

# 無線區域網控制器CPU負載故障排除

## 目錄

---

### [簡介](#)

### [瞭解CPU使用情況](#)

### [平台基礎知識](#)

#### [控制平面](#)

#### [資料平面](#)

### [AP負載平衡](#)

#### [如何確定目前有多少個WNCD？](#)

### [監控AP負載平衡](#)

#### [推薦的AP負載均衡機制是什麼？](#)

#### [AP WNCD分佈視覺化](#)

### [監控控制平面CPU使用情況](#)

#### [每個流程是什麼？](#)

### [高CPU保護機制](#)

#### [使用者端排除](#)

#### [針對資料流量的控制平面保護](#)

#### [無線呼叫准入控制](#)

### [mDNS保護](#)

---

## 簡介

本文說明如何監控Catalyst 9800無線LAN控制器上的CPU使用情況，另外還介紹了幾個配置建議。

## 瞭解CPU使用情況

在您深入瞭解CPU負載疑難排解之前，您必須先瞭解Catalyst 9800無線LAN控制器中如何使用CPU的基礎知識，以及有關軟體架構的一些詳細資訊。

通常，[Catalyst 9800最佳實踐文檔](#)定義了一組好的配置設定，這些設定可以防止應用程式級問題，例如，對mDNS使用位置過濾或確保始終啟用客戶端排除。建議您將這些建議與此處公開的主題一起應用。

## 平台基礎知識

Catalyst 9800控制器設計為靈活的平台，可針對不同的網路負載，專注於水準擴展。內部開發命名為「eWLC」，e代表「彈性」，表示相同的軟體架構可以從一個小型的單一CPU嵌入式系統運行到多個CPU/核心大型裝置。

每個WLC都有兩個不同的「端」：

- 控制平面：處理所有「管理」互動（如CLI、UI、Netconf）以及客戶端和AP的所有自註冊過程。
- 資料層面：負責實際的資料包轉發和CAPWAP解封、AVC策略實施等功能。

## 控制平面

- 大多數Cisco IOS-XE進程在BinOS（Linux核心）下運行，擁有自己的專用排程程式和監控命令。
- 有一組稱為無線網路控制常駐程式(WNCD)的重要處理作業，每個處理作業都有一個本機記憶體資料庫，可處理大部分的無線活動。每個CPU都擁有一個WNCD，可將負載分散到每個系統的所有可用CPU核心
- WNCD之間的負載分配在AP加入期間完成。當AP執行CAPWAP加入控制器時，內部負載平衡器使用一組可能的規則分配AP，以確保正確使用所有可用的CPU資源。
- Cisco IOS® 代碼在稱為IOSd的自身進程中運行，並且有其CPU排程程式和監控命令。這可以處理特定的功能，例如CLI、SNMP、多點傳送和路由。

在簡化檢視中，控制器具有控制和資料平面之間的通訊機制，「傳送」，將流量從網路傳送到控制平面，「注入」，將幀從控制平面傳送到網路。

作為可能的CPU使用率較高故障排除調查的一部分，您需要監控傳送機制，以評估哪些流量正在到達控制平面並可能導致高負載。

## 資料平面

對於Catalyst 9800控制器，這是作為Cisco資料包處理器(CPP)的一部分運行的，CPP是開發資料包轉發引擎的軟體架構，用於多種產品和技術。

該架構允許跨不同硬體或軟體實施提供通用功能集，例如，允許9800CL與9800-40的類似功能在不同吞吐量級別使用。

## AP負載平衡

在CAPWAP AP加入過程中，WLC在CPU之間執行負載均衡，關鍵區別點是AP站點標籤名稱。其思想是每個AP代表一個特定CPU負載（來自其客戶端活動）和AP本身。有幾種機制可以執行此平衡：

- 如果AP使用「default-tag」，則會以循環方式在所有CPU/WNCD之間平衡，每個新AP加入都會進入下一個WNCD。這是最簡單的方法，但影響不大：
  - 這是次優方案，因為同一RF漫遊域中的AP會頻繁進行WNCD間漫遊，包括額外的進程間通訊。執行處理間的漫遊速度會比較慢。
  - 對於FlexConnect（遠端）站點標籤，無可用的PMK金鑰分發。這意味著您無法對Flex模式執行快速漫遊，從而影響OKC/FT漫遊模式。

通常，預設標籤可用於低負載方案（例如，低於9800平台的40%的AP和客戶端負載），並且僅在不需要快速漫遊時用於FlexConenct部署。

- 如果AP具有自定義站點標籤，則屬於站點標籤名稱的AP首次加入控制器時，會將站點標籤分配給特定WNCD例項。具有相同標籤的所有後續附加AP加入將分配到同一個WNCD。這可以確保在同一站點標籤中的AP間漫遊，在單個WCND上下文中進行，從而提供更加最佳化的流和CPU使用率更低。支援跨WNCD漫遊，這與WNCD內漫遊不同。
- 預設負載平衡決策：將標籤分配給WNCD時，負載平衡器將選擇此時站點標籤計數最低的例項。因為不知道該站點標籤可能具有的總負載，所以可能導致次優平衡方案。這取決於AP加入的順序、已定義的站點標籤數量，以及它們之間的AP計數是否不對稱
- 靜態負載平衡：為了防止不平衡的站點標籤分配給WNCD，在17.9.3及更高版本中引入了site load命令，以允許管理員預先定義每個站點標籤的預期負載。這在處理園區場景或多個分支機構（每個分支機構對映到不同的AP計數）時特別有用，以確保負載在WNCD之間均勻分佈。

例如，如果您使用一台9800-40，處理一個總部，再加上5個分支機構，並且有不同的AP數量，則配置可能如下所示：

```
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
```

在此場景中，您不希望主辦公室標籤與branch-3和branch-4位於同一個WNCD上，總共有6個站點標籤，並且平台有5個WNCD，因此負載最高的站點標籤可能會位於同一個CPU上。透過使用load命令，您可以建立可預測的AP負載均衡拓撲。

load命令是預期的大小提示，它不必完全匹配AP計數，但它通常設定為可能加入的預期AP。

- 在單一控制器處理大型建築的情況下，僅為該特定平台建立與WNCD數量相同的站點標籤會更容易、更簡單（例如，C9800-40有5個，C9800-80有8個）。將同一區域或漫遊域中的AP分配到同一站點標籤，以最大程度地減少WNCD之間的通訊。
- RF負載平衡：使用RRM的RF鄰居關係，在WNCD例項間平衡AP，並根據AP彼此的接近程度建立子組。必須在AP已啟動並運行一段時間後執行此操作，並且無需配置任何靜態負載均衡設定。此版本適用於17.12及更高版本。

如何確定目前有多少個WNCD？

對於硬體平台，WNCD計數是固定的：9800-40有5,9800-80有8。對於9800CL（虛擬），WNCD的數量取決於初始部署期間使用的虛擬機器模板。

一般而言，如果您想瞭解系統中正在運行的WNCD數量，可以將此命令用於所有控制器型別：

<#root>

```
9800-40#show processes cpu platform sorted | count wncd
Number of lines which match regexp =
5
```

具體而言，對於9800-CL，您可以使用命令 `show platform software system all` 來收集虛擬平台上的詳細資訊：

<#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**

### 監控AP負載平衡

AP到WNCD分配是在AP CAPWAP加入過程中應用的，因此無論採用何種平衡方法，在操作過程中都不會發生更改，除非存在全網路CAPWAP重置事件，其中所有AP都斷開連線並重新加入。

使用CLI命令`show wireless loadbalance tag affinity`可以輕鬆檢視所有WNCD例項的AP負載均衡的當前狀態：

```
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
```

如果要將AP分佈與客戶端計數和CPU負載相關聯，最簡單的方法是使用[WCAE](#)支援工具，並載入繁忙時段拍攝的`show tech wireless`。該工具彙總了來自與其關聯的每個AP的WNCD客戶端計數。

適當平衡的控制器範例，在使用率及使用者端計數較低時：

Wireless Config Analyzer Express

WCAE Welcome to WCAE File: WLC3 Main(10.130.240.13)--20-46-18.log  
GUI: 0.7, Engine:0.22

Summary  
Checks  
Access Points  
Controller  
Interfaces  
Mobility Group  
RF Group  
RRM Settings  
Resources  
WNCD Load Distribution  
AAA Server Details  
Logs  
Certificates  
Site Tags  
WLANs Summary  
AP RF View  
RF Profiles

### WNCD Load Distribution

WNCD Details: Summary

ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load
0	1	Summary	55	24	1
1	1	Summary	62	5	0
2	1	Summary	50	13	0
3	1	Summary	87	264	2
4	1	Summary	74	128	2
5	1	Summary	76	61	1
6	1	Summary	58	45	1
7	1	Summary	43	29	0

另一個範例是對於負載較多的控制器，顯示一般CPU使用率：

Wireless Config Analyzer Express

WCAE Welcome to WCAE File: customer wlc\_tech\_wireless\_17.12.3.log  
GUI: 0.7, Engine:0.22

Summary  
Checks  
Access Points  
Controller  
Interfaces  
Mobility Group  
RF Group  
RRM Settings  
Resources  
WNCD Load Distribution  
AAA Server Details  
Logs  
Certificates  
Site Tags  
WLANs Summary  
AP RF View  
RF Profiles

### WNCD Load Distribution

WNCD Details: Summary

ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load
0	9	Summary	609	2103	25
1	8	Summary	351	1520	18
2	9	Summary	171	600	8
3	8	Summary	300	1322	14
4	9	Summary	651	1784	20
5	9	Summary	483	1541	17
6	9	Summary	217	615	6
7	8	Summary	527	1642	18

推薦的AP負載均衡機制是什麼？

簡而言之，您可以在下列各項中總結不同的選項：

- 小型網路，無需快速漫遊，控制器負載不到40%：預設標籤。
- 如果需要快速漫遊(OKC、FT、CCKM)或大型客戶端數量：

- 單一組建：建立與CPU數量相同的月台標籤（視平台而定）
- 在17.12之前，或少於500個AP計數：多個建築物、分支機構或大型園區：為每個物理RF位置建立一個站點標籤，並為每個站點配置負載命令。
- 500多個AP的17.12和更高版本：使用RF負載均衡。

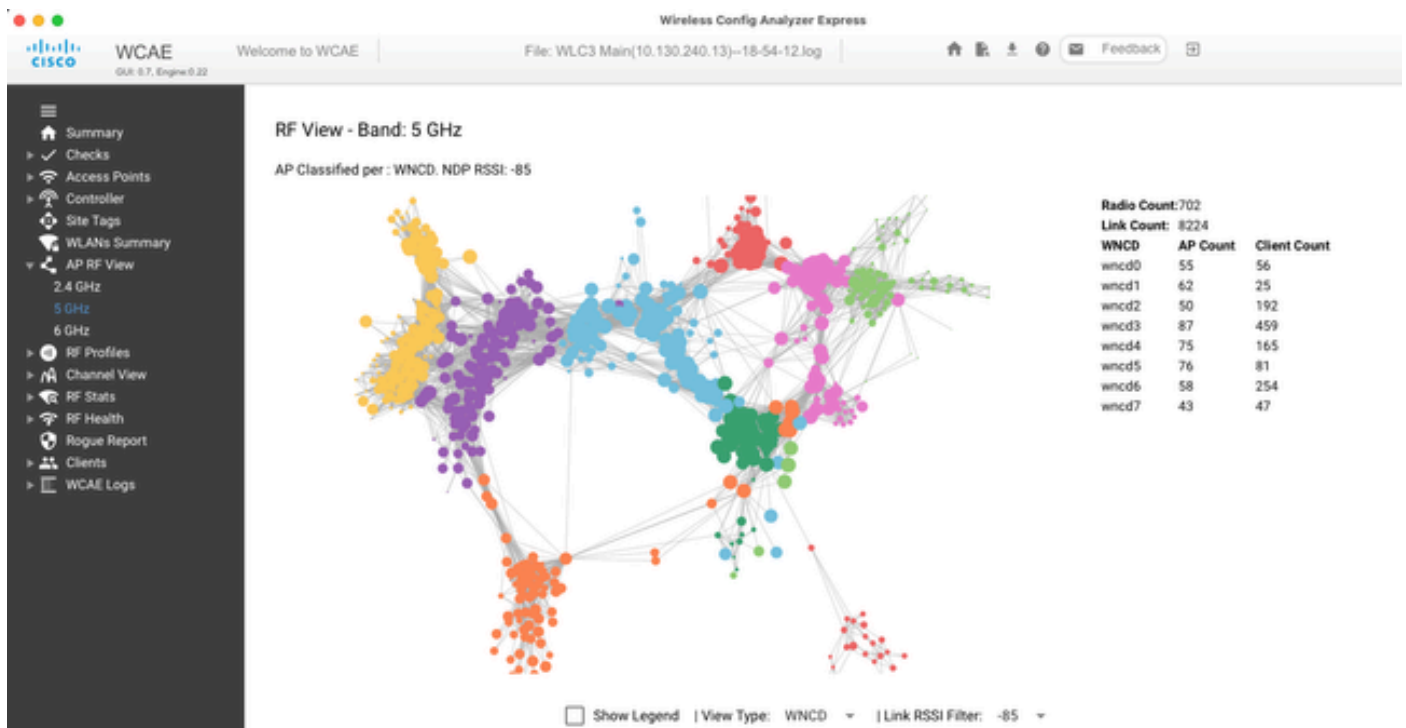
此500 AP閾值用於標籤應用負載均衡機制何時有效，因為預設情況下它將AP分組為100個單元的塊。

### AP WNCID分佈視覺化

有些情況需要執行更高級的AP均衡，最好對AP如何在CPU之間分佈進行精細控制，例如，在非常高密度的情況下，關鍵負載度量是客戶端計數，而不僅僅關注系統中存在的AP數量。

大型活動就是一個很好的例子：一個建築可以託管數千個客戶端，以及數百個AP，並且您需要將負載分配到儘可能多的CPU，但需要同時最佳化漫遊。因此，除非有需要，否則您不會在廣域網中漫遊。您想要避免在相同的物理位置混合不同WNCID/站點標籤中的多個AP的「鹽和胡椒」情況。

為了幫助微調並提供分佈視覺化，您可以使用WCAE工具，並利用AP RF檢視功能：



這使我們能夠看到AP/WNCID的分發，只需將View Type設定為WNCID。在這裡，每種顏色都代表WNCID/CPU。您也可以將RSSI過濾器設定為-85，以避免低訊號連線，這些連線也由控制器中的RRM演算法過濾。

在上一個與Ciscolive EMEA 24對應的示例中，您可以看到大多數相鄰的AP在同一個WNCD中很好地集群在一起，交叉重疊非常有限。

配置給同一WNCD的網站標籤，取得相同的顏色。

### 監控控制平面CPU使用情況

請務必牢記Cisco IOS-XE架構的概念，並牢記CPU使用情況的兩個主要「檢視」。一個來自歷史上的Cisco IOS支援，另一個是主要支援，它提供跨所有進程和核心的CPU整體檢視。

通常，您可以使用命令show processes cpu platform sorted收集整個Cisco IOS-XE的所有進程的詳細資訊：

```
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

這裡需要強調幾個要點：

- 進程ucode\_pkt\_PPE0處理9800L和9800CL平台上的資料平面，預計該進程將始終保持高利用率，甚至高於100%。這是執行的一部分，不構成問題。
- 區分峰值使用與持續負載並隔離給定場景中的預期情況非常重要。例如，收集非常大的CLI輸出(如show tech wireless)可能會在IOSd、smand和pubd進程上生成峰值負載，因為收集到非常大的文本輸出（並執行數百個CLI命令），這不是問題，輸出完成以後，負載就會下降。

```
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

```

- 預計在高客戶端活動期間，WNCD核心的利用率將達到峰值。可以看到80%的峰值，沒有任何功能影響，而且它們通常不會造成問題。

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

- 必須調查進程的CPU使用率持續高（超過90%，持續15分鐘以上）。
- 您可以使用命令 `show processes cpu sorted` 監控IOSd CPU使用率。這與Cisco IOS-XE清單的linux\_iosd-imag進程部分中的活動相對應。

```
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

```

- 您可以使用9800 GUI快速檢視IOSd負載、每個核心使用情況和資料平面負載：



IOS Daemon CPU Usage(Top 5 Process)

IOSD CPU Dump

Process	5Sec	1Min	5Min
HTTP CORE	12.87%	11.30%	2.65%
SEP_webui_wsma_h	1.51%	0.90%	0.20%
SIS Punt Process	0.07%	0.06%	0.07%
Check heaps	0.00%	0.09%	0.06%
L2 LISP Punt Pro	0.07%	0.04%	0.05%

Datapath Utilization

Datapath Utilization Dump

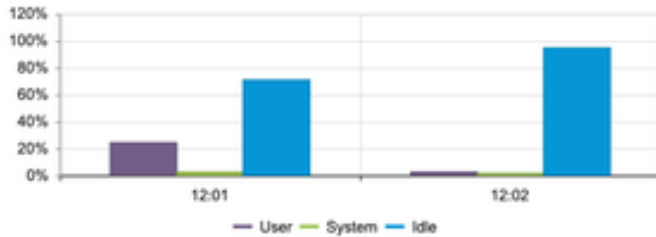
Data Plane	Core 2	Core 3
PP (%)	1.22	0.00
RX (%)	0.00	0.03
TM (%)	0.00	2.42
IDLE (%)	98.78	97.55

CPU trend  
(CPU (%) vs Device Time)

Slot: Active CPU:

0 (Platform/Control/Service Plane)

Control Plane Data



這在Monitoring/System/CPU Utilization頁籤中提供。

每個流程是什麼？

確切的進程清單因控制器型號以及Cisco IOS-XE版本而異。這是一些關鍵進程的清單，並不涵蓋所有可能的條目。

程式名稱	它有什麼作用？	評估
wncd_x	處理大部分的無線操作。視9800模型而定，您可以有1到8個例證	您可能會在繁忙時段看到高使用率的峰值。報告利用率在幾分鐘內是否停滯在95%或以上
linux_iosd-image	IOS進程	如果收集大量CLI輸出，預計會看到高利用率(show tech) 大或過於頻繁的SNMP操作可能導致高CPU
nginx	Web伺服器	此過程可以顯示峰值，並且只應在持續的高負載上報告
ucode_pkt_PPE0	資料平面採用9800CL/9800L	使用命令 <code>show platform hardware chassis active qfp datapath utilization</code> 監視此元件
伊斯曼	適用於介面的晶片組管理員	此處持續的CPU使用率高可能表示

		硬體問題或可能的核心軟體問題。 應該報告
dbm	資料庫管理員	此處應報告持續的高CPU使用率
odm_X	Operation Data Manager跨進程 處理統一資料庫	載入的系統預期的CPU使用率高
勒居德	處理惡意功能	此處應報告持續的高CPU使用率
smand	殼層管理員。處理CLI剖析和跨不 同處理序的互動	處理大量CLI輸出時，預期的 CPU使用率較高。應報告無負載時 的CPU使用率持續偏高
emd	殼層管理員。處理CLI剖析和跨不 同處理序的互動	處理大量CLI輸出時，預期的 CPU使用率較高。應報告無負載時 的持續高CPU使用率
已發佈	遙測處理的一部分	大型遙測訂閱預期的CPU使用率高 。應報告無負載時的持續高CPU使 用率

#### 高CPU保護機制

Catalyst 9800無線LAN控制器具備廣泛的網路或無線使用者端活動保護機制，可避免意外或蓄意的情況造成高CPU使用率。有幾項重要功能旨在幫助您控制有問題的裝置：

#### 使用者端排除

預設情況下，這是啟用的，並且是無線保護策略的一部分，並且可以根據策略配置檔案啟用或停用它。這可以檢測多種不同的行為問題，從網路中移除客戶端，並將其設定為「臨時排除清單」。當客戶端處於此排除狀態時，AP不會與其通訊，從而阻止任何進一步的操作。

排除計時器經過後（預設情況下為60秒），允許客戶端再次關聯。

客戶端排除有幾個觸發因素：

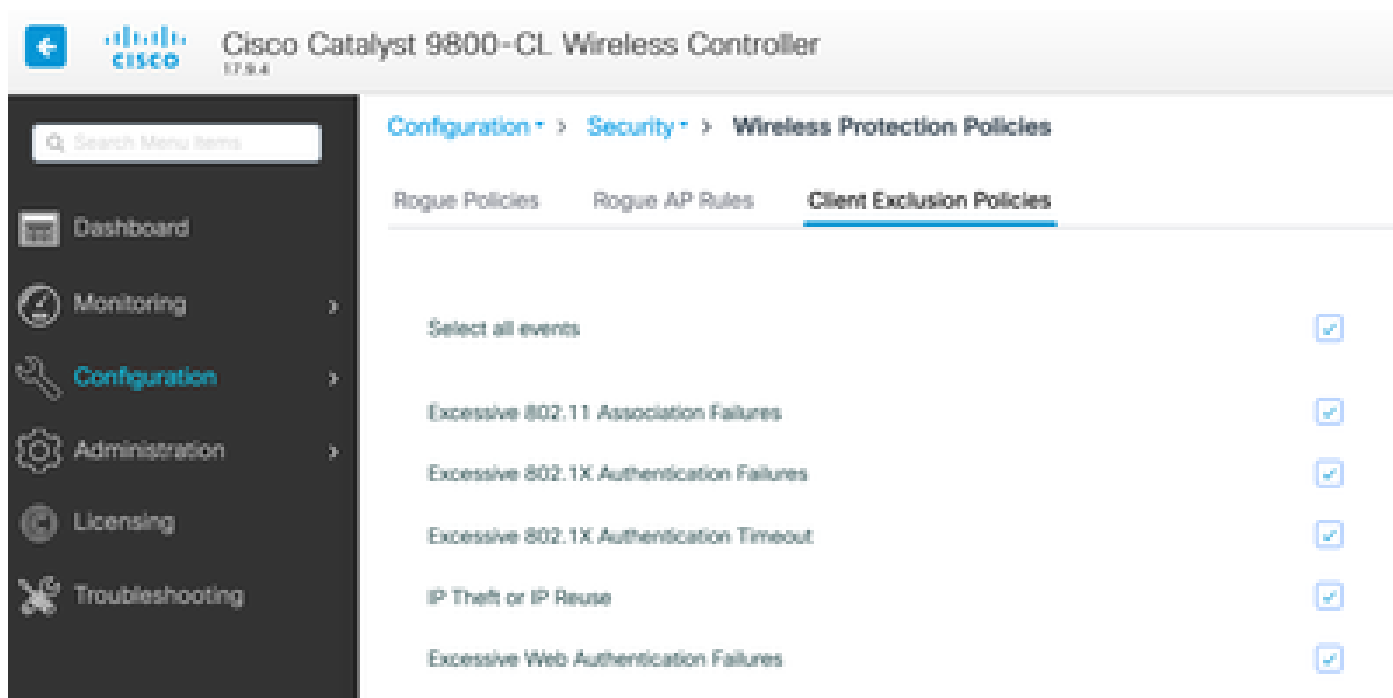
- 反覆的關聯失敗
- 3個或多個webauth、PSK或802.1x驗證錯誤

- 重複的驗證逾時 ( 使用者端沒有回應 )
- 嘗試重複使用已註冊到其他客戶端的IP地址
- 生成ARP泛洪

使用者端排除可保護您的控制器、AP和AAA基礎架構(Radius)不受可能導致高CPU的幾種高活動性型別的影響。一般而言，不建議停用任何排除方法，除非是疑難排解練習或相容性要求所需。

預設設定適用於幾乎所有情況，並且僅在某些特殊情況下才需要增加排除時間或停用某些特定觸發器。例如，由於無法輕鬆修補的客戶端缺陷，某些舊版或專用客戶端(IOT/Medical)可能需要停用關聯失敗觸發器

您可以在UI：配置/無線保護/客戶端排除策略中自定義觸發器：



ARP排除觸發器旨在全局級永久啟用，但可以在每個策略配置檔案中進行自定義。可以使用sh wireless profile policy all命令檢查狀態，以查詢以下特定輸出：

#### ARP Activity Limit

```
Exclusion          : ENABLED
PPS               : 100
Burst Interval    : 5
```

#### 針對資料流量的控制平面保護

這是資料平面中的一種高級機制，用於確保傳送到控制平面的流量不超過預定義的閾值集。此功能稱為「傳送監察器」，在幾乎所有情況下，都不需要觸控它們，即使這樣，也只能在與Cisco支援部門一起工作時使用。

這種保護的優點是，它可以非常詳細地洞察網路中正在發生的情況，以及是否存在任何速率增加或每秒資料包意外增加的特定活動。

這只能透過CLI顯示，因為它們通常是無需修改的高級功能的一部分。

要檢視所有傳送策略，請執行以下操作：

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

Per Punt-Cause Policer Configuration and Packet Counters

Punt Cause	Description	Config Rate(pps)		Conform Packets		Dropped Packets		Config Burst(pkts)		Config Alert	
		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 reposito	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

視軟體版本而定，此清單可能會很大，包含160個以上的專案。

在表輸出中，您想要檢查丟棄的資料包列以及在高丟棄計數上具有非零值的所有條目。

為簡化資料收集，您可以使用命令show platform software punt-policer drop-only僅過濾帶有丟棄的監察器條目。

此功能可用於辨識是否存在ARP風暴或802.11探測泛洪（它們使用隊列「發往LFTS的802.11資料包」）。LFTS代表Linux轉發傳輸服務）。

## 無線呼叫准入控制

在所有最近的維護版本中，控制器都有一個活動監控器，可動態地對CPU使用率過高做出反應，並確保AP CAPWAP隧道在不可持續的壓力下保持活動狀態。

該功能會檢查WNCD負載，並開始限制新客戶端活動，以確保保留足夠的資源來處理現有連線並保護CAPWAP穩定性。

此選項預設為啟用，且沒有組態選項。

定義了三個保護級別：L1為80%負載，L2為85%負載，L3為89%，每個觸發不同的傳入協定丟棄作為保護機制。一旦負載降低，保護將自動移除。

在正常的網路中，您不應看到L2或L3負載事件，如果它們經常發生，則應進行調查。

要使用命令wireless stats cac進行監控，如下圖所示。

```
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作為協定允許「零接觸」方法來跨裝置發現服務，但同時，它也可以非常活躍，如果配置不當，會顯著增加負載。

mDNS無需任何過濾，即可輕鬆提高WNCN CPU利用率，這有以下幾個因素：

- mDNS策略透過無限制的學習，控制器將獲得所有裝置提供的所有服務。這可能導致包含數百條條目的超大型服務清單。
- 未過濾的策略集：這將導致控制器將那些大型服務清單推送到詢問誰提供給定服務的每個客戶端。
- 有些mDNS特定服務由「所有」無線客戶端提供，導致更高的服務數量和活動，但作業系統版本對此有所變化。

您可以使用以下命令檢查每個服務的mDNS清單大小：

```
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

這可以讓您瞭解任意給定查詢可獲取的大小，它本身並不表示問題，只是監控所跟蹤內容的一種方式。

有一些重要的mDNS配置建議：

- 將mDNS傳輸設為單一通訊協定：

```
9800-1(config)# mdns-sd gateway
```

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

依預設，它會使用IPv4傳輸，為了提升效能，建議使用IPv6或IPv4，但不要同時使用兩者：

- 請始終在mDNS服務策略中設定位置過濾器，以避免未繫結的查詢/響應。一般而言，建議使用「site-tag」（站點標籤），但其他選項可能有效，具體取決於您的需要。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。