Überlegungen zur BGP-RR-Skalierung und KPI-Überwachung

Inhalt

Einleitung

In diesem Dokument werden die wichtigsten Faktoren für die maximale Skalierbarkeit beschrieben, die mit Border Gateway Protocol (BGP) Route-Reflectors (RR) erreicht werden kann, und es werden Orientierungshilfen zur BGP RR-Leistungsüberwachung gegeben.

Auswahl der HW-/SW-Plattform

Ein hochskalierter BGP-RR befindet sich in der Regel nicht im Weiterleitungspfad von Paketen, die Dienste enthalten, die von einem Internetdienstanbieter bereitgestellt werden. Aus diesem Grund unterscheiden sich die Hardwareanforderungen für einen BGP-RR und Router, die überwiegend Pakete im Datenpfad weiterleiten. Standard-Router verfügen über ein leistungsstarkes Datenpfad-Weiterleitungselement und ein vergleichsweise moderates Steuerpfad-Element. Ein BGP-RR führt alle seine Aufgaben in einem Kontrollplan aus. Innerhalb der Cisco IOS® XR-Produktfamilie können Sie zwischen drei Varianten von HW/SW-Plattformen für eine BGP-RR-Rolle wählen:

Physischer Cisco IOS XR-Router	Cisco IOS XRv 9000-Appliance	Cisco IOS XRv 9000-Router (auch bekannt als XRv9k)
• Moderate Kapazität der Steuerungsebene (in der Regel zwischen 2 und 6 CPU-Kernen, die RP XR VM zugewiesen sind) • Nicht genutzte Kapazität des Datenpfads	• Hohe Kapazität der Kontrollebene (auf Cisco UCS M5-basierter Appliance sind 36 CPU-Kerne für RP XR VM dediziert) • Gleiche Aufteilung zwischen Datenpfad- und Steuerpfad-Kapazität. • XRv9k-Image wird für maximale Leistung auf Barebone ausgeführt	• Anpassbare Kapazität der Kontrollebene • Gleiche Aufteilung zwischen Datenpfad- und Steuerpfad-Stromversorgung bei Verwendung des BGP RR-Image. • Eine zusätzliche Ebene der Virtualisierung beeinträchtigt die Leistung.

Zum Zeitpunkt der Erstellung dieses Dokuments stellt die XRv9k-Appliance die optimale Plattformauswahl für BGP RR dar, da sie eine maximale Kontrollebenenkapazität bei maximaler Leistung bietet.

Überlegungen zu Skalierung und Leistung

Die unterstützte Skalierung von Datenebenenentitäten ist relativ einfach auszudrücken, da die Leistung des Datenpfadelements selten von der Skalierung abhängt. Eine TCAM-Suche dauert beispielsweise unabhängig von der Anzahl der aktiven TCAM-Einträge dieselbe Zeit.
Die unterstützte Skalierung von Kontrollebenen-Einheiten ist oft sehr viel komplexer, da Skalierung und Leistung miteinander verbunden sind. Angenommen, es handelt sich um einen BGP-RR mit einer Million Routen. Die Arbeit, die ein BGP-Prozess zur Verwaltung dieser BGP-Tabelle leisten muss, hängt von folgenden Faktoren ab:

1. Wie viele BGP-Peers sind aktiv?
2. Welche Adressfamilien sind aktiv?

3. Wie werden sie in Aktualisierungsgruppen aufgeteilt?
4. Die Komplexität von RPLs (Routenrichtlinien)
5. Häufigkeit der Updates (eingehende und ausgehende Updates - Ankündigungsintervall).
6. TCP-MSS, Schnittstellen-/Pfad-MTU - diese Einstellung verbessert die Leistung.
7. Bei dualem RP: NSR aktiviert
8. Bekannte Slow-Peers, die sich nicht in einer separaten Update-Gruppe befinden
9. Nexthop-Trigger-Verzögerungswert

Anzahl der BGP-Peers

Die Anzahl der BGP-Peers ist in der Regel die erste und leider oft auch die einzige, die einem bei der BGP-Skalierung in den Sinn kommt. Die unterstützte BGP-Skalierung kann zwar nicht dargestellt werden, ohne die Anzahl der BGP-Peers anzugeben, sie ist jedoch nicht der wichtigste Faktor. Viele andere Aspekte sind gleichermaßen relevant.

Adressfamilien

Der Typ der Adressfamilie (AF) spielt bei der Beurteilung der BGP-Leistung eine wichtige Rolle, da er sich in typischen Bereitstellungen auf die Größe einer einzelnen Route auswirkt. Die Anzahl der IPv4-Routen, die in ein TCP-Segment gepackt werden können, ist deutlich höher als die Anzahl der VPNv4-Routen. Bei derselben Größenordnung von BGP-Tabellenänderungen hat ein IPv4-BGP-RR daher weniger Arbeit als ein VPNv4-BGP-RR. Bei Bereitstellungen, bei denen jeder Route eine erhebliche Anzahl von Communitys hinzugefügt wird, ist der Unterschied zwischen AFs natürlich geringer, aber die Größe einer einzelnen Route ist dann noch größer und muss berücksichtigt werden.

Anzahl der Aktualisierungsgruppen

Der BGP-Prozess bereitet ein einzelnes Update für alle Mitglieder derselben Update-Gruppe vor. Anschließend teilt der TCP-Prozess die Aktualisierungsdaten in eine erforderliche Anzahl von TCP-Segmenten (abhängig von TCP MSS) für jedes Mitglied der Aktualisierungsgruppe auf. Sie können die aktiven Aktualisierungsgruppen und ihre Mitglieder mithilfe des show bgp update-group Befehls anzeigen. Sie können beeinflussen, welche und wie viele Peers Mitglieder einer Update-Gruppe sind, indem Sie eine gemeinsame ausgehende Richtlinie für eine Gruppe von Peers erstellen, die derselben Update-Gruppe angehören sollen. Ein einzelnes Update, das vom BGP RR an eine große Anzahl von BGP RR-Clients gesendet wird, kann eine Flut von TCP-ACKs auslösen, die in der LPTS-Komponente (Local Packet Transport Service) der Cisco IOS XR-Router verworfen werden können.

Komplexität von RPLs (Routenrichtlinien)

Die Komplexität der vom BGP verwendeten Routenrichtlinien wirkt sich auf die Leistung des BGP-Prozesses aus. Jede empfangene oder gesendete Route muss anhand der konfigurierten Routenrichtlinie ausgewertet werden. Eine sehr lange Richtlinie erfordert viele CPU-Zyklen, die für diese Aktion ausgegeben werden müssen. Eine Routingrichtlinie, die einen regulären Ausdruck enthält, ist besonders aufwändig in der Verarbeitung. Mit einem regulären Ausdruck können Sie die Routingrichtlinie in einer geringeren Anzahl von Zeilen ausdrücken, während die Verarbeitung mehr CPU-Zyklen erfordert als mit der entsprechenden Routingrichtlinie, die keinen regulären Ausdruck verwendet.

Aktualisierungshäufigkeit

Die Häufigkeit von Updates spielt bei der BGP-Skala eine wichtige Rolle. Die Anzahl der Updates ist oft schwer vorherzusagen. Sie können die Aktualisierungshäufigkeit beeinflussen, indem Sie den Befehl "**`advertisement-interval"`** verwenden, der das minimale Intervall zwischen dem Senden von BGP)-Routing-Updates festlegt. Der Standardwert für iBGP-Peers ist 0 Sekunden und für eBGP-Peers 30 Sekunden.

TCP-MSS und Schnittstellen-/Pfad-MTU

Das Aufteilen eines Updates in viele TCP-Segmente kann die TCP-Prozessressourcen in einer umfangreichen und regelmäßig aktualisierten Umgebung stark belasten. Eine größere Pfad-MTU und größere TCP-MSS sind besser für die BGP- und TCP-Leistung.

NSR auf Dual-RP-Routern

NSR ist eine hervorragende Redundanzfunktion, hat jedoch Auswirkungen auf die BGP-Leistung. Auf Cisco IOS XR-Routern empfangen beide RPs gleichzeitig jedes BGP-Update direkt von der NPU auf der Eingangs-Linecard. Das bedeutet, dass der aktive RP keine Zeit für die Replikation des Updates auf den Standby-RP aufwenden muss. Alle vom aktiven RP generierten Updates müssen jedoch an den Standby-RP und von dort an den BGP-Peer gesendet werden. Auf diese Weise ist der Standby-RP hinsichtlich der Sequenz und der Bestätigungsnummern immer auf dem neuesten Stand, was sich jedoch auf die BGP-Gesamtleistung auswirkt. Aus diesem Grund wird empfohlen, dass ein BGP-RR ein Single-RP-Router ist.

Langsame Peers

Ein langsamer Peer kann die Updates für alle Mitglieder der Update-Gruppe verlangsamen, da der BGP-Prozess das Update im Speicher behalten muss, bis alle Peers es bestätigt haben. Wenn Sie wissen, dass einige Peers wesentlich langsamer sind (z. B. Router in einem älteren Teil des Netzwerks), teilen Sie sie vorab in eine Update-Gruppe auf. Standardmäßig meldet Cisco IOS XR einen langsamen Peer per Syslog-Meldung. Sie können statische langsame Peers erstellen (die die Update-Gruppe nie gemeinsam mit anderen nutzen) oder das Verhalten dynamischer langsamer Peers mithilfe des BGP-slow-peer Konfigurationsbefehls im globalen oder nachbarspezifischen Konfigurationsmodus optimieren. Eine weitere nützliche Anleitung hierzu finden Sie unter Fehlerbehebung bei langsamer BGP-Konvergenz aufgrund suboptimaler Routenrichtlinien in IOS-XR im Portal Cisco xrdocs.io.

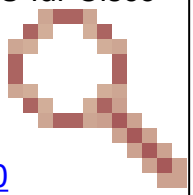
Nexthop-Triggerverzögerung

Wenn sich in einem kurzen Zeitintervall mehrere BGP Next-Hops ändern und der kritische Next-Hop Trigger-Delay-Wert Null in einer Adressfamilie (AF) mit einer hohen Anzahl von Routen konfiguriert ist, muss bei jedem Next-Hop Change-Ereignis ein vollständiger Walk des AF ausgeführt werden. Wiederholte Durchläufe dieses AF erhöhen die Konvergenzzeit in Adressfamilien mit niedrigeren kritischen NextHop-Trigger-Verzögerungs-Werten. Sie können die Werte für die Next-Hop-Triggerverzögerung anzeigen, indem Sie den Befehl "show bgp all nexthops" ausführen.

Beispiel einer validierten mehrdimensionalen BGP-RR-Skalierung

Die Ergebnisse der mehrdimensionalen Skalierung, insbesondere für die Merkmale der Kontrollebene, hängen stark von der jeweiligen Testumgebung ab. Die Testergebnisse können erheblich variieren, wenn einige Parameter geändert werden.

Parameter	Wert	Wert

Plattform	XRv9k Appliance (auf UCS M5 basiert)	ASR 9902
IOS XR-Version	7.5.2 + umbrella SMU für Cisco  Bug-ID CSCwf09600 . (Komponenten dieser übergeordneten SMU sind in Cisco IOS XR Version 7.9.2 und höher integriert)	7.11.2
Peers	VPNv4 eBGP: 2.500 VPNv4-iBGP: 1700	VPNv4 iBGP: 2.000
BGP-Routen	Pro Sitzung: 200 Gesamt: 400k Pfade pro Route: 1	Pro Sitzung: 750 VPNv4: 1,36 Mio. VPNv6: 150.000 IPv4: 950k IPv6: 200.000 Insgesamt: ~2,6 Mio. Pfade pro Route: 1
IGP-Routen	10.000 (IS)	10.000 (IS)
BGP-Aktualisierungsgruppen	1	1
BGP-Timer	standard	standard
LPTS-BGP-Rate (bekannte Überwachung)	50,000	25,000

tcp num-thread-Konfiguration	16 16	16 16
Größe des BGP-Sendepuffers	standard	standard
Zusammenfassung der Leistungskennzahlen	• Testfall mit höchster Eingangs- und Ausgangs-Paketrate: ◦ Eingabe: 49,4 Kbit/s ◦ Leistung: 95 Kbit/s ◦ ==> LPTS-Drops (Policer bei 50 Kbit/s) ◦ ==> Keine Drops auf NetIO-Clients ◦ ==> Max. XIPC-Warteschlangengröße (BGP): 1362 ◦ ==> Max. XIPC-Warteschlangengröße (TCP): 1248	• Testfall mit höchster Eingangspaketrate: ◦ Eingabe: 16030 Pkte/s ◦ Leistung: 31 Pkte/s ◦ ==> Keine Verluste bei LPTS- oder NetIO-Clients ◦ ==> Max. XIPC-Warteschlangengröße (BGP): 378 ◦ ==> Max. XIPC-Warteschlangengröße (TCP): 1.021 • Testfall mit höchster Paketausgangsrate: ◦ Eingabe: 12172 Pkte/s ◦ Ausgabe: 23465 Pkte/s ◦ ==> Keine Verluste bei LPTS- oder NetIO-Clients ◦ ==> Max. XIPC-Warteschlangengröße (BGP): 109 ◦ ==> Max. XIPC-Warteschlangengröße (TCP): 1518

Überlegungen zum Netzwerkdesign

Es gibt zwei Ansätze für die BGP RR-Platzierung im Netzwerk:

- Zentralisiertes/flaches BGP-RR-Design.
- Verteiltes/hierarchisches BGP-RR-Design.

In einem zentralisierten/flachen Design stellen alle BGP RR-Clients im Netzwerk BGP-Peering mit einer Gruppe (in der Regel ein Paar) von BGP RR-Geräten her, die exakt die gleichen Informationen enthalten. Dieser Ansatz ist einfach zu implementieren und funktioniert gut in kleinen bis mittleren Netzwerken. Jede Änderung in der BGP-Tabelle wird schnell an alle BGP RR-Clients weitergeleitet. Mit zunehmender Anzahl von BGP-RR-Clients kann das Design eine Skalierungsgrenze erreichen, wenn die Anzahl der TCP-Verbindungen auf den BGP-RR-Geräten so stark zunimmt, dass ihre Leistung beeinträchtigt wird.

Bei einem verteilten/hierarchischen Design wird das Netzwerk in mehrere Regionen unterteilt. Alle Router in einer Region stellen BGP-Peering mit einem Satz (in der Regel einem Paar) von BGP-RR-Geräten her, die exakt die gleichen Informationen enthalten. Diese BGP RR-Geräte fungieren als BGP RR-Clients für einen anderen Satz (in der Regel ein Paar) von BGP RR-Geräten. Dieser Designansatz ermöglicht eine einfache Netzwerkerweiterung, wobei die Anzahl der TCP-Verbindungen auf jedem einzelnen BGP-RR unter einem bestimmten Grenzwert gehalten wird.
Ein weiterer Designaspekt besteht darin, den Umfang der Empfänger von BGP-Updates genau anzupassen. Je nach VRF-Verteilung zwischen BGP-RR-Clients empfiehlt sich die Verteilung über RT (Constrained Route Distribution). Wenn alle BGP-RR-Clients über Schnittstellen in derselben VRF-Instanz verfügen, bietet die eingeschränkte RT-Routenverteilung keine großen Vorteile. Wenn VRFs jedoch nur geringfügig auf alle BGP RR-Clients verteilt sind, wird durch die RT Constrained Route Distribution die Last für den BGP-Prozess auf dem BGP RR erheblich verringert$f$.

Überwachen der BGP-Leistungskennzahlen

Die Überwachung der Key Performance Indicators (KPI) des BGP RR ist wichtig, um einen ordnungsgemäßen Netzwerkbetrieb zu gewährleisten.

Eine signifikante Änderung der Netzwerktopologie (z. B. eine größere DWDM-Link-Flap) kann Routing-Updates auslösen, die übermäßigen Datenverkehr zum und/oder vom BGP RR generieren. Ein erheblicher Datenverkehr, der den BGP RR erreicht, führt in der Regel Folgendes:

- Aktualisierungen von BGP-Peers.
- Von den BGP-Peers als Reaktion auf vom BGP RR gesendete Updates generierte TCP-ACKs und umgekehrt

In diesem Abschnitt wird erläutert, welche Leistungskennzahlen bei einem typischen BGP RR überwacht werden müssen und wie festgestellt werden kann, welcher der beiden signifikanten BGP-Datenverkehrstypen eine hohe Datenverkehrsrate auf der Kontrollebene verursacht.

Der Pfad der BGP-Pakete innerhalb des Routers kann wie folgt dargestellt werden:

Punt
Ethernet-Controller -(Paket)-> Data Path Forwarder -(Paket)-> LPTS -(Paket)-> SPP -(Paket) -> NetIO -(Paket)-> TCP -(Nachricht)-> BGP
Injizieren
BGP -(Nachricht)-> TCP -(Paket)-> NetIO -(Paket)-> SPP -(Paket) -> Data Path Forwarder -(Paket)-> Ethernet-Controller

KPIs können aufgeteilt werden in:

Grundlagen:

- DataPath-Weiterleitung
- LPTS (Einstellungen für Hardware-Point-Policers, Annahme von Zählern und Zählern zum Zurücksetzen)
- SPP
- NetIO
- IPC-Warteschlangen (NetIO <==> TCP <==> BGP)
- BGP InQ/OutQ-Größen

Optional:

- CPU-Auslastung
- Speichernutzung
- TCP-Statistik
- Leistung des BGP-Prozesses
- BGP-Konvergenz

Überwachen der Datenpfadweiterleitung

Auf XRv9000 ist der Datenpfad-Forwarder der Datenebenen-Agent (DPA), auf ASR9000-Plattformen der Netzwerkprozessor (NP).

Überwachung des XRv9000-Datenebenen-Agenten (DPA)

Der nützliche Befehl zum Anzeigen der Last und der Statistiken der DPA lautet:

```
show controllers dpa statistics global
```

Dieser Befehl zeigt den Zähler ungleich null an, der Ihnen einen Einblick in den Typ und die Anzahl der Pakete gibt, die von den Netzwerkschnittstellen an die RP-CPU gesendet, von der RP-CPU an die Netzwerkschnittstellen weitergeleitet und verworfen wurden:

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

```
show controllers dpa statistics global
```

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

Überwachung des ASR9000 Netzwerkprozessors (NP)

Die folgenden Befehle dienen zur Anzeige der Last und der Statistiken der einzelnen NPs im System:

show controllers np load all

show controllers np counters all

Der NP auf dem ASR9000 verfügt über eine Vielzahl von Zählern, die Anzahl, Geschwindigkeit und Typ verarbeiteter und verworfener Pakete anzeigen.

<#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
```

Überwachen von LPTS

Da sich ein Standard-BGP-RR nicht im Weiterleitungspfad befindet, werden alle an der Netzwerkschnittstelle empfangenen Pakete an die Steuerungsebene weitergeleitet. Das Datenpfadelement in einem BGP-RR führt eine kleine Anzahl einfacher Vorgänge aus, bevor Pakete auf die Kontrollebene gesendet werden. Da es sich bei dem Datenpfadelement wahrscheinlich nicht um einen Überlastungspunkt handelt, müssen auf der Linecard nur die LPTS-Statistiken überwacht werden.

Beachten Sie, dass im Fall von XRv9k die Hardwarestatistiken dem vPP zugeordnet sind.

Command:

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

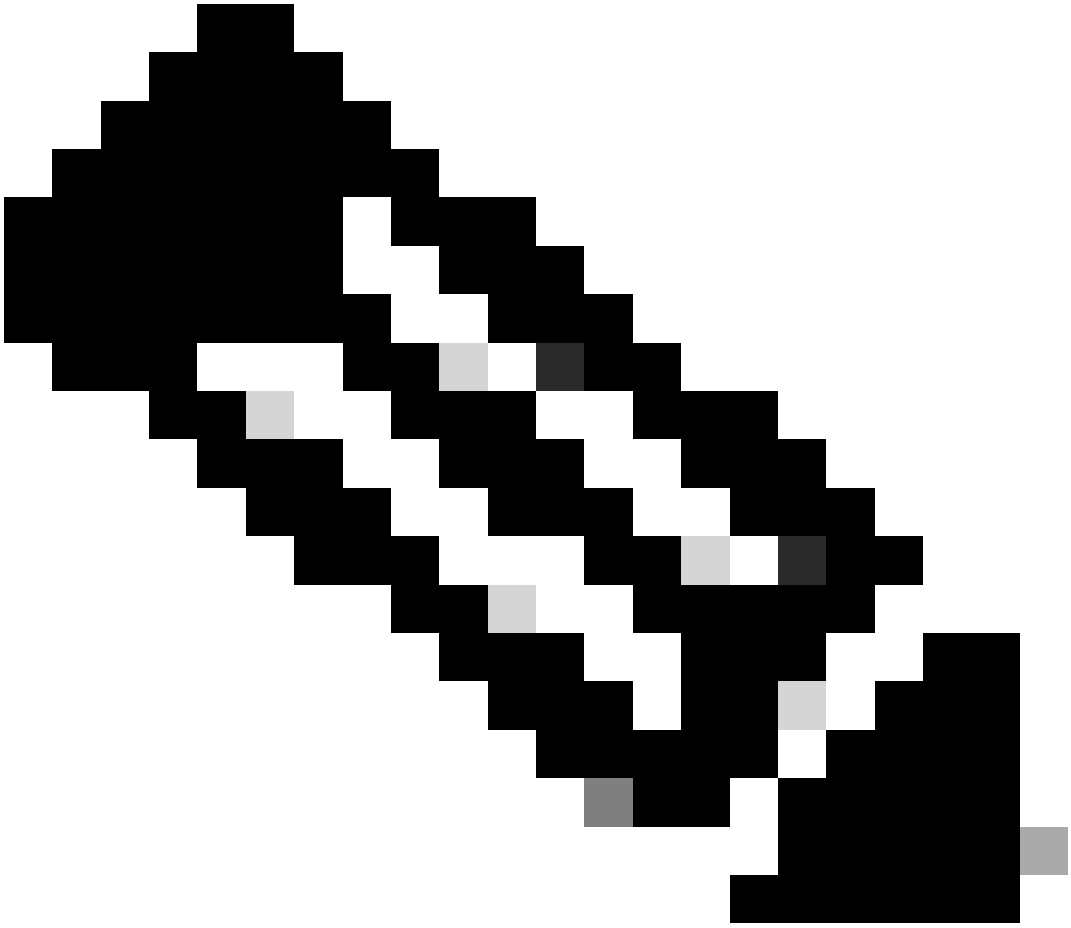
Beispiel:

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

Zu suchende Elemente:
Wenn ein signifikanter Anstieg von AggDrops im Vergleich zum BGP-bekannten Flow-Typ festgestellt wird, suchen Sie nach Netzwerktopologieänderungen, die eine derart massive Abwanderung von Kontrollebenen ausgelöst haben.

Telemetriedatenpfad:

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



Hinweis: LPTS-Statistikzähler können gelöscht werden. Diese Möglichkeit muss von Ihrem Überwachungssystem berücksichtigt werden.

SPP überwachen

SPP ist die erste Einheit auf dem Routingprozessor oder der Linecard-CPU, die das vom NP oder DPA gestanzte Paket über die interne Struktur empfängt, und der letzte Punkt in der Softwarepaketverarbeitung, bevor es zur Injektion in den NP oder DPA an die Struktur übergeben wird.

Relevante Befehle für die SPP-Überwachung:

show spp node-counters

show spp client

Der **show spp node-counters** Befehl zeigt die Rate der gesendeten/injizierten Pakete an und ist leicht zu lesen und zu verstehen. Bei BGP-Sitzungen befinden sich die relevanten Zähler unter **client/punt** und **client/inject** auf dem aktiven RP.

Die **show spp client** ist leistungsfähiger und bietet einen detaillierteren Einblick in die Anzahl der Pakete, die in die Warteschlange gestellt bzw. an Clients verworfen wurden, sowie in das hohe Wasserzeichen.

<#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) ----------

Überwachung von NetIO

Während die LPTS-Richtlinie nur die Anzahl der Pakete anzeigt, die von einer entsprechenden Richtlinie angenommen oder verworfen wurden, kann auf NetIO-Ebene die Rate der Pakete angezeigt werden, die an die RP-CPU gesendet wurden. Da bei einem typischen BGP-RR die große Mehrheit der empfangenen Pakete BGP-Pakete sind, gibt die NetIO-Rate insgesamt sehr genau die Rate der empfangenen BGP-Pakete an.

<#root>

Command:

show netio rates

Beispiel:

<#root>

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

show netio rates

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

Was ist zu beachten?

- Wenn ein signifikanter Anstieg der NetIO-Rate zu beobachten ist, suchen Sie nach Netzwerktopologieänderungen, die eine derart massive Abwanderung von Kontrollebenen ausgelöst haben.

Telemetriedatenpfad:

- nicht zutreffend, da die Telemetrie Zählerwerte und nicht Raten streamen muss. Der Accept-Zähler der BGP-bekannten LPTS-Richtlinie kann im Telemetrie Collector verwendet werden, um die durchschnittliche Rate der empfangenen BGP-Pakete von bekannten Peers zu schätzen.

XIPC-Warteschlangen überwachen

Auf dem Punt-Pfad werden Pakete, die NetIO vom LPTS empfängt, an TCP und BGP weitergeleitet. Folgende Warteschlangen müssen überwacht werden:

1. TCP-Warteschlange mit hoher Priorität, über die NetIO Pakete an TCP sendet
2. BGP-Steuerelementwarteschlange
3. BGP-Datenwarteschlange

Auf dem Einspeisepfad werden Pakete über TCP erstellt und an NetIO weitergeleitet. Folgende Warteschlangen müssen überwacht werden:

- OutputL-XIPC-Warteschlange

Befehle:

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

Beispiele:

NetIO zu TCP, vom NetIO-Standpunkt aus gesehen:

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 zu NetIO, vom NetIO-Standpunkt aus gesehen:

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

NetIO zu TCP, vom TCP-Prozessstandpunkt aus gesehen:

<#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 an 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-Datenwarteschlange:

<#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-Kontrollwarteschlange:

```
<#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:
```

Was ist zu beachten?

- es dürfen keine Verluste in relevanten Warteschlangen auftreten
- in XIPC-Warteschlangenstatistiken Hoher Wasserzeichen (HWM) darf 50 % der Warteschlangengröße nicht überschreiten

Um die Entwicklung von Wasserzeichen mit hohem Wert besser verfolgen zu können, müssen Sie den hohen Wasserzeichenwert nach jedem Lesen löschen. Beachten Sie, dass dadurch nicht nur der HWM-Zähler, sondern auch alle Warteschlangenstatistiken gelöscht werden. Das Format des Befehls zum Löschen der XIPC-Warteschlangenstatistik lautet: clear xipcq statistics queue-name <queue_name>

Da der Warteschlangenname häufig die Prozess-ID (PID) enthält, ändert sich der Warteschlangenname nach dem Neustart des Prozesses. Beispiele für Befehle zum Löschen der relevanten Warteschlangenstatistiken:

```
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
```

Telemetriepfad:

- Es gibt keine Telemetrie-Sensorpfade für XIPC.

Überwachen von BGP-Eingangs- und -Ausgangswarteschlangen

BGP unterhält eine Ein- und Ausgabewarteschlange für jeden BGP-Peer. Die Daten befinden sich in InQ, wenn sie vom TCP an das BGP weitergeleitet wurden, jedoch noch nicht vom BGP verarbeitet wurden. Die Daten befinden sich in OutQ, während BGP auf TCP wartet, um die Daten in Pakete aufzuteilen und zu übertragen. Die augenblickliche Größe von BGP InQ/OutQ zeigt gut an, wie beschäftigt der BGP-Prozess ist.

Command:

show bgp <AFI> <SAFI> summary

Beispiel:

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

Zu suchende Elemente:

- Die Größe von InQ/OutQ muss Null sein, wenn das Netzwerk stabil ist. Sie ändert sich schnell, wenn Updates ausgetauscht werden.
- Die InQ/OutQ-Größe darf im Laufe der Zeit nicht monoton zunehmen.

Telemetriepfad:

- Cisco-IOS-XR-ipv4-bgp-oper:bgp

Überwachen der BGP-Nachrichtenraten

Einige BGP-Nachbarn können kontinuierlich Updates oder Abhebungen senden, wenn die Netzwerktopologie instabil ist. Der BGP-RR muss diese Änderung der Routing-Tabelle dann tausendmal auf alle seine RR-Clients replizieren. Daher ist es wichtig, die von Nachbarn empfangenen Nachrichtenraten zu überwachen, um die Quellen von Instabilitäten zu verfolgen.

Command:

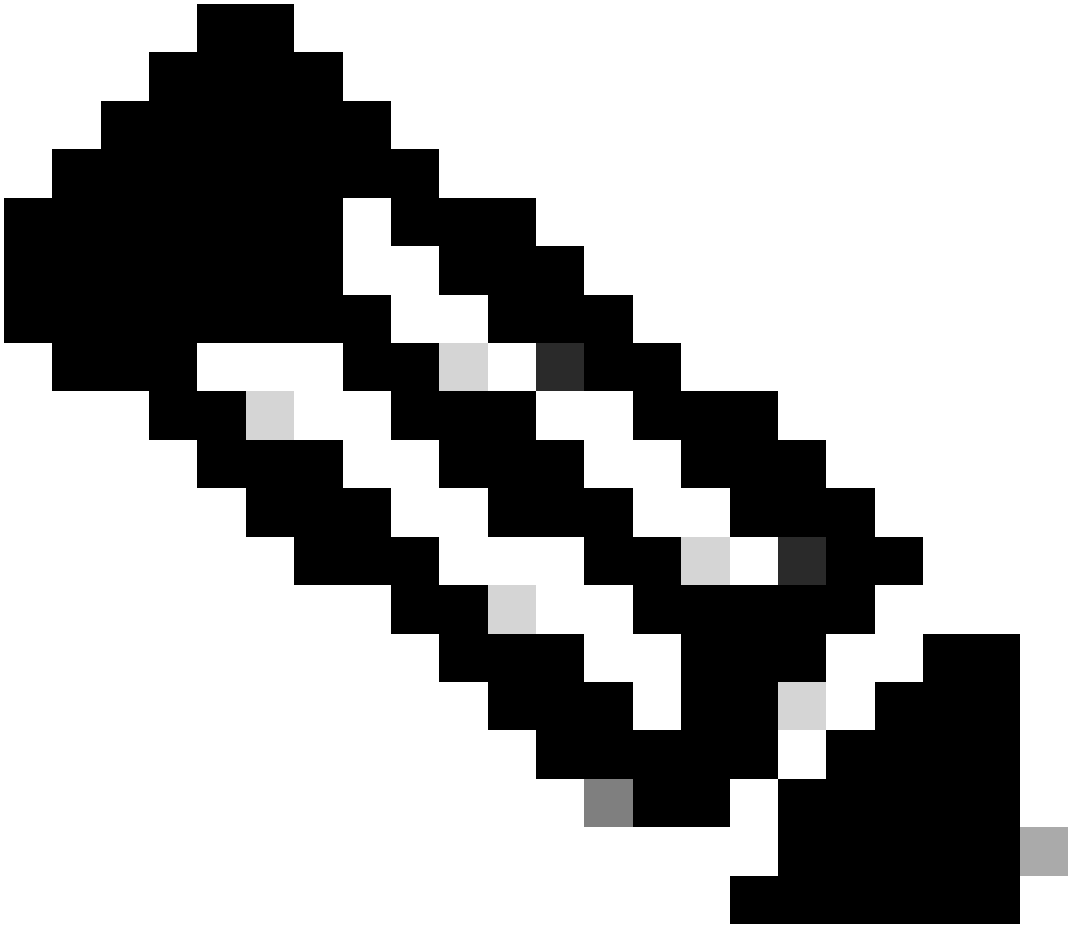
show bgp <AFI> <SAFI> summary

Beispiel:

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-Client-Warteschlangen haben in etwa die gleiche Anzahl von MsgSent, aber einige Nachbarn können eine höhere Anzahl von MsgRcvd haben als andere. Sie müssen mehrere Snapshots dieses Befehls erfassen, um die Rate der Nachrichten zu bewerten.

Nachdem Sie die schädlichen Peers identifiziert haben, können Sie andere Befehle wie **show bgp neighbor <neighbor> detail** und **show bgp neighbor <neighbor> performance-statistics** oder ausführen, **show bgp recent-prefixe**s um zu verstehen, welche Präfixe flattern und ob es sich immer um die gleichen oder um andere Präfixe handelt.



Hinweis: Die Zähler "MsgRcvd" und "MsgSent" sind nach Nachbarn, jedoch nicht nach Adressfamilie geordnet. Wenn Sie also einen Befehl wie ausführen, show bgp all all summary sehen Sie in den Abschnitten für die verschiedenen Adressfamilien die gleichen Zähler für die einzelnen Nachbarn. Sie stellen nicht die Anzahl der Nachrichten dar, die von diesem Nachbarn für diese Adressfamilie empfangen/an diesen Nachbarn gesendet wurden, sondern für alle Adressfamilien.

Überwachung der CPU-Auslastung

Die CPU-Auslastung muss auf jedem Router überwacht werden. Auf einem Router mit einer hohen Anzahl an CPU-Kernen, die der Kontrollebene zugeordnet sind, können einige Messwerte jedoch intuitiv sein. Auf einem BGP-RR mit einer hohen Anzahl von CPU-Kernen, die dem Routing-Prozessor (RP) zugewiesen sind, wie bei der XRv9k-Appliance, werden aktive Threads auf verschiedenen CPU-Kernen ausgeführt, während eine Anzahl von CPU-Kernen inaktiv bleibt. Infolgedessen können einige CPU-Kerne sehr ausgelastet sein, die gesamte CPU-Auslastung, die für alle CPU-Kerne berechnet wird, bleibt jedoch moderat.

Verwenden Sie daher den **show processes cpu thread** Befehl, um die CPU-Kernauslastung über die CLI richtig zu überwachen.

Überwachen von TCP-Statistiken

Cisco IOS® bietet detaillierte Statistiken zu jeder TCP-Sitzung. Der CLI-Befehl **show tcp brief** zeigt eine Liste aller vorhandenen TCP-Sitzungen an. In dieser Zusammenfassung werden für jede TCP-Sitzung folgende Informationen angezeigt:

- **PCB:** Unique TCP Session Identifier
- **VRF-ID**: Die ID der VRF-Instanz, in der die Sitzung stattfindet.
    - Führen Sie den folgenden Befehl aus, um den entsprechenden VRF-Namen anzuzeigen:
    - show cef vrf all summary | utility egrep "^VRF:|Vrfid" | utility egrep -B1 <VRF-ID>
- **Recv-Q:** Momentane Größe der Empfangs-Q. Empfangs-Warteschlange enthält von NetIO empfangene Pakete. Der **tcp**-Prozess extrahiert die Daten aus einem Paket und sendet sie an die entsprechende Anwendung.
- **Send-Q:** Momentane Größe der Sendewarteschlange. Sendewarteschlange enthält Daten, die von einer Anwendung empfangen wurden. Der **tcp**-Prozess teilt die Daten in TCP-Segmente auf (bestimmt durch die ausgehandelte maximale Segmentgröße - TCP MSS), kapselt jedes Segment in einen Layer-3-Header der entsprechenden Adressfamilie (IPv4 oder IPv6) und sendet das Paket an NetIO.
- **Lokale Adresse**: lokale IPv4- oder IPv6-Adresse, die mit dem TCP-Socket verknüpft ist. TCP-Sitzungen im LISTEN-Status sind in der Regel an "**beliebige"** IP-Adressen gebunden, die im Fall von IPv4 bzw. IPv6 als "0.0.0.0" oder "::" dargestellt werden.
- **Foreign-Adresse**: Remote-IPv4- oder -IPv6-Adresse, die dem TCP-Socket zugeordnet ist. TCP-Sitzungen im LISTEN-Status sind in der Regel an "**beliebige"** IP-Adressen gebunden, die im Fall von IPv4 bzw. IPv6 als "0.0.0.0" oder "::" dargestellt werden.
- **Status**: TCP-Sitzungsstatus. Mögliche TCP-Sitzungszustände sind: LISTEN, SYNSENT, SYNRCVD, ESTAB, LASTACK, CLOSING, CLOSEWAIT, FINWAIT1, FINWAIT2, TIMEWAIT, CLOSED.

Da die bekannte BGP-Portnummer 179 ist, können Sie die angezeigten TCP-Sitzungen auf die Sitzungen beschränken, die der BGP-Anwendung zugeordnet sind.

Beispiel:

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

Sie können den angezeigten PCB-Wert verwenden, um die Statistiken für eine bestimmte TCP-Sitzung zu erhalten. CLI-Befehle, die Einblicke in die Statistiken des TCP-Prozesses bieten:

Weltweit:

show tcp statistics clients location <active_RP>

show tcp statistics summary location <active_RP>

Pro Leiterplatte:

show tcp brief | i ":179"

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

show tcp statistics pcb <pcb> location <active_RP>

Globale TCP-Statistikbefehle zeigen den Gesamtzustand von TCP-Sitzungen an. Abgesehen von der Datenpaketstatistik (Eingang/Ausgang) können Sie zum Beispiel sehen, ob es Pakete mit Prüfsummenfehlern, fehlerhafte Pakete, Pakete, die aufgrund von Authentifizierungsfehlern verworfen wurden, ungeordnete Pakete, Pakete mit Daten nach dem Fenster gibt, was Ihnen einen Hinweis auf das Verhalten von TCP-Peers gibt.

In den PCB-Befehlen werden wichtige Parameter einer TCP-Sitzung angezeigt, z. B. MSS, die maximale Round-Trip-Zeit usw.

Die entsprechenden Zähler in der Ausgabe von show tcp detail pcb Befehlen sind:

- **Retrans Timer Starts**: gibt an, wie oft der Timer für die Neuübertragung gestartet wurde.
- **Retrans Timer Wakeups**: gibt an, wie oft der Timer für die Neuübertragung abgelaufen ist, wodurch eine Neuübertragung des TCP-Segments ausgelöst wurde.
- **Aktuelle Größe der Sendewarteschlange in Byte**: unbestätigte Bytes vom Peer.
- **Aktuelle Größe der Empfangswarteschlange in Byte/Paketen:** Byte/Pakete, die noch von der Anwendung (BGP) gelesen werden müssen.
- **Falsch geordnete Bytes:** Bytes, die aufgrund einer Lücke im TCP-Empfangsfenster in der Speicherwarteschlange stehen.

<#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

Überwachung der Speichernutzung

Die BGP-Routing-Tabelle wird im BGP-Prozess-Heap-Speicher gespeichert. Die Routing-Tabelle wird im RIB-Prozess-Heap-Speicher gespeichert.

Nützliche Befehle für die Heap-Speicherüberwachung:

- show memory summary
- show memory summary detail
- show memory-top-consumers
- show memory heap summary all

Telemetriesensor-Pfad:

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

FIB speichert Weiterleitungseinträge im gemeinsam genutzten Speicherplatz.

Nützliche Befehle für die Überwachung des gemeinsamen Speichers:

show memory summary

show memory summary detail

show shmwin summary

Überwachung der BGP-Prozessleistung

Nützlicher Befehl, der interne Daten zur Leistung des BGP-Prozesses bereitstellt:

show bgp process performance-statistics

show bgp process performance-statistics detail

Überwachung der BGP-Konvergenz

Ein weiterer nützlicher Befehl zeigt den Gesamtstatus der BGP-Konvergenz an: show bgp convergence

Wenn das Netzwerk stabil ist, sehen Sie Folgendes:

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

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.