動態多點IPsec VPN（使用多點GRE/NHRP擴展IPsec VPN）

目錄

簡介
背景資訊
DMVPN解決方案
自動IPsec加密啟動
為「輻條到中心」鏈路建立動態隧道
為「輻條到輻條」流量建立動態隧道
支援動態路由協定
適用於mGRE的Cisco快速轉送快速交換
使用通過IPsec保護的動態路由VPN
基本配置
中心輻射型路由器上的路由表示例
減小中心路由器配置大小
支援輻條上的動態地址
動態多點中心輻射型
動態多點IPsec VPN
RIP
EIGRP
OSPF
初始條件
在Spoke1和Spoke2之間建立動態鏈路之後的條件
含雙集線器的動態多點IPsec VPN
雙集線器 — 單DMVPN佈局
初始條件和更改
雙集線器 — 雙DMVPN佈局
初始條件和更改
結論
相關資訊

簡介

本檔案將討論動態多點IPsec VPN(DMVPN)，以及為什麼公司可能希望設計或遷移其網路以在Cisco IOS®軟體中使用此新IPsec VPN解決方案。

背景資訊

公司可能需要通過Internet將多個站點與主站點互連，甚至相互互連，同時加密流量以保護流量。例如，一組需要連線到公司總部進行庫存和訂購的零售商店可能還需要連線到公司內的其他商店以檢查產品可用性。過去，建立連線的唯一方法是使用第2層網路（如ISDN或幀中繼）將所有內容互連。為內部IP流量設定和支付這些硬線鏈路的費用既耗時又昂貴。如果所有站點（包括主站點）已經具有相對便宜的Internet訪問，則此Internet訪問還可以用於店舖和總部之間的內部IP通訊，通過使用IPsec隧道來確保隱私和資料完整性。

為了讓公司構建大型IPsec網路，使其站點通過Internet互連，您需要能夠擴展IPsec網路。IPsec對兩個端點（對等路由器）之間的流量進行加密，加密由兩個端點使用共用「金鑰」完成。 由於此金鑰僅在這兩個端點之間共用，因此加密網路本身就是點對點鏈路的集合。因此，IPsec本質上是一個點對點隧道網路。擴展大型點對點網路的最可行方法是將其組織成星型或全（部分）網狀網路。在大多數網路中，大多數IP流量位於輻條和集線器之間，而極少位於輻條之間，因此輻條設計通常是最佳選擇。此設計也適用於較舊的幀中繼網路，因為要為這些網路中的所有站點之間的鏈路支付極高的費用。

當使用Internet作為集線器和輻條之間的互連時，輻條之間也可以直接連線，無需額外成本，但設定和/或管理完整（部分）網狀網路非常困難，甚至是不可能的。全網狀或部分網狀網路通常是理想的，因為如果分支到分支的流量可以直接通過，而不是通過集線器，則可以節省成本。遍歷集線器的分支到分支流量會使用集線器資源，並可能導致額外的延遲，特別是在使用IPsec加密時，因為集線器將需要解密來自傳送分支的傳入資料包，然後重新加密流量以將其傳送到接收分支。直接輻條到輻條流量的另一個示例是兩個輻條位於同一城市且中心位於全國的情況。

隨著部署IPsec集中星型網路並擴大網路規模，要求它們儘可能動態地路由IP資料包變得更加理想。在較舊的幀中繼星型網路中，這是通過運行幀中繼鏈路上的動態路由協定（如OSPF或EIGRP）來實現的。這對於動態通告分支網路的可達性以及在IP路由網路中支援冗餘非常有用。如果網路丟失了中心路由器，備用中心路由器可以自動接管以保持與分支網路的網路連線。

IPsec隧道和動態路由協定存在根本問題。動態路由協定依賴於使用IP組播或廣播資料包，但IPsec不支援加密組播或廣播資料包。目前解決此問題的方法是將通用路由封裝(GRE)通道與IPsec加密結合使用。

而GRE通道支援將IP多點傳送和廣播封包傳輸到GRE通道的另一端。GRE通道封包是IP單點傳播封包，因此GRE封包可以使用IPsec加密。在此案例中，GRE執行通道工作，IPsec執行支援VPN網路的加密部分。設定GRE通道時，通道端點(**通道來源……、通道目的地……**)的IP位址必須透過另一個端點知道，且必須可透過Internet路由。這意味著集線器和此網路中的所有分支路由器都必須具有靜態非私有IP地址。

對於連線到Internet的小型站點，分支的外部IP地址通常會在每次連線到Internet時進行更改，因為每當分支聯機(非對稱數字使用者線路(ADSL)和電纜服務)，其網際網路服務提供商(ISP)都會動態提供外部介面地址(通過動態主機配置協定(DHCP))。 這種路由器的「外部地址」的動態分配允許ISP超訂用其Internet地址空間，因為並非所有使用者同時處於聯機狀態。支付提供商為分支路由器分配靜態地址的成本可能會高得多。通過IPsec VPN運行動態路由協定需要使用GRE隧道，但您會失去在其外部物理介面上使用動態分配IP地址的分支。

上述限制和其他一些限制歸納為以下四點：

- IPsec使用存取控制清單(ACL)來定義要加密的資料。因此，每次在分支或中心後面新增新的（子）網路時，客戶都必須更改中心路由器和分支路由器上的ACL。如果SP管理路由器，則客戶必須通知SP以更改IPsec ACL，以便加密新流量。
- 對於大型星型網路，中心路由器上的配置可能會變得非常大，甚至無法使用。例如，一台中心路由器需要最多3900行配置才能支援300台分支路由器。此值足夠大，因此很難顯示配置，也很難找到與正在調試的當前問題相關的配置部分。此外，此大小配置可能過大，無法容納在

NVRAM中，需要儲存在快閃記憶體中。

- GRE + IPsec必須知道端點對等體地址。輻條的IP地址通過它們自己的ISP直接連線到Internet，並且它們經常被設定以便其外部介面地址不是固定的。每次站點聯機時（通過DHCP）IP地址都會更改。
- 如果分支需要通過IPsec VPN直接相互通訊，則中心輻射型網路必須成為全網狀網路。由於不知道哪些輻條需要彼此直接對話，因此需要完全網狀，即使每個輻條可能不需要與每個其它輻條直接對話。此外，在小型分支路由器上配置IPsec使其與網路中所有其他分支路由器直接連線是不可行的；因此，分支路由器可能需要成為功能更強大的路由器。

DMVPN解決方案

DMVPN解決方案使用多點GRE(mGRE)和下一躍點解析協定(NHRP)以及IPsec和一些新的增強功能，以可擴充的方式解決上述問題。

自動IPsec加密啟動

如果不使用DMVPN解決方案，則不會啟動IPsec加密隧道，直到有資料流量需要使用此IPsec隧道。可能需要1到10秒才能完成IPsec隧道的啟動，並且在此時間內丟棄資料流量。將GRE與IPsec一起使用時，GRE通道配置已經包括GRE通道對等體(**通道目標……**)地址，該地址也是IPsec對等體地址。這兩個地址都已預先配置。

如果在集線器路由器上使用通道端點探索(TED)和動態密碼編譯對應，則可以避免在集線器上預先設定IPsec對等體位址，但需要先傳送和接收TED探測和回應，然後才能啟動ISAKMP協商。這並不是必需的，因為使用GRE時，對等體源地址和目的地址是已知的。它們位於配置中或使用NHRP解決（對於多點GRE隧道）。

使用DMVPN解決方案，點對點和多點GRE通道會立即觸發IPsec。此外，不需要設定任何加密ACL，因為它們將會自動從GRE通道來源和目的地位址衍生。以下命令用於定義IPsec加密引數。請注意，不需要使用**set peer ...**或**match address ...**命令，因為此資訊直接從關聯的GRE隧道或NHRP對映派生。

```
crypto ipsec profile
```

```
 set transform-set
```

以下命令將隧道介面與IPsec配置檔案相關聯。

```
interface tunnel
```

```
...
tunnel protection ipsec profile
```

為「輻條到中心」鏈路建立動態隧道

在DMVPN網路中的中心路由器上未配置有關分支的GRE或IPsec資訊。分支路由器的GRE通道已配置（通過NHRP命令），其中包含中心路由器的資訊。當分支路由器啟動時，它會自動啟動與中心路由器的IPsec隧道（如上所述）。然後使用NHRP通知集線器路由器其當前物理介面IP地址。這非常有用，原因有三：

- 如果分支路由器動態分配其物理介面IP地址（例如使用ADSL或CableModem），則中心路由器無法配置此資訊，因為分支路由器每次重新載入時都會獲得新的物理介面IP地址。
- 集線器路由器的配置會縮短和簡化，因為它不需要有關對等路由器的任何GRE或IPsec資訊。所有這些資訊都是通過NHRP動態獲取的。
- 將新的分支路由器新增到DMVPN網路時，無需更改中心路由器或任何當前分支路由器上的配置。新的分支路由器配置了中心資訊，當它啟動時，它將動態註冊到中心路由器。動態路由協定將此分支的路由資訊傳播到中心。集線器將此新路由資訊傳播到其他輻條。它還會將路由資訊從其他輻條傳播到此輻條。

為「輻條到輻條」流量建立動態隧道

如前所述，當前在網狀網路中，必須在所有路由器上配置所有點對點IPsec（或IPsec+GRE）隧道，即使其中有一部分/大部分隧道沒有運行或一直需要這些隧道。使用DMVPN解決方案時，一台路由器是集線器，而所有其他路由器（分支）都配置了通向集線器的隧道。輻條到集線器的隧道會持續啟動，而且輻條不需要配置直接隧道到任何其他輻條。相反，當一個分支想要將資料包傳輸到另一個分支（例如另一個分支後面的子網）時，它使用NHRP動態確定目標分支所需的目標地址。中心路由器充當NHRP伺服器並處理源分支的此請求。然後，兩個分支動態地在其之間建立一個IPsec隧道（通過單個mGRE介面），資料可以直接傳輸。此動態輻條到輻條隧道將在（可配置的）非活動週期後自動關閉。

支援動態路由協定

DMVPN解決方案基於支援隧道組播/廣播IP資料包的GRE隧道，因此DMVPN解決方案還支援通過IPsec+mGRE隧道運行的動態路由協定。之前，NHRP要求您為隧道目標IP地址顯式配置廣播/組播對映，以支援組播和廣播IP資料包的GRE隧道。例如，在中心位置，您需要為每個分支配置**ip nhrp map multicast <spoke-n-addr>**配置行。使用DMVPN解決方案時，分支地址是事先不知道的，因此無法進行此配置。相反，可以將NHRP配置為使用**ip nhrp map multicast dynamic**命令將每個分支自動新增到集線器上的組播目標清單。使用此命令，當分支路由器向NHRP伺服器（集線器）註冊其單播NHRP對映時，NHRP還將為此分支建立廣播/組播對映。這樣就無需預先知道分支地址。

適用於mGRE的Cisco快速轉送快速交換

目前，mGRE介面中的流量是執行序交換的，因此效能很差。DMVPN解決方案為mGRE流量新增了Cisco快速轉發交換，從而獲得更好的效能。無需任何配置命令即可啟用此功能。如果GRE通道

介面和傳出/傳入實體介面上允許思科快速轉送交換，則多點GRE通道封包將採用Cisco快速轉送交換。

使用通過IPsec保護的動態路由VPN

本節介紹當前（DMVPN解決方案之前）的事務狀態。IPsec在Cisco路由器上通過一組命令來實施，這些命令定義加密，然後在路由器的外部介面上應用**crypto map <map-name>**命令。由於此設計以及目前沒有使用IPsec加密IP多點傳送/廣播封包的標準，因此IP路由通訊協定封包無法透過IPsec通道「轉送」，且任何路由變更無法動態傳播到IPsec通道的另一端。

注意：除BGP以外的所有動態路由協定都使用廣播或多播IP資料包。將GRE通道與IPsec結合使用可解決此問題。

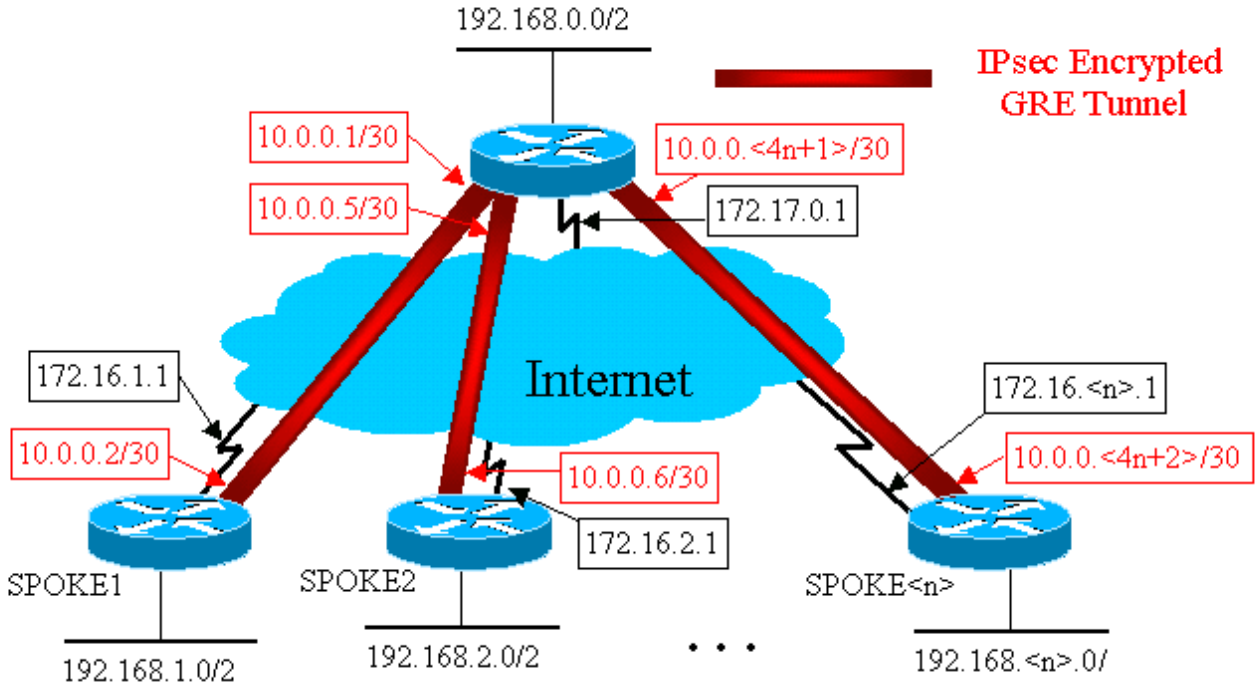
GRE通道是在思科路由器上使用虛擬通道介面(**介面通道<#>**)實作。 GRE通道通訊協定設計為處理IP多點傳送/廣播封包，因此動態路由通訊協定可以透過GRE通道「執行」。GRE通道封包是封裝原始IP多點傳送/單點傳播封包的IP單點傳播封包。然後，您可以使用IPsec加密GRE通道封包。您也可以在傳輸模式下運行IPsec並儲存20位元組，因為GRE已封裝原始資料包，因此您不需要IPsec將GRE IP資料包封裝在另一個IP報頭中。

在傳輸模式下運行IPsec時，要加密的資料包的IP源地址和目標地址必須與IPsec對等體地址（路由器本身）匹配這一限制。 在這種情況下，這只是表示GRE通道端點和IPsec對等地址必須相同。這不是問題，因為相同的路由器同時是IPsec和GRE通道端點。通過將GRE隧道與IPsec加密相結合，您可以使用動態IP路由協定更新加密隧道兩端的路由表。透過加密通道得知的網路的IP路由表專案，會將通道的另一端（GRE通道介面IP位址）作為IP下一躍點。因此，如果隧道兩端的網路發生更改，另一端將動態獲知此更改，並且連線將繼續，而不會在路由器上更改任何配置。

基本配置

以下是標準的點對點IPsec+GRE配置。在此之後，將會出現一系列配置示例，其中逐步新增DMVPN解決方案的特定功能，以顯示DMVPN的不同功能。每個示例都以前面的示例為基礎，展示如何在日益複雜的網路設計中使用DMVPN解決方案。此系列示例可用作將當前IPsec+GRE VPN遷移到DMVPN的模板。如果特定配置示例符合您的網路設計要求，您可以隨時停止「遷移」。

IPsec + GRE中心輻射型(n = 1,2,3,...)



集線器路由器

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
  set peer 172.16.1.1
  set transform-set trans2
  match address 101
 crypto map vpnmap1 20 ipsec-isakmp
  set peer 172.16.2.1
  set transform-set trans2
  match address 102
 . . .
 crypto map vpnmap1 <10*n> ipsec-isakmp
  set peer 172.16.




 interface Tunnel1
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
```

```
 tunnel destination 172.16.1.1
!
interface Tunnel2
 bandwidth 1000
 ip address 10.0.0.5 255.255.255.252
 ip mtu 1400
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.16.2.1
!
. . .
!
interface Tunnel




!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.17.0.1 host
172.16.1.1
access-list 102 permit gre host 172.17.0.1 host
172.16.2.1
...
access-list
```

Spoke1路由器

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
```

```
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.252
 ip mtu 1400
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
!
interface Ethernet0
 ip address 172.16.1.1 255.255.255.252
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.1.1 host
172.17.0.1
```

Spoke2路由器

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.6 255.255.255.252
 ip mtu 1400
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
!
interface Ethernet0
 ip address 172.16.2.1 255.255.255.252
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.2.1 host
172.17.0.1
```

分支<n>路由器

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 ipsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
 !
 interface Ethernet0
  ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
 !
 interface Ethernet1
  ip address 192.168.<n>.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.
```

在以上配置中，ACL用於定義將加密的流量。在中心路由器和分支路由器上，此ACL只需匹配GRE通道IP資料包。無論網路在任一端如何變化，GRE IP隧道資料包都不會變化，因此此ACL無需更改。

注意：使用12.2(13)T之前的Cisco IOS軟體版本時，必須將**crypto map vpnmap1配置命令應用於GRE隧道介面（隧道<x>）和物理介面（乙太網0）。** 在Cisco IOS版本12.2(13)T和更新版本中，只對實體介面(Ethernet0)應用**crypto map vpnmap1**組態命令。

中心輻射型路由器上的路由表示例

中心路由器上的路由表

```
172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
```

```
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 C       10.0.0.4 is directly connected, Tunnel2
 ...
 C       10.0.0.<4n-4> is directly connected, Tunnel<n>
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.2,
18:28:19, Tunnel1
 D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
Tunnel2
 ...
 D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
2d05h, Tunnel<n>
```

Spoke1路由器上的路由表

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
Tunnel0
 ...
 D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 C    192.168.1.0/24 is directly connected, Loopback0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
 ...
 D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
```

分支路由器上的路由表<n>

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.<n>.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 D       10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 ...
 C        10.0.0.<4n-4> is directly connected, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.1.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 ...
 C    192.168.<n>.0/24 is directly connected, Ethernet0
```

這是基本工作配置，用作與使用DMVPN解決方案時可能更複雜的配置進行比較的起點。第一次更改將減小中心路由器上的配置大小。這對數量較少的分支路由器並不重要，但當分支路由器數量超過50到100個時，這一點就變得非常重要。

減小中心路由器配置大小

在以下示例中，中心路由器上的配置從多個GRE點對點隧道介面更改到了單個GRE多點隧道介面，更改程度非常低。這是DMVPN解決方案的第一步。

中心路由器上有一個唯一的配置行塊，用於定義每個分支路由器的加密對映特性。此組態部分定義了該分支路由器的加密ACL和GRE通道介面。除了IP地址(**set peer ...,** tunnel destination ...)之外，所有輻條的**這些特徵大體相**同。

在中心路由器上檢視上述配置，您會看到每個分支路由器至少包含13行配置；加密對映為4個，加密ACL為1個，GRE通道介面為8個。如果有300台分支路由器，則配置線路總數為3900行。您還需要300(/30)個子網用於定址每個隧道鏈路。這種大小的配置非常難以管理，在排除VPN網路故障時更困難。要降低此值，可以使用動態加密對映，這將使上述值減少1200行，從而使300輻網路中的2700行保持原狀。

注意：使用動態加密對映時，IPsec加密隧道必須由分支路由器啟動。您還可以使用**ip unnumbered <interface>**來減少GRE通道所需的子網數量，但這可能會使以後的故障排除更加困難。

藉助DMVPN解決方案，您可以在中心路由器上配置單個多點GRE隧道介面和單個IPsec配置檔案以處理所有分支路由器。這樣，無論向VPN網路新增了多少台分支路由器，中心路由器上的配置大小都會保持不變。

DMVPN解決方案引入了以下新命令：

```
crypto ipsec profile
```

crypto ipsec profile <name>命令與動態加密對映類似，它專門為通道介面設計。此命令用於定義分支到集線器和分支到分支VPN隧道上的IPsec加密引數。配置檔案下唯一需要的引數是轉換集。IPsec代理的IPsec對等地址和**match address ...**子句從GRE隧道的NHRP對映中自動派生。

tunnel protection ipsec profile <name>命令是在GRE通道介面下配置的，用於將GRE通道介面與IPsec配置檔案相關聯。此外，**tunnel protection ipsec profile <name>**指令還可與點對點GRE通道一起使用。在這種情況下，它將從**隧道源……和隧道目標……配置**派生**IPsec對等體和代理**資訊。這簡化了配置，因為IPsec對等裝置和加密ACL不再需要。

注意：tunnel protection ...命令指定在將GRE封裝新增到資料包後執行IPsec加密。

前兩個新命令與配置加密對映和使用**crypto map <name>命令將加密對映分配給介面類似**。很大的區別在於，使用新命令時，您無需指定IPsec對等體地址或ACL來匹配要加密的資料包。這些引數是從mGRE通道介面的NHRP對映自動確定的。

注意：在隧道介面上使用**tunnel protection ...**命令時，未在物理傳出介面上配置**crypto map ...**命令。

最後一個新命令**ip nhrp map multicast dynamic**允許NHRP在這些分支路由器啟動mGRE+IPsec隧道並註冊其單播NHRP對映時，自動將分支路由器新增到組播NHRP對映。要使動態路由協定在集線器和輻條之間的mGRE+IPsec隧道上工作，就需要此命令。如果此命令不可用，則中心路由器需要單獨的配置行來將組播對映到每個分支。

注意：通過此配置，分支路由器必須啟動mGRE+IPsec隧道連線，因為中心路由器未配置有關分支

的任何資訊。但是，這不是問題，因為使用DMVPN時，當分支路由器啟動時，mGRE+IPsec隧道會自動啟動，並且始終保持運行。

注意：以下示例顯示分支路由器上的點對點GRE隧道介面，以及在中心路由器和分支路由器上新增的NHRP配置線路，以支援中心路由器上的mGRE隧道。配置更改如下。

集線器路由器（舊）

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.16.1.1
  set transform-set trans2
  match address 101
 crypto map vpnmap1 20 IPsec-isakmp
  set peer 172.16.2.1
  set transform-set trans2
  match address 102
 . . .
 crypto map vpnmap1 <10n> IPsec-isakmp
  set peer 172.16.




 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
  crypto map vpnmap1
 !
 access-list 101 permit gre host 172.17.0.1 host
172.16.1.1
 access-list 102 permit gre host 172.17.0.1 host
172.16.2.1
 . . .
 access-list
```

集線器路由器（新）

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
```

```
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
```

輻條<n>路由器（舊）

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
 !
interface Ethernet0
  ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
!
 . . .
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
 !
```

輻條<n>路由器（新）

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
 !
interface Ethernet0
  ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
!
 . . .
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
 !
```

在分支路由器上，子網掩碼已更改，並且隧道介面下新增了NHRP命令。NHRP命令是必需的，因為中心路由器現在使用NHRP將分支隧道介面IP地址對映到分支物理介面IP地址。

```
ip address 10.0.0.


      ip mtu 1400
      ip nhrp authentication test
      ip nhrp map 10.0.0.1 172.17.0.1
      ip nhrp network-id 100000
      ip nhrp holdtime 300
      ip nhrp nhs 10.0.0.1
      ...
      tunnel key 100000
```

子網現在是/24而不是/30，因此所有節點都位於同一個子網中，而不是不同的子網。輻條仍會透過集線器傳送輻條至輻條流量，因為它們使用點對點GRE通道介面。在集線器上收到通道封包和NHRP封包時，會使用**ip nhrp authentication ...**、**ip nhrp network-id ...**和**tunnel key ...**指令將通道封包和NHRP封包對映到正確的多點GRE通道介面和NHRP網路。**ip nhrp map ...**和**ip nhrp nhs** ...命令由NHRP在分支上使用，以將分支NHRP對映(10.0.0.<n+1> —> 172.16.<n>.1)通告給中心。從隧道介面上的**ip address ...命令檢索10.0.0.<n+1>地址，從隧道介面上的tunnel destination ...命令檢索172.16.<n>.1地**址。

如果分支路由器數量為300台，此更改將使中心配置線路的數量從3900條線路減少到16條（減少了3884條線路）。 每個分支路由器上的配置將增加6行。

支援輻條上的動態地址

在Cisco路由器上，每個IPsec對等路由器需要先配置另一個IPsec對等路由器的IP地址，然後才能啟動IPsec隧道。如果輻條路由器的物理介面上有一個動態地址，則執行此操作會遇到問題。對於通過DSL或電纜鏈路連線的路由器，動態地址是常見的。

TED允許一個IPsec對等體通過傳送一個特殊的Internet安全關聯和金鑰管理協定(ISAKMP)資料包到需要加密的原始資料包的IP目標地址來查詢另一個IPsec對等體。假設此封包會沿與IPsec通道封包相同的路徑經過干預網路。此封包將由另一端IPsec對等路由器擷取，該對等路由器會回應第一個對等路由器。然後，兩台路由器將協商ISAKMP和IPsec安全關聯(SA)並啟用IPsec隧道。只有要加密的資料包具有可路由IP地址時，此功能才會起作用。

TED可與GRE隧道結合使用，配置如前一部分所示。這已經過測試且有效，儘管早期版本的Cisco IOS軟體存在錯誤，其中TED強制對兩個IPsec對等路由器之間的所有IP流量進行加密，而不僅僅是GRE通道封包。DMVPN解決方案提供此功能和其他功能，無需主機使用網際網路可路由IP地址，也無需傳送探測和響應資料包。稍作修改後，最後一部分中的配置可用於支援分支路由器在其外部物理介面上具有動態IP地址。

集線器路由器（無變化）

```
crypto ipsec profile vpnprof
  set transform-set trans2
```

```
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
```

輻條<n>路由器（舊）

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 ...
 !
 access-list 101 permit gre host 172.16.
```

輻條<n>路由器（新）

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  set security-association level per-host
  match address 101
 !
 ...
 !
 access-list 101 permit gre any host 172.17.0.1
```

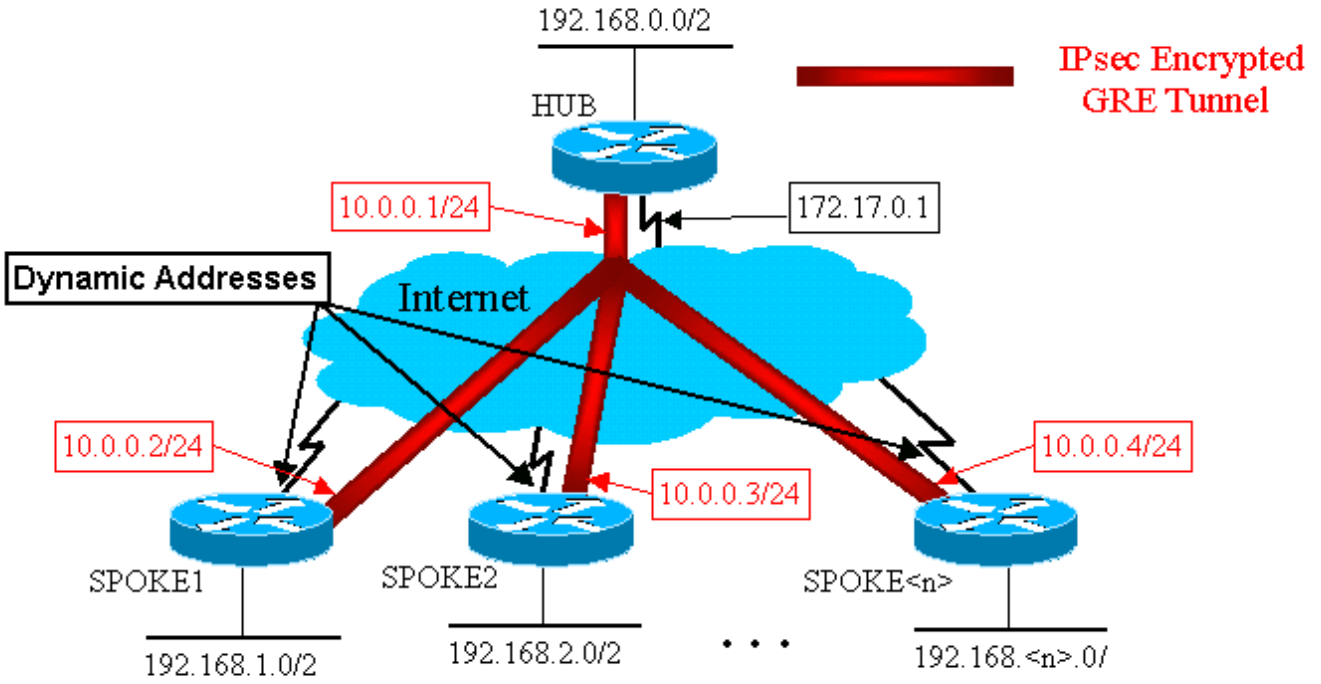
新分支配置中使用的功能如下。

- 當GRE通道介面啟動時，它會開始將NHRP註冊封包傳送到集線器路由器。這些NHRP註冊資料包將觸發啟動IPsec。在分支路由器上，配置了set peer <peer-address>和**match ip access-list <ACL>**命令。ACL會指定GRE作為協定，其中any用於源，而集線器IP地址用於目標。**注意：必須注意的是，any正被用作ACL中的源**地址，這必須是這種情況，因為分支路由器的IP地址是動態的，因此在物理介面處於活動狀態之前是未知的。如果動態分支介面地址將限制在該子網內的某個地址，則可以將IP子網用於ACL中的源。
- 使用**set security-association level per-host**命令可使分支IPsec代理中的IP源僅是分支的當前物理介面地址(/32)，而不是ACL中的「any」。如果將ACL中的「any」用作IPsec代理中的來源，則會阻止任何其他分支路由器也使用此集線器建立IPsec+GRE通道。這是因為集線器上產生

的IPsec代理相當於**permit gre host 172.17.0.1 any**。這表示所有目的地為任何輻條的GRE通道封包都會經過加密，並傳送到與集線器建立通道的第一輻條，因為其IPsec代理會為每個輻條匹配GRE封包。

- 建立IPsec通道後，NHRP註冊資料包將從分支路由器傳送到已配置的下一跳伺服器(NHS)。NHS是此星型網路的中心路由器。NHRP註冊資料包為中心路由器提供資訊，以便為該分支路由器建立NHRP對映。透過此對應，中心路由器便可透過mGRE+IPsec通道將單點傳播IP封包轉送到此分支路由器。此外，集線器還會將分支路由器新增到其NHRP組播對映清單。然後，集線器將開始向分支傳送動態IP路由組播資料包（如果配置了動態路由協定）。 然後，分支將成為中心點的路由協定鄰居，它們將交換路由更新。

IPsec + mGRE中心輻射型



集線器路由器

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
```

```
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

請注意，在上述集線器配置中，並未配置分支路由器的IP地址。中心節點通過NHRP動態獲取輻條的外部物理介面和到輻條的隧道介面IP地址的對映。這樣可動態分配分支的外部物理介面IP地址。

Spoke1路由器

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set security-association level per-host
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
!
interface Ethernet0
```

```
 ip address dhcp hostname Spoke1
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre 172.16.1.0 0.0.0.255 host
172.17.0.1
```

Spoke2路由器

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set security-association level per-host
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
!
interface Ethernet0
 ip address dhcp hostname Spoke2
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre 172.16.2.0 0.0.0.255 host
172.17.0.1
```

有關分支配置需要注意的主要事項包括：

- 外部物理介面(ethernet0)的IP地址通過DHCP是動態的。**ip address dhcp hostname Spoke2**
- 加密ACL(101)指定子網作為IPsec代理的源。**access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1**
- IPsec加密對映中的以下命令指定安全關聯將基於每個主機。**按主機設定安全關聯級別**
- 所有通道都是同一子網的一部分，因為它們都通過集線器路由器上的同一多點GRE介面連線。**ip address 10.0.0.2 255.255.255.0**

這三個命令的組合使得無需配置分支的外部物理介面IP地址。使用的IPsec代理將基於主機，而不是基於子網。

分支路由器上的配置配置了中心路由器的IP地址，因為它需要啟動IPsec+GRE隧道。請注意Spoke1和Spoke2配置之間的相似性。這兩個分支路由器配置不僅相似，而且相似。大多數情況下，所有輻條只需在其介面上提供唯一的IP地址，其餘配置將相同。這使得可以快速配置和部署許多分支路由器。

NHRP資料在中心和分支上類似於以下內容。

集線器路由器

```
Hub#show ip nhrp
   10.0.0.2/32 via 10.0.0.2, Tunnel0 created 01:25:18,
expire 00:03:51
     Type: dynamic, Flags: authoritative unique
registered
     NBMA address: 172.16.1.4
   10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:06:02,
expire 00:04:03
     Type: dynamic, Flags: authoritative unique
registered
     NBMA address: 172.16.2.10
   ...
   10.0.0.<n>/32 via 10.0.0.<n>, Tunnel0 created
00:06:00, expire 00:04:25
     Type: dynamic, Flags: authoritative unique
registered
     NBMA address: 172.16.<n>.41
```

Spoke1路由器

```
Spoke1#sho ip nhrp
   10.0.0.1/32 via 10.0.0.1, Tunnel0 created 4d08h,
never expire
     Type: static, Flags: authoritative
     NBMA address: 172.17.0.1
```

動態多點中心輻射型

上述分支路由器上的配置不依賴DMVPN解決方案的功能，因此分支路由器可以運行12.2(13)T之前的Cisco IOS軟體版本。中心路由器上的配置確實依賴DMVPN功能，因此必須運行Cisco IOS版本12.2(13)T或更高版本。這樣，在決定何時需要升級已部署的分支路由器時，您就可以有一定的靈活性。如果您的分支路由器也運行Cisco IOS版本12.2(13)T或更高版本，則可以按如下方式簡化分支配置。

輻條<n>路由器(Cisco IOS 12.2(13)T之前)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
 !
 interface Ethernet0
  ip address dhcp hostname Spoke<n>
  crypto map vpnmap1
 !
 . . .
 !
 access-list 101 permit gre any host 172.17.0.1
```

輻條<n>路由器(在Cisco IOS 12.2(13)T之後)

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke<n>
 !
```

請注意，我們已經完成了以下操作：

1. 已刪除crypto map vpnmap1 10 ipsec-isakmp命令，並將其替換為crypto ipsec profile

vpnprof。

2. 已從Ethernet0介面刪除**crypto map vpnmap1**命令，然後在Tunnel0介面上放置**tunnel protection ipsec profile vpnprof**命令。
3. 已刪除加密ACL**access-list 101 permit gre any host 172.17.0.1**。

在這種情況下，IPsec對等體地址和代理將自動從**隧道源……和**隧道**目標……配置**派生。對等體和代理如下所示(如**show crypto ipsec sa**命令的輸出所示):

```
...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...
```

總而言之，以下完整配置包括到此時為止從基本配置（IPsec+GRE中心和分支）進行的所有更改。

集線器路由器

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
 !
```

集線器配置沒有任何更改。

Spoke1路由器

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke2
 !
 interface Ethernet1
  ip address 192.168.1.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  no auto-summary
 !
```

Spoke2路由器

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
```

```
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!
```

動態多點IPsec VPN

本節中的概念和配置顯示了DMVPN的全部功能。NHRP使分支路由器能夠動態獲知VPN網路中其他分支路由器的外部物理介面地址。這表示分支路由器將具有足夠的資訊，可以動態建立直接連線到其他分支路由器的IPsec+mGRE隧道。這是有利的，因為如果此分支到分支資料流量是通過中心路由器傳送的，則必須對其進行加密/解密，這樣會增加兩次延遲和中心路由器上的負載。為了使用此功能，分支路由器需要從點對點GRE(p-pGRE)切換到多點GRE(mGRE)通道介面。他們還需要使用其它分支路由器隧道IP地址的IP下一跳，瞭解其它分支後可用的子（子）網路。分支路由器通過運行在與集線器的IPsec+mGRE隧道上的動態IP路由協定來瞭解這些（子）網路。

在中心路由器上運行的動態IP路由協定可以配置為將從一個分支獲知的路由從同一介面返回至所有其他分支，但這些路由上的IP下一跳通常是中心路由器，而不是中心獲知此路由的分支路由器。

注意：動態路由協定僅運行在中心和分支鏈路上，而非運行在動態分支到分支鏈路上。

需要在中心路由器上配置動態路由協定（RIP、OSPF和EIGRP），以從mGRE隧道介面通告路由，並在路由通告回其它分支時，將路由的IP下一跳設定為始發分支路由器。

以下是路由協定配置的要求。

RIP

您需要關閉集線器上mGRE通道介面上的水準分割，否則RIP不會將通過mGRE介面獲知的路由通告出該介面。

```
no ip split-horizon
```

無需進行其他更改。RIP會在路由上自動使用原始IP下一跳，並在獲知這些路由的同一介面上通告這些路由。

EIGRP

您需要關閉集線器上mGRE通道介面上的水準分割，否則EIGRP不會將通過mGRE介面獲知的路由通告出該介面。

```
no ip split-horizon eigrp
```

預設情況下，EIGRP會將IP下一跳設定為所通告路由的中心路由器，即使是在從獲取這些路由的同一介面通告這些路由時。在這種情況下，您需要使用以下配置命令來指示EIGRP在通告這些路由時使用原始IP下一跳。

```
no ip next-hop-self eigrp
```

注意：no ip next-hop-self eigrp <as>命令從Cisco IOS版本12.3(2)開始可用。 對於介於12.2(13)T和12.3(2)之間的Cisco IOS版本，必須執行以下操作：

- 如果不需要分支到分支的動態隧道，則不需要上述命令。
- 如果需要分支到分支的動態隧道，則必須在分支路由器上的隧道介面上使用進程交換。
- 否則，您需要在DMVPN上使用不同的路由協定。

OSPF

由於OSPF是鏈路狀態路由協定，因此不存在任何水準分割問題。通常，對於多點介面，您將OSPF網路型別配置為點對多點，但這會導致OSPF將主機路由新增到分支路由器的路由表中。這些主機路由將導致發往其它分支路由器後面的網路的資料包通過集線器轉發，而不是直接轉發到其它分支。要解決此問題，請使用命令配置要廣播的OSPF網路型別。

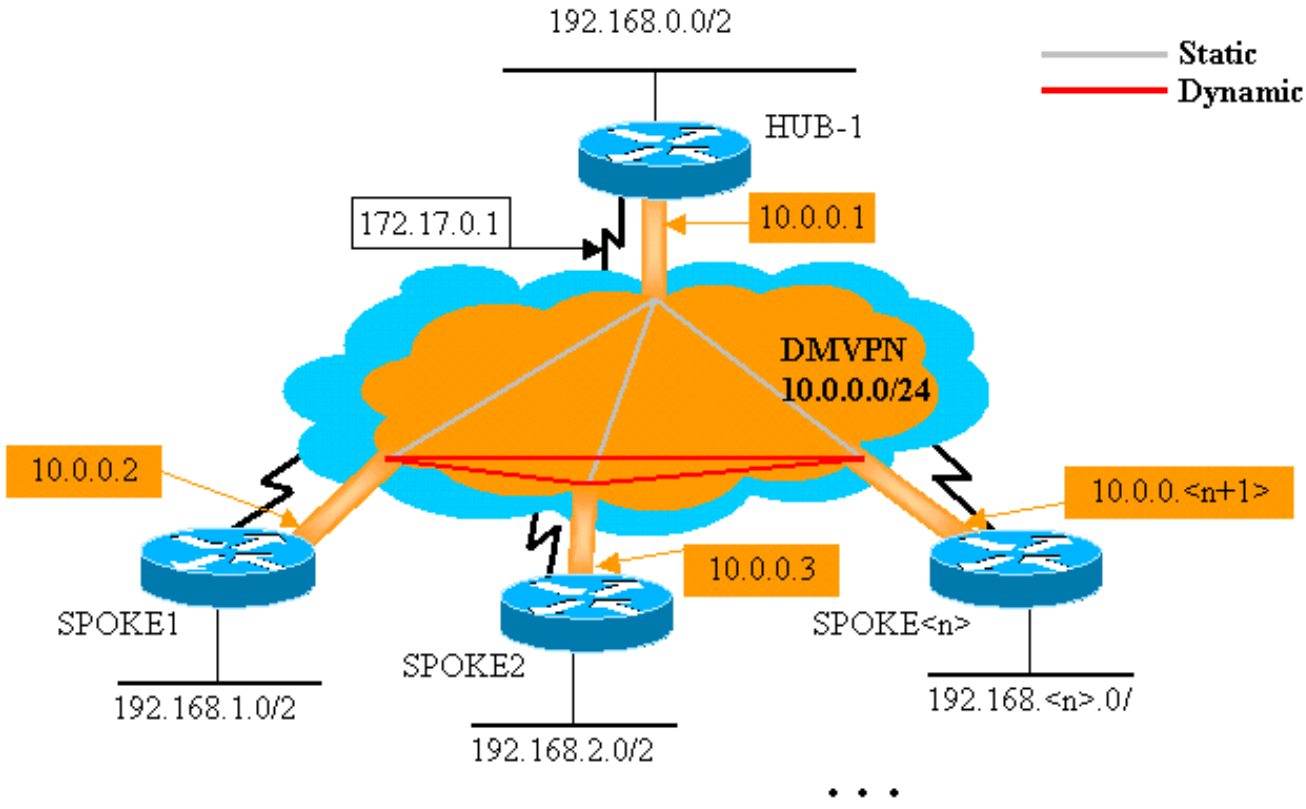
```
ip ospf network broadcast
```

您還需要確保中心路由器是IPsec+mGRE網路的指定路由器(DR)。這是通過將OSPF優先順序設定為在集線器上大於1，在分支上大於0完成的。

- 中心：**ip ospf priority 2**

- 分支：ip ospf priority 0

DMVPN單一集線器



集線器路由器

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast
  ip ospf priority 2
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
```

```
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
```

集線器配置中的唯一更改是OSPF是路由協定而不是EIGRP。請注意，OSPF網路型別設定為廣播，優先順序設定為2。將OSPF網路型別設定為廣播將導致OSPF為分支路由器後面的網路安裝路由，並將IP下一跳地址作為該分支路由器的GRE隧道地址。

Spoke1路由器

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
```

```
!
```

分支路由器上的配置現在與集線器上的配置非常相似。差異如下：

- OSPF優先順序設定為0。不能允許分支路由器成為mGRE非廣播多路訪問(NBMA)網路的DR。只有中心路由器與所有分支路由器具有直接靜態連線。DR必須能夠訪問NBMA網路的所有成員。
- 為集線器路由器配置了NHRP單播和組播對映。

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
```

  在先前的設定中，由於GRE通道是點對點通道，因此不需要使用**ip nhrp map multicast ...**指令。在這種情況下，組播資料包將通過隧道自動封裝到單個可能的目的地。現在需要使用此命令，因為分支GRE隧道已更改為多點，並且有多個可能的目的地。
- 當分支路由器啟動時，它必須與中心路由器啟動隧道連線，因為中心路由器未配置有關分支路由器的任何資訊，並且分支路由器可能具有動態分配的IP地址。分支路由器也配置中心作為其NHRP NHS。

  `ip nhrp nhs 10.0.0.1`

  使用上述命令，分支路由器將定期通過mGRE+IPsec隧道將NHRP註冊資料包傳送到中心路由器。這些註冊資料包提供分支路由器NHRP對映資訊，集線器路由器需要這些資訊才能將資料包通道回分支路由器。

Spoke2路由器

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.3 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast
  ip ospf priority 0
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
```

```
 interface Ethernet0
  ip address dhcp hostname Spoke1
 !
 interface Ethernet1
  ip address 192.168.3.1 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 0
  network 192.168.2.0 0.0.0.255 area 0
 !
```

分支<n>路由器

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast
  ip ospf priority 0
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke<n>
 !
 interface Ethernet1
  ip address 192.168.<n>.1 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 0
  network 192.168.




 !
```

請注意，所有分支路由器的配置非常相似。唯一的區別是本地介面上的IP地址。這在部署大量分支

路由器時很有幫助。所有分支路由器都可以以相同方式配置，並且只需要新增本地IP介面地址。

此時，請檢視中心路由器、Spoke1路由器和Spoke2路由器上的路由表和NHRP對映表，以檢視初始條件（Spoke1路由器和Spoke2路由器剛剛啟動之後）以及Spoke1和Spoke2路由器之間已建立動態鏈路之後的條件。

初始條件

中心路由器資訊

```
Hub#show ip route
      172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 O    192.168.1.0/24 [110/2] via 10.0.0.2, 00:19:53,
Tunnel0
 O    192.168.2.0/24 [110/2] via 10.0.0.3, 00:19:53,
Tunnel0
 Hub#show ip nhrp
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:57:27,
expire    00:04:13
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 10.0.0.3/32 via 10.0.0.3, Tunnel0 created 07:11:25,
expire    00:04:33
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 Hub#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
  204 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
  205 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
 2628 Tunnel0     10.0.0.1       set  HMAC_MD5
0     402
 2629 Tunnel0     10.0.0.1       set  HMAC_MD5
357       0
 2630 Tunnel0     10.0.0.1       set  HMAC_MD5
0     427
 2631 Tunnel0     10.0.0.1       set  HMAC_MD5
308       0
```

Spoke1路由器資訊

```
Spoke1#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.24 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:31:46,
Tunnel0
 C    192.168.1.0/24 is directly connected, Ethernet1
 O    192.168.2.0/24 [110/2] via 10.0.0.3, 00:31:46,
Tunnel0
 Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:42:00,
```

```
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 Spoke1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    2 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
 2064 Tunnel0     10.0.0.2       set  HMAC_MD5
0     244
 2065 Tunnel0     10.0.0.2       set  HMAC_MD5
276       0
```

Spoke2路由器資訊

```
Spoke2#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.2.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:38:52,
Tunnel0
 O    192.168.1.0/24 [110/2] via 10.0.0.2, 00:38:52,
Tunnel0
 C    192.168.2.0/24 is directly connected, Ethernet1
 Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:32:10,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 Spoke2#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
   17 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
 2070 Tunnel0     10.0.0.3       set  HMAC_MD5
0     279
 2071 Tunnel0     10.0.0.3       set  HMAC_MD5
316       0
```

此時，我們從192.168.1.2 ping 192.168.2.3。這些地址分別用於Spoke1和Spoke2路由器後面的主機。以下事件序列用於構建直接輻條到輻條mGRE+IPsec隧道。

1. Spoke1路由器收到目的地為192.168.2.3的ping資料包。它在路由表中查詢此目標，發現它需要將此資料包從Tunnel0介面轉發到IP下一跳10.0.0.3。
2. Spoke1路由器檢查目標10.0.0.3的NHRP對映表，發現沒有條目。Spoke1路由器建立一個NHRP解析請求資料包並將其傳送到其NHS（中心路由器）。
3. 中心路由器檢查其NHRP對映表以查詢目標10.0.0.3，並發現它對映到地址172.16.2.75。中心路由器建立NHRP解析應答資料包並將其傳送到Spoke1路由器。
4. Spoke1路由器收到NHRP解析應答，並在NHRP對映表中輸入10.0.0.3 —>172.16.2.75對映。新增NHRP對映觸發IPsec發起與對等體172.16.2.75的IPsec隧道。
5. Spoke1路由器使用172.16.2.75發起ISAKMP，並協商ISAKMP和IPsec SA。IPsec代理源自Tunnel0 **tunnel source <address>命**令和NHRP對映。

   ```
   local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0)
   ```

6. IPsec隧道完成構建後，所有到192.168.2.0/24子網的其他資料包都將直接傳送到Spoke2。

7. 將目的地為192.168.2.3的資料包轉發到主機後，此主機將傳送返回資料包到192.168.1.2。當Spoke2路由器收到目的地為192.168.1.2的資料包時，它將在路由表中查詢此目標，並發現它需要將此資料包從Tunnel0介面轉發到IP下一跳10.0.0.2。
8. Spoke2路由器檢查目標10.0.0.2的NHRP對映表，發現沒有條目。Spoke2路由器建立一個NHRP解析請求資料包並將其傳送到其NHS（中心路由器）。
9. 中心路由器檢查其NHRP對映表以查詢目標10.0.0.2，並發現它對映到地址172.16.1.24。中心路由器建立NHRP解析應答資料包並將其傳送到Spoke2路由器。
10. Spoke2路由器收到NHRP解析應答，並在NHRP對映表中輸入10.0.0.2 —> 172.16.1.24對映。新增NHRP對映觸發IPsec發起使用對等體172.16.1.24的IPsec隧道，但已經存在使用對等體172.16.1.24的IPsec隧道，因此無需執行其他操作。
11. 現在，Spoke1和Spoke2可以直接將資料包相互轉發。當NHRP對映在保持時間內未用於轉發資料包時，NHRP對映將被刪除。刪除NHRP對映條目將觸發IPsec刪除該直接鏈路的IPsec SA。

在Spoke1和Spoke2之間建立動態鏈路之後的條件

Spoke1路由器資訊

```
Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:34:16,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:05,
expire 00:03:35
   Type: dynamic, Flags: router unique used
   NBMA address: 172.16.2.75
 Spoke1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    2 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
    3 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
 2064 Tunnel0     10.0.0.2       set  HMAC_MD5
0     375
 2065 Tunnel0     10.0.0.2       set  HMAC_MD5
426       0
 2066 Tunnel0     10.0.0.2       set  HMAC_MD5
0      20
 2067 Tunnel0     10.0.0.2       set  HMAC_MD5
19        0
```

Spoke2路由器資訊

```
Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:18:25,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:00:24,
expire 00:04:35
   Type: dynamic, Flags: router unique used
   NBMA address: 172.16.1.24
 Spoke2#show crypto engine connection active
```

```
  ID  Interface   IP-Address     State Algorithm
Encrypt Decrypt
   17 Ethernet0   172.16.2.75     set  HMAC_SHA+DES_56_CB
0       0
   18 Ethernet0   172.16.2.75     set  HMAC_SHA+DES_56_CB
0       0
 2070 Tunnel0     10.0.0.3        set  HMAC_MD5
0     407
 2071 Tunnel0     10.0.0.3        set  HMAC_MD5
460       0
 2072 Tunnel0     10.0.0.3        set  HMAC_MD5
0      19
 2073 Tunnel0     10.0.0.3        set  HMAC_MD5
20        0
```

從上面的輸出中，您可以看到Spoke1和Spoke2已從中心路由器獲得彼此的NHRP對映，並且它們已建立並使用mGRE+IPsec隧道。NHRP對映將在五分鐘後過期（NHRP保持時間的當前值= 300秒）。 如果在到期前的最後一分鐘內使用NHRP對映，則會傳送NHRP解析請求和回覆以便在刪除條目之前對其進行刷新。否則，將刪除NHRP對映，這將觸發IPsec清除IPsec SA。

含雙集線器的動態多點IPsec VPN

藉助分支路由器的一些額外配置線路，您可以設定雙（或多台）中心路由器以實現冗餘。配置雙中心DMVPN有兩種方法。

- 單個DMVPN網路，每個分支使用單個多點GRE隧道介面並指向兩個不同的集線器作為其下一跳伺服器(NHS)。集線器路由器將只有一個多點GRE通道介面。
- 雙DMVPN網路，每個分支具有兩個GRE隧道介面（點對點或多點），每個GRE隧道連線到不同的中心路由器。同樣地，中心路由器將只有一個多點GRE通道介面。

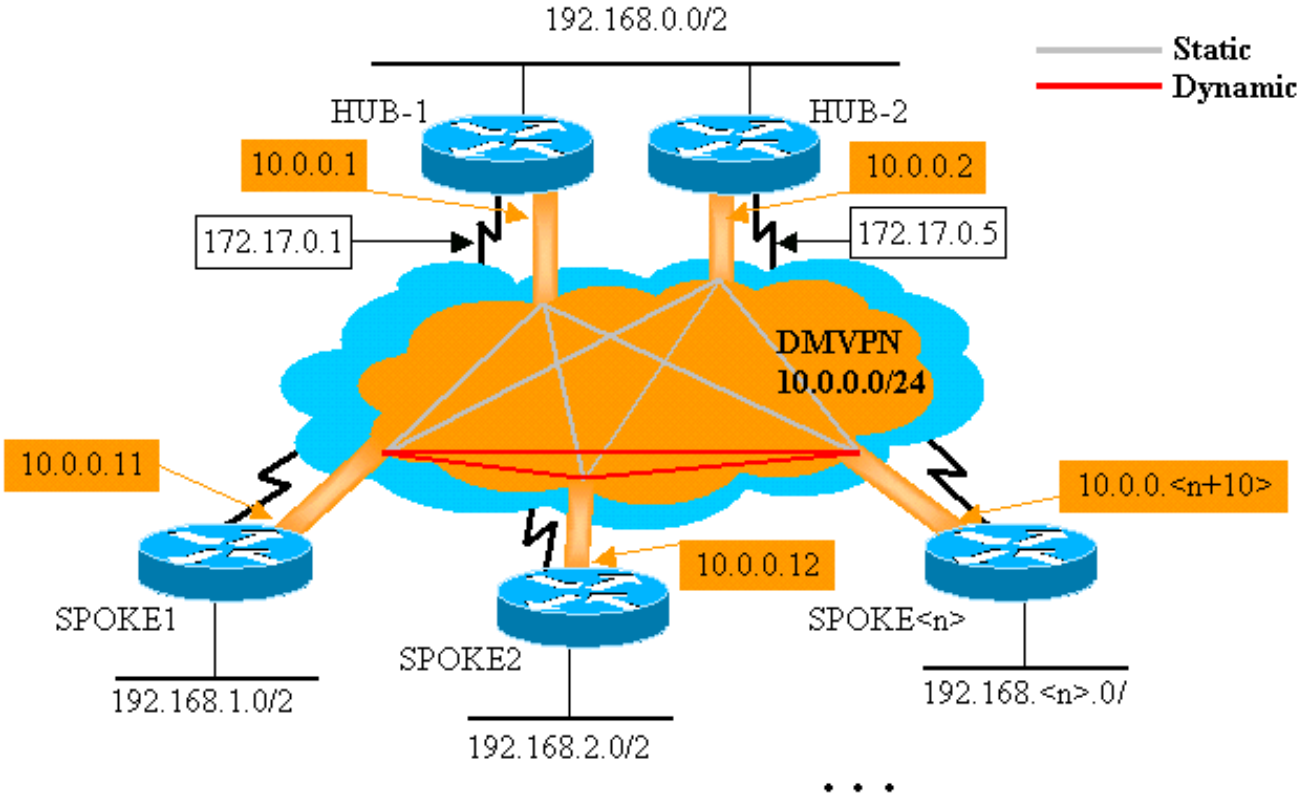
以下示例將介紹為雙中心DMVPN配置這兩種不同方案。在這兩種情況下，突出顯示的區別都與DMVPN單中心配置有關。

雙集線器 — 單DMVPN佈局

具有單一DMVPN佈局的雙集線器設定非常簡單，但它不能像具有雙DMVPN佈局的雙集線器那樣為您提供對DMVPN間路由的控制。此案例的想法是擁有一個DMVPN「雲」，其中包含所有集線器（此案例為兩個）以及所有連線到此單個子網的輻條（「雲」）。 從輻條到集線器的靜態NHRP對映定義了將運行動態路由協定的靜態IPsec+mGRE鏈路。動態路由協定不會在分支之間的動態IPsec+mGRE鏈路上運行。由於分支路由器與中心路由器在同一mGRE通道介面上是路由鄰居，因此不能使用鏈路或介面差異（如度量、成本、延遲或頻寬）來修改動態路由協定度量，以便在兩個中心都啟動時優先使用其中一個中心而不是另一個中心。如果需要此首選項，則必須使用路由協定配置內部技術。因此，最好使用EIGRP或RIP而不是OSPF作為動態路由協定。

注意：上述問題通常僅在中心路由器位於同一位置時才出現。如果沒有並置位置，正常的動態路由最終可能優先使用正確的集線器路由器，即使可以通過任一集線器路由器到達目的網路。

雙集線器 — 單DMVPN佈局



集線器路由器

```
version 12.3
 !
 hostname Hub1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast
  ip ospf priority 2
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
```

```
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.0.0 0.0.0.255 area 0
 !
```

集線器2路由器

```
version 12.3
 !
 hostname Hub2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 900
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map  multicast 172.17.0.1
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast
  ip ospf priority 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.5 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.2 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.0.0 0.0.0.255 area 0
 !
```

Hub1配置中的唯一更改是將OSPF更改為使用兩個區域。區域0用於兩個集線器後面的網路，區域1用於DMVPN網路和分支路由器後面的網路。OSPF可以使用單一區域，但此處使用兩個區域來演示多個OSPF區域的配置。

Hub2的配置與Hub1的配置基本相同，但相應的IP地址發生了更改。一個主要區別是Hub2也是Hub1的輻條（或客戶端），使Hub1成為主中心，Hub2成為輔助中心。完成此操作後，Hub2會通過mGRE隧道與Hub1成為OSPF鄰居。由於Hub1是OSPF DR，因此它必須通過mGRE介面（NBMA網路）與所有其他OSPF路由器建立直接連線。 如果沒有Hub1和Hub2之間的直接鏈路，Hub2不會參與OSPF路由，因為Hub1也處於開啟狀態。當Hub1關閉時，Hub2將成為DMVPN（NBMA網路）的OSPF DR。 當Hub1恢復運行時，它將接替DMVPN的OSPF DR。

由於GRE通道介面的頻寬設定為1000 Kb/sec，而Hub1和Hub2後面的路由器會使用Hub1將封包傳送到分支網路，因為GRE通道介面的頻寬設定為1000 Kb/sec，而Hub2上的頻寬設定為900 Kb/sec。相反，由於每個分支路由器上只有一個mGRE通道介面，且將有兩個等價路由，因此這些分支路由器會同時向Hub1和Hub2傳送封包。如果使用按資料包負載平衡，則可能導致資料包順序混亂。

Spoke1路由器

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map multicast 172.17.0.5
  ip nhrp map 10.0.0.2 172.17.0.5
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip nhrp nhs 10.0.0.2
  ip ospf network broadcast
  ip ospf priority 0
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke1
 !
 interface Ethernet1
  ip address 192.168.1.1 255.255.255.0
 !
 router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.1.0 0.0.0.255 area 1
```

```
!
```

分支路由器上的配置差異如下：

- 在新配置中，分支配置了用於Hub2的靜態NHRP對映，並且Hub2新增為下一跳伺服器。原始：

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp nhs 10.0.0.1
```

新增：

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp map multicast 172.17.0.5
ip nhrp map 10.0.0.2 172.17.0.5
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.0.2
```

- 分支路由器上的OSPF區域已更改為區域1。

請記住，通過在中心點的分支路由器上定義靜態NHRP對映和NHS，您將通過此隧道運行動態路由協定。這定義中心和分支路由或鄰居網路。請注意，Hub2是所有輻條的輻條中心，也是Hub1的輻條中心。因此，使用DMVPN解決方案時，可以輕鬆設計、配置和修改多層輻條網路。

Spoke2路由器

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map multicast 172.17.0.5
  ip nhrp map 10.0.0.2 172.17.0.5
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip nhrp nhs 10.0.0.2
  ip ospf network broadcast
  ip ospf priority 0
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
```

```
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
```

分支<n>路由器

```
version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<n+10> 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.5
 ip nhrp map 10.0.0.2 172.17.0.5
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<x>
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.
```

```
!
```

此時，您可以檢視路由器Hub1、Hub2、Spoke1和Spoke2上的路由表、NHRP對映表和IPsec連線，以檢視初始條件（在Spoke1和Spoke2路由器啟動之後）。

初始條件和更改

Hub1路由器資訊

```
Hub1#show ip route
      172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17,
Tunnel0
 O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17,
Tunnel0
 Hub1#show ip nhrp
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 1w3d, expire
00:03:15
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.17.0.5
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d,
expire 00:03:49
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 1w3d,
expire 00:04:06
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 Hub1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    4 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
    5 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
    6 Ethernet0   172.17.0.1     set  HMAC_SHA+DES_56_CB
0       0
 3532 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
0     232
 3533 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
212       0
 3534 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
0      18
 3535 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
17       0
 3536 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
0       7
 3537 Tunnel0     10.0.0.1       set  HMAC_MD5+DES_56_CB
7       0
```

Hub2路由器資訊

```
Hub2#show ip route
      172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15,
Tunnel0
 O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15,
Tunnel0
 Hub2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1w3d, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d,
expire 00:03:15
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:46:17,
expire 00:03:51
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 Hub2#show crypto engine connection active
   ID Interface   IP-Address    State Algorithm
Encrypt Decrypt
    4 Ethernet0   171.17.0.5     set  HMAC_SHA+DES_56_CB
0        0
    5 Ethernet0   171.17.0.5     set  HMAC_SHA+DES_56_CB
0        0
    6 Ethernet0   171.17.0.5     set  HMAC_SHA+DES_56_CB
0        0
 3520 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
0      351
 3521 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
326        0
 3522 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
0      311
 3523 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
339        0
 3524 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
0       25
 3525 Tunnel0     10.0.0.2       set  HMAC_MD5+DES_56_CB
22         0
```

Spoke1路由器資訊

```
Spoke1#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31,
Tunnel0
                     [110/11] via 10.0.0.2, 00:39:31,
Tunnel0
 C    192.168.1.0/24 is directly connected, Ethernet1
 O    192.168.2.0/24 [110/2] via 10.0.0.12, 00:37:58,
Tunnel0
 Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 00:56:40,
never expire
```

```
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:56:40,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.5
 Spoke1#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    1 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
    2 Ethernet0   172.16.1.24    set  HMAC_SHA+DES_56_CB
0       0
 2010 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
0     171
 2011 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
185       0
 2012 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
0      12
 2013 Tunnel0     10.0.0.11      set  HMAC_MD5+DES_56_CB
13        0
```

Spoke2路由器資訊

```
Spoke2#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.2.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56,
Tunnel0
                     [110/11] via 10.0.0.2, 00:57:56,
Tunnel0
 O    192.168.1.0/24 [110/2] via 10.0.0.11, 00:56:14,
Tunnel0
 C    192.168.2.0/24 is directly connected, Ethernet1
 Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 5w6d, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 6w6d, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.5
 Spoke2#show crypto engine connection active
  ID  Interface   IP-Address    State Algorithm
Encrypt Decrypt
    2 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
    3 Ethernet0   172.16.2.75    set  HMAC_SHA+DES_56_CB
0       0
 3712 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
0     302
 3713 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
331       0
 3716 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
0     216
 3717 Tunnel0     10.0.0.12      set  HMAC_MD5+DES_56_CB
236       0
```

關於Hub1、Hub2、Spoke1和Spoke2上的路由表，有幾個有趣的問題需要注意：

- 兩台中心路由器都有到達分支路由器後網路的等價路由。中心1:

```
O     192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0
O     192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0
```

中心2:

```
O     192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0
O     192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0
```

這意味著Hub1和Hub2會將分支路由器後面的網路的相同開銷通告給中心路由器後面的網路中的路由器。例如，直接連線到192.168.0.0/24 LAN的路由器R2上的路由表如下所示：R2：

```
O     IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3
                        [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3O
O     IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
                        [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3
```

- 分支路由器具有通過兩個中心路由器到達中心路由器後面的網路的等價路由。輻射點1:

```
O     IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0
                        [110/11] via 10.0.0.2, 00:39:31, Tunnel0
```

分支2:

```
O     IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0
                        [110/11] via 10.0.0.2, 00:57:56, Tunnel0
```

如果分支路由器正在執行每個資料包的負載均衡，則可能會產生亂序資料包。

為了避免在通向兩個集線器的鏈路上執行非對稱路由或每資料包負載均衡，您需要配置路由協定以優先使用兩個方向的一條分支到集線器的路徑。如果希望Hub1為主交換機，Hub2為備用交換機，則可以將集線器隧道介面上的OSPF開銷設定為不同。

中心1:

```
interface tunnel0
...
ip ospf cost 10
...
```

中心2:

```
interface tunnel0
...
ip ospf cost 20
...
```

現在路由如下所示：

中心1:

```
O     192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O     192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

中心2:

```
O     192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O     192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2：

```
O     IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O     IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

現在，兩台中心路由器在分支路由器後面的網路的路由上開銷不同。這意味著將流量轉發到分支路由器時，應優先使用Hub1，這一點在路由器R2上可以看到。這將解決上述第一個專案符號中描述

的非對稱路由問題。

如上述第二個專案符號所述，其他方向的不對稱路由仍然存在。將OSPF用作動態路由協定時，可以採用一種變通方法解決此問題，方法是在輻條上的**router ospf 1**下使用**distance ...**命令，以優先使用通過Hub1獲知的路由而不是通過Hub2獲知的路由。

輻射點1:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

分支2:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

現在路由如下所示：

輻射點1:

```
O     192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

分支2:

```
O     192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

上述路由配置將防止非對稱路由，同時允許在Hub1關閉時故障切換到中心2。這表示當兩個集線器都啟動時，只使用Hub1。如果您希望通過平衡集線器間的輻條來使用兩個集線器，同時提供故障切換保護並且沒有非對稱路由，則路由配置可能會變得複雜，特別是在使用OSPF時。因此，以下具有雙DMVPN佈局的雙集線器可能是更好的選擇。

雙集線器 — 雙DMVPN佈局

帶有雙DMVPN佈局的雙集線器設定稍微更困難，但它確實可以更好地控制通過DMVPN的路由。其理念是擁有兩個獨立的DMVPN「雲」。 每個集線器（這種情況下為兩個）連線到一個DMVPN子網（「雲」），分支連線到兩個DMVPN子網（「雲」）。 由於分支路由器是兩個中心路由器通過兩個GRE通道介面的路由鄰居，因此您可以使用介面配置差異（如頻寬、成本和延遲）來修改動態路由協定度量，以便在兩個中心路由器都啟動時優先使用其中一個中心路由器而不是另一個中心路由器。

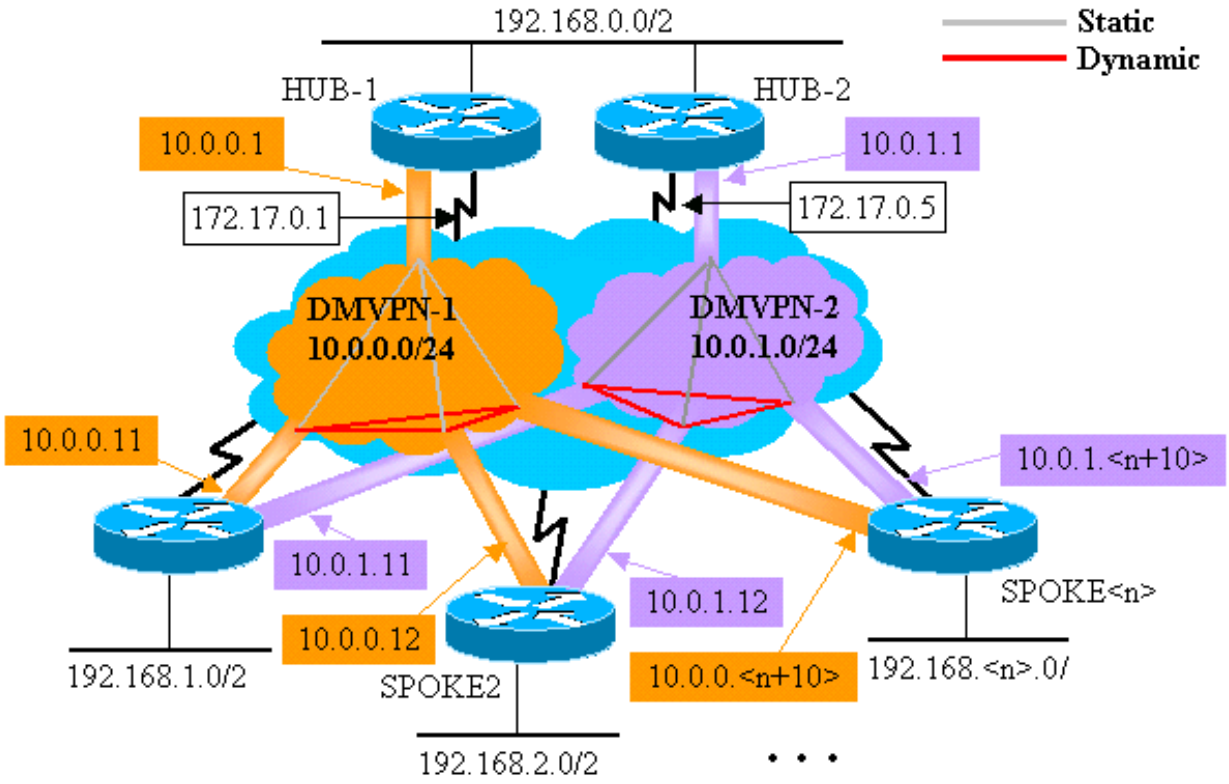
注意：上述問題通常僅在中心路由器位於同一位置時才相關。如果沒有並置位置，正常的動態路由最終可能優先使用正確的集線器路由器，即使可以通過任一集線器路由器到達目的網路。

可以在分支路由器上使用p-pGRE或mGRE隧道介面。分支路由器上的多個p-pGRE介面可以使用相同**的隧道源**……IP地址，但是分支路由器上的多個mGRE介面必須具有唯**一的隧道源**……IP 位址.這是因為當IPsec發起時，第一個封包是需要與其中一個mGRE通道關聯的ISAKMP封包。ISAKMP資料包只有目的IP地址（遠端IPsec對等地址）才能建立此關聯。此地址與**隧道源……地址匹配，但由於兩個隧道具有相同的隧道源……**地址，因此第一個mGRE隧道介面始終匹配。這意味著傳入的組播資料包可能與錯誤的mGRE介面關聯，從而中斷任何動態路由協定。

GRE資料包本身沒有此問題，因為它們具有用於區分兩個mGRE介面的**隧道金鑰**……值。從Cisco

IOS軟體版本12.3(5)和12.3(7)T開始，已匯入另一個引數以克服此限制：**隧道保護……shared**。**shared**關鍵字指示多個mGRE介面將使用具有相同源IP地址的IPSec加密。如果您有早期版本，您可以在此雙集線器中使用雙DMVPN佈局的p-pGRE通道。在p-pGRE通道的情況下，**通道來源**……和通**道目的地**……IP地址可用於匹配。在本例中，將在具有雙DMVPN佈局的此雙集線器中使用p-pGRE隧道，而不使用**共用**限定符。

雙集線器 — 雙DMVPN佈局



以下突出顯示的更改與本文檔前面所示的動態多點中心輻射型配置相關。

Hub1路由器

```
version 12.3
 !
 hostname Hub1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
```

```
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.252
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

集線器2路由器

```
version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.5 255.255.255.252
!
interface Ethernet1
 ip address 192.168.0.2 255.255.255.0
!
router eigrp 1
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
```

```
!
```

在本例中，Hub1和Hub2配置相似。主要區別在於，每個都是不同DMVPN的中心。每個DMVPN使用不同的：

- IP子網(10.0.0.0/24、10.0.0.1/24)
- NHRP網路ID(100000, 100001)
- 隧道金鑰(100000、100001)

動態路由協定已從OSPF切換到EIGRP，因為使用EIGRP設定和管理NBMA網路較為輕鬆，如本文檔稍後所述。

Spoke1路由器

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.5
  tunnel key 100001
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address dhcp hostname Spoke1
```

```
 !
 interface Ethernet1
  ip address 192.168.1.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  no auto-summary
 !
```

每個分支路由器都配置有兩個p-pGRE隧道介面，兩個DMVPN各一個。**ip address ...**、**ip nhrp network-id ...**、**tunnel key ...**和**tunnel destination ...**值用於區分兩個隧道。動態路由協定EIGRP運行在兩個p-pGRE隧道子網上，用於選擇一個p-pGRE介面(DMVPN)。

Spoke2路由器

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.5
  tunnel key 100001
  tunnel protection ipsec profile vpnprof
 !
```

```
 interface Ethernet0
  ip address dhcp hostname Spoke2
 !
 interface Ethernet1
  ip address 192.168.2.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  no auto-summary
 !
```

分支<n>路由器

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.




  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.




  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
```

```
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<x>
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.<n>.0 0.0.0.255
 no auto-summary
!
```

現在，我們來看看Hub1、Hub2、Spoke1和Spoke2路由器上的路由表、NHRP對映表和IPsec連線，瞭解初始條件（在Spoke1和Spoke2路由器啟動之後）。

初始條件和更改

Hub1路由器資訊

```
Hub1#show ip route
      172.17.0.0/30 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 2 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 D       10.0.1.0 [90/2611200] via 192.168.0.2,
00:00:46, Ethernet1
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.11,
00:00:59, Tunnel0
 D    192.168.2.0/24 [90/2841600] via 10.0.0.12,
00:00:34, Tunnel0
 Hub1#show ip nhrp
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 23:48:32,
expire 00:03:50
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 23:16:46,
expire 00:04:45
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 Hub1#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
   15 Ethernet0   172.17.63.18   set
HMAC_SHA+DES_56_CB      0        0
   16 Ethernet0   10.0.0.1       set
HMAC_SHA+DES_56_CB      0        0
 2038 Tunnel0     10.0.0.1       set
HMAC_MD5+DES_56_CB      0      759
 2039 Tunnel0     10.0.0.1       set
HMAC_MD5+DES_56_CB    726        0
 2040 Tunnel0     10.0.0.1       set
HMAC_MD5+DES_56_CB      0       37
```

```
 2041 Tunnel0     10.0.0.1       set
HMAC_MD5+DES_56_CB     36        0
```

Hub2路由器資訊

```
Hub2#show ip route
      172.17.0.0/30 is subnetted, 1 subnets
 C       172.17.0.4 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 2 subnets
 D       10.0.0.0 [90/2611200] via 192.168.0.1,
00:12:22, Ethernet1
 C       10.0.1.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.1.11,
00:13:24, Tunnel0
 D    192.168.2.0/24 [90/2841600] via 10.0.1.12,
00:12:11, Tunnel0
 Hub2#show ip nhrp
 10.0.1.12/32 via 10.0.1.12, Tunnel3 created 06:03:24,
expire 00:04:39
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 10.0.1.11/32 via 10.0.1.11, Tunnel3 created 23:06:47,
expire 00:04:54
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 Hub2#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
    4 Ethernet0   171.17.0.5     set
HMAC_SHA+DES_56_CB      0        0
    6 Ethernet0   171.17.0.5     set
HMAC_SHA+DES_56_CB      0        0
 2098 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB      0      722
 2099 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB    690        0
 2100 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB      0      268
 2101 Tunnel0     10.0.1.1       set
HMAC_MD5+DES_56_CB    254        0
```

Spoke1路由器資訊

```
Spoke1#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C       10.0.1.0 is directly connected, Tunnel1
 D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
00:26:30, Tunnel1
                     [90/2841600] via 10.0.0.1,
00:26:30, Tunnel0
 C    192.168.1.0/24 is directly connected, Ethernet1
 D    192.168.2.0/24 [90/3097600] via 10.0.1.1,
00:26:29, Tunnel1
                     [90/3097600] via 10.0.0.1,
00:26:29, Tunnel0
 Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 23:25:46,
never expire
```

```
   Type: static, Flags: authoritative
   NBMA address: 172.17.0.1
 10.0.1.1/32 via 10.0.1.1, Tunnel1 created 23:24:40,
never expire
   Type: static, Flags: authoritative
   NBMA address: 172.17.0.5
 Spoke1#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
   16 Ethernet0   172.16.1.24    set
HMAC_SHA+DES_56_CB      0        0
   18 Ethernet0   172.16.1.24    set
HMAC_SHA+DES_56_CB      0        0
 2118 Tunnel0     10.0.0.11      set
HMAC_MD5+DES_56_CB      0      181
 2119 Tunnel0     10.0.0.11      set
HMAC_MD5+DES_56_CB    186        0
 2120 Tunnel1     10.0.1.11      set
HMAC_MD5+DES_56_CB      0      105
 2121 Tunnel1     10.0.1.11      set
HMAC_MD5+DES_56_CB    110        0
```

Spoke2路由器資訊

```
Spoke2#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.2.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 2 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C       10.0.1.0 is directly connected, Tunnel1
 D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
00:38:04, Tunnel1
                     [90/2841600] via 10.0.0.1,
00:38:04, Tunnel0
 D    192.168.1.0/24 [90/3097600] via 10.0.1.1,
00:38:02, Tunnel1
                     [90/3097600] via 10.0.0.1,
00:38:02, Tunnel0
 C    192.168.2.0/24 is directly connected, Ethernet1
 Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1d02h, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.1.1/32 via 10.0.1.1, Tunnel1 created 1d02h, never
expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.5
 Spoke2#show crypto engine connection active
   ID Interface   IP-Address    State  Algorithm
Encrypt  Decrypt
    8 Ethernet0   172.16.2.75    set
HMAC_SHA+DES_56_CB      0        0
    9 Ethernet0   172.16.2.75    set
HMAC_SHA+DES_56_CB      0        0
 2036 Tunnel0     10.0.0.12      set
HMAC_MD5+DES_56_CB      0      585
 2037 Tunnel0     10.0.0.12      set
HMAC_MD5+DES_56_CB    614        0
 2038 Tunnel1     10.0.1.12      set
HMAC_MD5+DES_56_CB      0      408
 2039 Tunnel1     10.0.1.12      set
HMAC_MD5+DES_56_CB    424        0
```

同樣，有關Hub1、Hub2、Spoke1和Spoke2上的路由表，您會注意到一些有趣的事情：

- 兩台中心路由器都有到達分支路由器後網路的等價路由。中心1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0
```

中心2:

```
D    192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0
```

這意味著Hub1和Hub2會將分支路由器後面的網路的相同開銷通告給中心路由器後面的網路中的路由器。例如，直接連線到192.168.0.0/24 LAN的路由器R2上的路由表如下所示：R2：

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
                            [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                          [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3
```

- 分支路由器具有通過兩個中心路由器到達中心路由器後面的網路的等價路由。輻射點1:

```
D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1
                            [90/3097600] via 10.0.0.1, 00:26:30, Tunnel0
```

分支2:

```
D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1
                            [90/3097600] via 10.0.0.1, 00:38:04, Tunnel0
```

如果分支路由器正在執行每個資料包的負載均衡，則可能會產生亂序資料包。

為了避免在通向兩個集線器的鏈路上執行非對稱路由或每資料包負載均衡，您需要配置路由協定以優先使用兩個方向的一條分支到集線器的路徑。如果您希望Hub1為主用而Hub2為備份，則可以將集線器通道介面的延遲設定為不同。

中心1:

```
interface tunnel0
...
delay 1000
...
```

中心2:

```
interface tunnel0
...
delay 1050
...
```

註：在本例中，由於集線器2上的隧道介面的延遲小於兩個集線器(100)之間Ethernet1介面上的延遲，因此該延遲增加了50。 這樣，Hub2仍會直接將資料包轉發到分支路由器，但會向Hub1和Hub2後面的路由器通告比Hub1更低的路由。如果延遲增加超過100，則Hub2將通過乙太網1介面通過Hub1轉發分支路由器的資料包，而Hub1和Hub2後面的路由器仍會正確選擇Hub-1將資料包傳送到分支路由器。

現在路由如下所示：

中心1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

中心2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2：

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

兩個中心路由器對於分支路由器後面的網路路由具有不同的開銷，因此在這種情況下，將優先使用Hub1將流量轉發到分支路由器，如R2上所示。這將解決上述第一個專案符號中描述的問題。

上述第二個專案符號中描述的問題仍然存在，但由於您有兩個p-pGRE隧道介面，因此您可以分別設定隧道介面上的**delay ...** ，以更改從Hub1獲知的路由與Hub2獲知的路由的EIGRP度量。

輻射點1:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

分支2:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

現在路由如下所示：

輻射點1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

分支2:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

上述路由配置將防止非對稱路由，同時允許在Hub1關閉時故障切換到中心2。這表示當兩個集線器都啟動時，只使用Hub1。

如果您希望通過平衡集線器間的輻條來使用兩個集線器，同時提供故障切換保護並且沒有非對稱路由，則路由配置會更加複雜，但使用EIGRP時可以這樣做。為此，請將中心路由器通道介面上的**延遲……設為**相等，然後在分支路由器上使用**offset-list <acl> out <offset> <interface>**命令，為從GRE通道介面通告到備用中心的路由增加EIGRP度量。分支上的**Tunnel0和**Tunnel1介面之間的不等延遲……仍被使用，因此分支路由器將優先使用其主要中心路由器。分支路由器上的更改如下。

Spoke1路由器

```
version 12.3
 !
 hostname Spoke1
 !
 ...
```

```
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Tunnel1
  bandwidth 1000
  ip address 10.0.1.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.1.1 172.17.0.5
  ip nhrp network-id 100001
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.1.1
  delay 1500
  tunnel source Ethernet0
  tunnel destination 172.17.0.5
  tunnel key 100001
  tunnel protection ipsec profile vpnprof
 !
 ...
 !
 router eigrp 1
  offset-list 1 out 12800 Tunnel1
  network 10.0.0.0 0.0.0.255
  network 10.0.1.0 0.0.0.255
  network 192.168.1.0
  distribute-list 1 out
  no auto-summary
 !
 access-list 1 permit 192.168.1.0
 !
```

Spoke2路由器

```
version 12.3
 !
 hostname Spoke2
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1500
  tunnel source Ethernet0
```

```
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
...
!
router eigrp 1
 offset-list 1 out 12800 Tunnel1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.2.0
 distribute-list 1 out
 no auto-summary
!
access-list 1 permit 192.168.2.0
!
```

注意：偏移值12800(50*256)已新增到EIGRP度量中，因為它小於25600(100*256)。 此值(25600)是新增到中心路由器之間獲知的路由的EIGRP度量中的值。通過在**offset-list**命令中使用12800，備用中心路由器將直接將資料包轉發到分支路由器，而不是通過乙太網轉發這些資料包來通過主中心路由器轉發這些分支。由中心路由器通告的路由上的度量仍將保持優先使用正確的主中心路由器。請記住，有一半輻條將Hub1作為主路由器，另一半將Hub2作為主路由器。

注意：如果偏移值增加了25600以上(100*256)，則集線器會通過Ethernet1介面通過另一集線器轉發半分支路由器的資料包，即使這些集線器後面的路由器仍希望使用正確的集線器將資料包傳送到分支路由器。

注意：還新增了distribute-list 1 out命令，因為可以通過分支上的一個隧道介面從一個中心路由器獲知的路由可以通過另一個隧道通告回另一個中心。**distribute-list ...**命令可確保分支路由器只能通告自己的路由。

注意：如果您更喜歡在中心路由器上而不是分支路由器上控制路由通告，則<value> <interface>中的**offset-list <acl1>和distribute-list <acl2>命令可以在中心路由器上而不是分支上配置。**<acl2>存取清單會列出所有輻條後面的路由，而<acl1>存取清單只會列出從另一個集線器路由器為主集線器的輻條後面的路由。

通過這些更改，路由如下所示：

中心1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

中心2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2：

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

輻射點1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

分支2:

```
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

結論

DMVPN解決方案提供以下功能，以便更好地擴展大型和小型IPsec VPN網路。

- DMVPN允許更好地在全網狀或部分網狀IPsec VPN中進行擴展。當分支到分支的流量是零星的流量時（例如，並非每個分支都不斷向其他每個分支傳送資料），它特別有用。 只要分支之間存在直接IP連線，它允許任何分支直接將資料傳送到任何其他分支。
- DMVPN支援具有動態分配地址（如電纜、ISDN和DSL）的IPsec節點。這適用於星型和網狀網路。DMVPN可能要求中心到分支鏈路持續啟動。
- DMVPN可簡化VPN節點的新增。新增新的分支路由器時，只需配置分支路由器並將其插入網路（不過，您可能需要為中心上的新分支新增ISAKMP授權資訊）。 中心節點將動態瞭解新的分支，動態路由協定將路由傳播到中心節點和所有其他分支。
- DMVPN可減小VPN中所有路由器所需的配置大小。GRE+IPsec僅集中星型VPN網路也是如此。
- DMVPN使用GRE，因此支援跨VPN的IP多點傳送和動態路由流量。這意味著可以使用動態路由協定，並且協定可以支援冗餘「集線器」。還支援組播應用。
- DMVPN支援分支處的拆分隧道。

相關資訊

- 動態多點VPN(DMVPN)
- IPSec支援頁面
- 技術支援 - Cisco Systems