Solucionar problemas de APs COS

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Capturar Rastreamentos de Pacotes (Rastreamentos de Farejador)
PCAP com fio na porta AP
Procedimento
Opções de comando
PCAP com fio através do uso do filtro
Captura de rádio
Procedimento
Verificar
<u>Outras opções</u>
Controle o rastreamento do AP Client a partir do 9800 WLC
Pacote de depuração do cliente no AP
APs Catalyst 91xx em modo farejador
Dicas para Troubleshooting
MTU de Caminho
Para ativar depurações no momento da inicialização
Mecanismo de economia de energia
Clientes QoS
Verificação fora do canal
Conectividade do cliente
Cenários do Flexconnect
Sistema de arquivos AP
Armazenar e enviar syslogs
Pacote de suporte AP
Coletar arquivos centrais de AP remotamente
CLI AireOS
GUI do AireOS
CLI do Cisco IOS®
GUI do Cisco IOS®
loT e Bluetooth
Conclusão

Introdução

Este documento descreve algumas das ferramentas de solução de problemas disponíveis para APs que executam o sistema operacional COS (Cheetah OS, Click OS, simplesmente Cisco AP OS).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento concentra-se nos APs COS, como os modelos de APs das séries 2800, 3800, 1560 e 4800, bem como os novos APs 11ax Catalyst 91xx.

Este documento se concentra em muitos recursos disponíveis no AireOS 8.8 e posterior. E também o Cisco IOS® XE 16.12.2s e posterior.

Pode haver comentários sobre a disponibilidade de certos recursos em versões anteriores.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Capturar Rastreamentos de Pacotes (Rastreamentos de Farejador)

PCAP com fio na porta AP

É possível (a partir do 8.7 com o filtro disponível no 8.8) tomar um pcap na porta Ethernet do AP. Você pode exibir o resultado ao vivo na CLI (apenas com detalhes resumidos do pacote) ou salvá-lo como um pcap completo na flash do AP.

O pcap com fio captura tudo no lado Ethernet (tanto Rx/Tx) e o ponto de toque dentro do AP é imediatamente antes do pacote ser colocado no fio.

No entanto, ele apenas captura o tráfego plano de CPU do AP, o que significa o tráfego de e para o AP (DHCP do AP, túnel de controle de capwap do AP, ...) e não mostra o tráfego do cliente.

Observe que o tamanho é muito limitado (limite de tamanho máximo de 5 MB), portanto, pode ser necessário configurar filtros para capturar apenas o tráfego no qual você está interessado.

Certifique-se de interromper a captura de tráfego com "no debug traffic wired ip capture" ou simplesmente "undebug all" antes de tentar copiá-la (caso contrário, a cópia não termina quando os pacotes ainda são gravados).

Procedimento

Etapa 1. Inicie o pcap; selecione o tipo de tráfego com "debug traffic wired ip capture":

<#root>

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

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

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

Etapa 2. Aguarde até que o tráfego flua e, em seguida, pare a captura com o comando "no debug traffic wired ip capture" ou simplesmente "undebug all":

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

Etapa 3. Copie o arquivo para o servidor tftp/scp:

<#root>

AP70DB.98E1.3DEC#copy pcap

AP70DB.98E1.3DEC_capture.pcap0

Etapa 4. Agora você pode abrir o arquivo no Wireshark. O arquivo é pcap0. Altere para pcap de modo que ele se associe automaticamente ao wireshark.

Opções de comando

O comando debug traffic wired tem várias opções que podem ajudá-lo a capturar tráfego específico:

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

Você pode adicionar "verbose" no final do comando debug para ver o dump hexadecimal do pacote. Esteja ciente de que isso pode sobrecarregar sua sessão de CLI muito rapidamente se o

filtro não for estreito o suficiente.

PCAP com fio através do uso do filtro

O formato do filtro corresponde ao formato do filtro de captura tcpdump.

	Exemplo de filtro	Descrição			
	"host 192.168.2.5"	Isso filtra a captura de pacotes para coletar apenas pacotes que vão para ou vêm do host 192.168.2.5.			
Host	"src host 192.168.2.5"	Isso filtra a captura de pacotes para coletar apenas pacotes que vêm de 192.168.2.5.			
	"dst host 192.168.2.5"	Isso filtra a captura de pacotes para coletar apenas pacotes que vão para 192.168.2.5.			
	"porta 443"	Isso filtra a captura de pacotes para coletar apenas pacotes com uma origem ou um destino da porta 443.			
Porta	"src port 1055"	Isso captura o tráfego originado na porta 1055.			
	"dst port 443"	Isso captura o tráfego destinado à porta 443.			

Aqui está um exemplo onde a saída é exibida no console, mas também filtrada para ver apenas pacotes de dados CAPWAP:

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

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

Exemplo de saída no arquivo:

Para abrir a captura no Wireshark:

		·	
ply a display filter <ctrl-></ctrl->			Expression
Delta Source	Destination	Lengt Info	Payload Type Dit
1 0.000000 192.168.1.82	192.168.1.15	651 Application Data	0
2 0.001525 192.168.1.15	192.168.1.82	123 Application Data	0
3 8.601152 192.168.1.4	255.255.255.255	305 CAPWAP-Control - Primary Discovery Request[Malformed Packet]	0
4 9.638243 192.168.1.82	192.168.1.15	987 Application Data	CI
5 0.001627 192.168.1.15	192.168.1.82	123 Application Data	C1
6 0.010493 192.168.1.82	192.168.1.15	171 Application Data	C
7 0.001007 192.168.1.15	192.168.1.82	123 Application Data	C
8 0.000287 192.168.1.82	192.168.1.15	187 Application Data	C
9 0.000810 192.168.1.15	192.168.1.82	123 Application Data	c
10 28.344341 192.168.1.82	192.168.1.15	123 Application Data	c
11 0.001214 192.168.1.15	192.168.1.82	139 Application Data	c
12 21.065522 192.168.1.82	192.168.1.15	651 Application Data	0
13 0.001215 192.168.1.15	192.168.1.82	123 Application Data	ci

Captura de rádio

É possível ativar a captura de pacotes no plano de controle do rádio. Devido ao impacto no desempenho, não é possível capturar dados no painel de rádio.

Isso significa que o fluxo de associação do cliente (testes, autenticação, associação, eap, arp, pacotes dhcp, bem como pacotes de controle ipv6, icmp e ndp) é visível, mas não os dados que o cliente passa após a movimentação para o estado conectado.

Procedimento

Etapa 1. Adicione o endereço mac do cliente rastreado. Vários endereços MAC podem ser adicionados. Também é possível executar o comando para todos os clientes, mas isso não é recomendado.

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.

Etapa 2. Defina um filtro para registrar apenas protocolos específicos ou todos os protocolos suportados:

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

Etapa 3. Escolha exibir a saída no console (de forma assíncrona):

configure ap client-trace output console-log enable

Etapa 4. Inicie o rastreamento.

config ap client-trace start

Exemplo:

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

Para interromper a captura:

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

Verificar

Verificar Rastreamento de Cliente:

<#root> AP70DB.98E1.3DEC# show ap client-trace status Client Trace Status : Started Client Trace ALL Clients : disable Client Trace Address : a8:db:03:08:4c:4a Remote/Dump Client Trace Address : a8:db:03:08:4c:4a Client Trace Filter : probe Client Trace Filter : auth Client Trace Filter : assoc Client Trace Filter : eap Client Trace Filter : dhcp Client Trace Filter : dhcpv6 Client Trace Filter : icmp Client Trace Filter : icmpv6 Client Trace Filter : ndp Client Trace Filter : arp Client Trace Output : eventbuf Client Trace Output : console-: 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

Exemplo de uma conexão de cliente bem-sucedida:

Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5351] [1586169921:535099] [APOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11 AUTHENTICATION : (.)</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.53521 [1586169921:535224] [APOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <apr0vl> [U:W] DOT11 AUTHENTICATION : (.)</apr0vl>
Anr	6 10-45-21 kernel: 1+04/05/2020 10-45-21 53611 (1586169921-5361581 [AD0CD0 P894 46P41	AB: 4b: 03: 08: 4c: 4al capr0v0x [D:W] DOT11 AUTHENTICATION : ()
3.mm	10,45,31 barral, (#04/06/2020 10,45,31 5416) (150616002),641500) [\$00000 0004 4604]	a de de de de de de de de la construction de la con
where	0 10.35.61 KEINEL. [03/06/2020 10.35.51.5115] [1500103921.531590] [APOLDU.E093.3023]	action of the second se
apr	6 10:45:21 Kernel: [=04/06/2020 10:45:21.5441] [1586169921:544114] [APOCDO.F894.46E4]	[asidbiosideiacia] <aprovos (.)<="" :="" [biw]="" assoc="" doril="" response="" td=""></aprovos>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5501] [1586169921:550153] [APOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <apr0v0> [D:W] EAFOL_KEY.M1 : DescType 0x02 KeyInfo 0x008b</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5778] [1586169921:577836] [APOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL KEY.M2 : DescType 0x02 KeyInfo 0x010b</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5784] [1586169921:578476] [AFOCDO.F894.46E4]	[a8:db:03:08:4c:4a] <apr0v0> [D:W] EAFOL KEY.M3 : DescType 0x02 KeyInfo 0x13cb</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5955] [1586169921:595552] [APOCDO.F894.46E4]	a8:db:03:08:4c:4a] <apr0v0> [U:W] EAFOL KEY.M4 : DescType 0x02 KeyInfo 0x030b</apr0v0>
ann	6 10-45-21 bernel: [+04/06/2020 10-45-21 60031 [1586169921.6003411 [AB0070 F894 46F41]	as db.03.08.4c.4al captoron [m.w] potl action : ()
Sec.	C 10.45.31 Lame1. (604/06/2000 10.45.31 C0201 [106010301] [800001] [800001004 4084]	
apr	6 10:45:21 Kernel: [04/06/2020 10:45:21.6026] [1566169921:60261/] [APOCDU.F094.4624]	[asidbiosidsidsidsid] C EDVOS [Dim] DOTIT ACTION : (.)
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.64/5] [1586169921:64/518] [APOCDU.F894.46E4]	[as:db:03:08:4c:4a apr0v0> [U:w] DOTIL_ACTION : (.)
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.6475] [1586169921:647594] [APOCDO.F894.46E4]	[a8:db:03:08:40 <apr0v0> [D:W] DOT11_ACTION : (.)</apr0v0>
Apr	6 10:45:21 kernel: [+04/06/2020 10:45:21.8636] [1586169921:863610] [APOCD0.F894.46E4]	[a8:db:02
anr	6 10:45:21 kernel: [+04/06/2020 10:45:21 86361 [1586169921:8636441 [ap0CD0 F894 46F41	asideial caprovos (U:C) DECE DISCOVER : Trapaid 0xa38c01d6
See.	C 10.45.31 Langel, (404/06/2020 10.45.31 0637) (1506160031.063700) [ABOPD #004 46#4]	(and the fail dependence (and precovery a managed on Second
whit		
apr	6 10:45:21 kernel: [=04/06/2020 10:45:21.863/] [1586169921:863/31] [APOCDO.F894.46E4]	VOS:4C:4a] <aprovos :="" [u:c]="" dhcp="" discover="" td="" transid="" uxasscuide<=""></aprovos>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863741] [APOCD0.F894.4	J3:08:4c:4a] <nsscapwap0> [U:E] DHCP_DISCOVER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863762] [APOCDO.F824	5:03:08:4c:4a] <nsscapwap0> [U:E] DHCP_DISCOVER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [+04/06/2020 10:45:21.8676] [1586169921:867627] [APOCD0.	db:03:08:4c:4a] <nsscapwap0> [D:E] DHCP OFFER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8676] [1586169921:867664] [APOC	G:db:03:08:4c:4al <nsscapwap0> [D:C] DECP OFFER : TransId 0xa38c01d6</nsscapwap0>
ane	6 10:45:21 kernel: 1404/06/2020 10:45:21 86771 (1586169921:8677091 1	ABidbi02:00:4c:4al cosscaptan05 [D:C] DNCP OFFER : TransId 0xa28c01d6
2000	C 10.45.01 Land 1. [60/06/2000 10.45.01 06771 [1506160031.067740]	action of the second se
apr	6 10145121 kerneli [-04/06/2020 10145121.66//] [1566165921166//40	lastabiositeritaj caprovos [biw] back orrek i fransia ukaseculas
Apr	6 10:45:21 kernel: [=04/06/2020 10:45:21.8684] [1586169921:8687 [24]	[a8:db:03:08:4c:4a] <nsscapwapu> [D:E] DHCP_OFFER : TransId 0xa38c01d6</nsscapwapu>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8685] [1586169921:0 4624]	[a8:db:03:08:4c:4a] <nsscapwap0> [D:C] DHCP_OFFER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:20 http://doi.org/10.100/0000000000000000000000000000000	bodb:03:08:4c:4a] <nsscapwap0> [D:C] DHCP OFFER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:	:03:08:4c:4a] <apr0v0> [D:W] DHCP OFFER : TransId 0xa38c01d6</apr0v0>
Apr.	(1) II - Unlink packet (from client)	03:08:4c:4a] <apr0v0> [U:W] DHCP REQUEST : TransId 0xa38c01d6</apr0v0>
Znr	The optime packet (ITOM STIENC)	2:09:40:41 capromotion (U.C) DECE PROVEST : TransId Ove20:00146
MDI		osiositeitaj caprovos (bic) bace acousti iransid okasecolae
apr	D - Downlink packet (to client)	barbarteriaj caprovos [uic] bace Reguest : Transid Uxaseculde
Apr	and b boundering packet (co strend)	D3:08:4c:4a] <apr0v0> [U:C] DHCP_REQUEST : TransId 0xa38c01d6</apr0v0>
Apr	6 10	D3:08:4c:4a] <nsscapwap0> [U:E] DHCP_REQUEST : TransId 0xa38c01d6</nsscapwap0>
Apr	610 W - module Wireless 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	6 10 III medial a Thile means the last second	3:08:4c:4al <pre>capwap0> [D:C] DHCP ACK : TransId 0xa38c01d6</pre>
have	E - MOQUIE Etnernet driver	3:08:40:4al characanyan() [D:C] DBCD ACK : TransId Oxa38c01d6
Barra .	0 40	53.00.4.4.4. AD ADDA (DEL) DICE DOP AND A LABOR AND ADDA ADDA
whit	C modulo Click	Divisionacia (aprovos [Diw] DALP ALK : Transid Oxaseculae
Apr	• 10 C - MOQUIE CIICK	D3:08:40:4a] <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 0xa38c01d6</nsscapwap0>
Apr	6 10	03:08:4c:4a] <apr0v0> [D:W] DHCP ACK : TransId 0xa38c01d6</apr0v0>
Apr	6 10-	03:08:4c:4a] <apr0.00> [U:W] ABP OUERY : Sender 192.168.101.13 Targin 192.168.101.1</apr0.00>
Ane	6 10:45	The O3+O8+A+A+1 campbook [H+C] ADD ONPOV - Sendar 100 160 101 10 Target 100 10011
white,	1 10.10 - 10. 1. 1404/02/0000 10.46.00 10.11 11605120000 10.00101 1	La de 30.00.10.10.1 archive [Uic] are yours : sender 136.100.101.13 laggi 196.100.101.1
apr	e 10:45:22 Kernel: [-04/06/2020 10:45:22.1611] [1586164422:1611/7] [APOCD0.P894.4624]	[actub:v3:v0:4c:4a] <apr040> [Utc] ARP_QUERY : Sender 142.168.101.13 TargIp 192.168.101.1</apr040>
Apr	6 10:45:22 Kernel: [*04/06/2020 10:45:22.1612] [1586169922:161213] [APOCD0.F894.46E4]	[aS:db:03:05:4c: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] [AF0CD0.F894.46E4]	[a8:db:03:08:4c:4a] <nsscapwap0> [D:E] ARP_REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:4.</nsscapwap0>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164699] [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:4</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:4</nsscapwap0>
anr	6 10:45:22 kernel: (*04/06/2020 10:45:22 16471 (1586169922:164751) (henored #864 46#4)	[a8:db:03:08:4c:4a] carr0v05 [D:W] APP REPLY : Sender 192 168 101.1 Hubddr 54-7-56-69-67-96-47
angl in	A VALIMAN WANNANT I ALLANIMANA AATIMATAJII [TAAATAJIA11AT] [MEAAAAATAJIJAT]	Incimulationisation include the second to the second of th

As letras entre colchetes ajudam você a entender onde o quadro foi visto (E para Ethernet, W para Wireless, C para o módulo Click quando ele é interno ao AP) e em que direção (Upload ou Download).

Aqui está uma pequena tabela do significado dessas letras:

- U pacote de uplink (do cliente)
- D pacote downlink(para clicar)
- W driver de módulo sem fio
- E driver de módulo Ethernet
- C clique no módulo

Outras opções

Exibir log de forma assíncrona:

Os logs podem ser consultados com o comando: "show ap client-trace events mac xx:xx:xx:xx:xx:xx" (ou substitua o mac por "all")

<#root>

AP0CD0.F894.46E4#

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

```
[*04/06/2020 10:11:54.287675] [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]	[AP0CD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v1></apr0v1>	[U:W]	DOT11_PROBE_REQUEST

Despejar os pacotes no formato hexadecimal

Você pode despejar os pacotes no formato hexadecimal na CLI:

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

AP7009.9911.BDC2sconfigure ap client-trace start
earning: to recover mus pushed conting, need LAWAR restarts or reload to re-apply the conting from mus Applone 50% 100/films - 6 13/25/15 Maral: (#6/06/2000 11/25/15 20/07) averand(1): Starting Linderton Marchar -
Arrowissan subscape a selecto mana, i vivorenza a selecto selecto anderes anderes anderes a Arro 6 19:25:15 karnel / 164/02/020 19:25:15 3269 karned Lintend Matcher.
configure ap client-trace output dump address add a8(db:03:08)4c:4a
AP70DB.98E1.3DEC#Apr 6 13:25:02 kernel: [*04/06/2020 13:25:02.5997] HAC already exists: index 0
configure ap client-trace output dump
address Remote/Local dump Client Addresses
enable Enable Trace output for local dump
AP7078.9921 JDEC#configure ap client-trace output dump enable
<4-5000> Enter the packet dump length value
Ar/ous.swil.spaceconfigure ap client-trace output dump enable 100
SEP
AP7070 5981 3DEC4Apr 6 13:29:27 Mernel: [*04/06/2020 13:29:27.4648]
Apr 6 13:25:27 Kernel: [*04/06/2020 13:25:27.4648] Time:464876us Dir:Rx Rate:m7.2-2 Rest:-43 Ch:1 Fo:188 Dur:30 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 54:7c:69:b7:3f:42 Seq:126(294) Info:ARP Retry:0 Len:121 Typesub:28 Tid:q0
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0000 00 00 00 00 00 00 00 00 00 00 00
Apr 6 13:25:27 kernel: [*04/06/2020 13:25:27.4645] 0010 00 00 00 00 00 00 00 11 00 00 00 0
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4649] 0020 00 00 13 00 15 b3 ff ff 00 00 00 ff ab cd 02 00
Apr 6 13:25:27 kernel: [*04/06/2020 13:25:27.4645] 0030 00 03 700 00 06 00 07 00 01 00 00 00 00
Apr 6 13:39:27 Mernel: [*04/06/2020 13:39:27.4445] 0040 00 01 20 00 00 45 31 21 0f d5 a8 00 00 00 00
Apr 6 13:27:27 Kernel: [*04/06/2/22 13:27:27.449] 0000 00 00 00 00 00 00 00 00 00 00 00
Apr 6 13:35:37 kernel: [*04/06/2020 13:35:37.4650] 0050 4a c0 a8 65
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4748]
Apr 6 13:25:27 kernel: (*04/06/2020 13:25:27.4748) Time:474883us Dir:Tx Rate:1 Rasi:=55 Ch:1 Fc:208 Dur:13a a8:db:03:00:4c:4a 00:27:e3:36:4d:a0 54:7c:65:b7:3f:42 Seq:6(6) Info:ARP Retry:0 Len:104 Typesub:28 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 01 10 00 00 00 0
Apr 6 13:13:137 kernel: (*04/06/2020 13:13:13:137.4745) 0020 00 01 3 88 15 b5 ff ff 00 00 al al 00 50 00 50
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0030 00 00 6 8b 2e b6 00 07 3f 50 02 01 00 00 80 02
App = 1 2:27:27 Methel: [*04/06/2020 12:27:27.4743] 0040 34 01 40 00 00 47 43 36 40 40 54 70
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4745] 0070 65 01 40 db 03 08 4c 4a c0 a0 65 0d 00 00 00
Apr 6 13:25:27 kernel: [*04/06/2020 13:25:27.4745] 0080 00 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13:25:27 kernel: (*04/06/2020 13:25:27.4750) 0050 00 00 6b 6b 6b 6b 6b 6b
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1000]
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1000] Time:100019us Dir:Rx Rate:5 Resi:=36 Ch:1 Fo: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 13:31:03.1000] 0000 00 00 00 00 00 00 00 00 00 00
Apr 6 13:31:03 Kernel: 1 *04/06/2020 13:31:03:1003 0010 00 00 00 11 00 00 00 00 00 00 00 0
Apr 6 13:1:03 kernel: "04/6/2020 13:1:03.1000 0040 00 00 ff ff ff ff a0 db 03 08 40 4f ff
Apr 6 13:31:03 kernel: (*04/06/2020 13:31:03.1001) 0080 ff ff ff ff 70 27 00 00 01 04 02 04 0b 16 32 08
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1801] 0060 0c 12 10 24 30 48 60 6c 03 01 01 2d 1a 2d 00 1b
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1001] 0070 ff ff 00 00 00 00 00 00 00 00 00 00 00
Apr 6 13:31:03 kernel: (*04/06/2020 13:31:03.1801) 0080 00 00 00 00 00 00 07 0x 00 00 40 00 00
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1001] 0090 40 00 21 ff
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2000]
Apr 6 13:31:03 kernel: (*04/06/2020 13:31:03.2000) Them: 2000154s Dir:TX Rate1 Rasi-55 Chil Fe:50 Dur:12a as:db:03:08:4e:a0 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 8eg:65e(1630) Info:DOT11_PROBE_RESPONSE Retry:0 Len:250 Typesub:05
Apr = 13:3:03 kernel: ["04/06/2020]3:3:03.2003 0000 00 00 00 00 00 00 00 00 00 00 0
Age & 19141.00 Memoral 1947.04/2010 191-091.00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0030 00 00 6 6b 27 16 00 20 96 02 10 00 50 00
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0040 3a 01 a0 db 03 09 4c 4a 00 27 43 36 4d a0 00 27
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0050 e3 36 4d ao e0 65 96 00 12 18 24 03 01 0d 64 00
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0060 11 11 00 0c 74 65 73 74 65 77 6c 63 77 6c 61 6e
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0070 01 08 82 84 8b 96 00 12 18 24 03 01 01 07 06 49
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0080 4e 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 66 30 14 01
Apr - 4 1.1.1.1.1.1. Apr - 1 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1

Em seguida, você pode limpar o despejo hexadecimal e salvar em formato de texto e importar para o Wireshark:

Time:20010us Dir:Rx Rate:1 Rssi:-37 Ch:1 Fo:b0 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq:1(1) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b 0000 00 00 00 00 00 00 00 00 00 00 00 0	
Time:43054us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fo:d0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66c(1644) Info:DOT11_ACTION Retry:0 Len:54 Typesub:0d 0000 00 00 00 00 00 00 00 00 00 00 00 0	
Time:43155us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:b0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq:66d(1645) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Types: 0000 00 00 00 00 00 00 00 00 00 00 00 0	ıb: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:a0 Seq:2(2) Info:DOT11_ASSOC_REQUEST Retry:1 Len:220 Typesub:00 0010 00 00 00 00 00 00 00 00 00 00 00	

Open	Ctrl+O	£ £ £	· 역 역 역 표	
Open Recent				Expression
Merge		1		
Close	Ctrl+W		Wireshark - Import From Hex Dump ? X	
Save	Ctrl+S		Tenant Erem	
Save As	Ctrl+Shift+S	Data\Local\Temp		
File Set		234744 HelpDesk	File: C:/Users/tantunes/CISCO/11ax training/dump_example.txt Browse IBBF161F6_debugs.capture2.pcap (1	(MB)
rile set		O\00-SRs\SR 688	Offsets: Hexadecimal	(8)
Export Specified Packet	5	O\00-SRs\SR 688	4956 Bytes)	
Export Packet Dissectio	ns P	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	h	Data\Local\Temp	Direction indication:	
Export Objects	,	nloads\AP_trace_	Encansilation	
Print	Ctrl+P	O\IOS-Images\A	Encape lation Type: Ethernet	
Quit	Ctrl+Q		No dummy header	
,	apure	-	O Ethernet Ethertyne (hex):	
	using this filter: 📕	Enter a capture filter .	TPv4 Protocol (dec): All interfaces sho	wn 🕶
	Land Arm C			
	Npcap Loopt	back Adapter		
1	Ethernet_yell	owCable		
	Local Area Co	onnection* 3		
	Ethernet 4	onnection" 9	C Super1911 Bailand	
	Wi-Fi		C Expertition Payman	
	ThinkpadEth	ernetBlue		
	Local Area Co	onnection-11	Maximum frame length:	

Como a saída pode ser muito grande e considerar que a saída menciona apenas que tipo de quadro é visto e não qualquer detalhe interno, pode ser mais eficiente redirecionar a captura de pacotes para um laptop que execute um aplicativo de captura (como o wireshark).

Ative o recurso de captura remota para enviar os pacotes para um dispositivo externo com o Wireshark:

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

O comando significa que o AP encaminha todos os quadros capturados pelo filtro de rastreamento do cliente em direção ao laptop em 192.168.68.68 e usa o encapsulamento PEEKREMOTE (como os APs no modo farejador) na porta 5000.

Uma limitação é que o laptop de destino deve estar na mesma sub-rede do AP em que você executa esse comando. Você pode alterar o número da porta para acomodar quaisquer políticas de segurança em vigor na sua rede.

Depois de receber todos os pacotes no laptop que executa o Wireshark, você pode clicar com o botão direito no cabeçalho udp 5000 e escolher decodificar como e escolher PEEKREMOTE como ilustrado nesta figura:

📕 🔝 🙂 🛄 🔂 🗙 🖾 🧣 👄 🖷 udp.port == 5688	·≌ • ⊻ , 			Expression +
b. Deta Source 59 0.000000 Samsungt_08:4(-:4a) 60 0.038249 Sics_5:4:a0 61 0.038249 Sics_5:4:a0 62 0.000000 Samsungt_08:4:c:4a 63 0.000000 Samsungt_08:4:c:4a 64 0.038249 Samsungt_08:4:c:4a 65 0.000000 Samsungt_08:4:c:4a 66 0.030097 Samsungt_08:4:c:4a 67 0.010008 Sics_5:6:4:a0 68 0.009085 Samsungt_08:4:c:4a 70 0.020078 Sics.05:4:a0 72 0.009081 Samsungt_08:4:c:4a 73 0.020078 Sics.05:4:a0 74 0.020078 Sics.01:1 79 0.020078 Sics.01:1.1 90 0.020071 Sics.101.1 90 0.020091 Sics.101.1 91 0.0209955 Sics.101.1 92 0.029955 Sics.101.1 93 0.029955 Sics.101.1 94<	Destination 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 Conversation Filter Colorize Conversation SCTP Follow Copy Protocol Preferences Probacol Preferences Show Packet in New Window SamsingE_08:4c:4a Broadcast Dits:), 251 bytes Captured (2008 bi 70:db:98:e1:3d:ec), 0st: 60odRivyI_ 70:db:98:e1:3d:ec), 0st: 60odRivyI_	Lengt Info 251 Probe Request, SN-577, FN-0, Flags 292 Probe Requests, SN-410, FN-0, Flags 107 Authentication, SN-411, FN-0, Flags 206 Association Request, SN-579, FN-0, Flags 206 Association Response, SN-412, FN-0, Flags 207 Association Response, SN-412, FN-0, Flags 208 Association Response, SN-412, FN-0, Flags 209 K 201	Current Curren	NSDU NSDU NSDU NSDU NSDU NSDU NSDU NSDU
 AiroPeek/OmniPeek encapsulated IEE 802.11 radio information IEEE 802.11 Probe Request, Flags: IEEE 802.11 wireless LAN 	E 802.11 C	+ - 6 6	C. Kleen landunge (geoCate (Kommelli/Kreshart (decade as or OK Save Cancel Help	

Lista de bugs e aprimoramentos relacionados a esse recurso:



ID de bug da Cisco CSCvm09015



rastreamento de cliente mostra muitos ICMP_other com número de sequência nulo

ID de bug da Cisco CSCvm02676



O rastreamento de cliente do AP COS não captura pacotes de webauth

ID de bug da Cisco CSCvm02613



A saída remota de rastreamento de cliente AP COS não funciona

ID de bug da Cisco <u>CSCvm00855</u>



Números SEQ de rastreamento de cliente inconsistentes

Controle o rastreamento do AP Client a partir do 9800 WLC

Você pode configurar vários APs para fazer um rastreamento de cliente de rádio e acioná-lo a partir do

Etapa 1. Configurar um perfil de rastreamento de AP que defina qual tráfego capturar

config term wireless profile ap trace

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

Etapa 2. Adicione o perfil de rastreamento de AP a um perfil de junção de AP usado pelos APs que você direciona.

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

Certifique-se de que esse perfil de ingresso no aplicativo seja aplicado a uma marca de site usada por seus APs de destino

Etapa 4 Disparar início/parada

ap trace client start ap

client all/

ap trace client stop ap

client all/

client all/

ap trace client stop site

client all/

Comandos de verificação:

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

Pacote de depuração do cliente no AP

Em vez de coletar uma depuração/captura de rádio, pode ser mais fácil usar o recurso de pacote de depuração de cliente se você estiver depurando um ou mais clientes específicos.

Etapa 1. Identifique o cliente cujos problemas você deseja solucionar.

9164#show dot11 clients

Total dot11 clients	5:6						
Client MAC	Slot ID	WLAN ID	AID	WLAN Name	RSS	[Maxrate	is_wgb_wired is_
mld_sta							
52:1E:34:C9:D6:F3	1	2	35	MySSID	-62	M7	No
No							
80:A9:97:2C:DC:6E	1	2	34	MySSID	-47	MCS112SS	No
No							
E8:D8:D1:1F:71:F3	0	2	35	MySSID	-62	M7	No
No							
6A:E4:06:E7:AB:E1	1	2	33	MySSID	-44	MCS112SS	No
No							
00:1D:63:70:AC:23	0	2	33	MySSID	-56	M7	No
No							
68:72:C3:FD:17:F5	0	2	34	MySSID	-53	M15	No
No							

Etapa 2. Inicie a depuração para um ou mais endereços MAC do cliente

9164#debug client-bundle start debug 80:A9:97:2C:DC:6E WORD

Por padrão, nada será impresso na tela. Você pode habilitar o monitor de terminal e ver as depurações sendo impressas ao vivo, mas lembre-se de que isso tornará o terminal muito difícil de usar. Não é necessário imprimir as depurações no terminal para coletar o pacote.

Etapa 3. Você deve parar o pacote de depuração antes de carregar a saída dele:

debug client-bundle start debug 80:A9:97:2C:DC:6E

Etapa 4. Carregue o pacote em um servidor FTP ou SCP (como lembrete, a WLC pode atuar como servidor SCP)

```
9164#debug client-bundle upload tftp 192.168.129.29 80:a9:97:2c:dc:6e
2024-09-04 11:58:48 Creating client bundle, please wait...
2024-09-04 11:59:01 Client bundle file 9164-_client_bundle.17.15.1.6.20240904.115848.tgz created.
2024-09-04 11:59:01 TFTP uploading...
Successful file transfer:
9164_client_bundle.17.15.1.6.20240904.115848.tgz
```

9164#

O pacote TGZ contém 4 arquivos:

- · 2 contendo comandos show relativos aos rádios e ao cliente
- 1 sobre a depuração real (que é exibida no terminal se você usar o termo mon)
- 1 contendo syslogs

APs Catalyst 91xx em modo farejador

Os novos Catalyst 9115, 9117, 9120 e 9130 podem ser configurados no modo farejador. O procedimento é semelhante aos modelos de AP anteriores.

	Configuration * > Wireless * > Access Points	Edit AP	
		General Interfaces High Availability	Inventory Advanced
ashboard	 All Access Points 	General	Version
onitoring >	Number of AP(s): 4	AP Name* APC4F7.D54C.E770	Primary Software Version 16.12.3.13
onfiguration >	AP Name v AP Model v Slots v Status Address	Location* default location	Predownloaded Status N/A
dministration >	AP700B.98E1.3DEC AIR-AP3802I- 1-K9 2 9 192.168.1.83	Base Radio MAC c064.e422.1780	Predownloaded Version N/A
oubleshooting	AP0CD0.F894.46E4 C9117AXI-B 2 9192.168.1.95	Ethemet MAC c417.d54c.e77c	Next Retry Time N/A
, and a start of the start of t	APb4de.318b.fee0 AIR-	Admin Status	Boot Version 1.1.2.4
	APC4F7.D54C E77C C9120AXI-B 2 9 192.168.1.82	AP Mode Sniffer	10S Version 16.12.3.13
	i4 4 1 ⊯ 10 • Items per page	Operation Status Repostered	Mini IOS Version 0.0.0.0
	> 5 GHz Radios	Fabric Status Disabled	IP Config
	S. and Sectors	LED State	CAPWAP Preferred Mode IPv4
	2.4 GHz Radios	LED Brightness	DHCP IPv4 Address 192.168.1.82
	> Dual-Band Radios	CleanAir NSI Key	Static IP (IPv4/IPv6)
	> Country	Tags	Time Statistics
	> LSC Provision	Policy FlexPolicy	Vp Time 0 days +22 hrs +58 mins +49 secs
		Site TiagoOfficeSite	•

Dashboard All Access Points Number of AP(s): 4. Configure Detail Administration Troubleshooting A mane AP Model Stors Stors Status P dotress Administration Troubleshooting A GCMF2 DSGC 7/2 C 9120A0-B 2 192.168.1.95 Artenna A Artenna B Artenna C Artenna D Artenna D Artenna D Artenna D Stiffer Channel Assignment Stiffer Channel B Stiffer IP* 192.188.180 Stiffer IP* 192.188.180 Stiffer IP* 192.188.180 Stiffer IP* 192.188.180 Stiffer IP* 192.188.180 Stiffer IP* 192.188.180		Configuration * > W	fireless * > Ac	cess Points		Edit Radios 2.4 GHz B	and			
Dashboard All Access Points Monitoring Configuration Administration Administration <th></th> <th></th> <th></th> <th></th> <th></th> <th>Configure Detail</th> <th></th> <th></th> <th></th> <th></th>						Configure Detail				
Monitoring Monitoring <td>Dashboard</td> <td>Y All Access P</td> <td>oints</td> <td></td> <td></td> <td>Admin Status</td> <td>ENABLED</td> <td>Assignment Method</td> <td>Global 🔹</td> <td></td>	Dashboard	Y All Access P	oints			Admin Status	ENABLED	Assignment Method	Global 🔹	
Configuration Administration Administration Aproposed set: 1.30C C APCODO Rest 4.64: Option: 1.100 APCOD Rest 4.64: Option: 1.100 APCOD Rest 4.64: Option: 1.100 Option: 1.100 APCOD APCODO: 1.100 APCODO: 1.100 APCODO: 1.100 APCODO: 1.100 APCODO: 1.100 <) Monitoring	Number of AP(s): 4				CleanAir Admin Status		Tx Power Level Assignme	nt	
Administration Troubleshooting APOCDD F884 4EE4 APOCDD F884 4EE4 C9117AX0-B 2 0 192.168.183 APOC402 7029-1- 2 0 192.168.183 Artenna A Artenna A Artenna A Artenna A Artenna C Artenna C Artenna C Artenna C Artenna Gain 10 Sniffer Channel Assignment Frable Sniffing Sniffer Channel Sniffer Channel Sniffer Channel Sniffer Channel Sniffer IP* Sniffer Steten Noted Sniffer Steten Sniffer IP* Sniffer Steten Sniffer Steten Sniffe	Configuration >	AP Name	AP Model ~	Admin Slots v Status	- IP	Antenna Parameters		Current Tx Power Level		
AP0CD0.F894.46E4 C9117AU-B 2 192.168.1.95 Artenna A Antenna A AP0-469.318b.16e0 AIR- CAP3702H-2 192.168.1.95 AP0-477.D54C E77C C9120A0-B 2 192.168.1.82 Artenna B ✓ AP0-469.318b.16e0 Antenna C AP0-477.D54C E77C C9120A0-B 2 192.168.1.82 Artenna C ✓ Artenna Gain 10 Stiffer Channel Assignment Enable Sniffing Sniffer Channel 6 AP100B SEE1.30EC 0 0027.e336.44a0	Administration >	AP70DB.98E1.3DEC	AIR-AP38021- 1-K9	2 0	192.168.1.83	Antenna Type	Internal +	Assignment Method	Global	
APD-4dei: 318D-5ee0 APD-4dei: 318D-5ee0 Antenna B Antenna C Antenna D Antenna Gain 10 Sniffer Channel Assignment Enable: Sniffing Sniffer IP* 192:168.1:00 Sniffer IP* 1	Troubleshooting	AP0CD0 F894 46E4	C9117AXI-B	2	192.168.1.95	Antenna A				
APC4F7.D54C E77C 0120A00-B 2 0192.168.1.82 Attenna C Attenna D Attenna D Attenna Gain 10 5 GHz Radios Number of AP(s): 4 AP Name Slot No Base Radio MAC Admin St AP(0027.e336.4da0)		APb4de.318b.fee0	AIR- CAP37021-1-	2 0	192.168.1.79	Antenna B				
Antenna D C Antenna D C Antenna Gain 10 Sniffer Channel Assignment Enable Sniffing C Sniffer Channel 6 Sniffer IP* 192.168.1.100 Sniffer IP* 192.168.1.100		APC4F7.D54C.E77C	C9120AXI-B	2 0	192.168.1.82	Antenna C				
> 5 GHz Radios Antenna Gain 10 > 2.4 GHz Radios Sniffer Channel Assignment Number of AP(s): 4 Enable Sniffing AP Name Stot No Base Radio MAC Admin St AP70028 SEE1.3DEC 0 0027.e336.4440 Sniffer IP*		14 4 1 F	10 🖌 items	per page		Antenna D				
Source Source Source Source Source Source Number of AP(s): 4 Enable Sniffing AP Name Slot No						Anterina Gain	10			
• 2.4 GHz Radios Enable Sniffing Image: Channel Number of AP(s): 4 Sniff Channel 6 AP Name Slot No Base Radio MAC Admin St. AP70DB 39E1.3DEC 0 0027.e336.4440 Sniffer IP* 192.168.1.100		> 5 GHz Radio	S			Sniffer Channel Assign	ment			
Number of AP(s): 4 Sniff Channel 6 AP Name Slot No Base Radio MAC Admin St. Sniff Channel 6 AP Name Slot No Base Radio MAC Admin St. Sniff Channel 6 AP Name Slot No Base Radio MAC Admin St. Sniff Channel 6 AP70DB SBE1.3DEC 0 0027.e336.4da0 Sniff Channel Fabric RD Status Valid	한 것이 집	💙 2.4 GHz Rad	ios			Enable Sniffing				
AP Name Stot No. Base Radio MAC Admin St Sniffer IP* 192.168.1.100 AP70DB.96E1.3DE 0 0027.938.6.4da0 O Sniffer IP Sniffer IP Sniffer IP 192.168.1.100		Number of AP(s): 4				Sniff Channel	6 🔹	0		
AP70DB.98E1.3DEC 0 0027.e336.4da0		AP Name	- Slot No	- Base Radio MAC	 Admin St 	Sniffer IP*	192.168.1.100	22 		
Solider D Status		AP70DB.98E1.3DEC	0	0027.e336.4da0	۲					
APGCD0.F894.46E4 0 0cd0.897.03e0 O Grinter in Status Valid		AP0CD0.F894.46E4	0	0cd0.f897.03e0	0	Sniffer IP Status	Valid			
AP54de_318b.fee0 0 b4de_31a4.e030 💿		APb4de.318b.fee0	0	b4de.31a4.e030	۲					
APC4F7.054C.E77C 0 c064.e422.1780 C Download Core Dump to bootflash		APC4F7.D54C.E77C	0	c064.e422.1780	Q	Download Core Dump to	bootflash			

*ThinkpadEthernetBlue

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help 🛋 🔳 🧔 😬 🛄 🛣 🗳 🤉 👄 🗢 🕾 🐺 🛓 🚍 🔍 Q. Q. Q. 🖽

udp	.port == 5000					
vo.	Delta	Source	Destination	Lengt Info	Channel	BSS Color
2_	0.032866	SamsungE_08:4c:4a	Cisco_97:03:ef	107 Authentication, SN=37, FN=0, Flags=C	10	0
2	0.000001	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	0
2_	0.001720	Cisco_97:03:ef	SamsungE_08:4c:4a	107 Authentication, SN=0, FN=0, Flags=C	10	0
2	0.000301	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	0
2	0.000791	SamsungE_08:4c:4a	Cisco_97:03:ef	360 Association Request, SN=38, FN=0, Flags=C, SSID=testewlcwlan	10	0
2 <u> </u>	0.000230	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	0
2-	0.004269	Cisco_97:03:ef	SamsungE_08:4c:4a	398 Association Response, SN=1, FN=0, Flags=C	10	0 0x01
2	0.000750	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	0
2_	0.010966	Cisco_97:03:ef	SamsungE_08:4c:4a	221 Key (Message 1 of 4)	10	0
2	0.000001	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	0
2	0.021911	SamsungE_08:4c:4a	Cisco_97:03:ef	342 Key (Message 2 of 4)	10	0
2	0.000002	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	6
2	0.002186	Cisco_97:03:ef	SamsungE_08:4c:4a	391 Key (Message 3 of 4)	10	0
2	0.000935	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	0
2_	0.013829	SamsungE_08:4c:4a	Cisco_97:03:ef	199 Key (Message 4 of 4)	10	0
2	0.000174	192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	10	0
	 > Tag: Vet > Tag: Vet > Tag: HT > Tag: HT > Tag: Ex: > Tag: VH > Tag: VH > Tag: VH > Tag: Mol > Tag: Fa: 	ndor Specific: Microso ndor Specific: Cisco S Capabilities (802.11n Information (802.11n tended Capabilities (8 T Capabilities T Capabilities T Operation bility Domain st BSS Transition	ft Corp.: WMW/WME: Parameter E ystems, Inc.: Aironet Unknown D1.10) D1.10) octets)	lement (44)		
	> Tag: RM	Enabled Canabilities	(5 octate)			
	1061 101					

- ✓ Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)

- HE Operation Parameters: 0x003ff4
 BSS Color Information: 0x01
 Basic HE-MCS and NSS Set: 0xfffc

No Servação: os quadros de dados enviados com taxas de dados WIFI 6 são capturados,

mas, como o peekremote não está atualizado no Wireshark, eles são mostrados como tipo phy 802.11ax a partir de agora. A correção está no Wireshark 3.2.4, em que o Wireshark exibe a taxa de phy correta do wifi6.

Observação: os APs Cisco não podem capturar quadros MU-OFDMA no momento, mas podem capturar os quadros de acionamento (enviados na taxa de dados de gerenciamento) que anunciam uma janela MU-OFDMA. Você já pode inferir que a MU-OFDMA acontece (ou não) e com qual cliente.

Dicas para Troubleshooting

MTU de Caminho

Embora a Path MTU Discovery encontre a MTU ideal para o AP, é possível substituir essas configurações manualmente.

No AireOS 8.10.130 WLC, o comando config ap pmtu disable <ap/all> define uma MTU estática para um ou todos os APs em vez de confiar no mecanismo de descoberta dinâmica.

Para ativar depurações no momento da inicialização

Você pode executar config boot debug capwap para ativar as depurações capwap,DTLS e DHCP na próxima inicialização, antes mesmo de o SO ser inicializado e o prompt ser mostrado.

Você também tem "config boot debug memory xxxx" para várias depurações de memória.

Você pode ver se as depurações de inicialização estão ativadas ou não na próxima reinicialização com "show boot".

Eles podem ser desativados com a adição da palavra-chave disable no final, como "config boot debug capwap disable".

Mecanismo de economia de energia

A economia de energia de um determinado cliente pode ser solucionada com a execução

debug client trace <mac address>

Clientes QoS

Para verificar se as tags de QoS estão aplicadas, você pode executar "debug capwap client qos".

Ele exibe o valor UP de pacotes para clientes sem fio.

Não é filtrável por mac a partir do 8.8 ; solicitação de aprimoramento Cisco bug IDCSCvm08899 <.

labAP#debug capwap client qos

```
[*08/20/2018 09:43:36.3171] chatter: set_qos_up :: SetQosPriority: bridged packet dst: 00:AE:FA:78:36:8
[*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
```

Você também pode verificar a tabela Qos UP to DSCP no AP, bem como a quantidade total de pacotes marcados, modelados e descartados por Qos:

```
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#
```

Quando as políticas de Qos são definidas na WLC e baixadas no AP Flexconnect, você pode verificá-las com :

```
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
                                type:gos client:default
Policy Map platinum-up
   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
```

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

Verificação fora do canal

A depuração da verificação fora do canal do AP pode ser útil ao solucionar problemas de detecção de invasor (para validar se e quando o AP vai em um canal específico para verificar), mas também pode ser útil na solução de problemas de vídeo, em que um fluxo sensível em tempo real obtém interrupções constantes se o recurso "adiamento da verificação fora do canal" não for usado.

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_

Conectividade do cliente

É possível listar os clientes que foram desautenticados pelo ponto de acesso com o carimbo de data/hora do último evento:

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

Na saída anterior, o código de razão é o código de razão de desautenticação, conforme detalhado

neste link :

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

O vap refere-se ao identificador da WLAN dentro do AP (que é diferente do ID da WLAN no !!! da WLC).

Você pode relacioná-lo com outras saídas detalhadas posteriormente, que sempre mencionam o vap de clientes associados.

Você pode ver a lista de IDs de VAP com "show controllers Dot11Radio 0/1 wlan".

Quando os clientes ainda estiverem associados, você poderá obter detalhes sobre sua conexão com:

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

É possível obter muito mais detalhes sobre a entrada do cliente com:

```
LabAP#show client summ
Radio Driver client Summary:
_____
wifi0
[*08/20/2018 11:54:59.5340]
[*08/20/2018 11:54:59.5340] Total STA List Count 0
[*08/20/2018 11:54:59.5340] | NO| MAC|STATE|
[*08/20/2018 11:54:59.5340] ------
wifi1
[*08/20/2018 11:54:59.5357]
[*08/20/2018 11:54:59.5357] Total STA List Count 1
[*08/20/2018 11:54:59.5357] | NO| MAC|STATE|
[*08/20/2018 11:54:59.5357] ------
[*08/20/2018 11:54:59.5357] | 1| 0:ffffffae: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] ------
```

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: _____ mac port state local_client detect_ago associated_ago tx_pkts tx_bytes rx_pkts rx_bytes

Você pode forçar a desconexão de um cliente específico com :

test dot11 client deauthenticate

Os contadores de tráfego podem ser obtidos por cliente com:

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#	

Mais no nível do rádio, muitas informações podem ser obtidas nos "show controllers". Quando você adiciona o endereço mac do cliente, as taxas de dados suportadas, as taxas de dados atuais, os recursos PHY, bem como a quantidade de novas tentativas e txfail, são exibidos:

<#root>

LabAP#show controllers dot11Radio 0 client 00:AE:FA:78:36:89 mac radio vap aid state encr Maxrate is_wgb_wired wgb_mac_addr 00:AE:FA:78:36:89 0 9 1 FWD AES_CCM128 M15 false 00:00:00:00:00:00 Configured rates for client 00:AE:FA:78:36:89 Legacy Rates(Mbps): 11 HT Rates(MCS): M0 M1 M2 M3 M4 M5 M6 M7 M8 M9 M10 M11 M12 M13 M14 M15 VHT Rates: 1SS:M0-7 2SS:M0-7 HT:yes VHT:yes HE:no 40MHz:no 80MHz:no 80+80MHz:no 160MHz:no 11w:no MFP:no 11h:no encrypt_polocy: 4 WMM_MIXED_MODE:no _wmm_enabled:yes qos_capable:yes WME(11e):no short_preamble:yes short_slot_time:no short_hdr:yes SM_dyn:yes short_GI_20M:yes short_GI_40M:no short_GI_80M:yes LDPC:yes AMSDU:yes AMSDU_long:no su_mimo_capable:yes mu_mimo_capable:no is_wgb_wired:no is_wgb:no Additional info for client 00:AE:FA:78:36:89 RSSI: -90 PS : Legacy (Sleeping) Tx Rate: 0 Kbps Rx Rate: 117000 Kbps VHT_TXMAP: 0 CCX Ver: 4 Statistics for client 00:AE:FA:78:36:89 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 8 1 6 1038 1 0 0 31 1 1599 Per TID packet statistics for client 00:AE:FA:78:36:89 Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s) QID Tx Drops Tx Cur Olimit 0 899 460 1 1 144 0 0 1024 1 0 145 0 0 1024 0 0 0 2 0 0 0 0 146 0 0 1024 3 59 0 1024 0 0 0 147 0 4 0 0 0 0 1024 0 0 148 5 0 0 0 0 149 0 0 1024 6 0 0 0 0 150 0 0 1024 7 0 0 0 0 151 0 0 1024 Legacy Rate Statistics: Rx, Tx, Tx-Retries) (Mbps : 0, 0 11 Mbps : 2, 6 Mbps : 0, 9, 0 HT/VHT Rate Statistics: Rx, Rx-Ampdu, Tx, Tx-Ampdu, Tx-Retries) (Rate/SS/Width : 0/1/20 : 4, 4, 0, 0, 0 6/2/20 : 4, 4, 0, 0, 0 7/2/20 : 5, 0, 0, 0 5, webauth done:

Para acompanhar constantemente uma taxa de dados de cliente e/ou valor RSSI, você pode executar "debug dot11 client rate address <mac> " e isso registra essas informações a cada segundo:

LabAP#debug d	dot11 client ra [.]	te 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

Nesta saída, os contadores de pacotes Tx e Rx são pacotes transmitidos no segundo intervalo desde a última impressão, o mesmo para as Tentativas de Tx. No entanto, o RSSI, o SNR e a taxa de dados são os valores do último pacote desse intervalo (e não uma média para todos os pacotes nesse intervalo).

Cenários do Flexconnect

Você pode verificar quais ACLs estão atualmente aplicadas a um cliente em um cenário de préautorização (CWA, por exemplo) ou pós-autorização: 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

Você pode ver os contadores de acertos nas ACLs do Flexconnect habilitando debug flexconnect access-list counter client <cliente MAC>

As execuções subsequentes do comando show client access-list pre-auth/post-auth all <MAC> depois adicionam contadores de acertos para cada entrada da ACL. Isso funciona para todos os tipos de ACLs flex a partir do Cisco IOS® XE 17.13. Em versões anteriores, os mesmos comandos existem, mas somente as ACLs de VLAN têm seus contadores de ocorrências atualizados.

Você pode redefinir os contadores de acerto da ACL com clear counters access-list client <mac>

Sistema de arquivos AP

Os APs COS não permitem listar todo o conteúdo do sistema de arquivos como em plataformas unix.

O comando "show filesystems" fornece detalhes do uso e da distribuição de espaço na partição atual:

O comando "show flash" lista os arquivos principais na flash do AP. Você também pode anexar a palavra-chave syslog ou core para listar essas pastas específicas.

flash		57.5M	372.OK	54.	1M	1%,	/storage
Filesystem		Size	Used Av	 ailab	le le	Use% N	 lounted on
drwxr-xr-x	2 root	root	2176	Apr	15	11:10	syslogs
drwxr-xr-x	3 support	root	224	Jun	30	2017	support
-rw-rr	1 root	root	64	Apr	15	11:11	sensord_CSPRNG1
-rw-rr	1 root	root	64	Apr	15	11:11	sensord_CSPRNG0
-rw-rr	1 root	root	3	Jun	30	2017	rxtx_mode
-rw-rr	1 root	root	4096	Apr	26	09:36	random_seed
-rw-rr	1 root	root	215	Apr	26	09:29	part2_info.ver
-rw-rr	1 root	root	215	Apr	16	11:01	part1_info.ver
drwxr-xr-x	2 root	root	160	Jun	30	2017	lists
-rw-rr	1 root	root	222	Jan	2	2000	last_good_uplink_config
drwxr-xr-x	2 root	root	160	Jun	30	2017	images
drwxr-xr-x	2 root	root	320	Jun	30	2017	dropbear
drwxr-xr-x	2 root	root	160	Jun	30	2017	cores
-rw-rr	1 root	root	2253	Apr	26	09:43	config.wireless
-rw-rr	1 root	root	0	Jun	5	2018	config.oeap
-rw-rr	1 root	root	180	Apr	15	11:10	config.mobexp
-rw-rr	1 root	root	0	Jul	26	2018	config.mesh.dhcp
-rw-rr	1 root	root		Apr	15	11:09	config.local
-rw-rr	1 root	root	21	Apr	26	09:32	config.flex.maroup
-rw-rr	1 root	root	8116	Anr	26	09:32	config.flex
-rw-rr	1 root	root	18	Jun	30	2017	config
-rw-rr	1 root	root	5	Anr	26	09:29	bootloader verify shadow
-rw-rr	1 root	root	1230	Mar	27	13.51	bootloader log
-rw-rr	1 root	root	20	Δnr	26	10.31	bigac]
	4 J	root	6383	Apr	26	11.10	hase capwap of info
drwxr-xr-x	2 TOOL 4 5	root	2016	Anr	27 15	11.10	ap-images
-/w-/-//	2 root	root	160	Mar	13 27	12.52	RELUADED_AI_UIC
-/w-/-//	1 root	root	0 20	Apr	15	11.09	
-/w-/-//	1 root	root	0	Apr	15	11.09	BOOT_COUNT RECEIVE
-rw-rr	1 root	root	0	May	21 15	2010	
total 84	1	weat	0	Max	21	2010	1111
Directory of	/storage/						
ap_2802#snow	Tlasn						
2002#chow	flach						

Armazenar e enviar syslogs

A pasta syslog armazena a saída de syslog de reinicializações anteriores. O comando "show log" mostra apenas syslog desde a última reinicialização.

A cada ciclo de reinicialização, os syslogs são gravados em arquivos incrementais.

A primeira saída após a inicialização inicial é o arquivo 1.0 e um arquivo 1.1 é criado se 1.0 se tornar muito longo. Após a reinicialização, um novo arquivo 2.0 é criado e assim por diante.

Na WLC, você pode configurar o destino Syslog se quiser que seus APs enviem mensagens de syslog unicast para um servidor específico.

Por padrão, os APs enviam seus syslogs para um endereço de broadcast que pode causar uma certa tempestade de broadcast, portanto, assegure-se de configurar um servidor syslog.

O AP envia via syslog por padrão o que for impresso na saída do console.

No Controlador 9800, você pode alterar esses parâmetros no perfil Configuration -> AP Join, em Management.

Edit AP Jo	oin Profile							
General	Client	CAPWAP	AP	Management	Security	ICap	QoS	
Device	User	Credentials	CDP Ir	nterface				
TFTP D	owngrade	1			Teln	et/SSH Co	onfiguration	
IPv4/IPv6	6 Address	[0.0.0.0		Telne	t		
Image Fi	le Name	[Enter File N	lame	SSH			
System	Log				AP C	ore Dump)	
Facility V	/alue	(KERN	•	Enabl	e Core Dum	an 🗌	
Host IPv	4/IPv6 Addr	ess	192.168.1	.12				
Log Trap	Value	(Information	•				
Secured	í	(

Você pode alterar o valor de interceptação de log para também enviar depurações via syslog. Você pode, então, habilitar depurações na CLI do AP e a saída delas é enviada através de mensagens de syslog para seu servidor configurado.



Devido ao bug da Cisco ID <u>CSCvu75017</u> somente quando você define o recurso d

,somente quando você define o recurso de syslog como KERN (o valor padrão), o AP envia mensagens de syslog.

Se você estiver solucionando problemas em que um AP possivelmente perde a conectividade de rede (ou em um WGB, por exemplo), o syslog não será tão confiável quanto nenhuma mensagem será enviada se o AP perder a conectividade de uplink.

Portanto, depender dos arquivos de syslog armazenados na memória flash é uma ótima maneira de depurar e armazenar a saída no próprio AP e depois carregá-la periodicamente mais tarde.

Pacote de suporte AP

Algumas informações de diagnóstico comumente coletadas de vários tipos podem ser disponibilizadas em um único pacote que pode ser carregado de pontos de acesso.

As informações de diagnóstico que podem ser incluídas no pacote são:

- AP show tech
- Syslogs AP
- AP Capwapd Brain logs
- · Logs de inicialização e mensagens do AP
- Arquivos Coredump AP

Para obter o pacote de suporte do AP, você pode acessar a CLI do AP e inserir o comando "copy support-bundle tftp: x.x.x.x".

Depois disso, você pode verificar o arquivo nomeado com o nome do AP anexado a support.apversion.date.time.tgz, como mostrado subsequentemente:

Ao "descompactar" o arquivo, você pode exibir os vários arquivos coletados:

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

Coletar arquivos centrais de AP remotamente

Para coletar arquivos de núcleo de AP remotamente, habilite o dump de núcleo para ser incluído no pacote de suporte e, em seguida, carregue o pacote de suporte do AP ou envie diretamente para o servidor tftp. Os exemplos subsequentes usam o servidor tftp 192.168.1.100.

CLI AireOS

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

GUI do AireOS

cisco	MONITOR WLANS CONTROLLER WIRELESS SE	CURITY MANAGEMENT COMMANDS HE	P EEEDBACK			Sage Configuration E	ing Logout Befresh (ReadWrite) 📢 Home
Wireless	All APs > Details for AP70DB.98E1.3DEC					< Back	Apply
Access Points All APs Direct APs Radios Rections	General Credentials Interfaces High / Regulatory Domains	S02.11bg:-E 802.11a:-I	Intelligent Capture Power Over Ethernet Sett	ings			
802.118/g/n/ax Dual-Band Radios Dual-SG Radios Global Configuration	Country Code Cisco Discovery Protocol AP Group Name	IL (Israel) *	PoE Status Pre-standard 802.3af swi Power Injector State	tches	Full Power		
Advanced	Statistics Timer	180	AP Core Dump				
Mesh AP Group NTP ATF	Rogue Detection 2 Teinet	Global Config •	AP Core Dump TFTP Server IP File Name	192.168.1.100 apCores	Enabled		
RF Profiles	2 SSH NSI Ports State	Global Config * 🖗	File Compression	🗹 Enable			
 FlexConnect ACLs 	TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331)	TCP MSS is Globally Enabled	AP Retransmit Count	ameters	500		
FlexConnect VLAN Templates	LED State	Enable •	AP Retransmit Interval		3		
Network Lists 802.11a/n/ac/ax	LED Brightlevel LED Flash State	6 (1-8) 0 (1-3600)seconds	VLAN Tagging		Enabled		
802.11b/g/n/ax Modia Stream		Disable	Status Disabled				
Application Visibility	USB Module ID Override	USB Module	mDNS Configuration				
Lync Server Country Timers	USB Module Status USB Module Operational State Hyperlocation Configuration	₩ Not Detected	mDNS Snooping		Enabled		
NetflowQoS	2 Enable Hyperiocation Hyperiocation BLE Module	Global Config • D Present	TrustSec Config CMX Services Services Sub-Services	(MY Server In			

CLI do Cisco IOS®

<#root>

eWLC-9800-01(

config

)#ap profile TiagoOffice eWLC-9800-01(

config-

ap

-profile

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

GUI do Cisco IOS®



A partir do Cisco IOS® XE 17.3.1, você tem uma guia Support Bundle e pode baixar o AP SB da GUI da WLC.

Tudo o que ele faz é executar o comando "copy support-bundle" no AP e enviá-lo via SCP para a WLC (porque a WLC pode ser um servidor SCP).

E então você pode baixá-lo do seu navegador:

P780C-	AIR-					Edit AP						
085-49E6	AP2802I- A-K9	2	۲	81.244.9.50	502f.a836	General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle
4	1 + [10 😱 iter	ns per page			Destinatio	n	• This Device	ver	L	ast Export Stat	tus
5 GHz	Radios					Server IP		172.31.46.79	9		State Transfer Mode	
2.4 GH	Iz Radios					Destinatio	on File Path* 0	1			Server IP	
Dual-Band Radios			Usernam	9* 1*			File Path Time of Export					
Countr	У					Start Tra	insfer					
LSC Pr	rovision											

Isso significa que você pode fazer manualmente o mesmo truque em versões de eWLC anteriores à 17.3.1:

Copie o pacote de suporte do AP via SCP para o IP do eWLC se você não tiver um servidor TFTP acessível para o AP.

O eWLC é geralmente alcançável via SSH a partir do AP, então esse é um bom truque para o pré-17.3.

Etapa 1. Ative o SSH no 9800 v17.2.1

Etapa 2. Ative a SCP no Cisco IOS® XE v17.2.1

Este exemplo mostra como configurar a funcionalidade do servidor do SCP. Este exemplo usa um nome de usuário e uma senha definidos localmente:

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

Etapa 3. Use o comando "copy support-bundle" e precisamos especificar o nome de arquivo a ser criado no servidor SCP.

Dica: você pode executar o comando uma vez para obter um nome de arquivo significativo e, em seguida, copiar/colar esse nome de arquivo no comando:

AP70DB.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/				
Creating support bundle, please wait!tar: ./*.tgz: No such file or directory				
tar: error exit delayed from previous errors				
tar: ".tgz: No such file or directory				
tar: error exit delayed from organize errors				
+=== Support file AP70DB.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz created ===+				
Warning: Permanently added '192.168.1.15' (RSA) to the list of known hosts				
Password:				
Connection closed by 192.168.1.15 port 22				
lost connection				
AP70D8.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/AP70D8.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz				
Creating support bundle, please wait!tar: ./*.tgz: No such file or directory				
tar: error exit delayed from previous errors				
tar: *.tgz: No such file or directory				
tar: error exit delayed from previous errors				
+=== Support file AP70D8.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz created ===+				
Password:				
AP70D8.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz	100%	50KB	3.3MB/s	00:00
Connection to 192.168.1.15 closed by remote host.				
AP700B.98E1.3DEC#				

Etapa 4. Em seguida, você pode acessar a GUI do eWLC e obter o arquivo em: Administration > Management > File Manager:



IoT e Bluetooth

Os logs do servidor gRPC podem ser verificados no AP com:

```
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] spaces 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 "
```

A conectividade com o conector do Cisco DNA Spaces pode ser verificada com:

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

Para ver a configuração atual de broadcast BLE do AP:

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

Para ver os resultados verificados:

Unknown	3C:1D:AF:62:EC:EC	88	0	0000D:00H:00M:01S
iBeacon	18:04:ED:04:1C:5F	86	65	0000D:00H:00M:01S
Unknown	18:04:ED:04:1C:5F	78	65	0000D:00H:00M:01S
Unknown	04:45:E5:28:8E:E7	85	65	0000D:00H:00M:01S
Unknown	2D:97:FA:0F:92:9A	91	65	0000D:00H:00M:01S
iBeacon	E0:7D:EA:16:35:35	68	65	0000D:00H:00M:01S
Unknown	E0:7D:EA:16:35:35	68	65	0000D:00H:00M:01S
iBeacon	04:EE:03:53:74:22	45	256	0000D:00H:00M:01S
Unknown	04:EE:03:53:74:22	45	256	0000D:00H:00M:01S
	04:EE:03:53:6A:3A	72	N/A	0000D:00H:00M:01S
Unknown	04:EE:03:53:6A:3A	72	65	0000D:00H:00M:01S
iBeacon	E0:7D:EA:16:35:35	68	65	0000D:00H:00M:01S
Unknown	E0:7D:EA:16:35:35	67	65	0000D:00H:00M:01S
iBeacon	04:EE:03:53:74:22	60	256	0000D:00H:00M:01S
Unknown	04:EE:03:53:74:22	60	256	0000D:00H:00M:01S
Eddystone URL	04:EE:03:53:6A:3A	72	N/A	0000D:00H:00M:01S

Quando o AP atua no modo de gateway BLE avançado onde um aplicativo é implantado, você pode verificar o status do aplicativo IoX com :

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

Você pode se conectar ao aplicativo IOX com esses comandos e, em seguida, monitorar os logs durante a configuração de beacon da tribuna:

```
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

Conclusão

Há muitas ferramentas de solução de problemas disponíveis para nos ajudar na resolução de problemas relacionados aos APs COS.

Este documento lista os mais usados e é atualizado regularmente.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.