Contenu

Introduction

Ce document décrit comment déterminer si les instabilités voisines internes ou de l'External Border Gateway Protocol (BGP) sont provoqué par par des questions de Maximum Transmission Unit (MTU).

Conditions préalables

Assurez que vous vous terminez ces tâches sur les deux routeurs BGP avant que vous remplissiez les procédures dans ce document :

- Vérifiez la configuration BGP.
- Vérifiez que le voisin BGP est accessible par l'intermédiaire du Protocole ICMP (Internet Control Message Protocol) et aucune baisse n'est observée.
- Vérifiez que l'interface connectée utilisée pour scruter BGP n'est pas oversubscribed et n'a aucunes baisses ou erreur d'entrée/sortie.
- Vérifiez l'utilisation de CPU et mémoire.

Problème

Forme de voisins BGP ; cependant, au moment de l'échange de préfixe, les tomber d'état BGP et les logs génèrent le Keepalives manquant BGP bonjour ou l'autre pair termine la session.

Terminez-vous ces étapes afin de déterminer si le MTU fait agiter les voisins BGP :

1. Employez les commandes ci-dessous afin de vérifier quel voisin est affecté et l'interface connectée sur les deux routeurs BGP. Si l'adresse scrutante est une adresse de bouclage, vérifiez l'interface connectée par laquelle le bouclage est accessible. En outre, vérifiez le BGP OutQ sur les deux routeurs d'appairage. À OutQ différent de zéro cohérent est une indication forte que les mises à jour n'atteignent pas le pair dû à une question de MTU dans le chemin. `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. Vérifiez l'interface MTU des deux côtés : `Router#show ip int g1/0 | i MTU`
   `MTU is 1500 bytes`
   `Router#`
3. Confirmez le segment de données maximum convenu par TCP pour les deux speakers BGP : `Router#show ip bgp neigh 20.20.20.2 | inc segment`
   `Datagrams (max data segment is 1460 bytes):`
   `Router#`Dans l'exemple ci-dessus, 1460 est correct car 20 octets est assignés à une en-tête de TCP et à des 20 différents à l'en-tête IP.
4. Confirmez si le chemin-*mtu* utilisé par BGP *est activé* : `Router#show ip bgp neigh 10.10.10.2 | in tcp`
   `Transport(tcp) path-mtu-discovery is enabled`
   `Router#`
5. Cinglez le pair BGP avec l'interface MTU maximum et le bit DF (Don't Fragment) réglé :

```
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. Diminuez la valeur de taille d'ICMP afin de déterminer la taille de MTU maximal qui peut être utilisée : `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)
```

Solution

Voici quelques causes possibles :

- L'interface MTU sur les deux Routeurs ne s'assortissent pas.
- L'interface MTU sur les deux Routeurs s'assortissent, mais le domaine de la couche 2 au-dessus dont la session BGP est formée ne s'assortit pas.
- La découverte de MTU de chemin a déterminé le maximum incorrect datasize pour la session BGP de TCP.
- La détection de Maximum Transmission Unit de chemin BGP (PMTUD) pourrait être manquer dû aux paquets d'ICMP PMTUD bloqués (firewal ou l'ACL)

Voici les moyens possibles de résoudre des problèmes de MTU :

1. L'interface MTU sur les deux Routeurs devrait être identique ; exécutez le **show ip international | dans la** commande de **MTU** afin de vérifier les configurations en cours de MTU.

2. Si l'interface MTU sur les deux Routeurs sont correcte (par exemple, 1500) mais les tests de ping avec le positionnement de bit DF ne dépassent pas 1300, alors le domaine de la couche 2 sur lequel la session BGP affectée est formée pourrait inclure des configurations contradictoires de MTU. Vérifiez chaque MTU d'interface de couche 2. Corrigez le MTU d'interface de couche 2 afin de résoudre le problème.

3. Si vous devez vérifier incapable/modification le domaine de la couche 2, vous pouvez placer la commande globale d'**ip tcp mss à** peu de valeur comme 1000, qui forceront des sessions maximum tout localement lancées de segment de données de TCP (qui inclut le BGP) à 1000. Pour plus d'informations sur cette commande, référez-vous à la section d'ip tcp mss de la *référence de commandes de Services d'applications IP de Cisco IOS*.

   En outre, vous pouvez employer la commande d'**ip tcp adjust-mss** afin de dépanner plus loin ; cette commande est configurée au niveau d'interface et affecte toutes les sessions TCP. Pour plus d'informations sur cette commande, référez-vous à la section d'ip tcp adjust-mss de la *référence de commandes de Services d'applications IP de Cisco IOS*.

4. (*Facultatif*) la détection de Maximum Transmission Unit de chemin BGP (PMTUD) ne pourrait pas générer la taille de données maximum correcte. Vous pouvez le désactiver globalement ou par voisin afin de confirmer si c'est la cause. Quand BGP PMTUD est désactivé, la taille maximum de segment BGP (MSS) se transfère sur 536 comme défini dans RFC 879.

   Pour les informations sur la façon dont désactiver PMTUD, référez-vous au support de BGP configurant pour la découverte de MTU de chemin de TCP par section de session du *guide de configuration BGP de Cisco IOS*.

   Pour plus d'informations sur PMTUD, référez-vous à ce qui est PMTUD ?