Dépannage de la charge du processeur du contrôleur LAN sans fil

Table des matières

Introduction

Ce document décrit comment surveiller l'utilisation du CPU sur les contrôleurs LAN sans fil Catalyst 9800, et couvre plusieurs recommandations de configuration.

Présentation de l'utilisation du processeur

Avant de vous plonger dans le dépannage de la charge de CPU, vous devez comprendre les bases de la façon dont les CPU sont utilisés dans les contrôleurs LAN sans fil Catalyst 9800, et quelques détails sur l'architecture logicielle.

En général, le document Meilleures pratiques Catalyst 9800 définit un ensemble de bons paramètres de configuration qui peuvent empêcher les problèmes au niveau de l'application, par exemple, en utilisant le filtrage d'emplacement pour mDNS ou en s'assurant que l'exclusion de client est toujours activée. Nous vous conseillons d'appliquer ces recommandations avec les sujets exposés ici.

Notions de base

Les contrôleurs Catalyst 9800 ont été conçus comme une plate-forme flexible, ciblant différentes charges réseau et se concentrant sur l'évolutivité horizontale. Le nom de développement interne était « eWLC » avec le e pour « élastique », pour signifier que la même architecture logicielle, serait en mesure de fonctionner à partir d'un petit système intégré de CPU unique à plusieurs dispositifs de CPU / coeur à grande échelle.

Chaque WLC a deux « côtés » distincts :

- Plan de contrôle : gestion de toutes les interactions de « gestion » telles que CLI, UI, Netconf et tous les processus d'intégration pour les clients et les points d'accès.
- Plan de données : responsable du transfert réel des paquets et de la décapsulation du protocole CAPWAP, de l'application des politiques AVC, entre autres fonctionnalités.

Plan de contrôle

- La plupart des processus Cisco IOS-XE s'exécutent sous BinOS (noyau Linus), avec son propre planificateur spécialisé et ses propres commandes de surveillance.
- Il existe un ensemble de processus clés, appelés WNCD (Wireless Network Control Daemon), disposant chacun d'une base de données locale en mémoire, qui gèrent la majeure partie de l'activité sans fil. Chaque processeur possède un WNCD, pour répartir la charge sur tous les coeurs de processeur disponibles sur chaque système
- La répartition de la charge sur les WNCD est effectuée pendant la jonction AP. Quand un AP effectue une jonction CAPWAP au contrôleur, un équilibreur de charge interne distribue l'AP en utilisant un ensemble de règles possibles, pour assurer une utilisation correcte de toutes les ressources CPU disponibles.
- Le code Cisco IOS® s'exécute sur son propre processus appelé IOSd et possède son planificateur de CPU et ses commandes de surveillance. Cela permet de prendre en charge des fonctionnalités spécifiques, par exemple, CLI, SNMP, multidiffusion et routage.

Dans une vue simplifiée, le contrôleur comporte des mécanismes de communication entre le plan de commande et le plan de données, "punt", envoie du trafic du réseau au plan de commande, et "injection", pousse des trames du plan de commande dans le réseau.

Dans le cadre d'une enquête de dépannage de CPU élevée possible, vous devez surveiller le mécanisme punt, pour évaluer quel trafic atteint le plan de contrôle et pourrait conduire à une charge élevée.

Plan de données

Pour le contrôleur Catalyst 9800, il s'exécute dans le cadre du processeur de paquets Cisco (CPP), qui est une structure logicielle pour développer des moteurs de transfert de paquets, utilisés sur plusieurs produits et technologies.

L'architecture permet un ensemble de fonctionnalités communes, sur différentes implémentations matérielles ou logicielles, par exemple, permettant des fonctionnalités similaires pour le 9800CL par rapport au 9800-40, à différentes échelles de débit.

Équilibrage de charge AP

Le WLC effectue l'équilibrage de charge sur les CPU pendant le processus de jonction de point d'accès CAPWAP, avec le différenciateur clé étant le nom de balise de site AP. L'idée est que chaque AP représente une charge CPU spécifique ajoutée, provenant de son activité client, et l'AP lui-même. Il existe plusieurs mécanismes pour effectuer cet équilibrage :

- Si l'AP utilise « default-tag », il serait équilibré de manière circulaire sur tous les CPU/WNCD, avec chaque nouvelle jointure d'AP allant au WNCD suivant. C'est la méthode la plus simple, mais elle a peu d'implications :
    - C'est le scénario sous-optimal, car les points d'accès dans le même domaine d'itinérance RF effectueraient une itinérance Inter-WNCD fréquente, impliquant une communication inter-processus supplémentaire. L'itinérance entre les instances est plus lente d'un petit pourcentage.
    - Aucune distribution de clé PMK n'est disponible pour la balise de site FlexConnect (distant). Cela signifie que vous ne pouvez pas effectuer d'itinérance rapide pour le mode Flex, ce qui a un impact sur les modes d'itinérance OKC/FT.

      En général, la balise par défaut peut être utilisée sur des scénarios de charge inférieure (par exemple moins de 40 % de la charge du point d'accès et du client de la plate-forme 9800), et pour le déploiement de FlexConnect uniquement lorsque l'itinérance rapide n'est pas requise.

- Si l'AP a une balise de site personnalisée, la première fois qu'un AP appartenant au nom de la balise de site rejoint le contrôleur, la balise de site est assignée à une instance WNCD spécifique. Toutes les jointures supplémentaires suivantes d'AP avec la même balise sont attribuées au même WNCD. Cela garantit l'itinérance entre les AP dans la même étiquette de site, qui se produit dans le contexte WCND unique, qui fournit un flux plus optimal, avec une utilisation CPU inférieure. L'itinérance sur les WNCD est prise en charge, mais elle n'est pas aussi optimale que l'itinérance intra-WNCD.

- Décision d'équilibrage de charge par défaut : lorsqu'une balise est attribuée à un WNCD, l'équilibreur de charge sélectionne l'instance ayant le plus faible nombre de balises de site à ce moment-là. Comme la charge totale que cette balise de site peut avoir n'est pas connue, elle peut conduire à des scénarios d'équilibrage sous-optimaux. Cela dépend de l'ordre des jointures AP, combien de balises de site ont été définies, et si le nombre d'AP est asymétrique à travers eux

- Équilibrage de charge statique : pour empêcher l'affectation de balise de site non équilibrée à WNCD, la commande site load a été introduite dans la version 17.9.3 et ultérieure, pour permettre aux administrateurs de prédéfinir la charge attendue de chaque balise de site. Ceci est particulièrement utile lors de la gestion de scénarios de campus, ou de plusieurs filiales, chacune mappée à différents nombres d'AP, pour garantir que la charge est distribuée uniformément sur WNCD.

Par exemple, si vous avez un 9800-40, gérant un bureau principal, plus 5 filiales, avec des

nombres d'AP différents, la configuration pourrait ressembler à ceci :

```
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
```

Dans ce scénario, vous ne voulez pas que la balise du bureau central soit sur le même WNCD que Branch-3 et Branch-4, il y a au total 6 balises de site, et la plate-forme a 5 WNCD, donc il pourrait y avoir une chance que les balises de site les plus chargées atterrissent sur le même CPU. À l'aide de la commande load, vous pouvez créer une topologie prévisible d'équilibrage de charge AP.

La commande load est une indication de taille attendue, elle ne doit pas correspondre exactement au nombre d'AP, mais elle est normalement définie sur les AP attendus qui peuvent se joindre.

- Dans les scénarios où de grands bâtiments sont gérés par un seul contrôleur, il est plus facile et plus simple de créer autant de balises de site que de WNCD pour cette plate-forme spécifique (par exemple, C9800-40 en a cinq, C9800-80 en a 8). Attribuez les points d'accès de la même zone ou du même domaine d'itinérance aux mêmes balises de site afin de réduire la communication entre les WNCD.
- Équilibrage de charge RF : équilibre les points d'accès entre les instances WNCD, à l'aide de la relation de voisinage RF de RRM, et crée des sous-groupes en fonction de la proximité des points d'accès entre eux. Cela doit être fait après que les AP ont été en service pendant un certain temps et supprimer le besoin de configurer des paramètres d'équilibrage de charge statique. Disponible à partir de la version 17.12 et ultérieure.

Comment savoir combien de WNCD sont présents ?

Pour les plates-formes matérielles, le nombre de WNCD est fixe : 9800-40 a 5, 9800-80 a 8. Pour 9800CL (virtuel), le nombre de WNCD dépend du modèle de machine virtuelle utilisé lors du déploiement initial.

En règle générale, si vous voulez savoir combien de WNCD sont en cours d'exécution dans le système, vous pouvez utiliser cette commande sur tous les types de contrôleurs :

<#root>

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

5

Dans le cas du 9800-CL en particulier, vous pouvez utiliser la commande **show platform software system all** pour collecter des détails sur la plate-forme virtuelle :

<#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

Surveillance de l'équilibrage AP

L'affectation AP à WNCD est appliquée pendant le processus de jonction AP CAPWAP, de sorte qu'il n'est pas prévu qu'elle change pendant les opérations, quelle que soit la méthode d'équilibrage, à moins qu'il y ait un événement de réinitialisation CAPWAP à l'échelle du réseau où tous les AP se déconnectent et se rejoignent à nouveau.

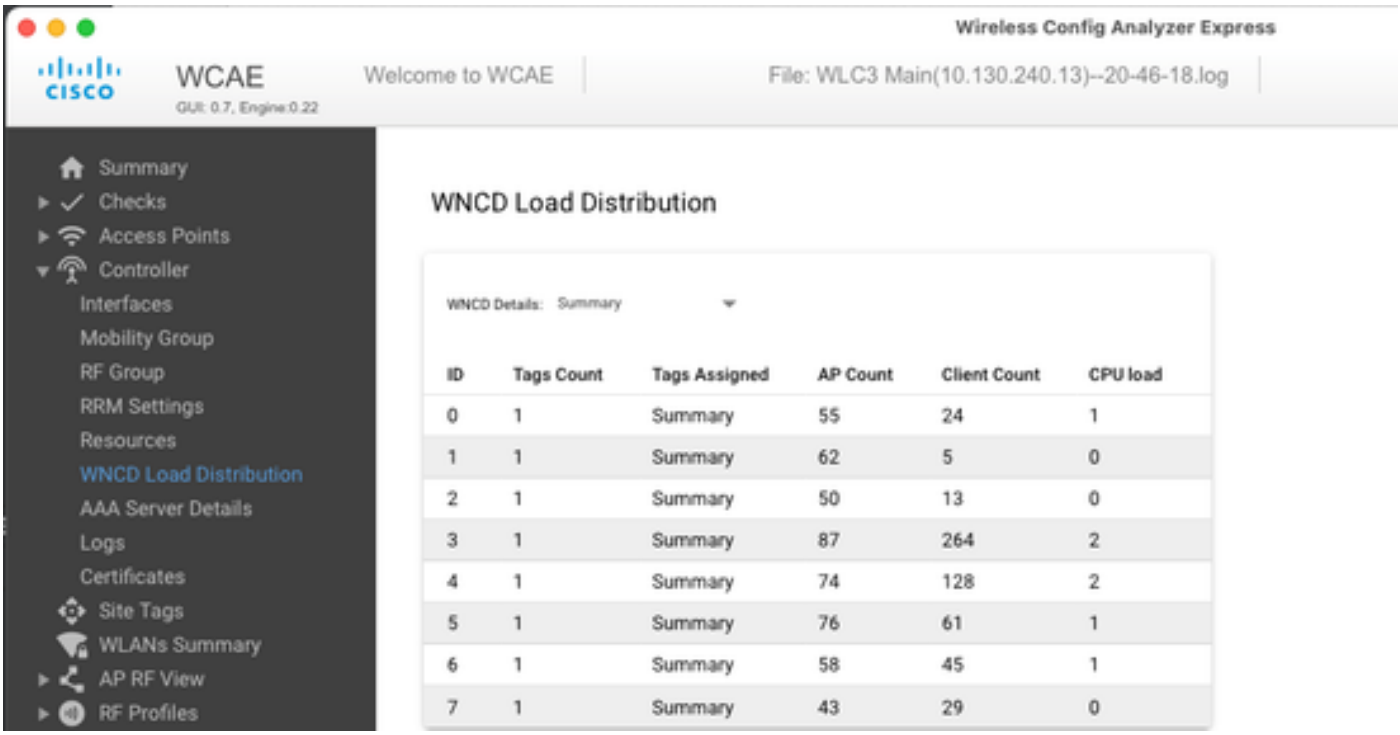
La commande CLI show wireless loadbalance tag affinity peut fournir un moyen facile de voir l'état actuel de l'équilibrage de charge AP sur toutes les instances WNCD :

98001#show wireless loadbalance tag affinity

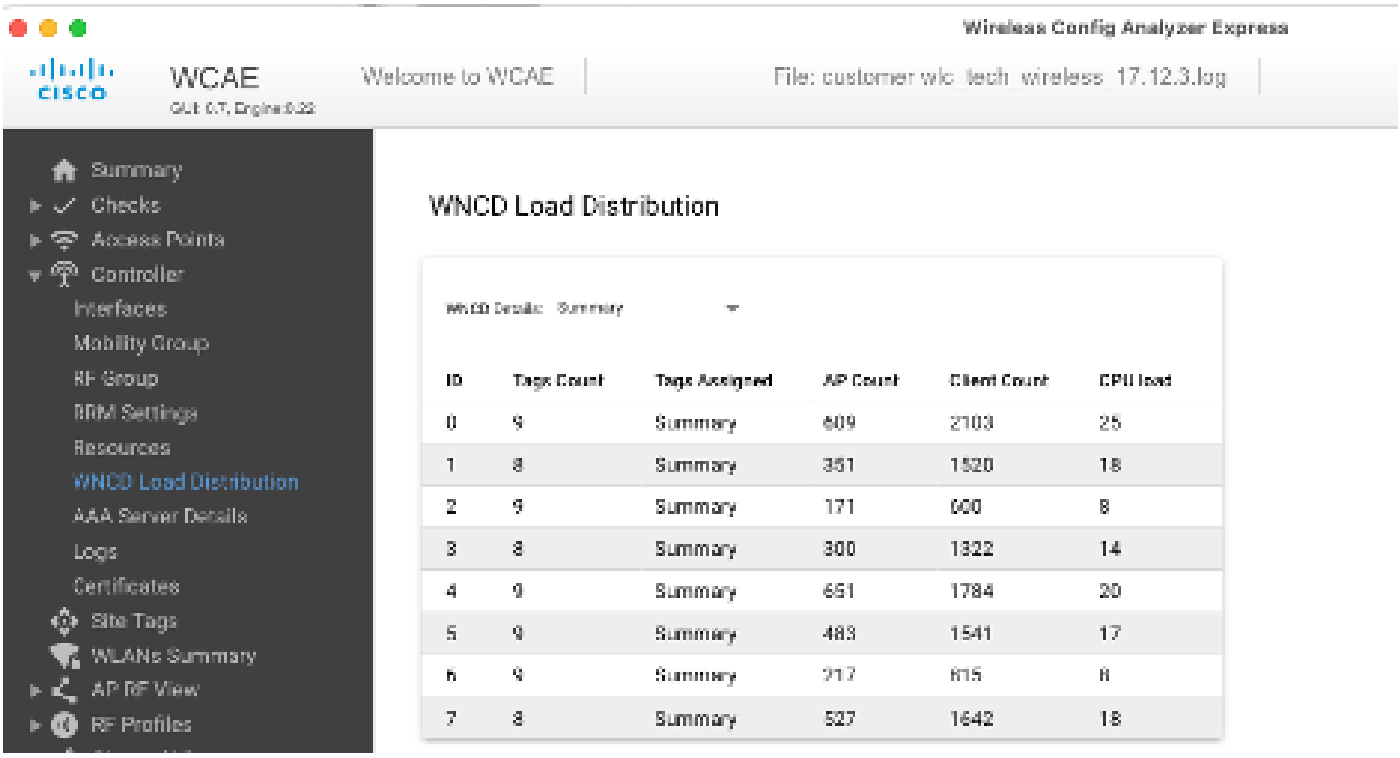
Tag	Tag type	No of AP's Joined	Load Config	Wncd Instance
Branch-tag	SITE TAG	10	0	0
Main-tag	SITE TAG	200	0	1
default-site-tag	SITE TAG	1	NA	2

si vous voulez corréler la distribution AP, avec le nombre de clients et la charge CPU, la façon la plus facile est d'utiliser l'outil de support WCAE et de charger une show tech wireless prise pendant les périodes occupées. L'outil récapitule le nombre de clients WNCD, pris à partir de chaque point d'accès qui lui est associé.

Exemple d'un contrôleur correctement équilibré, lors d'une faible utilisation et du nombre de clients :



Un autre exemple, pour un contrôleur plus chargé, montrant l'utilisation normale du CPU :



Quel est le mécanisme d'équilibrage de charge recommandé pour les points d'accès ?

En bref, vous pouvez résumer les différentes options dans :

- Petit réseau, pas besoin d'itinérance rapide, moins de 40 % de la charge du contrôleur : étiquette par défaut.
- Si l'itinérance rapide est nécessaire (OKC, FT, CCKM) ou si le nombre de clients est important :

- Bâtiment unique : créez autant de balises de site que de processeurs (dépendant de la plate-forme)
- Nombre de points d'accès avant 17h12, ou moins de 500 : plusieurs bâtiments, filiales ou grands campus : créez une étiquette de site par emplacement RF physique et configurez la commande load par site.
- 17.12 et supérieur avec plus de 500 points d'accès : utilisez l'équilibrage de charge RF.

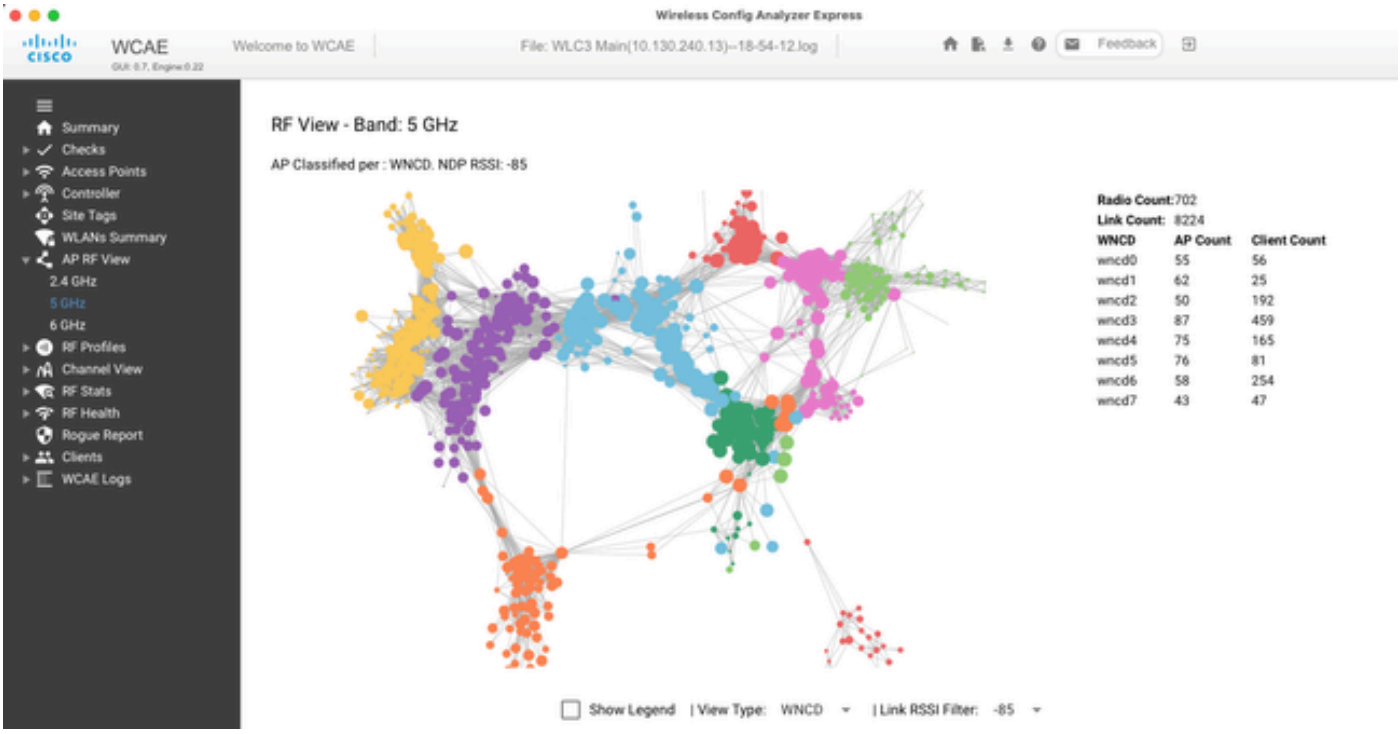
Ce seuil de 500 points d'accès, est pour marquer quand il est efficace d'appliquer le mécanisme d'équilibrage de charge, comme il groupe des points d'accès dans des blocs de 100 unités par défaut.

AP WNCD Distribution Visualization

Il y a des scénarios où vous voulez faire un équilibrage AP plus avancé, et il est souhaitable d'avoir un contrôle granulaire sur la façon dont les AP sont répartis sur les CPU, par exemple, des scénarios de très haute densité où la métrique de charge clé est le nombre de clients plutôt que de se concentrer uniquement sur le nombre d'AP présents dans le système.

Un bon exemple de cette situation est les grands événements : un bâtiment pourrait héberger des milliers de clients, plus de plusieurs centaines d'AP, et vous devriez répartir la charge sur autant de CPU que possible, mais optimiser l'itinérance en même temps. Ainsi, vous ne parcourez pas WNCD à moins d'en avoir besoin. Vous voulez éviter les situations « sel et poivre » où plusieurs points d'accès dans différents WNCD/balises de site sont mélangés dans le même emplacement physique.

Pour vous aider à affiner et fournir une visualisation de la distribution, vous pouvez utiliser l'outil WCAE et tirer parti de la fonctionnalité AP RF View :



Cela nous permet de voir la distribution AP/WNCD, simplement définie surView Type WNCD. Ici, chaque couleur représente un WNCD/CPU. Vous pouvez également définir le filtre RSSI sur -85, pour éviter les connexions à faible signal, qui sont également filtrées par l'algorithme RRM dans le contrôleur.

Dans l'exemple précédent, correspondant à CiscoLive EMEA 24, vous pouvez voir que la plupart des points d'accès adjacents sont regroupés en grappe dans le même WNCD, avec un chevauchement croisé très limité.

Les balises de site allouées au même WNCD, obtiennent la même couleur.

Surveillance de l'utilisation CPU du plan de contrôle

Il est important de se rappeler le concept d'architecture Cisco IOS-XE et de garder à l'esprit qu'il existe deux « vues » principales de l'utilisation du processeur. L'un provient de l'historique de la prise en charge de Cisco IOS, et le principal, avec une vue holistique du CPU sur tous les processus et coeurs.

En général, vous pouvez utiliser la commande show processes cpu platform sorted pour collecter des informations détaillées sur tous les processus de 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

Il y a plusieurs points importants à souligner ici :

- Le processus ucode_pkt_PPE0 gère le plan de données sur les plates-formes 9800L et 9800CL, et on s'attend à une utilisation élevée tout le temps, même supérieure à 100 %. Cela fait partie de la mise en oeuvre, et cela ne constitue pas un problème.

- Il est important de différencier l'utilisation maximale d'une charge soutenue et d'isoler ce qui est attendu dans un scénario donné. Par exemple, la collecte d'une sortie CLI très volumineuse, comme show tech wireless peut générer une charge de pointe sur les processus IOSd, smand, pubd, alors qu'une sortie de texte très volumineuse est collectée, avec des centaines de commandes CLI exécutées, ce n'est pas un problème, et la charge diminue une fois la sortie terminée.

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

- L'utilisation maximale des coeurs WNCD est prévue, pendant les périodes d'activité client élevée. Il est possible de voir des pics de 80 %, sans aucun impact fonctionnel, et ils ne constituent normalement pas un problème.

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

- Une utilisation élevée et durable du CPU sur un processus, supérieure à 90 %, pendant plus de 15 minutes, doit être étudiée.

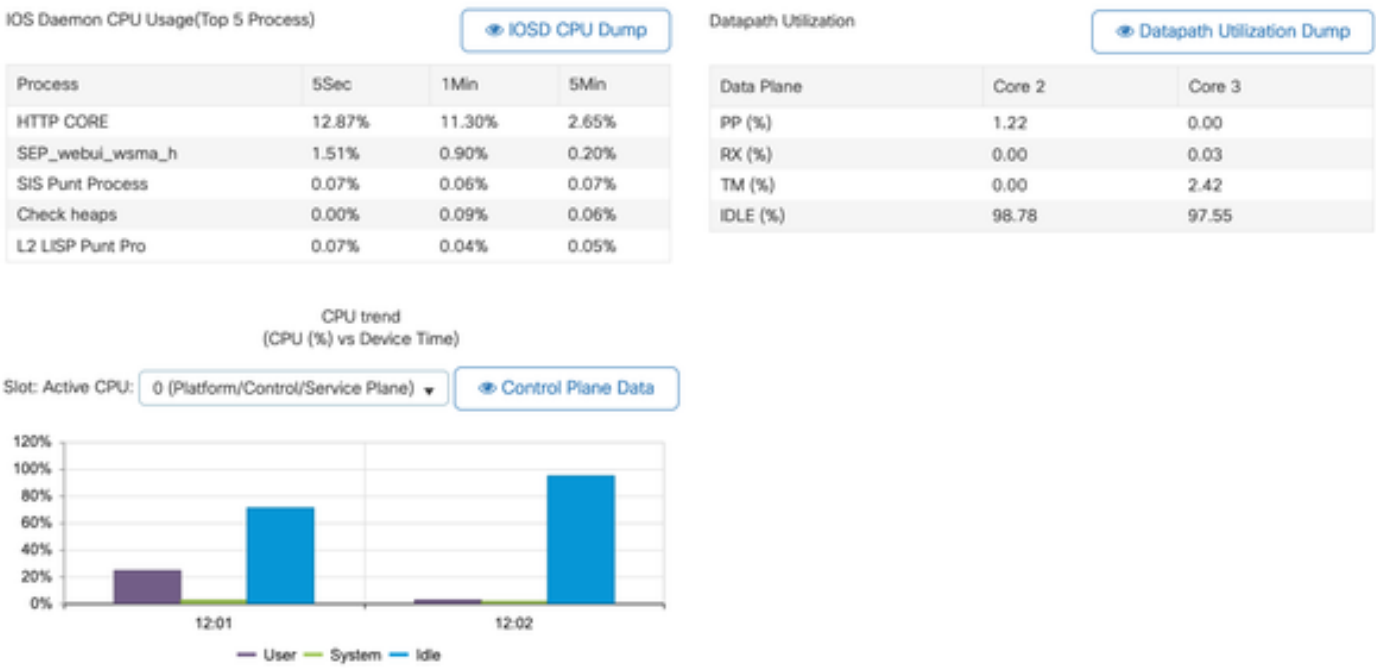
- Vous pouvez surveiller l'utilisation du processeur IOSd à l'aide de la commande show processes cpu sorted . Cela correspond à l'activité dans la partie processus linux_iosd-image de la liste Cisco IOS-XE.

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

- Vous pouvez utiliser l'interface utilisateur graphique du 9800 pour afficher rapidement la charge de l'IOSd, l'utilisation par coeur et la charge du plan de données :



Cette option est disponible dans l'Monitoring/System/CPU Utilizationonglet.

Quel est chaque processus ?

La liste exacte des processus varie en fonction du modèle de contrôleur et de la version de Cisco IOS-XE. Il s'agit d'une liste de certains des

processus clés, et il n'est pas destiné à couvrir toutes les entrées possibles.

Nom du processus	Qu'est-ce que ça fait ?	Évaluation
wncd_x	Gère la plupart des opérations sans fil. Selon le modèle 9800, vous pouvez avoir entre 1 et 8 instances	Vous pouvez observer des pics d'utilisation pendant les heures de pointe. Signalez si l'utilisation est bloquée à 95 % ou plus pendant plusieurs minutes
linux_iosd-image	processus IOS	Utilisation élevée attendue en cas de collecte de résultats CLI importants (show tech) Des opérations SNMP importantes ou trop fréquentes peuvent entraîner une utilisation CPU élevée
nginx	serveur Web	Ce processus peut présenter des pics et ne doit être signalé que sur une charge élevée soutenue
ucode_pkt_PPE0	Plan de données 9800CL/9800L	Utilisez la commande **show platform hardware chassis active qfp datapath utilization** pour surveiller ce composant
ezman	Gestionnaire de chipsets pour interfaces	Un processeur élevé et soutenu peut indiquer un problème matériel ou un problème logiciel du noyau. Elle doit être signalée
dbm	Gestionnaire de bases de données	Un CPU élevé et soutenu doit être signalé ici
odm_X	Operation Data Manager gère la base de données consolidée sur les processus	CPU élevé attendu sur les systèmes chargés

rugueux	Gère les fonctionnalités indésirables	Un CPU élevé et soutenu doit être signalé ici
feu	Gestionnaire de shell. Prend en charge l'analyse CLI et l'interaction entre les différents processus	CPU élevé attendu lors de la gestion de grandes sorties CLI. Un CPU élevé soutenu en l'absence de charge doit être signalé
emd	Gestionnaire de shell. Prend en charge l'analyse CLI et l'interaction entre les différents processus	CPU élevé attendu lors de la gestion de grandes sorties CLI. Un CPU élevé soutenu sur l'absence de charge doit être signalé
pub	Partie du traitement de télémétrie	CPU élevé attendu pour les abonnements télémétriques volumineux. Un CPU élevé soutenu sur l'absence de charge doit être signalé

Mécanismes de protection CPU élevée

Les contrôleurs LAN sans fil du Catalyst 9800 disposent de mécanismes de protection étendus pour les activités du réseau ou du client sans fil, afin d'empêcher une utilisation CPU élevée en raison de scénarios accidentels ou intentionnels. Il existe plusieurs fonctionnalités clés conçues pour vous aider à contenir les périphériques problématiques :

Exclusion du client

Cette option est activée par défaut et fait partie des stratégies de protection sans fil. Elle peut être activée ou désactivée par profil de stratégie. Cela permet de détecter plusieurs problèmes de comportement, de supprimer le client du réseau et de le placer dans une « liste d'exclusion temporaire ». Lorsque le client est dans cet état exclu, les AP ne leur parlent pas, ce qui empêche toute autre action.

Une fois le délai d'exclusion écoulé (60 secondes par défaut), le client est autorisé à s'associer à nouveau.

Il existe plusieurs déclencheurs d'exclusion de client :

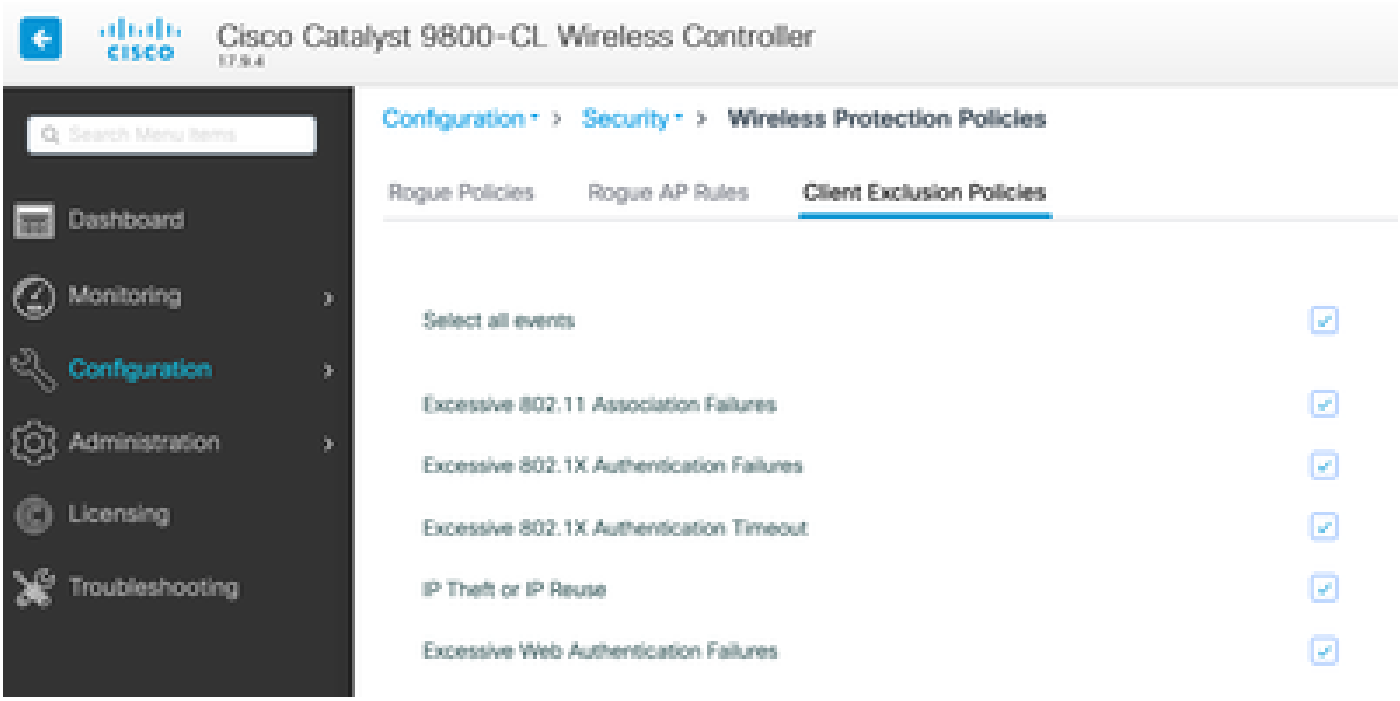
- Échecs d'association répétés
- 3 erreurs d'authentification webauth, PSK ou 802.1x ou plus
- Expirations répétées des délais d'authentification (aucune réponse du client)
- Tentative de réutilisation d'une adresse IP déjà enregistrée sur un autre client

- Génération d'une inondation ARP

L'exclusion des clients protège votre contrôleur, votre point d'accès et votre infrastructure AAA (Radius) contre plusieurs types de haute activité qui pourraient entraîner une CPU élevée. En général, il n'est pas conseillé de désactiver l'une des méthodes d'exclusion, sauf si cela est nécessaire pour un exercice de dépannage ou une exigence de compatibilité.

Les paramètres par défaut fonctionnent pour presque tous les cas, et seulement sur certains scénarios exceptionnels, est nécessaire pour augmenter le temps d'exclusion, ou désactiver un déclencheur spécifique. Par exemple, certains clients existants ou spécialisés (IOT/Medical) peuvent nécessiter la désactivation du déclencheur d'échec d'association, en raison de défauts côté client qui ne peuvent pas être facilement corrigés

Vous pouvez personnaliser les déclencheurs dans l'interface utilisateur : Configuration/Wireless Protection/Client Exclusion Policies :



Le déclencheur d'exclusion ARP a été conçu pour être activé de manière permanente au niveau global, mais il peut être personnalisé sur chaque profil de stratégie. Vous pouvez vérifier l'état à l'aide de la commande sh wireless profile policy all look for this specific output :

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

Protection du plan de contrôle contre le trafic de données

Il s'agit d'un mécanisme avancé dans le plan de données, destiné à garantir que le trafic envoyé au plan de contrôle ne dépasse pas un ensemble prédéfini de seuils. Cette fonctionnalité est appelée « Policiers ponctuels » et dans presque tous les scénarios, il n'est pas nécessaire de les toucher. Même dans ce cas, il suffit de travailler avec l'assistance Cisco.

L'avantage de cette protection est qu'elle fournit un aperçu très détaillé de ce qui se passe sur le réseau, et si une activité spécifique présente un débit accru, ou des paquets par seconde étonnamment élevés.

Cette fonctionnalité n'est disponible que via l'interface de ligne de commande, car elle fait généralement partie de fonctionnalités avancées rarement modifiées.

Pour obtenir une vue de toutes les politiques 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

Il peut s'agir d'une longue liste de plus de 160 entrées, selon la version du logiciel.

Dans la sortie de la table, vous voulez vérifier la colonne de paquets abandonnés avec toute entrée qui a une valeur non nulle sur le nombre d'abandons élevé.

Pour simplifier la collecte des données, vous pouvez utiliser la commande show platform software punt-policer drop-only , pour filtrer uniquement les entrées de l'analyseur avec des abandons.

Cette fonctionnalité peut être utile pour identifier s'il y a des tempêtes ARP ou des inondations de sonde 802.11 (ils utilisent la file d'attente « 802.11 Packets to LFTS »). LFTS signifie Linux Forwarding Transport Service).

Contrôle d'admission des appels sans fil

Dans toutes les versions de maintenance récentes, le contrôleur dispose d'un moniteur d'activité, pour réagir dynamiquement à une CPU élevée, et s'assurer que les tunnels AP CAPWAP restent actifs, face à une pression insoutenable.

La fonctionnalité vérifie la charge WNCD et commence à limiter la nouvelle activité du client, afin de s'assurer que suffisamment de ressources restent disponibles pour gérer les connexions existantes et protéger la stabilité CAPWAP.

Cette option est activée par défaut et ne dispose pas d'options de configuration.

Trois niveaux de protection sont définis, L1 à 80 % de charge, L2 à 85 % de charge et L3 à 89 %, chacun déclenchant des abandons de protocole entrants différents en tant que mécanismes de protection. La protection est automatiquement supprimée dès que la charge diminue.

Dans un réseau sain, vous ne devriez pas voir d'événements de chargement de couche 2 ou 3, et s'ils se produisent fréquemment, ils doivent être étudiés.

Pour surveiller, utilisez la commande wireless stats cac comme illustré dans l'image.

```
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
```

Protections mDNS

Le mDNS en tant que protocole permet une approche « sans intervention » pour détecter les services sur les périphériques, mais en même temps, il peut être très actif et entraîner une charge importante, s'il n'est pas configuré correctement.

mDNS, sans aucun filtrage, peut facilement augmenter l'utilisation du CPU WNCD, en raison de plusieurs facteurs :

- Stratégies mDNS avec apprentissage illimité, le contrôleur obtiendra tous les services offerts par tous les périphériques. Cela peut conduire à de très grandes listes de services, avec des centaines d'entrées.
- Stratégies définies sans filtrage : cela amènera le contrôleur à transmettre ces grandes listes de services, à chaque client qui demande qui fournit un service donné.
- Certains services spécifiques à mDNS sont fournis par « tous » les clients sans fil, ce qui augmente le nombre de services et l'activité, avec des variations par version du système d'exploitation.

Vous pouvez vérifier la taille de la liste mDNS par service avec cette commande :

```
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

Cela peut donner une idée de la taille d'une requête donnée, cela ne dénote pas un problème en soi, juste un moyen de surveiller ce qui est suivi.

Voici quelques recommandations importantes concernant la configuration de mDNS :

- Définissez le transport mDNS sur un protocole unique :

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

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

Par défaut, il utilise le transport IPv4. Pour des raisons de performances, il est conseillé d'utiliser IPv6 ou IPv4, mais pas les deux :

- Définissez toujours un filtre d'emplacement dans la stratégie de service mDNS, pour éviter les requêtes/réponses indépendantes. En général, il est recommandé d'utiliser « site-tag », mais d'autres options pourraient fonctionner, selon vos besoins.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.