Nota Técnica de Troubleshooting de Vecino BGP Flaps con MTU

Contenido

Introducción

Este documento describe cómo determinar si las inestabilidades del vecino BGP (protocolo de gateway fronterizo interno o externo) son causadas por problemas de unidad de transmisión máxima (MTU).

Prerequisites

Asegúrese de completar estas tareas en ambos routers BGP antes de completar los procedimientos en este documento:

- Verifique la configuración de BGP.
- Verifique que el vecino BGP sea accesible a través del protocolo de mensajes de control de Internet (ICMP) y que no se observe ninguna caída.
- Verifique que la interfaz conectada utilizada para peer BGP no esté sobresuscrita y no tenga caídas o errores de entrada/salida.
- Verifique el uso de la CPU y la memoria.

Problema

formulario de vecinos BGP; sin embargo, en el momento del intercambio de prefijos, el estado BGP se descarta y los registros generan señales de mantenimiento hello BGP faltantes o el otro par termina la sesión.

Complete estos pasos para determinar si la MTU hace que los vecinos BGP inunden:

1. Utilice los siguientes comandos para verificar qué vecino se ve afectado y la interfaz conectada en ambos routers BGP. Si la dirección de peering es una dirección de loopback, verifique la interfaz conectada a través de la cual se puede alcanzar el loopback. Además, verifique la salida de BGP en ambos routers de peering. La OutQ no nula coherente es una indicación fuerte de que las actualizaciones no llegan al par debido a un problema de MTU

en la trayectoria.

```
Router#show ip bgp summ | in InQ|10.10.10.2
Neighbor     V   AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.2    4   3     64      62       3     0    0   00:00:3       2


Router#show ip route 10.10.10.2
Routing entry for 10.10.10.0/24
 Known via "connected", distance 0, metric 0 (connected, via interface)
 Routing Descriptor Blocks:
 * directly connected, via GigabitEthernet1/0
     Route metric is 0, traffic share count is 1
```

2. Verifique la interfaz MTU en ambos lados:

```
Router#show ip int g1/0 | i MTU
MTU is 1500 bytes
Router#
```

3. Confirme el segmento de datos máximo acordado de TCP para ambos altavoces BGP:

```
Router#show ip bgp neigh 20.20.20.2 | inc segment
Datagrams (max data segment is 1460 bytes):
Router#
```

   En el ejemplo anterior, 1460 es correcto ya que 20 bytes se asignan al encabezado TCP y otros 20 al encabezado IP.

4. Confirme si BGP utilizó *path-mtu habilitado*:

```
Router#show ip bgp neigh 10.10.10.2 | in tcp
Transport(tcp) path-mtu-discovery is enabled
Router#
```

5. Haga ping al par BGP con el conjunto de bits MTU y DF (No fragmentar) de interfaz máxima:

```
Router#ping 10.10.10.2 size 1500 df

Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
Packet sent with the DF bit set
.....
Success rate is 0 percent (0/5)
```

6. Reduzca el valor de tamaño ICMP para determinar el tamaño máximo de MTU que se puede utilizar:

```
ping 10.10.10.2 size 1300 df
```

Solución

Estas son algunas de las causas posibles:

- La MTU de interfaz en ambos routers no coincide.
- La MTU de interfaz en ambos routers coincide, pero el dominio de Capa 2 sobre el cual se forma la sesión BGP no coincide.
- La detección de la MTU de la trayectoria determinó la cantidad de datos máxima incorrecta para la sesión TCP BGP.
- La detección de la unidad de transmisión máxima (PMTUD) de la ruta BGP podría fallar debido a que se bloquearon los paquetes ICMP PMTUD (firewall o ACL)

A continuación se muestran las posibles maneras de resolver los problemas de MTU:

1. La MTU de interfaz en ambos routers debe ser la misma; ejecute el comando **show ip int | en el** comando **MTU** para verificar la configuración de MTU actual.

2. Si la MTU de interfaz en ambos routers es correcta (por ejemplo, 1500) pero las pruebas ping con el bit DF configurado no exceden 1300, entonces el dominio de Capa 2 en el que se forma la sesión BGP afectada podría incluir configuraciones de MTU inconsistentes. Verifique cada MTU de interfaz de Capa 2. Corrija la MTU de la interfaz de Capa 2 para resolver el problema.

3. Si no puede verificar/cambiar el dominio de Capa 2, puede configurar el comando **ip tcp mss** global para que reduzca el valor como 1000, lo que obligará a todas las sesiones de segmentos de datos TCP máx originadas localmente (que incluye BGP) a 1000. Para obtener más información sobre este comando, refiérase a la sección ip tcp mss de la *Referencia de Comandos de IP Application Services de Cisco IOS*.

   Además, puede utilizar el comando **ip tcp adjust-mss** para resolver problemas adicionales; este comando se configura en el nivel de interfaz y afecta a todas las sesiones TCP. Para obtener más información sobre este comando, consulte la sección ip tcp adjust-mss de la *Referencia de Comandos de IP Application Services de Cisco IOS*.

4. (*Opcional*) Es posible que la Detección de la Unidad Máxima de Transmisión de Trayectoria de BGP (PMTUD) no genere el tamaño máximo de datos correcto. Puede desactivarla globalmente o por vecino para confirmar si esta es la causa. Cuando se inhabilita BGP PMTUD, el tamaño máximo de segmento (MSS) de BGP se establece de forma predeterminada en 536 como se define en RFC 879.

   Para obtener información sobre cómo inhabilitar PMTUD, consulte la sección Configuración del Soporte de BGP para Detección de MTU de Trayectoria TCP por Sesión de la *Guía de Configuración de BGP de Cisco IOS*.

   Para obtener más información sobre PMTUD, consulte ¿Qué es PMTUD?