BGP Neighbor Flaps com MTU Troubleshooting TechNote

Contents

Introduction

Este documento descreve como determinar se os flaps de vizinhos do BGP (Border Gateway Protocol) internos ou externos são causados por problemas de MTU (Maximum Transmission Unit [unidade de transmissão máxima]).

Prerequisites

Certifique-se de concluir essas tarefas em ambos os roteadores BGP antes de concluir os procedimentos neste documento:

- Verifique a configuração do BGP.
- Verifique se o vizinho BGP está acessível via Internet Control Message Protocol (ICMP) e se não foram observadas quedas.
- Verifique se a interface conectada usada para o BGP do peer não está com excesso de assinaturas e não tem nenhum descarte ou erro de entrada/saída.
- Verifique a utilização da CPU e da memória.

Problema

forma de vizinhos de BGP; no entanto, no momento da troca de prefixos, o estado BGP cai e os logs geram keepalives de saudação BGP ausentes ou o outro peer encerra a sessão.

Conclua estes passos para determinar se o MTU faz com que os vizinhos BGP oscilem:

1. Use os comandos abaixo para verificar qual vizinho é afetado e a interface conectada em ambos os roteadores BGP. Se o endereço de peering for um endereço de loopback, verifique a interface conectada através da qual o loopback pode ser alcançado. Além disso, verifique o BGP OutQ em ambos os roteadores de peering. A consistente OutQ diferente de zero é uma forte indicação de que as atualizações não atingem o peer devido a um problema de MTU no caminho.

```
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 o MTU da interface em ambos os lados:
```
Router#show ip int g1/0 | i MTU
MTU is 1500 bytes
Router#
```
3. Confirme o segmento de dados máximo acordado pelo TCP para ambos os alto-falantes BGP:
```
Router#show ip bgp neigh 20.20.20.2 | inc segment
Datagrams (max data segment is 1460 bytes):
Router#
```
No exemplo acima, 1460 está correto, pois 20 bytes estão atribuídos ao cabeçalho TCP e outros 20 ao cabeçalho IP.

4. Confirme se o BGP usado *path-mtu está habilitado*:
```
Router#show ip bgp neigh 10.10.10.2 | in tcp
Transport(tcp) path-mtu-discovery is enabled
Router#
```
5. Faça ping no peer BGP com o conjunto de bits MTU e DF (Don't Fragment) da interface 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. Diminua o valor do tamanho ICMP para determinar o tamanho máximo de MTU que pode ser usado:
```
ping 10.10.10.2 size 1300 df
```

Solução

Aqui estão algumas causas possíveis:

- A interface MTU em ambos os roteadores não corresponde.
- O MTU da interface em ambos os roteadores corresponde, mas o domínio da Camada 2 sobre o qual a sessão BGP é formada não corresponde.
- A descoberta de MTU de caminho determinou o tamanho máximo incorreto para a sessão TCP BGP.
- A PMTUD (Maximum Transmission Unit Discovery, descoberta de unidade de transmissão máxima) do caminho BGP pode estar falhando devido aos pacotes ICMP PMTUD bloqueados (firewall ou ACL)

Aqui estão possíveis maneiras de resolver problemas de MTU:

1. O MTU da interface em ambos os roteadores deve ser o mesmo; execute o **comando show**

ip int | no comando **MTU** para verificar as configurações atuais de MTU.

2. Se o MTU da interface em ambos os roteadores estiver correto (por exemplo, 1500), mas os testes de ping com o conjunto de bits DF não excederem 1300, o domínio da Camada 2 no qual a sessão de BGP afetada é formada poderá incluir configurações de MTU inconsistentes. Verifique cada MTU de interface de Camada 2. Corrija o MTU da interface da Camada 2 para resolver o problema.

3. Se você não puder verificar/alterar o domínio da Camada 2, poderá definir o comando global **ip tcp mss** com um valor menor, como 1000, que forçará todas as sessões de segmentos de dados TCP max originadas localmente (que inclui BGP) a 1000. Para obter mais informações sobre esse comando, consulte a seção ip tcp mss da *Referência de Comandos do Cisco IOS IP Application Services*.

   Além disso, você pode usar o comando **ip tcp adjust-mss** para fazer troubleshooting adicional; esse comando é configurado no nível da interface e afeta todas as sessões TCP. Para obter mais informações sobre esse comando, consulte a seção ip tcp adjust-mss da *Referência de Comandos do Cisco IOS IP Application Services*.

4. (*Opcional*) A PMTUD (Maximum Transmission Unit Discovery, Descoberta máxima de unidade de transmissão de caminho BGP) pode não gerar o tamanho máximo de dados correto. Você pode desativá-la globalmente ou por vizinho para confirmar se essa é a causa. Quando o BGP PMTUD é desabilitado, o padrão do BGP Maximum Segment Size (MSS) é 536, conforme definido no RFC 879.

   Para obter informações sobre como desabilitar o PMTUD, consulte a seção Configuração do Suporte BGP para TCP Path MTU Discovery por Sessão do *Guia de Configuração do BGP do Cisco IOS*.

   Para obter mais informações sobre PMTUD, consulte O que é PMTUD?