Verwenden Sie diese Kurzreferenz für häufige Wireless-Probleme.

Inhalt

Einleitung

In diesem Dokument wird eine Kurzreferenz beschrieben, die Debugs (in der Regel Debug-Client <MAC-Adresse>) nach gängigen Wireless-Problemen durchsucht.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen AireOS-Controllern.

- Controller - 440x, 5508, 5520, 75xx, 85xx, 2504, 3504 und vWLC sowie WISMs.
- Obwohl viele Konzepte in den IOS® XE Controllern und Switches für konvergenten Zugriff identisch sind, gilt dieses Dokument nicht für diese, da Ausgabe und Debugging sich grundlegend unterscheiden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Kurzer PEM-Status bei Client-Ausgabe anzeigen

Um den Show-Client und das Debugging zu durchsuchen, müssen Sie zunächst einige Power Entry Module (PEM)-Zustände und APF-Zustände kennen.

- START - Anfangsstatus für neuen Client-Eintrag.
- AUTHCHECK - Das WLAN muss eine L2-Authentifizierungsrichtlinie durchsetzen.
- 8021X_REQD: Der Client muss die 802.1x-Authentifizierung abschließen.
- L2AUTHCOMPLETE (L2AUTHCOMPLETE): Der Client hat die L2-Richtlinie erfolgreich abgeschlossen. Der Prozess kann jetzt mit L3-Richtlinien (Adresslernen, Webauthentifizierung usw.) fortfahren. Der Controller sendet die Mobilitätsankündigung, um L3-Informationen von anderen Controllern abzurufen, wenn es sich um einen Roaming-Client in derselben Mobilitätsgruppe handelt.
- WEP_REQD: Der Client muss die WEP-Authentifizierung abschließen.
- DHCP_REQD - Der Controller empfängt die L3-Adresse vom Client. Dies geschieht entweder durch ARP-Anforderung, DHCP-Anforderung oder -Erneuerung oder durch Informationen, die er von anderen Controllern in der Mobilitätsgruppe bezieht. Wenn DHCP Required im WLAN markiert ist, werden nur DHCP- oder Mobilitätsinformationen verwendet.
- WEBAUTH_REQD: Der Client muss die Webauthentifizierung abschließen. (L3-Richtlinie)
- CENTRAL_WEBAUTH_REQD: Der Client muss die CWA-Anmeldung abschließen. WLC wartet auf den Erhalt der CoA.
- RUN - Der Client hat die erforderlichen L2- und L3-Richtlinien erfolgreich abgeschlossen und kann nun Datenverkehr an das Netzwerk übertragen.

Die angegebenen Szenarien zeigen die wichtigsten Fehlerbehebungszeilen für häufige Fehlkonfigurationen in Wireless-Einrichtungen, wobei die wichtigsten Parameter fett dargestellt werden.

Szenario 1: Falsch konfigurierte Passphrase für WPA/WPA2 PSK-Authentifizierung auf dem 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

Schlussfolgerung

Obwohl timeoutEvt für M2-Schlüssel auch aufgrund von Treiber-/NIC-Fehlern sein kann, ist eines der häufigsten Probleme ein Benutzer, der falsche Anmeldeinformationen für PSK-Passwort eingibt (fehlende Groß-/Kleinschreibung/Sonderzeichen usw.) und keine Verbindung herstellen kann.

Szenario 2: Wireless-Telefon-Handset (792x/9971) kann nicht mit Wireless-Service Area verbunden werden

Referenz: 7925G-Handsets Fail Association to AP - Call Failed: TSPEC QOS Policy does not Match

Topologie

WLAN mit Cisco Unified Wireless IP-Telefonen.

Problemdetails

AIR-CT5508-50-K9 // aktualisierte Firmware für Telefone und Wireless Controller akzeptiert keine Telefonregistrierung.

Fehlerbehebungen und Protokolle:

<#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

Schlussfolgerung

Das Debuggen des WLC zeigt, dass das 7925G nicht zugeordnet werden kann, da der AP den Assoziationsstatuscode 201 zurückgibt.

Dies ist darauf zurückzuführen, dass eine Traffic SPECification (TSPEC)-Anfrage vom Hörer aufgrund der WLAN-Konfiguration abgelehnt wurde. Das WLAN 7925G, das eine Verbindung herzustellen versucht, wird mit einem QoS-Profil von Silver (UP 0,3) und nicht, falls erforderlich, mit Platin (UP 6,7) konfiguriert. Dies führt zu einer TSPEC-Diskrepanz beim Austausch von Sprachverkehr/Action-Frames vom Hörer durch das WLAN und letztendlich zur Ablehnung durch den WAP.

Erstellen Sie ein neues WLAN mit einem Platinum-QoS-Profil speziell für die 7925G-Telefone, das entsprechend der Best Practices konfiguriert und im Bereitstellungsleitfaden für 7925G definiert wurde:

Bereitstellungsleitfaden für Cisco Unified Wireless IP-Telefone 7925G, 7925G-EX und 7926G

Nach der korrekten Konfiguration ist das Problem behoben.

Szenario 3: Client für WPA konfiguriert, Access Point jedoch nur für WPA2 konfiguriert

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**

Szenario 4: Analyse von AAA-Rückgabe- oder Antwortcodes

Erforderliches Debugging zur Ausführung, um die erwarteten Protokolle zu erfassen:

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

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

(ODER)

(Cisco Controller) > **Debug-Client <mac>**

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

(Cisco Controller) > **AAA-Fehlerdebug aktivieren**

Bei einem AAA-Verbindungsausfall wird ein SNMP-Trap generiert, wenn Traps aktiviert sind.

Beispiel für Debugausgabe <snipped>:

<#root>

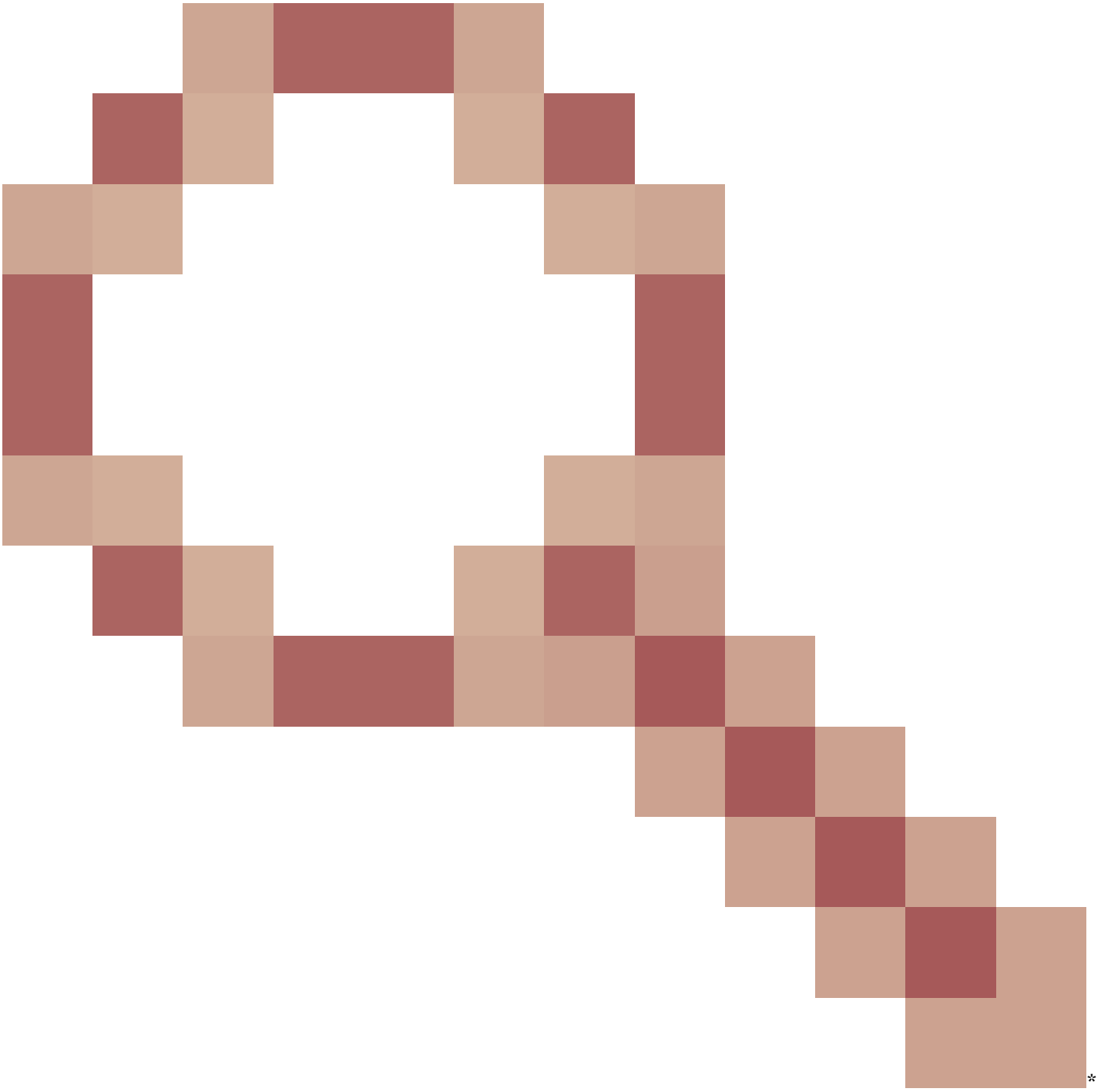
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from server 10.50.0.74 with id=213. Possible secret
*radiusTransportThread: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

Mögliche Gründe:

- Ungültiges Benutzerkonto und/oder Kennwort.
- Der Computer ist kein Mitglied der Domäne. Problem auf AD-Seite.

    - Die Zertifikatdienste funktionieren nicht ordnungsgemäß.
- Das Serverzertifikat ist abgelaufen oder wird nicht verwendet.
- RADIUS ist falsch konfiguriert.
- Der Zugriffsschlüssel wurde falsch eingegeben. Groß- und Kleinschreibung ist zu beachten (ebenso wie die SSID).
- Microsoft-Patches aktualisieren.
- EAP-Timer.
- Auf dem Client/Server wurde eine falsche EAP-Methode konfiguriert.
- Das Clientzertifikat ist abgelaufen oder wird nicht verwendet.

Timeout für Rückgabe-AAA-Fehler (-5) für Mobilgeräte
AAA-Server nicht erreichbar, gefolgt vom Client-Ausfall.

Beispiel:

<#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

Interner AAA-Fehler (-6) für Mobilgerät zurückgeben

Attributkonflikt. AAA sendet falsches/unangemessenes Attribut (falsche Länge), das nicht mit WLC verstanden/kompatibel ist. WLC sendet die Fehlermeldung, gefolgt von einer internen Fehlermeldung. Beispiel: Cisco Bug-ID CSCum83894 AAA Internal Error und Authentifizierung schlagen mit unbekannten Attributen beim Akzeptieren von Zugriffsrechten fehl.

Beispiel:

*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

Gibt AAA Error No Server (-7) für mobile Geräte zurück.

Radius ist nicht richtig konfiguriert und/oder wird nicht unterstützt.

Beispiel:

*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

Szenario 5: Client kann AP nicht zugeordnet werden

Verwendetes Debugging:

debug client <mac addr>

Zu analysierende Protokolle:

Senden der Assoc-Antwort an die Station auf BSSID 00:26:cb:94:44:c0 (Status 0) ApVapId 1 Steckplatz 0

- Steckplatz 0 = B/G(2.4)-Funkmodul
- Steckplatz 1 = A(5)-Funkmodul
- Sendet Assoc-Antwortstatus 0 = Erfolgreich

Alles andere als Status 0 ist Fehler.

Häufige Antwortcodes für Zuordnungen finden Sie unter: 802.11 Zuordnungsstatus, 802.11 Fehlerursachencodes

Szenario 6: Dissoziation des Clients aufgrund eines Leerlaufzeitlimits

Verwendetes Debugging:

debug client <mac addr>

Zu analysierende Protokolle

Empfangs-Leerlauf-Zeitüberschreitung von AP 00:26:cb:94:44:c0, Steckplatz 0 für STA 00:1e:8c:0f:a4:57

apfMsDeleteByMscb Terminierung mobil zum Löschen mit deleteGrund 4, GrundCode 4

Löschen der Mobilstation planen: (callerId: 30) in 1 Sekunden

apfMsExpireCallback (apf_ms.c:608) läuft ab!

Deauthentifizieren an Mobil unter BSSID 00:26:cb:94:44:c0 Steckplatz 0(Anrufer apf_ms.c:5094) gesendet

Bedingungen

Tritt auf, nachdem kein Datenverkehr vom Client empfangen wurde.

Die Standarddauer beträgt 300 Sekunden.

Problemumgehung

Erhöhte Leerlaufzeitüberschreitung entweder global vom WLC GUI>>Controller>>General oder per WLAN vom WLC **GUI>WLAN>ID>>Advanced**.

Szenario 7: Client-Trennung aufgrund von Sitzungs-Timeout

Verwendetes Debugging:

debug client <mac addr>

Zu analysierende Protokolle:

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

Bedingungen

Tritt während der geplanten Dauer auf (Standard: 1800 Sekunden).

Es zwingt den WEBAUTH-Benutzer wieder zu WEBAUTH.

Problemumgehung

Erhöhte oder deaktivierte Sitzungs-Zeitüberschreitung pro WLAN vom WLC **GUI>WLAN>ID>Advanced**.

Szenario 8: Trennung des Clients aufgrund von WLAN-Änderungen

Verwendetes Debugging:

debug client <mac addr>

Zu analysierendes Protokoll:

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

Bedingungen

Wenn Sie ein WLAN auf irgendeine Weise ändern, wird es deaktiviert und wieder aktiviert.

Problemumgehung

Dies ist ein erwartungsgemäßes Verhalten. Wenn WLAN-Änderungen vorgenommen wurden, trennen die Clients die Verbindung und verbinden sie erneut.

Szenario 9: Client-Trennung aufgrund manueller Löschung vom WLC

Verwendetes Debugging:

debug client <mac addr>

Zu analysierendes Protokoll:

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

Bedingungen

Aus GUI: Client entfernen

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

Szenario 10: Clienttrennung aufgrund eines Authentifizierungs-Timeouts

Verwendetes Debugging:

debug client <mac addr>

Zu analysierendes Protokoll:

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

Bedingungen

Maximale Anzahl an Neuübertragungen für Authentifizierung oder Schlüsselaustausch erreicht.

Problemumgehung

Überprüfen/Aktualisieren von Clienttreiber, Sicherheitskonfiguration, Zertifikaten usw.

Szenario 11: Trennung des Clients aufgrund von AP-Funkrücksetzung (Ein-/Ausgang)

Verwendetes Debugging:

debug client <mac addr>

Zu analysierendes Protokoll:

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

Bedingungen

AP trennt Clients, aber WLC löscht keinen Eintrag.

Problemumgehung

Erwartetes Verhalten

Szenario 12: Symantec-Client-Probleme mit 802.1x-"timeoutEvent"

Problem

Clients, auf denen die Symantec-Software ausgeführt wird, trennen die Verbindung mit dem 802.1X- timeoutEvt. Timer für die Station und für die Nachricht = M3.

Der EAP/Eapol-Prozess wird nicht abgeschlossen, unabhängig davon, welches A/G-Funkmodul auf der Intel/Broadcom-Karte verwendet wird. Kein Problem, wenn es verwendet wird wep, wpa-psk.

Bedingungen

Der WLC-Code spielt keine Rolle.

APs - alle Modelle - alle im lokalen Modus.
WLAN 3 - WPA2+802.1X PEAP + mshcapv2
SSID wird übertragen.

RADIUS-Server NPS 2008
Die Symantec-Antivirensoftware wird auf allen PCs installiert.

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

Betroffenes Betriebssystem - Windows 7 und XP

Betroffener Wireless-Adapter - Intel(6205) und Broadcom

Betroffene Treiber/Komponente - 15.2.0.19, verwenden Sie die native Komponente.

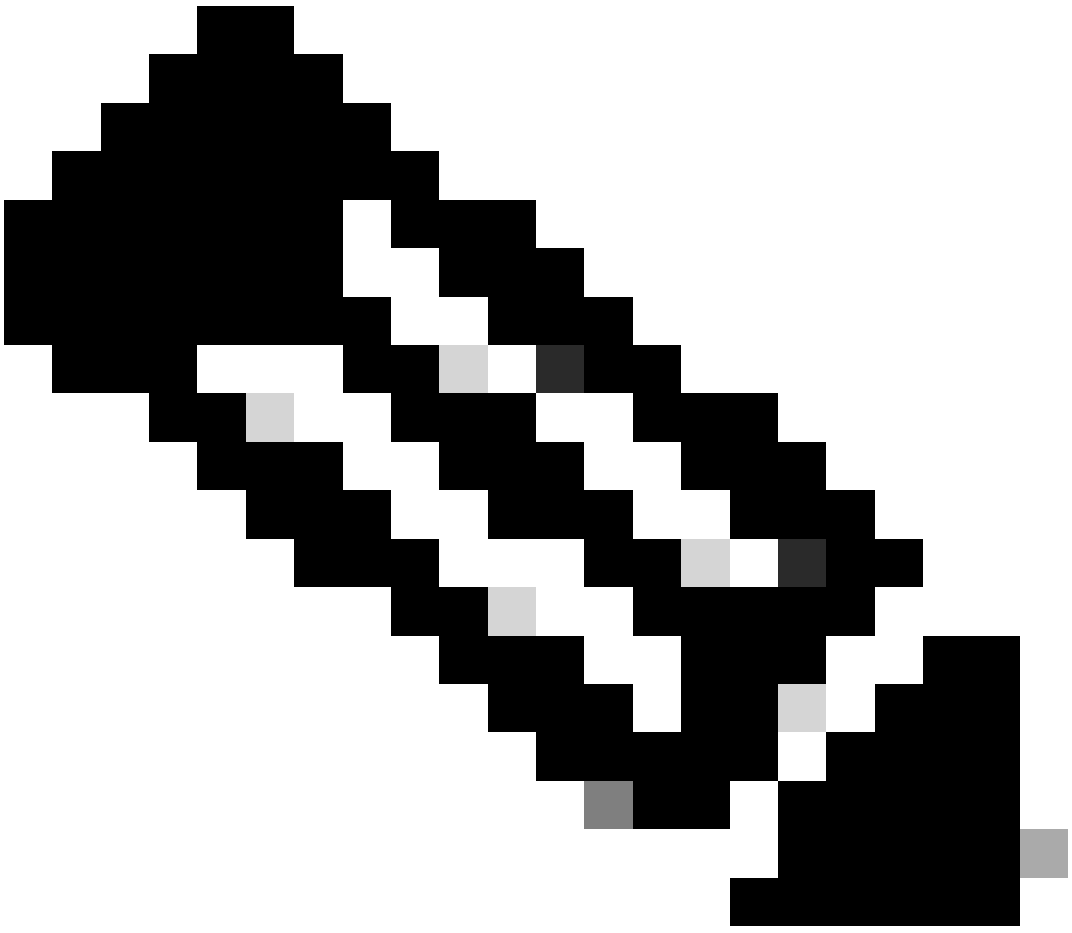
Beheben/Problemumgehung

Deaktivieren Sie Symantec Network Protection und Firewall auf win7 und xp. Es handelt sich um ein Symantec-Problem mit Windows 7 und XP.

Debug-Ausgabe:

*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

---



Hinweis: Es gibt ein Syndrom in 15.2 (auch in früheren Versionen gesehen), das wie folgt geht:
-Client empfängt M1 vom AP
-client sendet M2
-Client empfängt M3 vom AP
-Client lotet den neuen paarweisen Schlüssel aus, bevor er M4 sendet

---

- Client überträgt den M4 verschlüsselt mit dem neuen Schlüssel AP, verwirft die M4 Nachricht als "Entschlüsselungsfehler".

- Der WLC-Debug-Client zeigt an, dass bei M3-Neuübertragungen eine Zeitüberschreitung auftritt. Offensichtlich ist dies ein Problem zwischen Microsoft und Symantec, nicht Intel-spezifisch. Die Problemumgehung besteht darin, Symantec zu entfernen.

- Dies ist wirklich ein Bug, der wahrscheinlich in Windows ist, ausgelöst durch Symantec. Durch eine Anpassung des EAP-Timers wird dieses Problem nicht behoben.

- In Bezug auf dieses Problem leitet das Cisco TAC die betroffenen Benutzer an Symantec und Microsoft weiter.

Szenario 13: Der Air Print Service wird nicht auf Clients mit mDNS angezeigt, auf denen Snoop aktiviert wurde.

Der Client kann keine Geräte sehen, die AirPrint-Dienste auf Apple-Handheld-Clientgeräten bereitstellen, wenn mDNS-Snoop aktiviert ist.

Bedingungen

5508 WLC mit 7.6.100.0.
Bei aktiviertem mDNS-Snoop werden die Geräte, die AirPrint-Services bereitstellen, im Abschnitt "Services" des WLC aufgeführt.
Das entsprechende mDNS-Profil wurde dem WLAN und der Schnittstelle richtig zugeordnet.
Die AirPrint-Geräte auf dem Client sind immer noch nicht sichtbar.

Verwendetes Debugging:

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_

Erläuterung:

Der Client fordert _universal._sub._ipps._tcp.local oder _universal._sub._ipp._tcp.local anstelle von **_ipp._tcp.local** oder _ipp._tcp.local string an.
Der zusätzliche AirPrint-Service würde also nicht funktionieren. Sie wurde identifiziert, und der angeforderte Dienst-String wurde zugeordnet.

HP_Photosmart_Printer_1.
Derselbe Service wurde dem Profil hinzugefügt, das dem WLAN zugeordnet ist, und es war immer noch kein Service für das Gerät aufgelistet.

Es wurde festgestellt, dass der WLC aufgrund des angehängten Domänennamens und der Clientabfrage für dns-sd._udp.YVG lokal mit angehängtem Domänennamen das Bonjour-Paket nicht verarbeiten konnte, da es in der Datenbank nicht vorhanden istdns-sd._udp.YVG.local.

Identifiziert den gegebenen Verbesserungsfehler hinsichtlich desselben - Cisco Bug-ID CSCuj32157.

Problemumgehung

Die einzige Lösung bestand darin, die DHCP-Option 15 (Domänenname) zu deaktivieren oder den Domänennamen vom Client zu entfernen.

Szenario 14: Apple iOS-Client kann aufgrund einer deaktivierten schnellen SSID-Änderung nicht dem Netzwerk beitreten

Bedingungen

Bei den meisten Apple iOS-Geräten ist es problematisch, auf demselben Cisco WLC mit der Standardeinstellung von einem WLAN in ein anderes zu wechseln fast SSID change disabled.

Diese Einstellung bewirkt, dass der Controller die Authentifizierung des Clients gegenüber dem vorhandenen WLAN deaktiviert, sobald der Client eine Verbindung mit einem anderen herstellen möchte.

Das typische Ergebnis ist eine "nable to Join the Network" Umessage" auf dem iOS-Gerät.

Client anzeigen

(jk-2504-116) >**Netzwerkübersicht anzeigen**

<Snip>

Schnelle SSID-Änderung ..... Deaktiviert

Verwendetes Debugging:

<#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

Problemumgehung

Fast-SSID-Änderung vom WLC aus aktivieren GUI > Controller>General.

Szenario 15: Erfolgreiche Client-LDAP-Zuordnung

Secure LDAP hilft, die Verbindung zwischen dem Controller und dem LDAP-Server, der TLS verwendet, zu sichern. Diese Funktion wird von der Controller-Software Version 7.6 und höher unterstützt.

Der Controller kann zwei Arten von Abfragen an den LDAP-Server senden:

1. Anonym

Bei diesem Typ sendet der Controller eine Authentifizierungsanforderung an den LDAP-Server, wenn ein Client authentifiziert werden muss. Der LDAP-Server antwortet mit dem Ergebnis der Abfrage. Zum Zeitpunkt dieses Austauschs werden alle Informationen, die den Benutzernamen/das Passwort des Kunden enthalten, in Klartext gesendet. Der LDAP-Server antwortet auf eine Anfrage von jedem Benutzer, solange die Eingabe von Benutzername/Kennwort für die Anbindung erfolgt.

2. Authentifiziert

Bei diesem Typ wird der Controller mit einem Benutzernamen und einem Passwort konfiguriert, das er verwendet, um sich beim LDAP-Server zu authentifizieren. Das Kennwort wird mit MD5 SASL verschlüsselt und zum Zeitpunkt der Authentifizierung an den LDAP-Server gesendet. Dadurch kann der LDAP-Server die Quelle der Authentifizierungsanforderungen richtig identifizieren. Obwohl die Identität des Controllers geschützt ist, werden die Client-Daten im Klartext gesendet.

Der tatsächliche Bedarf an LDAP über TLS ergab sich aufgrund der Sicherheitslücke, die von diesen beiden Typen ausgeht, bei denen die Client-Authentifizierungsdaten und der Rest der Transaktion eindeutig sind.

Anforderungen

WLC führt die Softwareversion 7.6 und höher aus.

Der Microsoft-Server verwendet LDAP.

Verwendetes Debugging:

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

Szenario 16: Fehler bei der Client-Authentifizierung auf LDAP

Verwendetes Debugging:

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

Problemumgehung

Überprüfen Sie den LDAP-Server auf Ablehnungsgründe.

Szenario 17: Probleme mit der Clientzuordnung aufgrund einer falschen LDAP-Konfiguration auf dem WLC

Verwendetes Debugging:

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

Problemumgehung

Anmeldeinformationen für Client/WLC und LDAP-Server überprüfen.

Szenario 18: Probleme mit der Clientzuordnung, wenn der LDAP-Server nicht erreichbar ist

Verwendetes Debugging:

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

Problemumgehung

Verbindungsprobleme bei WLC- und LDAP-Servernetzwerken prüfen.

Szenario 19: Roaming-Probleme beim Apple-Client aufgrund einer fehlenden Sticky-Roaming-Konfiguration

Bedingungen

AIR-CT5508-K9 / 7.4.100.0

Apple-Geräte trennen die Verbindung zu einem Wireless-Netzwerk, das Folgendes verwendet:

- WPA2-Richtlinie
- WPA2-Verschlüsselung AES
- 802.1X-Authentifizierung aktiviert

Authentifizierung und Autorisierung durch die Cisco ISE.

Apple-Geräte trennen regelmäßig die Verbindung zur Broadcast-SSID. Ein Beispiel ist ein iPhone, das herunterfällt, während ein anderes Telefon am gleichen Standort verbunden bleibt. Daher geschieht dies zufällig (Zeit und Telefon).

Laptop-Clients ohne Probleme Sie sind mit derselben SSID verbunden.

Dieses Problem tritt während des normalen Betriebs auf, ohne Roaming und ohne Standby-Modus.

Das WLAN hat bereits alle möglichen Einstellungen entfernt, die zu Problemen führen könnten (Aironet ext).

Verwendetes Debugging:

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.
```

Problemumgehung

Für Kunden mit Sticky Key Caching (SKC)-Clients und WLC-Code 7.2 oder höher können Sie jetzt Roaming-Unterstützung für SKC aktivieren. Standardmäßig unterstützt der WLC nur Opportunistic Key Caching (OKC). Damit der Client seine alten PMKIDs verwenden kann, die er an jedem AP generiert hat, muss er diese über die WLC-CLI aktivieren.

config wlan security wpa wpa2 cache sticky enable <1>

Bitte beachten Sie, dass dies anfängliche Roaming aufgrund der Art von SKC nicht verbessert, jedoch späteres Roaming zu den gleichen APs (bis zu 8 laut Buch) verbessert. Stellen Sie sich einen Gang mit 8 APs vor. Die erste exemplarische Vorgehensweise besteht aus vollständigen Zuordnungen an jedem AP mit einer Verzögerung von etwa 1-2 Sekunden. Wenn Sie das Ende erreichen und zurückgehen, präsentiert der Client 8 eindeutige PMKIDs, während er zu denselben Zuordnungen zurückkehrt.

APs müssen keine vollständige Authentifizierung durchführen, wenn die SKC-Unterstützung aktiviert ist. Dadurch wird die Verzögerung beseitigt, und der Client scheint weiterhin verbunden zu bleiben.

Szenario 20: Überprüfen von Fast-Secure-Roaming (FSR) mit CCKM

802.11 WLAN-Roaming und Fast-Secure Roaming auf CUWN

Verwendetes Debugging:

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

Wie gezeigt, wird schnelles sicheres Roaming durchgeführt, um EAP-Authentifizierungs-Frames und noch mehr 4-Wege-Handshakes zu

vermeiden, da die neuen Verschlüsselungsschlüssel immer noch abgeleitet werden, aber auf dem CCKM-Verhandlungsschema basieren. Dies wird durch die Roaming-Zuordnungsrahmen und die zuvor vom Client und vom WLC zwischengespeicherten Informationen ergänzt**.**

Szenario 21: Überprüfung von Fast-Secure-Roaming (FSR) mit WPA2 PMKID-Cache

Verwendetes Debugging:

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

Szenario 22: Überprüfung von Fast-Secure Roaming mit Proactive Key Cache

Verwendetes Debugging:

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
```

Wie zu Beginn der Debugging-Phase gezeigt, muss die PMKID berechnet werden, nachdem die Reassoziationsanforderung vom Client empfangen wurde. Dies ist erforderlich, um die PMKID zu validieren und zu bestätigen, dass der zwischengespeicherte PMK mit dem 4-Wege-WPA2-Handshake verwendet wird, um die Verschlüsselungsschlüssel abzuleiten und das schnelle sichere Roaming zu beenden. Verwechseln Sie nicht die CCKM-Einträge auf den Debugs. Dies wird nicht verwendet, um CCKM auszuführen, sondern PKC/OKC, wie zuvor erläutert. Hierbei ist CCKM einfach ein vom WLC für diese Ausgaben verwendeter Name, z. B. der Name einer Funktion, die die Werte verarbeitet, um die PMKID zu berechnen.

Szenario 23: Überprüfung von Fast-Secure-Roaming (FSR) mit 802.11r

Verwendetes Debugging:

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

.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.