使用VRF-Lite功能在DMVPN分支上配置ISP冗余

目录

简介

本文档介绍如何通过虚拟路由和转发Lite(VRF-Lite)功能在动态多点VPN(DMVPN)辐条上配置互联网服务提供商(ISP)冗余。

先决条件

要求

思科建议您在尝试本文档中描述的配置之前先了解这些主题：

- VRF的基本知识
- 增强型内部网关路由协议(EIGRP)的基本知识
- DMVPN的基本知识

使用的组件

本文档中的信息基于Cisco IOS®版本15.4(2)T。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

VRF是IP网络路由器中包含的一种技术，允许路由表的多个实例在路由器中共存并同时工作。这增加了功能，因为它允许对网络路径进行分段，而无需使用多个设备。

使用双ISP实现冗余已成为一种常见做法。管理员使用两条ISP链路；一个用作主连接，另一个用作备用连接。

使用双ISP，可对分支上的DMVPN冗余实施相同的概念。本文档的目的是演示如*何使用VRF*-Lite来在分支具有双ISP时分离路由表。使用动态路由为通过DMVPN隧道的流量提供路径冗余。本文档中介绍的配置示例使用以下配置方案：

接口	IP Address	VRF	描述
以太网0/0	172.16.1.1	ISP1 VRF	主ISP
以太网0/1	172.16.2.1	ISP2 VRF	辅助ISP

借助VRF-Lite功能，DMVPN分支上可支持多个VPN路由/转发实例。VRF-Lite功能强制来自多个多点通用路由封装(mGRE)隧道接口的流量使用其各自的VRF路由表。例如，如果主ISP在ISP1 VRF中终止，而辅助ISP在ISP2 VRF中终止，则ISP2 VRF中生成的流量使用*ISP2* VRF路由表，而ISP1 VRF中生成的流量则使用ISP1的VRF路由表。

使用前门VRF(fVRF*)的优*势主要是从全局路由表（存在隧道接口）中创建单独的路由表。 使用内部VRF(iVRF)*的优*势在于定义专用空间以保存DMVPN和专用网络信息。这两种配置都提供了额外的安全性，可防止路由器受到来自Internet的攻击，在Internet中，路由信息是分开的。

这些VRF配置可在DMVPN中心和分支上使用。这相对于两个ISP在全局路由表中终止的情况具有极大优势。

如果两个ISP在全局VRF中终止，则它们共享相同的路由表，并且两个mGRE接口都依赖于全局路由信息。在这种情况下，如果主ISP发生故障，则如果故障点位于ISP的主干网络中且未直接连接，则主ISP接口可能不会关闭。这会导致两个mGRE隧道接口仍使用指向主ISP的默认路由，从而导致DMVPN冗余失败。

尽管有一些变通方法使用IP服务级别协议(IP SLA)或嵌入式事件管理器(EEM)脚本来解决此问题，但是它们可能并不总是最佳选择。

部署方法

本节简要概述拆分隧道和分支到分支隧道。

Split Tunneling

当通过mGRE接口获取特定子网或总结路由时，它称为*分割隧道*。如果默认路由是通过mGRE接口获取的，则称为*tunnel-all*。

本文档中提供的配置示例基于分割隧道。

分支到分支隧道

本文档中提供的配置示例是全隧道部署方法（默认路由通过mGRE接口获知）的良好设计。

使用两个fVRF可分隔路由表并确保将后GRE封装的数据包转发到相应的fVRF，这有助于确保分支到分支隧道启动活动ISP。

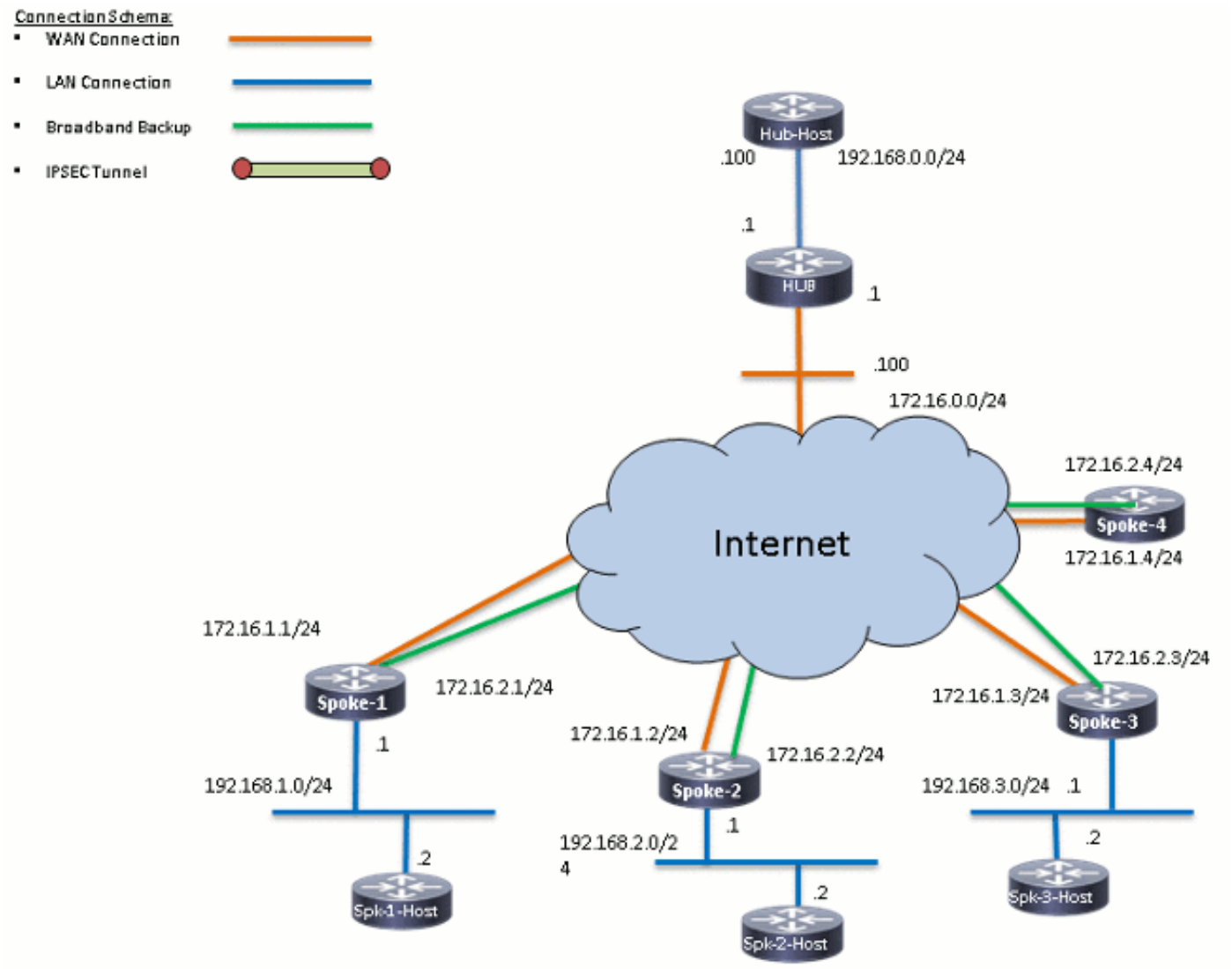
配置

本节介绍如何通过VRF-Lite功能在DMVPN分支上配置ISP冗余。

> **注意：**使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档中示例使用的拓扑如下：



中心配置

以下是有关集线器上相关配置的一些说明：

- 为了在此配置示*例中*将Tunnel0设置为主接口，更改了*delay*参数，使从Tunnel0获知的路由更*加*优先。
- 共享**关键**字用于隧道保护，并且所有mGRE接口上都添加了*唯*一隧道密钥，因为它们使用相同的隧道源*<interface>*。否则，入站通用路由封装(GRE)隧道数据包在解密后可能会被传送到不正确的隧道接口。
- 执行路由总结以确保所有辐射点通过mGRE隧道（全隧道）获**取默认路**由。

  注意：本示例中仅包含配置的相关部分。

```
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

以下是有关辐条上相关配置的一些说明：

- 对于分支冗余，*Tunnel0*和*Tunnel1*分别将*Ethernet0/0*和*Ethernet0/1*作为隧道源接口。以太网接口0/0连接到主ISP，以太网接口0/1连接到辅助ISP。
- 为了隔离ISP，使用VRF功能。主ISP使用*ISP1* VRF。对于辅助ISP，配置了名为*ISP2*的VRF。
- *隧道vrf ISP1*和*隧道vrf ISP2*分别配置在接口Tunnel0和Tunnel1上，以指示在VRF ISP1或ISP2中执行后GRE封装数据包的转发查找。
- 为了在此配置示例中将Tunnel0设置为主接口，更改了*delay*参数，使从Tunnel0获知的路由更为首选。

注意：本示例中仅包含配置的相关部分。

```
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
```

验证

使用本节中介绍的信息验证配置是否正常工作。

主要和辅助ISP处于活动状态

在此验证场景中，主ISP和辅助ISP都处于活动状态。以下是有关此场景的一些附加说明：

- 两个mGRE接口的第1阶段和第2阶段都处于启用状态。

- 两个隧道都会建立，但首选通过Tunnel0（通过主ISP发出）的路由。

以下是相关的**show**命令，您可以使用这些命令来验证您在此场景中的配置：

```
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关闭/辅助ISP活动

在此场景中，当ISP1链路断开时，EIGRP *Hold* 计时器将通过Tunnel0终止邻居关系，并且到集线器和其他分支的路由现在指向Tunnel1（源于Ethernet0/1）。

以下是相关的**show**命令，您可以使用这些命令来验证您在此场景中的配置：

```
*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链路恢复

当通过主ISP的连接恢复时，Tunnel0加密会话变为活动状态，并且首选通过Tunnel0接口获取的路由。

示例如下：

```
*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
```

故障排除

要排除配置故障，请启用**debug ip eigrp**和logging dmvpn。

示例如下：

```
################### 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
```

相关信息

- 最常见的 DMVPN 故障排除解决方案
- Cisco MDS 9000系列故障排除指南，版本2.x - Â Troubleshooting IPsec
- 技术支持和文档 - Cisco Systems