Nota tecnica sulla flap dei router adiacenti BGP con MTU per la risoluzione dei problemi

Sommario

Introduzione

In questo documento viene descritto come determinare se i flap dei nodi adiacenti del protocollo BGP (Border Gateway Protocol) interno o esterno sono causati da problemi di MTU (Maximum Transmission Unit).

Prerequisiti

Prima di completare le procedure descritte in questo documento, accertarsi di aver completato queste attività su entrambi i router BGP:

- Controllare la configurazione BGP.
- Verificare che il router adiacente BGP sia raggiungibile tramite il protocollo ICMP (Internet Control Message Protocol) e che non vengano rilevate perdite.
- Verificare che l'interfaccia connessa utilizzata per il peer BGP non sia sovrascritta e non contenga perdite o errori di input/output.
- Controllare l'utilizzo della CPU e della memoria.

Problema

formazione dei vicini BGP; tuttavia, al momento dello scambio del prefisso, lo stato BGP viene interrotto e i log generano hello keepalive BGP mancanti oppure l'altro peer termina la sessione.

Completare questi passaggi per determinare se l'MTU causa il flap dei router adiacenti BGP:

1. Utilizzare i comandi seguenti per controllare il router adiacente interessato e l'interfaccia connessa su entrambi i router BGP. Se l'indirizzo di peering è un indirizzo di loopback, controllare l'interfaccia connessa attraverso la quale il loopback è raggiungibile. Verificare inoltre la presenza di BGP OutQ su entrambi i router peer. OutQ diversi da zero coerenti sono una forte indicazione che gli aggiornamenti non raggiungono il peer a causa di un problema MTU nel percorso.

```
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. Controllare l'MTU dell'interfaccia su entrambi i lati:

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

3. Confermare il segmento di dati TCP massimo concordato per entrambi gli altoparlanti BGP:

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

   Nell'esempio di cui sopra, il valore 1460 è corretto in quanto 20 byte vengono assegnati all'intestazione TCP e altri 20 all'intestazione IP.

4. Verificare se l'*mtu del percorso* BGP utilizzato *è abilitata*:

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

5. Eseguire il ping del peer BGP con MTU dell'interfaccia massima e bit DF (non frammentare) impostati:

```
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. Diminuire il valore delle dimensioni ICMP per determinare le dimensioni massime della MTU utilizzabili:

```
ping 10.10.10.2 size 1300 df
```

Soluzione

Di seguito sono elencate alcune possibili cause:

- L'MTU dell'interfaccia su entrambi i router non corrisponde.
- L'MTU dell'interfaccia su entrambi i router corrisponde, ma il dominio di layer 2 su cui viene formata la sessione BGP non corrisponde.
- Il rilevamento dell'MTU del percorso ha determinato un valore errato nel formato dati massimo per la sessione TCP BGP.
- Impossibile eseguire il PMTUD (Maximum Transmission Unit Discovery) del percorso BGP a causa di pacchetti ICMP PMTUD bloccati (firewall o ACL)

Di seguito sono riportati i possibili modi per risolvere i problemi relativi all'MTU:

1. L'MTU dell'interfaccia su entrambi i router deve essere la stessa; eseguire il comando **show ip int | nel** comando **MTU** per controllare le impostazioni MTU correnti.

2. Se l'MTU dell'interfaccia su entrambi i router è corretta (ad esempio, 1500) ma i test ping con bit DF impostato non superano 1300, il dominio di layer 2 in cui si forma la sessione BGP interessata potrebbe includere configurazioni MTU incoerenti. Controllare ciascuna MTU dell'interfaccia di layer 2. Per risolvere il problema, correggere l'MTU dell'interfaccia di layer 2.

3. Se non è possibile controllare/modificare il dominio di layer 2, è possibile impostare il comando **ip tcp mss** global su un valore inferiore, come 1000, che forzerà tutte le sessioni del segmento dati TCP max originate localmente (incluso BGP) a 1000. Per ulteriori informazioni sul comando, consultare la sezione ip tcp mss nella *guida di riferimento dei comandi di Cisco IOS IP Application Services*.

   Inoltre, è possibile usare il comando **ip tcp adjust-mss** per risolvere ulteriormente il problema; questo comando è configurato a livello di interfaccia e influisce su tutte le sessioni TCP. Per ulteriori informazioni sul comando ip tcp adjust-mss, consultare la sezione ip tcp adjust-mss nella *guida di riferimento dei comandi di Cisco IOS IP Application Services*.

4. (*Facoltativo*) Il rilevamento della MT del percorso BGP potrebbe non generare le dimensioni massime dei dati corrette. È possibile disabilitarlo globalmente o per ciascun router adiacente per verificare se questa è la causa. Quando il PMTUD BGP è disabilitato, il valore predefinito del parametro BGP Maximum Segment Size (MSS) è 536, come definito nella RFC 879.

   Per informazioni su come disabilitare il PMTUD, fare riferimento alla sezione Configurazione del supporto BGP per il rilevamento dell'MTU del percorso TCP per sessione nella *guida alla configurazione BGP di Cisco IOS*.

   Per ulteriori informazioni sulla funzionalità PMTUD, consultare il documento sulla descrizione della funzionalità PMTUD?