Solucionar problemas de carga de CPU do controlador de LAN sem fio

Contents

Introdução

Este documento descreve como monitorar o uso da CPU em Catalyst 9800 Wireless LAN Controllers, além de abordar várias recomendações de configuração.

Entendendo o uso da CPU

Antes de aprofundar-se na solução de problemas de carga de CPU, você precisa entender os fundamentos de como as CPUs são usadas nos Controladores de LAN sem fio Catalyst 9800 e alguns detalhes sobre a arquitetura do software.

Em geral, o documento de práticas recomendadas do Catalyst 9800 define um conjunto de boas definições de configuração que podem evitar problemas no nível do aplicativo, por exemplo, usar a filtragem de local para mDNS ou garantir que a exclusão de cliente esteja sempre habilitada. Recomenda-se que você aplique essas recomendações junto com os tópicos expostos aqui.

Fundamentos da plataforma

Os controladores Catalyst 9800 foram projetados como uma plataforma flexível, voltada para diferentes cargas de rede e focada no dimensionamento horizontal. O nome de desenvolvimento interno era "eWLC" com o e para "elástico", significando que a mesma arquitetura de software seria capaz de ser executada de um sistema incorporado de uma única CPU para vários dispositivos de grande escala de CPU/núcleo.

Cada WLC teve dois "lados" distintos:

- Plano de controle: lidando com todas as interações de "gerenciamento", como CLI, UI, Netconf e todos os processos de integração para clientes e APs.
- Plano de dados: responsável pelo encaminhamento real de pacotes e pelo desencapsulamento do CAPWAP, aplicação da política AVC, entre outras funcionalidades.

Controle o plano

- A maioria dos processos do Cisco IOS-XE é executada no BinOS (Linus Kernel), com seu próprio programador especializado e comandos de monitoramento.
- Há um conjunto de processos-chave, chamado de Wireless Network Control Daemon (WNCD), cada um com um banco de dados local na memória, que lida com a maior parte da atividade sem fio. Cada CPU possui um WNCD, para distribuir a carga em todos os núcleos de CPU disponíveis para cada sistema
- A distribuição de carga em WNCDs é feita durante a junção de AP. Quando um AP executa uma junção CAPWAP com a controladora, um balanceador de carga interno distribui o AP usando um conjunto de regras possíveis, para garantir o uso adequado de todos os recursos de CPU disponíveis.
- O código do Cisco IOS® é executado em seu próprio processo chamado IOSd, e tem seu programador de CPU e comandos de monitoramento. Isso cuida da funcionalidade específica, por exemplo, CLI, SNMP, multicast e roteamento.

Em uma visão simplificada, o controlador tem mecanismos de comunicação entre o controle e o plano de dados, "punt", envia tráfego da rede para o plano de controle, e "injeção", envia quadros do plano de controle para a rede.

Como parte de uma possível investigação de identificação e solução de problemas de alta utilização da CPU, você precisa monitorar o mecanismo de punt para avaliar qual tráfego está chegando ao plano de controle e pode levar a uma carga alta.

Plano dos dados

Para o controlador Catalyst 9800, ele é executado como parte do Cisco Packet Processor (CPP), que é uma estrutura de software para desenvolver mecanismos de encaminhamento de pacotes, usados em vários produtos e tecnologias.

A arquitetura permite um conjunto de recursos comum, em diferentes implementações de hardware ou software, por exemplo, permitindo recursos similares para 9800CL vs 9800-40, em diferentes escalas de throughput.

Balanceamento de carga do AP

A WLC executa o balanceamento de carga através das CPUs durante o processo de junção CAPWAP AP AP, com o diferenciador-chave sendo o nome da tag do site do AP. A ideia é que cada AP represente uma carga de CPU específica adicionada, proveniente de sua atividade de cliente e do próprio AP. Há vários mecanismos para executar esse balanceamento:

- Se o AP estiver usando "default-tag", ele seria balanceado de forma alternada em todas as CPUs/WNCDs, com cada nova junção de AP indo para o próximo WNCD. Esse é o método mais simples, mas tem poucas implicações:
    - Esse é o cenário não ideal, pois os APs no mesmo domínio de roaming de RF fariam roaming inter-WNCD frequente, envolvendo comunicação entre processos adicional. O roaming nas instâncias é mais lento em uma pequena porcentagem.
    - Para a marca de site (remoto) do FlexConnect, não há distribuição de chave PMK disponível. Isso significa que você não pode fazer roaming rápido no modo Flex, afetando os modos de roaming OKC/FT.

      Em geral, a marca padrão pode ser usada em cenários de carga mais baixa (por exemplo, menos de 40% da carga de AP e cliente da plataforma 9800) e para a implantação do FlexConnect somente quando o roaming rápido não for um requisito.

- Se o AP tiver uma marca de site personalizada, na primeira vez que um AP pertencente ao nome da marca de site se une ao controlador, a marca de site é atribuída a uma instância WNCD específica. Todas as junções de AP adicionais subsequentes com a mesma marca são atribuídas ao mesmo WNCD. Isso garante o roaming nos APs na mesma marca de site, que acontece em um contexto WCND, que fornece um fluxo mais ideal, com menor uso da CPU. O roaming em WNCDs é suportado, mas não tão ideal quanto o roaming intraWNCD.

- Decisão de balanceamento de carga default: Quando uma tag é atribuída a um WNCD, o balanceador de carga seleciona a instância com a menor contagem de tag de site naquele momento. Como a carga total que essa marca de site pode ter não é conhecida, ela pode levar a cenários de balanceamento abaixo do ideal. Isso depende da ordem de junções de AP, quantas marcas de site foram definidas e se a contagem de APs é assimétrica entre elas

- Balanceamento de carga estática: para evitar a atribuição desbalanceada de marca de site ao WNCD, o comando de carga de site foi introduzido na versão 17.9.3 e posterior, para permitir que os administradores predefinam a carga esperada de cada marca de site. Isso é especialmente útil ao lidar com cenários de campus, ou várias filiais, cada uma mapeada para diferentes contagens de AP, para garantir que a carga seja distribuída uniformemente pelo WNCD.

Por exemplo, se você tiver um 9800-40, lidando com um escritório principal, mais 5 filiais, com contagens de AP diferentes, a configuração poderia ser assim:

```
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
```

Neste cenário, você não deseja que a tag do escritório principal esteja no mesmo WNCD que a filial 3 e a filial 4, há no total 6 tags de site e a plataforma tem 5 WNCDs, portanto pode haver uma chance de que as tags de site mais carregadas cheguem à mesma CPU. Usando o comando load, você pode criar uma topologia de balanceamento de carga de AP previsível.

O comando load é uma dica de tamanho esperada, ele não precisa corresponder exatamente à contagem de APs, mas é normalmente definido para os APs esperados que podem se unir.

- Em cenários onde você tem grandes edifícios tratados por um único controlador, é mais fácil e simples criar tantos sites-tag quanto WNCDs para essa plataforma específica (por exemplo, C9800-40 tem cinco, C9800-80 tem 8). Atribua APs na mesma área ou domínio de roaming às mesmas marcas de site para minimizar a comunicação entre WNCDs.
- Balanceamento de carga de RF: equilibra os APs nas instâncias WNCD, usando o relacionamento de vizinhança de RF do RRM, e cria subgrupos, dependendo de quão próximos os APs estão uns dos outros. Isso deve ser feito depois que os APs estiverem ativos e em execução por um tempo e elimina a necessidade de configurar qualquer configuração de balanceamento de carga estática. Disponível a partir da 17.12.

Como descobrir quantos WNCDs estão presentes?

Para plataformas de hardware, a contagem WNCD é fixa: 9800-40 tem 5, 9800-80 tem 8. Para 9800CL (virtual), o número de WNCDs dependeria do modelo de máquina virtual usado durante a implantação inicial.

Como regra geral, se quiser descobrir quantos WNCDs estão em execução no sistema, você pode usar este comando em todos os tipos de controlador:

<#root>

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

5

No caso do 9800-CL especificamente, você pode usar o comando **show platform software system all** para coletar detalhes na 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

Monitorando o balanceamento de carga do AP

A atribuição de AP para WNCD é aplicada durante o processo de junção de CAPWAP de AP, de modo que não se espera que seja alterada durante as operações, independentemente do método de balanceamento, a menos que haja um evento de redefinição de CAPWAP em toda a rede, em que todos os APs se desconectam e se unem novamente.

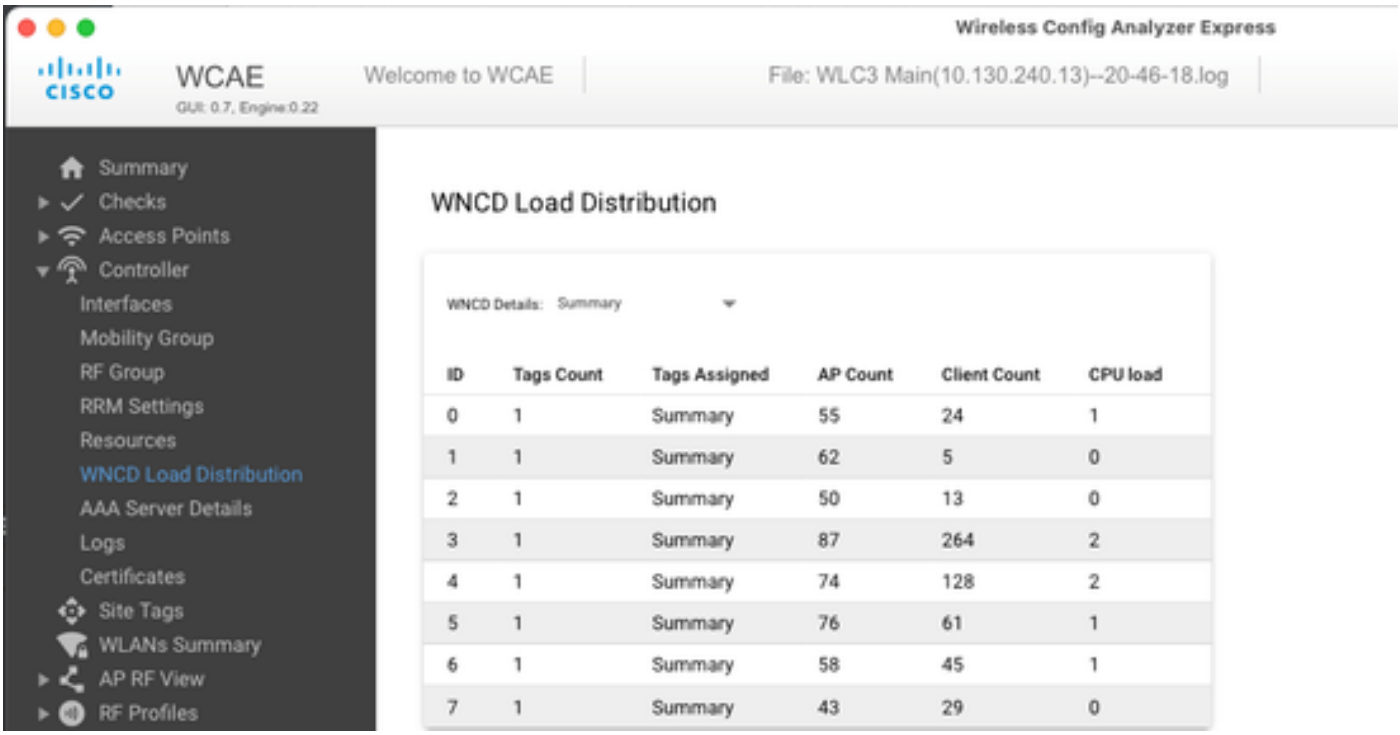
O comandoshow wireless loadbalance tag affinity CLI pode fornecer uma maneira fácil de ver o estado atual do balanceamento de carga do AP em todas as instâncias WNCD:

98001#show wireless loadbalance tag affinity

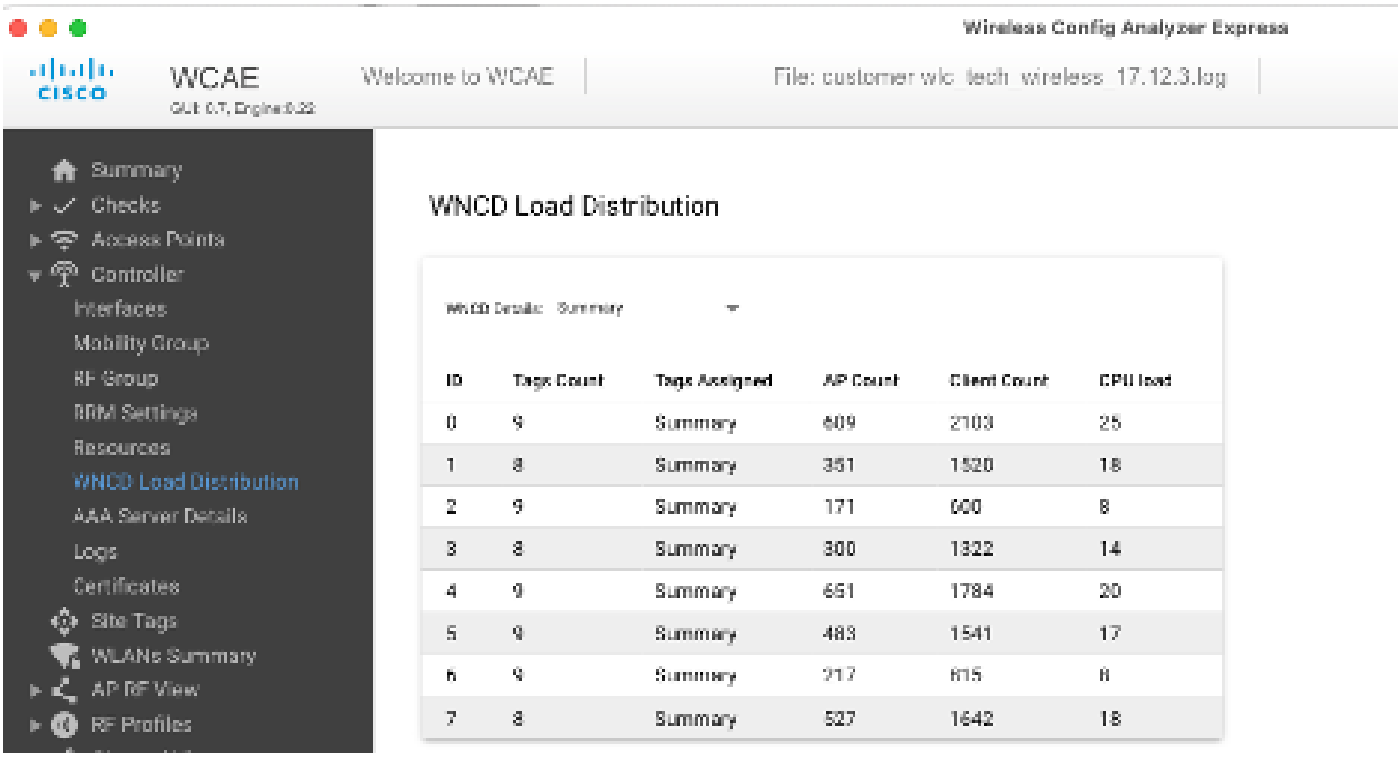
Tag	Tag type	No of AP's Joined	Load Config	Wncd Instance
Branch-tag	SITE TAG	10	0	0
Main-tag	SITE TAG	200	0	1
default-site-tag	SITE TAG	1	NA	2

se você quiser correlacionar a distribuição do AP com a contagem de clientes e a carga da CPU, a maneira mais fácil é usar a ferramenta de suporte WCAE e carregar uma show tech wireless tomada durante os horários de pico. A ferramenta resume a contagem de clientes WNCD, tirada de cada AP associado a ela.

Exemplo de um controlador balanceado corretamente, durante o baixo uso e a contagem de clientes:



Outro exemplo, para um controlador mais carregado, mostrando a utilização normal da CPU:



Qual é o mecanismo recomendado de balanceamento de carga do AP?

Resumindo, você pode resumir as diferentes opções em:

- Rede pequena, sem necessidade de roaming rápido, menos de 40% da carga do controlador: tag padrão.
- Se for necessário roaming rápido (OKC, FT, CCKM) ou grande número de clientes:

- Edifício único: criar tantos identificadores de site quanto CPUs (dependendo da plataforma)

- Antes das 17h12, ou menos de 500 contagens de AP: vários edifícios, filiais ou campus grande: crie uma marca de local por local de RF físico e configure o comando load por local.

- 17.12 e superior com mais de 500 APs: use o balanceamento de carga de RF.

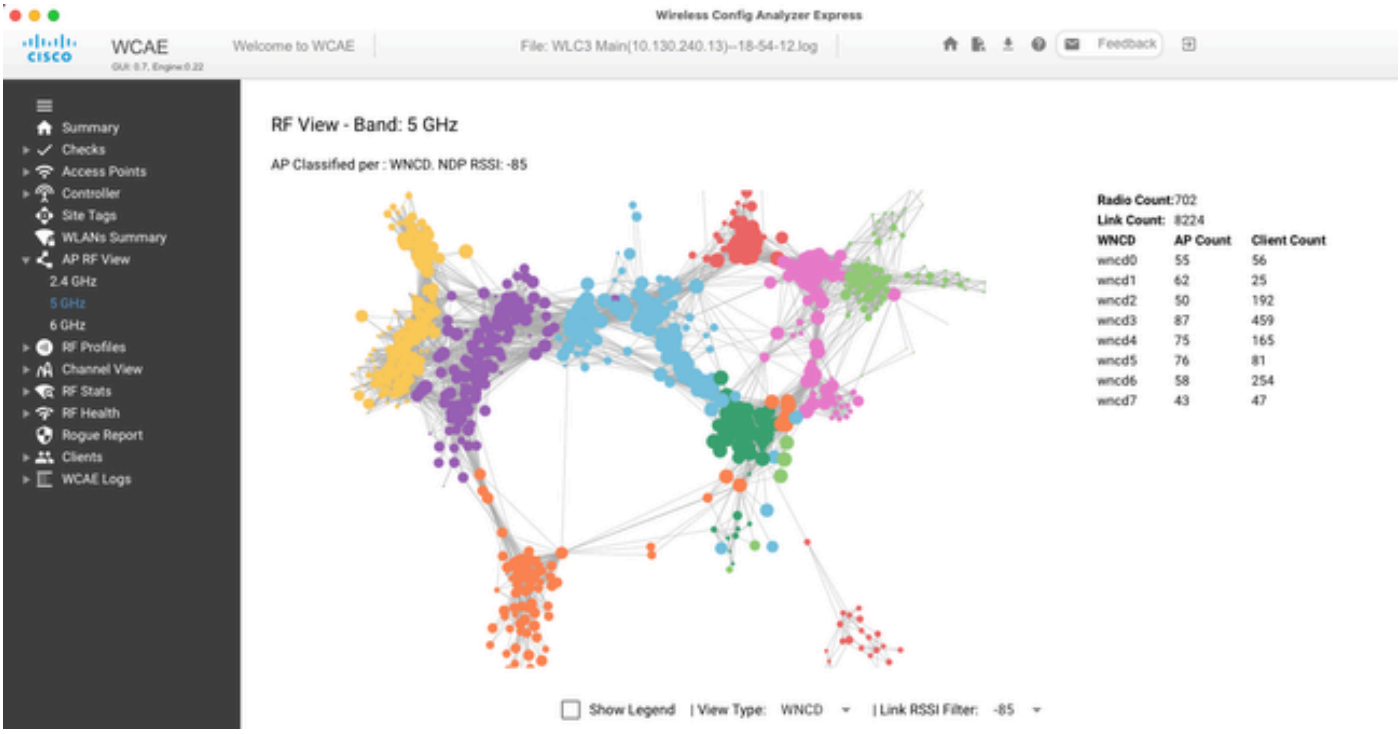
Esse limite de 500 APs deve ser marcado quando for eficaz aplicar o mecanismo de balanceamento de carga, pois ele agrupa APs em blocos de 100 unidades por padrão.

Visualização de distribuição WNCD do AP

Há cenários em que você deseja fazer um balanceamento de AP mais avançado e é desejável ter controle granular sobre como os APs são distribuídos pelas CPUs, por exemplo, cenários de densidade muito alta em que a principal métrica de carga é a contagem de clientes em vez de simplesmente focar no número de APs presentes no sistema.

Um bom exemplo dessa situação são os grandes eventos: um prédio poderia hospedar milhares de clientes, mais de várias centenas de APs e você precisaria dividir a carga em tantas CPUs quanto possível, mas otimizar o roaming ao mesmo tempo. Portanto, você não pode usar o WNCD em roaming, a menos que seja necessário. Você deseja evitar situações de "salt & pimenta" em que vários APs em WNCDs diferentes/marcas de site são misturados no mesmo local físico.

Para ajudar a fazer o ajuste fino e fornecer uma visualização da distribuição, você pode usar a ferramenta WCAE e aproveitar o recurso AP RF View:



Isso nos permite ver a distribuição AP/WNCD, apenas definida View Type como WNCD. Aqui cada cor representaria um WNCD/CPU. Você também pode definir o filtro RSSI como -85, para evitar conexões de sinal baixo, que também são filtradas pelo algoritmo RRM no controlador.

No exemplo anterior, correspondente ao Cisco Live EMEA 24, você pode ver que a maioria dos APs adjacentes são agrupados perfeitamente no mesmo WNCD, com sobreposição cruzada muito limitada.

As marcas de site alocadas para o mesmo WNCD obtêm a mesma cor.

Monitorando o Uso da CPU do Plano de Controle

É importante lembrar o conceito da arquitetura do Cisco IOS-XE e ter em mente que há duas "visões" principais do uso da CPU. Um vem do suporte histórico do Cisco IOS, e o principal, com uma visão holística da CPU em todos os processos e núcleos.

Em geral, você pode usar o comando show processes cpu platform sorted para coletar informações detalhadas de todos os processos no 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

Há vários pontos principais a serem destacados aqui:

- O processo ucode_pkt_PPE0 está manipulando o plano de dados nas plataformas 9800L e 9800CL e espera-se que ele observe uma alta utilização o tempo todo, ainda maior que 100%. Isso faz parte da implementação e não constitui um problema.

- É importante diferenciar o uso de pico em relação a uma carga sustentada e isolar o que é esperado em um determinado cenário. Por exemplo, a coleta de uma saída CLI muito grande, como show tech wireless pode gerar uma carga de pico em processos IOSd, smand, pubd, como uma saída de texto muito grande está sendo coletada, com centenas de comandos CLI executados, isso não é um problema e a carga diminui após a conclusão da saída.

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

- Espera-se a utilização de pico para núcleos WNCD durante tempos de atividade alta do cliente. É possível ver picos de 80%, sem impacto funcional, que normalmente não constituem 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

- Deve ser investigado um alto uso sustentado da CPU em um processo, superior a 90%, por mais de 15 minutos.

- Você pode monitorar a utilização da CPU do IOSd, com o comando show processes cpu sorted . Isso corresponde à atividade na

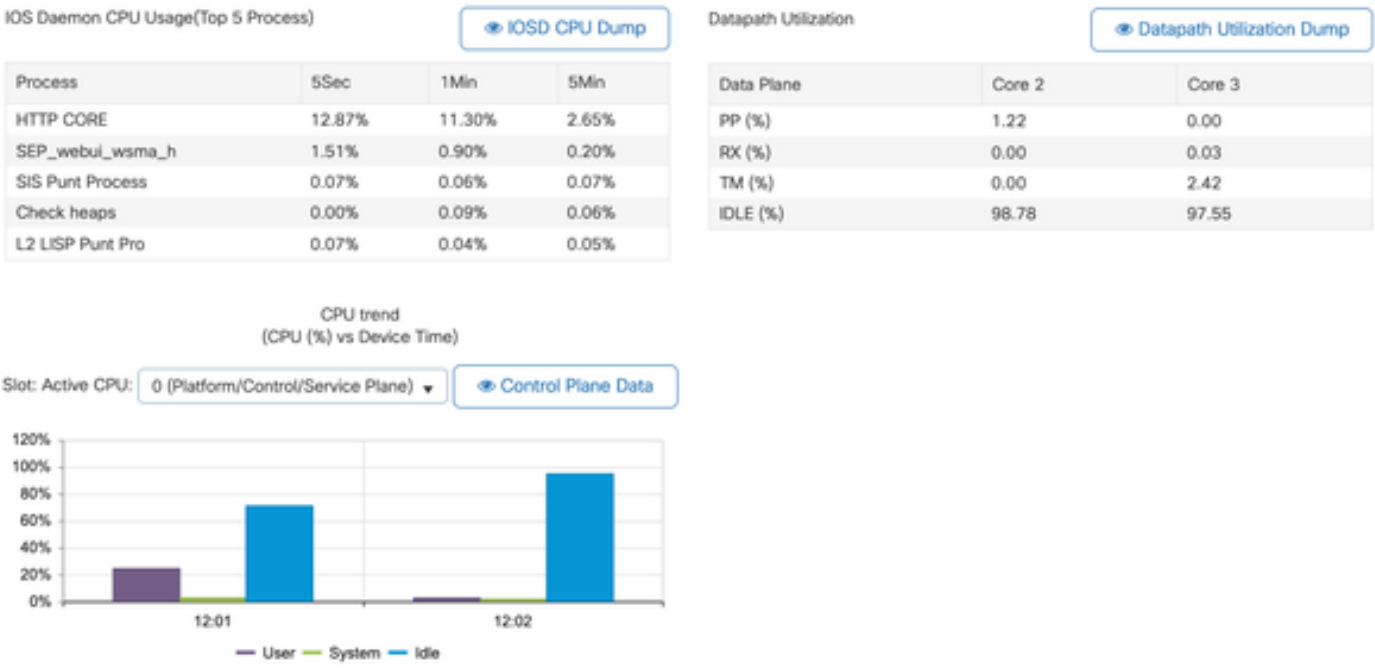
parte do processo linux_iosd-image da lista Cisco IOS-XE.

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

- Você pode usar a GUI do 9800 para obter uma visão rápida da carga do IOSd, do uso por núcleo e da carga do plano de dados:



Isso está disponível na guiaMonitoring/System/CPU Utilization .

O que é cada processo?

A lista de processos exata varia dependendo do modelo do controlador e da versão do Cisco IOS-XE. Esta é uma lista de alguns dos principais processos e não se destina a cobrir todas as entradas possíveis.

Nome do processo	O que ele faz?	Avaliação
wncd_x	Trata da maioria das operações sem fio. Dependendo do modelo 9800, você pode ter de 1 a 8 instâncias	Você pode ver picos de alta utilização durante horários de pico. Informar se a utilização ficou presa a 95% ou mais por vários minutos
linux_iosd-image	processo IOS	Esperava-se uma alta utilização ao coletar grandes saídas CLI (show tech) Operações SNMP grandes ou muito frequentes podem resultar em alta utilização da CPU
nginx	Servidor da Web	Esse processo pode mostrar picos e deve ser relatado somente em uma carga alta sustentada
ucode_pkt_PPE0	Plano de dados em 9800CL/9800L	Usar o comando **show platform hardware chassis active qfp datapath utilization** para monitorar este componente
ezman	Gerenciador de chipset para interfaces	Uma CPU alta sustentada aqui pode indicar um problema de HW ou um possível problema de software de kernel. Deve ser relatado
dbm	Gerenciador de Banco de Dados	Uma CPU alta sustentada deve ser informada aqui
odm_X	O Operation Data Manager lida com bancos de dados consolidados entre processos	CPU alta esperada em sistemas carregados
desonesto	Lida com a funcionalidade de invasor	Uma CPU alta sustentada deve ser informada aqui

smand	Gerenciador Shell. Cuida da análise CLI e da interação em diferentes processos	CPU alta esperada ao manipular grande saída CLI. CPU alta sustentada na ausência de carga deve ser informada
emd	Gerenciador Shell. Cuida da análise CLI e da interação em diferentes processos	CPU alta esperada ao manipular grande saída CLI. CPU com alto consumo sustentado na ausência de carga deve ser informada
pubd	Parte do tratamento de telemetria	Alta utilização de CPU esperada para grandes assinaturas de telemetria. CPU com alto consumo sustentado na ausência de carga deve ser informada

Mecanismos de proteção de alta CPU

Os controladores de LAN sem fio Catalyst 9800 têm mecanismos de proteção extensivos em torno da atividade da rede ou do cliente sem fio, para evitar alta utilização da CPU devido a cenários acidentais ou intencionais. Há vários recursos importantes projetados para ajudá-lo a conter dispositivos problemáticos:

Exclusão de Cliente

Essa opção é ativada por padrão, faz parte das Políticas de proteção sem fio e pode ser ativada ou desativada por Perfil de política. Isso pode detectar vários problemas de comportamento diferentes, remover o cliente da rede e defini-lo em uma "lista de exclusão temporária". Enquanto o cliente está nesse estado excluído, os APs não se comunicam com eles, impedindo qualquer ação adicional.

Depois que o temporizador de exclusão tiver passado (60 segundos por padrão), o cliente poderá se associar novamente.

Há vários desencadeadores para a exclusão de clientes:

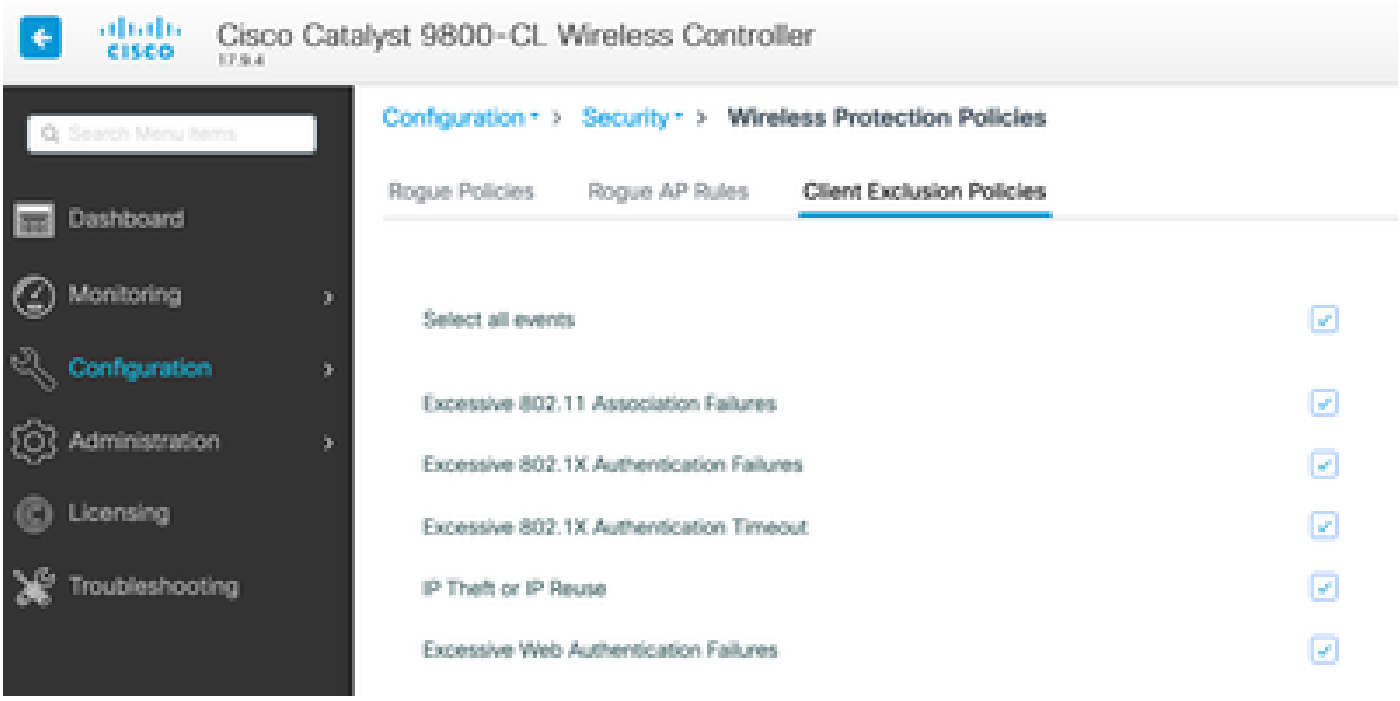
- Falhas de associação repetidas
- 3 ou mais erros de autenticação da Web, PSK ou 802.1x
- Tempos limite de autenticação repetidos (sem resposta do cliente)
- Tentando reutilizar um endereço IP já registrado em outro cliente
- Gerando uma inundação ARP

A exclusão de cliente protege seu controlador, AP e infraestrutura AAA (Radius) de vários tipos de alta atividade que podem levar a uma alta utilização da CPU. Em geral, não é aconselhável desativar qualquer um dos métodos de exclusão, a menos que seja necessário para um exercício

de Troubleshooting ou requisito de compatibilidade.

As configurações padrão funcionam para quase todos os casos, e somente em alguns cenários excepcionais, são necessárias para aumentar o tempo de exclusão ou desativar algum disparador específico. Por exemplo, alguns clientes legados ou especializados (IOT/Médico) talvez precisem ter o disparador de falha de associação desabilitado, devido a defeitos no lado do cliente que não podem ser corrigidos facilmente

Você pode personalizar os disparadores na interface do usuário: Configuração/Proteção sem fio/Políticas de exclusão de cliente:



O disparador de exclusão ARP foi projetado para ser habilitado permanentemente em um nível global, mas pode ser personalizado em cada perfil de política. Você pode verificar o status com o comando sh wireless profile policy all look for this specific output: (Procurar esta saída específica:)

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

Proteção do plano de controle contra tráfego de dados

Este é um mecanismo avançado no Plano de dados, para garantir que o tráfego enviado para o Plano de controle não exceda um conjunto predefinido de limites. O recurso é chamado de "Punt Policers" e, em quase todos os cenários, não é necessário tocá-los e, mesmo assim, só deve ser feito enquanto se trabalha com o Suporte da Cisco.

A vantagem dessa proteção é que ela fornece uma visão muito detalhada do que está acontecendo na rede e se há alguma atividade específica que esteja tendo uma taxa aumentada, ou pacotes inesperadamente altos por segundo.

Isso é exposto apenas por meio da CLI, pois eles normalmente fazem parte de uma funcionalidade avançada que raramente é necessária para modificação.

Para obter uma exibição de todas as 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

Pode ser uma lista grande, com mais de 160 entradas, dependendo da versão do software.

Na saída da tabela, você deseja verificar a coluna de pacotes descartados junto com qualquer entrada que tenha um valor diferente de zero na contagem alta de quedas.

Para simplificar a coleta de dados, você pode usar o comandoshow platform software punt-policer drop-only , para filtrar apenas entradas de vigilante com quedas.

Esse recurso pode ser útil para identificar se há tempestades ARP ou inundações de sondagem 802.11 (eles usam a fila "Pacotes 802.11 para LFTS"). LFTS significa Linux Forwarding Transport Service).

Controle de admissão de chamada sem fio

Em todas as versões de manutenção recentes, o controlador tem um monitor de atividade, para reagir dinamicamente à alta CPU e garantir que os túneis CAPWAP AP AP permaneçam ativos, em face da pressão insustentável.

O recurso verifica a carga WNCD e inicia a aceleração da nova atividade do cliente, para garantir que recursos suficientes permaneçam para lidar com as conexões existentes e proteger a estabilidade do CAPWAP.

Essa opção é ativada por padrão e não tem opções de configuração.

Há três níveis de proteção definidos: L1 com 80% de carga, L2 com 85% de carga e L3 com 89%, cada um disparando diferentes descartes de protocolo de entrada como mecanismos de proteção. A proteção é removida automaticamente assim que a carga diminui.

Em uma rede íntegra, você não deve ver eventos de carregamento de L2 ou L3 e, se eles estiverem ocorrendo com frequência, isso deve ser investigado.

Para monitorar, use o comandowireless stats cac como mostrado na imagem.

```
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
```

Proteções de mDNS

O mDNS como protocolo permite uma abordagem "automatizada" para detectar serviços entre dispositivos, mas, ao mesmo tempo, pode ser muito ativo e gerar carga significativamente, se não for configurado corretamente.

O mDNS, sem nenhuma filtragem, pode facilmente aumentar a utilização da CPU WNCD, vindo de vários fatores:

- Políticas mDNS com aprendizagem irrestrita, o controlador obterá todos os serviços oferecidos por todos os dispositivos. Isso pode levar a listas de serviços muito grandes, com centenas de entradas.
- Políticas definidas sem filtragem: isso fará com que o controlador envie essas grandes listas de serviços para cada cliente que perguntar quem está fornecendo um determinado serviço.
- Alguns serviços específicos do mDNS são fornecidos por "todos" os clientes sem fio, levando a um maior número de serviços e atividade, com variações disso por versão do sistema operacional.

Você pode verificar o tamanho da lista mDNS por serviço com 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
```

Isso pode fornecer uma ideia de quão grande pode obter qualquer consulta, não denota um problema por si só, apenas uma maneira de monitorar o que é rastreado.

Há algumas recomendações importantes de configuração do mDNS:

- Defina o transporte mDNS para um único protocolo:

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

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

Por padrão, ele usa transporte IPv4. Para obter desempenho, é recomendável usar IPv6 ou IPv4, mas não ambos:

- Sempre defina um filtro de localização na política de serviço mDNS, para evitar consultas/respostas não associadas. Em geral, recomenda-se o uso de "site-tag", mas outras opções podem funcionar, dependendo de suas necessidades.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.