BGP buurtaps met TechNotes voor probleemoplossing

Inhoud

Inleiding

In dit document wordt beschreven hoe kan worden vastgesteld of de BGP-problemen (internal or Buitenborder Gateway Protocol) bij de grensposten worden veroorzaakt door problemen met de maximale transmissieeenheid (MTU).

Voorwaarden

Zorg ervoor dat u deze taken op beide BGP-routers uitvoert voordat u de procedures in dit document uitvoert:

- Controleer de BGP-configuratie.
- Controleer dat de BGP-buurman bereikbaar is via Internet Control Message Protocol (ICMP), en er worden geen druppels waargenomen.
- Controleer dat de aangesloten interface die wordt gebruikt om BGP te peer niet oversubscript is, en geen input/output druppels of fouten heeft.
- Controleer de CPU en het geheugengebruik.

Probleem

BGP-buren vormen: op het moment dat het voorvoegsel wordt uitgewisseld, daalt de BGP-staat echter en het blog genereert ontbrekende BGP-hallo-keepalives of het andere peer-terminis de sessie.

Voltooi deze stappen om vast te stellen of de MTU de BGP-buren ertoe aanzet te flap te gaan:

1. Gebruik de volgende opdrachten om te controleren welke buurman wordt beïnvloed en de aangesloten interface op beide BGP-routers. Als het peeradres een loopback adres is, controleer de aangesloten interface waardoor de loopback bereikbaar is. Controleer ook op BGP OutQ op beide peilrouters. Het consistente niet-nulpunt van OutQ is een sterke aanwijzing dat updates niet de peer bereiken door een MTU-kwestie in het pad.

```
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. Controleer de interface-MTU aan beide kanten:
```
Router#show ip int g1/0 | i MTU
MTU is 1500 bytes
Router#
```
3. Bevestig het TCP-overeengekomen max-gegevenssegment voor beide BGP-luidsprekers:
```
Router#show ip bgp neigh 20.20.20.2 | inc segment
Datagrams (max data segment is 1460 bytes):
Router#
```
In het bovenstaande voorbeeld is 1460 correct aangezien 20 bytes zijn toegewezen aan de TCP-header en nog eens 20 aan de IP-header.

4. Controleer of BGP gebruikt *path-mtu is ingeschakeld*:
```
Router#show ip bgp neigh 10.10.10.2 | in tcp
Transport(tcp) path-mtu-discovery is enabled
Router#
```
5. Ping the BGP peer met max interface MTU en DF (Don't Fragment) bit set:
```
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. Verlaag de grootte van ICMP om de maximale grootte van MTU te bepalen die kan worden gebruikt:
```
ping 10.10.10.2 size 1300 df
```

Oplossing

Hier zijn een aantal mogelijke oorzaken:

- De interface MTU op beide routers komt niet overeen.
- De interface MTU op beide routers matchen maar het Layer 2-domein waarop de BGP-sessie wordt gevormd, komt niet overeen.
- De ontdekking van het pad MTU bepaalde de incorrecte max gegevens voor de TCP BGP-sessie.
- De PMTUD voor de detectie van de maximale transmissieeenheid van het BGP-pad (PPMTUD) kan niet werken door PMTUD ICMP-pakketten geblokkeerd (firewalls of ACL's)

Hier zijn mogelijke manieren om MTU-problemen op te lossen:

1. De interface-MTU op beide routers moet gelijk zijn; de **ip-toets uitvoeren | in MTU** commando om de huidige MTU-instellingen te controleren.

2. Als de interface-MTU op beide routers correct is (bijvoorbeeld 1500) maar de ping-tests met

DF-bit-set niet groter zijn dan 1300, kan Layer 2-domein waarop de getroffen BGP-sessie wordt gevormd, inconsistente MTU-configuraties omvatten. Controleer elke Layer 2 interface MTU. Corrigeer de Layer 2 interface MTU om het probleem op te lossen.

3. Als u Layer 2-domein niet kunt controleren/wijzigen, kunt u de **ip tcp mss** global opdracht instellen op minder waarde zoals 1000, wat alle lokaal geïnitieerde TCP max-datasegroepen (inclusief BGP) op 1000 zal dwingen. Raadpleeg voor meer informatie over deze opdracht het ip mss-gedeelte van de *Cisco IOS IP Application Services Opdracht Referentie*.

   Daarnaast kunt u de opdracht **ip** cp **adapt-mss** gebruiken om de oplossing verder te verhelpen; deze opdracht wordt ingesteld op interfaceniveau en heeft invloed op alle TCP sessies . Raadpleeg voor meer informatie over deze opdracht het IP TCP-aanpassings-mss gedeelte van de *Cisco IOS IP Application Services Opdracht Referentie*.

4. (*Optioneel*) Mogelijk genereert de PMTUD-detectie (Maximale Transmission Unit) van het BGP Path niet de juiste maximale gegevensgrootte. U kunt deze wereldwijd of per buurman uitschakelen om te bevestigen of dit de oorzaak is. Wanneer BGP PMTUD is uitgeschakeld, blijft de BGP Maximum Segment Size (MSS) standaard 536 zoals gedefinieerd in RFC 879.

   Raadpleeg voor informatie over het uitschakelen van PMTUD de BGP-ondersteuning configureren voor TCP Path MTU-detectie per sessie van de *Cisco IOS BGP-configuratiegids*.

   Raadpleeg voor meer informatie over PMTUD wat is PMTUD?