Verifica dell'impatto degli stati dell'interfaccia del tunnel GRE

Sommario

Introduzione

In questo documento vengono descritte le diverse condizioni che possono influire sullo stato di un'interfaccia del tunnel GRE (Generic Routing Encapsulation).

Premesse

I tunnel GRE sono progettati per essere completamente privi di stato. Ciò significa che ogni endpoint del tunnel non mantiene alcuna informazione sullo stato o sulla disponibilità dell'endpoint del tunnel remoto.

Di conseguenza, per impostazione predefinita, il router dell'endpoint del tunnel locale non può disattivare il protocollo di linea dell'interfaccia del tunnel GRE se l'estremità remota del tunnel non è raggiungibile.

La possibilità di contrassegnare un'interfaccia come "inattiva" (in questa situazione) viene usata per rimuovere eventuali route statiche nella tabella di routing che usano quell'interfaccia come interfaccia in uscita.

In particolare, se il protocollo di linea di un'interfaccia viene modificato in "down", le route statiche che indicano tale interfaccia vengono rimosse dalla tabella di routing.

In questo modo, è possibile installare un percorso statico alternativo (mobile) o un percorso PBR (Policy Based Routing) per selezionare un hop o un'interfaccia alternativi.

Inoltre, esistono altre applicazioni che vengono attivate quando cambia lo stato di un'interfaccia,

ad esempio 'backup interface <b-interface>'.

Quattro diversi stati del tunnel

Sono disponibili quattro stati possibili in cui esiste un'interfaccia del tunnel GRE:

1. Up/Up (Attivo/Attivo): indica che il tunnel è completamente funzionante e che trasmette il traffico. Il protocollo è attivo sia a livello amministrativo che amministrativo.
2. Spegnimento/arresto amministrativo: ciò implica che l'interfaccia è stata chiusa manualmente.
3. Up/Down: questo implica che, anche se il tunnel è amministrativamente attivo, qualcosa causa il mancato funzionamento del protocollo di linea sull'interfaccia.
4. Reset/down (Ripristino/inattività) - In genere si tratta di uno stato transitorio quando il software reimposta il tunnel. Questo in genere si verifica quando il tunnel è configurato in modo errato con un NHS (Next Hop Server) che sia il proprio indirizzo IP.

Quando si crea un'interfaccia del tunnel e non vi vengono applicate altre configurazioni, l'interfaccia non viene chiusa per impostazione predefinita:

<#root>

```
Router#
```

show run interface tunnel 1

```
Building configuration...

Current configuration : 40 bytes
!
interface Tunnel1
 no ip address
end
```

In questo stato, l'interfaccia è sempre su/giù:

<#root>

```
Router(config-if)#
```

do show ip interface brief

```
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         172.16.52.1     YES NVRAM  administratively down down
GigabitEthernet0/1         10.36.128.49    YES NVRAM  down                  down
GigabitEthernet0/2         unassigned      YES NVRAM  down                  down
GigabitEthernet0/3         unassigned      YES NVRAM  down                  down
Loopback1                  192.168.2.1     YES NVRAM  up                    up
Tunnel1                    unassigned      YES unset  up                    down
```

Infatti, poiché l'interfaccia è abilitata a livello amministrativo, ma non ha un'origine o una destinazione tunnel, il protocollo di linea non è attivo.

Per configurare l'interfaccia come attiva/inattiva, è necessario configurare un'origine e una destinazione del tunnel valide:

```
<#root>

Router#

show run interface tunnel  1


Building configuration...

Current configuration : 113 bytes
!
interface Tunnel1
 ip address 10.1.1.1 255.255.255.0
 tunnel source Loopback1
 tunnel destination 10.0.0.1
end

Router#

show ip interface brief


Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         172.16.52.1     YES NVRAM  up                    up
GigabitEthernet0/1         10.36.128.49    YES NVRAM  down                  down
GigabitEthernet0/2         unassigned      YES NVRAM  down                  down
GigabitEthernet0/3         unassigned      YES NVRAM  down                  down
Loopback0                  unassigned      YES unset  up                    up
Loopback1                  192.168.2.1     YES manual up                    up
Tunnel1                    10.1.1.1         YES manual up                    up
```

La sequenza precedente mostra che:

- Un'origine tunnel valida è costituita da qualsiasi interfaccia che si trova nello stato attivo/attivo e su cui è configurato un indirizzo IP.
- Ad esempio, se l'origine del tunnel è stata modificata in Loopback0, l'interfaccia del tunnel scenderà anche se Loopback0 si trova nello stato attivo/attivo:

```
<#root>

Router(config)#

interface tunnel 1


Router(config-if)#

tunnel source loopback 0
```

```
Router(config-if)#
*Sep  6 19:51:31.043: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to do
```

- Una destinazione del tunnel valida è una destinazione instradabile. Tuttavia, non è necessario che sia raggiungibile, come dimostra il seguente test ping:

<#root>

```
Router#
```

show ip route 10.0.0.1

```
% Network not in table
Router#
```

show ip route | inc 0.0.0.0

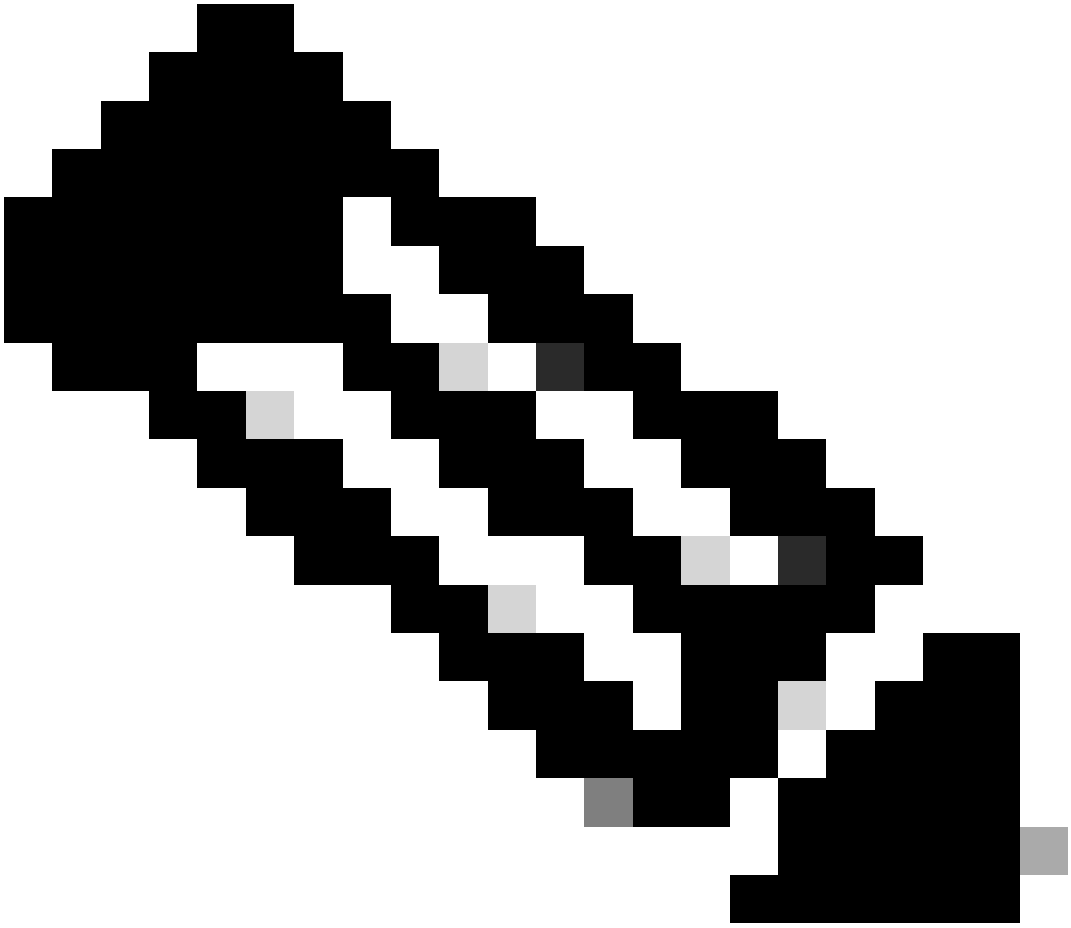
```
Gateway of last resort is 172.16.52.100 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 172.16.52.100
Router#
```

ping 10.0.0.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Finora il tunnel è stato configurato come tunnel GRE point-to-point (P2P), l'impostazione predefinita.

Se il tunnel dovesse essere modificato in un tunnel GRE (Multipoint GRE), tutto ciò che è necessario per uno stato attivo è un'origine tunnel valida.



Nota: un tunnel GRE può avere molte destinazioni tunnel, che non possono essere usate per controllare lo stato dell'interfaccia del tunnel.

<#root>

```
Router#
```

show run interface tunnel 1

```
Building configuration...

Current configuration : 129 bytes
!
interface Tunnel1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 tunnel source Loopback1
 tunnel mode gre multipoint
end

Router#
```

```
show ip interface brief | include Tunnel

Tunnel1                    10.1.1.1         YES manual up                    up
```

In qualsiasi momento, se l'interfaccia del tunnel è chiusa manualmente, il tunnel passa immediatamente allo stato di disattivazione/disattivazione amministrativa:

```
<#root>

Router#

show run interface tunnel 1


Building configuration...

Current configuration : 50 bytes
!
interface Tunnel1
 no ip address

shutdown


end

Router#

show ip interface brief | include Tunnel


Tunnel1                    unassigned      YES unset

administratively down down
```

Stato tunnel GRE P2P

Un'interfaccia del tunnel GRE P2P in genere viene visualizzata non appena configurata con un indirizzo di origine o un'interfaccia valida del tunnel attiva e un indirizzo IP di destinazione del tunnel instradabile (mostrato in precedenza).

Protocollo di linea non attivo localmente sul router

In circostanze normali, ci sono solo tre motivi per cui un tunnel GRE deve essere nello stato attivo/inattivo:

- Non è disponibile alcun percorso, incluso il percorso predefinito, verso l'indirizzo di destinazione del tunnel.
- L'interfaccia che ancora l'origine del tunnel è inattiva.

- Il percorso per l'indirizzo di destinazione del tunnel passa attraverso il tunnel stesso, il che determina la ricorsione.

Le tre regole seguenti (missingrouting, routing, interfaccia verso il basso e destinazione del tunnel con routing errato) sono problemi relativi alla posizione locale del router sugli endpoint del tunnel.

Non coprono i problemi della rete in corso o altre funzionalità relative al tunnel GRE che possono essere configurate. In questo documento vengono descritti gli scenari in cui altri fattori possono influenzare lo stato del tunnel GRE.

Keepalive tunnel GRE

Le regole di base non coprono i casi in cui i pacchetti con tunneling GRE vengono inoltrati correttamente ma vengono persi prima di raggiungere l'altra estremità del tunnel.

In questo modo, i pacchetti di dati che passano attraverso il tunnel GRE vengono persi, anche se è potenzialmente disponibile un percorso alternativo che utilizza il PBR o un percorso statico mobile tramite un'altra interfaccia.

I pacchetti keepalive sull'interfaccia del tunnel GRE vengono usati per risolvere il problema nello stesso modo in cui vengono usati sulle interfacce fisiche.

Con il software Cisco IOS® versione 12.2(8)T, è possibile configurare i pacchetti keepalive su un'interfaccia del tunnel GRE P2P. Con questa modifica, l'interfaccia del tunnel viene chiusa in modo dinamico se i pacchetti keepalive si interrompono per un determinato periodo di tempo.

Per ulteriori informazioni sul funzionamento dei pacchetti keepalive del tunnel GRE, consultare il documento sui pacchetti keepalive del tunnel GRE.

Nota: i pacchetti keepalive del tunnel GRE sono validi e hanno effetto solo sui tunnel GRE P2P; non sono validi e non hanno alcun effetto sui tunnel GRE.

Tunnel GRE con protezione tunnel

Nel software Cisco IOS® versione 15.4(3)M/15.4(3)S e successive, lo stato del protocollo della linea del tunnel GRE segue lo stato della Security Association (SA) dell'IPsec. Pertanto, il protocollo di linea può rimanere inattivo fino a quando la sessione IPSec non viene completamente stabilita.

A tal fine, è stato usato l'ID bug Cisco CSCum34057 (tentativo iniziale con l'ID bug Cisco CSCuj29996 e backup successivo con l'ID bug Cisco CSCuj9287).

Interfacce tunnel GRE (GRE) multipoint

Per le interfacce del tunnel GRE, alcuni dei controlli precedenti per i tunnel P2P non sono applicabili (perché non esiste una destinazione fissa per il tunnel).

Di seguito sono riportati i motivi per cui un protocollo della linea del tunnel GRE può essere nello stato inattivo:

- L'interfaccia dell'origine del tunnel è in stato inattivo.

- Se la funzione di controllo dello stato dell'interfaccia è abilitata per la VPN DMVPN (Dynamic Multipoint VPN) e nessun servizio NHS risponde, il protocollo di linea viene messo in stato non attivo.

- Per i dettagli sulla funzionalità di controllo dello stato dell'interfaccia, vedere la guida alla configurazione di monitoraggio e ripristino dello stato del tunnel DMVPN.

Dipendenze dallo stato di ridondanza

Quando un indirizzo IP di origine del tunnel è configurato come indirizzo IP di ridondanza (ad esempio, un indirizzo IP virtuale HSRP (Hot Standby Router Protocol)), lo stato dell'interfaccia del tunnel tiene traccia dello stato di ridondanza.

In questo modo viene aggiunto un altro controllo che mantiene tali interfacce tunnel nello stato del protocollo di linea inattivo finché lo stato di ridondanza non diventa ATTIVO.

Nell'esempio, una configurazione **predefinita della zona IPC** non configurata correttamente determina lo stato della ridondanza in NegATION e mantiene tali interfacce tunnel in uno stato inattivo:

<#root>

Router#

show redundancy state

```
       my state = 3  -
NEGOTIATION

     peer state = 1  -DISABLED
           Mode = Simplex
        Unit ID = 0

     Maintenance Mode = Disabled
    Manual Swact = disabled (system is simplex (no peer unit))
 Communications = Down      Reason: Simplex mode

   client count = 16
 client_notification_TMR = 60000 milliseconds
           RF debug mask = 0x0
```

<#root>

Router#

show interface tunnel100

```
Tunnel100 is up, line protocol is down

  Hardware is Tunnel
```

```
  Internet address is 172.16.1.100/24
  MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.122.162.254 (GigabitEthernet0/1)
   Tunnel Subblocks:
      src-track:
         Tunnel100 source tracking subblock associated with GigabitEthernet0/1
          Set of tunnels with source GigabitEthernet0/1, 2 members (includes
          iterators), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
<SNIP>
```

Risoluzione dei problemi

Oltre ai motivi descritti in precedenza, la valutazione dello stato della linea del tunnel per il motivo dell'inattività del tunnel può essere effettuata con il comando **show tunnel interface tunnel x** hidden:

<#root>

Router#

show tunnel interface tunnel 100

```
Tunnel100
   Mode:multi-GRE/IP, Destination UNKNOWN, Source GigabitEthernet0/1
   Application ID 1: unspecified
   Tunnel Subblocks:
      src-track:
         Tunnel100 source tracking subblock associated with GigabitEthernet0/1
          Set of tunnels with source GigabitEthernet0/1, 2 members (includes
          iterators), on interface <OK>
   Linestate - current down
```

Internal linestate - current down, evaluated down - interface not up

```
   Tunnel Source Flags: Local
   Transport IPv4 Header DF bit cleared
   OCE: IP tunnel decap
   Provider: interface Tu100, prot 47
     Performs protocol check [47]
     Performs Address save check
     Protocol Handler: GRE: key 0x64, opt 0x2000
       ptype: ipv4 [ipv4 dispatcher: drop]
       ptype: ipv6 [ipv6 dispatcher: drop]
       ptype: mpls [mpls dispatcher: drop]
       ptype: otv [mpls dispatcher: drop]
       ptype: generic [mpls dispatcher: drop]
```

Nota: è disponibile un miglioramento che rende più esplicito il motivo dell'inattività del tunnel per indicare che è dovuto allo stato di

ridondanza perché non è attivo. Questo errore viene segnalato dall'ID bug Cisco CSCuq31060.

Informazioni correlate

- **RFC 1701, GRE (Generic Router Encapsulation)**
- **RFC 2890, estensioni chiavi e numeri di sequenza per GRE**
- **Tunnel GRE (Generic Routing Encapsulation) Keepalive**
- **Frammentazione IP e PMTUD**
- **Documentazione e supporto tecnico – Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).