Dépanner les failles de voisinage BGP avec MTU

Table des matières

Introduction

Ce document décrit comment déterminer la cause de l'interne ou externe Border Gateway Protocol (BGP) Les battements de voisinage sont causés par MTU.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration BGP
- Unité de transmission maximale (MTU)

Assurez-vous d'effectuer ces tâches sur les deux routeurs BGP avant d'effectuer les procédures de ce document :

- Vérifiez la configuration BGP.
- Vérifiez que le voisin BGP est accessible via le protocole ICMP (Internet Control Message Protocol) et qu'aucune suppression n'est observée.
- Vérifiez que l'interface connectée utilisée pour homologue BGP n'est pas en sursouscription et n'a pas de pertes ou d'erreurs d'entrée/sortie.
- Vérifiez l'utilisation du processeur et de la mémoire.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Les voisins BGP se forment ; cependant, au moment de l'échange de préfixe, l'état BGP est abandonné et les journaux génèrent des messages de veille Hello manquants ou l'autre homologue termine la session.

Complétez ces étapes afin de déterminer si le MTU provoque le basculement des voisins BGP :

1. Utilisez les commandes suivantes afin de vérifier quel voisin est affecté et l'interface connectée sur les deux routeurs BGP. Si l'adresse d'appairage est une adresse de bouclage, vérifiez l'interface connectée via laquelle le bouclage est accessible. Vérifiez également le BGP OutQ sur les deux routeurs d'appairage. La constante OutQ non nulle est une indication forte que les mises à jour n'atteignent pas l'homologue en raison d'un problème de MTU dans le chemin.
   <#root>

   ```
   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
   ```

   <#root>

   ```
   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. Vérifiez le MTU de l'interface des deux côtés :
   <#root>

   ```
   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 haut-parleurs BGP :
<#root>

```
Router#

show ip bgp neigh 10.20.20.2 | inc segment


Datagrams (max data segment is

1460

 bytes):
Router#
```

Dans l'exemple ci-dessus, 1460 est correct car 20 octets sont affectés à l'en-tête TCP et 20 autres à l'en-tête IP.

4. Vérifiez si le chemin-mtu utilisé par BGP est activé :
<#root>

```
Router#

show ip bgp neigh 10.10.10.2 | in tcp


  Transport(tcp)

path-mtu-discovery is enabled


Router#
```

5. Envoyez une requête ping à l'homologue BGP avec le bit MTU et DF (Ne pas fragmenter) d'interface max défini :
<#root>

```
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 ICMP afin de déterminer la taille MTU maximale qui peut être utilisée :

   ```
   ping 10.10.10.2 size 1300 df
   ```

Solution

Voici quelques causes possibles :

- Le MTU de l'interface sur les deux routeurs ne correspond pas.
- Le MTU de l'interface sur les deux routeurs correspond, mais le domaine de couche 2 sur lequel la session BGP est formée ne correspond pas.
- La détection de MTU de chemin a déterminé la taille de données maximale incorrecte pour la session BGP TCP.
- La détection PMTUD (Maximum Transmission Unit Discovery) du chemin BGP a pu échouer en raison du blocage des paquets ICMP PMTUD (pare-feu ou ACL)

Voici quelques façons de résoudre les problèmes de MTU :

1. Le MTU de l'interface sur les deux routeurs doit être le même ; exécutez la commande show ip int | in MTU afin de vérifier les paramètres MTU actuels.

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

3. Si vous ne pouvez pas vérifier/modifier le domaine de couche 2, vous pouvez définir la commande globale ip tcp mss à une valeur inférieure comme 1000, ce qui peut forcer toutes les sessions de segment de données TCP max (qui inclut BGP) d'origine locale à 1000. Pour plus d'informations sur cette commande, référez-vous à la section ip tcp mss du Guide de référence des commandes des services d'applications IP Cisco IOS®.

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

4. (Facultatif) La détection PMTUD (Maximum Transmission Unit Discovery) du chemin BGP ne peut pas générer la taille de données maximale correcte. Vous pouvez le désactiver globalement ou par voisin afin de confirmer si c'est la cause. Lorsque la PMTUD BGP est

désactivée, la taille de segment maximale (MSS) BGP est définie par défaut sur 536 comme défini dans la RFC 879.

Pour plus d'informations sur la façon de désactiver PMTUD, référez-vous à la section Configuration de la prise en charge BGP pour la découverte de MTU de chemin TCP par session du Guide de configuration BGP de Cisco IOS.

Pour plus d'informations sur PMTUD, référez-vous à Résoudre la fragmentation IPv4, MTU, MSS et les problèmes PMTUD avec GRE et IPsec.

Informations connexes

- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.