일반적인 무선 문제에 대해 이 치트 시트 사용

목차

소개

이 문서에서는 일반적인 무선 문제에 대해 디버그를 통해 구문 분석하는 치트 시트(일반적으로 debug client <mac address>)에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 모든 AireOS 컨트롤러를 기반으로 합니다.

- 컨트롤러 - 440x, 5508, 5520, 75xx, 85xx, 2504, 3504, vWLC 및 WISM.
- Converged Access IOS® XE 컨트롤러와 스위치에서는 여러 개념이 동일하지만, 출력과 디버깅이 근본적으로 다르므로 이 문서는 여기에 적용되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Show Client Output의 Brief PEM 상태

먼저 show client 및 debug를 통해 구문 분석하려면 일부 PEM(Power Entry Module) 상태 및 APF 상태를 이해해야 합니다.

- START(시작) - 새 클라이언트 항목의 초기 상태입니다.
- AUTHCHECK—WLAN에 적용할 L2 인증 정책이 있습니다.

- 8021X_REQD - 클라이언트가 802.1x 인증을 완료해야 합니다.
- L2AUTHCOMPLETE - 클라이언트가 L2 정책을 성공적으로 완료했습니다. 이제 프로세스는 L3 정책(주소 학습, 웹 인증 등)으로 진행할 수 있습니다. 컨트롤러가 동일한 모빌리티 그룹의 로밍 클라이언트인 경우 다른 컨트롤러에서 L3 정보를 확인하기 위해 모빌리티 알림을 보냅니다.
- WEP_REQD - 클라이언트가 WEP 인증을 완료해야 합니다.
- DHCP_REQD - 컨트롤러가 클라이언트에서 L3 주소를 학습합니다. 이 학습은 ARP 요청, DHCP 요청 또는 갱신을 통해 수행되거나 모빌리티 그룹의 다른 컨트롤러에서 학습된 정보를 통해 수행됩니다. DHCP Required(DHCP 필요)가 WLAN에 표시된 경우 DHCP 또는 모빌리티 정보만 사용됩니다.
- WEBAUTH_REQD - 클라이언트가 웹 인증을 완료해야 합니다. (L3 정책)
- CENTRAL_WEBAUTH_REQD - 클라이언트가 CWA 로그인을 완료해야 합니다. WLC는 CoA 수신을 기다립니다.
- RUN(실행) - 클라이언트가 필요한 L2 및 L3 정책을 성공적으로 완료했으며 이제 네트워크로 트래픽을 전송할 수 있습니다.

제공된 시나리오는 무선 설정의 일반적인 구성 오류 시 주요 디버그 라인을 보여줍니다. 주요 매개변수가 굵게 표시됩니다.

시나리오 1: 클라이언트에서 WPA/WPA2 PSK 인증을 위한 암호가 잘못 구성되었습니다.

<#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

-------------------------
```

디버그 클라이언트 분석:

<#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
```

결론

timeoutEvt M2 키의 경우 드라이버/NIC 오류 때문일 수도 있지만 가장 일반적인 문제 중 하나는 PSK 암호에 대해 잘못된 자격 증명 (대/소문자 구분 없음/특수 문자 등)을 입력하고 연결할 수 없는 사용자입니다.

시나리오 2: 무선 전화기 핸드셋(792x/9971)이 무선 "Leaves Service Area(서비스 영역 종료)"와 연결되지 않음

참조: 7925G 핸드셋 AP 연결 실패 - 통화 실패: TSPEC QOS 정책이 일치하지 않음

토폴로지

Cisco Unified Wireless IP Phone을 통한 WLAN

문제 세부 정보

AIR-CT5508-50-K9 // 업그레이드된 전화기 및 무선 컨트롤러용 펌웨어는 전화 등록을 허용하지 않습니다.

디버깅 및 로그:

<#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

결론

WLC의 디버그는 AP가 연결 상태 코드 201을 반환할 때 7925G가 연결에 실패함을 보여줍니다.

이는 WLAN 컨피그레이션으로 인한 핸드셋 거부의 TSPEC(Traffic SPECification) 요청 때문입니다. 연결을 시도하는 WLAN 7925G는 필요에 따라 Platinum(UP 6,7)이 아닌 Silver(UP 0,3)의 QoS 프로필로 구성됩니다. 이로 인해 WLAN에 의한 핸드셋의 음성 트래픽/동작 프레임 교환에 대한 TSPEC 불일치가 발생하고, 궁극적으로 AP로부터의 거부가 발생합니다.

7925G 핸드셋용으로 특별히 Platinum의 QoS 프로필을 사용하여 새로운 WLAN을 생성하고, 설정된 모범 사례에 따라, 7925G 구축 가이드에 정의된 대로 구성합니다.

Cisco Unified Wireless IP Phone 7925G, 7925G-EX 및 7926G 구축 설명서

올바르게 구성되면 문제가 해결됩니다.

시나리오 3: 클라이언트가 WPA에 대해 구성되었지만 AP가 WPA2에 대해서만 구성되었습니다.

디버그 클라이언트 <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**

시나리오 4: AAA 반환 또는 응답 코드 구문 분석

예상 로그를 수집하기 위해 RUN에 필요한 디버깅:

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

(Cisco Controller) > debug aaa events enable(**aaa 이벤트 디버그 활성화)**

(또는)

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

(Cisco Controller) > debug aaa events enable(**aaa 이벤트 디버그 활성화)**

(Cisco Controller) > debug aaa **errors enable(디버그 aaa 오류 활성화)**

AAA 연결 실패는 트랩이 활성화된 경우 SNMP 트랩을 생성합니다.

디버그 출력 <스니핑됨> 예:

<#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

가능한 이유:

- 사용자 계정 및/또는 암호가 잘못되었습니다.
- 컴퓨터가 도메인의 구성원이 아닙니다. AD 측에서 발급됩니다.
- 인증서 서비스가 제대로 작동하지 않습니다.
- 서버 인증서가 만료되었거나 사용 중이 아닙니다.
- RADIUS가 잘못 구성되었습니다.
- 액세스 키가 잘못 입력되었습니다. 대소문자를 구분하며 SSID도 마찬가지입니다.
- Microsoft 패치를 업데이트합니다.
- EAP 타이머입니다.
- 클라이언트/서버에 잘못된 EAP 방법이 구성되었습니다.
- 클라이언트 인증서가 만료되었거나 사용 중이 아닙니다.

모바일에 대한 AAA 오류 시간 초과 반환(-5)
AAA Server Unreachable(AAA 서버 도달 불가), 클라이언트 deauth

예:

<#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

모바일에 대한 AAA 오류 내부 오류 반환(-6)

특성이 일치하지 않습니다. AAA는 WLC와 이해/호환되지 않는 부정확하거나 부적절한 특성(잘못된 길이)을 전송합니다. WLC는 Deauth 메시지를 보내고 그 뒤에 내부 오류 메시지를 보냅니다. 예: Cisco 버그 ID CSCum83894 AAA Internal Error 및 auth fail with

unknown attributes in access accept.

예:

*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

모바일용 AAA 오류 서버 없음(-7)을 반환합니다.
Radius가 제대로 구성되지 않았거나 지원되지 않는 컨피그레이션을 사용 중입니다.

예:

*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

시나리오 5: 클라이언트가 AP에 연결하지 못함

사용된 디버그:

디버그 클라이언트 <mac addr>

구문 분석할 로그:

BSSID 00:26:cb:94:44:c0(상태 0) ApVapId 1 슬롯 0에서 스테이션에 Assoc 응답 전송

- 슬롯 0 = B/G(2.4) 라디오
- 슬롯 1 = A(5) 라디오
- Assoc Response Status 0 = Success를 전송합니다.

상태 0이 아닌 다른 모든 것은 실패입니다.

공통 연결 응답 상태 코드는 802.11 연결 상태, 802.11 Deauth 이유 코드에서 찾을 수 있습니다.

시나리오 6: 유휴 시간 초과로 인한 클라이언트 연결 해제

사용된 디버그:

디버그 클라이언트 <mac addr>

구문 분석할 로그

AP에서 Idle-Timeout 수신 00:26:cb:94:44:c0, 슬롯 0(STA 00:1e:8c:0f:a4:57)

apfMsDeleteByMscb deleteReason 4, reasonCode 4를 사용하여 삭제할 모바일 예약

1초 내에 모바일 스테이션(callerId: 30)의 삭제 예약

apfMsExpireCallback (apf_ms.c:608) 만료 예정 모바일!

BSSID 00:26:cb:94:44:c0 slot 0(caller apf_ms.c:5094)에서 모바일로 인증 취소 전송

조건

클라이언트에서 수신된 트래픽이 없는 후에 발생합니다.

기본 지속 시간은 300초입니다.

해결 방법

WLC에서 전역 또는 WLC에서 WLANGUI>>Controller>>General 단위로 유휴 시간 제한 증가 **GUI>WLAN>ID>>Advanced**.

시나리오 7: 세션 시간 초과로 인한 클라이언트 연결 해제

사용된 디버그:

디버그 클라이언트 <mac addr>

구문 분석할 로그:

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

조건

예약된 기간(기본값 1800초)에 발생합니다.

WEBAUTH 사용자가 WEBAUTH를 다시 수행하도록 강제합니다.

해결 방법

WLC에서 WLAN당 세션 시간 제한을 늘리거나 **GUI>WLAN>ID>Advanced**비활성화합니다.

시나리오 8: WLAN 변경으로 인한 클라이언트 연결 해제

사용된 디버그:

디버그 클라이언트 <mac addr>

구문 분석할 로그:

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

조건

어떤 방식으로든 WLAN을 수정하려면 WLAN을 비활성화했다가 다시 활성화합니다.

해결 방법

이는 정상적인 동작입니다. WLAN이 변경되면 클라이언트는 연결을 끊고 다시 연결합니다.

시나리오 9: WLC에서 수동 삭제로 인한 클라이언트 연결 해제

사용된 디버그:

디버그 클라이언트 <mac addr>

구문 분석할 로그:

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

조건

GUI에서: 클라이언트 제거

CLI에서: **config client deauthenticate <mac address>**

시나리오 10: 인증 시간 초과로 인한 클라이언트 연결 해제

사용된 디버그:

디버그 클라이언트 <mac addr>

구문 분석할 로그:

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

조건

인증 또는 키 교환 최대 재전송 도달

해결 방법

클라이언트 드라이버, 보안 구성, 인증서 등을 확인/업데이트합니다.

시나리오 11: AP 무선 재설정(전원/채널)으로 인한 클라이언트 연결 해제

사용된 디버그:

디버그 클라이언트 <mac addr>

구문 분석할 로그:

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

조건

AP가 클라이언트를 연결 해제하지만 WLC는 항목을 삭제하지 않습니다.

해결 방법

필요한 동작입니다.

시나리오 12: 802.1X "timeoutEvt"의 Symantec 클라이언트 문제

문제

Symantec 소프트웨어를 실행하는 클라이언트가 메시지 802.1X 타이머와 연결 timeoutEvt. 해제되었습니다. 이 타이머는 스테이션에 대해 만료되었으며 메시지 = M3에 대해 만료되었습니다.

EAP/Eapol 프로세스는 intel/Broadcom 카드에서 사용되는 A/G 라디오와 상관없이 완료되지 않습니다. wep, wpa-psk를 사용하는 경우에는 문제가 없습니다.

조건

WLC 코드는 중요하지 않습니다.

AP - 모든 모델 - 모두 로컬 모드입니다.
wlan 3 - WPA2+802.1X PEAP + mshcapv2
SSID

는 브로드캐스트입니다.

RADIUS 서버 nps 2008.
Symantec 안티바이러스 소프트웨어는 모든 PC에 설치됩니다.

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

영향을 받는 OS - Windows 7 및 xp

영향을 받는 무선 어댑터 - Intel(6205) 및 Broadcom

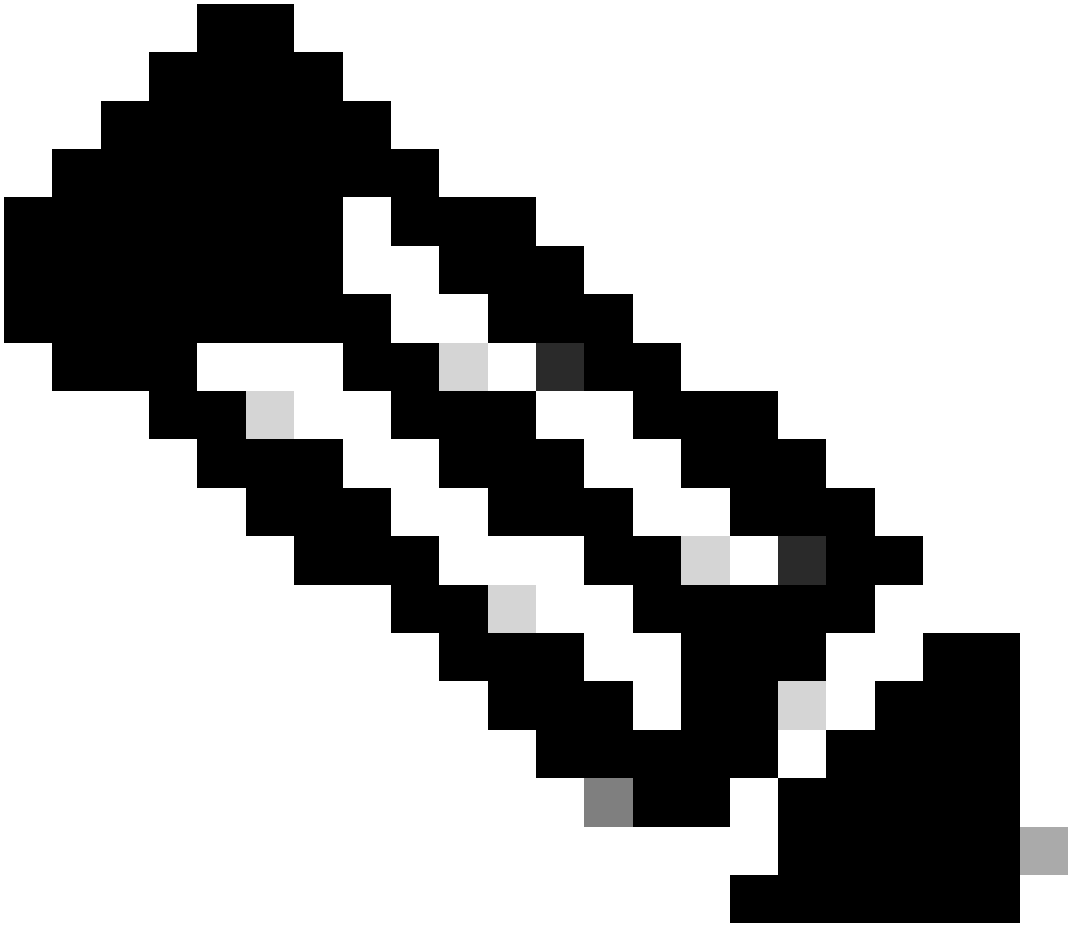
영향을 받는 드라이버/서플리컨트 - 15.2.0.19, 기본 서플리컨트를 사용합니다.

해결 방법

win7 및 xp에서 Symantec 네트워크 보호 및 방화벽을 비활성화합니다. Win 7 및 XP OS의 경우 Symantec 문제입니다.

디버그 출력:

*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



참고: 15.2에는 다음과 같은 신드롬이 있습니다(이전 버전에서도 나타남).
-client AP에서 M1 가져오기
-client가 M2 전송
-클라이언트가 AP에서 M3 가져오기
-client는 M4를 전송하기 전에 새 페어와이즈 키를 추가합니다.

- 클라이언트가 새 키 AP로 암호화된 M4를 전송하고 M4 메시지를 "해독 오류"로 삭제합니다.

- WLC 디버그 클라이언트에서 M3 재전송의 시간 초과를 표시합니다. 분명히 이것은 Intel만의 문제가 아니라 Microsoft와 Symantec의 문제입니다. 해결 방법은 Symantec을 제거하는 것입니다.

- Symantec에서 트리거한 Windows에 있는 버그입니다. EAP 타이머를 조정해도 이 문제는 해결되지 않습니다.

- 이 문제와 관련하여 Cisco TAC는 영향을 받는 사용자를 Symantec 및 Microsoft에 전달합니다.

시나리오 13: 스누프가 켜진 mDNS가 있는 클라이언트에 대해 Air Print Service가 표시되지 않음

mDNS 스누프가 켜져 있으면 클라이언트가 Apple 휴대용 클라이언트 장치에서 AirPrint 서비스를 제공하는 장치를 볼 수 없습니다.

조건

5508 WLC 및 7.6.100.0
mDNS 스누프가 활성화되면 WLC의 서비스 섹션 아래에 AirPrint 서비스를 제공하는 디바이스가 나열됩니다.
각 mDNS 프로필은 WLAN 및 인터페이스에 올바르게 매핑되었습니다.
여전히 클라이언트에서 AirPrint 디바이스를 볼 수 없습니다.

사용된 디버그:

디버그 클라이언트 <mac addr>

디버그 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_

설명:

클라이언트는 또는 문자열_universal._sub._ipps._tcp.local 대신 또_universal._sub._ipp._tcp.local **_ipp._tcp.local** 는 문자열을 _ipp._tcp.local요청합니다.
따라서 추가된 AirPrint 서비스가 작동하지 않습니다. 식별되었으며 매핑할 요청된 서비스 문자열 HP_Photosmart_Printer_1.
WLAN에 매핑된 프로필에 동일한 서비스가 추가되었지만 디바이스에 대해 나열된 서비스는 없었습니다.

도메인 이름이 추가되고 도메인 이름이 추가된 로컬의 dns-sd._udp.YVG 클라이언트 쿼리로 인해 WLC에서 Bonjour 패킷을 처리할 수 없는dns-sd._udp.YVG.local 것으로 확인되었습니다.

지정된 개선 버그가 동일과 관련하여 식별되었습니다. Cisco 버그 ID CSCuj32157입니다.

해결 방법

유일한 해결 방법은 DHCP 옵션 15(도메인 이름)를 비활성화하거나 클라이언트에서 도메인 이름을 제거하는 것이었습니다.

시나리오 14: Apple iOS Client "Unable to Join the Network" due to Disabled Fast SSID Change(Apple iOS 클라이언트가 네트워크에 연결할 수 없음)

조건

대부분의 Apple iOS 디바이스는 동일한 Cisco WLC에서 하나의 WLAN에서 다른 WLAN으로 이동할 때 기본적으로 문제가 fast SSID change disabled발생합니다.

이 설정은 클라이언트가 다른 클라이언트에 연결하려고 시도하면 컨트롤러가 WLAN에서 클라이언트를 인증하지 못하게 합니다.

일반적인 결과는 iOS nable to Join the Network" 디바이스의 "Umessage"입니다.

클라이언트 표시

(jk-2504-116) >**네트워크 요약 표시**

<snip>

고속 SSID 변경 ..... 비활성화됨

사용된 디버그:

<#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

해결 방법

WLC에서 fast-ssid 변경 활성화 GUI > Controller>General.

시나리오 15: 성공적인 클라이언트 LDAP 연결

Secure LDAP는 컨트롤러와 TLS를 사용하는 LDAP 서버 간의 연결을 보호하는 데 도움이 됩니다. 이 기능은 컨트롤러 소프트웨어 버전 7.6 이상에서 지원됩니다.

컨트롤러가 LDAP 서버로 전송할 수 있는 쿼리는 두 가지 유형입니다.

1. 익명

이 유형에서 컨트롤러는 클라이언트가 인증되어야 할 때 LDAP 서버에 인증 요청을 보냅니다. LDAP 서버가 쿼리 결과에 응답합니다. 이 교환 시 클라이언트 사용자 이름/비밀번호를 포함하는 모든 정보가 일반 텍스트로 전송됩니다. LDAP 서버는 바인드 사용자 이름/비밀번호가 추가된 한 누구의 쿼리에도 응답합니다.

2. 인증됨

이 유형에서 컨트롤러는 LDAP 서버로 자신을 인증하는 데 사용하는 사용자 이름과 비밀번호로 구성됩니다. 비밀번호는 MD5 SASL로 암호화되며 인증 프로세스 시 LDAP 서버로 전송됩니다. 이는 LDAP 서버가 인증 요청의 소스를 올바르게 식별하는 데 도움이 됩니다. 그러나 컨트롤러의 ID가 보호되더라도 클라이언트 세부사항은 일반 텍스트로 전송됩니다.

TLS를 통한 LDAP의 진정한 필요성은 클라이언트 인증 데이터와 트랜잭션의 나머지가 암호화되지 않은 상태에서 발생하는 이 두 가지 유형의 보안 취약성 때문입니다.

요구 사항

WLC는 소프트웨어 버전 7.6 이상을 실행합니다.

Microsoft 서버는 LDAP를 사용합니다.

사용된 디버그:

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

시나리오 16: LDAP에서 클라이언트 인증 실패

사용된 디버그:

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

해결 방법

LDAP 서버에서 거부 이유를 확인하십시오.

시나리오 17: WLC에서 잘못 구성된 LDAP로 인한 클라이언트 연결 문제

사용된 디버그:

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

해결 방법

클라이언트/WLC 및 LDAP 서버 전체에서 자격 증명을 확인합니다.

시나리오 18: LDAP 서버에 연결할 수 없을 때 클라이언트 연결 문제

사용된 디버그:

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

해결 방법

WLC 및 LDAP 서버 네트워크 연결 문제를 확인 합니다.

시나리오 19: 스티키 로밍 구성 누락으로 인한 Apple 클라이언트 로밍 문제

조건

AIR-CT5508-K9 / 7.4.100.0

Apple 장치는 다음을 사용하는 무선 네트워크에서 연결이 끊어집니다.

- WPA2 정책
- WPA2 암호화 AES
- 인증 802.1X 활성화됨

Cisco ISE의 인증 및 권한 부여.

Apple 디바이스는 브로드캐스트 SSID에서 주기적으로 연결을 끊습니다. 예를 들어, 동일한 위치에 있는 다른 전화기가 연결된 채로 있는 동안 끊어지는 iPhone을 들 수 있습니다. 따라서 이는 무작위(시간 및 전화)로 발생합니다.

문제가 없는 랩톱 클라이언트. 동일한 SSID에 연결됩니다.

이 문제는 로밍 및 대기 모드가 없는 정상 작동 중에 발생합니다.

WLAN에서 문제를 일으킬 수 있는 모든 가능한 설정을 이미 제거했습니다(aironet ext).

사용된 디버그:

디버그 클라이언트 <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.
```

해결 방법

SKC(Sticky Key Caching) 클라이언트가 있고 WLC 코드 7.2 이상이 있는 고객을 위해 지금 할 수 있는 일은 SKC에 대한 로밍 지원을 활성화하는 것입니다. 기본적으로 WLC는 OKC(Opportunistic Key Caching)만 지원합니다. 클라이언트가 각 AP에서 생성한 이전 PMKID를 사용할 수 있도록 하려면 WLC CLI에서 활성화해야 합니다.

config wlan security wpa2 cache sticky enable <1>

SKC의 특성상 초기 로밍이 개선되지는 않지만, 동일한 AP에 대한 후속 로밍이 개선됩니다(장부에 의해 최대 8개). AP가 8개인 복도를 따라 산책을 한다고 상상해 보십시오. 첫 번째 연습은 각 AP에서 약 1-2초 지연의 전체 연결로 구성됩니다. 끝에 도달한 후 뒤로 이동하면 클라이언트는 동일한 연결로 다시 이동할 때 8개의 고유한 PMKID를 제공합니다.

SKC 지원이 활성화된 경우 AP는 전체 인증을 거치지 않아도 됩니다. 이렇게 하면 지연 시간이 제거되고 클라이언트가 연결된 상태로 유지됩니다.

시나리오 20: CCKM으로 FSR(Fast-Secure-Roaming) 확인

802.11 WLAN Roaming 및 CUWN의 Fast-Secure Roaming

사용된 디버그:

디버그 클라이언트 <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

그림과 같이 EAP 인증 프레임 및 더 많은 4-Way 핸드셰이크를 방지하기 위해 빠른 보안 로밍이 수행됩니다. 새 암호화 키가 아직 파생되지만 CCKM 협상 체계를 기반으로 하기 때문입니다. 이 작업은 로밍 재연결 프레임 및 클라이언트와 WLC에서 이전에 캐시한 정보로 완료됩니다.

시나리오 21: WPA2 PMKID 캐시로 FSR(Fast-Secure-Roaming) 확인

사용된 디버그:

디버그 클라이언트 <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

시나리오 22: 사전 대응적 키 캐시로 빠른 보안 로밍 확인

사용된 디버그:

디버그 클라이언트 <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 comp

디버그를 시작할 때 표시된 것처럼 PMKID는 클라이언트로부터 재연결 요청을 받은 후에 계산되어야 합니다. 이는 PMKID를 검증하고 캐시된 PMK가 WPA2 4-Way 핸드셰이크와 함께 사용되어 암호화 키를 파생시키고 빠른 보안 로밍을 완료하는지 확인하기 위해 필요합니다. 디버그의 CCKM 항목을 혼동하지 마십시오. 앞서 설명한 대로 CCKM을 수행하기 위해 사용되지 않지만 PKC/OKC가 사용됩니다. 여기서 CCKM은 PMKID를 계산하기 위해 값을 처리하는 함수의 이름과 같이 해당 출력에 대해 WLC에서 사용하는 이름입니다.

시나리오 23: 802.11r로 FSR(Fast-Secure-Roaming) 확인

사용된 디버그:

디버그 클라이언트 <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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.