Contenido

Introducción

Este documento describe cómo determinar si las aletas vecinas internas o del Border Gateway Protocol externo del (BGP) son causadas por los problemas de la Unidad máxima de transmisión (MTU) (MTU).

Prerrequisitos

Asegúrese que usted complete estas tareas en ambos routeres BGP antes de que usted complete los procedimientos en este documento:

- Marque la configuración BGP.
- Verifique que el vecino BGP sea accesible vía el Internet Control Message Protocol (ICMP) y no se observa ningunos descensos.
- Verifique que la interfaz conectada usada para mirar BGP no sea oversubscribed y no tenga ningunos descensos o errores de la entrada-salida.
- Marque el CPU y la utilización de la memoria.

Problema

Forma de los vecinos BGP; sin embargo, a la hora del intercambio del prefijo, los descensos del estado BGP y los registros generan el Keepalives que falta BGP hola o el otro par termina la sesión.

Complete estos pasos para determinar si el MTU hace a los vecinos BGP agitar:

1. Utilice los comandos abajo para marcar qué vecino es afectado y la interfaz conectada en ambos routeres BGP. Si el direccionamiento del peering es un Loopback Address, marque la interfaz conectada a través de la cual el loopback es accesible. También, comprobación para el BGP OutQ en ambos routeres para redes entre peers. El OutQ no-cero constante es un indicio sólido que las actualizaciones no alcanzan al par debido a un problema 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 2Router#`**`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. Marque el MTU de interfaz en los ambos lados: `Router#show ip int g1/0 | i MTU`
   `MTU is 1500 bytes`
   `Router#`
3. Confirme el segmento de datos máximo estado de acuerdo TCP para ambos BGP de conversaciones: `Router#show ip bgp neigh 20.20.20.2 | inc segment`
   `Datagrams (max data segment is 1460 bytes):`
   `Router#`En el ejemplo anterior, 1460 está correctos pues 20 bytes se asignan al encabezado TCP y a otros 20 al encabezado IP.
4. Confirme si *se habilita el mtu de trayectoria* usado BGP: `Router#show ip bgp neigh 10.10.10.2 | in tcp`
   `Transport(tcp) path-mtu-discovery is enabled`
   `Router#`
5. Haga ping el peer BGP con el MTU de interfaz máximo y al conjunto de bits DF (Don't Fragment): `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. Disminuya el valor del tamaño ICMP para determinar el tamaño del MTU máximo que puede ser utilizado: `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)
   ```

Solución

Aquí están algunas posibles causas:

- El MTU de interfaz en ambo Routers no hace juego.
- El MTU de interfaz en ambo Routers hace juego, pero el dominio de la capa 2 sobre el cual forman a la sesión de BGP no hace juego.
- La detección de MTU de trayecto determinó el máximo incorrecto datasize para la sesión de BGP TCP.
- La detección de la Unidad máxima de transmisión (MTU) del trayecto BGP (PMTUD) podría ser el fallar debido a los paquetes icmp PMTUD bloqueados (firewal o el ACL)

Aquí están las maneras posibles de resolver los problemas MTU:

1. El MTU de interfaz en ambo Routers debe ser lo mismo; ejecute el **IP internacional de la demostración | en el comando mtu** para marcar las configuraciones de MTU actuales.

2. Si el MTU de interfaz en ambo Routers está correcto (por ejemplo, 1500) pero las pruebas de ping con el conjunto de bits DF no exceden de 1300, después el dominio de la capa 2 en el cual forman a la sesión de BGP afectada pudo incluir las configuraciones contrarias MTU. Marque cada interfaz de capa 2 MTU. Corrija el interfaz de capa 2 MTU para resolver el problema.

3. Si usted debe marcar incapaz/cambio el dominio de la capa 2, usted puede fijar el comando global de los **mss tcp del IP al** valor más bajo como 1000, que forzarán las sesiones máximas todo localmente originadas del segmento de datos TCP (que incluye el BGP) a 1000. Para más información sobre este comando, refiera a la sección de los mss tcp del IP de la *referencia de comandos de los Servicios de aplicación IP del Cisco IOS*.

   Además, usted puede utilizar el **comando ip tcp adjust-mss** para resolver problemas más lejos; este comando se configura en el nivel de la interfaz y afecta a todas las sesiones TCP. Para más información sobre este comando, refiera al IP tcp ajustan-mss la sección de la *referencia de comandos de los Servicios de aplicación IP del Cisco IOS*.

4. (*Opcional*) la detección de la Unidad máxima de transmisión (MTU) del trayecto BGP (PMTUD) no pudo generar el tamaño de los datos máximo correcto. Usted puede inhabilitarla global o por el vecino para confirmar si ésta es la causa. Cuando se inhabilita el BGP PMTUD, el Maximum Segment Size BGP (MSS) omite 536 según lo definido en el RFC 879.

   Para la información sobre cómo inhabilitar el PMTUD, refiera al soporte BGP que configura para la detección de MTU de trayecto TCP por la sección de la sesión de la *guía de configuración BGP del Cisco IOS*.

   ¿Para más información sobre el PMTUD, refiérase a cuál es PMTUD?