Use esta página para problemas comuns de conexões sem fio

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Brief Estado do PEM na saída do comando show client

Cenário 1: Senha configurada incorretamente para autenticação PSK WPA/WPA2 no cliente

- Conclusão

Cenário 2: O monofone do telefone sem fio (792x/9971) não se associa à "área de serviço de saídas" sem fio

- Topologia
- Detalhes do problema
- Conclusão

Cenário 3: Cliente configurado para WPA, mas AP configurado somente para WPA2

Cenário 4: Analisar códigos de retorno ou de resposta AAA

Cenário 5: Cliente não consegue se associar ao AP

Cenário 6: Desassociação de Cliente Devido a Tempo Limite de Ociosidade

- Condições
- Solução

Cenário 7: Desassociação de Cliente Devido a Tempo Limite de Sessão

- Condições
- Solução

Cenário 8: Desassociação de Cliente Devido a Alterações de WLAN

- Condições
- Solução

Cenário 9: Desassociação de Cliente Devido à Exclusão Manual do WLC

- Condições

Cenário 10: Desassociação de Cliente Devido a Tempo Limite de Autenticação

- Condições
- Solução

Cenário 11: Desassociação de Cliente Devido à Redefinição de Rádio do AP (Alimentação/Canal)

- Condições
- Solução

Cenário 12: Problemas do cliente Symantec com "timeoutEvt" 802.1X

- Problema
- Condições
- Correção/Solução alternativa

Cenário 13: O Air Print Service não aparece para clientes com mDNSque o snoop está ativado

- Condições

Solução

Cenário 14: Cliente Apple iOS "Não é possível ingressar na rede" devido à rápida alteração de SSID desativada

Condições

Solução

Cenário 15: Associação LDAP de Cliente Bem-sucedida

Cenário 16: Falha de autenticação do cliente no LDAP

Solução

Cenário 17: Problemas de Associação do Cliente Devido a LDAP Configurado Incorretamente no WLC

Solução

Cenário 18: Problemas de associação do cliente quando o servidor LDAP está inacessível

Solução

Cenário 19: Problemas de roaming do cliente Apple devido à configuração de roaming sticky ausente

Condições

Solução

Cenário 20: Verificar Fast-Secure-Roaming (FSR) com CCKM

Cenário 21: Verificar Fast-Secure-Roaming (FSR) com WPA2 PMKID Cache

Cenário 22: Verificar o roaming rápido e seguro com cache de chave proativa

Cenário 23: Verificar Fast-Secure-Roaming (FSR) com 802.11r

Introdução

Este documento descreve uma folha de ajuda que analisa as depurações (geralmente, debug client <mac address>) para problemas sem fio comuns.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas em todos os controladores AireOS.

- Controladores - 440x, 5508, 5520, 75xx, 85xx, 2504, 3504 e vWLC, bem como WISMs.
- Embora muitos conceitos sejam idênticos em controladores e switches de acesso convergente IOS® XE, este documento não se aplica a eles como saídas e depurações são radicalmente diferentes.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Brief Estado do PEM na saída do comando show client

Para analisar o show client e as depurações, primeiro é necessário entender alguns estados do Power Entry Module (PEM) e APF.

- START — Status inicial da nova entrada do cliente.
- AUTHCHECK—A WLAN tem uma política de autenticação L2 para aplicar.
- 8021X_REQD — O cliente deve concluir a autenticação 802.1x.
- L2AUTHCOMPLETE — O cliente concluiu com êxito a política L2. O processo agora pode prosseguir para as políticas de L3 (aprendizagem de endereço, autenticação da Web etc.). O controlador envia o anúncio de mobilidade para aprender informações de L3 de outros controladores se este for um cliente móvel no mesmo grupo de mobilidade.
- WEP_REQD — O cliente deve concluir a autenticação WEP.
- DHCP_REQD—A controladora aprende o endereço L3 do cliente, que é feito por solicitação ARP, solicitação ou renovação DHCP ou por informações aprendidas de outras controladoras no grupo de mobilidade. Se DHCP necessário estiver marcado na WLAN, somente as informações de DHCP ou mobilidade serão usadas.
- WEBAUTH_REQD — O cliente deve concluir a autenticação da Web. (política de L3)
- CENTRAL_WEBAUTH_REQD — O cliente deve concluir o login no CWA. A WLC espera para receber o CoA.
- EXECUTAR—O cliente concluiu com êxito as políticas L2 e L3 necessárias e agora pode transmitir o tráfego para a rede.

Os cenários fornecidos mostram as linhas de depuração principais para configurações incorretas comuns em configurações sem fio, que destacam os parâmetros principais em negrito.

Cenário 1: Senha configurada incorretamente para autenticação PSK WPA/WPA2 no 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 análise 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

Conclusão

Embora timeoutEvt para a chave M2 também possa ser devido a erros de driver/NIC, um dos problemas mais comuns é um usuário que insere credenciais incorretas para a senha PSK (caracteres especiais/com diferenciação de maiúsculas e minúsculas perdidos e assim por diante) e é incapaz de se conectar.

Cenário 2: O monofone do telefone sem fio (792x/9971) não se associa à "área de serviço de saídas" sem fio

Referência: Falta de associação dos aparelhos 7925G ao AP - Falha na chamada: a política de QOS do TSPEC não corresponde

Topologia

WLAN com telefones IP sem fio unificados da Cisco.

Detalhes do problema

AIR-CT5508-50-K9 // o firmware atualizado para telefones e controlador sem fio não aceita registros de telefone.

Depurações e logs:

<#root>

```
apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Association received from mobile on AP 3x:xx:cx:9

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx 0.0.0.0 START (0) Changing IPv4 ACL 'none' (ACL
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx 0.0.0.0 START (0) Changing IPv6 ACL 'none' (ACL
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying site-specific Local Bridging override
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Applying Local Bridging Interface Policy for st
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx processSsidIE  statusCode is 0 and status is 0
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx processSsidIE  ssid_done_flag is 0 finish_flag
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx STA - rates (4): 130 132 139 150 0 0 0 0 0 0 0
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx suppRates  statusCode is 0 and gotSuppRatesElem
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx STA - rates (12): 130 132 139 150 12 18 24 36 4
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx extSuppRates  statusCode is 0 and gotExtSuppRat
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Processing RSN IE type 48, length 22 for mobile
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx CCKM: Mobile is using CCKM
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Received RSN IE with 0 PMKIDs from mobile 1x:xx
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Setting active key cache index 8 ---> 8
*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx unsetting PmkIdValidatedByAp
```

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Sending Assoc Response to station on BSSID 3x:x

*apfMsConnTask_1: xx xx xx:50:xx.xxx: 1x:xx:1x:xx:xx:xx Scheduling deletion of Mobile Station: (caller

VoIP Call Failure: '1x:xx:1x:xx:xx:xx' client, detected by 'xx-xx-xx' AP on radio type '802.11b/g'. Rea

.

***Means platinum QoS was not configured on WLAN

1x:xx PM

Client Excluded: MACAddress:1x:xx:1x:xx:xx:xx Base Radio MAC :3x:xx:cx:9x:x0:x0 Slot: 1 User Name: dwpv

Conclusão

A depuração na WLC mostra que a associação do 7925G falha quando o AP retorna um código de status de associação de 201.

Isso se deve a uma solicitação de Especificação de Tráfego (TSPEC) do receptor de telefone devido à configuração da WLAN. A WLAN 7925G que tenta se conectar é configurada com um perfil de QoS Silver (UP 0,3), em vez de Platinum (UP 6,7), conforme necessário. Isso leva a uma incompatibilidade de TSPEC para tráfego de voz/troca de quadro de ação do monofone pela WLAN e, por fim, uma rejeição do AP.

Crie uma nova WLAN com um perfil de QoS Platinum especificamente para os aparelhos 7925G e configure de acordo com as melhores práticas estabelecidas e conforme definido no Guia de Implantação 7925G:

Guia de implantação do telefone IP Cisco Unified Wireless 7925G, 7925G-EX e 7926G

Depois de configurado corretamente, o problema é resolvido.

Cenário 3: Cliente configurado para WPA, mas AP configurado somente 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**

Cenário 4: Analisar códigos de retorno ou de resposta AAA

Depurações necessárias a serem executadas para coletar os logs esperados:

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

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

(OU)

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

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

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

A falha de conectividade AAA gera uma interceptação SNMP, se as interceptações estiverem habilitadas.

Exemplo de saída de depuração <snipped>:

<#root>

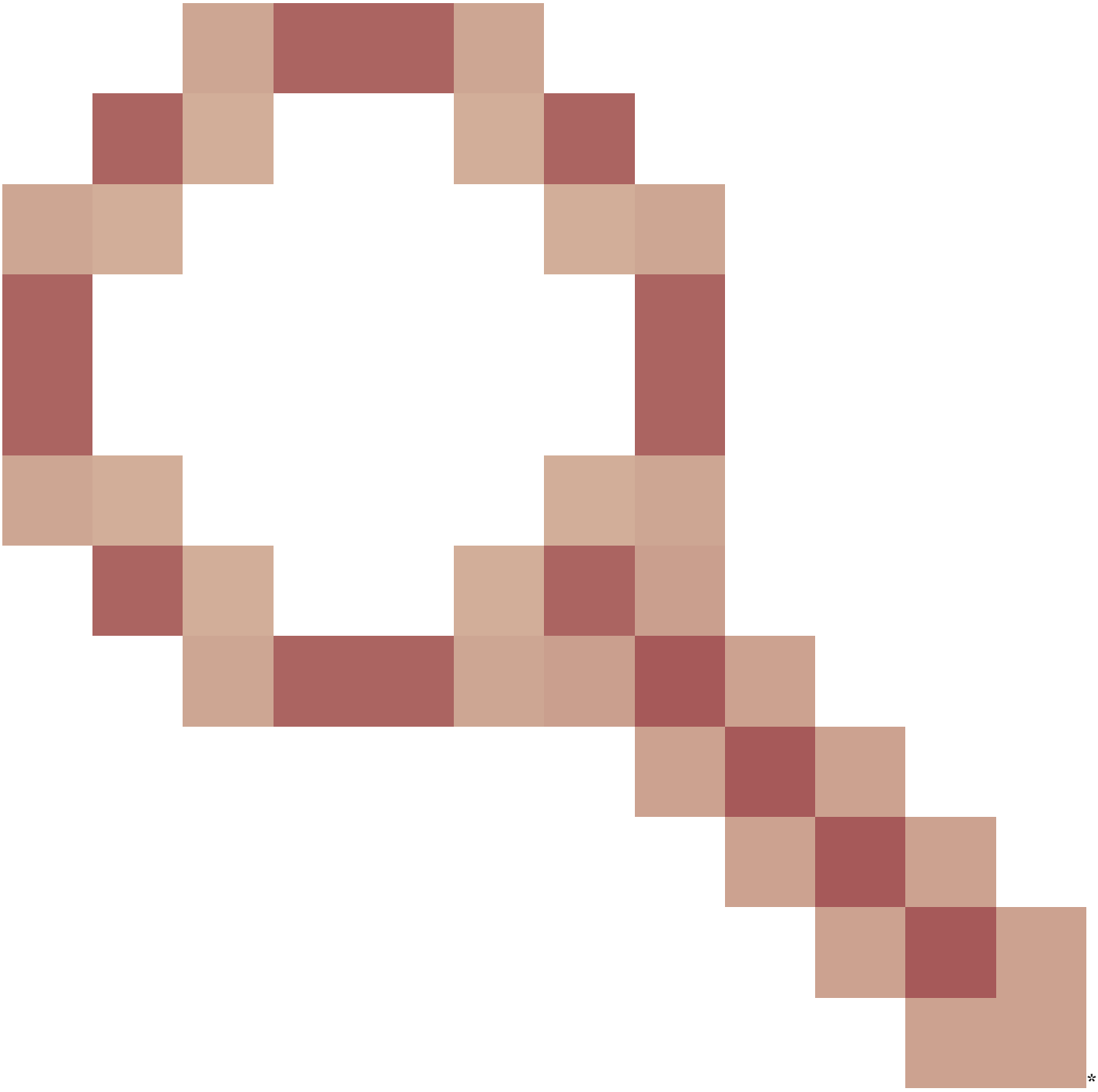
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 Invalid RADIUS message authenticator for mobile 70:f1:a1:69:7b:e7
*radiusTransportThread: Mar 26 17:54:58.054: 70:f1:a1:69:7b:e7 RADIUS message verification failed from server 10.50.0.74 with id=213. Possible secret
*radiusTransportThread: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

Motivos possíveis:

- Conta de usuário e/ou senha inválida.
- O computador não é membro do domínio, problema no lado do AD.

    - Os serviços de certificado não funcionam corretamente.
- O certificado do servidor expirou ou não está em uso.
- RADIUS configurado incorretamente.
- Chave de acesso inserida incorretamente - faz distinção entre maiúsculas e minúsculas (assim como o SSID).
- Atualize os patches da Microsoft.
- Temporizadores EAP.
- Método EAP incorreto configurado no cliente/servidor.
- O certificado do cliente expirou ou não está em uso.

Timeout de Erro AAA de Retorno (-5) para Mobile

Servidor AAA Inalcançável, seguido pela reautenticação do cliente.

Exemplo:

<#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

Erro interno de AAA de retorno (-6) para celular

Incompatibilidade de atributo. AAA envia atributo incorreto/inadequado (comprimento incorreto) que não é compreendido/compatível com WLC. A WLC envia uma mensagem de Deauth, seguida por uma mensagem de erro interno. Exemplo: o bug da Cisco ID CSCum83894 AAA Internal Error e auth falham com atributos desconhecidos no access accept.

Exemplo:

*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

Retorna um erro AAA no servidor (-7) para celular.

O Radius não está configurado corretamente e/ou não há suporte para a configuração em uso.

Exemplo:

*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

Cenário 5: Cliente não consegue se associar ao AP

Depuração usada:

debug client <mac addr>

Logs a analisar:

Enviando Resposta Assoc para estação em BSSID 00:26:cb:94:44:c0 (status 0) ApVapId 1 Slot 0

- Slot 0 = Rádio B/G(2.4)
- Slot 1 = Rádio A(5)
- Envia Status de Resposta de Associação 0 = Êxito

Qualquer coisa diferente de Status 0 é Falha.

Os códigos de status de Resposta de associação comuns podem ser encontrados em: Status de associação 802.11, Códigos de razão de desautorização 802.11

Cenário 6: Desassociação de Cliente Devido a Tempo Limite de Ociosidade

Depuração usada:

debug client <mac addr>

Logs para analisar

Tempo limite ocioso recebido do AP 00:26:cb:94:44:c0, slot 0 para STA 00:1e:8c:0f:a4:57

apfMsDeleteByMscb Agendamento móvel para exclusão com deleteReason 4, reasonCode 4

Agendamento da exclusão da Estação Móvel: (callerId: 30) em 1 segundo

apfMsExpireCallback (apf_ms.c:608) Expirando no Celular!

Enviado Desautenticar para celular no BSSID 00:26:cb:94:44:c0 slot 0(chamador apf_ms.c:5094)

Condições

Ocorre depois que nenhum tráfego é recebido do cliente.

A duração padrão é de 300 segundos.

Solução

Aumentar o tempo limite de ociosidade globalmente a partir da WLC GUI>>Controller>>General ou por WLAN da WLC **GUI>WLAN>ID>>Advanced**.

Cenário 7: Desassociação de Cliente Devido a Tempo Limite de Sessão

Depuração usada:

debug client <mac addr>

Logs a analisar:

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

Condições

Ocorre na duração agendada (padrão de 1800 segundos).

Ele força o usuário WEBAUTH a WEBAUTH novamente.

Solução

Aumente ou desabilite o tempo limite de sessão por WLAN do WLC **GUI>WLAN>ID>Advanced**.

Cenário 8: Desassociação de Cliente Devido a Alterações de WLAN

Depuração usada:

debug client <mac addr>

Log a ser analisado:

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

Condições

Modificar uma WLAN de qualquer forma desativa e reativa a WLAN.

Solução

Este é um comportamento esperado. Quando são feitas alterações na WLAN, os clientes desassociam e reassociam.

Cenário 9: Desassociação de Cliente Devido à Exclusão Manual do WLC

Depuração usada:

debug client <mac addr>

Log a ser analisado:

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

Condições

Da GUI: Remover cliente

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

Cenário 10: Desassociação de Cliente Devido a Tempo Limite de Autenticação

Depuração usada:

debug client <mac addr>

Log a ser analisado:

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

Condições

Máximo de retransmissões de Autenticação ou Troca de Chaves atingido.

Solução

Verificar/atualizar driver do cliente, configuração de segurança, certificados e assim por diante.

Cenário 11: Desassociação de Cliente Devido à Redefinição de Rádio do AP (Alimentação/Canal)

Depuração usada:

debug client <mac addr>

Log a ser analisado:

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

Condições

O AP desassocia os clientes, mas a WLC não exclui a entrada.

Solução

Comportamento esperado.

Cenário 12: Problemas do cliente Symantec com "timeoutEvt" 802.1X

Problema

Os clientes que executam o software Symantec se desassociam com a mensagem 802.1X timeoutEvt. Timer expirado para a estação e para a mensagem = M3

O processo EAP/Eapol não é concluído, independentemente do rádio A/G usado na placa intel/Broadcom. Sem problemas quando é usado wep, wpa-psk.

Condições

O código da WLC não importa.

APs - todos os modelos - tudo no modo local.
wlan 3 - WPA2+802.1X PEAP + mshcapv2
O SSID é transmitido.

Servidor RADIUS nps 2008.
O software antivírus da Symantec está instalado em todos os computadores.

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

SO afetado - Windows 7 e xp

Adaptador sem fio afetado - Intel(6205) e Broadcom

Driver/solicitante afetado - 15.2.0.19, use o solicitante nativo.

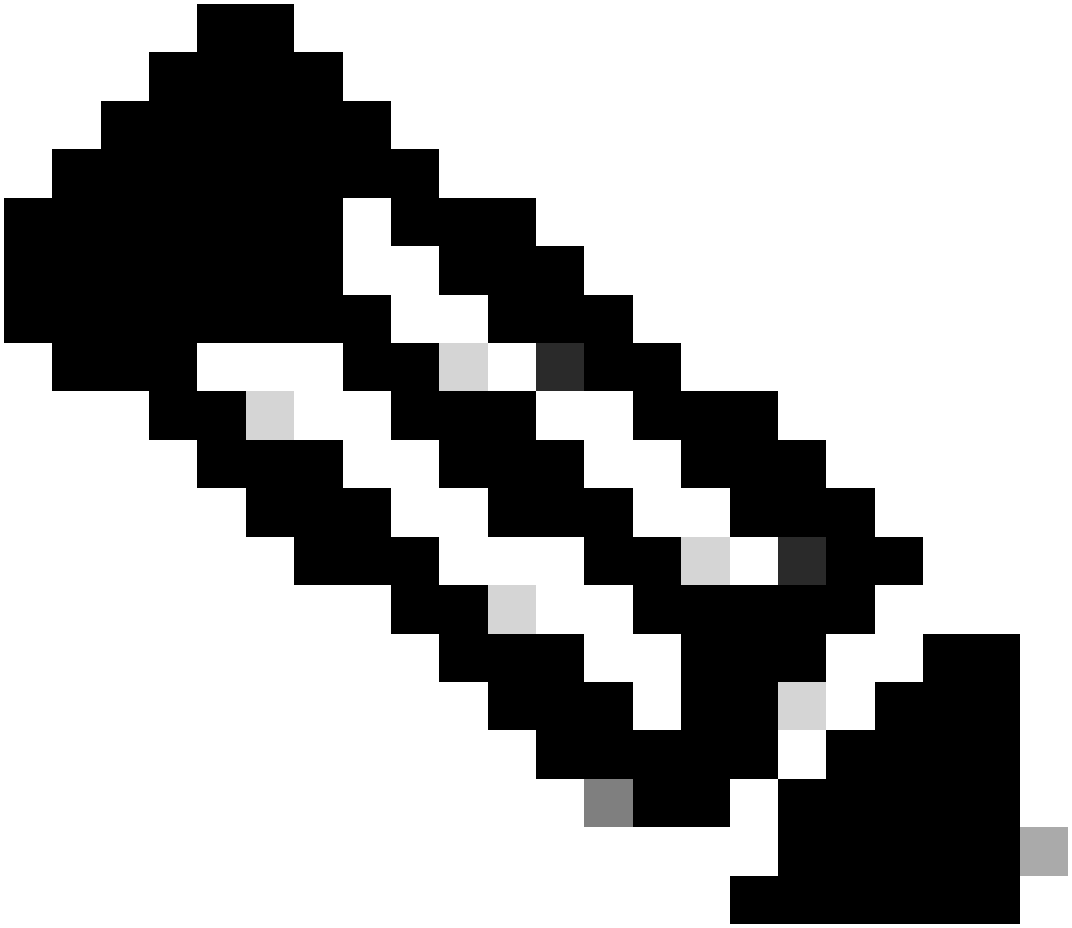
Correção/Solução alternativa

Desabilite o Symantec Network Protection e o Firewall no win7 e xp. É um problema da Symantec com os sistemas operacionais Win 7 e XP.

Saída de depurações:

*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: Há uma síndrome em 15.2 (também vista em versões anteriores) que é assim:
-o cliente obtém M1 do AP
-o cliente envia M2
-o cliente obtém M3 do AP
-client usa a nova chave emparelhada antes de enviar M4

- O cliente transmite o M4 criptografado com a nova chave AP, descarta a mensagem M4 como um "erro de descriptografia".

- O cliente de depuração WLC mostra que você atingiu o tempo limite em retransmissões M3. Obviamente, esse é um problema entre a Microsoft e a Symantec, não específico da Intel. A solução é remover a Symantec.

- Este é realmente um bug que provavelmente está no Windows, disparado pela Symantec. O ajuste do temporizador EAP não corrige esse problema.

- Em relação a esse problema, o Cisco TAC encaminha os usuários afetados para a Symantec e a Microsoft.

Cenário 13: o Air Print Service não aparece para clientes com mDNS que o snoop está ativado

O cliente não pode ver os dispositivos que fornecem o serviço AirPrint em dispositivos de cliente portáteis Apple quando o snoop mDNS está ativado.

Condições

5508 WLC com 7.6.100.0.
Com o snoop mDNS habilitado, você tem os dispositivos que fornecem serviços AirPrint listados na seção de serviços na WLC.
O respectivo perfil mDNS foi mapeado corretamente para a WLAN e a interface.
Ainda não é possível ver os dispositivos AirPrint no cliente.

Depuração usada:

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_

Explicação:

O cliente solicitaria _universal._sub._ipps._tcp.local ou _universal._sub._ipp._tcp.local em vez de **_ipp._tcp.local** ou _ipp._tcp.local string.
Portanto, o serviço AirPrint adicionado não funcionaria. Ele foi identificado e a cadeia de serviço solicitada será mapeada para

HP_Photosmart_Printer_1.

O mesmo serviço foi adicionado ao perfil mapeado para a WLAN e ainda não havia nenhum serviço listado para o dispositivo.

Foi descoberto que devido ao nome de domínio anexado e à consulta do cliente para dns-sd._udp.YVG local com o nome de domínio anexado, o WLC não pôde processar o pacote Bonjour, pois dns-sd._udp.YVG.local não existe no banco de dados.

Identificado o bug de aprimoramento dado com relação ao mesmo - ID de bug Cisco CSCuj32157.

Solução

A única solução alternativa era desabilitar a opção de DHCP 15 (Nome do domínio) ou remover o Nome do domínio do cliente.

Cenário 14: Cliente Apple iOS "Não é possível ingressar na rede" devido à rápida alteração de SSID desativada

Condições

A maioria dos dispositivos Apple iOS tem problemas para se mover de uma WLAN para outra na mesma WLC da Cisco com o fast SSID change disabledpadrão.

A configuração faz com que o controlador desautentique o cliente da WLAN que existe quando o cliente tenta se associar a outro.

O resultado típico é uma "nable to Join the Network" Umessage" no dispositivo iOS.

Mostrar cliente

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

<snip>

..... de alteração rápida de SSID Desabilitado

Depuração usada:

<#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
```

Solução

Habilitar alteração de ssid rápido do WLC GUI > Controller>General.

Cenário 15: Associação LDAP de Cliente Bem-sucedida

O LDAP seguro ajuda a proteger a conexão entre o controlador e o servidor LDAP que usa TLS. Este recurso é suportado com a versão 7.6 do software do controlador e superior.

Há dois tipos de consultas que podem ser enviadas pelo controlador ao servidor LDAP:

1. Anônimo

Nesse tipo, o controlador envia uma solicitação de autenticação ao servidor LDAP quando um cliente precisa ser autenticado. O servidor LDAP responde com o resultado da consulta. No momento dessa troca, todas as informações que incluem o nome de usuário/senha do cliente são enviadas em texto claro. O servidor LDAP responde a uma consulta de qualquer pessoa, desde que o nome de usuário/senha de vinculação seja adicionado.

2. Autenticado

Nesse tipo, o controlador é configurado com um nome de usuário e uma senha que ele usa para se autenticar no servidor LDAP. A senha é criptografada com MD5 SASL e é enviada ao servidor LDAP no momento do processo de autenticação. Isso ajuda o servidor LDAP a identificar corretamente a origem das solicitações de autenticação. No entanto, mesmo que a identidade do controlador esteja protegida, os detalhes do cliente são enviados em texto claro.

A necessidade real de LDAP sobre TLS veio devido à vulnerabilidade de segurança apresentada por ambos os tipos em que os dados de autenticação do cliente e o resto da transação acontecem sem criptografia.

Requisitos

A WLC executa a versão de software 7.6 e posterior.

O servidor Microsoft usa LDAP.

Depuração usada:

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
```

Cenário 16: Falha de autenticação do cliente no LDAP

Depuração usada:

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

Solução

Verifique o servidor LDAP para motivos de rejeição.

Cenário 17: Problemas de Associação do Cliente Devido a LDAP Configurado Incorretamente no WLC

Depuração usada:

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

Solução

Verifique as credenciais no cliente/WLC e no servidor LDAP.

Cenário 18: Problemas de associação do cliente quando o servidor LDAP está inacessível

Depuração usada:

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

Solução

Verifique os problemas de conectividade de rede do servidor WLC e LDAP.

Cenário 19: Problemas de roaming do cliente Apple devido à configuração de roaming sticky ausente

Condições

AIR-CT5508-K9/7.4.100.0

Os dispositivos Apple se desconectam de uma rede sem fio que usa:

- Política WPA2
- Criptografia WPA2 AES
- Autenticação 802.1X Habilitada

Autenticação e autorização pelo Cisco ISE.

Periodicamente, os dispositivos Apple se desconectam do SSID de broadcast. Um exemplo é um iPhone que cai enquanto outro telefone no mesmo local permanece conectado. Portanto, isso ocorre aleatoriamente (hora e telefone).

Clientes laptop sem problemas. Eles se conectam ao mesmo SSID.

Esse problema ocorre durante a operação normal, sem roaming e sem modo de espera.

A WLAN já removeu todas as configurações possíveis que poderiam causar problemas (aironet ext).

Depuração usada:

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.
```

Solução

O que você pode fazer agora para clientes que têm clientes Sticky Key Caching (SKC) e também têm o código WLC 7.2 e superior, é ativar o suporte de roam para SKC. Por padrão, a WLC suporta apenas o OKC (Opportunistic Key Caching). Para permitir que o cliente use seus PMKIDs antigos que ele gerou em cada AP, você deve habilitá-lo pela CLI da WLC.

config wlan security wpa wpa2 cache sticky enable <1>

Lembre-se de que isso não melhora os roams iniciais devido à natureza do SKC; no entanto, ele melhora os roams subsequentes para os mesmos APs (até 8 pelo livro). Imagine uma caminhada por um corredor com 8 APs. O primeiro passo a passo consiste em associações completas em cada AP com um atraso de cerca de 1 a 2 segundos. Quando você chega à extremidade e volta, o cliente apresenta 8 PMKIDs exclusivos conforme ele volta para as mesmas associações.

Os APs não precisam passar por uma autenticação completa se o suporte a SKC estiver habilitado. Isso remove o atraso e o cliente parece permanecer conectado.

Cenário 20: Verificar Fast-Secure-Roaming (FSR) com CCKM

802.11 Roaming de WLAN e Roaming Rápido Seguro no CUWN

Depuração usada:

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 mostrado, o roaming rápido e seguro é executado para evitar os quadros de autenticação EAP e ainda mais handshakes 4-Way, porque as

novas chaves de criptografia ainda são derivadas, mas com base no esquema de negociação CCKM. Isso é concluído com os quadros de reassociação de roaming e as informações anteriormente armazenadas em cache pelo cliente e pela WLC**.**

Cenário 21: Verificar Fast-Secure-Roaming (FSR) com WPA2 PMKID Cache

Depuração usada:

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

Cenário 22: Verificar o roaming rápido e seguro com cache de chave proativa

Depuração usada:

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 mostrado no início das depurações, o PMKID deve ser computado após o recebimento da Solicitação de Reassociação do cliente. Isso é necessário para validar o PMKID e confirmar se o PMK em cache é usado com o handshake de 4 vias WPA2 para derivar as chaves de criptografia e concluir o roaming rápido e seguro. Não confunda as entradas CCKM nas depurações; isso não é usado para executar o CCKM, mas o PKC/OKC, como explicado anteriormente. Aqui, CCKM é simplesmente um nome usado pela WLC para essas saídas, como o nome de uma função que manipula os valores para computar o PMKID.

Cenário 23: Verificar Fast-Secure-Roaming (FSR) com 802.11r

Depuração usada:

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

.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.