Dépannage de la charge du processeur du contrôleur LAN sans fil

Table des matières

Introduction

Présentation de l'utilisation du processeur

Notions de base

- Plan de contrôle
- Plan de données

Équilibrage de charge AP

- Comment savoir combien de WNCD sont présents

Surveillance de l'équilibrage AP

- Quel est le mécanisme d'équilibrage de charge recommandé pour les points d'accès
- AP WNCD Distribution Visualization

Surveillance de l'utilisation CPU du plan de contrôle

- Qu'est-ce que chaque processus

Mécanismes de protection CPU élevée

- Exclusion du client
- Protection du plan de contrôle contre le trafic de données
- Contrôle d'admission des appels sans fil

Protections mDNS

J'ai besoin de plus d'assistance

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 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 du client est toujours activée. Nous vous conseillons d'appliquer ces recommandations avec les rubriques présentées 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 s'exécuterait 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 et de la décapsulation réels des paquets CAPWAP, de l'application des politiques AVC, entre autres fonctionnalités.

Plan de contrôle

- La plupart des processus Cisco IOS® s'exécutent sous BinOS (noyau Linux) avec son propre planificateur spécialisé et ses propres commandes de surveillance.
- Il existe un ensemble de processus clés, appelés WNCD (Wireless Network Control Daemon), chacun d'eux disposant d'une base de données locale en mémoire, qui gère la plupart des activités 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 terminée pendant une jointure 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 a son planificateur de CPU. Cela permet de prendre en charge des fonctionnalités spécifiques, par exemple, CLI, SNMP, multidiffusion et routage.

Dans une vue simplifiée, l'unité de commande possède des mécanismes de communication entre le plan de commande et le plan de données, punt, envoie du trafic du réseau au plan de

commande, injecte et 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 peut 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 permettant de développer des moteurs de transfert de paquets utilisés sur plusieurs produits et technologies.

L'architecture permet un ensemble de fonctionnalités communes à différentes mises en oeuvre matérielles ou logicielles. Par exemple, il permet 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 de l'AP lui-même. Il existe plusieurs mécanismes pour effectuer cet équilibrage :

- Si le point d'accès utilise une balise default-tag, il équilibre de manière circulaire sur tous les CPU/WNCD avec chaque nouvelle jointure de point d'accès allant au WNCD suivant. C'est la méthode la plus simple, cependant, elle a quelques implications :
    - C'est le scénario sous-optimal, car les points d'accès dans le même domaine d'itinérance RF ont 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 affecte les modes d'itinérance OKC/FT.

En général, la balise par défaut peut être utilisée dans 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 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 appartient 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 que l'itinérance entre les AP dans la même balise de site se produit dans le seul contexte WCND. Cela permet d'obtenir un flux plus optimal, avec une utilisation moindre du processeur. L'itinérance sur les WNCD est prise en charge, mais elle n'est pas aussi optimale dans 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 petit nombre de balises de site à ce moment-là. La charge totale que la balise de site peut avoir est inconnue, elle peut conduire à des scénarios d'équilibrage sous-optimaux. Cela dépend de l'ordre dans lequel le point d'accès se joint, combien de balises de site ont été définies, et si le nombre de points d'accès est asymétrique entre eux.

- Équilibrage de charge statique : Pour empêcher l'attribution de balises de site non équilibrées à WNCD, la commande site load a été introduite dans la version 17.9.3 et ultérieure. Cela permet aux administrateurs de prédéfinir la charge attendue de chaque balise de site. Cela est utile lors de la gestion de scénarios de campus ou de plusieurs filiales, chacune étant mappée à des nombres d'AP différents pour garantir une répartition uniforme de la charge sur WNCD.

Si vous disposez d'un 9800-40 gérant un bureau principal, plus 5 filiales avec des nombres de points d'accès différents, la configuration peut 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 6 balises de site au total et la plate-forme a 5 WNCD et il y a une chance que les balises de site les plus chargées atterrissent sur le même processeur. En exécutant la commande load, vous pouvez créer une topologie prévisible d'équilibrage de charge AP.

La commande load est une taille attendue. Il n'a pas besoin de correspondre exactement au nombre d'AP, cependant, il est normalement défini 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 de créer autant de balises de site que de WNCD pour cette plate-forme spécifique (par exemple, C9800-40 en a 5, 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 : Cela équilibre les AP entre les instances WNCD, en utilisant la relation de voisinage RF de RRM, et crée des sous-groupes en fonction de la proximité des AP les uns par rapport aux autres. Il doit être terminé 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 trouver et déterminer combien de WNCD sont en cours d'exécution dans le système, vous pouvez exécuter 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, vous pouvez exécuter 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

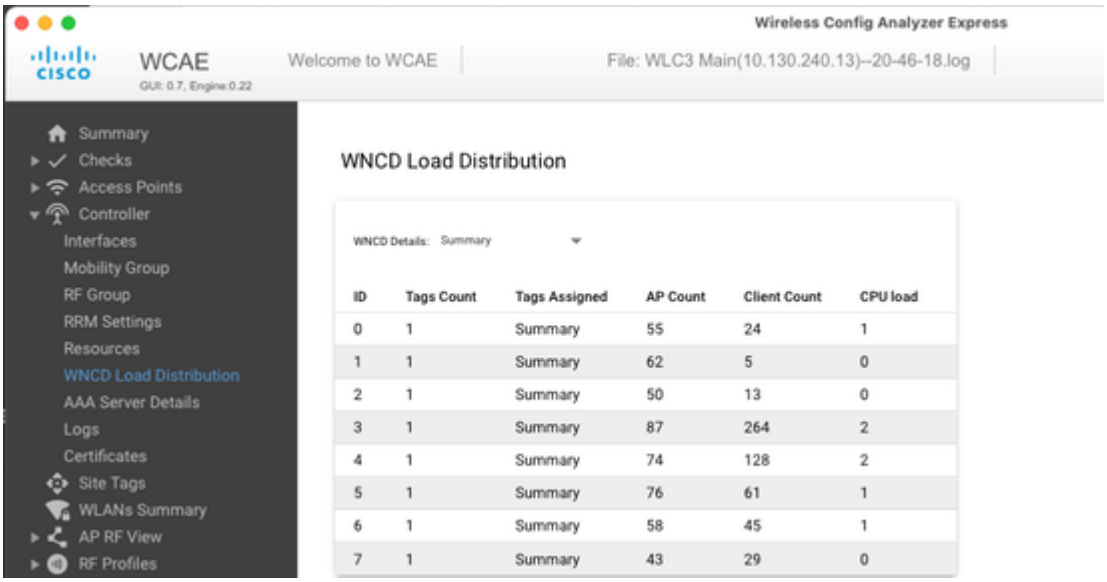
L'affectation AP à WNCD est appliquée pendant le processus de jointure AP CAPWAP et il n'est pas prévu qu'elle change pendant les opérations, quelle que soit la méthode d'équilibrage. Sauf s'il existe un événement de réinitialisation CAPWAP à l'échelle du réseau où tous les points d'accès se déconnectent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

L'exécution de la commande CLI show wireless loadbalance tag affininity peut fournir un moyen facile d'afficher 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
```

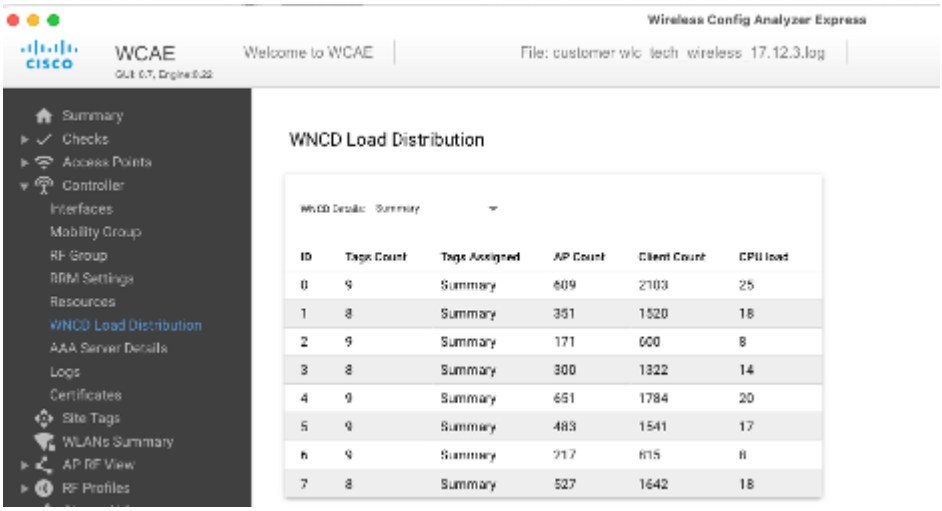
Si vous voulez mettre en corrélation la distribution AP avec le nombre de clients et la charge CPU, vous pouvez utiliser l'outil de support WCAE et charger un show tech wireless pris pendant les heures de pointe. L'outil récapitule le nombre de clients WNCD, pris à partir de chaque point d'accès qui lui est associé.

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



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

Un autre exemple est pour un contrôleur plus chargé, montrant l'utilisation normale du 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	815	8
7	8	Summary	527	1642	18

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

En bref, vous pouvez résumer les différentes options dans :

- Petits réseaux, pas besoin d'itinérance rapide, moins de 40 % de la charge du contrôleur : Balise par défaut.
- Si l'itinérance rapide est requise (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).
  - Avant 17.12, ou moins de 500 points d'accès : Bâtiments multiples, succursales 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 : utiliser l'équilibrage de charge RF.

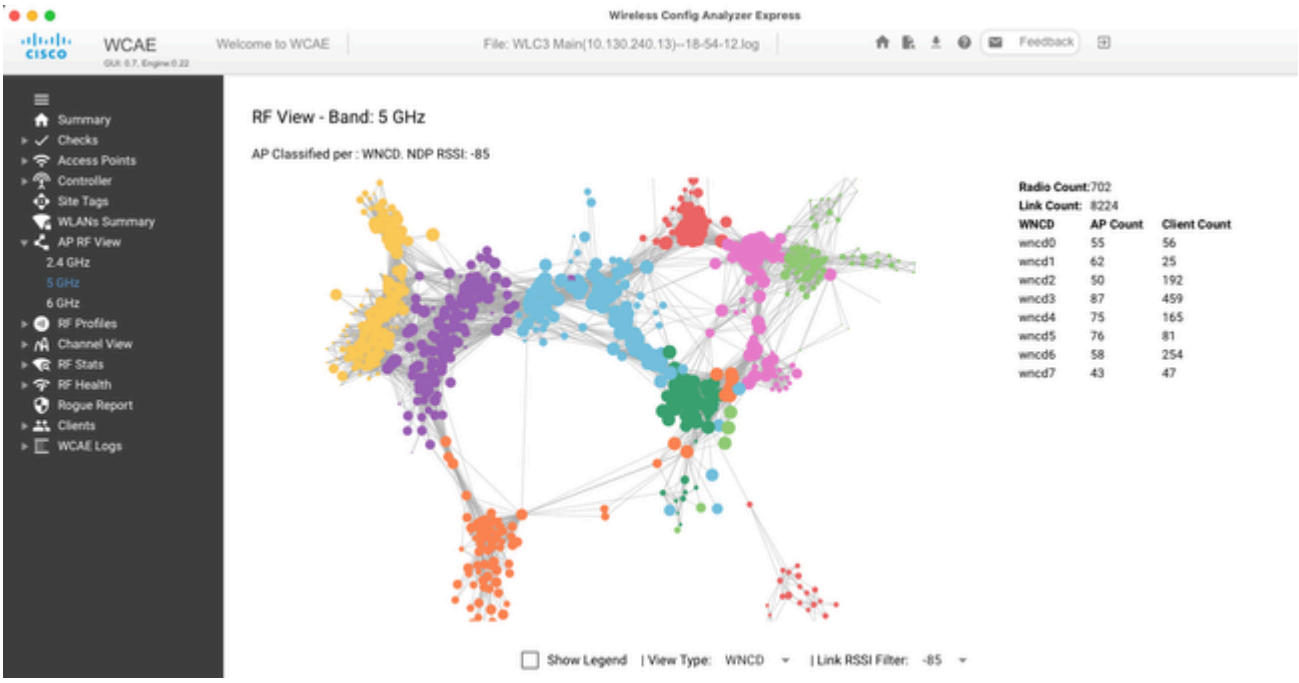
Ce seuil de 500 points d'accès, est à marquer quand il est efficace d'appliquer le mécanisme d'équilibrage de charge, comme il groupe des points d'accès dans des blocs de 100 unités par défaut.

AP WNCD Distribution Visualization

Il existe des scénarios où vous pouvez appliquer l'équilibrage avancé des AP, et il est souhaitable d'avoir un contrôle granulaire sur la façon dont les AP sont répartis sur les CPU. Par exemple, les scénarios de très haute densité dans lesquels la métrique de charge principale est le nombre de clients plutôt que de se concentrer sur le nombre de points d'accès présents dans le système.

Un bon exemple de cette situation est les grands événements où un bâtiment peut héberger des milliers de clients sur plusieurs centaines d'AP, et où vous devez répartir la charge sur autant de CPU que possible, mais optimiser l'itinérance en même temps. Vous ne parcourez pas WNCD à moins d'en avoir besoin. Vous voulez éviter les situations où plusieurs AP 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 vous permet d'afficher la distribution AP/WNCD, il suffit de définir le Type d'affichage sur WNCD. Chaque couleur représente un WNCD/CPU et vous pouvez définir le filtre RSSI sur -85 pour éviter les connexions à faible signal. Ils sont également filtrés 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 mis en grappe sur le même WNCD avec un chevauchement croisé très limité. Les balises de site attribuées au même WNCD reçoivent 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 présente une vue globale du processeur sur tous les processus et coeurs.

En général, vous pouvez exécuter la commande show processes cpu platform triée pour collecter des informations détaillées pour tous les processus à travers 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 :

- Le processus ucode_pkt_PPE0 gère le plan de données sur les plates-formes 9800L et 9800CL. On s'attend à une utilisation élevée tout le temps, même supérieure à 100%. Cela fait partie de la mise en oeuvre et 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 très grande sortie CLI, comme show tech wireless peut générer une charge de pointe sur les processus IOSd, smand et pubd, car une très grande sortie de texte est collectée avec des centaines de commandes CLI exécutées. Ce n'est pas un problème et la charge diminue une fois que le résultat est terminé.

```
   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 posent normalement pas de 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 supérieur à 90 % pendant plus de 15 minutes doit être étudiée.

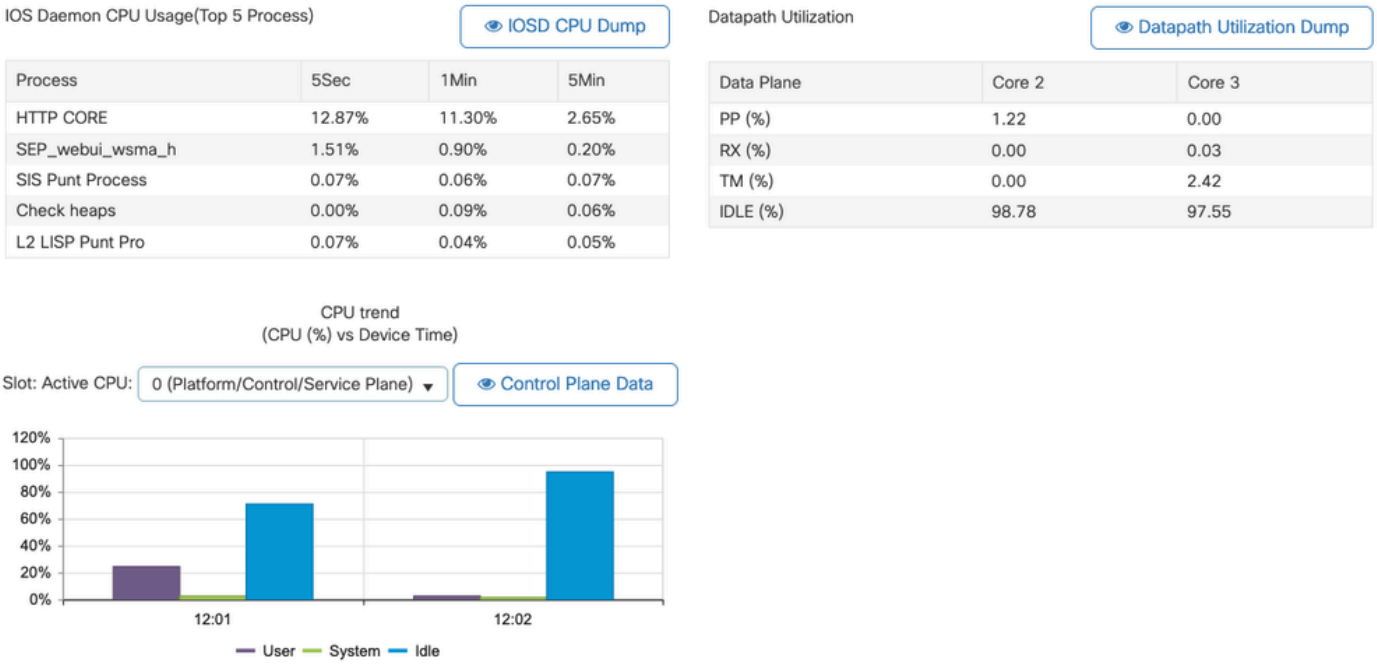
- Vous pouvez surveiller l'utilisation du processeur IOSd en exécutant la commande show processes cpu sorted. Cela correspond à l'activité dans la partie processus linux_iosd-image de la liste Cisco IOS XE.

```
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'onglet Monitoring/System/CPU Utilization.

Qu'est-ce que chaque processus

La liste des processus varie selon le modèle du contrôleur et la version de Cisco IOS XE. Il s'agit d'une liste de certains processus clés et elle n'est pas destinée à couvrir toutes les entrées possibles.

Nom du processus	Que fait-il ?	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 élevés pendant les heures de pointe. Indiquez si l'utilisation est bloquée pendant 95 % ou plus pendant plusieurs minutes.
linux_iosd-image	Processus Cisco IOS	Attendez-vous à une utilisation élevée si vous collectez des résultats CLI importants (show tech). Des opérations SNMP importantes ou trop fréquentes peuvent entraîner une utilisation élevée du processeur.
nginx	Serveur Web	Ce processus peut afficher des pics et ne peut être signalé que sur une charge élevée soutenue.
ucode_pkt_PPE0	Plan de données 9800CL/9800L	Exécutez la commande show platform hardware chassis active qfp datapath use pour surveiller ce composant.
ezman	Gestionnaire de chipsets pour interfaces	Un CPU élevé et soutenu peut indiquer soit un problème matériel, soit un éventuel problème logiciel du noyau (il peut être signalé).
dbm	Gestionnaire de bases de données	Un CPU élevé et soutenu peut 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 peut être signalé ici.

feu	Shell Manager se charge de l'analyse CLI et de l'interaction entre les différents processus.	CPU élevé attendu lors de la gestion d'une sortie CLI importante. Un CPU élevé soutenu en l'absence de charge peut être signalé.
emd	Gestionnaire de shell : gère l'analyse CLI et les interactions entre les différents processus	CPU élevé attendu lors de la gestion d'une sortie CLI importante. Un CPU élevé soutenu sur l'absence de charge peut 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 peut être signalé.

Mécanismes de protection CPU élevée

Les contrôleurs LAN sans fil du Catalyst 9800 disposent de mécanismes de protection étendus autour de l'activité du réseau ou du client sans fil pour empêcher un processeur élevé en raison de scénarios accidentels ou intentionnels. Il existe plusieurs fonctionnalités clés conçues pour 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 :

- Génération d'une inondation ARP
- 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

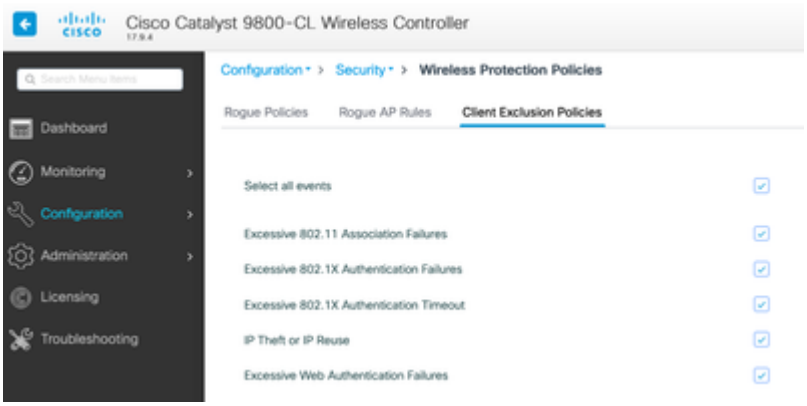
---

L'exclusion des clients protège votre contrôleur, votre point d'accès et votre infrastructure AAA (Radius) contre plusieurs types de haute activité pouvant entraîner une CPU élevée. Il n'est pas conseillé de désactiver les méthodes d'exclusion, sauf si elles sont requises pour un exercice de dépannage ou des exigences de compatibilité.

Les paramètres par défaut fonctionnent pour presque tous les cas et seuls certains scénarios exceptionnels sont nécessaires pour augmenter le temps d'exclusion ou désactiver certains déclencheurs spécifiques. Par exemple, certains clients existants ou spécialisés (IOT/Medical) doivent avoir le déclencheur d'échec d'association désactivé, en raison de défauts côté client qui ne peuvent pas être facilement corrigés

---

Vous pouvez personnaliser les déclencheurs dans l'interface utilisateur : Configuration/Protection sans fil/Stratégies d'exclusion des clients :



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 en exécutant la commande sh wireless profile policy all et rechercher ce résultat spécifique :

```
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 pour garantir que le trafic envoyé au plan de contrôle ne dépasse pas un ensemble de seuils prédéfinis. Cette fonction est appelée Punt Policers et dans presque tous les scénarios, il n'est pas nécessaire de les toucher, et même alors, ne doit être utilisé que lors de l'utilisation de l'assistance Cisco.

L'avantage de cette protection est qu'elle fournit une visibilité détaillée sur le réseau, et si une activité spécifique présente un débit accru ou des paquets élevés inattendus par seconde.

Cela n'est visible que via l'interface de ligne de commande, car elles font normalement partie de fonctionnalités avancées qui nécessitent rarement des modifications.

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 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
  4    PPP Control                    437      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
```

Il peut s'agir d'une longue liste de plus de 160 entrées, selon la version du logiciel. Dans la sortie de la table, vérifiez la colonne de paquets abandonnés ainsi que toute entrée ayant une valeur non nulle sur le nombre d'abandons élevé. Pour simplifier la collecte de données, vous pouvez exécuter la commande show platform software punt-policer drop-only pour filtrer uniquement les entrées du régulateur 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 et LFTS est l'acronyme de 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. Cette fonctionnalité vérifie la charge WNCD et commence à limiter la nouvelle activité du client pour s'assurer que suffisamment de ressources restent disponibles pour gérer les connexions existantes et pour protéger la stabilité CAPWAP. Cette fonctionnalité est activée par défaut et ne dispose pas d'options de configuration.

Trois niveaux de protection sont définis : L1 à 80 % de la charge, L2 à 85 % de la charge et L3 à 89 %. Chacun déclenchant un protocole entrant différent abandonne en tant que mécanismes de protection. La protection est automatiquement supprimée dès que la charge diminue.

Dans un réseau sain, vous ne pouvez pas voir les événements de chargement L2 ou L3 et s'ils se produisent fréquemment, ils peuvent être examinés.

Pour surveiller, exécutez la commande wireless stats cac :

```
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 obtient tous les services offerts par tous les périphériques. Cela peut conduire à de grandes listes de services, avec des centaines d'entrées.
- Les stratégies définies sans filtrage amènent 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 de ce nombre par version du système d'exploitation.

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

```
9800-1#  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 que peut avoir une requête donnée. Il ne désigne pas un problème en lui-même, 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 et, 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 la balise de site, mais d'autres options peuvent fonctionner, selon vos besoins.

J'ai besoin de plus d'assistance

Si vous constatez une charge CPU élevée et qu'aucune des étapes précédentes ne vous aide, contactez Customer Experience (CX) via un dossier et ajoutez ces données comme point de départ :

- Données de base, car elles incluent la configuration du point d'accès/contrôleur, le réseau et les valeurs opérationnelles RF :

```
show tech-support wireless
```

- Archivage de toutes les traces de contrôleur. Il s'agit d'un fichier volumineux similaire à un concept de boîte noire qui peut être collecté en exécutant cette commande :

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

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.