# 无线局域网控制器CPU负载故障排除

目录

简介 <u>了解CPU使用情况</u> 平台基础知识 <u>控制层面</u> 数据层面 AP负载均衡 <u>如何确定存在多少个WNCD</u> 监控AP负载均衡 <u>推荐的AP负载均衡机制是什么</u> AP WNCD分布虚拟化 监控控制平面CPU使用情况 <u>每个流程是什么</u> 高CPU保护机制 <u>客户端排除</u> 针对数据流量的控制平面保护 无线呼叫准入控制 <u>mDNS保护</u> 我需要更多帮助

## 简介

本文档介绍如何监控Catalyst 9800无线LAN控制器上的CPU使用率,另外还介绍了几项配置建议。

## 了解CPU使用情况

在深入了解CPU负载故障排除之前,您需要了解Catalyst 9800无线LAN控制器中如何使用CPU的基础知识,以及有关软件架构的一些详细信息。

通常,<u>Catalyst 9800最佳实践文档</u>定义了一组可以防止应用级问题的良好配置设置。例如,对 mDNS使用位置过滤,或确保始终启用客户端排除。建议您将这些建议与此处介绍的主题一起应用 。

### 平台基础知识

Catalyst 9800控制器设计为灵活的平台,针对不同的网络负载,专注于水平扩展。内部开发命名为 eWLC和e for elastic,表示同一软件架构能够从小型单CPU嵌入式系统运行到多个CPU/核心大型设 备。

每个WLC都有两个不同的方面:

- 控制层面:处理所有管理交互(如CLI、UI、Netconf)以及客户端和AP的所有自注册过程。
- •数据层面:负责实际数据包转发、解封CAPWAP、AVC策略实施等功能。

#### 控制层面

- 大多数Cisco IOS XE进程在BinOS(Linux内核)下运行,带有其自己的专用调度程序和监控 命令。
- 有一组称为无线网络控制后台守护程序(WNCD)的关键进程,每个进程都有一个本地内存数据 库,用于处理大多数无线活动。每个CPU拥有一个WNCD,以将负载分散到每个系统的所有 可用CPU核心
- WNCD之间的负载分配在AP加入期间完成。当AP执行CAPWAP加入控制器时,内部负载均 衡器使用一组可能的规则分配AP,以确保正确使用所有可用的CPU资源。
- Cisco IOS®代码运行在它自己的名为IOSd的进程上,并且具有CPU调度程序。这涉及特定功能,例如CLI、SNMP、组播和路由。

在简化视图中,控制器在控制平面和数据平面之间具有通信机制,发送、将流量从网络发送到控制 平面,然后注入、将帧从控制平面推送到网络。

作为可能的高CPU故障排除调查的一部分,您需要监控分流机制,以评估哪些流量正在到达控制平 面并可能导致高负载。

#### 数据层面

对于Catalyst 9800控制器,这是作为思科数据包处理器(CPP)的一部分运行的,CPP是用于开发数 据包转发引擎的软件框架,可在多种产品和技术中使用。

该架构允许跨不同的硬件或软件实施使用通用功能集。例如,允许9800CL与9800-40具有类似的功 能,但吞吐量级别不同。

### AP负载均衡

在CAPWAP AP加入过程中,WLC在CPU之间执行负载均衡,关键区别在于AP站点标记名称。其 理念是每个AP代表一个特定CPU负载,该负载来自其客户端活动和AP本身。有多种机制来执行这 种平衡:

- 如果AP使用默认标记,则会在所有CPU/WNCD之间以轮询方式对其进行平衡,每个新AP加入将转至下一个WNCD。这是最简单的方法,但影响不大:
  - 这是次佳方案,因为同一RF漫游域中的AP将频繁进行WNCD间漫游,包括额外的进程 间通信。跨实例漫游的速度较慢,只是略低。
  - 对于FlexConnect(远程)站点标签,无可用的PMK密钥分配。这意味着您不能对 Flex模式执行快速漫游,从而影响OKC/FT漫游模式。

通常,默认标记可用于低负载方案(例如,低于9800平台的AP和客户端负载的 40%),并且仅在不需要快速漫游时用于FlexConnect部署。

• 如果AP具有自定义站点标记,则属于站点标记名称的AP首次加入控制器时,站点标记会分配

给特定WNCD实例。具有相同标记的所有后续附加AP加入都分配到相同的WNCD。这可确保 在同一个站点标签中的AP间漫游,在一个WCND环境中发生,从而提供更优化的流和更低的 CPU使用率。支持在WNCD间漫游,只是不如WNCD内漫游那样理想。

- 默认负载均衡决策:将标签分配给WNCD时,负载均衡器会选择当时站点标签计数最低的实例。由于站点标记可以具有的总负载未知,因此可能导致次优平衡方案。这取决于AP加入的顺序、已定义的站点标签数量,以及它们之间的AP计数是否不对称
- 静态负载平衡:为了防止向WNCD分配不平衡的站点标记,17.9.3及更高版本中引入了site load命令,以允许管理员预定义每个站点标记的预期负载。这在处理园区场景或多个分支机构 (每个分支机构映射到不同的AP计数)时特别有用,可以确保负载在WNCD上均匀分布。

例如,如果您使用9800-40,处理一个主办公室,再加上5个分支办公室,并且有不同的AP计数,则 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
```

在此场景中,您不希望主办公室标记与branch-3和branch-4位于同一WNCD上,总共有6个站点标记 ,并且平台有5个WNCD,因此负载最高的站点标记可能位于同一CPU上。通过使用load命令,您 可以创建可预测的AP负载均衡拓扑。

load命令是预期大小。它不必完全匹配AP计数,但通常设置为可加入的预期AP。

- 在单个控制器处理大型建筑的场景中,仅为该特定平台创建与WNCD同样多的站点标记会更容易、更简单(例如,C9800-40有5个,C9800-80有8个)。将同一区域或漫游域中的AP分配到同一站点标记,以最小化WNCD间通信。
- RF负载均衡:这使用RRM的RF邻居关系来平衡WNCD实例上的AP,并根据AP彼此的接近程度创建子组。必须在AP已启动并运行一段时间后执行此操作,并且无需配置任何静态负载均衡设置。此版本适用于17.12及更高版本。

如何确定存在多少个WNCD

对于硬件平台,WNCD计数是固定的:9800-40有5,9800-80有8。对于9800CL(虚拟),WNCD的 数量取决于初始部署期间使用的虚拟机模板。

一般而言,如果要了解系统中正在运行的WNCD的数量,可以在所有控制器类型之间使用此命令:

<#root>

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

5

具体而言,对于9800-CL,您可以使用命令在虚show platform software system all 拟平台上收集详细信息:

<#root>

WNCD instances: 1

### 监控AP负载均衡

AP到WNCD分配在AP CAPWAP加入过程中应用,因此无论使用何种平衡方法,在操作过程中都不 会更改,除非存在全网范围的CAPWAP重置事件,其中所有AP都断开并重新加入。

CLI命令可show wireless loadbalance tag affinity,提供查看所有WNCD实例之间AP负载均衡当前状态的简便方法:

98001#show wireless Tag	loadbalance tag aff Tag t	inity ype No of A	P's Joined Load (	Config Wncd Inst	ance
Branch-tag	SITE	TAG 10	0	0	
Main-tag	SITE	TAG 200	0	1	
default-site-tag	SITE	TAG 1	NA	2	

如果要将AP分布与客户端计数和CPU负载相关联,最简单的方法是使用<u>WCAE</u> support tool并加载 繁忙时占用的数据<sub>show tech wireless</sub>。该工具汇总了从与其关联的每个AP获取的WNCD客户端计数。

在使用率和客户端计数较低时适当平衡的控制器示例:

WCAE Welcome to WCAE   Gue 0.7, Engine 0.22   File: WLC3 Main(10.130.240.13)20-46-18 File: WLC3 Main(10.13	•••						Wireless Co	onfig Analyzer E
Summary   Checks   Access Points   Controller   Interfaces   Mobility Group   RF Group   RRM Settings   Resources   WNCD Load Distribution   AAA Server Details   Logs   Certificates   Site Tags   Site Tags   WLANs Summary   AP RF View <td< th=""><th>cisco</th><th>WCAE GUE 0.7, Engine:0.22</th><th>Welcome to</th><th>WCAE</th><th>Fi</th><th>e: WLC3 Ma</th><th>in(10.130.240.1</th><th>13)20-46-18.lo</th></td<>	cisco	WCAE GUE 0.7, Engine:0.22	Welcome to	WCAE	Fi	e: WLC3 Ma	in(10.130.240.1	13)20-46-18.lo
Interfaces       WNCD Details:       Summary       Image: Summary         Mobility Group       RF Group       ID       Tags Count       Tags Assigned       AP Count       Client Count       CPU load         RRM Settings       0       1       Summary       55       24       1         NCD Load Distribution       AAA Server Details       0       1       Summary       62       5       0         2       1       Summary       50       13       0	<ul> <li>♠ Summ</li> <li>▶ ✓ Check</li> <li>▶ &lt; Accel</li> <li>■ &lt; Accel</li> </ul>	mary ks ss Points	WNG	CD Load Dist	ribution			
RF GroupIDTags CountTags AssignedAP CountClient CountCPU loadRRM Settings01Summary55241Resources11Summary6250WNCD Load Distribution21Summary625021Summary50130Logs31Summary872642Certificates41Summary741282Site Tags51Summary76611WLANs Summary61Summary58451	♥ "Y" Contr Interfac Mobility	roller ces y Group	WNC	D Details: Summary	Ť			
Num Sectings01Summary55241Resources111Summary6250MNCD Load Distribution21Summary625021Summary50130221Summary872642231Summary74128241Summary741282551Summary7661161Summary58451	RF Grou	up attings	ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load
WNCD Load Distribution AAA Server Details Logs Certificates11Summary625021Summary5013031Summary87264241Summary74128251Summary7661161Summary58451	Resour	nes	0	1	Summary	55	24	1
AAA Server Details         2         1         Summary         50         13         0           Logs         3         1         Summary         87         264         2           Certificates         4         1         Summary         74         128         2           Site Tags         5         1         Summary         76         61         1           WLANs Summary         6         1         Summary         58         45         1	WNCD	Load Distribution	1	1	Summary	62	5	0
Logs         3         1         Summary         87         264         2           Certificates         4         1         Summary         74         128         2           Site Tags         5         1         Summary         76         61         1           K AP RF View         Provide         Summary         58         45         1	AAA Se	erver Details	2	1	Summary	50	13	0
Certificates         4         1         Summary         74         128         2           Image: Site Tags         5         1         Summary         76         61         1           Image: WLANs Summary         Image: Site Tags         Image:	Logs		3	1	Summary	87	264	2
Site Tags         5         1         Summary         76         61         1           WLANs Summary         6         1         Summary         58         45         1	Certific	ates	4	1	Summary	74	128	2
WLANs Summary         6         1         Summary         58         45         1           >          AP RF View         6         1         Summary         58         45         1	💠 Site 1	Tags	5	1	Summary	76	61	1
AP RF View	WLAI	Ns Summary	6	1	Summary	58	45	1
7 1 Summany 40 00	AP R	F View	7		Summany	40	20	

### 另一个示例是,对于负载较重的控制器,显示正常CPU利用率:

					Wireless Co	onfig Analyzer E
CISCO WCAE GUE 07, Engine 0.22	Welcome to )	NCAE	Fil	e: customer ·	wic tech wirek	sss_17.12.3.log
<ul> <li>♠ Summary</li> <li>▶ ✓ Checks</li> <li>▶ ♀ Access Points</li> <li>♥ ♀ Controller</li> <li>Harefuger</li> </ul>	WNC	D Load Dist	ribution			
Mobility Group RF-Group DDM Santions	ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load
Resources WNCD Load Distribution	1	8	Summary	809 351	2103	25 18
AAA Server Details Logs	2	9	Summary Summary	171 300	600 1322	8
Certificates	4	9	Summary	651	1784	20
WLANS Summary	5	9	Summary Summary	483	1541 615	17 8
► 🚯 RF Profiles	7	8	Summary	527	1642	18

### 推荐的AP负载均衡机制是什么

简而言之,您可以在以下方面总结不同的选项:

- 小型网络,无需快速漫游,控制器负载不到40%:默认标记。
- 如果需要快速漫游(OKC、FT、CCKM)或大型客户端计数:
  - ◎ 单栋建筑:创建与CPU数量相同的站点标签(取决于平台)。
  - 。在17.12之前,或低于500个AP计数:多栋建筑物、分支机构或大型园区:为每个物理

RF位置创建一个站点标记,并为每个站点配置load命令。 • 17.12及更高版本(超过500个AP):使用RF负载均衡。

此500 AP阈值用于标记应用负载均衡机制有效时间,因为默认情况下它将AP分组为100个单元的数 据块。

AP WNCD分布虚拟化

有些情况下,您需要执行更高级的AP平衡,并且希望对AP在CPU中的分布方式进行精细控制。例 如,在非常高密度的情况下,关键负载指标是客户端计数,而不仅仅只关注系统中存在的AP数量。

大型事件就是很好的例子:一座建筑可以托管数千个客户端,以及数百个AP,并且您需要将负载分 配到尽可能多的CPU上,但需要同时优化漫游。因此,除非有需要,否则请勿在WNCD上漫游。您 想要防止不同WNCD/站点标签中的多个AP在同一物理位置混杂在一起的盐和胡椒情况。

为了帮助微调并提供分布的可视化,您可以使用WCAE工具,并利用AP RF视图功能:



这允许您查看AP/WNCD分发,刚刚设置view Type为WNCD。这里,每种颜色代表WNCD/CPU。您还可以将RSSI过滤器设置为–85,以避免低信号连接,这些连接也由控制器中的RRM算法过滤。

在上一个与Ciscolive EMEA 24对应的示例中,您可以看到大多数相邻的AP在同一个WNCD中交叉 排列整齐,交叉重叠非常有限。

分配给同一WNCD的站点标签,获取相同的颜色。

### 监控控制平面CPU使用情况

请务必记住Cisco IOS XE架构的概念,并牢记CPU使用情况的两个主要视图。一个来自历史上的 Cisco IOS支持,另一个是主要支持,具有跨所有进程和内核的CPU整体视图。

通常,您可以使用命令show processes cpu platform sorted,收集整个Cisco IOS XE中所有进程的详细信息:

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

CPU uti	lization	for five	e seconds	8%,	one	minu	ite:	14%, fiv	/e mir	nutes:	11%	
Core 0:	CPU util	ization	for five	second	ls:	6%,	one	minute:	11%,	five n	minutes:	5%
Core 1:	CPU util	ization	for five	second	ls:	2%,	one	minute:	8%,	five n	minutes:	5%
Core 2:	CPU util	ization	for five	second	ls:	4%,	one	minute:	12%,	five n	minutes:	12%
Core 3:	CPU util	ization	for five	second	ls:	19%,	one	minute:	23%,	five n	minutes:	24%
Pid	PPid	5Sec	1Min	5Min	Sta	atus		Size	Name	9		
T8823	19514	44%	44%	44%	S			190880	ucoo	de_pkt	_PPE0	
28947	8857	3%	10%	4%	S			1268696	linu	ux_ios	d-imag	
19503	19034	3%	3%	3%	S			247332	fmar	ı_fp_i	mage	
30839	2	0%	0%	0%	Ι			0	kwoi	rker/0	:0	
30330	30319	0%	0%	0%	S			5660	ngin	าx		
30329	30319	0%	1%	0%	S			20136	ngin	าx		
30319	30224	0%	0%	0%	S			12480	ngin	าx		
30263	1	0%	0%	0%	S			4024	rote	ee		
30224	8413	0%	0%	0%	S			4600	pmar	า		
30106	2	0%	0%	0%	Ι			0	kwoi	rker/u	11:0	
30002	2	0%	0%	0%	S			0	Sar	EosdMoi	nd	
29918	29917	0%	0%	0%	S			1648	ine	t_geth	ost	

此处需要强调几个要点:

- 进程ucode\_pkt\_PPE0在9800L和9800CL平台上处理数据平面,预期它始终会看到较高的利用 率,甚至高于100%。这是执行的一部分,这不构成问题。
- 区分峰值使用与持续负载并隔离给定场景中的预期情况非常重要。例如,收集非常大的CLI输出(如show tech wireless)可能会在IOSd、smand和pubd进程上生成峰值负载,因为会收集非常大的文本输出,并且会执行数百个CLI命令。这不是问题,输出完成后,负载会下降。

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

• 在高客户端活动时间内,WNCD核心的利用率预计会达到峰值。可以看到80%的峰值,而不存在任何功能影响,并且它们通常不会构成问题。

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	

- 必须调查进程上持续高的CPU使用率(超过90%,超过15分钟)。
- 您可以使用命令监控IOSd CPU使用率show processes cpu sorted。这与Cisco IOS XE列表的 linux\_iosd-imag进程部分中的活动相对应。

9800cl-1#show processes cpu sorted

CPU ι	utilization for	five seconds:	2%/0%;	one m	inute:	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%	O 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快速查看IOSd负载、每个核心使用率以及数据平面负载:

IOS Daemon CPU Usage(Top 5 Pr	ocess)	@ 105	SD CPU Dump	Datapath Utilization	(	Datapath Utilization Dump
Process	5Sec	1Min	5Min	Data Plane	Core 2	Core 3
HTTP CORE	12.87%	11.30%	2.65%	PP (%)	1.22	0.00
SEP_webui_wsma_h	1.51%	0.90%	0.20%	RX (%)	0.00	0.03
SIS Punt Process	0.07%	0.06%	0.07%	TM (%)	0.00	2.42
Check heaps	0.00%	0.09%	0.06%	IDLE (%)	98.78	97.55
L2 LISP Punt Pro	0.07%	0.04%	0.05%			



### 该选项在选项卡上可用Monitoring/System/CPU Utilization。

### 每个流程是什么

确切的过程列表会因控制器型号和Cisco IOS XE版本而异。这是一些关键流程的列表,并不旨在涵 盖所有可能的条目。

进程名	它能做什么	评估
wncd_x	处理大多数无线操作。根据 9800型号,可以有1到8个实例。	在繁忙时段,您可以看到高使用率 峰值。报告利用率是否停滞了 95%或以上几分钟。
linux_iosd-imag	IOS进程	如果收集大量CLI输出(show tech),预期会看到高利用率。 SNMP操作过大或过于频繁会导致 高CPU。
nginx	Web 服务器	此过程可以显示峰值,并且只能在 持续的高负载上报告。
ucode_pkt_PPE0	9800CL/9800L中的数据平面	使用命令show platform hardware chassis active qfp datapath utilization监视此组件 。
ezman	用于接口的芯片组管理器	此处的CPU持续高可能表明HW问 题或可能的内核软件问题。可以报 告。
dbm	数据库管理器	可以报告此处的持续高CPU。
odm_X	Operation Data Manager跨多个 进程处理统一数据库。	加载的系统应使用高CPU。
rogued	处理欺诈功能	可以报告此处的持续高CPU。
smand	Shell Manager负责在不同进程之 间进行CLI解析和交互。	处理大量CLI输出时预计高CPU。 可以报告在缺少负载的情况下持续 的高的CPU。

EMD	外壳管理器。处理CLI解析和不同 进程之间的交互。	处理大量CLI输出时预计高CPU。 可以报告无负载时持续的高的 CPU。
pubd	遥测处理的一部分	大型遥测订用预计高CPU。可以报 告无负载时持续的高的CPU。

## 高CPU保护机制

Catalyst 9800无线LAN控制器具有广泛的网络或无线客户端活动保护机制,可防止意外或有意的情况导致高CPU。有几个关键功能旨在帮助您遏制有问题的设备:

#### 客户端排除

默认情况下,这是启用的,并且是无线保护策略的一部分,可以按策略配置文件启用或禁用。这可 以检测几种不同的行为问题,从网络中删除客户端,并将其设置为临时排除列表。当客户端处于此 排除状态时,AP不会与其通信,从而阻止任何进一步操作。

排除计时器超时后(默认情况下为60秒),允许客户端再次关联。

客户端排除有多个触发器:

- 反复的关联失败
- 3个或更多网络身份验证、PSK或802.1x身份验证错误
- 重复的身份验证超时(客户端无响应)
- 尝试重复使用已注册到其他客户端的IP地址
- 生成ARP泛洪

客户端排除功能可保护控制器、AP和AAA基础设施(Radius)免受可能导致高CPU的几种高活动类型 的影响。一般来说,除非出于故障排除练习或兼容性要求需要,否则不建议禁用任何排除方法。

默认设置适用于几乎所有情况,并且仅在某些例外情况下有效,需要增加排除时间或禁用某些特定 触发器。例如,某些传统或专业客户端(IOT/Medical)需要禁用关联故障触发器,因为客户端缺陷无 法轻松打补丁

您可以在UI中自定义触发器:配置/无线保护/客户端排除策略:

÷	cisco (	Cisco Catal	yst 9800-CL Wireless Controller	
Q	Search Menu Item		Configuration * > Security * > Wireless Protection Policies	
H	Dashboard		Rogue Policies Rogue AP Rules Client Exclusion Policies	
٢	Monitoring	,	Select all events	
2	Configuration	*	Excessive 802.11 Association Failures	
<u>છ</u> ા	Administration		Excessive 802.1X Authentication Failures	
©	Licensing		Excessive 802.1X Authentication Timeout	
X	Troubleshootin	a	IP Theft or IP Reuse	
			Excessive Web Authentication Failures	

ARP Exclusion触发器旨在全局级别永久启用,但可以在每个策略配置文件中进行自定义。您可以 使用命令look for this specificsh wireless profile policy all output检查状态:

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

### 针对数据流量的控制平面保护

这是数据平面中的一种高级机制,用于确保发送到控制平面的流量不超过预定义的阈值集。该功能称为Punt策略器,几乎在所有情况下,都不需要触碰它们,即使如此,也只能在与Cisco支持部门配合工作时执行。

这种保护的优点是它提供对网络中正在发生什么的非常详细的了解,以及是否存在任何速率增加或 每秒数据包意外增加的特定活动。

这仅通过CLI显示,因为它们通常是无需修改的高级功能的一部分。

要查看所有投掷策略,请执行以下操作:

9800-1#show platform software punt-policer

Per Pu	nt-Cause Policer Configurati	on and Pac	ket Count	ers			
Punt		Config Rate(pps)		Conform Packets		Dropped Pack	
Cause	Description	Normal	High	Normal	High	Normal	
2	IPv4 Options	874	655	0	0	0	
3	Layer2 control and legacy	8738	2185	33	0	0	

Δ	PPP Control	437	1000	0	0	0
-		- J <i>I</i>	1000	0	0	0
5	CLNS IS-IS Control	8738	2185	0	0	0
6	HDLC keepalives	437	1000	0	0	0
7	ARP request or response	437	1000	0	330176	0
8	Reverse ARP request or repso	437	1000	0	24	0
9	Frame-relay LMI Control	437	1000	0	0	0
10	Incomplete adjacency	437	1000	0	0	0
11	For-us data	40000	5000	442919246	203771	0
12	Mcast Directly Connected Sou	437	1000	0	0	0

此列表可能很大,包含超过160个条目,具体取决于软件版本。

在表输出中,您要检查丢弃的数据包列以及在高丢弃计数上具有非零值的任何条目。

为了简化数据收集,您可以使用命令show platform software punt-policer drop-only,仅过滤带有丢弃的监察器条目。

此功能可用于识别是否存在ARP风暴或802.11探测泛洪(它们使用到LFTS的队列802.11数据包)。LFTS代表Linux转发传输服务)。

#### 无线呼叫准入控制

在所有最近的维护版本中,控制器都有一个活动监视器,用于动态响应高CPU,并确保AP CAPWAP隧道在面临不可持续的压力时保持活动状态。该功能检查WNCD负载,并开始限制新客户 端活动,以确保保留足够的资源来处理现有连接并保护CAPWAP稳定性。该功能在默认情况下启用 ,并且它没有配置选项。

定义了三个保护级别:L1为80%负载,L2为85%负载,L3为89%,每个级别触发不同的传入协议丢 弃作为保护机制。一旦负载减少,保护就会自动删除。

在正常的网络中,您无法看到L2或L3负载事件,如果它们频繁发生,可以进行调查。

要监控,请使用wireless stats cac(如图所示)命令。

9800-1# show wireless stats cac

WIRESLESS CAC STATISTICS

L1 CPU Threshold: 80	L2 CPU Threshold: 85	L3 CPU	Threshold: 89
Total Number of CAC throttle	e due to IP Learn: O		
Total Number of CAC throttle	e due to AAA: 0		
Total Number of CAC throttle	e due to Mobility Discove	ry: 0	
Total Number of CAC throttle	e 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: 1223	31 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保护

mDNS作为一种协议允许使用零接触方法来发现设备间的服务,但同时,它可能非常活跃,并且如 果配置不当,会显着增加负载。

mDNS无需任何过滤,可以轻松地提高WNCD CPU利用率,原因有以下几点:

- mDNS策略通过无限制学习,控制器获取所有设备提供的所有服务。这可能导致包含数百个条目的超大服务列表。
- 未过滤的策略设置:这会导致控制器将这些大型服务列表推送到询问谁提供给定服务的每个客 户端。
- 某些mDNS特定服务由所有无线客户端提供,从而导致较高的服务计数和活动,但操作系统版 本对此有所差异。

您可以使用以下命令检查每个服务的mDNS列表大小:

9800-1# show mdns-sd service statistics	Service Count
_ipptcp.local	84
_ippstcp.local	52
_raoptcp.local	950
_airplaytcp.local	988
_printertcp.local	13
_googlerpctcp.local	12
_googlecasttcp.local	70
_googlezonetcp.local	37
_home-sharingtcp.local	7
_cupssubipptcp.local	26

这可以提供任何给定查询可获取的最大值的概念。它本身并不表示问题,而只是监控所跟踪内容的 一种方式。

以下是一些重要的mDNS配置建议:

• 将mDNS传输设置为单一协议:

9800-1(config)# mdns-sd gateway

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

默认情况下,它使用IPv4传输。为了获得性能,建议使用IPv6或IPv4,但不要同时使用两者。

• 请务必在mDNS服务策略中设置位置过滤器,以避免未绑定的查询/响应。通常,建议使用 site-tag,但是其他选项也可以使用,具体取决于您的需要。

## 我需要更多帮助

如果您看到高CPU负载,并且前面步骤没有任何帮助,请通过案例联系CX,并将此数据作为起点添加:

• 基础数据,包括无线接入点/控制器配置以及网络和RF操作值:

show tech-support wireless

• 存档所有控制器跟踪。这是一个类似于黑盒概念的大文件,可使用以下命令进行收集:

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

### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。