Consideraciones de la Escala RR BGP y Monitoreo KPI

Contenido

Introducción

Este documento describe los principales contribuyentes a la escala máxima que un Border Gateway Protocol (BGP) Route-Reflectors (RR) puede alcanzar y guía sobre la supervisión del rendimiento de BGP RR.

Selección de plataforma de HW/SW

Un RR BGP de gran escala no suele estar en la ruta de reenvío de paquetes que transportan servicios proporcionados por un proveedor de servicios de Internet. Por lo tanto, los requisitos de hardware para un RR BGP y los routers que están reenviando predominantemente paquetes en la trayectoria de datos son diferentes. Los routers estándar están construidos con un poderoso elemento de reenvío de trayectoria de datos y un elemento de trayectoria de control relativamente moderado. Un RR BGP realiza todas sus tareas en un plan de control.
Dentro de la familia de productos Cisco IOS® XR, puede elegir entre 3 tipos de plataformas de HW/SW para un rol de RR BGP:

Router físico Cisco IOS XR	Dispositivo Cisco IOS XRv 9000	Router Cisco IOS XRv 9000 (también conocido como XRv9k)
• Capacidad de plano de control moderada (normalmente entre 2 y 6 núcleos de CPU asignados a la máquina virtual RP XR) • Capacidad de ruta de datos no utilizada	• Gran capacidad del plano de control (en los dispositivos basados en Cisco UCS M5, 36 núcleos de CPU están dedicados a RP XR VM) • División equitativa entre la capacidad de ruta de datos y de ruta de control. • La imagen del XRv9k se ejecuta en la estructura básica para obtener el máximo rendimiento	• Capacidad de plano de control personalizable • División igual entre la potencia de la ruta de datos y la de la ruta de control cuando se utiliza la imagen RR BGP. • Una capa adicional de virtualización afecta al rendimiento.

Al momento de escribir esto, el dispositivo XRv9k es la opción de plataforma óptima para BGP RR porque proporciona la mayor capacidad del plano de control con el máximo rendimiento.

Consideraciones De Escalabilidad Y Rendimiento

La escala admitida de entidades de plano de datos es relativamente fácil de expresar porque el rendimiento del elemento de ruta de datos rara vez depende de la escala. Por ejemplo, una búsqueda TCAM toma el mismo tiempo independientemente del número de entradas TCAM activas.
La escala admitida de entidades del plano de control suele ser mucho más compleja porque la escala y el rendimiento están interconectados. Considere un RR BGP con rutas 1M. El trabajo que debe realizar un proceso BGP para mantener esta tabla BGP depende de:

1. ¿Cuántos peers BGP están activos?

2. ¿Qué familias de direcciones están activas?
3. ¿Cómo se distribuyen en grupos de actualización?
4. La complejidad de los RPL (políticas de ruta)
5. Frecuencia de actualizaciones (actualizaciones entrantes y también actualizaciones salientes: intervalo de anuncio).
6. TCP MSS, MTU de interfaz/ruta: ajustar esto ayudará a mejorar el rendimiento
7. Si el procesador de routing dual está activado, NSR
8. Cualquier par lento conocido que no esté en un grupo de actualización separado
9. Valor de retraso del desencadenador del siguiente salto

Número de Peers BGP

El número de peers BGP suele ser el primero y, desafortunadamente, a menudo es lo único que viene a la mente al considerar la escala BGP. Aunque la escala BGP soportada no puede representarse sin mencionar el número de peers BGP, no es el factor más importante. Muchos otros aspectos son igualmente pertinentes.

Familias de direcciones

El tipo de familia de direcciones (AF) es un factor importante en las consideraciones de rendimiento de BGP, ya que en las implementaciones típicas afecta al tamaño de una única ruta. El número de rutas IPv4 que se pueden empaquetar en un solo segmento TCP es significativamente mayor que el número de rutas VPNv4. Por lo tanto, para la misma escala de cambios en la tabla BGP, un RR BGP IPv4 tiene menos trabajo que hacer en comparación con un RR BGP VPNv4. Obviamente, en las implementaciones en las que se agrega un número significativo de comunidades a cada ruta, la diferencia entre AF se vuelve menos significativa, pero el tamaño de una sola ruta es aún mayor y requiere consideración.

Número De Grupos De Actualización

El proceso BGP prepara una única actualización para todos los miembros del mismo grupo de actualización. Luego, el proceso TCP divide los datos de actualización en un número requerido de segmentos TCP (dependiendo de TCP MSS) hacia cada miembro del grupo de actualización. Puede ver los grupos de actualización activos y sus miembros mediante el show bgp update-group comando. Puede influir en qué pares y cuántos son miembros de un grupo de actualización creando una política de salida común para un grupo de pares que desea que estén en el mismo grupo de actualización. Una sola actualización enviada por el RR BGP a un número elevado de clientes RR BGP puede desencadenar una ráfaga de ACK TCP que se puede descartar en el componente Servicio de transporte de paquetes locales (LPTS) de los routers Cisco IOS XR.

Complejidad de RPL (políticas de ruta)

La complejidad de las políticas de ruta utilizadas por BGP afecta el rendimiento del proceso BGP. Todas las rutas recibidas o enviadas deben evaluarse con respecto a la política de rutas configurada. Una política muy larga requiere que se gasten muchos ciclos de CPU en esta acción. Una política de ruta que incluye una expresión regular es especialmente pesada en el procesamiento. Una expresión regular ayuda a expresar la política de ruta en un número menor de líneas, pero requiere más ciclos de CPU durante el procesamiento que la política de ruta equivalente que no utiliza la expresión regular.

Frecuencia De Actualizaciones

La frecuencia de las actualizaciones tiene una influencia importante en la escala BGP. El número de actualizaciones suele ser difícil de predecir. Puede influir en la frecuencia de las actualizaciones mediante el comando "**`advertisement-interval`**", que establece el intervalo mínimo entre el envío de actualizaciones de ruteo (BGP). El valor predeterminado para los peers iBGP es 0 segundos y 30 para los peers eBGP es 30 segundos.

TCP MSS y MTU de interfaz/ruta

La división de una actualización en muchos segmentos TCP puede ejercer mucha presión sobre los recursos de proceso TCP en un entorno de alta frecuencia y gran escala de actualización. Una MTU de trayecto más grande y un TCP MSS más grande son mejores para el rendimiento de BGP y TCP.

NSR en routers Dual-RP

El NSR es una gran función para la redundancia, pero tiene un impacto en el rendimiento de BGP. En los routers Cisco IOS XR, ambos RP reciben simultáneamente cada actualización de BGP directamente desde la NPU en la tarjeta de línea de ingreso, lo que significa que el RP activo no tiene que dedicar tiempo a replicar la actualización en el RP en espera. Sin embargo, cada actualización generada por el RP activo debe enviarse al RP en espera y, desde allí, al par BGP. Esto permite que el RP en espera esté siempre actualizado en los números de secuencia y reconocimiento, pero tiene un impacto en el rendimiento general de BGP. Esta es la razón por la que se recomienda que un RR BGP sea un router de RP único.

Peers lentos

Un peer lento puede ralentizar las actualizaciones hacia todos los miembros del grupo de actualización porque el proceso BGP debe mantener la actualización en su memoria hasta que todos los peers la hayan reconocido. Si sabe que algunos pares son mucho más lentos (por ejemplo, routers en una parte heredada de la red), sepárelos por adelantado en un grupo de actualización. De forma predeterminada, Cisco IOS XR informa un par lento a través del mensaje syslog. Puede crear peers lentos estáticos (que nunca comparten el grupo de actualización con otros) o ajustar el comportamiento del peer lento dinámico mediante el comando de configuración BGPslow-peer en el modo de configuración global o por vecino. Se puede encontrar una buena lectura adicional sobre esto en Resolución de Problemas de Convergencia Lenta de BGP Debido a Políticas de Ruta Subóptimas en IOS-XR en el portal xrdocs.io de Cisco.

Nexthop trigger-delay

Si varios saltos siguientes BGP cambian en un intervalo de tiempo corto y el valor crítico de demora de disparador de salto siguiente de cero se configura en una familia de direcciones (AF) con un número alto de rutas, se debe ejecutar un recorrido completo del AF en cada evento de cambio de salto siguiente. Los recorridos repetidos de ese AF aumentan el tiempo de convergencia en las familias de direcciones con valores críticos de retardo de activación de próximo salto más bajos. Puede ver los valores de retardo de disparador de siguiente salto ejecutando el comando "show bgp all nexthops".

Ejemplo de Escala de RR BGP Multidimensional Validada

Los resultados de la escala multidimensional, especialmente para las funciones del plano de control, dependen en gran medida del entorno de prueba específico. Los resultados de las pruebas pueden variar considerablemente si se modifican algunos de los parámetros.

Parámetro	Valor	Valor
Platform	Dispositivo XRv9k (basado en UCS M5)	ASR9902
versión IOS XR	7.5.2 + SMU paraguas para el ID de bug de Cisco CSCwf09600 . (los componentes de esta SMU paraguas están integrados en Cisco IOS XR versión 7.9.2 y posteriores)	7.11.2
Pares	VPNv4 eBGP: 2500 iBGP VPNv4: 1700	iBGP VPNv4: 2000
Rutas BGP	Por sesión: 200 Total: 400 000 Rutas por ruta: 1	Por sesión: 750 VPNv4: 1,36 millones VPNv6: 150 000 IPv4: 950 000 IPv6: 200 000 Total: ~2,6 millones Rutas por ruta: 1
Rutas IGP	10 000 (ISIS)	10 000 (ISIS)
Grupos de actualización BGP	1	1
Temporizadores BGP	predeterminado	predeterminado
LPTS BGP-known policer rate	50,000	25,000

tcp num-thread configuration	16 16	16 16
BGP send-buffer-size	predeterminado	predeterminado
Resumen de indicadores clave de rendimiento (KPI)	• Caso de prueba con la mayor velocidad de paquetes de entrada y salida: ◦ Entrada: 49,4 kpps ◦ Salida: 95 kpps ◦ ==> caídas de LPTS (regulador a 50 kpps) ◦ ==> Sin caídas en clientes NetIO ◦ ==> Tamaño máximo de cola XIPC (BGP): 1362 ◦ ==> Tamaño máximo de cola XIPC (TCP): 1248	• Caso de prueba con la mayor velocidad de paquetes de entrada: ◦ Entrada: 16030 paquetes/s ◦ Salida: 31 pkts/s ◦ ==> Sin caídas en clientes LPTS ni NetIO ◦ ==> Tamaño máximo de cola XIPC (BGP): 378 ◦ ==> Tamaño máximo de cola XIPC (TCP): 1021 • Caso de prueba con la mayor velocidad de paquetes de salida: ◦ Entrada: 12172 paquetes/s ◦ Salida: 23465 pkts/s ◦ ==> Sin caídas en clientes LPTS ni NetIO ◦ ==> Tamaño máximo de cola XIPC

		(BGP): 109 ==> Tamaño máximo de cola XIPC (TCP): 1518

Aspectos del diseño

Existen dos enfoques para la colocación de BGP RR en la red:

- Diseño de RR BGP plano/centralizado.
- Diseño de RR BGP distribuido/jerárquico.

En un diseño centralizado/plano, todos los clientes BGP RR en la red establecen el peering BGP con un conjunto (generalmente un par) de dispositivos BGP RR que contienen exactamente la misma información. Este enfoque es fácil de implementar y funciona bien en redes de escala pequeña o moderada. Cualquier cambio en la tabla BGP se propaga rápidamente a todos los clientes BGP RR. A medida que crece el número de clientes BGP RR, el diseño puede alcanzar un límite de escala cuando el número de conexiones TCP en los dispositivos BGP RR crece en la medida en que su rendimiento se ve afectado.

En un diseño distribuido/jerárquico, la red se divide en varias regiones. Todos los routers de una región establecen el peering BGP con un conjunto (generalmente un par) de dispositivos BGP RR que contienen exactamente la misma información. Estos dispositivos RR BGP actúan como clientes RR BGP a otro conjunto (normalmente un par) de dispositivos RR BGP. Este enfoque de diseño permite una fácil expansión de la red, al tiempo que mantiene el número de conexiones TCP en cada RR BGP individual bajo cierto límite.
Otra consideración de diseño es adaptar el alcance de los destinatarios de las actualizaciones de BGP. Dependiendo de la distribución VRF entre los clientes BGP RR, vale la pena considerar la distribución de rutas restringidas RT. Si todos los clientes BGP RR tienen interfaces en el mismo VRF, la Distribución de Rutas Restringidas RT no aporta muchos beneficios. Sin embargo, si los VRF se distribuyen escasamente entre todos los clientes RR BGP, el uso de la distribución de ruta restringida RT reduce$f$ significativamente la carga en el proceso bgp en el RR BGP.

Supervisar los indicadores clave de rendimiento (KPI) de BGP

La supervisión de los indicadores clave de rendimiento (KPI) de RR BGP es importante para garantizar el funcionamiento correcto de la red.

Un cambio significativo en la topología de la red (por ejemplo, una inestabilidad de enlace de DWDM importante) puede desencadenar actualizaciones de routing que generan un tráfico excesivo hacia y/o desde el RR BGP. El tráfico significativo que llega al RR BGP normalmente lleva:

- Actualizaciones de peers BGP.
- TCP ACK generados por los peers BGP, en respuesta a las actualizaciones enviadas por BGP RR y viceversa

Esta sección del documento explica el KPI que se debe monitorear en un RR BGP típico y también cómo saber cuál de los dos tipos de tráfico BGP significativos está causando una alta velocidad de tráfico del plano de control.

La trayectoria de los paquetes BGP dentro del router se puede representar de la siguiente manera:

Punt
Controlador Ethernet -(packet)-> reenviador de ruta de datos -(packet)-> LPTS -(packet)-> SPP -(packet) -> NetIO -(packet)-> TCP -(message)-> BGP
Inyectar
BGP -(mensaje)-> TCP -(paquete)-> NetIO -(paquete)-> SPP -(paquete) -> reenviador de ruta de datos -(paquete)-> controlador Ethernet

Los KPI se pueden dividir en:

Aspectos básicos:

- Datapath Forwarder
- LPTS (configuración de controladores de punt de hardware, aceptación de contadores y contadores de caídas)
- SPP
- NetIO
- Colas IPC (NetIO <==> TCP <==> BGP)
- Tamaños de BGP InQ/OutQ

Opcional:

- utilización de CPU
- Uso de memoria
- estadísticas de TCP
- rendimiento del proceso BGP
- convergencia BGP

Monitor Datapath Forwarder

En el XRv9000, el reenviador de ruta de datos es el agente de plano de datos (DPA), mientras que en las plataformas ASR9000 es el procesador de red (NP).

Supervisión del agente de plano de datos (DPA) XRv9000

El comando útil para ver la carga y las estadísticas del DPA es:

show controllers dpa statistics global

Este comando muestra todos los contadores distintos de cero, que le proporcionan información sobre el tipo y el número de paquetes impulsados desde las interfaces de red a la CPU del RP, inyectados desde la CPU del RP hacia las interfaces de red, y el número de paquetes descartados:

<#root>

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

show controllers dpa statistics global

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

Supervisión del procesador de red (NP) ASR9000

Los comandos útiles para ver la carga y las estadísticas de cada NP en el sistema son:

show controllers np load all

show controllers np counters all

NP en ASR9000 tiene un amplio conjunto de contadores que le muestran el número, la velocidad y el tipo de paquetes procesados y descartados.

<#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
```

Supervisar LPTS

Como un RR BGP estándar no está en el trayecto de reenvío, todos los paquetes recibidos en la interfaz de red se envían al plano de control. El elemento de trayectoria de datos en un RR BGP realiza un pequeño número de operaciones simples antes de que los paquetes sean impulsados al plano de control. Dado que es poco probable que el elemento de trayectoria de datos sea un punto de congestión, el único elemento de la tarjeta de línea que necesita supervisión son las estadísticas LPTS.

Tenga en cuenta que, en el caso del XRv9k, las estadísticas de hardware se asignan al vPP

Comando:

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

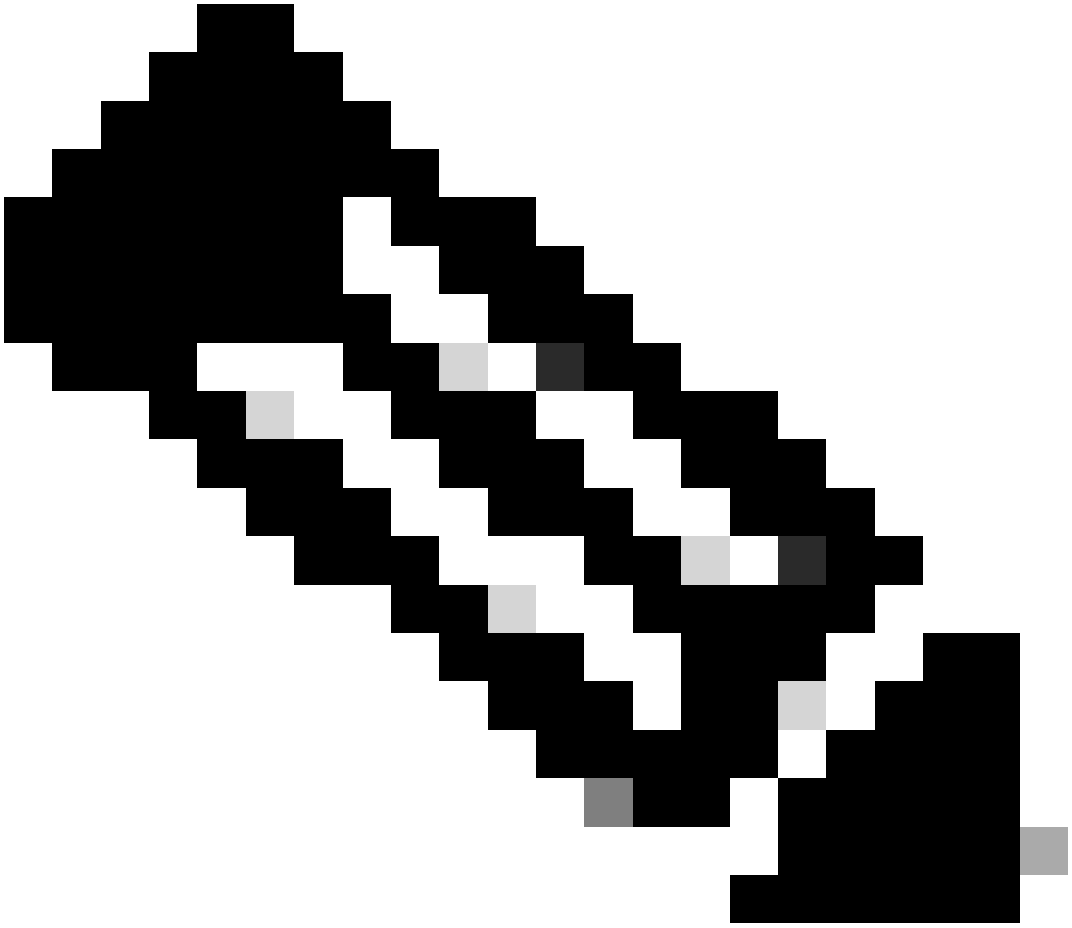
Ejemplo:

```
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
```

Qué buscar:
Si se observa un salto significativo en AggDrops contra el tipo de flujo conocido de BGP, comience a buscar cambios en la topología de la red que hayan desencadenado tal agitación masiva del plano de control.

Ruta de datos de telemetría:

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



Nota: Los contadores de estadísticas LPTS se pueden borrar. Su sistema de supervisión debe tener en cuenta esta posibilidad.

Supervisar SPP

SPP es la primera entidad en el procesador de ruta o la CPU de la tarjeta de línea que recibe el paquete impulsado desde el NP o DPA a través del entramado interno, y el último punto en el procesamiento de paquetes de software antes de que se entregue al entramado para su inyección en el NP o DPA.

Comandos relevantes para el monitoreo SPP:

show spp node-counters

show spp client

El **show spp node-counters** comando muestra la velocidad de los paquetes punteados/inyectados y es fácil de leer y comprender. Para las sesiones BGP, los contadores relevantes se encuentran bajo **client/pun**t y **client/inject** en el RP activo.

El **show spp client** es más rico en resultados y ofrece una perspectiva más detallada del número de paquetes en cola/descartados hacia los clientes, así como la marca de agua alta.

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

Supervisar NetIO

Mientras que el regulador LPTS sólo muestra el conteo de paquetes aceptados o descartados por un regulador correspondiente, en el nivel de NetIO podemos ver la velocidad de paquetes impulsados a la CPU RP. Dado que en un RR BGP típico la gran mayoría de los paquetes recibidos son paquetes BGP, la velocidad NetIO general indica muy de cerca la velocidad de los paquetes BGP recibidos.

<#root>

Command:

show netio rates

Ejemplo:

<#root>

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

show netio rates

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

Qué buscar:

- Si se observa un salto significativo en la velocidad de NetIO, comience a buscar cambios en la topología de la red que hayan desencadenado tal agitación masiva del plano de control.

Ruta de datos de telemetría:

- no se puede aplicar ya que la telemetría debe transmitir valores de contador, no velocidades. El contador de aceptación del regulador LPTS conocido por BGP se puede utilizar en el colector de telemetría para aproximar la velocidad promedio de paquetes BGP recibidos de pares conocidos.

Supervisar colas XIPC

En el trayecto de punt, los paquetes recibidos por NetIO desde LPTS se pasan a TCP y BGP. Es importante supervisar estas colas:

1. Cola de alta prioridad TCP a través de la cual NetIO entrega paquetes a TCP
2. Cola de control BGP
3. Cola de datos BGP

En el trayecto de inyección, los paquetes son creados por TCP y pasados a NetIO. Es importante supervisar estas colas:

- Cola XIPC OutputL

Comandos:

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

Examples:

NetIO a TCP, vista desde el punto de vista de 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

TCP a NetIO, vista desde el punto de vista de NetIO:

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

NetIO a TCP, vista desde el punto de vista del proceso 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 ------ ----------

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 ------ ----------

Cola de datos 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
```

Cola de control 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:
```

Qué buscar:

- no debe haber caídas en las colas relevantes
- en estadísticas de cola XIPC La marca de agua alta (HWM) no debe superar el 50% del tamaño de la cola

Para realizar un mejor seguimiento de la evolución de los valores de marca de agua altos, debe borrar el valor de marca de agua alta después de cada lectura. Tenga en cuenta que esto no borra solamente el contador HWM, sino que también borra todas las estadísticas de cola. El formato del comando para borrar las estadísticas de cola XIPC es: clear xipcq statistics queue-name <queue_name>

Como el nombre de la cola suele incluir el ID de proceso (PID), el nombre de la cola cambia después de reiniciar el proceso.
Algunos ejemplos de comandos para borrar las estadísticas de colas relevantes:

```
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
```

Ruta de telemetría:

- No hay rutas de sensor de telemetría para XIPC.

Supervisar las colas de entrada y salida BGP

BGP mantiene una cola de entrada y salida para cada par BGP. Los datos se ubican en InQ cuando TCP los ha pasado a BGP, pero BGP aún no los ha procesado. Los datos se ubican en OutQ mientras BGP espera en TCP para dividir los datos en paquetes y transmitirlos. El tamaño

instantáneo de BGP InQ/OutQ proporciona una buena indicación de cuán ocupado está el proceso BGP.

Comando:

show bgp <AFI> <SAFI> summary

Ejemplo:

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

Qué buscar:

- El tamaño de InQ/OutQ debe ser cero cuando la red está estable. Cambia rápidamente cuando se intercambian actualizaciones.
- El tamaño de InQ/OutQ no debe aumentar monótonamente con el tiempo.

Ruta de telemetría:

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

Supervisar velocidades de mensajes BGP

Algunos vecinos BGP pueden enviar continuamente actualizaciones o retiros si la topología de red es inestable. El RR BGP debe entonces replicar dicho cambio de tabla de ruteo miles de veces a todos sus clientes RR. Por lo tanto, es importante monitorear las tasas de mensajes recibidos de los vecinos, para rastrear las fuentes de inestabilidades.

Comando:

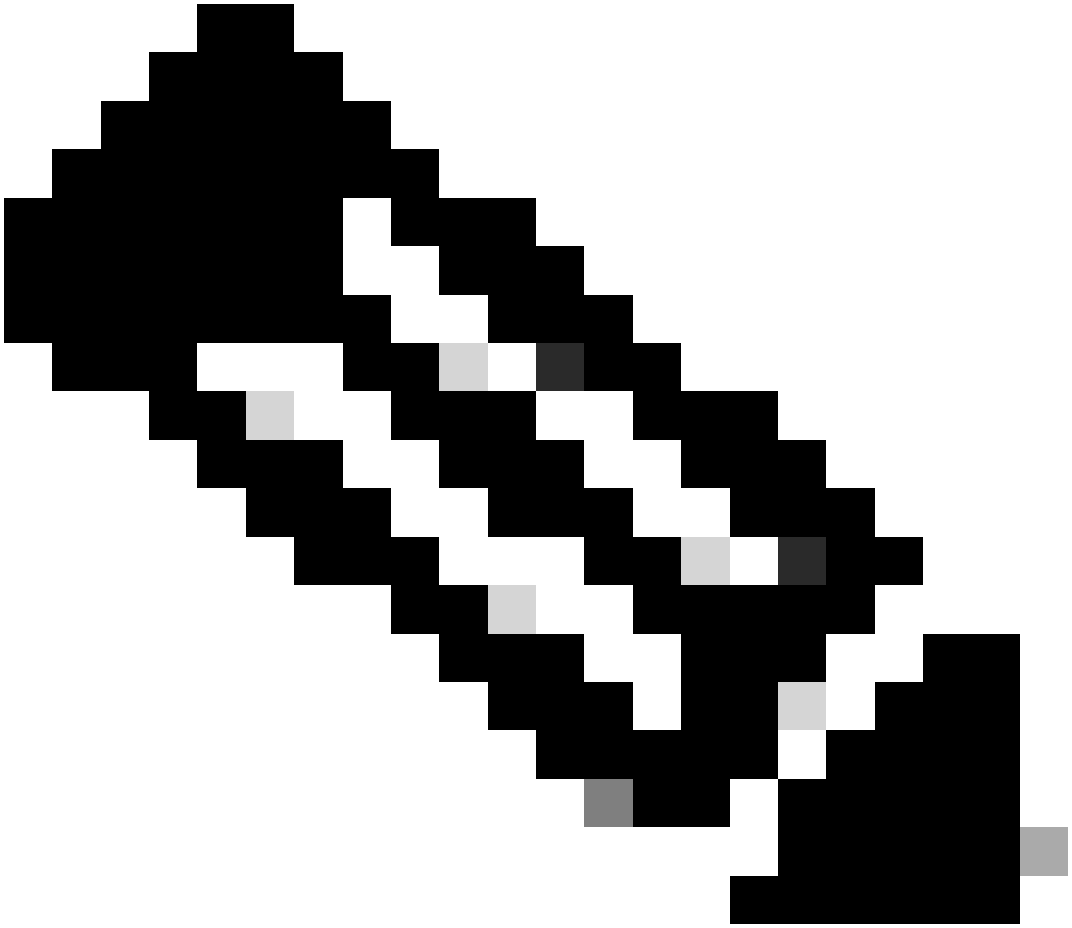
show bgp <AFI> <SAFI> summary

Ejemplo:

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

Las colas de clientes RR tienen aproximadamente la misma cantidad de MsgSent, pero algunos vecinos pueden tener un número de MsgRcvd mayor que otros. Debe capturar varias instantáneas de este comando para evaluar la velocidad de los mensajes.

Una vez que haya identificado a los peers infractores, puede pasar por otros comandos como **show bgp neighbor <neighbor> detail** y **show bgp neighbor <neighbor> performance-statistics** o **show bgp recent-prefixe**s para tratar de entender qué prefijos son inestables y si siempre son los mismos o diferentes.



Nota: Los contadores MsgRcvd y MsgSent son por vecino pero no por familia de direcciones. Por lo tanto, al ejecutar un comando como show bgp all all summary , se ven los mismos contadores por vecino en las secciones para las diversas familias de direcciones. No representan el número de mensajes recibidos/enviados desde/hacia ese vecino para esa familia de direcciones, sino entre familias de direcciones.

Supervisar el uso de CPU

El uso de la CPU debe ser monitoreado en cada router, pero en un router con un alto número de núcleos de CPU dedicados al plano de control algunas lecturas pueden ser poco intuitivas. En un RR BGP con un número elevado de núcleos de CPU dedicados al procesador de routing (RP), como en el caso del appliance XRv9k, los subprocesos activos se ejecutan en núcleos de CPU diferentes, mientras que varios núcleos de CPU permanecen inactivos. Como consecuencia, algunos núcleos de CPU pueden estar muy ocupados, pero el uso general de CPU calculado a través de todos los núcleos de CPU sigue siendo moderado.

Por lo tanto, para una supervisión adecuada de la utilización de los núcleos de CPU a través de CLI, utilice el **show processes cpu thread** comando.

Supervisar estadísticas de TCP

Cisco IOS® mantiene estadísticas detalladas sobre cada sesión TCP. El comando CLI **show tcp brief** muestra la lista de todas las sesiones TCP existentes. En esta salida de resumen, para cada sesión TCP puede ver esta información:

- **PCB:** identificador de sesión TCP único.
- **VRF-ID**: ID del VRF en el que existe la sesión.
  - Para ver el nombre VRF correspondiente, ejecute este comando:
  - show cef vrf all summary | utility egrep "^VRF:|Vrfid" | utility egrep -B1 <VRF-ID>
- **Recv-Q**: tamaño instantáneo de la cola de recepción Q. La cola de recepción contiene los paquetes recibidos de NetIO. El proceso **tcp** extrae los datos de un paquete y los envía a la aplicación correspondiente.
- **Send-Q**: tamaño instantáneo de la cola de envío. La cola de envío contiene los datos recibidos de una aplicación. El proceso **tcp** divide los datos en segmentos TCP (dictados por el tamaño de segmento máximo negociado - TCP MSS), encapsula cada segmento en un encabezado de capa 3 de la familia de direcciones correspondiente (IPv4 o IPv6) y envía el paquete a NetIO.
- **Dirección local**: dirección IPv4 o IPv6 local asociada al socket TCP. Las sesiones TCP en estado LISTEN se suelen enlazar a "**cualquier**" dirección IP, que se representa como "0.0.0.0" o "::" en el caso de IPv4 o IPv6 respectivamente.
- **Dirección externa**: dirección IPv4 o IPv6 remota asociada al socket TCP. Las sesiones TCP en estado LISTEN se suelen enlazar a "**cualquier**" dirección IP, que se representa como "0.0.0.0" o "::" en el caso de IPv4 o IPv6 respectivamente.
- **Estado**: estado de la sesión TCP. Los estados de sesión TCP posibles son: LISTEN, SYNSENT, SYNRCVD, ESTAB, LASTACK, CLOSING, CLOSEWAIT, FINWAIT1, FINWAIT2, TIMEWAIT, CLOSED.

Dado que el número de puerto BGP conocido es 179, puede limitar las sesiones TCP mostradas a aquellas que están asociadas con la aplicación BGP.

Ejemplo:

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

Puede utilizar el valor PCB mostrado para obtener las estadísticas para una sesión TCP determinada. Comandos CLI que proporcionan información sobre las estadísticas de los procesos TCP:

Global:

show tcp statistics clients location <active_RP>

show tcp statistics summary location <active_RP>

Por PCB:

show tcp brief | i ":179"

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

show tcp statistics pcb <pcb> location <active_RP>

Los comandos de estadísticas TCP globales muestran el estado general de las sesiones TCP. Aparte de las estadísticas de paquetes de datos (entrada/salida), puede ver por ejemplo si hay paquetes con errores de suma de comprobación, paquetes mal formados, paquetes perdidos debido a errores de autenticación, paquetes fuera de orden, paquetes con datos después de la ventana, lo que le da una indicación del comportamiento de los pares TCP.

En los comandos por PCB, puede ver parámetros importantes de una sesión TCP, como MSS, tiempo máximo de ida y vuelta, etc.

Los contadores relevantes en el resultado del show tcp detail pcb comando son:

- **Retrans Timer Starts**: indica cuántas veces se inició el temporizador de retransmisión.
- **Retrans Timer Wakeups**: indica cuántas veces se agotó el temporizador de retransmisión, lo que desencadenó una retransmisión del segmento TCP.
- **Tamaño actual de la cola de envío en bytes**: bytes sin acuse de recibo del par.
- **Tamaño actual de la cola de recepción en bytes/paquetes**: bytes/paquetes que aún debe leer la aplicación (BGP).
- **bytes mal ordenados**: bytes que están en cola en la cola de almacenamiento debido a un agujero en la ventana de recepción TCP.

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

Supervisión de la utilización de memoria

La tabla de rutas BGP se almacena en la memoria de pila de procesos BGP. La tabla de ruteo se almacena en la memoria del montón del proceso RIB.

Comandos útiles para la supervisión de la memoria de montón:

show memory summary

show memory summary detail

show memory-top-consumers

show memory heap summary all

Ruta del sensor de telemetría:

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

La FIB almacena las entradas de reenvío en el espacio de memoria compartida.

Comandos útiles para la supervisión de la memoria compartida:

show memory summary

show memory summary detail

show shmwin summary

Supervisar el rendimiento del proceso BGP

Comando útil que proporciona datos internos sobre el rendimiento del proceso BGP:

show bgp process performance-statistics

show bgp process performance-statistics detail

Supervisión de la convergencia BGP

Otro comando útil es el que muestra el estado general de la convergencia BGP: show bgp convergence

Cuando la red es estable, se ve algo como esto:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).