BGP المجاورة في رفرفة جيران أخطاء استكشاف MTU مع MTU وإصلاحها ملاحظة فنية

المحتويات

المقدمة
المتطلبات الأساسية
المشكلة
الحل

المقدمة

يوضح هذا المستند كيفية تحديد ما إذا كانت عمليات التدفق المجاورة لبروتوكول العبارة الحدودية (BGP) الداخلية أو الخارجية ناجمة عن مشاكل الحد الأقصى لوحدة الإرسال (MTU).

المتطلبات الأساسية

تأكد من إكمال هذه المهام على كل من موجهات BGP قبل إكمال الإجراءات الواردة في هذا المستند:

- تحقق من تكوين BGP.
- تحقق من إمكانية الوصول إلى جار BGP عبر بروتوكول رسائل التحكم في الإنترنت (ICMP) ومن عدم ملاحظة حالات السقوط.
- دققت أن القارن يربط يستعمل أن نظير BGP ليس oversubscribed ولا يتلقى أي مدخل/إنتاج يسقط أو خطأ.
- تحقق من وحدة المعالجة المركزية (CPU) واستخدام الذاكرة.

المشكلة

نموذج جيران BGP، ومع ذلك، في وقت تبادل البادئة، تسقط حالة BGP وتولد السجلات رسائل keepalive الخاصة بمرحبا إلى BGP المفقودة أو يقوم النظير الآخر بإنهاء الجلسة.

أكمل هذه الخطوات لتحديد ما إذا كانت وحدة الحد الأقصى للنقل (MTU) تتسبب في رفرفة جيران BGP:

1. أستخدم الأوامر التالية للتحقق من الجوار المتأثر والواجهة المتصلة على كل من موجهات BGP. إذا كان عنوان نظير عبارة عن عنوان إسترجاع، فتحقق من الواجهة المتصلة التي يمكن من خلالها الوصول إلى الاسترجاع. تحقق أيضا من BGP OutQ على كلا موجهات نظير. OutQ الثابت غير الصفري هو إشارة قوية إلى أن التحديثات لا تصل إلى النظير بسبب وجود مشكلة في وحدة الحد الأقصى للنقل (MTU) في المسار.

```
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      2 00:00:3     0       0        3       62       64      3    4
```

```
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. تحقق من وحدة الحد الأقصى للنقل (MTU) للواجهة على كلا الجانبين:

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

3. تأكيد مقطع بيانات الحد الأقصى المتفق عليه ل TCP لكل من مكبرات صوت BGP:

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

في المثال أعلاه، 1460 صحيح حيث يتم تعيين 20 بايت إلى رأس TCP و 20 أخرى إلى رأس IP.

4. تأكيد ما إذا كان BGP المستخدم *للمسار-MTU ممكنا*:

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

5. إختبار اتصال نظير BGP باستخدام مجموعة بت الحد الأقصى للواجهة MTU و DF (عدم التجزئة):

```
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. قم بتقليل قيمة حجم ICMP لتحديد الحد الأقصى لحجم MTU الذي يمكن إستخدامه:

```
ping 10.10.10.2 size 1300 df
```

الحل

فيما يلي بعض الأسباب المحتملة:

- وحدة الحد الأقصى للنقل (MTU) للواجهة على كلا الموجهين غير متطابقة.
- تطابق وحدة الحد الأقصى للنقل (MTU) للواجهة على كلا الموجهين، ولكن مجال الطبقة 2 الذي تم تكوين جلسة BGP عليه غير مطابق.
- قام اكتشاف وحدة الحد الأقصى للنقل (MTU) للمسار بتحديد الحد الأقصى غير الصحيح لبيانات جلسة عمل TCP BGP.
- يمكن أن يفشل اكتشاف وحدة الإرسال القصوى لمسار (PMTUD) BGP بسبب حزم ICMP PMTUD المحظورة (Firewal أو ACL)

فيما يلي طرق محتملة لحل المشكلات المتعلقة بالوحدة:

1. يجب أن تكون وحدة الحد الأقصى للنقل (MTU) للواجهة على كلا الموجهين هي نفسها؛ قم بتشغيل **show ip int | في** أمر **MTU** للتحقق من إعدادات MTU الحالية.

2. إذا كانت وحدة الحد الأقصى للنقل (MTU) الخاصة بالواجهة على كلا الموجهين صحيحة (على سبيل المثال، 1500) ولكن إختبارات الاتصال مع مجموعة بت DF لا تتجاوز 1300، فقد يتضمن مجال الطبقة 2 الذي تم تكوين جلسة BGP المتأثرة عليه تكوينات MTU غير متناسقة. تحقق من كل واجهة من الطبقة 2 MTU. صححت الطبقة 2 قارن MTU in order to حللت الإصدار.

3. إذا لم تكن قادرا على التحقق/التغيير في مجال الطبقة 2، فيمكنك تعيين الأمر العام **ip tcp mss** إلى قيمة أقل مثل 1000، وهو ما سيفرض جميع جلسات أجزاء بيانات TCP max التي تم إنشاؤها محليا (والتي تتضمن BGP) على 1000. لمزيد من المعلومات حول هذا الأمر، ارجع إلى قسم ip tcp mss من *مرجع أوامر خدمات*

تطبيق IP من Cisco IOS.

بالإضافة إلى ذلك، يمكنك إستخدام الأمر **ip tcp adjust-mss** لاستكشاف الأخطاء وإصلاحها بشكل إضافي؛ يتم تكوين هذا الأمر على مستوى الواجهة ويؤثر على جميع جلسات عمل TCP. لمزيد من المعلومات حول هذا الأمر، ارجع إلى قسم ip tcp adjust-mss في *مرجع أوامر خدمات تطبيق IP من Cisco IOS*.

4. (*إختياري*) قد لا يعمل اكتشاف وحدة الإرسال القصوى لمسار BGP (PMTUD) على إنشاء الحد الأقصى الصحيح لحجم البيانات. يمكنك تعطيله بشكل عام أو لكل جار لتأكيد ما إذا كان هذا هو السبب. عندما يتم تعطيل BGP PMTUD، يتم تعيين الحد الأقصى لحجم مقطع BGP (MSS) افتراضيا على 536 كما هو محدد في RFC 879.

أحلت لمعلومة على كيف أن يعجز PMTUD، ال بشكل BGP دعم ل TCP ممر MTU إكتشاف لكل جلسة قسم من *ال cisco ios BGP تشكيل مرشد*.

لمزيد من المعلومات حول PMTUD، ارجع إلى ما هو PMTUD؟

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).