Bestimmen der Auswirkungen auf die GRE-Tunnelschnittstellenstatus

Inhalt

Einleitung

In diesem Dokument werden die verschiedenen Bedingungen beschrieben, die den Status einer GRE-Tunnel-Schnittstelle (Generic Routing Encapsulation) beeinflussen können.

Hintergrundinformationen

GRE-Tunnel sind vollständig stateless. Das bedeutet, dass jeder Tunnelendpunkt keine Informationen über den Status oder die Verfügbarkeit des entfernten Tunnelendpunkts speichert. Dies hat zur Folge, dass der lokale Tunnel-Endpunkt-Router standardmäßig nicht in der Lage ist, das Leitungsprotokoll der GRE-Tunnelschnittstelle herunterzufahren, wenn das Remote-Ende des Tunnels nicht erreichbar ist. Die Möglichkeit, eine Schnittstelle als ausgefallen zu markieren, wenn das Remote-Ende der Verbindung nicht verfügbar ist, wird verwendet, um Routen (insbesondere statische Routen) in der Routing-Tabelle zu entfernen, die diese Schnittstelle als ausgehende Schnittstelle verwenden. Wenn das Leitungsprotokoll für eine Schnittstelle in "Down" (Heruntergefahren) geändert wird, werden alle statischen Routen, die auf diese Schnittstelle hinweisen, aus der Routing-Tabelle entfernt. Dies ermöglicht die Installation einer alternativen (schwebenden) statischen Route oder eines richtlinienbasierten Routing (Policy Based Routing, PBR), um einen alternativen Next-Hop oder eine alternative Schnittstelle auszuwählen. Es gibt auch andere Anwendungen, die ausgelöst werden, wenn sich der Zustand einer Schnittstelle ändert. Beispiel: 'backup interface <b-interface>'.

Vier verschiedene Tunnelzustände

Es gibt vier mögliche Zustände, in denen eine GRE-Tunnelschnittstelle verwendet werden kann:

1. Up/up (Hochgefahren/Hochgefahren) - Dies impliziert, dass der Tunnel voll funktionsfähig ist und den Datenverkehr weiterleitet. Sie ist sowohl administrativ als auch protokollarisch in

Ordnung.

2. Administrative Aus-/Herunterfahren - Dies impliziert, dass die Schnittstelle vom Administrator heruntergefahren wurde.
3. Up/Down - Dies impliziert, dass, obwohl der Tunnel administrativ aktiv ist, etwas dazu führt, dass das Leitungsprotokoll auf der Schnittstelle ausgefallen ist.
4. Reset/Down - Dies ist normalerweise ein vorübergehender Zustand, wenn der Tunnel durch Software zurückgesetzt wird. Dies geschieht in der Regel, wenn der Tunnel mit einem Next Hop Server (NHS) falsch konfiguriert ist, der seine eigene IP-Adresse hat.

Wenn eine Tunnelschnittstelle zum ersten Mal erstellt und keine andere Konfiguration darauf angewendet wird, wird die Schnittstelle nicht standardmäßig geschlossen:

```
Router#show run interface tunnel 1
Building configuration...

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

In diesem Zustand ist die Schnittstelle immer aktiv/inaktiv:

```
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
```

Dies liegt daran, dass die Schnittstelle administrativ aktiviert ist, das Leitungsprotokoll jedoch ausgefallen ist, da sie weder eine Tunnelquelle noch ein Tunnelziel aufweist.

Damit diese Schnittstelle aktiviert bzw. aktiviert wird, muss eine gültige Tunnelquelle und ein gültiges Tunnelziel konfiguriert werden:

```
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
```

Die vorige Sequenz zeigt Folgendes:

- Eine gültige Tunnelquelle besteht aus einer Schnittstelle, die sich selbst im eingeschalteten Zustand befindet und für die eine IP-Adresse konfiguriert ist. Wenn beispielsweise die Tunnelquelle in **Loopback0** geändert wurde, würde die Tunnelschnittstelle ausfallen, obwohl **Loopback0** im Status "up/up" ist:

```
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 down
```

- Ein gültiges Tunnelziel kann geroutet werden. Sie muss jedoch nicht erreichbar sein, wie aus diesem Ping-Test hervorgeht:

```
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)
```

Bisher wurde der Tunnel als Point-to-Point (P2P) GRE-Tunnel konfiguriert, was der Standard ist. Wenn dieser Tunnel in einen mGRE-Tunnel (Multipoint GRE) umgewandelt werden sollte, muss der Tunnel nur in einen aktiven Zustand versetzt werden, damit eine gültige Tunnelquelle verfügbar ist (ein mGRE-Tunnel kann viele Tunnelziele haben, sodass dieser nicht zur Steuerung des Tunnelschnittstellenzustands verwendet werden kann):

```
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
```

Wenn die Tunnelschnittstelle vom Administrator deaktiviert wurde, wechselt der Tunnel sofort in den administrativen Aus-/Zustand:

```
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
```

P2P GRE-Tunnelstatus

Eine P2P GRE-Tunnelschnittstelle wird in der Regel aktiviert, sobald sie mit einer gültigen Tunnelquellenadresse oder Schnittstelle konfiguriert ist, die aktiviert ist, **und** einer Tunnelziel-IP-Adresse, die wie im vorherigen Abschnitt gezeigt geroutet werden kann.

Leitungsprotokoll lokal auf dem Router heruntergefahren

Unter normalen Umständen gibt es nur drei Gründe, warum ein GRE-Tunnel im Hoch-/Herunterzustand ist:

- Es gibt keine Route (einschließlich der Standardroute) zur Tunnel-Zieladresse.
- Die Schnittstelle, die die Tunnelquelle verankert, ist ausgefallen.
- Die Route zur Tunnel-Zieladresse verläuft durch den Tunnel selbst, was zu einer Rekursion führt.

Diese drei Regeln (missing, Route, Interface Down und fehlgeleitetes Tunnelziel) sind Probleme, die sich lokal auf den Router an den Tunnelendpunkten befinden, und decken keine Probleme im dazwischen liegenden Netzwerk oder andere Funktionen im Zusammenhang mit dem GRE-Tunnel ab, die konfiguriert werden können. In diesem Dokument werden Szenarien beschrieben, in denen andere Faktoren den Zustand des GRE-Tunnels beeinflussen können.

GRE-Tunnel-Keepalive

Die Grundregeln gelten nicht für den Fall, dass GRE-getunnelte Pakete erfolgreich weitergeleitet werden, aber verloren gehen, bevor sie das andere Ende des Tunnels erreichen. Dies führt dazu, dass Datenpakete, die den GRE-Tunnel durchlaufen, "schwarz durchlöchert" werden, obwohl potenziell eine alternative Route verfügbar ist, die PBR verwendet, oder eine statische Floating-Route über eine andere Schnittstelle. Keepalives an der GRE-Tunnelschnittstelle werden verwendet, um dieses Problem auf die gleiche Weise zu lösen wie Keepalives an physischen Schnittstellen.

Mit Cisco IOS® Software Release 12.2(8)T ist es möglich, Keepalives auf einer P2P GRE-Tunnelschnittstelle zu konfigurieren. Mit dieser Änderung wird die Tunnelschnittstelle dynamisch heruntergefahren, wenn die Keepalives für einen bestimmten Zeitraum fehlschlagen. Um besser zu verstehen, wie GRE-Tunnelkeepalives funktionieren, lesen Sie GRE-Tunnelkeepalives.

> **Anmerkung:** GRE-Tunnel-Keepalives sind nur gültig und wirken sich auf P2P-GRE-Tunnel aus; Sie sind ungültig und haben keine Auswirkungen auf mGRE-Tunnel.

GRE-Tunnel mit Tunnelschutz

In den Cisco IOS Software-Versionen 15.4(3)M/15.4(3)S und höher kann der Status des GRE-Tunnelleitungsprotokolls dem Status der IPsec-Sicherheitszuordnung (SA) folgen, sodass das

Leitungsprotokoll solange nicht verfügbar ist, bis die IPsec-Sitzung vollständig hergestellt ist. Dies wurde mit der Cisco Bug-ID CSCum34057 bestätigt (erster Versuch mit der Cisco Bug-ID CSCuj29996 und anschließend mit der Cisco Bug-ID CSCuj9287).

mGRE-Tunnelschnittstellen (Multipoint GRE)

Da es für mGRE-Tunnelschnittstellen kein festes Tunnelziel gibt, sind einige der vorherigen Prüfungen für P2P-Tunnel nicht anwendbar. Die Gründe, warum ein mGRE-Tunnelleitungsprotokoll ausgefallen sein kann, sind wie folgt:

- Die Tunnelquellenschnittstelle ist ausgefallen.
- Wenn die Schnittstellenzustandssteuerung für Dynamic Multipoint VPN (DMVPN) aktiviert ist und keiner der NHS antwortet, wird das Leitungsprotokoll deaktiviert. Weitere Informationen zur Schnittstellenzustandskontrolle finden Sie im Konfigurationsleitfaden zur Überwachung und Wiederherstellung des DMVPN-Tunnels.

Abhängigkeiten vom Redundanzstatus

Wenn eine Tunnel-Quell-IP-Adresse als Redundanz-IP-Adresse konfiguriert ist (z. B. eine Hot Standby Router Protocol Virtual IP (HSRP VIP)-Adresse), verfolgt der Tunnel-Schnittstellenstatus den Redundanzstatus nach.

Dadurch wurde eine zusätzliche Überprüfung hinzugefügt, die solche Tunnelschnittstellen im Leitungsprotokoll-Down-Zustand belässt, bis der Redundanzstatus zu ACTIVE wechselt. In diesem Beispiel führt eine falsch konfigurierte **IP-Zone-Standardkonfiguration** dazu, dass sich die Redundanz im VERHANDLUNGS-Zustand befindet, und hält solche Tunnelschnittstellen im ausgefallenen Zustand:

```
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

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>
```

Fehlerbehebung

Zusätzlich zu den oben angeführten Gründen kann die Auswertung des Tunnellinienstatus für den Grund für den Tunnel-Absturz mit dem Befehl **show tunnel interface tunnel x** hidden wie folgt angezeigt werden:

```
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]
```

> **Anmerkung:** Durch eine offene Erweiterung wird der Grund für den Tunnelausfall genauer angegeben, um anzuzeigen, dass er auf den Redundanzstatus zurückzuführen ist, da er nicht aktiv ist. Diese wird über die Cisco Bug-ID CSCuq31060 verfolgt.

Zugehörige Informationen

- RFC 1701, Generic Router Encapsulation (GRE)
- RFC 2890, Key and Sequence Number Extensions to GRE
- Generic Routing Encapsulation (GRE) Tunnel Keepalive
- IP-Fragmentierung und PMTUD
- Technischer Support und Dokumentation für Cisco Systeme

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.