

BGP Neighbor Flaps mit MTU-Fehlerbehebung - Technische Hinweise

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Problem](#)

[Lösung](#)

Einführung

In diesem Dokument wird beschrieben, wie festgestellt werden kann, ob interne oder externe Border Gateway Protocol (BGP)-Nachbar-Flaps durch Probleme mit der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) verursacht werden.

Voraussetzungen

Stellen Sie sicher, dass Sie diese Aufgaben auf beiden BGP-Routern ausführen, bevor Sie die in diesem Dokument beschriebenen Schritte durchführen:

- Überprüfen Sie die BGP-Konfiguration.
- Stellen Sie sicher, dass der BGP-Nachbar über das Internet Control Message Protocol (ICMP) erreichbar ist und dass keine Verwerfungen beobachtet werden.
- Stellen Sie sicher, dass die verbundene Schnittstelle, die für das Peer-BGP verwendet wird, nicht überbelegt ist und keine Eingabe-/Ausgabeverluste oder Fehler aufweist.
- Überprüfen Sie die CPU- und Speichernutzung.

Problem

BGP-Nachbarn Beim Präfixaustausch wird der BGP-Status jedoch unterbrochen, und die Protokolle generieren fehlende BGP Hello-Keepalives, oder der andere Peer beendet die Sitzung.

Gehen Sie wie folgt vor, um zu ermitteln, ob die MTU die Flapping-Ursache für die BGP-Nachbarn ist:

1. Mit den folgenden Befehlen können Sie überprüfen, welcher Nachbar von beiden BGP-Routern betroffen ist und welche Schnittstelle mit ihnen verbunden ist. Wenn es sich bei der Peering-Adresse um eine Loopback-Adresse handelt, überprüfen Sie die verbundene Schnittstelle, über die der Loopback erreichbar ist. Überprüfen Sie außerdem, ob der BGP OutQ auf beiden Peering-Routern angezeigt wird. Der konsistente Nicht-Null-OutQ ist ein

starker Hinweis darauf, dass Updates aufgrund eines MTU-Problems im Pfad nicht den Peer erreichen.

```
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. Überprüfen Sie die MTU-Schnittstellengröße auf beiden Seiten:

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

3. Bestätigen Sie das TCP-vereinbarte max. Datensegment für beide BGP-Lautsprecher:

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

Im obigen Beispiel ist 1460 richtig, da dem TCP-Header 20 Byte und dem IP-Header 20 Byte zugewiesen werden.

4. Überprüfen Sie, ob BGP *path-mtu* verwendet ist:

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

5. Pingen Sie den BGP-Peer mit einem MTU- und DF-Bitsatz (keine Fragment) für die maximale Schnittstelle:

```
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. Verringern Sie den ICMP-Größenwert, um die maximale MTU-Größe zu bestimmen, die verwendet werden kann:

```
ping 10.10.10.2 size 1300 df
```

Lösung

Hier einige mögliche Ursachen:

- Die Schnittstellen-MTU auf beiden Routern stimmt nicht überein.
- Die Schnittstellen-MTU auf beiden Routern stimmt überein, die Layer-2-Domäne, über die die BGP-Sitzung gebildet wird, stimmt jedoch nicht überein.
- Die MTU-Pfaderkennung hat die falsche maximale Datenbasis für die TCP-BGP-Sitzung ermittelt.
- Die PMTUD (Maximum Transmission Unit Discovery) für BGP Path könnte fehlschlagen, da PMTUD-ICMP-Pakete blockiert sind (Firewall oder ACL).

Es gibt folgende Möglichkeiten zur Behebung von MTU-Problemen:

1. Die Schnittstellen-MTU auf beiden Routern muss identisch sein. Ausführen der **show ip int |**

im **MTU**-Befehl, um die aktuellen MTU-Einstellungen zu überprüfen.

2. Wenn die MTU der Schnittstelle auf beiden Routern korrekt ist (z. B. 1500), die Ping-Tests mit DF-Bitsatz jedoch 1300 nicht überschreiten, kann die Layer-2-Domäne, auf der die betroffene BGP-Sitzung gebildet wird, inkonsistente MTU-Konfigurationen enthalten. Überprüfen Sie alle MTUs der Layer-2-Schnittstellen. Korrigieren Sie die MTU der Layer-2-Schnittstelle, um das Problem zu beheben.
3. Wenn Sie die Layer-2-Domäne nicht überprüfen/ändern können, können Sie den globalen Befehl **ip tcp mss** auf einen niedrigeren Wert wie 1000 festlegen, der alle lokal erstellten TCP-Sitzungen für max. Datensegmente (einschließlich BGP) auf 1000 zwingt. Weitere Informationen zu diesem Befehl finden Sie im Abschnitt [ip tcp mss](#) der *Befehlsreferenz für Cisco IOS IP-Anwendungsdienste*.

Darüber hinaus können Sie den Befehl **ip tcp adjust-mss** verwenden, um weitere Probleme zu beheben. Dieser Befehl wird auf Schnittstellenebene konfiguriert und betrifft alle TCP-Sitzungen. Weitere Informationen zu diesem Befehl finden Sie im Abschnitt [ip tcp adjust-mss](#) der *Befehlsreferenz für Cisco IOS IP-Anwendungsdienste*.

4. (*Optional*) Möglicherweise generiert die PMTUD (Maximum Transmission Unit Discovery) von BGP Path nicht die richtige maximale Datengröße. Sie können die Funktion global oder pro Nachbar deaktivieren, um zu überprüfen, ob dies die Ursache ist. Wenn die BGP-PMTUD deaktiviert ist, wird die in [RFC 879](#) definierte maximale Segmentgröße (MSS) für BGP auf 536 festgelegt.

Informationen zum Deaktivieren der PMTUD finden Sie im Abschnitt [Konfigurieren der BGP-Unterstützung für die TCP-Pfad-MTU-Erkennung pro Sitzung](#) im *Cisco IOS BGP-Konfigurationshandbuch*.

Weitere Informationen zur PMTUD finden Sie unter [Was ist die PMTUD?](#)