

Catalyst 9800ワイヤレスLANコントローラ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](#)

[背景説明](#)

[9800 WLC内のバケットフロー](#)

[コントロールプレーントレース](#)

[Syslog](#)

[常時トレース](#)

[条件付きデバッグとRadioActiveトレース](#)

[Web UIによる放射性トレース](#)

[CLIによる放射性トレース](#)

[プロセスごとの非条件付きデバッグ](#)

[データプレーンパケットトレース](#)

[Embedded Packet Capture](#)

[アラームLEDおよび重要なプラットフォームアラーム](#)

はじめに

このドキュメントでは、Catalyst 9800のトラブルシューティングに活用されるCisco IOS® XEのすべての機能について説明し、その概要を示します。

前提条件

要件

- ワイヤレスLANコントローラ(WLC)に関する基礎知識。
- WLCの使用に関連するユースケースフローの基本的な知識。

使用するコンポーネント

このドキュメントでは、9800-CL、9800-L、9800-40、および9800-80コントローラについて説明します。これは主に17.3 Cisco IOS® XEバージョンに基づいています。

背景説明

9800 WLC上で動作するCisco IOS® XEは、基本的にCisco IOS®を搭載したLinuxカーネル

(binOS)と、デーモンとして実装されたすべてのワイヤレスプロセスで構成されます。

すべてのプロセスデーモンは、一般用語であるコントロールプレーン(CP)にバンドルでき、アクセスポイントの制御とプロビジョニング(CAPWAP)、モビリティ、Radio Resource Management(RRM)を担当します。不正管理、および9800 WLCを宛先および送信元とするネットワークモビリティサービスプロトコル(NMSP)。

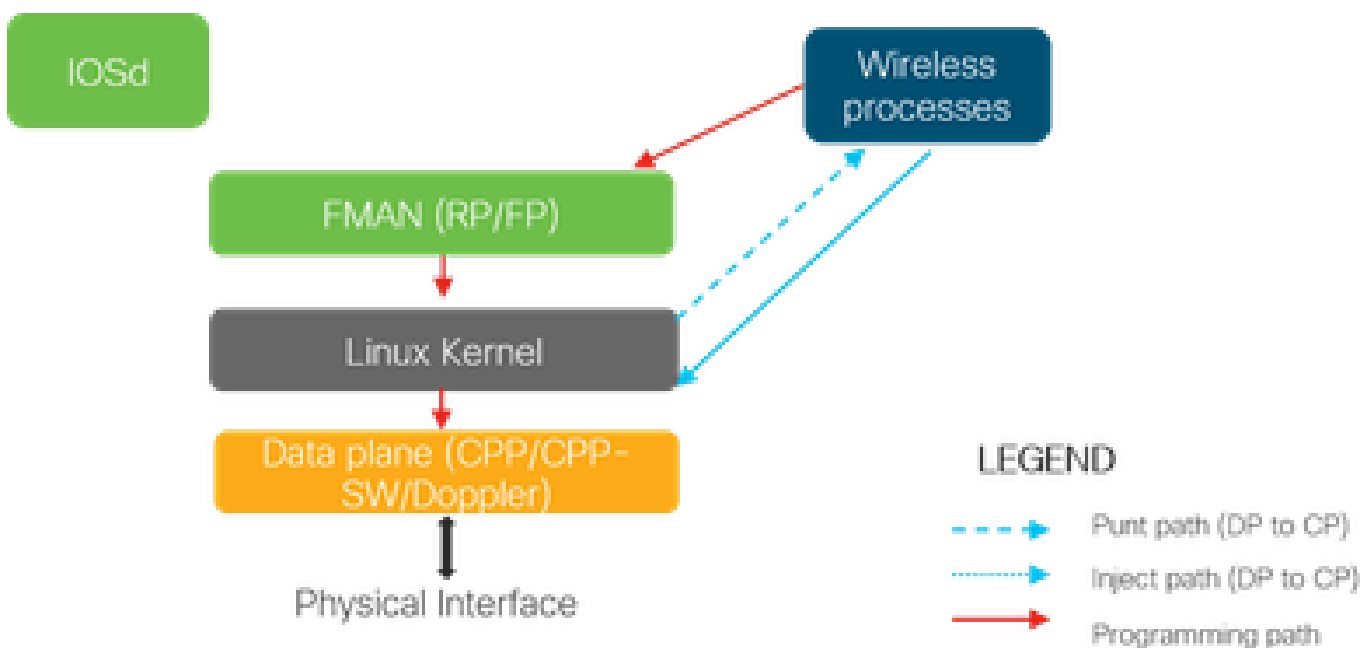
データプレーン(DP)とは、9800 WLC上でデータを転送するコンポーネントを指します。

9800のすべてのイテレーション(9800-40、9800-80、9800-CL、9800-SW、9800-L)では、コントロールプレーンはかなり一般的なままです。

ただし、データプレーンは、ASR1kと同様のハードウェアQuantum Flow Processor(QFP)コンプレックスを使用する9800-40および9800-80によって異なり、9800-CLおよび9800-LはCisco Packet Processor(CPP)のソフトウェア実装を使用します。

9800-SWは、Catalyst 9000シリーズスイッチ上のドップラーチップセットを活用してデータ転送を行います。

9800 WLC内のパケットフロー



物理ポートから9800 WLCに入るパケットは、制御トラフィックと判断されると、対応するコントロールプレーンプロセスにパントされます。

AP加入の場合、これはAPから送信されるすべてのcapwapとdtls交換です。クライアントが参加する場合、クライアントがRUN状態になるまで、クライアントから送信されるすべてのトラフィックがこの状態になります。

さまざまなデーモンが着信トラフィックを処理する際に、クライアントに送信される9800 WLCからのリターントラフィック (capwap応答、 dot11、 dot1x、 dcp応答) が、物理ポートから送信されるデータプレーンに再び注入されます。

AP加入、クライアント加入、モビリティ交換、データプレーン进行处理する際には、データトラフィック転送を処理できるようにプログラムする必要があります。

これは、イメージに示されているプログラミングパス上で複数のコンポーネントが順番にプログラムされている場合に発生します。

Cisco IOS® XEは、パケットが9800 WLCに入った瞬間から、処理されたトラフィックがボックスから出るまでをトレースする、多目的なツールセットを提供します。

次の項では、これらのツールをコマンドラインインターフェイス(CLI)から起動するために使用するコマンドとともに、これらのツールを紹介します。

コントロールプレーントレース

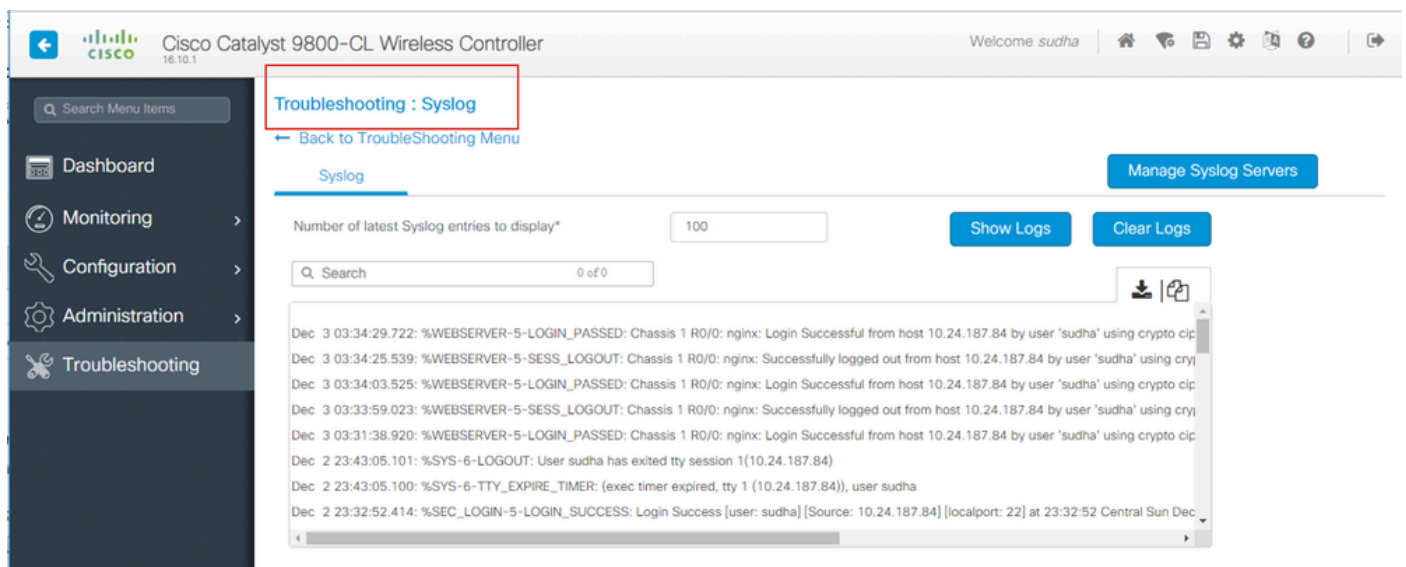
この項では、9800 WLC向けのパケットがDPからパントされた後、または9800 WLCから送信された応答パケットをDPに注入して物理インターフェイスを送信する前に、コントロールプレーンプロセスによって実行される処理を表示するために使用できるコマンドとツールについて説明します

Syslog

9800 WLCによって生成されるログは、システムの一般的な健全性を確認するための最初的手段です。

CPU、メモリ、バッファなどのシステムリソースの事前定義されたしきい値に違反すると、ログに報告されます。

また、サブシステムによって生成されたエラーはログに書き込まれます。ログを表示するには、Troubleshooting > Syslogの順に移動します。




The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller web interface. The top navigation bar includes the Cisco logo, the device name 'Cisco Catalyst 9800-CL Wireless Controller', and the user name 'Welcome sudha'. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The 'Troubleshooting : Syslog' menu item is highlighted with a red box. The main content area shows the Syslog configuration page with a 'Manage Syslog Servers' button, a 'Number of latest Syslog entries to display*' field set to 100, and 'Show Logs' and 'Clear Logs' buttons. A search bar is also present above the log entries.

または、CLIコマンドを実行します。

```
# show logging
```

次の出力では、一般的なログと、一部のワイヤレス固有のログが示されています。ただし、従来のCisco IOS®とは異なり、ワイヤレスデバッグは通常、このログ出力に到達しません。

 注：これらのログを外部syslogサーバにリダイレクトするようにWLC9800が設定されている場合は、外部syslogサーバでもログを確認する必要があります。

常時トレース

WLC9800上のすべてのコントロールプレーンプロセスは、専用バッファにNoticeのログレベルで継続的にロギングされます。これは、常時トレースと呼ばれます。

これは、障害状態の再現を要求することなく、発生した障害に関するコンテキストデータを取得できる独自の機能です。

たとえば、AireOSに精通している場合、クライアント接続のトラブルシューティングを行うには、デバッグを有効にし、根本原因を特定するためにクライアント接続の問題の状態を再現する必要があります。

常時トレース機能を使用すると、すでにキャプチャされたトレースを振り返り、それが一般的な根本原因であるかどうかを特定できます。生成されるログの量に応じて、数時間から数日を振り返ることができます。

トレースは個々のプロセスごとにログに記録されますが、クライアントMAC、AP MAC、またはAP IPアドレスなど、対象となる特定のコンテキストについて総合的に表示できます。そのためには、次のコマンドを実行します


```
# show logging profile wireless filter mac to-file bootflash:
```

デフォルトでは、このコマンドはログの生成とデコードに10分しか時間がかかりません。以下を使用して、さらに時間をさかのぼることができます。

```
# show logging profile wireless start last <number> [minutes|hours|days] filter mac to-file bootflash:
```

プロセスごとのログを表示するには、コマンドを実行します

```
# show logging process to-file bootflash:
```

 注：これらのCLIには、モジュール、ログレベル、開始タイムスタンプなど、複数のフィルタリングオプションがあります。これらのオプションを表示するには、次のコマンドを実行します


```
# show logging profile wireless ?  
# show logging process ?
```


条件付きデバッグとRadioActiveトレース

条件付きデバッグを使用すると、対象の条件に対する特定の機能に関するデバッグレベルのロギングを有効にできます。

RadioActiveトレースでは、さらに一歩進んで、対象の条件を満たすプロセスやスレッド間でデバッグ情報を条件付きで印刷する機能が追加されています。

つまり、基盤となるアーキテクチャが完全に抽象化されます。

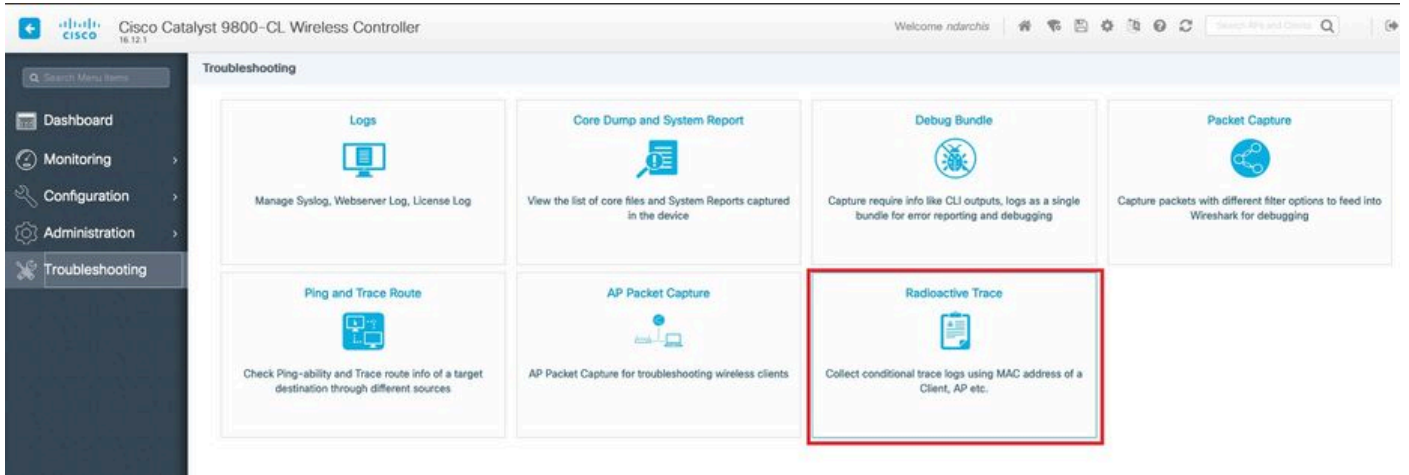
 注：16.12では、放射性トレースが実行されるのは、AP無線およびイーサネットMACアドレスによるAP加入、クライアントMACアドレスによるクライアント加入、およびモビリティピアIPによるモビリティの問題とCMX IPアドレスによるCMX接続を対象とするモビリティの問題のトラブルシューティングのためだけです。

 注：条件としてのMACアドレスとIPアドレスでは、異なるプロセスが同じネットワークエンティティ（AP、クライアント、またはモビリティピア）の異なるIDを認識するため、異なる出力が提供されます。

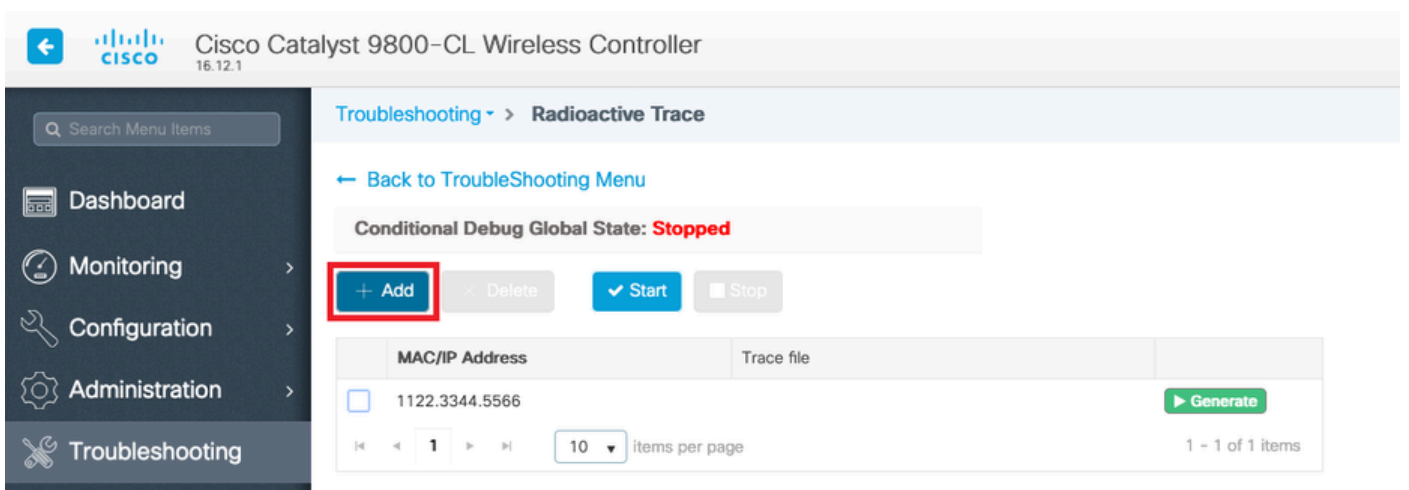
トラブルシューティングの例としてクライアント接続を使用すると、クライアントmacに対して条件付きデバッグが実行され、コントロールプレーンでエンドツーエンドのビューが取得されます。

Web UIによる放射性トレース

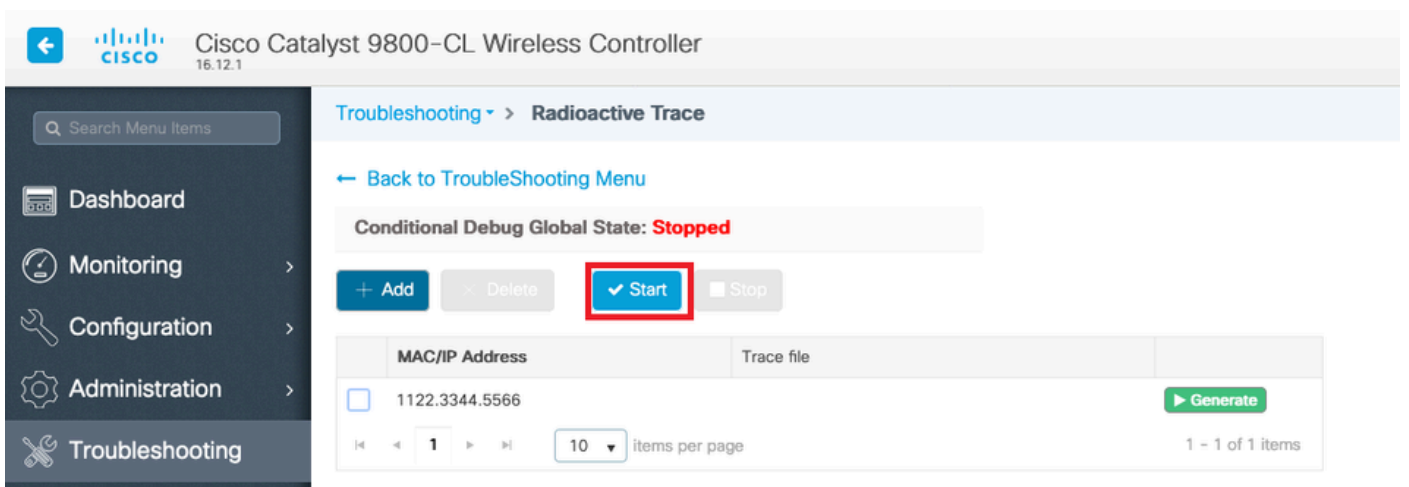
Troubleshootingページメニューに移動し、Radioactive Tracingを選択します



Addをクリックして、トラブルシューティングを行うクライアントまたはAPのMACアドレスを入力します。 16.12では、GUIから追加できるのはMACアドレスだけです。CLIを使用してIPアドレスを追加できます。

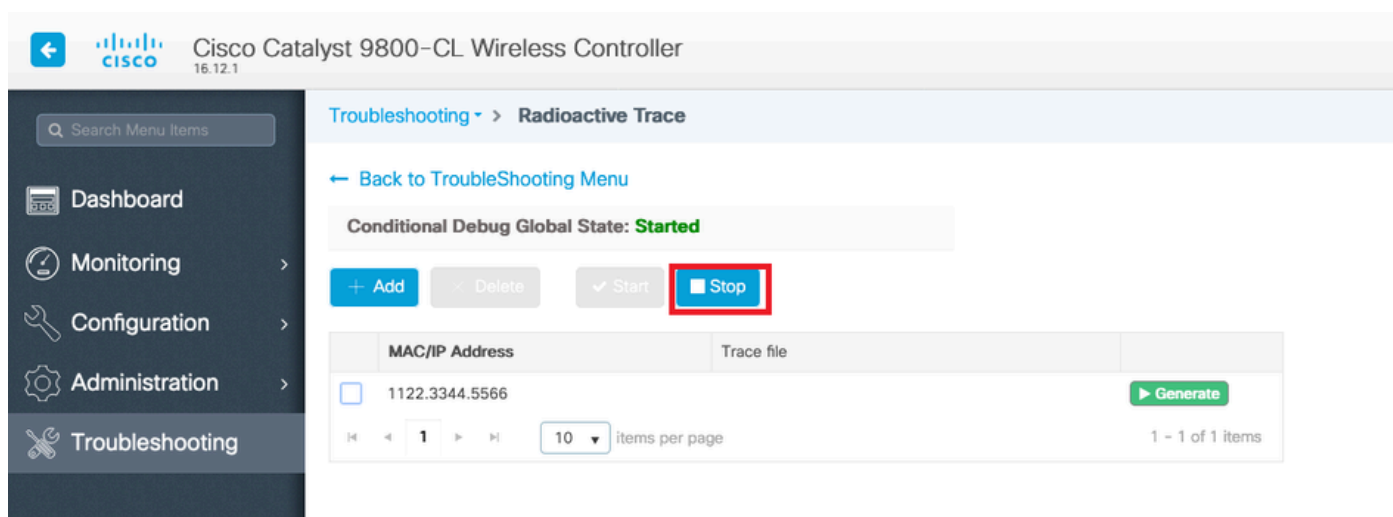


追跡するMACアドレスを複数追加できます。放射性トレースを開始する準備ができたなら、startをクリックします。



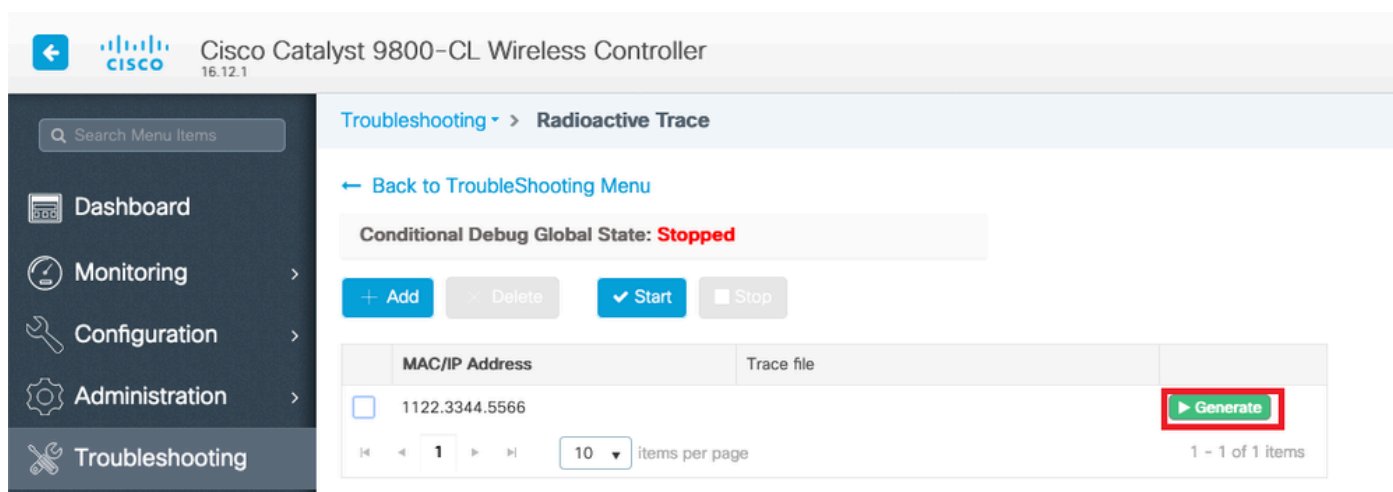
いったん開始されると、追跡されたMACアドレスに関連するコントロールプレーンの処理に関するデバッグロギングがディスクに書き込まれます。

トラブルシューティングする問題を再現したら、Stopをクリックします。



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area is titled 'Troubleshooting > Radioactive Trace'. Below the title, there is a 'Back to Troubleshooting Menu' link and a 'Conditional Debug Global State: Started' indicator. A row of buttons includes '+ Add', 'Delete', 'Start', and 'Stop', with the 'Stop' button highlighted by a red box. Below the buttons is a table with columns for 'MAC/IP Address' and 'Trace file'. The table contains one entry with the MAC address '1122.3344.5566' and a 'Generate' button. The page also shows pagination controls for 10 items per page and '1 - 1 of 1 items'.

デバッグしたMACアドレスごとに、Generateをクリックして、そのMACアドレスに関連するすべてのログを集計するログファイルを生成できます。



The screenshot shows the same Cisco Catalyst 9800-CL Wireless Controller interface. The 'Conditional Debug Global State' is now 'Stopped'. The 'Start' button is active, and the 'Stop' button is disabled. The 'Generate' button in the table is highlighted by a red box. The rest of the interface, including the sidebar and table structure, remains the same.

照合済みログファイルの取得時間を選択し、Apply to Deviceをクリックします。

Enter time interval



Generate logs for last 10 minutes

30 minutes

1 hour

since last boot

seconds



Cancel

Apply to Device

ファイル名の横にある小さいアイコンをクリックすると、ファイルをダウンロードできます。このファイルはコントローラのブートフラッシュドライブにあり、CLIを使用してコピーすることもできます。

Troubleshooting > Radioactive Trace

[← Back to TroubleShooting Menu](#)

Conditional Debug Global State: **Stopped**

+ Add

× Delete

✓ Start

■ Stop

	MAC/IP Address	Trace file	
<input type="checkbox"/>	1122.3344.5566	debugTrace_1122.3344.5566.txt	<input type="button" value="Generate"/>

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

CLIによる放射性トレース

条件付きデバッグをイネーブルにするには、次のコマンドを実行します


```
# debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds}
```

現在有効な条件を表示するには、次のコマンドを実行します。


```
# show debugging
```

これらのデバッグでは、ターミナルセッションで出力は出力されませんが、後で取得して分析するために、デバッグ出力ファイルがフラッシュに保存されます。ファイルは、命名規則 ra_trace で保存されます_*

たとえば、macアドレスaaaa.bbbb.ccccの場合、生成されるファイル名は ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log です

1つの利点は、同じコマンドを使用して、APの加入の問題（入力AP無線MACおよびイーサネットMAC）、クライアントの接続の問題（入力クライアントMAC）、モビリティトンネルの問題（入力ピアIP）、クライアントのローミングの問題（入力クライアントMAC）をトラブルシューティングできることです。

つまり、debug capwap、debug client、debug mobilityなどの複数のコマンドを覚えておく必要はありません。

 注：debug wirelessでは、FTPサーバをポイントして、キーワードinternalを使用してさらに詳細なロギングを実行することもできます。現時点ではこれらはお勧めできません。一部の問題が解決されていないためです。

ターミナルセッションの出力ファイルをデバッグするには、次のコマンドを実行します

```
# more bootflash:ra_trace_MAC_*.log
```

オフライン分析のためにデバッグ出力を外部サーバにリダイレクトするには、次のコマンドを実行します


```
# copy bootflash:ra_trace_MAC_*.log ftp://username:password@FTPSERVERIP/path/RATRACE_FILENAME.txt
```

同じデバッグログレベルのより詳細なビューがあります。この詳細ビューを表示するには、次のコマンドを実行します

```
# show logging profile wireless internal filter mac to-file
```

特定のコンテキストのデバッグを無効にする、または設定された監視時間またはデフォルトの監視時間がアップする前にデバッグを無効にするには、コマンドを実行します。

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

 **注意：**条件付きデバッグを使用すると、デバッグレベルのロギングが有効になり、生成されるログの量が増加します。これを実行したままにすると、ログを表示できる時間を短縮できます。そのため、トラブルシューティングセッションの最後には常にデバッグを無効にすることを推奨します。

すべてのデバッグを無効にするには、次のコマンドを実行します

```
# clear platform condition all
# undebug all
```

プロセスごとの非条件付きデバッグ

放射性トレース用に実装されていないユースケースやプロセスでは、デバッグレベルのトレースを取得できません。特定のプロセスのデバッグレベルを設定するには、次のコマンドを使用します。

```
# set platform software trace <PROCESS_NAME> wireless chassis active R0 { module_name | all-modules }
```

さまざまなモジュールのトレースレベルを確認するには、次のコマンドを実行します

```
# show platform software trace level <PROCESS_NAME> chassis active R0
```

収集されたトレースを表示するには、次のコマンドを実行します

```
# show logging process to-file
```

データプレーンパケットトレース

パケットが最初に9800 WLCに入ると、トラフィックがコントロールプレーンかデータプレーンかを識別するために、データプレーンでいくつかの処理が行われます。

パケットトレース機能は、データプレーンで実行されるこのCisco IOS® XE処理と、パケットをパント、転送、ドロップ、または使用するかどうかの決定の詳細を示します。


WLC 9800のこの機能は、ASR1kでの実装とまったく同じように動作します。

9800 WLCのPacket Tracerは、ASR1Kと同じ3つのレベルの検査を提供します。

- 統計情報：ネットワークプロセッサに出入りするパケットの数を示します。
- 要約-
 - これは、対象の特定の条件に一致する限られた数のパケットについて収集されます。
 - サマリー出力は、入インターフェイスと出インターフェイス、データプレーンによって行われたルックアップの決定を示し、パント、ドロップ、およびインジェクトのパケット（存在する場合）を追跡します。
 - この出力は、データプレーン処理の簡潔なビューを提供します
- パスデータ：DPパケット処理の最も詳細なビューを提供します。収集されるパケット数には制限があり、DPパケットをコントロールプレーンデバッグ、タイムスタンプ、および機能固有のパストレースデータに関連付けるために使用できる条件付きデバッグIDが含まれます。この詳細ビューには、2つのオプション機能があります
 - パケットコピーを使用すると、パケットのさまざまなレイヤ（レイヤ2、レイヤ3、およびレイヤ4）で入出力パケットをコピーできます
 - Feature Invocation array(FIA)は、データプレーンによってパケット上で実行される機能のシーケンシャルリストです。次の機能は、WLC 9800のデフォルトおよびユーザ対応の設定から取得されます


機能とサブオプションの詳細な説明については、『Cisco [IOS XEデータパスパケットトレース機能](#)』を参照してください


AP加入、クライアント接続などのワイヤレスワークフローでは、アップリンクを双方向でトレースします

 注意：データプレーンパケットトレースは、外側のCAPWAPヘッダーのみを解析します。したがって、ワイヤレスクライアントmacなどの条件では有用な出力が得られません。

ステップ 1：対象の条件を定義します。

```
# debug platform condition { interface | mac | ingress | egress | both | ipv4 | ipv6 | mpls | match }
```

 警告:debug platform condition featureコマンドとdebug platform condition mac aaaa.bbbb.ccccコマンドは両方ともコントロールプレーンパケットトレースを目的としてお

 り、データプレーンパケットトレースを一切返しません。

ステップ 2 : 現在有効な条件を表示するには、次のコマンドを実行します。

```
# show platform conditions
```

ステップ 3 : 限られた数のパケットに対してパケットトレーサを有効にします。このパケット番号は、16 ~ 8192の範囲で2の累乗として定義されます。デフォルトでは、サマリーデータとフィーチャデータの両方がキャプチャされます。オプションで、summary-onlyサブオプションを使用した場合にのみ、サマリービューを取得するように選択できます。fiaトレースの取得、パケットサイズのバイト単位の定義、パントのトレース、パケットのインジェクトまたはドロップなどのサブオプションも使用できます。

```
# debug platform packet-tracer packet <packet-number> {fia-trace}
```

ステップ4: (オプション) トレースされたパケットをコピーしてダンプできます

```
# debug platform packet-trace copy packet both size 2048 { 12 | 13 | 14 }
```

ステップ 5 : 条件付きデバッグを有効にします。

```
# debug platform condition start
```

手順 6 : パケットトレースで出力が収集されているかどうかを確認するには、統計情報を確認します

```
# show platform packet-trace statistics
```

手順 7 : パケットトレースの出力を表示するには、次のコマンドを実行します

```
# show platform packet-tracer summary
```

ステップ8: (オプション) Cisco TACによるオフライン分析用にパケットダンプをエクスポート
できます

```
# show platform packet-trace packet all | redirect { bootflash: | tftp: | ftp: } pacrac.txt
```

Embedded Packet Capture

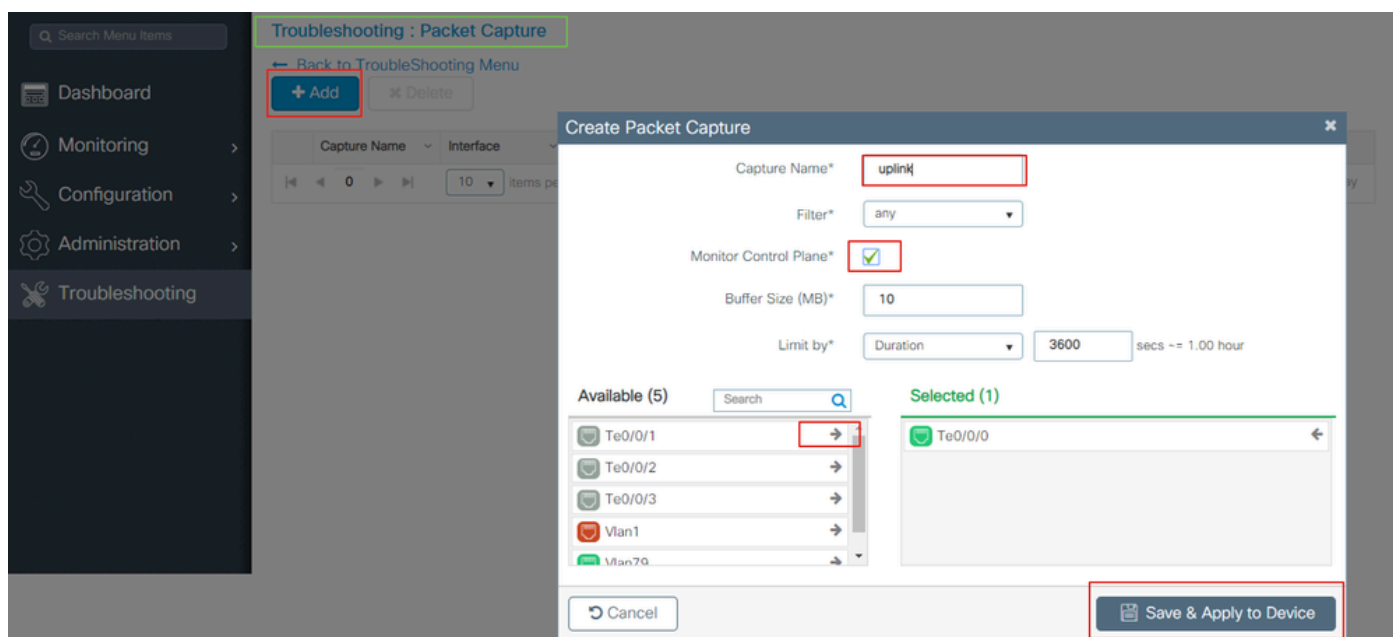
組み込みパケットキャプチャ(EPC)は、Catalyst 9800 WLCを送受信するパケットを表示できるパケットキャプチャ機能です。これらのキャプチャは、Wiresharkによるオフライン分析のためにエクスポートできます。

機能の詳細については、『[EPC設定ガイド](#)』を参照してください。

AireOSと比較して、9800 WLCでは、アップリンクスイッチのパケットキャプチャおよびトラフィックミラーリング機能に依存する代わりに、ボックス自体でpcapキャプチャが可能です。

9800では、このキャプチャはコマンドラインインターフェイス(CLI)とグラフィカルユーザーインターフェイス(GUI)の両方から設定できます。

GUIを使用して設定するには、Troubleshooting > Packet Capture > +Addの順に移動します。



ステップ 1 : パケットキャプチャの名前を定義します。最大8文字まで入力できます。

ステップ 2 : フィルタを定義する (存在する場合)

ステップ 3 : トラフィックがシステムCPUにパントされ、データプレーンに再び注入されるのを確認するには、Monitor Control Trafficのチェックボックスをオンにします

ステップ 4 : バッファサイズを定義します。最大100 MBまで使用できます

ステップ 5：必要に応じて、1 ~ 1000000秒の範囲を指定できる期間または1 ~ 100000パケットの範囲を指定できるパケット数で制限を定義します

手順 6：左側の列のインターフェイスのリストからインターフェイスを選択し、矢印を選択して右側の列に移動します


手順 7：保存してデバイスに適用

ステップ 8：キャプチャを開始するには、Startを選択します。

ステップ 9：キャプチャを定義された制限まで実行できます。キャプチャを手動で停止するには、Stopを選択します。

ステップ 10：停止すると、Exportボタンがクリック可能になり、httpsまたはTFTPサーバ、FTPサーバ、あるいはローカルシステムのハードディスクまたはフラッシュを介してローカルデスクトップにキャプチャファイル(.pcap)をダウンロードするオプションが表示されます。

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> uplink	TenGigabitEthernet0/0/0	Yes	0%	any	0 secs	Inactive	▶ Start

 注:CLIでは、Limit byなどのオプションの粒度がもう少し細かくなっています。GUIは、一般的な使用例のパケットをキャプチャするのに十分です。

CLIを使用して設定するには、次の手順を実行します。

モニタキャプチャを作成します。

```
monitor capture uplink interface <uplink_of_the_9800> both
```

フィルタを関連付けます。フィルタはインラインで指定するか、ACLまたはクラスマップを参照できます。

この例では、9800と別のWLC 5520の2つのIPアドレス間のトラフィックを照合するACLです。モビリティトラブルシューティングの一般的なシナリオ：

```
conf t
ip access-list extended mobilitywlc
permit ip host <5520_ip_address> host <9800_ip_address>
  permit ip host <9800_ip_address> host <5520_ip_address>
```

```
end
```

```
monitor capture uplink access-list mobilitywlcs
```

キャプチャを循環バッファで実行する場合は、問題に気付いてから、キャプチャを停止して保存する時間があります。

たとえば、50MBバッファに設定した場合です。9800では最大50 MBのディスクが必要で、問題の発生を期待して数分のデータをキャプチャするにはかなり大きなディスクが必要です。

```
monitor capture uplink buffer circular size 50
```

キャプチャの開始.GUIまたはCLIから実行できます。

```
monitor capture uplink start
```

これでキャプチャがアクティブになりました。

必要なデータの収集を許可します。

キャプチャを停止します。これは、GUIまたはCLIを使用して実行できます。

```
monitor capture uplink stop
```

キャプチャは、GUI > Troubleshooting > Packet Capture > Exportで取得できます。

または、CLIからサーバにアップロードします。ftp経由の例：

```
monitor capture uplink export ftp://x.x.x.x/MobilityCAP.pcap
```

必要なデータが収集されたら、キャプチャを削除します。

```
no monitor capture uplink
```

アラームLEDおよび重要なプラットフォームアラーム

9800アプライアンス (9800-L、9800-40、および9800-80) の前面パネルには、すべてALM LEDが付いています。このLEDが赤色に点灯する場合は、プラットフォームにクリティカルアラームがあることを意味します。

show facility-alarm statusコマンドで、LEDが赤色になる原因となるアラームを確認できます

```
WLC#show facility-alarm status
```

```
System Totals Critical: 2 Major: 0 Minor: 0
```

Source	Time	Severity	Description [Index]
-----	-----	-----	-----
TenGigabitEthernet0/1/0	Jul 26 2019 15:14:04	CRITICAL	Physical Port Link Down [1]
TenGigabitEthernet0/1/1	Jul 26 2019 15:14:04	CRITICAL	Physical Port Link Down [1]

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。