Utilisez cette fiche de discussion pour les problèmes sans fil courants

Table des matières

Introduction

Ce document décrit une fiche de travail qui analyse les débogages (généralement, debug client <adresse MAC>) pour les problèmes sans fil courants.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations de ce document sont basées sur tous les contrôleurs AireOS.

- Contrôleurs : 440x, 5508, 5520, 75xx, 85xx, 2504, 3504 et vWLC, ainsi que WISM.
- Bien que de nombreux concepts soient identiques dans les contrôleurs et commutateurs IOS® XE d'accès convergé, ce document ne s'applique pas à eux, car les sorties et les débogages sont radicalement différents.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Brève description de l'état PEM sur la sortie Show Client

Pour analyser show client et debugs, vous devez d'abord comprendre certains états PEM (Power Entry Module) et APF.

- START : état initial de la nouvelle entrée client.
- AUTHCHECK : le WLAN dispose d'une stratégie d'authentification L2 à appliquer.
- 8021X_REQD : le client doit effectuer l'authentification 802.1x.
- L2AUTHCOMPLETE : le client a terminé avec succès la stratégie L2. Le processus peut maintenant passer aux politiques de couche 3 (apprentissage d'adresses, authentification Web, etc.). Le contrôleur envoie l'annonce de mobilité pour apprendre les informations de couche 3 d'autres contrôleurs s'il s'agit d'un client itinérant dans le même groupe de mobilité.
- WEP_REQD : le client doit effectuer l'authentification WEP.
- DHCP_REQD : le contrôleur apprend l'adresse L3 du client, ce qui est fait soit par requête ARP, requête DHCP ou renouvellement, soit par des informations apprises d'autres contrôleurs dans le groupe de mobilité. Si DHCP Required est marqué sur le WLAN, seules les informations DHCP ou de mobilité sont utilisées.
- WEBAUTH_REQD : le client doit effectuer l'authentification Web. (politique de couche 3)
- CENTRAL_WEBAUTH_REQD : le client doit se connecter à CWA. WLC attend de recevoir le CoA.
- EXÉCUTION : le client a réussi à appliquer les stratégies L2 et L3 requises et peut désormais transmettre le trafic au réseau.

Les scénarios donnés montrent les lignes de débogage clés pour les erreurs de configuration courantes dans les configurations sans fil, ce qui met en évidence les paramètres clés en gras.

Scénario 1 : phrase de passe mal configurée pour l'authentification WPA/WPA2 PSK sur le 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
-------------------------
```

Analyse du client de débogage :

<#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

Conclusion

Bien que timeoutEvt pour la clé M2 puisse également être due à des erreurs de pilote/carte réseau, l'un des problèmes les plus courants est un utilisateur qui entre des informations d'identification incorrectes pour le mot de passe PSK (caractères spéciaux/sensibles à la casse manqués, etc.) et qui ne parvient pas à se connecter.

Scénario 2 : échec de l'association du combiné téléphonique sans fil (792x/9971) avec la zone de service « Leaves » sans fil

Référence : 7925G Handsets Failing Association to AP - Call Failed : TSPEC QOS Policy does not match

Topologie

WLAN avec téléphones IP sans fil Cisco Unified.

Détails du problème

AIR-CT5508-50-K9 // le micrologiciel mis à niveau pour les téléphones et le contrôleur sans fil n'accepte pas les enregistrements téléphoniques.

Débogages et journaux :

<#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

Conclusion

Le débogage sur le WLC montre que l'association du 7925G échoue car le point d'accès renvoie un code d'état d'association de 201.

Cela est dû à une demande de spécification du trafic (TSPEC) provenant du refus du combiné en raison de la configuration WLAN. Le WLAN 7925G qui tente de se connecter est configuré avec un profil QoS Silver (UP 0,3), plutôt que Platinum (UP 6,7), selon les besoins. Cela entraîne une non-concordance TSPEC pour le trafic vocal/l'échange de trames d'action à partir du combiné par le WLAN, et finalement un rejet de la part du point d'accès.

Créez un nouveau WLAN avec un profil QoS Platinum spécifique pour les combinés 7925G et configuré conformément aux meilleures pratiques établies, et tel que défini dans le Guide de déploiement du 7925G :

Guide de déploiement des téléphones IP sans fil Cisco Unified 7925G, 7925G-EX et 7926G

Une fois configuré correctement, le problème est résolu.

Scénario 3 : client configuré pour WPA mais point d'accès configuré uniquement pour 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**

Scénario 4 : analyse des codes de retour ou de réponse AAA

Débogages requis pour EXÉCUTER pour collecter les journaux attendus :

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

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

(OU)

(Contrôleur Cisco) > **client de débogage <mac>**

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

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

Une panne de connectivité AAA génère une interruption SNMP, si les interruptions sont activées.

Exemple de sortie de débogage <snipped> :

<#root>

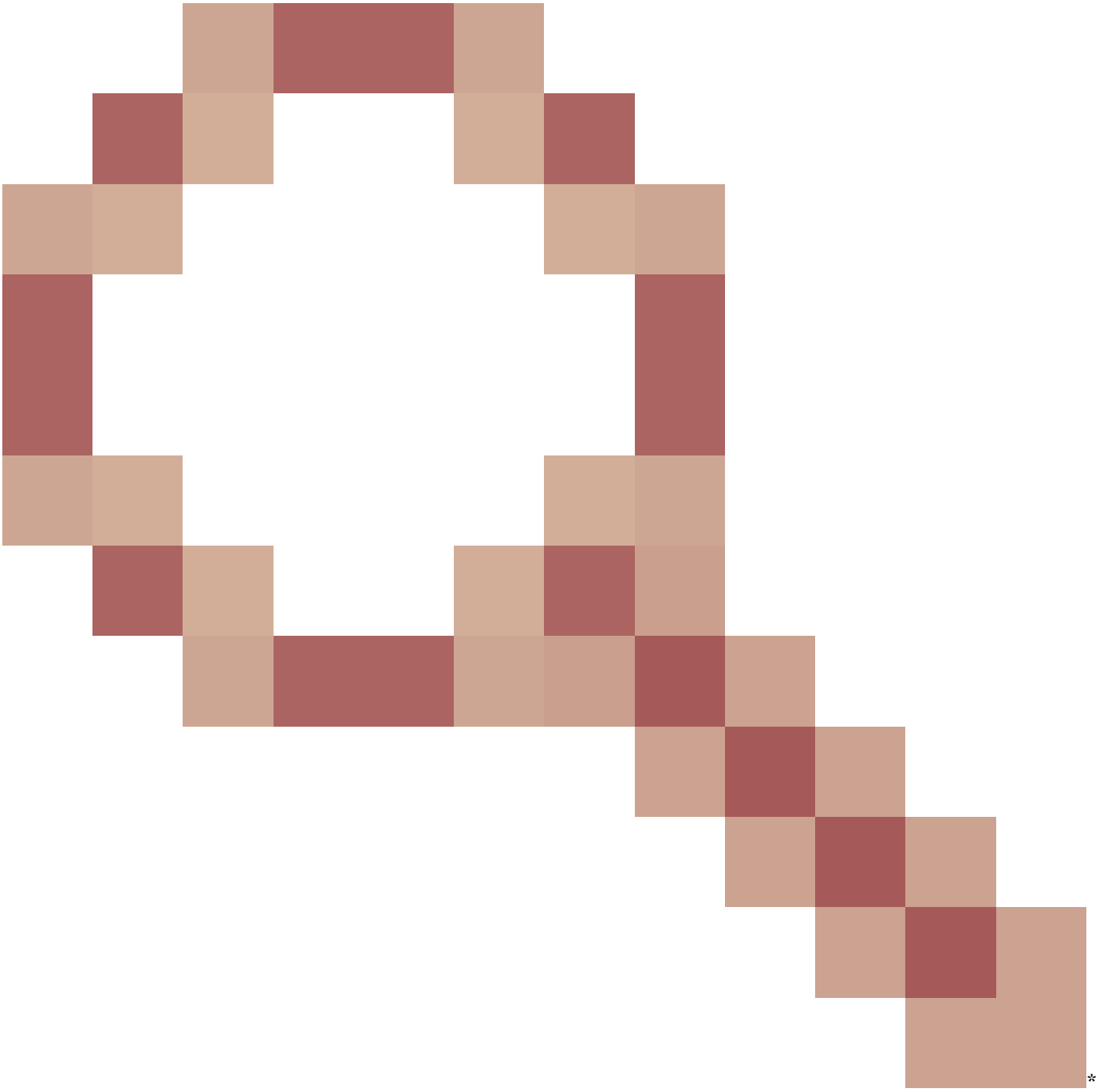
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from server 10.50.0.74 with id=213. Possible secret
*radiusTransportThread: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

Raisons possibles :

- Compte utilisateur et/ou mot de passe non valides.
- Ordinateur non membre du domaine, problème côté service d'annuaire.

    - Les services de certificats ne fonctionnent pas correctement.
- Le certificat du serveur a expiré ou n'est pas utilisé.
- RADIUS mal configuré.
- La clé d'accès saisie est incorrecte : elle est sensible à la casse (et le SSID l'est également).
- Mettre à jour les correctifs Microsoft.
- Minuteurs EAP.
- Méthode EAP incorrecte configurée sur le client/serveur.
- Le certificat client a expiré ou n'est pas utilisé.

Délai d'attente d'erreur AAA de retour (-5) pour Mobile

Serveur AAA inaccessible, suivi de l'authentification du client.

Exemple :

<#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

Erreur AAA de retour Erreur interne (-6) pour Mobile

Non-concordance des attributs. AAA envoie un attribut incorrect/inapproprié (longueur incorrecte) qui n'est pas compris/compatible avec le WLC. Le WLC envoie un message d'erreur Deauth, suivi d'un message d'erreur interne. Exemple : le bogue Cisco ayant l'ID CSCum83894 AAA Internal Error et l'authentification échouent avec des attributs inconnus dans access accept.

Exemple :

*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

Renvoie l'erreur AAA No Server (-7) pour mobile.

Radius n'est pas correctement configuré et/ou une configuration non prise en charge est utilisée.

Exemple :

*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

Scénario 5 : le client ne s'associe pas au point d'accès

Débogage utilisé :

debug client <adresse mac>

Journaux à analyser :

Envoi de la réponse Assoc à la station sur BSSID 00:26:cb:94:44:c0 (état 0) ApVapId 1 Slot 0

- Logement 0 = radio B/G(2.4)
- Logement 1 = Radio A(5)
- Envoie l'état de réponse Assoc 0 = Réussite

Tout autre état que l'état 0 est Échec.

Les codes d'état de réponse d'association courants sont disponibles à l'adresse suivante : 802.11 Association Status, 802.11 Deauth Reason Codes

Scénario 6 : dissociation du client en raison du délai d'inactivité

Débogage utilisé :

debug client <adresse mac>

Journaux à analyser

Délai d'inactivité reçu du point d'accès 00:26:cb:94:44:c0, logement 0 pour STA 00:1e:8c:0f:a4:57

apfMsDeleteByMscb Planification de la suppression avec deleteReason 4, reasonCode 4

Planification de la suppression de la station mobile : (callerId : 30) en 1 secondes

apfMsExpireCallback (apf_ms.c:608) Expiration de Mobile !

Déconnexion envoyée au mobile sur BSSID 00:26:cb:94:44:c0, emplacement 0(appelant apf_ms.c:5094)

Conditions

Se produit après l'absence de trafic reçu du client.

La durée par défaut est de 300 secondes.

Solution de contournement

Augmenter le délai d'inactivité soit globalement depuis WLC GUI>>Controller>>General, soit par WLAN depuis WLC **GUI>WLAN>ID>>Advanced**.

Scénario 7 : dissociation du client en raison du dépassement du délai de session

Débogage utilisé :

debug client <adresse mac>

Journaux à analyser :

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

Conditions

Se produit à la durée planifiée (1 800 secondes par défaut).

Elle force l'utilisateur WEBAUTH à utiliser à nouveau WEBAUTH.

Solution de contournement

Augmenter ou désactiver le délai d'expiration de session par WLAN à partir du WLC **GUI>WLAN>ID>Advanced**.

Scénario 8 : dissociation du client en raison de modifications du WLAN

Débogage utilisé :

debug client <adresse mac>

Journal à analyser :

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

Conditions

Pour modifier un WLAN de quelque manière que ce soit, désactivez et réactivez le WLAN.

Solution de contournement

C’est un comportement attendu. Lorsque des modifications sont apportées au WLAN, les clients se dissocient et se réassocient.

Scénario 9 : dissociation du client en raison d'une suppression manuelle du WLC

Débogage utilisé :

debug client <adresse mac>

Journal à analyser :

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

Conditions

À partir de l'interface utilisateur : Supprimer le client

À partir de CLI : **config client deauthenticate <mac address>**

Scénario 10 : dissociation du client en raison du délai d'authentification

Débogage utilisé :

debug client <adresse mac>

Journal à analyser :

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

Conditions

Nombre maximal de retransmissions d'authentification ou d'échange de clés atteint.

Solution de contournement

Vérifier/mettre à jour le pilote client, la configuration de la sécurité, les certificats, etc.

Scénario 11 : dissociation du client en raison de la réinitialisation radio du point d'accès (alimentation/canal)

Débogage utilisé :

debug client <adresse mac>

Journal à analyser :

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

Conditions

AP dissocie les clients, mais WLC ne supprime pas l'entrée.

Solution de contournement

Comportement attendu.

Scénario 12 : Problèmes de client Symantec avec 802.1X « timeoutEvt »

Problème

Les clients qui exécutent le logiciel Symantec se dissocient du message 802.1X timeoutEvt. Timer expiré pour la station et pour message = M3

Le processus EAP/Eapol n'est pas terminé, quelle que soit la radio A/G utilisée sur la carte Intel/Broadcom. Pas de problème quand il est utilisé wep, wpa-psk.

Conditions

Le code WLC ne compte pas.

Points d'accès - tous les modèles - Tous en mode local.
wlan 3 - WPA2+802.1X PEAP + mshcapv2
Le SSID est diffusé.

Serveur RADIUS nps 2008.
Le logiciel antivirus Symantec est installé sur tous les ordinateurs.

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

Système d'exploitation concerné - Windows 7 et XP

Carte sans fil affectée - Intel(6205) et Broadcom

Pilote/demandeur affecté - 15.2.0.19, utilisez le demandeur natif.

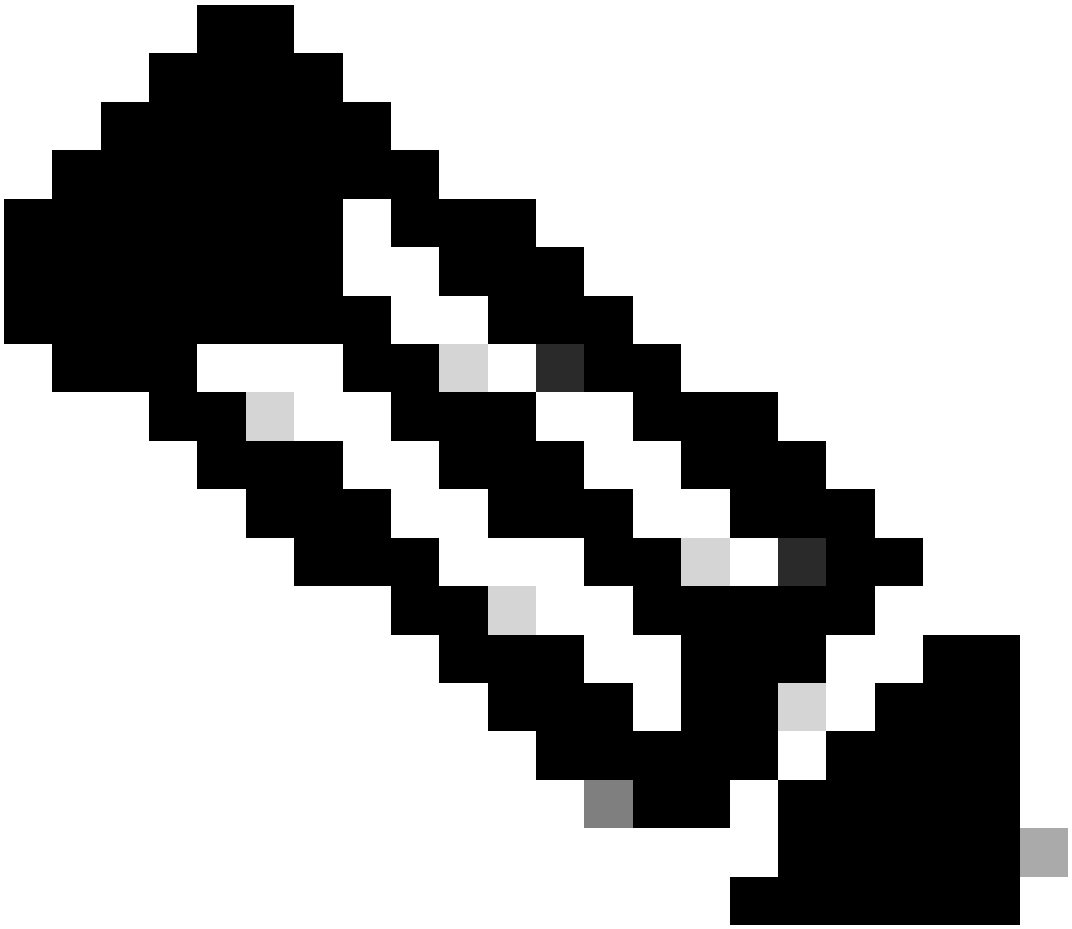
Correction/Solution

Désactivez Symantec Network Protection et Firewall sur win7 et xp. Il s'agit d'un problème Symantec avec les systèmes d'exploitation Windows 7 et XP.

Sortie de débogage :

*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

---



Remarque : il y a un syndrome dans 15.2 (également vu dans les versions antérieures) qui va comme :
-client obtient M1 du point d'accès

-client envoie M2
-client obtient M3 du point d'accès
-client ajuste la nouvelle clé par paire avant d'envoyer M4

- Le client transmet le M4 chiffré avec la nouvelle clé AP, abandonne le message M4 comme une "erreur de déchiffrement".

- Le client de débogage WLC indique que vous avez dépassé le délai d'attente des retransmissions M3. Il s'agit manifestement d'un problème entre Microsoft et Symantec, et non d'un problème propre à Intel. La solution de contournement consiste à supprimer Symantec.

- C'est vraiment un bogue qui est probablement dans Windows, déclenché par Symantec. Le réglage du minuteur EAP ne résout pas ce problème.

- En ce qui concerne ce problème, le centre d'assistance technique Cisco transmet les utilisateurs concernés à Symantec et Microsoft.

Scénario 13 : le service d'impression à chaud n'apparaît pas pour les clients avec mDNS que Snoop est activé

Le client ne peut pas voir les périphériques qui fournissent le service AirPrint sur les périphériques clients portables Apple lorsque la surveillance mDNS est activée.

Conditions

5508 WLC avec 7.6.100.0.
Lorsque la surveillance mDNS est activée, vous disposez des périphériques qui fournissent des services AirPrint répertoriés dans la section Services du WLC.
Le profil mDNS respectif a été correctement mappé au WLAN et à l'interface.
Impossible de voir les périphériques AirPrint sur le client.

Débogage utilisé :

debug client <adresse mac>

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_

Explication:

Le client demande _universal._sub._ipps._tcp.local ou _universal._sub._ipp._tcp.local au lieu de **_ipp._tcp.local** ou _ipp._tcp.local chaîne.
Ainsi, le service AirPrint ajouté ne fonctionnerait pas. Elle a été identifiée et la chaîne de service demandée à mapper HP_Photosmart_Printer_1.
Le même service a été ajouté dans le profil mappé au WLAN et aucun service n'est toujours répertorié pour le périphérique.

Il a été constaté qu'en raison du nom de domaine ajouté et de la requête du client pour le dns-sd._udp.YVG local avec le nom de domaine ajouté,

le WLC n'a pas pu traiter le paquet Bonjour car il n'existe pas dans la base de données. dns-sd._udp.YVG.local.

Identifié le bogue d'amélioration donné par rapport au même - ID de bogue Cisco CSCuj32157.

Solution de contournement

La seule solution a été de désactiver l'option DHCP 15 (nom de domaine) ou de supprimer le nom de domaine du client.

Scénario 14 : Client Apple iOS « Impossible de se connecter au réseau » en raison d'une désactivation du changement rapide de SSID

Conditions

La plupart des appareils Apple iOS ont des problèmes pour passer d'un WLAN à un autre sur le même WLC Cisco avec le fast SSID change disableddéfaut.

Le paramètre entraîne la désauthentification du client du WLAN qui existe une fois que le client tente de s'associer à un autre.

Le résultat typique est un « nable to Join the Network" Umessage » sur le périphérique iOS.

Afficher le client

(jk-2504-116) >**show network summary**

<snip>

Changement de SSID rapide ..... Désactivé

Débogage utilisé :

<#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
```

Solution de contournement

Activer la modification fast-ssid depuis WLC GUI > Controller>General.

Scénario 15 : Association LDAP de client réussie

Secure LDAP permet de sécuriser la connexion entre le contrôleur et le serveur LDAP qui utilise TLS. Cette fonctionnalité est prise en charge par le logiciel du contrôleur version 7.6 et ultérieure.

Il existe deux types de requêtes qui peuvent être envoyées par le contrôleur au serveur LDAP :

1. Anonyme

Dans ce type, le contrôleur envoie une demande d'authentification au serveur LDAP lorsqu'un client doit être authentifié. Le serveur LDAP répond avec le résultat de la requête. Au moment de cet échange, toutes les informations incluant le nom d'utilisateur/mot de passe du client sont envoyées en texte clair. Le serveur LDAP répond à une requête de n'importe qui, tant que le nom d'utilisateur/mot de passe de liaison est ajouté.

2. Authentifié

Dans ce type, le contrôleur est configuré avec un nom d'utilisateur et un mot de passe qu'il utilise pour s'authentifier auprès du serveur LDAP. Le mot de passe est chiffré avec MD5 SASL et est envoyé au serveur LDAP au moment du processus d'authentification. Cela permet au serveur LDAP d'identifier correctement la source des demandes d'authentification. Cependant, même si l'identité du contrôleur est protégée, les détails du client sont envoyés en texte clair.

Le besoin réel de LDAP sur TLS est venu de la vulnérabilité de sécurité posée par ces deux types où les données d'authentification du client et le reste de la transaction se produisent en clair.

Exigences

WLC exécute la version 7.6 du logiciel et les versions ultérieures.

Le serveur Microsoft utilise LDAP.

Débogage utilisé :

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
```

Scénario 16 : échec de l'authentification client sur LDAP

Débogage utilisé :

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

Solution de contournement

Recherchez les motifs de rejet sur le serveur LDAP.

Scénario 17 : Problèmes d'association de clients en raison d'une configuration LDAP incorrecte sur le WLC

Débogage utilisé :

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

Solution de contournement

Vérifiez les informations d'identification sur le client/WLC et le serveur LDAP.

Scénario 18 : problèmes d'association de clients lorsque le serveur LDAP est inaccessible

Débogage utilisé :

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

Solution de contournement

Vérifiez les problèmes de connectivité réseau des serveurs WLC et LDAP.

Scénario 19 : Problèmes d'itinérance client Apple dus à une configuration d'itinérance rémanente manquante

Conditions

AIR-CT5508-K9 / 7.4.100.0

Les périphériques Apple se déconnectent d'un réseau sans fil qui utilise :

- Stratégie WPA2
- Cryptage WPA2 AES
- Authentification 802.1X activée

Authentification et autorisation par Cisco ISE.

Les périphériques Apple se déconnectent périodiquement du SSID de diffusion. Par exemple, un iPhone tombe alors qu'un autre téléphone situé au même endroit reste connecté. Par conséquent, cela se produit de manière aléatoire (heure et téléphone).

Clients d'ordinateurs portables sans problème. Ils se connectent au même SSID.

Ce problème se produit en fonctionnement normal, sans itinérance et sans mode veille.

Le réseau local sans fil a déjà supprimé tous les paramètres possibles susceptibles de provoquer des problèmes (aironet ext).

Débogage utilisé :

debug client <adresse mac>

<#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.
```

Solution de contournement

Ce que vous pouvez faire maintenant pour les clients qui ont des clients Sticky Key Caching (SKC) et ont également le code WLC 7.2 et plus, est d'activer la prise en charge de l'itinérance pour SKC. Par défaut, le WLC prend uniquement en charge la mise en cache de clé opportuniste (OKC). Afin de permettre au client d'utiliser ses anciens PMKID qu'il a générés à chaque AP, vous devez l'activer par l'interface de ligne de commande du WLC.

config wlan security wpa wpa2 cache sticky enable <1>

Gardez à l'esprit que cela n'améliore pas les itinéraires initiaux en raison de la nature de SKC ; cependant, cela améliore les itinéraires suivants vers les mêmes AP (jusqu'à 8 par le livre). Imaginez une promenade dans un couloir avec 8 points d'accès. La première procédure pas à pas consiste en des associations complètes au niveau de chaque point d'accès avec un décalage d'environ 1 à 2 secondes. Lorsque vous atteignez la fin et revenez, le client présente 8 PMKID uniques lorsqu'il revient aux mêmes associations.

Les points d'accès n'ont pas besoin de passer par une authentification complète si la prise en charge SKC est activée. Cela supprime le décalage et le client semble rester connecté.

Scénario 20 : vérification de l'itinérance Fast-Secure (FSR) avec CCKM

Itinérance WLAN 802.11 et itinérance Fast-Secure sur CUWN

Débogage utilisé :

debug client <adresse mac>

<#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

Comme illustré, l'itinérance sécurisée rapide est effectuée pour éviter les trames d'authentification EAP et encore plus de connexions en quatre étapes, car les nouvelles clés de cryptage sont toujours dérivées, mais basées sur le schéma de négociation CCKM. Ceci est complété avec les

trames de réassociation d'itinérance et les informations précédemment mises en cache par le client et le WLC**.**

Scénario 21 : vérification de l'itinérance rapide et sécurisée (FSR) avec le cache PMKID WPA2

Débogage utilisé :

debug client <adresse mac>

<#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

Scénario 22 : Vérifier l'itinérance rapide et sécurisée avec le cache de clés proactif

Débogage utilisé :

debug client <adresse mac>

<#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

Comme indiqué au début des débogages, le PMKID doit être calculé après la réception de la demande de réassociation du client. Ceci est nécessaire afin de valider le PMKID et de confirmer que le PMK mis en cache est utilisé avec la connexion en 4 étapes WPA2 pour dériver les clés de cryptage et terminer l'itinérance sécurisée rapide. Ne confondez pas les entrées CCKM sur les débogages ; ceci n'est pas utilisé pour exécuter CCKM, mais PKC/OKC, comme expliqué précédemment. Ici CCKM est simplement un nom utilisé par le WLC pour ces sorties, comme le nom d'une fonction qui gère les valeurs afin de calculer le PMKID.

Scénario 23 : vérification de l'itinérance Fast-Secure (FSR) avec 802.11r

Débogage utilisé :

debug client <adresse mac>

*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

.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.