Solucionar problemas de carga de CPU del controlador LAN inalámbrico

Contenido

Introducción

Este documento describe cómo monitorear el uso de la CPU en los controladores de LAN inalámbrica de Catalyst 9800, además de cubrir varias recomendaciones de configuración.

Comprensión del uso de CPU

Antes de profundizar en la resolución de problemas de carga de CPU, debe comprender los aspectos básicos del uso de las CPU en los controladores de LAN inalámbrica de Catalyst 9800 y algunos detalles sobre la arquitectura de software.

En general, el documento Prácticas recomendadas de Catalyst 9800 define un conjunto de buenas configuraciones que pueden evitar problemas en el nivel de la aplicación, por ejemplo, el uso del filtrado de ubicación para mDNS o la garantía de que la exclusión del cliente siempre está habilitada. Se recomienda que aplique esas recomendaciones junto con los temas expuestos aquí.

Fundamentos de plataforma

Los controladores Catalyst 9800 se diseñaron como una plataforma flexible, orientada a diferentes cargas de red y centrada en la escalabilidad horizontal. La denominación de desarrollo interno era "eWLC" con la e para "elástico", para significar que la misma arquitectura de software, sería capaz de funcionar desde un solo sistema integrado de CPU pequeño a múltiples dispositivos de gran escala de CPU/núcleo.

Cada WLC ha tenido dos "lados" distintos:

- Plano de control: gestión de todas las interacciones de "gestión", como CLI, UI, Netconf y todos los procesos de incorporación para clientes y AP.
- Plano de datos: responsable del reenvío real de paquetes y la desencapsulación de CAPWAP, la aplicación de políticas AVC, entre otras funcionalidades.

Plano de Control

- La mayoría de los procesos de Cisco IOS-XE se ejecutan en BinOS (núcleo de Linux), con su propio programador especializado y comandos de supervisión.
- Existe un conjunto de procesos clave, denominados Wireless Network Control Daemon (WNCD), cada uno con una base de datos en memoria local, que controlan la mayor parte de la actividad inalámbrica. Cada CPU posee un WNCD, para distribuir la carga a través de todos los núcleos de CPU disponibles a cada sistema
- La distribución de carga a través de WNCD se realiza durante la unión de AP. Cuando un AP realiza una unión CAPWAP al controlador, un balanceador de carga interno distribuye el AP usando un conjunto de reglas posibles, para asegurar el uso correcto de todos los recursos de CPU disponibles.
- El código de Cisco IOS® se ejecuta en su propio proceso llamado IOSd, y tiene su programador de CPU y comandos de monitoreo. Esto se ocupa de funciones específicas, por ejemplo, CLI, SNMP, multidifusión y routing.

En una vista simplificada, el controlador tiene mecanismos de comunicación entre el plano de control y el plano de datos, "punt", envía el tráfico de la red al plano de control y "inyección", envía tramas desde el plano de control a la red.

Como parte de una posible investigación de resolución de problemas de CPU alta, es necesario monitorear el mecanismo de punt, para evaluar qué tráfico está llegando al plano de control y podría conducir a una carga alta.

Plano de Datos

Para el controlador Catalyst 9800, esto se ejecuta como parte del procesador de paquetes de Cisco (CPP), que es un marco de software para desarrollar motores de reenvío de paquetes, que se utilizan en varios productos y tecnologías.

La arquitectura permite un conjunto de funciones comunes, entre diferentes implementaciones de hardware o software, por ejemplo, lo que permite funciones similares para 9800CL frente a 9800-40, con diferentes escalas de rendimiento.

Balanceo de Carga de AP

El WLC realiza el balanceo de carga a través de las CPU durante el proceso de unión CAPWAP AP AP, con el diferenciador clave que es el nombre de la etiqueta del sitio AP. La idea es que cada AP represente una carga específica de CPU agregada, proveniente de su actividad de cliente, y el AP mismo. Existen varios mecanismos para realizar este equilibrio:

- Si el AP está usando "default-tag", se equilibraría en un ordenamiento cíclico a través de todas las CPU/WNCD, con cada nueva unión del AP yendo al WNCD siguiente. Este es el método más sencillo, pero tiene pocas implicaciones:
    - Este es el escenario subóptimo, ya que los AP en el mismo dominio de roaming de RF harían roaming frecuente entre WNCD, lo que implica una comunicación entre procesos adicional. La itinerancia entre instancias es un poco más lenta.
    - En el caso de la etiqueta del sitio (remoto) de FlexConnect, no hay ninguna distribución de claves PMK disponible. Esto significa que no puede realizar la itinerancia rápida para el modo Flex, lo que afecta a los modos de itinerancia OKC/FT.

      En general, la etiqueta predeterminada se puede utilizar en escenarios de carga más baja (por ejemplo, menos del 40% de la carga de AP y cliente de la plataforma 9800), y para la implementación de FlexConnect solo cuando no se requiere la itinerancia rápida.

- Si el AP tiene una etiqueta de sitio personalizada, la primera vez que un AP que pertenece al nombre de la etiqueta de sitio se une al controlador, la etiqueta de sitio se asigna a una instancia WNCD específica. Todas las uniones de AP adicionales subsiguientes con la misma etiqueta se asignan al mismo WNCD. Esto garantiza la itinerancia entre los AP en la misma etiqueta de sitio, sucede en el contexto WCND, que proporciona un flujo más óptimo, con un menor uso de la CPU. Se admite la itinerancia a través de WNCD, pero no es tan óptima como la itinerancia dentro de WNCD.

- Decisión de equilibrio de carga predeterminada: cuando se asigna una etiqueta a un WNCD, el equilibrador de carga selecciona la instancia con el recuento de etiquetas de sitio más bajo en ese momento. Dado que no se conoce la carga total que podría tener esa etiqueta de sitio, puede dar lugar a situaciones de equilibrio subóptimas. Esto depende del orden de las uniones de AP, cuántas etiquetas de sitio se han definido y si el conteo de AP es asimétrico a través de ellas

- Equilibrio de carga estática: para evitar una asignación desequilibrada de la etiqueta de sitio a WNCD, se introdujo el comando de carga de sitio en 17.9.3 y versiones posteriores, para permitir a los administradores predefinir la carga esperada de cada etiqueta de sitio. Esto resulta especialmente útil cuando se gestionan escenarios de campus, o varias sucursales, cada una asignada a diferentes recuentos de AP, para garantizar que la carga se distribuye uniformemente a través de WNCD.

Por ejemplo, si tiene un 9800-40, que maneja una oficina principal, más 5 sucursales, con diferentes conteos de AP, la configuración podría verse de la siguiente manera:

```
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
```

En esta situación, no desea que la etiqueta de la oficina principal esté en el mismo WNCD que la sucursal 3 y la sucursal 4, hay en total 6 etiquetas de sitio y la plataforma tiene 5 WNCD, por lo que podría haber una posibilidad de que las etiquetas de sitio cargadas más altas aterrizaran en la misma CPU. Con el comando load, puede crear una topología de balanceo de carga de AP predecible.

El comando load es un indicio de tamaño esperado, no tiene que coincidir exactamente con el conteo de AP, pero normalmente se configura en los AP esperados que podrían unirse.

- En los escenarios en los que hay edificios grandes gestionados por un solo controlador, es más fácil y sencillo crear tantas etiquetas de sitio como WNCD para esa plataforma específica (por ejemplo, C9800-40 tiene cinco, C9800-80 tiene ocho). Asigne AP en la misma área o dominio de roaming a las mismas etiquetas del sitio para minimizar la comunicación entre WNCD.
- Equilibrio de carga de RF: Equilibra los AP a través de las instancias WNCD, usando la relación de vecino de RF de RRM, y crea subgrupos dependiendo de lo cerca que estén los AP entre sí. Se debe hacer después de que los AP se hayan estado ejecutando por un tiempo y eliminar la necesidad de configurar cualquier configuración de equilibrio de carga estática. Está disponible a partir de las 17.12 horas.

¿Cómo averiguar cuántas WNCD hay presentes?

Para las plataformas de hardware, el recuento de WNCD es fijo: 9800-40 tiene 5, 9800-80 tiene 8. Para 9800CL (virtual), el número de WNCD dependería de la plantilla de máquina virtual utilizada durante la implementación inicial.

Como regla general, si desea averiguar cuántas WNCD se están ejecutando en el sistema, puede utilizar este comando en todos los tipos de controladores:

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

5

En el caso específico de 9800-CL, puede utilizar el comando **show platform software system all** para recopilar detalles sobre la plataforma virtual:

<#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

Monitoreo del balanceo de carga AP

La asignación de AP a WNCD se aplica durante el proceso de unión CAPWAP AP AP, por lo que no se espera que cambie durante las operaciones, independientemente del método de equilibrio, a menos que haya un evento de reinicio CAPWAP en toda la red donde todos los AP se desconecten y se vuelvan a unir.

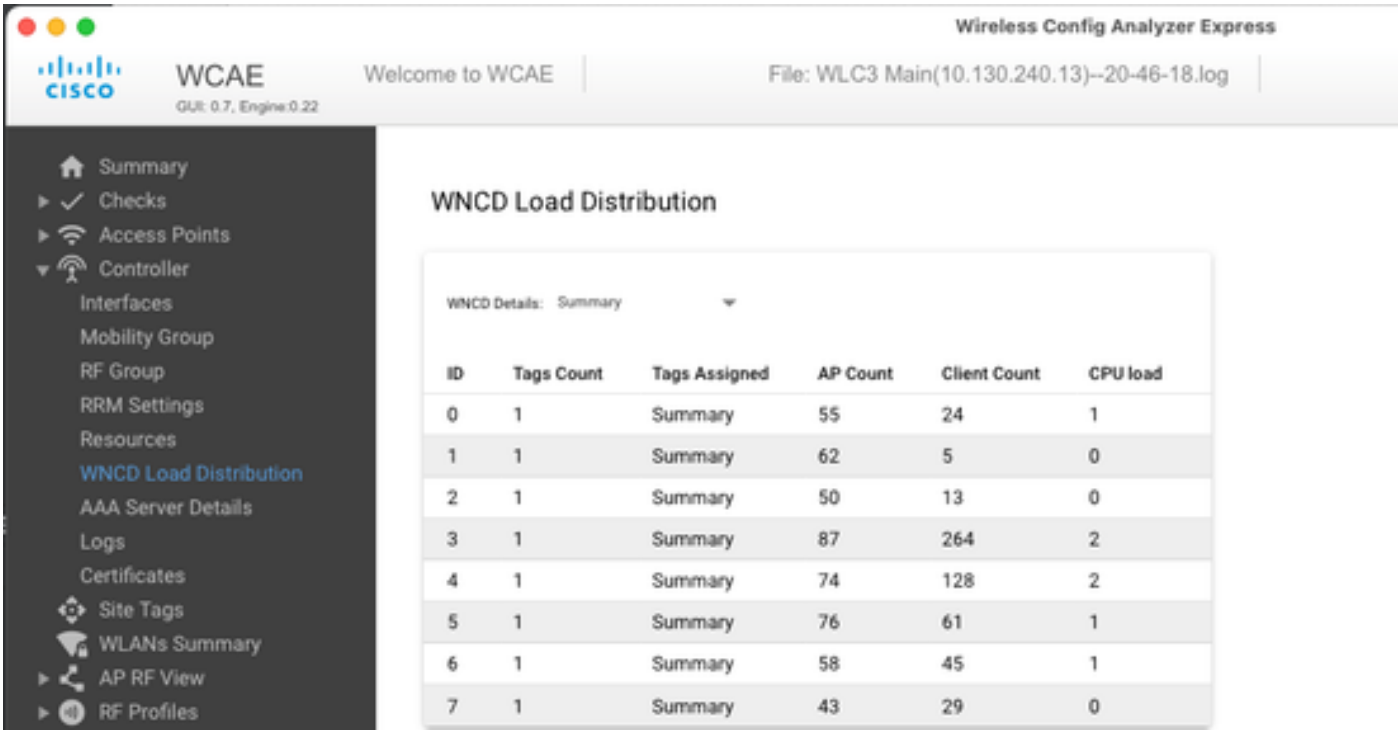
El comando CLI show wireless loadbalance tag affinity puede proporcionar una manera fácil de ver el estado actual del equilibrio de carga de AP en todas las instancias WNCD:

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

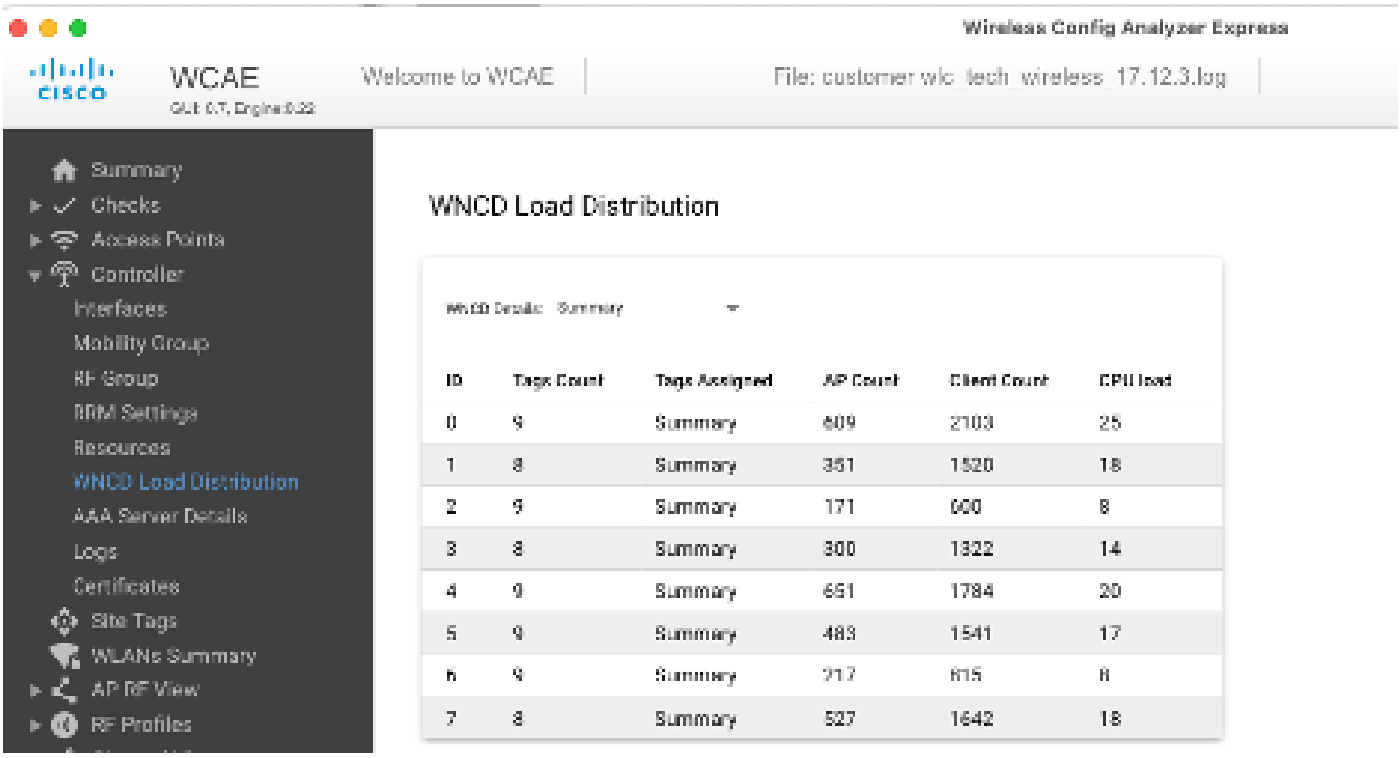
si desea correlacionar la distribución de AP, contra el conteo de clientes y la carga de CPU, la manera más fácil es utilizar la herramienta de soporte de WCAE y cargar un show tech wireless tomado durante las horas ocupadas. La herramienta resume el conteo de clientes WNCD, tomado de cada AP que está asociado con él.

Ejemplo de un controlador debidamente balanceado, durante el bajo uso y el conteo de clientes:



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

Otro ejemplo, para un controlador más cargado, que muestra el uso normal de la CPU:



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	8
7	8	Summary	527	1642	18

¿Cuál es el mecanismo de balanceo de carga de AP recomendado?

En resumen, puede resumir las diferentes opciones en:

- Red pequeña, sin necesidad de itinerancia rápida, menos del 40% de la carga del controlador: etiqueta predeterminada.
- Si se necesita la itinerancia rápida (OKC, FT, CCKM) o una gran cantidad de clientes:

- Edificio único: cree tantas etiquetas de sitio como CPU (según la plataforma)
- Antes de la 17.12, o menos de 500 AP: varios edificios, sucursales o campus grande: cree una etiqueta de sitio por ubicación de RF física y configure el comando de carga por sitio.
- 17.12 y superior con más de 500 puntos de acceso: utilice el equilibrio de carga de RF.

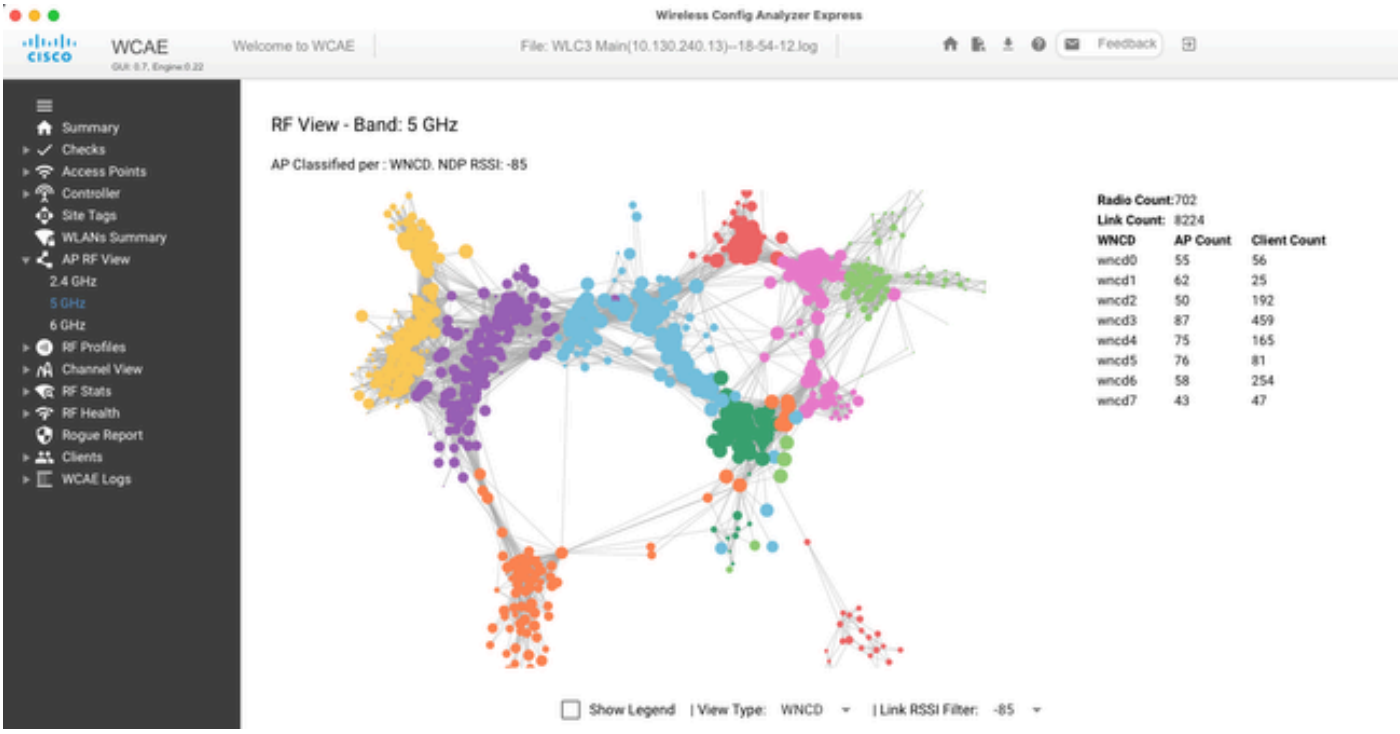
Este umbral de 500 AP es para marcar cuándo es efectivo aplicar el mecanismo de balanceo de carga, ya que agrupa los AP en bloques de 100 unidades de forma predeterminada.

Visualización de distribución WNCD de PA

Hay escenarios en los que se desea hacer un equilibrio de AP más avanzado, y es deseable tener un control granular sobre cómo los AP se distribuyen a través de las CPU, por ejemplo, escenarios de muy alta densidad donde la métrica de carga clave es el conteo de clientes frente a centrarse únicamente en el número de AP presentes en el sistema.

Un buen ejemplo de esta situación son los eventos de gran tamaño: un edificio podría alojar miles de clientes, más de varios cientos de puntos de acceso, y tendría que dividir la carga en tantas CPU como sea posible, pero optimizar la itinerancia al mismo tiempo. Por lo tanto, no se desplaza por WNCD a menos que sea necesario. Usted quiere prevenir situaciones de "sal y pimienta" donde múltiples APs en diferentes WNCDs/etiquetas de sitio se entremezclan en la misma ubicación física.

Para ayudar a ajustar y proporcionar una visualización de la distribución, puede utilizar la herramienta WCAE y aprovechar la función AP RF View:



Esto nos permite ver la distribución de AP/WNCD, simplemente ajustada View Type a WNCD. Aquí cada color representaría un WNCD/CPU. También puede establecer el filtro RSSI en -85, para evitar conexiones de señal baja, que también son filtradas por el algoritmo RRM en el controlador.

En el ejemplo anterior, correspondiente a Cisco Live EMEA 24, puede ver que la mayoría de los AP adyacentes se agrupan bien en el mismo WNCD, con superposición cruzada muy limitada.

Las etiquetas de sitio asignadas al mismo WNCD, obtienen el mismo color.

Supervisión del uso de CPU del plano de control

Es importante recordar el concepto de la arquitectura Cisco IOS-XE y tener en cuenta que hay dos "vistas" principales del uso de la CPU. Uno proviene del soporte histórico de Cisco IOS, y el principal, con una vista holística de la CPU en todos los procesos y núcleos.

En general, puede utilizar el comando show processes cpu platform sorted para recopilar información detallada para todos los procesos en Cisco IOS-XE:

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

Hay varios puntos clave que destacar aquí:

- El proceso ucode_pkt_PPE0 está gestionando el plano de datos en las plataformas 9800L y 9800CL, y se espera que observe una alta utilización en todo momento, incluso superior al 100%. Esto forma parte de la aplicación, y no constituye un problema.

- Es importante diferenciar el uso máximo frente a una carga sostenida y aislar lo que se espera en un escenario determinado. Por ejemplo, recolectar una salida CLI muy grande, como show tech wireless puede generar una carga máxima en procesos IOSd, smand, pubd, ya que se está recolectando una salida de texto muy grande, con cientos de comandos CLI ejecutados, esto no es un problema, y la carga se interrumpe después de que se haya completado la salida.

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

- Se espera un uso máximo de los núcleos WNCD durante los periodos de mayor actividad del cliente. Es posible ver picos del 80%, sin ningún impacto funcional, y normalmente no constituyen un problema.

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

- Debe investigarse un uso elevado y sostenido de la CPU en un proceso, superior al 90%, durante más de 15 minutos.

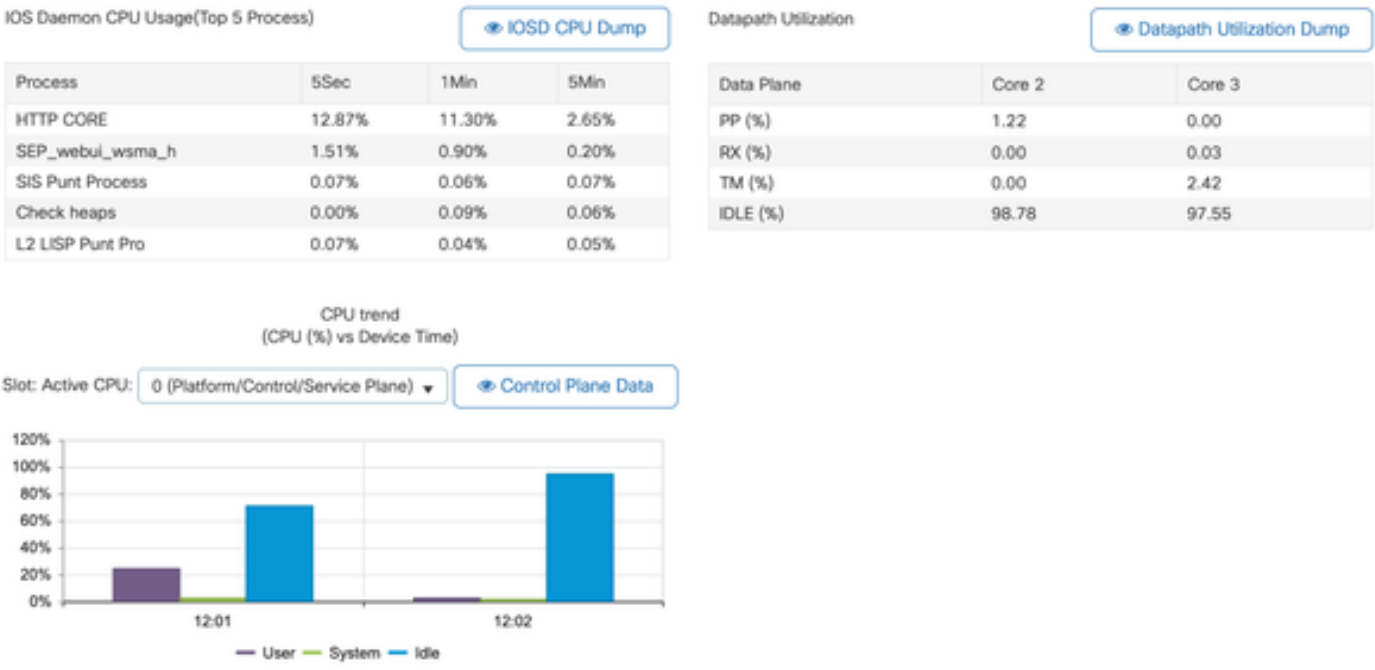
- Puede monitorear la utilización de la CPU IOSd, con el comando show processes cpu sorted . Esto corresponde a la actividad en la parte de proceso linux_iosd-image de la lista Cisco IOS-XE.

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

- Puede utilizar la GUI del 9800 para obtener una vista rápida de la carga de IOSd, el uso por núcleo y la carga del plano de datos:



Esta opción está disponible en la Monitoring/System/CPU Utilization ficha .

¿Qué es cada proceso?

La lista exacta de procesos variaría según el modelo de controlador y la versión de Cisco IOS-XE. Esta es una lista de algunos de los procesos clave, y no pretende cubrir todas las entradas posibles.

Nombre del proceso	¿Qué hace?	Evaluación
wncd_x	Gestiona la mayoría de las operaciones inalámbricas. Según el modelo 9800, puede tener entre 1 y 8 instancias	Se pueden ver picos de utilización alta durante las horas punta. Informe si la utilización se bloquea un 95% o más durante varios minutos
linux_iosd-image	proceso IOS	Se espera un uso elevado si se recopila una gran salida de CLI (show tech) Las operaciones SNMP grandes o demasiado frecuentes pueden conducir a una CPU alta
nginx	Servidor Web	Este proceso puede mostrar picos y solo debe notificarse con una carga alta sostenida
ucode_pkt_PPE0	Plano de datos en 9800CL/9800L	Utilice el comando **show platform hardware chassis active qfp datapath utilization** para supervisar este componente
ezman	Administrador de chipsets para interfaces	Una CPU alta sostenida aquí podría indicar un problema de hardware o un posible problema de software del núcleo. Se debe informar
dbm	Administrador de bases de datos	Debe informarse de una CPU alta y sostenida aquí
odm_X	Operation Data Manager gestiona las bases de datos consolidadas entre los procesos	Se espera una CPU alta en los sistemas cargados
pícaro	Gestiona la funcionalidad de acceso no deseado	Debe informarse de una CPU alta y sostenida aquí

smand	Administrador de Shell. Se encarga del análisis de CLI y de la interacción entre los diferentes procesos	Se esperaba una CPU alta mientras se gestionaba una salida CLI grande. Se debe informar de una CPU alta y sostenida en ausencia de carga
emd	Administrador de Shell. Se encarga del análisis de CLI y de la interacción entre los diferentes procesos	Se esperaba una CPU alta mientras se gestionaba una salida CLI grande. Se debe informar de una CPU alta y sostenida en ausencia de carga
púbico	Parte de la gestión de telemetría	Se esperaba una CPU alta para suscripciones de telemetría grandes. Se debe informar de una CPU alta y sostenida en ausencia de carga

Mecanismos de protección de CPU altos

Los controladores de LAN inalámbrica de Catalyst 9800 cuentan con mecanismos de protección extensos en torno a la actividad de la red o del cliente inalámbrico, para evitar un uso elevado de la CPU debido a situaciones accidentales o intencionales. Existen varias funciones clave diseñadas para ayudarle a contener dispositivos problemáticos:

Exclusión de clientes

Esta opción está activada de forma predeterminada y forma parte de las políticas de protección inalámbrica, y se puede activar o desactivar según el perfil de política. Esto puede detectar varios problemas de comportamiento diferentes, quitar el cliente de la red y configurarlo en una "lista de exclusión temporal". Mientras que el cliente está en este estado excluido, los AP no hablan con ellos, evitando cualquier acción adicional.

Una vez transcurrido el temporizador de exclusión (60 segundos de forma predeterminada), se permite al cliente volver a asociarse.

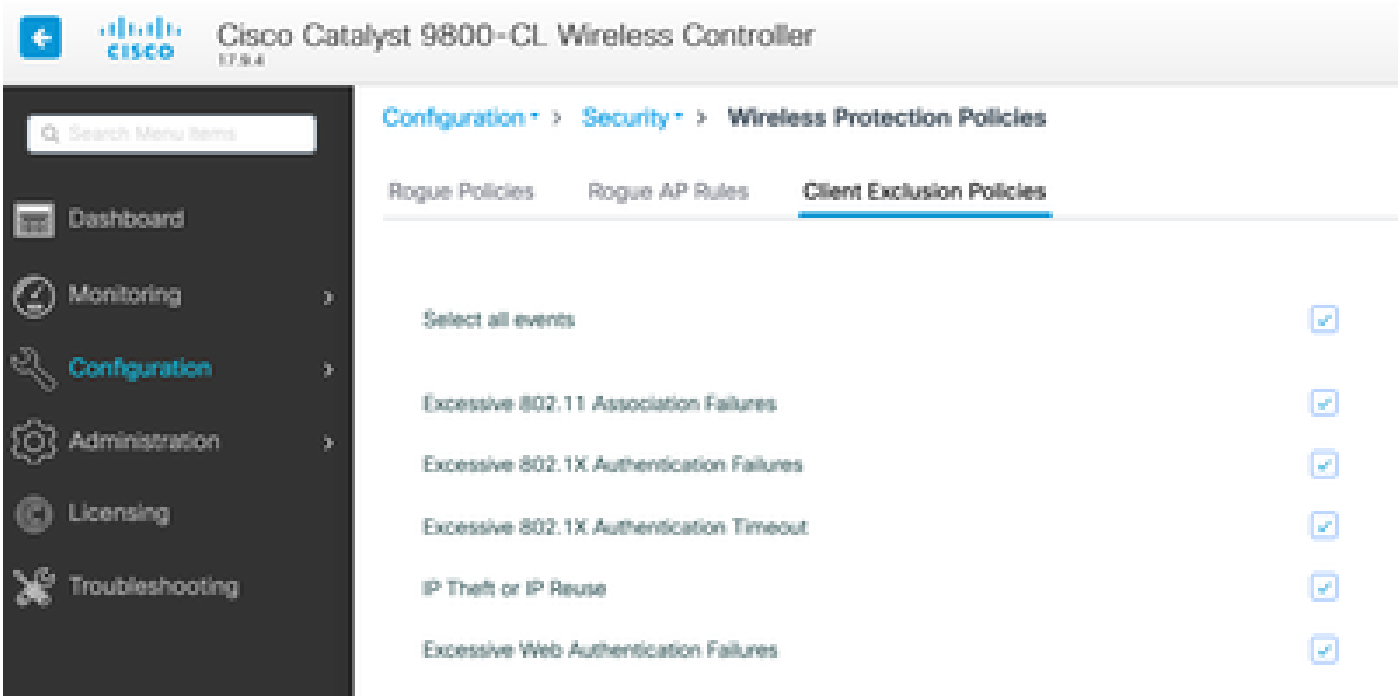
Existen varios desencadenadores para la exclusión de clientes:

- Fallos de asociación repetidos
- 3 o más errores de autenticación webauth, PSK o 802.1x
- Tiempos de espera de autenticación repetidos (sin respuesta del cliente)
- Intentando reutilizar una dirección IP, ya registrada en otro cliente
- Generación de una inundación ARP

La exclusión del cliente protege su controlador, AP e infraestructura AAA (Radius) de varios tipos de actividad alta que podrían conducir a una CPU alta. En general, no es recomendable deshabilitar ninguno de los métodos de exclusión, a menos que sea necesario para un ejercicio de solución de problemas o un requisito de compatibilidad.

La configuración predeterminada funciona para casi todos los casos y solo en algunos escenarios excepcionales, es necesaria para aumentar el tiempo de exclusión o deshabilitar algún desencadenador específico. Por ejemplo, es posible que algunos clientes antiguos o especializados (IOT/Medicina) necesiten que se desactive el desencadenador de fallo de asociación debido a defectos en el lado del cliente que no se pueden solucionar fácilmente

Puede personalizar los desencadenadores en la interfaz de usuario: Configuración/Protección inalámbrica/Políticas de exclusión de clientes:



El disparador de exclusión ARP se diseñó para habilitarse permanentemente a nivel global, pero se puede personalizar en cada perfil de política. Puede verificar el estado con el comando sh wireless profile policy all look para este resultado específico:

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

Protección del plano de control del tráfico de datos

Se trata de un mecanismo avanzado en el plano de datos para garantizar que el tráfico enviado al plano de control no supere un conjunto predefinido de umbrales. La función se denomina "Punt Policers" y en casi todos los escenarios, no es necesario tocarlos, e incluso entonces, solo se debe hacer mientras se trabaja junto con el Soporte de Cisco.

La ventaja de esta protección es que proporciona una perspectiva muy detallada de lo que está sucediendo en la red, y si hay alguna actividad específica que esté teniendo una velocidad aumentada, o paquetes inesperadamente altos por segundo.

Esto solo se expone a través de CLI, ya que normalmente forman parte de una funcionalidad avanzada que rara vez se necesita modificar.

Para obtener una vista de todas las políticas de punt:

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

Esta puede ser una lista grande, con más de 160 entradas, dependiendo de la versión del software.

En el resultado de la tabla, desea verificar la columna de paquetes descartados junto con cualquier entrada que tenga un valor distinto de cero en el conteo de descartes alto.

Para simplificar la recopilación de datos, puede utilizar el comando show platform software punt-policer drop-only , para filtrar sólo las entradas del regulador con caídas.

Esta función podría ser útil para identificar si hay tormentas ARP o inundaciones de sonda 802.11 (utilizan la cola "Paquetes 802.11 a LFTS"). LFTS significa servicio de transporte de reenvío de Linux).

Control de admisión de llamadas inalámbrico

En todas las versiones de mantenimiento recientes, el controlador tiene un monitor de actividad, para reaccionar dinámicamente a la CPU alta, y garantizar que los túneles CAPWAP AP AP permanezcan activos, ante una presión insostenible.

La función verifica la carga WNCD y comienza a limitar la actividad del nuevo cliente para garantizar que quedan suficientes recursos para manejar las conexiones existentes y proteger la estabilidad CAPWAP.

Esta opción está activada de forma predeterminada y no dispone de opciones de configuración.

Hay tres niveles de protección definidos, L1 con 80% de carga, L2 con 85% de carga y L3 con 89%, cada uno desencadenando diferentes caídas de protocolos entrantes como mecanismos de protección. La protección se elimina automáticamente en cuanto disminuye la carga.

En una red saludable, no debería ver los eventos de carga L2 o L3, y si ocurren con frecuencia, debería ser investigado.

Para monitorear, utilice el comando wireless stats cac como se muestra en la imagen.

```
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
```

Protecciones mDNS

mDNS como protocolo permite un enfoque de "no intervención" para detectar servicios en los dispositivos, pero al mismo tiempo, puede ser muy activo y aumentar la carga significativamente, si no se configura correctamente.

mDNS, sin ningún tipo de filtrado, puede impulsar fácilmente el uso de la CPU WNCD, viniendo de varios factores:

- políticas mDNS con aprendizaje ilimitado, el controlador obtendrá todos los servicios ofrecidos por todos los dispositivos. Esto puede dar lugar a listas de servicios muy grandes, con cientos de entradas.
- Políticas establecidas sin filtrado: esto hará que el controlador envíe esas listas de servicios grandes a cada cliente que pregunte quién está proporcionando un servicio determinado.
- Algunos servicios específicos de mDNS los proporcionan "todos" los clientes inalámbricos, lo que conlleva un mayor número de servicios y actividad, con variaciones en esta función según la versión del sistema operativo.

Puede verificar el tamaño de la lista mDNS por servicio con este comando:

```
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
```

Esto puede proporcionar una idea de cuán grande puede obtener una consulta dada, no denota un problema por sí mismo, solo una manera de monitorear lo que se rastrea.

Existen algunas recomendaciones importantes para la configuración de mDNS:

- Establezca el transporte mDNS en un único protocolo:

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

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

De forma predeterminada, utiliza transporte IPv4. Para obtener rendimiento, se recomienda utilizar IPv6 o IPv4, pero no ambos:

- Establezca siempre un filtro de ubicación en la directiva de servicio mDNS para evitar consultas o respuestas independientes. En general, se recomienda utilizar "site-tag", pero otras opciones podrían funcionar, dependiendo de sus necesidades.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).