Risoluzione dei problemi dei punti di accesso COS

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Acquisisci tracce pacchetto (tracce sniffer)
PCAP cablato su porta AP
Procedura
Opzioni del comando
Protocollo PCAP cablato tramite filtro
Acquisizione radio
Procedura
Verifica
Altre opzioni
Controllo della traccia del client AP dal WLC 9800
AP Catalyst 91xx in modalità sniffer
Suggerimenti per la risoluzione dei problemi
MTU percorso
Per abilitare i debug all'avvio
Meccanismo di risparmio energetico
QoS client
Scansione off-channel
Connettività client
Scenari di Flexconnect
File system AP
Archivia e invia syslog
Pacchetto di supporto AP
Raccogli file di base AP in remoto
CLI AireOS
Interfaccia grafica AireOS
CLI di Cisco IOS®
GUI Cisco IOS®
IoT e Bluetooth
Conclusioni

Introduzione

Questo documento descrive alcuni degli strumenti di risoluzione dei problemi disponibili per i Cheatah OS AP (alias COS AP).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Questo documento si concentra sui punti di accesso COS, come i modelli AP delle serie 2800, 3800, 1560 e 4800, nonché sui nuovi 11ax AP Catalyst 91xx.

Nel documento vengono descritte molte delle funzionalità disponibili in AireOS 8.8 e versioni successive. E anche Cisco IOS® XE 16.2.2s e versioni successive.

Nelle versioni precedenti, sono disponibili alcuni commenti sulla disponibilità di alcune funzionalità.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Acquisisci tracce pacchetto (tracce sniffer)

PCAP cablato su porta AP

È possibile (a partire dalla versione 8.7 con il filtro disponibile nella versione 8.8) applicare un cappuccio alla porta Ethernet dell'access point. È possibile visualizzare il risultato in tempo reale sulla CLI (solo con i dettagli del pacchetto di riepilogo) o salvarlo come cap completo nella memoria flash dell'access point.

La protezione per cavi cattura tutto il contenuto sul lato Ethernet (sia Rx che Tx) e il punto di rubinetto all'interno dell'access point viene raggiunto immediatamente prima che il pacchetto venga inoltrato.

Tuttavia, acquisisce solo il traffico del piano CPU del punto di accesso, ossia il traffico da e verso il punto di accesso (DHCP del punto di accesso, tunnel di controllo capwap del punto di accesso, ecc.) e non mostra il traffico del client.

Notare che le dimensioni sono molto limitate (limite massimo di 5 MB), quindi può essere necessario configurare dei filtri per acquisire solo il traffico a cui si è interessati.

Arrestare l'acquisizione del traffico senza eseguire il debug dell'acquisizione IP cablata del traffico o semplicemente annullare il debug di tutto prima di provare a copiarla (altrimenti la copia non termina quando i pacchetti vengono ancora scritti).

Procedura

Passaggio 1. Avviare il pcap; selezionare il tipo di traffico con "debug traffic wired ip capture" (Esegui debug 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)
```

Passaggio 2. Attendere il flusso del traffico, quindi arrestare l'acquisizione con il comando "no debug traffic wired ip capture" o semplicemente "undebug all":

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

Passaggio 3. Copiare il file sul server tftp/scp:

<#root>

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

AP70DB.98E1.3DEC_capture.pcap0

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

Passaggio 4. A questo punto è possibile aprire il file in wireshark. Il file è pcap0. Passate a pcap in modo che si associ automaticamente a wireshark.

Opzioni del comando

Il comando debug traffic wired offre diverse opzioni che consentono di acquisire il traffico specifico:

```
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
```

È possibile aggiungere "verbose" alla fine del comando debug per visualizzare il dump esadecimale del pacchetto. Tenere presente che questo può sovraccaricare la sessione CLI molto rapidamente se il filtro non è sufficientemente stretto.

Protocollo PCAP cablato tramite filtro

Il formato del filtro corrisponde al formato del filtro di acquisizione tcpdump.

	Esempio di filtro	**Descrizione**
Host	"host 192.168.2.5"	In questo modo viene filtrata l'acquisizione dei pacchetti in modo da raccogliere solo i pacchetti provenienti o diretti all'host 192.168.2.5.
	"host src 192.168.2.5"	Filtra l'acquisizione dei pacchetti per raccogliere solo i pacchetti provenienti da 192.168.2.5.

	"host dst 192.168.2.5"	Filtra l'acquisizione dei pacchetti per raccogliere solo i pacchetti che vanno a 192.168.2.5.
Port	"porta 443"	Questa opzione filtra l'acquisizione dei pacchetti per raccogliere solo i pacchetti con origine o destinazione 443.
	"src port 1055"	Il traffico che proviene dalla porta 1055.
	"porta dst 443"	Acquisisce il traffico destinato alla porta 443.

Di seguito è riportato un esempio di output visualizzato sulla console ma filtrato in modo da visualizzare solo i pacchetti dati CAPWAP:

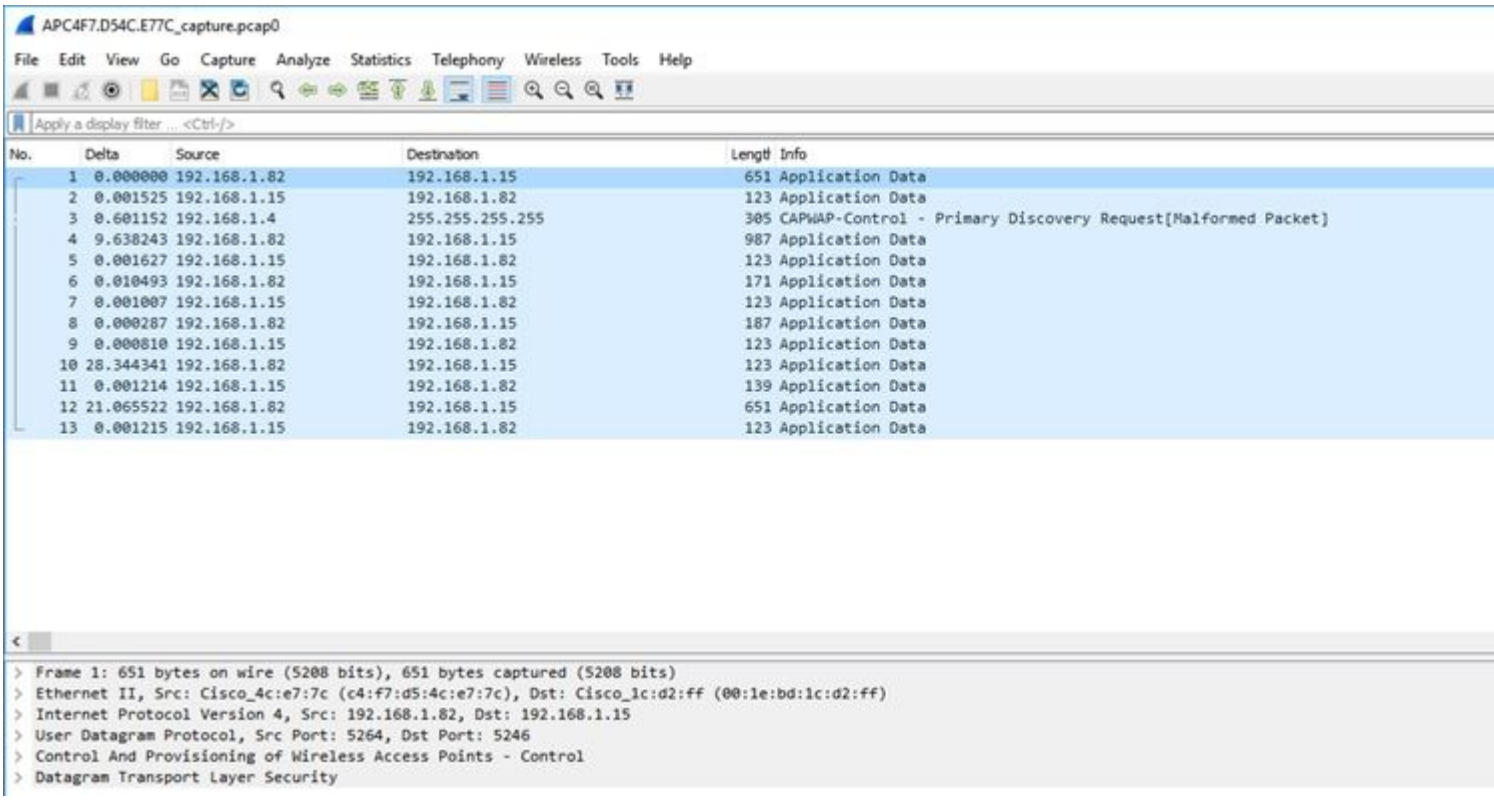
```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
12:20:50.483125 IP APC4F7-D54C-E77C.lan.5264 > 192.168.1.15.5246: UDP, length 81
12:20:50.484361 IP 192.168.1.15.5246 > APC4F7-D54C-E77C.lan.5264: UDP, length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

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

Esempio di output su file:

```
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#
```

Per aprire la cattura su wireshark:



Acquisizione radio

È possibile abilitare la cattura dei pacchetti sul control plane della radio. A causa dell'impatto sulle prestazioni, non è possibile eseguire l'acquisizione sulla corsia dati radio.

Ciò significa che il flusso dell'associazione client (probe, autenticazione, associazione, eap, arp, pacchetti dhcp e pacchetti di controllo ipv6, icmp e ndp) è visibile ma non i dati passati dal client dopo il passaggio allo stato connesso.

Procedura

Passaggio 1. Aggiungere l'indirizzo MAC del client rilevato. È possibile aggiungere diversi indirizzi MAC. È inoltre possibile eseguire il comando per tutti i client, ma non è consigliabile.

```
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.
```

Passaggio 2. Impostare un filtro per registrare solo i protocolli specifici o tutti i protocolli supportati:

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

Passaggio 3. Scegliere di visualizzare l'output sulla console (in modo asincrono):

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

Passaggio 4. Avvia la traccia.

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

Esempio:

<#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
```

Per interrompere la cattura:

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

Verifica

Verifica traccia client:

<#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
```

Esempio di connessione client riuscita:

Le lettere tra parentesi consentono di capire dove è stato visualizzato il frame (E per Ethernet, W per Wireless, C per il modulo Click quando è interno all'access point) e in quale direzione (Carica o Scarica).

Ecco una piccola tabella con il significato di queste lettere:

U - Pacchetto uplink (dal client)
D - downlink packet (fare clic con il mouse)
W - driver wireless del modulo
Driver Ethernet modulo E
C - modulo Clic

Altre opzioni

Visualizza registro in modo asincrono:

I log possono quindi essere consultati con il comando: "**show ap client-trace events mac xx:xx:xx:xx:xx:xx**" (o sostituire il mac con "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
```

Scarica i pacchetti in formato esadecimale

È possibile eseguire il dump dei pacchetti in formato esadecimale nella 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
```

```
AP70DB.90E1.3DEC#configure ap client-trace start
Warning: To recover WLC pushed config, need CAPWAP restart or reload to re-apply the config from WLC
AP70DB.90E1.3DEC#Apr  6 13:20:53 kernel: [*04/06/2020 13:20:53.2837] systemd[1]: Starting Lighttpd Watcher...
Apr  6 13:20:53 kernel: [*04/06/2020 13:20:53.3269] systemd[1]: Started Lighttpd Watcher.
configure ap client-trace output dump address add a8:db:03:08:4c:4a
AP70DB.90E1.3DEC#Apr  6 13:29:02 kernel: [*04/06/2020 13:29:02.5997] MAC already exists: index 0
configure ap client-trace output dump
  address  Remote/Local dump Client Addresses
  enable   Enable Trace output for local dump
AP70DB.90E1.3DEC#configure ap client-trace output dump enable
  <4-5000>  Enter the packet dump length value
AP70DB.90E1.3DEC#configure ap client-trace output dump enable 100
  <cr>
AP70DB.90E1.3DEC#configure ap client-trace output dump enable 100
AP70DB.90E1.3DEC#Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4648]
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4648] Time:464876us Dir:Rx Rate:m7.2-2  Rssi:-43 Ch:1 Fc:188 Dur:30 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 54:7c:69:b7:3f:42 Seq:1
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0010 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0020 00 00 13 88 15 b3 ff ff 00 00 00 00 ff ab cd 02 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0030 00 00 37 00 00 00 06 00 07 00 01 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0040 00 01 2c 00 00 49 31 21 0f d5 a0 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0050 00 00 00 00 3e 00 3e 00 00 5e 8b 2e b6 00 07 30
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0060 ed 88 01 30 00 00 27 e3 36 4d a0 a8 db 03 08 4c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0070 4a 54 7c 69 b7 3f 42 60 12 00 00 aa aa 03 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4650] 0080 00 08 06 00 01 08 00 06 04 00 01 a8 db 03 08 4c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4650] 0090 4a c0 a8 65
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4740]
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4740] Time:474803us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:200 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 54:7c:69:b7:3f:42 Seq:6(6)
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0010 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 50 00 50
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0030 00 00 5e 8b 2e b6 00 07 3f 50 02 01 00 00 88 02
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 54 7c
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0050 69 b7 3f 42 60 00 00 00 aa aa 03 00 00 00 08 06
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0060 00 01 08 00 06 04 00 02 54 7c 69 b7 3f 42 c0 a8
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0070 65 01 a8 db 03 08 4c 4a c0 a8 65 0d 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4750] 0090 00 00 6b 6b 6b 6b 6b 6b
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] Time:180019us Dir:Rx Rate:5 Rssi:-36 Ch:1 Fc:40 Dur:0 ff:ff:ff:ff:ff:ff a8:db:03:08:4c:4a ff:ff:ff:ff:ff:ff Seq:277(631)
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0010 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0020 00 00 13 88 15 b3 ff ff 00 00 dc c8 00 ad 00 ad
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0030 00 00 5e 8b 2f 16 00 02 c2 75 0b 01 14 00 40 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0040 00 00 ff ff ff ff ff ff a8 db 03 08 4c 4a ff ff
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0050 ff ff ff ff 70 27 00 00 01 04 02 04 0b 16 32 08
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0060 0c 12 18 24 30 48 60 6c 03 01 01 2d 1a 2d 00 1b
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0070 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0080 00 00 00 00 00 00 7f 0a 00 00 48 00 00 40 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0090 40 00 21 ff
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] Time:200019us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:50 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:65e(16
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0010 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 e2 00 e2
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0030 00 00 5e 8b 2f 16 00 02 c2 96 02 01 00 00 50 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0040 3a 01 a8 db 03 08 4c 4a 00 27 e3 36 4d a0 00 27
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0050 e3 36 4d a0 e0 65 96 0c 12 18 24 03 01 0d 64 00
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0060 11 11 00 0c 74 65 73 74 65 77 6c 63 77 6c 61 6e
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0070 01 08 82 84 8b 96 0c 12 18 24 03 01 01 07 06 49
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0080 4c 20 01 0d 12 20 01 00 2a 01 00 32 04 30 48 60
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0090 6c 30 14 01
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001]
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] Time:200161us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:50 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a1 00:27:e3:36:4d:a1 Seq:65f(16
Apr  6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
```

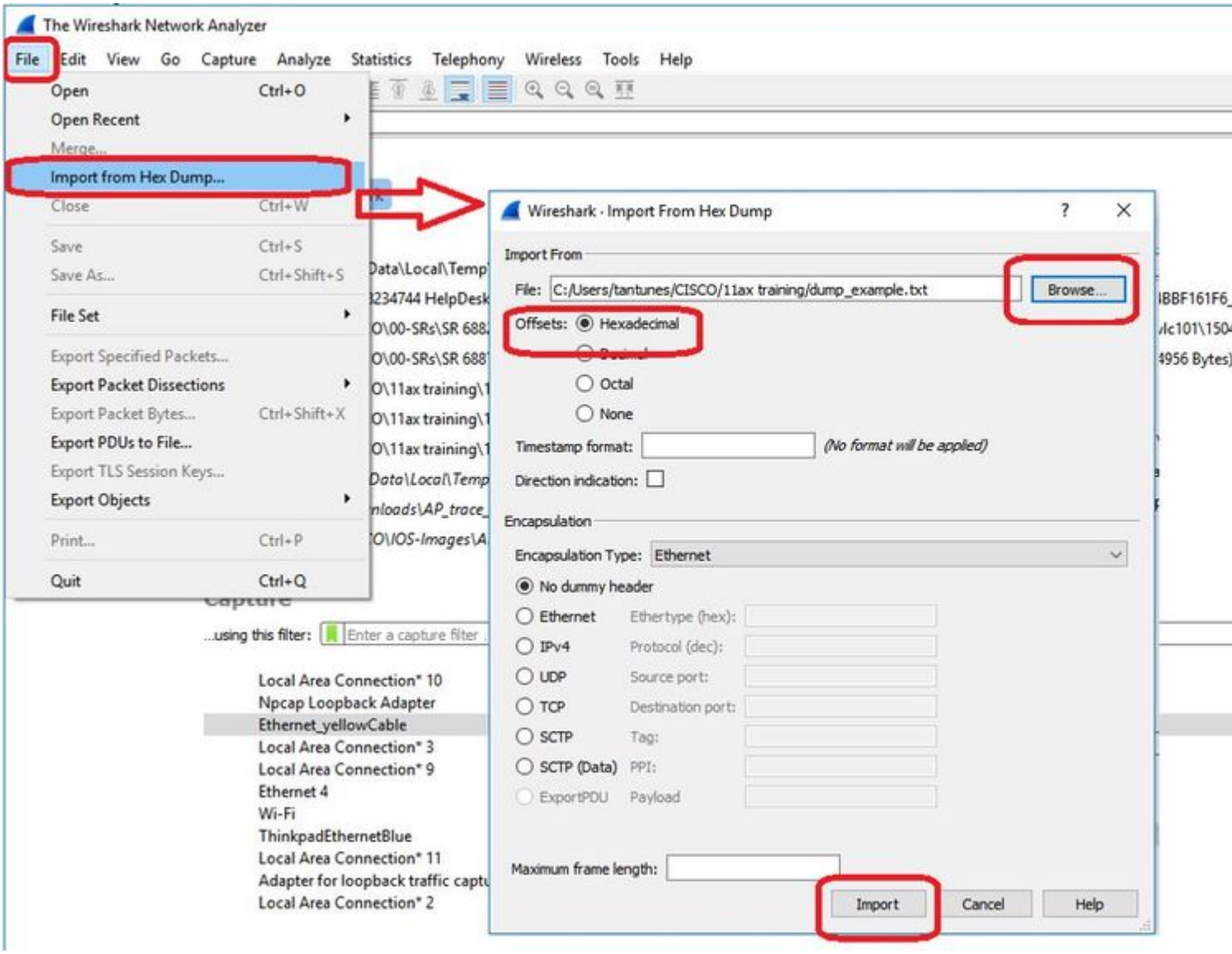
Quindi, è possibile pulire la dump esadecimale e salvare in formato txt e importare in wireshark:

```
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 00 08 00 45 00
0010 00 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 00 08 00 45 00
0010 00 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 00 08 00 45 00
0010 00 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 00 08 00 45 00
0010 00 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
```



Poiché l'output può essere molto grande e per tenere presente che l'output menziona solo il tipo di frame visualizzato e non i dettagli interni, può essere più efficiente reindirizzare l'acquisizione del pacchetto su un laptop che esegue un'applicazione di acquisizione (ad esempio wireshark).

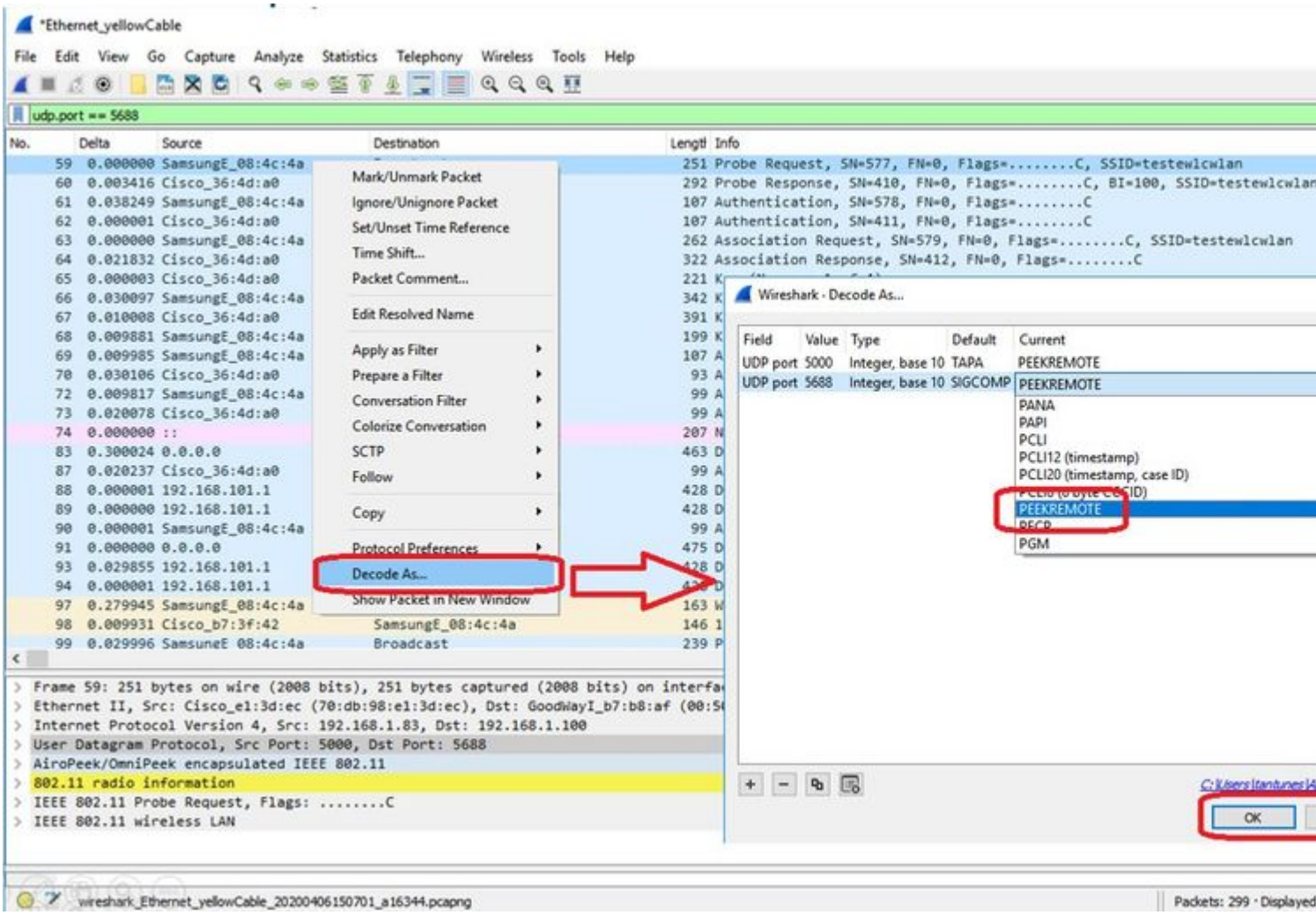
Abilitare la funzione di acquisizione remota per inviare i pacchetti a un dispositivo esterno con wireshark:

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

Il comando indica che l'access point inoltra ogni frame catturato dal filtro di traccia del client verso il notebook in modalità 192.168.68.68 e usa l'incapsulamento PEEKREMOTE (proprio come gli access point in modalità sniffer) sulla porta 5000.

Un limite è rappresentato dal fatto che il laptop di destinazione deve trovarsi nella stessa subnet dell'access point su cui si esegue questo comando. È possibile modificare il numero di porta in base a qualsiasi criterio di sicurezza in vigore nella rete.

Una volta ricevuti tutti i pacchetti sul laptop con Wireshark, è possibile fare clic con il pulsante destro del mouse sull'intestazione udp 5000 e scegliere **decodifica con nome** e scegliere PEEKREMOTE, come mostrato nella seguente figura:



Elenco di bug e miglioramenti relativi a questa funzione:

ID bug Cisco CSCvm09020 DNS non più visibile dalla traccia del client nella versione 8.8

ID bug Cisco CSCvm09015 nella traccia client vengono visualizzati molti valori di ICMP_other con numero di sequenza null

ID bug Cisco CSCvm02676 AP COS client-trace non acquisisce i pacchetti webauth

Cisco ID bug CSCvm02613 L'output remoto di traccia client AP COS non funziona

Cisco ID bug CSCvm00855 Numeri SEQ di traccia client incoerenti

Controllo della traccia del client AP dal WLC 9800

È possibile configurare più access point in modo che eseguano una traccia del client radio e la attivino dal

Passaggio 1. Configurare un profilo di traccia AP che definisca il traffico da acquisire

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

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

Passaggio 2. Aggiungere il profilo di traccia AP a un profilo di join AP utilizzato dagli access point di destinazione.

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

Accertarsi che il profilo di join sia applicato a un tag del sito utilizzato dai punti di accesso di destinazione

Passaggio 4 Avvio/arresto del trigger

```
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
```

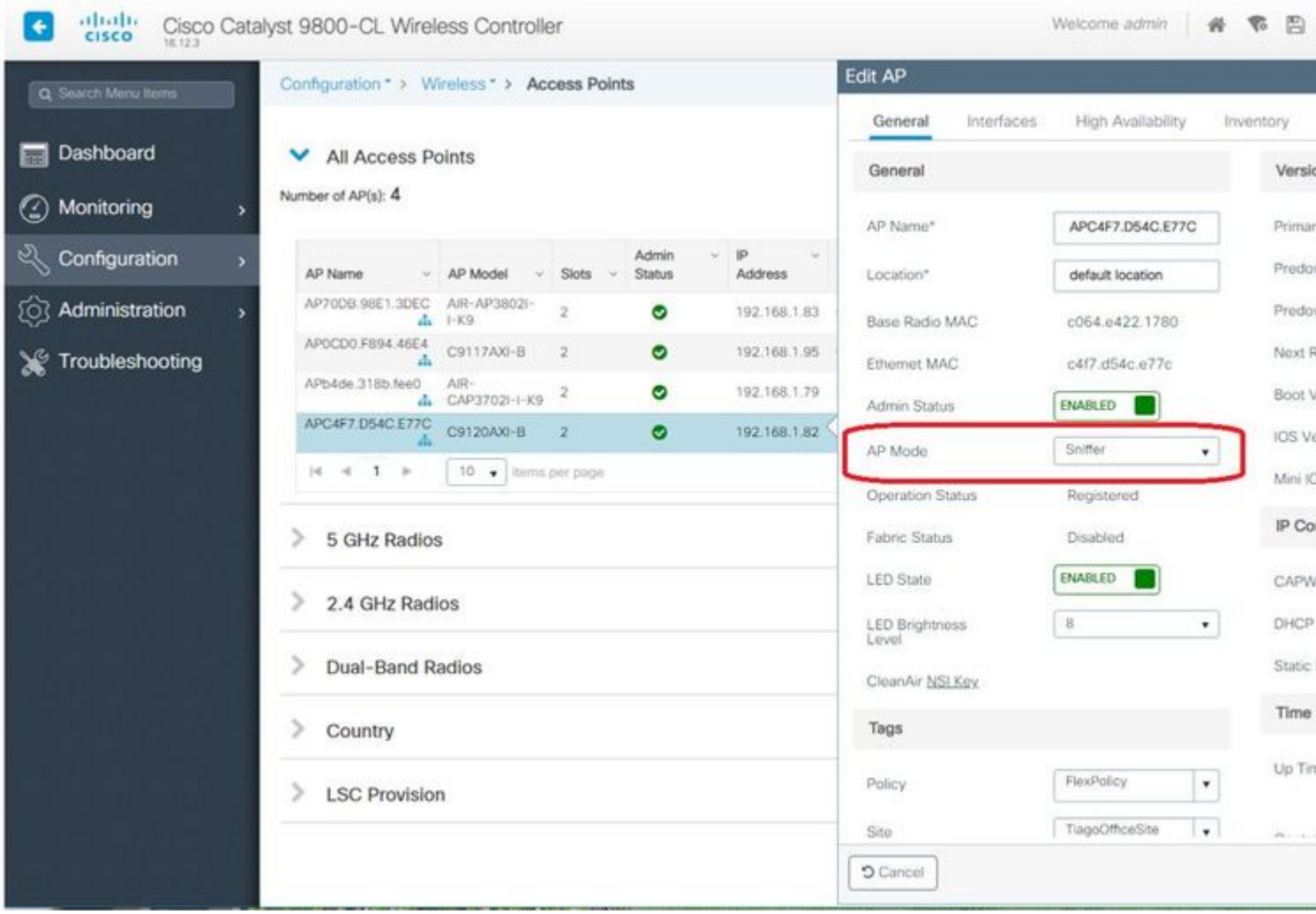
```
client all/
```

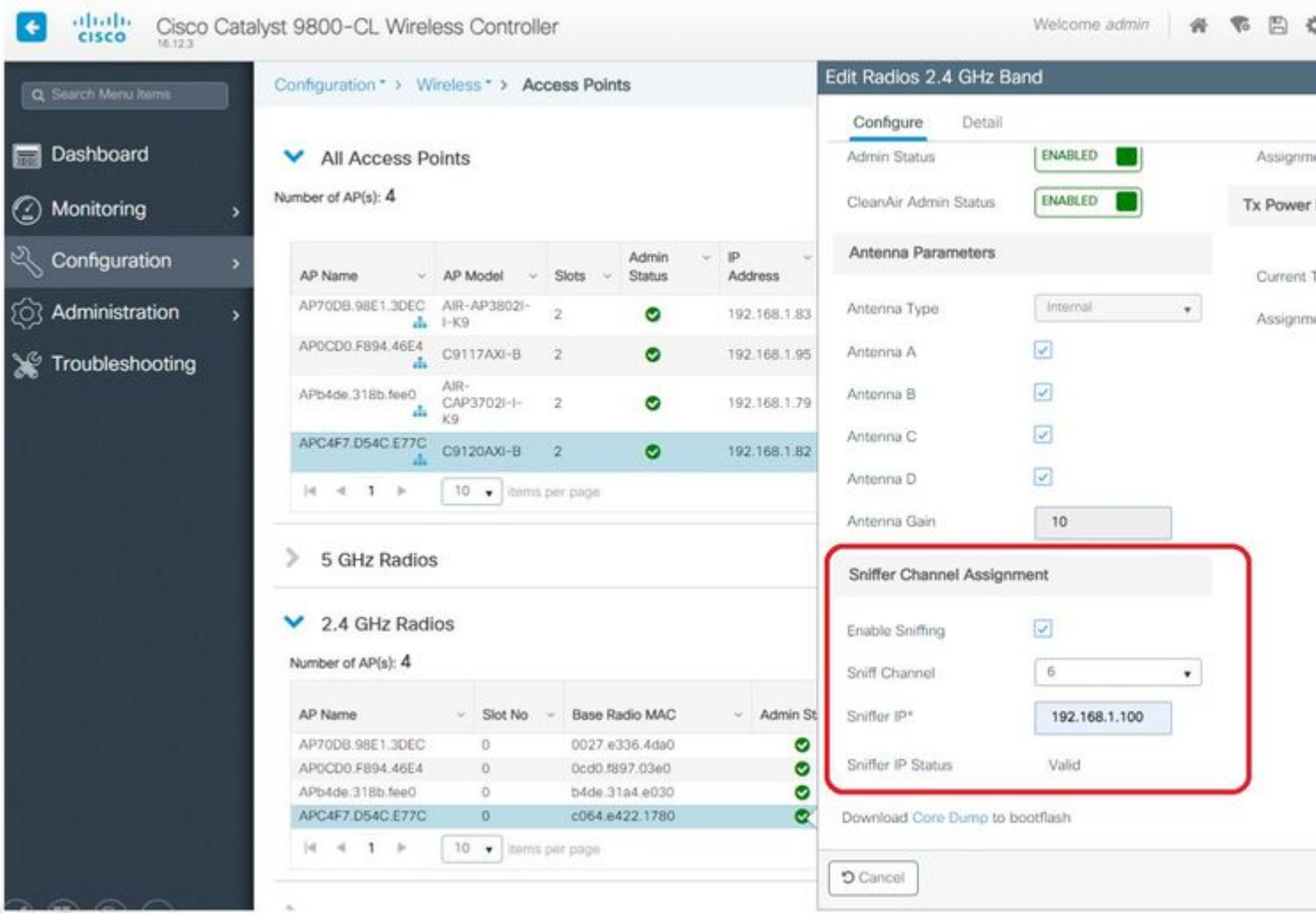
Comandi di verifica:

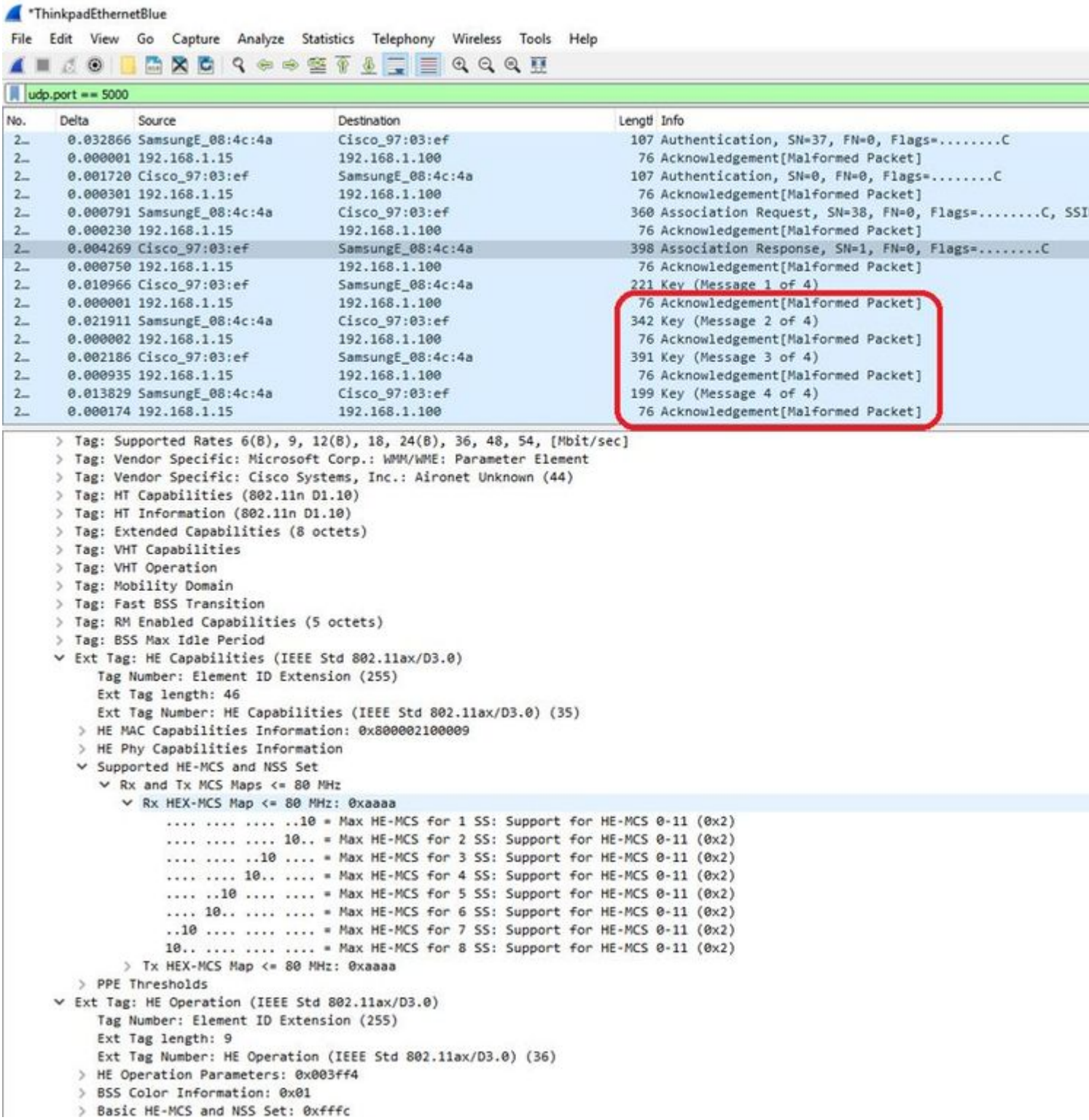
```
show wireless profile ap trace summary
show wireless profile ap trace detailed PROF_NAME detail
sh ap trace client summary
show ap trace unsupported-ap summary
```

AP Catalyst 91xx in modalità sniffer

I nuovi Catalyst 9115, 9117, 9120 e 9130 possono essere configurati in modalità sniffer. La procedura è simile ai modelli AP precedenti.


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: i frame di dati inviati alla velocità di trasmissione dati WIFI 6 vengono acquisiti ma, poiché peekremote non è aggiornato su Wireshark, vengono visualizzati come 802.11ax phy type al momento. La correzione è in Wireshark 3.2.4 dove Wireshark mostra la corretta frequenza di WiFi6.

Nota: in questo momento i Cisco AP non sono in grado di acquisire frame MU-OFDMA, ma possono acquisire i frame di trigger (inviati alla velocità di gestione dei dati) che annunciano una finestra MU-OFDMA. È già possibile dedurre che MU-OFDMA si verifica (o meno) e con quale client.

Suggerimenti per la risoluzione dei problemi

MTU percorso

Anche se il rilevamento della MTU del percorso trova la MTU ottimale per l'access point, è possibile ignorare manualmente queste impostazioni.

Sul protocollo WLC 8.10.130, il comando **config ap pmtu disable <ap/all>**imposta una MTU statica per uno o tutti gli access point anziché basarsi sul meccanismo di rilevamento dinamico.

Per abilitare i debug all'avvio

È possibile eseguire il comando config boot debug capwap per abilitare i debug capwap, DTLS e DHCP all'avvio successivo, anche prima dell'avvio del sistema operativo e della visualizzazione del prompt.

Inoltre, si dispone di "config boot debug memory xxxx" per diversi debug della memoria.

Per verificare se i debug di avvio sono abilitati o meno, usare il comando "show boot" al successivo riavvio.

I parametri possono essere disabilitati aggiungendo la parola chiave disable al termine della procedura, ad esempio "config boot debug capwap disable".

Meccanismo di risparmio energetico

Il risparmio energia di un determinato client può essere risolto eseguendo

debug client trace <indirizzo mac>

QoS client

Per verificare che i tag QoS siano applicati, è possibile eseguire "***debug capwap client qos***".

Visualizza il valore UP dei pacchetti per i client wireless.

Non è mac filtrabile a partire dalla versione 8.8 (richiesta di miglioramento bug Cisco 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
```

È inoltre possibile verificare la tabella Qos-UP-DSCP sull'access point così come la quantità totale di pacchetti contrassegnati, modellati e scartati da 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#
```

Quando i criteri Qos sono definiti sul WLC e scaricati sull'access point Flexconnect, è possibile verificarli 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
```

In caso di limitazione delle velocità 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
```

Scansione off-channel

Il debug della scansione off-channel dell'access point può essere utile quando si risolvono problemi di

rilevamento rogue (per verificare se e quando l'access point passa su un canale specifico da analizzare), ma può anche essere utile nella risoluzione di problemi video dove un flusso in tempo reale sensibile ottiene interruzioni costanti se la funzione "off channel scan defer" non viene utilizzata.

```
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_I
[*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_I
[*06/11/2020 09:45:43.6570] noise measurement channel 140 noise 97
```

Connettività client

È possibile elencare i client che sono stati deautenticati dal punto di accesso con il timestamp dell'ultimo 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
```

Nell'output precedente, il codice motivo è il codice motivo di deautenticazione, come descritto in questo collegamento:

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

Il vap si riferisce all'identificatore della WLAN all'interno dell'access point (che è diverso dall'ID WLAN sul WLC !!!).

Potete metterlo in relazione incrociata con altri output dettagliati successivamente, che menziona sempre il vap dei client associati.

È possibile visualizzare l'elenco degli ID VAP con "***show controller Dot11Radio 0/1 wlan***".

Quando i client sono ancora associati, è possibile ottenere dettagli sulla loro connessione 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
```

Per ulteriori dettagli sulla voce relativa al cliente, consultare:

```
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
```

È possibile forzare la disconnessione di un client specifico con:

```
test dot11 client deauthenticate
```

I contatori del traffico possono essere ottenuti per client 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#
```

A livello di radio, molte informazioni possono essere ottenute in "***show controllers***". Quando si aggiunge l'indirizzo MAC del client, vengono visualizzate le velocità dati supportate, le velocità dati correnti, le funzionalità PHY, nonché la quantità di tentativi e errori di testo:

<#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
```

Per tenere costantemente traccia di una velocità dati client e/o di un valore RSSI, è possibile eseguire "**debug dot11 client rate address <mac>** " e questa operazione registra queste informazioni ogni secondo:

```
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
```

In questo output, i contatori dei pacchetti Tx e Rx sono pacchetti trasmessi nel secondo intervallo dall'ultima stampa, lo stesso per i tentativi Tx. Tuttavia RSSI, SNR e data rate sono i valori dell'ultimo pacchetto dell'intervallo (e non una media per tutti i pacchetti dell'intervallo).

Scenari di Flexconnect

È possibile verificare gli ACL attualmente applicati a un client in uno scenario di pre-autenticazione (ad esempio, CWA) o post-autenticazione:

```
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
```

File system AP

I punti di accesso COS non consentono di elencare tutto il contenuto del file system come nelle piattaforme unix.

Il comando "***show filesystems***" fornisce un dettaglio dell'utilizzo e della distribuzione dello spazio nella partizione corrente:

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

Il comando "***show flash***" elenca i file principali sul flash AP. È inoltre possibile aggiungere la parola chiave syslog o core per elencare tali cartelle specifiche.

```
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
```

Archivia e invia syslog

La cartella syslog memorizza l'output syslog dei riavvii precedenti. Il comando "***show log***" mostra syslog solo dopo l'ultimo riavvio.

Ad ogni ciclo di riavvio, i syslog vengono scritti su file incrementali.

```
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
```

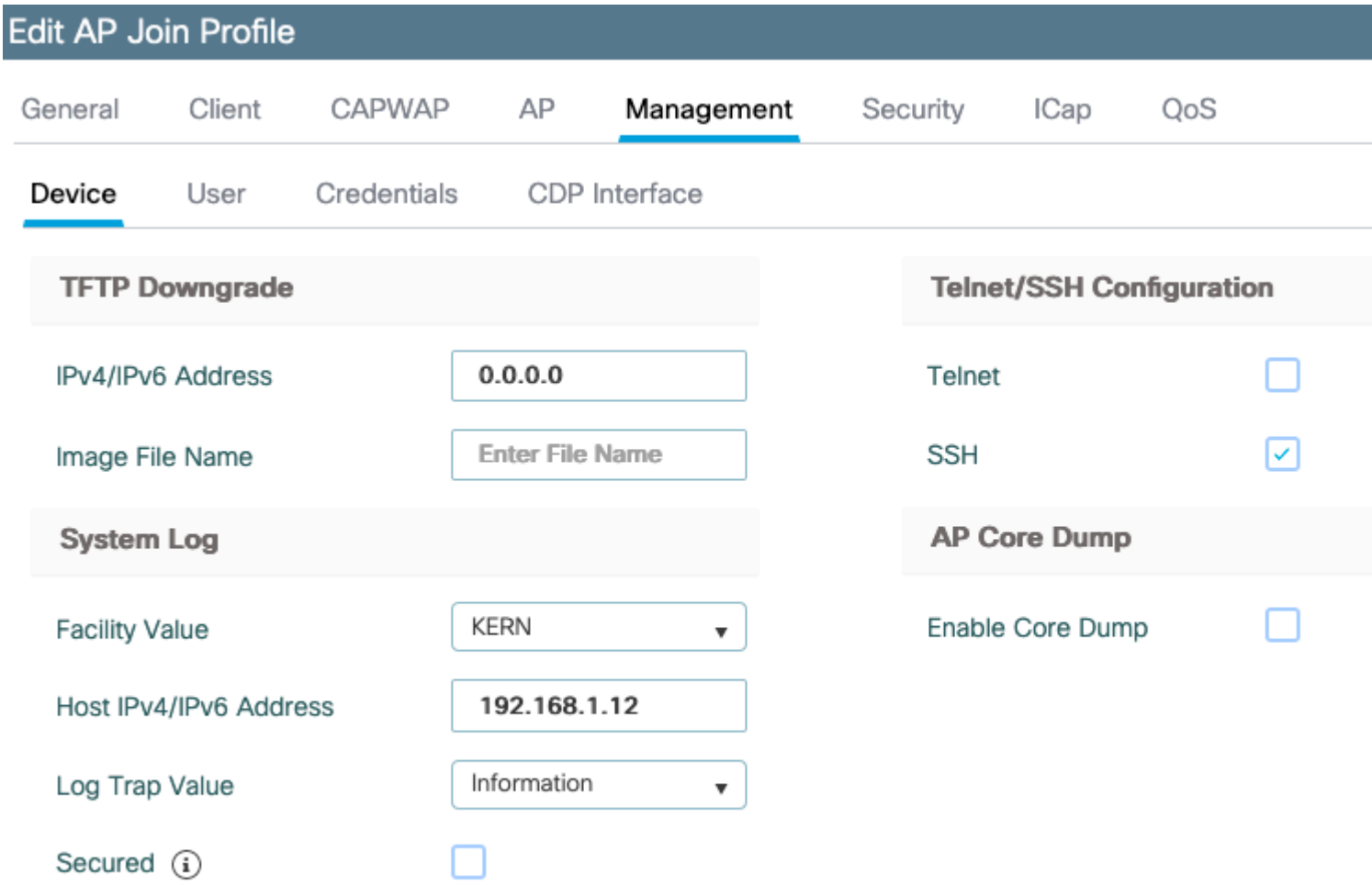
Il primo output dopo l'avvio iniziale è il file 1.0 e viene creato un file 1.1 se la versione 1.0 diventa troppo lunga. Dopo il riavvio, viene creato un nuovo file 2.0 e così via.

Dal WLC, è possibile configurare la destinazione del syslog se si desidera che gli access point inviino i messaggi unicast del syslog a un server specifico.

Per impostazione predefinita, gli access point inviano i syslog a un indirizzo di broadcast che può causare un certo numero di problemi di trasmissione, quindi accertarsi di configurare un server syslog.

Per impostazione predefinita, l'access point invia tramite syslog qualsiasi informazione stampata sull'output della console.

Sul controller 9800, è possibile modificare questi parametri nel profilo Configurazione -> Join AP, in Gestione.



È possibile modificare il valore **Log Trap** per inviare i debug anche tramite syslog. È quindi possibile abilitare i debug sulla CLI dell'access point e l'output di questi messaggi viene inviato al server configurato tramite messaggi syslog.

A causa dell'ID bug Cisco CSCvu75017 ,solo quando si imposta la funzione syslog su KERN (valore predefinito), l'access point invia messaggi syslog in uscita.

Se si stanno risolvendo problemi in cui un access point potrebbe perdere la connettività di rete (o su un server WGB, ad esempio), syslog non è affidabile come nessun messaggio inviato se l'access point perde la connettività uplink.

Pertanto, l'utilizzo dei file syslog archiviati in flash è un ottimo modo per eseguire il debug e memorizzare l'output sull'access point stesso e quindi caricarlo periodicamente in seguito.

Pacchetto di supporto AP

Alcune informazioni di diagnostica di vario tipo raccolte di frequente possono essere rese disponibili in un unico pacchetto che è possibile caricare dai punti di accesso.

Le informazioni di diagnostica che è possibile includere nel bundle sono:

- AP show tech
- syslog AP

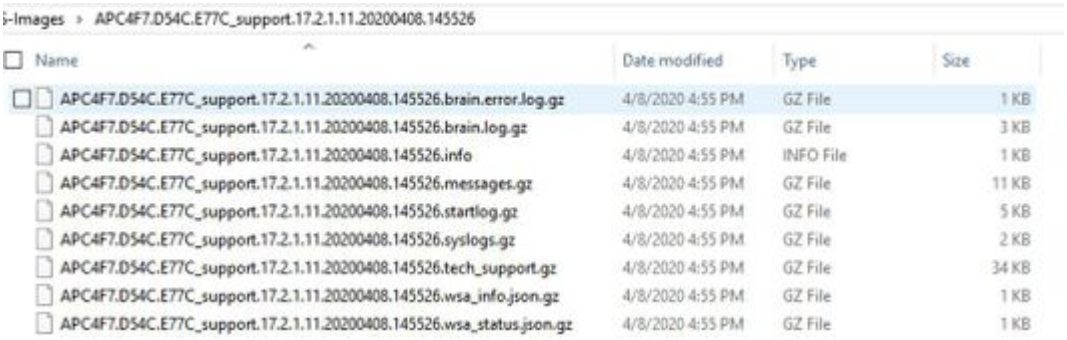
- Log Brain Capwapd AP
- Registri di avvio e messaggi AP
- File Coredump AP

Per ottenere il bundle di supporto per l'access point, andare nella CLI dell'access point e immettere il comando "***copy* support-bundle tftp: x.x.x.x**".

A questo punto è possibile controllare il file denominato con il nome dell'access point seguito dal nome **support.apversion.date.time.tgz**, come mostrato di seguito:

```
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#
```

Quando si "disattiva" il file è possibile visualizzare i vari file raccolti:



Raccogli file di base AP in remoto

Per raccogliere i file di base dell'access point in remoto, abilitare il dump del core da includere nel pacchetto di supporto, quindi caricare il pacchetto di supporto dall'access point o inviarlo direttamente al server FTP. Negli esempi seguenti viene utilizzato il server tftp 192.168.1.100.

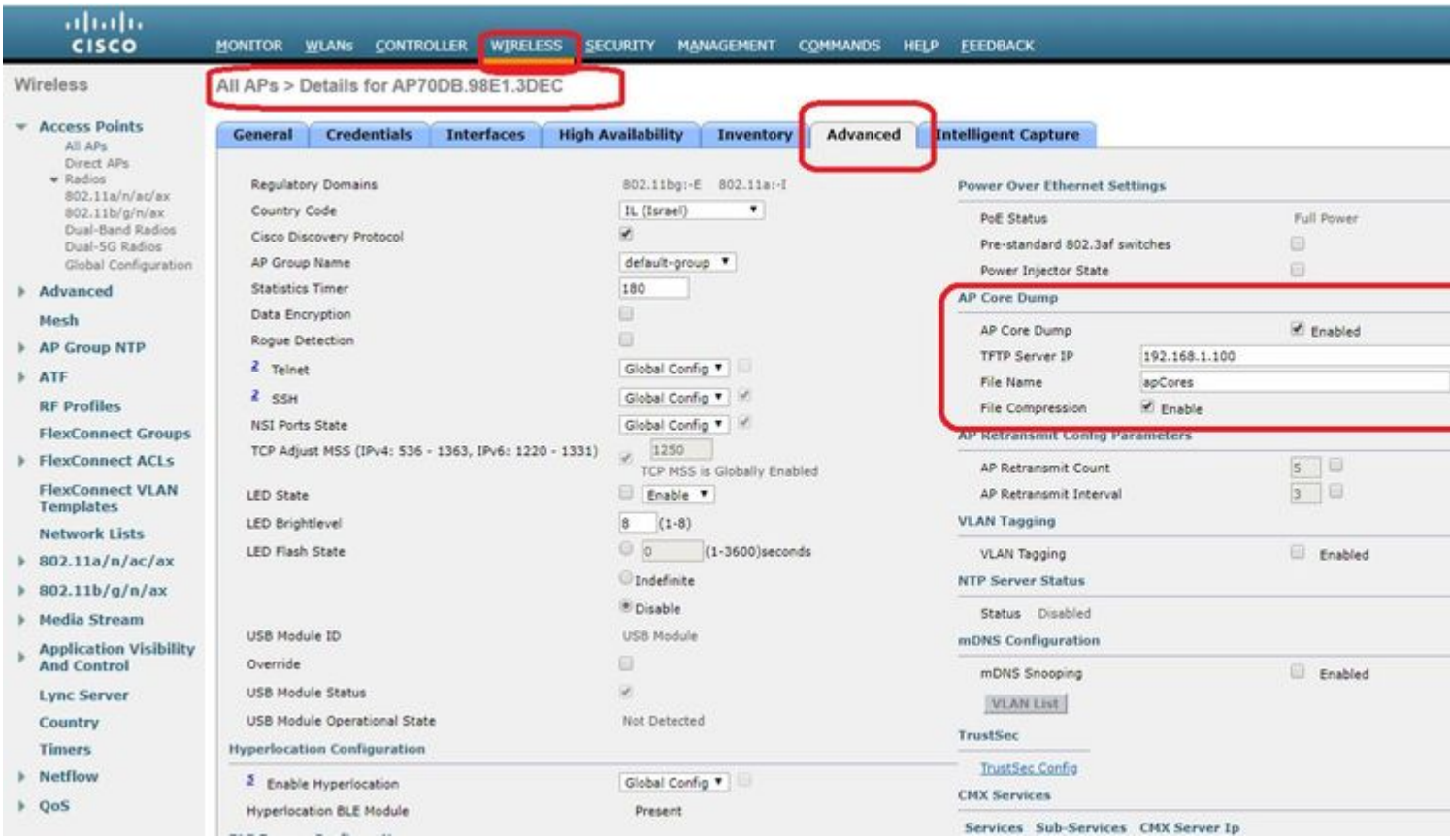
CLI AireOS

```
(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.
```

Interfaccia grafica AireOS



CLI di Cisco IOS®

<#root>

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

config

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

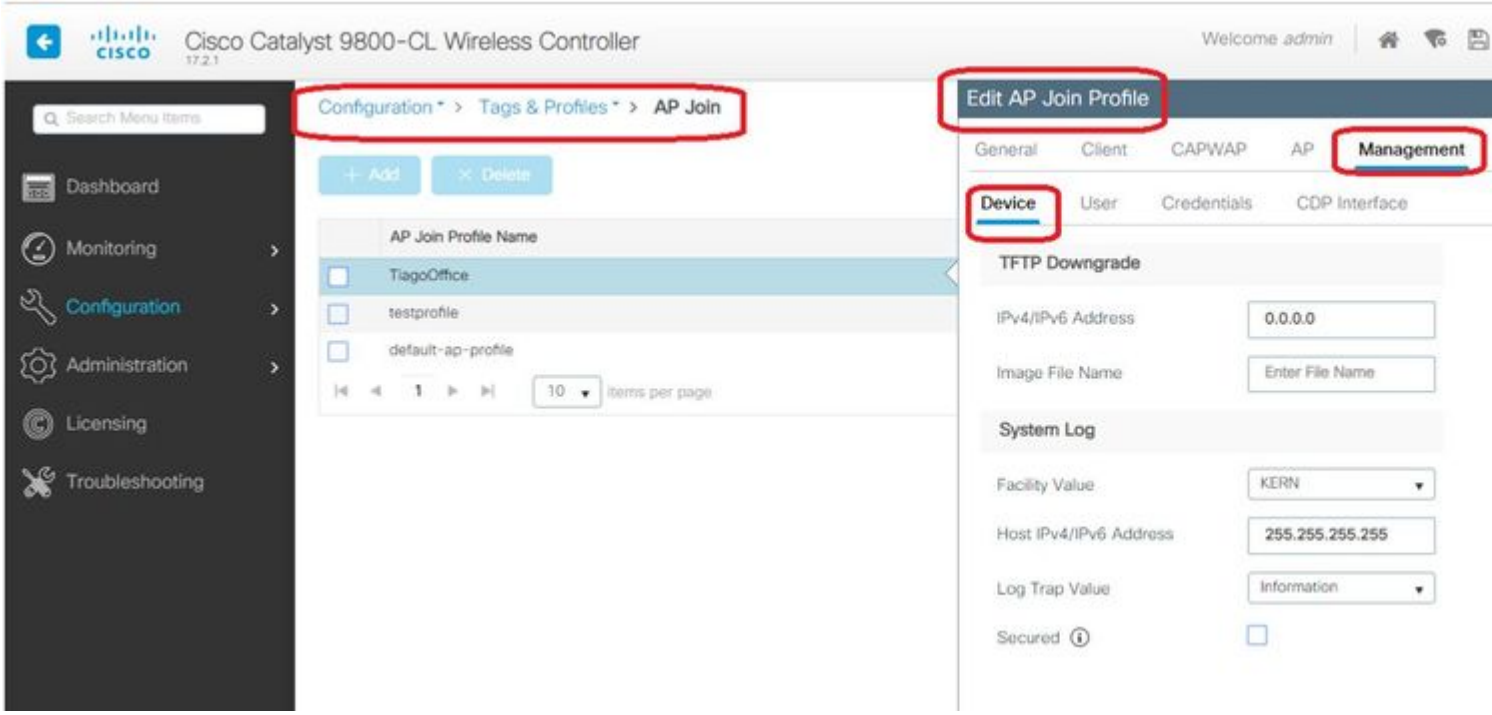
config-

ap

-profile

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

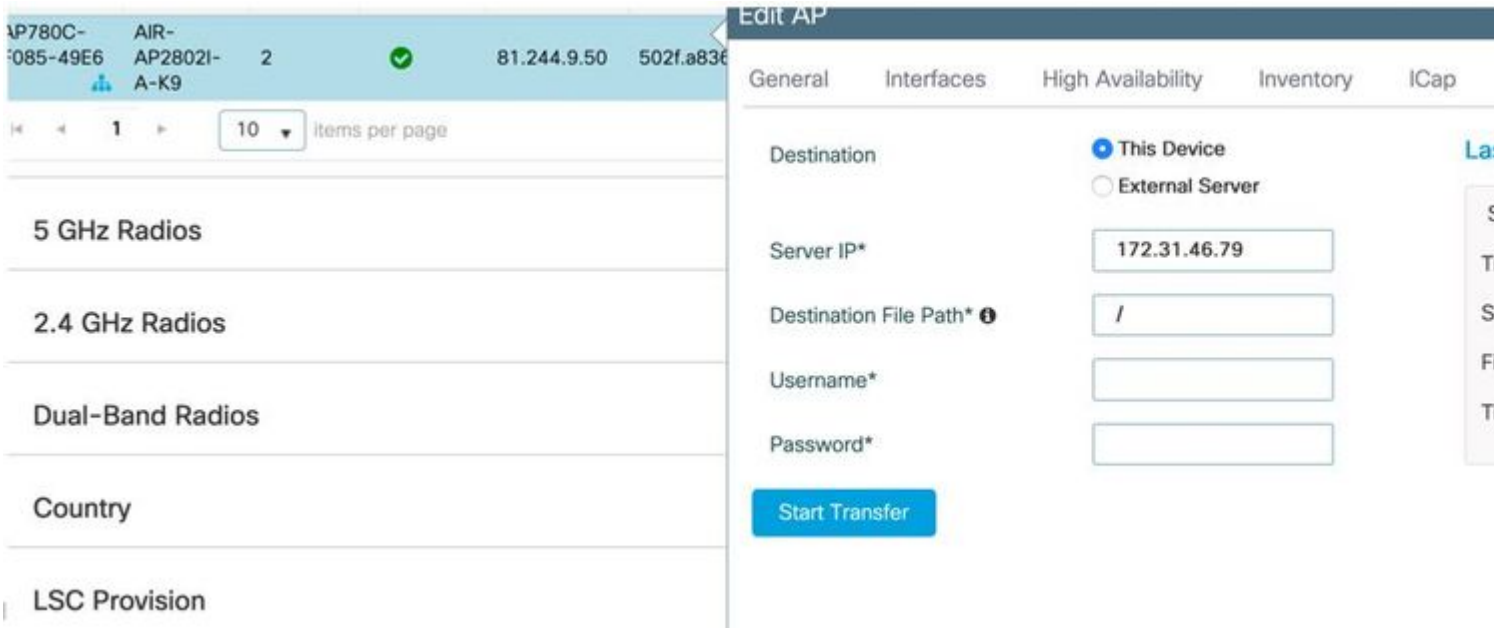
GUI Cisco IOS®



A partire da Cisco IOS® XE 17.3.1, si dispone della scheda Support Bundle e si può scaricare l'AP SB dalla GUI del WLC.

Non fa altro che eseguire il comando "***copy support-bundle***" sull'access point e inviarlo al WLC tramite SCP (perché il WLC può essere un server SCP).

E poi lo puoi scaricare dal tuo browser:



Ciò significa che è possibile eseguire manualmente la stessa procedura nelle versioni di eWLC precedenti alla 17.3.1:

Copiare il bundle di supporto dall'access point tramite SCP all'indirizzo IP eWLC se non si dispone di un server TFTP raggiungibile dall'access point.

Il WLC è solitamente raggiungibile tramite SSH dall'access point, quindi è un buon trucco per le versioni

precedenti alla 17.3.

Passaggio 1. Abilitare SSH su 9800 v17.2.1

Passaggio 2. Abilitare SCP su Cisco IOS® XE v17.2.1

Nell'esempio viene mostrato come configurare la funzionalità sul lato server di SCP. In questo esempio vengono utilizzati un nome utente e una password definiti localmente:

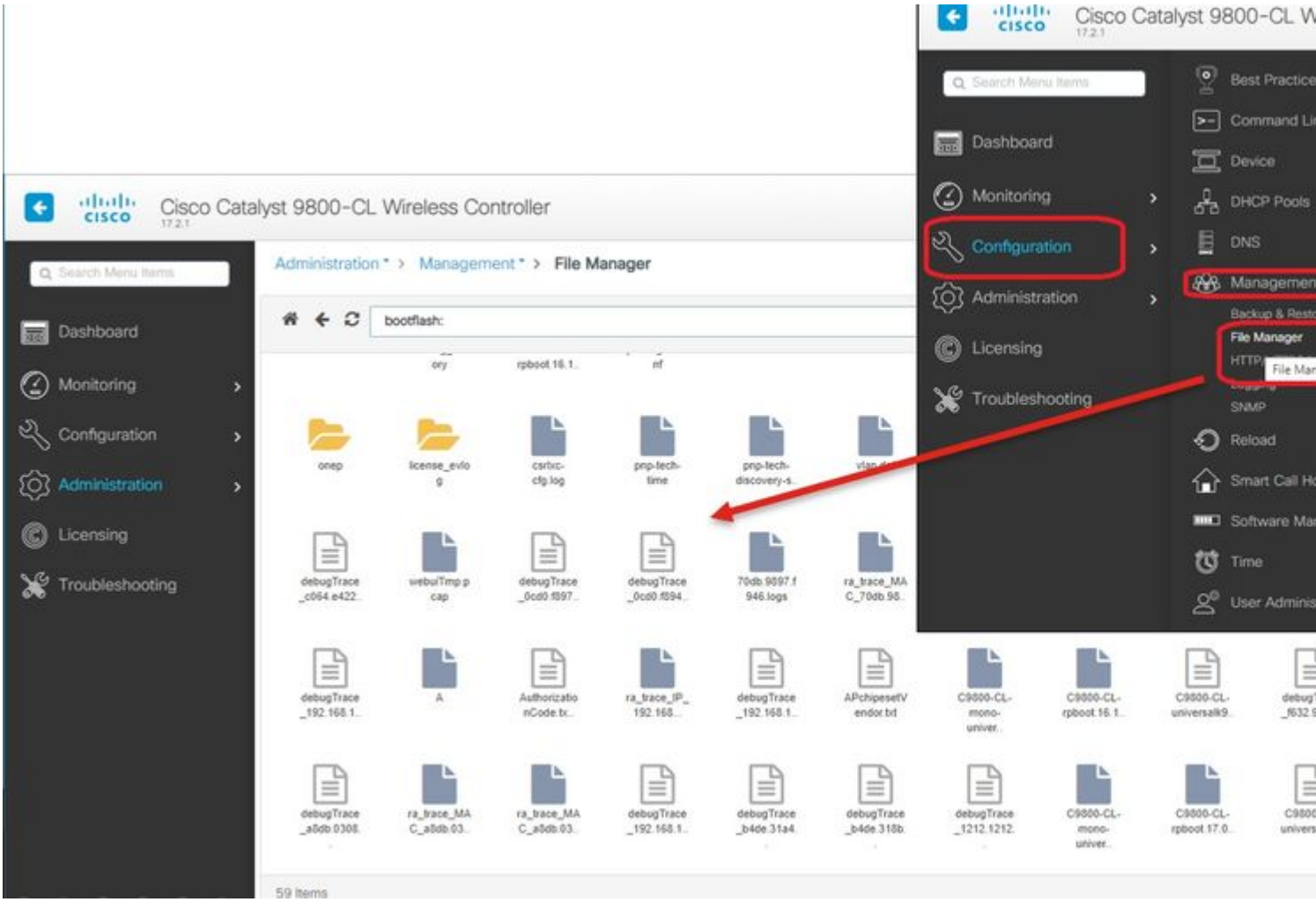
```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username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

Passaggio 3. Usare il comando "***copy support-bundle***" ed è necessario specificare il nome del file da creare nel server SCP.

Suggerimento: è possibile eseguire il comando una volta per ottenere un nome di file significativo e quindi copiare/incollare tale nome nel comando:

```
AP70DB.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/
Creating support bundle, please wait...!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 AP70DB.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz created ===+
Warning: Permanently added '192.168.1.15' (RSA) to the list of known hosts.
Password:
Connection closed by 192.168.1.15 port 22
lost connection
AP70DB.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/AP70DB.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz
Creating support bundle, please wait...!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 AP70DB.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz created ===+
Password:
AP70DB.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz
Connection to 192.168.1.15 closed by remote host.
AP70DB.98E1.3DEC#
```

Passaggio 4. Quindi è possibile accedere alla GUI del WLC e ottenere il file in: **Amministrazione > Gestione > File Manager**:



IoT e Bluetooth

I registri del server RPC possono essere controllati nell'access point 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 connettività al connettore DNA Spaces può essere verificata 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
```

Per visualizzare la configurazione di trasmissione BLE corrente dell'access point:

```
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)          : 000000000005446089c
Instance-ID (hex)        : 7f0000001f00

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

Per visualizzare i risultati dell'analisi:

```
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
```

Quando il punto di accesso opera in modalità gateway BLE avanzata in cui viene distribuita un'app, è possibile controllare lo stato dell'applicazione 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
```

È possibile connettersi all'applicazione IOX con questi comandi e quindi monitorare i registri durante la configurazione del beacon di reparto:

```
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
```

Conclusioni

Sono disponibili numerosi strumenti di risoluzione dei problemi che consentono di risolvere i problemi relativi ai punti di accesso COS.

Il presente documento contiene l'elenco dei documenti di uso più frequente e viene regolarmente aggiornato.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).