

COS APのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[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](#)

[手順](#)

[コマンドのオプション](#)

[フィルタを使用した有線PCAP](#)

[無線キャプチャ](#)

[手順](#)

[確認](#)

[その他のオプション](#)

[9800 WLCからのAPクライアントトレースの制御](#)

[AP上のクライアントデバッグバンドル](#)

[スニファモードのAP Catalyst 91xx](#)

[トラブルシューティングのヒント](#)

[バスMTU](#)

[ブート時にデバッグを有効にするには](#)

[省電カメカニズム](#)

[クライアントQoS](#)

[オフチャネルスキャン](#)

[クライアント接続](#)

[Flexconnectのシナリオ](#)

[APファイルシステム](#)

[syslogの保存と送信](#)

[APサポートバンドル](#)

[APコアファイルのリモート収集](#)

[AireOSのCLI](#)

[AireOSのGUI](#)

[Cisco IOS®のCLI](#)

[Cisco IOS®のGUI](#)

[IoTとBluetooth](#)

[結論](#)

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可用性に関して、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（スニファートレース）

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
```

```
tftp 192.168.1.100
```

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

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
ホスト	「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。
	「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。
	「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。
ポート	“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。
	「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。
	「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。

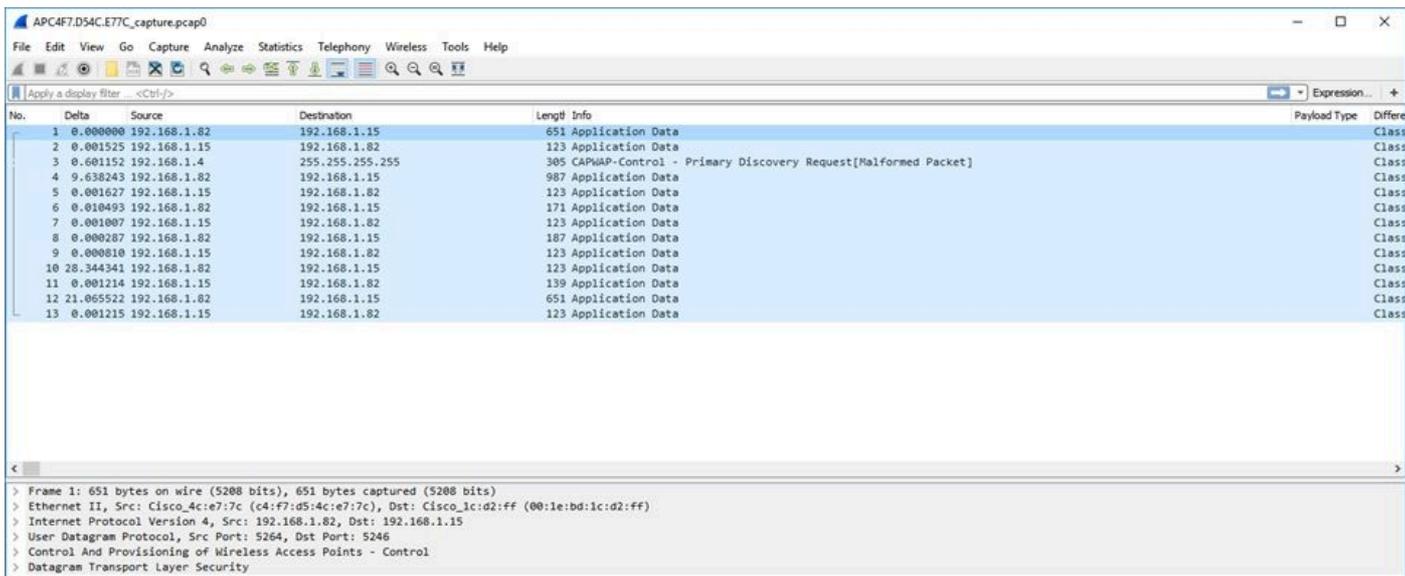
```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246"  
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)  
12:20:50.483125 IP APC4F7-D54C-E77C.lan.5264 > 192.168.1.15.5246: UDP, length 81  
12:20:50.484361 IP 192.168.1.15.5246 > APC4F7-D54C-E77C.lan.5264: UDP,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

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

ファイルの出力例：

```
APC4F7.D54C.E77C#debug traffic wired filter "port 5246" capture
% Writing packets to "/tmp/pcap/APC4F7.D54C.E77C_capture.pcap0"
APC4F7.D54C.E77C#reading from file /dev/click_wired_log, link-type EN10MB (Ethernet)
APC4F7.D54C.E77C#no debug traffic wired filter "port 5246" capture
APC4F7.D54C.E77C#copy pcap APC4F7.D54C.E77C_capture.pcap0 tftp 192.168.1.100
#####
APC4F7.D54C.E77C#
```

Wiresharkでキャプチャを開くには、次の手順を実行します。



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
```

```
0 1 1 testewlclan -41 MCS92SS No
```

```
APOCD0.F894.46E4#config ap client-trace address add
```

```
A8:DB:03:08:4C:4A
```

```
APOCD0.F894.46E4#config ap client-trace filter
```

```
all Trace ALL filters
arp Trace arp Packets
assoc Trace assoc Packets
auth Trace auth Packets
dhcp Trace dhcp Packets
eap Trace eap Packets
icmp Trace icmp Packets
ipv6 Trace IPv6 Packets
ndp Trace ndp Packets
probe Trace probe Packets
```

```
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          : icmpv6
Client Trace Filter          : ndp
Client Trace Filter          : arp

Client Trace Output          : eventbuf
Client Trace Output          : console-log
Client Trace Output          : dump
Client Trace Output          : remote

Remote trace IP              : 192.168.1.100
Remote trace dest port       : 5688
NOTE - Only VIP packets are seen on remote if VIP is enabled

Dump packet length          : 10
Client Trace Inline Monitor   : disable
Client Trace Inline Monitor pkt-attach : disable
```

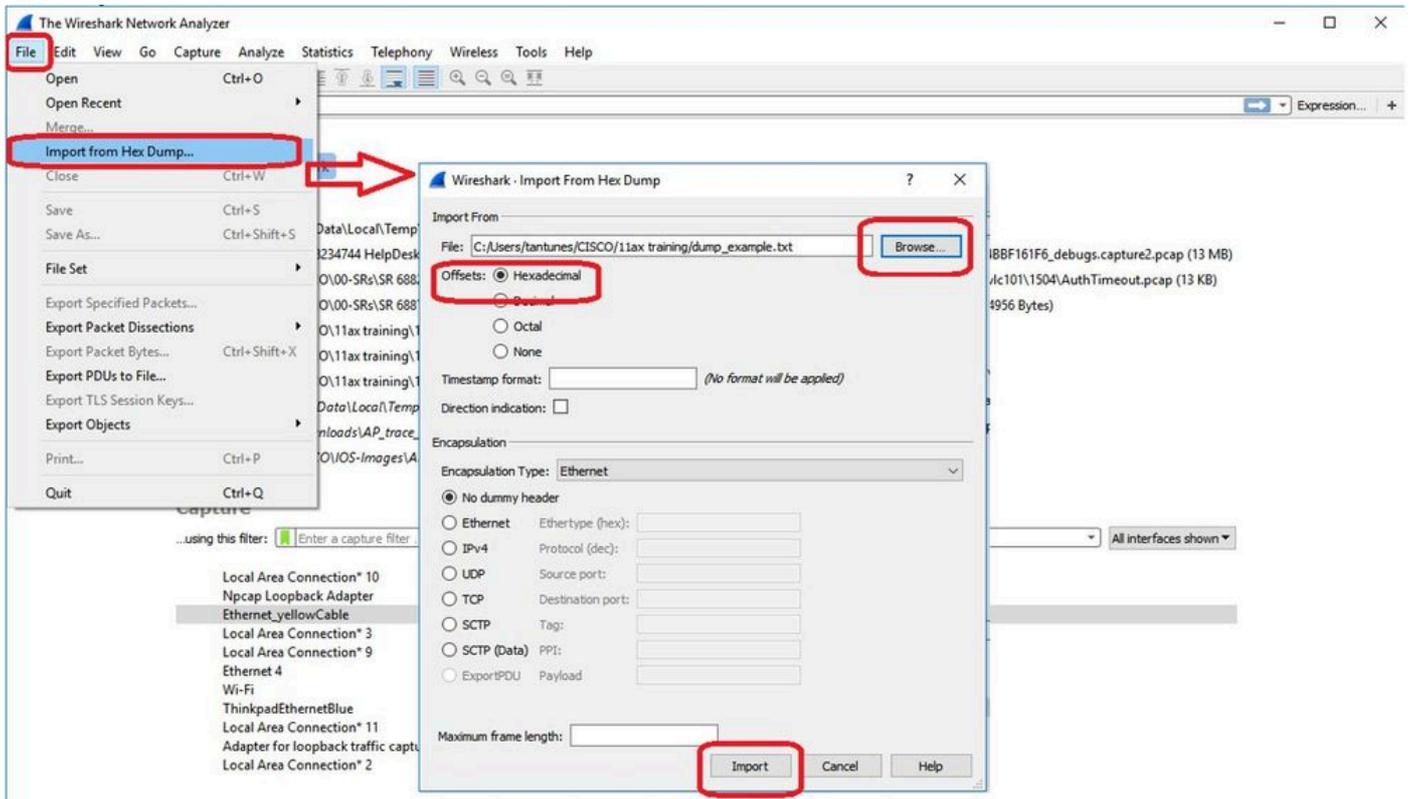
正常なクライアント接続の例：


```
[*04/06/2020 10:11:54.377237] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:11:54.390255] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:11:54.396855] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.416650] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469089] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:54.469157] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921877] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:11:57.921942] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:15:36.123119] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DEAUTHENTICATI
[*04/06/2020 10:15:36.127731] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr1v0> [D:W] DOT11_DISASSOC : (.)
[*04/06/2020 10:17:24.128751] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.128870] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v1> [U:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.129303] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_AUTHENTICATIO
[*04/06/2020 10:17:24.133026] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ASSOC_REQUEST
[*04/06/2020 10:17:24.136095] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ASSOC_RESPONS
[*04/06/2020 10:17:24.138732] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M1 : Desc
[*04/06/2020 10:17:24.257295] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M2 : Desc
[*04/06/2020 10:17:24.258105] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] EAPOL_KEY.M3 : Desc
[*04/06/2020 10:17:24.278937] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] EAPOL_KEY.M4 : Desc
[*04/06/2020 10:17:24.287459] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.301344] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327482] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.327517] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430136] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_ACTION : (.)
[*04/06/2020 10:17:24.430202] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_ACTION : (.)
[*04/06/2020 10:19:08.075326] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [U:W] DOT11_PROBE_REQUEST
[*04/06/2020 10:19:08.075392] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <apr0v0> [D:W] DOT11_PROBE_RESPONS
[*04/06/2020 10:19:08.075437] [APOCD0.F894.46E4] [a8:db:03:08:4c:4a] <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:xx
configure ap client-trace output dump enable x -> Enter the packet dump length value
```

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。

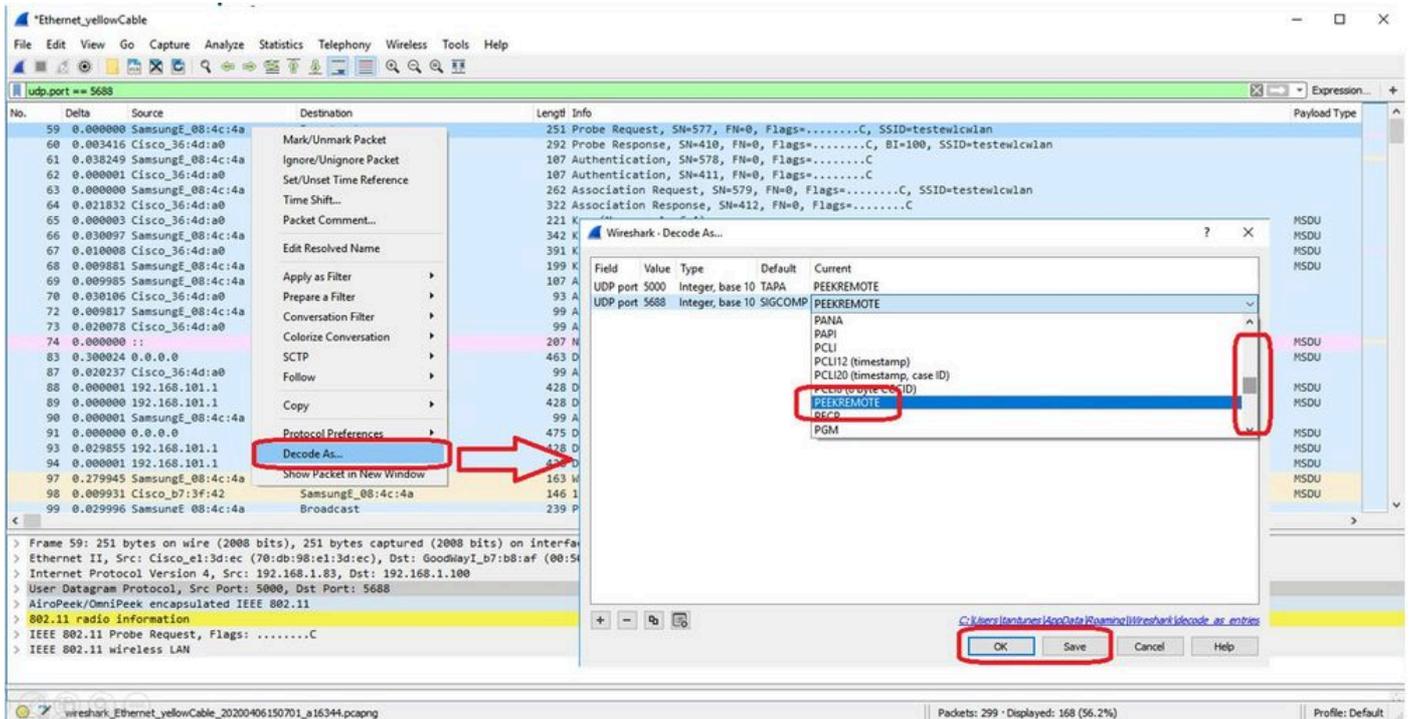
リモートキャプチャ機能を有効にして、Wiresharkを使用して外部デバイスにパケットを送信します。

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

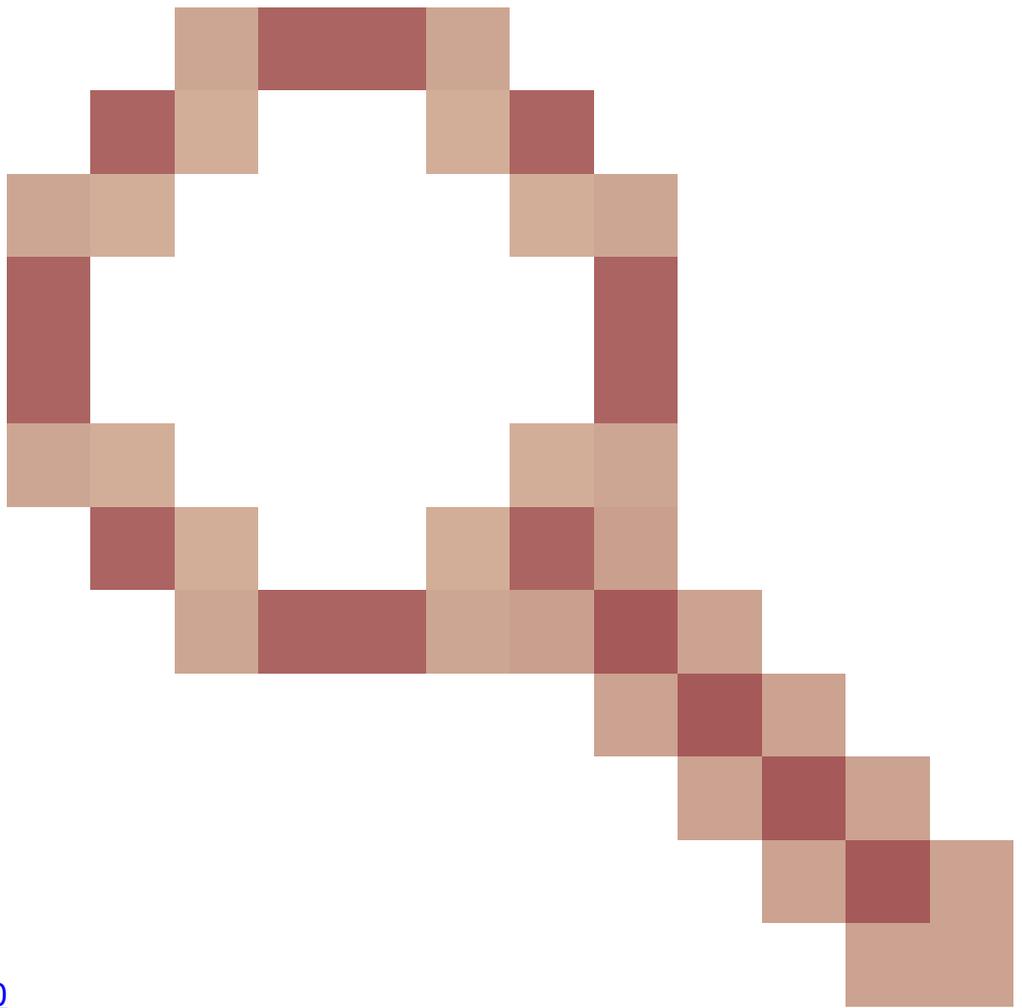
このコマンドは、クライアントトレースフィルタによってキャプチャされたすべてのフレームを 192.168.68.68 のラップトップに転送し、ポート 5000 で PEEKREMOTE カプセル化を使用する (スニファモードの AP と同様) ことを意味します。

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。



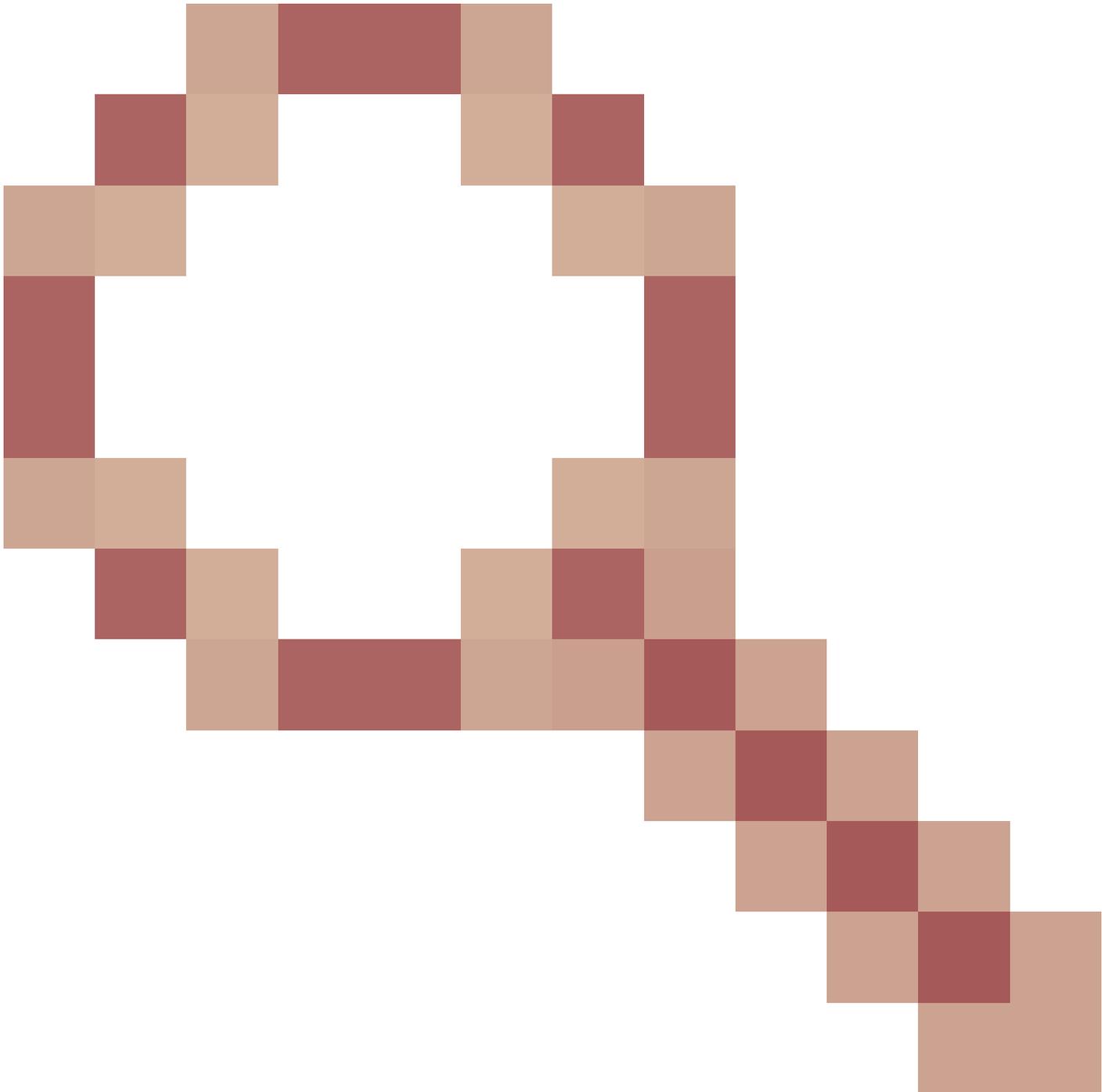
この機能に関連するバグと機能拡張のリスト：



[Cisco Bug ID CSCvm09020](#)

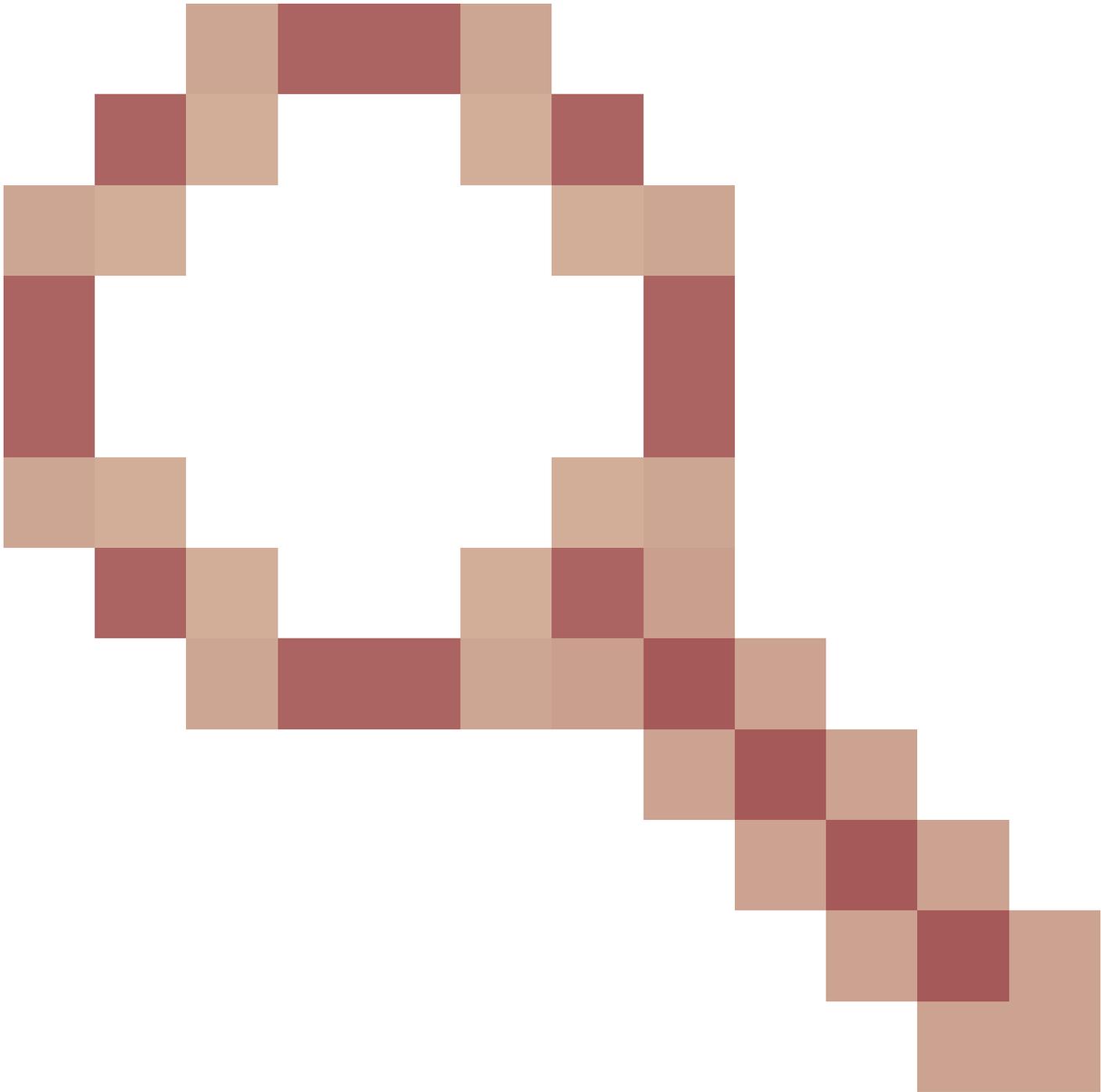
8.8ではクライアントトレースでDNSが見られなくなりました。

[Cisco Bug ID CSCvm09015](#)



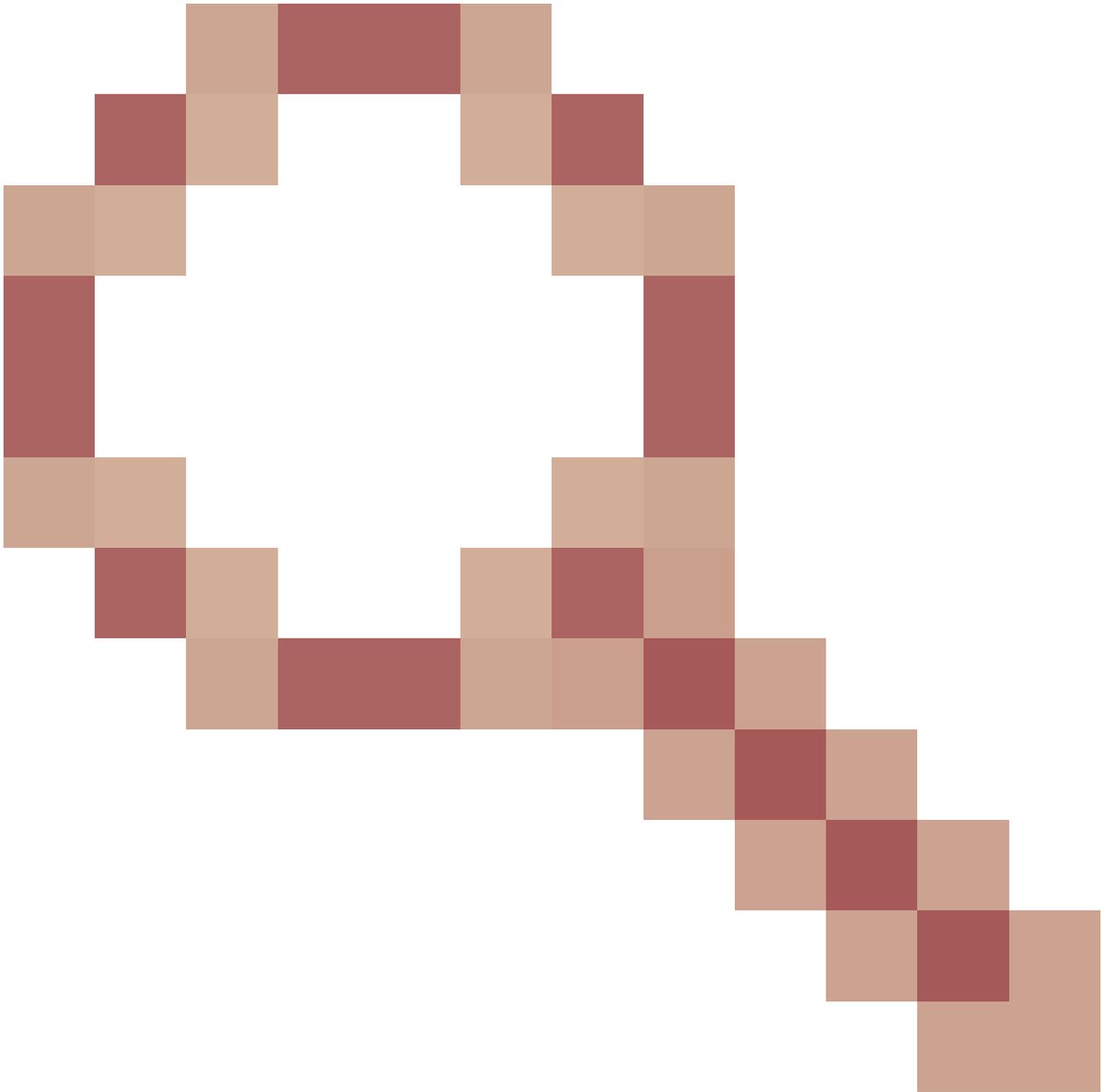
クライアントトレースで、ヌルのシーケンス番号を持つ多くのICMP_otherが表示される

[Cisco Bug ID CSCvm02676](#)



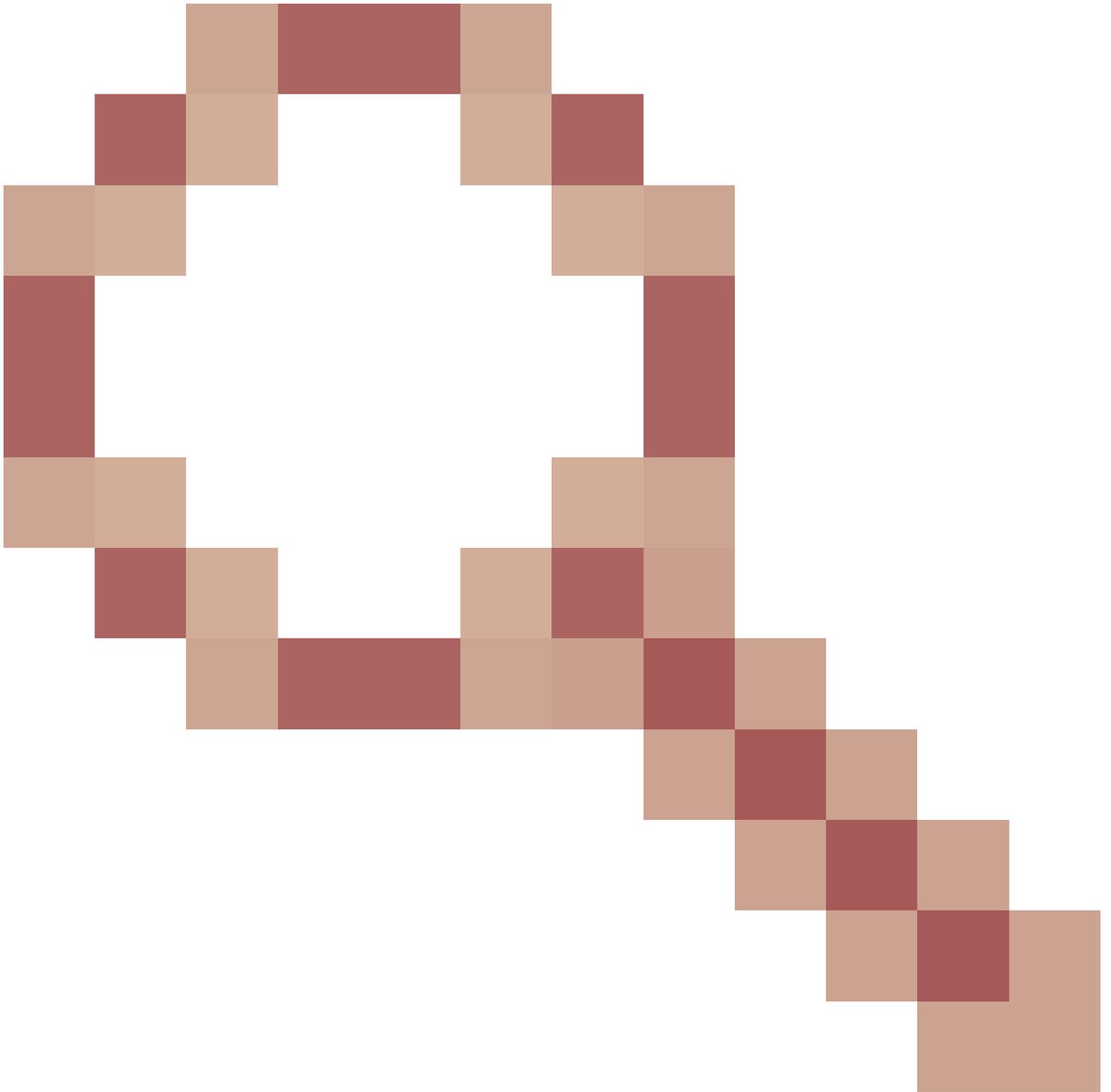
AP COS client-traceでWebAuthパッケージがキャプチャされない

Cisco Bug ID [CSCvm02613](#)



AP COS client-trace remote出力が機能しない

Cisco Bug ID [CSCvm00855](#)



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
```

```
Total dot11 clients: 6
```

Client MAC	Slot	ID	WLAN ID	AID	WLAN Name	RSSI	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									

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。

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. The left sidebar shows navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area is divided into two panes. The left pane, titled 'All Access Points', shows a table of APs with columns for AP Name, AP Model, Slots, Admin Status, and IP Address. The AP 'APC4F7.D54C.E77C' is selected. The right pane, titled 'Edit AP', shows configuration options for the selected AP. The 'AP Mode' dropdown menu is highlighted with a red box and set to 'Sniffer'. Other configuration options include AP Name, Location, Base Radio MAC, Ethernet MAC, Admin Status (ENABLED), Operation Status (Registered), Fabric Status (Disabled), LED State (ENABLED), LED Brightness Level (8), CleanAir (NSL/Kgy), Policy (FlexPolicy), and Site (TiagoOfficeSite). The 'Update & Apply to Device' button is visible at the bottom right.

AP Name	AP Model	Slots	Admin Status	IP Address
AP700B.96E1.3DEC	AIR-AP3802I-I-K9	2	✓	192.168.1.83
AP0CD0.F894.46E4	C9117AXI-B	2	✓	192.168.1.95
APb4de.318b.fee0	AIR-CAP3702I-I-K9	2	✓	192.168.1.79
APC4F7.D54C.E77C	C9120AXI-B	2	✓	192.168.1.82

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 4

AP Name	AP Model	Slots	Admin Status	IP Address
AP70DB.98E1.3DEC	AIR-AP3802I-I-K9	2	✓	192.168.1.83
APCCDD.F894.46E4	C9117AXI-B	2	✓	192.168.1.95
APb4de.318b.fee0	AIR-CAP3702I-I-K9	2	✓	192.168.1.79
APC4F7.D54C.E77C	C9120AXI-B	2	✓	192.168.1.82

5 GHz Radios

2.4 GHz Radios

Number of AP(s): 4

AP Name	Slot No.	Base Radio MAC	Admin Status
AP70DB.98E1.3DEC	0	0027.e336.4da0	✓
APCCDD.F894.46E4	0	0cd0.897.03e0	✓
APb4de.318b.fee0	0	b4de.31a4.e030	✓
APC4F7.D54C.E77C	0	cd64.e422.1780	✓

Edit Radios 2.4 GHz Band

Configure

Admin Status: ENABLED

CleanAir Admin Status: ENABLED

Assignment Method: Global

Tx Power Level Assignment

Antenna Parameters

Antenna Type: Internal

Antenna A:

Antenna B:

Antenna C:

Antenna D:

Antenna Gain: 10

Current Tx Power Level: 1

Assignment Method: Global

Sniffer Channel Assignment

Enable Sniffing:

Sniff Channel: 6

Sniffer IP*: 192.168.1.100

Sniffer IP Status: Valid

Download Core Dump to bootflash

Update & Apply to Device

*ThinkpadEthernetBlue

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 5000

No.	Delta	Source	Destination	Length	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..	0.009001	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=testewlclan	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	0x01
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	SamsungE_08:4c:4a	Cisco_97:03:ef	342	Key (Message 2 of 4)	100	
2..	0.000002	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.002186	Cisco_97:03:ef	SamsungE_08:4c:4a	391	Key (Message 3 of 4)	100	
2..	0.000935	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	
2..	0.013829	SamsungE_08:4c:4a	Cisco_97:03:ef	199	Key (Message 4 of 4)	100	
2..	0.000174	192.168.1.15	192.168.1.100	76	Acknowledgement[Malformed Packet]	100	

> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

> Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (44)

> Tag: HT Capabilities (802.11n D1.10)

> Tag: HT Information (802.11n D1.10)

> Tag: Extended Capabilities (8 octets)

> Tag: VHT Capabilities

> Tag: VHT Operation

> Tag: Mobility Domain

> Tag: Fast BSS Transition

> Tag: RM Enabled Capabilities (5 octets)

> Tag: BSS Max Idle Period

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

Tag Number: Element ID Extension (255)

Ext Tag length: 46

Ext Tag Number: HE Capabilities (IEEE Std 802.11ax/D3.0) (35)

> HE MAC Capabilities Information: 0x800002100009

> HE Phy Capabilities Information

> Supported HE-MCS and NSS Set

> Rx and Tx MCS Maps <= 80 MHz

> Rx HEX-MCS Map <= 80 MHz: 0xaaaa

.... 10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)

.... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)

.... ..10 = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)

.... ..10.. = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)

.... ..10 = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)

.... ..10.. = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)

.... ..10 = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)

.... ..10.. = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)

> Tx HEX-MCS Map <= 80 MHz: 0xaaaa

> PPE Thresholds

> Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)

Tag Number: Element ID Extension (255)

Ext Tag length: 9

Ext Tag Number: HE Operation (IEEE Std 802.11ax/D3.0) (36)

> HE Operation Parameters: 0x003fff4

> BSS Color Information: 0x01

> Basic HE-MCS and NSS Set: 0xffff

注:WIFI 6データレートで送信されたデータフレームはキャプチャされますが、

 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せん。

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](https://bugzilla.cisco.com/show_bug.cgi?id=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 dscp2dot1p Table Value:
[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1
[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1
[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1
[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1
[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1
[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1
[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1
[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1
LabAP#
```

Qos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
Policy Map BWLimitAAAClients          type:qos client:default
  Class BWLimitAAAClients_AVC_UI_CLASS
    drop

  Class BWLimitAAAClients_ADV_UI_CLASS
    set dscp af41 (34)

  Class class-default
    police rate 5000000 bps (625000Bytes/s)
    conform-action
    exceed-action

Policy Map platinum-up                type:qos client:default
  Class cm-dscp-set1-for-up-4
    set dscp af41 (34)

  Class cm-dscp-set2-for-up-4
    set dscp af41 (34)

  Class cm-dscp-for-up-5
    set dscp af41 (34)

  Class cm-dscp-for-up-6
    set dscp ef (46)

  Class cm-dscp-for-up-7
    set dscp ef (46)

  Class class-default
    no actions
```

Qosレート制限の場合：

```
AP780C-F085-49E6#show rate-limit client
```

```
Config:
```

```
          mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst
A8:DB:03:6F:7A:46 2          0          0          0          0          0          0          0
```

```
Statistics:
```

```
      name      up  down
      Unshaped   0   0
      Client RT pass 0   0
      Client NRT pass 0   0
      Client RT drops 0   0
      Client NRT drops 0 38621
                9 54922  0
```

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-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 09:45:43.6570] 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 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
```

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:ffffffae:fffffffa:78:36:ffffff89|      8|
```

```
Radio Driver Client AID List:
```

```
=====
wifi0
[*08/20/2018 11:54:59.5415]
[*08/20/2018 11:54:59.5415] Total STA-ID List Count 0
[*08/20/2018 11:54:59.5415] | NO|                MAC|STA-ID|
[*08/20/2018 11:54:59.5415] -----
wifi1
[*08/20/2018 11:54:59.5431]
[*08/20/2018 11:54:59.5431] Total STA-ID List Count 1
[*08/20/2018 11:54:59.5431] | NO|                MAC|STA-ID|
[*08/20/2018 11:54:59.5432] -----
```

[*08/20/2018 11:54:59.5432] | 1| 0:ffffffae:fffffffa:78:36:ffffff89| 6|

WCP client Summary:

=====

mac	radio	vap	aid	state	encr	Maxrate	is_wgb_wired	wgb_mac_addr
00:AE:FA:78:36:89	1	9	1	FWD	AES_CCM128	MCS82SS	false	00:00:00:00:00:00

NSS client Summary:

=====

Current Count: 3

MAC	OPAQUE	PRI	POL	VLAN	BR	TN	QCF	BSS	RADID	MYMAC
F8:0B:CB:E4:7F:41	00000000		3	0	1	1	0	2	3	1
F8:0B:CB:E4:7F:40	00000000		3	0	1	1	0	2	3	1
00:AE:FA:78:36:89	00000003		1	0	1	1	0	9	1	0

Datapath IPv4 client Summary:

=====

id	vap	port	node	tunnel	mac	seen_ip	hashed_ip	sniff_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

HT:yes      VHT:yes      HE:no      40MHz:no      80MHz:no      80+80MHz:no      160MHz:no
11w:no      MFP:no      11h:no      encrypt_polocy: 4
_wmm_enabled:yes      qos_capable:yes      WME(11e):no      WMM_MIXED_MODE:no
short_preamble:yes      short_slot_time:no      short_hdr:yes      SM_dyn:yes
short_GI_20M:yes      short_GI_40M:no      short_GI_80M:yes      LDPC:yes      AMSDU:yes      AMSDU_long:no
su_mimo_capable:yes      mu_mimo_capable:no      is_wgb_wired:no      is_wgb:no

Additional info for client 00:AE:FA:78:36:89
RSSI: -90
PS : Legacy (Sleeping)
Tx Rate: 0 Kbps
Rx Rate: 117000 Kbps
VHT_TXMAP: 0
CCX Ver: 4

Statistics for client 00:AE:FA:78:36:89
      mac      intf TxData TxMgmt TxUC TxBytes

TxFail

      TxDcrd TxCumRetries RxData RxMgmt RxBytes RxErr TxRt      RxRt idle_counter stats_ago expiration
00:AE:FA:78:36:89 apr0v9      8      1      6      1038      1      0      0      31      1      1599

Per TID packet statistics for client 00:AE:FA:78:36:89
Priority Rx Pkts Tx Pkts Rx(last 5 s) Tx (last 5 s) QID Tx Drops Tx Cur Qlimit
0      899      460      1      1 144      0      0      1024
1      0      0      0      0 145      0      0      1024
2      0      0      0      0 146      0      0      1024
3      59      0      0      0 147      0      0      1024
4      0      0      0      0 148      0      0      1024
5      0      0      0      0 149      0      0      1024
6      0      0      0      0 150      0      0      1024
7      0      0      0      0 151      0      0      1024

Legacy Rate Statistics:
(Mbps : Rx, Tx, Tx-Retries)
11 Mbps : 2, 0, 0
6 Mbps : 0, 9, 0

HT/VHT Rate Statistics:
(Rate/SS/Width : Rx, Rx-Ampdu, Tx, Tx-Ampdu, Tx-Retries)
0/1/20 : 4, 4, 0, 0, 0
6/2/20 : 4, 4, 0, 0, 0
7/2/20 : 5, 5, 0, 0, 0

webauth done:
```

false

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 rate address 00:AE:FA:78:36:89
[*08/20/2018 14:17:28.0928]          MAC      Tx-Pkts   Rx-Pkts   Tx-Rate   Rx-Rate   RSSI     SNR  Tx-R
[*08/20/2018 14:17:28.0928] 00:AE:FA:78:36:89          0         0         12   a8.2-2s  -45     53
[*08/20/2018 14:17:29.0931] 00:AE:FA:78:36:89          7        18         12   a8.2-2s  -45     53
[*08/20/2018 14:17:30.0934] 00:AE:FA:78:36:89          3        18         12   a8.2-2s  -45     53
[*08/20/2018 14:17:31.0937] 00:AE:FA:78:36:89          2        20         12   a8.2-2s  -45     53
[*08/20/2018 14:17:32.0939] 00:AE:FA:78:36:89          2        20         12   a8.2-2s  -45     53
[*08/20/2018 14:17:33.0942] 00:AE:FA:78:36:89          2        21         12   a8.2-2s  -46     52
[*08/20/2018 14:17:34.0988] 00:AE:FA:78:36:89          1         4         12   a8.2-2s  -46     52
[*08/20/2018 14:17:35.0990] 00:AE:FA:78:36:89          9       23         12   a8.2-2s  -46     52
[*08/20/2018 14:17:36.0993] 00:AE:FA:78:36:89          3         7         12   a8.2-2s  -46     52
[*08/20/2018 14:17:37.0996] 00:AE:FA:78:36:89          2         6         12   a8.2-2s  -46     52
[*08/20/2018 14:17:38.0999] 00:AE:FA:78:36:89          2        14         12   a8.2-2s  -46     52
[*08/20/2018 14:17:39.1002] 00:AE:FA:78:36:89          2        10         12   a8.2-2s  -46     52
[*08/20/2018 14:17:40.1004] 00:AE:FA:78:36:89          1         6         12   a8.2-2s  -46     52
[*08/20/2018 14:17:41.1007] 00:AE:FA:78:36:89          9       20         12   a8.2-2s  -46     52
[*08/20/2018 14:17:42.1010] 00:AE:FA:78:36:89          0         0         12   a8.2-2s  -46     52
[*08/20/2018 14:17:43.1013] 00:AE:FA:78:36:89          2         8         12   a8.2-2s  -46     52
[*08/20/2018 14:17:44.1015] 00:AE:FA:78:36:89          0         0         12   a8.2-2s  -46     52
[*08/20/2018 14:17:45.1018] 00:AE:FA:78:36:89          0         0         12   a8.2-2s  -46     52
[*08/20/2018 14:17:46.1021] 00:AE:FA:78:36:89          0         0         12   a8.2-2s  -46     52
[*08/20/2018 14:17:47.1024] 00:AE:FA:78:36:89          0         0         12   a8.2-2s  -46     52
[*08/20/2018 14:17:48.1026] 00:AE:FA:78:36:89          7       15         12   a8.2-2s  -46     52
[*08/20/2018 14:17:49.1029] 00:AE:FA:78:36:89          0         6         12   a8.2-2s  -46     52
[*08/20/2018 14:17:50.1032] 00:AE:FA:78:36:89          0         0         12   a8.2-2s  -46     52
[*08/20/2018 14:17:51.1035] 00:AE:FA:78:36:89          1         7         12   a8.2-2s  -46     52
[*08/20/2018 14:17:52.1037] 00:AE:FA:78:36:89          0       17         12   a8.2-2s  -46     52
[*08/20/2018 14:17:53.1040] 00:AE:FA:78:36:89          1       19         12   a8.2-2s  -46     52
[*08/20/2018 14:17:54.1043] 00:AE:FA:78:36:89          2       17         12   a8.2-2s  -46     52
[*08/20/2018 14:17:55.1046] 00:AE:FA:78:36:89          2       22         12   a8.2-2s  -45     53
[*08/20/2018 14:17:56.1048] 00:AE:FA:78:36:89          1       18         12   a8.2-2s  -45     53
[*08/20/2018 14:17:57.1053] 00:AE:FA:78:36:89          2       18         12   a8.2-2s  -45     53
[*08/20/2018 14:17:58.1055] 00:AE:FA:78:36:89         12       37         12   a8.2-2s  -45     53
```

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。

```
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
```

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。

```
ap_2802#show flash
Directory of /storage/
total 84
-rw-r--r--    1 root    root           0 May 21  2018 1111
-rw-r--r--    1 root    root           6 Apr 15 11:09 BOOT_COUNT
-rw-r--r--    1 root    root           6 Apr 15 11:09 BOOT_COUNT.reserve
-rw-r--r--    1 root    root          29 Apr 15 11:09 RELOADED_AT_UTC
drwxr-xr-x    2 root    root          160 Mar 27 13:53 ap-images
drwxr-xr-x    4 5      root        2016 Apr 15 11:10 application
-rw-r--r--    1 root    root        6383 Apr 26 09:32 base_capwap_cfg_info
-rw-r--r--    1 root    root          20 Apr 26 10:31 bigacl
-rw-r--r--    1 root    root        1230 Mar 27 13:53 bootloader.log
-rw-r--r--    1 root    root           5 Apr 26 09:29 bootloader_verify.shadow
-rw-r--r--    1 root    root           18 Jun 30  2017 config
-rw-r--r--    1 root    root        8116 Apr 26 09:32 config.flex
-rw-r--r--    1 root    root        21 Apr 26 09:32 config.flex.mgroup
-rw-r--r--    1 root    root           0 Apr 15 11:09 config.local
-rw-r--r--    1 root    root           0 Jul 26  2018 config.mesh.dhcp
-rw-r--r--    1 root    root         180 Apr 15 11:10 config.mobexp
-rw-r--r--    1 root    root           0 Jun  5  2018 config.oep
-rw-r--r--    1 root    root       2253 Apr 26 09:43 config.wireless
drwxr-xr-x    2 root    root          160 Jun 30  2017 cores
drwxr-xr-x    2 root    root          320 Jun 30  2017 dropbear
drwxr-xr-x    2 root    root          160 Jun 30  2017 images
-rw-r--r--    1 root    root         222 Jan  2  2000 last_good_uplink_config
drwxr-xr-x    2 root    root          160 Jun 30  2017 lists
-rw-r--r--    1 root    root         215 Apr 16 11:01 part1_info.ver
-rw-r--r--    1 root    root         215 Apr 26 09:29 part2_info.ver
-rw-r--r--    1 root    root       4096 Apr 26 09:36 random_seed
-rw-r--r--    1 root    root           3 Jun 30  2017 rxtx_mode
-rw-r--r--    1 root    root          64 Apr 15 11:11 sensord_CSPRNG0
-rw-r--r--    1 root    root          64 Apr 15 11:11 sensord_CSPRNG1
drwxr-xr-x    3 support  root         224 Jun 30  2017 support
drwxr-xr-x    2 root    root        2176 Apr 15 11:10 syslogs
```

Filesystem	Size	Used	Available	Use%	Mounted on
flash	57.5M	372.0K	54.1M	1%	/storage

syslogの保存と送信

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

レポ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 15:23 2.0
-rw-r--r-- 1 root root 313 Jul 6 16:46 2.last_write
-rw-r--r-- 1 root root 20422 Jul 6 15:23 2.start

```

```

-----
Filesystem      Size      Used Available Use% Mounted on
flash           57.6M    88.0K    54.5M    0% /storage

```

```

artaki# show flash cores
Directory of /storage/cores/
total 0

```

```

-----
Filesystem      Size      Used Available Use% Mounted on
flash           57.6M    88.0K    54.5M    0% /storage

```

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 Join Profile

General Client CAPWAP AP **Management** Security ICap QoS

Device User Credentials CDP Interface

TFTP Downgrade

IPv4/IPv6 Address

Image File Name

System Log

Facility Value

Host IPv4/IPv6 Address

Log Trap Value

Secured ⓘ

Telnet/SSH Configuration

Telnet

SSH

AP Core Dump

Enable Core Dump

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。

これは、Cisco Bug ID [CSCvu75017](#)

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) 。

```
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
<cr>
APC4F7.D54C.E77C#copy support-bundle tftp: 192.168.1.100
Creating support bundle, please wait...ifconfig: wired1: error fetching interface information: Device not found
Unit systemd-journald.socket could not be found.
tar: ./*.tgz: No such file or directory
tar: error exit delayed from previous errors
tar: *.tgz: No such file or directory
tar: error exit delayed from previous errors
+=== Support file APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz created ===+
##### 100.0%
Successful file transfer:
APC4F7.D54C.E77C_support.17.2.1.11.20200408.145526.tgz
APC4F7.D54C.E77C#
```

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	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

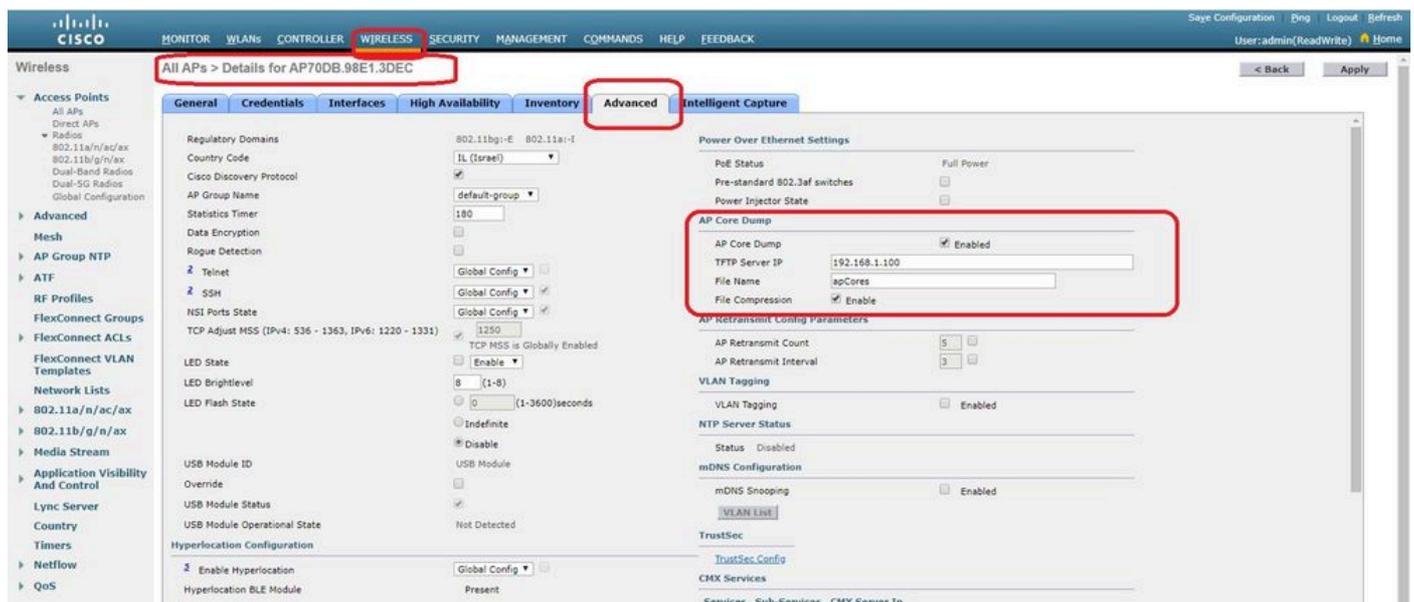
APコアファイルのリモート収集

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 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

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation path is "Configuration > Tags & Profiles > AP Join". The "Edit AP Join Profile" page is open, with the "Management" tab selected. The "Device" sub-tab is also selected. The "AP Core Dump" section is highlighted with a red box, showing the following configuration:

- Enable Core Dump:
- TFTP Server* (IPv4/IPv6): 192.168.1.100
- File Name*: default
- Enable File Compression:

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。

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation path is "Configuration > Tags & Profiles > AP". The "Edit AP" page is open, with the "Support Bundle" tab selected. The "Destination" section is highlighted with a red box, showing the following configuration:

- Destination: This Device
- Server IP*: 172.31.46.79
- Destination File Path*: /
- Username*:
- Password*:

The "Start Transfer" button is visible at the bottom of the "Destination" section. The "Last Export Status" section is also visible on the right side of the page.

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 : [9800 v17.2.1でSSHを有効にする](#)

ステップ 2 : [Cisco IOS® XE v17.2.1でSCPを有効にする](#)

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。

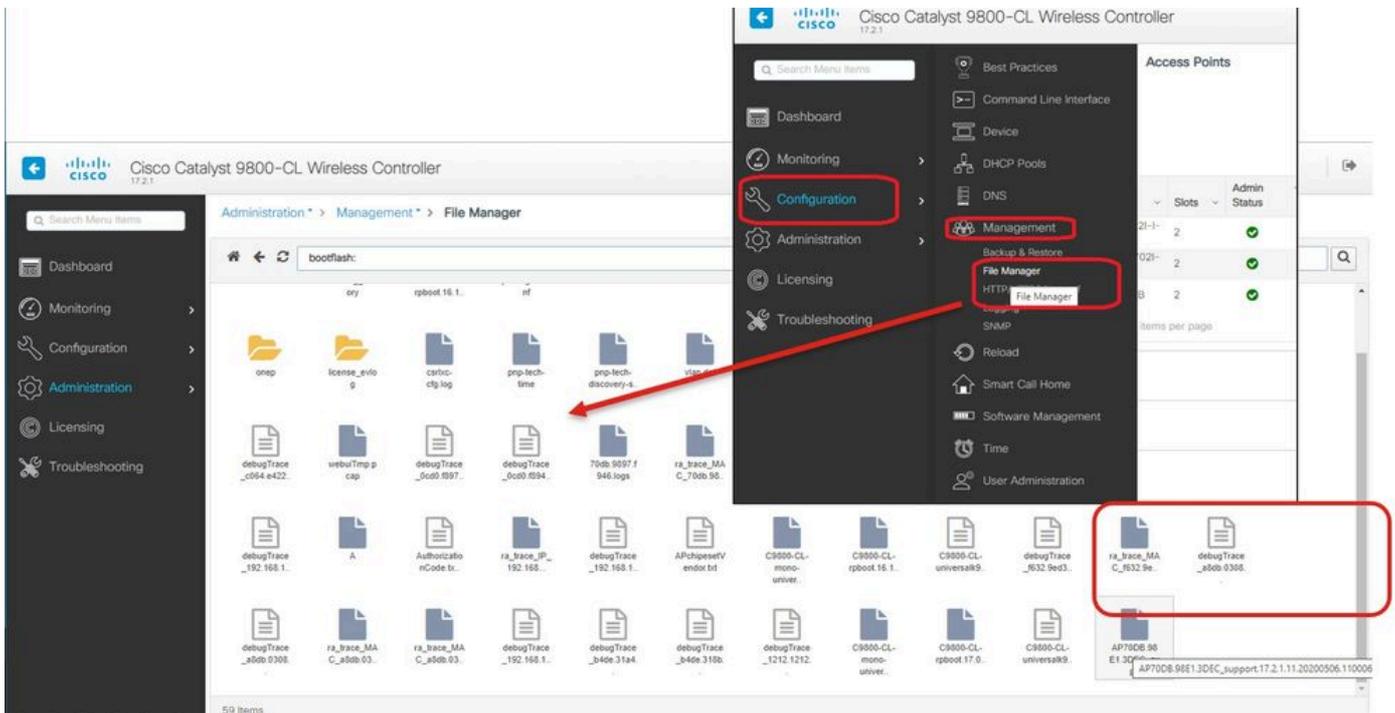
```
! AAA authentication and authorization must be configured properly in order for SCP to work.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username 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。

```
AP700B.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 AP700B.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
AP700B.98E1.3DEC#copy support-bundle scp: admin@192.168.1.15:/AP700B.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 AP700B.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz created ====
Password:
AP700B.98E1.3DEC_support.17.2.1.11.20200506.110400.tgz
Connection to 192.168.1.15 closed by remote host.
100% 50KB 3.3MB/s 00:00
AP700B.98E1.3DEC#
```

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 msg="[DNAS] entering stopDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting stopDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] entering startDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] launching token request cycle"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] exiting startDNASpacesTmpTokenRoutine"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] spaces token expiration time 2020-04-02 01:36:52 +0000 UTC"
time="2020-04-01T01:36:52Z" level=info msg="Calling startDNASpacesConn routine "
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Receive Success status"
time="2020-04-01T01:36:52Z" level=info msg="[DNAS] Connection not in ready state sleeping for 10 second"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Setup Stream for the gRPC connection"
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] Connect RPC Succeeded."
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] RX routine got enabled "
time="2020-04-01T01:37:02Z" level=info msg="[DNAS] TX routine got enabled "

```

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

```


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]: 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。