# ワイヤレスLANコントローラのCPU負荷のトラブルシューティング

## 内容



## はじめに

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(WLC)のCPU使用率を監視する方法について説明し、いくつかの設定に関する推奨事項について説明します。

## CPU使用率について

CPUの負荷のトラブルシューティングを行う前に、Catalyst 9800ワイヤレスLANコントローラでのCPUの使用方法の基本と、ソフトウェアアーキテクチャの詳細を理解する必要があります。

一般的に、Catalyst 9800のベストプラクティスドキュメントでは、mDNSのロケーションフィルタリングを使用したり、クライアントの除外を常に有効にするなど、アプリケーションレベルの問題を防ぐことができる一連の適切な構成設定を定義しています。これらの推奨事項は、ここで説明するトピックとともに適用することをお勧めします。

## プラットフォームの基礎

Catalyst 9800コントローラは、さまざまなネットワーク負荷を対象とし、水平スケーリングに重点を置いた柔軟なプラットフォームとして設計されています。内部開発の名称は「eWLC」で、eは「elastic」を意味します。これは、同じソフトウェアアーキテクチャが小規模な単一のCPU組み込みシステムから複数のCPU/コア大規模アプライアンスまで実行できることを意味します。

各WLCには2つの異なる「側面」があります。

- コントロールプレーン：CLI、UI、Netconfなどのすべての「管理」インタラクションと、クライアントおよびAPのすべてのオンボーディングプロセスを処理します。
- データプレーン：実際のパケット転送、CAPWAPのカプセル化解除、AVCポリシーの適用などの機能を担当します。

## コントロール プレーン

- ほとんどのCisco IOS-XEプロセスは、専用のスケジューラおよびモニタリングコマンドを使用して、BinOS（Linuxカーネル）で実行されます。
- Wireless Network Control Daemon（WNCD；無線ネットワーク制御デーモン）と呼ばれる一連の主要なプロセスがあり、それぞれがローカルのインメモリデータベースを持ち、無線アクティビティのほとんどを処理します。各CPUはWNCDを所有し、使用可能なすべてのCPUコアから各システムに負荷を分散させます
- WNCD間の負荷分散は、AP加入時に行われます。APがコントローラへのCAPWAP加入を実行すると、使用可能なすべてのCPUリソースが適切に使用されるように、内部ロードバランサが一連の使用可能なルールを使用してAPを分散します。
- Cisco IOS® コードはIOSdと呼ばれる独自のプロセスで実行され、CPUスケジューラを備えています。これは、CLI、SNMP、マルチキャスト、ルーティングなどの特定の機能を処理します。

簡略化すると、コントローラはコントロールプレーンとデータプレーンの間に通信メカニズムを備えています。この通信メカニズムでは、「パント」がネットワークからコントロールプレーンにトラフィックを送信し、「インジェクション」がコントロールプレーンからネットワークにフレームをプッシュします。

高CPUトラブルシューティング調査の一環として、パントメカニズムを監視し、どのトラフィックがコントロールプレーンに到達していて高負荷につながる可能性があるかを評価する必要があります。

## データ プレーン

Catalyst 9800コントローラの場合、これはCisco Packet Processor(CPP)の一部として実行されます。CPPは、パケット転送エンジンを開発するためのソフトウェアフレームワークであり、複数の製品およびテクノロジーで使用されます。

このアーキテクチャにより、異なるハードウェアやソフトウェアの実装で共通の機能セットを使用できます。たとえば、9800CLと9800-40で同じ機能を異なるスループットスケールで使用できます。

# AP ロード バランシング

WLCは、CAPWAP AP加入プロセス中にCPU間でロードバランシングを実行します。主な差別化要因はAPサイトタグ名です。これは、各APがクライアントアクティビティとAP自体から発生する、追加された特定のCPU負荷を表すという概念に基づいています。このバランシングを実行するメカニズムは複数あります。

- APが「default-tag」を使用している場合、すべてのCPU/WNCDにラウンドロビン方式でバランスが取られ、新しいAPの加入が次のWNCDに送られます。これは最も簡単な方法ですが、影響はほとんどありません。
  - 同じRFローミングドメイン内のAPは、追加のプロセス間通信を含む頻繁なWNCD間ローミングを実行するため、これは最適なシナリオではありません。インスタンス間のローミングは少し遅くなります。
  - FlexConnect（リモート）サイトタグの場合、PMKキー配布は使用できません。これは、Flexモードで高速ローミングを実行できないことを意味し、OKC/FTローミングモードに影響します。

    一般に、デフォルトタグは負荷の低いシナリオ（たとえば、9800プラットフォームのAPとクライアントの負荷の40 %未満）で、高速ローミングが要件でない場合にのみFlexConnectの導入で使用できます。

- APにカスタムサイトタグがある場合、サイトタグ名に属するAPが初めてコントローラに加入するときには、サイトタグが特定のWNCDインスタンスに割り当てられます。同じタグを持つ後続の追加AP加入はすべて、同じWNCDに割り当てられます。これにより、同じサイトタグ内のAP間でのローミングが1つのWCNDコンテキストで実行され、より最適なフローが低いCPU使用率で提供されます。WNCD間のローミングはサポートされていますが、WNCD内のローミングほど最適ではありません。

- デフォルトのロードバランシング決定：タグがWNCDに割り当てられると、ロードバランサはその時点でサイトタグ数が最も少ないインスタンスを選択します。サイトタグが持つ可能性がある総負荷は不明であるため、最適なバランシングシナリオにはならない可能性があります。これは、APの加入の順序、定義されているサイトタグの数、およびAPカウントがそれらの間で非対称であるかどうかによって異なります

- 静的なロードバランシング：WNCDに対するサイトタグの割り当ての不均衡を防ぐために、site loadコマンドが17.9.3以降で導入されました。このコマンドを使用すると、管理者は各サイトタグの予期される負荷を事前に定義できます。これは、キャンパスのシナリオを処理する場合、または複数のブランチオフィスで、それぞれが異なるAP数にマッピングされている場合に、負荷がWNCD全体に均等に分散されるようにするのに特に便利です。

たとえば、9800-40があり、1つの本社と5つの支社を処理し、AP数が異なる場合、設定は次のようになります。

```
wireless tag site office-main
 load 120
```

```
wireless tag site branch-1
 load 10

wireless tag site branch-2
 load 12

wireless tag site branch-3
 load 45

wireless tag site branch-4
 load 80

wireless tag site branch-5
 load 5
```

このシナリオでは、本社のタグをbranch-3およびbranch-4と同じWNCDに配置せず、合計6つのサイトタグを配置し、プラットフォームに5つのWNCDを配置します。したがって、ロードされたサイトタグの中で最も高いタグが同じCPUに配置される可能性があります。loadコマンドを使用すると、予測可能なAPロードバランシングトポロジを作成できます。

loadコマンドは予期されるサイズのヒントであり、APカウントと正確に一致する必要はありませんが、通常は加入する可能性のある予期されるAPに設定されます。

- 単一のコントローラで処理される大規模な建物があるシナリオでは、その特定のプラットフォームのWNCDと同じ数のサイトタグを簡単に作成できます（たとえば、C9800-40には5つ、C9800-80には8つなど）。同じエリアまたはローミングドメイン内のAPを同じサイトタグに割り当てると、WNCD間の通信が最小限に抑えられます。
- RFロードバランシング：RRMからのRFネイバー関係を使用して、WNCDインスタンス間でAPのバランシングを行い、AP同士の距離に応じてサブグループを作成します。この作業は、APがしばらく起動して実行した後で行う必要があり、静的なロードバランス設定を行う必要はありません。これは17.12以降で利用可能です。

## WNCDがいくつあるか調べる方法は？

ハードウェアプラットフォームの場合、WNCDカウントは固定です。9800-40には5が、9800-80には8が割り当てられています。9800CL（仮想）の場合、WNCDの数は、初期導入時に使用される仮想マシンテンプレートによって異なります。

一般的な規則として、システムで実行されているWNCDの数を調べる場合は、すべてのコントローラタイプに対して次のコマンドを使用できます。

<#root>

```
9800-40#show processes cpu platform sorted  |  count wncd
Number of lines which match regexp =
```

**5**

特に9800-CLの場合は、 **show platform software system all** コマンドを使用して仮想プラットフォームの詳細を収集できま

す。

<#root>

9800cl-1#show platform software system all
Controller Details:
==========
VM Template: small
Throughput Profile: low
AP Scale: 1000
Client Scale: 10000

**WNCD instances: 1**

APロードバランシングのモニタリング

APからWNCDへの割り当ては、APのCAPWAP加入プロセス中に適用されるため、すべてのAPが切断されて再加入するネットワーク全体のCAPWAPリセットイベントがない限り、バランシング方式にかかわらず、動作中に変更されることはありません。

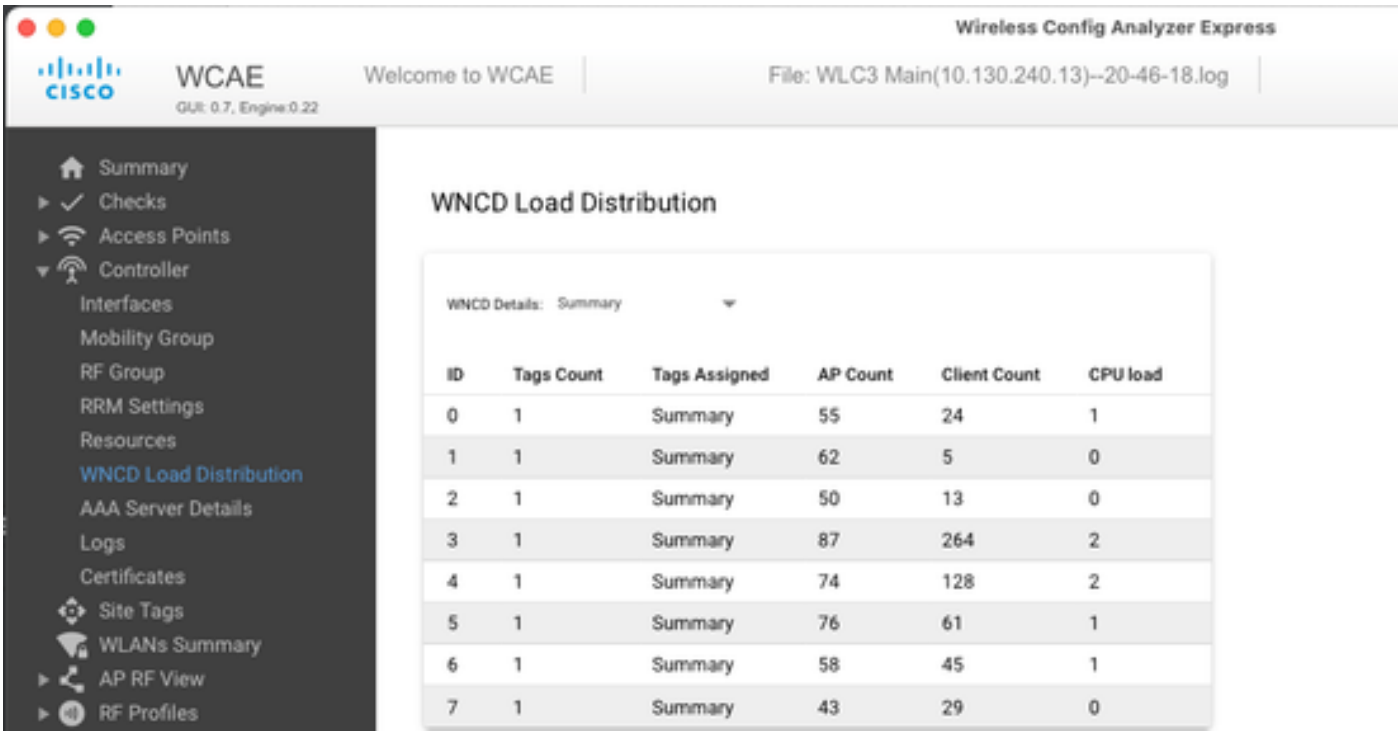
CLIコマンドshow wireless loadbalance tag affinity(登録ユーザ専用)を使用すると、すべてのWNCDインスタンスのAPロードバランスの現在の状態を簡単に確認できます。

98001#show wireless loadbalance tag affinity

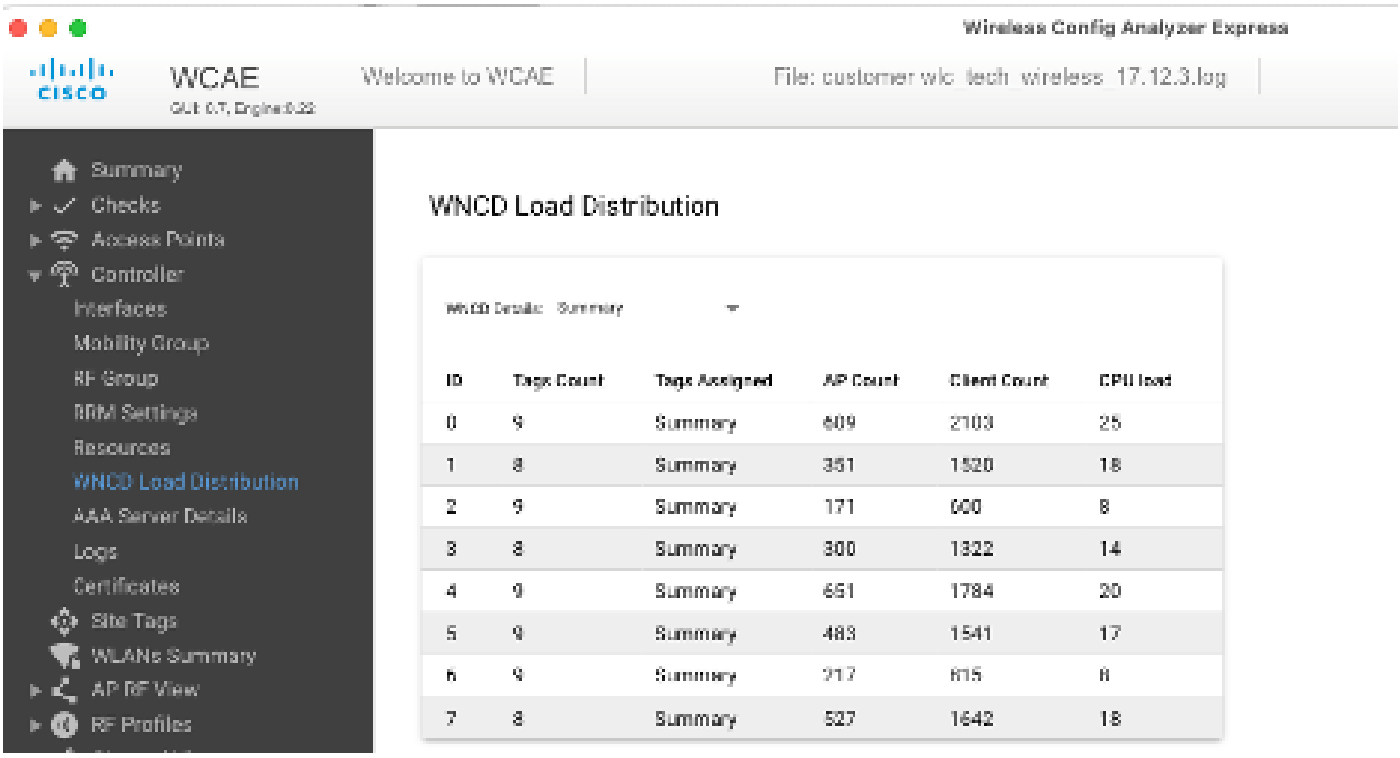
| Tag | Tag type | No of AP's Joined | Load Config | Wncd Instance |
|---|---|---|---|---|
| Branch-tag | SITE TAG | 10 | 0 | 0 |
| Main-tag | SITE TAG | 200 | 0 | 1 |
| default-site-tag | SITE TAG | 1 | NA | 2 |

show tech wireless apの分散をクライアント数とCPUの負荷に関連付ける場合、最も簡単な方法はWCAEサポートツールを使用して、ビジー時に実行したトラフィックをロードする方法です。このツールは、関連付けられている各APから取得したWNCDクライアント数を要約します。

使用率が低くクライアント数が少ない場合の、適切にバランスのとれたコントローラの例：




通常のCPU使用率を示す、より負荷の高いコントローラの別の例：




推奨されるAPロードバランシングメカニズムは何ですか。

つまり、さまざまなオプションを次にまとめることができます。

- 小規模ネットワーク、高速ローミング不要、コントローラ負荷の40 %未満：デフォルトタグ。
- 高速ローミングが必要な場合(OKC、FT、CCKM)、または大きなクライアント数：

- 単一の建物：CPUと同じ数のサイトタグを作成（プラットフォームによって異なる）
- 17.12より前、または500未満のAP数：複数の建物、ブランチ、または大規模キャンパス：物理RFロケーションごとにサイトタグを作成し、サイトごとにloadコマンドを設定します。
- 17.12以降（500を超えるAPがある場合）:RFロードバランシングを使用します。

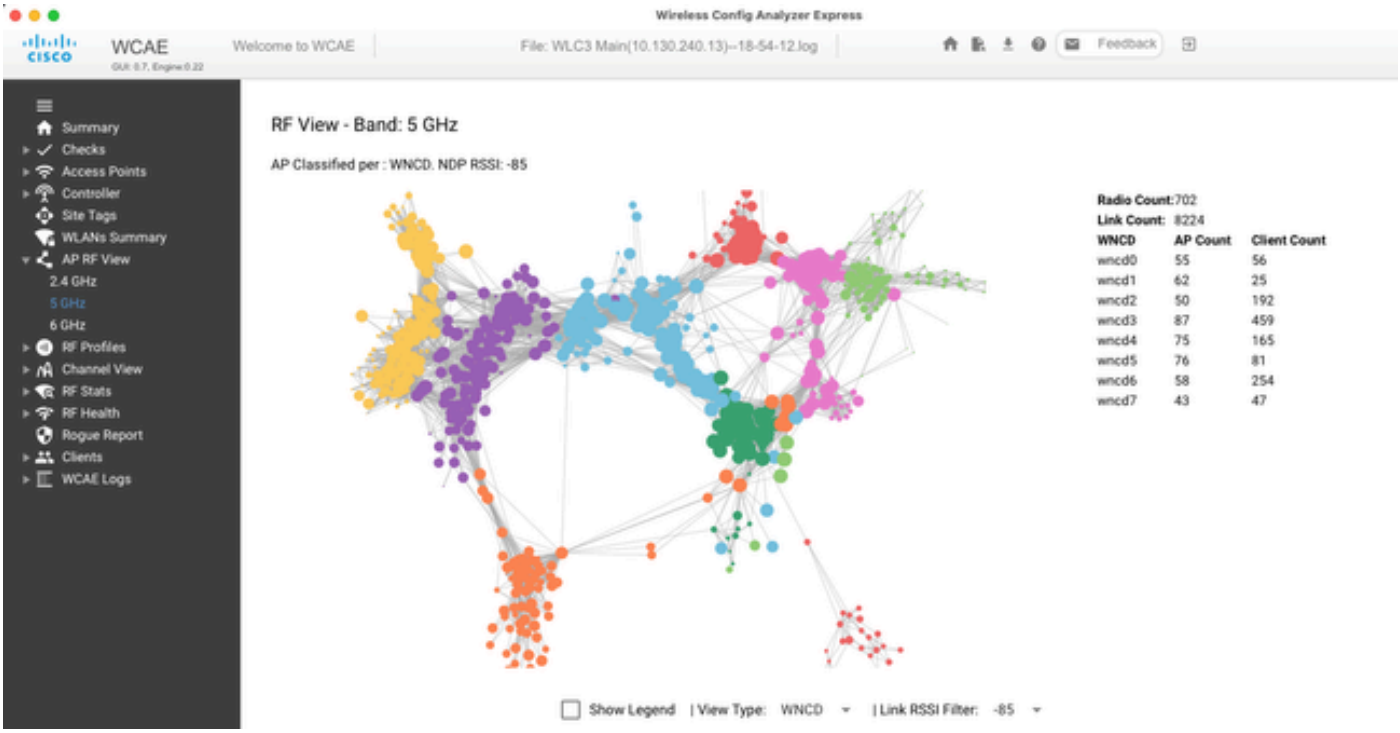
この500個のAPしきい値は、デフォルトで100ユニットのブロックにAPをグループ化するため、ロードバランシングメカニズムの適用が有効な場合にマーキングされます。

AP WNCD配信の可視化

より高度なAPバランシングを実行する必要があり、APがCPU間でどのように分散されるかをきめ細かく制御することが望ましいシナリオがあります。たとえば、キーの負荷メトリックがクライアント数である高密度シナリオと、単にシステム内に存在するAPの数だけを対象とするシナリオです。

この状況の良い例は大規模なイベントです。1つの建物が数千台のクライアント（数百AP以上）をホストしている場合は、負荷を可能な限り多くのCPUに分散する必要がありますが、同時にローミングを最適化する必要があります。そのため、必要でない限りWNCDを介してローミングしません。異なるWNCDまたはサイトタグの複数のAPが同じ物理的な場所に混在するような「ソルトアンドペッパー」の状況を防ぐ必要があります。

WCAEツールを使用してAP RFビュー機能を利用すると、分散の微調整や視覚化が容易になります。



これにより、単にView TypeをWNCDに設定するだけで、AP/WNCD分散を確認できます。ここで、各色はWNCD/CPUを表します。また、RSSIフィルタを–85に設定して、コントローラのRRMアルゴリズムによってフィルタリングされる低信号の接続を回避することもできます。

前の例では、Ciscolive EMEA 24に対応し、ほとんどの隣接APが同じWNCD内で適切にクラスタ化され、クロスオーバーラップが非常に限られていることがわかります。

同じWNCDに割り当てられているサイトタグは、同じ色になります。

## コントロールプレーンのCPU使用率のモニタリング

Cisco IOS-XEアーキテクチャの概念を覚えておくことが重要です。CPU使用率には2つの主要な「ビュー」があることに留意してください。1つはCisco IOSのサポート履歴で、もう1つは主なサポート履歴で、すべてのプロセスとコアのCPUを包括的に把握できます。

通常は、show processes cpu platform sortedコマンドを使用してCisco IOS-XEのすべてのプロセスに関する詳細情報を収集できます。

```
9800cl-1#show processes cpu platform sorted

CPU utilization for five seconds:  8%, one minute: 14%, five minutes: 11%
Core 0: CPU utilization for five seconds:  6%, one minute: 11%, five minutes:  5%
Core 1: CPU utilization for five seconds:  2%, one minute:  8%, five minutes:  5%
Core 2: CPU utilization for five seconds:  4%, one minute: 12%, five minutes: 12%
Core 3: CPU utilization for five seconds: 19%, one minute: 23%, five minutes: 24%
  Pid    PPid    5Sec    1Min    5Min  Status       Size  Name
--------------------------------------------------------------------------------
 19953   19514    44%    44%    44%  S          190880  ucode_pkt_PPE0
 28947    8857     3%    10%     4%  S         1268696  linux_iosd-imag
 19503   19034     3%     3%     3%  S          247332  fman_fp_image
 30839       2     0%     0%     0%  I               0  kworker/0:0
 30330   30319     0%     0%     0%  S            5660  nginx
 30329   30319     0%     1%     0%  S           20136  nginx
 30319   30224     0%     0%     0%  S           12480  nginx
 30263       1     0%     0%     0%  S            4024  rotee
 30224    8413     0%     0%     0%  S            4600  pman
 30106       2     0%     0%     0%  I               0  kworker/u11:0
 30002       2     0%     0%     0%  S               0  SarIosdMond
 29918   29917     0%     0%     0%  S            1648  inet_gethost
```

ここでは、いくつかの重要なポイントを強調します。

- ucode_pkt_PPE0プロセスは、9800Lおよび9800CLプラットフォーム上のデータプレーンを処理しており、常に使用率が高く、100 %を超えると予想されます。これは実装の一部であり、問題にはなりません。

- ピーク時の使用率と持続的な負荷を区別し、特定のシナリオで予想される結果を特定することが重要です。たとえば、show tech wirelessのように非常に大きなCLI出力を収集すると、IOSd、smand、pubdプロセスにピーク負荷が発生する可能性があります。非常に大きなテキスト出力が収集され、数百のCLIコマンドが実行されるためです。これは問題ではなく

、出力が完了すると負荷は低下します。

```
  Pid    PPid    5Sec    1Min    5Min  Status       Size  Name
-------------------------------------------------------------------------------
 19371   19355    62%     83%     20%  R          128120  smand
 27624   27617    53%     59%     59%  S         1120656  pubd
  4192    4123    11%      5%      4%  S         1485604  linux_iosd-imag
```

- クライアントのアクティビティが高い時間帯には、WNCDコアの使用率のピークが予想されます。80 %のピークは機能に影響を与えることなく確認できますが、通常は問題になりません。

```
  Pid    PPid    5Sec    1Min    5Min  Status       Size  Name
-------------------------------------------------------------------------------
 21094   21086    25%     25%     25%  S          978116  wncd_0
 21757   21743    21%     20%     20%  R         1146384  wncd_4
 22480   22465    18%     18%     18%  S         1152496  wncd_7
 22015   21998    18%     17%     17%  S          840720  wncd_5
 21209   21201    16%     18%     18%  S          779292  wncd_1
 21528   21520    14%     15%     14%  S          926528  wncd_3
```

- プロセスのCPU使用率が90 %を超える状態が15分以上続く場合は、調査が必要です。

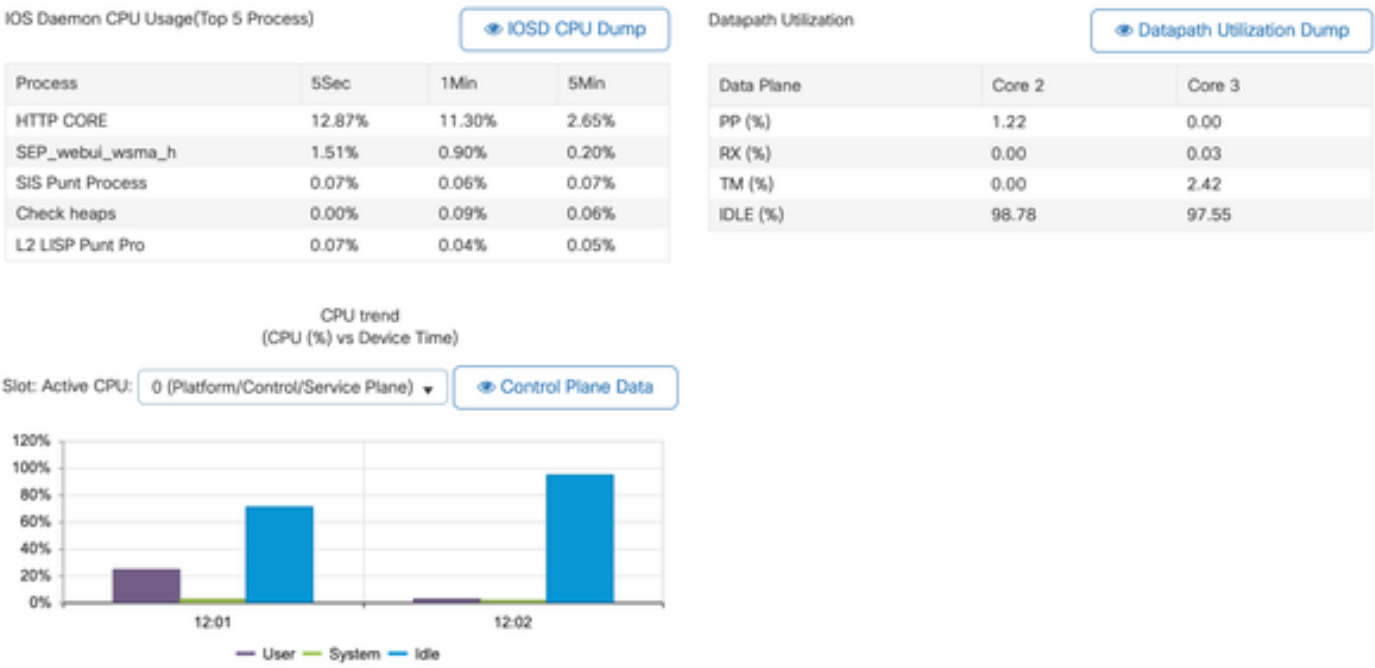
- show processes cpu sortedコマンドで、IOSdのCPU使用率を監視できます。これは、Cisco IOS-XEリストのlinux_iosd-imagプロセス部分のアクティビティに対応します。

```
9800cl-1#show processes cpu sorted

CPU utilization for five seconds: 2%/0%; one minute: 3%; five minutes: 3%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 215         81          88        920  1.51%  0.12%  0.02%   1 SSH Process
 673     164441     7262624         22  0.07%  0.00%  0.00%   0 SBC main process
 137    2264141   225095413         10  0.07%  0.04%  0.05%   0 L2 LISP Punt Pro
 133     534184    21515771         24  0.07%  0.04%  0.04%   0 IOSXE-RP Punt Se
 474    1184139    56733445         20  0.07%  0.03%  0.00%   0 MMA DB TIMER
   5          0           1          0  0.00%  0.00%  0.00%   0 CTS SGACL db cor
   6          0           1          0  0.00%  0.00%  0.00%   0 Retransmission o
   2     198433      726367        273  0.00%  0.00%  0.00%   0 Load Meter
   7          0           1          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
  10    3254791      586076       5553  0.00%  0.11%  0.07%   0 Check heaps
```

```
 4       57       15      3800  0.00%  0.00%  0.00%   0 RF Slave Main Th
 8       0        1          0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
```

- 9800 GUIを使用して、IOSdの負荷、コアごとの使用状況、およびデータプレーンの負荷をすばやく表示できます。




これは、[Monitoring/System/CPU Utilization]タブで使用できます。

各プロセスとは何ですか。

正確なプロセスリストは、コントローラモデルとCisco IOS-XEバージョンによって異なります。これは重要なプロセスの一部を示したものであり、すべてのエントリを網羅するものではありません。

| プロセス名 | それは何をしますか？ | 評価 |
|---|---|---|
| wncd_x | ほとんどの無線操作を処理します。9800モデルに応じて、1 ~ 8のインスタンスを作成できます | 混雑時に高使用率のピークが見られることがあります。使用率が95%以上上昇し続けている場合は、数分間報告します。 |
| linux_iosd-imag | IOSプロセス | 大規模なCLI出力を収集する場合、高い使用率が予想される(show tech)<br><br>SNMP操作が多すぎたり頻繁すぎたりすると、CPU使用率が高くな |

| | | |
|---|---|---|
| | | る可能性がある |
| nginx | Webサーバ | このプロセスはピークを示すことがあるため、高負荷が続いている場合にのみ報告する必要があります |
| ucode_pkt_PPE0 | 9800CL/9800Lのデータプレーン | このコンポーネントを監視するには、 **show platform hardware chassis active qfp datapath utilization** コマンドを使用します |
| エズマン | インターフェイス用チップセットマネージャー | この状態でCPUの使用率が高い場合は、ハードウェアの問題か、カーネルソフトウェアの問題である可能性があります。これは報告されるべきです |
| dbm | データベースマネージャ | この状態でCPU使用率が高い状態が続いていることが報告されます。 |
| odm_X | Operation Data Managerは複数のプロセスにまたがる統合データベースを処理 | 負荷の高いシステムでは高いCPU使用率が予想される |
| 不正な | 不正機能の処理 | この状態でCPU使用率が高い状態が続いていることが報告されます。 |
| smand | Shell Manager.CLIの解析と異なるプロセス間でのインタラクションを処理 | 大きなCLI出力の処理中に高いCPU使用率が予想される。負荷がない状態でCPU使用率が高い状態が続いている場合は、報告する必要があります |
| emd | Shell Manager.CLIの解析と異なるプロセス間でのインタラクションを処理 | 大きなCLI出力の処理中に高いCPU使用率が予想される。負荷がない状態でCPU使用率が高い状態が続いていることが報告されます |

| | | |
|---|---|---|
| | | 。 |
| パブ | テレメトリ処理の一部 | 大規模なテレメトリサブスクリプションではCPUの使用率が高くなることが予想されます。負荷がない状態でCPU使用率が高い状態が続いていることが報告されます。 |

高CPU保護メカニズム

Catalyst 9800ワイヤレスLANコントローラには、ネットワークまたはワイヤレスクライアントアクティビティに関する広範な保護メカニズムがあり、偶発的または意図的なシナリオによる高CPU使用率を防止します。問題のあるデバイスの封じ込めに役立つ、いくつかの主要な機能が設計されています。

クライアント除外

これはデフォルトで有効になっており、ワイヤレス保護ポリシーの一部であり、ポリシープロファイルごとに有効または無効にできます。これにより、いくつかの異なる動作の問題を検出し、クライアントをネットワークから削除し、「一時的な除外リスト」に設定できます。クライアントがこの除外状態にある間、APはクライアントと通信しないため、それ以上の操作ができなくなります。

除外タイマーが経過した後（デフォルトでは60秒）、クライアントは再度関連付けを許可されます。

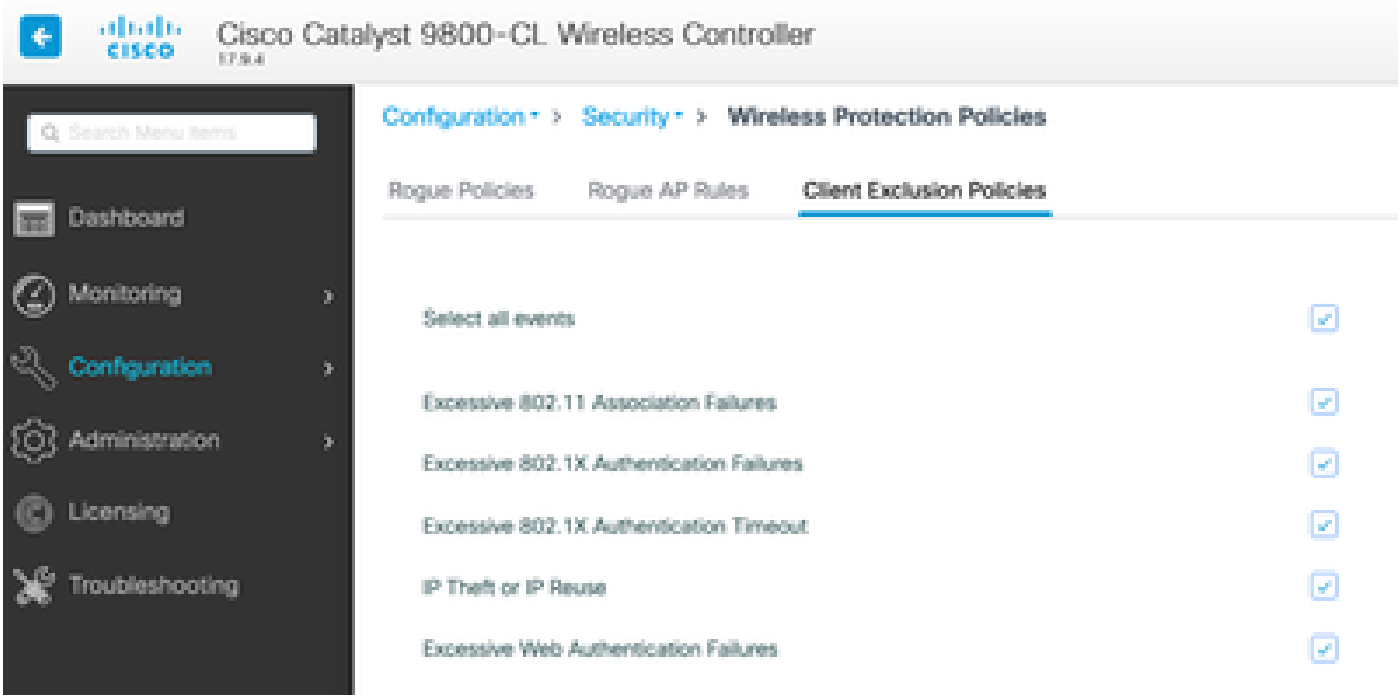
クライアントの除外には、次の複数のトリガーがあります。

- アソシエーションの失敗が繰り返される
- 3つ以上のWebAuth、PSK、または802.1x認証エラー
- 認証タイムアウトの繰り返し（クライアントからの応答なし）
- 別のクライアントにすでに登録されているIPアドレスを再利用しようとする
- ARPフラッドの生成

クライアントを除外すると、CPU使用率が高くなる可能性のある複数のアクティビティの高いタイプから、コントローラ、AP、およびAAAインフラストラクチャ(Radius)が保護されます。一般に、トラブルシューティングの演習や互換性の要件で必要な場合を除き、除外方法を無効にすることは推奨されません。

デフォルト設定はほとんどのケースに対して有効で、例外シナリオに対してのみ有効です。除外時間を長くするか、特定のトリガーを無効にする必要があります。たとえば、一部のレガシークライアントや特殊なクライアント（IOT/医療）では、クライアント側の不具合に簡単にパッチを適用できないため、アソシエーション障害のトリガーを無効にする必要がある場合があります

トリガーは、UIのConfiguration/Wireless Protection/Client Exclusion Policiesでカスタマイズできます。




ARP除外トリガーは、グローバルレベルで永続的に有効になるように設計されていますが、各ポリシープロファイルでカスタマイズできます。sh wireless profile policy allコマンドを使用してステータスを確認し、次の特定の出力を探すことができます。

```
ARP Activity Limit
  Exclusion                 : ENABLED
  PPS                       : 100
  Burst Interval            : 5
```

データトラフィックからのコントロールプレーン保護

これは、コントロールプレーンに送信されるトラフィックが事前に定義されたしきい値セットを超えないようにするための、データプレーンの高度なメカニズムです。この機能は「パントポリサー」と呼ばれ、ほぼすべてのシナリオにおいて、これらの機能に触れる必要はなく、シスコサポートと連携している間にのみ行う必要があります。

この保護の利点は、ネットワークで何が行われているか、およびレートが上昇しているか、または1秒あたりのパケット数が予想外に多い特定のアクティビティがあるかどうかを非常に詳細に把握できることです。

これはCLIを通じてのみ公開されます。通常、これらの機能は変更が必要になることはめったになく、高度な機能の一部であるためです。

すべてのパントポリシーを表示するには、次の手順を実行します。

```
9800-l#show platform software punt-policer

Per Punt-Cause Policer Configuration and Packet Counters
Punt                          Config Rate(pps)     Conform Packets              Dropped Packets              Config Burst(pkts)  Config Alert
Cause  Description              Normal   High     Normal         High          Normal         High          Normal   High     Normal   High
-------------------------------------------------------------------------------------------------------------------------------------------------
```

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | IPv4 Options | 874 | 655 | 0 | 0 | 0 | 0 | 874 | 655 | Off | Off |
| 3 | Layer2 control and legacy | 8738 | 2185 | 33 | 0 | 0 | 0 | 8738 | 2185 | Off | Off |
| 4 | PPP Control | 437 | 1000 | 0 | 0 | 0 | 0 | 437 | 1000 | Off | Off |
| 5 | CLNS IS-IS Control | 8738 | 2185 | 0 | 0 | 0 | 0 | 8738 | 2185 | Off | Off |
| 6 | HDLC keepalives | 437 | 1000 | 0 | 0 | 0 | 0 | 437 | 1000 | Off | Off |
| 7 | ARP request or response | 437 | 1000 | 0 | 330176 | 0 | 0 | 437 | 1000 | Off | Off |
| 8 | Reverse ARP request or repso | 437 | 1000 | 0 | 24 | 0 | 0 | 437 | 1000 | Off | Off |
| 9 | Frame-relay LMI Control | 437 | 1000 | 0 | 0 | 0 | 0 | 437 | 1000 | Off | Off |
| 10 | Incomplete adjacency | 437 | 1000 | 0 | 0 | 0 | 0 | 437 | 1000 | Off | Off |
| 11 | For-us data | 40000 | 5000 | 442919246 | 203771 | 0 | 0 | 40000 | 5000 | Off | Off |
| 12 | Mcast Directly Connected Sou | 437 | 1000 | 0 | 0 | 0 | 0 | 437 | 1000 | Off | Off |

ソフトウェアのバージョンによっては、160エントリを超える大きなリストになる場合があります。

テーブルの出力で、ドロップされたパケットのカラムと、ドロップ数が多いエントリを調べます。このカラムには、ゼロ以外の値が入っています。

データ収集を簡素化するには、show platform software punt-policer drop-onlyコマンドを使用して、ドロップのあるポリサーエントリだけをフィルタリングします。

この機能は、ARPストームまたは802.11プローブのフラッド ( キュー「LFTSへの802.11パケット」を使用 ) があるかどうかを特定するのに役立つ可能性があります。LFTSはLinux Forwarding Transport Serviceの略です)。

ワイヤレスコールアドミッション制御

最近のすべてのメンテナンスリリースで、コントローラにはアクティビティモニタが搭載されており、高いCPU使用率に動的に対応し、持続不可能なプレッシャーにさらされてもAP CAPWAPトンネルがアクティブな状態を維持します。

この機能は、WNCDの負荷をチェックし、新しいクライアントアクティビティのスロットリングを開始して、既存の接続を処理し、CAPWAPの安定性を保護するために十分なリソースが残っていることを確認します。

これはデフォルトで有効になっており、設定オプションはありません。

定義されている3つのレベルの保護があります。L1では80 %の負荷、L2では85 %の負荷、L3では89 %の負荷であり、それぞれ異なる着信プロトコル廃棄を保護メカニズムとしてトリガーします。負荷が減少するとすぐに、保護は自動的に削除されます。

正常なネットワークでは、L2またはL3のロードイベントは表示されません。これらが頻繁に発生する場合は、調査する必要があります。

モニタするには、図に示すようにwireless stats cacコマンドを使用します。

```
9800-l#  show wireless stats cac

WIRESLESS CAC STATISTICS
-----------------------------------------------
L1 CPU Threshold: 80        L2 CPU Threshold: 85        L3 CPU Threshold: 89
Total Number of CAC throttle due to IP Learn:  0
Total Number of CAC throttle due to AAA:       0
Total Number of CAC throttle due to Mobility Discovery:  0
Total Number of CAC throttle due to IPC:       0
```

CPU Throttle Stats
L1-Assoc-Drop: 0 L2-Assoc-Drop: 0 L3-Assoc-Drop: 0
L1-Reassoc-Drop: 0 L2-Reassoc-Drop: 0 L3-Reassoc-Drop: 0
L1-Probe-Drop: 12231 L2-Probe-Drop: 11608 L3-Probe-Drop: 93240
L1-RFID-Drop: 0 L2-RFID-Drop: 0 L3-RFID-Drop: 0
L1-MDNS-Drop: 0 L2-MDNS-Drop: 0 L3-MDNS-Drop: 0

mDNS保護

mDNSをプロトコルとして使用すると、「ゼロタッチ」方式でデバイス間のサービスを検出できますが、同時に、適切に設定しないと非常にアクティブになり、負荷が大幅に増大する可能性があります。

mDNSは、フィルタリングを行わずに、次のような複数の要因によりWNCDのCPU使用率を簡単に上げることができます。

- mDNSポリシーに無制限の学習が含まれている場合、コントローラはすべてのデバイスが提供するすべてのサービスを取得します。これにより、数百のエントリを含む非常に大規模なサービスリストが作成される可能性があります。
- フィルタリングなしで設定されたポリシー：これにより、コントローラは、これらの大きなサービスリストを、特定のサービスを提供しているユーザを尋ねる各クライアントにプッシュします。
- mDNS固有のサービスの中には、「すべて」のワイヤレスクライアントによって提供されるものもあり、サービスの数とアクティビティが増加しますが、OSバージョンによって異なります。

次のコマンドを使用して、サービスごとのmDNSリストサイズを確認できます。

```
9800-l#  show mdns-sd service statistics
Service Name                                  Service Count
--------------------------------------------------------------------------------
_ipp._tcp.local                               84
_ipps._tcp.local                              52
_raop._tcp.local                              950
_airplay._tcp.local                           988
_printer._tcp.local                           13
_googlerpc._tcp.local                         12
_googlecast._tcp.local                        70
_googlezone._tcp.local                        37
_home-sharing._tcp.local                      7
_cups._sub._ipp._tcp.local                    26
```

これは、どの程度の大きさのクエリーを取得できるかを示す概念であり、単独で問題を示すものではなく、何が追跡されているかを監視する方法を示すものです。

mDNSの設定に関する重要な推奨事項を次に示します。

- mDNSトランスポートを単一のプロトコルに設定します。

9800-1(config)# mdns-sd gateway

9800-1(config-mdns-sd)# transport ipv4

デフォルトではIPv4トランスポートを使用します。パフォーマンスを向上させるために、IPv6またはIPv4のいずれかを使用することをお勧めしますが、両方は使用しません。

- mDNSサービスポリシーでロケーションフィルタを常に設定して、バインドされていないクエリ/応答を回避します。一般に、「site-tag」を使用することをお勧めしますが、必要に応じて他のオプションが機能する可能性があります。

もっと助けが必要だ

CPUの負荷が高く、上記のいずれも役に立たない場合は、ケースを通じてCXに連絡し、このデータを開始点として追加してください。

- 基本データには、AP/コントローラの設定、ネットワークおよびRFの動作値が含まれます。

show tech-support wireless

- すべてのコントローラトレースをアーカイブします。これは、「ブラックボックス」の概念に似た大きなファイルで、次のコマンドを使用して収集できます。

request platform software trace archive last <days> to-file bootflash:<archive file>

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。