Probleemoplossing voor draadloze LAN-controller en CPU-belasting

Inhoud

Inleiding

Dit document beschrijft hoe u het CPU-gebruik op Catalyst 9800 draadloze LAN-controllers kunt controleren en bevat bovendien verschillende configuratieaanbevelingen.

CPU-gebruik begrijpen

Voordat u zich gaat bezighouden met het oplossen van problemen met CPU-belasting, moet u de basisprincipes begrijpen van hoe CPU's worden gebruikt in Catalyst 9800 draadloze LAN-controllers en bepaalde details van de softwarearchitectuur.

In het algemeen definieert Catalyst 9800 Best Practices een verzameling goede configuratie-instellingen die problemen op toepassingsniveau kunnen voorkomen, bijvoorbeeld door locatiefiltering voor mDNS te gebruiken of door ervoor te zorgen dat uitsluiting van clients altijd is ingeschakeld. We raden u aan deze aanbevelingen toe te passen, samen met de onderwerpen die hier worden belicht.

Platformbasisfuncties

Catalyst 9800 controllers zijn ontworpen als een flexibel platform, gericht op verschillende netwerkbelasting en gericht op horizontale schaling. De naam van de interne ontwikkeling was "eWLC" met de e voor "elastisch", om aan te geven dat dezelfde software architectuur in staat zou zijn om van een klein geïntegreerd CPU-systeem naar meerdere grootschalige CPU/core toestellen te draaien.

Elke WLC heeft twee verschillende "kanten":

- Besturingsplane: verwerking van alle "beheer" interacties zoals CLI, UI, Netconf en alle onboarding processen voor clients en AP's.
- Datasvlak: verantwoordelijk voor het daadwerkelijke pakketdoorsturen, en decapsulation van CAPWAP, AVC-beleidshandhaving, onder andere functionaliteiten.

Besturingsplane

- De meeste processen van Cisco IOS-XE worden uitgevoerd onder BinOS (Linus Kernel), met zijn eigen gespecialiseerde planner- en controleopdrachten.
- Er is een reeks belangrijke processen, genoemd Wireless Network Control Daemon (WNCD) elk met een lokale in-memory database, die de meeste draadloze activiteit verwerken. Elke CPU heeft een WNCD, die de werklast over alle beschikbare CPU-cores naar elk systeem kan verdelen
- De taakverdeling over WNCD's wordt uitgevoerd tijdens AP-verbinding. Wanneer een AP een CAPWAP-verbinding uitvoert met de controller, verdeelt een interne taakverdeling het toegangspunt met behulp van een aantal mogelijke regels, om er zeker van te zijn dat alle beschikbare CPU-bronnen correct worden gebruikt.
- Cisco IOS®-code werkt op een eigen proces, IOSd genaamd, en heeft zijn CPU-planner en bewakingsopdrachten. Dit zorgt voor specifieke functionaliteit, bijvoorbeeld CLI, SNMP, multicast en routing.

In een vereenvoudigde weergave, de controller heeft communicatiemechanismen tussen het controle- en dataplaat, "punt", verstuurt verkeer van het netwerk naar het besturingsplane, en "injectie", duwt frames van het besturingsplane naar het netwerk.

Als deel van een mogelijk hoog CPU probleemoplossing onderzoek, moet u het punt mechanisme te controleren, om te evalueren welk verkeer het besturingsplane bereikt en kan leiden tot een hoge belasting.

Dataplane

Voor de Catalyst 9800 controller wordt dit uitgevoerd als onderdeel van Cisco Packet Processor (CPP), een softwareframework om packet-forward-machines te ontwikkelen die worden gebruikt op meerdere producten en technologieën.

De architectuur maakt een gemeenschappelijke functieset mogelijk, voor verschillende hardware- of software-implementaties, waardoor vergelijkbare functies mogelijk zijn voor 9800CL vs 9800-40, op verschillende doorvoerschalen.

AP-taakverdeling

De WLC voert taakverdeling over CPU's uit tijdens het CAPWAP-samenvoegproces, waarbij de belangrijkste differentiator de naam van de site-tag van het AP is. Het idee is dat elke AP een specifieke toegevoegde cpu lading vertegenwoordigt, die uit zijn cliëntactiviteit, en AP zelf komt. Er zijn verschillende mechanismen om deze afweging te maken:

- Als de AP "standaard-tag" gebruikt, zou het worden gebalanceerd op een ronde-robin manier over alle CPU's/WNCD's, waarbij elke nieuwe AP toetreedt naar de volgende WNCD. Dit is de eenvoudigste methode, maar heeft weinig implicaties:
    - Dit is het suboptimale scenario, aangezien APs in hetzelfde RF-roamingdomein frequente Inter-WNCD-roaming zouden doen, waarbij extra procescommunicatie nodig is. Zwerven over instanties is langzamer met een klein percentage.
    - Voor de FlexConnect-site tag (op afstand) is geen PMK-sleuteldistributie beschikbaar. Dit betekent dat u niet snel kunt roamen voor Flex-modus, waardoor OKC/FT-roamingmodi worden beïnvloed.

      Over het algemeen kan de standaardtag worden gebruikt op scenario's met een lagere lading (bijvoorbeeld minder dan 40% van de AP en de clientbelasting van het 9800-platform), en voor FlexConnect-implementatie alleen wanneer snel zwerven geen vereiste is.

- Als het toegangspunt over een eigen sitetag beschikt, wordt de sitetag bij een specifieke WNCD-instantie toegewezen wanneer het toegangspunt met de sitenaam bij de controller wordt aangesloten. Alle daaropvolgende aanvullende AP-verbindingen met dezelfde tag worden toegewezen aan dezelfde WNCD. Dit garandeert zwerven over AP's in dezelfde site-tag, gebeurt in de één WCND-context, die een meer optimale flow biedt, met minder CPU-gebruik. Roaming over WNCD's wordt ondersteund, net niet zo optimaal als intra-WNCD roaming.

- Standaard load balancing beslissing: Wanneer een tag is toegewezen aan een WNCD, selecteert de load balancer de instantie met de laagste site tag telling op dat moment. Omdat de totale belasting die dat sitetag kan hebben niet bekend is, kan dit leiden tot suboptimale balanceringsscenario's. Dit is afhankelijk van de volgorde van AP-joins, hoeveel site-tags zijn gedefinieerd en of de AP-telling asymmetrisch is over hen

- Statische taakverdeling: om ongebalanceerde toewijzing van sitetaken aan WNCD te voorkomen, werd de opdracht voor het laden van de site geïntroduceerd in 17.9.3 en hoger, zodat beheerders vooraf de verwachte lading van elke sitetag kunnen definiëren. Dit is vooral handig bij het verwerken van campusscenario's, of meerdere vestigingen, elk toegewezen aan verschillende AP tellingen, om ervoor te zorgen dat de lading gelijkmatig is verdeeld over WNCD.

Bijvoorbeeld, als u een 9800-40 hebt, behandelend één hoofdbureau, plus 5 bijkantoren, met verschillende AP tellingen, zou de configuratie als dit kunnen kijken:

```
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 dit scenario, wilt u niet de belangrijkste bureaumarkering om op zelfde WNCD te zijn zoals tak-3 en tak-4, zijn er in totaal 6 plaatsmarkeringen, en het platform heeft 5 WNCDs, zodat kan er een kans zijn dat de hoogste geladen plaatsafspraken op zelfde cpu landen. Door de ladingsopdracht te gebruiken, kunt u een voorspelbare AP-werklastverdeling topologie maken.

De laadopdracht is een verwachte groottehint, het hoeft niet exact overeen te komen met het aantal AP's, maar het is normaal gesproken ingesteld op de verwachte AP's die zouden kunnen toetreden.

- In scenario's waar grote gebouwen behandeld worden door één controller, is het gemakkelijker en eenvoudiger om net zoveel site-tag te maken als WNCD's voor dat specifieke platform (bijvoorbeeld C9800-40 heeft er vijf, C9800-80 heeft er 8). Wijs AP's in hetzelfde gebied of zwervend domein toe aan dezelfde site tags om inter-WNCD communicatie te minimaliseren.
- RF-taakverdeling: hiermee worden AP's over WNCD-instanties verdeeld, waarbij de RF-buurrelatie van RRM wordt gebruikt, en worden subgroepen gemaakt afhankelijk van hoe dicht de AP's bij elkaar staan. Dit moet gebeuren nadat een toegangspunt een tijdje actief is geweest en het niet meer nodig is om statische instellingen voor de taakverdeling te configureren. Dit is beschikbaar vanaf 17.12 en hoger.

Hoe te weten te komen hoeveel WNCD's aanwezig zijn?

Voor hardwareplatforms is de WNCD-telling vast: 9800-40 heeft 5, 9800-80 heeft 8. Voor 9800CL (virtueel), het aantal WNCD's zou afhangen van de virtuele machine template die gebruikt werd tijdens de eerste implementatie.

Als een algemene regel, als u wilt weten hoeveel WNCDs in het systeem lopen, kunt u deze opdracht over alle controllertypes gebruiken:

<#root>

```
9800-40#show processes cpu platform sorted  |  count wncd
```

```
Number of lines which match regexp =
5
```

In het geval van de 9800-CL specifiek, kunt u de opdracht gebruiken **show platform software system all** om gegevens te verzamelen op het virtuele platform:

<#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

Taakverdeling van AP-bewaking

De AP-to-WNCD-toewijzing wordt toegepast tijdens het AP-CAPWAP-samenvoegproces. Er wordt dus niet verwacht dat deze tijdens bewerkingen verandert, ongeacht de balanceringsmethode, tenzij er een netwerkbrede CAPWAP-reset-gebeurtenis is waarbij alle AP's zich weer aansluiten en opnieuw aansluiten.

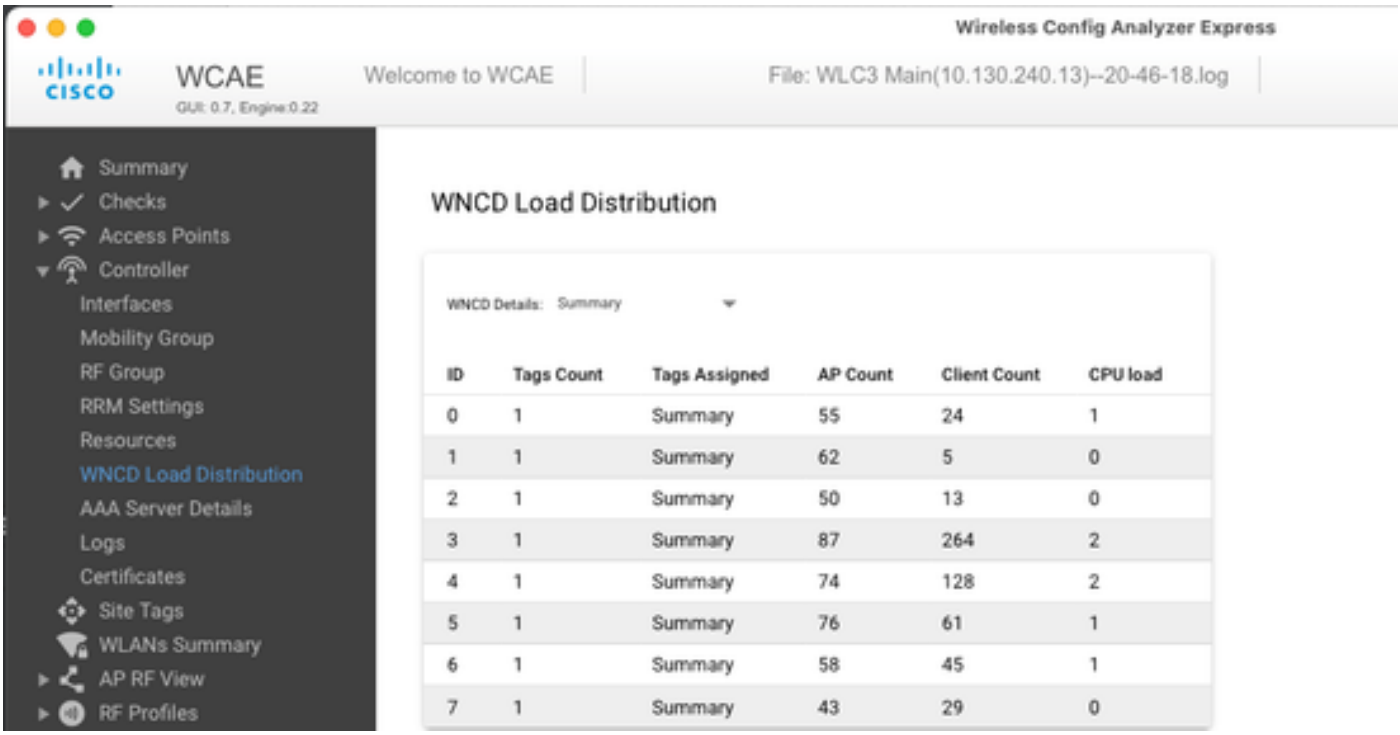
De CLI-opdracht show wireless loadbalance tag affinity kan een eenvoudige manier bieden om de huidige status van de taakverdeling van het toegangspunt in alle WNCD-instanties te zien:

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

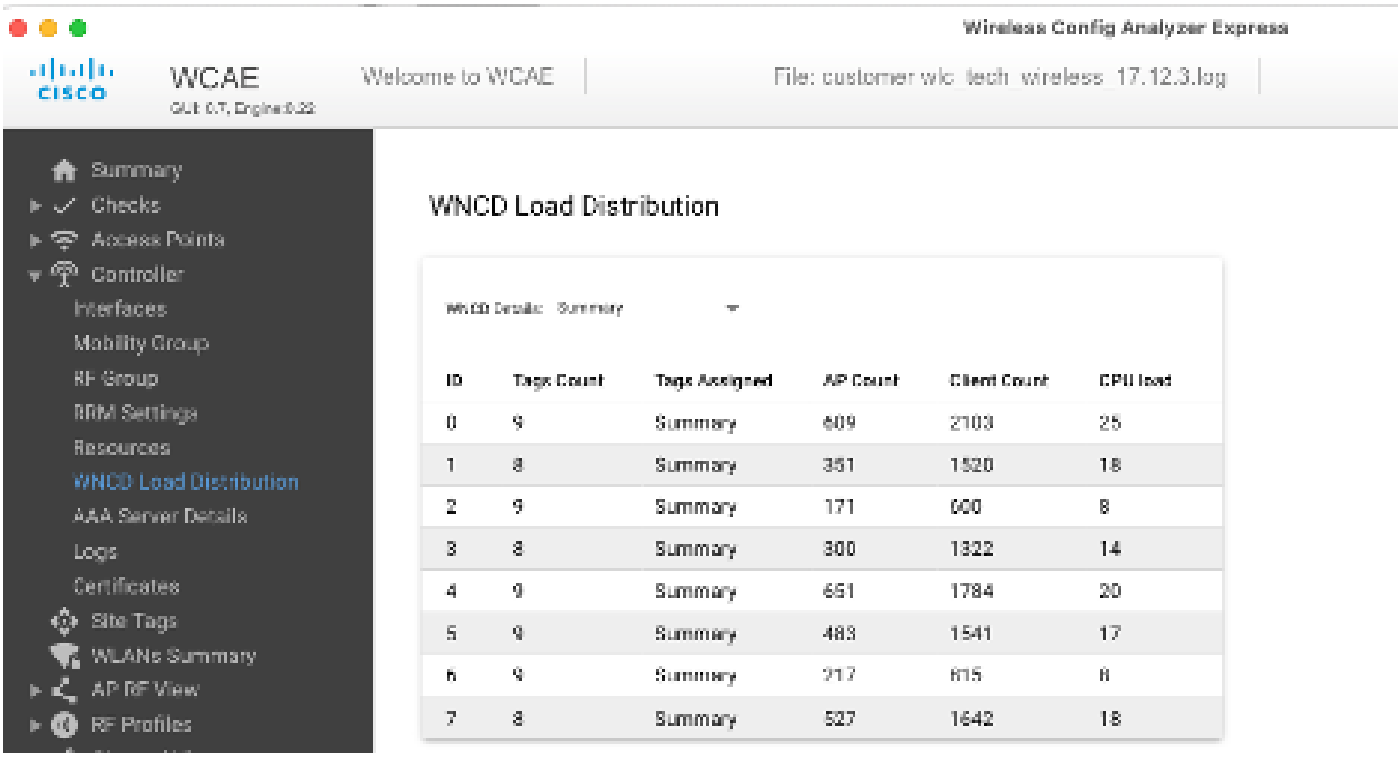
als u de AP-distributie wilt correleren, tegen het aantal clients en de CPU-belasting, is de eenvoudigste manier om het WCAE-ondersteuningsgereedschap te gebruiken en een show tech wireless te laden tijdens drukke tijden. De tool geeft een overzicht van het aantal WNCD-clients, genomen van elke AP die aan de tool is gekoppeld.

Voorbeeld van een goed uitgebalanceerde controller, bij weinig gebruik en een laag aantal klanten:



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

Een ander voorbeeld, voor een meer geladen controller, die normaal CPU-gebruik laat zien:



ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load
0	9	Summary	609	2103	25
1	8	Summary	351	1520	18
2	9	Summary	171	600	8
3	8	Summary	300	1322	14
4	9	Summary	651	1784	20
5	9	Summary	483	1541	17
6	9	Summary	217	615	8
7	8	Summary	527	1642	18

Wat is het aanbevolen taakverdelingsmechanisme van het AP?

Kort samengevat kunt u de verschillende opties samenvatten in:

- Klein netwerk, geen behoefte aan snel zwerven, minder dan 40% van de controllerlading: Default tag.
- Als snel roamen nodig is (OKC, FT, CCKM), of een groot aantal klanten:

- Eén gebouw: maak evenveel site-tags als CPU’s (afhankelijk van het platform)
- Vóór 17.12, of minder dan 500 AP tellen: Meerdere gebouwen, takken of grote campus: Maak een site-tag per fysieke RF-locatie, en vorm load commando per site.
- 17.12 en hoger met meer dan 500 AP’s: gebruik RF-taakverdeling.

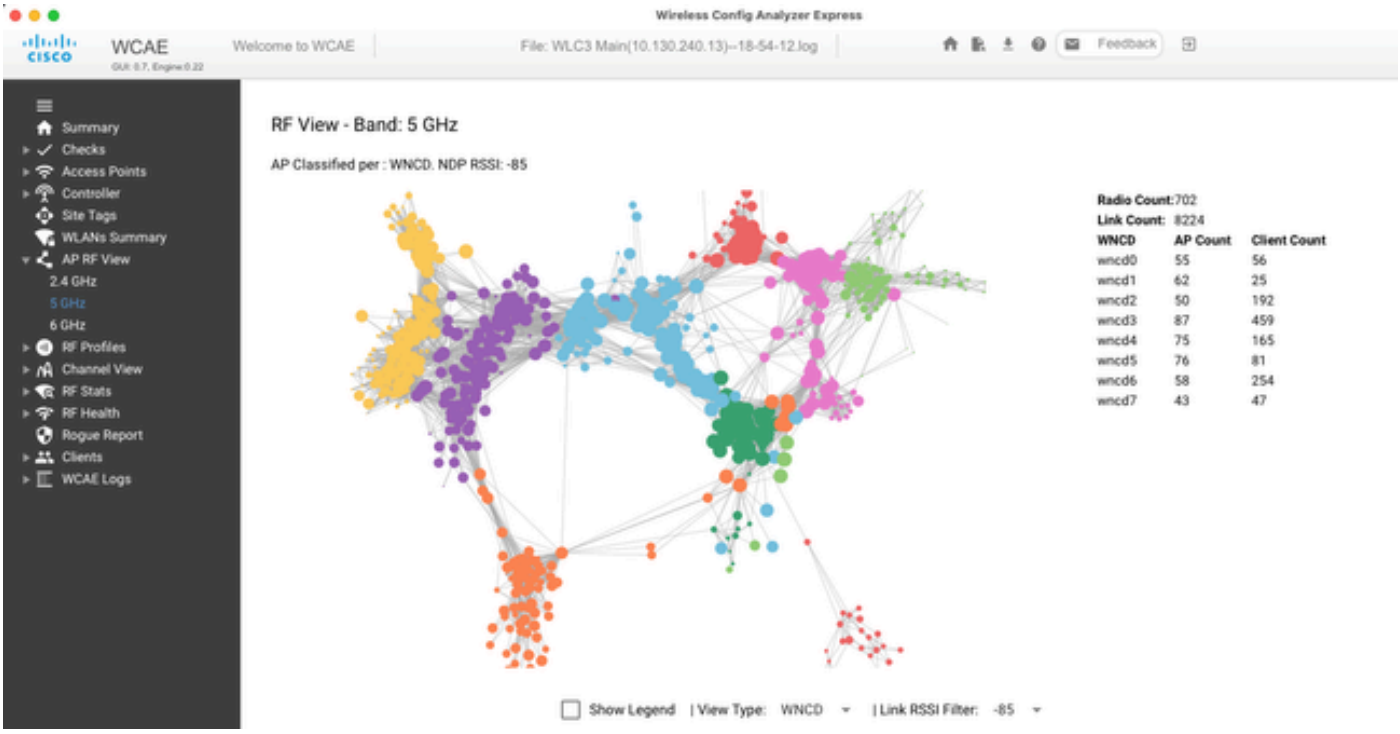
Deze drempel van 500 AP, is te merken wanneer het efficiënt is om het mechanisme van de lastverdeling toe te passen, aangezien het APs in blokken van 100 eenheden door gebrek groepeert.

Visualisatie van AP WNCD-distributie

Er zijn scenario's waar u een geavanceerdere AP balancering wilt doen, en het is wenselijk om granulaire controle te hebben over hoe APs over CPUs worden uitgespreid, bijvoorbeeld, zeer high-density scenario's waar de belangrijkste belasting metrisch is cliënttelling tegenover enkel het concentreren van het aantal APs aanwezig in het systeem.

Een goed voorbeeld van deze situatie zijn grote gebeurtenissen: een gebouw kan duizenden klanten, meer dan enkele honderden AP's, ontvangen en je zou de belasting over zoveel mogelijk CPU's moeten verdelen, maar tegelijkertijd roaming optimaliseren. Dus, u zwerft niet over WNCD tenzij het nodig is. U wilt "zout & peper" situaties voorkomen waarbij meerdere AP's in verschillende WNCD's / site tags worden vermengd in dezelfde fysieke locatie.

Om te helpen verfijnen en een visualisatie van de distributie te bieden, kunt u het WCAE-gereedschap gebruiken en profiteren van de functie RF-weergave:



Dit staat ons toe om AP/WNCD distributie te zien, enkel geplaatst View Type aan WNCD. Hier zou elke kleur een WNCD/CPU vertegenwoordigen. U kunt het RSSI-filter ook instellen op -85 om laagsignaalverbindingen te voorkomen die ook worden gefilterd door het RRM-algoritme in de controller.

In het vorige voorbeeld, dat aan CiscoLive EMEA 24 beantwoordt, kunt u zien dat de meeste aangrenzende APs mooi over in zelfde WNCD, met zeer beperkte dwars-overlappende worden gegroepeerd.

Site-tags toegewezen aan dezelfde WNCD, krijgen dezelfde kleur.

Bewakingsplane voor CPU-gebruik

Het is belangrijk om het concept van Cisco IOS-XE architectuur te onthouden en houd er rekening mee dat er twee belangrijke "weergaven" van het CPU-gebruik zijn. Een daarvan is afkomstig van historische Cisco IOS-ondersteuning en de belangrijkste, met een holistische weergave van de CPU in alle processen en kernen.

In het algemeen kunt u de opdracht gebruiken show processes cpu platform sorted om gedetailleerde informatie te verzamelen voor alle processen in 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

Er zijn hier verschillende belangrijke punten die naar voren moeten worden gebracht:

- Het proces ucode_pkt_PPE0 verwerkt het dataplatform op 9800L en 9800CL platforms, en het wordt verwacht om een hoge benutting te zien de hele tijd, zelfs hoger dan 100%. Dit is onderdeel van de tenuitvoerlegging, en dat is geen probleem.

- Het is belangrijk om piekgebruik versus een aanhoudende lading te onderscheiden en te isoleren wat in een bepaald scenario wordt verwacht. Bijvoorbeeld, het verzamelen van een zeer grote CLI output, zoals show tech wireless kan een pieklading op IOSd, klein, openbare processen, als een zeer grote tekstoutput wordt verzameld, met honderden CLI uitgevoerde bevelen, is dit geen probleem, en de lading daalt nadat de output is voltooid.

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

- Piekgebruik voor WNCD-kernen wordt verwacht, tijdens tijden van hoge clientactiviteit. Het is mogelijk om pieken van 80% te zien, zonder enige functionele impact, en ze vormen normaliter geen probleem.

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

- Een langdurig hoog CPU-gebruik op een proces, hoger dan 90%, gedurende meer dan 15 minuten, moet worden onderzocht.

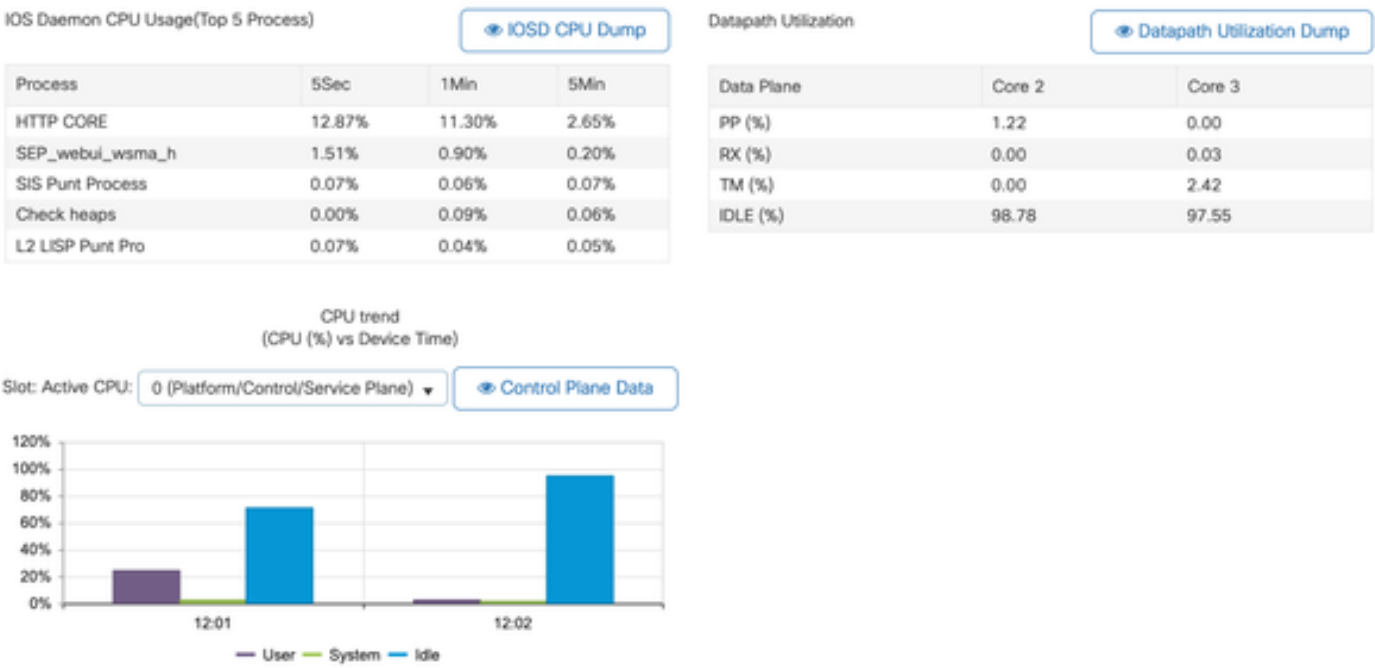
- U kunt IOSd CPU-gebruik controleren met de opdracht show processes cpu sorted . Dit komt overeen met de activiteit in het procesgedeelte linux_iosd-imag van de Cisco IOS-XE lijst.

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

- U kunt de 9800 GUI gebruiken voor een snelle weergave van de IOSd-lading, per kerngebruik en de lading van het dataplatform:



Dit is beschikbaar op het Monitoring/System/CPU Utilization tabblad.

Wat is elk proces?

De exacte proceslijst is afhankelijk van het controllermodel en de Cisco IOS-XE versie. Dit is een lijst van enkele van de belangrijkste

processen, en het is niet bedoeld om alle mogelijke ingangen te bestrijken.

Procesnaam	Wat doet het?	Evaluatie
wd_x	Verwerkt de meeste draadloze bewerkingen. Afhankelijk van het 9800 model, kunt u tussen 1 tot 8 instanties hebben	Je kon pieken van hoge benutting zien tijdens de drukke uren. Rapporteer als het gebruik 95% of meer gedurende enkele minuten is vastgezet
linux_josd-imag	IOS-proces	Verwacht om hoog gebruik te zien als het verzamelen van grote CLI output (toon technologie) Grote of te frequente SNMP-bewerkingen kunnen leiden tot een hoge CPU
nevel	Webserver	Dit proces kan pieken vertonen en dient alleen bij een aanhoudende hoge belasting te worden gerapporteerd
ucode_pkt_PPE0	Gegevensvlak in 9800CL/9800L	Gebruik de opdracht **show platform hardware chassis active qfp datapath utilization** om deze component te bewaken
ezman	Chipset Manager voor interfaces	Een aanhoudende hoge CPU hier kan wijzen op een HW-probleem of een mogelijk kernelsoftwareprobleem. Dit dient te worden gerapporteerd
DBM	Databasemanagement	Hier moet een aanhoudende hoge CPU worden gerapporteerd
odm_X	Operations Data Manager verwerkt geconsolideerde DB over processen	Hoge CPU verwacht op geladen systemen

gemeen	Verwerkt schurkenfunctionaliteit	Hier moet een aanhoudende hoge CPU worden gerapporteerd
klein	Shell Manager. verzorgt CLI-parsing en interactie tussen verschillende processen	Hoge CPU die wordt verwacht bij het verwerken van grote CLI-uitvoer. Er moet melding worden gemaakt van een aanhoudend hoge CPU bij afwezigheid van belasting
emd	Shell Manager. verzorgt CLI-parsing en interactie tussen verschillende processen	Hoge CPU die wordt verwacht bij het verwerken van grote CLI-uitvoer. Aanhoudende hoge CPU bij afwezigheid van belasting moet worden gerapporteerd
schaambeen	Deel van telemetriebehandeling	Hoge CPU die voor grote telemetrieabonnementen wordt verwacht. Aanhoudende hoge CPU bij afwezigheid van belasting moet worden gerapporteerd

Mechanismen voor hoge CPU-bescherming

Catalyst 9800 draadloze LAN-controllers hebben uitgebreide beveiligingsmechanismen rond de activiteit van een netwerk of draadloze client, om een hoge CPU te voorkomen als gevolg van accidentele of opzettelijke scenario's. Er zijn verschillende belangrijke functies ontworpen om u te helpen probleemapparaten te bevatten:

Uitsluiting client

Dit is standaard ingeschakeld en maakt deel uit van Wireless Protection Policies. Het kan worden ingeschakeld of uitgeschakeld per beleidsprofiel. Dit kan verschillende gedragsproblemen detecteren, de client uit het netwerk verwijderen en in een "tijdelijke uitsluitingslijst" plaatsen. Terwijl de klant zich in deze uitgesloten staat bevindt, praten de AP's niet met hen, waardoor verdere acties worden verhinderd.

Nadat de uitsluitingstimer is doorgegeven (standaard 60 seconden), mag de client opnieuw associëren.

Er zijn verschillende triggers voor client uitsluiting:

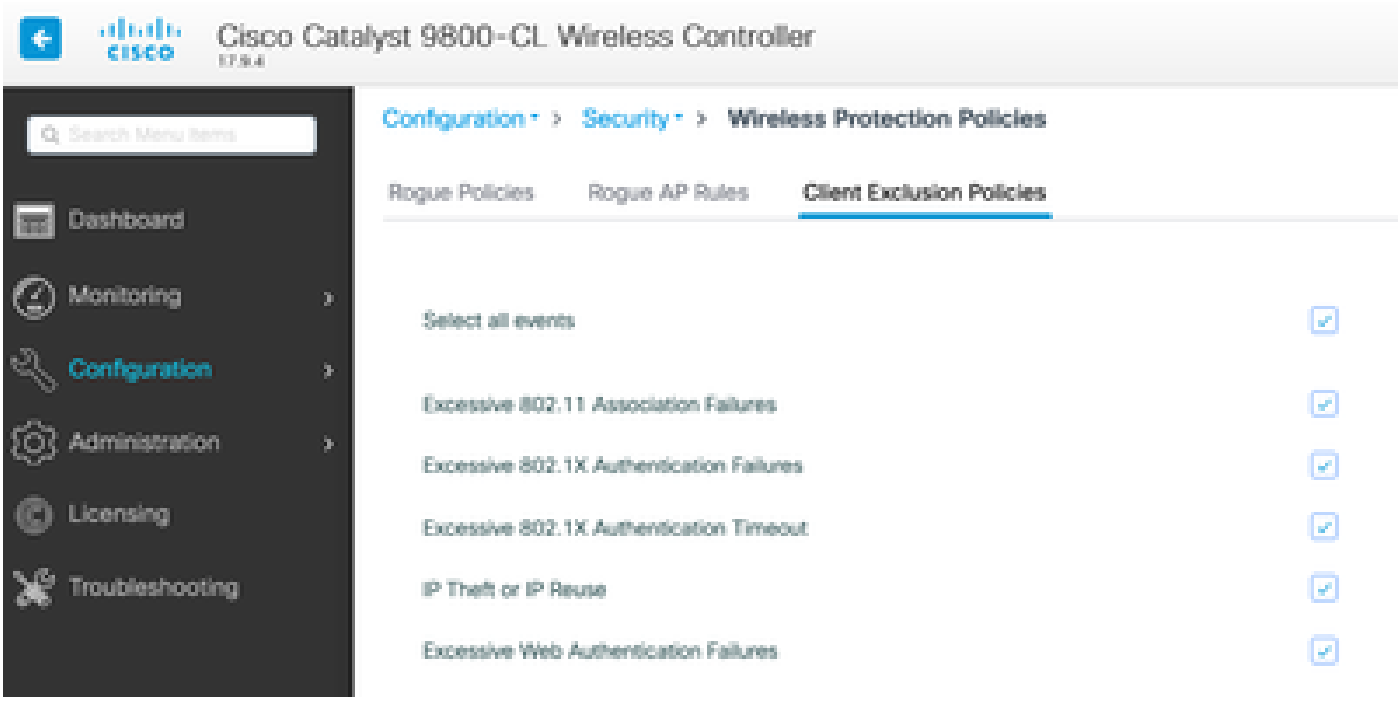
- Herhaalde associatiefouten
- 3 of meer webauth-, PSK- of 802.1x-verificatiefouten
- Herhaalde verificatietime-outs (geen respons van client)

- Probeer een IP-adres te hergebruiken dat al bij een andere client is geregistreerd
- Een ARP-overstroming genereren

De uitsluiting van de client beschermt uw controller, AP en AAA infrastructuur (Radius) tegen verschillende soorten hoge activiteit die kunnen leiden tot een hoge CPU. Over het algemeen is het niet raadzaam om een van de uitsluitingsmethoden uit te schakelen, tenzij dit nodig is voor een probleemoplossing of compatibiliteitseis.

De standaardinstellingen werken voor bijna alle gevallen, en alleen voor enkele uitzonderlijke scenario's, is nodig om de uitsluitingstijd te verhogen, of een specifieke trigger uit te schakelen. Bijvoorbeeld, sommige erfenis of gespecialiseerde cliënten (IOT/Medisch), kunnen de trekkende van de verenigingsmislukking hebben om worden onbruikbaar gemaakt, wegens cliënt-zijdefects die niet gemakkelijk kunnen worden hersteld

U kunt de triggers aanpassen in de UI: Configuration/Wireless Protection/Client Exclusion Policies:



ARP Exclusion trigger is ontworpen om permanent ingeschakeld te worden op mondiaal niveau, maar kan worden aangepast op elk beleidsprofiel. U kunt de status controleren met de opdracht sh wireless profile policy all naar deze specifieke uitvoer zoeken:

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

Beveiliging van besturingsplane tegen gegevensverkeer

Dit is een geavanceerd mechanisme in het Dataplane, om ervoor te zorgen dat het verkeer dat naar Control Plane wordt verzonden een vooraf bepaalde reeks drempels niet overschrijdt. Deze functie wordt "Punt Policers" genoemd en in bijna alle scenario's is het niet nodig om ze aan te raken, en zelfs dan moet alleen worden gedaan tijdens het werken met Cisco Support.

Het voordeel van deze bescherming is dat het een zeer gedetailleerd inzicht biedt in wat er in het netwerk gebeurt, en als er een specifieke activiteit is die een verhoogd tarief heeft, of onverwacht hoge pakketten per seconde.

Dit wordt alleen via CLI getoond, omdat deze normaal deel uitmaken van geavanceerde functionaliteit die zelden hoeft te worden aangepast.

Om een overzicht te krijgen van alle beleid van het 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

Afhankelijk van de softwareversie kan dit een grote lijst zijn met meer dan 160 lemma's.

Op de tabeluitvoer wilt u de gedropte pakketkolom controleren samen met elke ingang die een niet-nulwaarde heeft op de hoge drop-telling.

Om de gegevensverzameling te vereenvoudigen, kunt u de opdracht gebruiken show platform software punt-policer drop-only, om alleen te filteren op policer-vermeldingen met druppels.

Deze functie kan handig zijn om te identificeren als er ARP stormen of 802.11 sonde overstromingen zijn (ze gebruiken wachtrij "802.11 Packets to LFTS". LFTS staat voor Linux Forwarding Transport Service).

Draadloze gesprekstoegangscontrole

In alle recente onderhoudsreleases heeft de controller een activiteitsmonitor, om dynamisch op hoge CPU te reageren en ervoor te zorgen dat AP CAPWAP-tunnels actief blijven, in het geval van niet-duurzame druk.

De functie controleert de WNCD-lading en begint de nieuwe clientactiviteit te vertragen om er zeker van te zijn dat er voldoende resources overblijven om de bestaande verbindingen te verwerken en de CAPWAP-stabiliteit te beschermen.

Dit is standaard ingeschakeld en het heeft geen configuratieopties.

Er zijn drie beveiligingsniveaus gedefinieerd: L1 bij 80% belasting, L2 bij 85% belasting en L3 bij 89%, waarbij elke niveau verschillende inkomende protocollen laat vallen als beveiligingsmechanismen. De beveiliging wordt automatisch verwijderd zodra de lading afneemt.

In een gezond netwerk, moet u geen L2 of L3 ladingsgebeurtenissen zien, en als zij vaak gebeuren, moet het worden onderzocht.

Om te controleren gebruik de opdracht wireless stats cac zoals in de afbeelding.

```
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-bescherming

mDNS als protocol staat een "nul-aanraking"benadering toe om de diensten over apparaten te ontdekken, maar tezelfdertijd kan het zeer actief zijn, en drijflading beduidend, als niet behoorlijk gevormd.

mDNS, zonder enige filtering, kan gemakkelijk het gebruik van WNCD CPU, die uit verscheidene factoren komt opdrijven:

- mDNS-beleid met onbeperkt leren, de controller zal alle diensten die door alle apparaten worden aangeboden krijgen. Dit kan leiden tot zeer grote lijsten van de dienst, met honderden ingangen.
- Beleid zonder filtering: dit zal de controller ertoe aanzetten om die grote servicelijsten te duwen, naar elke klant die vraagt wie een bepaalde service levert.
- Sommige mDNS-specifieke services worden geleverd door "alle" draadloze clients, wat leidt tot een hoger aantal services en activiteit, met variaties op dit door OS-versie.

U kunt mDNS-lijstgrootte per service controleren met deze opdracht:

```
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
```

Dit kan een idee geven van hoe groot een bepaalde query kan krijgen, het duidt niet op een probleem alleen, alleen een manier om te controleren wat wordt gevolgd.

Er zijn enkele belangrijke mDNS-configuratieaanbevelingen:

- Stel mDNS-transport in op één protocol:

9800-1(config)# mdns-sd gateway

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

Standaard wordt IPv4-transport gebruikt. Voor de prestaties is het raadzaam IPv6 of IPv4 te gebruiken, maar niet beide:

- Stel altijd een locatiefilter in het mDNS-servicebeleid in om ongebonden vragen/antwoorden te voorkomen. In het algemeen wordt aanbevolen om "site-tag" te gebruiken, maar andere opties kunnen werken, afhankelijk van uw behoeften.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.