

Fehlerbehebung bei Flapping-BGP-Routen (rekursiver Routing-Fehler)

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konventionen](#)

[Problem](#)

[Symptome](#)

[Fehler bei rekursivem Routing](#)

[Ursachen für einen Fehler beim rekursiven Routing](#)

[Lösung](#)

[Streckendämpfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Flapping-Border Gateway Protocol (BGP)-Routen beschrieben, die durch rekursive Routing-Fehler verursacht wurden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

In diesem Dokument wird die Fehlerbehebung bei Flapping-Border Gateway Protocol (BGP)-Routen beschrieben, die durch rekursive Routing-Fehler verursacht wurden.

Häufige Symptome eines rekursiven Routing-Fehlers im BGP:

- Ständiges Löschen und Wiedereinsetzen von BGP-Routen in die Routing-Tabelle
- Verlust der Verbindung zu Zielen, die vom BGP erfasst wurden

Weitere Informationen finden Sie im folgenden Netzwerkdiagramm, wenn Sie dieses Dokument verwenden:



Netzwerkdiagramm

Weitere Informationen finden Sie in den folgenden Konfigurationen, wenn Sie dieses Dokument verwenden:

Rtr-A

```
hostname RTR-A
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface Serial8/0
 ip address 192.168.16.1 255.255.255.252
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 10.20.20.20 remote-as 2
 neighbor 10.20.20.20 ebgp-multihop 2
 neighbor 10.20.20.20 update-source Loopback0
!
ip route 10.20.20.0 255.255.255.0 192.168.16.2
```

Rtr-B

```
hostname RTR-B
!
interface Loopback0
 ip address 10.20.20.20 255.255.255.255
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
!
interface Serial8/0
 ip address 192.168.16.2 255.255.255.252
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 network 10.20.20.20 mask 255.255.255.255
```

```

network 172.16.1.0 mask 255.255.255.0
neighbor 10.10.10.10 remote-as 1
neighbor 10.10.10.10 ebgp-multihop 2
neighbor 10.10.10.10 update-source Loopback0
no auto-summary
!
ip route 10.10.10.0 255.255.255.0 192.168.16.1
!
```

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Problem

Symptome

Diese beiden Symptome treten bei einem rekursiven Routing-Fehler auf:

- Kontinuierliches Flapping der vom BGP bezogenen Routen in der IP-Routing-Tabelle. Beobachten Sie die Routing-Tabelle kontinuierlich für einige Minuten, um das Flapping zu sehen.

```
RTR-A#show ip route
```

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - ISIS level-1, L2 - ISIS level-2, ia - ISIS inter are
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B       10.20.20.20/32 [20/0] via 10.20.20.20, 00:00:35
S       10.20.20.0/24 [1/0] via 192.168.16.2
      172.16.0.0/24 is subnetted, 1 subnets
B       172.16.1.0 [20/0] via 10.20.20.20, 00:00:35
      10.0.0.0/32 is subnetted, 1 subnets
C       10.10.10.10 is directly connected, Loopback0
      192.168.16.0/30 is subnetted, 1 subnets
C       192.168.16.0 is directly connected, Serial18/0
```

Hinweis: Es ist hilfreich, die **show ip-Route** zu verwenden. | **include , 00:00** Befehl, um Flapping-Routen bei großen Routing-Tabellen zu beobachten.

Nachdem Sie etwa eine Minute gewartet haben, ändern sich die Ergebnisse des Befehls **show ip route** wie folgt:

```
RTR-A#show ip route
[...]
```

Gateway of last resort is not set

```
10.0.0.0/24 is subnetted, 1 subnets
S    10.20.20.0 [1/0] via 192.168.16.2
10.0.0.0/32 is subnetted, 1 subnets
C    10.10.10.10 is directly connected, Loopback0
192.168.16.0/30 is subnetted, 1 subnets
C    192.168.16.0 is directly connected, Serial18/0
```

Hinweis: Die BGP-Routen fehlen in der vorherigen Routing-Tabelle.

- Wenn die BGP-Routen in der Routing-Tabelle vorhanden sind, schlägt die Verbindung zu diesen Netzwerken fehl. Um dies zu beobachten, schlägt ein Ping an den gültigen Host 172.16.1.1 fehl, wenn die Routing-Tabelle des Rtr-A die vom BGP bezogene Route 172.16.1.0/24 in ihrer Routing-Tabelle enthält.

```
RTR-A#show ip route 172.16.1.0
Routing entry for 172.16.1.0/24
  Known via "bgp 1", distance 20, metric 0
  Tag 2, type external
  Last update from 10.20.20.20 00:00:16 ago
  Routing Descriptor Blocks:
    * 10.20.20.20, from 10.20.20.20, 00:00:16 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

```
RTR-A#ping 172.16.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
RTR-A#
```

Fehler bei rekursivem Routing

Beobachten Sie auf Rtr-A die Route zum BGP-Peer 10.20.20.20. Die Route flattert zwischen den beiden nächsten Hops durchgängig jede Minute oder so.

```
RTR-A#show ip route 10.20.20.20
Routing entry for 10.20.20.20/32
  Known via "bgp 1", distance 20, metric 0
  Tag 2, type external
  Last update from 10.20.20.20 00:00:35 ago
  Routing Descriptor Blocks:
    * 10.20.20.20, from 10.20.20.20, 00:00:35 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

Die Route zur BGP-Peer-IP-Adresse wird vom BGP selbst erfasst. Dadurch kommt es zu einem rekursiven Routing-Fehler.

Nach etwa einer Minute ändert sich die Route wie folgt:

```
RTR-A#show ip route 10.20.20.20
Routing entry for 10.20.20.0/24
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
    * 192.168.16.2
```

Route metric is 0, traffic share count is 1

Ursachen für einen Fehler beim rekursiven Routing

Diese Schritte beschreiben die Ursache von rekursiven Routing-Fehlern:

1. Weitere Informationen finden Sie in der Konfiguration [von Rtr-A](#). In dieser Konfiguration wird die statische Route 10.20.20.0/24 so konfiguriert, dass sie auf den direkt verbundenen Next-Hop 192.168.16.2 verweist. Bei dieser statischen Route wird eine BGP-Sitzung mit Peer-Rtr-B 10.20.20.20 eingerichtet.
2. Rtr-B kündigt die BGP-Routen 172.16.1.0/24 und 10.20.20.20/32 zu Rtr-A mit seiner Loopback-IP-Adresse 10.20.20.20 als Next-Hop an.
3. Rtr-A empfängt von Rtr-B angekündigte BGP-Routen und versucht, 10.20.20.20/32 zu installieren. Dies ist spezifischer als 10.20.20.0/24, die bereits in Rtr-A als statische Route konfiguriert ist. Da die Route mit der längsten Übereinstimmung bevorzugt wird, wird 10.20.20.20/32 gegenüber 10.20.20.0/24 bevorzugt. Weitere Informationen finden Sie unter [Routenauswahl in Cisco Routern](#). Die installierte Route 10.20.20.20/32 hat den Next-Hop 10.20.20.20 (Rtr-B Peering-IP-Adresse) in der Routing-Tabelle. Dies führt zu einem rekursiven Routing-Fehler, da die Route zu 10.20.20.20/32 einen Next-Hop von sich selbst aufweist. Um zu verstehen, warum das rekursive Routing in dieser speziellen Situation fehlschlägt, müssen Sie verstehen, wie der Routing-Algorithmus funktioniert. Für jede nicht direkt verbundene Route in der Routing-Tabelle, deren nächste Hop-IP-Adresse keine direkt verbundene Schnittstelle des Routers ist, sucht der Algorithmus rekursiv in der Routing-Tabelle, bis er eine direkt verbundene Schnittstelle findet, an die er die Pakete weiterleiten kann. In dieser speziellen Situation lernt Rtr-A eine Route zum nicht direkt verbundenen Netzwerk 10.20.20.20/32 mit einem nicht direkt verbundenen nächsten Hop von 10.20.20.20 (selbst). Der Routing-Algorithmus führt einen rekursiven Routing-Schleifenfehler aus, da er keine direkt verbundene Schnittstelle findet, an die Pakete gesendet werden sollen, die für 10.20.20.20/32 bestimmt sind.
4. Der Router erkennt, dass diese nicht direkt verbundene Route 10.20.20.20/32 einen rekursiven Routing-Fehler aufweist, und zieht 10.20.20.20/32 aus der Routing-Tabelle zurück. Daher werden alle vom BGP bezogenen Routen mit der Next-Hop-IP-Adresse 10.20.20.20 ebenfalls aus der Routing-Tabelle entfernt.
5. Der gesamte Prozess wiederholt sich ab [Schritt 1](#). Sie können dies bestätigen, wenn Sie den Befehl `debug ip routing` ausführen. **Hinweis:** Führen Sie vor dem Ausführen eines **Debug-**Befehls den Befehl `debug` für eine Zugriffskontrollliste (ACL) für ein bestimmtes Netzwerk aus, um die Ausgabe von debug einzuschränken. Konfigurieren Sie in diesem Beispiel eine ACL, um die Debug-Ausgabe einzuschränken.

```
RTR-A(config)#access-list 1 permit 10.20.20.20
RTR-A(config)#access-list 1 permit 172.16.1.0
RTR-A(config)#end
```

```
RTR-A#debug ip routing 1
```

```
IP routing debugging is on for access list 1
```

```
00:29:50: RT: add 10.20.20.20/32 via 10.20.20.20, bgp metric [20/0]
```

```
00:29:50: RT: add 172.16.1.0/24 via 10.20.20.20, bgp metric [20/0]
```

```
00:30:45: RT: recursion error routing 10.20.20.20 - probable routing loop
```

```
00:30:45: RT: recursion error routing 10.20.20.20 - probable routing loop
```

```
00:30:45: RT: recursion error routing 10.20.20.20 - probable routing loop
```

```
00:30:46: RT: recursion error routing 10.20.20.20 - probable routing loop
```

```
00:30:46: RT: recursion error routing 10.20.20.20 - probable routing loop
00:30:48: RT: recursion error routing 10.20.20.20 - probable routing loop
00:30:48: RT: recursion error routing 10.20.20.20 - probable routing loop
00:30:50: RT: del 10.20.20.20/32 via 10.20.20.20, bgp metric [20/0]
00:30:50: RT: delete subnet route to 10.20.20.20/32
00:30:50: RT: del 172.16.1.0/24 via 10.20.20.20, bgp metric [20/0]
00:30:50: RT: delete subnet route to 172.16.1.0/24
```

6. Wenn die Routenrekursion kontinuierlich fehlschlägt, wird diese Fehlermeldung angezeigt:

```
%COMMON_FIB-SP-6-FIB_RECURSION: 10.71.124.25/32 has too many (8) levels of
recursion during setting up switching info
%COMMON_FIB-SP-STDBY-6-FIB_RECURSION: 10.71.124.25/32 has too many (8)
levels of recursion during setting up switching info
```

Dies ist darauf zurückzuführen, dass TCP-Neuübertragungen in einem MPLS-fähigen Netzwerk erfolgen. Wenn einmal ein Fehler beim Senden einer BGP-Keepalive-Nachricht an den BGP-Peer auftritt, weil die Transportverbindung unterbrochen ist, akzeptiert der benachbarte BGP-Peer keine weiteren Keepalive-Pakete, obwohl TCP die ausgefallene Nachricht erneut über den Backup-Pfad sendet. Dies führt letztendlich dazu, dass der BGP-Peer ausfällt und die Verweilzeit abläuft. Dieses Problem tritt nur auf, wenn MPLS auf Catalyst 6500 oder Cisco 7600 konfiguriert ist. Diese Informationen sind in der Cisco Bug-ID [CSCsj89544](#) enthalten. **Hinweis:** Nur registrierte Cisco Benutzer können auf interne Fehlerinformationen und andere Tools zugreifen.

Lösung

Die Lösung(en) für dieses Problem werden in diesen Details erläutert.

Fügen Sie in Rtr-A eine bestimmte statische Route für die IP-Adresse des BGP-Peers hinzu (in diesem Fall 10.20.20.20).

```
RTR-A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RTR-A(config)#ip route 10.20.20.20 255.255.255.255 192.168.16.2
```

Durch die Konfiguration einer statischen Route für das Präfix 10.20.20.20/32 wird sichergestellt, dass eine dynamisch ermittelte BGP-Route 10.20.20.20/32 nicht in die Routing-Tabelle installiert wird und somit die rekursive Routing-Schleifensituation vermieden wird. Weitere Informationen finden Sie unter [Routenauswahl in Cisco Routern](#).

Hinweis: Wenn EBGP-Peers so konfiguriert sind, dass sie einander mit Standardrouten erreichen, wird die BGP-Nachbarschaft nicht angezeigt. Dies dient dazu, Fluktuationen und Routing-Schleifen zu vermeiden.

Ein Ping an 172.16.1.1 bestätigt die Lösung.

```
RTR-A#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/40 ms
```

Streckendämpfung

Route Dampening ist eine BGP-Funktion, die entwickelt wurde, um die Propagierung von Flapping-Routen über ein Internetwork zu minimieren. Die vom ISP empfohlenen Werte sind die Standardwerte unter Cisco IOS[®]. Sie müssen diesen Befehl nur konfigurieren, um ihn zu aktivieren.

```
router bgp <AS number>  
  bgp dampening
```

Der Befehl **bgp dampening** legt Standardwerte für die Dämpfungparameter fest, z. B. Halbzeit = 15 Minuten, Wiederverwendung = 750, Unterdrückung = 2000 und Maximale Unterdrückungszeit = 60. Diese Werte können vom Benutzer konfiguriert werden. Cisco empfiehlt jedoch, sie unverändert zu lassen.

Zugehörige Informationen

- [Was bedeutet die Fehlermeldung "%BGP-3-INSUFCHUNKS: Ungenügende Chunk-Pools für aspath"?](#)
- [Warum schalten BGP-Nachbarn zwischen Inaktivität, Verbindungs- und Aktivstatus um?](#)
- [IP-Routing-/BGP-Unterstützung](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.