使用VRF-Lite功能在DMVPN分支上配置ISP冗餘

目錄

簡介

本檔案介紹如何透過虛擬路由和轉送Lite(VRF-Lite)功能在動態多點VPN(DMVPN)分支上設定網際網路服務供應商(ISP)備援。

必要條件

需求

思科建議您在嘗試本檔案所述的設定之前，先瞭解以下主題：

- VRF基礎知識
- 增強型內部網關路由協定(EIGRP)基礎知識
- DMVPN基礎知識

採用元件

本檔案中的資訊是根據Cisco IOS®版本15.4(2)T。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

VRF技術包含在IP網路路由器中，可讓路由表的多個例項共存於路由器中，且同時工作。這增加了功能，因為它允許在不使用多個裝置的情況下分割網路路徑。

使用雙ISP實現冗餘已成為一種常見的做法。管理員使用兩條ISP鏈路；一個充當主連線，另一個充當備用連線。

使用雙ISP可在輻條上實施DMVPN冗餘的相同概念。本文檔旨在演示當輻條具有雙ISP時，如何使用*VRF-Lite*來分離路由表。動態路由用於為通過DMVPN通道的流量提供路徑備援。本文檔中介紹的配置示例使用以下配置方案：

介面	IP 位址	VRF	說明
Ethernet0/0	172.16.1.1	ISP1 VRF	主ISP
Ethernet0/1	172.16.2.1	ISP2 VRF	輔助ISP

藉助VRF-Lite功能，DMVPN分支可以支援多個VPN路由/轉發例項。VRF-Lite功能強制來自多個多點通用路由封裝(mGRE)隧道介面的流量使用各自的VRF路由表。例如，如果主ISP在ISP1 VRF中終止，輔助ISP在ISP2 VRF中終止，則ISP2 VRF中生成的流量使用*ISP2* VRF路由表，而*ISP1* VRF中生成的流量使用ISP1*VRF路由表。*

使用前門VRF(*fVRF)的優勢主要在於從全域性路由表（存在隧道介面的位置）中劃分出單獨的路由*表。 使用*內部*VRF(iVRF)的優勢是定義專用空間以儲存DMVPN和專用網路資訊。這兩種配置都能提供額外的安全性，防止路由資訊被分隔的Internet對路由器發起攻擊。

這些VRF配置可用於DMVPN中心和分支上。相較於兩個ISP都終止於全域性路由表中的情況，這具有很大的優勢。

如果兩個ISP都終止於全域性VRF，則它們共用同一個路由表，並且兩個mGRE介面都依賴於全域性路由資訊。在這種情況下，如果主ISP發生故障，則如果故障點位於ISP的主幹網路中而不是直接連線，主ISP介面可能不會關閉。這會導致兩個mGRE隧道介面仍使用指向主ISP的預設路由，導致DMVPN冗餘失敗。

雖然有些解決方案使用IP服務級別協定(IP SLA)或嵌入式事件管理器(EEM)指令碼來解決此問題，但不使用VRF-Lite，但它們可能並非始終是最佳選擇。

部署方法

本節簡要概述分割隧道和輻條到輻條隧道。

分割通道

當通過mGRE介面獲知特定子網或總結路由時，它稱為*分割隧道*。如果通過mGRE介面獲知預設路由，則稱為*tunnel-all*。

本文提供的組態範例是基於分割通道。

輻射對輻射隧道

本文提供的組態範例是適用於全通道部署方法的良好設計（預設路由是透過mGRE介面得知的）。

使用兩個fVRF可分離路由表，並確保將GRE後封裝的資料包轉發到各自的fVRF，這有助於確保分支到分支的隧道具有活動的ISP。

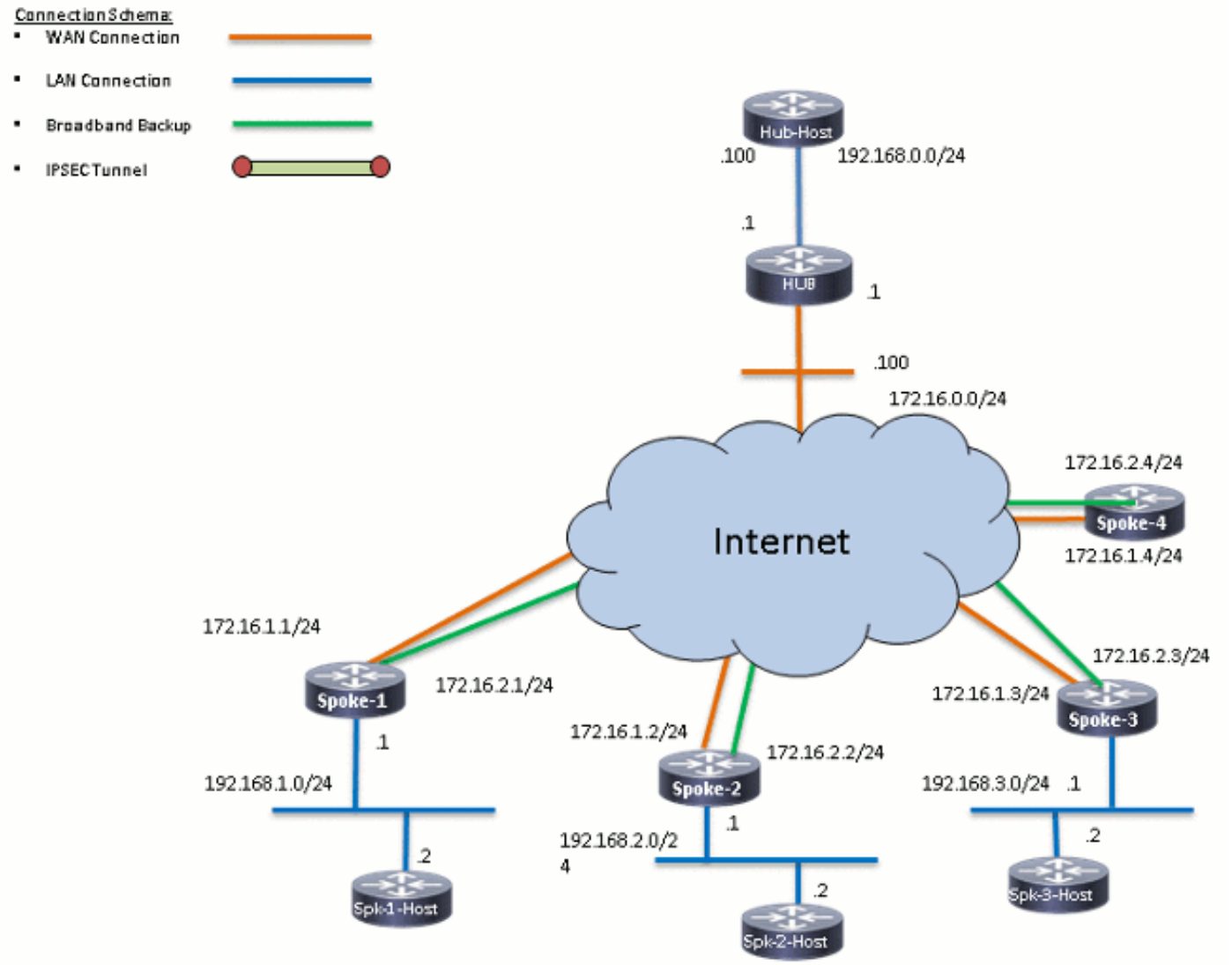
設定

本節介紹如何通過VRF-Lite功能在DMVPN分支上配置ISP冗餘。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表

以下拓撲用於本文檔中的示例：



集線器配置

以下是有關集線器上相關組態的一些說明：

- 在本配置示例中，為了將*Tunnel0*設定為主介面，*delay*引數已更改，這使得從*Tunnel0*獲知的路由變得更加優先。
- **shared**關鍵字與通道保護搭配使用，且所有mGRE介面上都會新增唯一的*通道金鑰*，因為它們使用相同的*通道源<interface>*。否則，在解密後，傳入的通用路由封裝(GRE)通道封包可能會被傳送到錯誤的通道介面。
- 執行路由總結以確保所有分支都通過mGRE通道(**tunnel-all**)獲知預設路由。

附註：本示例中僅包含配置的相關部分。

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HUB1
```

```
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback0
 description LAN
 ip address 192.168.0.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn shared
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile profile-dmvpn shared
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
!
end
```

分支配置

以下是有關輻射點上相關配置的一些說明：

- 對於分支冗餘，*Tunnel0*和*Tunnel1*分別將*Ethernet0/0*和*Ethernet0/1*作為隧道源介面。Ethernet0/0連線到主ISP，Ethernet0/1連線到輔助ISP。
- 為了隔離ISP，使用VRF功能。主ISP使用*ISP1* VRF。對於輔助ISP，配置了名為*ISP2*的VRF。
- *tunnel vrf ISP1*和*tunnel vrf ISP2*分別配置在介面Tunnel0和Tunnel1上，以指示在VRF ISP1或ISP2中執行後GRE封裝資料包的轉發查詢。
- 在本配置示例中，為了將Tunnel0設定為主介面，*delay*引數已更改，這使得從Tunnel0獲知的路由變得更加優先。

  附註：本示例中僅包含配置的相關部分。

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SPOKE1
!
vrf definition ISP1
 rd 1:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition ISP2
 rd 2:2
 !
 address-family ipv4
 exit-address-family
!
crypto keyring ISP2 vrf ISP2
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring ISP1 vrf ISP1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback10
 ip address 192.168.1.1 255.255.255.0
```

```
!
interface Tunnel0
 description Primary mGRE interface source as Primary ISP
 bandwidth 1000
 ip address 10.0.0.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel vrf ISP1
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel1
 description Secondary mGRE interface source as Secondary ISP
 bandwidth 1000
 ip address 10.0.1.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100001
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.1.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel vrf ISP2
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 description Primary ISP
 vrf forwarding ISP1
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/1
 description Seconday ISP
 vrf forwarding ISP2
 ip address 172.16.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route vrf ISP1 0.0.0.0 0.0.0.0 172.16.1.254
ip route vrf ISP2 0.0.0.0 0.0.0.0 172.16.2.254
!
logging dmvpn
!
end
```

驗證

使用本節所述的資訊來驗證您的組態是否正常運作。

主和輔助ISP處於活動狀態

在此驗證方案中，主ISP和輔助ISP均處於活動狀態。以下是關於此案例的一些其他說明：

- 兩個mGRE介面的第1階段和第2階段均已啟動。

- 兩個隧道都啟動，但首選通過Tunnel0（通過主ISP獲得）的路由。

以下是可用於驗證此案例中配置的相關**show**命令：

```
SPOKE1#show ip route
<snip>
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 1w0d, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
```

```
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

主ISP關閉/輔助ISP活動

在此案例中，當ISP1鏈路斷開時，通過Tunnel0的鄰居的EIGRP *Hold*計時器將過期，並且現在通向集線器和其它分支的路由指向Tunnel1（源自Ethernet0/1）。

以下是可用於驗證此案例中配置的相關**show**命令：

```
*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.1.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/3072000] via 10.0.1.1, 00:00:20, Tunnel1

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2
```

```
Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: DOWN
Peer: 172.16.0.1 port 500
 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

       Active SAs: 0, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: DOWN-NEGOTIATING
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive
```

主ISP鏈路恢復

當通過主ISP的連線恢復時，Tunnel0加密會話將變為活動狀態，並且首選通過Tunnel0介面獲知的路由。

以下是範例：

```
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.0.1 to network 0.0.0.0
```

```
D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 00:00:45, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

疑難排解

若要對配置進行故障排除，請啟用debug ip eigrp和logging dmvpn。

以下是範例：

```
################### Tunnel0 Failed and Tunnel1 routes installed ####################

*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired
*Sep  2 14:07:33.374: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:07:33.391: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:33.399: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:36.686: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is DOWN
*Sep  2 14:07:36.686: %DMVPN-5-NHRP_NHS_DOWN: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1 ) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is DOWN, Reason:
External(NHRP: no error)
```

```
################## Tunnel0 came up and routes via Tunnel0 installed #################

*Sep  2 14:15:55.120: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is UP
*Sep  2 14:15:56.109: %DMVPN-5-NHRP_NHS_UP: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is  UP
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/2944000) origin(10.0.0.1)
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel0
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
```

相關資訊

- 最常見的DMVPN故障排除解決方案
- Cisco MDS 9000系列故障排除指南，2.x版â‚âIPsecâ故障排除
- 技術支援與文件 - Cisco Systems