Utilice esta hoja de referencia para problemas inalámbricos comunes

Contenido

Introducción

Este documento describe una hoja de referencia que analiza los debugs (por lo general, debug client <mac address>) para detectar problemas comunes de conexión inalámbrica.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en todos los controladores de AireOS.

- Controladores: 440x, 5508, 5520, 75xx, 85xx, 2504, 3504 y vWLC, así como WISM.
- Aunque muchos conceptos son idénticos en los controladores y switches IOS® XE de acceso convergente, este documento no se aplica a ellos ya que los resultados y las depuraciones son radicalmente diferentes.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Breve estado de PEM en la salida de Show Client

Para analizar a través de show client y debugs primero se requiere entender algunos estados del Módulo de entrada de energía (PEM) y estados APF.

- START: estado inicial de la nueva entrada de cliente.
- AUTHCHECK: WLAN tiene una política de autenticación L2 que aplicar.
- 8021X_REQD: el cliente debe completar la autenticación 802.1x.
- L2AUTHCOMPLETE: el cliente ha finalizado correctamente la política L2. El proceso ahora puede continuar con las políticas L3 (aprendizaje de direcciones, autenticación Web, etc.). El controlador envía el anuncio de movilidad para obtener información de nivel 3 de otros controladores si se trata de un cliente de roaming en el mismo grupo de movilidad.
- WEP_REQD: el cliente debe completar la autenticación WEP.
- DHCP_REQD: el controlador aprende la dirección L3 del cliente, lo que se realiza mediante una solicitud ARP, una solicitud DHCP o una renovación, o bien mediante información obtenida de otros controladores del grupo de movilidad. Si DHCP Required está marcado en el WLAN, sólo se utiliza la información de movilidad o DHCP.
- WEBAUTH_REQD: el cliente debe completar la autenticación Web. (política L3)
- CENTRAL_WEBAUTH_REQD: el cliente debe completar el inicio de sesión de CWA. El WLC espera para recibir el CoA.
- RUN: el cliente ha completado correctamente las políticas L2 y L3 necesarias y ahora puede transmitir tráfico a la red.

Los escenarios dados muestran las líneas de depuración clave para las configuraciones erróneas comunes en las configuraciones inalámbricas, que resalta los parámetros clave en negrita.

Situación 1: Frase de paso mal configurada para la autenticación WPA/WPA2 PSK en el cliente

<#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
-------------------------
```

Depurar análisis de cliente:

<#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

Conclusión

Aunque timeoutEvt para la clave M2 también podría deberse a errores de controlador/NIC, uno de los problemas más comunes es un usuario que ingresa credenciales incorrectas para la contraseña PSK (distingue entre mayúsculas y minúsculas, caracteres especiales, etc.) y no puede conectarse.

Situación 2: el auricular del teléfono inalámbrico (792x/9971) no se puede asociar al área de servicio de "abandono" inalámbrico

Referencia: Asociación fallida de terminales 7925G a AP - Llamada fallida: la política de QOS de TSPEC no coincide

Topología

WLAN con teléfonos IP inalámbricos de Cisco Unified.

Detalles del problema

AIR-CT5508-50-K9 // El firmware actualizado para teléfonos y controladores inalámbricos no acepta registros telefónicos.

Depuraciones y registros:

<#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

Conclusión

La depuración en el WLC muestra que el 7925G falla la asociación ya que el AP devuelve un código de estado de asociación de 201.

Esto se debe a una solicitud de Traffic SPECification (TSPEC) del rechazo del terminal debido a la configuración WLAN. El WLAN 7925G que intenta conectarse se configura con un perfil de QoS Silver (UP 0,3), en lugar de Platinum (UP 6,7), según sea necesario. Esto lleva a una discordancia TSPEC para el tráfico de voz/intercambio de tramas de acción desde el auricular por parte de la WLAN y, en última instancia, a un rechazo del AP.

Cree una nueva WLAN con un perfil de QoS de Platinum específico para los terminales 7925G y configurado según las prácticas recomendadas establecidas y según se define en la Guía de implementación de 7925G:

Guía de implementación de los teléfonos IP inalámbricos 7925G, 7925G-EX y 7926G de Cisco Unified

Una vez configurado correctamente, el problema se resuelve.

Situación 3: Cliente configurado para WPA pero AP configurado sólo para 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**

Situación 4: análisis de códigos de respuesta o devolución AAA

Depuraciones necesarias para que RUN recopile los registros esperados:

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

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

(O)

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

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

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

Un fallo de conectividad AAA genera una trampa SNMP, si las trampas están habilitadas.

Ejemplo de resultado de debug <snipped>:

<#root>

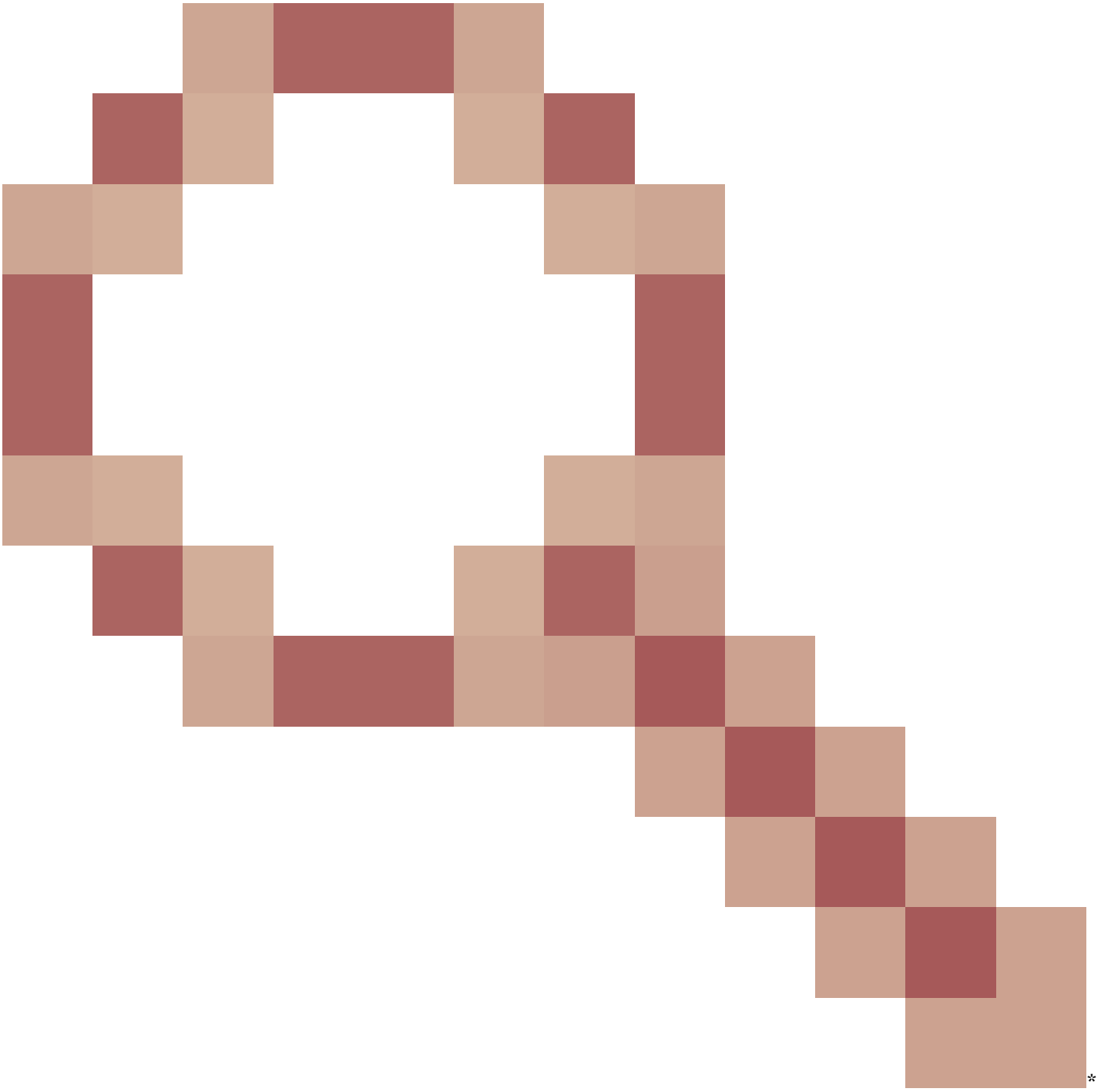
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from server 10.50.0.74 with id=213. Possible secret
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Returning AAA Error 'Authentication Failed' (-4) for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: AuthorizationResponse: 0x4259f944

Returning AAA Error 'Success' (0) for mobile

Successful Authentication happened, AAA returns access-accept prior to Success (0) to confirm the same.

Returning AAA Error 'Out of Memory' (-2) for mobile

***it's the rare reason. Cisco bug ID CSCud12582



***Proc

Returning AAA Error 'Authentication Failed' (-4) for mobile

***its the most common reason seen

Posibles Motivos:

- Cuenta de usuario y/o contraseña no válidas.
- El equipo no es miembro del dominio, problema en el lado AD.

    - Los servicios de Certificate Server no funcionan correctamente.
- El certificado de servidor ha caducado o no está en uso.
- RADIUS configurado incorrectamente.
- Clave de acceso introducida incorrectamente: distingue entre mayúsculas y minúsculas (al igual que el SSID).
- Actualizar revisiones de Microsoft.
- Temporizadores EAP.
- Método EAP incorrecto configurado en el cliente/servidor.
- El certificado de cliente ha caducado o no está en uso.

Tiempo de espera de error AAA devuelto (-5) para móvil

AAA Server Unreachable (Servidor AAA inalcanzable), seguido de client default.

Ejemplo:

<#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

Devolver error AAA Error interno (-6) para móvil

Discordancia de atributos. AAA envía un atributo incorrecto/inapropiado (longitud incorrecta) que no se entiende/es compatible con el WLC. El WLC envía el mensaje de Deauth, seguido por el mensaje de error interno. Ejemplo: Cisco bug ID CSCum83894 AAA Internal Error y auth fail con atributos desconocidos en access accept.

Ejemplo:

*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

Devuelve AAA Error No Server (-7) para móvil.

Radius no está configurado correctamente y/o se está usando una configuración no compatible.

Ejemplo:

*Jun 22 20:32:10.229: 00:21:e9:57:3c:bf Returning AAA Error 'No Server' (-7) for mobile 00:21:e9:57:3c:bf *Jun 22 20:32:10.229: AuthorizationRespons

Escenario 5: el cliente no se asocia al AP

Depuración utilizada:

debug client <mac addr>

Registros para analizar:

Enviando respuesta de assoc a la estación en BSSID 00:26:cb:94:44:c0 (estado 0) ApVapId 1 ranura 0

- Ranura 0 = Radio B/G(2.4)
- Ranura 1 = Radio A(5)
- Envía El Estado De Respuesta De Asociación 0 = Correcto

Todo lo que no sea el estado 0 es Falla.

Los códigos de estado de respuesta de asociación comunes se pueden encontrar en: 802.11 Association Status, 802.11 Deauth Reason Codes

Situación 6: desasociación de clientes debido a tiempo de espera inactivo

Depuración utilizada:

debug client <mac addr>

Registros para analizar

Tiempo de espera de inactividad recibido desde AP 00:26:cb:94:44:c0, ranura 0 para STA 00:1e:8c:0f:a4:57

apfMsDeleteByMscb Programación móvil para eliminación con deleteReason 4, reasonCode 4

Programación de eliminación de Mobile Station: (callerId: 30) en 1 segundo

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

Enviado desde la autenticación al móvil en BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)

Condiciones

Se produce después de que no se reciba tráfico del cliente.

La duración predeterminada es de 300 segundos.

Solución Aternativa

Aumente el tiempo de espera inactivo globalmente desde el WLC GUI>>Controller>>General, o por WLAN desde el WLC **GUI>WLAN>ID>>Advanced**.

Situación 7: desasociación del cliente debido al tiempo de espera de la sesión

Depuración utilizada:

debug client <mac addr>

Registros para analizar:

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

Condiciones

Se produce en una duración programada (valor predeterminado: 1800 segundos).

Fuerza al usuario WEBAUTH a WEBAUTH nuevamente.

Solución Aternativa

Aumente o inhabilite el tiempo de espera de sesión por WLAN del WLC **GUI>WLAN>ID>Advanced**.

Situación 8: desasociación de clientes debido a cambios en la WLAN

Depuración utilizada:

debug client <mac addr>

Registro para analizar:

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

Condiciones

Para modificar una WLAN de cualquier manera, inhabilita y vuelve a habilitar la WLAN.

Solución Aternativa

Debe ocurrir lo siguiente. Cuando se realizan cambios en la WLAN, los clientes se desasocian y vuelven a asociarse.

Situación 9: Desasociación del cliente debido a la eliminación manual del WLC

Depuración utilizada:

debug client <mac addr>

Registro para analizar:

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

Condiciones

Desde la GUI: eliminar cliente

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

Situación 10: desasociación del cliente debido al tiempo de espera de autenticación

Depuración utilizada:

debug client <mac addr>

Registro para analizar:

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

Condiciones

Se alcanzaron retransmisiones máximas de autenticación o intercambio de claves.

Solución Aternativa

Comprobar/actualizar el controlador de cliente, la configuración de seguridad, los certificados, etc.

Situación 11: desasociación de clientes debido a reinicio de radio AP (alimentación/canal)

Depuración utilizada:

debug client <mac addr>

Registro para analizar:

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

Condiciones

El AP desasocia a los clientes, pero el WLC no elimina la entrada.

Solución Aternativa

Comportamiento esperado.

Situación 12: problemas del cliente Symantec con 802.1X "timeoutEvt"

Problema

Los clientes que ejecutan el software Symantec no se asocian con el mensaje 802.1X timeoutEvt. Timer caducaron para la estación y para el mensaje = M3

El proceso EAP/EAPOL no se completa, independientemente de la radio A/G utilizada en la tarjeta Intel/Broadcom. No hay problema cuando se utiliza wep, wpa-psk.

Condiciones

El código WLC no importa.

AP - todos los modelos - Todos en modo local.
wlan 3: WPA2+802.1X PEAP + mshcapv2
SSID se difunde.

Servidor RADIUS nps 2008.
El software antivirus Symantec está instalado en todos los PC.

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

SO afectado: Windows 7 y XP

Adaptador inalámbrico afectado: Intel(6205) y Broadcom

Controlador/suplicante afectado: 15.2.0.19; utilice suplicante nativo.

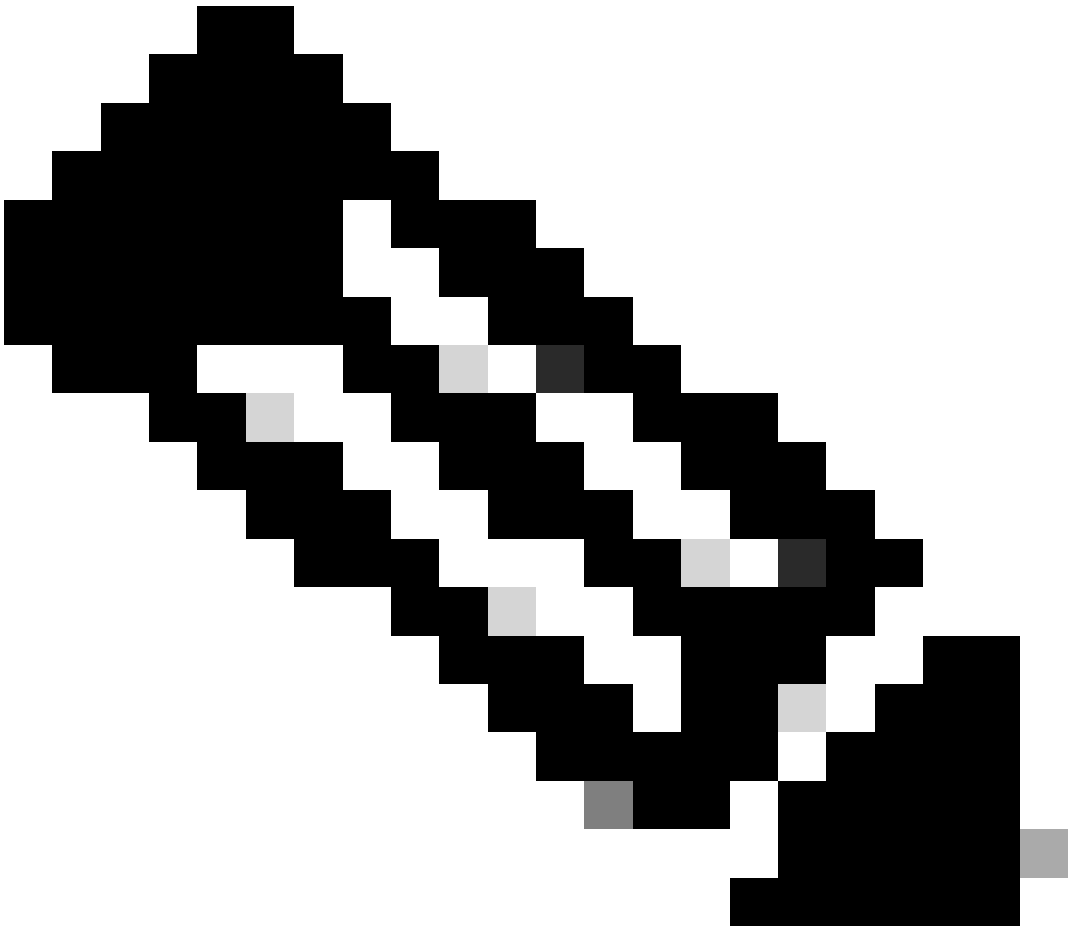
Solución/Solución alternativa

Deshabilite Symantec Network Protection and Firewall en win7 y xp. Es un problema de Symantec con Win 7 y XP OS.

Resultado de depuración:

*dot1xMsgTask: Apr 12 11:45:39.335: 84:3a:4b:7a:d5:ac Retransmit 1 of EAPOL-Key M3 (length 155) for mobile 84:3a:4b:7a:d5:ac *osapiBsnTimer: Ap
*dot1xMsgTask: Apr 12 11:45:44.336: 84:3a:4b:7a:d5:ac Retransmit 2 of EAPOL-Key M3 (length 155) for mobile 84:3a:4b:7a:d5:ac *osapiBsnTimer: Ap
*dot1xMsgTask: Apr 12 11:45:49.336: 84:3a:4b:7a:d5:ac Retransmit 3 of EAPOL-Key M3 (length 155) for mobile 84:3a:4b:7a:d5:ac *osapiBsnTimer: Ap

---



Nota: Hay un síndrome en 15.2 (también visto en versiones anteriores) que va como:

-client obtiene M1 del AP
-client envía M2
-client obtiene M3 desde AP
-client sondea la nueva clave de par antes de enviar M4

- El cliente transmite el M4 cifrado con el nuevo AP de clave, descarta el mensaje M4 como un "error de descifrado".

- El cliente de depuración del WLC muestra que usted agota el tiempo de espera en las retransmisiones M3. Evidentemente, se trata de un problema entre Microsoft y Symantec, no específico de Intel. La solución alternativa es eliminar Symantec.

- Este es realmente un bug que está probablemente en Windows, disparado por Symantec. El ajuste del temporizador EAP no soluciona este problema.

- Con respecto a este problema, Cisco TAC reenvía a los usuarios afectados a Symantec y Microsoft.

Situación 13: el servicio de impresión aérea no se muestra a los clientes con mDNS que activaron Snoop

El cliente no puede ver los dispositivos que proporcionan el servicio AirPrint en los dispositivos cliente de mano de Apple cuando se activa la función de detección de mDNS.

Condiciones

WLC 5508 con 7.6.100.0.
Con mDNS snoop habilitado, usted tiene los dispositivos que proporcionan los servicios de AirPrint enumerados en la sección de servicios en el WLC.
El perfil mDNS respectivo se asignó correctamente a la WLAN y a la interfaz.
Todavía no se pueden ver los dispositivos AirPrint en el cliente.

Depuración utilizada:

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_

Explicación:

El cliente solicitaría _universal._sub._ipps._tcp.local o _universal._sub._ipp._tcp.local en lugar de **_ipp._tcp.local** o _ipp._tcp.local cadena.
Por lo tanto, el servicio AirPrint agregado no funcionaría. Se identificó y se asignó la cadena de servicio solicitada HP_Photosmart_Printer_1.
Se agregó el mismo servicio en el perfil asignado a la WLAN y aún no había ningún servicio enumerado para el dispositivo.

Se encontró que debido al nombre de dominio anexado y a la consulta del cliente para dns-sd._udp.YVG local con el nombre de dominio anexado, el WLC no pudo procesar el paquete Bonjour pues dns-sd._udp.YVG.local no existe en la base de datos.

Se identificó el error de mejora dado con respecto al mismo: ID de error de Cisco CSCuj32157.

Solución Aternativa

La única solución consiste en desactivar la opción DHCP 15 (nombre de dominio) o quitar el nombre de dominio del cliente.

Situación 14: el cliente Apple iOS "no puede conectarse a la red" debido a un cambio rápido de SSID deshabilitado

Condiciones

La mayoría de los dispositivos Apple iOS tienen problemas para moverse de una WLAN a otra en el mismo WLC de Cisco con el valor predeterminado fast SSID change disabled.

La configuración hace que el controlador desautentique al cliente de la WLAN que existe una vez que el cliente intenta asociarse con otro.

El resultado típico es un mensaje "nable to Join the Network" Umessage" en el dispositivo con iOS.

Mostrar cliente

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

<snip>

Cambio rápido de SSID ..... Inhabilitado

Depuración utilizada:

<#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
```

Solución Aternativa

Habilite el cambio rápido de SSID del WLC GUI > Controller>General.

Situación 15: Asociación LDAP de cliente satisfactoria

LDAP seguro ayuda a proteger la conexión entre el controlador y el servidor LDAP que utiliza TLS. Esta función es compatible con el software de controlador versión 7.6 y posteriores.

Hay dos tipos de consultas que el controlador puede enviar al servidor LDAP:

1. Anónimo

En este tipo, el controlador envía una solicitud de autenticación al servidor LDAP cuando un cliente necesita ser autenticado. El servidor LDAP responde con el resultado de la consulta. En el momento de este intercambio, toda la información que incluye el nombre de usuario/contraseña del cliente se envía en texto sin formato. El servidor LDAP responde a una consulta de cualquier persona, siempre y cuando se agreguen el nombre de usuario/contraseña de enlace.

2. Autenticado

En este tipo, el controlador se configura con un nombre de usuario y una contraseña que utiliza para autenticarse con el servidor LDAP. La contraseña se cifra con MD5 SASL y se envía al servidor LDAP en el momento del proceso de autenticación. Esto ayuda al servidor LDAP a identificar correctamente el origen de las solicitudes de autenticación. Sin embargo, aunque la identidad del controlador esté protegida, los detalles del cliente se envían en texto claro.

La necesidad real de LDAP sobre TLS vino debido a la vulnerabilidad de seguridad planteada por estos dos tipos donde los datos de autenticación del cliente y el resto de la transacción ocurren en forma clara.

Requirements

WLC ejecuta la versión de software 7.6 y superior.

El servidor de Microsoft utiliza LDAP.

Depuración utilizada:

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

Situación 16: Error de autenticación del cliente en LDAP

Depuración utilizada:

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

Solución Aternativa

Verifique el servidor LDAP por razones de rechazo.

Situación 17: Problemas de asociación del cliente debido a una configuración incorrecta de LDAP en WLC

Depuración utilizada:

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

Solución Aternativa

Verifique las credenciales a través del cliente/WLC y el servidor LDAP.

Situación 18: Problemas de asociación del cliente cuando el servidor LDAP es inalcanzable

Depuración utilizada:

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

Solución Aternativa

Verifique los problemas de conectividad de red del servidor LDAP y WLC.

Situación 19: problemas de roaming del cliente de Apple debido a la falta de configuración de roaming persistente

Condiciones

AIR-CT5508-K9 / 7.4.100.0

Los dispositivos Apple se desconectan de una red inalámbrica que utiliza:

- Política WPA2
- Encriptación WPA2 AES
- Autenticación 802.1X habilitada

Autenticación y autorización mediante Cisco ISE.

Los dispositivos Apple se desconectan periódicamente del SSID de difusión. Un ejemplo es un iPhone que se cae mientras otro teléfono en la misma ubicación permanece conectado. Por lo tanto, esto ocurre aleatoriamente (hora y teléfono).

Clientes de portátiles sin problemas. Se conectan al mismo SSID.

Este problema ocurre durante el funcionamiento normal, sin itinerancia y sin modo de espera.

La WLAN ya ha eliminado todas las configuraciones posibles que podrían causar problemas (Aironet ext).

Depuración utilizada:

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.
```

Solución Aternativa

Lo que puede hacer ahora para los clientes que tienen clientes de Sticky Key Caching (SKC) y también tienen código WLC 7.2 y superior, es habilitar el soporte de roaming para SKC. Por defecto, el WLC soporta solamente el almacenamiento en caché de la llave oportunista (OKC). Para permitir que el cliente utilice sus PMKID viejos que generó en cada AP, usted tiene que habilitarlo por el WLC CLI.

config wlan security wpa wpa2 cache sticky enable <1>

Tenga en cuenta que esto no mejora las itinerancias iniciales debido a la naturaleza de SKC; sin embargo, mejora las itinerancias subsiguientes a los mismos AP (hasta 8 según el libro). Imaginen un paseo por un pasillo con 8 AP. El primer tutorial consta de asociaciones completas en cada AP con un retraso de aproximadamente 1 a 2 segundos. Cuando llega al final y retrocede, el cliente presenta 8 PMKID únicos a medida que vuelve a las mismas asociaciones.

Los AP no tienen que pasar por una autenticación completa si el soporte de SKC está habilitado. Esto elimina el retraso y el cliente parece permanecer conectado.

Situación 20: verificación de la itinerancia rápida y segura (FSR) con CCKM

Roaming WLAN 802.11 y Roaming Fast-Secure en CUWN

Depuración utilizada:

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

Como se muestra, el roaming seguro rápido se realiza para evitar las tramas de autenticación EAP y más handshakes de 4 vías, porque las nuevas

claves de cifrado aún se derivan, pero se basan en el esquema de negociación CCKM. Esto se completa con las tramas de reasociación de roaming y la información previamente almacenada en caché por el cliente y el WLC**.**

Situación 21: verificación de la itinerancia rápida y segura (FSR) con caché PMKID de WPA2

Depuración utilizada:

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

Situación 2: verificación de la itinerancia segura y rápida con caché de claves proactiva

Depuración utilizada:

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
```

Como se muestra al inicio de las depuraciones, el PMKID debe calcularse después de que se reciba la solicitud de reasociación del cliente. Esto es necesario para validar el PMKID y confirmar que el PMK almacenado en caché se utiliza con el protocolo de enlace de 4 vías WPA2 para derivar las claves de cifrado y finalizar el roaming de seguridad rápida. No confunda las entradas de CCKM en los debugs; esto no se utiliza para realizar CCKM, sino PKC/OKC, como se explicó anteriormente. Aquí CCKM es simplemente un nombre utilizado por el WLC para esas salidas, como el nombre de una función que maneja los valores para calcular el PMKID.

Situación 23: verificación de la itinerancia rápida y segura (FSR) con 802.11r

Depuración utilizada:

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

.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).