

# Solución de problemas básicos de Border Gateway Protocol

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Topología](#)

[Escenarios y problemas](#)

[Adyacencia hacia abajo](#)

[Sin conectividad](#)

[Problemas de configuración](#)

[Problemas de TCPSession](#)

[Rebotes de adyacencia](#)

[Flap de interfaz](#)

[Temporizador de espera vencido](#)

[Problemas AFI/SAFI](#)

[Instalación y selección de rutas](#)

[Salto siguiente](#)

[Fallo de RIB](#)

[Condición de carrera](#)

[Otros problemas](#)

[BGP Slow Peer](#)

[Problemas de memoria](#)

[Uso elevado de la CPU](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo resolver los problemas más comunes con el Protocolo de gateway fronterizo (BGP) y proporciona soluciones y pautas básicas.

## Prerequisites

## Requirements

No hay requisitos previos específicos para este documento. El conocimiento básico del protocolo BGP es útil, puede consultar la [Guía de Configuración BGP](#) para obtener más información.

## Componentes Utilizados

Este documento no se limita a versiones específicas de software y hardware, pero los comandos son aplicables para Cisco IOS® y Cisco IOS® XE.

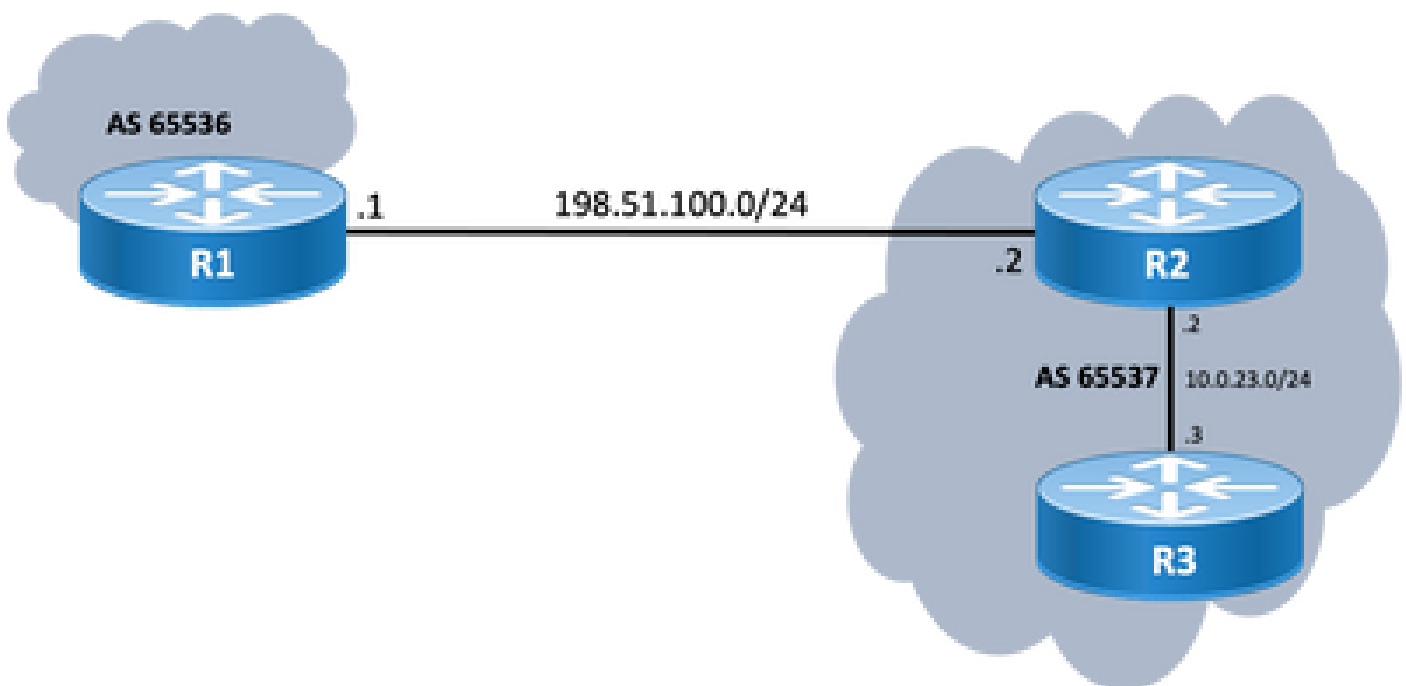
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Este documento describe una guía básica para resolver los problemas más comunes en el Protocolo de gateway fronterizo (BGP), proporciona acciones correctivas, comandos/depuraciones útiles para detectar la causa raíz de los problemas y prácticas recomendadas para evitar posibles problemas. Tenga en cuenta que no se pueden considerar todas las variables y escenarios posibles y que Cisco TAC podría requerir un análisis más profundo.

## Topología

Utilice este diagrama de topología como referencia para los resultados proporcionados en este documento.



## Escenarios y problemas

Adyacencia hacia abajo

Si una sesión BGP está inactiva y no se activa, ejecute el comando `show ip bgp all summary`. Aquí puede encontrar el estado actual de la sesión:

- Si la sesión no está en estado activo, puede variar entre IDLE y ACTIVE (depende del proceso de la máquina de estado finito).
- Si la sesión está activa, verá el número de prefijos recibidos.

```
<#root>
```

```
R2#
```

```
show ip bgp all summary
```

```
For address family: IPv4 Unicast
BGP router identifier 198.51.100.2, local AS number 65537
BGP table version is 19, main routing table version 19
18 network entries using 4464 bytes of memory
18 path entries using 2448 bytes of memory
1/1 BGP path/bestpath attribute entries using 296 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 7208 total bytes of memory
BGP activity 18/0 prefixes, 18/0 paths, scan interval 60 secs
18 networks peaked at 11:21:00 Jun 30 2022 CST (00:01:35.450 ago)
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.0.23.3	4	65537	6	5	19	0	0	00:01:34	18
198.51.100.1	4	65536	0	0	1	0	0	never	Idle

## Sin conectividad

El primer requisito que debe garantizarse es la conectividad entre ambos peers para que se pueda establecer la sesión TCP en el puerto 179. Están conectados directamente o no. Un simple ping es útil para este asunto. Si se establece el peering entre las interfaces de loopback, se debe realizar un loopback a un ping de loopback. Si se realiza una prueba de ping sin un loopback específico como interfaz de origen, la dirección IP de la interfaz física saliente se utiliza como dirección IP de origen del paquete en lugar de la dirección IP de loopback del router.

Si el ping no es exitoso, considere estas causas:

- Sin par de ruta conectado o sin ruta en absoluto: `show ip route peer_IP_address` se puede utilizar.
- Problema de capa 1: debe tenerse en cuenta el problema de la interfaz física, el SFP (conector), el cable o el problema externo (transporte y proveedor, si procede).
- Compruebe cualquier firewall o lista de acceso que pueda bloquear la conexión.

Si el ping es exitoso, considere lo siguiente:

## Problemas de configuración

- Dirección IP incorrecta o AS configurado: para IP incorrecta , no se muestra dicho mensaje, pero asegúrese de que se realiza la configuración correcta. Para el AS incorrecto, debe ver un mensaje como con el `show logging` comando.

```
%BGP-3-NOTIFICATION: sent to neighbor 198.51.100.1 passive 2/2 (peer in wrong AS) 2 bytes 1B39
```

Verifique la configuración BGP en ambos extremos para corregir los números AS o la dirección IP del par.

- ID de router duplicado:

```
%BGP-3-NOTIFICATION: sent to neighbor 198.51.100.1 passive 2/3 (BGP identifier wrong) 4 bytes 0A0A0A0A
```

Verifique el identificador BGP en ambos extremos a través de `show ip bgp all summary` y corrija el problema de duplicado. Esto se puede lograr manualmente con el comando global `bgp router-id x.x.x.x` en configuración del router `bgp`. Como práctica recomendada, asegúrese de que el ID del router se establece manualmente en un número único.

- Origen BGP y TTL:

La mayoría de las sesiones de iBGP se configuran a través de las interfaces de loopback alcanzables a través de un IGP. Esta interfaz de loopback debe definirse explícitamente como el origen. Haga esto con el comando `neighbor ip-address update-source interface-id` .

Para el peer eBGP, las interfaces conectadas directamente se utilizan generalmente para el peering, y hay una verificación para que Cisco IOS/Cisco IOS XE cumpla con este propósito, o lo hace ni siquiera intente establecer la sesión. Si se intenta eBGP desde el loopback al loopback en los routers conectados directamente, esta verificación se puede inhabilitar para un vecino específico en ambos extremos mediante `neighbor ip-address disable-connected-check` .

Sin embargo, si hay saltos múltiples entre los peers eBGP, se requiere un conteo de saltos adecuado, asegúrese de que el `neighbor ip-address ebgp-multihop [hop-count]` está configurado con el conteo de saltos correcto para que se pueda establecer la sesión.

Si no se especifica el conteo de saltos, el valor TTL predeterminado para las sesiones iBGP es 255, mientras que el valor TTL predeterminado para las sesiones eBGP es 1.

## Problemas de sesión TCP

Una acción útil para probar el puerto 179 es un telnet manual de un par al otro:

<#root>

R1#

```
telnet 198.51.100.2 179
```

```
Trying 198.51.100.2, 179 ... Open
```

```
[Connection to 198.51.100.2 closed by foreign host]
```

Abrir/cerrar conexión, o la conexión rechazada por el host remoto indica que los paquetes alcanzan el extremo remoto, entonces, asegúrese de que no haya problemas con el plano de control en el extremo lejano. De lo contrario, si hay un destino inalcanzable, verifique cualquier firewall o lista de acceso que pueda bloquear el puerto TCP 179, o los paquetes BGP, o cualquier pérdida de paquetes en la trayectoria.

En caso de problema de autenticación, los mensajes que puede ver:

```
%TCP-6-BADAUTH: Invalid MD5 digest from 198.51.100.1(179) to 198.51.100.2(20062) tableid - 0  
%TCP-6-BADAUTH: No MD5 digest from 198.51.100.1(179) to 198.51.100.2(20062) tableid - 0
```

Verifique los métodos de autenticación, la contraseña y la configuración relacionada, y para resolver problemas adicionales consulte [Ejemplo de Configuración de Autenticación MD5 entre Peers BGP](#).

Si la sesión TCP no aparece, puede utilizar los siguientes comandos para el aislamiento:

```
show tcp brief all  
show control-plane host open-ports  
debug ip tcp transactions
```

## Rebotes de adyacencia

Si la sesión está activa o inactiva, busque `show log` y pueden ver algunos escenarios.

## Flap de interfaz

```
%BGP-5-ADJCHANGE: neighbor 198.51.100.2 Down Interface flap
```

Como indica el mensaje, la razón de esta falla es la situación de la interfaz inactiva, busque cualquier problema físico en el puerto/SFP, el cable o las desconexiones.

## Temporizador de espera vencido

```
%BGP-3-NOTIFICATION: sent to neighbor 198.51.100.2 4/0 (hold time expired) 0 bytes
```

Es una situación muy común; significa que el router no recibió ni procesó un mensaje de keepalive o cualquier mensaje de actualización antes de que caducara el temporizador de espera. El dispositivo envía un mensaje de notificación y cierra la sesión. Las razones más comunes para este problema se enumeran aquí:

- Problemas de interfaz: busque cualquier error de entrada, caídas de la cola de entrada o problemas físicos en las interfaces conectadas de ambos pares; `show interface` puede utilizarse con este fin.
- Pérdida de paquetes en tránsito: a veces, los paquetes Hello se pueden descartar en tránsito, la mejor manera de asegurarse de que esto es una captura de paquetes en el nivel de interfaz.
  - Puede utilizar la [captura de paquetes integrada](#) en los dispositivos Cisco IOS y Cisco IOS XE.
  - En caso de que los paquetes se vean a nivel de interfaz, debe asegurarse de que alcanzan el plano de control, EPC en el plano de control, o `debug bgp [vrf name] ipv4 unicast keepalives` es útil.
- CPU alta: una condición de CPU alta puede causar caídas en el plano de control, `show processes cpu [sorted|history]` es útil para identificar el problema. Según la plataforma, puede encontrar el siguiente paso para resolver problemas con el [documento de referencia de CPU](#)
- Problemas de política de CoPP: la metodología de solución de problemas varía para cada plataforma y está fuera del alcance de este documento.
- Discordancia de MTU: Si hay discrepancias de MTU en la trayectoria, y si los mensajes ICMP están bloqueados en la trayectoria de origen a destino, la PMTUD no funciona y puede dar lugar a inestabilidad de sesión. Las actualizaciones se envían con el valor MSS negociado y un conjunto de bits DF. Si un dispositivo en la trayectoria o incluso el destino no puede aceptar los paquetes con una MTU más alta, envía un mensaje de error ICMP de vuelta al altavoz BGP. El router de destino espera que el keepalive BGP o el paquete de actualización BGP actualice su temporizador de retención.
  - Puede verificar el MSS negociado con `show ip bgp neighbors ip_address`.

Una prueba de ping a un vecino específico con el conjunto df puede mostrarle si dicha MTU es

válida a lo largo de la trayectoria:

```
<#root>
```

```
ping 198.51.100.2 size
```

```
max_seg_size
```

```
df
```

Si se encuentran problemas de MTU, se debe realizar una revisión precisa de la configuración para garantizar que los valores de MTU sean consistentes en toda la red.

---

Nota: Para obtener más información sobre MTU, consulte [Inestabilidad de Vecino BGP con Troubleshooting de MTU](#).

---

## Problemas con AFI/SAFI

```
%BGP-5-ADJCHANGE: neighbor 198.51.100.2 passive Down AFI/SAFI not supported
```

```
%BGP-3-NOTIFICATION: received from neighbor 198.51.100.2 active 2/8 (no supported AFI/SAFI) 3 bytes 000
```

El identificador de familia de direcciones (AFI) es una extensión de capacidad agregada por BGP multiprotocolo (MP-BGP). Correlaciona con un protocolo de red específico, como IPv4, IPv6 y similares, y granularidad adicional a través de un identificador de familia de direcciones subsiguiente (SAFI), como unidifusión y multidifusión. MBGP logra esta separación mediante los atributos de trayectoria BGP (PA) MP\_REACH\_NLRI y MP\_UNREACH\_NLRI. Estos atributos se transportan dentro de los mensajes de actualización BGP y se utilizan para transportar información de alcance de red para diferentes familias de direcciones.

El mensaje le da los números de estos AFI/SAFI registrados por IANA:

- [Números de familia de direcciones IANA](#)
- [Parámetros de identificadores de familia de direcciones \(SAFI\) posteriores](#)
- Verifique la configuración BGP para las familias de direcciones que se pretenden en ambos lados para corregir cualquier familia de direcciones no deseada.
- Uso `neighbor ip-address dont-capability-negotiate` en ambos extremos. Para obtener más información, consulte [Funciones no admitidas que causan el mal funcionamiento del par BGP](#).

## Instalación y selección de rutas

Para una mejor explicación sobre cómo funciona BGP y para seleccionar la mejor trayectoria,

consulte [Algoritmo de Selección de la Mejor Trayectoria BGP](#).

## Salto siguiente

Para que una ruta se instale en nuestra tabla de ruteo, el salto siguiente debe ser alcanzable; de lo contrario, incluso si el prefijo está en nuestra tabla de BGP Loc-RIB, no ingresa en RIB. Como regla de evitación de loop, en Cisco IOS/Cisco IOS XE, iBGP no cambia el atributo de salto siguiente y deja AS\_PATH solo mientras eBGP reescribe el salto siguiente y antepone su AS\_PATH.

Puede comprobar el siguiente salto con `show ip bgp [prefix]`. Le da el siguiente salto y la palabra inaccesible. En el ejemplo, este es un prefijo anunciado por R1 vía eBGP a R2 y aprendido por R3 vía conexión iBGP desde R2.

<#root>

R3#

```
show ip bgp 192.0.2.1
```

```
BGP routing table entry for 192.0.2.1/32, version 0
```

```
Paths: (1 available, no best path)
```

```
Not advertised to any peer
```

```
Refresh Epoch 1
```

```
65536
```

```
198.51.100.1 (inaccessible)
```

```
from 10.0.23.2 (10.2.2.2)
```

```
Origin incomplete, metric 0, localpref 100, valid, internal
```

```
rx pathid: 0, tx pathid: 0
```

```
Updated on Jul 1 2022 13:44:19 CST
```

En la salida, el salto siguiente es la interfaz saliente de R1 que no es conocida por R3. Para solucionar esta situación, puede anunciar el siguiente salto a través de IGP, la ruta estática o utilizar el `neighbor ip-address next-hop-self` comando en el peer iBGP para modificar la IP del siguiente salto (que está conectada directamente). En el ejemplo del diagrama, esta configuración debe estar en R2; el vecino hacia R3 (`vecino 10.0.23.3 next-hop-self`).

Como resultado, el salto siguiente cambia (después de un `clear ip bgp 10.0.23.2 soft`) a la interfaz conectada directamente (alcanzable) y el prefijo está instalado.

<#root>

R3#

```
show ip bgp 192.0.2.1
```



BGP routing table entry for 192.0.2.1/32, version 24

Paths: (1 available, best #1, table default)

Not advertised to any peer  
Refresh Epoch 1  
65536

10.0.23.2

from 10.0.23.2 (10.2.2.2)  
Origin incomplete, metric 0, localpref 100, valid, internal, best  
rx pathid: 0, tx pathid: 0x0  
Updated on Jul 1 2022 13:46:53 CST

## Fallo de RIB

Esto sucede cuando la ruta no se puede instalar en el RIB global, lo que resulta en una falla del RIB. La razón común es cuando el mismo prefijo ya está en RIB para otro protocolo de ruteo con una distancia administrativa menor, pero la razón exacta de una falla de RIB se observa con el comando `show ip bgp rib-failure`. Para obtener una explicación más detallada, puede consultar este enlace:

---

Nota: Puede identificar y corregir este problema tal como se explica en [Comprensión de BGP RIB-failure y El Comando `bgp suppress-inactive`](#).

---

## Condición de carrera

El problema más común observado es cuando se prefiere IGP sobre eBGP en un escenario de redistribución mutua. Cuando una ruta IGP se redistribuye en BGP, se considera generada localmente por BGP y obtiene un peso de 32768 de forma predeterminada. A todos los prefijos recibidos de un par BGP se les asigna un peso local de 0 de forma predeterminada. Por lo tanto, si se debe comparar el mismo prefijo, el prefijo con el peso más alto se instala en la tabla de ruteo según el proceso de selección de la mejor trayectoria BGP y es por esto que la ruta IGP se instala en RIB.

La solución para este problema, es establecer un peso más alto para todas las rutas recibidas del peer BGP bajo la configuración `bgp` del router:

```
<#root>  
neighbor  
ip-address  
weight 40000
```

---

Nota: Para obtener una explicación detallada, consulte [Comprensión de la Importancia del Atributo BGP Weight Path en los Escenarios de Failover de Red.](#)

---

## Otros problemas

### BGP Slow Peer

Es un peer que no puede mantenerse al día con la velocidad a la que el remitente genera mensajes de actualización. Hay muchas razones para que un par muestre este problema; CPU alta en uno de los pares, tráfico excesivo o pérdida de tráfico en un link, recurso de ancho de banda, entre otros.

---

Nota: Para ayudar a identificar y corregir problemas de peers lentos, consulte [Uso de la Función "Peer Lento" de BGP para Resolver Problemas de Peers Lentos.](#)

---

### Problemas de memoria

BGP utiliza la memoria asignada al proceso de Cisco IOS para mantener los prefijos de red, las mejores trayectorias, las políticas y toda la configuración relacionada para funcionar correctamente. Los procesos generales se ven con el comando `show processes memory sorted`:

<#root>

R1#

`show processes memory sorted`

Processor Pool Total: 2121414332 Used: 255911152 Free: 1865503180

reserve P Pool Total: 102404 Used: 88 Free: 102316

tsmpi\_io Pool Total: 3149400 Used: 3148568 Free: 832

PID	TTY	Allocated	Freed
-----	-----	-----------	-------

Holding

Getbufs	Retbufs	Process				
0	0	266231616	81418808	160053760	0	0 *Init*
662	0	34427640	51720	34751920	0	0 SBC main process
85	0	9463568	0	8982224	0	0 IOSD ipc task
0	0	34864888	25213216	8513400	8616279	0 *Dead*
504	0	696632	0	738576	0	0 QOS_MODULE_MAIN
518	0	940000	8616			

613760

0 0

BGP Router

228	0	856064	345488	510080	0	0 mDNS
82	0	547096	118360	417520	0	0 SAMsgThread
0	0	0	0	395408	0	0 *MallocLite*

El conjunto de procesadores es la memoria utilizada; en el ejemplo, alrededor de 2,1 GB. A continuación, debe observar la columna Holding (Retención) para identificar el subproceso que contiene la mayor parte de ella. Luego, debe verificar las sesiones BGP que tiene, cuántas rutas se reciben y la configuración utilizada.

Pasos comunes para reducir la retención de memoria por BGP:

- Filtrado BGP: si no es necesario recibir una tabla BGP completa, utilice políticas para filtrar rutas e instalar solamente los prefijos que necesite.
- Reconfiguración de software: busque `neighbor ip_address soft-reconfiguration inbound` bajo configuración BGP; este comando le permite ver todos los prefijos recibidos antes de cualquier política entrante (Adj-RIB-in). Sin embargo, esta tabla necesita alrededor de la mitad de la tabla BGP Local RIB actual para almacenar esta información para que pueda evitar esta configuración a menos que se requiera obligatoriamente, o sus prefijos actuales sean pocos.

---

Nota: Para obtener más información sobre cómo optimizar BGP, consulte [Configuración de Routers BGP para un Rendimiento Óptimo y un Consumo de Memoria Reducido](#).

---

## Uso elevado de la CPU

Los routers utilizan diferentes procesos para que BGP funcione. Para verificar que el proceso BGP es la causa de una alta utilización de la CPU, utilice el comando `show process cpu sorted` comando.

<#root>

R3#

`show processes cpu sorted`

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
163	36	1463	24	0.07%	0.00%	0.00%	0	ADJ background
62	28	132	212	0.07%	0.00%	0.00%	0	Exec
2	39	294	132	0.00%	0.00%	0.00%	0	Load Meter
1	0	4	0	0.00%	0.00%	0.00%	0	Chunk Manager
3	27	1429	18	0.00%	0.00%	0.00%	0	

**BGP Scheduler**

4	0	1	0	0.00%	0.00%	0.00%	0	R0 Notify Timers
63	4	61	65	0.00%	0.00%	0.00%	0	

**BGP I/O**

83	924	26	35538	0.00%	0.03%	0.04%	0	
----	-----	----	-------	-------	-------	-------	---	--

**BGP Scanner**

96	142	11651	12	0.00%	0.00%	0.00%	0 Tunnel BGP
7	0	1	0	0.00%	0.00%	0.00%	0 DiscardQ Backgro

Estos son los procesos comunes, las causas y los pasos generales para superar la alta utilización de la CPU debido a BGP:

- Router BGP: se ejecuta una vez por segundo para proteger una convergencia más rápida. Es uno de los hilos más importantes. Lee los mensajes de actualización de bgp, valida los prefijos/redes y atributos, actualiza la tabla de red/prefijo y la tabla de atributos por AFI/SAFI, realiza el cálculo de la mejor trayectoria entre muchas otras tareas. Una gran pérdida de rutas es un escenario muy común que lleva a esta situación.
- Escáner BGP: proceso de baja prioridad que se ejecuta cada 60 segundos de forma predeterminada. Este proceso verifica la tabla BGP completa para verificar la disponibilidad del siguiente salto y actualiza la tabla BGP en consecuencia, en caso de que haya algún cambio para una trayectoria. Se ejecuta a través de la Base de información de routing (RIB) con fines de redistribución. Verifique la escalabilidad de la plataforma, a medida que se instalan más prefijos y rutas y se utiliza TCAM, se necesitan más recursos y, por lo general, un dispositivo sobrecargado conduce a tales situaciones.

---

Nota: Para obtener más información sobre cómo resolver problemas de estos dos procesos, consulte [Resolución de Problemas de CPU Elevada Causados por el Proceso del Router o Escáner BGP](#).

---

- E/S BGP: se ejecuta cuando se reciben paquetes de control BGP y gestiona la colocación en cola y el procesamiento de paquetes BGP. Si hay paquetes excesivos recibidos en la cola BGP durante un período largo, o si hay un problema con TCP, el router muestra síntomas de CPU alta debido al proceso de E/S BGP. (Generalmente, el router BGP también es alto en esta situación. Observe los recuentos de mensajes para identificar los pares y los paquetes de captura para identificar el origen de estos mensajes.)
- BGP Open: proceso utilizado al establecer la sesión. No es un problema común de CPU alta a menos que la sesión se atasque en el estado abierto.
- Evento BGP: es responsable del procesamiento del siguiente salto. Busque los flaps next-hops en los prefijos recibidos.

## Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Guía de configuración de BGP](#)
- [Ejemplo de Configuración de Autenticación MD5 entre Peers BGP](#)
- [Captura de paquetes integrada](#)
- [Inestabilidad de Vecino BGP con Troubleshooting de MTU](#)
- [Números de familia de direcciones IANA](#)

- [Parámetros de identificadores de familia de direcciones \(SAFI\) posteriores](#)
- [Las Funciones no Soportadas Causan el Malfuncionamiento del Peer BGP](#)
- [Algoritmo de selección del mejor trayecto BGP](#)
- [Comprensión de BGP RIB-failure and The Command bgp suppress-inactive](#)
- [Comprenda la importancia del atributo de ruta de peso BGP en situaciones de conmutación por error de red](#)
- [Utilice la Función "Slow Peer" de BGP para Resolver Problemas de Peer Lento](#)
- [Configuración de routers BGP para obtener un rendimiento óptimo y un consumo de memoria reducido](#)
- [Resolución de Problemas de CPU Elevada Causada por el Proceso del Router o Escáner BGP](#)

## 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).