BGP RF-schaaloverwegingen en KPI-bewaking

Inhoud

Inleiding

In dit document worden de belangrijkste factoren beschreven die bijdragen aan de maximale schaal die een BGP-routereflectoren (RR) (Border Gateway Protocol) kunnen bereiken en bieden zij richtlijnen voor BGP RR-prestatiebewaking.

HW/SW-platformselectie

Een grootschalige BGP-RR bevindt zich doorgaans niet in het doorsturen van pakketten die services van een internetserviceprovider bevatten. Daarom zijn de hardwarevereisten voor een BGP RF en routers die voornamelijk pakketten doorsturen in het gegevenspad verschillend. Standaardrouters zijn gebouwd met een krachtig gegevenspad-doorsturen element en een relatief gematigd controle-pad element. Een BGP RR voert al zijn taken uit in een controleplan.
Binnen de Cisco IOS® XR-reeks producten kunt u kiezen uit drie smaken van HW/SW-platforms voor een BGP RR-rol:

Fysieke Cisco IOS XR-router	Cisco IOS XRv 9000 applicatie	Cisco IOS XRv 9000 router (ook bekend als XRv9k)
• Matige capaciteit van het bedieningsvliegtuig (meestal tussen 2 en 6 CPU-kernen toegewezen aan RP XR VM) • Ongebruikte gegevenspadcapaciteit	• Capaciteit van hoog bedieningsvliegtuig (op een Cisco UCS M5-gebaseerd apparaat zijn 36 CPU-kernen bestemd voor RP XR VM) • Gelijke verdeling tussen gegevenspad en regelpadcapaciteit. • XRv9k image draait op barebone voor maximale prestaties	• Aanpasbare capaciteit van het bedieningsvliegtuig • Gelijke splitsing tussen gegevenspad en regelpad bij gebruik van BGP RR-afbeelding. • Een extra laag virtualisatie heeft invloed op de prestaties.

Ten tijde van het schrijven van dit artikel is de XRv9k-applicatie de optimale platformkeuze voor BGP RR, omdat deze de hoogste besturingsplantecapaciteit biedt met maximale prestaties.

Overwegingen over schaal en prestaties

De ondersteunde schaal van data-plane entiteiten is relatief eenvoudig uit te drukken omdat de prestaties van het data-path element zelden afhankelijk is van de schaal. Een TCAM-zoekopdracht neemt bijvoorbeeld dezelfde tijd in, ongeacht het aantal actieve TCAM-vermeldingen.
De ondersteunde schaal van besturings-vlakke entiteiten is vaak veel complexer omdat de schaal en de prestaties onderling verbonden zijn. Overweeg een BGP RF met 1M routes. Het werk dat een BGP-proces moet uitvoeren om deze BGP-tabel te onderhouden, hangt af van:

1. Hoeveel BGP-peers zijn actief?
2. Welke adresfamilies zijn actief?
3. Hoe worden ze verdeeld over updategroepen?
4. De complexiteit van RPL's (routebeleid)
5. Frequentie van updates (inkomende updates en ook uitgaande updates - advertentieinterval).
6. TCP MSS, Interface/Path MTU - afstemming van dit zal helpen bij betere prestaties

7. Bij dual-RP is NSR ingeschakeld
8. Alle bekende slow-peers die niet in een aparte update-groep zitten
9. Waarde Nexthop trigger-vertraging

Aantal BGP-peers

Het aantal BGP-peers is meestal het eerste en helaas vaak het enige dat in gedachten komt bij het overwegen van de BGP-schaal. Hoewel de ondersteunde BGP-schaal niet kan worden weergegeven zonder het aantal BGP-peers te vermelden, is dit niet de belangrijkste factor. Veel andere aspecten zijn even relevant.

Adresfamilies

Het type adresfamilie (AF) is een belangrijke factor in BGP-prestatieoverwegingen, omdat het bij typische implementaties invloed heeft op de omvang van één route. Het aantal IPv4-routes dat in één TCP-segment kan worden ingepakt, is aanzienlijk hoger dan het aantal VPNv4-routes. Om dezelfde schaal van BGP-tabelwijzigingen mogelijk te maken, heeft een IPv4 BGP-RR minder werk te doen dan een VPNv4 BGP-RR. In implementaties waar een aanzienlijk aantal gemeenschappen aan elke route wordt toegevoegd, wordt het verschil tussen AF's minder groot, maar de omvang van een enkele route is dan nog groter en vereist aandacht.

Aantal updategroepen

Het BGP-proces bereidt één update voor alle leden van dezelfde updategroep voor. Vervolgens splitst TCP-proces de updategegevens in een vereist aantal TCP-segmenten (afhankelijk van TCP MSS) naar elk lid van de updategroep. U kunt de actieve updategroepen en hun leden zien door het show bgp update-group bevel te gebruiken. U kunt beïnvloeden welke en hoeveel peers lid zijn van een updategroep door een gemeenschappelijk uitgaand beleid te creëren voor een groep peers die u in dezelfde updategroep wilt zijn. Een enkele update die door de BGP RR naar een groot aantal BGP RR-clients wordt verzonden, kan een burst van TCP-ACK's genereren die in LPTS-component (Local Packet Transport Service) van Cisco IOS XR-routers kan worden gedropt.

Complexiteit van RPL’s (routebeleid)

De complexiteit van het routebeleid dat door BGP wordt gebruikt, heeft invloed op de prestaties van het BGP-proces. Elke ontvangen of verzonden route moet worden beoordeeld aan de hand van het geconfigureerde routebeleid. Een zeer lang beleid vereist dat veel CPU-cycli aan deze actie worden besteed. Een routebeleid dat een reguliere expressie omvat, is met name zwaar bij de verwerking. Een reguliere expressie helpt u het routebeleid uit te drukken in een kleiner aantal regels, maar vereist meer CPU-cycli tijdens het verwerken dan het equivalente routebeleid dat geen reguliere expressie gebruikt.

Frequentie van de bijwerkingen

De frequentie van updates heeft een belangrijke invloed op de BGP-schaal. Het aantal updates is vaak moeilijk te voorspellen. U kunt de frequentie van updates beïnvloeden door de opdracht "**`advertentieinterval`**" te gebruiken, die het minimuminterval instelt tussen het verzenden van (BGP)-routingupdates. De standaardwaarde voor iBGP-peers is 0 seconden en 30 seconden voor eBGP-peers is het 30 seconden.

TCP/MSS en interface/pad-MTU

Het verdelen van een update in vele segmenten van TCP kan veel spanning op TCP procesmiddelen in een high-scale en high-update frequentiemilieu zetten. Een groter pad MTU en grotere TCP MSS zijn beter voor BGP en TCP prestaties.

NSR op dual-RP routers

NSR is een geweldige functie voor redundantie, maar het heeft wel invloed op BGP-prestaties. Op Cisco IOS XR-routers ontvangen beide RP's tegelijkertijd elke BGP-update rechtstreeks van de NPU op de indringerlijnkaart, wat betekent dat de Active RP geen tijd hoeft te besteden aan het repliceren van de update naar de Standby RP. Elke update die door de Active RP wordt gegenereerd, moet echter worden verzonden naar de Standby RP en van daaruit naar de BGP peer. Dit maakt het mogelijk dat de Standby RP altijd up-to-date is op de volgorde en de bevestigingsnummers, maar heeft wel invloed op de algemene BGP-prestaties. Dit is waarom het wordt geadviseerd dat een BGP RR een single-RP router is.

Langzame peers

Een slow peer kan de updates voor alle leden van de updategroep vertragen omdat het BGP-proces de update in het geheugen moet houden tot alle peers het hebben bevestigd. Als u weet dat sommige peers veel langzamer zijn (bijvoorbeeld routers in een legacy-deel van het netwerk), scheidt u ze van tevoren in een updategroep. Standaard rapporteert Cisco IOS XR een trage peer via een syslogbericht. U kunt statische langzame peers (die nooit de updategroep met anderen delen) tot stand brengen of het dynamische langzame peer gedrag verfijnen door het BGP slow-peer configuratiebevel in globale of per-buur configuratiewijze te gebruiken. Een goede verdere informatie hierover kan worden gevonden in Probleemoplossing voor langzame BGP-convergentie als gevolg van suboptimaal routebeleid op IOS-XR op het Cisco xrdocs.io-portal.

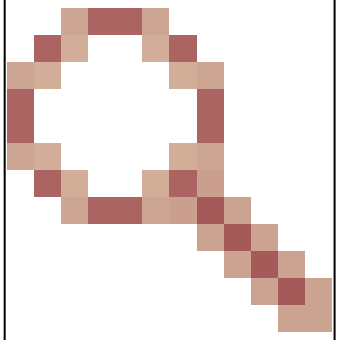
Nexus trigger-vertraging

Als meerdere BGP next-hops veranderen in een kort tijdsinterval en de kritische nexthop trigger-vertraging waarde van nul is geconfigureerd in een adresfamilie (AF) met een groot aantal routes, moet een volledige wandeling van de AF worden uitgevoerd op elke volgende-hop verandering gebeurtenis. Herhaalde wandelingen van die AF verhogen de convergentietijd in adresfamilies met lagere kritische nexthop trigger-vertragingwaarden. U kunt de volgende-hop trigger-vertraging waarden zien door de "show bgp alle nexthops" opdracht.

Voorbeeld van gevalideerde multidimensionale BGP RR-schaal

Multidimensionale schaalresultaten, met name voor de eigenschappen van het regelvlak, zijn sterk afhankelijk van de specifieke testomgeving. De testresultaten kunnen aanzienlijk variëren als bepaalde parameters worden gewijzigd.

Parameter	Waarde	Waarde
Platform	XRv9k-applicatie (UCS M5-gebaseerd)	ASR 9902 router
IOS XR-release	7.5.2 + paraplu SMU voor Cisco bug-id CSCwf09600	7.11.2

	 . (De onderdelen van deze paraplu-SMU zijn geïntegreerd in Cisco IOS XR-release 7.9.2 en hoger)	
Gelijken	VPNv4 eBGP: 2500 VPNv4 iBGP: 1700	VPNv4 iBGP: 2000
BGP-routers	Per sessie: 200 Totaal: 400k Paden per route: 1	Per sessie: 750 VPNv4: 1,36M VPNv6: 150k IPv4: 950k IPv6: 200k Totaal: ~2,6M Paden per route: 1
IGP-routers	10k (ISIS)	10k (ISIS)
BGP-updategroepen	1	1
BGP-timers	standaard	standaard
LPTS BGP-bekend aantal policers	50,000	25,000
TCP-netwerkdraadconfiguratie	16 16	16 16

BGP-verzendbuffergrootte	standaard	standaard
Samenvatting van kernprestatie-indicatoren (KPI)	• Testcase met hoogste input en output pakketsnelheid: ◦ Invoer: 49,4 kpps ◦ Output: 95kpps ◦ ==> LPTS druppels (policer op 50kpps) ◦ ==> Geen druppels in NetIO-clients ◦ ==> Max. grootte XIPC-wachtrij (BGP): 1362 ◦ ==> Max. grootte XIPC-wachtrij (TCP): 1248	• Testcase met hoogste invoerpakketsnelheid: ◦ Invoer: 16030 ◦ Uitvoer: 31 pkts/s ◦ ==> Geen druppels in LPTS of NetIO-clients ◦ ==> Max. grootte XIPC-wachtrij (BGP): 378 ◦ ==> Max. grootte XIPC-wachtrij (TCP): 1021 • Testcase met hoogste pakketuitvoersnelheid: ◦ Invoer: 12172 ◦ Uitvoer: 23465 pkts/s ◦ ==> Geen druppels in LPTS of NetIO-clients ◦ ==> Max. grootte XIPC-wachtrij (BGP): 109 ◦ ==> Max. grootte XIPC-wachtrij (TCP): 1518

Ontwerpoverwegingen

Er zijn twee benaderingen voor BGP RR-plaatsing in het netwerk:

- Gecentraliseerd/plat BGP RF-ontwerp.
- Gedistribueerd/hiërarchisch BGP RR-ontwerp.

In een gecentraliseerd/vlak ontwerp, alle BGP RR-clients in het netwerk maken BGP peering met een set (meestal een paar) BGP RR-apparaten die exact dezelfde informatie bevatten. Deze benadering is eenvoudig uit te voeren en werkt goed in netwerken op kleine tot middelgrote schaal. Elke wijziging in de BGP-tabel wordt snel doorgevoerd naar alle BGP RR-clients. Naarmate het aantal BGP RR-clients toeneemt, kan het ontwerp een schaallimiet bereiken wanneer het aantal TCP-verbindingen op de BGP RR-apparaten zodanig toeneemt dat hun prestaties worden beïnvloed.

In een gedistribueerd/hiërarchisch ontwerp wordt het netwerk in verschillende regio's verdeeld. Alle routers in een regio maken BGP-peiling met een set (meestal een paar) BGP RR-apparaten die exact dezelfde informatie bevatten. Deze BGP RR-apparaten fungeren als BGP RR-clients voor een andere set (meestal een paar) BGP RR-apparaten. Deze ontwerpbenadering zorgt voor een eenvoudige netwerkuitbreiding, terwijl het aantal TCP-verbindingen op elke BGP RR onder een bepaalde limiet blijft.
Een andere ontwerpoverweging is het afstemmen van het bereik van ontvangers van BGP-updates. Afhankelijk van de VRF-distributie onder BGP RR-clients is het de moeite waard om de RT Constrained Route Distribution te overwegen. Als alle BGP RR-clients interfaces in dezelfde VRF hebben, levert RT Constrained Route Distribution niet veel voordelen op. Als VRF's echter schaars verdeeld zijn over alle BGP RR-clients, vermindert het gebruik van RT Constrained Route Distribution aanzienlijk$f$ de belasting op het bgp-proces op de BGP RR.

Monitor BGP-toetsprestatie-indicatoren (KPI)

De controle van de Belangrijkste Prestatie Indicatoren van BGP RR (KPI) is belangrijk voor het verzekeren van juiste netwerkverrichting.

Een significante verandering in de netwerktopologie (bijvoorbeeld een belangrijke DWDM-linkflap) kan leiden tot routingupdates die buitensporig verkeer naar en/of van de BGP-router genereren. Significant verkeer dat de BGP RR raakt, heeft doorgaans de volgende kenmerken:

- Updates van BGP-peers.
- TCP-ACK's gegenereerd door de BGP-peers, in antwoord op updates verzonden door BGP R en vice versa

In dit gedeelte van het document wordt de KPI uitgelegd die op een typische BGP RR moet worden bewaakt en ook hoe u kunt vertellen welke van de twee belangrijke BGP-verkeerstypen een hoge verkeerspercentage veroorzaken.

Het pad van BGP-pakketten binnen de router kan als volgt worden weergegeven:

Punt
Ethernet-controller -(pakket)-> datapath-doorvoerder -(pakket)-> LPTS -(pakket)-> SPP -(pakket) -> NetIO -(pakket)-> TCP -(bericht)-> BGP
Injecteren
BGP -(bericht)-> TCP -(pakket)-> NetIO -(pakket)-> SPP -(pakket) -> datapath-doorvoerder -(pakket)-> Ethernet-controller

KPI's kunnen worden opgesplitst in:

Essentiële elementen:

- Datapath Forwarder
- LPTS (hardware punt policers instellingen, acceptatie tellers en drop tellers)
- SPP
- NetIO
- IPC-wachtrijen (NetIO <==> TCP <==> BGP)
- BGP InQ/OutQ-formaten

Optioneel:

- CPU-gebruik
- Geheugengebruik
- TCP-statistieken
- BGP-procesprestaties
- BGP-convergentie

Monitor Datapath Forwarder

Op XRv9000 is de datapath-doorvoerder de Data Plane Agent (DPA) en op ASR9000-platforms is het de Network Processor (NP).

Monitor XRv9000 dataplane agent (DPA)

Handige opdracht om de belasting en statistieken van de DPA te zien is:

```
show controllers dpa statistics global
```

Deze opdracht toont alle niet-nul teller, die u inzicht geeft in het type en aantal pakketten die van netwerkinterfaces naar RP CPU worden gepunteerd, die van RP CPU naar netwerkinterfaces worden geïnjecteerd, en het aantal pakketten dat daalde:

RP/0/RP0/CPU0:xrv9k-01#

show controllers dpa statistics global

```
 Index Debug Count ------------------------------------------------------------------------------ 350 TBP
```

Monitor ASR 9000 netwerkprocessor (NP)

Handige opdrachten om de belasting en statistieken van elke NP in het systeem te zien zijn:

- show controllers np load all
- show controllers np counters all

NP op ASR9000 heeft een rijke set tellers die u het aantal, tarief en type van verwerkte en gevallen pakketten, tonen.

<#root>

RP/0/RSP0/CPU0:ASR9k-B#

show controllers np load all

```
 Node: 0/0/CPU0: ---------------------------------------------------------------- Load Packet Rate NP0:
```

<#root>

RP/0/RSP0/CPU0:ASR9k-B#

show controllers np counters all

```
 Node: 0/0/CPU0: ---------------------------------------------------------------- Show global stats cou
```

Monitor LPTS

Aangezien een standaardBGP RR niet in de voorwaartse weg is, worden alle pakketten die op netwerkinterface worden ontvangen gestraft aan controle-vliegtuig. Het data-path element op een BGP RR voert een klein aantal eenvoudige bewerkingen uit voordat pakketten worden gepunteerd op control-plane. Aangezien het gegevenspad-element waarschijnlijk geen congestiepunt zal zijn, zijn de LPTS-stats het enige element op de lijnkaart dat bewaking behoeft.

Houd er rekening mee dat in het geval van XRv9k de hardwarestatistiek aan de vPP is toegewezen

Opdracht:

- show lpts pifib hardware police location <location> | inc "Node|flow_type|BGP"

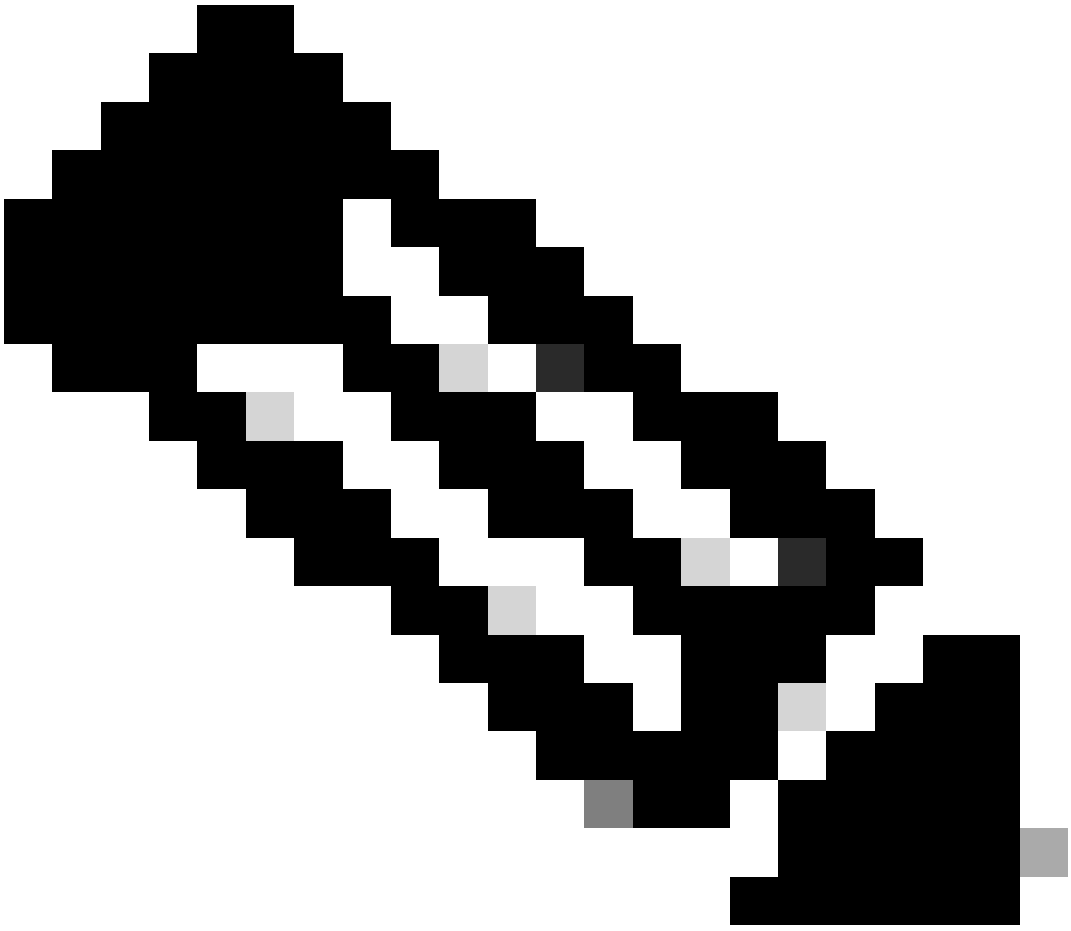
Voorbeeld:

RP/0/RP0/CPU0:xrv9k-01#sh lpts pifib hardware police location 0/0/CPU0 | i "Node|flow_type|BGP" Node 0/0/CPU0: flow_type priority sw_police_id hw

Wat u moet zoeken:
Als een significante sprong in AggDrops tegen BGP-bekend stroomtype wordt waargenomen, begin te zoeken naar de veranderingen van de netwerktopologie die dergelijke massale controlevliegtuigkarnton hebben teweeggebracht.

Gegevenspad telemetrie:

Cisco-IOS-XR-lpts-pre-ifib-oper:lpts-pifib



Opmerking: LPTS-statstellers kunnen worden gewist. Uw controlesysteem moet rekening houden met deze mogelijkheid.

SPP monitor

SPP is de eerste entiteit op de routeprocessor of lijnkaart CPU die het pakket ontvangt dat via interne stof van de NP of DPA wordt geprikt, en het laatste punt in de verwerking van softwarepakketten voordat het wordt overhandigd aan de stof voor injectie in de NP of DPA.

Relevante opdrachten voor SPP-bewaking:

show spp node-counters

show spp client

De **show spp node-counters** opdracht toont de snelheid van gepunte/geïnjecteerde pakketten en is gemakkelijk te lezen en te begrijpen. Voor BGP-sessies staan de relevante tellers onder **client/punt** en **client/inject** op de actieve RP.

Het **show spp client** is rijker in output en geeft een gedetailleerder inzicht in het aantal pakketten die naar klanten worden gevraagd of afgestoten, evenals het hoge watermerk.

```
<#root>
RP/0/RP0/CPU0:xrv9k-01#
show spp node-counters

0/RP0/CPU0:
 socket/rx Punted packets: 595305 Punt bulk reads: 6 Punt non-bulk reads: 595293 Management packets: 74
client/inject Injected from client: 140534413 Non-bulk injects: 140534413 ----------------------------
------------------------------ 0/0/CPU0: <. . .>
```

```
<#root>
RP/0/RP0/CPU0:xrv9k-01#
show spp client

 Sat Apr 20 17:11:40.725 UTC 0/RP0/CPU0: Clients ======= <. . .> netio, JID 254 (pid 4591) ----------
```

Monitor NetIO

Terwijl de LPTS-policer alleen de hoeveelheid pakketten toont die door een corresponderende policer worden geaccepteerd of afgestoten, kunnen we op NetIO-niveau de snelheid zien van pakketten die worden gepunteerd op RP CPU. Aangezien op een typische BGP RR de overgrote meerderheid van de ontvangen pakketten BGP-pakketten zijn, geeft het totale NetIO-tarief zeer nauw het tarief van ontvangen BGP-pakketten aan.

<#root>

Command:

show netio rates

Voorbeeld:

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show netio rates

```
 Netio packet rate for node 0/RP0/CPU0 ----------------------------------- Current rate (updated 0 seco
```

Wat te zoeken:

- Als een significante sprong in tarief NetIO wordt waargenomen, begin het zoeken naar veranderingen van de netwerktopologie die dergelijke massale de vliegtuigkarnton hebben teweeggebracht.

Gegevenspad telemetrie:

- niet van toepassing omdat telemetrie tegenwaarden moet streamen, niet tarieven. BGP-bekende LPTS policer accepteert teller kan worden gebruikt op de Telemetry Collector om de gemiddelde snelheid van ontvangen BGP pakketten van bekende peers te benaderen.

Monitor XIPC-wachtrijen

Op het punt pad worden pakketten die NetIO van LPTS ontvangt doorgegeven aan TCP en BGP. Het is belangrijk om deze wachtrijen te bewaken:

1. TCP-wachtrij met hoge prioriteit waarin NetIO pakketten levert aan TCP
2. BGP-controlewachtrij

3. BGP-gegevenswachtrij

Op de injectiepad worden pakketten aangemaakt door TCP en doorgegeven aan NetIO. Het is belangrijk om deze wachtrijen te bewaken:

- UitvoerL XIPC-wachtrij

Opdrachten:

show netio clients show processes bgp | i "Job Id" show xipcq jid <bgp_job_id> show xipcq jid <bgp_job_id> queue-id <n>

Voorbeelden:

NetIO naar TCP, weergave vanuit NetIO-standpunt:

RP/0/RP0/CPU0:xrv9k-01#show netio clients <. . .> Input Punt XIPC InputQ XIPC PuntQ ClientID Drop/Total Drop/Total Cur/High/Max Cur/High/Max

TCP naar NetIO, weergave vanuit NetIO-standpunt:

RP/0/RP0/CPU0:xrv9k-01#show netio clients <. . .> XIPC queues Dropped/Queued Cur/High/Max ---------- Outp

NetIO naar TCP, weergave vanuit TCP-processtandpunt:

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show processes tcp

```
 | i "Job Id"
 Job Id: 430
RP/0/RP0/CPU0:xrv9k-01#
```

show xipcq jid

```
 430 Mon Apr 17 16:16:11.315 CEST Id Name Size Cur Size Produced Dropped HWM ------ ------------------
```

TCP naar BGP:

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show processes bgp

 | i "Job Id" Job Id: 1078 RP/0/RP0/CPU0:xrv9k-01#

show xipcq jid

 1078 Mon Apr 17 16:09:33.046 CEST Id Name Size Cur Size Produced Dropped HWM ------ ------------------

BGP-gegevenswachtrij:

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show xipcq jid

 1078

queue-id 1

 XIPC_xipcq_12_0_9854_6506_inst_1_data_toapp

:

 Magic: 12344321 Version: 0 SHM Size: 192392 Owner PID: 9854 Owner JID: 1078 Queue ID: 1 Owner MQ handl

BGP-controlewachtrij:

<#root>

RP/0/RP0/CPU0:xrv9k-01#

show xipcq jid

 1078

queue-id

 2 XIPC_xipcq_12_0_9854_6506_inst_1_ctrl_toapp: Magic: 12344321 Version: 0 SHM Size: 480392 Owner PID:

Wat te zoeken:

- de relevante rijen mogen niet worden ingelopen
- in XIPC-wachtrijstats Hoog watermerk (HWM) mag niet groter zijn dan 50% van wachtrijgrootte

Voor een betere tracering van de evolutie met een hoge watermerkwaarde moet u de hoge watermerkwaarde na elke aflezing verwijderen. Merk op dat dit niet alleen de HWM teller ontruimt maar ook alle wachtrijstatistieken ontruimt. Het formaat van het bevel voor het ontruimen van de

XIPC rijstatistieken is: clear xipcq statistics queue-name <queue_name>

Aangezien de naam van de wachtrij vaak de proces-ID (PID) bevat, verandert de naam van de wachtrij na het opnieuw opstarten van het proces. Enkele voorbeelden van opdrachten voor het wissen van de relevante wachtrijstatistieken:

```
clear xipcq statistics queue-name XIPC_tcp_i0
clear xipcq statistics queue-name XIPC_tcp_i1
clear xipcq statistics queue-name XIPC_xipcq_12_0_9854_6506_inst_1_data_toapp
clear xipcq statistics queue-name XIPC_xipcq_12_0_9854_6506_inst_1_ctrl_toapp
```

Telemetriepad:

- Er zijn geen Telemetry sensorpaden voor XIPC.

Monitor BGP-ingangen en -uitvoerwachtrijen

BGP houdt een invoer- en uitvoerwachtrij bij voor elke BGP-peer. Gegevens worden opgeslagen in InQ wanneer TCP het heeft doorgegeven aan BGP, maar BGP heeft deze nog niet verwerkt. Gegevens worden opgeslagen in OutQ terwijl BGP op TCP wacht om de gegevens in pakketten te splitsen en te verzenden. De momentane grootte van BGP InQ/OutQ geeft een goede indicatie van hoe druk het BGP-proces is.

Opdracht:

show bgp <AFI> <SAFI> summary

Voorbeeld:

RP/0/RP0/CPU0:xrv9k-01#show bgp all all summary Address Family: VPNv4 Unicast ---------- BGP router identifier 192.168.0.1, local A

Wat u moet zoeken:

- De grootte van InQ/OutQ moet nul zijn wanneer het netwerk stabiel is. Het verandert snel wanneer updates worden uitgewisseld.
- De InQ/OutQ-grootte mag in de loop der tijd niet monotoon toenemen.

Telemetriepad:

- Cisco 800-IOS-XR-IP4-bgp-oper:bgp

BGP-berichtsnelheden controleren

Sommige BGP-buren kunnen continu updates of intrekkingen verzenden als de netwerktopologie instabiel is. De BGP RR moet deze routeringstabel vervolgens duizenden keren wijzigen in al zijn RR-clients. Daarom is het belangrijk om de van de buurlanden ontvangen berichtsnelheden te controleren en de bronnen van instabiliteit te volgen.

Opdracht:

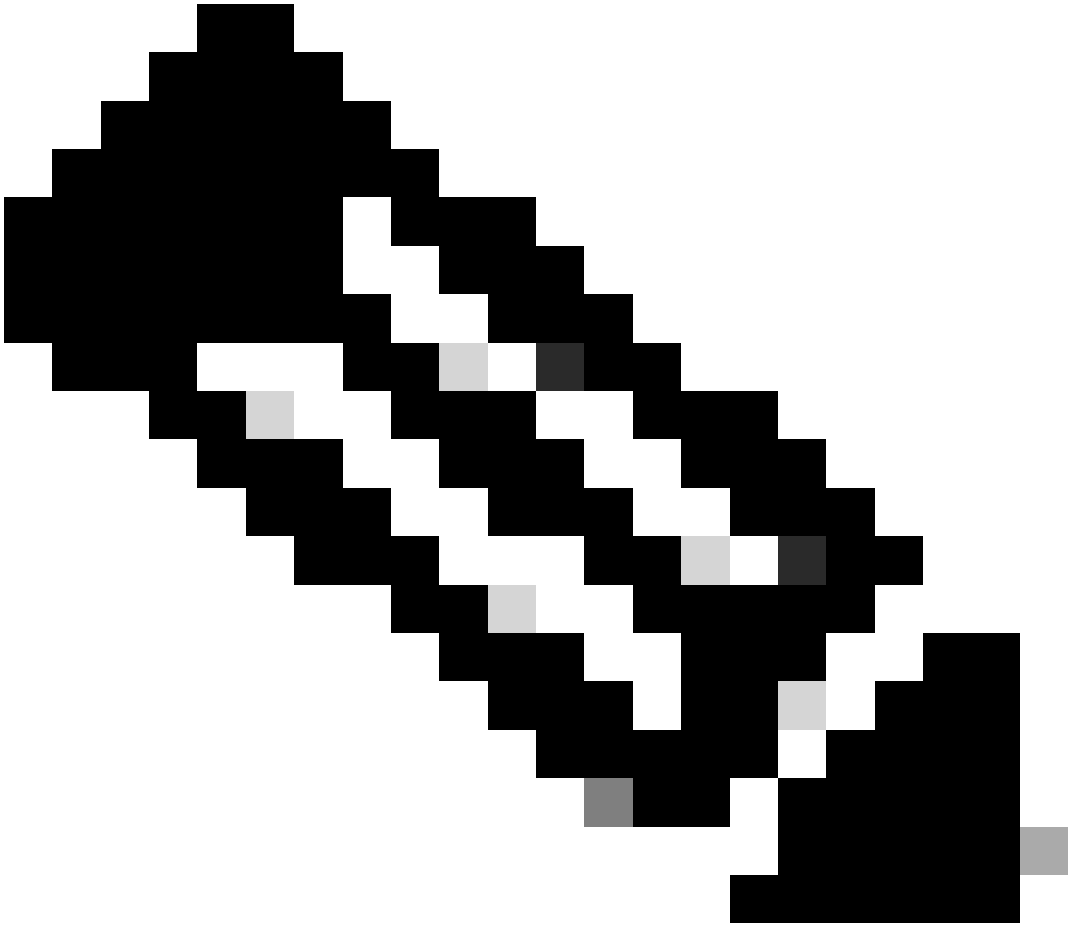
show bgp <AFI> <SAFI> summary

Voorbeeld:

RP/0/RP0/CPU0:xrv9k-01#show bgp all all summary Address Family: VPNv4 Unicast ---------- BGP router identifier 192.168.0.1, local A

RR-clients hebben ruwweg dezelfde hoeveelheid MsgSent, maar sommige buren kunnen een aantal MsgRcvd hoger hebben dan anderen. U moet meerdere snapshots van deze opdracht opnemen om de snelheid van de berichten te bepalen.

Zodra u de beledigende peers hebt geïdentificeerd, kunt u vervolgens andere opdrachten doorlopen zoals **show bgp neighbor <neighbor> detail** en **show bgp neighbor <neighbor> performance-statistics** of proberen **show bgp recent-prefixe**s te begrijpen welke prefixes knipperen en of het altijd dezelfde of verschillende zijn.



Opmerking: de MsgRcvd- en MsgSent-tellers zijn per-buurman maar niet per adresfamilie. Dus als je een commando uitvoert zoals show bgp all all summary , zie je dezelfde tellers per buur in de secties voor de verschillende adresfamilies. Zij vertegenwoordigen niet het aantal ontvangen/verzonden berichten van/naar die buur voor die adresfamilie, maar over adresfamilies heen.

CPU-gebruik voor monitoren

Het gebruik van cpu moet op elke router worden gecontroleerd, maar op een router met een hoog aantal cpu kernen gewijd aan controlevliegtuig kunnen sommige lezingen unintuïtief zijn. Op een BGP-router met een groot aantal CPU-cores die specifiek zijn voor Routing Processor (RTP), zoals bij de XRv9k-applicatie, werken actieve threads op verschillende CPU-cores, terwijl een aantal CPU-cores inactief blijft. Als gevolg kunnen sommige CPU-kernen erg druk zijn, maar het totale CPU-gebruik dat voor alle CPU-kernen wordt berekend, blijft gematigd.

Gebruik daarom de **show processes cpu thread** opdracht voor goede bewaking van het gebruik van CPU-cores via CLI.

TCP-statistieken controleren

Cisco IOS® onderhoudt gedetailleerde statistieken over elke TCP-sessie. De CLI-opdracht **show tcp brief** geeft een lijst weer van alle bestaande TCP-sessies. In deze samenvatting van de output, voor elke TCP sessie kunt u deze informatie zien:

- **PCB:** unieke TCP sessie-identificatie.
- **VRF-ID**: de ID van de VRF waarin de sessie bestaat.
  - Om de corresponderende VRF-naam te zien, voert u deze opdracht uit:
  - show cef vrf all summary | utility egrep "^VRF:|Vrfid" | utility egrep -B1 <VRF-ID>
- **Recv-Q**: onmiddellijke grootte van de ontvangstwachtrij Q. Ontvang wachtrijen voor pakketten ontvangen van NetIO. Het **TCP-**proces extraheert de gegevens uit een pakket en stuurt deze naar de corresponderende toepassing.
- **Send-Q**: onmiddellijke grootte van de Send Q. Send wachtrij houdt gegevens die van een toepassing zijn ontvangen. Het **TCP-**proces splitst de gegevens in TCP-segmenten (gedicteerd door overeengekomen maximale segmentgrootte - TCP MSS), kapselt elk segment in in een Layer 3-header van de corresponderende adresfamilie (IPv4 of IPv6) en verstuurt het pakket naar NetIO.
- **Lokaal adres**: lokaal IPv4- of IPv6-adres dat aan de TCP-socket is gekoppeld. TCP-sessies in LISTEN-staat zijn doorgaans gebonden aan "**elk**" IP-adres, dat wordt weergegeven als "0.0.0.0" of ":" in het geval van IPv4 of IPv6.
- **Vreemd adres**: extern IPv4- of IPv6-adres gekoppeld aan de TCP-socket. TCP-sessies in LISTEN-staat zijn doorgaans gebonden aan "**elk**" IP-adres, dat wordt weergegeven als "0.0.0.0" of ":" in het geval van IPv4 of IPv6.
- **Status**: TCP-sessiestatus. Mogelijke TCP-sessiestatus is: LUISTEREN, SYNSEND, SYNRCVD, ESTAB, LASTACK, SLUITEN, CLOSEwait, FINwait1, FINwait2, timewait, GESLOTEN.

Aangezien het bekende BGP-poortnummer 179 is, kunt u de weergegeven TCP-sessies beperken tot de sessies die aan de BGP-toepassing zijn gekoppeld.

Voorbeeld:

RP/0/RSP0/CPU0:ASR9k-B#show tcp brief | include "PCB|:179 " PCB VRF-ID Recv-Q Send-Q Local Address Foreign Address State 0x00007ff7d403bd

U kunt de weergegeven PCB-waarde gebruiken om de statistieken voor een bepaalde TCP-sessie te verkrijgen. CLI-opdrachten die inzicht bieden in TCP-processtatistieken:

Wereldwijd:

show tcp statistics clients location <active_RP>

show tcp statistics summary location <active_RP>

Per PCB:

show tcp brief | i ":179"

show tcp detail pcb <pcb> location 0/RP0/CPU0

show tcp statistics pcb <pcb> location <active_RP>

De globale TCP statistieken bevelen tonen de algemene gezondheid van TCP zittingen. Naast de statistieken van het gegevenspakket (in/out), kunt u bijvoorbeeld zien of er pakketten met controlesomfouten zijn, misvormde pakketten, pakketten die wegens verificatiefouten zijn gelaten vallen, out-of-order pakketten, pakketten met gegevens na venster, wat u een indicatie geeft van het gedrag van TCP-peers.

In de per-PCB opdrachten, kunt u belangrijke parameters van een TCP-sessie zien, zoals MSS, maximale round-trip tijd, enzovoort.

Relevante tellers in de uitvoer van show tcp detail pcb commando zijn:

- **Begint timer terug**: geeft aan hoe vaak de timer voor herverzending is gestart.
- **Retrans Timer Wakeups**: geeft aan hoe vaak de hertransmissie-timer is uitgelopen, waardoor een hertransmissie van het TCP-segment wordt geactiveerd.
- **Huidige verzend wachtrijgrootte in bytes**: niet erkende bytes van de edele.
- **Stroom ontvangt wachtrijgrootte in bytes/pakketten**: bytes/pakketten die nog moeten worden gelezen door de applicatie (BGP).
- **niet-geordende bytes**: bytes die in de wachtrij voor opslaan als gevolg van een gat in TCP-ontvangstvenster in de wachtrij staan.

<#root>

RP/0/RSP0/CPU0:ASR9k-B#

show tcp detail pcb 0x4a4400e4

========== Connection state is ESTAB, I/O status:

Current send queue size in bytes: 0 (max 16384)

Current receive queue size in bytes: 0 (max 65535)

mis-ordered: 0 bytes

Current receive queue size in packets: 0 (max 60)

Timer Starts Wakeups Next(msec)

Retrans 2795 0 0

SendWnd 1341 0 0 TimeWait 0 0 0 AckHold 274 2 0 KeepAlive 333 1 299983 PmtuAger 0 0 0 GiveUp 0 0 0 Thro
SRTT: 162 ms, RTTO: 415 ms, RTV: 253 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 247 ms ACK hold time: 200 ms, Keepalive time: 300 sec, SYN waittime: 30 sec Giveu

Monitorgeheugengebruik

De BGP-routetabel wordt opgeslagen in het BGP-geheugen van de processtapel. De routeringstabel wordt opgeslagen in het RIB-processtapgeheugen.

Handige opdrachten voor bewaking van heapgeheugen:

show memory summary

show memory summary detail

show memory-top-consumers

show memory heap summary all

Pad telemetriesensor:

Cisco-IOS-XR-nto-misc-oper:memory-summary/nodes/node/detail

FIB slaat het doorsturen van ingangen op in gedeelde geheugenruimte.

Handige opdrachten voor gedeelde geheugenbewaking:

show memory summary

show memory summary detail

show shmwin summary

BGP-procesprestaties bewaken

Handige opdracht die interne gegevens over BGP-procesprestaties levert:

show bgp process performance-statistics

show bgp process performance-statistics detail

BGP-convergentie controleren

Een andere nuttige opdracht is de opdracht die de algemene status van BGP-convergentie toont: show bgp convergence

Als het netwerk stabiel is, zie je zoiets:

RP/0/RP0/CPU0:ASR9k-B#show bgp convergence Mon Dec 18 13:55:47.976 UTC Converged. All received routes in RIB, all neighbors updated. All neig

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.