# Utilizzare questa scheda per i problemi comuni relativi al wireless

## Sommario

# Introduzione

In questo documento viene descritta una scheda che analizza i debug (in genere, debug client <indirizzo MAC>) per individuare i problemi wireless più comuni.

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Le informazioni discusse in questo documento si basano su tutti i controller AireOS.

- Controller: 440x, 5508, 5520, 75xx, 85xx, 2504, 3504 e vWLC, nonché WISM.
- Sebbene molti concetti siano identici nei controller e negli switch Converged Access IOS® XE, questo documento non li applica in quanto gli output e i debug sono radicalmente diversi.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Brief - Stato PEM su Mostra output client

Per analizzare prima il client show e i debug, è necessario conoscere alcuni stati del Power Entry Module (PEM) e alcuni stati dell'APF.

- START - Stato iniziale della nuova voce client.
- AUTHCHECK: la WLAN dispone di un criterio di autenticazione L2 da applicare.
- 8021X_REQD: il client deve completare l'autenticazione 802.1x.
- L2AUTHCOMPLETE: il client ha completato il criterio L2. Il processo può ora passare ai criteri L3 (apprendimento degli indirizzi, autenticazione Web e così via). Il controller invia l'annuncio di mobilità per apprendere informazioni L3 da altri controller se si tratta di un client in roaming nello stesso gruppo di mobilità.
- WEP_REQD - Il client deve completare l'autenticazione WEP.
- DHCP_REQD: il controller apprende l'indirizzo L3 dal client, operazione eseguita da richiesta ARP, richiesta DHCP o rinnovo o da informazioni apprese da altri controller nel gruppo di mobilità. Se DHCP Required è contrassegnato sulla WLAN, vengono utilizzate solo le informazioni DHCP o sulla mobilità.
- WEBAUTH_REQD: il client deve completare l'autenticazione Web. (criterio L3)
- CENTRAL_WEBAUTH_REQD - Il client deve completare l'accesso a CWA. Il WLC attende di ricevere il CoA.
- RUN - Il client ha completato i criteri L2 e L3 richiesti e può ora trasmettere il traffico alla rete.

Gli scenari forniti mostrano le righe di debug principali per le configurazioni errate comuni nelle configurazioni wireless, evidenziando i parametri principali in grassetto.

# Scenario 1: Passphrase non configurata correttamente per l'autenticazione WPA/WPA2 PSK sul client

<#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 analisi client:

<#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

## Conclusioni

Sebbene timeoutEvt per la chiave M2 possa essere dovuta anche a errori di driver/scheda NIC, uno dei problemi più comuni è rappresentato da un utente che immette credenziali non corrette per la password PSK (maiuscole/minuscole, caratteri speciali e così via) e non è in grado di connettersi.

Scenario 2: ricevitore per telefono wireless (792x/9971) non collegato all'area di servizio uscita wireless

Riferimento: Handset 7925G con associazione non riuscita all'access point - Chiamata non riuscita: criterio QOS TSPEC non corrispondente

**Topologia**

WLAN con Cisco Unified Wireless IP Phone.

**Dettagli problema**

AIR-CT5508-50-K9 // firmware aggiornato per telefoni e controller wireless non accetta registrazioni telefoniche.

Debug e registri:

<#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**

**Conclusioni**

Il comando Debug sul WLC mostra che l'associazione 7925G non riesce in quanto l'access point restituisce un codice di stato dell'associazione 201.

Ciò è dovuto a una richiesta TSPEC (Traffic SPECification) inviata dal rifiuto del ricevitore a causa della configurazione WLAN. Lo switch WLAN 7925G che tenta di connettersi è configurato con un profilo QoS argento (UP 0,3), anziché platino (UP 6,7) come richiesto. Ciò porta a una mancata corrispondenza TSPEC per lo scambio di traffico vocale/frame di azione dal ricevitore tramite la WLAN, e in ultima analisi a un rifiuto da parte dell'access point.

Creare una nuova WLAN con un profilo QoS Platinum specifico per i telefoni 7925G, configurata secondo le best practice definite e come definito nella Guida all'installazione di 7925G:

Guida all'installazione di Cisco Unified 7925G, 7925G-EX e 7926G Wireless IP Phone

Una volta configurata correttamente, il problema è risolto.

Scenario 3: client configurato per WPA ma AP configurato solo per 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**

Scenario 4: Analisi dei codici restituzione o risposta AAA

**Debug necessari da ESEGUIRE per raccogliere i log previsti:**

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

(Cisco Controller) > **abilitazione eventi debug aaa**

(O)

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

(Cisco Controller) > **abilitazione eventi debug aaa**

(Cisco Controller) > **errori debug aaa abilitati**

Un errore di connettività AAA genera una trap SNMP, se sono abilitate le trap.

Output di esempio del comando debug <snipped>:

<#root>

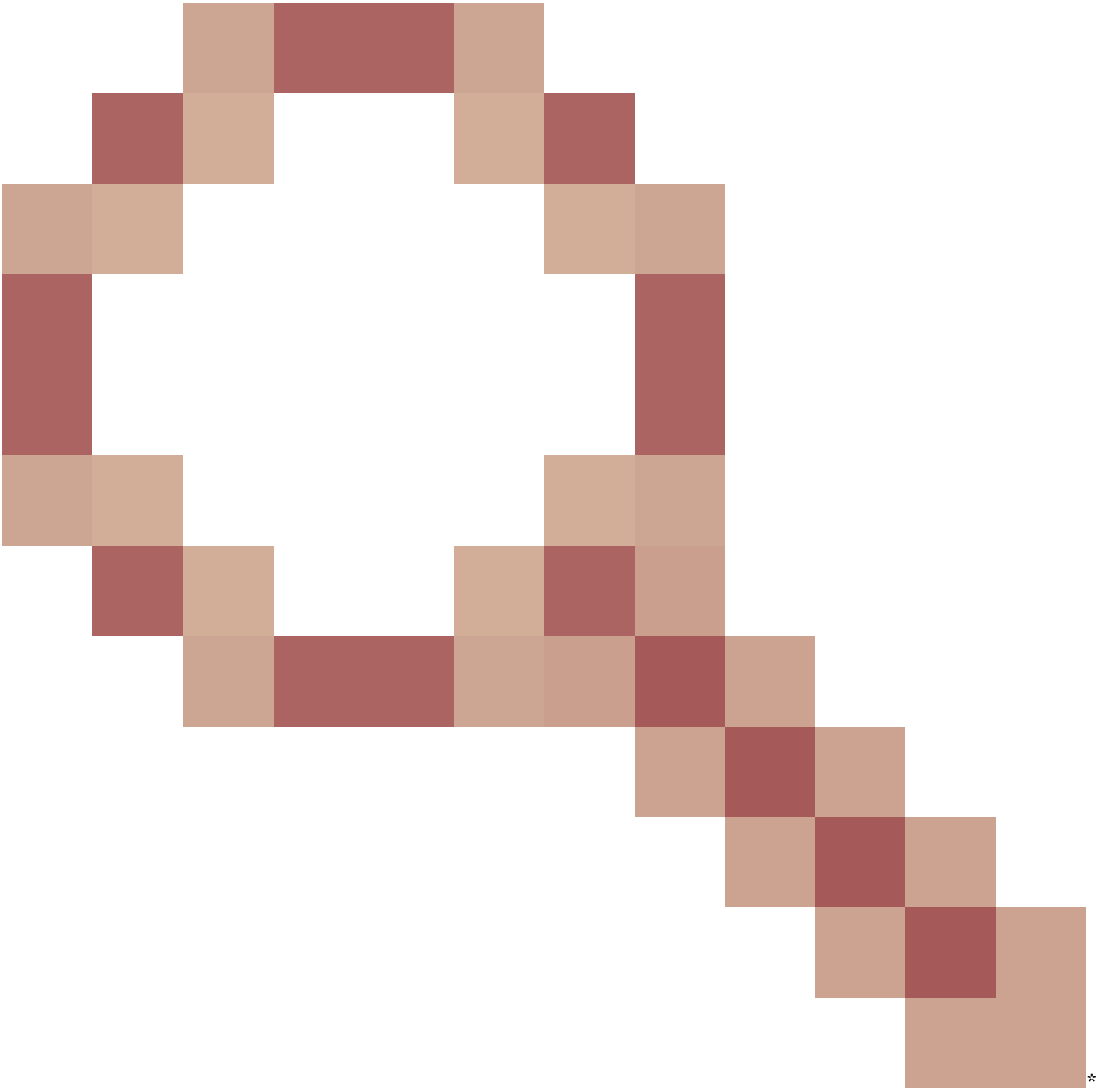
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from server 10.50.0.74 with id=213. Possible secret
*radiusTransportThread: 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

Possibili motivi:

- Account utente e/o password non validi.
- Computer non membro del dominio, problema sul lato Active Directory.

    - I servizi certificati non funzionano correttamente.
- Certificato server scaduto o non in uso.
- RADIUS non configurato correttamente.
- La chiave di accesso non è stata immessa correttamente. Fa distinzione tra maiuscole e minuscole (e anche l'SSID).
- Aggiornare le patch di Microsoft.
- Timer EAP.
- Metodo EAP non corretto configurato sul client/server.
- Il certificato client è scaduto o non è in uso.

Restituisci timeout errore AAA (-5) per dispositivo mobile

Server AAA non raggiungibile, seguito da impostazione predefinita del client.

Esempio:

<#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

Errore interno AAA restituito (-6) per dispositivo mobile

Attributo non corrispondente. AAA invia un attributo errato/inappropriato (lunghezza errata) che non è riconosciuto/compatibile con WLC.

WLC invia un messaggio di disattivazione, seguito da un messaggio di errore interno. Esempio: errore di autenticazione Cisco CSCum83894

AAA Internal Error e autenticazione con attributi sconosciuti in access accept.

Esempio:

*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

Restituisce l'errore AAA sul server (-7) per il dispositivo mobile.

Radius non è configurato correttamente e/o la configurazione in uso non è supportata.

Esempio:

*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

Scenario 5: il client non riesce ad associarsi al punto di accesso

Debug utilizzato:

**debug client <mac addr>**

Registri da analizzare:

Invio di una risposta assoc alla stazione su BSSID 00:26:cb:94:44:c0 (stato 0) ApVapId 1 Slot 0

- Slot 0 = B/G(2.4) Radio
- Slot 1 = A(5) Radio
- Invia stato risposta assoc 0 = Operazione riuscita

Qualsiasi elemento diverso dallo stato 0 è Errore.

I codici di stato di risposta associazione comuni sono disponibili all'indirizzo: 802.11 Association Status, 802.11 Deauth Reason Codes (Codici motivi scadenza)

Scenario 6: dissociazione del client per timeout di inattività

Debug utilizzato:

**debug client <mac addr>**

Log da analizzare

Ricevuto timeout di inattività da AP 00:26:cb:94:44:c0, slot 0 per STA 00:1e:8c:0f:a4:57

apfMsDeleteByMscb Pianificazione dell'eliminazione del dispositivo mobile con deleteReason 4, codice motivo 4

Pianificazione dell'eliminazione della stazione mobile: (ID chiamante: 30) in 1 secondo

apfMsExpireCallback (apf_ms.c:608) Scadenza cellulare.

Inviato Deauthentication to mobile su BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

**Condizioni**

Si verifica dopo la mancata ricezione di traffico dal client.

La durata predefinita è 300 secondi.

**Soluzione alternativa**

Aumento del timeout di inattività a livello globale dal WLC GUI>>Controller>>General o per WLAN dal WLC **GUI>WLAN>ID>>Advanced**.

Scenario 7: dissociazione del client a causa di un timeout della sessione

Debug utilizzato:

**debug client <mac addr>**

Registri da analizzare:

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

**Condizioni**

Si verifica alla durata pianificata (impostazione predefinita 1800 secondi).

Impone nuovamente all'utente WEBAUTH di utilizzare WEBAUTH.

**Soluzione alternativa**

Aumentare o disabilitare il timeout della sessione per WLAN dal **GUI>WLAN>ID>Advanced**WLC.

Scenario 8: dissociazione dei client a causa di modifiche alla WLAN

Debug utilizzato:

**debug client <mac addr>**

Log da analizzare:

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

**Condizioni**

Per modificare una WLAN in qualsiasi modo, disabilitare e riabilitare la WLAN.

**Soluzione alternativa**

Si tratta di un comportamento normale. Quando vengono apportate modifiche alla WLAN, i client disassociano e riassociano.

Scenario 9: dissociazione del client a causa dell'eliminazione manuale dal WLC

Debug utilizzato:

**debug client <mac addr>**

Log da analizzare:

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

**Condizioni**

Dalla GUI: Rimuovi client

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

Scenario 10: dissociazione del client per timeout di autenticazione

Debug utilizzato:

**debug client <mac addr>**

Log da analizzare:

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

**Condizioni**

Raggiunto numero massimo di ritrasmissioni di autenticazione o scambio chiave.

**Soluzione alternativa**

Verifica/aggiorna driver client, configurazione di protezione, certificati e così via.

Scenario 11: dissociazione del client a causa di un reset della radio del punto di accesso (alimentazione/canale)

Debug utilizzato:

**debug client <mac addr>**

Log da analizzare:

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

**Condizioni**

AP disassocia i client, ma WLC non elimina la voce.

**Soluzione alternativa**

Comportamento previsto.

Scenario 12: problemi del client Symantec con "timeoutEvt" 802.1X

**Problema**

I client che eseguono il software Symantec disassociano il messaggio 802.1X timeoutEvt. Timer scaduto per la stazione e per il messaggio = M3

Il processo EAP/Eapol non viene completato, indipendentemente dalla radio A/G utilizzata sulla scheda Intel/Broadcom. Nessun problema quando viene utilizzato wep, wpa-psk.

**Condizioni**

Il codice WLC non ha importanza.

AP - all model - All in modalità locale.
wlan 3 - WPA2+802.1X PEAP + mshcapv2
SSID trasmesso.

Server dei criteri di rete RADIUS 2008.
Il software antivirus Symantec è installato su tutti i PC.

Utilizzare Asus, Broadcom, Intel - win7, win-xp.

Sistema operativo interessato - Windows 7 e xp

Scheda di rete wireless interessata - Intel(6205) e Broadcom

Driver/supplicant interessato - 15.2.0.19, utilizzare Supplicant nativo.

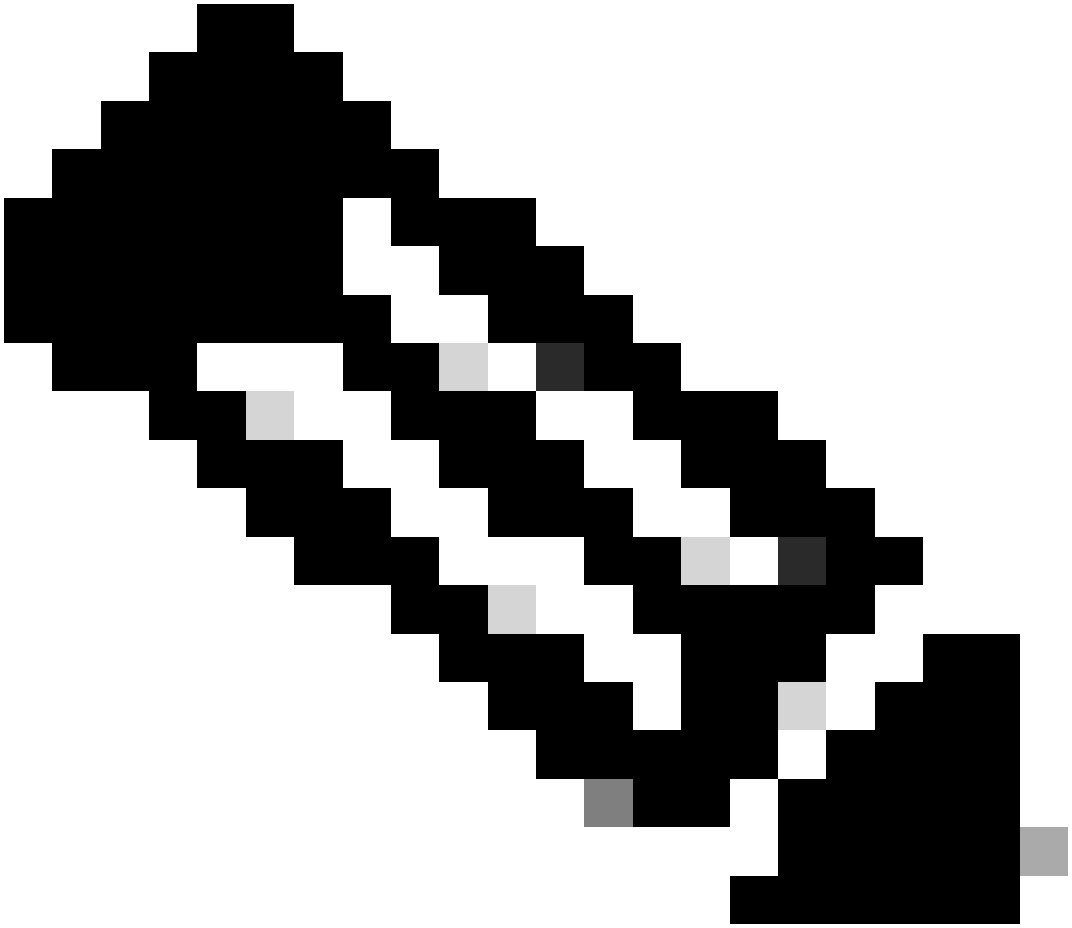
**Correzione/Soluzione**

Disabilitare Symantec Network Protection e Firewall su win7 e xp. Si tratta di un problema Symantec con Windows 7 e XP OS.

Output di debug:

*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

---



---

**Nota**: C'è una sindrome in 15.2 (vista anche nelle versioni precedenti) che va come:
-il client ottiene M1 dal punto di accesso
-il client invia M2
-il client ottiene M3 dal punto di accesso
-client esegue il plumbing della nuova chiave pairwise prima dell'invio di M4

---

- Il client trasmette l'M4 crittografato con il nuovo access point a chiave, scarta il messaggio M4 come un "errore di decrittografia".

- Il client di debug WLC mostra il timeout durante le ritrasmissioni M3. Evidentemente, si tratta di un problema tra Microsoft e Symantec, non specifico di Intel. Per ovviare al problema, rimuovere Symantec.

- Si tratta di un bug che probabilmente è stato generato da Symantec in Windows. La regolazione del timer EAP non risolve il problema.

- Per quanto riguarda questo problema, Cisco TAC inoltra gli utenti interessati a Symantec e Microsoft.

Scenario 13: il servizio di stampa aerea non viene visualizzato per i client con mDNS attivato dallo snoop

Il client non riesce a vedere i dispositivi che forniscono il servizio AirPrint sui dispositivi client palmari Apple quando lo snoop mDNS è attivato.

**Condizioni**

WLC con 7.6.100.0.
Se lo snoop mDNS è abilitato, i dispositivi che forniscono i servizi AirPrint sono elencati nella sezione servizi del WLC.
Il profilo mDNS corrispondente è stato mappato correttamente alla WLAN e all'interfaccia.
Ancora in grado di vedere i dispositivi AirPrint sul client.

Debug utilizzato:

**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_

Spiegazione:

Il client richiederebbe _universal._sub._ipps._tcp.local o _universal._sub._ipp._tcp.local invece di **_ipp._tcp.local** o _ipp._tcp.local string.
Quindi il servizio AirPrint aggiunto non funzionerebbe. È stata identificata e la stringa di servizio richiesta a cui eseguire il mapping HP_Photosmart_Printer_1.

Lo stesso servizio è stato aggiunto nel profilo mappato alla WLAN e non è ancora presente alcun servizio elencato per il dispositivo.

È stato rilevato che a causa del nome di dominio aggiunto e della query del client per il dns-sd._udp.YVG locale con il nome di dominio aggiunto, il WLC non è stato in grado di elaborare il pacchetto Bonjour perché dns-sd._udp.YVG.local non esiste nel database.

Identificato il bug del miglioramento specificato rispetto allo stesso - ID bug Cisco CSCuj32157.

**Soluzione alternativa**

L'unica soluzione è stata disabilitare l'opzione DHCP 15 (nome di dominio) o rimuovere il nome di dominio dal client.

Scenario 14: il client iOS Apple "Unable to join the Network" (%SSID non può essere aggiunto alla rete) a causa di una modifica rapida SSID disabilitata

**Condizioni**

La maggior parte dei dispositivi Apple iOS ha problemi a spostarsi da una WLAN all'altra sullo stesso WLC Cisco con la fast SSID change disabledporta predefinita.

Questa impostazione determina la rimozione dell'autenticazione del client dalla WLAN esistente quando il client tenta di associarsi a un'altra.

Il risultato tipico è un "nable to Join the Network" Umessage" sul dispositivo iOS.

Mostra client

(jk-2504-116) >**mostra riepilogo rete**

<cattura>

Cambio rapido
SSID.....
Disabled

Debug utilizzato:

<#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
```

**Soluzione alternativa**

Abilita modifica fast-ssid da WLC GUI > Controller>General.

Scenario 15: associazione LDAP client riuscita

LDAP sicuro consente di proteggere la connessione tra il controller e il server LDAP che utilizza TLS. Questa funzione è supportata dal software del controller versione 7.6 e successive.

Esistono due tipi di query che possono essere inviate dal controller al server LDAP:

1. Anonimi

In questo tipo, il controller invia una richiesta di autenticazione al server LDAP quando un client deve essere autenticato. Il server LDAP risponde con il risultato della query. Al momento dello scambio, tutte le informazioni che includono il nome utente/password del client vengono inviate in formato non crittografato. Il server LDAP risponde a una query di qualsiasi utente, purché vengano aggiunti il nome utente e la password di binding.

2. Autenticato

In questo tipo, il controller è configurato con un nome utente e una password che utilizza per autenticarsi con il server LDAP. La password viene crittografata con MD5 SASL e inviata al server LDAP al momento del processo di autenticazione. Ciò consente al server LDAP di identificare correttamente l'origine delle richieste di autenticazione. Tuttavia, anche se l'identità del controller è protetta, i dettagli del client vengono inviati in formato testo non crittografato.

L'esigenza reale di LDAP su TLS è dovuta alla vulnerabilità della sicurezza posta da entrambi questi due tipi, dove i dati di autenticazione del client e il resto della transazione avvengono in chiaro.

**Requisiti**

WLC esegue la versione software 7.6 e successive.

Il server Microsoft utilizza LDAP.

Debug utilizzato:

**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

Scenario 16: Autenticazione client non riuscita su LDAP

Debug utilizzato:

**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

**Soluzione alternativa**

Controllare il server LDAP per i motivi di rifiuto.

Scenario 17: problemi di associazione dei client causati da LDAP non configurato correttamente sul WLC

Debug utilizzato:

**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

**Soluzione alternativa**

Verificare le credenziali su client/WLC e server LDAP.

Scenario 18: problemi di associazione client quando il server LDAP non è raggiungibile

Debug utilizzato:

**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

**Soluzione alternativa**

Controllare i problemi di connettività di rete del server WLC e LDAP.

Scenario 19: problemi di roaming dei client Apple a causa di una configurazione di roaming sticky mancante

**Condizioni**

AIR-CT5508-K9/7.4.100.0

I dispositivi Apple si disconnettono da una rete wireless che utilizza:

- WPA2
- WPA2 Encryption AES
- Autenticazione 802.1X abilitata

Autenticazione e autorizzazione di Cisco ISE.

I dispositivi Apple si disconnettono periodicamente dal SSID di trasmissione. Un esempio è un iPhone che cade mentre un altro telefono nella stessa posizione rimane connesso. Pertanto, questo si verifica in modo casuale (ora e telefono).

Client notebook senza problemi. Si connettono allo stesso SSID.

Il problema si verifica durante il funzionamento normale, senza roaming e modalità standby.

La WLAN ha già rimosso tutte le possibili impostazioni che potrebbero causare problemi (aironet ext).

Debug utilizzato:

**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.
```

**Soluzione alternativa**

Per i clienti che dispongono di client SKC (Sticky Key Caching) e di codice WLC 7.2 e versioni successive, è possibile abilitare il supporto roaming per SKC. Per impostazione predefinita, il WLC supporta solo l'OKC (Opportunistic Key Caching). Per consentire al client di utilizzare i

PMKID precedenti generati in ogni access point, è necessario abilitarli dalla CLI del WLC.

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

Tenere presente che questo non migliora i roaming iniziali a causa della natura di SKC; tuttavia, migliora i roaming successivi agli stessi AP (fino a 8 dal libro). Immaginate una passeggiata lungo un corridoio con 8 punti di accesso. La prima procedura dettagliata è costituita da associazioni complete in ogni punto di accesso con un ritardo di circa 1-2 secondi. Quando si raggiunge la fine e si torna indietro, il client presenta 8 PMKID univoci mentre torna alle stesse associazioni.

Se il supporto SKC è abilitato, non è necessario che gli access point passino attraverso un'autenticazione completa. In questo modo si rimuove il ritardo e il client sembra rimanere connesso.

Scenario 20: Verifica della funzionalità Fast-Secure-Roaming (FSR) con CCKM

Roaming WLAN 802.11 e roaming Fast-Secure su CUWN

Debug utilizzato:

**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

Come mostrato, il roaming veloce e sicuro viene eseguito per evitare i frame di autenticazione EAP e ancora più handshake a 4 vie, perché le nuove chiavi di crittografia sono ancora derivate, ma basate sullo schema di negoziazione CCKM. Questa operazione viene completata con i frame di riassociazione mobili e le informazioni precedentemente memorizzate nella cache dal client e dal WLC**.**

Scenario 21: verificare Fast-Secure-Roaming (FSR) con la cache PMKID WPA2

Debug utilizzato:

**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

Scenario 22: Verifica del roaming Fast-Secure con la cache delle chiavi proattive

Debug utilizzato:

**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
```

Come mostrato all'inizio dei debug, il PMKID deve essere calcolato dopo la richiesta di riassociazione del client. Questa operazione è necessaria per convalidare PMKID e confermare che la chiave PMK memorizzata nella cache viene utilizzata con l'handshake a 4 vie WPA2 per derivare le chiavi di crittografia e completare il roaming a protezione rapida. Non confondere le voci CCKM sui debug; questo non viene usato per eseguire CCKM, ma PKC/OKC, come spiegato in precedenza. In questo caso, CCKM è semplicemente un nome utilizzato dal WLC per tali output, ad esempio il nome di una funzione che gestisce i valori per calcolare il PMKID.

Scenario 23: Verifica di Fast-Secure-Roaming (FSR) con 802.11r

Debug utilizzato:

**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

.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).