Fehlerbehebung bei COS-APs

Inhalt

Einleitung

Dieses Dokument beschreibt einige der Tools zur Fehlerbehebung, die für Cheatah OS APs (auch COS APs genannt) verfügbar sind.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument konzentriert sich auf COS-APs wie die APs der Serien 2800, 3800, 1560 und 4800 sowie die neuen 11ax APs Catalyst 91xx.

Dieses Dokument konzentriert sich auf viele Funktionen, die in AireOS 8.8 und höher verfügbar sind. sowie Cisco IOS® XE 16.2.2s und höher

Es kann Kommentare zur Verfügbarkeit bestimmter Funktionen in früheren Versionen geben.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Erfassen von Paketspuren (Sniffer-Spuren)

Kabelgebundenes PCAP am AP-Port

Es ist möglich (ab Version 8.7 mit dem Filter, der in Version 8.8 verfügbar ist), einen pcap-Wert am Ethernet-Port des AP zu verwenden. Sie können das Ergebnis entweder live in der CLI anzeigen (mit nur zusammengefassten Paketdetails) oder als vollständige Zusammenfassung im AP-Flash-Speicher speichern.

Die kabelgebundene Abdeckung erfasst alle Daten auf der Ethernet-Seite (Rx/Tx), und der Anschlusspunkt im AP befindet sich unmittelbar bevor das Paket verkabelt wird.

Es erfasst jedoch nur Datenverkehr auf AP-CPU-Ebene, d. h. Datenverkehr vom und zum AP (AP DHCP, AP Capwap Control Tunnel, ...), und zeigt keinen Client-Datenverkehr an.

Beachten Sie, dass die Größe sehr begrenzt ist (max. Größenbeschränkung von 5 MB), daher kann es erforderlich sein, Filter zu konfigurieren, um nur den Datenverkehr zu erfassen, der Sie interessiert.

Stellen Sie sicher, dass Sie die Datenerfassung mit "no debug traffic wired ip capture" oder einfach "undebug all" beenden, bevor Sie versuchen, sie zu kopieren (andernfalls endet die Kopie nicht, wenn die Pakete noch geschrieben werden).

Vorgehensweise

Schritt 1: Starten Sie pcap, und wählen Sie den Datenverkehrstyp mit "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)
```

Schritt 2: Warten Sie, bis der Datenverkehr fließt, und stoppen Sie dann die Erfassung mit dem Befehl "no debug traffic wired ip capture" oder einfach "undebug all":

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

Schritt 3: Kopieren Sie die Datei auf den tftp/scp-Server:

<#root>

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

AP70DB.98E1.3DEC_capture.pcap0

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

Schritt 4: Jetzt können Sie die Datei in Wireshark öffnen. Die Datei ist pcap0. Ändern Sie den Wert in pcap, sodass er automatisch Wireshark zugeordnet wird.

Befehlsoptionen

Der Befehl debug traffic wired bietet mehrere Optionen, mit denen Sie bestimmten Datenverkehr erfassen können:

```
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
```

Sie können am Ende des Debug-Befehls "verbose" hinzufügen, um den Hex Dump des Pakets anzuzeigen. Beachten Sie, dass dies Ihre CLI-Sitzung sehr schnell überlasten kann, wenn Ihr Filter nicht eng genug ist.

Kabelgebundenes PCAP durch die Verwendung von Filter

Das Filterformat entspricht dem tcpdump-Erfassungsfilterformat.

	Beispiel für Filter	**Beschreibung**
Host	"host 192.168.2.5"	Dadurch wird die Paketerfassung gefiltert, sodass nur Pakete erfasst werden, die an den Host 192.168.2.5 gehen oder von diesem kommen.
	"src host 192.168.2.5"	Dadurch wird die Paketerfassung gefiltert, sodass nur Pakete aus 192.168.2.5 gesammelt werden.

	"dst host 192,168.2,5"	Dadurch wird die Paketerfassung gefiltert, sodass nur Pakete erfasst werden, die an 192.168.2.5 gehen.
Anschluss	Port 443	Dadurch wird die Paketerfassung gefiltert, sodass nur Pakete mit einer Quelle oder einem Ziel von Port 443 gesammelt werden.
	"src port 1055"	Dieser erfasst den Datenverkehr, der von Port 1055 stammt.
	"dst port 443"	Dieser Befehl erfasst den Datenverkehr für Port 443.

Im folgenden Beispiel wird die Ausgabe in der Konsole angezeigt, aber auch gefiltert, sodass nur CAPWAP-Datenpakete angezeigt werden:

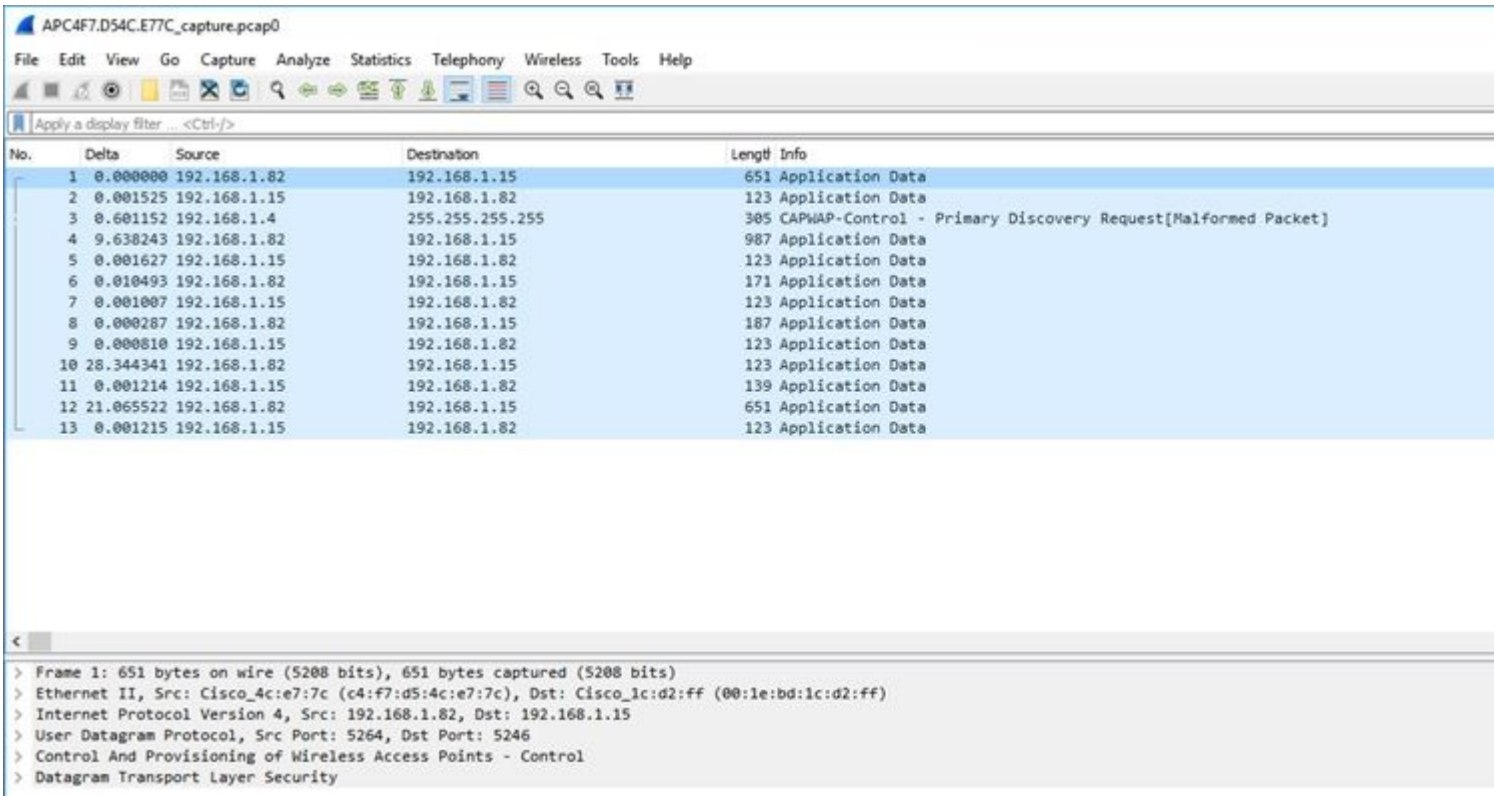
```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
12:20:50.483125 IP APC4F7-D54C-E77C.lan.5264 > 192.168.1.15.5246: UDP, length 81
12:20:50.484361 IP 192.168.1.15.5246 > APC4F7-D54C-E77C.lan.5264: UDP, length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

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

Beispiel für Ausgabe in Datei:

```
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#
```

So öffnen Sie die Erfassung in Wireshark:



Funkerfassung

Es ist möglich, die Erfassung von Paketen auf der Steuerungsebene des Funkmoduls zu ermöglichen. Aufgrund von Leistungseinbußen ist es nicht möglich, Daten auf dem Radio-Datenflugzeug zu erfassen.

Dies bedeutet, dass der Client-Assoziationsfluss (Tests, Authentifizierung, Verknüpfung, EAP, ARP, DHCP-Pakete sowie IPv6-Steuerungspakete, ICMP und NDP) sichtbar ist, jedoch nicht die Daten, die der Client nach dem Übergang in den verbundenen Zustand weitergibt.

Vorgehensweise

Schritt 1: Fügen Sie die verfolgte Client-MAC-Adresse hinzu. Es können mehrere MAC-Adressen hinzugefügt werden. Es ist auch möglich, den Befehl für alle Clients auszuführen. Dies wird jedoch nicht empfohlen.

```
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.
```

Schritt 2: Legen Sie einen Filter fest, der nur bestimmte Protokolle oder alle unterstützten Protokolle protokolliert:

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

Schritt 3: Anzeige der Ausgabe in der Konsole (asynchron):

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

Schritt 4: Starten Sie die Ablaufverfolgung.

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

Beispiel:

<#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
```

So stoppen Sie die Erfassung:

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

Überprüfung

Client-Ablaufverfolgung überprüfen:

<#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
```

Beispiel einer erfolgreichen Client-Verbindung:

Die Buchstaben zwischen den Klammern helfen Ihnen zu verstehen, wo der Frame zu sehen war (E für Ethernet, W für Wireless, C für das Click-Modul, wenn es sich um ein internes AP handelt) und in welche Richtung (Upload oder Download).

Hier ist eine kleine Tabelle mit der Bedeutung dieser Buchstaben:

U - Uplink-Paket (vom Client)
D - Downlink-Paket (zum Klicken)
W - Modul-Wireless-Treiber
E - Modul-Ethernet-Treiber
C - Modul Klicken

Weitere Optionen

Protokoll asynchron anzeigen:

Die Protokolle können dann mit dem Befehl "**show ap client-trace events mac xx:xx:xx:xx:xx:xx:xx" aufgerufen** werden (oder MAC durch "all" ersetzen).

<#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
```

Pakete im Hexadezimalformat ausgeben

Sie können die Pakete im Hexadezimalformat in der CLI auslesen:

```
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.98E1.3DEC#configure ap client-trace start
Warning: To recover WLC pushed config, need CAPWAP restart or reload to re-apply the config from WLC
AP70DB.98E1.3DEC#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.98E1.3DEC#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.98E1.3DEC#configure ap client-trace output dump enable
  <4-5000>  Enter the packet dump length value
AP70DB.98E1.3DEC#configure ap client-trace output dump enable 100
  <cr>
AP70DB.98E1.3DEC#configure ap client-trace output dump enable 100
AP70DB.98E1.3DEC#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 11 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 ff ab cd 02 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 13:29:27.4748]
Apr  6 13:29:27 kernel: [*04/06/2020 13:29:27.4748] Time:474883us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:288 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 54:7c:69:b7:3f:42 Seq:6(6) 1
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 11 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 08 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 11 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(161
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 11 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(161
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
```

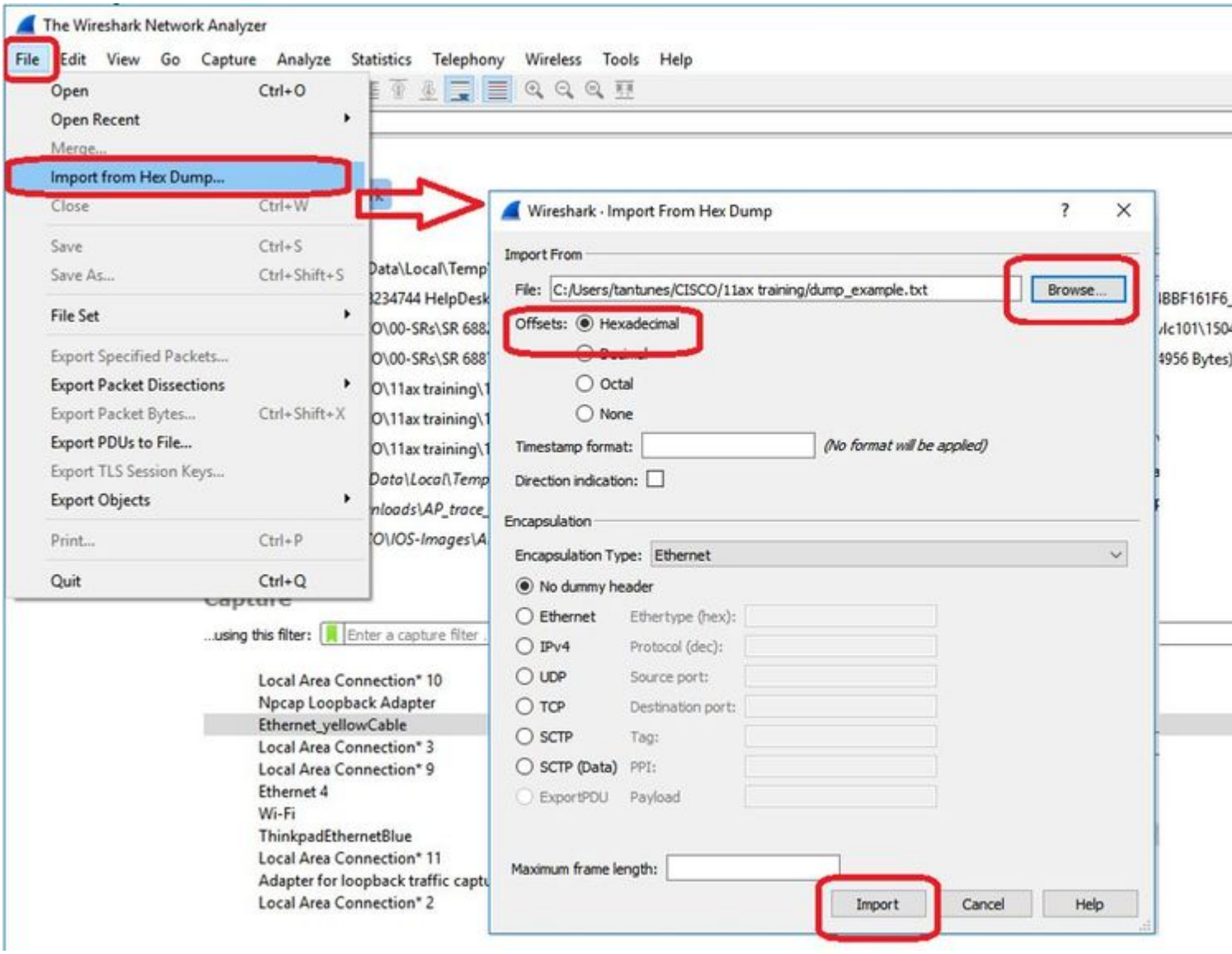
Anschließend können Sie das Hex Dump bereinigen und im Textformat speichern und in Wireshark importieren:

```
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 00 11 00 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 00 11 00 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 00 11 00 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 00 11 00 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
```



Da die Ausgabe sehr groß sein kann und nur der sichtbare Frame-Typ und nicht das innere Detail angegeben werden, kann es effizienter sein, die Paketerfassung auf einen Laptop umzuleiten, auf dem eine Erfassungsanwendung (z. B. Wireshark) ausgeführt wird.

Aktivieren Sie die Remote-Erfassungsfunktion, um die Pakete mit Wireshark an ein externes Gerät zu senden:

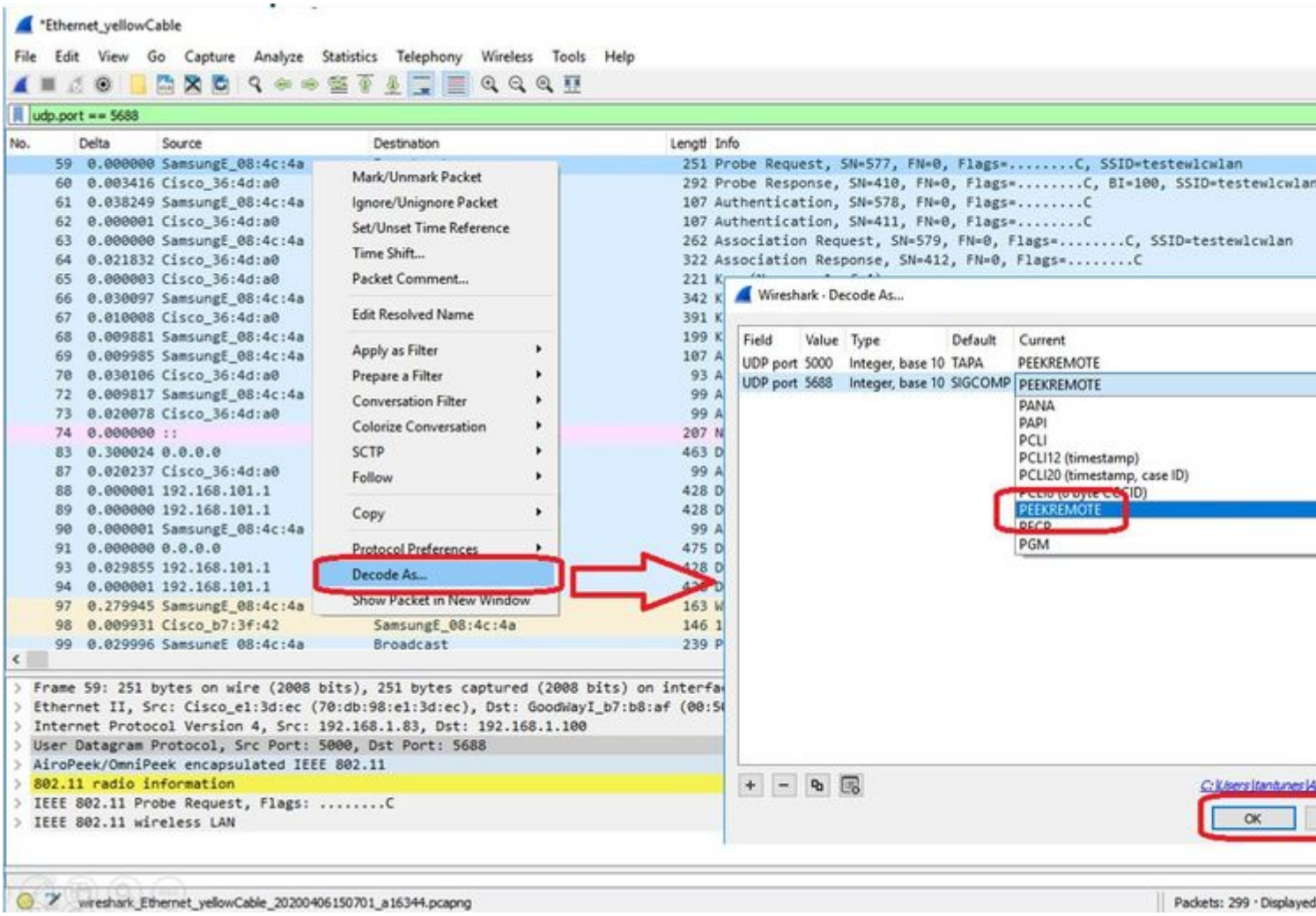
```
config ap client-trace output remote enable
```

Der Befehl bedeutet, dass der AP jeden vom Client-Trace-Filter erfassten Frame an den Laptop mit der Nummer 192.168.68.68 weiterleitet und PEEKREMOTE-Kapselung (genau wie APs im Sniffer-Modus) auf Port 5000 verwendet.

Eine Einschränkung besteht darin, dass sich der Ziel-Laptop im gleichen Subnetz wie der Access Point befinden muss, auf dem Sie diesen Befehl ausführen. Sie können die Port-Nummer ändern, um die in Ihrem Netzwerk geltenden Sicherheitsrichtlinien zu berücksichtigen.

Sobald Sie alle Pakete auf dem Laptop empfangen haben, auf dem Wireshark läuft, können Sie mit der rechten Maustaste auf den udp 5000-Header klicken und **decodieren** auswählen und PEEKREMOTE

auswählen, wie in dieser Abbildung dargestellt:



Liste der Bugs und Verbesserungen für diese Funktion:

Cisco Bug-ID CSCvm09020 DNS wird von Client-Trace auf 8.8 nicht mehr erkannt

Cisco Bug-ID CSCvm09015 Client-Ablaufverfolgung zeigt viele ICMP_Other mit Nullsequenznummer an

Cisco Bug-ID CSCvm02676 AP COS Client-Trace erfasst keine Webauthentifizierungspakete

Cisco Bug-ID CSCvm02613 AP COS-Client-Trace-Remoteausgabe funktioniert nicht

Cisco Bug-ID CSCvm00855 lient-trace SEQ-Nummern inkonsistent

Steuerung der AP-Client-Verfolgung vom 9800 WLC

Sie können mehrere APs so konfigurieren, dass sie eine Radio Client-Überwachung durchführen und diese vom

Schritt 1: Konfigurieren eines AP-Ablaufverfolgungsprofils, das den zu erfassenden Datenverkehr definiert

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

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

Schritt 2: Fügen Sie das AP-Ablaufverfolgungsprofil einem AP-Zugangsprofil hinzu, das von den APs verwendet wird, auf die Sie abzielen.

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

Stellen Sie sicher, dass dieses Zugangsprofil auf ein Site-Tag angewendet wird, das von Ihren Ziel-APs verwendet wird.

Schritt 4 Start/Stopp auslösen

```
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
```

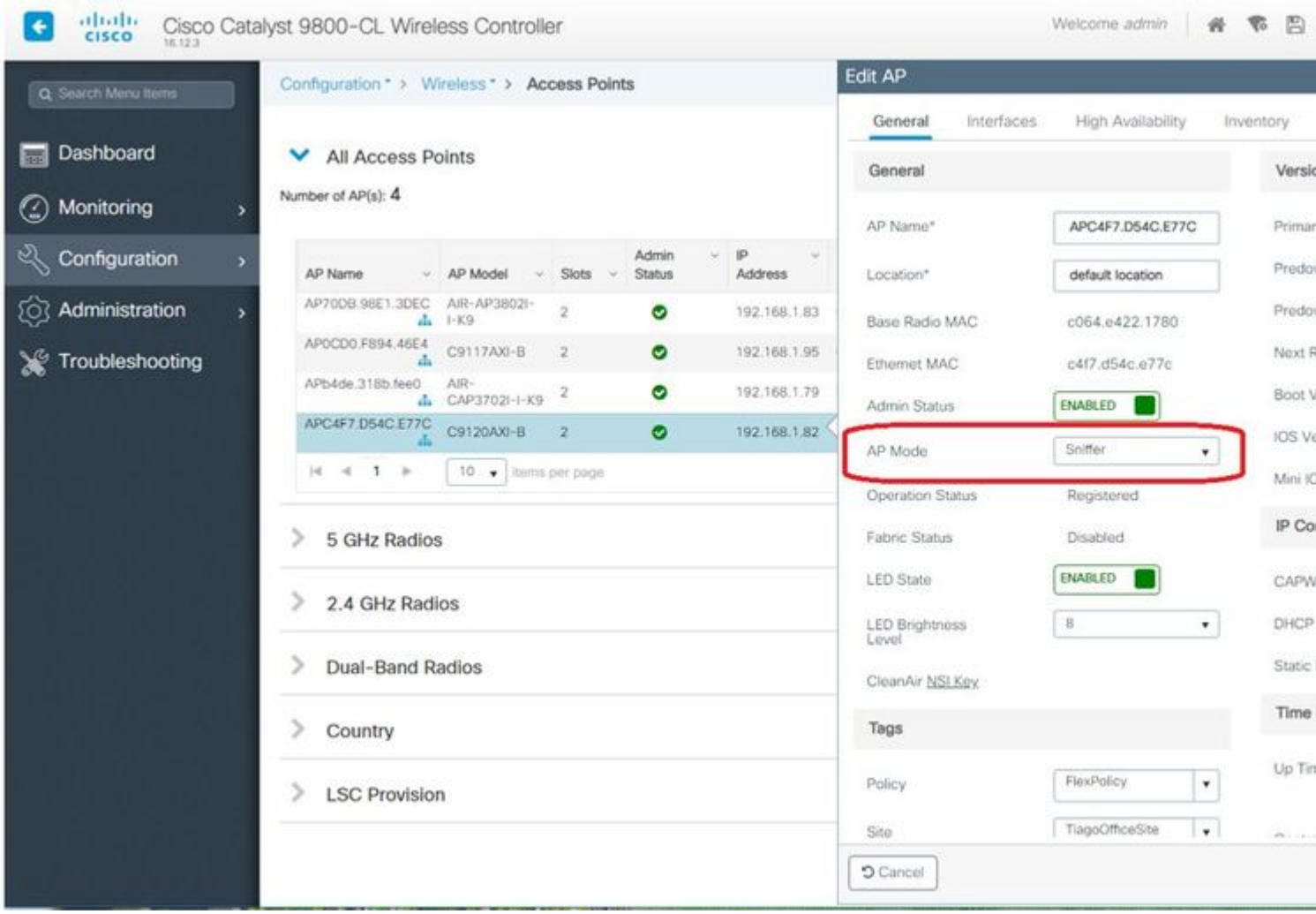
```
client all/
```

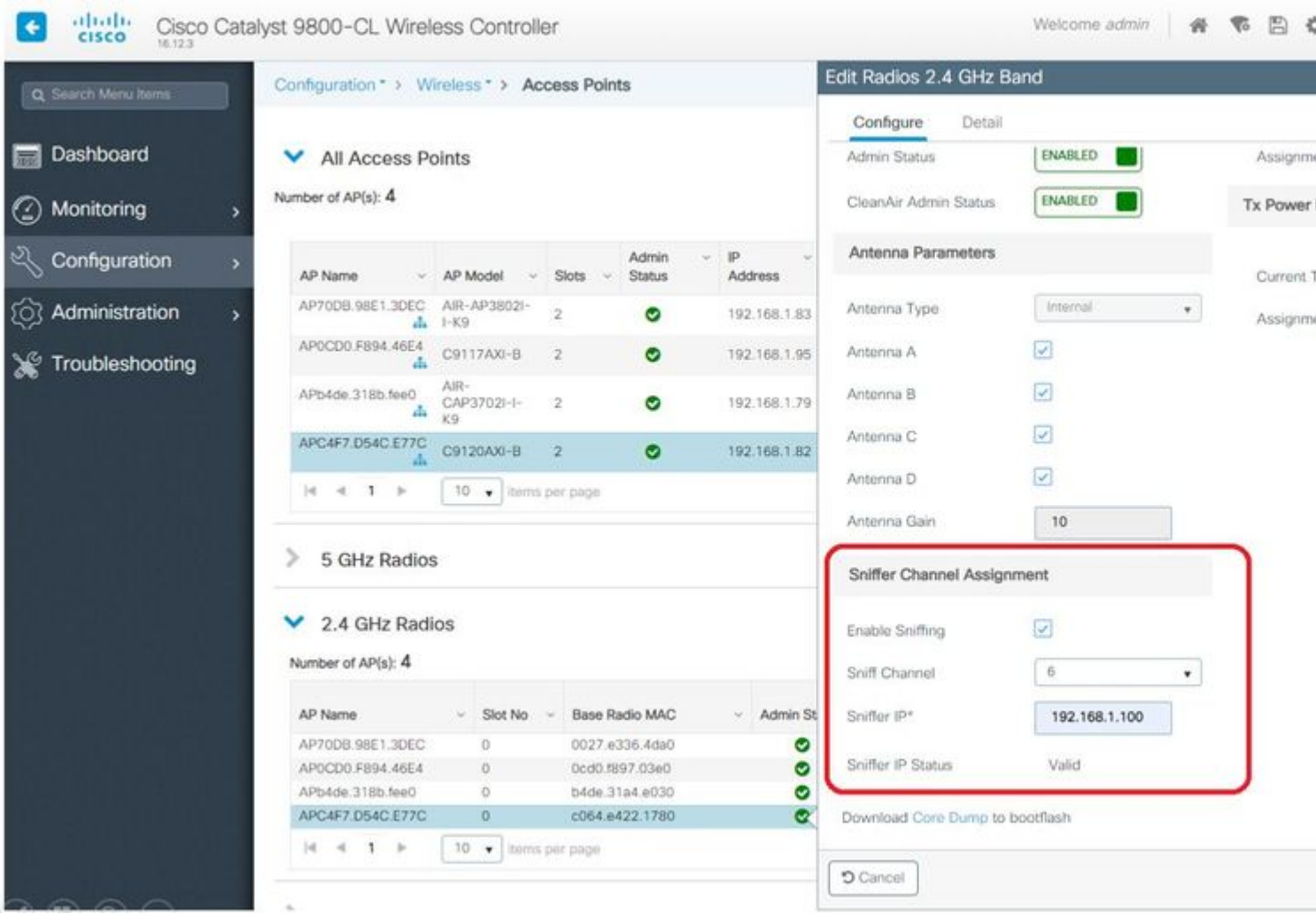
Verifizierungsbefehle:

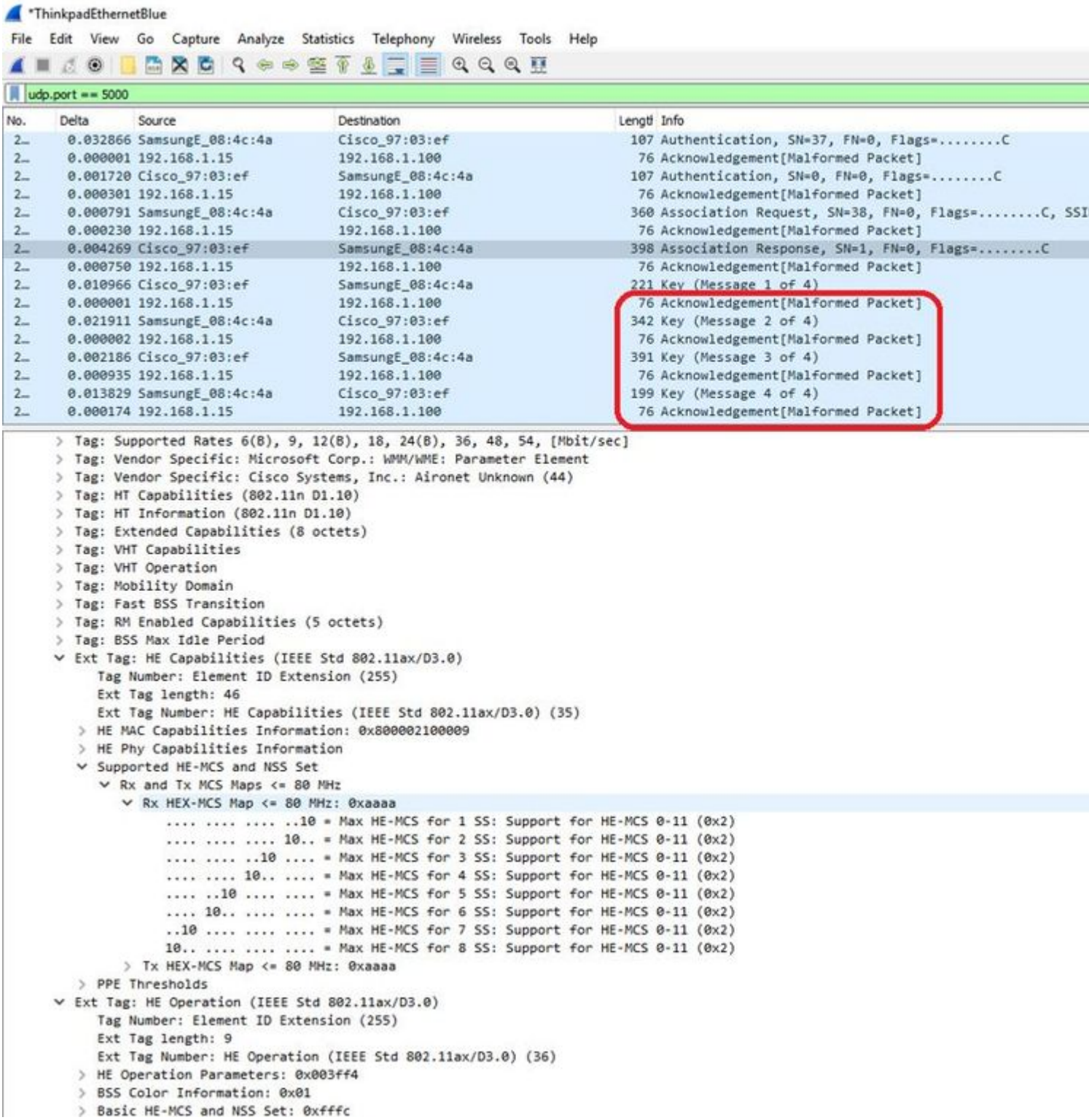
```
show wireless profile ap trace summary
show wireless profile ap trace detailed PROF_NAME detail
sh ap trace client summary
show ap trace unsupported-ap summary
```

APs Catalyst 91xx im Sniffer-Modus

Der neue Catalyst 9115, 9117, 9120 und 9130 kann im Sniffer-Modus konfiguriert werden. Die Vorgehensweise ist ähnlich wie bei früheren AP-Modellen.




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



Hinweis: Daten-Frames, die mit WIFI 6-Datenraten gesendet werden, werden erfasst. Da peekremote jedoch in Wireshark nicht aktuell ist, werden sie ab sofort als 802.11ax-Phy-Typ angezeigt. Die Lösung ist in Wireshark 3.2.4, wo Wireshark zeigt die richtige Wifi6 Phy-Rate.

Hinweis: Cisco APs können MU-OFDMA-Frames derzeit nicht erfassen, jedoch die Trigger-Frames (gesendet mit Management-Datenrate) erfassen, die ein MU-OFDMA-Fenster ankündigen. Sie können bereits ableiten, dass MU-OFDMA passiert (oder nicht) und mit welchem Client.

Tipps zur Fehlerbehebung

Pfad-MTU

Obwohl die MTU-Pfaderkennung die optimale MTU für den Access Point findet, können diese Einstellungen manuell überschrieben werden.

Unter AireOS 8.10.130 WLC wird mit dem Befehl **config ap pmtu disable <ap/all>** eine statische MTU für einen oder alle APs festgelegt, anstatt sich auf den dynamischen Erkennungsmechanismus zu verlassen.

So aktivieren Sie Debugging-Vorgänge beim Booten

Sie können das Konfigurationsboot-Debug-Capwap ausführen, um das Capwap-, DTLS- und DHCP-Debugging beim nächsten Start zu aktivieren, noch bevor das Betriebssystem gestartet wurde und die Eingabeaufforderung angezeigt wird.

Sie haben auch "config boot debug memory xxxx" für mehrere Speicherdebugs.

Mit "show boot" können Sie beim nächsten Neustart sehen, ob die Boot-Fehlerbehebung aktiviert ist oder nicht.

Sie können mit dem disable-Schlüsselwort am Ende wie "config boot debug capwap disable" deaktiviert werden.

Energiesparmechanismus

Die Stromsparfunktion eines Clients kann durch Ausführen von

debug client trace <MAC-Adresse>

Clients-QoS

Um zu überprüfen, ob QoS-Tags angewendet werden, können Sie "***debug capwap client qos"*** ausführen.

Es zeigt den UP-Wert von Paketen für Wireless-Clients an.

Es ist seit 8.8 nicht mehr mac-filterbar (Erweiterungsanfrage 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
```

Sie können auch die QoS-Tabelle "Bis zu DSCP" auf dem Access Point sowie die Gesamtzahl der Pakete überprüfen, die durch QoS markiert, geformt und verworfen wurden:

```
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#
```

Wenn QoS-Richtlinien auf dem WLC definiert und auf den Flexconnect AP heruntergeladen wurden, können Sie sie wie folgt überprüfen:

```
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
```

Bei QoS-Ratenbegrenzung:

```
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
```

Scannen außerhalb des Kanals

Das Debuggen des Off-Channel-Scans des Access Points kann bei der Fehlerbehebung von nicht autorisierter Erkennung hilfreich sein (um zu überprüfen, ob und wann der Access Point einen bestimmten Kanal scannt), kann aber auch bei der Fehlerbehebung von Videos nützlich sein, wenn ein empfindlicher Echtzeit-Stream ständige Unterbrechungen erhält, wenn die Funktion "Off-Channel-Scan zurückstellen" nicht verwendet wird.

```
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_1
[*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_1
[*06/11/2020 09:45:43.6570] noise measurement channel 140 noise 97
```

Client-Verbindungen

Es ist möglich, Clients aufzulisten, deren Authentifizierung vom Access Point aufgehoben wurde, und zwar mit dem letzten Ereignis-Zeitstempel:

```
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
```

In der vorherigen Ausgabe ist der Ursachencode der Deauthentifizierungsursachencode, wie in diesem Link beschrieben:

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

Die vap bezieht sich auf die Kennung des WLAN innerhalb des WAP (die sich von der WLAN-ID auf dem WLC !!! unterscheidet).

Sie können es mit anderen Ausgaben kreuzen, die später detailliert werden, wobei immer die vap der zugehörigen Clients erwähnt wird.

Sie können die Liste der VAP-IDs mit "***show controller Dot11Radio 0/1 wlan***".

Wenn Clients noch verbunden sind, erhalten Sie Details zu ihrer Verbindung mit:

```
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
```

Weitere Informationen zum Client-Eintrag finden Sie unter:

```
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
```

Sie können die Trennung eines bestimmten Clients erzwingen mit:

```
test dot11 client deauthenticate
```

Datenverkehrszähler können pro Client abgerufen werden mit:

```
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#
```

Mehr auf der Funkebene gibt es in den "***Show Controllern"*** viele Informationen. Wenn Sie die MAC-Adresse des Clients hinzufügen, werden die unterstützten Datenraten, die aktuellen Datenmengen, die PHY-Funktionen sowie die Anzahl der Wiederholungsversuche und der Textfehler angezeigt:

<#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
```

Um eine Client-Datenrate und/oder einen RSSI-Wert stets im Auge zu behalten, können Sie "**debug dot11 client rate address <mac>** ausführen. Diese Informationen werden jede Sekunde protokolliert:

```
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 dieser Ausgabe werden die Tx- und Rx-Paketzähler in dem zweiten Intervall seit dem letzten Druck übertragen. Dies gilt auch für die Tx Retries. RSSI, SNR und Datenrate sind jedoch die Werte des letzten Pakets dieses Intervalls (und nicht der Durchschnitt aller Pakete in diesem Intervall).

Flexconnect-Szenarien

Sie können überprüfen, welche ACLs derzeit in einem Pre-Auth-Szenario (z. B. CWA) oder Post-Auth-Szenario auf einen Client angewendet werden:

```
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-Dateisystem

COS-APs erlauben es nicht, den gesamten Inhalt des Dateisystems aufzulisten, wie auf Unix-Plattformen.

Der Befehl "***show filesystems***" gibt einen Überblick über die Speichernutzung und Verteilung auf der aktuellen Partition:

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

Der Befehl "***show flash***" listet die Hauptdateien auf dem AP-Flash auf. Sie können auch das Schlüsselwort syslog oder core anhängen, um diese spezifischen Ordner aufzulisten.

```
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
```

Speichern und Senden von Syslogs

Der Syslog-Ordner speichert die Syslog-Ausgabe früherer Neustarts. Der Befehl "***show log***" zeigt nur das Syslog seit dem letzten Neustart an.

Bei jedem Neustart werden die Syslogs auf inkrementelle Dateien geschrieben.

```
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
```

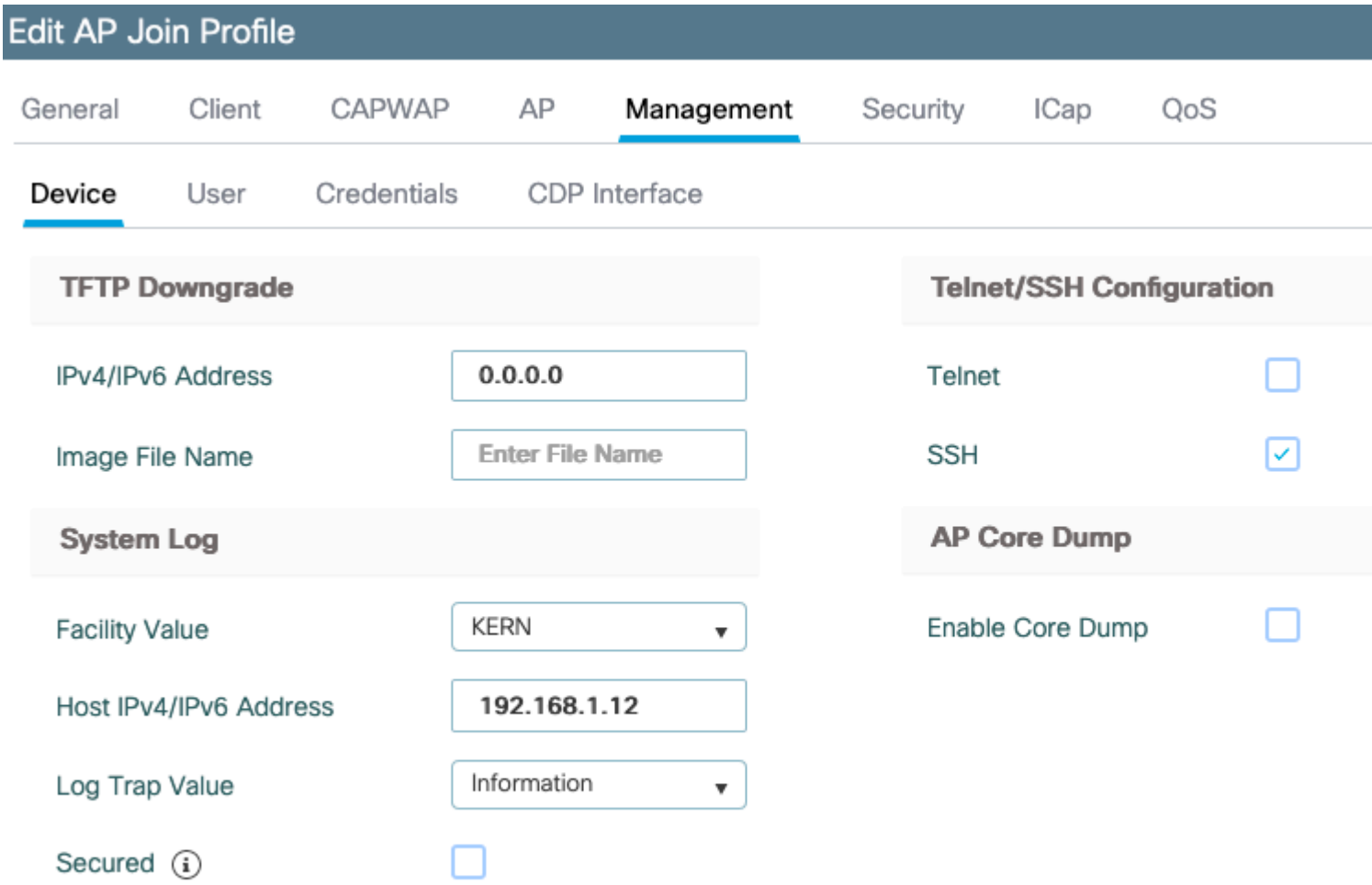
Die erste Ausgabe nach dem ersten Start ist Datei 1.0, und eine Datei 1.1 wird erstellt, wenn 1.0 zu lang wird. Nach dem Neustart wird eine neue Datei 2.0 erstellt usw.

Über den WLC können Sie das Syslog-Ziel konfigurieren, wenn Ihre APs ihre Syslog-Meldungen als Unicast an einen bestimmten Server senden sollen.

Standardmäßig senden APs ihre Syslogs an eine Broadcast-Adresse, die einen gewissen Broadcast-Sturm verursachen kann. Konfigurieren Sie deshalb einen Syslog-Server.

Der Access Point sendet standardmäßig über Syslog alle Drucke, die auf seiner Konsolenausgabe stehen.

Auf dem 9800-Controller können Sie diese Parameter im Profil "Configuration -> AP Join" (Konfiguration -> AP-Beitritt) unter Management ändern.



Sie können den **Protokolltrap-Wert** ändern, um Debug-Meldungen auch über Syslog zu senden. Anschließend können Sie Debug-Vorgänge in der AP-CLI aktivieren, und die Ausgabe dieser Meldungen wird über Syslog-Meldungen an den konfigurierten Server gesendet.

Aufgrund Cisco Bug-ID CSCvu75017 nur dann, wenn Sie die Syslog-Funktion auf KERN (den Standardwert) setzen, sendet der WAP Syslog-Meldungen.

Wenn Sie Probleme beheben, bei denen die Netzwerkverbindung eines Access Points möglicherweise verloren geht (z. B. bei einem WGB), ist das Syslog nicht so zuverlässig, wie wenn die Uplink-Verbindung des Access Points unterbrochen wird, werden keine Meldungen gesendet.

Daher ist die Abhängigkeit von den im Flash gespeicherten Syslog-Dateien eine hervorragende Möglichkeit, die Ausgabe zu debuggen, auf dem Access Point selbst zu speichern und dann zu einem späteren Zeitpunkt regelmäßig hochzuladen.

AP-Supportpaket

Einige häufig gesammelte Diagnoseinformationen verschiedener Typen können in einem einzigen Paket bereitgestellt werden, das Sie von Access Points hochladen können.

Folgende Diagnoseinformationen können Sie in das Paket aufnehmen:

- AP Show Tech

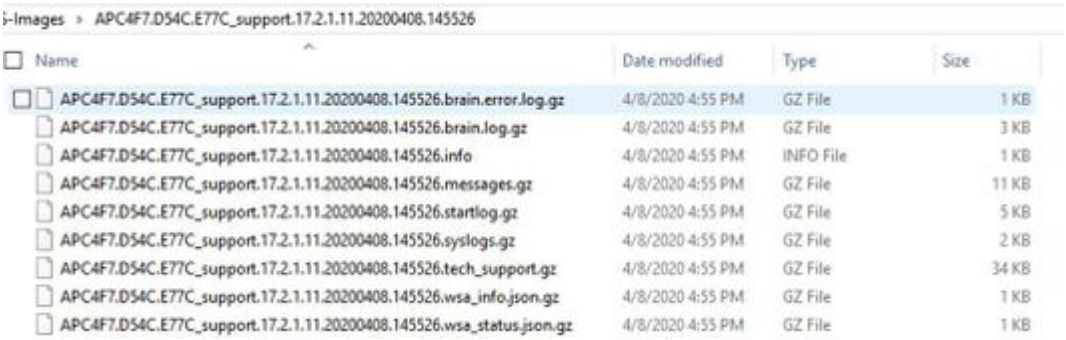
- AP-Syslogs
- AP Capwapd Brain Logs
- AP-Start- und Nachrichtenprotokolle
- AP Coredump-Dateien

Um das AP-Supportpaket zu erhalten, können Sie in die AP-CLI gehen und den Befehl "***copy* support-bundle tftp: x.x.x.x**" eingeben.

Anschließend können Sie die Datei mit dem Namen AP suchen, der an die Datei **support.apversion.date.time.tgz** angehängt wurde, wie nachfolgend gezeigt:

```
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#
```

Wenn Sie die Datei "untar", können Sie die verschiedenen Dateien gesammelt anzeigen:



Remote-Erfassung von AP-Core-Dateien

Um AP-Core-Dateien ferngesteuert zu sammeln, aktivieren Sie das Core Dump, das im Supportpaket enthalten sein soll, und laden Sie dann das Supportpaket vom AP hoch, oder senden Sie es direkt an den TFTP-Server. In den folgenden Beispielen wird der TFTP-Server 192.168.1.100 verwendet.

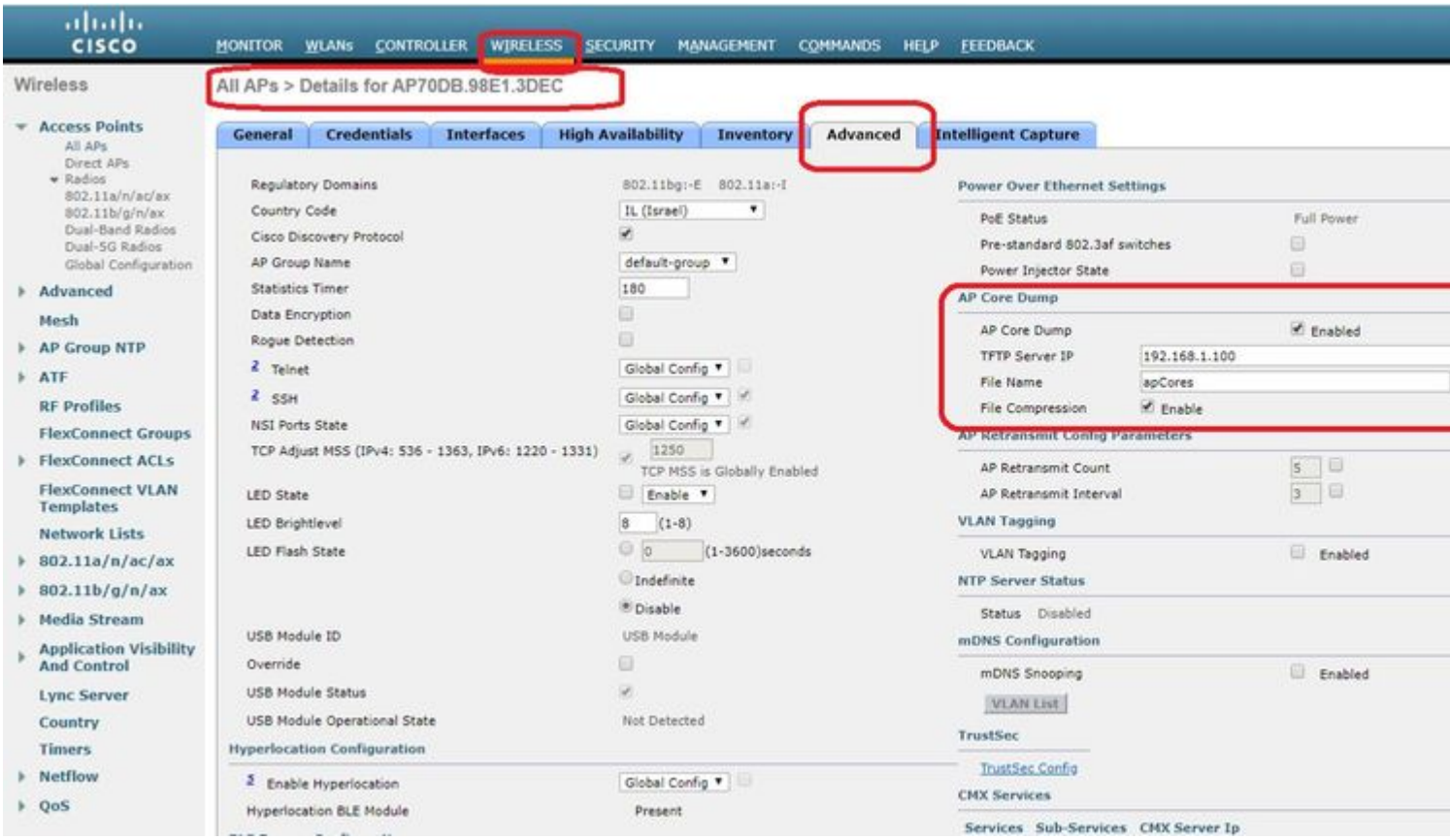
AireOS-CLI

```
(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.
```

AireOS-Benutzeroberfläche



Cisco IOS®-CLI

<#root>

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

config

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

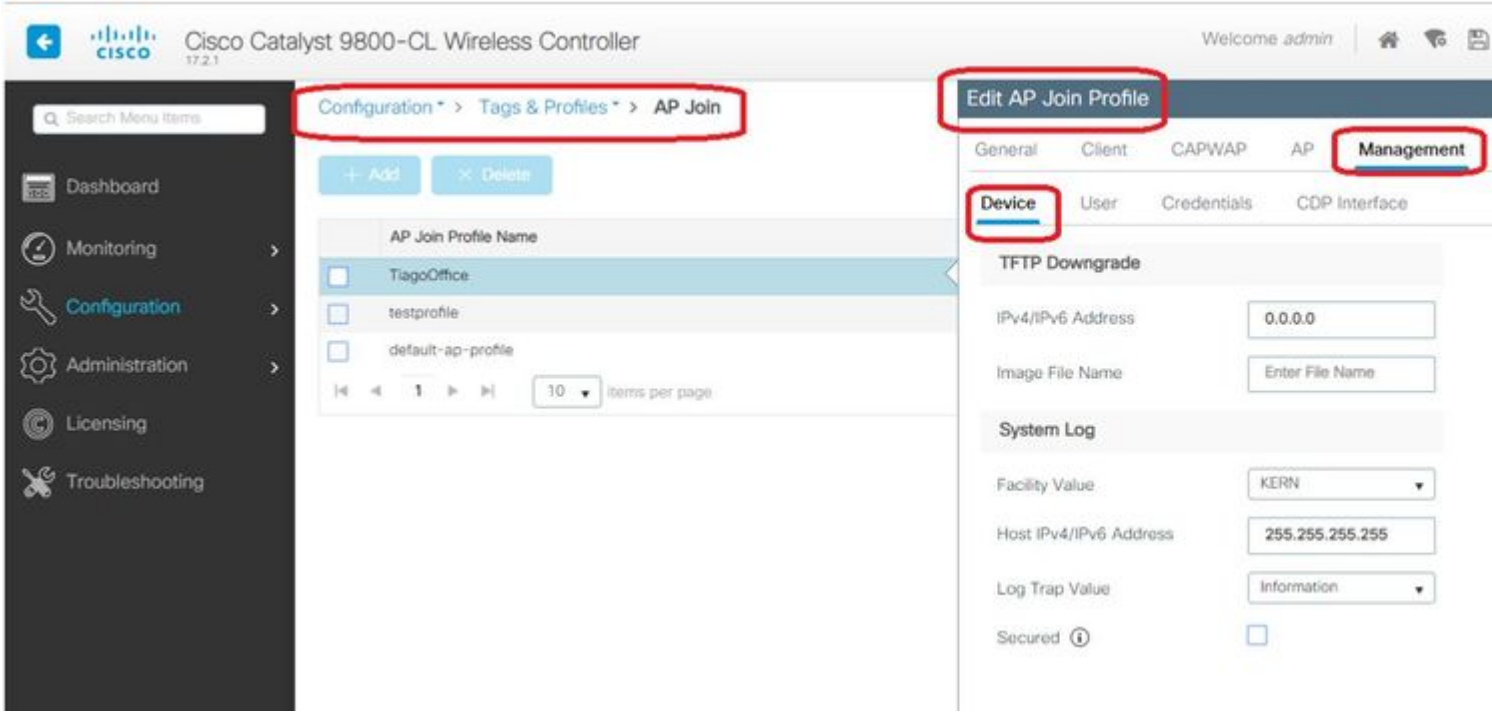
config-

ap

-profile

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

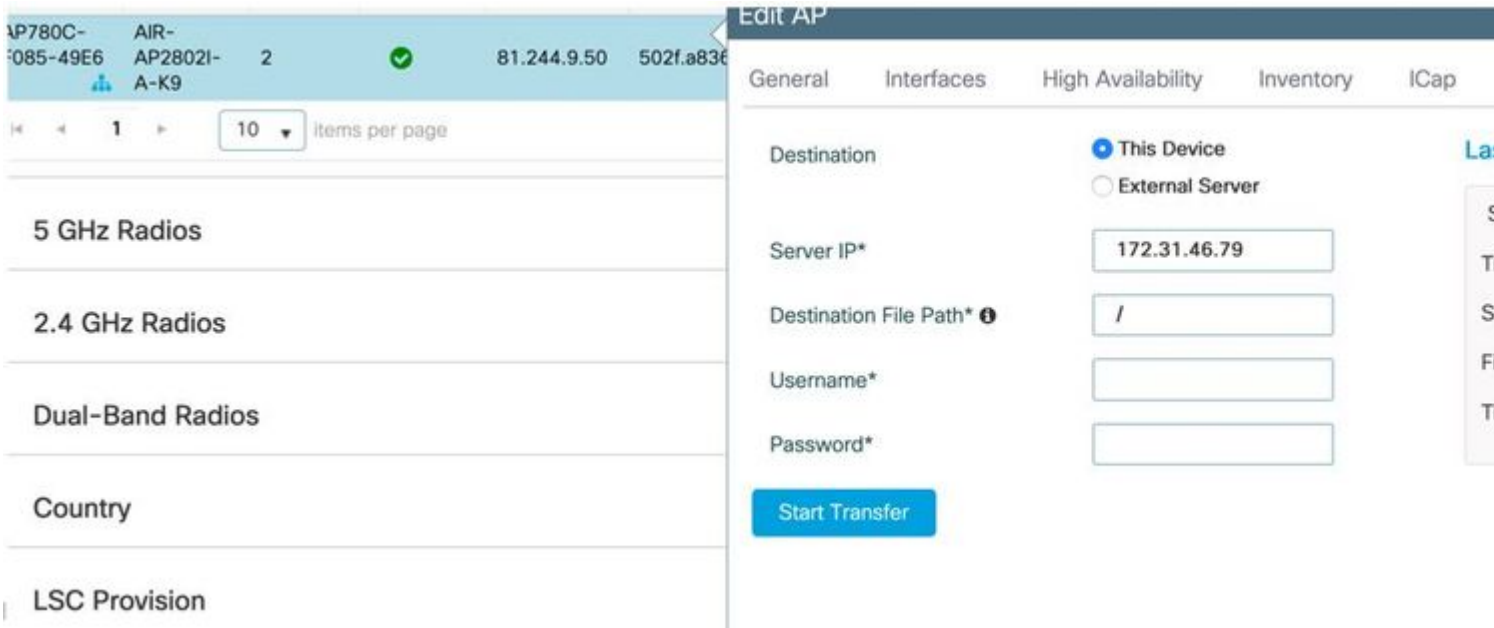
Benutzeroberfläche von Cisco IOS®



Ab Cisco IOS® XE 17.3.1 haben Sie die Registerkarte für Support-Pakete und können den AP SB über die WLC-GUI herunterladen.

Er führt lediglich den Befehl "***copy support-bundle"*** auf dem AP aus und sendet ihn über SCP an den WLC (da es sich bei dem WLC um einen SCP-Server handeln kann).

Und dann können Sie es von Ihrem Browser herunterladen:



Das bedeutet, dass Sie in eWLC-Versionen vor 17.3.1 den gleichen Trick manuell ausführen können:

Kopieren Sie das Support-Paket von AP über SCP nach eWLC IP, wenn kein TFTP-Server mit dem AP erreichbar ist.

Der eWLC ist in der Regel über SSH vom Access Point aus erreichbar, sodass ein guter Trick für die Zeit vor 17.3 gegeben ist.

Schritt 1: SSH auf 9800 v17.2.1 aktivieren

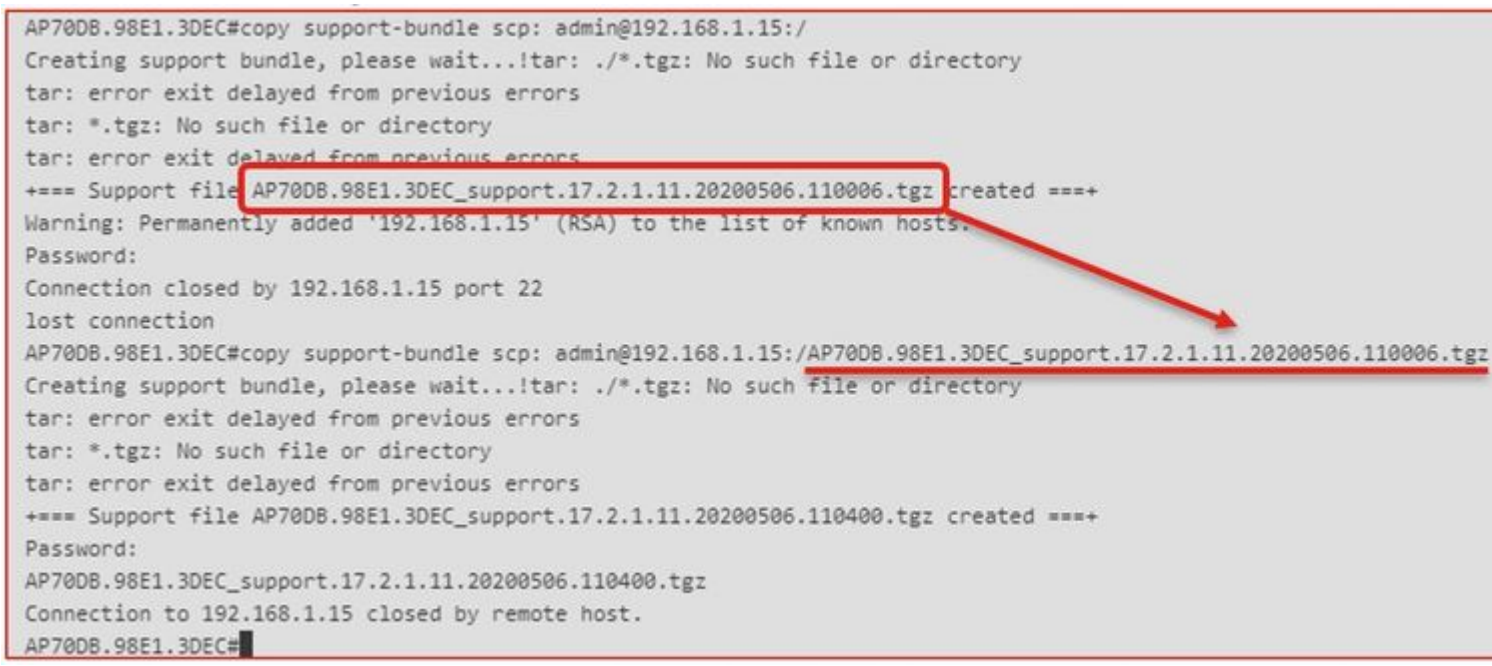
Schritt 2: Aktivierung von SCP unter Cisco IOS® XE v17.2.1

Dieses Beispiel zeigt, wie die serverseitige Funktionalität von SCP konfiguriert wird. In diesem Beispiel werden ein lokal definierter Benutzername und ein Kennwort verwendet:

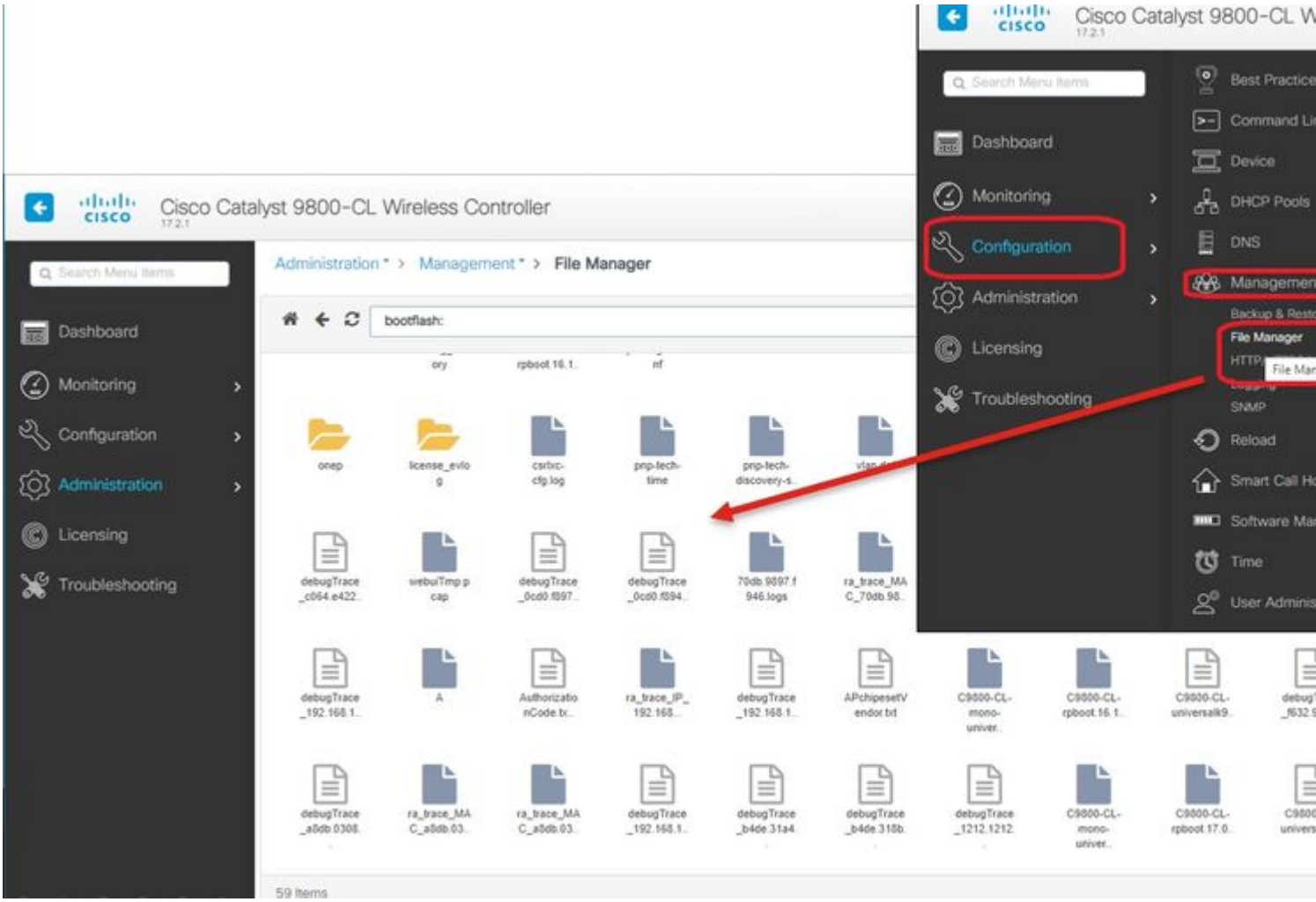
```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username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

Schritt 3: Verwenden Sie den Befehl "***copy support-bundle***", und wir müssen den Dateinamen angeben, der auf dem SCP-Server erstellt werden soll.

Tipp: Sie können den Befehl einmal ausführen, um einen aussagekräftigen Dateinamen zu erhalten, und diesen Dateinamen dann kopieren/einfügen:



Schritt 4: Anschließend können Sie in die eWLC-GUI gehen und die Datei unter: **Administration > Management > File Manager** abrufen:



IoT und Bluetooth

Die gRPC-Serverprotokolle können auf dem Access Point mit folgenden Einstellungen überprüft werden:

```
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 "
```

Die Verbindung zum DNA Spaces-Connector kann wie folgt überprüft werden:

```
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
```

So zeigen Sie die aktuelle BLE-Broadcast-Konfiguration des Access Points an:

```
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.
```

Die gescannten Ergebnisse finden Sie unter:

```
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
```

Wenn der Access Point im erweiterten BLE-Gateway-Modus agiert, in dem eine Anwendung bereitgestellt wird, können Sie den Status der IoX-Anwendung überprüfen:

```
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
```

Sie können sich mit diesen Befehlen mit der IOX-Anwendung verbinden und dann die Protokolle während der Konfiguration des Beacons überwachen:

```
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
```

Schlussfolgerung

Es stehen zahlreiche Tools zur Fehlerbehebung zur Verfügung, die uns bei der Behebung von Problemen im Zusammenhang mit COS-APs helfen.

Dieses Dokument listet die am häufigsten verwendeten auf und wird regelmäßig aktualisiert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.