COS APのトラブルシューティング

内容
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>パケットトレースのキャプチャ(スニファトレース)</u>
<u>APポートの有線PCAP</u>
<u>手順</u>
<u>コマンドのオプション</u>
<u>フィルタを使用した有線PCAP</u>
<u>無線キャプチャ</u>
<u>手順</u>
<u>確認</u>
<u>その他のオプション</u>
<u>9800 WLCからのAPクライアントトレースの制御</u>
<u>AP上のクライアントデバッグバンドル</u>
<u>スニファモードのAP Catalyst 91xx</u>
<u>トラブルシューティングのヒント</u>
<u>/Хдмтu</u>
<u>ブート時にデバッグを有効にするには</u>
省電力メカニズム
<u>クライアントQoS</u>
オフチャネルスキャン
クライアント接続
<u>Flexconnectのシナリオ</u>
<u>APファイルシステム</u>
<u>syslogの保存と送信</u>
<u>APサポートバンドル</u>
<u>APコアファイルのリモート収集</u>
<u>AireOSのCLI</u>
AireOSのGUI
<u>Cisco IOS®のCLI</u>
<u>Cisco IOS®のGUI</u>
<u>IoTとBluetooth</u>
<u>結論</u>

はじめに

このドキュメントでは、COSオペレーティングシステム(Cheetah OS、Click OS、単にCisco AP OS)を実行するAPで使用可能ないくつかのトラブルシューティングツールについて説明しま す。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントでは、シリーズ2800、3800、1560および4800のAPモデルのようなCOS APと 、新しい11ax AP Catalyst 91xxに焦点を当てています。

このドキュメントでは、AireOS 8.8以降で使用可能な多くの機能に焦点を当てています。また、 Cisco IOS® XE 16.12.2s以降もサポートします。

以前のリリースでの特定の機能のアベイラビリティに関して、コメントがある場合があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

パケットトレースのキャプチャ(スニファトレース)

APポートの有線PCAP

(8.8で使用可能なフィルタを使用した8.7の時点で)APのイーサネットポートでpcapを取得でき ます。CLIで結果をライブで表示するか(集約パケットの詳細のみ)、完全なpcapとしてAPフラ ッシュに保存できます。

有線pcapはイーサネット側(RxとTxの両方)のすべてをキャプチャし、パケットが有線接続され る直前にAP内のタップ点が検出されます。

ただし、キャプチャされるのはAPのCPUプレーントラフィックだけです。これは、APとの間で 送受信されるトラフィック(AP DHCP、AP capwapコントロールトンネルなど)であり、クライ アントトラフィックは表示しません。

サイズは非常に制限されています(最大サイズ制限は5 MB)。そのため、対象のトラフィックの みをキャプチャするようにフィルタを設定する必要がある場合があります。

トラフィックをコピーする前に、「no debug traffic wired ip capture」または単に「undebug all」 を実行してトラフィックキャプチャを停止します(そうしないと、パケットがまだ書き込まれて いるため、コピーは終了しません)。

手順

ステップ1:pcapを起動し、「debug traffic wired ip capture」でトラフィックタイプを選択します。

<#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)

ステップ 2:トラフィックが流れるのを待ってから、コマンド「no debug traffic wired ip capture」または単に「undebug all」を使用してキャプチャを停止します。

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

ステップ3:ファイルをtftp/scpサーバにコピーします。

<#root>

AP70DB.98E1.3DEC#copy pcap

AP70DB.98E1.3DEC_capture.pcap0

ステップ4:これで、Wiresharkでファイルを開くことができます。ファイルはpcap0です。 pcapに変更して、Wiresharkと自動的に関連付けられるようにします。

コマンドのオプション

debug traffic wiredコマンドには、特定のトラフィックのキャプチャに役立つ複数のオプションがあります。

APC4F7.D54C.E77C#debug traffic wired <0-3> wired debug interface number

filter filter packets with tcpdump filter string

ip Enable wired ip traffic dump
tcp Enable wired tcp traffic dump

udp Enable wired udp traffic dum

debugコマンドの最後に「verbose」を追加すると、パケットの16進数ダンプを確認できます。フィルタの幅が十分でない場合は、CLIセッションに短時間で過大な負荷がかかることに注意してく

ださい。

フィルタを使用した有線PCAP

フィルタの形式は、tcpdumpキャプチャフィルタの形式に対応します。

	フィルタの例	説明				
	[「] host 192.168.2.5」	これにより、ホスト192.168.2.5を行き来するパケットだ けを収集するようにパケットキャプチャがフィルタ処理 されます。				
ホスト	「送信元ホスト192.168.2.5」	これにより、192.168.2.5から到達するパケットだけを収 集するようにパケットキャプチャがフィルタリングされ ます。				
	^Γ dst host 192.168.2.5」	これにより、192.168.2.5に向かうパケットだけを収集す るようにパケットキャプチャがフィルタリングされます 。				
	"port 443"	これにより、送信元または宛先がポート443のパケット だけが収集されるようにパケットキャプチャがフィルタ 処理されます。				
ポート	「送信元ポート1055」	これにより、ポート1055を送信元とするトラフィックが キャプチャされます。				
	^Γ dst port 443」	これにより、ポート443宛てのトラフィックがキャプチ ャされます。				

次の例では、出力はコンソールに表示されますが、CAPWAPデータパケットのみを表示するよう にフィルタリングされています。

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#Killed

ファ	アイ	NO)出力	例	:
----	----	----	-----	---	---

Wiresharkでキャプチャを開くには、次の手順を実行します。

pply a display filter <ctrl-></ctrl->			Expression
Delta Source	Destination	Lengt Info	Payload Type Dif
1 0.000000 192.168.1.82	192.168.1.15	651 Application Data	C1
2 0.001525 192.168.1.15	192.168.1.82	123 Application Data	C1
3 8.681152 192.168.1.4	255.255.255.255	305 CAPWAP-Control - Primary Discovery Request[Malformed Packet]	C
4 9.638243 192.168.1.82	192.168.1.15	987 Application Data	C
5 0.001627 192.168.1.15	192.168.1.82	123 Application Data	
6 0.010495 192.108.1.82 7 0.001007 102 168 1 16	192.108.1.15	1/1 Application Data	u a
0.000100/ 192.108.1.15	192.100.1.02	123 Application Data	u a
0 0 000207 192.100.1.02	102 168 1 83	107 Application Data	0
10 28 344341 192 168 1 82	192 168 1 15	123 Application Data	0
11 0.001214 192.168.1.15	192.168.1.82	139 Application Data	0
12 21.065522 192.168.1.82	192,168,1,15	651 Application Data	a
13 0.001215 192.168.1.15	192.168.1.82	123 Application Data	a
rame 1: 651 bytes on wire (5208	bits), 651 bytes captured (5208	sits)	

無線キャプチャ

無線のコントロールプレーンでパケットのキャプチャを有効にできます。パフォーマンスへの影響のため、無線データプレーンではキャプチャできません。

つまり、クライアントのアソシエーションフロー(プローブ、認証、アソシエーション、eap、 arp、dhcpパケット、ipv6制御パケット、icmp、ndp)は表示されますが、接続状態への移行後に クライアントが渡すデータは表示されません。

手順

ステップ1:トラッキング対象クライアントのMACアドレスを追加します。複数のMACアドレス を追加できます。すべてのクライアントに対してコマンドを実行することもできますが、これは 推奨されません。

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. ステップ2:特定のプロトコルのみ、またはサポートされているすべてのプロトコルをログに記録するようにフィルタを設定します。

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

ステップ3:コンソールに出力を表示することを選択します(非同期)。

configure ap client-trace output console-log enable

ステップ4:トレースを開始します。

config ap client-trace start

以下に例を挙げます。

<#root>

APOCD0.F894.46E4#show dot11 clients Total dot11 clients: 1 Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate WGB A8:DB:03:08:4C:4A 1 1 testewlcwlan -41 MCS92SS No 0 APOCD0.F894.46E4#config ap client-trace address add A8:DB:03:08:4C:4A APOCD0.F894.46E4#config ap client-trace filter all Trace ALL filters Trace arp Packets arp assoc Trace assoc Packets auth Trace auth Packets Trace dhcp Packets dhcp Trace eap Packets eap icmp Trace icmp Packets Trace IPv6 Packets ipv6 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

キャプチャを停止するには、次の手順を実行します。

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

確認

クライアントトレースの確認:

<#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	: 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

正常なクライアント接続の例:

Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5351] [1586169921:535099] [APOCDO.F	<pre>P894.4624] [a8:db:03:08:4c:4a]</pre>	<apr0v0> [U:W] DOT11_AUTHENTICATION : (.)</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5352] [1586169921:535224] [APOCDO.E	[894.46E4] [a8:db:03:08:4c:4a]	<apr0vl> [U:W] DOT11 AUTHENTICATION ; (.)</apr0vl>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5361] [1586169921:536158] [APOCDO.E	7894.46E41 [a8:db:03:08:4c:4a]	<apr0v0> [D:W] DOT11 AUTHENTICATION : (.)</apr0v0>
Anr	6 10:45:21 kernel: (+04/05/2020 10:45:21 54161 (1586169921:541598) [APOCDO F	2894 46F41 [a8:db:03:08:4c:4a]	CAREGORIA (U-W) DOTIL ASSOC REQUEST ()
20.0	6 10.45.21 keynal: (+04/06/2020 10.45.21 54411 [150616021.544114] [NB00700 1	1004 46941 [a0:db:02:00:4a14]	CARACTER DOTIL RECOR DECOMPERTY ()
Mor	10.45.21 Refer. ['04/06/2020 10.45.21.25411] [B0010521.554114] [RP0000.1	-004 4(m4) [ab.db.00.00.44-1	
whit	6 10145.21 RETRET: [-04/06/2020 1014521.501] [156169521.50153] [APOCDO.	COMINGENI [abidbidbidbidbidbidbidbidbidbidbidbidbidb	Capitovos [Diw] EAFOD KEIKI i Descrype Oxoz keyinio Oxobab
Apr	6 10:45:21 Kernel: [~04/06/2020 10:45:21.5//8] [1586169921:5//836] [APOCDO.2	(894.46E4) [as:db:03:08:4C:4a]	<aprovos 0x0105<="" 0x02="" :="" [uin]="" descrype="" eapol="" ket.m2="" keyinto="" td=""></aprovos>
apr	6 10:45:21 Kernel: [=04/06/2020 10:45:21.5784] [1586169921:578476] [APOCDO.E	(894.46E4) [asidb:03:08:40:4a]	<aprovos 0x02="" 0x13cb<="" :="" [diw]="" descrype="" eapol_key.m3="" keyinto="" td=""></aprovos>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.5955] [1586169921:595552] [APOCDO.F	F894.46E4] [a8:db:03:08:4c:4a]	<apr0v0> [UIW] EAFOL_KEY.M4 : DescType 0x02 KeyInfo 0x030b</apr0v0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.6003] [1586169921:600341] [APOCDO.F	<pre>[894.46E4] [a8:db:03:08:4c:4a]</pre>	<apr></apr> apr/60> [U:W] DOT11_ACTION : (.)
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.6028] [1586169921:602817] [APOCDO.M	<pre>P894.4624] [a8:db:03:08:4c:4a]</pre>	COVO> [D:W] DOT11 ACTION : (.)
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.6475] [1586169921:647518] [APOCDO.F	1894.46E4] [a8:db:03:08:4c:4	Apr0v0> (U:W) DOT11 ACTION : (.)
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.6475] [1586169921:647594] [APOCDO.F	7894.46E4] [a8:db:03:08:4	<aprovo> [D:W] DOT11 ACTION : (.)</aprovo>
_			
anr	6 10:45:21 kernel: [*04/06/2020 10:45:21.86361 [1586169921:863610] [APOCDO.F	r894.46F41 [a8:db:02 4a]	<pre>capr0v0> (U:W) DHCP DISCOVER : Transid 0xa38c01d6</pre>
2mm	6 10:45:21 kernel: (*04/06/2020 10:45:21 86361 (1586168821.863644) [ABO(TO B	1004 46941 [a0.d]	(app/10) [U.C] DECE DISCOURD : Trapatd 0xa28c01df
here	C 10.45.31 hereal [04/06/2020 10.45.31 0637] [1506163031 063703 [herear	P004 46#41 [a010 140.4a]	Capitorios [Dic] Dich Discours : Transit Okasesidide
whi	6 1014121 KEINEI: [-04/06/2020 1014121.863/] [1561695211665/00] [APOCDO.		Capitovo (of c) back biscovek i Hansid Casscolde
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.863/] [1586169921:863/31] [APOCDO.F	1894.46E4 (US:4c:4a)	<aprovos :="" [u:c]="" dhcp="" discover="" td="" transid="" uxasecuide<=""></aprovos>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8637] [1586169921:863741] [APOCDO.E	[894.4] [3:08:4c: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.F	7894 0:03:08:4c:4a]	<nsscapwap0> [U:E] DHCP_DISCOVER : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8676] [1586169921:867627] [APOCDO	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] [APOP	3:db:03:08:4c:4a]	<pre><nsscapwap0> [D:C] DHCP OFFER : TransId 0xa38c01d6</nsscapwap0></pre>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.8677] [1586169921:867709] [2	[a8:db:03:08:4c:4a]	<pre><nsscapwap0> [D:C] DHCP OFFER : TransId 0xa38c01d6</nsscapwap0></pre>
Apr	6 10:45:21 kernel: [*04/06/2020 10:45:21.86771 [1586169921:867740]	[a8:db:03:08:4c:4a]	<apr0v0> [D:W] DHCP OFFER : Transid 0xa38c01d6</apr0v0>
anr	6 10:45:21 kernel: [*04/06/2020 10:45:21.86841 [1586169921:868	241 [a8:db:03:08:4c:4a]	<pre>spascapwap0> [D:E] DHCP OFFEB : TransId 0xa38c01d6</pre>
anr	6 10-45-21 kernel: [*04/06/2020 10-45-21 86851 [1586169921-	46E41 [a8:db:03:08:4c:4a]	<pre>cnascanwan0> [D.C] DBCP OFFER : TransId 0xa38c01d6</pre>
3mm	6 10:45:20 1 1 10:0000000 10 10 00 00000 10 00000		CONSCIENCE DECE OFFER . Transid Ora38c01d6
2 mar	6 10 4	02:09:40:40]	Canada (D.M. DACD OFFER , Transfel Que 2000146
apr.	(14) II . Imlink packet (from alient	- 03:00:40:4a)	Capitorio (M.M.) DECE OFFICE . THERE I descended
whr	0 - Uplink packet (from citen)	L) 03:08:40:4a)	caprovos [otw] bhcp kroutsi : iransid oxasecolde
apr	6 10	J3:08:40:48]	<aprovos :="" [0:0]="" dhcp_request="" oxassooide<="" td="" transid=""></aprovos>
Apr	1. D - Downlink packet (to client	D3:08:4c:4a]	<apr0v0> [U:C] DHCP_REQUEST : TransId 0xa38c01d6</apr0v0>
Apr	and b boundering packet (to effent		<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	610 E modulo Ethernet driver	D3:08:4c:4a]	<nsscapwap0> [D:C] DHCP ACK : TransId 0xa38c01d6</nsscapwap0>
Apr	6 10 E - MODULE ELNEINEL GILVEL	D3:08:4c:4a1	<pre><nsscapwap0> [D:C] DHCP ACK : TransId 0xa38c01d6</nsscapwap0></pre>
Apr	6 10	03:08:4c:4a1	<aprovo> (D:W) DHCP ACK : Transid 0xa38c01d6</aprovo>
Zne	in C - module Click	03:08:40:40]	cnescanyan() [D:F] DHCP ACK : Tranald Ova38c01d6
Page 1	C MODULE CLICK	02.00.40.40	Characteristic (D.C.) Dicr_Ack . Attended Construction
MDT		03100140144]	Chascapwapob [Dic] DHCP ACK : Industa Oxasscolade
apr	6 10	D3:08:40:48]	chascapwapus [Dic] bhcP Ack : Iransid uxasecula
apr	6 10	U3:08:40:4aj	<aprovos 0xa38c0ide<="" :="" [d:w]="" dhcp_ack="" td="" transid=""></aprovos>
Apr	6 10:	[03:08:4c:4a]	<pre><apruvu> [U:w] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</apruvu></pre>
Apr	6 10:45	db:03:08:4c:4a]	<pre><apr0v0> [U:C] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</apr0v0></pre>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1611] [1586169922:161177] [APOCDO.F	[894.46E4] [a8:db:03:08:4c:4a]	<pre><apr0v0> [U:C] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</apr0v0></pre>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1612] [1586169922:161213] [APOCDO.F	<pre>r894.46E4] [a8:db:03:08:4c:4a]</pre>	<pre><nsscapwap0> [U:E] ARP_QUERY : Sender 192.168.101.13 TargIp 192.168.101.1</nsscapwap0></pre>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1646] [1586169922:164673] [AF0CD0.F	r894.46E4] [a8:db:03:08:4c:4a]	<pre><nsscapwap0> [D:E] ARP REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:4</nsscapwap0></pre>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164699] [APOCDO.F	(894.46E4) [a8:db:03:08:4c:4a]	<pre><nsscapwap0> [D:C] ARP REPLY : Sender 192.168.101.1 HwAddr 54:7c:69:b7:3f:4</nsscapwap0></pre>
Apr	6 10:45:22 kernel: [*04/06/2020 10:45:22.1647] [1586169922:164722] [APOCDO.F	r894.46E41 [a8:db:03:08:4c:4a]	<pre><nsscapwap0> [D:C] ARP REPLY : Sender 192,168,101,1 HwAddr 54:7c:69:b7:3f:4</nsscapwap0></pre>
anr	6 10:45:22 kernel: [+04/06/2020 10:45:22 1647] [1586169922:164751] [ABOCDO.8	1894.46841 [a8:db:03:08:4c:4a]	<pre><apr0v0> [D:W] ARP REPLY : Sender 192,168,101.1 Hubddr 54:7c:69:b7:35:42</apr0v0></pre>
- dece	I enterinees settementeril Inconstructioni [Mccopoin	The second secon	inter the second s

カッコ内の文字は、フレームが配置された場所(イーサネットの場合はE、ワイヤレスの場合は W、APに対して内部にある場合はClickモジュールの場合はC)とフレームの方向(アップロード またはダウンロード)を理解するのに役立ちます。

これらの文字の意味を示す小さな表を次に示します。

U:アップリンクパケット(クライアントから) D:ダウンリンクパケット(クリックに対して) W:モジュールワイヤレスドライバ E:Module Ethernet driver(モジュールイーサネットドライバ) C-モジュールクリック

その他のオプション

ログを非同期で表示する:

次に、コマンド「show ap client-trace events mac xx:xx:xx:xx:xx:xx」を使用して(または macを「all」に置き換えて)ログを調べることができます。

<#root>

APOCD0.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]	[APOCD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v0></apr0v0>	[D:W]	DOT11_PROBE_RESPONS
[*04/06/2020	10:19:08.075437]	[APOCD0.F894.46E4]	[a8:db:03:08:4c:4a]	<apr0v1></apr0v1>	[U:W]	DOT11_PROBE_REQUEST

パケットを16進形式でダンプする

CLIで16進形式のパケットをダンプできます。

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. SOEl. SDEC#configur	e ap client-trace start
Warning: To recover WLC p	ushed config, meed CAIWAP restart or reload to re-apply the config from WLC
AP70DB.98E1.3DEC#Apr 6 1	3:28:53 kernel: [+04/06/2020 13:28:53.2837] systemd[1]: Starting Lightpd Watcher
Apr 6 10:20:53 kernel: [*04/06/2020 13:28:53.32691 systemd[1]: Started Lighttod Watcher.
configure ap client-trace	output dump address add a8:db:03:00:4c:4a
AP70DB.90E1.3DEC#Apr 6 1	3:29:02 kernel: [*04/06/2020 13:29:02.5997] NAC already exists: index 0
configure an client-trace	autout dump
address Remote/Local d	Client Addresses
enable Enable Trace o	utnut for local dump
APTODE SERI 2000 fimer	an of dispertance of the same
vesting the part the part	a ny siavito tato olapo sany mania
AD2008 SSP1 305CReen fi mus	and characterized wave
AP TODD . FER . SPACECONLLYUL	a b organi-trace output output too
SPROPE ANDI SPROATS AL	
APTODE SERI SPECIAL SU	
AFTODE. SOLL SDECEMPE 6 1	
Apr 6 13:29:27 Kernel: ["Ververzono initerio interiorente parter estative entre receptor entre estative es
Apr & 13:29:27 Fernel: [
Apr 6 13:29:27 Kernel: [·04/06/2020 13/29/27.46493 0010 00 00 00 00 00 00 11 00 00 00 00 0
White P 13:23:24 Keiner: ["04/08/2020 13:39:17.4449] 0020 00 01 13 00 15 03 17 FT 00 00 00 17 mB cd 02 00
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.46491 0030 00 00 37 00 00 00 00 00 00 00 00 00 00 00 00 00
Apr 6 13139137 Sernel1 1	-04/06/2010 13:39:27.4449) 0040 00 01 20 00 00 49 31 21 0E 85 #0 00 00 00 00 00
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4649) 0050 00 00 00 00 3e 00 3e 00 3e 00 00 5e b5 2e b5 00 07 30
Apr 6 13:29:27 kernel: [*04/06/2020 13:23:27.4649] 0060 ed 80 01 30 00 00 27 e3 36 4d a0 a0 db 03 00 4c
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:37.46491 0070 4a 54 70 69 b7 3E 42 40 12 00 00 aa aa 03 00 00
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4650] 0080 00 08 06 00 01 08 00 06 04 00 01 a8 db 03 08 4c
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.46503 0099 4m c0 m8 65
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4740]
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4740) Time:474003us Dir:TH Rate:1 Rsi:=95 Ch:1 Fc:200 Dur:13a a0:db:03:00:4c:4a 00:27:e3:36:4d:a0 54:7c:69:b7:3f:42 Seq:6(6) Info:ARP Retry:0 Len:104 Typesub:20 Tid:q0
Apr 6 13:29:27 kernel: [*04/0€/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 00 00 00 00 0
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.47491 0020 00 01 13 00 15 b3 ff ff 00 00 ml ml 00 50 00 50
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4749] 0030 00 00 5e 8b 2e b6 00 07 3f 58 02 01 00 00 88 02
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.4749; 0040 3a 01 a0 db 03 00 4c 4a 00 27 e3 36 4d a0 54 7c
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.47491 0050 69 b7 3f 42 60 00 00 0m mm mm 03 00 00 00 06
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.47493 0060 00 01 08 00 06 04 00 02 54 7c 69 b7 3f 42 c0 a0
Apr 6 13:29:27 kernel: [*04/06/2020 13:29:27.47491 0070 65 01 m8 db 03 00 4c 4m c0 m0 65 0d 00 00 00
Apr 6 13:25:27 kernel: [*04/06/2020 13:29:27.47491 0080 00 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13:25:27 kernel: [*04/06/2020 13:29:27.47501 0090 00 00 66 66 66 66 66
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.18003
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.1800) Time:180015us Dir:Rx Rate:5 Rasi:=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 13:31:03.18001 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 11 00 00 00 00 0
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.10001 0020 00 01 13 00 15 b3 ff ff 00 00 dc c0 00 ad 00 ad
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03 10001 0030 00 05 m th 27 16 00 02 c2 75 0h 01 14 00 40 00
Apr 6 13:31:03 kernel: [104/06/2020 13:31:03.18001 0040 00 00 ff ff ff ff ff an db 03 08 4c 4a ff ff
Apr 6 13:31:03 kernel: (104/06/2020 13-31-03 10013 0050 ## ## ## 70 27 00 00 01 04 02 04 00 16 32 08
Apr 6 13:31:03 kernel: /	104/06/2020 13:31:03 18011 0050 0e 12 18 24 30 48 60 4e 03 01 01 24 1a 24 00 1b
her d 13.31.03 hernel: f	
how d 12:21:02 hernel: /	
Apr 6 13:31:03 kernel: 1	
Apr d 12:31:03 Refnel: [The second as a second s
Apra - 13:31:03 Kernel: [THE PERSON ADDRESS OF ADDRESS ADDRE
Apr 6 13131103 Merneli ("OK/OK/2010 ISISIIO3.2000] TIME:2001505 DETTH RANE!
Apr e 13:31:03 kernel: [104/06/1020 13/37/03/10000 00 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13:31:03 kernel: [*04/06/1020 13:31:03.2000] 0010 00 00 00 00 00 00 00 00 00 00 00 0
Apr 6 13:31:03 Kernel: (adelade Talarida' Tadal dala da na Ta ma Te El 00 00 #1 #1 00 65 00 #5
Apr 6 13:31:03 kernel: (*04/06/2020 13:31:03.2000] 0030 00 00 5e 8b 2f 16 00 02 c2 96 02 01 00 00 50 00
Apr 6 13:31:03 kernel: (*04/06/2020 13:31:03.2000] 0040 3a 01 a0 db 03 00 4e 4a 00 27 e3 36 4d a0 00 27
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2000] 0050 e3 36 4d m0 e0 65 96 0c 12 10 24 03 01 0d 64 00
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0060 11 11 00 0c 74 65 73 74 65 77 6c 63 77 6c 61 6e
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0070 01 08 82 84 8b 96 0c 12 18 24 02 01 01 07 06 49
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001] 0080 4c 20 01 0d 12 20 01 00 2a 01 00 32 04 30 48 60
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001) 0090 6e 30 14 01
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001]
Apr 6 13:31:03 kernel: [*04/06/2020 13:31:03.2001) Time:20016lus Dir:Tr Rate:1 Rasi:=55 Ch:1 Fo:50 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a1 00:27:e3:36:4d:a1 Seq:65f(1631) Info:DOT11_PROBE_RESPONSE Retry:0 Len:251 Typesub:05
Ang 6 13:31:03 kernel: f	*04/06/2020 13:31:03.20011 0000 00 00 00 00 00 00 00 00 00 00

次に、16進数ダンプを消去してtxt形式で保存し、Wiresharkにインポートできます。

Time:20010us Dir:Rx Rate:1 Rasi:-37 Ch:1 Pc:bD Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 Seq 0000 00 00 00 00 00 00 00 00 00 00 00 0	:1(1) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
Time:43054us Dir:Tx Rate:1 Rssi:-95 Ch:1 Fc:d0 Dur:13a a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 00:27:e3:36:4d:a0 Seq 0000 00 00 00 00 00 00 00 00 00 00 00 0	:66c(1644) Info:DOT11_ACTION Retry:0 Len:54 Typesub:0d
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 0000 00 00 00 00 00 00 00 00 00 00 00 0	:66d(1645) Info:DOT11_AUTHENTICATION Retry:0 Len:65 Typesub:0b
Time:43261us Dir:Rx Rate:1 Rssi:-34 Ch:1 Fc:800 Dur:13a 00:27:e3:36:4d:a0 a8:db:03:08:4c:4a 00:27:e3:36:4d:a0 8e 0000 00 00 00 00 00 00 00 00 00 00 00 0	q:2(2) Info:DOT11_ASSOC_REQUEST Retry:1 Len:220 Typesub:00

Open	Ctrl+O	ET &		
Open Recent				Expression
Merge				
Import from Hex Dump		Ler.		
Close	Ctrl+W		Wireshark - Import From Hex Dump ? ×	
Save	Ctrl+S		Import From	
Save As	Ctrl+Shift+S	Data\Local\Temp	Elas C. Alease/Isotumas/CICCO/11av training/dump avample byt	
File Set		234744 HelpDesk	IBBF161F6_debugs.capture2.pcap (13	MB)
	200	O\00-SRs\SR 688.	Virses: Vi	8)
Export Specified Packet	5	O\00-SRs\SR 688	4956 Bytes)	
Export Packet Butes	Ctrl+Shift+V	O\11ax training\1	O None	
xport PDUs to File	Curtonintex	O\11ax training\1	Transform format and the protect	
vnort TLS Session Kevs		O\11ax training\1	Imestamp format:	
Export Objects		Data\Local\Temp	Direction indication:	
		nloads\AP_trace_	Encapsulation	
Print	Ctrl+P	O\IOS-Images\A	Encapsulation Type: Ethernet	
Quit	Ctrl+Q		No dummy header	
,	apture		O Ethernet Ethertype (hex):	
	using this filter:	Enter a capture filter .	O IPv4 Protocol (dec):	An T
	Local Area Co	onnection* 10	O UDP Source port:	
	Npcap Loop	oack Adapter	O TCP Destination port:	
	Ethernet_yell	owCable	O SCTP Tag:	
	Local Area Co	onnection* 9	O SCTP (Data) PPI:	
	Ethernet 4		O ExportPDU Payload	
	Wi-Fi ThinknadFth	ernetBlue		
	Local Area Co	onnection* 11	Maxim m frame langths	
	Adapter for l	popback traffic captu	maximum iname lengun:	
	Local Area Co	onnection" 2	Import Cancel Help	

出力は非常に大きく、表示されるフレームタイプだけを示し、内部詳細を示すものではないこと を考慮すると、キャプチャアプリケーション(Wiresharkなど)を実行するラップトップにパケッ トキャプチャをリダイレクトするほうが効率的です。

リモートキャプチャ機能を有効にして、Wiresharkを使用して外部デバイスにパケットを送信します。

config ap client-trace output remote enable

このコマンドは、クライアントトレースフィルタによってキャプチャされたすべてのフレームを 192.168.68.68のラップトップに転送し、ポート5000でPEEKREMOTEカプセル化を使用する(ス ニファモードのAPと同様)ことを意味します。

1つの制限は、ターゲットラップトップが、このコマンドを実行するAPと同じサブネット上にあ る必要があることです。ネットワーク内のセキュリティポリシーに合わせてポート番号を変更で きます。

Wiresharkを実行しているラップトップですべてのパケットを受信したら、udp 5000ヘッダーを 右クリックして、decode asを選択し、次の図に示すようにPEEKREMOTEを選択します。

■ 2 • • • • • • • • • • • • • • • • • •		ney		R	- Extression	
Delta Source	Destination	Lengt Info		CeJ 1	Payload Type	
59 0.000000 Samsungt_08:4c:4a 60 0.003416 Cisco_35:4d:a0 61 0.038249 Samsungt_08:4c:4a 62 0.000001 Cisco_36:4d:a0 63 0.0000000 Samsungt_08:4c:4a 64 0.021832 Cisco_36:4d:a0 65 0.000003 Cisco_36:4d:a0 66 0.030097 Samsungt_08:4c:4a 67 0.010088 Cisco_36:4d:a0 68 0.009881 Samsungt_08:4c:4a 69 0.009985 Samsungt_08:4c:4a 69 0.009085 Cisco_36:4d:a0 72 0.002078 Cisco_36:4d:a0 73 0.022078 Cisco_36:4d:a0 74 0.000000 : 73 0.022078 Cisco_36:4d:a0 74 0.000000 1: 74 0.000000 1: 75 0.00000 1: 74 0.000000 1: 75 0.00000 1: 76 0.00000 1: 76 0.00000 0.0.0 76 0.00000 0.0.0 77 0.022078 Cisco_36:4d:a0 78 0.000000 1: 79 0.022055 192.168.101.1 79 0.020028 Cisco_36:4d:a0 70 0.02000 0.0.0 70 0.00000 0.0000 0.0 70 0.00000 0.0.0 70 0.00000 0.0000 0.0 70 0.00000 0.0 70 0.0 70 0.00000 0.0 70 0	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 Colorise Conversation SCTP Follow Copy Protocol Preferences Decode As Show Vacket in New Window SamsungE_08:4c:4a Broadcast Dits), 251 bytes captured (2008 bil 19:10:98:e1:3d:ec), Dst: GoodNiayI_ 19:2.168.1.189, Dst: 19:2.168.1.100 1006, Dst Port: 5688	251 Probe Reguest, SH-572, FH-6, Flags 292 Probe Reguest, SH-578, FH-6, Flags 107 Authentication, SH-578, FH-6, Flag 107 Authentication, SH-578, FH-6, 107 Authentication, SH-579, FH-6, 322 Association Reguest, SH-579, FH-6, 322 Association Reguest, SH-612, FN-6 221 K Wireshark - Decode As 394 K 109 K 109 A 109 port 5000 Integer, base 10 SIGCOM 99 A 428 D 99 A 428 D 109 port 5688 Integer, base 10 SIGCOM 99 A 428 D 109 port 5688 Integer, base 10 SIGCOM 109 por	<pre>C, SSID=testewlcwlan s=C, BI=100, SSID=testewlcwlan s=C Flags=C Current PELSEXEMOTE PEREMOTE PEREMOTE PEREMOTE PEREMOTE PELL2 (timestamp) PCL12 (timestamp, cseID) PCL20 (timestamp, cseID) PEREMOTE PEREM</pre>	2 ×	MSDU MSDU MSDU MSDU MSDU MSDU MSDU MSDU	
AiroPeek/OmniPeek encapsulated IEEE 802.11 radio information IEEE 802.11 Probe Request, Flags: . IEEE 802.11 wireless LAN	: 882.11	+	Crit Kennikanter Konstante Konstante i Konstanti i sikoo OK Save Cancel	<u>de as entries</u> Help		

この機能に関連するバグと機能拡張のリスト:



Cisco Bug ID CSCvm09020 8.8ではクライアントトレースでDNSが見られなくなりました。



クライアントトレースで、ヌルのシーケンス番号を持つ多くのICMP_otherが表示される



AP COS client-traceでWebAuthパケットがキャプチャされない



AP COS client-trace remote出力が機能しない



クライアント – トレースSEQ番号が一致しません

9800 WLCからのAPクライアントトレースの制御

複数のAPを設定して、無線クライアントのトレースを実行し、

ステップ1:キャプチャするトラフィックを定義するAPトレースプロファイルを設定します

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

ステップ2:APトレースプロファイルを、対象のAPで使用されるAP加入プロファイルに追加しま す。

ap profile < ap join profile name> trace

このap加入プロファイルが、ターゲットAPで使用されるサイトタグに適用されていることを確認 します

ステップ4トリガーの開始/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/

確認コマンド:

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

AP上のクライアントデバッグバンドル

特定の1つ以上のクライアントをデバッグする場合、無線のデバッグ/キャプチャを収集するより も、クライアントデバッグバンドル機能を使用する方が簡単な場合があります。

ステップ1:トラブルシューティングするクライアントを特定します。

9164#show dot11 clients

dot11 cliont									
Client MAC	Slot ID	WLAN I	D AI	D WLAN	Name	RSSI	. Maxrate	is_wgb_wired	1S_
a									
34:C9:D6:F3	1		23	5 My	SSID	-62	M7	No	
0				-					
97:2C:DC:6E	1		23	4 My	SSID	-47	MCS112SS	No	
0				-					
D1:1F:71:F3	0		23	5 My	SSID	-62	M7	No	
0				-					
06:E7:AB:E1	1		23	3 My	SSID	-44	MCS112SS	No	
0				-					
63:70:AC:23	0		23	3 My	SSID	-56	M7	No	
0				,					
C3:FD:17:F5	0		23	4 M∨	SSID	-53	M15	No	
0			-	,					
	<pre>dot11 clients Client MAC a 34:C9:D6:F3 o 97:2C:DC:6E o D1:1F:71:F3 o 06:E7:AB:E1 o 63:70:AC:23 o C3:FD:17:F5 o</pre>	dot11 clients: 6 Client MAC Slot ID a 34:C9:D6:F3 1 o 97:2C:DC:6E 1 o D1:1F:71:F3 0 o 06:E7:AB:E1 1 o 63:70:AC:23 0 o C3:FD:17:F5 0 o	dot11 clients: 6 Client MAC Slot ID WLAN I a 34:C9:D6:F3 1 o 97:2C:DC:6E 1 o D1:1F:71:F3 0 o 06:E7:AB:E1 1 o 63:70:AC:23 0 o C3:FD:17:F5 0 o	dot11 clients: 6 Client MAC Slot ID WLAN ID AI a 34:C9:D6:F3 1 2 3 o 97:2C:DC:6E 1 2 3 o D1:1F:71:F3 0 2 3 o 06:E7:AB:E1 1 2 3 o 63:70:AC:23 0 2 3 o C3:FD:17:F5 0 2 3 o	dot11 clients: 6 Client MAC Slot ID WLAN ID AID WLAN a 34:C9:D6:F3 1 2 35 My o 97:2C:DC:6E 1 2 34 My o D1:1F:71:F3 0 2 35 My o 06:E7:AB:E1 1 2 33 My o 63:70:AC:23 0 2 33 My o C3:FD:17:F5 0 2 34 My	dot11 clients: 6 Client MAC Slot ID WLAN ID AID WLAN Name a 34:C9:D6:F3 1 2 35 MySSID o 97:2C:DC:6E 1 2 34 MySSID o D1:1F:71:F3 0 2 35 MySSID o 06:E7:AB:E1 1 2 33 MySSID o 63:70:AC:23 0 2 33 MySSID o C3:FD:17:F5 0 2 34 MySSID o	dot11 clients: 6 Client MAC Slot ID WLAN ID AID WLAN Name RSSI a 34:C9:D6:F3 1 2 35 MySSID -62 o 97:2C:DC:6E 1 2 34 MySSID -47 o D1:1F:71:F3 0 2 35 MySSID -62 o 06:E7:AB:E1 1 2 33 MySSID -62 o 63:70:AC:23 0 2 33 MySSID -56 o C3:FD:17:F5 0 2 34 MySSID -53	dot11 clients: 6 Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate a 34:C9:D6:F3 1 2 35 MySSID -62 M7 o 97:2C:DC:6E 1 2 34 MySSID -47 MCS112SS o D1:1F:71:F3 0 2 35 MySSID -62 M7 o 06:E7:AB:E1 1 2 33 MySSID -62 M7 o 63:70:AC:23 0 2 33 MySSID -56 M7 o C3:FD:17:F5 0 2 34 MySSID -53 M15	dot11 clients: 6 Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired a 34:C9:D6:F3 1 2 35 MySSID -62 M7 No o 97:2C:DC:6E 1 2 34 MySSID -47 MCS112SS No o 0 2 35 MySSID -62 M7 No o 0 2 35 MySSID -47 MCS112SS No o 0 2 35 MySSID -62 M7 No o 0 2 35 MySSID -62 M7 No o 0 2 33 MySSID -62 M7 No o 0 2 33 MySSID -56 M7 No o 0 2 34 MySSID -56 M7 No o 0 2 34 MySSID -53 M15 No

ステップ2:1つ以上のクライアントMACアドレスのデバッグを開始します

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

デフォルトでは、画面には何も表示されません。端末モニタを有効にすると、デバッグ出力をラ イブで表示できますが、この場合は端末が非常に使いにくくなることに注意してください。バン ドルを収集するために、端末にデバッグを出力する必要はありません。

ステップ3:デバッグバンドルの出力をアップロードする前に、デバッグバンドルを停止する必要があります。

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

ステップ 4:バンドルをFTPサーバまたはSCPサーバにアップロードします(WLCがSCPサーバ として動作できることを確認してください)。

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#

TGZバンドルには、次の4つのファイルが含まれます。

- 2無線とクライアントに関するshowコマンドを含む
- ・ 実際のデバッグについて1(term monを実行した場合に端末に表示される)
- syslogを含む1個

スニファモードのAP Catalyst 91xx

新しいCatalyst 9115、9117、9120、および9130は、スニファモードで設定できます。手順は以前のAPモデルと同様です。

	Configuration * > Wireless * > Access Points	Edit AP	×
Dashboard	✓ All Access Points	General Interfaces High Availability Interfaces General	entory Advanced +
Monitoring	Number of AP(s): 4	AP Name* APC4F7.D54C.E77C	Primary Software Version 16.12.3.13
🖏 Configuration 🔹 🔸	AP Name v AP Model v Stots v Status Address	Location* default location	Predownloaded Status N/A
() Administration >	AP7008-9861.3DEC AIR-AP3802I- 1-K9 2 9 192.168.1.83	Base Radio MAC c064.e422.1780	Predownloaded Version N/A
X Troubleshooting	APOCD0.F894.46E4 C9117AXI-B 2 9 192.168.1.95	Ethemet MAC c417.d54c.e77c	Next Retry Time N/A
	APb4de.318b.fee0 AIR-	Admin Status	Boot Version 1.1.2.4
	APC4F7 D54C E77C C9120AXI-B 2 912168.1.82	AP Mode Sniffer 🔹	IOS Version 16.12.3.13
	14 4 1 🕨 10 🔹 Items per page	Operation Status Registered	Mini IOS Version 0.0.0.0
	> 5 GHz Radios	Fabric Status Disabled	IP Config
	> 2.4 GHz Radios	LED State	CAPWAP Preferred Mode IPv4
	Dual-Band Radios	CleanAir NSI Key	Static IP (IPv4/IPv6)
	> Country	Tags	Time Statistics
	> LSC Provision	Policy FlexPolicy V	Up Time 0 days +22 hrs +58 mins +49 secs
		Site TiageOfficeSite .	

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 Band								
Dashboard All Access Points Monitoring Configuration Administration Appedes all Bible of AP(9): 4 Appedes all Bi						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 Option: 1.100 Option: 1.100 Option: 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 Noted Sniffer Steten Noted Sniffer Steten Noted Sniffer Steten Sniffer Steten Noted Sniffer Steten Noted Sniffer Steten Noted Sniffer Steten Noted Sniffer Steten Noted Sniffer Steten Noted Sniffer Steten Sniffer Steten Snif	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* 192,168,1,100 Sniffer IP* 192,168,1,100 APD-4D-4D-4D-4D-4D-4D-4D-4D-4D-4D-4D-4D-4D	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							10	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 Assignment								
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		💙 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	0									
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. 🖽

U	dp.port == 5000			
No.	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	100
2_	0.000001 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
2_	0.001720 Cisco_97:03:ef	SamsungE_08:4c:4a	107 Authentication, SN=0, FN=0, Flags=C	100
2	0.000301 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
2_	0.000791 SamsungE_08:4c:4a	Cisco_97:03:ef	360 Association Request, SN=38, FN=0, Flags=C, SSID=testewlcwlan	100
2_	0.000230 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
2_	0.004269 Cisco_97:03:ef	SamsungE_08:4c:4a	398 Association Response, SN=1, FN=0, Flags=C	100 0×01
2	0.000750 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
2_	0.010966 Cisco_97:03:ef	SamsungE_08:4c:4a	221 Key (Message 1 of 4)	100
2_	0.000001 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
2-	0.021911 Samsungt_08:4c:4a	C15C0_97:03:e+	342 Key (Message 2 of 4)	100
Z-	0.000002 192.168.1.15	192.168.1.100	76 Acknowledgement[Malformed Packet]	100
2-	0.002186 C15c0_97:03;et	Samsungt_08:4c:4a	391 Key (Message 3 of 4)	100
2-	0.000935 192.106.1.15	192.168.1.100	76 Acknowledgement[Matformed Packet]	100
4-	0.013029 Samsungc_00;4C;4a	C15C0_97:03:er	199 key (message 4 of 4)	100
2-	0.000174 192.100.1.15	192.168.1.100	Vo Acknowledgement[Maitormed Packet]	100
	> Tag: HT Information (802.11n C > Tag: Extended Capabilities (8 > Tag: VHT Capabilities > Tag: VHT Capabilities > Tag: NHT Operation > Tag: Rast BSS Transition > Tag: RAST Enabled Capabilities (> Tag: SSS Max Idle Period > Ext Tag: HE Capabilities (IEEE Tag Number: Element ID Exte Ext Tag Number: HE Capabili > HE MAC Capabilities Informm > HE Phy Capabilities Informm > Supported HE-MCS and NSS Sc ~ Rx and Tx MCS Maps <= 80	11.10) octets) (5 octets) E Std 802.11ax/D3.0) nnsion (255) ities (IEEE Std 802.11ax/D3.0) ition: 0x800002100009 ition: 0x800002100009 ition MHz: 0xaaaa	(35)	
	<pre></pre>	0 = Max HE-MCS for 1 SS: Supp = Max HE-MCS for 2 SS: Supp = Max HE-MCS for 3 SS: Supp = Max HE-MCS for 4 SS: Supp = Max HE-MCS for 5 SS: Supp = Max HE-MCS for 6 SS: Supp = Max HE-MCS for 8 SS: Supp = Max HE-MCS for 8 SS: Supp MHz: 0xaaaa d 802.11ax/D3.0) ension (255) on (IEEE Std 802.11ax/D3.0) (3 a003ff4	ort for HE-MCS 0-11 (0x2) ort for HE-MCS 0-11 (0x2) 6)	

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



✿ peekremoteはWiresharkで最新ではないため、現時点では802.11ax phyタイプとして表示されます。修正はWireshark 3.2.4で、Wiresharkに適切なwifi6物理レートが表示されます。

注:Cisco APは、この時点ではMU-OFDMAフレームをキャプチャできませんが、MU-OFDMAウィンドウを通知する(管理データレートで送信される)トリガーフレームをキャ プチャできます。MU-OFDMAが発生している(または発生していない)と、どのクライア ントで発生しているかはすでに推測できます。

トラブルシューティングのヒント

パスMTU

パスMTUディスカバリではAPに最適なMTUが検出されますが、この設定を手動で上書きできま す。

AireOS 8.10.130 WLCでは、コマンドconfig ap pmtu disable <ap/all>により、ダイナミックディ スカバリメカニズムに依存する代わりに、1つまたはすべてのAPのスタティックMTUが設定され ます。

ブート時にデバッグを有効にするには

config boot debug capwapを実行すると、OSが起動してプロンプトが表示される前でも、次回の ブート時にcapwap、DTLS、およびDHCPのデバッグを有効にできます。

また、複数のメモリデバッグ用に「config boot debug memory xxxx」があります。

次回のリブート時に「show boot」コマンドを実行すると、ブートデバッグが有効になっているか どうかを確認できます。

これらは、「config boot debug capwap disable」などのdisableキーワードを最後に追加することで無効にできます。

省電力メカニズム

特定のクライアントの省電力は、次のコマンドを実行してトラブルシューティングできます。

debug client trace <macアドレス>

クライアントQoS

QoSタグが適用されていることを確認するには、「debug capwap client qos」を実行します。 ワイヤレスクライアントのパケットのUP値を表示する。

8.8の時点ではmacフィルタリングはできません。 機能拡張要求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

```
また、AP上のQoSからDSCPまでのテーブル、およびQoSによってマーキング、シェーピング、
廃棄されたパケットの総量も確認できます。
```

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 dscp2dotlp Table Value:
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
LabAP#
```

```
QosポリシーがWLCで定義され、Flexconnect APにダウンロードされると、次のコマンドを使用
してそれらを確認できます。
```

```
AP780C-F085-49E6#show policy-map
2 policymaps
                                        type:qos client:default
Policy Map BWLimitAAAClients
    Class BWLimitAAAClients_AVC_UI_CLASS
      drop
    Class BWLimitAAAClients_ADV_UI_CLASS
      set dscp af41 (34)
    Class class-default
      police rate 5000000 bps (625000Bytes/s)
        conform-action
        exceed-action
Policy Map platinum-up
                                type:qos client:default
    Class cm-dscp-set1-for-up-4
      set dscp af41 (34)
    Class cm-dscp-set2-for-up-4
      set dscp af41 (34)
    Class cm-dscp-for-up-5
      set dscp af41 (34)
    Class cm-dscp-for-up-6
      set dscp ef (46)
   Class cm-dscp-for-up-7
      set dscp ef (46)
    Class class-default
      no actions
```

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 0 0 0 0 2 0 0 Statistics: up down name 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

オフチャネルスキャン

APのオフチャネルスキャンのデバッグは、不正検出のトラブルシューティング(APがスキャン する特定のチャネルにアクセスするかどうかを検証する)に役立つ場合がありますが、「オフチ ャネルスキャンの延期」機能を使用しない場合に機密リアルタイムストリームが絶えず中断され るビデオのトラブルシューティングにも役立ちます。

debug rrm off-channel defer debug rrm off-chanel dbg (starting 17.8.1) debug rrm off-channel schedule debug rrm off-channel voice (starting 17.8.1) debug rrm schedule (starting 17.8.1, debug NDP packet tx) show trace dot_11 channel enable

[*06/11/2020 09:45:38.9530] wcp/rrm_userspace_0/rrm_schedule :: RRMSchedule process_int_duration_timer_ [*06/11/2020 09:45:39.0550] noise measurement channel 5 noise 89 [*06/11/2020 09:45:43.5490] wcp/rrm_userspace_1/rrm_schedule :: RRMSchedule process_int_duration_timer_ [*06/11/2020 09:45:43.6570] noise measurement channel 140 noise 97

クライアント接続

アクセスポイントによって認証解除されたクライアントを、最後のイベントのタイムスタンプとともに一覧表示できます。

LabAP#show dot11 clients						auth			
timestamp)		mac	vap	reason_code
Mon	Aug	20	09:50:5	59 201	B AC	:BC:32:A4	:2C:D3	9	4
Mon	Aug	20	09:52:1	14 201	3 00	:AE:FA:78	:36:89	9	4
Mon	Aua	20	10:31:5	54 201	3 00	:AE:FA:78	:36:89	9	4

上記の出力で、理由コードは次のリンクに記載されている認証解除理由コードです(詳細は後述)。

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

vapは、AP内のWLANのIDを参照します(WLC !!!のWLAN IDとは異なります)。

その後に説明する他の出力と相互に関連付けることができます。出力には、常に関連付けられた クライアントのvapが示されます。

「show controllers Dot11Radio 0/1 wlan」でVAP IDのリストを確認できます。

クライアントがまだ関連付けられている場合は、次のクライアントの接続に関する詳細を取得で きます。

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

クライアントエントリに関する詳細は、次のドキュメントを参照してください。

LabAP#show client summ

Radio Driver client Summary: _____ wifi0 [*08/20/2018 11:54:59.5340] [*08/20/2018 11:54:59.5340] Total STA List Count 0 [*08/20/2018 11:54:59.5340] | NO| MAC|STATE| [*08/20/2018 11:54:59.5340] -----wifi1 [*08/20/2018 11:54:59.5357] [*08/20/2018 11:54:59.5357] Total STA List Count 1 [*08/20/2018 11:54:59.5357] | NO| MAC|STATE| [*08/20/2018 11:54:59.5357] ------[*08/20/2018 11:54:59.5357] | 1| 0:fffffae:ffffffa:78:36:ffffff89| 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| 61 WCP client Summary: _____ mac radio vap aid state encr Maxrate is_wgb_wired wgb_mac_addr 00:AE:FA:78:36:89 1 9 1 FWD AES_CCM128 MCS82SS false 00:00:00:00:00:00 NSS client Summary: _____ Current Count: 3 MAC | OPAQUE | PRI POL | VLAN | BR | TN | QCF | BSS | RADID | MYMAC |

 |F8:0B:CB:E4:7F:41|00000000|
 3|
 0|
 1|
 1|
 0|
 2|
 3|
 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

特定のクライアントを強制的に切断するには、次のコマンドを使用します。

test dot11 client deauthenticate

トラフィックカウンタは、次のコマンドを使用してクライアントごとに取得できます。

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#	

無線レベルの詳細については、「show controllers」で多くの情報を入手できます。クライアント のMACアドレスを追加すると、サポートされているデータレート、現在のデータレート、PHY機 能、および再試行回数とtxfailsが表示されます。

<#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 HE:no 40MHz:no HT:yes VHT:yes 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 0 1024 0 0 0 147 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 : 0, 4, 4, 0, 0 6/2/20 : 4, 4, 0, 0, 0 7/2/20 : 5, 0, 0, 0 5, webauth done:

クライアントデータレートやRSSI値を継続的に追跡するには、「debug dot11 client rate address <mac>」を実行すると、この情報が毎秒ログに記録されます。

LabAP#debug	dot11 client ra	te address 00:AE:F	A:78:36:89					
[*08/20/2018	14:17:28.0928]	MA	C 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

この出力では、TxとRxのパケットカウンタは最後の印刷後2番目のインターバルで送信されたパケットで、Txリトライの場合と同じです。ただし、RSSI、SNR、およびデータレートは、そのインターバルの最後のパケットの値です(そのインターバルのすべてのパケットの平均値ではありません)。

Flexconnectのシナリオ

事前認証(CWAなど)または事後認証シナリオで現在クライアントに適用されているACLを確認 できます。 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

Flexconnect ACLのヒットカウンタを確認するには、debug flexconnect access-list counter client <client MAC>

その後のshow client access-list pre-auth/post-auth all <MAC> の実行では、各ACLエントリのヒッ トカウンタが追加されます。これは、Cisco IOS® XE 17.13以降のすべてのタイプのFlex ACLで 機能します。以前のバージョンでは同じコマンドが存在しますが、ヒットカウンタが更新されて いるのはVLAN ACLだけです。

clear counters access-list client <mac>を使用して、ACLヒットカウンタをリセットできます。

APファイルシステム

COS APでは、UNIXプラットフォームと同様に、ファイルシステムのすべての内容をリストする ことはできません。

コマンド「show filesystems」は、現在のパーティションの領域の使用状況と分布の詳細を表示します。

2802#show filesystems Filesystem Size Used Available Use% Mounted on /dev/ubivol/storage 57.5M 364.0K 54.1M 1% /storage 2802# コマンド「show flash」は、APフラッシュのメインファイルをリストします。syslogまたは coreキーワードを追加して、これらの特定のフォルダをリストすることもできます。

flash		57.5M	372.OK	54.1	M 1%	/storage
Filesystem		Size	Used Av	 ailabl	e Use%	 Mounted on
drwxr-xr-x	2 root	root	2176	Apr 1	5 11:10	syslogs
drwxr-xr-x	3 support	root	224	Jun 3	0 2017	support
-rw-rr	1 root	root	64	Apr 1	5 11:11	sensord_CSPRNG1
-rw-rr	1 root	root	64	Apr 1	5 11:11	sensord_CSPRNG0
-rw-rr	1 root	root	3	Jun 3	0 2017	rxtx_mode
-rw-rr	1 root	root	4096	Apr 2	6 09:36	random_seed
-rw-rr	1 root	root	215	Apr 2	6 09:29	part2_info.ver
-rw-rr	1 root	root	215	Apr 1	6 11:01	part1_info.ver
drwxr-xr-x	2 root	root	160	Jun 3	0 2017	lists
-rw-rr	1 root	root	222	Jan	2 2000	last_good_uplink_config
drwxr-xr-x	2 root	root	160	Jun 3	0 2017	images
drwxr-xr-x	2 root	root	320	Jun 3	0 2017	dropbear
drwxr-xr-x	2 root	root	160	Jun 3	0 2017	cores
-rw-rr	1 root	root	2253	Apr 2	6 09:43	config.wireless
-rw-rr	1 root	root	0	Jun	5 2018	config.oeap
-rw-rr	1 root	root	180	Apr 1	5 11:10	config.mobexp
-rw-rr	1 root	root	0	Jul 2	6 2018	config.mesh.dhcp
-rw-rr	1 root	root	0	Apr 1	5 11:09	config.local
-rw-rr	1 root	root	21	Apr 2	6 09:32	config.flex.maroup
-rw-rr	1 root	root	8116	Apr 2	6 09:32	config.flex
-rw-rr	1 root	root	18	Jun 3	0 2017	config
-rw-rr	1 root	root	5	Apr 2	6 09:29	bootloader verify shadow
-rw-rr	1 root	root	1230	Mar 2	7 13:53	bootloader log
-rw-rr	1 root	root	20	Anr 2	6 10.31	higacl
-rw-rr	1 root	root	6383	Δnr 2	6 09.32	hase canwan cfg info
drwyr-yr-y	4 5	root	2016	Δnr 1	, 11.10	aphilication
drwyr-yr-y	$\frac{1}{2}$ root	root	160	Mar 2	7 12.53	ap_images
-rw-rr	1 root	root	29	Apr 1	5 11.09	
-rw-rr	1 root	root	6	Apr 1	5 11.09	BOOT COUNT reserve
-rw-rr	1 root	root	0	May 2	5 11·00	BOOT COUNT
-rw-rr	1 root	root	0	May 2	1 2018	1111
total 84	/storage/					
ap_2802#snow	Tlash (storage (
n 2802 # chow	flach					

syslogの保存と送信

syslogフォルダには、以前のリブートからのsyslog出力が保存されます。コマンド「show log」 は、最後のリブート以降のsyslogのみを表示します。

リブートが繰り返されるたびに、syslogは差分ファイルに書き込まれます。

artaki# show flash syslogs Directory of /storage/syslogs/ total 128 -rw-r--r-- 1 root root 11963 Jul 6 15:23 1 -rw-r--r-- 1 root root 20406 Jan 1 2000 1.0

 -rw-r--r- 1 root
 root
 313 Jul 6 15:23 1.last_write

 -rw-r--r- 1 root
 root
 20364 Jan 1 2000 1.start

 -rw-r--r- 1 root
 root
 33 Jul 6 15:23 1.watchdog_status

 -rw-r--r- 1 root
 root
 19788 Jul 6 16:46 2

 -rw-r--r- 1 root
 root
 20481 Jul 6 16:46 2

 -rw-r--r- 1 root
 root
 313 Jul 6 16:46 2

 -rw-r--r- 1 root
 root
 20481 Jul 6 16:46 2.last_write

 -rw-r--r- 1 root
 root
 313 Jul 6 16:46 2.last_write

 -rw-r--r- 1 root
 root
 20422 Jul 6 15:23 2.0

 -rw-r--r- 1 root
 root
 20422 Jul 6 15:23 2.start

 -rw-r--r- 1 root
 root
 20422 Jul 6 15:23 2.start

 -rw-r--r- 1 root
 root
 20422 Jul 6 15:23 2.start

 ----- 57.6M
 88.0K
 54.5M
 0% /storage

 artaki# show flash cores
 ----- ----- -----

 Directory of /storage/cores/
 ----- ----- ------

 Filesystem
 Size
 Used Available
 Use% Mounted on

初回ブート後の最初の出力はファイル1.0で、1.0が長くなりすぎた場合はファイル1.1が作成され ます。再起動後に、新しいファイル2.0が作成されます。

APがsyslogメッセージを特定のサーバにユニキャストで送信するように、WLCからsyslog宛先を 設定できます。

デフォルトでは、APはsyslogをブロードキャストアドレスに送信します。ブロードキャストスト ームの原因となる可能性があるため、syslogサーバを設定してください。

APはデフォルトで、コンソール出力に表示されるものはすべてsyslog経由で送信します。

9800コントローラでは、Configuration -> AP Join profileのManagementの下でこれらのパラメー タを変更できます。

Edit AP Jo	oin Profile									
General	Client	CAPWAP	AP	Management	Secu	urity	ICap	QoS		
Device	User	Credentials	CDP Ir	terface						
TFTP D	owngrade					Telnet/	SSH Conf	iguratio	n	
IPv4/IPv6	6 Address		0.0.0.0			Telnet				
Image File Name			Enter File N	ame		SSH			 Image: A start of the start of	
System	Log					AP Cor	e Dump			
Facility V	'alue		KERN	•		Enable C	Core Dump			
Host IPv4	4/IPv6 Addre	ess	192.168.1.	12						
Log Trap	Value		Information	v						
Secured	(i)	C								

Log Trap Valueを変更して、syslog経由でデバッグを送信することもできます。その後、AP CLIでデバッグを有効にすると、デバッグの出力がsyslogメッセージを介して設定済みサーバ (WLC)に送信されます。



syslogファシリティをKERN(デフォルト値)に設定した場合のみ、APはsyslogメッセージを送 信します。

APがネットワーク接続を失う可能性がある問題のトラブルシューティングを行っている場合(またはWGB上にある場合など)、APがアップリンク接続を失うと、syslogはメッセージが送信されないほど信頼性が高くありません。

したがって、フラッシュに保存されたsyslogファイルに依存することは、デバッグを行って出力 をAP自体に保存し、その出力を後で定期的にアップロードする優れた方法です。

APサポートバンドル

さまざまなタイプの一般的に収集される診断情報の一部は、アクセスポイントからアップロード できる単一のバンドルで使用できます。

バンドルに含めることができる診断情報は次のとおりです。

- APのshow tech
- AP syslog
- AP Capwapdブレインログ
- APの起動とメッセージログ
- APコアダンプファイル

APサポートバンドルを入手するには、AP CLIに移動し、コマンド「copy support-bundle tftp: x.x.x.x」を入力します。

その後、次に示すように、support.apversion.date.time.tgzを付加したAP名で名前が付けられたファイルを確認できます(ファイル名の後ろにAP名が付きます)。



ファイルを「untar」すると、収集されたさまざまなファイルを表示できます。

i-Images > APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526

Name A	Date modified	Type	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

APコアファイルのリモート収集

APコアファイルをリモートで収集するには、コアダンプを有効にしてサポートバンドルに含める ようにし、APからサポートバンドルをアップロードするか、またはtftpサーバに直接送信します 。以降の例では、tftpサーバ192.168.1.100を使用しています。

AireOSの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のGUI

cisco	MONITOR WLANS CONTROLLER WIRELESS SEA	curity management commands h	LP <u>F</u> EEDBACK		Saye Configuration Eing Logout Befresh User:admin(ReadWrite) 1 Home
Wireless	All APs > Details for AP70DB.98E1.3DEC]			< Back Apply
Access Points All APs Direct APs * Radios #001 11a/n/ar/ay	General Credentials Interfaces High A Regulatory Domains	S02.11bg:-E 802.11a:-I	Intelligent Capture Power Over Ethernet Settings		
802.11b/g/n/ax Dual-Band Radios Dual-SG Radios Global Configuration	Country Code Cisco Discovery Protocol AP Group Name	IL (Israel)	Poll Status Pre-standard 802.3af switches Power Injector State	Full Power	
Advanced	Statistics Timer	180	AP Core Dump		
Mesh AP Group NTP ATF	Rogue Detection	Global Config Y	AP Core Dump TFTP Server IP 192.168. File Name acCores	Enabled	
RF Profiles FlexConnect Groups	SSH NSI Ports State	Global Config • 14 Global Config • 14	File Compression 🗹 Enable		
FlexConnect ACLs	TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331)	TCP MSS is Globally Enabled	AP Retransmit Count	s 0	
FlexConnect VLAN Templates	LED State	Enable •	AP Retransmit Interval	3	
Network Lists 802.11a/n/ac/ax	LED Rightlevel LED Flash State	8 (1-8) 0 (1-3600)seconds	VLAN Tagging	Enabled	
802.11b/g/n/ax Media Stream		Disable	Status Disabled		
Application Visibility And Control	US8 Module ID Override	USB Module	mDNS Configuration		-2
Lync Server Country Timers	USB Module Status USB Module Operational State Hyperlocation Configuration		mDNS Snooping VLAN List TrustSec	Enabled	
NetflowQoS	2 Enable Hyperiocation Hyperiocation BLE Module	Global Config *]	TrustSec.Config CMX Services Samilary Sub-Samilary CMX Sam		

Cisco IOS®の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®のGUI



Cisco IOS® XE 17.3.1以降にはSupport Bundleタブがあり、WLC GUIからAP SBをダウンロードできます。

実行するのは、APで「copy support-bundle」コマンドを実行して、それをSCP経由でWLCに送 信することだけです(WLCはSCPサーバになる可能性があるためです)。

次に、ブラウザからダウンロードできます。

P780C-	AIR-					Edit AP	Edit AP								
085-49E6	AP2802I- A-K9	2	0	81.244.9.50	502f.a836	General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle			
4	•	10 🔹 item	is per page			Destination	on	• This Device		L	us				
5 GHz Radios 2.4 GHz Radios			Server IP		172.31.46.7	9	State Transfer Mode								
			Destination File Path* 0		1		Server IP								
Dual-Band Radios Country			Usernam Passwore	e* d*			File Path Time of Export								
				Start Tra	ansfer										
LSC Pr	ovision														

つまり、17.3.1より前のリリースのeWLCでも同じ操作を手動で行えます。

APに到達可能なTFTPサーバがない場合は、SCP経由でAPからeWLC IPにサポートバンドルをコ ピーします。

eWLCは通常、APからSSHを介して到達可能であるため、17.3よりも前では有効です。

ステップ1:<u>9800 v17.2.1でSSHを有効にする</u>

ステップ 2: <u>Cisco IOS® XE v17.2.1でSCPを有効にする</u>

次の例は、SCPのサーバ側の機能を設定する方法を示しています。この例では、ローカルに定義 されたユーザ名とパスワードを使用します。

! 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

ステップ3:コマンド「copy support-bundle」を使用して、SCPサーバに作成するファイル名を 指定する必要があります。

ヒント:このコマンドを1回実行すると、意味のあるファイル名を取得できます。次に、そのファ イル名をコマンドにコピーして貼り付けます。

						_
ĺ	AP70DB.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/					
	Creating support bundle, please wait!tar: ./*.tgz: No such file or directory					
	tar: error exit delayed from previous errors					
	tar: *.tgz: No such file or directory					
	tar: error exit delayed from previous errors					
	+=== Support file AP70DB.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz created ===+					
	Warning: Permanently added '192.168.1.15' (RSA) to the list of known hosts.					
	Password:					
	Connection closed by 192.168.1.15 port 22					
	lost connection					
	AP70DB.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/AP70DB.98E1.3DEC_support.17.2.1.11.20200506.110006.tgz					
	Creating support bundle, please wait!tar: ./*.tgz: No such file or directory					
	tar: error exit delayed from previous errors					
	tar: *.tgz: No such file or directory					
	tar: error exit delayed from previous errors					
	+=== Support file AP70D8.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz created ===+					
	Password:					
	AP70DB.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.					
	AP7008.9851.305C#					

ステップ 4:その後、eWLC GUIに移動し、Administration > Management > File Managerでファ イルを取得できます。



IoTとBluetooth

AP上のgRPCサーバログは、次のコマンドでチェックできます。

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	<pre>msg="[DNAS]</pre>	entering stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z"	level=info	<pre>msg="[DNAS]</pre>	exiting stopDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z"	level=info	<pre>msg="[DNAS]</pre>	entering startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z"	level=info	<pre>msg="[DNAS]</pre>	launching token request cycle"
time="2020-04-01T01:36:52Z"	level=info	<pre>msg="[DNAS]</pre>	exiting startDNAspacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z"	level=info	<pre>msg="[DNAS]</pre>	spaces token expiration time 2020-04-02 01:36:52 +00
time="2020-04-01T01:36:52Z"	level=info	msg=" Callin	ng startDNASpacesConn routine "
time="2020-04-01T01:36:52Z"	level=info	<pre>msg="[DNAS]</pre>	Receive Success status"
time="2020-04-01T01:36:52Z"	level=info	<pre>msg="[DNAS]</pre>	Connection not in ready state sleeping for 10 second
time="2020-04-01T01:37:02Z"	level=info	<pre>msg="[DNAS]</pre>	Setup Stream for the gRPC connection"
time="2020-04-01T01:37:02Z"	level=info	<pre>msg="[DNAS]</pre>	Connect RPC Succeeded."
time="2020-04-01T01:37:02Z"	level=info	<pre>msg="[DNAS]</pre>	RX routine got enabled "
time="2020-04-01T01:37:02Z"	level=info	msg="[DNAS]	TX routine got enabled "

Cisco DNA Spacesコネクタへの接続は、次のコマンドで確認できます。

```
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 con	ne	ction detail
Connection State :	R	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

APの現在のBLEブロードキャスト設定を表示するには、次の手順を実行します。

AP# show controllers ioTRadio ble 0 broadcast

BLE Profile Config				
Active profile Profile 0 (iBeacon)	:	v-iBeacon		
UUID	:	000010000000000000000000000000000000000		
Interval (ms)	:	100		
Power (dBm)	:	-21		
Advertised Power (dBm)	:	-65		
Minor	:	0		
Major	:	0		
TxPower byte	:	bfbfbfbfbfbfbfbfbfbfbfbfbf		
Profile 1 (Eddystone UID)				
Namespace (hex)	:	000000000005446089c		
Instance-ID (hex)	:	7f000001f00		
Profile 2 (Eddystone URL)				
URL	:	http://www.		

スキャン結果を表示するには、次の手順を実行します。

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

アプリケーションが導入されている高度なBLEゲートウェイモードでAPが動作している場合は、 次のコマンドを使用してIoXアプリケーションのステータスを確認できます。

AP#show iox applications Total Number of Apps : 1		
App Name	:	cisco_dnas_ble_iox_app
App Ip		192.168.11.2
App State	:	RUNNING
App Token	:	02fb3e98-ac02-4356-95ba-c43e8a1f4217
App Protocol	:	ble
App Grpc Connection	:	Up
Rx Pkts From App		3878345
Tx Pkts To App	:	6460
Tx Pkts To Wlc	:	0
Tx Data Pkts To DNASpaces	:	3866864
Tx Cfg Resp To DNASpaces	:	1
Rx KeepAlive from App	:	11480
Dropped Pkts	:	0
App keepAlive Received On	:	Mar 24 05:56:49

次のコマンドを使用してIOXアプリケーションに接続し、フロアビーコンの設定中にログをモニ タできます(ログはIOXによって異なります)。

```
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

結論

COS APに関連する問題の解決に役立つトラブルシューティングツールは多数あります。

このドキュメントには、最も一般的に使用されるものがリストされており、定期的に更新されています。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。