# 排除COS AP故障

## 目录

<u>简介</u>

<u>先决条件</u>

<u>要求</u>

<u>使用的组件</u>

<u>捕获数据包跟踪(嗅探器跟踪)</u>

AP端口上的有线PCAP

<u>步骤</u>

<u>命令选项</u>

<u>使用过滤器实现有线PCAP</u>

<u>无线电捕获</u>

<u>步骤</u>

<u>验证</u>

<u>其他选项</u>

<u>从9800 WLC控制AP客户端跟踪</u>

<u>嗅探器模式下的AP Catalyst 91xx</u>

<u>故障排除提示</u>

<u>路径MTU</u>

<u>要在引导时启用调试,请执行以下操作:</u>

<u>省电机制</u>

<u>客户端Qos</u>

<u>信道外扫描</u>

<u>客户端连接</u>

<u>Flexconnect方案</u>

<u>AP文件系统</u>

<u>存储和发送系统日志</u>

<u>AP支持套件</u>

<u>远程收集AP核心文件</u>

AireOS CLI AireOS GUI Cisco IOS® CLI Cisco IOS® GUI

<u>物联网和蓝牙</u>

<u>结论</u>

# 简介

本文档介绍一些适用于Cheatah OS AP(也称为COS AP)的故障排除工具。

# 先决条件

#### 要求

本文档没有任何特定的要求。

使用的组件

本文档重点介绍COS AP,如2800、3800、1560和4800系列的AP型号,以及新的11ax AP Catalyst 91xx。

本文档重点介绍AireOS 8.8及更高版本中的许多功能。以及Cisco IOS® XE 16.2.2s及更高版本。

在之前的版本中,可能会出现有关某些功能可用性的注释。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 捕获数据包跟踪(嗅探器跟踪)

#### AP端口上的有线PCAP

在AP以太网端口上执行pcap是可能的(从8.7开始,8.8中提供了过滤器)。您可以在CLI上显示实 时结果(仅包含汇总的数据包详细信息),也可以将其保存为AP闪存中的完整pcap。

有线pcap捕获以太网端(包括Rx/Tx)上的所有内容,并且AP内的分路点紧接数据包连线之前。

但是,它仅捕获AP CPU平面流量,这意味着流入和流出AP的流量(AP DHCP、AP capwap控制隧 道……),并且不显示客户端流量。

请注意,大小非常有限(最大大小限制为5MB),因此可能需要配置过滤器以仅捕获您感兴趣的流 量。

在您尝试复制流量捕获之前,请确保使用"no debug traffic wired ip capture"或只使用"undebug all"来停止流量捕获(否则,复制不会随着数据包的写入而结束)。

#### 步骤

步骤1:启动pcap;使用"debug traffic wired ip capture"选择流量类型:

#### <#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)

第二步:等待流量流动,然后使用命令"no debug traffic wired ip capture"或简单的"undebug all"停 止捕获:

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

第三步:将文件复制到tftp/scp服务器:

<#root>

AP70DB.98E1.3DEC#copy pcap

AP70DB.98E1.3DEC\_capture.pcap0

第四步:现在您可以在wireshark中打开该文件。 文件为pcap0。更改为pcap,使其自动与 wireshark关联。

命令选项

debug traffic wired命令有几个选项可以帮助您捕获特定流量:

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

您可以在debug命令末尾添加"verbose"以查看数据包的十六进制转储。请注意,如果您的过滤条件 不够严格,这会很快淹没CLI会话。

使用过滤器实现有线PCAP

过滤器格式与tcpdump捕获过滤器格式相对应。

	过滤器示例	描述
主机	"主机192.168.2.5"	这将过滤数据包捕获,只收集进入或来自主机

		192.168.2.5的数据包。
	"源主机192.168.2.5"	这将过滤数据包捕获,仅收集来自192.168.2.5的数据包 。
	"dst host 192.168.2.5"	这将过滤数据包捕获,只收集到达192.168.2.5的数据包 。
端口	"端口 443"	这将过滤数据包捕获,仅收集源或目标端口为443的数据 包。
	"源端口1055"	捕获来自端口1055的流量。
	"目标端口443"	这可以捕获发往端口443的流量。

以下是一个示例,输出显示在控制台上,但也经过过滤以仅查看CAPWAP数据包:

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#

文件输出示例:

要在wireshark上打开捕获,请执行以下操作:

APC4F7.D54C.E77C_capture.pcap0			- 🗆 ×
File Edit View Go Capture Analyze	Statistics Telephony Wireless Tools	s Help	
	+ 🕾 Ŧ 🛦 🚍 🔳 Q Q Q 🔢		
Apply a display filter <ctrl-></ctrl->			Expression +
No. Delta Source	Destination	Lengt Info	Payload Type Differ
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 8.601152 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>Frame 1: 651 bytes on wire (\$208</li> <li>Ethernet II, Src: Cisco_4c:e7:7c</li> <li>Internet Protocol Version 4, Src.</li> <li>User Datagram Protocol, Src Port</li> <li>Control And Provisioning of Wirei</li> <li>Datagram Transport Layer Security</li> </ul>	bits), 651 bytes captured (5208 t (c4:f7:d5:4c:e7:7c), Dst: Cisco_1 : 192.168.1.82, Dst: 192.168.1.15 : 5264, Dst Port: 5246 less Access Points - Control y	bits) L::d2:ff (00:le:bd:lc:d2:ff)	

## 无线电捕获

可以在无线电的控制平面上捕获数据包。由于性能影响,无法捕获无线电数据平面上的数据。

这意味着客户端关联流(探测、身份验证、关联、eap、arp、dhcp数据包以及ipv6控制数据包、 icmp和ndp)可见,但客户端在移动到连接状态后传递的数据不可见。

#### 步骤

步骤1:添加跟踪的客户端mac地址。可以添加多个mac地址。也可以对所有客户端运行该命令,但不建议这样做。

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.

第二步:将过滤器设置为仅记录特定协议或所有支持的协议:

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

第三步:选择在控制台上显示输出(异步):

configure ap client-trace output console-log enable

第四步:开始跟踪。

config ap client-trace start

示例:

<#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 0 1 1 testewlcwlan -41 MCS92SS No APOCD0.F894.46E4#config ap client-trace address add A8:DB:03:08:4C:4A APOCD0.F894.46E4#config ap client-trace filter a]] Trace ALL filters Trace arp Packets arp assoc Trace assoc Packets auth Trace auth Packets Trace dhcp Packets dhcp Trace eap Packets eap Trace icmp Packets icmp 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

要停止捕获,请执行以下操作:

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

验证

验证客户端跟踪:

<#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 Add	dress : 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	: icmp∨6
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

# 成功的客户端连接示例:

		_
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5351] [1586169921:535099] [APOCD0.F894.4624]	[a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11 AUTHENTICATION : (.)</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5352] [1586169921:535224] [APOCD0.F894.46E4]	[a8:db:03:08:4c:4a] <aprovl> [U:W] DOT11 AUTHENTICATION : (.)</aprovl>
Apr	6 10:45:21 kernel: [+04/06/2020 10:45:21.53611 [1586169921:536158] [APOCD0.F894.46E4]	[a8:db:03:08:4c:4a] <aprovo> [D:W] DOT11 AUTHENTICATION : (.)</aprovo>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5416] [1586169921:541598] [APOCD0.F894.46E4]	[a8:db:03:08:4c:4a] <aprov0> (U:W] DOT11 ASSOC REQUEST : (.)</aprov0>
anr	6 10:45:21 kernel: [*04/06/2020 10:45:21.54411 [1586169921:544114] [APOCD0.F894.46F4]	LaStdb:03:08:4c:4al capr0v0> [D:W] DOT11 ASSOC RESPONSE : (.)
2 mm	6 10.45.21 karnal. (#04/06/2020 10.45.21 55011 [150616021.550152] [ADDORD #064 4684]	(acid):02:00:do:da:da: capyord) [D:1] FIRT FY M1 : DarTime 0x02 Fautric 0x000h
Sox	6 10:45:21 kervel: (-04/06/2020 10:45:21 57301] [156:16021.57302] [ADD/TO P04 4024]	[abidbi03:00.40:40; abidbi03:00.000] [Dis] ERON FEY M2 : Descrype 0x02 ReyInfo 0x010b
2 mar	C 10.45.91 bergal (404/06/2000 10.45.91 5704) [15061600364.07030] [EPOCPO P004 4024]	[a0.db.02.00.dc.da] dapAnob [D.0] ELCON DECEMBER & DECEMBER OND RELEASE
Apr	6 10:45:21 KEEREL: [-04/06/2020 10:45:21:504] [1506169921:50476] [AF0CD0:F094.4024]	[acidbiositerterta] (approvos [Din] ExPos AEI.MS : Descripe 0x02 Revinto 0x13CD
MDT	6 10.45.21 KEINEI: [-04/06/2020 10.45.21 2005] [1506165521355552] [APOCDO.F0514624]	[acidbio3:00:40:40] (approved [ora] back arises : (a)
Apr	6 10145121 Kernel: [-04/06/2020 10145121.6003] [1561694211600341] [APOCDO.F694.4624]	[asidbiosiderecta] captoros [one] borni acrion : (.)
Apr	6 10:45:21 Kernel: [-04/06/2020 10:45:21.6020] [136616952160261/] [APOCDO.F054.4624]	[asidbio3:06:46:44] C FUVOS [DIN] DOTI ACTION : (.)
apr	6 10:45:21 Kernel: ["04/06/2020 10:45:21.64/5] [1566169921:64/516] [APOCDO.F094.46E4]	[asidbiosids:4c:4c aprovos [usin] borni Action : (.)
wbr	0 10:45:21 KELHET: [-04/00/2020 10:45:21.04/5] [1500103421:04/544] [MP0CD0.F034.4024]	[astabiosiositat caprovos [Diw] Dorit_Action : (.)
7.50	· · · · · · · · · · · · · · · · · · ·	
apr	6 10:45:21 Kernel: ["04/06/2020 10:45:21.8636] [1586169921:863610] [APUCDO.F894.8624]	[asidbid] [asidbid] [u:w] DHCP DISCOVER : Transid Oxasscolad
apr	6 ID145121 Kernel: [404/06/2020 ID145121.8636] [15861699211865644] [APOCDD.F894.4624]	[asid Heita] (aprovos [oic] DHCF DISCOVER I Transid Oxaseculae
Apr	6 10:45:21 kernel: [=04/06/2020 10:45:21.8637] [1586169921:863700] [APOCD0.F894.46E4]	[a citatia] <apr0v0> [UiC] DHCP DISCOVER : Transid 0xa38c0146</apr0v0>
Apr	6 10:45:21 kernel: [=04/06/2020 10:45:21.863/] [1586169921:863/31] [AP0CD0.F894.46E4	vosiecitaj (aprovos [U:C] DHCP DISCOVER : Transid Uxasscolde
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863741] [APOCD0.F894.4	3:08:4c:4a] <nsscapwap0> [U:E] DHCP_DISCOVER : TransId 0xa36c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [=04/06/2020 10:45:21.8637] [1586169921:863762] [APOCDO.F89	0:03:08:4c:4a] <nsscapwap0> [U:E] DHCP_DISCOVER : Transid Uxa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8676] [1586169921:867627] [APOCDO	db:03:08:4c:4a] <nsscapwap0> [D:E] DHCP_OPPER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8676] [1586169921:867664] [APOC	B:db:03:08:4c:4a] <nsscapwap0> [D:C] DHCP_OFFER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8677] [1586169921:867709] [2	[a8:db:03:08:4c:4a] <nsscapwap0> [D:C] DHCP_OFFER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8677] [1586169921:867740	[a8:db:03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8684] [1586169921:8684] [24]	[a8:db:03:08:4c:4a] <nsscapwap0> [D:E] DHCP_OFFER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:4 4624]	<pre>[a8:db:03:08:4c:4a] <nsscapwap0> [D:C] DHCP_OFFER : TransId 0xa38c01d6</nsscapwap0></pre>
Apr	6 10:45	db:03:08:4c:4a] <nsscapwap0> [D:C] DHCP_OFFER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:0	[03:08:4c:4a] <apr0v0> [D:W] DHCP_OFFER : TransId 0xa38c01d6</apr0v0>
Apr	<sup>6 10</sup> U - Uplink packet (from client)	03:08:4c:4a) <apr0v0> [U:W] DHCP_REQUEST : TransId 0xa38c01d6</apr0v0>
Apr	6 10	D3:08:4c:4a] <apr0v0> [U:C] DHCP_REQUEST : TransId 0xa38c01d6</apr0v0>
Apr	<sup>10</sup> D - Downlink packet (to client)	D3:08:4c:4a] <apr0v0> [U:C] DHCP_REQUEST : TransId 0xa38c01d6</apr0v0>
Apr	6 10 D DOWNLINK PROMOL (CO STICHC)	D3:08:4c:4a] <apr0v0> [U:C] DHCP_REQUEST : TransId 0xa38c01d6</apr0v0>
Apr		<pre>D3:08:4c:4a] <nsscapwap0> [U:E] DHCP_REQUEST : TransId 0xa38c01d6</nsscapwap0></pre>
Apr	<sup>6 10</sup> W - module <b>Wireless</b> driver	D3:08:4c:4a] <nsscapwap0> [U:E] DHCP_REQUEST : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10	D3:08:4c:4a] <nsscapwap0> [D:E] DHCP_ACK : TransId 0xa38c01d6</nsscapwap0>
Apr	<sup>610</sup> E - module <b>Ethernet</b> driver	D3:08:4c:4a] <nsscapwap0> [D:C] DHCP_ACK : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10 E MOUTE ECHCENCE CHIVEE	D3:08:4c:4a] <nsscapwap0> [D:C] DHCP_ACK : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10	D3:08:4c:4a] <apr0v0> [D:W] DHCP_ACK : TransId 0xa38c01d6</apr0v0>
Apr	6 10 C - MODULE CLICK	D3:08:4c:4a] <nsscapwap0> [D:E] DHCP_ACK : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10	D3:08:4c:4a] <nsscapwap0> [D:C] DHCP_ACK : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10	D3:08:4c:4a] <nsscapwap0> [D:C] DHCP_ACK : TransId 0xa38c0ld6</nsscapwap0>
Apr	6 10	D3:D8:4c:4a] <apr0v0> [D:W] DHCP_ACK : TransId 0xa38c01d6</apr0v0>
Apr	6 10:	03:08:4c:4a] <apr0v0> [U:W] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</apr0v0>
Apr	6 10:45.	db:03:08:4c:4a] <apr0v0> [U:C] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</apr0v0>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1611] [1586169922:161177] [APOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <apr0v0> [U:C] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</apr0v0>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1612] [1586169922:161213] [AF0CD0.F894.46E4]	[a8:db:03:08:4c:4a] <nsscapwap0> [U:E] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</nsscapwap0>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1646] [1586169922:164673] [AFOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <nsscapwap0> [D:E] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:42</nsscapwap0>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164699] [AF0CD0.F894.46E4]	[a8:db:03:08:4c:4a] <nsscapwap0> [D:C] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:42</nsscapwap0>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164722] [APOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <nsscapwap0> [D:C] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:42</nsscapwap0>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164751] [APOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <apr0v0> [D:W] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:42</apr0v0>

方括号中的字母可帮助您了解帧出现在何处(E表示以太网,W表示无线,C表示在AP内部的 Click模块),以及在哪个方向(上传或下载)。

下面是一张小表,上面列出了这些字母的含义:

U — 上行链路数据包(来自客户端) D — 下行链路数据包(单击) W — 模块无线驱动程序 E — 模块以太网驱动程序 C — 模块点击

其他选项

异步查看日志:

然后,可以使用命令"show ap client-trace events mac xx:xx:xx:xx:xx:xx:xx:xx"(或将mac替换为 "all")来查阅日志

#### <#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></apr1v1>	[U:W]	DOT11_AUTHENTICATIO
[*04/06/2020	10:11:54.288144]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	DOT11_AUTHENTICATIO
[*04/06/2020	10:11:54.289870]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[U:W]	DOT11_ASSOC_REQUEST
[*04/06/2020	10:11:54.317341]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	DOT11_ASSOC_RESPONS
[*04/06/2020	10:11:54.341370]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></apr1v0>	[D:W]	EAPOL_KEY.M1 : Desc
[*04/06/2020	10:11:54.374500]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr1v0></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]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v1></apr0v1>	[U:W]	DOT11_PROBE_REQUEST

## 以十六进制格式转储数据包

您可以在CLI中转储十六进制格式的数据包:

#### 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.9011 BDECtconfigure ap client-trace start
Warning: To recover NLC pushed config, need CANWAP restart or reload to re-apply the config from MLC
AP7058.9811.3DEC#Apr 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-trace output dump address add a8:d0:03:00:4c:4a
AP70DB.90EL.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 Zemote/Local dump Client Addresses
enaole shabi e itake output for local dump anable 19700 (1990) and anable itake output for local dump anable 1970/08 (1990) (199
<pre>c4=500. Enter the name that where the same time to be a same to b</pre>
AP70DB.9871.3DEC#configure ap client=trace output dump enable 100
<61>
AP70D8.90E1.3DEC#configure ap client-trace output dump enable 100
AP70DB.50E1.3DEC#Apr 6 13:29:27 kernel: (*04/06/2020 13:29:27.4648)
Apr 6 13:25:27 kernel: [*04/06/2020 13:25:27.4640] Time:464076us Dir:Rx Rate:m7.2-2 Rssi:-43 Ch:1 Fo:100 Dur:30 00:27:e3:36:4d:a0 a0:db:03:00:4c:4a 54:70:65:b7:3f:42 Seq:126(254) Info:ARP Retry:0 Len:121 Typesub:20 Tid:q0
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4643] 0000 00 00 00 00 00 00 00 00 00 00 00
Apr 6 13/29/27 Refnet: [ 04/04/2020 13/29/27 4449] 0010 00 00 00 00 11 00 00 00 00 00 00 0
Asy 6 12:05:27 kernel: (*04/06/2020 13:25:27 4445) 0040 00 01 20 00 00 45 31 21 0f 45 a0 00 00 00
Apr 6 13:29:27 Rernel: (*04/06/2020 13:29:27.4645) 0050 00 00 00 00 00 00 00 00 5e 00 00 5e 00 07 30
Apr 6 13:25:27 kernel: [*04/06/2020 13:25:27.4649] 0060 ed 08 01 30 00 00 27 e3 36 4d a0 a0 db 03 00 4c
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0070 4m 54 7c 69 b7 3f 42 60 12 00 00 mm am 03 00 00
Apr 4 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 a0 65
Apr 6 [3:29:27 kernel: [*04/06/2020 ]3:29:27.4746]
Apr 6 13/12/127 Rennel: (04/04/2020 13/12/12/4740) Time/440000 Dirit Rest: 755 Unit Fride Durits astab:03/00/40/140 04/7/03/15/12/142 Begte(6) Into APR Wetry: 0 Lenito Time/400 Dirits astab:03/00/40/140 05/17/03/15/12/142 Begte(6) Into APR Wetry: 0 Lenito Time/400 Dirits astab:03/00/40/140 05/17/03/15/12/142 Begte(6) Into APR Wetry: 0 Lenito Time/400 Dirits astab:03/00/40/140 05/17/03/15/12/142 Begte(6) Into APR Wetry: 0 Lenito Time/400 Dirits astab:03/00/40/140 05/17/03/15/142 Begte(6) Into APR Wetry: 0 Lenito Time/400 Dirits astab:03/00/40/140 05/17/03/15/142 Begte(6) Into APR Wetry: 0 Lenito Time/400 Dirits astab:03/00/40/140 Dirits astab:03/00/40/140/140/140/140/140/140/140/140/1
Apr 6 13129127 Refer. [04/04/2020 13129127.4749] 0000 00 00 00 00 00 00 00 00 00 00 00
Apr 6 13 13 13 12 Market 1 (104 (04 )20 13 13 13 13 13 13 13 13 13 13 13 17 17 10 00 00 10 10 00 00 00 00 00 00 00 00
Apr 6 13:35:27 kernel: (*04/06/2020 13:29:27.4745) 0030 00 00 5e 6b 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 ao 54 7c
Apr 6 13:29:27 kernel: (*04/06/2020 13:29:27.4749) 0050 69 b7 3f 42 40 00 00 0n an an 03 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 3£ 42 c0 a0
Apr 4 13:29:27 kernel: (*04/08/2020 13:29:27.4745) 0070 65 01 a0 db 03 00 4c 4a c0 a0 65 0d 00 00 00 00
Apr 6 13:29:27 %ernel: [04/06/2020 13:29:27.4745] 0080 00 00 00 00 00 00 00 00 00 00 00 0
Apr 4 13/27/27 Rethet: (104/04/2020 13/27/27.47.470) 00/00 40 40 40 40 40 40
Apr 6 13:11:03 Repress 1: 00/07/2000 13:01:00.0001 Time:180014us Dir:Br Bate:5 Basi:03 (c):1 Fr:40 Dur:0 ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0000 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1800] 0010 00 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1000] 0020 00 00 13 00 15 h3 ff ff 00 00 dc c0 00 ad 00 ad
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1000] 0030 00 00 5e 0b 2f 16 00 02 c2 75 0b 01 14 00 40 00.
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1900] 0040 00 00 ff ff ff ff ff ff a0 db 03 00 4e 4a ff ff
Apr 6 13:31:03 kernel: ['04/06/2020 13:31:03.1001] 0050 ff ff ff ff 70 17 00 00 01 04 02 04 05 16 32 00
Apr 6 13131/03 Netres: ['04/04/2020 13131/0318091] 0050 05 12 10 40 05 10 00 00 00 00 00 00 00 00
Apr 6 13:13:103 herman 1 (104/05/2020 13:13:103.1061) 000 00 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0090 40 00 21 ff
Apr 4 13:31:03 kernel: [*04/04/2020 13:31:03.2000]
Apr 6 13:31:03 kernel: (*04/06/2020 13:31:03.2000) Time:200019us Dir:Tm Rate:1 Rssi:=56 Ch:1 Fe:50 Dur:13a a0:db:03:08:4e:4a 00:27:e3:36:4d:a0 8eq:65e(1630) Info:DOT11_PROSE_RESPONSE Retry:0 Len:250 Typesub:05
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0000 00 00 00 00 00 00 00 00 00 00
Apr 6 13:31:03 kernel: (*04/06/2020 13:31:03.2000) 0010 00 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13/31/03 Xernel: ['04/04/2020 13/31/03.2000] 0020 00 00 13 00 15 B3 fF fF 00 00 e1 a1 00 e2 00 e2
Apr 6 13:51:03 kernel: [*04/06/2030 13:51:03.2001] 0060 11 11 00 0c 74 65 73 74 65 77 6c 61 77 6c 61 6e
Apr 6 13:31:03 kernel: 1*04/06/2020 13:31:03.20013 0070 01 08 82 84 85 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] 0050 6c 30 14 01
Apr 6 13:31:03 Wernel: [*04/06/2020 13:31:03.2001]
Apr = 1313103 Kernel: ["VV/VV/VVV 313103.2001] 11me:20016408 DETTR Resel: Rest;"55 Ch:1 F0:50 Dur:13a 80:db:03:00:40:40 00:27:e3:36:4d:a1 5eq:65f(1631) Info:DOT11_PROBE_RESPONSE Resty:0 Len:251 Typesub:05
when a value is a second a second second a second and an

## 然后,您可以清除十六进制转储并以txt格式保存并导入到wireshark中:

$\begin{array}{c} \texttt{Time:} 2001 \texttt{Ous} \ \texttt{Dir:} \texttt{Rx} \ \texttt{Rate:} \texttt{Rat:} \texttt{R37} \ \texttt{Chil} \ \texttt{Fc:b0} \ \texttt{Dur:} \texttt{I38} \\ \texttt{O000} \ \texttt{O} \ \texttt{O0} \$	00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:1(1) Info:DOT11_AUTHENTICATION Rebry:0 Len:65 Typesub:0b
$\begin{array}{c} {\tt Time:} + 305 {\tt dus} \ {\tt Dir:} {\tt Tx} \ {\tt Rate:} 1 \ {\tt Rst:} - 55 \ {\tt Ch:} 1 \ {\tt Fo:} {\tt d0} \ {\tt Dur:} 13a \\ 0000 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \$	a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66c(1644) Info:DOT11_ACTION Retry:0 Len:54 Typesub:0d
$ \begin{array}{c} \texttt{Time: 43155us \ Dir: Tx \ Rate: 1 \ Rssi: -95 \ Ch: 1 \ Fc: b0 \ Dur: 13a \\ \texttt{OOO} \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ $	a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66d(1645) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
$ \begin{array}{llllllllllllllllllllllllllllllllllll$	a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:2(2) Info:DOTI1_ASSOC_REQUEST Retry:1 Len:220 Typesub:00

Open	Ctrl+O	P & _	Q Q Q U	
Open Recent	,			Expression
Merge				
Close	Ctrl+W		Wireshark - Import From Hex Dump ? X	
Save	Ctrl+S	-		
Save As	Ctrl+Shift+S	Data\Local\Temp	Import From	
		234744 HelpDesk	File: C:/Users/tantunes/CISCO/11ax training/dump_example.txt Browse IBBF161F6_debugs.capture2.pcap (13	(MB)
File Set		O\00-SRs\SR 688.	Offsets:   Hexadecimal	(B)
Export Specified Packets.	•	O\00-SRs\SR 688	9956 Bytes)	
Export Packet Dissections		O\11ax training\1	○ Octal	
xport Packet Bytes	Ctrl+Shift+X	O\11ax training\1	O None	
export PDUs to File		O\11ax training\1	Timestamp format: (No format will be applied)	
Export TLS Session Keys		Data\Local\Temp	Direction indication:	
Export Objects	,	nloads\AP_trace_	Econolition	
Print	Ctrl+P	:0\IOS-Images\A	Exception	
Ouit	Ctrl+O	-	encapsulation i ype:   Emernet	
0	ipeure	_	No dummy neader     State of the state	
	sing this filter: 📕	Enter a capture filter .	All interfaces sho	wn 🕶
	10			International Contraction of Contrac
	Local Area Co	onnection* 10	O dup source port:	
	Ethernet yelle	owCable	O TOP Destination port:	
	Local Area Co	onnection* 3	O SCTP Tag:	-
	Local Area Co	onnection* 9	O SCTP (Data) PPI:	
	Wi-Fi		C ExportPDU Payload	
	ThinkpadEthe	ernetBlue		
	Local Area Co	onnection* 11	Marine Constants	

由于输出可能非常大,并且考虑到输出只提到看到的帧类型,而不提到任何内部细节,因此将数据 包捕获重定向到运行捕获应用程序(如wireshark)的笔记本电脑会更有效。

启用远程捕获功能,以通过wireshark将数据包发送到外部设备:

config ap client-trace output remote enable

此命令意味着AP将客户端跟踪过滤器捕获的每个帧转发到位于192.168.68.68的笔记本电脑,并在端口5000上使用PEEKREMOTE封装(与嗅探器模式中的AP一样)。

一个限制是,目标笔记本电脑必须与您运行此命令的AP位于同一子网中。您可以更改端口号以容纳 网络中的任何现有安全策略。

在运行Wireshark的笔记本电脑上收到所有数据包后,您可以右键点击udp 5000报头,然后选择 decode as并选择PEEKREMOTE,如下图所示:

udp.port == 5688			X	Expression
Delta Source	Destination	Lengti Info		Payload Type
59 0.000000 SamsungE_08:4c:4a 60 0.033416 Cisco_3c:4d:a0 61 0.038249 SamsungE_08:4c:4a 62 0.0000001 Cisco_3c:4d:a0 63 0.0000001 Cisco_3c:4d:a0 64 0.021832 Cisco_3c:4d:a0 65 0.000008 Cisco_3c:4d:a0 66 0.030097 SamsungE_08:4c:4a 67 0.018008 Cisco_3c:4d:a0 68 0.009881 SamsungE_08:4c:4a 70 0.030086 Cisco_3c:4d:a0 70 0.030086 Cisco_3c:4d:a0 70 0.030086 Cisco_3c:4d:a0 70 0.030086 Cisco_3c:4d:a0 70 0.020078 Cisco_36:4d:a0 70 0.020078 Cisco_36:4d:a0 70 0.020078 Cisco_36:4d:a0 70 0.020078 Cisco_36:4d:a0 70 0.020078 Cisco_36:4d:a0 70 0.020277 Cisco_36:4d:a0 70 0.020277 Cisco_36:4d:a0 70 0.020277 Cisco_36:4d:a0 70 0.020277 Cisco_36:4d:a0 70 0.020277 Cisco_36:4d:a0 70 0.020277 Cisco_36:4d:a0 70 0.020297 Cisco_36:4d:a0 70 0.02097 Cisco_36:4d:	Mark/Unmark Packet Ignore/Unignore Packet Set/Unset Time Reference Time Shift Packet Comment Edit Resolved Name Apply as Filter Prepare a Filter Conversation Filter Stopy Acket in New Window SamsungE_08:4c:4a Broadcast Stopy Jast Dytes Captured (2008 bi Stopy 192:165.1.189 Sologe, Dat Port: 5688	251 Probe Request, SH-577, FH-6, Flags 292 Probe Request, SH-577, FH-6, Flags 107 Authentication, SH-578, FN-6, Flags 107 Authentication, SH-578, FN-6, Flags 262 Association Reuponse, SH-572, FN-6, Flag 322 Association Response, SH-572, FN-6, Flag 324 Association Response, SH-572, FN-6, Flag 325 Association Response, SH-572, FN-6, Flag 326 Association Response, SH-572, FN-6, Flag 327 Association Response, SH-572, FN-6, Flag 328 Association Response, SH-572, FN-6, Flag 93 A 93 A 94 Association Response, SH-572, FN-6, Flag 94 Association Response, SH-572, FN-6, Flag 95 A 96 A 428 D 97 A 428 D 98 A 428 D 99 A 428 D 428	C, SSID-testewilkwian C, SSID-testewilkwian C SS=C SS=C SSEEMOTE EXREMOTE EXREMOTE UI UI (timestamp) UID (timestam	NSDU NSDU NSDU NSDU NSDU NSDU NSDU NSDU
AiroPeek/OmniPeek encapsulated IEEE 802.11 radio information IEEE 802.11 Probe Request, Flags: . IEEE 802.11 wireless LAN	E 802.11	+ - <b>b</b> B	C: Keens Instrumes KeenOrate Reparance With earbank ideocadeas. entriess OK Savve Cancel Help	

有关此功能的错误和增强功能的列表:



<u>Cisco Bug ID CSCvm09020</u> 客户端跟踪在8.8上不再显示DNS



## 客户端跟踪显示多个ICMP\_other,序列号为null



AP COS client-trace不捕获webauth数据包



## AP COS客户端跟踪远程输出不起作用



客户端跟踪SEQ号不一致

从9800 WLC控制AP客户端跟踪

您可以将多个AP配置为执行无线客户端跟踪并从

步骤1:配置定义要捕获的流量的AP跟踪配置文件

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

步骤2.将AP跟踪配置文件添加到目标的AP使用的AP加入配置文件。

ap profile < ap join profile name> trace

确保此AP加入配置文件应用于目标AP使用的站点标记

第4步触发启动/停止

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/

验证命令:

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

嗅探器模式下的AP Catalyst 91xx

新的Catalyst 9115、9117、9120和9130可在嗅探器模式下配置。此过程与之前的AP型号类似。





*ThinknadEthernetRlue
THINKDOUCHIEITIELDIUE

1	== 5000			
Del	ta Source	Destination	Lenati 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 0x01
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 Packet]	100
0	013829 SamsungE 08:4c:4a	Cisco 97:03:ef	199 Key (Message 4 of 4)	100
8	.000174 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
	<pre>fag: WHT Operation fag: Mobility Domain fag: Fast BSS Transition fag: RM Enabled Capabilities fag: BSS Max Idle Period fixt Tag: HE Capabilities (IEE</pre>	(5 octets) E Std 802.11ax/D3.0)		
> 1 > 1 > 1 > 1 > 1	<pre>fag: VMT Operation fag: Nobility Domain fag: Fast BSS Transition fag: RM Enabled Capabilities fag: BSS Max Idle Period fag: BSS Max Idle Period fag: BSS Max Idle Period Ext Tag: HE Capabilities (IEE Ext Tag Length: 46 Ext Tag Number: HE Capabil ) HE PhQ Capabilities Inform Supported HE-MCS and NSS S V Rx and Tx MCS Maps &lt;= 80 V Rx HCX-MCS Maps &lt;= 80 V Rx HCX-MCS Maps &lt;= 80</pre>	(5 octets) E Std 802.11ax/D3.0) ension (255) ities (IEEE Std 802.11ax/D3.0) ation: 0x800002100009 ation et 0 MHz: MHz: 0xaaaa	(35)	
	<pre>rag: VHT Operation rag: RADITY Domain rag: RADITY Domain rag: RA Enabled Capabilities rag: BSS Max Idle Period rag: RA Idle Period rag: RADITY RADITY rag: HE Phy Capabilities Inform Supported HE-MCS and NSS S</pre>	(S octets) E Std 802.11ax/D3.0) ension (255) ities (IEEE Std 802.11ax/D3.0) ation: 0x800002100009 ation et 0 MHz MHz: 0xaaaa N0 = Nax HE-MCS for 1 SS: Suppo = Max HE-MCS for 2 SS: Suppo = Max HE-MCS for 4 SS: Suppo = Max HE-MCS for 5 SS: Suppo = Max HE-MCS for 7 SS: Suppo = Max HE-MCS for 7 SS: Suppo = Max HE-MCS for 8 SS: Suppo	(35) rt for HE-MCS 0-11 (0x2) rt for HE-MCS 0-11 (0x2)	
	<pre>fag: VMT Operation fag: Robity Domain fag: Fast BSS Transition fag: RM Enabled Capabilities fag: BSS Max Tale Period fag: RM Enabled Capabilities fag: Number: Element ID Ext fag Number: Element ID Ext fag Number: HE Capabilities Inform HE Phy Capabilities Inform HE Phy Capabilities Inform M Supported HE-MCS and NSS S</pre>	(5 octets) E Std 802.11ax/D3.0) ension (255) ities (IEEE Std 802.11ax/D3.0) ation: 0x800002100009 ation et 0 MHz: NHz: 0xaaaa NH E-MCS for 1 SS: Suppo Max HE-MCS for 4 SS: Suppo Max HE-MCS for 4 SS: Suppo Max HE-MCS for 5 SS: Suppo Max HE-MCS for 6 SS: Suppo Max HE-MCS for 8 SS: Supp	(35) rt for HE-MCS 0-11 (0x2) rt for HE-MCS 0-11 (0x2)	
> 1 > 1 > 1 > 1	<pre>ag: VMT Operation fag: Robity Domain fag: Rast BSS Transition fag: Rast BSS Transition fag: RM Enabled Capabilities fag: BSS Max Tale Period Ext Tag: HE Capabilities (IEEE Tag Number: ELement ID Ext tag Length: 46 Ext Tag Lumber: HE Capabilities HE PAy Capabilities Inform HE Phy Capabilities Inform MS Supported HE-MCS and NSS S V Rx and TX MCS Maps &lt;= 80 V Rx HEX-MCS Map &lt;= 80 V RX HEX MAD &lt;</pre>	(5 octets) E Std 802.11ax/D3.0) ension (255) ities (IEEE Std 802.11ax/D3.0) ation: 0x800002100009 ation et 0 MMz MMz: 0xaaaa M0 = Nax HE-MCS for 1 SS: Suppo = Max HE-MCS for 2 SS: Suppo = Max HE-MCS for 3 SS: Suppo = Max HE-MCS for 6 SS: Suppo = Max HE-MCS for 6 SS: Suppo = Max HE-MCS for 6 SS: Suppo = Max HE-MCS for 8 SS: 8 SS SS SS SS SS SS SSS SS SS SS SS SS	(35) rt for HE-MCS 0-11 (0x2) rt for HE-MCS 0-11 (0x2) i)	
> 1 > 1 > 1 > 1	<pre>fag: VMT Operation fag: Robity Domain fag: Fast BSS Transition fag: RM Enabled Capabilities fag: BSS Max Idle Period fag: RM Enabled Capabilities (IEE fag Number: Element ID Ext fag Langth: 46 Ext Tag Langth: 46 Ext Tag Number: HE Capabil     HE Ph Capabilities Inform     Supported HE-MCS and NSS S     K and Tx MCS Maps &lt;= 80</pre>	(5 octets) E Std 802.11ax/D3.0) ension (255) ities (IEEE Std 802.11ax/D3.0) ation: 0x800002100009 ation et 0 MHz MHZ: 0xaaaa 80 = Max HE-MCS for 1 SS: Support Max HE-MCS for 2 SS: Support Max HE-MCS for 3 SS: Support Max HE-MCS for 4 SS: Support Max HE-MCS for 6 SS: Support Max HE-MCS for 6 SS: Support Max HE-MCS for 8 SS: Support MHZ: 0xaaaa td 802.11ax/D3.0) ension (255) on (IEEE Std 802.11ax/D3.0) (36 x003Ff4	(35) rt for HE-MCS 0-11 (0x2) rt for HE-MCS 0-11 (0x2)	

◆ 注:捕获以WIFI 6数据速率发送的数据帧,但是,由于peekremote在Wireshark上不是最新的,因此它们现在显示为802.11ax phy类型。修复在Wireshark 3.2.4中,Wireshark显示适当的Wifi6物理速率。

✤ 注意:Cisco AP此时无法捕获MU-OFDMA帧,但可以捕获通告MU-OFDMA窗口的触发帧 (以管理数据速率发送)。您已经可以推断MU-OFDMA发生(或没有)以及客户端与哪个发 生。

## 故障排除提示

路径MTU

虽然路径MTU发现可找到AP的最佳MTU,但可以手动覆盖此设置。

在AireOS 8.10.130 WLC上,命令config ap pmtu disable <ap/all>为一个或所有AP设置静态 MTU,而不是依赖动态发现机制。

要在引导时启用调试,请执行以下操作:

您可以在下次启动时运行config boot debug capwap以启用capwap、DTLS和DHCP调试,甚至在操 作系统已启动并显示提示符之前。

您还有"config boot debug memory xxxx"用于几个内存调试。

您可以通过"show boot"查看下次重新启动时是否启用了引导调试。

可以通过在末尾添加disable关键字(例如"config boot debug capwap disable")来禁用它们。

## 省电机制

可以通过运行以下命令排除给定客户端的节能故障

debug client trace <mac address>

客户端Qos

要验证是否已应用QoS标记,可以运行"debug capwap client qos"。

它显示无线客户端的数据包的UP值。



从8.8开始,它不能进行MAC过滤(增强请求Cisco bug <u>IDCSCvm08899</u> 影响。

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

您还可以验证AP上的Qos UP to DSCP表以及Qos标记、整形和丢弃的数据包总数:

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#

在WLC上定义Qos策略并在Flexconnect AP上下载时,可以使用进行验证:

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:gos 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
对于Qos速率限制:
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
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
```

## 信道外扫描

在排除欺诈检测故障时(验证AP是否和何时进入要扫描的特定信道)调试AP的信道外扫描非常有 用,但在未使用"信道外扫描延迟"功能时,如果敏感实时流不断中断,则调试信道外扫描也非常有

0

debug rrm off-channel defer debug rrm off-channel 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 09:45:43.5490] mcp/rrm\_userspace\_1/rrm\_schedule :: RRMSchedule process\_int\_duration\_timer\_ [\*06/11/2020 09:45:43.5490] mcp/rrm\_userspace\_1/rrm\_schedule :: RRMSchedule process\_int\_duration\_timer\_

## 客户端连接

可以使用最后一个事件时间戳列出已经由接入点取消身份验证的客户端:

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

在上一个输出中,原因代码是取消身份验证原因代码,如以下链接中所述:

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

vap是指AP内部WLAN的标识符(不同于WLC路由器上的WLAN !!!)。

您可以将其与随后详细描述的其他输出交叉关联,这些输出始终提及关联客户端的vap。

您可以使用"show controllers Dot11Radio 0/1 wlan"查看VAP ID列表。

当客户端仍然关联时,您可以获取有关其连接的详细信息:

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

有关客户端条目的更多详细信息,可以通过:

用。

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:ffffffa: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:ffffffa: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|

 |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\_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: \_\_\_\_\_

LabAP#show client summ

mac port state local\_client detect\_ago associated\_ago tx\_pkts tx\_bytes rx\_pkts rx\_bytes

您可以使用强制断开特定客户端的连接:

test dot11 client deauthenticate

可以使用以下方式为每个客户端获取流量计数器:

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 : 153 Tx Control Packets Tx Data Packets : 462 Tx Data Bytes : 145899 Tx Unicast Data Packets : 600 Rx Packets : 2910 Rx Management Packets : 13 Rx Control Packets : 943 : 1954 Rx Data Packets Rx Data Bytes : 145699 LabAP#

在无线电级别上,很多信息可以在"show controllers"中获得。添加客户端mac地址时,将显示支持 的数据速率、当前数据创建量、PHY功能以及重试次数和失败次数:

<#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:MO-7 2SS:MO-7 VHT:yes HT:yes HE:no 40MHz:no 80MHz:no 80+80MHz:no 160MHz:no 11w:no MFP:no 11h:no encrypt\_polocy: 4 qos\_capable:yes WME(11e):no WMM\_MIXED\_MODE:no \_wmm\_enabled:yes short\_preamble:yes short\_slot\_time:no short\_hdr:yes SM\_dyn:yes AMSDU:yes short\_GI\_20M:yes short\_GI\_40M:no short\_GI\_80M:yes LDPC: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	TxCu	umRetr	ries	RxDa	ita R	xMgmt	RxByt	es RxE	rr Tx	Rt	RxRt	idle_	_counte	r stats	_ago e	xpirati	on	
00:AE:F	A:78:	36:89	) ap	r0v9		8	1	6	1038		1	0		0	31	1	15	99
						-1	+ 00.		70.20									
Per IID	раск	(et si		STICS	5 TOP	citer	ιτ 00:/	AE:FA:	/8:36	:89		_						
Priorit	y Rx	Pkts	Tx	Pkts	Rx(I	ast 5	s) Tx	(last	:5s)	QID	Tx Dr	rops T	x 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	Stati	isti	cs:														
(Mbps	:	Rx, ⊺	Гх, '	Tx-Re	etrie	s)												
11 Mbps	:	2,	0	,	0													
6 Mbps	:	0,	9	,	0													
HT/VHT	Rate	Stati	isti	cs:														
(Rate/S	S/Wic	lth :	R	x, Rx	-Amp	du, Tx	<, Tx-/	Ampdu,	Tx-R	etrie	es)							
	0/1/	20 :		4,	4,	0,	0,	0										
	6/2/	20 :		4.	4.	0.	0.	0										
	7/2/	/20 :		s,	5,	0,	0,	0										
webauth	done	9:																
false																		

为了持续跟踪客户端数据速率和/或RSSI值,您可以运行"debug dot11 client rate address <mac>",此命令每秒记录一次此信息:

LabAP#debug dot11 client ra	te address 00:AE:FA:7	8:36:89					
[*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

在此输出中,Tx和Rx数据包计数器是自上次打印以来的第二个间隔中传输的数据包,与Tx重试相同 。但是,RSSI、SNR和数据速率是该间隔的最后一个数据包的值(而不是该间隔中所有数据包的平 均值)。

#### Flexconnect方案

您可以在身份验证前(例如CWA)或身份验证后方案中验证当前应用于客户端的ACL:

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 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文件系统

COS AP不允许在unix平台上列出文件系统的所有内容。

命令"show filesystems"提供当前分区上的空间使用情况和分布的详细信息:

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

命令"show flash"列出了AP闪存上的主文件。您还可以附加syslog或core关键字以列出这些特定文件 夹。

ap_2802#show	flash						
Directory of	/stora	ge/					
total 84							
-rw-rr	1 roo	t root	0	May	21	2018	1111
-rw-rr	1 roo	t root	6	Apr	15	11:09	BOOT_COUNT
-rw-rr	1 roo	t root	6	Apr	15	11:09	BOOT_COUNT.reserve
-rw-rr	1 roo	t root	29	Apr	15	11:09	RELOADED_AT_UTC
drwxr-xr-x	2 root	t root	160	Mar	27	13:53	ap-images
drwxr-xr-x	45	root	2016	Apr	15	11:10	application
-rw-rr	1 roo	t root	6383	Apr	26	09:32	base_capwap_cfg_info
-rw-rr	1 roo	t root	20	Apr	26	10:31	bigacl
-rw-rr	1 roo	t root	1230	Mar	27	13:53	bootloader.log
-rw-rr	1 roo	t root	5	Apr	26	09:29	<pre>bootloader_verify.shadow</pre>
-rw-rr	1 roo	t root	18	Jun	30	2017	config
-rw-rr	1 roo	t root	8116	Apr	26	09:32	config.flex
-rw-rr	1 roo	t root	21	Apr	26	09:32	config.flex.mgroup
-rw-rr	1 roo	t root	0	Apr	15	11:09	config.local
-rw-rr	1 roo	t root	0	Jul	26	2018	config.mesh.dhcp
-rw-rr	1 roo	t root	180	Apr	15	11:10	config.mobexp
-rw-rr	1 roo	t root	0	Jun	5	2018	config.oeap
-rw-rr	1 roo	t root	2253	Apr	26	09:43	config.wireless
drwxr-xr-x	2 roo	t root	160	Jun	30	2017	cores
drwxr-xr-x	2 root	t root	320	Jun	30	2017	dropbear
drwxr-xr-x	2 root	t root	160	Jun	30	2017	images
-rw-rr	1 roo	t root	222	Jan	2	2000	last_good_uplink_config
drwxr-xr-x	2 roo	t root	160	Jun	30	2017	lists
-rw-rr	1 roo	t root	215	Apr	16	11:01	part1_info.ver
-rw-rr	1 roo	t root	215	Apr	26	09:29	part2_info.ver
-rw-rr	1 roo	t root	4096	Apr	26	09:36	random_seed
-rw-rr	1 roo	t root	3	Jun	30	2017	rxtx_mode
-rw-rr	1 roo	t root	64	Apr	15	11:11	sensord_CSPRNG0
-rw-rr	1 roo	t root	64	Apr	15	11:11	sensord_CSPRNG1
drwxr-xr-x	3 sup	port root	224	Jun	30	2017	support
drwxr-xr-x	2 roo	t root	2176	Apr	15	11:10	syslogs
Filesystem		Siz	e Used Av	ailab	ole	Use% N	Mounted on
flash		57.5	M 372.0K	54.	1M	1%,	/storage

存储和发送系统日志

syslog文件夹存储先前重新启动的syslog输出。命令show log仅显示自上次重新启动后的系统日志

## 在每个重新启动周期中,系统日志会写入增量文件。

artaki# show Directory of total 128	flash syslog /storage/sys	gs slogs/			
-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% Mounted on
flash		57.6M	88.OK	54.5M	0% /storage
artaki# show Directory of total 0	flash cores /storage/co	res/			
Filesystem		Size	Used Av	ailable	Use% Mounted on
flash		57.6M	88.OK	54.5M	0% /storage

初始启动后的第一个输出是文件1.0,如果1.0过长,则会创建文件1.1。重新启动后,将创建一个新 文件2.0,以此类推。

如果希望AP将其系统日志消息单播发送到特定服务器,可以从WLC配置系统日志目标。

默认情况下,AP将其syslog发送到可能导致相当多的广播风暴的广播地址,因此请确保配置 syslog服务器。

默认情况下,AP通过syslog发送其控制台输出上打印的任何内容。

在9800控制器上,您可以在Management下的Configuration -> AP Join配置文件中更改这些参数。

o

Edit AP Jo	oin Profile									
General	Client	CAPWAP	AP	Management	Sec	urity	ICap	QoS		
Device	User	Credentials	CDP I	nterface						
TFTP D	owngrade					Telnet	/SSH Co	nfiguratio	on	
IPv4/IPv6	6 Address		0.0.0.0			Telnet				
Image Fil	le Name		Enter File	Name		SSH			~	
System	Log					AP Co	re Dump			
Facility V	alue		KERN	•		Enable	Core Dum	ıp		
Host IPv4	4/IPv6 Addr	ess	192.168.1	.12						
Log Trap	Value		Information	•						
Secured	i	C								

您可以更改Log Trap Value,以便也通过syslog发送调试。然后,您可以在AP CLI上启用调试,这 些调试的输出通过syslog消息发送到配置的服务器。



,只有当您将syslog设施设置为KERN(默认值)时,AP才会发送syslog消息。

如果您正在排除AP可能失去网络连接(例如,在WGB上)的问题,则系统日志不如在AP失去上行 链路连接时发送消息那么可靠。

因此,依靠闪存中存储的系统日志文件是调试和存储AP本身输出并在稍后定期上传输出的好方法。

## AP支持套件

一些通常收集的各种类型的诊断信息可在单个捆绑包中提供,您可以从接入点上传。

可以包含在捆绑包中的诊断信息包括:

- · AP show tech
- AP系统日志
- AP Capwapd 大脑日志
- AP启动和消息日志
- AP核心转储文件

要获取AP支持捆绑包,您可以进入AP CLI并输入命令"copy support-bundle tftp: x.x.x.x"。

之后,您可以检查名为AP名称并附加了support.apversion.date.time.tgz的文件,如下所示:

## 当您"解压缩"该文件时,可以查看收集的各种文件:

5-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

## 远程收集AP核心文件

要远程收集AP核心文件,请启用要包含在支持捆绑包中的核心转储,然后从AP上传支持捆绑包 ,或直接发送到tftp服务器。后续示例使用tftp服务器192.168.1.100。

```
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 GUI

սիսիս					Sage Configuration Ding Logout Befresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SE	CURITY MANAGEMENT COMMANDS HEL	P FEEDBACK		User:admin(ReadWrite) 🔒 Home
Wireless	All APs > Details for AP70DB.98E1.3DEC				< Back Apply
* Access Points All APs	General Credentials Interfaces High A	vailability Inventory Advanced	Intelligent Capture		
Virect APs • Radios 802.11a/n/ac/ax	Regulatory Domains	802.11bg:-E 802.11a:-I	Power Over Ethernet Settings		i l
802.11b/g/n/ax	Country Code	IL (Israel)	PoE Status	Full Power	
Dual-SG Radios	Cisco Discovery Protocol	*	Pre-standard 802.3af switches	0	
Global Configuration	AP Group Name	default-group *	Power Injector State	8	
Advanced	Statistics Timer	180	AP Core Dump	5	
Mesh	Data Encryption		AP Core Dump	🗹 Enabled	
AP Group NTP	2 million	Child Confert 1	TFTP Server IP 192.168.1.1	00	
▶ ATF	Teines	Grobal Corrig +	File Name apCores		
RF Profiles	4 SSH	Global Config •	File Compression 🕅 Enable		
FlexConnect Groups	NSI Ports State	Global Config • In	AP Retransmit Config Parameters		
FlexConnect ACLs	TCP Adjust MSS (IPV4: 536 - 1363, IPV6: 1220 - 1331)	TCP MSS is Globally Enabled	AP Retransmit Count	5	
FlexConnect VLAN	LED State	Enable	AP Retransmit Interval	3	
Templates	LED Brightlevel	8 (1-8)	VLAN Tagging		
Network Lists	LED Flash State	(1-3600)seconds	VLAN Tagging	Enabled	
# 802.118/8/8C/8X		© Indefinite	NTP Server Status		
▶ 802.110/g/n/ax		🖲 Disable	Status Disabled		
Media Stream	USB Module ID	USB Module	mDNS Configuration		
Application Visibility And Control	Override			(1)	
Lync Server	USB Module Status	×	mores shooping	C Enabled	-
Country	USB Module Operational State	Not Detected	VLAN LIST		
Timers	Hyperlocation Configuration		TrustSec		
▶ Netflow	5 Bashia Musalashia	Glabal Coofin *	TrustSec.Config		
▶ QoS	- Energie Hyperiocation	Descart	CMX Services		
	Library and the same	Present	Services Sub-Services CMX Server	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

Cisco Catalyst 9800-CL Wireless Controller	We	elcome admin   🐐 🐔	🖺 💠 🐚 🛛 📿 Search /	IPs and Clients Q
Q, Search Menu Itams Configuration * > Tags & Profiles * > AP Join	Edit AP Join Profile			
Deshboard	General Client CAPW	tials CDP Interface	Security ICap QoS	
Monitoring     AP Join Profile Name     TisgoOffice	TFTP Downgrade		Telnet/SSH Configuratio	n
Configuration > testprofile	IPv4/IPv6 Address	0.0.0.0	Telnet	
Administration	Image File Name	Enter File Name	SSH	<b>v</b>
Licensing	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 ()		Enable File Compression	V

从Cisco IOS® XE 17.3.1,您有一个支持捆绑包选项卡,可以从WLC GUI下载AP SB。

它所做的只是在AP上执行"copy support-bundle"命令并通过SCP将其发送到WLC(因为WLC可以是 SCP服务器)。

然后,您可以从浏览器下载:

P780C-	AIR-			81.244.9.50	502f.a836	Edit AP							
085-49E6	AP2802 A-K9	I- 2	0			General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle	
<ul> <li>1 &gt; 10 • Items per page</li> <li>5 GHz Radios</li> <li>2.4 GHz Radios</li> </ul>				Destination Server IP* Destination File Path* 0		This Device External Server 172.31.46,79		Last Export Status State					
								Transfer Mode Server IP File Path					
Dual-Band Radios					Username Password	s* *			Time of Export				
Country				Start Tra	nsfer								
LSC Pr	rovision												

这意味着,您可以在17.3.1之前的eWLC版本中手动执行相同的技巧:

如果您没有可连接到AP的TFTP服务器,请通过SCP将支持捆绑包从AP复制到eWLC IP。

eWLC通常通过SSH从AP到达,因此对于17.3之前版本来说这是一个不错的技巧。

步骤1:<u>在9800 v17.2.1上启用SSH</u>

第二步: 在Cisco IOS® XE v17.2.1上启用SCP

此示例说明如何配置SCP的服务器端功能。此示例使用本地定义的用户名和密码:

! 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

第三步: 使用命令copy support-bundle,我们需要指定在SCP服务器中创建的文件名。

提示:您可以运行一次命令以获取有意义的文件名,然后在命令中复制/粘贴该文件名:



# 第四步:然后,您可以进入eWLC GUI并在以下位置获取文件:Administration > Management > File Manager:



#### 物联网和蓝牙

可以在AP上使用检查gRPC服务器日志:

```
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=" 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] Connection not in ready state sleeping for 10 second
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 "
```

可使用验证与DNA空间连接器的连接:

```
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	conr	nect	ion deta	il					
Connection State	:	READ	DY						
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	:	202	20-04-01	00:32:47	.891433113	+0000	UTC I	m=+34598	85.338898246
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 pk	ts	:	5						

#### 要查看AP的当前BLE广播配置:

PLE Drofile Config

AP# show controllers ioTRadio ble 0 broadcast

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) Instance-ID (hex)	:	000000000005446089c 7f0000001f00
Profile 2 (Eddystone URL) URL	:	http://www.

## 要查看扫描结果,请执行以下操作:

AP# show controllers ioTRadio ble 0 scan brief MAC RSSI(-dBm) RSSI@1meter(-dBm) Profile 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 78 Unknown 18:04:ED:04:1C:5F 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 65 0000D:00H:00M:01S iBeacon E0:7D:EA:16:35:35 68 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 72 04:EE:03:53:6A:3A N/A 0000D:00H:00M:01S 72 Unknown 04:EE:03:53:6A:3A 65 0000D:00H:00M:01S iBeacon E0:7D:EA:16:35:35 68 65 0000D:00H:00M:01S 67 Unknown E0:7D:EA:16:35:35 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

当AP在部署应用的高级BLE网关模式下工作时,您可以使用检查IoX应用的状态:

您可以使用以下命令连接到IOX应用,然后在楼层信标配置期间监控日志:

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

结论

有许多故障排除工具可以帮助我们解决与COS AP相关的问题。

本文档列出了最常用的文档,并会定期更新。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。