限切れ、または使用されていない

モバイルの場合はAAAエラータイムアウト(-5)を返す
AAA サーバが到達不能なため、クライアントが認証解除されました。

以下に例を挙げます。

<#root>

```
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 Max retransmission of Access-Request (id 100) to 209.165.20
Wed Oct 26 20:08:50 2011: 00:13:ce:1a:92:41 [Error] Client requested no retries for mobile 00:13:CE:1A:
```

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

モバイルの場合はAAAエラー内部エラー(-6)を返す

属性が一致しません。AAAが送信する属性が不正または不適切で（長さが間違っている）、WLCに理解されず、WLCと互換性がない。WLCがDeauthメッセージを送信し、続いて内部エラーメッセージが送信されます。 Internal Error 例：Cisco Bug ID CSCum83894 AAAおよび認証が失敗し、アクセス承認に不明な属性が含まれる。

以下に例を挙げます。

*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 Invalid RADIUS response received from server 192.0.2.254 with id=9 for mobile 40:f0:2f
*radiusTransportThread: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd [Error] Client requested no retries for mobile 40:F0:2F:11:A9:FD
*radiusTransportThread: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd Returning AAA Error 'Internal Error' (-6) for mobile 40:f0:2f:11:a9:fd
*radiusTransportThread: Feb 21 12:14:36.109:
resultCode.....-6
*Dot1x_NW_MsgTask_5: Feb 21 12:14:36.109: 40:f0:2f:11:a9:fd Processing AAA Error 'Internal Error' (-6) for mobile 40:f0:2f:11:a9:fd

モバイルの場合、AAAエラーNo Server (-7)を返します。
RADIUSが正しく設定されていないか、サポートされていない設定が使用されています。

以下に例を挙げます。

*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: 0x1eebb3ec

シナリオ5：クライアントがAPとの関連付けに失敗する

使用するデバッグ：

debug client <mac addr>

解析するログ:

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

- アソシエーション応答ステータス0 =成功を送信

Status 0以外の値はFailureです。

一般的な関連付け応答ステータスコードは、次のリンクで確認できます。802.11 Association Status, 802.11 Deauth Reason Codes

シナリオ6：アイドルタイムアウトによるクライアントのアソシエーション解除

使用するデバッグ：

debug client <mac addr>

解析するログ

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

モバイルステーション(callerId:30)の削除を1秒でスケジュール

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

クライアントからトラフィックが受信されなかった後に発生します。

デフォルトの期間は300秒です。

回避策

アイドルタイムアウトをWLCからグローバルに増やすか、WLCからWLANごとに増やすGUI>>Controller>>General **GUI>WLAN>ID>>Advanced**.

シナリオ7：セッションタイムアウトによるクライアントのアソシエーション解除

使用するデバッグ：

debug client <mac addr>

解析するログ:

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

スケジュールされた期間に発生します（既定は1800秒）。

WEBAUTHユーザに再びWEBAUTHを強制します。

回避策

WLCからのWLANごとのセッションタイムアウトを増加またはディセーブルにします(**GUI>WLAN>ID>Advanced**)。

シナリオ8:WLANの変更によるクライアントのアソシエーション解除

使用するデバッグ：

debug client <mac addr>

解析するログ:

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

WLANを変更すると、WLANが無効になり、再度有効になります。

回避策

これは正常な動作です。WLANに変更を加えると、クライアントのアソシエーションが解除され、再アソシエーションが実行されます。

シナリオ9:WLCからの手動削除によるクライアントのアソシエーション解除

使用するデバッグ：

debug client <mac addr>

解析するログ:

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

条件

GUIから：Remove Client

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

シナリオ10：認証タイムアウトによるクライアントのアソシエーション解除

使用するデバッグ：

debug client <mac addr>

解析するログ:

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

認証またはキー交換の再送信の最大回数に到達.

回避策

クライアントドライバ、セキュリティ構成、証明書などを確認し、更新します。

シナリオ11:APの無線リセットによるクライアントのアソシエーション解除（電源/チャネル）

使用するデバッグ：

debug client <mac addr>

解析するログ:

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はクライアントの関連付けを解除しますが、WLCはエントリを削除しません。

回避策

予想される動作です。

シナリオ12:802.1X「timeoutEvt」に関するSymantecクライアントの問題

問題

Symantecソフトウェアを実行しているクライアントは、ステーションおよびメッセージ= M3のメッセージ「802.1X timeoutEvt. Timer expired」でアソシエーションを解除します。

Intel/Broadcomカードで使用されているA/G無線に関係なく、EAP/Eapolプロセスが完了しません。wep、wpa-pskを使用する場合は問題ありません。

条件

WLCコードは重要ではありません。

AP – すべてのモデル – すべてローカルモード。
wlan 3 - WPA2+802.1X PEAP + mshcapv2
SSIDがブロードキャストされます。

RADIUS サーバ：NPS 2008.
Symantec アンチウイルス ソフトウェアがすべての PC にインストール済み.

Asus、Broadcom、Intel - win7、win-xpを使用します。

影響を受ける OS：Windows 7 および XP

影響を受けるワイヤレス アダプタ：Intel (6205) および Broadcom

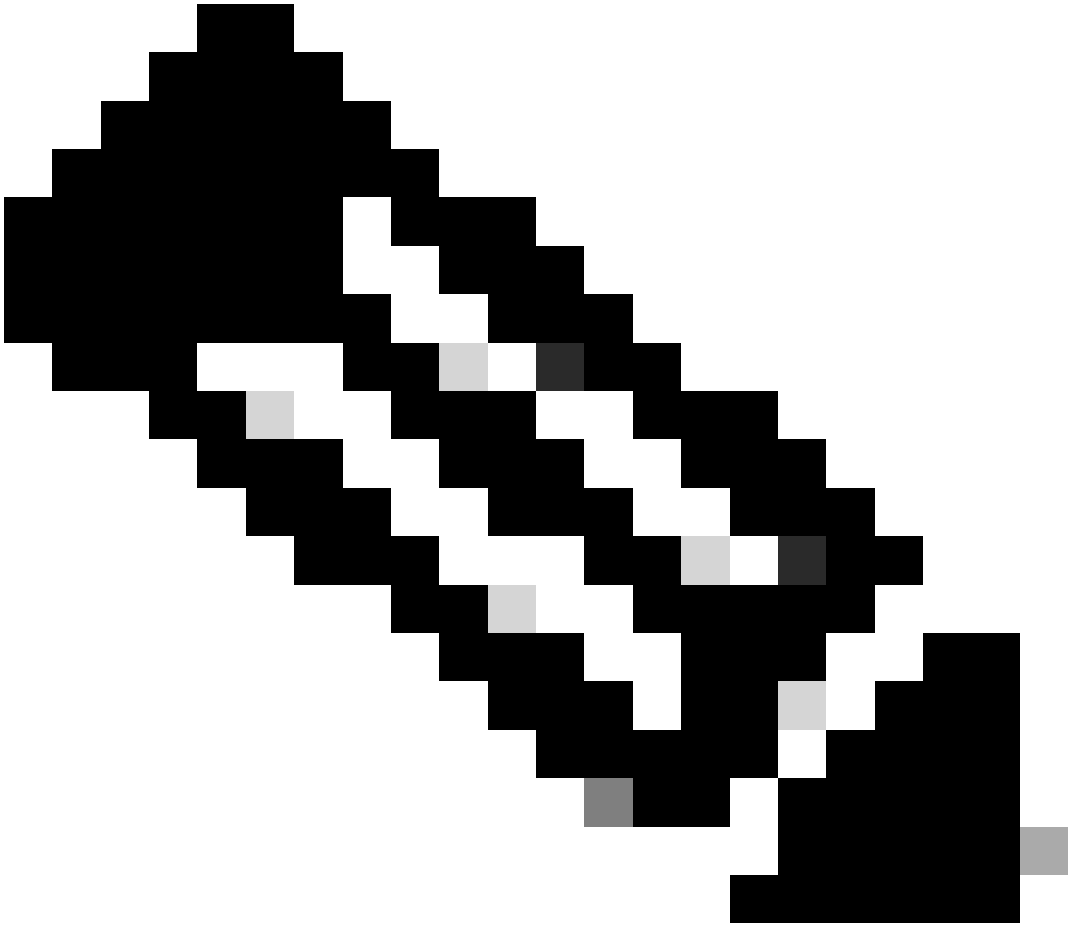
該当するドライバ/サプリカント：15.2.0.19、ネイティブサプリカントを使用

修正/回避策

Windows 7 および XP で、Symantec ソフトウェアによるネットワーク保護およびファイアウォールを無効にします。これは、Win 7およびXP OSに関するSymantecの問題です。

デバッグ出力：

*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:15.2には次のようなシンドロームがあります（以前のバージョンでも見られます）。
- クライアントが AP から M1 を受信
- クライアントが M2 を送信
- クライアントが AP から M3 を受信
- クライアントは M4 を送信する前に、新たなキー ペアを組み込み

– クライアントは新しいキーAPで暗号化されたM4を送信し、M4メッセージを「復号化エラー」としてドロップします。

- WLCデバッグクライアントは、M3再送信でタイムアウトしたことを示します。明らかに、これはMicrosoftとSymantecの間の問題であり、Intel固有の問題ではありません。回避策は、Symantecを削除することです。

-これはおそらく Windows 側のバグであり、Symantec ソフトウェアがトリガとなって発生すると考えられます。EAPタイマーを調整しても、この問題は解決しません。

– この問題に関して、Cisco TACは該当ユーザをSymantecおよびMicrosoftに転送します。

シナリオ13：スヌープがオンになっているmDNSを持つクライアントにAir Print Serviceが表示されない

mDNSスヌープがオンになっているときに、Appleハンドヘルドクライアントデバイスで AirPrintサービスを提供するデバイスがクライアントに表示されない。

条件

7.6.100.0が稼働する5508 WLC。
mDNSスヌープを有効にすると、AirPrintサービスを提供するデバイスがWLCのサービスセクションにリストされます。
それぞれのmDNSプロファイルは、WLANとインターフェイスに正しくマッピングされています。
しかし、クライアント上にこれらの AirPrint デバイスが表示されません。

使用するデバッグ：

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_

説明：

クライアントは、or **_ipp._tcp.local** または_ipp._tcp.local stringの代わりに_universal._sub._ipps._tcp.localまたは _universal._sub._ipp._tcp.localを要求します。
したがって、追加されたAirPrintサービスは機能しません。サービス文字列が特定され、要求されたサービス文字列が HP_Photosmart_Printer_1.
これと同じサービスが、WLAN にマッピングされたプロファイルに追加されていますが、デバイスにはサービスが表示されません。

ドメイン名が追加され、ドメイン名が追加されたdns-sd._udp.YVG localに対するクライアントクエリが原因で、データベースに存在しないdns-sd._udp.YVG.localBonjourパケットをWLCが処理できないことが判明しました。

同じ問題に関して、特定の拡張バグを確認 – Cisco Bug ID CSCuj32157。

回避策

唯一の回避策は、DHCPオプション15（ドメイン名）を無効にするか、クライアントからドメイン名を削除することです。

シナリオ14：無効になっているFast SSID Changeが原因でApple iOSクライアントがネットワークに参加できない

条件

ほとんどのApple iOSデバイスでは、デフォルトの fast SSID change disabledを使用して同じCisco WLC上のあるWLANから別のWLANに移動すると問題が発生します。

この設定により、クライアントが別のクライアントへの関連付けを試行すると、コントローラは既存のWLANからクライアントの認証を解除します。

一般的な結果は、iOSデバイスでの「nable to Join the Network" Umessage」です。

クライアントの表示

(jk-2504-116) >show network summary

<中略>

高速SSID変更.....Disabled

使用するデバッグ：

<#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

回避策

WLCからのfast-ssid changeの有効化 GUI > Controller>General.

シナリオ15：クライアントのLDAPアソシエーションの成功

セキュアLDAPは、コントローラとTLSを使用するLDAPサーバ間の接続を保護するのに役立ちます。この機能は、コントローラソフトウェアバージョン7.6以降でサポートされています。

コントローラから LDAP サーバには、次の 2 種類のクエリを送信できます。

1. 匿名

このタイプでは、クライアントを認証する必要があるときに、コントローラからLDAPサーバに認証要求が送信されます。LDAPサーバはクエリの結果を返します。この交換の時点で、クライアントのユーザ名とパスワードを含むすべての情報はクリアテキストで送信されます。LDAPサーバは、バインドユーザ名/パスワードが追加されている限り、誰からのクエリにも応答します。

2. 認証

このタイプでは、コントローラは、LDAPサーバで自身を認証するために使用するユーザ名とパスワードで設定されます。パスワードはMD5 SASLで暗号化され、認証プロセス時にLDAPサーバに送信されます。これにより、LDAP サーバは認証要求の送信元を正しく識別できます。ただし、コントローラのIDは保護されますが、クライアントの詳細はクリアテキストで送信されます。

LDAP over TLSの本当の二ーズは、クライアント認証データとその他のトランザクションが暗号化されずに実行される、これら2つのタイプによってもたらされるセキュリティの脆弱性によるものです。

要件

WLCはソフトウェアバージョン7.6以降を実行します。

Microsoftサーバは LDAPを使用します。

使用するデバッグ：

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

シナリオ16:LDAPでのクライアント認証の失敗

使用するデバッグ：

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

回避策

LDAP サーバをチェックし、拒否理由を確認します。

シナリオ17:WLCでのLDAPの誤設定によるクライアント関連付けの問題

使用するデバッグ：

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

回避策

クライアント/WLC および LDAP サーバ間でやり取りされるクレデンシャルを検証します。

シナリオ18:LDAPサーバに到達できない場合のクライアントアソシエーションの問題

使用するデバッグ：

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

回避策

WLC および LDAP サーバのネットワーク接続問題を確認します。

シナリオ19：固定(Sticky)ローミングが設定されていないAppleクライアントのローミング問題

条件

AIR-CT5508-K9 / 7.4.100.0

Appleのデバイスは、次のものを使用するワイヤレスネットワークから切断されます。

- WPA2ポリシー
- WPA2暗号化AES
– 認証802.1Xが有効

Cisco ISEによる認証および認可

Appleデバイスは、ブロードキャストSSIDから定期的に切断されます。たとえば、同じ場所にある別の電話機が接続されている間に切断されるiPhoneなどです。したがって、これはランダムに発生します（時間と電話）。

問題のないラップトップクライアント同じSSIDに接続する

この問題は、ローミングもスタンバイモードもない通常の動作中に発生します。

WLANでは、問題を引き起こす可能性のあるすべての設定がすでに削除されています(aironet ext)。

使用するデバッグ：

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.
```

回避策

Sticky Key Caching(SKC)クライアントを使用し、WLCコード7.2以降を使用しているお客様に対して、SKCのローミングサポートを有効にできるようになりました。デフォルトでは、WLCはOpportunistic Key Caching(OKC)のみをサポートします。クライアントが各APで生成した古いPMKIDを使用できるようにするには、WLC CLIでそれを有効にする必要があります。

config wlan security wpa wpa2 cache sticky enable <1>

これはSKCの性質上、初期ローミングを改善するものではないことに注意してください。ただし、同じAPへの後続のローミングは改善されます（書籍では8まで）。8つのAPがある廊下を歩いていると想像してください。最初のウォークスルーは、各APで約1 ~ 2秒間の遅延を伴う完全な関連付けから構成されます。最後に到達して戻ると、クライアントは同じアソシエーションに戻るときに8つの一意のPMKIDを提示します。

SKCサポートが有効になっている場合、APは完全な認証を通過する必要はありません。これにより遅延が解消され、クライアントは接続されたままになります。

シナリオ20:CCKMでの高速セキュアローミング(FSR)の確認

CUWN での 802.11 WLAN ローミングと高速セキュア ローミング

使用するデバッグ：

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

上に示すように、新しい暗号キーが引き続き導出されていますが、CCKMネゴシエーションスキームに基づいているため、EAP認証フレームやさらに多くの4方向ハンドシェイクを回避するために、高速セキュアローミングが実行されます。これは、ローミングの再関連付けフレームと、クライアントおよびWLCによって以前にキャッシュされた情報を使用して完了します。

シナリオ21:WPA2 PMKIDキャッシュを使用した高速セキュアローミング(FSR)の確認

使用するデバッグ：

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

シナリオ22：プロアクティブキーキャッシュを使用した高速セキュアローミング(FSR)の確認

使用するデバッグ：

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

デバッグの最初に示すように、クライアントからの再関連付け要求を受信した後にPMKIDを計算する必要があります。これは、PMKID を検証することで、キャッシュされた PMK が WPA2 4 ウェイ ハンドシェイクに使用され、暗号化キーが生成され、高速セキュア ローミングが完了したことを確認するために必要となります。デバッグのCCKMエントリを混同しないでください。これは、すでに説明したように、CCKMではなくPKC/OKCを実行するために使用されます。ここでは、CCKMは、PMKIDを計算するために値を処理する関数の名前など、これらの出力のためにWLCによって使用される単なる名前です。

シナリオ23:802.11rでの高速セキュアローミング(FSR)の確認

使用するデバッグ：

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

.

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。