瞭解GRE通道Keepalive

目錄

[簡介](#)
[GRE通道](#)
[通道Keepalive的運作方式](#)
[GRE通道Keepalive](#)
[GRE Keepalive和單點傳送反向路徑轉送](#)
[IPsec和GRE Keepalive](#)
[採用IPsec的GRE通道](#)
[合併IPsec和GRE時Keepalive問題](#)
[案例 1](#)
[案例 2](#)
[案例 3](#)
[因應措施](#)
[相關資訊](#)

簡介

本檔案將說明通用路由封裝(GRE)keepalive的用途及其運作方式。

GRE通道

GRE通道是思科路由器上的邏輯介面，可用來封裝傳輸通訊協定中的乘客封包。這個架構的目的是提供服務以實作點對點封裝配置。

GRE通道設計為完全無狀態。這表示每個通道端點不保留有關遠端通道端點的狀態或可用性的任何資訊。其後果是，如果通道的遠端無法連線，本地通道端點路由器將無法使GRE通道介面的線路通訊協定關閉。當鏈路的遠端不可用時將介面標籤為關閉的功能可用於刪除路由表中使用該介面作為出站介面的任何路由（特別是靜態路由）。具體來說，如果介面的線路協定更改為關閉，則任何指出該介面的靜態路由將從路由表中刪除。這樣可安裝備用（浮動）靜態路由或用於基於策略的路由(PBR)，以便選擇備用下一跳或介面。

一般情況下，GRE通道介面會在設定後立即啟動，且只要存在有效的通道來源位址或介面啟動，介面就會一直啟動。通道目的地IP位址也必須可路由。即使尚未設定通道的另一端，情況也是如此。這表示即使GRE通道封包沒有到達通道的另一端，透過GRE通道介面的封包靜態路由或PBR轉送仍然有效。

實施GRE keepalive之前，只有方法可以確定路由器上的本地問題，沒有方法可以確定介入網路的問題。例如，GRE通道化的封包成功轉送，但在到達通道另一端之前遺失的情況。此類情況將導致通過GRE通道的資料包被「黑洞」，即使可以使用使用PBR的備用路由或通過其他介面的浮動靜態路由也是如此。GRE通道介面上的Keepalive的使用方式與實體介面上使用Keepalive的方式相同，目的在於解決此問題。

注意：在任何情況下，都不支援GRE keepalive和IPsec隧道保護。本檔案將討論此問題。

通道Keepalive的運作方式

GRE通道keepalive機制與PPP keepalive類似，因為它允許一方向遠端路由器發起和接收keepalive封包，即使遠端路由器不支援GRE keepalive也如此。由於GRE是用於在IP內部對IP進行通道化的封包通道機制，因此可以在另一個GRE IP通道封包中建立GRE IP通道封包。若是GRE keepalive，傳送者會在原始keepalive要求封包中預先建立keepalive回應封包，以便遠端只需對外部GRE IP標頭執行標準GRE解除封裝，然後將內部IP GRE封包還原到傳送者。這些封包解釋了IP通道概念，其中GRE是封裝通訊協定，IP是傳輸通訊協定。乘客通訊協定也是IP(雖然也可以是另一個通訊協定，例如Decnet、網際網路封包交換(IPX)或Appletalk)。

正常封包:

IP報頭 TCP報頭 Telnet

隧道資料包：

GRE IP標頭 GRE IP報頭 TCP報頭 Telnet

- IP是傳輸通訊協定。
- GRE 是封裝通訊協定。
- IP是乘客通訊協定。

以下是來自路由器A且目的地為路由器B的keepalive封包範例。路由器B返回到路由器A的keepalive響應已位於內部IP報頭中。路由器B只是將keepalive封包解除封裝，並將其從實體介面(S2)傳送回。它會像處理任何其他GRE IP資料包一樣處理GRE keepalive資料包。

GRE Keepalive:

GRE IP標頭		GRE		IP報頭		GRE
來源A	目的地B	PT=IP	來源B	目的地A		PT=0

此機制會導致keepalive響應從實體介面而非通道介面轉發出去。這表示GRE keepalive回應封包不會受到通道介面上任何輸出功能的影響，例如「通道保護……」、QoS、虛擬路由和轉送(VRF)等。

> **註**：如果在GRE通道介面上設定了傳入存取控制清單(ACL)，則必須允許對端裝置傳送的GRE通道存留封包。如果沒有，則另一台裝置GRE隧道會關閉。(**access-list** <number> **permit gre host** <tunnel-source> **host** <tunnel-destination>)

GRE通道keepalive的另一個屬性是兩端keepalive計時器是獨立的，不需要相符，類似PPP keepalive。

> **提示**：只在通道的一端設定keepalive的問題在於，只有已設定keepalive的路由器會將其通道介面標籤為關閉，因為keepalive計時器會過期。未設定keepalive的另一端的GRE通道介面，即使通道的另一端已關閉，也會保持開啟。通道可能成為從未設定keepalive的一側導向通道中的封包的黑洞。

> **提示**：在大型集中星型GRE隧道網路中，可以只將配置的GRE keepalive配置在分支端，而不配置在中心端。這是因為輻射點發現中心無法到達並因此切換到備份路徑（例如撥號備份）通

常更為重要。

GRE通道Keepalive

使用Cisco IOS®軟體版本12.2(8)T，可以在點對點GRE通道介面上設定keepalive。透過此變更，如果keepalive在一段時間內失敗，通道介面就會動態關閉。

如需其他形式keepalive運作方式的詳細資訊，請參閱Cisco IOS上的Keepalive機制概觀。

註：僅在點對點GRE通道上支援GRE通道keepalive。通道keepalive可以在多點GRE(mGRE)通道上設定，但無效。

註：通常，在隧道介面和fVRF('tunnel vrf ...)上使用VRF時，隧道keepalive無法工作。')和iVRF('ip vrf forwarding ...' (在隧道介面上) 不匹配。這對於將keepalive「反射」回請求者的隧道端點非常重要。當收到keepalive請求時，在fVRF中接收該請求並將其解除封裝。這顯示預先建立的keepalive回覆，該回覆需要轉回給傳送方，但轉發是在隧道介面上的iVRF上下文中。因此，如果iVRF和fVRF不匹配，則keepalive應答資料包不會轉發回傳送方。即使將iVRF和/或fVRF替換為「global」也是如此。

此輸出會顯示您在GRE通道上設定keepalive所使用的命令。

```
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].



!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

為了更好地瞭解通道保持連線機制的運作方式，請考慮以下通道拓撲和配置示例：

路由器A

```
interface loopback 0
ip address 192.168.1.1 255.255.255.255
interface tunnel 0
ip address 10.10.10.1 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.2
keepalive 5 4
```

路由器B

```
interface loopback 0
ip address 192.168.1.2 255.255.255.255
interface tunnel 0
ip address 10.10.10.2 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.1
keepalive 5 4
```

在此案例中，路由器A會執行以下步驟：

1. 每5秒構建一個內部IP報頭，其中：

   來源設定為本地通道目的地，即192.168.1.2目的地設定為本地通道來源，即192.168.1.1

   並且GRE報頭新增的協定型別(PT)為0

   由路由器A生成但未傳送的資料包：

2. 將該資料包從其隧道介面傳送出去，這會導致使用外部IP報頭封裝資料包，其中：

   來源設定為本地通道來源，即192.168.1.1目的地設定為本地通道目的地，即192.168.1.2

   並使用PT = IP新增GRE報頭。

   從路由器A傳送到路由器B的資料包：

3. 將隧道保持連線計數器遞增1。

4. 如果有到達遠端通道端點的方式，且通道線路通訊協定沒有因為其他原因而關閉，則封包會到達路由器B。然後將其與通道0匹配，解除封裝，並轉發到目標IP，即路由器A上的通道源IP地址。

   從路由器B傳送到路由器A:

5. 到達路由器A後，資料包將解除封裝，對PT的檢查結果為0。這表示這是一個keepalive封包。然後，將隧道保持連線計數器重置為0並丟棄資料包。

如果路由器B無法連線，路由器A會繼續構建和傳送keepalive封包以及正常流量。如果keepalive未傳回，則只要tunnel keepalive計數器小於重試次數（在本例中為4），通道線路協定就會保持運行。如果條件不成立，則下次路由器A嘗試向路由器B傳送keepalive時，線路協定會關閉。

註：在開啟/關閉狀態下，通道不會轉送或處理任何資料流量。但是，它會繼續傳送keepalive資料包。在收到keepalive響應時（表示隧道端點再次可到達），隧道keepalive計數器重置為0，並且隧道上的線路協定啟動。

若要檢視keepalive的作用中，請啟用**debug tunnel**和**debug tunnel keepalive**。

路由器A的調試示例：

```
debug tunnel keepalive
Tunnel keepalive debugging is on
01:19:16.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=15
01:19:21.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=16
01:19:26.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=17
```

GRE Keepalive和單點傳送反向路徑轉送

單點傳播RPF（單點傳播反向路徑轉送）是一項安全功能，可透過根據路由表驗證封包來源位址，協助偵測和捨棄偽裝IP流量。 在嚴格模式(**ip verify unicast source reachable-via rx)下執行單點傳播RPF時，必須在路由器將使用的介面上接收封包，以便轉送傳回封包。**如果在接收GRE keepalive封包的路由器的通道介面上啟用嚴格模式或鬆動模式單點傳播RPF，則由於通往封包來源位址（路由器自己的通道來源位址）的路由沒有經過通道介面，因此RPF會在通道解除封裝後捨棄keepalive封包。在**show ip traffic**輸出中可觀察到RPF封包捨棄，如下所示：

```
Router#show ip traffic | section Drop
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
0 no route, 156 unicast RPF, 0 forced drop
0 options denied
```

因此，通道keepalive的發起端會因為遺失的keepalive傳回封包而關閉通道。因此，單播RPF不能配置為嚴格或鬆散模式，GRE隧道keepalive才能正常工作。有關單播RPF的詳細資訊，請參閱瞭解單播反向路徑轉發。

IPsec和GRE Keepalive

採用IPsec的GRE通道

由於IPsec不支援IP組播資料包，因此GRE隧道有時會與IPsec結合使用。因此，動態路由協定無法通過IPsec VPN網路成功運行。由於GRE通道確實支援IP多點傳送，因此可以透過GRE通道執行動態路由通訊協定。產生的GRE IP單播資料包可以由IPsec加密。

IPsec加密GRE封包的方式有兩種：

- 其中一種方法是使用密碼編譯對應。使用密碼編譯對應時，會將其套用到GRE通道封包的傳出實體介面。在這種情況下，步驟順序如下：

  加密的封包抵達實體介面。封包將解密並轉送到通道介面。封包將解除封裝，然後以明文形式轉送到IP目的地。

- 另一種方法是使用通道保護。使用通道保護時，會在GRE通道介面上設定該保護。tunnel protection命令在Cisco IOS軟體版本12.2(13)T中可用。在這種情況下，步驟順序如下：

  加密資料包到達物理介面。將封包轉送到通道介面。封包經過解密和解除封裝，然後以明文形式轉送到IP目的地。

這兩種方法都指定在新增GRE封裝後執行IPsec加密。使用密碼編譯對應和使用通道保護之間存在兩個主要差異：

- IPsec加密對映與物理介面繫結，並在資料包從物理介面轉發出去時進行檢查。

  GRE通道已在此時間點將GRE封裝封包。
- 通道保護將加密功能繫結到GRE通道，並在GRE封裝封包之後但在將封包傳送到實體介面之前進行檢查。

合併IPsec和GRE時Keepalive問題

根據兩種向GRE通道新增加密的方法，有三種不同的方法來設定加密的GRE通道：

1. 對等體A在通道介面上配置了通道保護，而對等體B在物理介面上配置了加密對映。
2. 對等體A在物理介面上配置了加密對映，而對等體B在隧道介面上配置了隧道保護。
3. 兩個對等點都在通道介面上設定了通道保護。

方案1和2中描述的配置通常採用集中星型設計。在中心路由器上配置了通道保護以減少配置的大小，並且每個分支都使用靜態加密對映。

請考慮在對等B（分支）上啟用GRE keepalive且使用通道模式進行加密的每種方案。

案例 1

設定：

- 對等A使用通道保護。
- 對等B使用加密對映。
- 對等B上啟用Keepalive。
- IPsec加密在隧道模式下完成。

在此案例中，由於對等B上設定了GRE keepalive，因此產生keepalive時的序列事件如下：

1. 對等B會產生keepalive封包，該封包經GRE封裝，然後轉送到實體介面，在該介面上對其進行加密，然後傳送到通道目的地Peer A。

   從對等點B傳送到對等點A的封包：

2. 在對等方A上，GRE keepalive被解密接收：

   解除封裝：

然後內部GRE keepalive響應資料包根據其目的地址（對等B）進行路由。這表示在對等A上，封包會立即從實體介面路由回對等B。由於對等A在通道介面上使用通道保護，因此keepalive封包不會加密。

因此，從對等點A傳送到對等點B的封包：

附註: keepalive並未加密。

3. 對等B現在收到GRE keepalive回應，該回應在其實體介面上未加密，但由於在實體介面上設定的密碼編譯對應，它預期收到加密封包，因此捨棄該封包。

因此，即使對等點A對keepalive做出回應，而路由器對等點B收到回應，它也不會處理這些回應，最終會將通道介面的線路通訊協定變更為down狀態。

Result:

對等B上啟用的Keepalive會導致對等B上的通道狀態變更為up/down。

案例 2

設定：

- 對等A使用加密對映。
- 對等B使用通道保護。
- 對等B上啟用Keepalive。
- IPsec加密在隧道模式下完成。

在此案例中，由於對等體B上設定了GRE keepalive，因此產生keepalive時的序列事件如下：

1. 對等B會產生keepalive封包，此封包經GRE封裝，然後透過通道介面上的通道保護進行加密，然後轉送到實體介面。

   從對等點B傳送到對等點A的封包：

2. 在對等方A上，GRE keepalive被解密接收：

   解除封裝：

   然後內部GRE keepalive響應資料包根據其目的地址（對等B）進行路由。這表示在對等A上，封包會立即從實體介面路由回對等B。由於對等A在實體介面上使用密碼編譯對應，因此會

在轉送此封包之前先對其進行加密。

因此，從對等點A傳送到對等點B的封包：

註:keepalive響應已加密。

3. 對等B現在會收到加密的GRE keepalive回應，其目的地被轉送到已解密的通道介面：

由於Protocal Type設定為0，對等B知道這是一個keepalive響應並照此處理。
Result:

在對等B上啟用的Keepalive成功根據通道目的地的可用性確定通道狀態是什麼。

案例 3

設定：

- 兩個對等點都使用通道保護。
- 對等B上啟用Keepalive。
- IPsec加密在隧道模式下完成。

此案例與案例1類似，當對等A收到加密的keepalive時，會將其解密和解除封裝。但是，當響應轉回時，不會對其進行加密，因為對等體A在隧道介面上使用隧道保護。因此，對等B會丟棄未加密的keepalive響應而不對其進行處理。

Result:

對等B上啟用的Keepalive會導致對等B上的通道狀態變更為up/down。

因應措施

在必須加密GRE資料包的情況下，有三種可能的解決方案：

1. 在對等A上使用加密對映，對等B使用隧道保護，對等B啟用keepalive。

   由於此類配置主要用在中心輻射型設定中，並且因為在這種設定中，輻射點必須知道輻射點的可達性更為重要，因此解決方案是在輻射點（對等點A）上使用動態加密對映，在輻射點（對等點B）上使用隧道保護，並在輻射點上啟用GRE keepalive。這樣，雖然集線器上的GRE通道介面仍處於開啟狀態，但路由鄰居和通過該通道的路由會遺失，且可以建立替代路由。在分支上，隧道介面關閉這一事實可觸發它啟用撥號程式介面並回叫到中心（或中心處的另一台路由器），然後建立新連線。

2. 使用GRE keepalive以外的內容來確定對等體可連線。

   如果兩台路由器都配置了隧道保護，則任何方向都不能使用GRE隧道鎖鑰。在這種情況下，唯一的選項是使用路由協定或其他機制（例如服務保證代理）來發現對等體是否可以訪問。

3. 在對等A和對等B上使用加密對映。

   如果兩台路由器都設定了密碼編譯對應，則通道keepalive可以在兩個方向通過，而GRE通道介面可以在任一方向或兩個方向關閉，並觸發建立備份連線。這是最靈活的選項。

相關資訊

- RFC 1701，通用路由器封裝(GRE)
- RFC 2890,GRE的金鑰和序列號擴展
- 通用路由封裝(GRE)通道存留
- IP分段和PMTUD
- Cisco IOS上的Keepalive機制概述
- 技術支援 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。