Considerazioni sulla scala BGP RR e monitoraggio KPI

Sommario

Introduzione

Questo documento descrive i principali fattori che contribuiscono alla massima scalabilità che un Border Gateway Protocol (BGP) Route-Reflector (RR) può raggiungere e le linee guida per il monitoraggio delle prestazioni del BGP RR.

Selezione piattaforme hardware/software

Un record di risorse BGP su larga scala non è in genere presente nel percorso di inoltro dei pacchetti che trasportano i servizi forniti da un provider di servizi Internet. Pertanto, i requisiti hardware per un router BGP RR e per i router che inoltrano principalmente i pacchetti nel percorso dati sono diversi. I router standard sono costruiti con un potente elemento di inoltro del percorso dati e un elemento del percorso di controllo relativamente moderato. Un record di risorse BGP esegue tutte le attività in un piano di controllo.
All'interno della famiglia di prodotti Cisco IOS® XR, è possibile scegliere tra 3 tipi di piattaforme HW/SW per un ruolo BGP RR:

Router Cisco IOS XR fisico	Appliance Cisco IOS XRv 9000	Cisco IOS XRv 9000 Router (alias XRv9k)
• Capacità moderata del control plane (generalmente tra 2 e 6 core CPU allocati alla VM RP XR) • Capacità del percorso dati non utilizzata	• Elevata capacità del control plane (sull'appliance Cisco UCS M5 i 36 core CPU sono dedicati a VM RP XR) • Divisione equa tra capacità del percorso dati e del percorso di controllo. • L'immagine XRv9k viene eseguita su barebone per ottenere le massime prestazioni	• Capacità personalizzabile del control plane • Divisione uniforme tra l'alimentazione del percorso dati e del percorso di controllo quando si utilizza l'immagine BGP RR. • Un ulteriore livello di virtualizzazione influisce sulle prestazioni.

Al momento della stesura di questo documento, l'appliance XRv9k è la scelta ottimale per la piattaforma BGP RR, in quanto fornisce la massima capacità del control plane e le massime prestazioni.

Considerazioni Su Scalabilità E Prestazioni

La scala supportata delle entità del piano dati è relativamente facile da esprimere perché le prestazioni dell'elemento del percorso dati dipendono raramente dalla scala. Ad esempio, una ricerca TCAM richiede lo stesso tempo indipendentemente dal numero di voci TCAM attive.
La scala supportata delle entità del piano di controllo è spesso molto più complessa perché la scala e le prestazioni sono interconnesse. Prendiamo in considerazione un record di risorse BGP con 1 milione di route. Il lavoro che un processo BGP deve eseguire per mantenere questa tabella BGP dipende da:

1. Quanti peer BGP sono attivi?
2. Quali famiglie di indirizzi sono attive?

3. In che modo sono distribuiti nei gruppi di aggiornamento?
4. La complessità delle RPL (Route Policies)
5. Frequenza degli aggiornamenti (aggiornamenti in ingresso e aggiornamenti in uscita - intervallo di annunci).
6. TCP MSS, MTU di interfaccia/percorso: la regolazione di questo valore consente di migliorare le prestazioni
7. Se Dual-RP, NSR è abilitato
8. Tutti i peer lenti noti, che non si trovano in un gruppo di aggiornamento separato
9. Valore trigger-delay successivo

Numero di peer BGP

Il numero di peer BGP è solitamente il primo e, sfortunatamente, spesso l'unica cosa che viene in mente quando si considera la scala BGP. Anche se la scala BGP supportata non può essere rappresentata senza menzionare il numero di peer BGP, non è il fattore più importante. Molti altri aspetti sono ugualmente rilevanti.

Famiglie di indirizzi

Il tipo di famiglia di indirizzi (AF, Address Family) è un fattore importante nelle considerazioni sulle prestazioni BGP, in quanto nelle implementazioni tipiche influisce sulle dimensioni di una singola route. Il numero di route IPv4 che possono essere compresse in un singolo segmento TCP è notevolmente superiore al numero di route VPNv4. Pertanto, per le stesse modifiche alla tabella BGP, un record di risorse BGP IPv4 ha meno lavoro da fare rispetto a un record di risorse BGP VPNv4. Ovviamente, nelle implementazioni in cui un numero significativo di comunità viene aggiunto a ogni percorso, la differenza tra le AF diventa meno significativa, ma la dimensione di un singolo percorso è poi ancora più grande e richiede una considerazione.

Numero di gruppi di aggiornamento

Il processo BGP prepara un singolo aggiornamento per tutti i membri dello stesso gruppo di aggiornamento. Il processo TCP suddivide i dati di aggiornamento in un numero richiesto di segmenti TCP (a seconda del valore TCP MSS) verso ciascun membro del gruppo di aggiornamento. Per visualizzare i gruppi di aggiornamento attivi e i relativi membri, utilizzare il show bgp update-group comando. È possibile determinare quali e quanti peer sono membri di un gruppo di aggiornamento creando un criterio in uscita comune per un gruppo di peer che si desidera includere nello stesso gruppo di aggiornamento. Un singolo aggiornamento inviato da BGP RR a un numero elevato di client BGP RR può attivare una frammentazione di ACK TCP che possono essere scartati nel componente Local Packet Transport Service (LPTS) dei router Cisco IOS XR.

Complessità delle RPL (Route Policies)

La complessità delle policy di routing utilizzate da BGP influisce sulle prestazioni del processo BGP. Ogni route ricevuta o inviata deve essere valutata in base ai criteri di route configurati. Un criterio molto lungo richiede molti cicli della CPU da utilizzare per questa azione. I criteri di route che includono un'espressione regolare sono particolarmente complessi da elaborare. Un'espressione regolare consente di esprimere il criterio di route in un numero di righe inferiore, ma richiede più cicli di CPU durante l'elaborazione rispetto al criterio di route equivalente che non utilizza l'espressione regolare.

Frequenza Di Aggiornamento

La frequenza degli aggiornamenti ha un'incidenza importante sulla scala BGP. Il numero di aggiornamenti è spesso difficile da prevedere. È possibile influenzare la frequenza degli aggiornamenti utilizzando il comando "**`advertising-interval`**" per impostare l'intervallo minimo tra l'invio degli aggiornamenti di routing (BGP). Il valore predefinito per i peer iBGP è 0 secondi e 30 per i peer eBGP è 30 secondi.

TCP MSS e MTU interfaccia/percorso

La suddivisione di un aggiornamento in molti segmenti TCP può mettere a dura prova le risorse di processo TCP in un ambiente ad alta scala e ad alta frequenza di aggiornamento. Una MTU del percorso più grande e un TCP MSS più grande sono migliori per le prestazioni BGP e TCP.

NSR su router Dual-RP

L'NSR è una grande funzione per la ridondanza, ma ha un impatto sulle prestazioni BGP. Sui router Cisco IOS XR entrambi gli RP ricevono simultaneamente ogni aggiornamento BGP direttamente dalla NPU sulla scheda di linea in entrata, il che significa che l'RP attivo non deve impiegare tempo per replicare l'aggiornamento all'RP in standby. Tuttavia, ogni aggiornamento generato dall'RP attivo deve essere inviato all'RP in standby e da lì al peer BGP. In questo modo l'RP in standby è sempre aggiornato sui numeri di sequenza e riconoscimento, ma ha un impatto sulle prestazioni BGP complessive. Per questo motivo, si consiglia che un router BGP RR sia un router a RP singola.

Peer lenti

Un peer lento può rallentare gli aggiornamenti verso tutti i membri del gruppo di aggiornamento perché il processo BGP deve mantenere l'aggiornamento nella sua memoria fino a quando tutti i peer non lo riconoscono. Se si è a conoscenza del fatto che alcuni peer sono molto più lenti (ad esempio i router di una parte legacy della rete), separarli in un gruppo di aggiornamento. Per impostazione predefinita, Cisco IOS XR segnala un peer lento tramite un messaggio syslog. È possibile creare peer lenti statici (che non condividono mai il gruppo di aggiornamento con altri utenti) o ottimizzare il comportamento del peer lento dinamico utilizzando il comando di configurazione BGPslow-peer in modalità di configurazione globale o per router adiacenti. Per ulteriori informazioni, vedere il documento sulla risoluzione dei problemi di convergenza BGP lenta a causa di policy di route non ottimali su IOS-XR sul portale Cisco xrdocs.io.

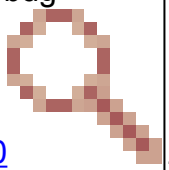
Ritardo trigger Nexthop

Se più hop BGP successivi cambiano in un breve intervallo di tempo e il valore critico di ritardo di attivazione del nexthop pari a zero è configurato in una famiglia di indirizzi (AF) con un numero elevato di route, è necessario eseguire una procedura completa dell'AF a ogni evento di modifica dell'hop successivo. Le ripetute passeggiate di tale AF aumentano il tempo di convergenza nelle famiglie di indirizzi con valori di ritardo di trigger nexthop critici inferiori. Per visualizzare i valori di ritardo del trigger dell'hop successivo, eseguire il comando "show bgp all nexthops".

Esempio di scala BGP RR multidimensionale convalidata

I risultati della scala multidimensionale, in particolare per le feature del piano di controllo, dipendono in modo significativo dall'ambiente di prova specifico. I risultati dei test possono variare in modo significativo se alcuni parametri vengono modificati.

Parametro	Valore	Valore

Piattaforma	Appliance XRv9k (basata su UCS M5)	ASR 9902
IOS XR release	7.5.2 + SMU ombrello per Cisco ID bug  CSCwf09600 . (i componenti di questo SMU sono integrati in Cisco IOS XR versione 7.9.2 e successive)	7.11.2
Peer	VPN eBGP: 2500 VPNv4 iBGP: 1700	VPNv4 iBGP: 2000
Route BGP	Per sessione: 200 Totale: 400k Percorsi per route: 1	Per sessione: 750 VPNv4: 1,36 M VPNv6: 150.000 IPv4: 950 k IPv6: 200 k Totale: circa 2,6 M Percorsi per route: 1
Route IGP	10k (ISIS)	10k (ISIS)
Gruppi di aggiornamento BGP	1	1
Timer BGP	predefinito	predefinito
Frequenza policer noti BGP LPTS	50,000	25,000
configurazione num-thread tcp	16 16	16 16

Dimensione buffer di invio BGP	predefinito	predefinito
Riepilogo indicatori prestazioni chiave (KPI)	• Test case con la massima velocità dei pacchetti di input e output: ◦ Ingresso: 49,4 kpps ◦ Uscita: 95 kpps ◦ ==> Cadute LPTS (policer a 50 kpps) ◦ ==> Nessun calo nei client NetIO ◦ ==> Dimensione massima coda XIPC (BGP): 1362 ◦ ==> Dimensione massima coda XIPC (TCP): 1248	• Test case con la massima velocità dei pacchetti di input: ◦ Ingresso: 16030 pkts/s ◦ Uscita: 31 pkt/s ◦ ==> Nessun calo nei client LPTS o NetIO ◦ ==> Dimensione massima coda XIPC (BGP): 378 ◦ ==> Dimensione massima coda XIPC (TCP): 1021 • Test case con la massima velocità del pacchetto di output: ◦ Ingresso: 12172 pkts/s ◦ Uscita: 23465 pkts/s ◦ ==> Nessun calo nei client LPTS o NetIO ◦ ==> Dimensione massima coda XIPC (BGP): 109 ◦ ==> Dimensione massima coda XIPC

		(TCP): 1518

Considerazioni sulla progettazione

Esistono due approcci al posizionamento di BGP RR nella rete:

- Design BGP RR centralizzato/piatto.
- Progetto BGP RR distribuito/gerarchico.

In un design centralizzato/piatto, tutti i client BGP RR nella rete stabiliscono il peering BGP con un set (di solito una coppia) di dispositivi BGP RR che contengono esattamente le stesse informazioni. Questo approccio è semplice da implementare e funziona bene nelle reti di piccole e medie dimensioni. Qualsiasi modifica nella tabella BGP viene propagata rapidamente a tutti i client BGP RR. Con l'aumento del numero di client BGP RR, la progettazione può raggiungere un limite di scala quando il numero di connessioni TCP sui dispositivi BGP RR aumenta in modo da influire sulle prestazioni.

In una struttura distribuita/gerarchica, la rete è suddivisa in più aree. Tutti i router di una regione stabiliscono il peering BGP con un set (di solito una coppia) di dispositivi BGP RR che contengono esattamente le stesse informazioni. Questi dispositivi BGP RR agiscono da client BGP RR per un altro set di dispositivi BGP RR, in genere una coppia. Questo approccio progettuale consente una facile espansione della rete, mantenendo al contempo il numero di connessioni TCP su ogni singola RR BGP sotto un certo limite.
Un'altra considerazione a livello di progettazione è la personalizzazione dell'ambito dei destinatari degli aggiornamenti BGP. A seconda della distribuzione VRF tra i client BGP RR, vale la pena considerare la distribuzione della route vincolata RT. Se tutti i client BGP RR dispongono di interfacce nello stesso VRF, la distribuzione delle route vincolate RT non comporta molti vantaggi. Tuttavia, se i VRF vengono distribuiti in modo sparso tra tutti i client BGP RR, l'uso di RT Constrained Route Distribution riduce in modo significativo il carico sul processo BGP RR.

Monitoraggio degli indicatori di prestazioni chiave (KPI) BGP

Il monitoraggio degli indicatori di prestazioni chiave (KPI) di BGP RR è importante per garantire il corretto funzionamento della rete.

Un cambiamento significativo nella topologia di rete (ad esempio un link flap del DWDM principale) può attivare aggiornamenti del routing che generano un traffico eccessivo verso e/o dal router BGP RR. Il traffico significativo che colpisce il record di risorse BGP in genere comporta:

- Aggiornamenti dai peer BGP.
- ACK TCP generati dai peer BGP, in risposta agli aggiornamenti inviati da RR BGP e viceversa

In questa sezione del documento viene spiegato l'indicatore KPI che deve essere monitorato su un tipico record di risorse BGP e viene spiegato anche come stabilire quale dei due tipi di traffico BGP significativi sta causando un'alta velocità di controllo del traffico aereo.

Il percorso dei pacchetti BGP all'interno del router può essere rappresentato come segue:

Punt
Controller Ethernet -(packet)-> datapath forwarder -(packet)-> LPTS -(packet)-> SPP -(packet) -> NetIO -(packet)-> TCP -(message)-> BGP
Inserisci
BGP -(messaggio)-> TCP -(pacchetto)-> NetIO -(pacchetto)-> SPP -(pacchetto) -> datapath forwarder -(pacchetto)-> Ethernet controller

Gli indicatori KPI possono essere suddivisi in:

Caratteristiche principali:

- Server d'inoltro datapath
- LPTS (impostazioni dei criteri punt hardware, accetta contatori e contatori drop)
- SPP
- NetIO
- Code IPC (NetIO <=> TCP <=> BGP)
- Dimensioni InQ/OutQ BGP

Facoltativo:

- Utilizzo CPU
- Utilizzo della memoria
- statistiche TCP
- Prestazioni del processo BGP
- Convergenza BGP

Monitor Datapath Forwarder

Su XRv9000 il server di inoltro dei percorsi dati è l'agente DPA (Data Plane Agent), mentre sulle piattaforme ASR9000 è l'np (Network Processor).

Monitorare l'agente DPA XRv9000

Il comando utile per visualizzare il carico e le statistiche di DPA è:

show controllers dpa statistics global

Questo comando mostra tutti i contatori diversi da zero, che forniscono informazioni sul tipo e sul numero di pacchetti inviati dalle interfacce di rete alla CPU RP, iniettati dalla CPU RP verso le interfacce di rete, e sul numero di pacchetti scartati:

<#root>

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

show controllers dpa statistics global

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

Monitor ASR9000 Network Processor (NP)

I comandi utili per visualizzare il carico e le statistiche di ogni NP nel sistema sono:

show controllers np load all

show controllers np counters all

NP su ASR9000 ha un ricco set di contatori che mostrano il numero, la frequenza e il tipo di pacchetti elaborati e scartati,.

<#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
```

Monitoraggio LPTS

Poiché un RR BGP standard non è nel percorso di inoltro, tutti i pacchetti ricevuti sull'interfaccia di rete vengono indirizzati al control-plane. L'elemento data-path su un RR BGP esegue un piccolo numero di semplici operazioni prima che i pacchetti vengano puntati al control-plane. Poiché è improbabile che l'elemento del percorso dati sia un punto di congestione, l'unico elemento della scheda di linea che deve essere monitorato è lo stato LPTS.

Nel caso di XRv9k, le statistiche dell'hardware vengono mappate sul vPP

Comando:

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

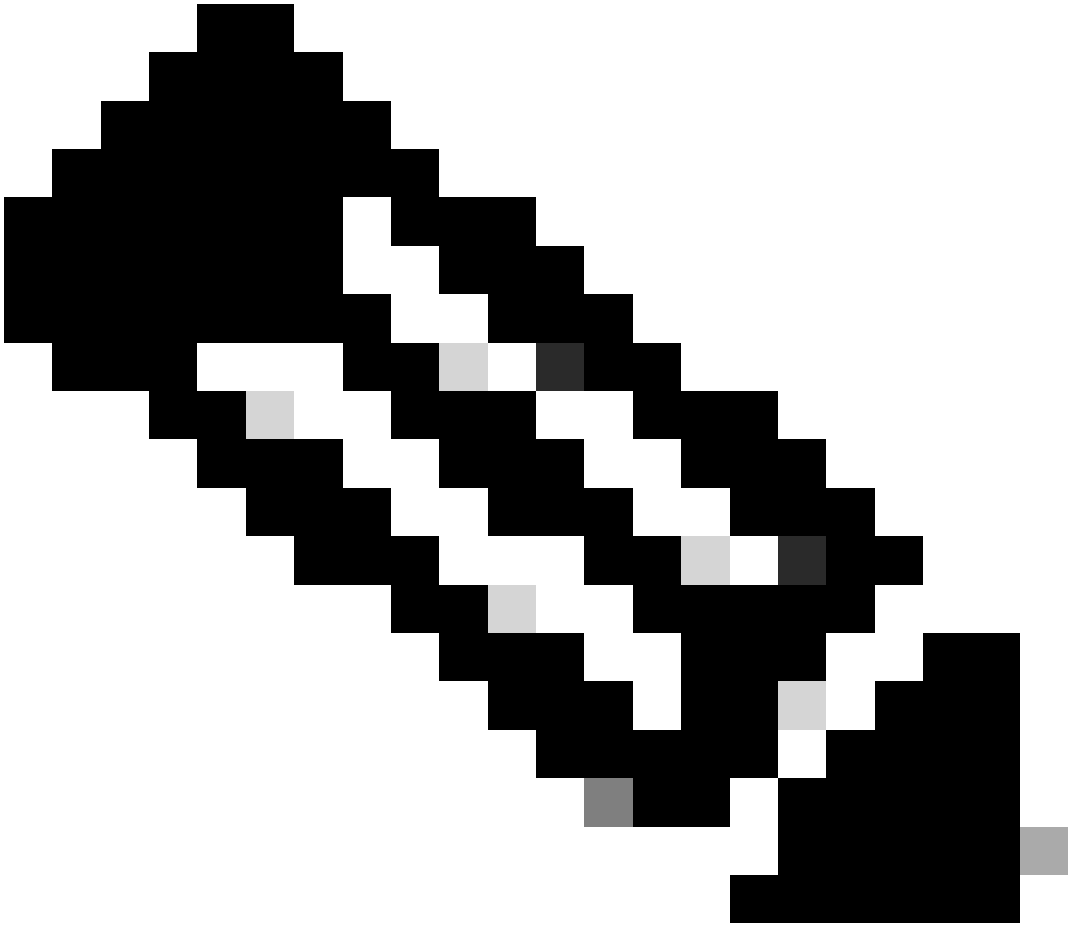
Esempio:

```
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
```

Cosa cercare:
Se si osserva un salto significativo di AggDrops rispetto al tipo di flusso noto BGP, iniziare a cercare le modifiche della topologia di rete che hanno attivato tale cambiamento massiccio del control plane.

Percorso dati di telemetria:

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



Nota: i contatori di stato LPTS possono essere cancellati. Il sistema di monitoraggio deve tenere conto di questa possibilità.

SPP monitor

L'SPP è la prima entità sulla CPU del processore di routing o della scheda di linea che riceve il pacchetto puntato dall'NP o da DPA tramite la struttura interna e l'ultimo punto nell'elaborazione del pacchetto software prima di essere consegnato al fabric per l'iniezione nell'NP o DPA.

Comandi relativi al monitoraggio SPP:

show spp node-counters

show spp client

Il **show spp node-counters** comando mostra la frequenza dei pacchetti puntati/iniettati ed è di facile lettura e comprensione. Per le sessioni BGP, i contatori rilevanti si trovano sotto **client/punt** e **client/inject** sul RP attivo.

La funzione **show spp client** è più ricca di output e offre una visione più dettagliata del numero di pacchetti accodati/scartati verso i client, nonché del limite massimo.

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

Monitorare NetIO

Mentre il policer LPTS mostra solo il conteggio dei pacchetti accettati o scartati da un policer corrispondente, a livello NetIO è possibile vedere la frequenza dei pacchetti puntati alla CPU RP. Poiché su un tipico RR BGP la grande maggioranza dei pacchetti ricevuti sono pacchetti BGP, la velocità complessiva di NetIO indica molto da vicino la velocità dei pacchetti BGP ricevuti.

<#root>

Command:

show netio rates

Esempio:

<#root>

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

show netio rates

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

Cosa cercare:

- Se si osserva un aumento significativo della frequenza NetIO, iniziare a cercare le modifiche della topologia di rete che hanno attivato tale cambiamento massiccio del control plane.

Percorso dati di telemetria:

- non applicabile in quanto la telemetria deve trasmettere i valori dei contatori, non le velocità. Il contatore di accettazione del policer LPTS noto di BGP può essere utilizzato sul collettore di telemetria per approssimare la velocità media dei pacchetti BGP ricevuti da peer noti.

Monitoraggio delle code XIPC

Sul percorso punt, i pacchetti ricevuti da NetIO da LPTS vengono passati a TCP e BGP. È importante monitorare queste code:

1. Coda TCP ad alta priorità attraverso la quale NetIO consegna i pacchetti al TCP
2. Coda di controllo BGP
3. Coda dati BGP

Sul percorso di inserimento, i pacchetti vengono creati dal protocollo TCP e passati a NetIO. È importante monitorare queste code:

- Coda XIPC OutputL

Comandi:

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

Esempi:

Da NetIO a TCP, vista dal punto di vista di NetIO:

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

Da TCP a NetIO, vista dal punto di vista NetIO:

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

Da NetIO a TCP, vista dal punto di vista del processo TCP:

<#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 ------ ----------

Da TCP a 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 ------ ----------

Coda dati BGP:

<#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
```

Coda di controllo BGP:

```
<#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:
```

Cosa cercare:

- non devono esserci cali nelle code rilevanti
- negli stati della coda XIPC il limite massimo (High Watermark, HWM) non deve superare il 50% delle dimensioni della coda

Per tenere traccia in modo più accurato dell'evoluzione del valore di filigrana elevato, è necessario cancellare tale valore dopo ogni lettura. Si noti che questa operazione non cancella solo il contatore HWM, ma cancella anche tutte le statistiche della coda. Il formato del comando per cancellare le statistiche della coda XIPC è: clear xipcq statistics queue-name <queue_name>

Poiché il nome della coda spesso include l'ID processo (PID), il nome della coda cambia dopo il riavvio del processo.
Di seguito sono riportati alcuni esempi di comandi per cancellare le statistiche relative alle code:

```
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
```

Percorso di telemetria:

- Nessun percorso dei sensori di telemetria per XIPC.

Monitoraggio delle code di input e output BGP

BGP mantiene una coda di input e output per ogni peer BGP. I dati risiedono in InQ quando il protocollo TCP li ha passati a BGP, ma BGP non li ha ancora elaborati. I dati risiedono in OutQ mentre BGP attende su TCP di suddividere i dati in pacchetti e trasmetterli. Le dimensioni

istantanee di BGP InQ/OutQ forniscono una buona indicazione di quanto è occupato il processo BGP.

Comando:

show bgp <AFI> <SAFI> summary

Esempio:

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

Cosa cercare:

- Le dimensioni di InQ/OutQ devono essere pari a zero quando la rete è stabile. Cambia rapidamente quando si scambiano gli aggiornamenti.
- Le dimensioni di InQ/OutQ non devono aumentare in modo monotono nel tempo.

Percorso di telemetria:

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

Monitoraggio delle velocità dei messaggi BGP

Alcuni router BGP adiacenti possono inviare continuamente aggiornamenti o ritiri se la topologia di rete è instabile. Il record di risorse BGP deve quindi replicare tale tabella di routing per migliaia di volte in tutti i relativi client di risorse. Pertanto è importante monitorare le frequenze dei messaggi ricevuti dai vicini, per tenere traccia delle fonti di instabilità.

Comando:

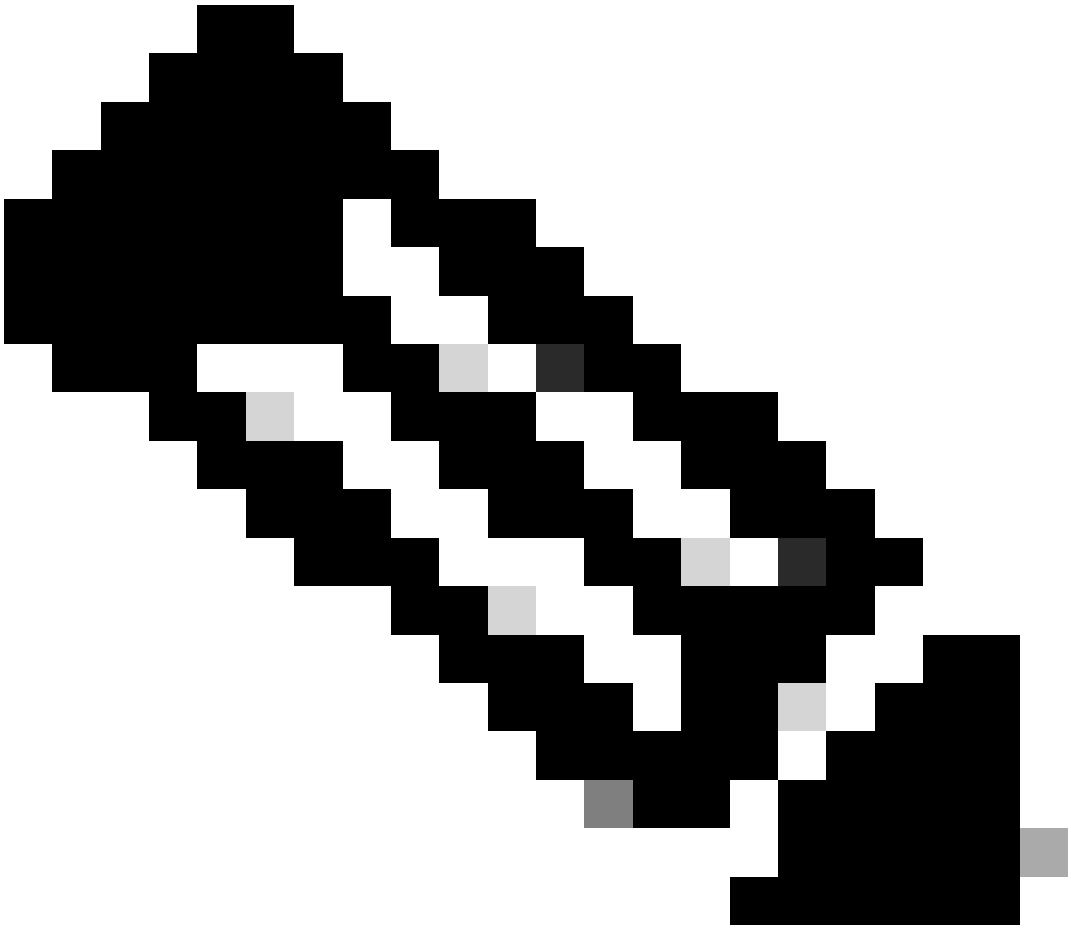
show bgp <AFI> <SAFI> summary

Esempio:

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

Le code dei client RR hanno all'incirca la stessa quantità di messaggi MsgSent, ma alcuni router adiacenti possono avere un numero di messaggi MsgRcvd superiore ad altri. È necessario acquisire più snapshot di questo comando per valutare la frequenza dei messaggi.

Una volta identificati i peer che causano l'errore, è possibile eseguire altri comandi come **show bgp neighbor <neighbor> detail** and **show bgp neighbor <neighbor> performance-statistics** o **show bgp recent-prefixe**s per cercare di capire quali prefissi stanno lampeggiando e se sono sempre gli stessi o diversi.



Nota: i contatori MsgRcvd e MsgSent sono per router adiacente ma non per famiglia di indirizzi. Quando si esegue un comando simile show bgp all all summary , nelle sezioni relative alle varie famiglie di indirizzi vengono visualizzati gli stessi contatori per ogni vicino. Non rappresentano il numero di messaggi ricevuti/inviati da/a quel vicino per quella famiglia di indirizzi ma tra più famiglie di indirizzi.

Monitoraggio utilizzo CPU

L'utilizzo della CPU deve essere monitorato su ogni router, ma su un router con un numero elevato di core CPU dedicati al control plane alcuni passaggi possono non essere intuitivi. In un record di risorse BGP con un numero elevato di core CPU dedicati al processore di routing (RP), come nel caso dell'accessorio XRv9k, i thread attivi vengono eseguiti su core CPU diversi, mentre un numero di core CPU rimane inattivo. Di conseguenza, alcuni core CPU possono essere molto occupati, ma l'utilizzo complessivo della CPU calcolato per tutti i core CPU rimane moderato.

Pertanto, per il corretto monitoraggio dell'utilizzo dei core CPU tramite CLI, utilizzare il **show processes cpu thread** comando.

Monitoraggio delle statistiche TCP

Cisco IOS® gestisce statistiche dettagliate su ciascuna sessione TCP. Il comando CLI **show tcp brief** visualizza l'elenco di tutte le sessioni TCP esistenti. In questo output di riepilogo, per ogni sessione TCP è possibile visualizzare le seguenti informazioni:

- **PCB:** identificatore univoco della sessione TCP.
- **VRF-ID**: l'ID del VRF in cui si trova la sessione.
    - Per visualizzare il nome VRF corrispondente, eseguire questo comando:
    - show cef vrf all summary | utility egrep "^VRF:|Vrfid" | utility egrep -B1 <VRF-ID>
- **Recv-Q**: dimensioni istantanee della coda di ricezione Q. La coda di ricezione contiene i pacchetti ricevuti da NetIO. Il processo **tcp** estrae i dati da un pacchetto e li invia all'applicazione corrispondente.
- **Send-Q**: dimensione istantanea della coda di invio. La coda di invio contiene i dati ricevuti da un'applicazione. Il processo **tcp** suddivide i dati in segmenti TCP (determinati dalle dimensioni massime del segmento negoziate - TCP MSS), incapsula ogni segmento in un'intestazione di layer 3 della famiglia di indirizzi corrispondente (IPv4 o IPv6) e invia il pacchetto a NetIO.
- **Indirizzo locale**: indirizzo IPv4 o IPv6 locale associato al socket TCP. Le sessioni TCP in stato LISTEN sono in genere associate a un indirizzo IP "**any**", rappresentato rispettivamente come "0.0.0.0" o "::" in caso di IPv4 o IPv6.
- **Indirizzo esterno**: indirizzo IPv4 o IPv6 remoto associato al socket TCP. Le sessioni TCP in stato LISTEN sono in genere associate a un indirizzo IP "**any**", rappresentato rispettivamente come "0.0.0.0" o "::" in caso di IPv4 o IPv6.
- **Stato**: lo stato della sessione TCP. Gli stati possibili della sessione TCP sono: LISTEN, SYNSENT, SYNRCVD, ESTAB, LASTACK, CLOSING, CLOSEWAIT, FINWAIT1, FINWAIT2, TIMEWAIT, CLOSED.

Poiché il numero di porta BGP noto è 179, è possibile limitare le sessioni TCP visualizzate a quelle associate all'applicazione BGP.

Esempio:

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

È possibile utilizzare il valore di PCB visualizzato per ottenere le statistiche per una particolare sessione TCP. Comandi CLI che forniscono informazioni dettagliate sulle statistiche dei processi TCP:

Globale:

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>

I comandi delle statistiche TCP globali mostrano lo stato complessivo delle sessioni TCP. A parte le statistiche dei pacchetti di dati (in/out), è possibile vedere per esempio se ci sono pacchetti con errori di checksum, pacchetti in formato non valido, pacchetti scartati a causa di errori di autenticazione, pacchetti non ordinati, pacchetti con dati dopo finestra, che dà un'indicazione del comportamento dei peer TCP.

Nei comandi per PCB, è possibile visualizzare parametri importanti di una sessione TCP, come MSS, tempo massimo di andata e ritorno e così via.

I contatori rilevanti nell'output del show tcp detail pcb comando sono:

- **Avvio timer ritrasmissione**: indica quante volte è stato avviato il timer di ritrasmissione.
- **Retrans Timer Wakeups**: indica quante volte si è esaurito il timer di ritrasmissione, attivando una ritrasmissione del segmento TCP.
- **Dimensioni correnti della coda di invio in byte**: byte non riconosciuti dal peer.
- **Dimensioni correnti della coda di ricezione in byte/pacchetti**: byte/pacchetti non ancora letti dall'applicazione (BGP).
- **byte non ordinati**: byte accodati nella coda di salvataggio a causa di un buco nella finestra di ricezione TCP.

<#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

Monitoraggio dell'utilizzo della memoria

La tabella delle route BGP è archiviata nella memoria heap del processo BGP. La tabella di routing viene archiviata nella memoria heap del processo RIB.

Comandi utili per il monitoraggio della memoria heap:

show memory summary

show memory summary detail

show memory-top-consumers

show memory heap summary all

Percorso sensore di telemetria:

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

FIB memorizza le voci di inoltro nello spazio di memoria condivisa.

Comandi utili per il monitoraggio della memoria condivisa:

show memory summary

show memory summary detail

show shmwin summary

Monitoraggio delle prestazioni dei processi BGP

Comando utile che fornisce dati interni sulle prestazioni del processo BGP:

show bgp process performance-statistics

show bgp process performance-statistics detail

Convergenza Monitor BGP

Un altro comando utile è quello che mostra lo stato generale della convergenza BGP: show bgp convergence

Quando la rete è stabile, si può vedere qualcosa come questo:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).