# COS AP 문제 해결

## 목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> 패킷 추적 캡처(스니퍼 추적) <u>AP 포트의 유선 PCAP</u> <u>절차</u> <u>명령 옵션</u> 필터를 사용한 유선 PCAP 무선 캡처 <u>절차</u> <u>다음을 확인합니다.</u> <u>기타 옵션</u> <u>9800 WLC에서 AP 클라이언트 추적 제어</u> <u>스니퍼 모드의 AP Catalyst 91xx</u> 문제 해결 정보 <u>경로 MTU</u> 부팅 시 디버그를 활성화하려면 <u>절전 메커니즘</u> 클라이언트 QoS <u>Off-Channel 스캔</u> <u>클라이언트 연결</u> Flexconnect 시나리오 <u>AP 파일 시스템</u> <u>syslog 저장 및 전송</u> <u>AP 지원 번들</u> <u>원격으로 AP 코어 파일 수집</u> AireOS CLI AireOS GUI Cisco IOS® CLI Cisco IOS® GUI <u>IoT 및 Bluetooth</u> 결론

## 소개

이 문서에서는 Cheatah OS AP(COS AP라고도 함)에 사용할 수 있는 몇 가지 문제 해결 툴에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

#### 사용되는 구성 요소

이 문서에서는 시리즈 2800, 3800, 1560, 4800의 AP 모델과 같은 COS AP와 새로운 11ax AP Catalyst 91xx에 대해 중점적으로 살펴봅니다.

이 문서에서는 AireOS 8.8 이상에서 사용할 수 있는 여러 기능에 초점을 맞추고 있습니다. 또한 Cisco IOS® XE 16.2.2s 이상도 포함됩니다.

이전 릴리스의 특정 기능 가용성에 대한 의견이 있을 수 있습니다.

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

## 패킷 추적 캡처(스니퍼 추적)

#### AP 포트의 유선 PCAP

AP 이더넷 포트에서 pcap를 사용할 수 있는 것은 (8.8에서 사용 가능한 필터의 경우 8.7부터) 가능 합니다. CLI에서 결과를 실시간으로 표시하거나(요약된 패킷 세부사항만 포함) AP 플래시에 전체 캡으로 저장할 수 있습니다.

유선 pcap는 이더넷 측(Rx/Tx 모두)의 모든 것을 캡처하며, AP 내부의 탭 포인트는 패킷이 배선되 기 바로 전에 있습니다.

그러나 AP CPU 플레인 트래픽만 캡처합니다. 즉, AP로 드나드는 트래픽(AP DHCP, AP capwap 제 어 터널, ...)을 의미하며 클라이언트 트래픽은 표시되지 않습니다.

크기가 매우 제한적이므로(최대 크기 제한 5MB) 관심 있는 트래픽만 캡처하도록 필터를 구성해야 할 수 있습니다.

트래픽 캡처를 복사하기 전에 "no debug traffic wired ip capture(디버그 트래픽 유선 IP 캡처 없음)" 또는 단순히 "undebug all(모두 디버그 해제)"을 사용하여 트래픽 캡처를 중지해야 합니다. 그렇지 않으면 패킷이 계속 기록되므로 복사가 끝나지 않습니다.

#### 절차

1단계. pcap를 시작하고 "debug traffic wired ip capture"로 트래픽 유형을 선택합니다.

<#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)

2단계. 트래픽이 이동할 때까지 기다린 다음 "no debug traffic wired ip capture" 또는 "undebug all" 명령을 사용하여 캡처를 중지합니다.

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

3단계. 파일을 tftp/scp 서버에 복사합니다.

<#root>

AP70DB.98E1.3DEC#copy pcap

AP70DB.98E1.3DEC\_capture.pcap0

4단계. 이제 wireshark에서 파일을 열 수 있습니다. 파일은 pcap0입니다. 자동으로 wireshark와 연 결되도록 pcap로 변경합니다.

명령 옵션

debug traffic wired 명령에는 특정 트래픽을 캡처하는 데 도움이 되는 몇 가지 옵션이 있습니다.

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

debug 명령의 끝에 "verbose"를 추가하여 패킷의 16진수 덤프를 확인할 수 있습니다. 필터가 충분 히 좁지 않으면 CLI 세션이 매우 빠르게 마비될 수 있습니다.

필터를 사용한 유선 PCAP

필터 형식은 tcpdump 캡처 필터 형식과 일치합니다.

	필터 예	설명		
호스트	"호스트 192.168.2.5"	이렇게 하면 패킷 캡처가 필터링되어 호스트 192.168.2.5로 이동하거나 호스트 192.168.2.5에서 오는 패킷만 수집합니다.		
	"src host 192.168.2.5"	이렇게 하면 패킷 캡처가 필터링되어 192.168.2.5에서 오 는 패킷만 수집됩니다.		
	"dst host 192.168.2.5"	이렇게 하면 패킷 캡처가 필터링되어 192.168.2.5로 이동 하는 패킷만 수집됩니다.		
포트	"포트 443"	이는 소스 또는 대상이 포트 443인 패킷만 수집하도록 패 킷 캡처를 필터링합니다.		
	"src port 1055"	이는 포트 1055에서 시작되는 트래픽을 캡처합니다.		
	"dst port 443"	이는 포트 443으로 향하는 트래픽을 캡처합니다.		

다음은 콘솔에 출력이 표시되지만 CAPWAP 데이터 패킷만 보려면 필터링한 예입니다.

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#

파일의 출력 예:

#### wireshark에서 캡처를 열려면

APC4F7.D54C.E77C_capture.pcap0			- 🗆 X
File Edit View Go Capture Analyze	Statistics Telephony Wireless Tool	s Help	
Apply a display filter <ctrl-></ctrl->			Expression +
No. Delta Source	Destination	Lengt Info	Payload Type Diffe
1 0.000000 192.168.1.82	192.168.1.15	651 Application Data	Clas
2 0.001525 192.168.1.15	192.168.1.82	123 Application Data	Clas
3 0.601152 192.168.1.4	255.255.255.255	305 CAPWAP-Control - Primary Discovery Request[Malformed Packet]	Clas
4 9.638243 192.168.1.82	192.168.1.15	987 Application Data	Clas
5 0.001627 192.168.1.15	192.168.1.82	123 Application Data	Clas
6 0.010493 192.168.1.82	192.168.1.15	171 Application Data	Clas
7 0.001007 192.168.1.15	192.168.1.82	123 Application Data	Clas
8 0.000287 192.168.1.82	192.168.1.15	187 Application Data	Clas
9 0.000810 192.168.1.15	192.168.1.82	123 Application Data	Clas
10 28.344341 192.168.1.82	192.168.1.15	123 Application Data	Clas
11 0.001214 192.168.1.15	192.168.1.82	139 Application Data	Clas
12 21.065522 192.168.1.82	192.168.1.15	651 Application Data	Clas
- 13 0.001215 192.168.1.15	192.168.1.82	123 Application Data	Clas
¢			
<ul> <li>&gt; Frame 1: 651 bytes on wire (5208 b)</li> <li>&gt; Ethernet II, Src: Cisco_4c:e7:7c (</li> <li>&gt; Internet Protocol Version 4, Src:</li> <li>&gt; User Datagram Protocol, Src: Port:</li> <li>&gt; Control And Provisioning of Wirele</li> <li>&gt; Datagram Transport Layer Security</li> </ul>	its), 651 bytes captured (\$208 c4:f7:d5:4c:e7:7c), Dst: Cisco_ 192.168.1.82, Dst: 192.168.1.15 5264, Dst Port: 5246 iss Access Points - Control	bits) lc:d2:ff (00:le:bd:lc:d2:ff)	

### 무선 캡처

라디오의 제어 평면에서 패킷 캡처를 활성화할 수 있습니다. 성능 영향으로 인해 무선 데이터 플레 인에서 캡처할 수 없습니다.

즉, 클라이언트 연결 흐름(프로브, 인증, 연결, eap, arp, dhcp 패킷 및 ipv6 제어 패킷, icmp, ndp)은 표시되지만 연결 상태로 이동한 후 클라이언트가 전달하는 데이터는 표시되지 않습니다.

절차

1단계. 추적된 클라이언트 mac 주소를 추가합니다. 여러 mac 주소를 추가할 수 있습니다. 모든 클 라이언트에 대해 명령을 실행할 수도 있지만 권장하지 않습니다.

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.

2단계. 특정 프로토콜 또는 지원되는 모든 프로토콜만 기록하도록 필터를 설정합니다.

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

3단계. 콘솔에 출력을 표시하도록 선택(비동기적으로):

4단계. 추적을 시작합니다.

config ap client-trace start

예:

<#root>

APOCD0.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 1 1 testewlcwlan -41 MCS92SS No 0 APOCD0.F894.46E4#config ap client-trace address add A8:DB:03:08:4C:4A APOCD0.F894.46E4#config ap client-trace filter Trace ALL filters all arp Trace arp Packets assoc Trace assoc Packets Trace auth Packets auth Trace dhcp Packets dhcp eap Trace eap Packets icmp Trace icmp Packets ipv6 Trace IPv6 Packets ndp Trace ndp Packets probe Trace probe Packets APOCD0.F894.46E4#config ap client-trace filter all enable APOCD0.F894.46E4#configure ap client-trace output console-log enable APOCD0.F894.46E4#configure ap client-trace start APOCD0.F894.46E4#term mon

캡처를 중지하려면

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

다음을 확인합니다.

#### 클라이언트 추적 확인:

<#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 : probe Client Trace Filter Client Trace Filter 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 : icmp∨6 Client Trace Filter : ndp Client Trace Filter : arp Client Trace Output : eventbuf Client Trace Output : console-: console-log Client Trace Output : dump Client Trace Output : remote Remote trace IP : 192.168.1.100 κemote trace IP: 192.3Remote 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

성공적인 클라이언트 연결의 예:

Apr Apr Apr Apr Apr Apr Apr Apr Apr Apr	6 10:45:21 kernel: [+04/06/2020 10:45:21.5351] [1566169921:535099] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:21.5351] [1566169921:536215] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:21.54616] [1566169921:545145] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:21.54616] [1566169921:545145] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:21.54616] [1566169921:545145] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.54616] [1566169921:545144] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5761] [1566169921:545144] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:547616] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:547616] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:54552] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:54552] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:54552] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:55552] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:55552] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.5764] [1566169921:55552] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.6757] [1566169921:602871] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.6757] [1566169921:602871] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.6757] [1566169921:67558] [APOCD0.PE94.4624] 6 10:45:21 kernel: [+04/06/2020 10:45:22.6757] [1566169921:67518] [APOCD0.PE94.4624]	[a5:db:03:05:4c:4a] <apr0v0> [U:N] DOTI_ATTHENTICATION : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DOTI_ATTHENTICATION : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DOTI_ASTOC REQUEST : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DOTI_ASTOC REPORTS : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DOTI_ASTOC REPORTS : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATIA_STOC REPORTS : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATIA_STOC REPORTS : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATOA IN : Descrype 0x02 KeyInfo 0x008b [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATOA IN : Descrype 0x02 KeyInfo 0x018b [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATOA IN : Descrype 0x02 KeyInfo 0x030b [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATOA IN : Descrype 0x02 KeyInfo 0x030b [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATOA IN : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATIA_ATION : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATIA_ATION : (.) [a6:db:03:06:4c:4a] <apr0v0> [D:N] DATIA_ATION : (.)</apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0></apr0v0>
Apr Apr Apr Apr Apr Apr Apr Apr Apr Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8636] [1586169921:863610] [APOCDD.F894.46E4] 6 10:45:21 kernel: [*04/06/2020 10:45:21.8636] [1586169921:863644] [APOCDD.F894.46E4] 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863703] [APOCDD.F894.46E4] 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863731] [APOCDD.F894.46E4] 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:86374] [APOCDD.F894.46E4] 6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:86374] [APOCDD.F894.46E4] 6 10:45:21 kernel: [*04/06/2020 10:45:21.8677] [1586169921:86374] [APOCDD.F894.46E4] 6 10:45:12 kernel: [*04/06/2020 10:45:21.8677] [1586169921:86764] [APOCD 6 10:45:12 kernel: [*04/06/2020 10:45:21.8677] [1586169921:86749] [APOCD 6 10:45:12 kernel: [*04/06/2020 10:45:21.8678] [1586169921:867740] [APOCD 6 10:45:12 kernel: [*04/06/2020 10:45:21.8678] [1586169921:86749] [APOCD 6 10:45:21 kernel: [*04/06/2020 10:45:21.8678] [1586169921:	<pre>[a8:db:02*1.4:a] <apr0v0> [U:W] DHCP_DISCOVER : TransId 0xa38c0ld6 [a8:db:02*1.4:a] <apr0v0> [U:C] DHCP_DISCOVER : TransId 0xa38c0ld6 [a8:db:03:05:4:4:a] <apr0v0> [U:C] DHCP_DISCOVER : TransId 0xa38c0ld6 [a5:05:4:4:a] <apr0v0> [U:C] DHCP_DISCOVER : TransId 0xa38c0ld6 [a5:05:4:4:4] <aproxempa0> [U:E] DHCP_DISCOVER : TransId 0xa38c0ld6 [a5:05:4:4:4] <aproxempa0>[U:E] DHCP_DIFER : TransId 0xa38c0ld6 [a5:05:4:4:4] <aproxempa0>[U:C] DHCP_OFFER : TransId 0xa38c0ld6 [a5:05:4:4:4] <aproxempa0>[U:C] DHCP_OFFER : TransId 0xa38c0ld6 [a5:05:03:06:4:4:4] <aproxempa0>[U:R] DHCP_OFFER : TransId 0xa38c0ld6 [a5:05:03:06:4:4:4] <apre>[a5:05:03:06:4:4:4] <apre>[a5:05:03:06:4:4:4] <apre>[a5:05:06:06:06:06:06:06:06:06:06:06:06:06:06:</apre></apre></apre></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></aproxempa0></apr0v0></apr0v0></apr0v0></apr0v0></pre>
April	U - Uplink packet (from client) D - Downlink packet (to client) W - module Wireless driver E - module Ethernet driver C - module Click	03:00:4c:4a (appr00: [D:W] DHCP_OFTER : TransId Oxa36cOldd 03:00:4c:4a (appr00: [D:W] DHCP_REQUEST : TransId Oxa36cOldd 03:00:4c:4a (appr00: [D:W] DHCP_REQUEST : TransId Oxa36cOldd 03:00:4c:4a (appr00: [D:C] DHCP_RCX : TransId Oxa36cOldd
Apr Apr Apr Apr Apr Apr Apr Apr Apr	6 10 6 10 6 10: 6 10: 6 10: 6 10:45.2 kernel: [+04/06/2020 10:45:22.1611] [1586169922:161177] [APOCDO.F894.46E4] 6 10:45:22 kernel: [+04/06/2020 10:45:22.1612] [1586169922:161213] [APOCDO.F894.46E4] 6 10:45:22 kernel: [+04/06/2020 10:45:22.1646] [1586169922:164673] [APOCDO.F894.46E4] 6 10:45:22 kernel: [+04/06/2020 10:45:22.1647] [1586169922:164673] [APOCDO.F894.46E4] 6 10:45:22 kernel: [+04/06/2020 10:45:22.1647] [1586169922:164672] [APOCDO.F894.46E4] 6 10:45:22 kernel: [+04/06/2020 10:45:22.1647] [1586169922:164732] [APOCDO.F894.46E4] 6 10:45:22 kernel: [+04/06/2020 10:45:22.1647] [1586169922:164732] [APOCDO.F894.46E4]	D3:08:4c:4a] <msscapwap0> [D:C] DHCP_ACK : TransId 0xa38c01d6 D3:08:4c:4a] <mprov0> [D:N] NUCP_ACK : TransId 0xa38c01d6 AC 03:08:4c:4a] <mprov0> [D:N] NUCP_ACK : TransId 0xa38c01d6 AC 03:08:4c:4a] <mprov0> [U:C] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1 [A8:db:03:06:4c:4a] <mprov0> [U:C] ARP_REPX : Sender 192.168.101.13 TargIp 192.168.101.1 [A8:db:03:06:4c:4a] <mscapwap0> [D:C] ARP_REPX : Sender 192.168.101.1 NwAddr 54:7:c60:b7:36:42 [A8:db:03:06:4c:4a] <mscapwap0> [D:C] ARP_REPX : Sender 192.168.101.1 NwAddr 54:7:c60:b7:36:42 [A8:db:03:06:4c:4a] <mscapwap0> [D:C] ARP_REPX : Sender 192.168.101.1 NwAddr 54:7:c60:b7:36:42 [A8:db:03:06:4c:4a] <mscapwap0> [D:C] ARP_REPX : Sender 192.168.101.1 NwAddr 54:7:c60:b7:36:42</mscapwap0></mscapwap0></mscapwap0></mscapwap0></mprov0></mprov0></mprov0></mprov0></mprov0></mprov0></mprov0></msscapwap0>

대괄호 사이의 문자는 해당 프레임이 어디에서 표시되었는지(이더넷의 경우 E, 무선의 경우 W, AP의 내부에 있는 경우 Click 모듈의 경우 C) 및 어느 방향(Upload 또는 Download)으로 표시되었는 지를 이해하는 데 도움이 됩니다.

여기 이 글자들의 의미를 보여주는 작은 표가 있다:

U - 업링크 패킷(클라이언트에서) D - 다운링크 패킷(클릭하여) W - 모듈 무선 드라이버 E - 모듈 이더넷 드라이버 C - 모듈 클릭

기타 옵션

비동기적으로 로그 보기:

그런 다음 "show ap client-trace events mac xx:xx:xx:xx:xx" 명령을 사용하여 로그를 참조할 수 있습니다(또는 mac을 "all"로 대체).

<#root>

AP0CD0.F894.46E4#

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

```
[*04/06/2020 10:11:54.287675] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.288144] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:11:54.289870] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:11:54.317341] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:11:54.341370] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:11:54.341370] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:11:54.374500] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M2 : Desc
```

[*04/06/2020	10:11:54.377237]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	EAPOL_KEY.M3 : Desc
[*04/06/2020	10:11:54.390255]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[U:W]	EAPOL_KEY.M4 : Desc
[*04/06/2020	10:11:54.396855]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[U:W]	DOT11_ACTION : (.)
[*04/06/2020	10:11:54.416650]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	DOT11_ACTION : (.)
[*04/06/2020	10:11:54.469089]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[U:W]	DOT11_ACTION : (.)
[*04/06/2020	10:11:54.469157]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	DOT11_ACTION : (.)
[*04/06/2020	10:11:57.921877]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[U:W]	DOT11_ACTION : (.)
[*04/06/2020	10:11:57.921942]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	DOT11_ACTION : (.)
[*04/06/2020	10:15:36.123119]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	DOT11_DEAUTHENTICAT
[*04/06/2020	10:15:36.127731]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	DOT11_DISASSOC : (.
[*04/06/2020	10:17:24.128751]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	DOT11_AUTHENTICATIO
[*04/06/2020	10:17:24.128870]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v1></apr0v1>	[U:W]	DOT11_AUTHENTICATIO
[*04/06/2020	10:17:24.129303]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	DOT11_AUTHENTICATIO
[*04/06/2020	10:17:24.133026]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	DOT11_ASSOC_REQUEST
[*04/06/2020	10:17:24.136095]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	DOT11_ASSOC_RESPONS
[*04/06/2020	10:17:24.138732]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	EAPOL_KEY.M1 : Desc
[*04/06/2020	10:17:24.257295]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	EAPOL_KEY.M2 : Desc
[*04/06/2020	10:17:24.258105]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	EAPOL_KEY.M3 : Desc
[*04/06/2020	10:17:24.278937]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	EAPOL_KEY.M4 : Desc
[*04/06/2020	10:17:24.287459]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	DOT11_ACTION : (.)
[*04/06/2020	10:17:24.301344]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	DOT11_ACTION : (.)
[*04/06/2020	10:17:24.327482]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	DOT11_ACTION : (.)
[*04/06/2020	10:17:24.327517]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	DOT11_ACTION : (.)
[*04/06/2020	10:17:24.430136]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	DOT11_ACTION : (.)
[*04/06/2020	10:17:24.430202]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	DOT11_ACTION : (.)
[*04/06/2020	10:19:08.075326]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[U:W]	DOT11_PROBE_REQUEST
[*04/06/2020	10:19:08.075392]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	DOT11_PROBE_RESPONS
[*04/06/2020	10:19:08.075437]	[APOCD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v1></apr0v1>	[U:W]	DOT11_PROBE_REQUEST

16진수 형식으로 패킷 덤프

CLI에서 16진수 형식의 패킷을 덤프할 수 있습니다.

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

AP70DB.90E1.3DEC#configu	ire 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#Apz 6	13:20:53 kernel: [*04/06/2020 13:20:53:2037] 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-trac	re output dump address add a8:dD103:00:40:4a
AP70DB.90E1.3DEC#Apr 6	13:29:02 kernel: [*04/06/2020 13:29:02.5997] MAC already exists: index 0
configure ap client-trac	e output dump
address Remote/Local	dump Client Addresses
enable Enable Trace	output for local dump
AP70DB.90E1.3DEC#configu	ire ap client-trace output dump enable
<e-s000> Enter the pa</e-s000>	sczet dump length value
AP70DB.SUEL.SDEC#Configu	ire ap client-trace output dump enable 100
SCEP	
APTOLS. SEEL. SDECECONFLOR	ire ap dilent-trade dutput dump emable 100
APTODD. SOLL SDECEMPE 6	10:27:27:27:27:27:27:27:27:27:27:27:27:27:
Apr 6 13:30:37 kernel:	
hor d 13:25:27 kernel:	
Apr. 6 13-29-27 kernel:	
Apr # 13-29-27 kernel:	104/06/2020 13:23:27 26 46 31 0030 00 00 37 00 00 06 00 07 00 01 00 00 00 00
Apr 6 13:29:27 kernel:	104/06/2020 13:29:27 46451 0040 00 01 2c 00 00 45 31 21 0f 45 48 00 00 00 00 00
Apr 6 13:29:27 kernel:	1*04/06/2020 13:29:27 46451 0050 00 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 80 01 30 00 00 27 e3 36 4d a0 a8 db 03 08 4e
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 13:29:27.46501 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] 0050 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:474003us Dir:Tx Rate:1 Rssi:=95 Ch:1 Fc:200 Dur:13a a0:db:03:00:4c:4a 00:27:e3:36:4d:a0 54:7c:69:b7:3f:42 Seq:6(6) Info:ARP Retry:0 Len:104 Typesub:20 Tid:q0
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
Apr 6 13:29:27 kernel:	(*04/06/2020 13:29:27.4749) 0010 00 00 00 00 00 00 11 00 00 00 00 0
Apr 6 13:29:27 kernel:	(*04/06/2020 13:29:27.4745) 0020 00 00 13 88 15 b3 ff ff 00 00 ml ml 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 80 02
Apr 6 13:29:27 kernel:	(*04/06/2020 13:29:27.4745) 0040 3a 01 a0 db 03 08 4c 4a 00 27 e3 36 4d a0 54 7c
Apr 6 13:29:27 kernel:	1*04/06/2020 13:29:27.47491 0050 69 b7 3f 42 60 00 00 00 am am 03 00 00 00 06
Apr 6 13:29:27 kernel:	[*04/06/2020 13:29:27.4749] 0060 00 01 08 00 06 04 00 02 84 7c 69 b7 3f 42 co a8
Apr 6 13:29:27 kernel:	[*04/06/2020 13:29:27.4749] 0070 65 01 48 db 03 08 4c 4a c0 a8 65 0d 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 0
Apr 6 13:29:27 kernel:	(*04/06/2020 13:29:27.4750) 0090 00 00 ED
Apr 6 13:31:03 kernel:	[*04/04/2020 13:31:03.1800]
Apr 6 13:31:03 Kernel:	["04/04/2020 13:31:03.1000] Time: S0001908 Dir:kk kate's kss1-34 Ch:1 F0:40 Dar:0 Fr:Fr:Fr:Fr:Fr:Fr:Fr:Fr:Fr:Fr:Fr:Fr:Fr:F
Apr 6 13:31:03 kernel:	
Apr 6 13:31:03 Rernel:	
Apr d 13:31:03 kernel:	
Apr 6 13:31:03 kernel:	
Apr d 13:31:03 kernel:	
Apr 6 13:31:03 kernel:	
apr 6 13:31:03 kernel:	
Apr. 6 13:31:03 kernel:	1-04/06/2020 13:31:03 18011 0080 00 00 00 00 00 00 07 04 00 00 48 00 00 40 00
Apr 6 13:31:03 kernel:	104/06/2020 13:31:03 18011 0050 40 00 31 ff
Apr 6 13:31:03 kernel:	(+04/06/2020 13:31:03.2000)
Apr 6 13:31:03 kernel:	1-04/06/2020 13:31:03.20001 Time: 200015us Dir: Tx Base: 1 Basi: -55 Ch:1 Fe:50 Dur: 13a a0:db:03:00:4e:4a 00:27:=3:36:4d:a0 00:27:=3:36:4d:a0 Sec: 65e(1630) Info: DOT11 DROBE DESCONSE Betry: 0 Len: 250 Typesub: 05
Apr 6 13:31:03 kernel:	1+04/06/2020 13:31:03.20001 0000 00 00 00 00 00 00 00 00 00 00
Apr 6 13:31:03 kernel:	1+04/06/2020 13:31-03.20001 0010 00 00 00 00 00 00 11 00 00 00
Apr 6 13:31:03 kernel:	f*04/06/2020 13:31:03.20001 0020 00 00 13 88 15 b3 ff ff 00 00 a1 a1 00 e2 00 e3
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 a0 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 00 12 18 34 03 01 0d 64 00
Apr 6 13:31:03 kernel:	(*04/06/2020 13:31:03.2001) 0060 11 11 00 00 74 65 73 74 65 77 60 61 77 60 61 60
Apr 6 13:31:03 kernel:	1*04/06/2020 13:31:03.20011 0070 01 08 82 84 8b 96 00 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 6e 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:20016lus Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:50 Dur:13a a0:db:03:00:4c:4a 00:27:e3:36:4d:a1 Seq:65f(1631) Info:DOT11_PROBE_RESPONSE Retry:0 Len:251 Typesub:05
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

## 그런 다음 hex 덤프를 정리하고 txt 형식으로 저장한 다음 wireshark로 가져올 수 있습니다.

Time:2001Ous 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:a 0000 00 00 00 00 00 00 00 00 00 00 00 0	0 Seq:1(1) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
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:a 0000 00 00 00 00 00 00 00 00 00 00 00 0	0 Seq:66c(1644) Info:DOT11_ACTION Retry:0 Len:54 Typesub:0d
Time:43155us Dir:Tx Rate:1 Rss:-95 Ch:1 Fc:b0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a 0000 00 00 00 00 00 00 00 00 00 00 00 0	0 Seq:66d(1645) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
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: 0000 00 00 00 00 00 00 00 00 00 00 00 0	a0 Seq:2(2) Info:DOT11_ASSOC_REQUEST Retry:1 Len:220 Typesub:00

The Wireshark Network An Edit View Go Cap	alyzer oture Analyze S	statistics Telephon	Wireless Tools Help	-		×
Open Open Recent Merge	Ctrl+O		Q Q Q II		Expression	less
Close Save Save As File Set Export Specified Packets Export Packet Dissections Export Packet Bytes	Ctrl+W Ctrl+S Ctrl+Shift+S	Data\Local\Temp 234744 HelpDesk O\00-SRs\SR 688 O\00-SRs\SR 688 O\11ax training\1 O\11ax training\1	Wireshark - Import From Hex Dump ? X Import From File: C:/Users/tantunes/CISCO/11ax training/dump_example.txt Browse Offsets:  Hexadecimal Contal O Octal None	)		
Export PDUs to File Export TLS Session Keys Export Objects Print	• Ctrl+P	O\11ax training\1 Data\Local\Temp nloads\AP_trace_ O\IOS-Images\A	Timestamp format: (No format will be applied) Direction indication: Encapsulation Encapsulation Type: Ethernet			
Quit	Ctrl+Q	nter a capture filter .	No dummy header     Etherstype (hex):     IPv4 Protocol (dec):     VIDP Source port:	1		
	Npcap Loopbi Ethernet_yello Local Area Co Local Area Co Ethernet 4 Wi-Fi ThinkpadEthe Local Area Co Adapter for Io Local Area Co	Act Adapter wCable nnection* 3 nnection* 9 rnetBlue nnection* 11 opback traffic captu nnection* 2	TCP     Destination port:       SCTP     Tag:       SCTP (Data)     PP1:       ExportPOU     Payload   Maximum frame length:	L		

출력이 매우 클 수 있으며, 출력에 표시되는 프레임 유형만 언급되고 내부 세부사항은 언급되지 않 으므로 패킷 캡처를 캡처 애플리케이션(예: wireshark)을 실행하는 랩톱으로 리디렉션하는 것이 더 효율적일 수 있습니다.

원격 캡처 기능을 활성화하여 wireshark를 사용하는 외부 디바이스로 패킷을 전송합니다.

config ap client-trace output remote enable

이 명령은 AP가 클라이언트 추적 필터에 의해 캡처된 모든 프레임을 192.168.68.68의 랩톱으로 전 달하고 포트 5000에서 PEEKREMOTE 캡슐화(스니퍼 모드의 AP와 유사)를 사용함을 의미합니다.

한 가지 제한 사항은 대상 랩톱이 이 명령을 실행하는 AP와 동일한 서브넷에 있어야 한다는 것입니 다. 네트워크의 보안 정책을 수용하려면 포트 번호를 변경할 수 있습니다.

Wireshark를 실행하는 랩톱에서 모든 패킷을 수신하면 udp 5000 헤더를 마우스 오른쪽 버튼으로 클릭하고 decode as를 선택하고 다음 그림에 나와 있는 것처럼 PEEKREMOTE를 선택할 수 있습 니다.

🕻 🗏 🔬 🛞 🧧 🚰 🛣 🖉 🤤 👄				201	- Extransi	on 4
lo, Delta Source	Destination	Lengt Info		CaD is	Payload Type	
59         0.000000           60         0.00116         0.05146           61         0.03146         0.05146           62         0.000000         SamsungE_0014c14a           62         0.000000         SamsungE_0014c14a           63         0.000000         SamsungE_0014c14a           64         0.021832         Clisco_3614d1a0           65         0.000000         SamsungE_0014c14a           66         0.030097         SamsungE_0014c14a           67         0.010008         Clisco_3614d1a0           68         0.000905         SamsungE_0014c14a           69         0.09095         SamsungE_0014c14a           70         0.03015         Clisco_3614d1a0           71         0.030075         Clisco_3614d1a0           72         0.09095         SamsungE_0014c14a           73         0.020075         Clisco_3614d1a0           74         0.000005         IssansungE_00112           75         0.020277         Clisco_3614d1a0           86         0.000001         IssansungE_0014c14a           76         0.020001         SamsungE_0014c14a           77         0.0000001         SamsungE_0014c14a	Mark/Unmark Packet Ignore/Unignore Packet Set/Unset Time Reference Time Shift Packet Comment Edit Resolved Name Apply as Filter Prepare a Filter Prepare a Filter Conversation Filter Colorize Conversation SCTP Follow Copy Protocol Preferences Decode As Show Vacket in New Window Samsung E_08:4c:14a Broadcast Stits), 251 bytes captured (2008 bd Soriab): 251 bytes captured (2008 bd S	251 Probe Request, SH-877, FH-0, Flag 292 Probe Response, SH-410, FN-0, Fla 107 Authentication, SH-578, FN-0, Fla 107 Authentication, SH-578, FN-0, Fla 202 Association Request, SH-637, FN-0 312 Association Response, SH-412, FN- 324 x 331 x 331 x 342 x 351 x 351 x 352 x 352 x 353 x 353 x 354 x 354 x 354 x 354 x 354 x 354 x 355 x	ssC, SSID-testewlcwlan gssC, BE-100, SSID-testewlcwlan gssC gssC SSID-testewlcwlan 0, FlagssC K Current PEEKREMOTE PANA PANA PANA PANA PANA PANA PCLI (imestamp) PCLI2 (imestamp) PCLI2 (imestamp) PCLI2 (imestamp) PCLI2 (imestamp) PCLI3 (	? X	MSDU MSDU MSDU MSDU MSDU MSDU MSDU MSDU	
<ul> <li>AiroPeek/OmniPeek encapsulated IEEE</li> <li>802.11 radio information</li> <li>IEEE 802.11 Probe Request, Flags: .</li> <li>IEEE 802.11 wireless LAN</li> </ul>	E 802.11 C	• - • 5	Ci Kenni Kantures Ken Data Kenamine i Vitresh CK Save Cance	nkidecode as entries I Help		

### 이 기능에 대한 버그 및 개선 사항 목록:



<u>Cisco 버그 ID CSCvm09020</u> 8.8에서 클라이언트 추적에서 더 이상 볼 수 없는 DNS

<u>Cisco 버그 ID CSCvm09015</u>



클라이언트 추적은 Null 시퀀스 번호의 많은 ICMP\_other를 표시합니다.

<u>Cisco 버그 ID CSCvm02676</u>



## AP COS client-trace는 webauth 패킷을 캡처하지 않습니다

Cisco 버그 ID <u>CSCvm02613</u>



### AP COS 클라이언트-추적 원격 출력이 작동하지 않음

Cisco 버그 ID <u>CSCvm00855</u>



클라이언트 추적 SEQ 번호가 일치하지 않습니다.

9800 WLC에서 AP 클라이언트 추적 제어

여러 AP를 구성하여 무선 클라이언트 추적을 수행하고

1단계. 캡처할 트래픽을 정의하는 AP 추적 프로필을 구성합니다

config term wireless profile ap trace filter all no filter probe output console-log

2단계. 대상 AP에서 사용하는 AP 가입 프로파일에 AP 추적 프로파일을 추가합니다.

ap profile < ap join profile name> trace

이 AP 가입 프로필이 대상 AP에서 사용하는 사이트 태그에 적용되었는지 확인합니다

4단계 시작/중지 트리거

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/

확인 명령:

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

스니퍼 모드의 AP Catalyst 91xx

새로운 Catalyst 9115, 9117, 9120 및 9130은 스니퍼 모드로 구성할 수 있습니다. 이 절차는 이전 AP 모델과 동일합니다.





	*ThinknadEthernetRlue
<i>i</i>	minkpaucmemetoide

	Edit View Go Capture Analyze St	atistics Telephony Wireless Too	ls Help	
	। 🧟 🖲 🔚 🖾 🖾 🤇 🗢 🖗	s 🛛 🛓 🚍 🔍 Q Q 🛛	[	
ud	p.port == 5000			
	Delta Source	Destination	Lengti Info	Channel BSS Color
	0.032866 SamsungE_08:4c:4a	Cisco_97:03:ef	107 Authentication, SN=37, FN=0, Flags=C	100
	0.000001 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
	0.001720 Cisco_97:03:ef	SamsungE_08:4c:4a	107 Authentication, SN=0, FN=0, Flags=C	100
	0.000301 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
	0.000791 SamsungE_08:4c:4a	Cisco_97:03:ef	360 Association Request, SN=38, FN=0, Flags=C, SSID=testewlcwlan	100
	0.000230 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
	0.004269 Cisco_97:03:ef	SamsungE_08:4c:4a	398 Association Response, SN=1, FN=0, Flags=C	100 0×01
	0.000750 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
	0.010966 Cisco_97:03:ef	SamsungE_08:4c:4a	221 Key (Message 1 of 4)	100
	0.000001 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
	0.021911 SamsungE 08:4c:4a	Cisco 97:03:ef	342 Key (Message 2 of 4)	100
	0.000002 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
	0.002186 Cisco 97:03:ef	SamsungE 08:4c:4a	391 Key (Message 3 of 4)	100
	0 000935 192 168 1 15	192 168 1 100	76 Acknowledgement[Malformed Dacket]	100
	0.013829 SamcungE 08:4c:4a	Cisco 97:93:ef	109 Key (Maccade A of A)	100
	0.000174 100 160 1 15	102 168 1 100	75 Acknowl adment (Malformed Dacket)	100
_	0.0001/4 192.100.1.15	192.100.1.100	To Acknowledgement[halformed Facket]	100
	> Tag: Fast BSS Transition > Tag: RM Enabled Capabilities ( > Tag: BSS Max Idle Period > Ext Tag: HE Capabilities (IEEE Tag Number: Element ID Exte Ext Tag Length: 46 Ext Tag Number: HE Capabili > HE MAC Capabilities Informa > HE Phy Capabilities Informa > HE Phy Capabilities Informa > Kupported HE-MCS and NSS Se > Rx Max-MCS Maps <= 80 > R HEX-MCS Maps <= 80	5 octets) Std 802.11ax/D3.0) nsion (255) ties (IEEE Std 802.11ax/D3.0) tion: 0.800002100009 tion t MHz: 0xaaaa	(35)	
		= Max HE-MCS for 1 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	10	= Max HE-MCS for 2 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	10	= Max HE-MCS for 3 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	10	= Max HE-MCS for 4 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	10	= Max HE-MCS for 5 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	10	= Max HE-MCS for 6 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	10	= Max HE-MCS for 7 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	10	= Max HE-MCS for 8 SS: Suppo	ort for HE-MCS 0-11 (0x2)	
	> Tx HEX-MCS Map <= 80 M	Hz: Oxaaaa		
	> PPE Thresholds			
	✓ Ext Tag: HE Operation (IEEE St	d 802.11ax/D3.0)		
	Tag Number: Element ID Exte	nsion (255)		
	Ext Tag length: 9			
	Ext Tag Number: HE Operatio	(IEEE Std 802,11ax/D3 0) (3	6)	
	The rep number i he operacio	(		
	) HF Operation Parameters: Gv	993444		
	> HE Operation Parameters: 0x > BSS Color Information: 0x01	003ff4		
	<ul> <li>&gt; HE Operation Parameters: 0x</li> <li>&gt; BSS Color Information: 0x01</li> <li>&gt; Paris HE-MCS and NSS Set 0</li> </ul>	903ff4		

✤ 참고: WIFI 6 데이터 속도로 전송된 데이터 프레임은 캡처되지만, Wireshark에서 peekremote가 최신 상태가 아니므로 현재 802.11ax phy 유형으로 표시됩니다. 이 수정 사항 은 Wireshark 3.2.4에서 Wireshark가 적절한 wifi6 phy 속도를 표시합니다.

✤ 참고: Cisco AP는 현재 MU-OFDMA 프레임을 캡처할 수 없지만 MU-OFDMA 윈도우를 알리 는 트리거 프레임(관리 데이터 속도로 전송)을 캡처할 수 있습니다. MU-OFDMA가 어떤 클라 이언트에 발생하는지(또는 발생하지 않는지) 미리 추론할 수 있습니다.

## 문제 해결 정보

경로 MTU

경로 MTU 검색은 AP에 대한 최적의 MTU를 찾지만 이 설정을 수동으로 재정의할 수 있습니다.

AireOS 8.10.130 WLC에서 명령 config ap pmtu disable <ap/all>은 동적 검색 메커니즘에 의존하지 않고 하나 또는 모든 AP에 대해 고정 MTU를 설정합니다.

부팅 시 디버그를 활성화하려면

config boot debug capwap을 실행하여 다음 부팅 시 OS가 부팅되어 프롬프트가 표시되기 전이라 도 capwap,DTLS 및 DHCP 디버그를 활성화할 수 있습니다.

또한 여러 메모리 디버그에 대해 "config boot debug memory xxxx"가 있습니다.

다음 재부팅 시 "show boot"를 사용하여 부팅 디버그가 활성화되었는지 확인할 수 있습니다.

끝에 disable 키워드가 추가되면 "config boot debug capwap disable"과 같이 비활성화할 수 있습니 다.

절전 메커니즘

특정 클라이언트의 절전 기능은 다음을 실행하여 문제를 해결할 수 있습니다.

디버그 클라이언트 추적 <mac address>

클라이언트 QoS

QoS 태그가 적용되는지 확인하려면 "debug capwap client qos"를 실행할 수 있습니다.

무선 클라이언트에 대한 패킷의 UP 값을 표시합니다.



8.8(개선 요청 Cisco 버그 <u>IDCSCvm08899</u>).

labAP#debug capwap client qos

[\*08/20/2018 09:43:36.3171] chatter: set\_qos\_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8 [\*08/20/2018 09:43:45.0051] chatter: set\_qos\_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8 [\*08/20/2018 09:43:45.5463] chatter: set\_qos\_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8 [\*08/20/2018 09:43:46.5687] chatter: set\_qos\_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:3
[\*08/20/2018 09:43:47.0982] chatter: set\_qos\_up :: SetQosPriority: bridged packet dst: AC:81:12:C7:CD:3

또한 AP의 Qos UP TO DSCP 테이블뿐 아니라 Qos에 의해 표시, 셰이핑 및 삭제된 패킷의 총량도 확인할 수 있습니다.

LabAP#show dot11 gos 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#

Qos 정책이 WLC에 정의되어 있고 Flexconnect AP에 다운로드되어 있는 경우 다음 항목을 사용하여 확인할 수 있습니다.

```
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
Qos 속도 제한의 경우:
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 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

Off-Channel 스캔

AP의 오프 채널 스캔을 디버깅하는 것은 비인가 탐지(AP가 특정 채널을 통해 스캔되는지 여부와 스캔될 때를 검증하기 위해)를 트러블슈팅할 때 유용할 수 있지만, "오프 채널 스캔 지연" 기능이 사 용되지 않을 경우 민감한 실시간 스트림이 지속적으로 중단되는 비디오 트러블슈팅에서도 유용할 수 있습니다.

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

### 클라이언트 연결

액세스 포인트에 의해 최종 이벤트 타임스탬프로 인증되지 않은 클라이언트를 나열할 수 있습니다.

LabA	AP#sł	IOW	dot11	c1i	ents	deauth		
			ti	mes	stamp	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

이전 출력에서 이유 코드는 이 링크에 자세히 설명된 인증 취소 이유 코드입니다.

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

vap는 AP 내의 WLAN(WLC 서버의 WLAN ID와 다름)의 식별자를 !!!.

연결된 클라이언트의 vap를 항상 언급하는 기타 세부 출력과 상호 연관시킬 수 있습니다.

"show controllers Dot11Radio 0/1 wlan"으로 VAP ID 목록을 볼 수 있습니다.

클라이언트가 계속 연결되어 있는 경우 다음 사용자와의 연결에 대한 세부 정보를 얻을 수 있습니 다.

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

클라이언트 항목에 대한 자세한 내용은 다음을 통해 얻을 수 있습니다.

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:fffffae:ffffffa:78:36:ffffff89| 81 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:ffffffa:78:36:ffffff89| 61 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|

 11 |F8:0B:CB:E4:7F:40|00000000| 3 0 1 1 2 3| 1| 1 0 1 1 9 00:AE:FA:78:36:890000003 1| 0 Datapath IPv4 client Summary: \_\_\_\_\_ id vap port node tunnel mac seen\_ip hashed\_ip sniff\_a 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

다음을 사용하여 특정 클라이언트의 연결을 강제로 해제할 수 있습니다.

test dot11 client deauthenticate

트래픽 카운터는 다음과 같은 방법으로 클라이언트당 얻을 수 있습니다.

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#	

무선 통신 레벨에 대한 자세한 내용은 "show controllers"에서 얻을 수 있습니다. 클라이언트 mac 주 소를 추가하면 지원되는 데이터 속도, 현재 데이터 속도, PHY 기능, 재시도 횟수 및 txfail이 표시됩 니다.

#### <#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 160MHz:no 80MHz:no 80+80MHz:no HT:yes VHT:yes HE:no 40MHz: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 mu\_mimo\_capable:no su\_mimo\_capable:yes 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 intf TxData TxMgmt TxUC TxBytes mac TxFail TxDcrd TxCumRetries RxData RxMgmt RxBytes RxErr TxRt RxRt idle\_counter stats\_ago expiration 00:AE:FA:78:36:89 apr0v9 1 0 0 31 1 1599 8 1 6 1038 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 1024 0 0 0 0 146 0 0 3 59 0 0 0 147 0 0 1024 4 0 0 0 0 148 0 0 1024 5 0 149 1024 0 0 0 0 0 0 0 150 1024 6 0 0 0 0 7 0 0 0 151 0 0 1024 0 Legacy Rate Statistics: (Mbps : Rx, Tx, Tx-Retries) 0, 11 Mbps : 2, 0 6 Mbps : 0 0, 9. 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 : 0 4, 4, 0, 0, 7/2/20 : 0, 0, 0 5, 5, webauth done: false

지속적으로 클라이언트 데이터 속도 및/또는 RSSI 값을 추적하기 위해 "debug dot11 client rate address <mac>"을 실행할 수 있으며 이 정보는 매초마다 기록됩니다.

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-R [\*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

이 출력에서 Tx 및 Rx 패킷 카운터는 마지막으로 인쇄된 이후 두 번째 간격으로 전송된 패킷이며 Tx 재시도에 대해서도 동일합니다. 그러나 RSSI, SNR 및 데이터 속도는 해당 간격의 마지막 패킷 의 값이며 해당 간격의 모든 패킷에 대한 평균이 아닙니다.

Flexconnect 시나리오

사전 인증(예: CWA) 또는 사후 인증 시나리오에서 클라이언트에 현재 어떤 ACL이 적용되었는지 확 인할 수 있습니다.

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 파일 시스템

COS AP는 파일 시스템의 모든 내용을 unix 플랫폼에서처럼 나열하는 것을 허용하지 않습니다.

"show filesystems" 명령은 현재 파티션의 공간 사용량 및 배포에 대한 세부 정보를 제공합니다.

2802#show filesystems						
Filesystem	Size	Used	Available	Use%	Mounted o	n
/dev/ubivol/storage	57.5M	364.OK	54.1M	1%	/storage	
2802#						

"show flash" 명령은 AP 플래시의 기본 파일을 나열합니다. 특정 폴더를 나열하려면 syslog 또는 core 키워드를 추가할 수도 있습니다.

ap_2802#show	flash						
Directory of	/storage/						
total 84							
-rw-rr	1 root	root	0	May	21	2018	1111
-rw-rr	1 root	root	6	Apr	15	11:09	BOOT_COUNT
-rw-rr	1 root	root	6	Apr	15	11:09	BOOT_COUNT.reserve
-rw-rr	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-rr	1 root	root	6383	Apr	26	09:32	base_capwap_cfg_info
-rw-rr	1 root	root	20	Apr	26	10:31	bigacl
-rw-rr	1 root	root	1230	Mar	27	13:53	bootloader.log
-rw-rr	1 root	root	5	Apr	26	09:29	bootloader_verify.shadow
-rw-rr	1 root	root	18	Jun	30	2017	config
-rw-rr	1 root	root	8116	Apr	26	09:32	config.flex
-rw-rr	1 root	root	21	Apr	26	09:32	config.flex.mgroup
-rw-rr	1 root	root	0	Apr	15	11:09	config.local
-rw-rr	1 root	root	0	Jul	26	2018	config.mesh.dhcp
-rw-rr	1 root	root	180	Apr	15	11:10	config.mobexp
-rw-rr	1 root	root	0	Jun	5	2018	config.oeap
-rw-rr	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-rr	1 root	root	222	Jan	2	2000	last_good_uplink_config
drwxr-xr-x	2 root	root	160	Jun	30	2017	lists
-rw-rr	1 root	root	215	Apr	16	11:01	part1_info.ver
-rw-rr	1 root	root	215	Apr	26	09:29	part2_info.ver
-rw-rr	1 root	root	4096	Apr	26	09:36	random_seed
-rw-rr	1 root	root	3	Jun	30	2017	rxtx_mode
-rw-rr	1 root	root	64	Apr	15	11:11	sensord_CSPRNG0
-rw-rr	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 flash		Size 57.5M	Used Av 372.0K	ailak 54.	ole .1M	Use% N 1% ,	Aounted on /storage

syslog 저장 및 전송

syslog 폴더는 이전 재부팅 시 syslog 출력을 저장합니다. "show log" 명령은 마지막 재부팅 이후의 syslog만 표시합니다.

각 재부팅 주기에서 syslog는 증분 파일에 기록됩니다.

artaki# show	flash syslo	gs				
Directory of	/storage/sy	slogs/				
total 128						
-rw-rr	1 root	root	11963	Jul 6	15:23	1
-rw-rr	1 root	root	20406	Jan 1	2000	1.0
-rw-rr	1 root	root	313	Jul 6	15:23	1.last_write
-rw-rr	1 root	root	20364	Jan 1	2000	1.start
-rw-rr	1 root	root	33	Jul 6	15:23	1.watchdog_status
-rw-rr	1 root	root	19788	Jul 6	16:46	2
-rw-rr	1 root	root	20481	Jul 6	15:23	2.0
-rw-rr	1 root	root	313	Jul 6	16:46	2.last_write
-rw-rr	1 root	root	20422	Jul 6	15:23	2.start
Filesystem		Size	Used Av	ailable	Use% I	Mounted on
flash		57.6M	88.OK	54.5M	0%,	/storage
artaki# show Directory of total O	flash cores /storage/co	res/				
 Filesystem flash		Size 57.6M	Used Av 88.0K	ailable 54.5M	Use%   0% ,	Mounted on /storage

초기 부팅 후 첫 번째 출력은 파일 1.0이며 1.0이 너무 길어지면 파일 1.1이 생성됩니다. 재부팅 후 새 파일 2.0이 생성되는 등의 작업을 수행합니다.

AP가 특정 서버에 유니캐스트로 syslog 메시지를 전송하도록 하려면 WLC에서 Syslog 대상을 구성 할 수 있습니다.

기본적으로 AP는 syslog를 브로드캐스트 주소로 전송하므로 브로드캐스트 스톰이 발생할 수 있으 므로 syslog 서버를 구성해야 합니다.

AP는 기본적으로 콘솔 출력에 인쇄되는 모든 것을 syslog를 통해 전송합니다.

9800 컨트롤러의 Management(관리) 아래에 있는 Configuration(컨피그레이션) -> AP Join profile(AP 조인 프로파일)에서 이러한 매개변수를 변경할 수 있습니다.

Edit AP Jo	oin Profile									
General	Client	CAPWAP	AP	Manageme	ent Sec	curity	ICap	QoS		
Device	User	Credentials	CDP Ir	nterface						
TFTP D	owngrade					Telnet	/SSH Con	figuratio	n	
IPv4/IPv	6 Address	(	0.0.0.0			Telnet				
Image Fi	le Name	E	Enter File N	lame		SSH			<ul> <li></li> </ul>	
System	Log					AP Co	re Dump			
Facility V	/alue	К	ERN	•		Enable (	Core Dump	1		
Host IPv	4/IPv6 Addr	ess 1	92.168.1.	12						
Log Trap	Value	In	formation	•						
Secured	i									

Log Trap Value(로그 트랩 값)를 변경하여 syslog를 통해 디버그도 전송할 수 있습니다. 그런 다음 AP CLI에서 디버그를 활성화할 수 있으며 이 디버그의 출력은 syslog 메시지를 통해 구성된 서버로 전송됩니다.

Cisco 버그 ID CSCvu로 <u>인해75017</u>



는 syslog 기능을 KERN(기본값)으로 설정한 경우에만 AP가 syslog 메시지를 전송합니다.

AP의 네트워크 연결이 끊어질 수 있는 문제(예: WGB에서)를 해결하는 경우, AP의 업링크 연결이 끊기면 syslog는 메시지가 전송되지 않는 것만큼 안정적이지 않습니다.

따라서 플래시에 저장된 syslog 파일에 의존하는 것이 AP 자체에 출력을 디버깅하고 저장한 다음 나중에 주기적으로 업로드하는 훌륭한 방법입니다.

AP 지원 번들

액세스 포인트에서 업로드할 수 있는 단일 번들에서 다양한 유형의 자주 수집된 진단 정보를 사용 할 수 있습니다. 번들에 포함할 수 있는 진단 정보는 다음과 같습니다.

- AP 쇼 테크
- AP syslogs
- AP Capwapd 브레인 로그
- AP 시작 및 메시지 로그
- AP 코어덤프 파일

AP 지원 번들을 가져오려면 AP CLI로 이동하여 "copy support-bundle tftp: x.x.x.x" 명령을 입력합니 다.

그 후에는 다음 그림과 같이 support.apversion.date.time.tgz가 추가된 AP 이름으로 명명된 파일을 확인할 수 있습니다.

APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100 <cr></cr>
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
Creating support bundle, please waitifconfig: 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#

### 파일을 "untar"할 때 수집되는 다양한 파일을 볼 수 있습니다.

i-Images > APC4F7.D54C.E77C\_support.17.2.1.11.20200408.145526

Name A	Date modified	Туре	Size
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.brain.error.log.gz	4/8/2020 4:55 PM	GZ File	1 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.brain.log.gz	4/8/2020 4:55 PM	GZ File	3 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.info	4/8/2020 4:55 PM	INFO File	1 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.messages.gz	4/8/2020 4:55 PM	GZ File	11 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.startlog.gz	4/8/2020 4:55 PM	GZ File	5 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.syslogs.gz	4/8/2020 4:55 PM	GZ File	2 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tech_support.gz	4/8/2020 4:55 PM	GZ File	34 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.wsa_info.json.gz	4/8/2020 4:55 PM	GZ File	1 KB
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.wsa_status.json.gz	4/8/2020 4:55 PM	GZ File	1 KB

### 원격으로 AP 코어 파일 수집

AP 코어 파일을 원격으로 수집하려면 코어 덤프가 지원 번들에 포함되도록 설정한 다음 AP에서 지 원 번들을 업로드하거나 tftp 서버로 직접 전송하십시오. 후속 예에서는 tftp 서버 192.168.1.100을 사용합니다.

AireOS CLI

(c3504-01) >	config ap core-dump enable 192.168.1.100 apCores uncompress ?
<cisco ap=""></cisco>	Enter the name of the Cisco AP.
all	Applies the configuration to all connected APs.

### AireOS GUI

cisco	MONITOR WLANS CONTROLLER WIRELESS SE	CURITY MANAGEMENT COMMANDS HE	LP <u>F</u> EEDBACK		User:admin(ReadWrite) 📫 Home
Wireless	All APs > Details for AP70DB.98E1.3DEC				< Back Apply
* Access Points All APs	General Credentials Interfaces High /	Availability Inventory Advanced	Intelligent Capture		
<ul> <li>Radios</li> <li>802.11a/n/ac/ax</li> </ul>	Regulatory Domains	802.11bg:-E 802.11a:-I	Power Over Ethernet Settings		
802.11b/g/n/ax	Country Code	IL (Israel)	PoE Status	Full Power	
Dual-SG Radios	Cisco Discovery Protocol	*	Pre-standard 802.3af switches	8	
Global Configuration	AP Group Name	default-group *	Power Injector State	8	
Advanced	Statistics Timer	180	AP Core Dump		
Mesh	Data Encryption		AP Core Dump	Enabled	
AP Group NTP	2 valuet	Glabal Config *	TFTP Server IP 192.168.1	1.100	
▶ ATF	- remer	Cickel Coole * 1	File Name apCores		
RF Profiles	· Soft	Global Config *	File Compression 🕅 Enable		
FlexConnect Groups	TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331)	1250	AP Netransmit Config Parameters		
FlexConnect ACLs		TCP MSS is Globally Enabled	AP Retransmit Count	s 🗆	
FlexConnect VLAN Templates	LED State	Enable *	AP Retransmit Interval	3	
Network Lists	LED Brightlevel	8 (1-8)	VLAN Tagging		
▶ 802.11a/n/ac/ax	LED Flash State	0 (1-3600)seconds	VLAN Tagging	Enabled	
802.11b/g/n/ax		O Indefinite	NTP Server Status		
Media Stream		* Disable	Status Disabled		
Application Visibility	USB Module ID	USB Module	mDNS Configuration		
And Control	Override		mDNS Snooping	Enabled	
Lync Server	USB Module Status	×.	VLAN LIST		
Country	USB Module Operational State	Not Detected	Trustfor		
Timers	Hyperlocation Configuration		TUSION		
Netflow	2 Enable Hyperiocation	Global Config *	Inustaec config		
▶ QoS	Hyperlocation BLE Module	Present	CPIA Services		-3
			Services Sub-Services CMX Serv	er Ip	

### 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

Cisco IOS® GUI

O. Count Many Items	Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile			
Dashboard	+ Add × Delete	General Client CAPW	AP Management	Security ICap QoS	
Monitoring >	AP Join Profile Name	TETP Downgrade		Telnet/SSH Configuration	n
Configuration >	TiagoOffice testprofile	IPv4/IPv6 Address	0.0.0.0	Teinet	
Administration >	default-ap-profile	Image File Name	Enter File Name	SSH	
Licensing	IN A 1 P P 30 ·	System Log		AP Core Dump	
Troubleshooting		Facility Value	KERN	Enable Core Dump	
		Host IPv4/IPv6 Address	255.255.255.255	TFTP Server* (IPv4/IPv6)	192.168.1.100
		Log Trap Value	Information +	File Name*	default
		Secured (i)		Enable File Compression	

Cisco IOS® XE 17.3.1에서와 마찬가지로 Support Bundle(지원 번들) 탭이 있으며 WLC GUI에서 AP SB를 다운로드할 수 있습니다.

WLC가 SCP 서버가 될 수 있으므로 AP에서 "copy support-bundle" 명령을 실행하여 SCP를 통해 WLC에 전송하는 것이 전부입니다.

그런 다음 브라우저에서 다운로드할 수 있습니다.

VP780C- AIR-		1	Edit AP								
085-49E6 AP2802I- 2 A-K9	0	81.244.9.50	502f.a83	General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle	
<ul> <li>1 ⊨ 10 v iter</li> </ul>	ns per page			Destination		This Device     External Sen	This Device External Server		Last Export Status		
5 GHz Radios		Server IP* Destination File Path* 0		172.31.46.79 /		State Transfer Mode					
2.4 GHz Radios Dual-Band Radios						Server IP					
			Username Password	3* *		File Path Time of Export					
Country				Start Tra	nsfer						
LSC Provision											

즉, 17.3.1 이전의 eWLC 릴리스에서 동일한 트릭을 수동으로 수행할 수 있습니다.

AP에 연결할 수 있는 TFTP 서버가 없는 경우 SCP를 통해 AP에서 eWLC IP로 지원 번들을 복사합 니다.

eWLC는 일반적으로 AP에서 SSH를 통해 연결할 수 있으므로 17.3 이전의 경우 좋은 방법입니다.

1단계. <u>9800 v17.2.1에서 SSH 활성화</u>

2단계. <u>Cisco IOS® XE v17.2.1에서 SCP 활성화</u>

이 예에서는 SCP의 서버측 기능을 구성하는 방법을 보여줍니다. 이 예에서는 로컬로 정의된 사용 자 이름 및 비밀번호를 사용합니다. ! 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

3단계. "copy support-bundle" 명령을 사용하고 SCP 서버에서 생성할 파일 이름을 지정해야 합니다

팁: 명령을 한 번 실행하여 의미 있는 파일 이름을 가져온 다음 해당 파일 이름을 명령에 복사/붙여 넣을 수 있습니다.



4단계. 그런 다음 eWLC GUI로 이동하여 아래의 파일을 가져올 수 있습니다. Administration > Management > File Manager:



### IoT 및 Bluetooth

gRPC 서버 로그는 AP에서 다음을 사용하여 확인할 수 있습니다.

```
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] launching token request cycle"

time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces token expiration time 2020-04-02 01:36:52 +00

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] Receive Success status"

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 second

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 "
```

#### DNA Spaces 커넥터에 대한 연결은 다음으로 확인할 수 있습니다.

```
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
```

AP# show cloud connector c	onn	ection detail
Connection State	: 1	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 pkt	s	: 5
Number of Tx APP data pkts		: 2776829

### AP의 현재 BLE 브로드캐스트 컨피그레이션을 보려면

AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config		
Active profile Profile 0 (iBeacon)	:	v-iBeacon
UUID	:	000010000000000000000000000000000000000
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)	:	7f000001f00
Profile 2 (Eddystone URL)	)	
URL	:	http://www.

스캔한 결과를 보려면

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

앱이 구축된 Advanced BLE 게이트웨이 모드에서 AP가 작동하는 경우, 다음을 사용하여 IoX 애플 리케이션의 상태를 확인할 수 있습니다.

AP#show iox applications Total Number of Apps : 1		
App Name	:	cisco_dnas_ble_iox_app
Арр Ір	:	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

다음 명령을 사용하여 IOX 애플리케이션에 연결한 다음 현장 비컨 컨피그레이션 중에 로그를 모니 터링할 수 있습니다.

```
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]: 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

## 결론

COS AP와 관련된 문제를 해결하는 데 도움이 되는 다양한 트러블슈팅 툴이 있습니다.

이 문서는 가장 일반적으로 사용되는 문서를 나열하며 정기적으로 업데이트됩니다.

이 번역에 관하여

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