Fehlerbehebung: CPU-Last des Wireless LAN-Controllers

Inhalt

Einleitung

Dieses Dokument beschreibt die Überwachung der CPU-Auslastung auf Catalyst 9800 Wireless LAN Controllern und enthält verschiedene Konfigurationsempfehlungen.

Verständnis der CPU-Nutzung

Bevor Sie sich mit der Fehlerbehebung bei CPU-Auslastung befassen, müssen Sie sich mit den Grundlagen der Verwendung von CPUs in Catalyst 9800 Wireless LAN-Controllern sowie mit einigen Details zur Softwarearchitektur vertraut machen.

Im Allgemeinen definiert das Catalyst 9800 Best Practices-Dokument eine Reihe guter Konfigurationseinstellungen, die Probleme auf Anwendungsebene verhindern können, z. B. durch die Verwendung von Standortfilterung für mDNS oder die Sicherstellung, dass der Client-Ausschluss immer aktiviert ist. Es wird empfohlen, diese Empfehlungen zusammen mit den hier behandelten Themen anzuwenden.

Plattformgrundlagen

Die Catalyst Controller der Serie 9800 wurden als flexible Plattform konzipiert, die auf unterschiedliche Netzwerklasten ausgerichtet ist und sich auf die horizontale Skalierung konzentriert. Die interne Bezeichnung für die Entwicklung lautete "eWLC", wobei "e" für "elastisch" steht, um anzugeben, dass dieselbe Softwarearchitektur von einem kleinen, in eine CPU eingebetteten System zu mehreren großen CPU/Core-Appliances ausgeführt werden kann.

Jeder WLC hat zwei verschiedene "Seiten":

- Kontrollebene: Verarbeitung aller "Management"-Interaktionen wie CLI, UI, Netconf und aller Onboarding-Prozesse für Clients und APs.
- Datenebene: zuständig für die tatsächliche Paketweiterleitung und die Entkapselung von CAPWAP, die Durchsetzung von AVC-Richtlinien und andere Funktionen.

Steuern Sie Fläche

- Die meisten Cisco IOS-XE-Prozesse werden unter BinOS (Linus Kernel) mit eigenen speziellen Scheduler- und Überwachungsbefehlen ausgeführt.
- Es gibt eine Reihe von Schlüsselprozessen, den so genannten Wireless Network Control Daemon (WNCD), die jeweils über eine lokale In-Memory-Datenbank verfügen und den Großteil der Wireless-Aktivitäten verarbeiten. Jede CPU besitzt einen WNCD, um die Last auf alle verfügbaren CPU-Kerne auf die einzelnen Systeme zu verteilen
- Die Lastverteilung auf die WNCDs erfolgt während des AP-Joins. Wenn ein WAP eine CAPWAP-Verbindung mit dem Controller durchführt, verteilt ein interner Load Balancer den WAP unter Verwendung einer Reihe möglicher Regeln, um die ordnungsgemäße Verwendung aller verfügbaren CPU-Ressourcen sicherzustellen.
- Der Cisco IOS®-Code wird auf einem eigenen Prozess namens IOSd ausgeführt und verfügt über einen CPU-Planer sowie Überwachungsbefehle. Dies übernimmt bestimmte Funktionen, z. B. CLI, SNMP, Multicast und Routing.

In einer vereinfachten Ansicht verfügt der Controller über Kommunikationsmechanismen zwischen der Kontroll- und Datenebene, "Punkt", sendet Datenverkehr vom Netzwerk an die Kontrollebene, und "Injektion" überträgt Frames von der Kontrollebene in das Netzwerk.

Im Rahmen einer Untersuchung zur möglichen hohen CPU-Fehlerbehebung müssen Sie den Punt-Mechanismus überwachen, um zu bewerten, welcher Datenverkehr die Kontrollebene erreicht und zu einer hohen Auslastung führen kann.

Daten-Fläche

Für den Catalyst Controller der Serie 9800 wird dies im Rahmen des Cisco Packet Processor (CPP) ausgeführt, einem Software-Framework zur Entwicklung von Paketweiterleitungs-Engines, die für verschiedene Produkte und Technologien verwendet werden.

Die Architektur ermöglicht ein gemeinsames Feature-Set für verschiedene Hardware- oder Software-Implementierungen, z. B. ähnliche Funktionen für 9800CL im Vergleich zu 9800-40 bei unterschiedlichen Durchsatzskala.

AP-Lastenausgleich

Der WLC führt während des CAPWAP-Join-Prozesses einen Lastenausgleich über die CPUs hinweg durch, wobei das Hauptunterscheidungsmerkmal der Tag-Name des AP-Standorts ist. Die Idee dahinter ist, dass jeder Access Point eine spezifische CPU-Last repräsentiert, die aufgrund seiner Client-Aktivität und des Access Points selbst hinzugefügt wird. Es gibt mehrere Mechanismen, um diesen Balancing auszuführen:

- Wenn der Access Point ein "default-tag" verwendet, wird ein Round-Robin-Ausgleich für alle CPUs/WNCDs durchgeführt, wobei jeder neue AP-Join zum nächsten WNCD weitergeleitet wird. Dies ist die einfachste Methode, hat aber kaum Auswirkungen:
    - Dies ist ein suboptimales Szenario, da die Access Points in derselben RF-Roaming-Domäne häufig Inter-WNCD-Roaming ausführen würden, was eine zusätzliche Kommunikation zwischen den Prozessen erfordern würde. Das Roaming zwischen Instanzen ist um einen kleinen Prozentsatz langsamer.
    - Für das FlexConnect-Site-Tag (remote) ist keine PMK-Schlüsselverteilung verfügbar. Dies bedeutet, dass Sie kein schnelles Roaming für den Flex-Modus durchführen können, was sich auf den OKC/FT-Roaming-Modus auswirkt.

      Im Allgemeinen kann das Standard-Tag bei Szenarien mit geringerer Auslastung (z. B. weniger als 40 % der AP- und Client-Auslastung der 9800-Plattform) und bei FlexConnect-Bereitstellungen nur dann verwendet werden, wenn kein schnelles Roaming erforderlich ist.

- Wenn der WAP über ein benutzerdefiniertes Site-Tag verfügt, wird das Site-Tag bei der ersten Verknüpfung eines WAP mit dem Namen des Site-Tags mit dem Controller einer bestimmten WNCD-Instanz zugewiesen. Alle nachfolgenden zusätzlichen AP-Joins mit demselben Tag werden demselben WNCD zugewiesen. Dadurch wird sichergestellt, dass das Roaming zwischen APs unter demselben Site-Tag im selben WCND-Kontext erfolgt, wodurch ein optimaler Datenfluss bei geringerer CPU-Auslastung ermöglicht wird. Roaming zwischen WNCDs wird unterstützt, jedoch nicht so optimal wie Intra-WNCD-Roaming.

- Standardentscheidung für den Lastenausgleich: Wenn einem WNCD ein Tag zugewiesen wird, wählt der Lastenausgleich die Instanz mit der niedrigsten Anzahl von Standorttags zu diesem Zeitpunkt aus. Da die Gesamtlast dieses Site-Tags nicht bekannt ist, kann es zu suboptimalen Ausgleichsszenarien kommen. Dies hängt von der Reihenfolge der AP-Joins ab, von der Anzahl der definierten Site-Tags und davon, ob die Anzahl der APs in diesen Geräten asymmetrisch ist

- Static Load Balancing: Um eine unausgeglichene Zuweisung von Site-Tags zu WNCD zu verhindern, wurde der Befehl site load in Version 17.9.3 und höher eingeführt, damit Administratoren die erwartete Last jedes Site-Tags vordefinieren können. Dies ist besonders bei Campus-Szenarien oder mehreren Zweigstellen nützlich, die jeweils unterschiedlichen AP-Nummern zugeordnet sind, um eine gleichmäßige Verteilung der Last auf die WNCD sicherzustellen.

Wenn beispielsweise ein Router der Serie 9800-40 für eine Hauptniederlassung und fünf Zweigstellen mit unterschiedlichen AP-Nummern konfiguriert ist, könnte die Konfiguration wie folgt aussehen:

```
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
```

In diesem Szenario soll sich das Tag der Hauptniederlassung nicht auf demselben WNCD wie branch-3 und branch-4 befinden, es gibt insgesamt 6 Standort-Tags, und die Plattform verfügt über 5 WNCDs, sodass die Möglichkeit besteht, dass die am höchsten geladenen Standort-Tags auf derselben CPU landen. Mit dem Befehl load können Sie eine vorhersagbare AP-Lastenausgleichstopologie erstellen.

Der Befehl "load" ist ein Hinweis auf die erwartete Größe. Er muss nicht genau der AP-Anzahl entsprechen, wird aber normalerweise auf die erwarteten APs festgelegt, die möglicherweise beitreten.

- In Szenarien, in denen große Gebäude von einem einzigen Controller verwaltet werden, ist es einfacher und einfacher, für diese Plattform einfach so viele Site-Tags wie WNCDs zu erstellen (z. B. C980-40 mit fünf, C9800-80 mit acht). Weisen Sie APs im gleichen Bereich oder in der gleichen Roaming-Domäne den gleichen Standort-Tags zu, um die Kommunikation zwischen WNCDs zu minimieren.
- RF-Lastenausgleich: Auf diese Weise werden APs unter Verwendung der RF-Nachbarbeziehung vom RRM zwischen WNCD-Instanzen ausgeglichen, und es werden Untergruppen erstellt, je nachdem, wie nahe die APs einander sind. Dieser Vorgang muss nach einer gewissen Zeit durchgeführt werden, nachdem die APs betriebsbereit waren. Außerdem müssen keine statischen Lastenausgleichseinstellungen mehr konfiguriert werden. Diese Version ist ab dem 17.12. und höher verfügbar.

Wie kann man herausfinden, wie viele WNCDs vorhanden sind?

Für Hardwareplattformen ist die WNCD-Anzahl fest: 9800-40 hat 5, 9800-80 hat 8. Für 9800CL (virtuell) hängt die Anzahl der WNCDs von der Vorlage des virtuellen Systems ab, die bei der

Erstbereitstellung verwendet wurde.

Wenn Sie herausfinden möchten, wie viele WNCDs im System ausgeführt werden, können Sie diesen Befehl in der Regel für alle Controller-Typen verwenden:

<#root>

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

5

Im Fall von 9800-CL können Sie den Befehl verwenden, **show platform software system all** um Details zur virtuellen Plattform zu sammeln:

<#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

Überwachen der AP-Lastverteilung

Die Zuordnung von AP zu WNCD wird während des AP-CAPWAP-Join-Vorgangs angewendet. Daher ist unabhängig von der Balancing-Methode keine Änderung während des Vorgangs zu erwarten, es sei denn, es gibt ein netzwerkweites CAPWAP-Reset-Ereignis, bei dem alle APs die Verbindung trennen und erneut verbinden.

Der CLI-Befehl show wireless loadbalance tag affinity bietet eine einfache Möglichkeit, den aktuellen Status des AP-Lastenausgleichs für alle WNCD-Instanzen anzuzeigen:

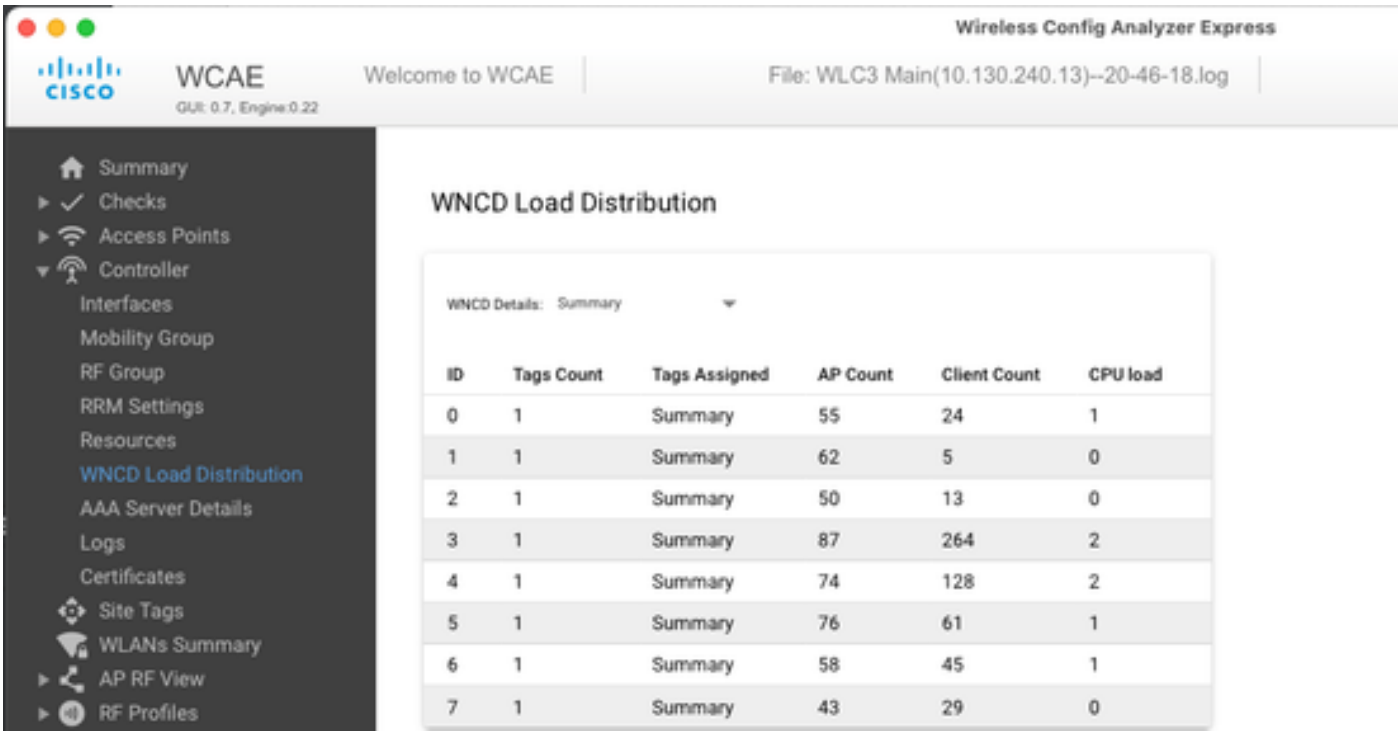
98001#show wireless loadbalance tag affinity

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

Wenn Sie die AP-Verteilung mit der Client-Anzahl und der CPU-Auslastung korrelieren möchten, ist der einfachste Weg, das WCAE-Support-Tool zu verwenden und eine während der Stoßzeiten durchgeführte auszuladenshow tech wireless. Das Tool fasst die Anzahl der WNCD-Clients

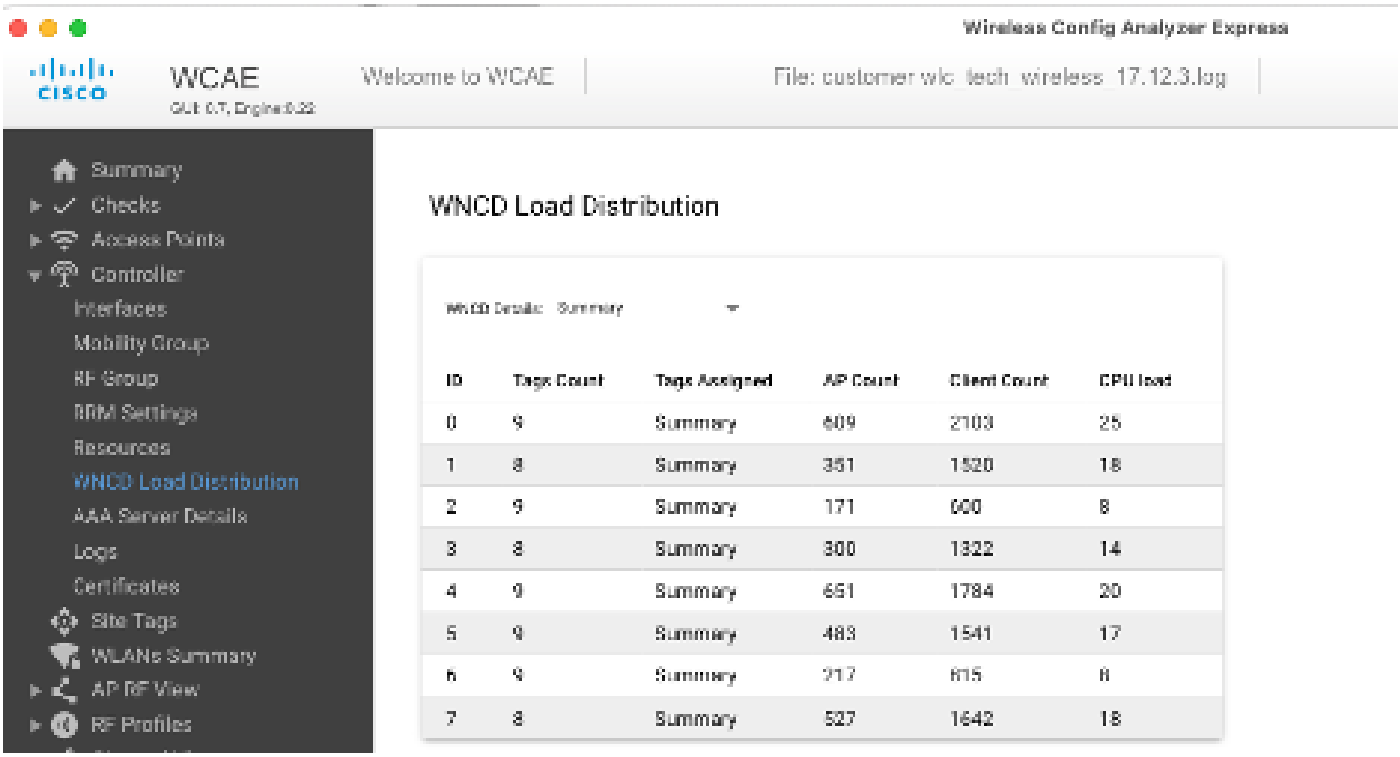
zusammen, die von jedem AP genommen werden, der ihm zugeordnet ist.

Beispiel für einen richtig ausgeglichenen Controller bei geringer Nutzung und geringer Client-Anzahl:



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

Ein weiteres Beispiel für einen stärker ausgelasteten Controller, das die normale CPU-Auslastung zeigt:



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	661	1784	20
5	9	Summary	483	1541	17
6	9	Summary	217	615	8
7	8	Summary	527	1642	18

Welcher Mechanismus für den AP-Lastenausgleich wird empfohlen?

Kurz gesagt, können Sie die verschiedenen Optionen in den folgenden Punkten zusammenfassen:

- Kleines Netzwerk, kein schnelles Roaming erforderlich, weniger als 40 % der Controller-Last: Standard-Tag.

- Wenn schnelles Roaming erforderlich ist (OKC, FT, CCKM), oder eine große Client-Anzahl:

  - Einzelgebäude: Erstellung von so vielen Site-Tags wie CPUs (plattformabhängig)

  - Bis 17.12 oder weniger als 500 APs: mehrere Gebäude, Zweigstellen oder großer Campus: Erstellung eines Site-Tags pro physischem RF-Standort und Konfiguration des Load-Befehls pro Standort.

  - 17.12 und höher mit mehr als 500 APs: RF-Lastenausgleich

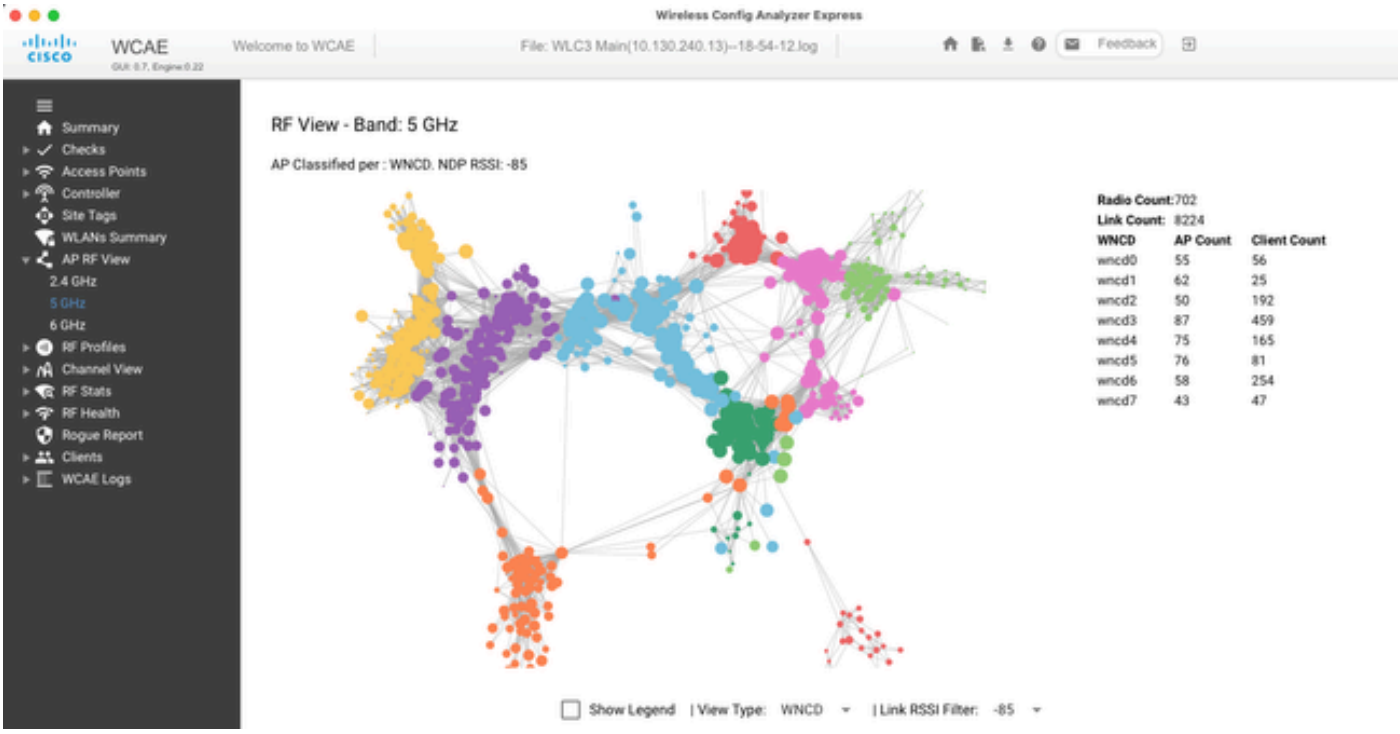
Dieser Schwellenwert von 500 APs ist zu markieren, wenn der Lastverteilungsmechanismus wirksam angewendet werden soll, da APs standardmäßig in Blöcken von 100 Einheiten gruppiert werden.

AP-WNCD-Verteilungsvisualisierung

Es gibt Szenarien, in denen Sie ein erweitertes AP-Balancing durchführen möchten, und es ist wünschenswert, die Verteilung von APs über CPUs präzise zu steuern. Dies sind z. B. Szenarien mit sehr hoher Dichte, bei denen die Hauptauslastungsmetrik die Client-Anzahl ist, anstatt sich nur auf die Anzahl der im System vorhandenen APs zu konzentrieren.

Ein gutes Beispiel für diese Situation sind große Ereignisse: Ein Gebäude könnte Tausende von Clients über mehrere Hundert APs hosten, und Sie müssten die Last auf so viele CPUs wie möglich aufteilen, aber gleichzeitig das Roaming optimieren. Sie können also nur dann über WNCD roamen, wenn dies erforderlich ist. Sie möchten Situationen vermeiden, in denen mehrere APs in verschiedenen WNCDs/Site-Tags am gleichen physischen Standort gemischt sind.

Mit dem WCAE-Tool können Sie die Access Point-RF-Ansicht optimieren und eine visuelle Darstellung der Verteilung bereitstellen:



Dies ermöglicht es uns, die AP/WNCD-Verteilung zu sehen, setzen Sie einfach auf WNCDView Type. Hier würde jede Farbe eine WNCD/CPU repräsentieren. Sie können den RSSI-Filter auch auf -85 einstellen, um Low-Signal-Verbindungen zu vermeiden, die ebenfalls vom RRM-Algorithmus im Controller gefiltert werden.

Im vorherigen Beispiel, das mit Cisco Live EMEA 24 korrespondiert, können Sie sehen, dass die meisten benachbarten APs in einem WNCD-Cluster gut zusammengefasst sind, mit sehr begrenzten Überschneidungen.

Site-Tags, die demselben WNCD zugewiesen sind, erhalten dieselbe Farbe.

Überwachung der CPU-Nutzung der Kontrollebene

Denken Sie an das Konzept der Cisco IOS-XE-Architektur, und beachten Sie, dass es zwei Hauptansichten der CPU-Auslastung gibt. Die eine Option stammt aus dem bisherigen Cisco IOS-Support und die andere aus der Hauptanwendung mit einem umfassenden Überblick über die CPU über alle Prozesse und Kerne hinweg.

Im Allgemeinen können Sie mit dem Befehl detaillierte Informationen zu allen Prozessen in Cisco IOS-XE sammelnshow processes cpu platform sorted:

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

Hier sind einige wichtige Punkte hervorzuheben:

- Der Prozess ucode_pkt_PPE0 verarbeitet die Datenebene auf 9800L- und 9800CL-Plattformen, und es wird erwartet, dass die Auslastung ständig hoch ist, sogar über 100 %. Das ist Teil der Umsetzung, und das stellt kein Problem dar.

- Es ist wichtig, die Spitzenauslastung von einer anhaltenden Auslastung zu unterscheiden und zu isolieren, was in einem bestimmten Szenario erwartet wird. Beispielsweise kann das Erfassen einer sehr großen CLI-Ausgabe, z. B.show tech wireless. eine Spitzenauslastung bei IOSd-, smand- und pubd-Prozessen generieren, da eine sehr große Textausgabe erfasst wird und Hunderte von CLI-Befehlen ausgeführt werden. Dies stellt kein Problem dar, und die Auslastung sinkt, nachdem die Ausgabe abgeschlossen wurde.

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

- Es wird eine Spitzenauslastung für WNCD-Kerne während hoher Client-Aktivitätszeiten erwartet. Man kann Spitzen von 80% sehen, ohne irgendeinen funktionalen Einfluss, und sie stellen normalerweise kein Problem dar.

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

- Eine anhaltend hohe CPU-Auslastung bei einem Prozess von mehr als 90 % über einen Zeitraum von mehr als 15 Minuten muss untersucht werden.

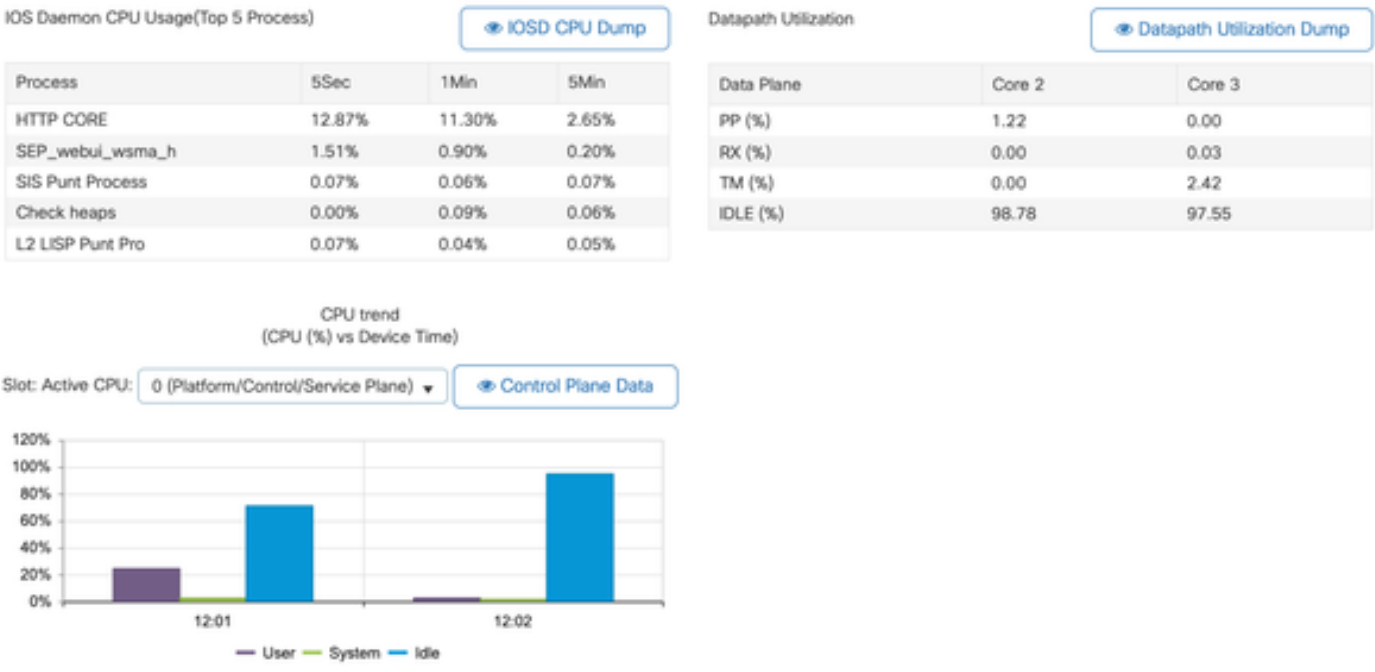
- Sie können die IOSd CPU-Auslastung mit dem Befehl show processes cpu sorted überwachen. Dies entspricht der Aktivität im linux_iosd-imag Prozess Teil der Cisco IOS-XE Liste.

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

- Sie können die Benutzeroberfläche des 9800 verwenden, um eine kurze Übersicht über die IOSd-Last, die Nutzung pro Kern und die Last auf Datenebene zu erhalten:



Dies ist auf der Monitoring/System/CPU Utilization Registerkarte verfügbar.

Was sind die einzelnen Prozesse?

Die genaue Prozessliste hängt vom Controller-Modell und der Cisco IOS-XE-Version ab. Dies ist eine Liste einiger der wichtigsten Prozesse, und es ist nicht beabsichtigt, alle möglichen Einträge abzudecken.

Prozessname	Was macht es?	Evaluierung
wcd_x	Verarbeitung der meisten Wireless-Vorgänge Je nach Modell 9800 können zwischen 1 und 8 Instanzen vorhanden sein.	Zu Spitzenzeiten war die Auslastung hoch. Melden, wenn die Auslastung für mehrere Minuten bei 95 % oder mehr liegt
linux_iosd-image	IOS-Prozess	Hohe Auslastung bei großer CLI-Ausgabe erwartet (Technik anzeigen) Große oder zu häufige SNMP-Vorgänge können zu einer hohen CPU-Auslastung führen.
Nginx	Webserver	Dieser Prozess kann Spitzen aufweisen und sollte nur bei anhaltend hoher Belastung gemeldet werden
ucode_pkt_PPE0	Datenebene in 9800CL/9800L	Verwenden Sie den Befehl, **show platform hardware chassis active qfp datapath utilization** um diese Komponente zu überwachen.
Esman	Chipsatzmanager für Schnittstellen	Eine anhaltend hohe CPU hier könnte entweder auf ein HW-Problem oder ein mögliches Kernel-Software-Problem hinweisen. Es sollte gemeldet werden
dbm	Datenbank-Manager	Eine dauerhaft hohe CPU sollte gemeldet werden.
odm_X	Operations Data Manager verwaltet eine konsolidierte Datenbank prozessübergreifend	Hohe CPU auf ausgelasteten Systemen erwartet

ungewollt	Behandelt Funktionen für nicht autorisierte Zugriffe	Eine dauerhaft hohe CPU sollte gemeldet werden.
klug	Shell-Manager. CLI-Parsing und Interaktion über verschiedene Prozesse hinweg	Hohe CPU bei Verarbeitung großer CLI-Ausgaben erwartet. Eine dauerhaft hohe CPU sollte bei nicht vorhandener Last gemeldet werden.
Mittelwert	Shell-Manager. CLI-Parsing und Interaktion über verschiedene Prozesse hinweg	Hohe CPU bei Verarbeitung großer CLI-Ausgaben erwartet. Eine anhaltend hohe CPU-Auslastung sollte gemeldet werden.
Kneipe	Teil der Telemetriehandlung	Hohe CPU für große Telemetrie-Abonnements erwartet. Eine anhaltend hohe CPU-Auslastung sollte gemeldet werden.

Hohe CPU-Schutzmechanismen

Die Catalyst Wireless LAN Controller 9800 verfügen über umfassende Schutzmechanismen für die Netzwerk- oder Wireless-Client-Aktivität, um eine hohe CPU-Auslastung aufgrund von Zufällen oder Absichten zu vermeiden. Es gibt eine Reihe von wichtigen Funktionen, die Sie bei der Eindämmung problematischer Geräte unterstützen:

Client-Ausschluss

Diese Funktion ist standardmäßig aktiviert und ist Teil der Wireless-Sicherheitsrichtlinien. Sie kann über das Richtlinienprofil aktiviert oder deaktiviert werden. Dadurch können verschiedene Verhaltensprobleme erkannt, der Client aus dem Netzwerk entfernt und in eine "temporäre Ausschlussliste" gesetzt werden. Während sich der Client in diesem ausgeschlossenen Zustand befindet, kommunizieren die Access Points nicht mit ihnen und verhindern somit weitere Aktionen.

Nach Ablauf des Ausschlusszeitgebers (standardmäßig 60 Sekunden) kann der Client erneut eine Verbindung herstellen.

Es gibt mehrere Auslöser für den Ausschluss von Clients:

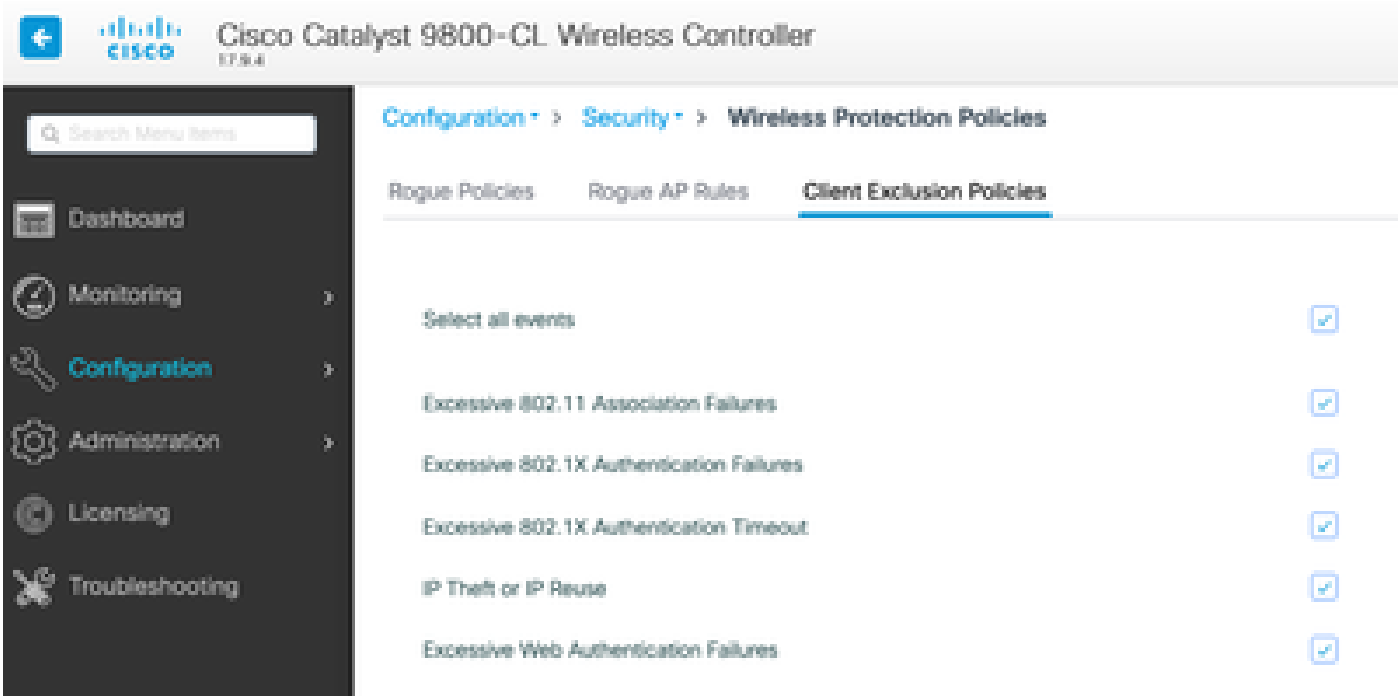
- Wiederholte Zuordnungsfehler
- 3 oder mehr WebAuth-, PSK- oder 802.1x-Authentifizierungsfehler
- Timeouts für wiederholte Authentifizierung (keine Antwort vom Client)
- Es wird versucht, eine bereits bei einem anderen Client registrierte IP-Adresse wiederzuverwenden.

- Generieren einer ARP-Flut

Der Ausschluss des Clients schützt Ihren Controller, Ihren AP und Ihre AAA-Infrastruktur (Radius) vor verschiedenen Typen hoher Aktivität, die zu einer hohen CPU-Auslastung führen können. Im Allgemeinen ist es nicht ratsam, eine der Ausschlussmethoden zu deaktivieren, es sei denn, dies ist für eine Fehlerbehebung oder eine Kompatibilitätsanforderung erforderlich.

Die Standardeinstellungen funktionieren für fast alle Fälle, und nur in einigen Ausnahmefällen ist erforderlich, um die Ausschlusszeit zu erhöhen oder bestimmte Auslöser zu deaktivieren. Bei einigen älteren oder spezialisierten Clients (IOT/Medical) muss möglicherweise der Auslöser für das Zuordnungsausfall deaktiviert werden, da Client-seitige Defekte nicht einfach zu beheben sind.

Sie können die Auslöser in der Benutzeroberfläche anpassen: Konfiguration/Wireless-Schutz/Client-Ausschlussrichtlinien:



Der Auslöser für ARP-Ausschlüsse wurde so konzipiert, dass er auf globaler Ebene dauerhaft aktiviert ist. Er kann jedoch für jedes Richtlinienprofil angepasst werden. Sie können den Status mit dem Befehl sh wireless profile policy all look for this specific output:

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

Schutz der Kontrollebene vor Datenverkehr

Dies ist ein erweiterter Mechanismus in der Datenebene, der sicherstellt, dass der an die Kontrollebene gesendete Datenverkehr einen vordefinierten Satz von Schwellenwerten nicht überschreitet. Die Funktion wird als "Punt Policers" bezeichnet und in fast allen Szenarien ist es nicht erforderlich, sie zu berühren, und selbst dann muss nur in Zusammenarbeit mit dem Cisco Support gearbeitet werden.

Der Vorteil dieses Schutzes besteht darin, dass er einen sehr detaillierten Einblick in die Vorgänge im Netzwerk bietet und Aufschluss darüber

gibt, ob eine bestimmte Aktivität mit einer erhöhten Rate oder unerwartet hohen Paketen pro Sekunde stattfindet.

Dies wird nur über die CLI verfügbar gemacht, da sie normalerweise Teil erweiterter Funktionen sind, die selten geändert werden müssen.

So erhalten Sie einen Überblick über alle Strategien:

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

Dies kann eine große Liste mit mehr als 160 Einträgen sein, je nach Softwareversion.

In der Tabellenausgabe möchten Sie die Spalte für verworfene Pakete zusammen mit allen Einträgen überprüfen, die einen Wert ungleich null für die hohe Verworfenzahl haben.

Um die Datensammlung zu vereinfachen, können Sie mit dem Befehl show platform software punt-policer drop-only nach Richtlinieneinträgen mit Verwerfungen filtern.

Diese Funktion kann nützlich sein, um ARP-Stürme oder 802.11-Überflutungen zu identifizieren (dabei wird die Warteschlange "802.11 Packets to LFTS" verwendet). LFTS steht für Linux Forwarding Transport Service).

Wireless-Anrufzugangskontrolle

In allen aktuellen Wartungsversionen verfügt der Controller über einen Aktivitätsmonitor, um dynamisch auf hohe CPUs zu reagieren und sicherzustellen, dass AP-CAPWAP-Tunnel trotz nicht aufrecht zu erhaltenden Drucks aktiv bleiben.

Die Funktion überprüft die WNCD-Last und drosselt neue Client-Aktivitäten, um sicherzustellen, dass genügend Ressourcen verbleiben, um die vorhandenen Verbindungen zu verarbeiten und die CAPWAP-Stabilität zu schützen.

Diese Option ist standardmäßig aktiviert und bietet keine Konfigurationsoptionen.

Es sind drei Schutzstufen definiert: L1 bei 80 % Last, L2 bei 85 % Last und L3 bei 89 %, von denen jede unterschiedliche eingehende Protokollverluste als Schutzmechanismen auslöst. Der Schutz wird automatisch entfernt, sobald die Last abnimmt.

In einem intakten Netzwerk sollten L2- oder L3-Lastereignisse nicht auftreten, und wenn sie häufig auftreten, sollten sie untersucht werden.

Verwenden Sie zum Überwachen den Befehl wireless stats cac, wie im Bild dargestellt.

```
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
```

mDNS-Schutz

mDNS als Protokoll ermöglicht einen "Zero-Touch"-Ansatz zur Erkennung von Diensten auf verschiedenen Geräten. Gleichzeitig kann es jedoch sehr aktiv sein und die Auslastung deutlich erhöhen, wenn es nicht richtig konfiguriert ist.

mDNS kann die WNCD-CPU-Auslastung ohne jegliche Filterung aus verschiedenen Gründen erhöhen:

- mDNS-Richtlinien mit uneingeschränktem Lernen: Der Controller erhält alle Dienste, die von allen Geräten angeboten werden. Dies kann zu sehr großen Servicelisten mit Hunderten von Einträgen führen.
- Richtlinien ohne Filterung festgelegt: Dadurch sendet der Controller diese großen Servicelisten an jeden Client, der fragt, wer einen bestimmten Service bereitstellt.
- Einige mDNS-spezifische Dienste werden von "allen" Wireless-Clients bereitgestellt, was zu einer höheren Anzahl von Diensten und einer höheren Aktivität führt, wobei es je nach Betriebssystemversion Unterschiede gibt.

Mit dem folgenden Befehl können Sie die Größe der mDNS-Liste pro Dienst überprüfen:

```
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
```

Dies kann eine Vorstellung davon geben, wie groß eine bestimmte Abfrage sein kann, es stellt kein Problem an sich dar, sondern nur eine Möglichkeit, zu überwachen, was verfolgt wird.

Es gibt einige wichtige Empfehlungen für die mDNS-Konfiguration:

- Legen Sie für den mDNS-Transport ein einzelnes Protokoll fest:

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

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

Standardmäßig wird IPv4-Transport verwendet. Aus Leistungsgründen ist es ratsam, IPv6 oder IPv4 zu verwenden, jedoch nicht beides:

- Legen Sie in der mDNS-Dienstrichtlinie immer einen Standortfilter fest, um ungebundene Abfragen/Antworten zu vermeiden. Im Allgemeinen wird empfohlen, "site-tag" zu verwenden, aber andere Optionen können je nach Ihren Anforderungen funktionieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.