Gebruik dit cheatblad voor veelvoorkomende draadloze problemen

Inhoud

Inleiding

Dit document beschrijft een cheat sheet dat door debugs (gewoonlijk, debug client <mac address>) wordt geparseerd voor gebruikelijke draadloze problemen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op alle AireOS-controllers.

- Controllers - 440x, 5508, 5520, 75xx, 85xx, 2504, 3504 en vWLC, evenals WISM's.
- Hoewel veel concepten identiek zijn in geconvergeerde access IOS® XE-controllers en -switches, is dit document niet op hen van toepassing omdat de uitgangen en debugs radicaal verschillend zijn.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Korte PEM-status op weergave clientuitvoer

Om te ontleden door toon client en debugs eerst vereist u om bepaalde Power Entry Module (PEM) staten en APF staten te begrijpen.

- START: initiële status voor nieuwe client.
- AUTHCHECK-WLAN heeft een L2-verificatiebeleid dat moet worden uitgevoerd.
- 8021X_REQD—De client moet 802.1x-verificatie voltooien.
- L2AUTHCOMPLETE - De client heeft het L2 beleid met succes afgerond. Het proces kan nu verder gaan naar L3 beleid (adresleren, Web auth, enzovoort). Controller stuurt de mobiliteitsaankondiging om L3-informatie van andere controllers te leren als dit een roamende client in dezelfde mobiliteitsgroep is.
- WEP_REQD—De client moet de WEP-verificatie voltooien.
- DHCP_REQD-Controller leert het L3-adres van de client, wat wordt gedaan door ARP-verzoek, DHCP-verzoek of hernieuwd, of door informatie die van andere controllers in de mobiliteitsgroep is geleerd. Als DHCP Required is gemarkeerd op het WLAN, wordt alleen DHCP- of mobiliteitsinformatie gebruikt.
- WEBAUTH_REQD—De client moet de webverificatie voltooien. (L3-beleid)
- CENTRAL_WEBAUTH_REQD—De client moet CWA-aanmelding voltooien. WLC wacht om de CoA te ontvangen.
- RUN-client heeft met succes het vereiste L2- en L3-beleid voltooid en kan nu verkeer naar het netwerk verzenden.

De gegeven scenario's tonen zeer belangrijke debug lijnen voor gemeenschappelijke misconfigurations in draadloze opstellingen, die zeer belangrijke parameters in vette letters benadrukt.

Scenario 1: verkeerd ingesteld wachtwoord voor WPA/WPA2 PSK-verificatie op 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 clientanalyse:

<#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

Conclusie

Hoewel timeoutEvt de M2-toets ook te wijten kan zijn aan fouten van de driver/NIC, is een van de meest voorkomende problemen een

gebruiker die onjuiste referenties voor PSK-wachtwoord invoert (gemiste hoofdlettergevoeligheid/speciale tekens, enzovoort) en geen verbinding kan maken.

Scenario 2: Draadloze telefoon handset (792x/9971) kan niet worden geassocieerd met draadloze "verlaat serviceruimte"

Referentie: 7925G-handsets die niet kunnen worden gekoppeld aan AP - Gesprek mislukt: TSPEC QOS-beleid komt niet overeen

Topologie

WLAN met Cisco Unified draadloze IP-telefoons.

Probleemgegevens

AIR-CT5508-50-K9 / / opgewaardeerde firmware voor telefoons en draadloze controller accepteert geen telefoonregistraties.

Debugs en logs:

<#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

Conclusie

Debug op de WLC laat zien dat de 7925G associatie mislukt als de AP een associatiestatuscode van 2010 retourneert.

Dit komt door een Traffic SPECification (TSPEC)-verzoek van de weigering van de handset als gevolg van de WLAN-configuratie. De WLAN 7925G die probeert verbinding te maken, wordt geconfigureerd met een QoS-profiel van Silver (UP 0,3) in plaats van Platinum (UP 6,7) zoals vereist. Dit leidt tot een TSPEC wanverhouding voor stemverkeer/de uitwisseling van het actiekader van de zaktelefoon door WLAN, en uiteindelijk een verwerping van AP.

Maak een nieuw WLAN met een QoS-profiel van Platinum specifiek voor de 7925G-handsets en geconfigureerd volgens de vastgelegde best practices, en zoals gedefinieerd in de 7925G implementatiegids:

Implementatiegids voor Cisco Unified draadloze IP-telefoon 7925G, 7925G-EX en 7926G

Zodra correct geconfigureerd is, wordt het probleem opgelost.

Scenario 3: client geconfigureerd voor WPA maar AP alleen geconfigureerd voor 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: AAA-terugkeer- of -responscodes parseren

Vereiste debugs om te LOPEN om de verwachte logboeken te verzamelen:

(Cisco-controller) > **debug mac-adres <mac>**

(Cisco Controller) > **Debug aaa-gebeurtenissen inschakelen**

(OF)

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

(Cisco Controller) > **Debug aaa-gebeurtenissen inschakelen**

(Cisco Controller) > **debug aaa-fouten inschakelen**

AAA-connectiviteitsfout genereert een SNMP-trap als traps zijn ingeschakeld.

Voorbeeld debug uitvoer <snipped>:

<#root>

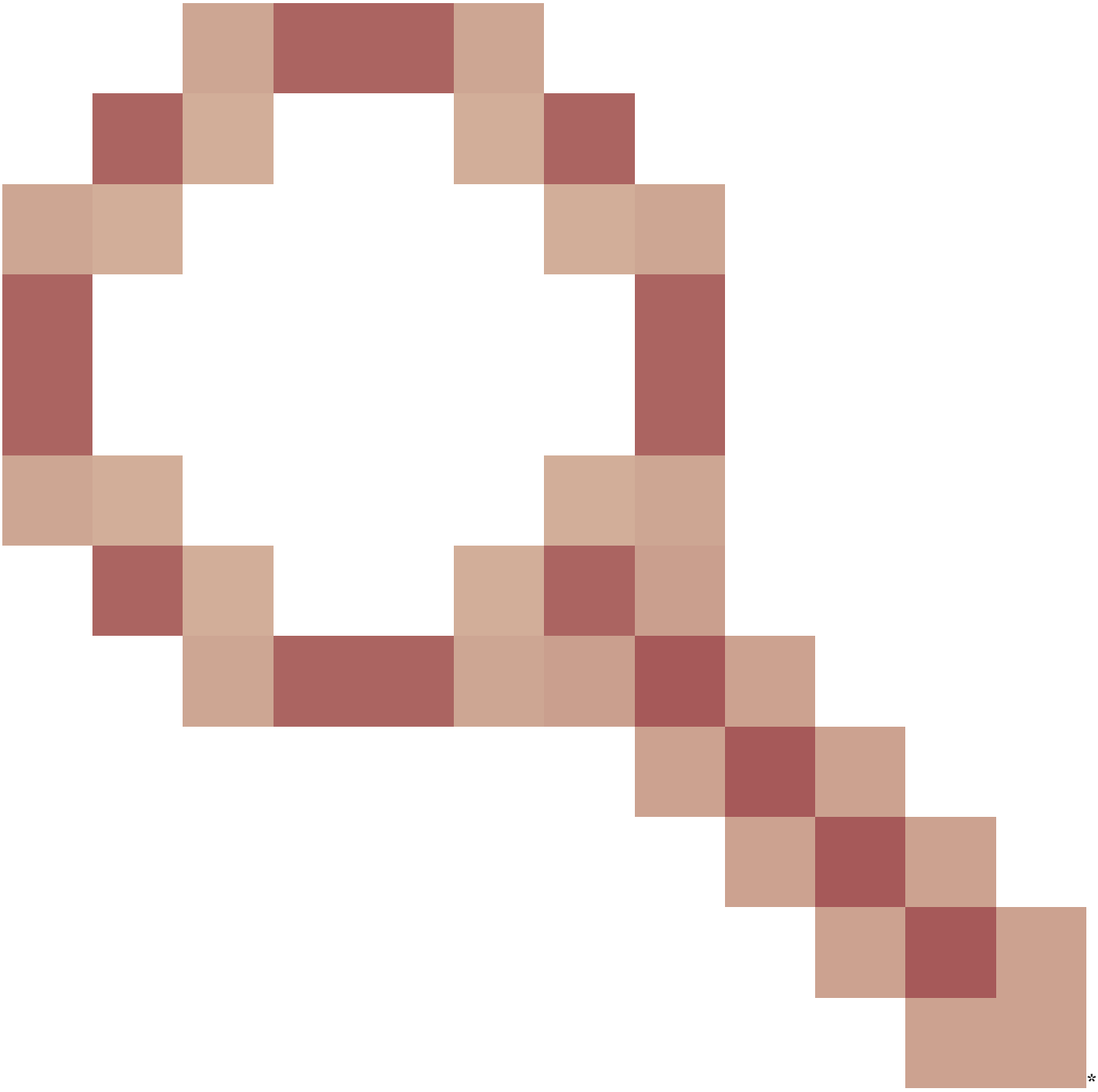
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from server 10.50.0.74 with id=213. Possible secret
*radiusTransportThread: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

Mogelijke redenen:

- Ongeldig gebruikersaccount en/of wachtwoord.
- Computer is geen lid van een domein, probleem op AD-zijde.

    - Certificaatservices werken niet naar behoren.
- Servercertificaat verlopen of niet in gebruik.
- RADIUS is niet correct geconfigureerd.
- Toegangstoets niet correct ingevoerd - het is hoofdlettergevoelig (en de SSID dus).
- Update Microsoft patches.
- EAP-timers.
- Onjuiste EAP-methode geconfigureerd op client/server.
- Clientcertificaat is verlopen of niet in gebruik.

Time-out AAA-fout (-5) retourneren voor mobiel

AAA-server onbereikbaar, gevolgd door clientdood.

Voorbeeld:

<#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

Interne fout AAA-fout (-6) retourneren voor mobiel

Onjuist kenmerk. AAA stuurt onjuiste/ongepaste attributen (verkeerde lengte) die niet worden begrepen/compatibel zijn met WLC. WLC verstuurt Deauth bericht, gevolgd door interne foutmelding. Voorbeeld: Cisco bug-id CSCum83894 AAA Internal Error en auth fail met onbekende eigenschappen in access acceptatie.

Voorbeeld:

*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

Geeft AAA fout geen server (-7) terug voor mobiel.

Straal is niet goed geconfigureerd en/of niet-ondersteunde configuratie in gebruik.

Voorbeeld:

*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: AuthorizationRespons

Scenario 5: client kan niet worden gekoppeld aan AP

Debug gebruikt:

debug client <mac addr>

Log voor parseren:

Verzenden van ASSOC-respons op station op BSSID 00:26:cb:94:44:c0 (status 0) APvapID 1 sleuf 0

- Sleuf 0 = B/G(2.4)-radio
- Sleuf 1 = A(5)-radio
- Verzendt ASSOC Response Status 0 = Success

Om het even wat buiten Status 0 is Mislukking.

U vindt de volgende statuscodes van de Common Association: 802.11 Association Status, 802.11 Deauth Reason Codes

Scenario 6: Clientdisassociatie als gevolg van time-out bij inactiviteitstimer

Debug gebruikt:

debug client <mac addr>

Te ontleden logbestanden

Ontvangen inactiviteitstimer van AP 00:26:cb:94:44:c0, sleuf 0 voor STA 0:1e:8c:0f:a4:57

apfMsDeleteByMscb Scheduling mobiel voor wissen met deleteReden 4, RedenCode 4

Scheduling wissen van Mobile Station: (callerId: 30) in 1 seconden

apfMSexpireCallback (apf_ms.c:608) Verloopt mobiel!

Verzonden Deauthenticate naar mobiel op BSSID 00:26:cb:94:44:c0 slot 0(beller apf_ms.c:5094)

Voorwaarden

Komt voor nadat geen verkeer van Cliënt wordt ontvangen.

De standaardduur is 300 seconden.

Tijdelijke oplossing

Time-out bij inactiviteitstimer vergroten, ofwel wereldwijd van WLC GUI>>Controller>>General, of per WLAN van WLC **GUI>WLAN>ID>>Advanced**.

Scenario 7: Clientdisassociatie als gevolg van time-out voor sessie

Debug gebruikt:

debug client <mac addr>

Log voor parseren:

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

Voorwaarden

Komt voor op geplande duur (standaard 1800 seconden).

Het dwingt de WEBAUTH gebruiker weer naar WEBAUTH.

Tijdelijke oplossing

Sessietime-out per WLAN verhogen of uitschakelen vanaf WLC **GUI>WLAN>ID>Advanced**.

Scenario 8: Clientdisassociatie als gevolg van WLAN-wijzigingen

Debug gebruikt:

debug client <mac addr>

Log voor parseren:

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

Voorwaarden

Als u een WLAN op een bepaalde manier wilt wijzigen, schakelt u WLAN uit en opnieuw in.

Tijdelijke oplossing

Dit is verwacht gedrag. Wanneer er WLAN-wijzigingen zijn aangebracht, scheiden de clients en koppelen ze opnieuw aan elkaar.

Scenario 9: Clientdisassociatie als gevolg van handmatige verwijdering van WLC

Debug gebruikt:

debug client <mac addr>

Log voor parseren:

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

Voorwaarden

Van GUI: client verwijderen

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

Scenario 10: Clientdisassociatie als gevolg van tijdelijke verificatie

Debug gebruikt:

debug client <mac addr>

Log voor parseren:

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

Voorwaarden

Verificatie of Key Exchange max-hertransmissies bereikt.

Tijdelijke oplossing

Controleer/update het clientstuurprogramma, beveiligingsconfiguratie, certificaten, enzovoort.

Scenario 11: Clientdisassociatie als gevolg van reset van AP-radio (voeding/kanaal)

Debug gebruikt:

debug client <mac addr>

Log voor parseren:

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

Voorwaarden

AP scheidt clients, maar WLC verwijdert geen entry.

Tijdelijke oplossing

Verwacht gedrag.

Scenario 12: Symantec-clientproblemen met 802.1x "time-outEvent"

Probleem

Clients die Symantec-software uitvoeren, afscheiden van bericht 802.1X timeoutEvt. Timer verlopen voor station en voor bericht = M3

Het EAP/Eapol-proces wordt niet voltooid, ongeacht de A/G-radio die op de intel/Broadcom-kaart wordt gebruikt. Geen probleem bij gebruik van wep, wpa-psk.

Voorwaarden

De WLC-code doet er niet toe.

APs - al model - allen op lokale wijze.
WLAN 3 - WPA2+802.1X PEAP + mshcapv2
SSID wordt uitgezonden.

RADIUS-server NPS 2008.
Symantec antivirussoftware is op alle pc’s geïnstalleerd.

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

Betrokken besturingssysteem - Windows 7 en XP

Betrokken draadloze adapter - Intel(6205) en Broadcom

Betrokken bestuurder/supplicant - 15.2.0.19, gebruik de native supplicant.

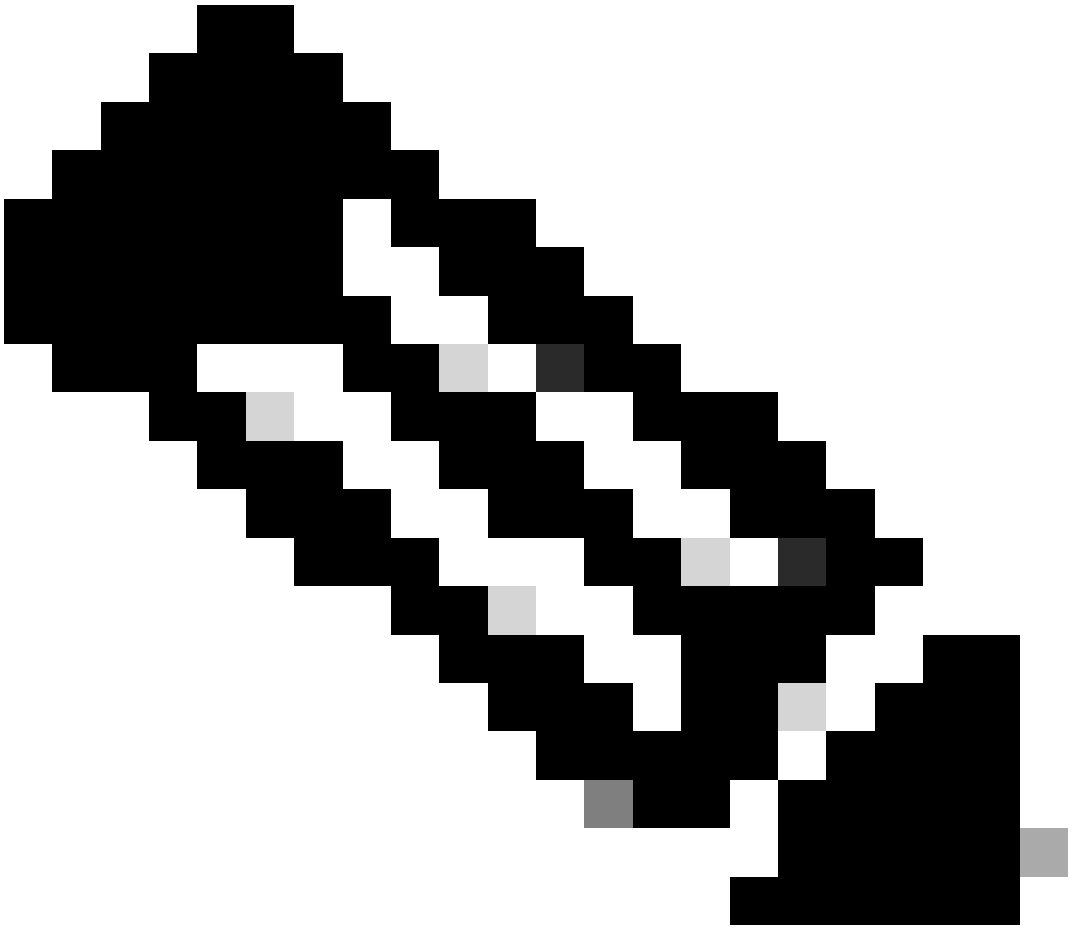
Repareren/tijdelijke oplossing

Schakel Symantec Network Protection and Firewall uit op Win7 en XP. Het is een Symantec probleem met Win 7 en XP OS.

Debug uitvoer:

*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

---



Opmerking: Er is een syndroom in 15.2 (ook in eerdere versies) dat als volgt gaat:
-client krijgt M1 van AP
-client verzendt M2

-client krijgt M3 van AP
-client plumbs de nieuwe paarsgewijze toets voordat het M4 verstuurt

---

- De client verzendt de M4 versleuteld met de nieuwe sleutel AP, laat het M4 bericht vallen als een "decrypt fout".

- WLC debug client toont dat u tijd uit op M3 heruitzendingen. Dit is duidelijk een probleem tussen Microsoft en Symantec, niet tussen Intel-specifieke producten. De oplossing is om Symantec te verwijderen.

- Dit is echt een bug die waarschijnlijk in Windows, veroorzaakt door Symantec. Tweak van de EAP-timer lost dit probleem niet op.

- Wat dit probleem betreft, stuurt Cisco TAC de betrokken gebruikers door naar Symantec en Microsoft.

Scenario 13: Air Print Service verschijnt niet voor clients met mDNS dat Snoop ingeschakeld is

De client is niet in staat om apparaten te zien die AirPrint-service bieden op Apple handheld-clientapparaten wanneer mDNS-snoop is ingeschakeld.

Voorwaarden

5508 WLC met 7.6.100.0.
Als mDNS-snoop is ingeschakeld, hebt u de apparaten die AirPrint-services leveren die worden vermeld onder de sectie Services op de WLC.
Het betreffende mDNS-profiel is correct toegewezen aan het WLAN en de interface.
De AirPrint-apparaten kunnen nog steeds niet worden weergegeven op de client.

Debug gebruikt:

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_

Uitleg:

De client zou vragen om _universal._sub._ipps._tcp.local of _universal._sub._ipp._tcp.local in plaats van **_ipp._tcp.local** of _ipp._tcp.local string.
De toegevoegde AirPrint-service werkt dus niet. Het is geïdentificeerd en de gevraagde dienst wordt in kaart gebracht aan HP_Photosmart_Printer_1.
Dezelfde service is toegevoegd in het profiel dat is toegewezen aan het WLAN en er is nog steeds geen service vermeld voor het apparaat.

Er werd vastgesteld dat vanwege de domeinnaam toegevoegd en de client query voor dns-sd._udp.YVG lokaal met de domeinnaam toegevoegd,

de WLC niet in staat was om het Bonjour pakket te verwerken, aangezien dns-sd._udp.YVG.local niet bestaat in de database.

Identificeerde de gegeven enhancement bug met betrekking tot het zelfde - Cisco bug-id CSCuj32157.

Tijdelijke oplossing

Het enige werk rondom was DHCP optie 15 (Domeinnaam) onbruikbaar te maken of de Domeinnaam te verwijderen uit de cliënt.

Scenario 14: Apple iOS-client "kan niet toetreden tot het netwerk" vanwege snelle SSID-wijziging uitgeschakeld

Voorwaarden

De meeste Apple iOS-apparaten hebben problemen om van het ene WLAN naar het andere op dezelfde Cisco WLC te gaan met de standaardwaarde fast SSID change disabled.

De instelling zorgt ervoor dat de controller de client van het WLAN deauthenticeert wanneer de client probeert te koppelen aan een andere client.

Het typische resultaat is een "nable to Join the Network" Umessage" op het iOS-apparaat.

client weergeven

(jk-2504-116) >**netwerksamenvatting weergeven**

<knip>

Snelle SID-..... Uitgeschakeld

Debug gebruikt:

<#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
```

Tijdelijke oplossing

Schakel snelle verandering van WLC in GUI > Controller>General.

Scenario 15: succesvolle client-LDAP-vereniging

Secure LDAP helpt de verbinding tussen de controller en de LDAP-server die TLS gebruikt, te beveiligen. Deze optie wordt ondersteund met controller-softwareversie 7.6 en hoger.

Er zijn twee soorten vragen die door de controller naar de LDAP-server kunnen worden verstuurd:

1. Anoniem

In dit type stuurt de controller een verificatieaanvraag naar de LDAP-server wanneer een client moet worden geverifieerd. De LDAP-server reageert met het resultaat van de query. Op het moment van deze uitwisseling wordt alle informatie die de gebruikersnaam/het wachtwoord van de client bevat, in duidelijke tekst verzonden. De LDAP-server reageert op een vraag van iemand, zolang de bind-gebruikersnaam/wachtwoord wordt toegevoegd.

2. Gewaarmerkt

In dit type wordt de controller geconfigureerd met een gebruikersnaam en wachtwoord die worden gebruikt om zichzelf te verifiëren met de LDAP-server. Het wachtwoord wordt versleuteld met MD5 SASL en wordt naar de LDAP-server verzonden tijdens het verificatieproces. Hierdoor kan de LDAP-server de bron van de verificatieverzoeken correct identificeren. Hoewel de identiteit van de controller is beveiligd, worden de klantgegevens in duidelijke tekst verzonden.

De echte behoefte aan LDAP over TLS kwam door de veiligheidskwetsbaarheid die door beide types wordt gevormd waar de gegevens van de cliëntauthentificatie en de rest van de transactie in duidelijk gebeurt.

Vereisten

WLC voert softwareversie 7.6 en hoger uit.

Microsoft-server maakt gebruik van LDAP.

Debug gebruikt:

debug aaa ldap activeren

*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: Clientverificatie op LDAP mislukt

Debug gebruikt:

debug aaa ldap activeren

*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

Tijdelijke oplossing

Controleer LDAP-server om afwijzingsredenen.

Scenario 17: Problemen met clientassociatie door LDAP verkeerd geconfigureerd op WLC

Debug gebruikt:

debug aaa ldap activeren

*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

Tijdelijke oplossing

Controleer de referenties op de client/WLC- en LDAP-server.

Scenario 18: Problemen met clientassociatie wanneer LDAP-server onbereikbaar is

Debug gebruikt:

debug aaa ldap activeren

*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

Tijdelijke oplossing

Controleer problemen met de netwerkconnectiviteit van WLC en LDAP-servers.

Scenario 19: Problemen met Apple-clientroaming als gevolg van ontbrekende tijdelijke roamingconfiguratie

Voorwaarden

AIR-CT5508-K9 / 7.4.100.0

Apple-apparaten verbreken de verbinding met een draadloos netwerk dat gebruikmaakt van:

- WPA2-beleid
- WAP2-encryptie AES
- Verificatie 802.1X ingeschakeld

Verificatie en autorisatie door Cisco ISE.

Apple-apparaten maken periodiek de verbinding met de broadcast-SSID los. Een voorbeeld is een iPhone die valt terwijl een andere telefoon in dezelfde locatie verbonden blijft. Daarom gebeurt dit willekeurig (tijd en telefoon).

Notebookclients zonder problemen. Ze maken verbinding met dezelfde SSID.

Dit probleem treedt op tijdens normaal gebruik, zonder roaming en zonder stand-by modus.

WLAN heeft al alle mogelijke instellingen verwijderd die problemen (Aironet-tekst) kunnen veroorzaken.

Debug gebruikt:

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.
```

Tijdelijke oplossing

Wat u nu kunt doen voor klanten die Sticky Key Caching (SKC)-clients hebben en ook WLC-code 7.2 en hoger hebben, is roam ondersteuning voor SKC mogelijk maken. Standaard ondersteunt de WLC alleen Opportunistische Key Caching (OKC). Om de client in staat te stellen om de oude PMKID's te gebruiken die bij elke AP zijn gegenereerd, moet u deze via de WLC CLI inschakelen.

config WLAN security wpa wpa2 cache sticky inschakelen <1>

Houd er rekening mee dat dit geen verbetering van initiële zwerven vanwege de aard van SKC; echter, het verbetert volgende zwermen naar dezelfde AP's (tot 8 in het boek). Stel je een wandeling voor over een hal met 8 toegangspunten. De eerste walkthrough bestaat uit volledige associaties bij elke AP met een vertraging van ongeveer 1-2. Wanneer u het einde bereikt en terugloopt, presenteert de klant 8 unieke PMKID's als hij teruggaat naar dezelfde associaties.

APs hoeven niet door een volledige authentificatie te gaan als de steun van SKC wordt toegelaten. Dit verwijdert de vertraging en de client lijkt verbonden te blijven.

Scenario 20: Controleer Fast-Secure-Roaming (FSR) met CCKM

802.11 WLAN-roaming en Fast-Secure-roaming op CUWN

Debug gebruikt:

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

Zoals getoond, wordt snel-veilig roaming uitgevoerd om de EAP-verificatiekaders en nog meer 4-way handshakes te vermijden, omdat de

nieuwe coderingssleutels nog steeds worden afgeleid, maar gebaseerd op het CCKM-onderhandelingsschema. Dit wordt voltooid met de zwervende reassociatieframes en de informatie die eerder door de client en de WLC wordt gecachet**.**

Scenario 21: Controleer Fast-Secure-Roaming (FSR) met WPA2 PMKID Cache

Debug gebruikt:

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 2: Controleer Fast-Secure Roaming met Proactive Key Cache

Debug gebruikt:

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
```

Zoals getoond aan het begin van de debugs, moet de PMKID worden berekend nadat de Reassociation-aanvraag van de client is ontvangen. Dit is nodig om de PMKID te valideren en te bevestigen dat de gecachede PMK wordt gebruikt met de WPA2 4-Way handshake om de encryptiesleutels af te leiden en het snel-beveiligde zwerven te voltooien. Verwar de CCKM-vermeldingen niet met de debugs; dit wordt niet gebruikt om CCKM uit te voeren, maar PKC/OKC, zoals eerder uitgelegd. Hier is CCKM simpelweg een naam die door de WLC wordt gebruikt voor die uitgangen, zoals de naam van een functie die de waarden verwerkt om de PMKID te berekenen.

Scenario 23: Controleer Fast-Secure-Roaming (FSR) met 802.11r

Debug gebruikt:

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

.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.