# Solucionar problemas de COS AP

## Contenido



## Introducción

Este documento describe algunas de las herramientas de troubleshooting disponibles para los AP de Cheatah OS (también conocidos como AP COS).

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

Este documento se centra en los AP COS como los modelos de AP de las series 2800, 3800, 1560 y 4800, así como los nuevos AP 11ax Catalyst 91xx.

Este documento se centra en muchas funciones disponibles en AireOS 8.8 y versiones posteriores. Y también Cisco IOS® XE 16.2.2s y versiones posteriores.

Puede haber comentarios sobre la disponibilidad de ciertas funciones en versiones anteriores.

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.

# Capturar seguimientos de paquetes (seguimientos de sabueso)

## PCAP cableado en puerto AP

Es posible (a partir de 8.7 con el filtro disponible en 8.8) tomar un pcap en el puerto Ethernet AP. Puede mostrar el resultado en vivo en la CLI (solo con detalles resumidos de paquetes) o guardarlo como una pcap completa en la flash del AP.

El pcap cableado captura todo en el lado de Ethernet (tanto Rx/Tx) y el punto de toque dentro del AP es inmediatamente antes de que el paquete se ponga en el cable.

Sin embargo, solo captura el tráfico del plano de CPU del AP, lo que significa tráfico hacia y desde el AP (DHCP del AP, túnel de control capwap del AP, ...) y no muestra el tráfico del cliente.

Tenga en cuenta que el tamaño es muy limitado (límite de tamaño máximo de 5 MB), por lo que puede ser necesario configurar filtros para capturar solo el tráfico que le interese.

Asegúrese de detener la captura de tráfico con "no debug traffic wired ip capture" o simplemente "undebug all" antes de intentar copiarla (de lo contrario, la copia no termina ya que los paquetes aún se escriben).

### Procedimiento

Paso 1. Inicie el pcap; seleccione el tipo de tráfico con "debug traffic wired ip capture":

<#root>

```
AP70DB.98E1.3DEC#debug traffic wired ip capture
% Writing packets to "/tmp/pcap/
```

**AP70DB.98E1.3DEC_capture.pcap0"**

```
AP70DB.98E1.3DEC#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
```

Paso 2. Espere a que el tráfico fluya y luego detenga la captura con el comando "no debug traffic wired ip capture" o simplemente "undebug all":

```
AP70DB.98E1.3DEC#no debug traffic wired ip capture
```

Paso 3. Copie el archivo en el servidor tftp/scp:

<#root>

```
AP70DB.98E1.3DEC#copy pcap
```

**AP70DB.98E1.3DEC_capture.pcap0**

```
 tftp 192.168.1.100
##################################################################################################################
AP70DB.98E1.3DEC#
```

Paso 4. Ahora puede abrir el archivo en wireshark. El archivo es pcap0. Cambie a pcap para que se asocie automáticamente con wireshark.

**Opciones del Comando**

El comando debug traffic wired tiene varias opciones que pueden ayudarlo a capturar tráfico específico:

```
APC4F7.D54C.E77C#debug traffic wired
  <0-3>   wired debug interface number
  filter  filter packets with tcpdump  filter string
  ip      Enable wired ip traffic dump
  tcp     Enable wired tcp traffic dump
  udp     Enable wired udp traffic dum
```

Puede agregar "verbose" al final del comando debug para ver el volcado hexadecimal del paquete. Tenga en cuenta que esto puede saturar su sesión CLI muy rápidamente si su filtro no es lo suficientemente estrecho.

**PCAP con cables mediante el uso de filtro**

El formato del filtro corresponde con el formato del filtro de captura tcpdump.

| | **Ejemplo de filtro** | **Descripción** |
|---|---|---|
| Anfitrión | "host 192.168.2.5" | Esto filtra la captura de paquetes para reunir solamente los paquetes que van o vienen del host 192.168.2.5. |
| | "src host 192.168.2.5" | Esto filtra la captura de paquetes para reunir solamente paquetes que provienen de 192.168.2.5. |
| | "dst host 192.168.2.5" | Esto filtra la captura de paquetes para reunir solamente los paquetes que van a 192.168.2.5. |

| | | |
|---|---|---|
| Puerto | â€œport 443â€ | Esto filtra la captura de paquetes para reunir solamente paquetes con un origen o destino del puerto 443. |
| | "src port 1055" | Esto captura el tráfico que se origina en el puerto 1055. |
| | "dst port 443" | Esto captura el tráfico destinado al puerto 443. |

Aquí hay un ejemplo donde la salida se muestra en la consola pero también se filtra para ver solamente los paquetes de datos CAPWAP:

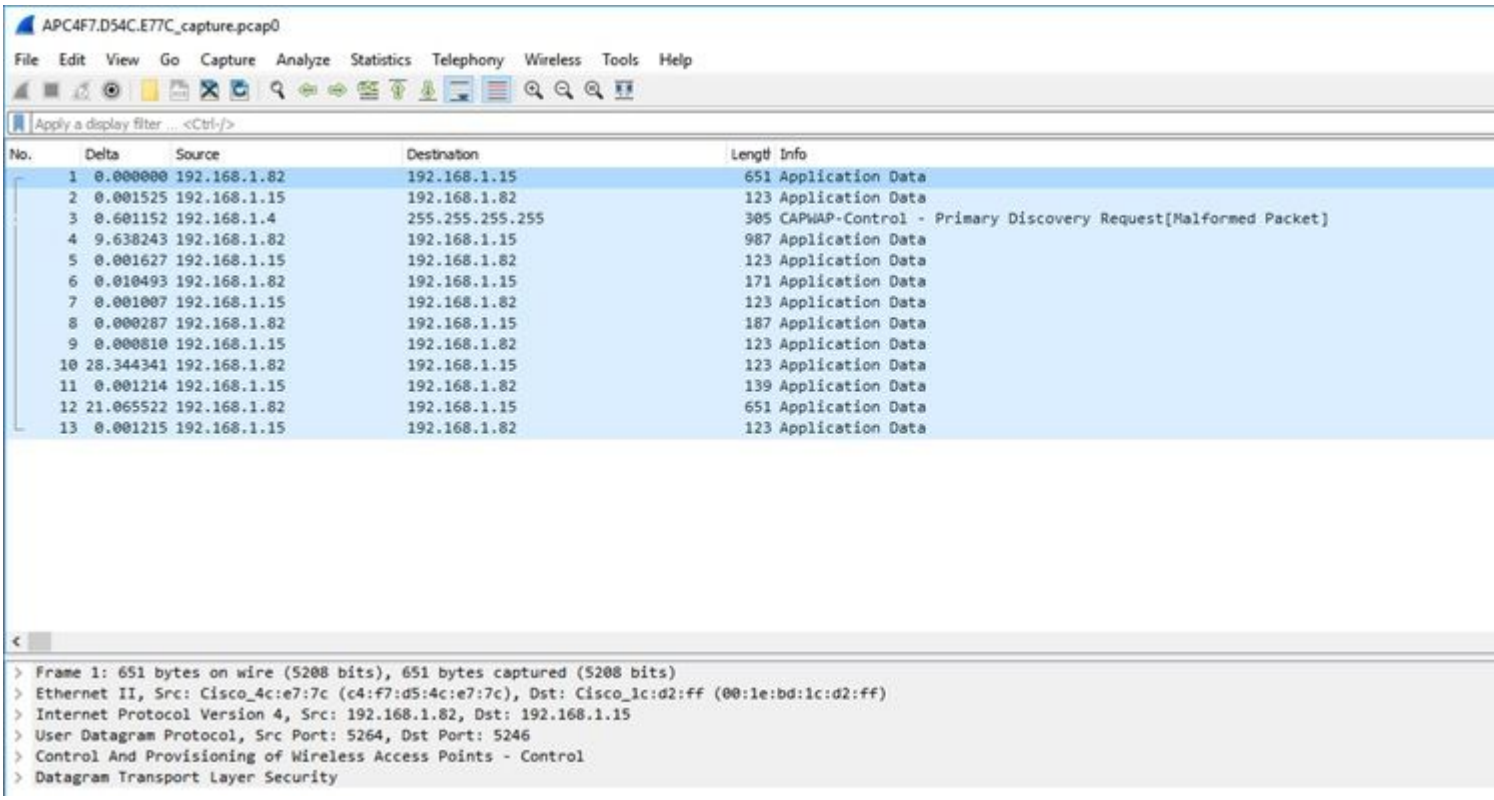
```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
12:20:50.483125 IP APC4F7-D54C-E77C.lan.5264 > 192.168.1.15.5246: UDP, length 81
12:20:50.484361 IP 192.168.1.15.5246 > APC4F7-D54C-E77C.lan.5264: UDP, length 97

APC4F7.D54C.E77C#no debug traffic wired filter "port 5246"
APC4F7.D54C.E77C#Killed
APC4F7.D54C.E77C#
```

Ejemplo de salida en archivo:

```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246" capture
% Writing packets to "/tmp/pcap/APC4F7.D54C.E77C_capture.pcap0"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
APC4F7.D54C.E77C#no debug traffic wired filter "port 5246" capture
APC4F7.D54C.E77C#copy pcap APC4F7.D54C.E77C_capture.pcap0 tftp 192.168.1.100
##################################################################################################################
APC4F7.D54C.E77C#
```

Para abrir la captura en wireshark:




## Captura de radio

Es posible habilitar la captura de paquetes en el plano de control de la radio. Debido al impacto en el rendimiento, no es posible realizar la captura en el plano de datos de radio.

Esto significa que el flujo de asociación del cliente (sondeos, autenticación, asociación, eap, arp, paquetes dhcp así como paquetes de control ipv6, icmp y ndp) es visible pero no los datos que el cliente pasa después del movimiento al estado conectado.

### Procedimiento

Paso 1. Agregue la dirección MAC del cliente objeto de seguimiento. Se pueden agregar varias direcciones MAC. También es posible ejecutar el comando para todos los clientes, pero no se recomienda.

```
config ap client-trace address add < client-mac> --- Per client debugging. Allows multiple macs.
config ap client-trace all-clients <enable | disable>  -- All clients debugging. Not recommended.
```

Paso 2. Establezca un filtro para registrar solamente protocolos específicos o todos los protocolos admitidos:

```
config ap client-trace filter <all|arp|assoc|auth|dhcp|eap|icmp|ipv6|ndp|probe> <enable|disable>
```

Paso 3. Elija mostrar el resultado en la consola (de forma asincrónica):

```
configure ap client-trace output console-log enable
```

Paso 4. Inicie el seguimiento.

```
config ap client-trace start
```

Ejemplo:

<#root>

```
AP0CD0.F894.46E4#show dot11 clients

Total dot11 clients: 1
       Client MAC Slot ID WLAN ID AID    WLAN Name RSSI Maxrate WGB

A8:DB:03:08:4C:4A

       0       1   1 testewlcwlan  -41 MCS92SS  No

AP0CD0.F894.46E4#config ap client-trace address add

A8:DB:03:08:4C:4A


AP0CD0.F894.46E4#config ap client-trace filter
  all    Trace ALL filters
  arp    Trace arp Packets
  assoc  Trace assoc Packets
  auth   Trace auth Packets
  dhcp   Trace dhcp Packets
  eap    Trace eap Packets
  icmp   Trace icmp Packets
  ipv6   Trace IPv6 Packets
  ndp    Trace ndp Packets
  probe  Trace probe Packets
AP0CD0.F894.46E4#config ap client-trace filter all enable
AP0CD0.F894.46E4#configure ap client-trace output console-log enable
AP0CD0.F894.46E4#configure ap client-trace start
AP0CD0.F894.46E4#term mon
```

Para detener la captura:

```
configure ap client-trace stop
configure ap client-trace clear
configure ap client-trace address clear
```

**Verificación**

Verificar seguimiento del cliente:

<#root>

```
AP70DB.98E1.3DEC#
```

**show ap client-trace status**

```
Client Trace Status         : Started

Client Trace ALL Clients    : disable

Client Trace Address        : a8:db:03:08:4c:4a

Remote/Dump Client Trace Address    : a8:db:03:08:4c:4a

Client Trace Filter         : probe
Client Trace Filter         : auth
Client Trace Filter         : assoc
Client Trace Filter         : eap
Client Trace Filter         : dhcp
Client Trace Filter         : dhcpv6
Client Trace Filter         : icmp
Client Trace Filter         : icmpv6
Client Trace Filter         : ndp
Client Trace Filter         : arp

Client Trace Output         : eventbuf
Client Trace Output         : console-log
Client Trace Output         : dump
Client Trace Output         : remote

Remote trace IP             : 192.168.1.100
Remote trace dest port      : 5688
NOTE - Only VIP packets are seen on remote if VIP is enabled

Dump packet length          : 10
Client Trace Inline Monitor            : disable
Client Trace Inline Monitor pkt-attach : disable
```

Ejemplo de una conexión de cliente exitosa:


Las letras entre corchetes le ayudan a entender dónde se vio esa trama (E para Ethernet, W para Wireless, C para el módulo Click cuando es interno al AP) y en qué dirección (Cargar o Descargar).

Aquí hay una pequeña tabla del significado de esas letras:

U - paquete de enlace ascendente(desde el cliente)
D - paquete de enlace descendente(para hacer clic)
W: controlador inalámbrico del módulo
E: controlador Ethernet del módulo
C - módulo Haga clic

**Otras Opciones**

Ver registro asincrónicamente:

Los registros se pueden consultar con el comando: "**show ap client-trace events mac xx:xx:xx:xx:xx:xx:xx:xx"** (o reemplace el mac por "all")

<#root>

```
AP0CD0.F894.46E4#
```

```
show ap client-trace events mac a8:db:03:08:4c:4a
```

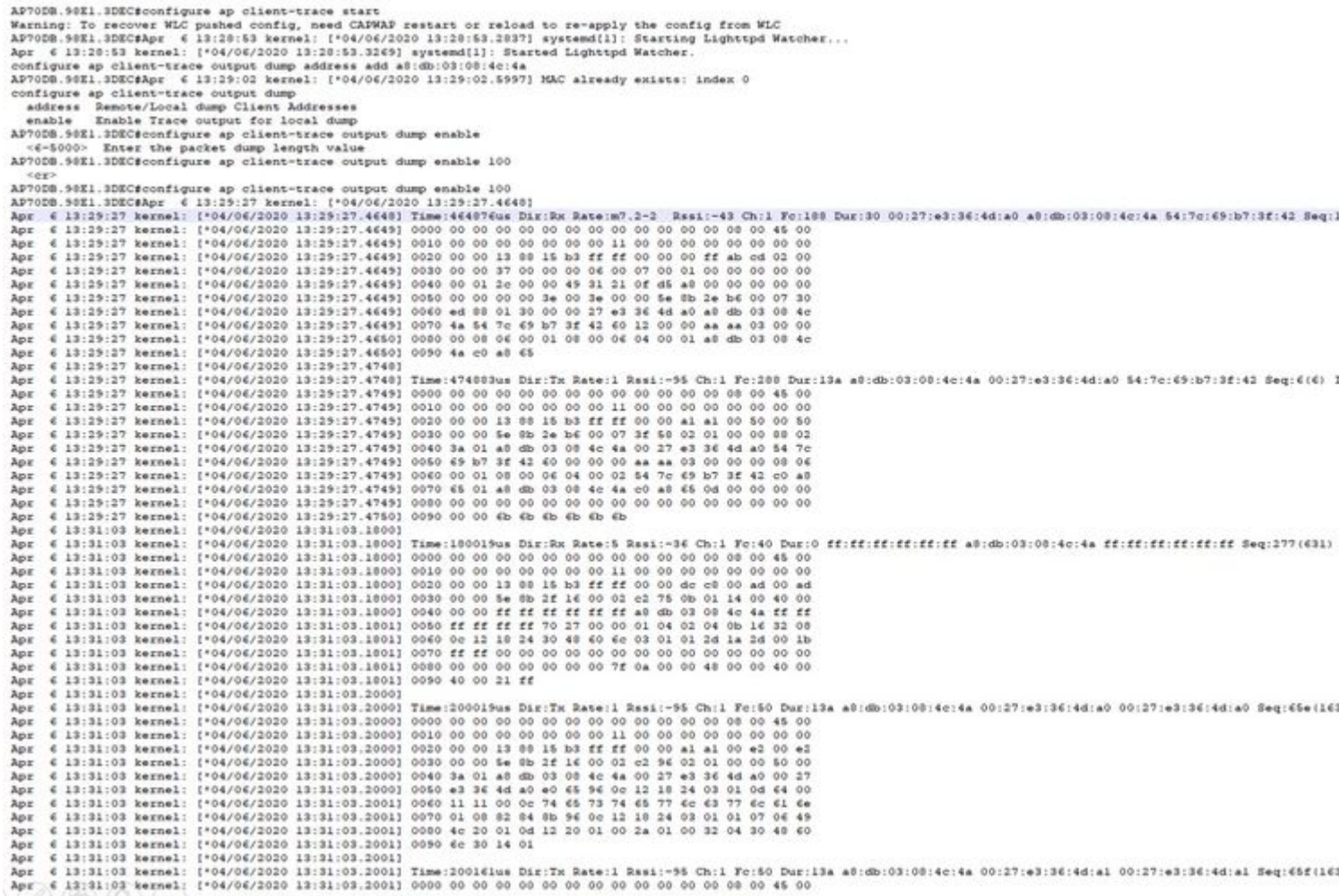
```
[*04/06/2020 10:11:54.287675] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v1> [U:W] DOT11_AUTHENTICATION
```

```
[*04/06/2020 10:11:54.288144] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_AUTHENTICATION
[*04/06/2020 10:11:54.289870] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:11:54.317341] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ASSOC_RESPONSE
[*04/06/2020 10:11:54.341370] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M1 : Descl
[*04/06/2020 10:11:54.374500] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M2 : Descl
[*04/06/2020 10:11:54.377237] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M3 : Descl
[*04/06/2020 10:11:54.390255] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M4 : Descl
[*04/06/2020 10:11:54.396855] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.416650] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469089] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469157] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921877] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921942] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:15:36.123119] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DEAUTHENTICATI
[*04/06/2020 10:15:36.127731] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DISASSOC : (.)
[*04/06/2020 10:17:24.128751] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_AUTHENTICATION
[*04/06/2020 10:17:24.128870] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_AUTHENTICATION
[*04/06/2020 10:17:24.129303] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_AUTHENTICATION
[*04/06/2020 10:17:24.133026] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:17:24.136095] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ASSOC_RESPONSE
[*04/06/2020 10:17:24.138732] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M1 : Descl
[*04/06/2020 10:17:24.257295] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M2 : Descl
[*04/06/2020 10:17:24.258105] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M3 : Descl
[*04/06/2020 10:17:24.278937] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M4 : Descl
[*04/06/2020 10:17:24.287459] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.301344] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327482] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327517] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430136] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430202] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:19:08.075326] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_PROBE_REQUEST
[*04/06/2020 10:19:08.075392] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_PROBE_RESPONSE
[*04/06/2020 10:19:08.075437] [AP0CD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_PROBE_REQUEST
```

Volcar los paquetes en formato hexadecimal

Puede volcar los paquetes en formato hexadecimal en la CLI:

```
configure ap client-trace output dump address add xx:xx:xx:xx:xx:xx
configure ap client-trace output dump enable x -> Enter the packet dump length value
```



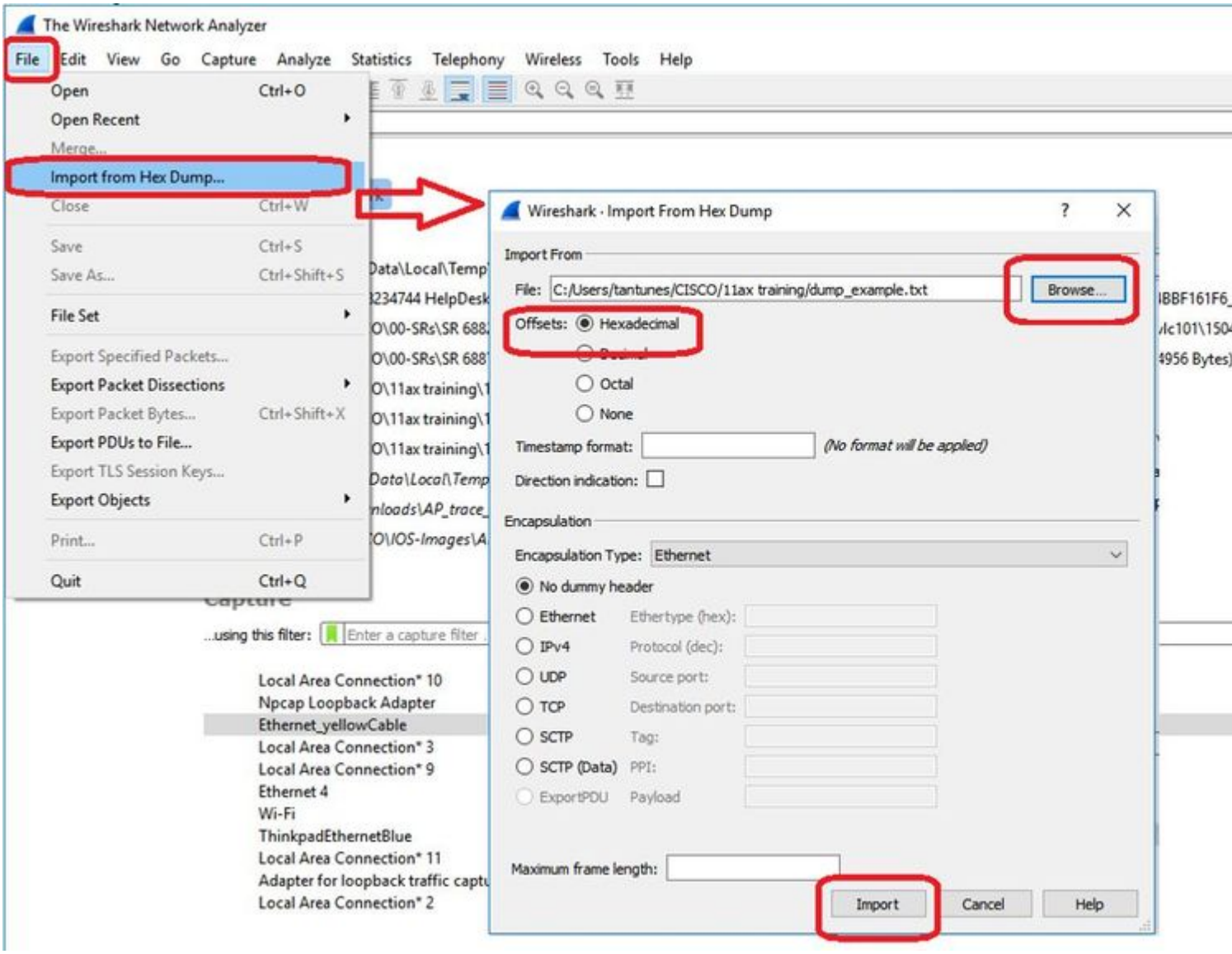

A continuación, puede limpiar el volcado hexadecimal y guardarlo en formato txt e importarlo a wireshark:

```
Time:20010us Dir:Rx Rate:1 Rssi:-37 Ch:1 Fc:b0 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:1(1) Info:DOT11_AUTH
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 db c8 00 29 00 29
0030 00 00 5e 8b 2f 1f 00 00 57 36 02 01 13 00 b0 00
0040 3a 01 00 27 e3 36 4d a0 a8 db 03 08 4c 4a 00 27
0050 e3 36 4d a0 10 00 00 00 01 00 00 00 dd 09 00 10
0060 18 02 00 00 10 00 00 00 00 00 00 6b 6b 6b 6b 6b
0070 6b

Time:43054us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:d0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66c(1644) Info:DOT11
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 1e 00 1e
0030 00 00 5e 8b 2f 1f 00 00 57 b2 02 01 00 00 d0 00
0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
0050 e3 36 4d a0 c0 66 03 02 00 08 01 00 00 00 00 00
0060 6b 6b 6b 6b 6b 6b

Time:43155us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:b0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66d(1645) Info:DOT11
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 29 00 29
0030 00 00 5e 8b 2f 1f 00 00 5d 06 02 01 00 00 b0 00
0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
0050 e3 36 4d a0 d0 66 00 00 02 00 00 00 dd 09 00 10
0060 18 02 00 00 10 00 00 00 00 00 00 6b 6b 6b 6b 6b
0070 6b

Time:43261us Dir:Rx Rate:1 Rssi:-34 Ch:1 Fc:800 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:2(2) Info:DOT11_ASS
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00
0020 00 00 13 88 15 b3 ff ff 00 00 de cc 00 c4 00 c4
0030 00 00 5e 8b 2f 1f 00 00 8a a1 02 01 12 00 00 08
0040 3a 01 00 27 e3 36 4d a0 a8 db 03 08 4c 4a 00 27
0050 e3 36 4d a0 20 00 31 15 0a 00 00 0c 74 65 73 74
0060 65 77 6c 63 77 6c 61 6e 01 08 82 84 8b 96 24 30
0070 48 6c 32 04 0c 12 18 60 21 02 05 13 24 02 01 0d
0080 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00
0090 00 0f ac 04
```




Dado que el resultado puede ser muy grande y tener en cuenta que el resultado solo menciona qué tipo de trama se ve y no ninguno de los detalles internos, puede ser más eficiente redirigir la captura de paquetes a un portátil que ejecute una aplicación de captura (como wireshark).

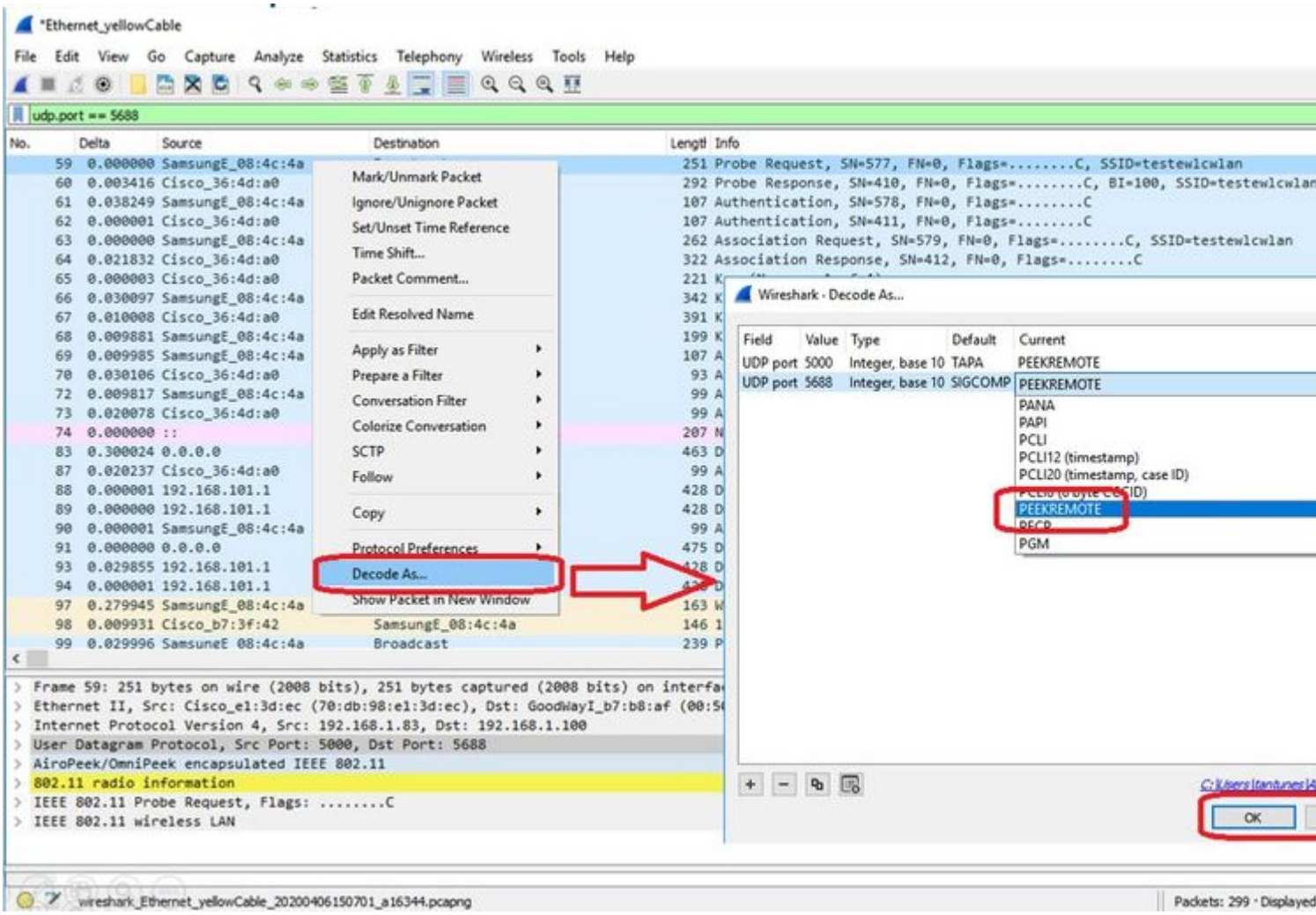
Active la función de captura remota para enviar los paquetes a un dispositivo externo con Wireshark:

```
config ap client-trace output remote enable
```

El comando significa que el AP reenvía cada trama capturada por el filtro de seguimiento del cliente hacia el portátil en 192.168.68.68 y utiliza la encapsulación PEEKREMOTE (al igual que los AP en modo sabueso) en el puerto 5000.

Una limitación es que el equipo portátil de destino tiene que estar en la misma subred que el AP donde ejecuta este comando. Puede cambiar el número de puerto para que se ajuste a las políticas de seguridad de la red.

Una vez que haya recibido todos los paquetes en el portátil que ejecuta Wireshark, puede hacer clic con el botón derecho del ratón en el encabezado udp 5000 y seleccionar **decode as** y elegir PEEKREMOTE como se muestra en esta figura:




Lista de errores y mejoras en torno a esta función:

ID de bug de Cisco CSCvm09020 El seguimiento del cliente ya no ve DNS en 8.8

ID de bug de Cisco CSCvm09015 El seguimiento del cliente muestra muchos ICMP_other con un número de secuencia nulo

ID de bug de Cisco CSCvm02676 AP COS client-trace no captura los paquetes webauth

ID de bug de Cisco CSCvm02613 El resultado remoto de seguimiento de cliente de COS de AP no funciona

ID de bug de Cisco CSCvm00855 Client-trace SEQ numbers inconsistent

**Controle el seguimiento del cliente AP desde el WLC 9800**

Puede configurar varios AP para realizar un seguimiento del cliente de radio y activarlo desde el

Paso 1. Configure un perfil de seguimiento de AP que defina qué tráfico capturar

```
config term
   wireless profile ap trace
```

```
filter all no filter probe output console-log
```

Paso 2.  Agregue el perfil de seguimiento de AP a un perfil de unión de AP que utilizan los AP que usted elige como destino.

```
ap profile < ap join profile name>
    trace
```

Asegúrese de que este perfil de unión de AP se aplique a una etiqueta de sitio que utilicen sus AP de destino

Paso 4 Inicio/parada del desencadenador

```
ap trace client start ap
```

```
client all/
```

```
 ap trace client stop ap
```

```
  client all/
```

```
   ap trace client start site
```

```
client all/
```

```
ap trace client stop site
```

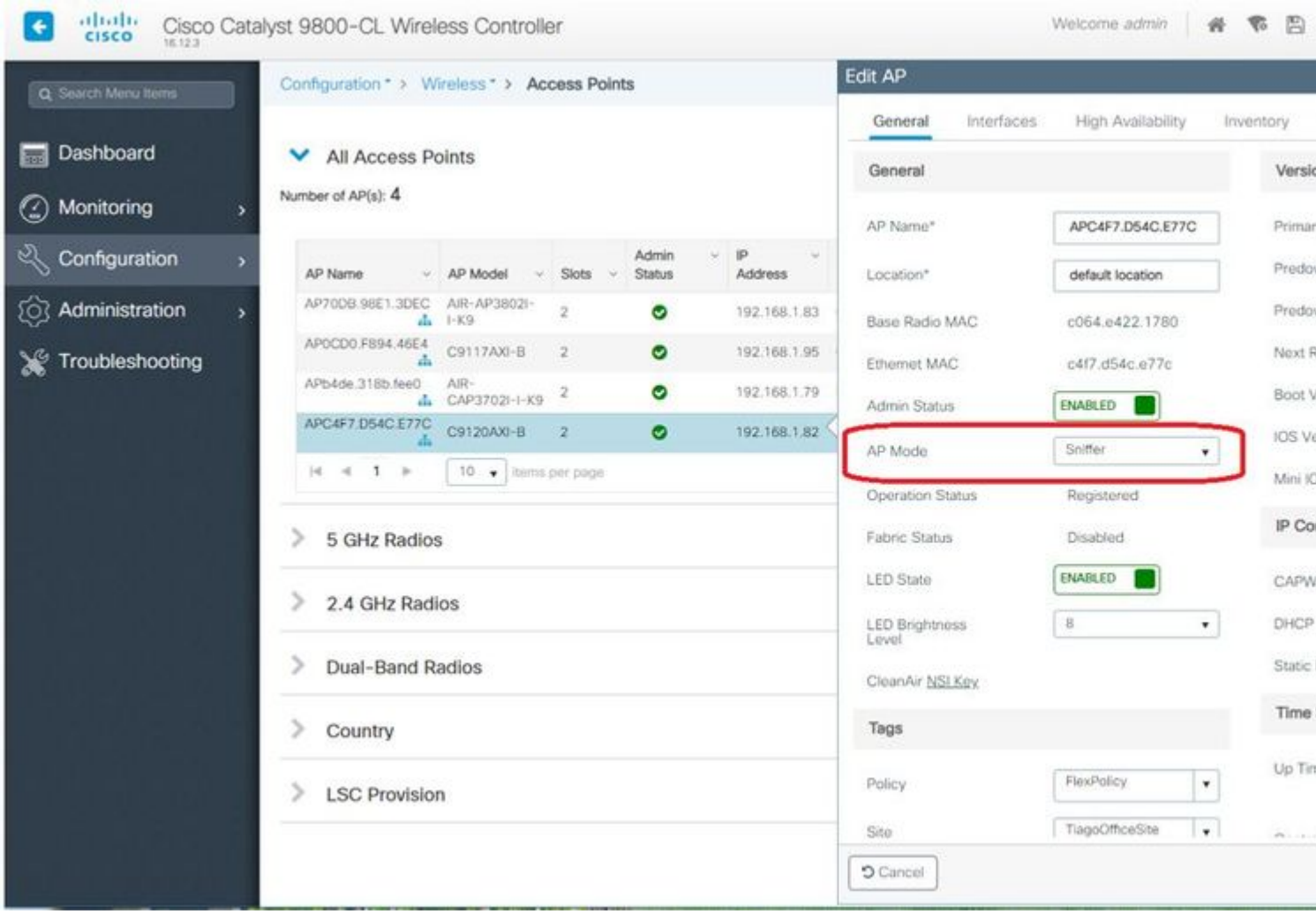
```
client all/
```

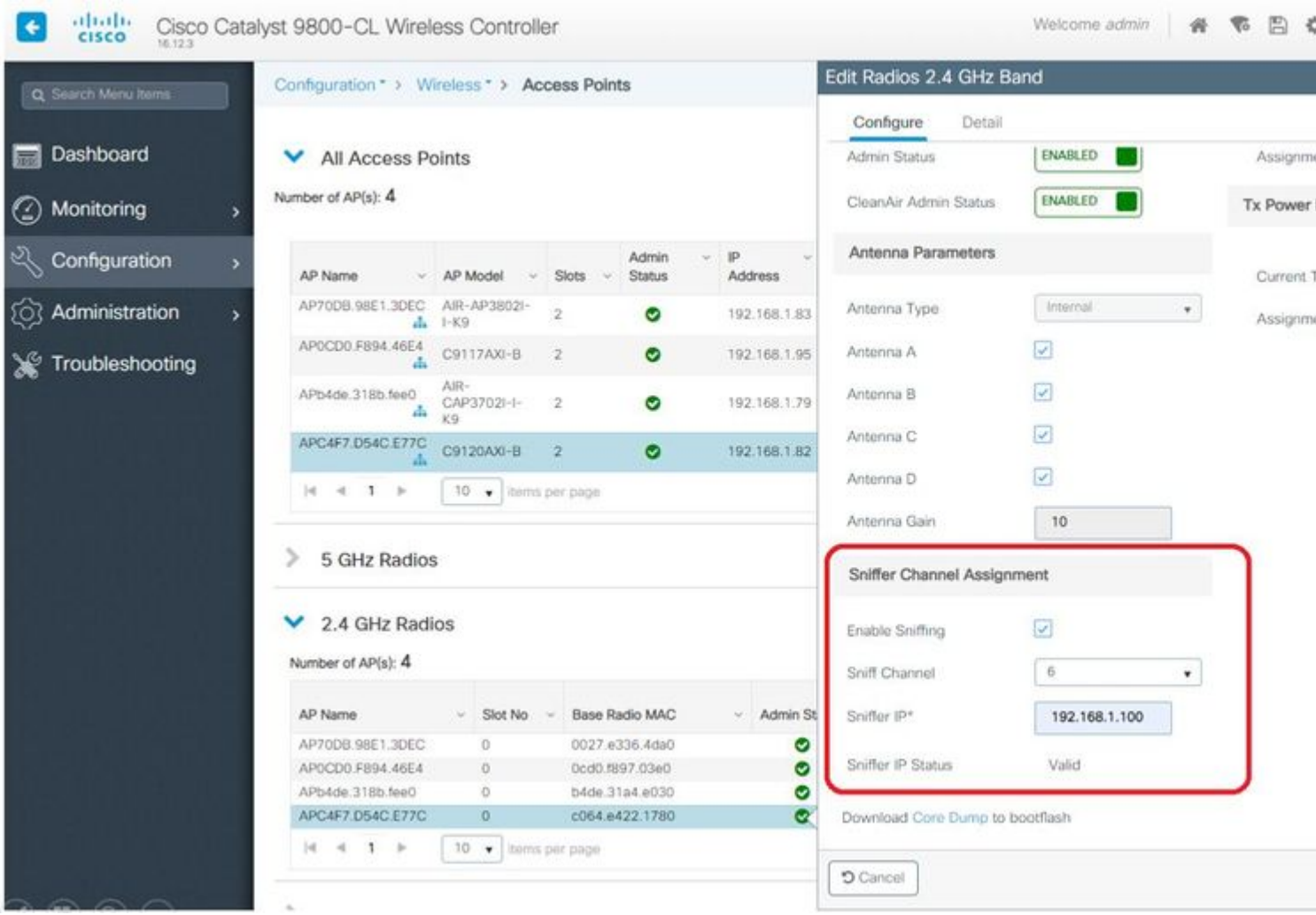
Comandos de verificación:

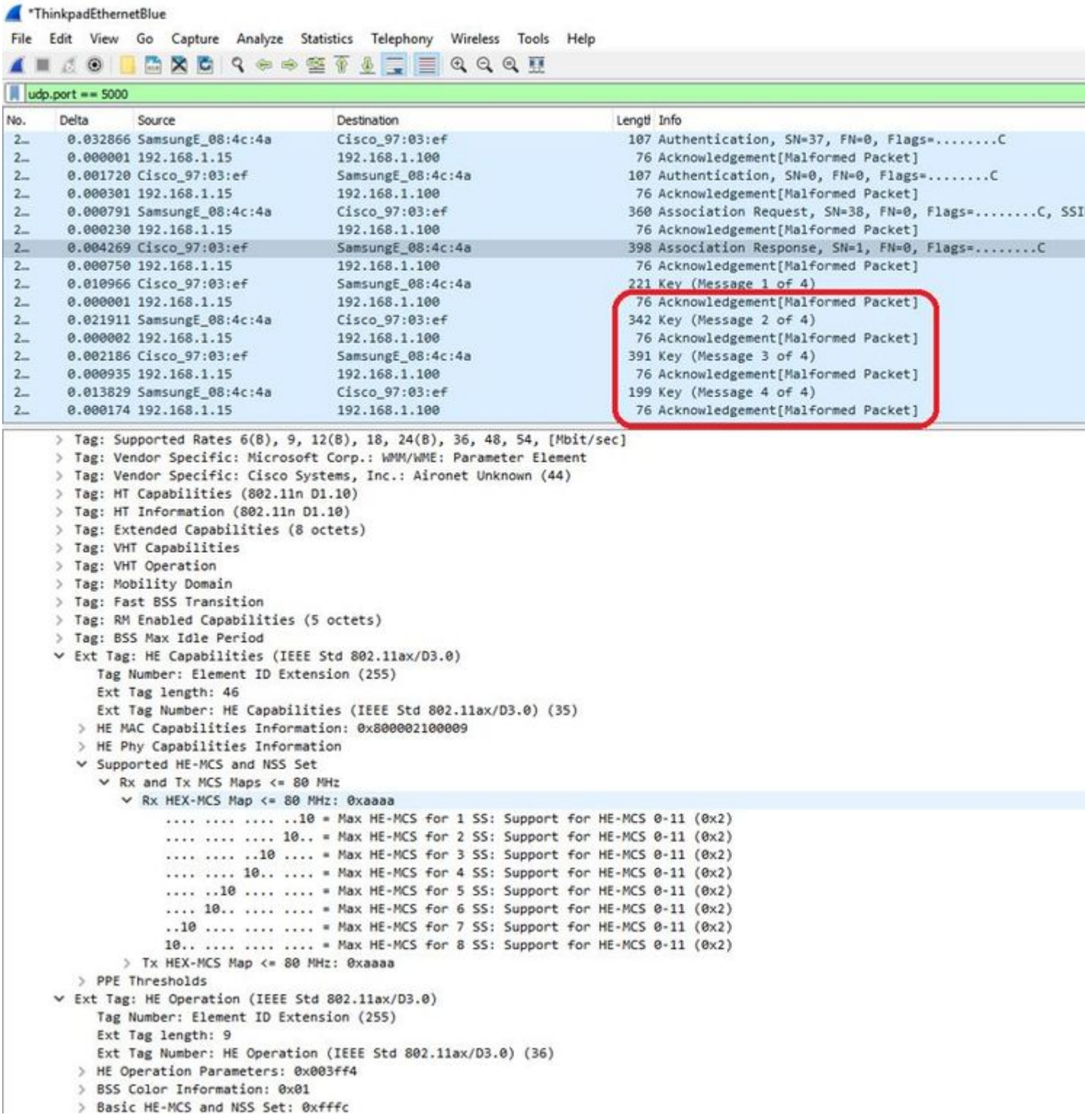
```
show wireless profile ap trace summary
show wireless profile ap trace detailed PROF_NAME detail
sh ap trace client summary
show ap trace unsupported-ap summary
```

## AP Catalyst 91xx en modo sabueso

Los nuevos Catalyst 9115, 9117, 9120 y 9130 se pueden configurar en modo sniffer. El procedimiento es similar al de los modelos AP anteriores.


Cisco Catalyst 9800-CL Wireless Controller
Welcome admin
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Wireless > Access Points
All Access Points
Number of AP(s): 4
AP Name
AP Model
Slots
Admin Status
IP Address
AP70DB.98E1.3DEC
AIR-AP3802I-I-K9
2
192.168.1.83
AP0CD0.F894.46E4
C9117AXI-B
2
192.168.1.95
APb4de.318b.fee0
AIR-CAP3702I-I-K9
2
192.168.1.79
APC4F7.D54C.E77C
C9120AXI-B
2
192.168.1.82
items per page
5 GHz Radios
2.4 GHz Radios
Dual-Band Radios
Country
LSC Provision
Edit AP
General
Interfaces
High Availability
Inventory
General
AP Name*
APC4F7.D54C.E77C
Location*
default location
Base Radio MAC
c064.e422.1780
Ethernet MAC
c4f7.d54c.e77c
Admin Status
ENABLED
AP Mode
Sniffer
Operation Status
Registered
Fabric Status
Disabled
LED State
ENABLED
LED Brightness Level
8
CleanAir NSI Key
Tags
Policy
FlexPolicy
Site
TiagoOfficeSite
Cancel


Cisco Catalyst 9800-CL Wireless Controller
16.12.3
Welcome admin
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration > Wireless > Access Points
All Access Points
Number of AP(s): 4
AP Name
AP Model
Slots
Admin Status
IP Address
AP70DB.98E1.3DEC
AIR-AP3802I-I-K9
2
192.168.1.83
A0CD0.F894.46E4
C9117AXI-B
2
192.168.1.95
APb4de.318b.fee0
AIR-CAP3702I-I-K9
2
192.168.1.79
APC4F7.D54C.E77C
C9120AXI-B
2
192.168.1.82
items per page
5 GHz Radios
2.4 GHz Radios
Number of AP(s): 4
AP Name
Slot No
Base Radio MAC
Admin St
AP70DB.98E1.3DEC
0
0027.e336.4da0
A0CD0.F894.46E4
0
0cd0.f897.03e0
APb4de.318b.fee0
0
b4de.31a4.e030
APC4F7.D54C.E77C
0
c064.e422.1780
items per page
Edit Radios 2.4 GHz Band
Configure
Detail
Admin Status
ENABLED
CleanAir Admin Status
ENABLED
Assignme
Tx Power
Antenna Parameters
Current T
Antenna Type
Internal
Assignme
Antenna A
Antenna B
Antenna C
Antenna D
Antenna Gain
10
Sniffer Channel Assignment
Enable Sniffing
Sniff Channel
6
Sniffer IP*
192.168.1.100
Sniffer IP Status
Valid
Download Core Dump to bootflash
Cancel




---

**Nota**: Las tramas de datos enviadas a velocidades de datos WIFI 6 se capturan pero, como peekremote no está actualizado en Wireshark, se muestran como tipo de archivo 802.11ax a partir de ahora. La solución está en Wireshark 3.2.4, donde Wireshark muestra la velocidad de fidelización wifi6 adecuada.

---

**Nota**: Los AP de Cisco no pueden capturar tramas MU-OFDMA en este momento, pero pueden capturar las tramas de disparo (enviadas a velocidad de datos de administración) que anuncian una ventana MU-OFDMA. Ya puede inferir que MU-OFDMA sucede (o no) y con qué cliente.

---

# Consejos de Troubleshooting

## MTU de trayecto

Aunque la detección de MTU de Trayectoria encuentra la MTU óptima para el AP, es posible invalidar esta configuración manualmente.

En AireOS 8.10.130 WLC, el comando **config ap pmtu disable <ap/all>** establece una MTU estática para uno o todos los AP en lugar de depender del mecanismo de detección dinámico.

## Para habilitar las depuraciones durante el arranque

Puede ejecutar config boot debug capwap para habilitar los debugs capwap, DTLS y DHCP en el siguiente inicio, incluso antes de que el sistema operativo se haya iniciado y se muestre el mensaje.

También tiene "config boot debug memory xxxx" para varios debugs de memoria.

Puede ver si los debugs de inicio están habilitados o no en el próximo reinicio con "show boot".

Se pueden inhabilitar con la adición de la palabra clave disable al final, como "config boot debug capwap disable".

## Mecanismo de ahorro de energía

El ahorro de energía de un cliente determinado se puede solucionar ejecutando

**debug client trace <mac address>**

## QoS de clientes

Para verificar que se aplican las etiquetas QoS, puede ejecutar "***debug capwap client qos***".

Muestra el valor UP de los paquetes para los clientes inalámbricos.

No se puede filtrar por mac a partir de la versión 8.8 (petición de mejora Cisco bug IDCSCvm08899 ).

```
labAP#debug capwap client qos

[*08/20/2018 09:43:36.3171] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:89
[*08/20/2018 09:43:45.0051] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:89
[*08/20/2018 09:43:45.5463] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:89
[*08/20/2018 09:43:46.5687] chatter: set_qos_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:35
[*08/20/2018 09:43:47.0982] chatter: set_qos_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:35
```

También puede verificar la tabla Qos UP a DSCP en el AP, así como la cantidad total de paquetes marcados, modelados y descartados por Qos:

```
LabAP#show dot11 qos
Qos Policy Maps (UPSTREAM)
```

```
no policymap
Qos Stats (UPSTREAM)

total packets:   0
dropped packets: 0
marked packets:  0
shaped packets:  0
policed packets: 0
copied packets:  0

DSCP TO DOT1P (UPSTREAM)

Default dscp2dot1p Table Value:
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48
Active dscp2dot1p Table Value:
[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48

Qos Policy Maps (DOWNSTREAM)

no policymap
Qos Stats (DOWNSTREAM)

total packets:   0
dropped packets: 0
marked packets:  0
shaped packets:  0
policed packets: 0
copied packets:  0

DSCP TO DOT1P (DOWNSTREAM)

Default dscp2dot1p Table Value:
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
Active dscp2dot1p Table Value:
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
LabAP#
```

Cuando las políticas de QoS se definen en el WLC y se descargan en el AP Flexconnect, puede verificarlas con :

```
AP780C-F085-49E6#show policy-map
2 policymaps
Policy Map BWLimitAAAClients            type:qos client:default
    Class BWLimitAAAClients_AVC_UI_CLASS
```

```
      drop

    Class BWLimitAAAClients_ADV_UI_CLASS
      set dscp af41 (34)


    Class class-default
      police rate 5000000 bps (625000Bytes/s)
        conform-action
        exceed-action


Policy Map platinum-up          type:qos client:default
    Class cm-dscp-set1-for-up-4
      set dscp af41 (34)


    Class cm-dscp-set2-for-up-4
      set dscp af41 (34)


    Class cm-dscp-for-up-5
      set dscp af41 (34)


    Class cm-dscp-for-up-6
      set dscp ef (46)


    Class cm-dscp-for-up-7
      set dscp ef (46)


    Class class-default
      no actions
```

En caso de limitación de velocidad de QoS:

```
AP780C-F085-49E6#show rate-limit client
Config:
              mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst
A8:DB:03:6F:7A:46   2           0          0            0           0             0           0
Statistics:
            name    up  down
        Unshaped     0     0
  Client RT pass     0     0
 Client NRT pass     0     0
 Client RT drops     0     0
Client NRT drops     0 38621
               9 54922     0
```

## Análisis fuera de canal

Depurar el escaneo fuera del canal del AP puede ser útil al resolver problemas de detección no autorizada

(para validar si el AP va en un canal específico para escanear), pero también puede ser útil en la resolución de problemas de video donde un flujo sensible en tiempo real recibe interrupciones constantes si la función "aplazamiento del escaneo fuera del canal" no se utiliza.

```
debug rrm off-channel defer
debug rrm off-chanel dbg (starting 17.8.1)
debug rrm off-channel schedule
debug rrm off-channel voice (starting 17.8.1)
debug rrm schedule (starting 17.8.1, debug NDP packet tx)
show trace dot_11 channel enable

[*06/11/2020 09:45:38.9530] wcp/rrm_userspace_0/rrm_schedule :: RRMSchedule process_int_duration_timer_l
[*06/11/2020 09:45:39.0550] noise measurement channel 5 noise 89
[*06/11/2020 09:45:43.5490] wcp/rrm_userspace_1/rrm_schedule :: RRMSchedule process_int_duration_timer_l
[*06/11/2020 09:45:43.6570] noise measurement channel 140 noise 97
```

## Conectividad del cliente

Es posible enumerar los clientes que han sido desautenticados por el punto de acceso con el último registro de hora del evento:

```
LabAP#show dot11 clients deauth
               timestamp               mac vap reason_code
Mon Aug 20 09:50:59 2018 AC:BC:32:A4:2C:D3   9           4
Mon Aug 20 09:52:14 2018 00:AE:FA:78:36:89   9           4
Mon Aug 20 10:31:54 2018 00:AE:FA:78:36:89   9           4
```

En la salida anterior, el código de motivo es el código de motivo de desautenticación como se detalla en este link :

https://community.cisco.com:443/t5/wireless-mobility-knowledge-base/802-11-association-status-802-11-deauth-reason-codes/ta-p/3148055

El vap se refiere al identificador de la WLAN dentro del AP (que es diferente del ID de WLAN en el WLC !!!).

Puede relacionarlo con otros resultados detallados posteriormente, que siempre menciona el vap de clientes asociados.

Puede ver la lista de ID de VAP con "***show controllers Dot11Radio 0/1 wlan***".

Cuando los clientes aún están asociados, puede obtener detalles sobre su conexión con:

```
LabAP#show dot11 clients

Total dot11 clients: 1
       Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate WGB
00:AE:FA:78:36:89       1      10   1   TestSSID -25 MCS82SS  No
```

Se pueden obtener muchos más detalles sobre la entrada del cliente con:

```
LabAP#show client summ

Radio Driver client Summary:
============================
wifi0
[*08/20/2018 11:54:59.5340]
[*08/20/2018 11:54:59.5340] Total STA List Count 0
[*08/20/2018 11:54:59.5340] | NO|              MAC|STATE|
[*08/20/2018 11:54:59.5340] ----------------------------
wifi1
[*08/20/2018 11:54:59.5357]
[*08/20/2018 11:54:59.5357] Total STA List Count 1
[*08/20/2018 11:54:59.5357] | NO|              MAC|STATE|
[*08/20/2018 11:54:59.5357] ----------------------------
[*08/20/2018 11:54:59.5357] |  1| 0:ffffffae:fffffffa:78:36:ffffff89|    8|

Radio Driver Client AID List:
============================
wifi0
[*08/20/2018 11:54:59.5415]
[*08/20/2018 11:54:59.5415] Total STA-ID List Count 0
[*08/20/2018 11:54:59.5415] | NO|              MAC|STA-ID|
[*08/20/2018 11:54:59.5415] ----------------------------
wifi1
[*08/20/2018 11:54:59.5431]
[*08/20/2018 11:54:59.5431] Total STA-ID List Count 1
[*08/20/2018 11:54:59.5431] | NO|              MAC|STA-ID|
[*08/20/2018 11:54:59.5432] ----------------------------
[*08/20/2018 11:54:59.5432] |  1| 0:ffffffae:fffffffa:78:36:ffffff89|     6|

WCP client Summary:
===================

              mac radio vap aid state       encr Maxrate is_wgb_wired      wgb_mac_addr
00:AE:FA:78:36:89     1   9   1   FWD AES_CCM128 MCS82SS        false 00:00:00:00:00:00


NSS client Summary:
===================
Current Count: 3
|       MAC       | OPAQUE |PRI POL|VLAN|BR|TN|QCF|BSS|RADID|MYMAC|
|F8:0B:CB:E4:7F:41|00000000|      3|   0| 1| 1|  0|  2|    3|    1|
|F8:0B:CB:E4:7F:40|00000000|      3|   0| 1| 1|  0|  2|    3|    1|
|00:AE:FA:78:36:89|00000003|      1|   0| 1| 1|  0|  9|    1|    0|

Datapath IPv4 client Summary:
=============================
               id vap   port         node tunnel               mac        seen_ip     hashed_ip sniff_ag
00:AE:FA:78:36:89   9 apr1v9 192.0.2.13      - 00:AE:FA:78:36:89 192.168.68.209 10.228.153.45  5.990000

Datapath IPv6 client Summary:
=============================
client               mac                 seen_ip6 age      scope   port
     1 00:AE:FA:78:36:89 fe80::2ae:faff:fe78:3689  61 link-local apr1v9

Wired client Summary:
=====================
mac port state local_client detect_ago associated_ago tx_pkts tx_bytes rx_pkts rx_bytes
```

Puede forzar la desconexión de un cliente específico con :

```
test dot11 client deauthenticate
```

Los contadores de tráfico se pueden obtener por cliente con:

```
LabAP#show client statistics wireless 00:AE:FA:78:36:89
Client MAC address: 00:AE:FA:78:36:89
Tx Packets                    : 621
Tx Management Packets         : 6
Tx Control Packets            : 153
Tx Data Packets               : 462
Tx Data Bytes                 : 145899
Tx Unicast Data Packets       : 600
Rx Packets                    : 2910
Rx Management Packets         : 13
Rx Control Packets            : 943
Rx Data Packets               : 1954
Rx Data Bytes                 : 145699
LabAP#
```

Más en el nivel de radio, una gran cantidad de información se puede obtener en el "***show controllers***". Al agregar la dirección MAC del cliente, se muestran las velocidades de datos admitidas, las creaciones de datos actuales, las capacidades PHY, así como la cantidad de reintentos y de errores de texto:

<#root>

```
LabAP#show controllers dot11Radio 0 client 00:AE:FA:78:36:89
              mac radio vap aid state       encr Maxrate is_wgb_wired      wgb_mac_addr
00:AE:FA:78:36:89     0   9   1   FWD AES_CCM128    M15         false 00:00:00:00:00:00
Configured rates for client 00:AE:FA:78:36:89
Legacy Rates(Mbps): 11
HT Rates(MCS):M0 M1 M2 M3 M4 M5 M6 M7 M8 M9 M10 M11 M12 M13 M14 M15
VHT Rates: 1SS:M0-7 2SS:M0-7

HT:yes     VHT:yes     HE:no     40MHz:no     80MHz:no     80+80MHz:no     160MHz:no
11w:no     MFP:no     11h:no     encrypt_polocy: 4
_wmm_enabled:yes     qos_capable:yes     WME(11e):no     WMM_MIXED_MODE:no
short_preamble:yes     short_slot_time:no     short_hdr:yes     SM_dyn:yes
short_GI_20M:yes     short_GI_40M:no     short_GI_80M:yes     LDPC:yes     AMSDU:yes     AMSDU_long:no
su_mimo_capable:yes     mu_mimo_capable:no     is_wgb_wired:no     is_wgb:no

Additional info for client 00:AE:FA:78:36:89
RSSI: -90
PS  : Legacy (Sleeping)
Tx Rate: 0 Kbps
Rx Rate: 117000 Kbps
VHT_TXMAP: 0
CCX Ver: 4

Statistics for client 00:AE:FA:78:36:89
```

```
              mac   intf TxData TxMgmt TxUC TxBytes
```

**TxFail**

```
 TxDcrd TxCumRetries RxData RxMgmt RxBytes RxErr TxRt   RxRt idle_counter stats_ago expiration
00:AE:FA:78:36:89 apr0v9      8      1    6    1038      1      0            0     31      1    1599

Per TID packet statistics for client 00:AE:FA:78:36:89
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s) QID Tx Drops Tx Cur Qlimit
       0     899     460            1             1 144        0      0   1024
       1       0       0            0             0 145        0      0   1024
       2       0       0            0             0 146        0      0   1024
       3      59       0            0             0 147        0      0   1024
       4       0       0            0             0 148        0      0   1024
       5       0       0            0             0 149        0      0   1024
       6       0       0            0             0 150        0      0   1024
       7       0       0            0             0 151        0      0   1024

Legacy Rate Statistics:
  (Mbps :   Rx, Tx, Tx-Retries)
11 Mbps :    2,    0,    0
 6 Mbps :    0,    9,    0

HT/VHT Rate Statistics:
(Rate/SS/Width :   Rx, Rx-Ampdu, Tx, Tx-Ampdu, Tx-Retries)
        0/1/20 :    4,    4,    0,    0,    0
        6/2/20 :    4,    4,    0,    0,    0
        7/2/20 :    5,    5,    0,    0,    0

webauth done:
false
```

Para realizar un seguimiento constante de la velocidad de datos de un cliente y/o del valor RSSI, puede ejecutar "**debug dot11 client rate address <mac>** " y esto registra esta información cada segundo:

```
LabAP#debug dot11 client rate address 00:AE:FA:78:36:89
[*08/20/2018 14:17:28.0928]                MAC    Tx-Pkts    Rx-Pkts  Tx-Rate  Rx-Rate  RSSI   SNR Tx-Re
[*08/20/2018 14:17:28.0928] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -45    53
[*08/20/2018 14:17:29.0931] 00:AE:FA:78:36:89          7         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:30.0934] 00:AE:FA:78:36:89          3         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:31.0937] 00:AE:FA:78:36:89          2         20       12  a8.2-2s   -45    53
[*08/20/2018 14:17:32.0939] 00:AE:FA:78:36:89          2         20       12  a8.2-2s   -45    53
[*08/20/2018 14:17:33.0942] 00:AE:FA:78:36:89          2         21       12  a8.2-2s   -46    52
[*08/20/2018 14:17:34.0988] 00:AE:FA:78:36:89          1          4       12  a8.2-2s   -46    52
[*08/20/2018 14:17:35.0990] 00:AE:FA:78:36:89          9         23       12  a8.2-2s   -46    52
[*08/20/2018 14:17:36.0993] 00:AE:FA:78:36:89          3          7       12  a8.2-2s   -46    52
[*08/20/2018 14:17:37.0996] 00:AE:FA:78:36:89          2          6       12  a8.2-2s   -46    52
[*08/20/2018 14:17:38.0999] 00:AE:FA:78:36:89          2         14       12  a8.2-2s   -46    52
[*08/20/2018 14:17:39.1002] 00:AE:FA:78:36:89          2         10       12  a8.2-2s   -46    52
[*08/20/2018 14:17:40.1004] 00:AE:FA:78:36:89          1          6       12  a8.2-2s   -46    52
[*08/20/2018 14:17:41.1007] 00:AE:FA:78:36:89          9         20       12  a8.2-2s   -46    52
[*08/20/2018 14:17:42.1010] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:43.1013] 00:AE:FA:78:36:89          2          8       12  a8.2-2s   -46    52
[*08/20/2018 14:17:44.1015] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:45.1018] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:46.1021] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:47.1024] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:48.1026] 00:AE:FA:78:36:89          7         15       12  a8.2-2s   -46    52
[*08/20/2018 14:17:49.1029] 00:AE:FA:78:36:89          0          6       12  a8.2-2s   -46    52
```

```
[*08/20/2018 14:17:50.1032] 00:AE:FA:78:36:89          0          0       12  a8.2-2s   -46    52
[*08/20/2018 14:17:51.1035] 00:AE:FA:78:36:89          1          7       12  a8.2-2s   -46    52
[*08/20/2018 14:17:52.1037] 00:AE:FA:78:36:89          0         17       12  a8.2-2s   -46    52
[*08/20/2018 14:17:53.1040] 00:AE:FA:78:36:89          1         19       12  a8.2-2s   -46    52
[*08/20/2018 14:17:54.1043] 00:AE:FA:78:36:89          2         17       12  a8.2-2s   -46    52
[*08/20/2018 14:17:55.1046] 00:AE:FA:78:36:89          2         22       12  a8.2-2s   -45    53
[*08/20/2018 14:17:56.1048] 00:AE:FA:78:36:89          1         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:57.1053] 00:AE:FA:78:36:89          2         18       12  a8.2-2s   -45    53
[*08/20/2018 14:17:58.1055] 00:AE:FA:78:36:89         12         37       12  a8.2-2s   -45    53
```

En esta salida, los contadores de paquetes Tx y Rx son paquetes transmitidos en el segundo intervalo desde la última impresión, lo mismo para los reintentos Tx. Sin embargo, RSSI, SNR y velocidad de datos son los valores del último paquete de ese intervalo (y no un promedio para todos los paquetes en ese intervalo).

## Escenarios de Flexconnect

Puede verificar qué ACL se aplican actualmente a un cliente en un escenario anterior a la autenticación (CWA por ejemplo) o posterior a la autenticación:

```
AP#show client access-lists pre-auth all f48c.507a.b9ad
Pre-Auth URL ACLs for Client: F4:8C:50:7A:B9:AD
IPv4 ACL: IPv6 ACL:
ACTION URL-LIST

Resolved IPs for Client: F4:8C:50:7A:B9:AD
HIT-COUNT URL ACTION IP-LIST

REDIRECT
rule 0: allow true and ip proto 17 and src port 53
rule 1: allow true and ip proto 17 and dst port 53
rule 2: allow true and src 10.48.39.161mask 255.255.255.255
rule 3: allow true and dst 10.48.39.161mask 255.255.255.255
rule 4: deny true
No IPv6 ACL found


AP#show client access-lists post-auth all f48c.507a.b9ad
Post-Auth URL ACLs for Client: F4:8C:50:7A:B9:AD
IPv4 ACL: IPv6 ACL:
ACTION URL-LIST

Resolved IPs for Client: F4:8C:50:7A:B9:AD
HIT-COUNT URL ACTION IP-LIST

post-auth
rule 0: deny true and dst 192.0.0.0mask 255.0.0.0
rule 1: deny true and src 192.0.0.0mask 255.0.0.0
rule 2: allow true
No IPv6 ACL found
```

## AP Filesystem

Los COS AP no permiten enumerar todo el contenido del sistema de archivos como en las plataformas Unix.

El comando "***show filesystems***" proporciona un detalle del uso y la distribución del espacio en la partición actual:

```
2802#show filesystems
Filesystem                Size      Used Available Use% Mounted on
/dev/ubivol/storage      57.5M    364.0K     54.1M   1% /storage
2802#
```

El comando "***show flash***" enumera los archivos principales en la memoria flash del AP. También puede anexar la palabra clave syslog o core para enumerar esas carpetas específicas.

```
ap_2802#show flash
Directory of /storage/
total 84
-rw-r--r--    1 root     root             0 May 21  2018 1111
-rw-r--r--    1 root     root             6 Apr 15 11:09 BOOT_COUNT
-rw-r--r--    1 root     root             6 Apr 15 11:09 BOOT_COUNT.reserve
-rw-r--r--    1 root     root            29 Apr 15 11:09 RELOADED_AT_UTC
drwxr-xr-x    2 root     root           160 Mar 27 13:53 ap-images
drwxr-xr-x    4 5        root          2016 Apr 15 11:10 application
-rw-r--r--    1 root     root          6383 Apr 26 09:32 base_capwap_cfg_info
-rw-r--r--    1 root     root            20 Apr 26 10:31 bigacl
-rw-r--r--    1 root     root          1230 Mar 27 13:53 bootloader.log
-rw-r--r--    1 root     root             5 Apr 26 09:29 bootloader_verify.shadow
-rw-r--r--    1 root     root            18 Jun 30  2017 config
-rw-r--r--    1 root     root          8116 Apr 26 09:32 config.flex
-rw-r--r--    1 root     root            21 Apr 26 09:32 config.flex.mgroup
-rw-r--r--    1 root     root             0 Apr 15 11:09 config.local
-rw-r--r--    1 root     root             0 Jul 26  2018 config.mesh.dhcp
-rw-r--r--    1 root     root           180 Apr 15 11:10 config.mobexp
-rw-r--r--    1 root     root             0 Jun  5  2018 config.oeap
-rw-r--r--    1 root     root          2253 Apr 26 09:43 config.wireless
drwxr-xr-x    2 root     root           160 Jun 30  2017 cores
drwxr-xr-x    2 root     root           320 Jun 30  2017 dropbear
drwxr-xr-x    2 root     root           160 Jun 30  2017 images
-rw-r--r--    1 root     root           222 Jan  2  2000 last_good_uplink_config
drwxr-xr-x    2 root     root           160 Jun 30  2017 lists
-rw-r--r--    1 root     root           215 Apr 16 11:01 part1_info.ver
-rw-r--r--    1 root     root           215 Apr 26 09:29 part2_info.ver
-rw-r--r--    1 root     root          4096 Apr 26 09:36 random_seed
-rw-r--r--    1 root     root             3 Jun 30  2017 rxtx_mode
-rw-r--r--    1 root     root            64 Apr 15 11:11 sensord_CSPRNG0
-rw-r--r--    1 root     root            64 Apr 15 11:11 sensord_CSPRNG1
drwxr-xr-x    3 support  root           224 Jun 30  2017 support
drwxr-xr-x    2 root     root          2176 Apr 15 11:10 syslogs
---------------------------------------------------------------------------
Filesystem                Size      Used Available Use% Mounted on
flash                    57.5M    372.0K     54.1M   1% /storage
```

## Almacenar y enviar registros del sistema

La carpeta syslog almacena la salida de syslog de reinicios anteriores. El comando "***show log***" sólo muestra syslog desde el último reinicio.

En cada ciclo de reinicio, los registros del sistema se escriben en archivos incrementales.

```
artaki# show flash syslogs
Directory of /storage/syslogs/
total 128
-rw-r--r--    1 root     root         11963 Jul  6 15:23 1
-rw-r--r--    1 root     root         20406 Jan  1  2000 1.0
-rw-r--r--    1 root     root           313 Jul  6 15:23 1.last_write
-rw-r--r--    1 root     root         20364 Jan  1  2000 1.start
-rw-r--r--    1 root     root            33 Jul  6 15:23 1.watchdog_status
-rw-r--r--    1 root     root         19788 Jul  6 16:46 2
-rw-r--r--    1 root     root         20481 Jul  6 15:23 2.0
-rw-r--r--    1 root     root           313 Jul  6 16:46 2.last_write
-rw-r--r--    1 root     root         20422 Jul  6 15:23 2.start
---------------------------------------------------------------------------
Filesystem                Size      Used Available Use% Mounted on
flash                    57.6M     88.0K     54.5M   0% /storage

artaki# show flash cores
Directory of /storage/cores/
total 0
---------------------------------------------------------------------------
Filesystem                Size      Used Available Use% Mounted on
flash                    57.6M     88.0K     54.5M   0% /storage
```

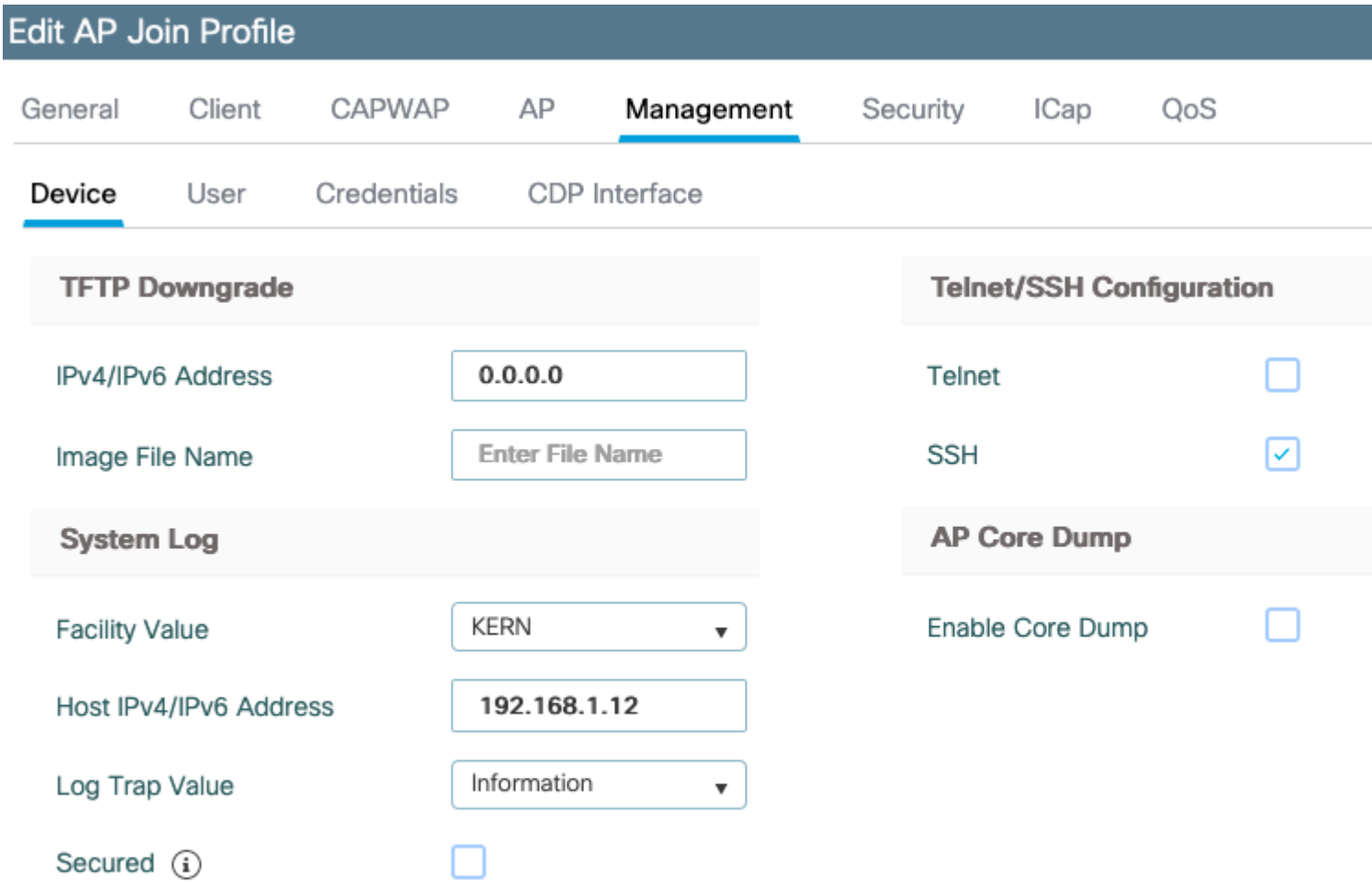
La primera salida después del arranque inicial es el archivo 1.0 y se crea un archivo 1.1 si 1.0 se vuelve demasiado largo. Después del reinicio, se crea un nuevo archivo 2.0, etc.

Desde el WLC, puede configurar el destino de Syslog si desea que sus AP envíen sus mensajes de syslog unicast a un servidor específico.

De forma predeterminada, los AP envían sus registros del sistema a una dirección de difusión que puede causar una tormenta de difusión, así que asegúrese de configurar un servidor de registro del sistema.

El AP envía vía syslog por defecto lo que se imprime en su salida de la consola.

En 9800 Controller, puede cambiar estos parámetros en el perfil Configuration -> AP Join, en Management.




Puede cambiar el **Valor de Trampa de Registro** para enviar también depuraciones vía syslog. Luego puede habilitar los debugs en la CLI del AP y la salida de éstos se envía a través de mensajes de syslog al servidor configurado .

Debido al ID de bug de Cisco CSCvu75017 ,sólo cuando configura la función syslog en KERN (el valor predeterminado) el AP envía mensajes syslog fuera.

Si está resolviendo problemas en los que un AP posiblemente pierda conectividad de red (o en un WGB por ejemplo), syslog no es tan confiable como no se envían mensajes si el AP pierde su conectividad de link ascendente.

Por lo tanto, la confianza en los archivos syslog almacenados en flash es una gran manera de depurar y almacenar la salida en el propio AP y luego cargarla periódicamente más adelante.

## Paquete de soporte de AP

Algunos de los datos de diagnóstico recopilados habitualmente de varios tipos pueden estar disponibles en un único paquete que puede cargar desde los puntos de acceso.

La información de diagnóstico que puede incluir en el paquete es la siguiente:

- AP show tech
- Registros del sistema AP

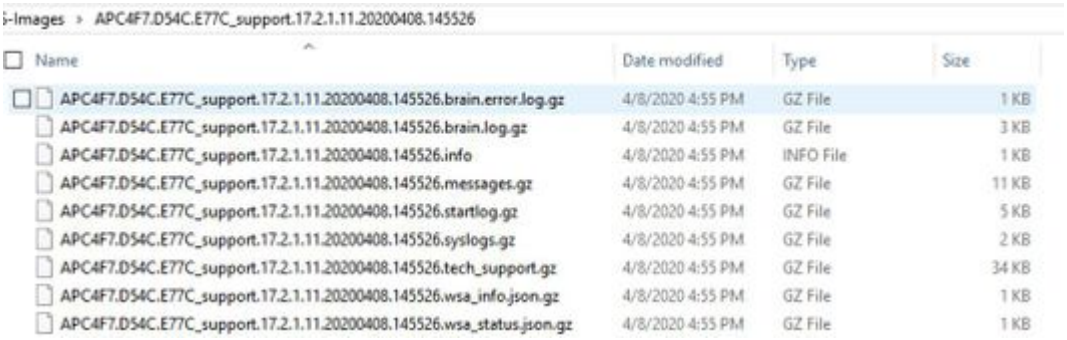
- AP Capwapd Registros cerebrales
- Registros de inicio y mensajes de AP
- Archivos Coredump de AP

Para obtener el paquete de soporte de AP, puede ir a la CLI de AP e ingresar el comando "***copy* support-bundle tftp: x.x.x.x**".

Después de esto, puede verificar el archivo llamado con el nombre AP agregado con el **support.apversion.date.time.tgz** como se muestra a continuación :

```
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
  <cr>
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
Creating support bundle, please wait...ifconfig: wired1: error fetching interface information: Device not found
Unit systemd-journald.socket could not be found.
tar: ./*.tgz: No such file or directory
tar: error exit delayed from previous errors
tar: *.tgz: No such file or directory
tar: error exit delayed from previous errors
+=== Support file APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz created ===+
################################################################################################################################################
Successful file transfer:
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz
APC4F7.D54C.E77C#
```

Cuando "untar" el archivo puede ver los diversos archivos recopilados:




## Recopile los archivos principales de AP de forma remota

Para recolectar los archivos de núcleo del AP remotamente, habilite el vaciado de memoria para ser incluido en el paquete de soporte y luego Cargue el paquete de soporte desde el AP, o envíe directamente al servidor tftp. Los siguientes ejemplos utilizan el servidor tftp 192.168.1.100.

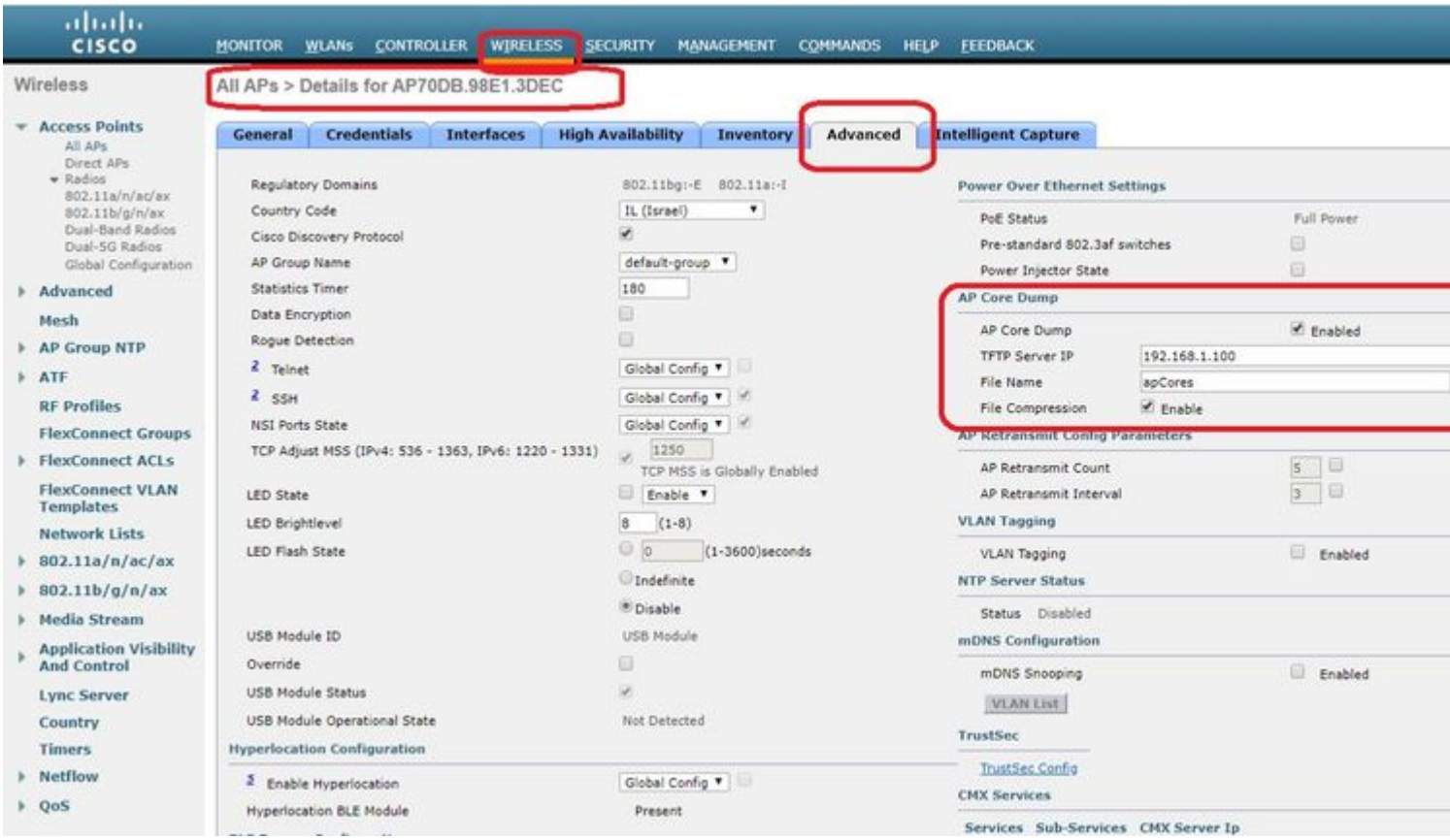
### CLI de AireOS

```
(c3504-01) >config ap core-dump enable 192.168.1.100 apCores uncompress ?

<Cisco AP>     Enter the name of the Cisco AP.

all            Applies the configuration to all connected APs.
```

### GUI de AireOS




## CLI de Cisco IOS®

<#root>

```
eWLC-9800-01(
```

**config**

```
)#ap profile TiagoOffice
eWLC-9800-01(
```

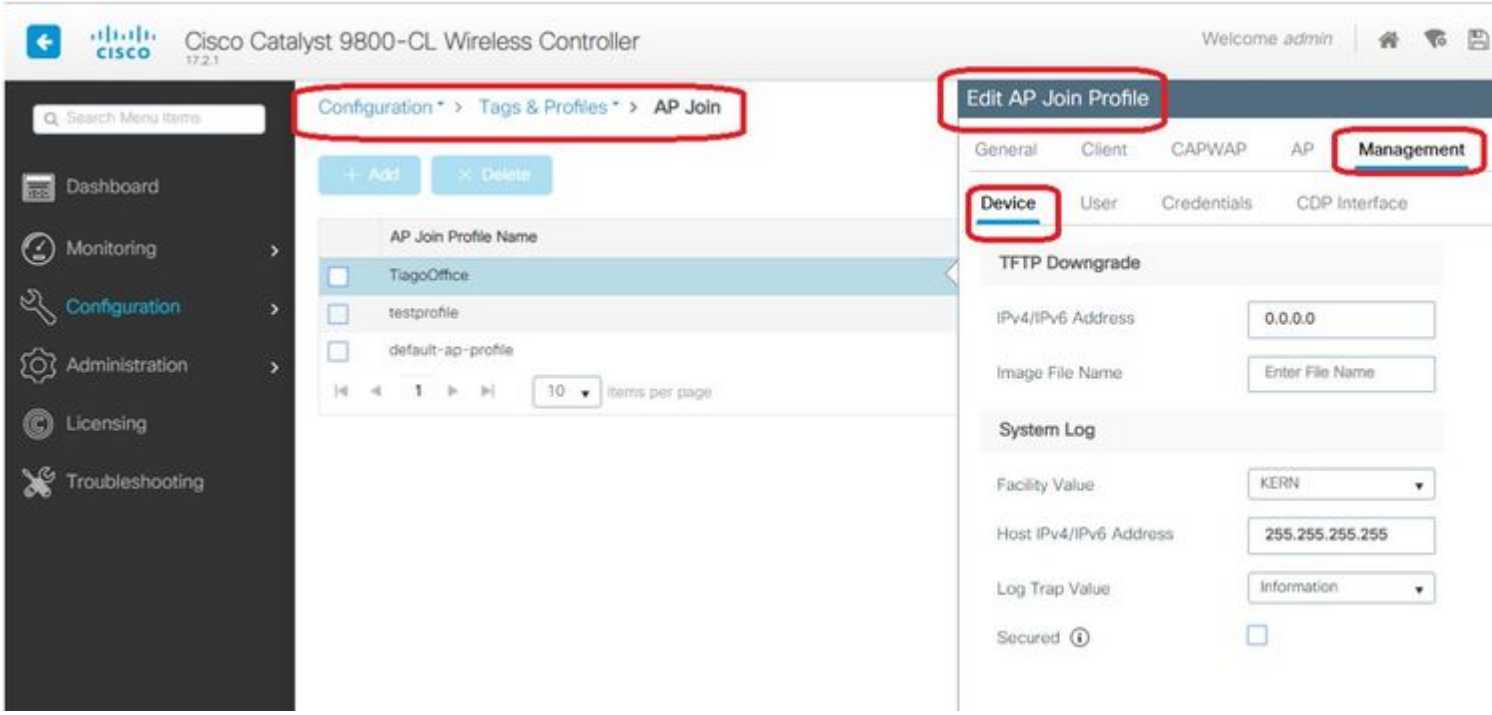
**config-**

**ap**

**-profile**

```
)#core-dump tftp-server 192.168.1.100 file apCores uncompress
```

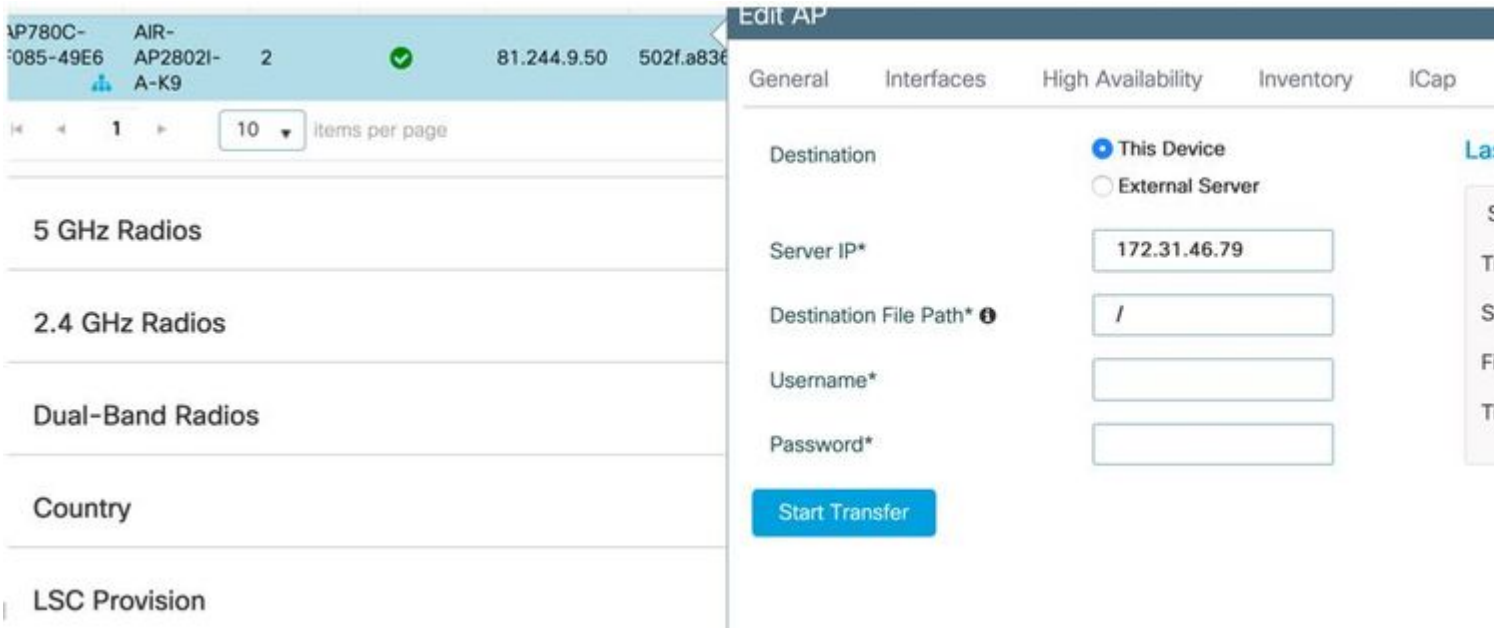
## GUI de Cisco IOS®




A partir de Cisco IOS® XE 17.3.1, tiene una pestaña Support Bundle y puede descargar el AP SB desde la GUI del WLC.

Todo lo que hace es ejecutar el comando "***copy support-bundle***" en el AP y lo envía vía SCP al WLC (porque el WLC puede ser un servidor SCP).

Y luego puedes descargarlo desde tu navegador:




Esto significa que usted puede hacer manualmente el mismo truco en las versiones del eWLC antes de 17.3.1:

Copie el paquete de soporte del AP vía SCP a la IP del eWLC si usted no tiene un servidor TFTP alcanzable al AP.

El eWLC es generalmente alcanzable vía SSH desde el AP, así que ése es un buen truco para pre-17.3.

Paso 1. Activar SSH en 9800 v17.2.1

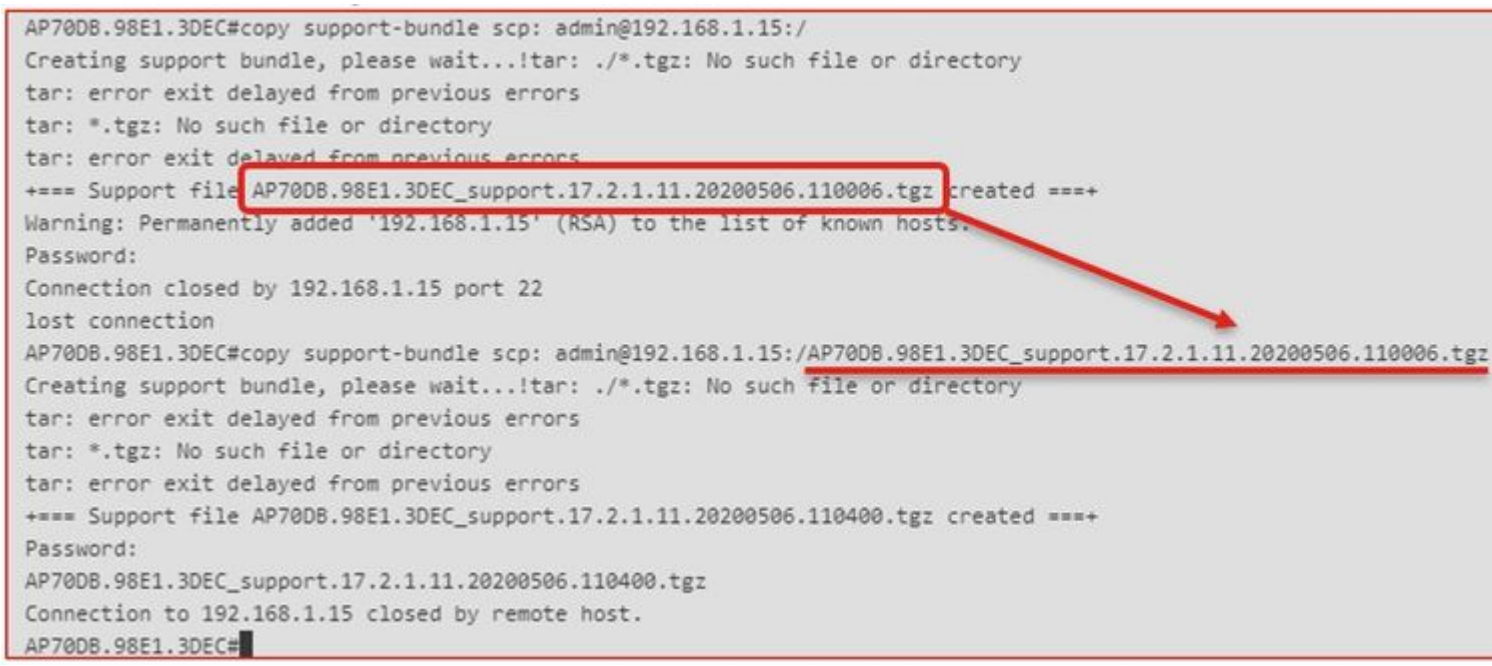
Paso 2. Habilitación de SCP en Cisco IOS® XE v17.2.1

Este ejemplo muestra cómo configurar la funcionalidad de servidor de SCP. Este ejemplo utiliza un nombre de usuario y una contraseña definidos localmente:

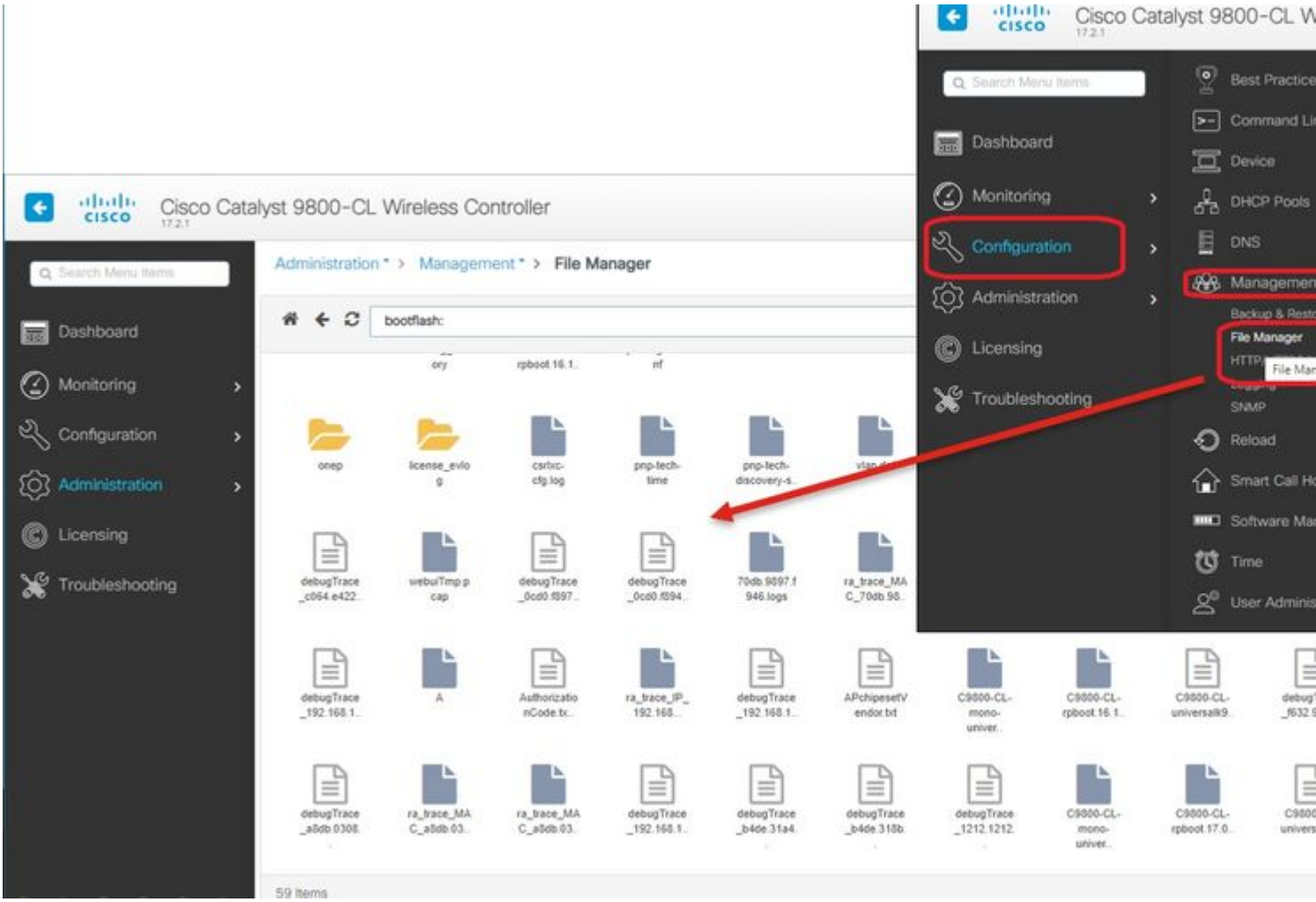
```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
Device(config)# ip scp server enable
Device(config)# end
```

Paso 3. Utilice el comando "***copy support-bundle***" y necesitamos especificar el nombre de archivo que se creará en el servidor SCP.

Sugerencia: Puede ejecutar el comando una vez para obtener un nombre de archivo significativo y, a continuación, copiar/pegar ese nombre de archivo en el comando:




Paso 4. A continuación, puede ir en la GUI eWLC y obtener el archivo en: **Administration > Management > File Manager**:




## IoT y Bluetooth

Los registros del servidor gRPC se pueden verificar en el AP con :

```
AP# show grpc server log
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces conn url 10.22.243.33:8000"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] launching token request cycle"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces token expiration time 2020-04-02 01:36:52 +000
time="2020-04-01T01:36:52Z" level=info msg=" Calling startDNASpacesConn routine "
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Receive Success status"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Connection not in ready state sleeping for 10 seconds
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Setup Stream for the gRPC connection"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Connect RPC Succeeded."
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] RX  routine got enabled "
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] TX routine got enabled "
```

La conectividad con el conector DNA Spaces se puede verificar con :

```
AP# show cloud connector key access
Token Valid : Yes
Token Stats :
        Number of Attempts  : 44
        Number of Failures  : 27
        Last Failure on     : 2020-03-28 02:02:15.649556818 +0000 UTC m=+5753.097022576
        Last Failure reason : curl: SSL connect error
        Last Success on     : 2020-04-01 00:48:37.313511596 +0000 UTC m=+346934.760976625
        Expiration time     : 2020-04-02 00:48:37 +0000 UTC
Connection Retry Interval : 30
```

```
AP# show cloud connector connection detail
Connection State           : READY
Connection Url             :  10.22.243.33:8000
Certificate Available      :  true
Controller Ip              :  10.22.243.31
Stream Setup Interval      :  30
Keepalive Interval         :  30
Last Keepalive Rcvd On     :  2020-04-01 00:32:47.891433113 +0000 UTC m=+345985.338898246
Number of Dials               :  2
Number of Tx Pkts             :  2788175
Number of Rx Pkts             :  11341
Number of Dropped Pkts        :  0
Number of Rx Keepalive        :  11341
Number of Tx Keepalive        :  11341
Number of Rx Cfg Request      :  0
Number of Tx AP Cfg Resp      :  0
Number of Tx APP Cfg Resp     :  0
Number of Tx APP state pkts   :  5
Number of Tx APP data pkts    :  2776829
```

Para ver la configuración de difusión BLE actual del AP:

```
AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config
-------------------
Active profile           : v-iBeacon
Profile 0 (iBeacon)
UUID                     : 00001000000000000000000000000000
Interval (ms)            : 100
Power (dBm)              : -21
Advertised Power (dBm)   : -65
Minor                    : 0
Major                    : 0
TxPower byte             : bfbfbfbfbfbfbfbfbfbfbfbfbf

Profile 1 (Eddystone UID)
Namespace (hex)          : 0000000000005446089c
Instance-ID (hex)        : 7f0000001f00

Profile 2 (Eddystone URL)
URL                      : http://www.
```

Para ver los resultados escaneados:

```
AP# show controllers ioTRadio ble 0 scan brief
      Profile               MAC  RSSI(-dBm)  RSSI@1meter(-dBm)        Last-heard
      Unknown 3C:1D:AF:62:EC:EC          88                  0 0000D:00H:00M:01S
      iBeacon 18:04:ED:04:1C:5F          86                 65 0000D:00H:00M:01S
      Unknown 18:04:ED:04:1C:5F          78                 65 0000D:00H:00M:01S
      Unknown 04:45:E5:28:8E:E7          85                 65 0000D:00H:00M:01S
      Unknown 2D:97:FA:0F:92:9A          91                 65 0000D:00H:00M:01S
      iBeacon E0:7D:EA:16:35:35          68                 65 0000D:00H:00M:01S
      Unknown E0:7D:EA:16:35:35          68                 65 0000D:00H:00M:01S
      iBeacon 04:EE:03:53:74:22          45                256 0000D:00H:00M:01S
      Unknown 04:EE:03:53:74:22          45                256 0000D:00H:00M:01S
              04:EE:03:53:6A:3A          72                N/A 0000D:00H:00M:01S
      Unknown 04:EE:03:53:6A:3A          72                 65 0000D:00H:00M:01S
      iBeacon E0:7D:EA:16:35:35          68                 65 0000D:00H:00M:01S
      Unknown E0:7D:EA:16:35:35          67                 65 0000D:00H:00M:01S
      iBeacon 04:EE:03:53:74:22          60                256 0000D:00H:00M:01S
      Unknown 04:EE:03:53:74:22          60                256 0000D:00H:00M:01S
Eddystone URL 04:EE:03:53:6A:3A          72                N/A 0000D:00H:00M:01S
```

Cuando el AP actúa en el modo de gateway de BLE avanzado donde se implementa una aplicación, puede verificar el estado de la aplicación de IoX con :

```
AP#show iox applications
Total Number of Apps : 1
--------------------------
App Name                      : cisco_dnas_ble_iox_app
   App Ip                     : 192.168.11.2
   App State                  : RUNNING
   App Token                  : 02fb3e98-ac02-4356-95ba-c43e8a1f4217
   App Protocol               : ble
   App Grpc Connection        : Up
   Rx Pkts From App           : 3878345
   Tx Pkts To App             : 6460
   Tx Pkts To Wlc             : 0
   Tx Data Pkts To DNASpaces  : 3866864
   Tx Cfg Resp To DNASpaces   : 1
   Rx KeepAlive from App      : 11480
   Dropped Pkts               : 0
   App keepAlive Received On  : Mar 24 05:56:49
```

Puede conectarse a la aplicación IOX con estos comandos y luego monitorear los registros durante la configuración de la baliza de piso :

```
AP#connect iox application
/ #

/# tail -F /tmp/dnas_ble.log
Tue Mar 24 06:55:21 2020 [INFO]: Starting DNA Spaces BLE IOx Application
Tue Mar 24 06:55:21 2020 [INFO]: Auth token file contents: db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Setting gRPC endpoint to: 1.1.7.101:57777
```

```
Tue Mar 24 06:55:21 2020 [INFO]: Auth with token: db26a8ab-e800-4fe9-a128-80683ea17b12
Tue Mar 24 06:55:21 2020 [INFO]: Attempt to connect to DNAS Channel
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run metrics
Tue Mar 24 06:55:21 2020 [INFO]: Starting to run Channel Keepalive
Tue Mar 24 06:55:21 2020 [INFO]: Initialize DNAS Reader Channel
Tue Mar 24 06:55:21 2020 [INFO]: Start listener for messages
Tue Mar 24 06:55:21 2020 [INFO]: Running BLE scan thread
```

# Conclusión

Hay muchas herramientas de troubleshooting disponibles para ayudarnos en la resolución de problemas relacionados con los AP COS.

Este documento enumera los más utilizados y se actualiza regularmente.

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).