在同一设备上从DMVPN硬迁移到FlexVPN

目录

简介

本文档提供有关如何从现有DMVPN网络迁移到相同设备上的FlexVPN的信息。

两个框架的配置在设备上共存。

在本文档中，仅显示最常见的场景：DMVPN使用预共享密钥进行身份验证，EIGRP作为路由协议。

本文档演示了向BGP（推荐的路由协议）和不太理想的EIGRP的迁移。

先决条件

要求

本文档假设读者了解DMVPN和FlexVPN的基本概念。

使用的组件

请注意，并非所有软件和硬件都支持IKEv2。有关信息，请参阅Cisco功能导航器。理想情况下，要使用的软件版本为：

- ISR - 15.2(4)M1或更高版本
- ASR1k - 3.6.2版本15.2(2)S2或更高版本

较新平台和软件的优势之一是，可能使用下一代加密技术，例如AES GCM在IPsec中加密。RFC 4106中对此进行了讨论。

AES GCM允许在某些硬件上实现更快的加密速度。

要查看思科有关使用和迁移到下一代加密的建议，请参阅：

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

迁移步骤

目前，建议从DMVPN迁移到FlexVPN的方法是使两个框架不能同时运行。

此限制将因ASR 3.10版本中将引入的新迁移功能而取消，这些功能在思科方面的多个增强请求(包括CSCuc08066)下进行跟踪。这些功能应于2013年6月下旬推出。

在相同设备上同时存在和运行两个框架的迁移称为软迁移，它表示从一个框架到另一个框架的影响最小且故障切换平稳。

两个框架的配置共存但不同时运行的迁移称为硬迁移。这表示从一个框架切换到另一个框架意味着VPN上的通信缺乏，即使通信最少。

在相同设备上硬迁移

本文档讨论从现有DMVPN网络迁移到相同设备上的新FlexVPN网络。

此迁移要求两个框架不能同时在设备上运行，这实质上要求在启用FlexVPN之前在全局禁用DMVPN功能。

在新迁移功能可用之前，使用相同设备执行迁移的方法是：

1. 检验DMVPN上的连接。
2. 在适当位置添加FlexVPN配置并关闭属于新配置的隧道和虚拟模板接口。
3. （在维护窗口期间）关闭所有分支和集线器上的所有DMVPN隧道接口，然后再转到步骤4。
4. 取消关闭FlexVPN隧道接口。
5. 检验辐射点到中心点的连接。
6. 检验辐射到辐射的连通性。
7. *如果第5点或第6点中的验证未通过关闭FlexVPN接口和取消关闭DMVPN接口正确恢复到DMVPN。*
8. *检验辐条与中心通信。*
9. *验证辐条与辐条的通信。*

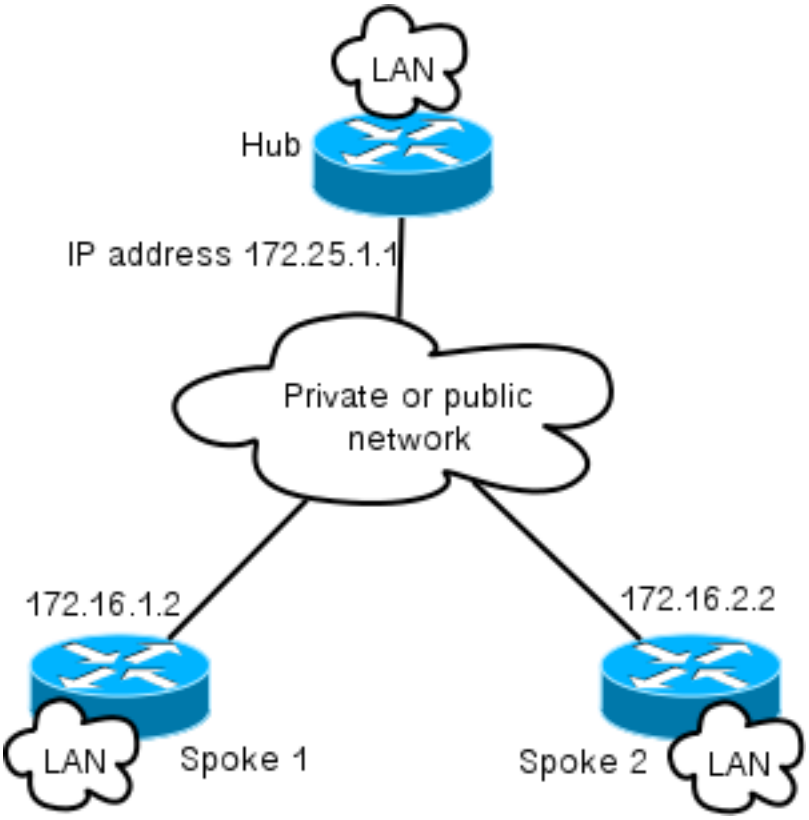
自定义方法

如果由于网络或路由的复杂性，此方法可能不是您的最佳选择，请在迁移前与思科代表展开讨论。讨论自定义迁移流程的最佳人选是系统工程师或高级服务工程师。

网络拓扑

传输网络拓扑

此图显示了Internet上主机的典型连接拓扑。在本文档中，集线器的IP地址loopback0(172.25.1.1)用于终止IPsec会话。

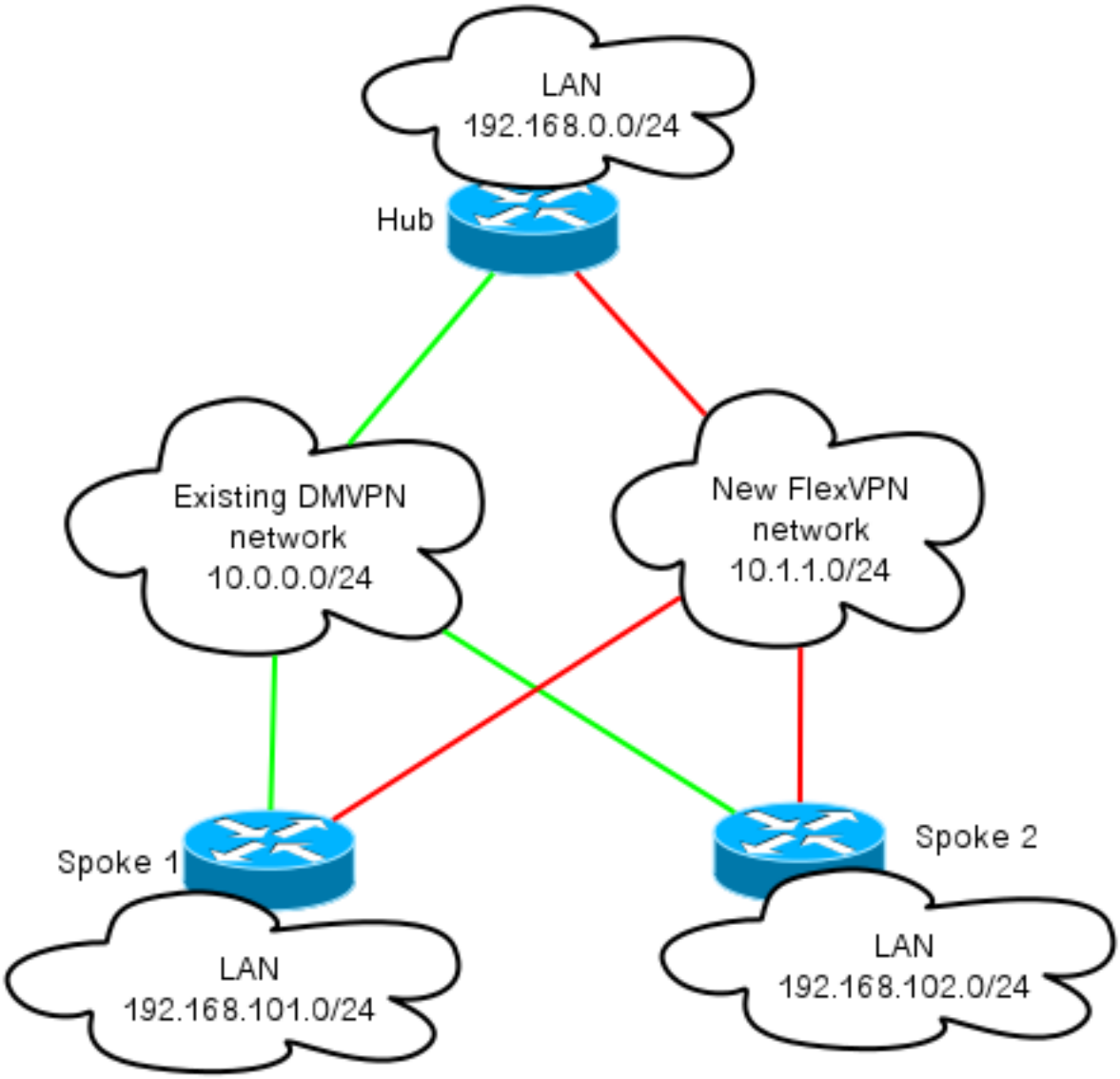


重叠网络拓扑

此拓扑图显示了用于重叠的两个独立云：DMVPN（绿色连接）和FlexVPN连接。

显示相应端的局域网前缀。

10.1.1.0/24子网在接口编址方面并不代表实际的子网，而是专用于FlexVPN云的IP空间块。其背后的原理将在FlexVPN配置一节中讨论。



配置

DMVPN 配置

本节包含DMVPN中心和分支的基本配置。

预共享密钥(PSK)用于IKEv1身份验证。

建立IPsec后，NHRP注册会从分支到中心执行，以便中心可以学习动态分支的NBMA编址。

当NHRP在分支和中心上执行注册时，路由邻接可以建立并交换路由。在本例中，EIGRP用作重叠网络的基本路由协议。

分支DMVPN配置

这是DMVPN的基本示例配置，它使用预共享密钥身份验证和EIGRP作为路由协议。

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto isakmp keepalive 30 5
crypto isakmp profile DMVPN_IKEv1
  keyring DMVPN_IKEv1
  match identity address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
  mode transport
crypto ipsec profile DMVPN_IKEv1
  set transform-set IKEv1
  set isakmp-profile DMVPN_IKEv1
interface Tunnel0
ip address 10.0.0.101 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 10.0.0.1 172.25.1.1
 ip nhrp map multicast 172.25.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp nhs 10.0.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.102.0
 passive-interface default
 no passive-interface Tunnel0
```

集线器DMVPN配置

在集线器配置中，隧道源自IP地址为172.25.1.1的loopback0。

其余是使用EIGRP作为路由协议的DMVPN中心的标准部署。

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
 mode transport
crypto ipsec profile DMVPN_IKEv1
 set transform-set IKEv1
 interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp server-only
```

```
 ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
 ip tcp adjust-mss 1360
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel0
```

FlexVPN配置

FlexVPN基于以下相同的基本技术：

- IPSEC:与DMVPN中的默认值不同，IKEv2用于协商IPsec SA，而不是IKEv1。IKEv2提供了IKEv1的改进，从恢复能力开始，以建立受保护数据通道所需的消息数结束。
- GRE:与DMVPN不同，静态和动态点对点接口使用，不仅在静态多点GRE接口上使用。此配置可增加灵活性，尤其是针对每分支/每中心行为。
- NHRP:在FlexVPN中，NHRP主要用于建立分支到分支通信。辐条不注册到集线器。
- 路由：由于辐条不向集线器执行NHRP注册，因此您需要依靠其他机制来确保集线器和辐条能够双向通信。与DMVPN类似，动态路由协议也可以使用。但是，FlexVPN允许您使用IPsec来引入路由信息。默认为隧道另一端的IP地址引入/32路由，这将允许分支到中心直接通信。

在从DMVPN硬迁移到FlexVPN时，两个框架在同一设备上不能同时工作。但是，建议将它们分开。

将它们分为多个级别：

- NHRP — 使用不同的NHRP网络ID（推荐）。
- 路由 — 使用单独的路由进程（推荐）。
- VRF - VRF分离可增加灵活性，但此处不讨论（可选）。

分支FlexVPN配置

与DMVPN相比，FlexVPN中分支配置的一个区别是您可能有两个接口。

有必要的隧道用于分支到中心通信，有可选隧道用于分支到分支隧道。如果选择不使用动态分支到分支隧道，而是希望所有内容都通过中心设备，则可以删除虚拟模板接口并从隧道接口删除NHRP快捷方式交换。

您还会注意到，静态隧道接口根据协商接收了IP地址。这样，集线器就可以动态地提供隧道接口IP到分支，而无需在FlexVPN云中创建静态编址。

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

思科建议在支持AES GCM的硬件中使用AES GCM。

```
crypto ipsec transform-set IKEv2 esp-gcm
    mode transport
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Tunnel1
 ip address negotiated
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 shutdown
 tunnel source Ethernet0/0
 tunnel destination 172.25.1.1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

PKI是在IKEv2中执行大规模身份验证的推荐方法。

但是，只要您知道预共享密钥的局限性，您仍然可以使用预共享密钥。

以下是使用“cisco”作为PSK的配置示例：

```
crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
```

FlexVPN集线器配置

通常，中心仅会终止动态分支到中心隧道。这就是为什么在集线器配置中，您找不到FlexVPN的静态隧道接口，而使用虚拟模板接口的原因。这将为每个连接生成虚拟访问接口。

请注意，在中心端，您需要指出要分配给辐条的池地址。

此地址池的地址稍后将作为每个分支的/32路由添加到路由表中。

```
aaa new-model
aaa authorization network default local
```

```
aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

思科建议在支持AES GCM的硬件中使用AES GCM。

```
crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

请注意，在AES GCM操作下的配置中，已注释掉。

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
interface Loopback100
 ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip nhrp network-id 2
 ip nhrp redirect
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

在IKEv2中进行身份验证时，在集线器上和在辐条上应用相同的原则。

为了实现可扩展性和灵活性，请使用证书。但是，您可以重新使用与分支上相同的PSK配置。

注意：IKEv2在身份验证方面提供灵活性。一端可以使用PSK进行身份验证，而另一端使用RSA-SIG。

流量迁移

作为重叠路由协议迁移到BGP [推荐]

BGP是基于单播交换的路由协议。由于它的特点，它已成为DMVPN网络中最佳的扩展协议。

在本例中，使用iBGP。

分支BGP配置

分支迁移包括两部分。启用BGP作为动态路由。

```
router bgp 65001
 bgp log-neighbor-changes
 network 192.168.101.0
 neighbor 10.1.1.1 remote-as 65001
```

在BGP邻居启动（请参阅此迁移部分中的集线器BGP配置）并获知BGP上的新前缀后，您可以将流量从现有DMVPN云转移到新的FlexVPN云。

集线器BGP配置

在集线器上，为避免单独为每个分支保持邻居关系配置，将配置动态侦听程序。

在此设置中，BGP不会启动新连接，但会接受来自所提供IP地址池的连接。在本例中，所述池为10.1.1.0/24，即新FlexVPN云中的所有地址。

```
router bgp 65001
 network 192.168.0.0
 bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
 neighbor Spokes peer-group
 neighbor Spokes remote-as 65001
```

将流量迁移到FlexVPN

如前所述，迁移需要通过关闭DMVPN功能和启用FlexVPN来完成。

此程序可保证最小影响。

1. 所有辐条：
   ```
   interface tunnel 0
      shut
   ```
2. 在集线器上：
   ```
   interface tunnel 0
     shut
   ```
   此时，请确保没有从分支建立到此集线器的IKEv1会话。这可以通过检查show crypto isakmp sa命令的输出和监控**加密日志记录会**话生成的系统日志消息来验证。确认后，您可以继续启动FlexVPN。
3. 在集线器上继续：
   ```
   interface Virtual-template 1
    no shut
   ```
4. 辐条：
   ```
   interface tunnel 1
      no shut
   ```

验证步骤

IPsec稳定性

评估IPsec稳定性的最佳方法是通过启用以下配置命令监控系统日志：

```
crypto logging session
```

如果您看到会话处于上下运行状态，这可能表示IKEv2/FlexVPN级别上的问题，在迁移开始之前需

要纠正。

填充BGP信息

如果IPsec稳定，请确保BGP表中填充了来自辐条（在集线器上）的条目和来自集线器（在辐条上）的摘要。

对于BGP，可通过执行以下操作来查看：

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

集线器中正确信息的示例：

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1
*10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

您可以看到，集线器已获知来自每个辐条和两个辐条的1个前缀是动态的(标有星号(*))。

来自辐条的类似信息示例：

```
Spoke1#show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 11 11 6 0 0 00:03:43 1
```

辐条已从集线器收到一个前缀。在此设置中，此前缀应是在集线器上通告的摘要。

使用EIGRP迁移到新隧道

EIGRP是DMVPN网络中的常用选择，因为它部署相对简单且收敛快。

但是，它的扩展性会比BGP更差，并且不提供许多可由BGP直接开箱使用的高级机制。

下一节介绍使用新EIGRP进程迁移到FlexVPN的方法之一。

更新的分支配置

在本例中，新AS添加了单独的EIGRP进程。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
```

```
 passive-interface default
 no passive-interface Tunnel1
```
注意：您应避免在分支到分支隧道上建立路由协议邻接关系，因此仅使tunnel1（分支到中心）的接口不是被动接口。

更新的集线器配置

同样，在集线器上，DMVPN应仍是交换流量的首选方式。但是，FlexVPN应该已经通告和学习相同的前缀。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```
有两种方法可向辐条提供总结。

- 重分发指向null0（首选选项）的静态路由。
  ```
  ip route 192.168.0.0 255.255.0.0 null 0
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
   distribute-list EIGRP_SUMMARY out Virtual-Template1
   redistribute static metric 1500 10 10 1 1500
  ```
  此选项允许控制摘要和重分发，而不接触集线器的VT配置。
- 或者，您可以在虚拟模板上设置DMVPN样式的摘要地址。不建议使用此配置，因为内部处理和将此摘要复制到每个虚拟访问。此处显示供参考：
  ```
  interface Virtual-Template1 type tunnel
   ip summary-address eigrp 200 172.16.1.0 255.255.255.0
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   delay 2000
  ```

将流量迁移到FlexVPN

迁移需要通过关闭DMVPN功能和启用FlexVPN来完成。

以下程序保证最小影响。

1. 所有辐条：
   ```
   interface tunnel 0
      shut
   ```
2. 在集线器上：
   ```
   interface tunnel 0
     shut
   ```
   此时，请确保没有从分支建立到此集线器的IKEv1会话。这可以通过检查show crypto isakmp sa命令的输出并监**控加密日志记录**会话生成的系统日志消息来验证。确认后，您可以继续启动FlexVPN。
3. 在集线器上继续：
   ```
   interface Virtual-template 1
    no shut
   ```
4. 所有辐条：
   ```
   interface tunnel 1
      no shut
   ```

验证步骤

IPsec稳定性

与BGP一样，您需要评估IPsec是否稳定。实现此目的的最佳方法是启用以下配置命令监控系统日志：

```
crypto logging session
```

如果您看到会话处于上下运行状态，这可能表示IKEv2/FlexVPN级别上的问题，在迁移开始之前需要纠正。

拓扑表中的EIGRP信息

确保EIGRP拓扑表在集线器上填充有分支LAN条目，在分支上填充有摘要。这可以通过在中心辐射点上发出此命令来验证。

```
show ip eigrp topology
```

辐条的正确输出示例：

```
Spoke1#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted as output related to DMVPN cloud ...)
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
 via Rstatic (26112000/0)


P 192.168.101.0/24, 1 successors, FD is 281600 via Connected, Ethernet1/0 P 192.168.0.0/16, 1
successors, FD is 26114560
 via 10.1.1.1 (26114560/1709056), Tunnel1


P 10.1.1.107/32, 1 successors, FD is 26112000
 via Connected, Tunnel1
```

您会注意到，辐条知道其LAN子网（斜体）和其摘要(粗体)。

集线器正确输出的示例。

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
 via Connected, Loopback100
```

```
P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 10.1.1.107/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 10.1.1.106/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 0.0.0.0/0, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

您会注意到，集线器通过协商了解分支的LAN子网（斜体）、它通告的汇总前缀(**粗体**)以及每个分支的分配IP地址。

其他注意事项

现有分支到分支隧道

由于关闭DMVPN隧道接口会导致NHRP条目被删除，因此现有的分支到分支隧道将被拆除。

清除NHRP条目

如前所述，FlexVPN中心不会依赖来自分支的NHRP注册流程来了解如何将流量路由回来。但是，动态分支到分支隧道依赖于NHRP条目。

在DMVPN中，清除集线器上的NHRP可能导致短期连接问题。

在FlexVPN中，在分支上清除NHRP将导致与分支到分支隧道相关的FlexVPN IPsec会话断开。清除NHRP时，集线器不会对FlexVPN会话产生影响。

这是由于FlexVPN默认情况下：

- 辐条不注册到集线器。
- 集线器仅作为NHRP重定向器工作，不安装NHRP条目。
- NHRP快捷方式条目安装在分支到分支隧道的分支上，并且是动态的。

已知问题说明

分支到分支的流量可能受CSCub07382影响。

相关信息

- 技术支持和文档 - Cisco Systems