动态多点IPSec VPN (使用扩展多点的GRE/NHRP IPsec VPN)

Contents

Introduction

本文档讨论了动态多点 IPsec VPN (DMVPN) 以及公司为何需要设计或迁移其网络以便在 Cisco IOS® 软件中使用此新的 IPsec VPN 解决方案。

背景信息

或许公司可能需要也互联许多站点到一个主要站点，和彼此，在互联网间，当加密数据流保护它时。例如，需要连接到库存和预定的公司总部的一套零售店在公司内可能也需要连接到其他存储检查产品供货信息。以前，建立联系的唯一方法是使用一第2层网络例如ISDN或帧中继互联一切。设置和支付内部IP数据流的这些硬联线链路可以是费时和昂贵的。如果所有站点(包括主要站点)已经有相对便宜的互联网访问，则此互联网访问可能也用于存储和总部之间的内部IP通信通过使用IPSec隧道保证保密性和数据完整性。

为了公司能建立互联他们的在互联网间的大IPsec网络站点，您需要能扩展IPsec网络。IPsec加密两个终端(对等体)之间的数据流，并且加密由两个终端完成使用一个共有的“秘密”。因为此秘密仅共享在这两个终端之间，被加密的网络固有地是点到点链路的一集。因此， IPsec内在地是一个点到点隧道网络。扩展一个大点到点网络的可行方法将组织它为一个星型网或充分的(部分)网状网络。在多数网络中， IP数据流的多数是在spoke和集线器之间，并且很少是在spoke之间，因此星型设计经常是最佳的选择。因为是高费用支付整个场地之间的链路这些网络的，此设计与更旧的帧中继网络也配比。

当使用互联网作为在星型网之间时的互连， spoke彼此也有直接访问没有增加成本，但是非常困难的，如果不不可能，建立并且/或者管理一个充分的(部分)网状网络。充分或部分网状网络经常是理想的，因为可以有成本节省，如果spoke-to-spoke数据流可以通过集线器通过直接地去相当然后。横断集线器用途集线器资源的spoke-to-spoke数据流，并且能导致额外延迟，特别是当使用IPSec加密时，因为集线器将需要解码自发送的spoke的流入信息包然后再加密数据流发送它到接受分支。直接spoke-to-spoke数据流是有用的另一个示例是两个spoke在同一个城市和集线器的实际情形全国各地。

当IPsec集中星型网络在大小上配置了并且增长，安排他们一样动态地路由IP信息包尽可能变得更加理想。在更旧的帧中继集中星型网络中这通过运行一个动态路由协议完成类似OSPF或EIGRP在帧中继链路。这为动态通知分支网络的可到达性是有用的并且支持在IP路由网络的冗余。如果网络丢失集线路由器，备用集线器路由器可能自动地接管保留网络连通性到分支网络。

有IPSec隧道和动态路由协议的一个基本问题。动态路由协议取决于使用IP组播或广播包，但是IPsec不支持加密的组播或广播包。解决此问题的当前方法将使用通用路由封装(GRE)隧道与IPSec加密的组合。

GRE封装隧道支持传输IP组播和广播包对GRE封装隧道的另一个末端。GRE隧道信息包是IP单播信息包，使用IPsec，因此GRE信息包可以被加密。在此方案中， GRE完成隧道工作，并且IPsec执行支持VPN网络的加密零件。当配置GRE封装隧道，隧道(**隧道源...**，**隧道目的地的**终端的IP地址**...**)必须由另一个终端知道，并且一定是可路由的在互联网。这意味着集线器和所有此网络的分支路由器必须有静态non-private IP地址。

对于与互联网的小的站点连接，它是典型的为了spoke的外部IP地址能更改，每次连接到互联网，因为他们的互联网服务提供商(ISP)动态地提供外部接口地址(通过动态主机配置协议(DHCP))每次分支在线路来(非对称数字用户线(ADSL)和电缆设施)。因为不是所有的用户同时，联机“外部地址的”此动态分配的路由器允许ISP过度预定使用他们的网际地址空间。可以是显著地更加消耗大的支付供应商分配分支路由器的一个静态地址。运行在IPSec VPN的一个动态路由协议要求使用GRE封装隧道，但是您丢失选项有spoke用在他们的外部物理接口的动态地分配的IP地址。

上述限制和一些其他在以下四个点中被总结：

- IPsec使用访问控制表(ACL)定义什么数据将被加密。因此，每次新的(子)网络在分支或集线器后被添加，用户必须更改在两星型网路由器的ACL。如果SP管理路由器，则用户必须通知SP为了获得IPsec ACL更改，以便新数据流将被加密。
- 使用大集中星型网络，配置的大小在集线路由器的能变得非常大，在某种程度上是不可用的。例如集线路由器将需要配置3900条线路支持300分支路由器。这足够大显示配置和查找与一个

当前问题是相关的调试配置的部分是难的。并且此大小配置在闪存可能太大以至于不能适合NVRAM，并且需要存储。

- GRE+IPsec必须认识终端对等体地址。spoke的IP地址被连接直接地到互联网通过他们自己的ISP，并且他们经常设置，以便他们的外部接口地址不是固定的。IP地址能更改，每次站点来联机(通过DHCP)。
- 如果spoke需要彼此直接地谈在IPSec VPN，则集中星型网络必须成为全网状连接。因为已经不知道哪些spoke将需要直接地彼此谈，需要全网状连接，即使每分支可能不需要直接地与其他分支谈。并且，不是可行的配置在一小的分支路由器的IPsec，以便它有直接连接用其他分支路由器在网络;因而分支路由器可能需要是强大的路由器。

DMVPN解决方案

DMVPN解决方案以IPsec和一些新的增进使用多点GRE (mGRE)和下一跳解析协议(NHRP)，以可升级的方式解决上述问题。

IPsec加密自动发起

使用DMVPN解决方案，当不，没有发起IPSec加密隧道，直到有要求使用此IPSec隧道的数据流量。它可能用完成IPSec隧道的开始的1到10秒在此时间，并且数据流量降低。当使用GRE以IPsec时，GRE隧道配置已经包括GRE隧道对等体(**隧道目的地…**)地址，也是IPSec对等体地址。预先配置这两个地址。

如果使用隧道终端发现(TED)和动态加密映射在集线路由器，则您能避免必须预先配置IPSec对等体地址在集线器，但是需要发送TED探测和答复和被收到，在ISAKMP协商能开始前。这不应该是必要的，因为，当曾经GRE时，对等体源地址和目的地址已经知道。他们在配置或解决与NHRP (多点GRE封装隧道)。

用DMVPN解决方案， IPsec为点到点和多点GRE封装隧道立即被触发。并且，因为这些从GRE隧道源及目的地源点地址，将自动地派生配置所有加密ACL是不必要的。以下命令用于定义IPSec加密参数。注意没有**集对等体…**或**匹配地址…** required命令，因为此信息直接地从相关的GRE封装隧道或NHRP映射派生。

```
crypto ipsec profile <profile-name>
 set transform-set <transform-name>
```

以下命令关联与IPSec配置文件的一个隧道接口。

```
interface tunnel<number>
 ...
 tunnel protection ipsec profile <profile-name>
```

“spoke-to-hub”链路的动态隧道创建

GRE或IPSec信息关于分支在集线路由器没有被配置在DMVPN网络。分支路由器的GRE封装隧道配置有(通过NHRP命令)关于集线路由器的信息。当分支路由器启动时，它如上所述自动地发起IPSec隧道用集线路由器。它然后使用NHRP通知其当前物理接口IP地址集线路由器。这由于三个原因是有用的：

- 如果分支路由器安排其物理接口IP地址动态地分配(例如与ADSL或CableModem)，则集线路由器不可能配置有此信息，因为，每次分支路由器重新载入将获得一个新的物理接口IP地址。
- 因为不需要有任何GRE或IPSec信息关于对等体路由器，集线路由器的配置缩短并且被简单化。所有此信息通过NHRP动态地了解。
- 当您添加一新的分支路由器到DMVPN网络时，您不需要更改配置在集线器或在任何当前分支路由器。新的分支路由器配置有集线器信息，并且，当开始时，动态地向集线路由器登记。动态路由协议传播此的路由信息与集线器讲了话。集线器传播此新路由信息对其他spoke。它也传播从其他spoke的路由信息到此分支。

"spoke-to-spoke"数据流的动态隧道创建

如陈述前，当前在网状网络，所有点到点IPsec (或IPsec+GRE)隧道在所有路由器必须配置，即使其中一些/大多隧道不运行或一直需要。用DMVPN解决方案，一个路由器是集线器，并且所有其他路由器(spoke)配置有对集线器的隧道。spoke-to-hub隧道不断地是UP，并且spoke不需要直接隧道的配置对任何其他spoke。反而，当分支要传达信息包给另一分支(例如在另一分支后的子网)时，它使用NHRP动态地确定目标令牌的所要求的目的地目标地址。集线路由器作为NHRP服务器并且处理此要求来源分支。两个spoke (通过单个mGRE接口)动态地然后创建在他们之间的一个IPSec隧道，并且可以直接地传递数据。此动态spoke-to-spoke隧道在a (可配置)休止时期之后将自动地被切断。

支持的动态路由协议

DMVPN解决方案根据支持隧道组播/广播IP信息包的GRE封装隧道，因此DMVPN解决方案也支持运行在IPsec+mGRE隧道的动态路由协议。以前， NHRP要求您明确配置广播/组播映射隧道目的地IP地址的能支持组播和广播IP信息包GRE封装隧道。例如，在集线器您会需要每分支的**ip nhrp map multicast <spoke-n-addr>**配置行。用DMVPN解决方案，分支地址事先不知道，因此此配置不是可能的。反而，可以配置NHRP自动地添加每与在集线器的组播目的地列表讲了话与**ip nhrp map multicast dynamic命令**。用此命令，当分支路由器注册他们的单播NHRP映射用NHRP服务器(集线器)， NHRP也将创建广播/组播映射此分支的。这排除需要对于分支地址事先知道。

mGRE的Cisco快速转发快速的交换

目前，在mGRE接口的数据流进程交换，造成低性能。DMVPN解决方案添加mGRE数据流的Cisco快速转发交换，造成好性能。没有必要的配置命令打开此功能。如果Cisco快速转发交换在GRE隧道接口和流出/流入物理接口允许，则多点GRE通道信息包Cisco快速转发交换的。

使用在IPsec保护的VPN的动态路由

此部分描述当前(pre-DMVPN解决方案)事态。IPsec在定义了在路由器的外部接口然后一个**加密映射<map-name>**命令实施的加密的Cisco路由器实现通过一组命令。因此请设计，并且事实当前没有一个标准为使用IPsec加密IP组播/广播包， IP路由协议信息包不可能"通过IPSec隧道转发"，并且不可能动态地传播任何路由更改对IPSec隧道的另一边。

Note: 除了BGP使用广播或组播IP信息包的所有动态路由协议。GRE封装隧道用于与IPsec的组合解决此问题。

通过使用一个虚拟隧道接口(**接口tunnel<->**)， GRE封装隧道在Cisco路由器实现。GRE隧道协议设计处理IP组播/广播包，因此一个动态路由协议可以"运行" GRE封装隧道。GRE隧道信息包是封装原始IP组播/单播信息包的IP单播信息包。您能然后使用IPsec加密GRE隧道信息包。您能也运行在传输模式的IPsec和保存20个字节，因为GRE已经封装原始信息包，因此您不需要IPsec封装在另一个

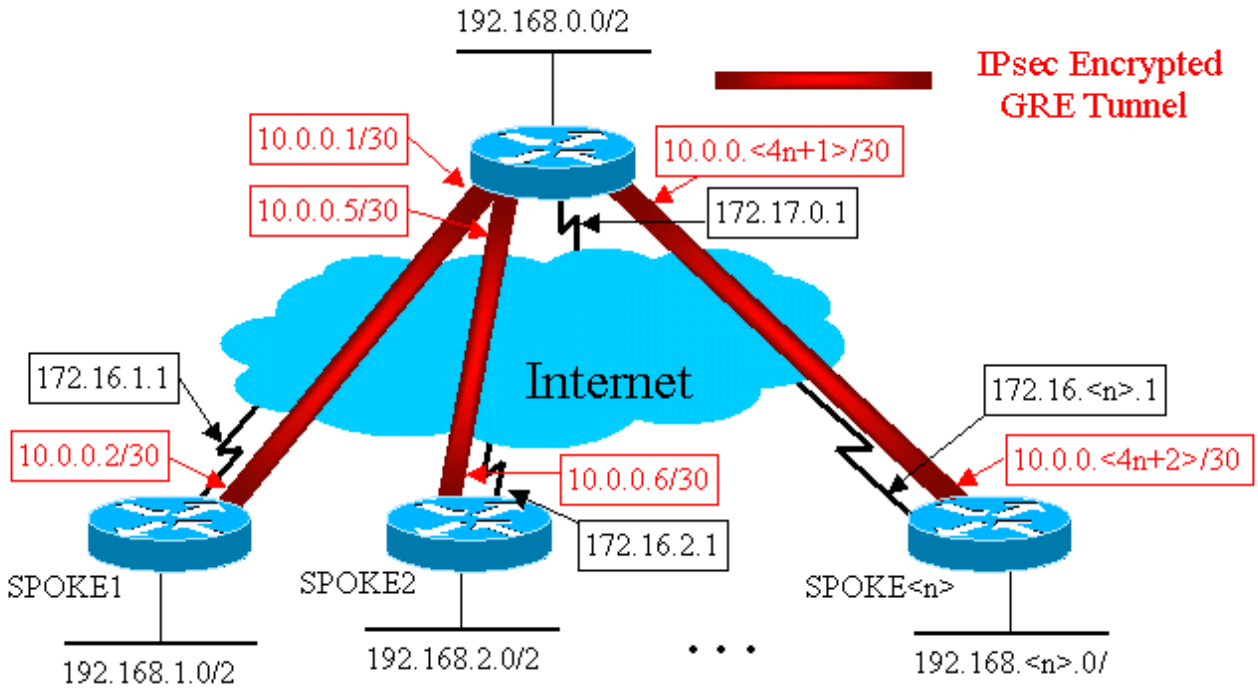
IP头的GRE IP信息包。

当运行在传输模式的IPsec，有将被加密的信息包IP源地址和目的地址必须匹配IPSec对等体地址的限制(路由器)。在这种情况下，这意味着GRE隧道终点和IPSec对等体地址必须是相同的。因为同一路由器是IPsec和GRE隧道终点，这不是问题。通过结合GRE封装隧道与IPSec加密，您能使用动态IP路由协议更新在加密的隧道的两端的路由表。通过加密的隧道是获知的网络的IP路由条目将有隧道(GRE隧道接口IP地址)的另一个末端作为IP下一跳。因此，如果在隧道的每一边网络更改，另一边将动态地然后得知更改和连接将继续，不用任何配置更改在路由器。

基本配置

下列是标准点到点IPsec+GRE配置。在这那里是一系列的配置示例哪里特定DMVPN解决方案的功能后被添加在步骤显示DMVPN的不同的功能。在显示如何的前面的示例的每个示例修造使用DMVPN解决方案在逐渐复杂化的网络设计。示例此连续可以使用作为模板移植当前IPsec+GRE VPN到DMVPN。如果该特定配置示例匹配您的网络设计要求，您能终止"迁移"在任意时候。

IPsec+GRE星型网(n = 1,2,3，...)



集线路由器

```
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.<n>.1
 set transform-set trans2
 match address <n+100>
!
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<n>
 bandwidth 1000
 ip address 10.0.0.<4n-3> 255.255.255.252
 ip mtu 1400
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.16.<n>.1
!
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 <n+100> permit gre host 172.17.0.1 host
172.16.<n>.1
```

分支1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
```

分支2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
```

Spoke<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.<n>.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
```

在上述配置中， ACL用于定义什么数据流将被加密。在两星型网路由器上，此ACL只需要匹配GRE隧道IP信息包。无论在任一个末端的网络更改， GRE IP隧道信息包不会更改，因此此ACL请勿需要更改。

Note: 当在12.2(13)T之前的使用Cisco IOS软件版本，您必须实施**crypto map vpnmap1 configuration命令**于GRE隧道接口(Tunnel<x>)和物理接口(Ethernet0)。使用Cisco IOS版本12.2(13)T和以后，您只实施**crypto map vpnmap1 configuration命令**于物理接口(Ethernet0)。

路由表的示例在星型网路由器的

在集线路由器的路由表

```
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.<n>.0 0.0.0.255
  no auto-summary
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
```

在分支1路由器的路由表

```
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.<n>.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
```

在Spoke<n>路由器的路由表

```
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.<n>.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
```

这是一个工作配置和使用，因为一个起始点比较与复杂配置可能使用DMVPN解决方案。第一更改将减少配置的大小在集线路由器的。这对很小数量的分支路由器不是重要的，但是变得重要，当有超过50到100分支路由器时。

减少集线器路由器配置大小

在以下示例中，配置在集线路由器最低限度地更改从多个GRE点到点隧道接口到单个GRE多点隧道接口。这是第一步到DMVPN解决方案。

有配置行一个唯一块在定义每分支路由器的加密映射特性的集线路由器的。配置的此部分定义了加密ACL和GRE隧道接口该分支路由器的。这些特性是主要相同的为所有spoke，除了IP地址(请**设置对等体...**，**隧道目的地...**)。

查看在集线路由器的上述配置，您看到有配置至少13条线路每分支路由器;四加密映射的，一个加密ACL的和八GRE隧道接口的。配置行总数，如果有300分支路由器，是3900条线路。您也需要寻址的每条隧道链路300个(/30)子网。当排除VPN网络故障时，此大小的配置是非常难管理和更加困难。要降低此值，您可能使用动态加密映射，将由1200条线路降低上述值，把2700条线路留在300分支网络。

Note: 当曾经动态加密映射时，必须由分支路由器发起IPSec加密隧道。您能也使用**ip未编号的<interface>**减少为GRE封装隧道需要的子网的数量，但是这可能做排除更加困难以后故障。

用DMVPN解决方案，您能配置单个多点GRE通道接口和单个IPSec配置文件在集线路由器处理所有分支路由器。这允许配置的大小在集线路由器的依然是常数，无论许多分支路由器被添加到VPN网络。

DMVPN解决方案引入以下新的命令：

```
crypto ipsec profile <name>
 <ipsec parameters>

tunnel protection ipsec profile <name>

ip nhrp map multicast dynamic
```

crypto ipsec profile <name>命令使用类似一个动态加密映射，并且为隧道接口特别地设计。此命令用于定义IPSec加密的参数在spoke-to-hub和spoke-to-spoke VPN隧道。需要在配置文件下的唯一的参数是转换集。IPSec对等体地址和**匹配地址...**条款IPSec代理的从NHRP映射自动地派生GRE封装隧道的。

隧道保护IPSec配置文件<name>命令被配置在GRE隧道接口下和用于关联与IPSec配置文件的GRE隧道接口。另外，**隧道保护IPSec配置文件<name>**命令可能也与一个点到点GRE封装隧道一

起使用。在这种情况下它从**隧道源…**和**隧道目的地…**配置将派生IPSec对等体和代理信息。因为IPSec对等体和加密ACL不再必要，这简单化配置。

Note: 隧道保护…命令指定IPSec加密将完成，在GRE封装被添加了到信息包后。

这些前两个新的命令类似于配置一个加密映射和分配加密映射到接口使用**加密映射<name>**命令。大差值是，用新的命令，您不需要指定IPSec对等体地址或ACL匹配信息包将被加密。这些参数从mGRE通道接口的NHRP映射自动地确定。

Note: 当曾经**隧道保护…** on命令时隧道接口，一个**加密映射…**命令在物理流出的接口没有被配置。

当这些分支路由器发起mGRE+IPsec隧道并且注册他们的单播NHRP映射时，最后new命令，**动态的ip nhrp map multicast**，允许NHRP自动地添加分支路由器到组播NHRP映射。这是需要的工作的enable (event)动态路由协议在星型网之间的mGRE+IPsec隧道。如果此命令不是可用的，则集线路由器将需要有组播映射的分离配置行到每分支。

Note: 使用此配置，因为集线路由器没有配置有关于spoke的任何信息分支路由器必须首次mGRE+IPsec隧道连接。但是，这不是问题，因为与DMVPN自动地发起mGRE+IPsec隧道，当分支路由器启动时，并且总是坚持。

Note: 以下示例显示在两星型网路由器和线路的点到点GRE隧道接口添加的NHRP配置分支路由器支持在集线路由器的mGRE通道。配置更改如下。

集线路由器(老)

```
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.<n>.1
 set transform-set trans2
 match address <n+100>
!
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<n>
  bandwidth 1000
  ip address 10.0.0.<4n-1> 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.16.<n>.1
 !
 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 <n+100> permit gre host 172.17.0.1 host
172.16.<n>.1
```

集线路由器(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
```

Spoke<n>路由器(老)

```
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
 !
```

Spoke<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.<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 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，子网掩码更改了，并且NHRP命令被添加了在隧道接口下。因为集线路由器当前使用NHRP映射分支隧道接口IP地址到分支物理接口IP地址， NHRP命令是必要的。

```
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
      ...
      tunnel key 100000
```

子网当前是/24而不是/30，因此所有节点在相同子网，而不是不同的子网。因为他们使用一个点到点GRE隧道接口， spoke通过集线器仍然发送spoke-to-spoke数据流。**ip nhrp authentication…**， **ip NHRP网络id…**和**隧道键…**命令用于映射隧道信息包，并且对正确的多点GRE通道的NHRP信息包建立接口和NHRP网络，当他们在集线器时被接受。**ip nhrp map…**和**ip nhrp nhs**…命令由在的NHRP使用讲话通告spoke NHRP映射(10.0.0.<n+1>--> 172.16.<n>.1)对集线器。10.0.0.<n+1>地址

从**IP地址…** on命令被检索隧道接口，并且172.16.<n>.1地址从**tunnel destination…命令**被检索在隧道接口。

在有300分支路由器的案件，此更改使配置行降低的数量在集线器的从3900条线路到16条线路(3884条线路的减少)。在每分支路由器的配置将按6条线路增加。

在Spoke的支持的动态地址

在Cisco路由器上，在IPSec隧道可以提出前，每IPSec对等体需要配置有另一IPSec对等体的IP地址。有关于执行此的一个问题，如果分支路由器有在其物理接口的一个动态地址，为路由器是普通通过DSL或电缆链路被联络。

TED允许一IPSec对等体通过发送一个特殊互联网安全协会和密钥管理协议(ISAKMP)信息包查找另一IPSec对等体到需要被加密原始信息包的IP目的地地址。假定是此信息包将穿程沿路径的干预的网络和采取一样由IPsec隧道信息包。此信息包将由其他终端IPSec对等体拾起，将回应第一个对等体。两路由器然后将协商ISAKMP和IPsec安全关联(SA)并且带来IPSec隧道。如果将被加密的数据包有可路由IP地址，这只将运作。

TED可以使用与GRE封装隧道的组合如前面的部分所配置的一样。这测试了和工作，虽然有在的Cisco IOS软件的更早版本的一个Bug TED强制两IPSec对等体之间的所有IP数据流被加密，不仅GRE隧道信息包。DMVPN解决方案提供此和另外的功能，不用必须的主机使用互联网可路由IP地址和，而不必发送探测和响应信息包。使用轻微的修改，从最后一部分的配置可以用于支持分支路由器用在他们的外部物理接口的动态IP地址。

集线路由器(没有更改)

```
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
      ...
      tunnel key 100000
```

Spoke<n>路由器(老)

```
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.<n>.1 host
172.17.0.1
```

Spoke<n>路由器(新)

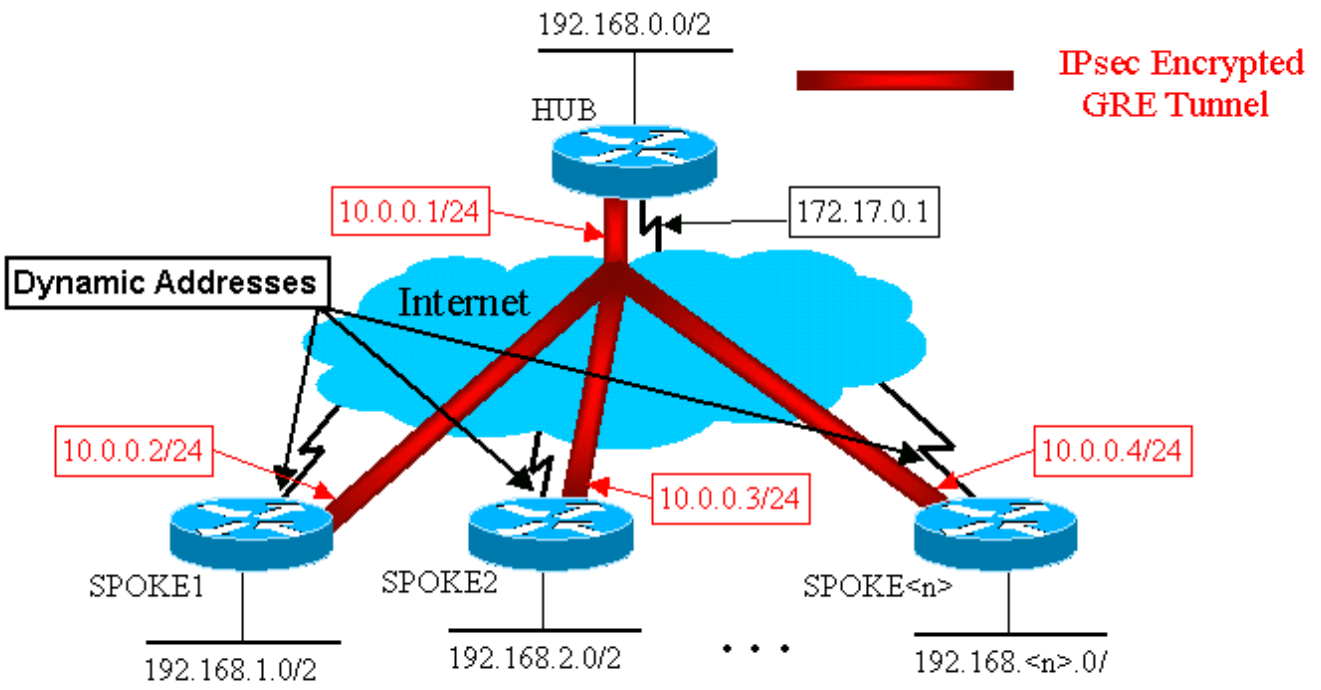
```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
```

```
 set transform-set trans2
 set security-association level per-host
 match address 101
!
...
!
access-list 101 permit gre any host 172.17.0.1
```

在新的分支配置使用的功能如下。

- 当GRE隧道接口出来，将开始发送NHRP注册信息包到集线路由器。这些NHRP注册信息包将触发将被起动的IPsec。在分支路由器上，配置集对等体<peer-address>和**匹配ip访问列表<ACL>**命令。ACL指定GRE作为协议，其中任一个为来源和集线器IP地址为目的地。**Note:** 请注意其中任一使用作为来源在ACL，并且这必须是实际情形，因为分支路由器的IP地址是动态，并且，因此，没已知，在物理接口是活跃的前。如果动态分支接口地址将限于在该子网内的一个地址IP子网可以用于来源在ACL。
- **set security-association level per-host命令**使用，以便在spoke IPSec代理的IP源将是spoke当前物理接口地址(/32)，而不是“其中任一”从ACL。如果“其中任一”从ACL使用了作为来源在IPSec代理，将阻止从也设置一条IPsec+GRE隧道的其他分支路由器用此集线器。这是因为在集线器的发生的IPSec代理是等同的**允许gre主机172.17.0.1其中任一**。这意味着所有GRE隧道信息包被注定对所有分支将被加密并且被发送了到设立一条隧道用集线器的第一分支，因为其IPSec代理匹配每分支的GRE信息包。
- 一旦IPSec隧道设置， NHRP注册信息包从分支路由器去被配置的下一跳服务器(NHS)。NHS是此集中星型网络集线路由器。NHRP注册信息包为集线路由器提供信息创建此分支路由器的NHRP映射。使用此映射，集线路由器能然后转发单播IP数据包到在mGRE+IPsec隧道的此分支路由器。并且，集线器添加分支路由器到其NHRP组播映射列表。(如果配置一个动态路由协议)，集线器然后将启动发送动态IP路由组播信息包到分支。分支然后将适合集线器的路由协议邻接，并且他们将交换路由更新。

IPsec+mGRE星型网



集线路由器

```
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
 !
```

在上述集线器上配置的公告没有配置分支路由器的IP地址。对spoke的隧道接口IP地址集线器动态地了解spoke的外部物理接口和映射通过NHRP。这允许spoke的外部物理接口IP地址动态地分配。

分支1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
```

分支2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
```

注意的主要业关于分支配置是：

- 外部物理接口(ethernet0) IP地址通过DHCP是动态。**IP地址dhcp主机名-分支2**
- 加密ACL (101)指定子网作为来源为IPSec代理。**访问列表101许可证gre 172.16.2.0 0.0.0.255主机172.17.0.1**
- 以下in命令IPsec加密映射指定安全关联将是每台主机。**set security-association level per-host**
- 因为所有通过在集线路由器的同一个多点GRE接口连接所有隧道是相同子网的一部分。**IP地址 10.0.0.2 255.255.255.0**

这三个命令的组合使不必要为了spoke的外部物理接口IP地址能被配置。使用的IPSec代理招待基础相当然后基于子网的。

因为需要发起IPsec+GRE隧道，在分支路由器的配置有被配置的集线路由器的IP地址。注意在分支1和分支2配置之间的相似性。不仅是这两类似，但是所有分支路由器配置将是类似的。在许多情况下，所有spoke需要在他们的接口的唯一IP地址，并且他们的配置的其余将是相同的。这使成为可能迅速配置和配置许多分支路由器。

NHRP数据看起来象以下在星型网。

集线路由器

```
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
```

分支1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
```

动态多点星型网

在以上的分支路由器的配置不依靠从DMVPN解决方案的功能，因此分支路由器能在12.2(13)T之前运行Cisco IOS软件版本。在集线路由器的配置依靠DMVPN功能，因此必须运行Cisco IOS版本12.2(13)T或以上。这给您在决定的若干灵活性，当您需要升级已经配置的您的分支路由器时。如果您的分支路由器也运行Cisco IOS版本12.2(13)T或以上，则您能简单化分支配置如下。

Spoke<n>路由器(在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
```

Spoke<n>路由器(在Cisco IOS 12.2(13)T以后)

```
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>
!
```

注意我们执行以下：

1. 删除了**crypto map vpnmap1 10 ipsec-isakmp命令**和替换它用**crypto ipsec profile vpnprof**。
2. 从Ethernet0接口在隧道0接口删除了**crypto map vpnmap1命令**并且放置**tunnel protection ipsec profile vpnprof命令**。
3. 去除了加密ACL，**访问列表101许可证gre所有主机172.17.0.1**。

在这种情况下IPSec对等体地址和代理从**隧道源…**和**隧道目的地…**配置自动地派生。对等体和代理如下(如在**show crypto ipsec sa命令的**输出中看到) ：

```
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>
!
```

总之，以下完全配置包括所有变动做至此点从基本配置(IPsec+GRE星型网)。

集线路由器

```
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>
 !
```

没有在集线器上配置上的变化。

分支1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
!
```

分支2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
!
```

动态多点IPSec VPN

概念和配置在此部分显示DMVPN的全部的功能。NHRP为分支路由器提供功能动态地了解其他分支路由器的外部物理接口地址VPN网络的。这意味着分支路由器将有足够的信息动态建立IPsec+mGRE隧道直接地到其他分支路由器。这是有利的，因为，如果此spoke-to-spoke数据流量通过集线路由器被发送了，然后必须加密/解码，两次增加延迟和负荷在集线路由器。为了使用此功能，分支路由器需要从点到点GRE (p-pGRE)转换到多点GRE (mGRE)隧道接口。他们也需要了解在与另一分支路由器的通道IP地址IP下个跳跃的其他spoke后是可用的(子)网络。分支路由器通过运作在IPsec+mGRE隧道的动态IP路由协议了解这些(子)网络用集线器。

可以配置运行在集线路由器的动态IP路由协议反射从一分支的获知的路由取消同一个接口对所有其他spoke，但是在这些路由的IP下个跳跃通常将是集线路由器的不是分支路由器集线器了解此路由

。

Note: 动态路由协议在星型网链路在动态spoke-to-spoke链路只运行，它不运行。

动态路由协议(RIP、OSPF和EIGRP)在集线路由器需要被配置通告路由取消mGRE通道接口，并且设置IP下个跳越对获知的路由的产生分支路由器从一个讲了话，当路由做通告取消对其他spoke时
。

下列是路由协议配置的需求。

RIP

您需要启用在mGRE通道接口的被分裂的展望期在集线器，否则RIP不会通过mGRE接口通告获知的路由取消同样接口。

```
no ip split-horizon
```

其他更改不是必要的。RIP将自动地使用在通告取消同一个接口的路由的原始IP下个跳跃了解这些路由的地方。

EIGRP

您需要启用在mGRE通道接口的被分裂的展望期在集线器，否则EIGRP不会通过mGRE接口通告获知的路由取消同样接口。

```
no ip split-horizon eigrp <as>
```

默认情况下， EIGRP将设置IP下个跳越是通告，既使当做通告那些路由取消同一个接口的路由的集线路由器了解他们的地方。那么，当通告这些路由时，在这种情况下，您需要以下配置命令指示EIGRP使用原始IP下个跳跃。

```
no ip next-hop-self eigrp <as>
```

Note: ip next-hop-self eigrp <as>命令不会是可用开始在Cisco IOS版本12.3(2)。对于在12.2(13)T和12.3(2)您之间的Cisco IOS版本必须执行以下：

- 如果spoke-to-spoke动态隧道没有希望，则上述命令不是需要的。
- 如果spoke-to-spoke动态隧道希望，则您必须使用交换在分支路由器的隧道接口的进程。
- 否则，您将需要使用在DMVPN的一个不同的路由协议。

OSPF

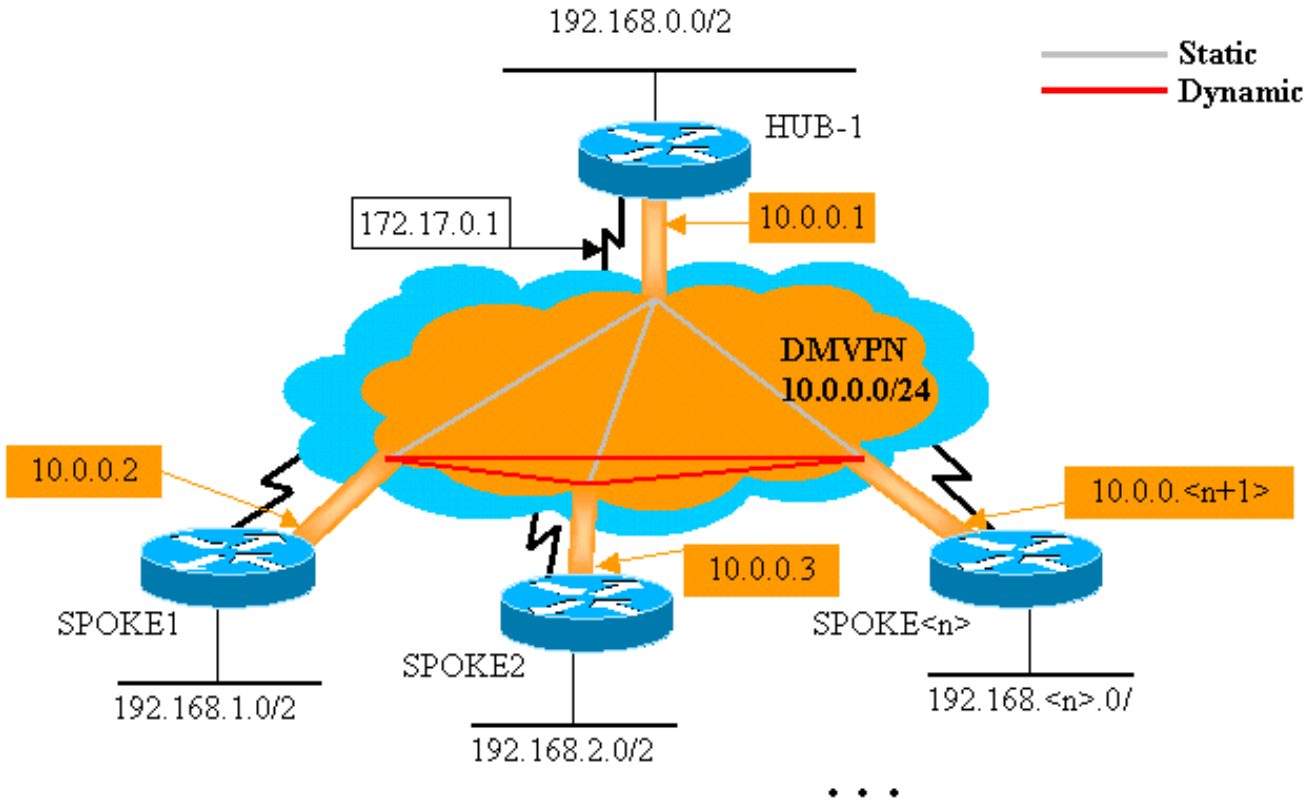
因为OSPF是连接状态的路由协议，没有所有已分解展望期问题。通常对于多点接口您配置OSPF网络类型点对多点，但是这将造成OSPF添加主机路由到在分支路由器的路由表。这些主机路由将导致被注定的信息包网络在通过集线器将转发的其他分支路由器背后，相当然后转发直接地到另一分支。使用命令，要避过此问题，请配置OSPF网络类型是广播。

```
ip ospf network broadcast
```

您也需要确信，集线路由器将是IPsec+mGRE网络的指定路由器(DR)。这由设置OSPF优先级比1在集线器和0完成极大在spoke。

- 集线器：ip ospf priority 2
- 分支：ip ospf priority 0

DMVPN单台集线器



集线路由器

```
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
!
```

在集线器上配置上的唯一的变化是OSPF是路由协议而不是EIGRP。注意设置OSPF网络类型播放和优先级设置到设置OSPF网络类型的2.播放将造成OSPF在有IP下一跳地址的辐射路由器后安装网络的路由作为该分支路由器的GRE封装隧道地址。

分支1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
!
```

在分支路由器的配置当前非常类似于在集线器的配置。区别如下：

- OSPF优先级设置到0。分支路由器不可能允许成为mGRE非广播多重接入(NBMA)网络的DR。仅集线路由器有对所有分支路由器的直接静态连接。DR必须访问NBMA网络的所有成员。
- 有NHRP单播和为集线路由器配置的组播映射。

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

  在早先配置中，因为GRE封装隧道点到点， **ip nhrp map multicast…**命令不是需要的。在那种情况下，组播信息包通过对单个可能的目标地址的隧道将自动地被封装。此命令当前必要，因为spoke GRE封装隧道更改了到多点，并且有然后一可能的目标地址。
- 当分支路由器过来时，它必须首次隧道连接用集线器，因为集线路由器没有配置有关于分支路由器的任何信息，并且分支路由器可能有动态地指定的IP地址。分支路由器也配置有集线器作为他们的NHRP NHS。

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

  用上述命令，分支路由器定期将发送NHRP注册信息包到mGRE+IPsec隧道到集线路由器。这些注册信息包提供由集线路由器必要到隧道信息包回到分支路由器的分支NHRP映射信息。

分支2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
!
```

Spoke<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.<n>.0 0.0.0.255 area 0
```

```
!
```

注意所有的配置分支路由器是非常类似的。唯一的区别是在本地接口的IP地址。这帮助，当配置很大数量的分支路由器。可以相等地配置所有分支路由器，并且仅本地IP接口地址需要被添加。

这时，请看一看在路由表和在集线器的NHRP映射表，分支1和分支2路由器发现初始情况(在分支1和分支2路由器出现)之后和条件，在分支1和分支2创建了他们之间后的一个动态链路。

初始情况

集线器路由器信息

```
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
```

分支1路由器信息

```
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
```

分支2路由器信息

```
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
```

这时我们从192.168.1.2连接到192.168.2.3。这些地址分别为为主机在分支1和分支2路由器背后。以下事件顺序发生构建直接spoke-to-spoke mGRE+IPsec隧道。

1. 分支1路由器收到与目的地192.168.2.3的ping信息包。它在路由表里查寻此目的地并且发现需要转发此信息包隧道0接口到IP nexthop， 10.0.0.3。
2. 分支1路由器检查NHRP映射表目的地10.0.0.3并且发现没有条目。分支1路由器创建一个NHRP解决方法请求信息包并且发送它到其NHS (集线路由器)。
3. 集线路由器检查其NHRP映射表目的地10.0.0.3并且发现映射对地址172.16.2.75。集线路由器创建一个NHRP解决方法回复信息包并且发送它到分支1路由器。
4. 分支1路由器收到NHRP解决方法回复，并且在其NHRP映射表里输入10.0.0.3 —>172.16.2.75映射。NHRP映射的添加触发IPsec发起有对等体的172.16.2.75一个IPSec隧道。
5. 分支1路由器起动与172.16.2.75的ISAKMP并且协商ISAKMP和IPSec SAS。IPSec代理从隧道0**隧道源<address>**命令和NHRP映射派生。

   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. 一旦IPSec隧道完成被构件，对192.168.2.0/24子网的所有进一步数据包被发送直接地到分支2。
7. 在信息包被注定对192.168.2.3转发了到主机后，此主机将发送一个返回信息包到192.168.1.2。当分支2路由器收到此信息包被注定对192.168.1.2，在路由表里将查寻此目的地并且发现需要转发此信息包隧道0接口到IP下个跳跃， 10.0.0.2。
8. 分支2路由器检查NHRP映射表目的地10.0.0.2并且发现没有条目。分支2路由器创建一个NHRP解决方法请求信息包并且发送它到其NHS (集线路由器)。
9. 集线路由器检查其NHRP映射表目的地10.0.0.2并且发现映射对地址172.16.1.24。集线路由器创建一个NHRP解决方法回复信息包并且发送它到分支2路由器。
10. 分支2路由器收到NHRP解决方法回复，并且输入10.0.0.2 — >映射在其NHRP映射表里的172.16.1.24。NHRP映射的添加触发IPsec发起有对等体的172.16.1.24一个IPSec隧道，但是已经有对等体的172.16.1.24一个IPSec隧道，因此没什么进一步需要执行。
11. 分支1和分支2能直接地当前转发信息包彼此。当NHRP映射未使用转发维持时间的信息包，NHRP映射将被删除。NHRP映射条目的删除将触发IPsec删除此直接链接的IPSec SAS。

在动态链路以后的条件创造在分支1和分支2之间

分支1路由器信息

```
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
```

分支2路由器信息

```
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
```

从上述输出您能看到分支1和分支2从集线路由器得到彼此的NHRP映射，并且他们构建了并且使用了mGRE+IPsec隧道。NHRP映射expire after五分钟(NHRP持有时间的当前值= 300秒)。如果NHRP映射在最后一刻内使用在到期前，则将发送NHRP解决方法请求和回复刷新条目，在被删除前。否则， NHRP映射将被删除，并且那将触发IPsec清除IPSec SAS。

动态多点IPSec VPN用双集线器

使用对分支路由器的一些条更多的配置线路您能设置双重(或多个)集线路由器，冗余的。有两种方式配置双集线器DMVPNs。

- 与每分支使用单个多点GRE通道接口和指向的单个DMVPN网络两不同集线器作为其Next-Hop-Server (NHS)。集线路由器只将有单个多点GRE通道接口。
- 与有每分支的双重DMVPN网络两个GRE隧道接口(点到点或多点)和每个GRE封装隧道被连接到一个不同的集线路由器。再次，集线路由器只将有单个多点GRE通道接口。

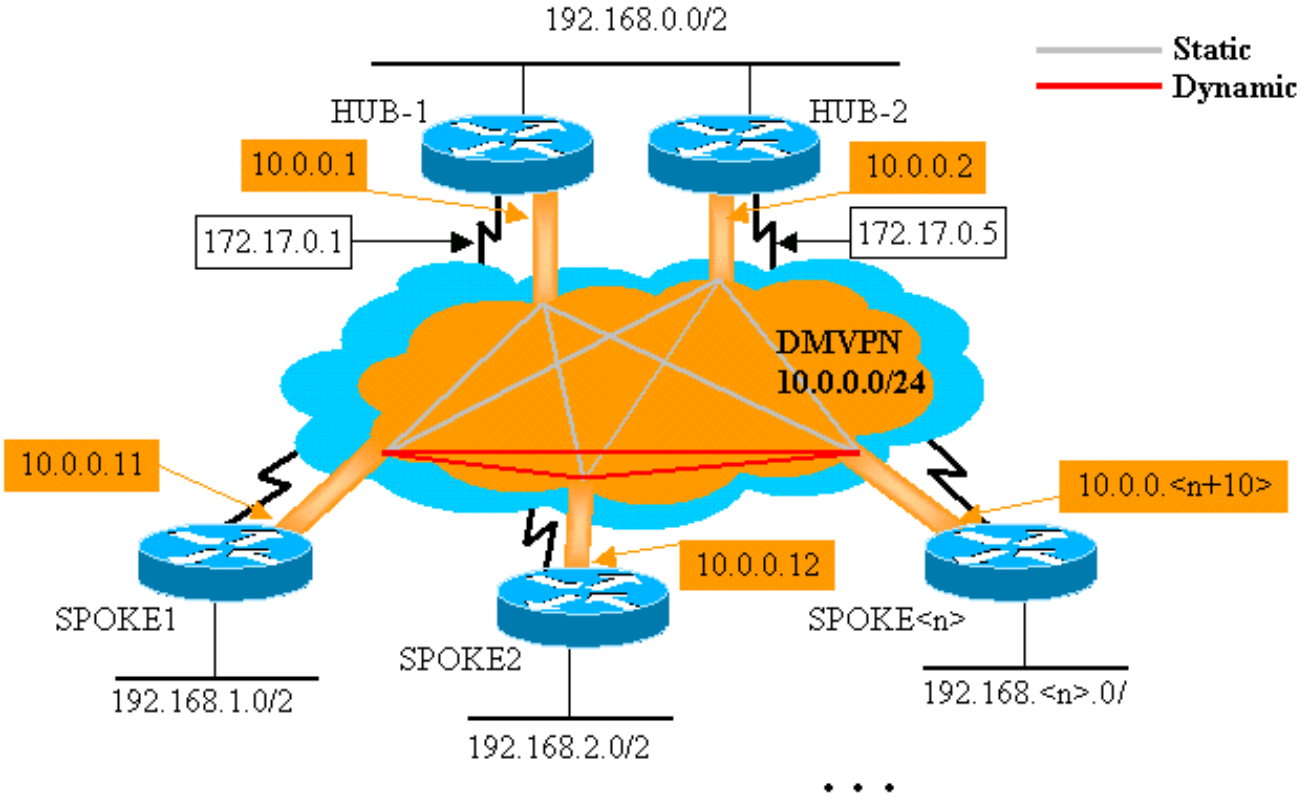
以下示例将看似配置这两个不同的方案为双集线器DMVPNs。在两种情况下，突出显示的区别是相对DMVPN单台集线器配置。

双集线器-单DMVPN布局

有单DMVPN布局的双集线器是非常容易设置，但是不产生您同样多对路由的控制在DMVPN间，象有双重DMVPNs布局的双集线器。想法在这种情况下是有单个DMVPN “网云”与所有集线器(两在这种情况下)和所有spoke被连接到此单个子网(“网云”)。从spoke的静态NHRP映射到集线器定义了动态路由协议将运行的静态IPsec+mGRE链路。动态路由协议不会运行动态IPsec+mGRE链路在spoke之间。因为分支路由器是路由邻居用在同样mGRE通道的集线路由器建立接口，您不能使用链路或建立接口区别(类似权值，请开销，延迟或者带宽)修改动态路由协议权值更喜欢在另一台集线器的一台集线器，当他们两个上升时。如果此首选是需要的，则必须使用技术内部对路由协议的配置。为此，使用EIGRP或RIP而不是OSPF动态路由协议可能是更好的。

Note: 如果集线路由器是并行定位的，上述问题通常是仅问题。当他们不是并行定位的，正常动态路由可能将导致更喜欢正确的集线路由器，即使目的地网络可以通过任一个集线路由器到达。

双集线器-单DMVPN布局



集线路由器

```
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
!
```

Hub2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
!
```

在Hub1配置上的唯一的变化是更改OSPF使用两个区域。Area 0使用网络在两集线器背后，并且第1区使用DMVPN网络和网络在分支路由器背后。OSPF可能使用一个区域，但是两个区域用于得这里展示多个OSPF区域的配置。

Hub2的配置基本上是作为Hub1配置用适当的IP地址更改的相同的。这一个主要区别是Hub2也是分支(或客户端) Hub1，做Hub1主集线器和Hub2附属集线器。这执行，以便Hub2是有Hub1的一个OSPF邻居在mGRE通道。因为Hub1是OSPF DR，必须有与其他OSPF路由器的直接连接在mGRE接口(NBMA网络)。没有Hub1和Hub2之间的直接链接，当Hub1也是时， Hub2不会参加OSPF路由。当Hub1发生故障， Hub2将是DMVPN的(NBMA网络) OSPF DR。当Hub1恢复，将接管是DMVPN的OSPF DR。

因为GRE隧道接口的带宽设置为1000 Kb/sec与在Hub2的900 Kb/sec在Hub1和Hub2后的路由器将使用Hub1发送信息包到分支网络。相反，分支路由器在集线路由器后将发送网络的信息包到Hub1和Hub2，因为有在每分支路由器的仅单个mGRE通道接口，并且将有两等价路由。如果使用每个信息包负载均衡这能导致无序信息包。

分支1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
 !
```

在配置上的区别在分支路由器如下：

- 在新的配置中，分支配置有Hub2和Hub2的静态NHRP映射被添加作为一个下一跳服务器。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：

```
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
```

- 在分支路由器的OSPF区域更改了到第1.区。

切记通过定义静态NHRP映射和NHS在一分支路由器集线器的，您运行动态路由协议在此隧道。这定义了星型网路由或相邻网络。注意Hub2是所有的一台集线器spoke和它也是Hub1的一分支。当您使用DMVPN解决方案时，这使容易设计，配置和修改多层集中星型网络。

分支2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
!
```

Spoke<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.<n>.0 0.0.0.255 area 0
!
```

这时，您能看一看在路由表、NHRP映射表和IPSec连接在Hub1、Hub2、分支1和分支2路由器发现

初始情况(在分支1和分支2路由器之后请出现)。

初始状况和更改

Hub1路由器信息

```
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路由器信息

```
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
```

分支1路由器信息

```
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
```

分支2路由器信息

```
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
```

有注意的两三个有趣问题关于在Hub1、Hub2、分支1和分支2的路由表：

- 两个集线路由器有等价路由对网络在分支路由器背后。Hub1 ：

```
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
```

Hub2 ：

```
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
```

这意味着Hub1和Hub2为网络将通告同一费用在分支路由器背后到网络的路由器在集线路由器背后。例如，在路由器的路由表， R2，被连接直接地到192.168.0.0/24 LAN将看起来象以下：R2 ：

```
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
```

- 分支路由器有等价路由通过两个集线路由器对网络在集线路由器背后。分支1 ：

```
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
```

分支2 ：

```
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
```

如果分支路由器执行每个信息包负载均衡，则您可能得到无序信息包。

要避免执行不对称路由或每个信息包负载均衡在链路间的两集线器，您需要配置路由协议选一条spoke-to-hub路径在两个方向。如果希望Hub1是主要的和的Hub2备份，则您能设置在集线器隧道接口的OSPF开销是不同的。

Hub1 ：

```
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
```

Hub2 ：

```
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
```

现在路由看起来象以下：

Hub1 ：

```
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
```

Hub2 ：

```
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
```

R2 ：

```
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
```

两个集线路由器当前有在路由的不同的费用网络的在分支路由器背后。这意味着Hub1为转发对分支路由器的数据流将更喜欢，和在路由器R2能被看到。这在上面第一个项目符号描述的照料不对称路由问题。

在另一个方向的不对称路由，正如以上第二个的项目符号所描述，仍然是那里。当使用OSPF作为动态路由协议时，您能修正此用解决方法通过使用**距离…**命令在spoke的**router ospf 1**下更喜欢获知的路由通过在获知的路由的Hub1通过Hub2。

分支1 ：

```
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
```

分支2 ：

```
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
```

现在路由看起来以下：

分支1 ：

```
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
```

分支2 ：

```
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
```

上述路由配置将防止受到不对称路由，当同时允许故障切换对Hub2时，如果Hub1断开。意味着，当两集线器是UP时，只有使用Hub1。如果要通过平衡在集线器间的spoke使用两集线器，与故障切换保护和没有不对称路由，则路由配置能获得复杂，特别是当使用OSPF时。为此，有双重DMVPN布局的以下双集线器可能是一个更好的选择。

双集线器-双重DMVPN布局

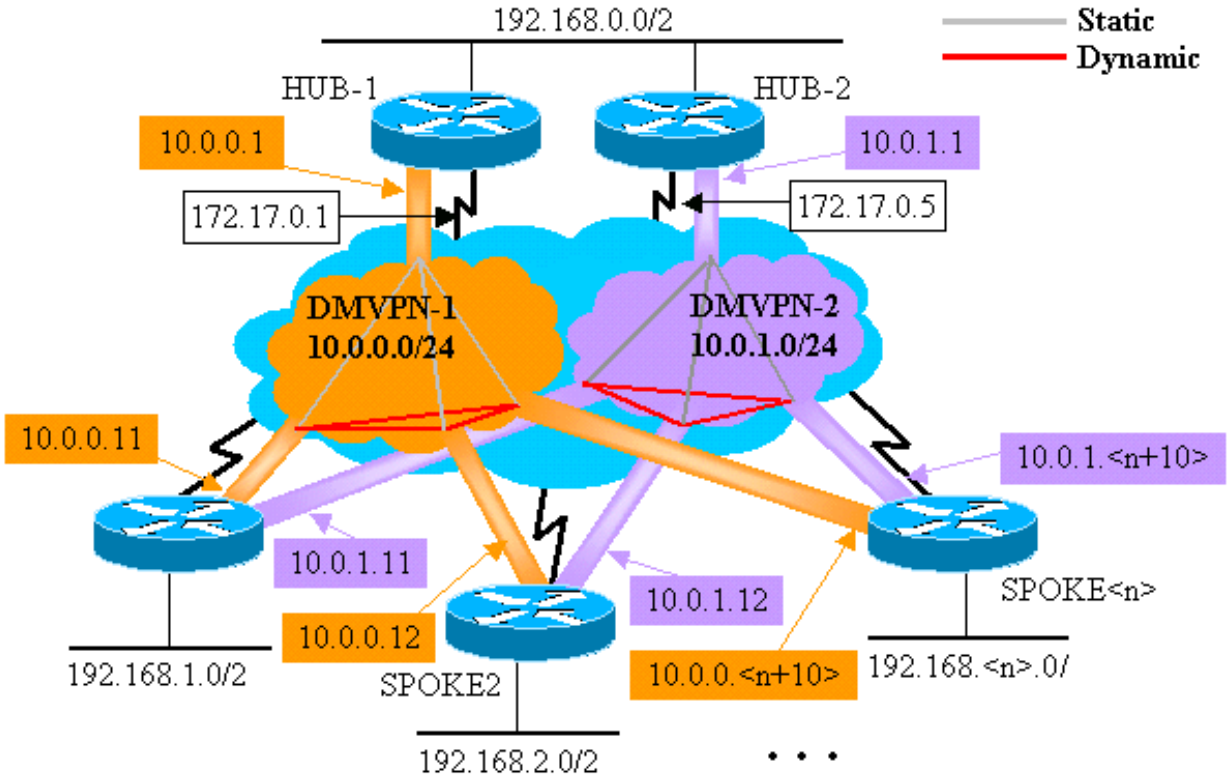
有双重DMVPN布局的双集线器是轻微更难设置，但是产生您路由的更好的控制在DMVPN间的。想法是有一两分开的DMVPN “网云”。每台集线器(两在这种情况下)连接到一个DMVPN子网(“网云”)和spoke被连接到两个DMVPN子网(“网云”)。因为分支路由器是路由邻居用在两个GRE隧道接口的两个集线路由器，您能使用接口配置区别(例如带宽，请开销和延迟)修改动态路由协议权值更喜欢在另一台集线器的一台集线器，当他们两个上升时。

Note: 如果集线路由器是并行定位的，上述问题只通常是相关的。当他们不是并行定位的，正常动态路由可能将导致更喜欢正确的集线路由器，即使目的地网络可以通过任一个集线路由器到达。

您能使用在分支路由器的p-pGRE或mGRE通道接口。在分支路由器的多个p-pGRE接口能使用同样**隧道源…** IP地址，但是在分支路由器的多个mGRE接口必须有唯一隧道**来源…** IP地址。这是因为，当IPsec起动时，第一个信息包是需要与一个mGRE产生关联建立隧道的ISAKMP信息包。ISAKMP信息包只有目的地IP地址(远程IPSec对等体地址)用做此关联。此地址被匹配**隧道源…**地址，但是，因为两条隧道有同一个**隧道源…**地址，第一个mGRE通道接口总是被匹配。这意味着流入组播信息包可能与错误的mGRE接口产生关联，中断所有动态路由协议。

因为他们有**隧道键…**值区分在两个mGRE接口之间， GRE信息包没有此问题。开始在Cisco IOS Software Releases 12.3(5)和，其它参数介绍12.3(7)T解决此限制：**隧道保护….共享。共有的**关键字表明mutiple mGRE接口以同样IP原地址将使用IPSec加密。如果有一个更早版本您在此双集线器能使用p-pGRE隧道与双重DMVPN布局。在p-pGRE隧道盒，**隧道源…**和**隧道目的地…** IP地址可以用于匹配。对于此示例p-pGRE隧道用于此双集线器与双重DMVPN布局和不使用**共有的**合格者。

双集线器-双重DMVPN布局



以下突出显示的更改是相对在本文说明的前动态多点星型网配置。

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
 !
```

Hub2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
 !
```

在这种情况下， Hub1和Hub2配置是类似的。主要区别是其中每一台是一不同的DMVPN的集线器。每DMVPN使用一不同：

- IP子网(10.0.0.0/24， 10.0.0.1/24)
- NHRP网络ID (100000， 100001)

- 隧道键(100000， 100001)

动态路由协议从OSPF在本文转换到EIGRP，使用EIGRP，因为建立和管理NBMA网络是更加容易的，如所描述以后。

分支1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
```

```
!
```

其中每一分支路由器配置有两p-pGRE隧道接口，一个在中的每一两个DMVPNs。**IP地址…**， **ip NHRP网络id…**，**隧道键…**和**隧道目的地…**值用于区分在两条隧道之间。动态路由协议，EIGRP，在p-pGRE隧道子网运行和用于选择一个p-pGRE接口(DMVPN)在其他。

分支2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
!
```

Spoke<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 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.<n+10> 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 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
!
```

这时，请让我们看一看在路由表、NHRP映射表和IPSec连接在Hub1、Hub2、分支1和分支2路由器发现初始情况(在分支1和分支2路由器之后请出现)。

初始状况和更改

Hub1路由器信息

```
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路由器信息

```
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
```

分支1路由器信息

```
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
```

分支2路由器信息

```
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
```

再次，有注意的两三件有趣事关于在Hub1、Hub2、分支1和分支2的路由表：

- 两个集线路由器有等价路由对网络在分支路由器背后。Hub1 ：

```
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
```

Hub2 ：

```
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
```

这意味着Hub1和Hub2为网络将通告同一费用在分支路由器背后到网络的路由器在集线路由器背后。例如，在路由器的路由表， R2，被连接直接地到192.168.0.0/24 LAN将看起来象以下：R2 ：

```
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
```

- 分支路由器有等价路由通过两个集线路由器对网络在集线路由器背后。分支1 ：

```
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
```

分支2 ：

```
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
```

如果分支路由器执行每信息包负载平衡，则您可能得到无序信息包。

要避免执行不对称路由或每个信息包负载均衡在链路间的两集线器，您需要配置路由协议选一条

spoke-to-hub路径在两个方向。如果希望Hub1是主要的和的Hub2备份，则您能设置在集线器隧道接口的延迟是不同的。

Hub1 ：

```
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
```

Hub2 ：

```
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
```

Note: 在本例中， 50加了到在隧道接口的延迟在Hub2，因为小于在Ethernet 1接口的延迟两集线器(100)之间。通过该执行， Hub2将转发信息包直接地到分支路由器，但是比Hub1将通告一个不太理想的路由到在Hub1和Hub2后的路由器。如果延迟增加由超过100，则Hub2通过Hub1将转发分支路由器的信息包通过Ethernet 1接口，仍然，虽然在Hub1和Hub2后的路由器正确地会更喜欢发送的信息包Hub-1到分支路由器。

现在路由看起来象以下：

Hub1 ：

```
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
```

Hub2 ：

```
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
```

R2 ：

```
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
```

两个集线路由器有网络路由的不同的费用在分支路由器背后，如此，在这种情况下， Hub1为转发对分支路由器的数据流将更喜欢，和在R2能被看到。这在上面第一个项目符号问题描述的照料。

在第二个项目符号描述的问题以上仍然是那里，但是，因为您有两个p-pGRE隧道接口，您能分开设置**延迟…**在隧道接口从Hub1更改获知的路由的EIGRP度量与Hub2。

分支1 ：

```
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
```

分支2 ：

```
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
```

现在路由看起来以下：

分支1 ：

```
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
```

分支2 ：

```
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
```

上述路由配置将防止受到不对称路由，当同时允许故障切换对Hub2时，如果Hub1断开。意味着，当两集线器是UP时，只有使用Hub1。

如果要通过平衡在集线器间的spoke使用两集线器，与故障切换保护和没有不对称路由，则路由配置是更加复杂的，但是您能执行它，当使用EIGRP时。要完成此，请送回**延迟...**在集线路由器的隧道接口到是相等的然后请使用**offset-list <acl> <offset> <interface>** on命令分支路由器增加EIGRP度量为路由通告了GRE隧道接口对备用集线器。**...**在分支的隧道0和Tunnel1接口之间仍然使用不同等的**延迟**，因此分支路由器将更喜欢其主集线器路由器。在分支路由器的更改如下。

分支1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
!
```

分支2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
!
```

Note: 偏移值为12800 (50*256)被添加了到EIGRP度量，因为小于25600 (100*256)。此值(25600)，是什么被添加到获知的路由的EIGRP度量在集线路由器之间。通过使用12800在**offset-list命令**，备用集线器路由器将转发信息包直接地到分支路由器，而不是转发这些信息包通过以太网通过那些spoke的主集线器路由器。在集线路由器做通告的路由的权值将是这样正确的主集线器路由器将更喜欢。切记spoke的一半有Hub1作为他们的主路由器和另外一半有Hub2作为他们的主路由器。

Note: 如果偏移值增加由超过25600 (100*256)，则集线器将转发分支路由器的一半的信息包到另一台集线器通过Ethernet 1接口，即使路由器在集线器背后会更喜欢发送的信息包正确的集线器到分支路由器。

Note: out命令的distribute-list 1也被添加了，因为很可能，从一个集线路由器的获知的路由通过在分支的一个隧道接口可能做通告回到另一台集线器通过另一条隧道。**distribute-list…**命令保证分支路由器能只通告其自己的路由。

Note: 如果喜欢控制在集线路由器的路由通告而不是分支路由器的，则**在<value> <interface>的offset-list <acl1>**和**在**命令的**distribute-list <acl2>**在集线路由器可以被配置而不是spoke的。<acl2>访问列表将列出路由从后面所有spoke，并且<acl1>访问列表将列出仅路由从另一个集线路由器是主集线器的后面spoke。

使用这些更改路由看起来象以下：

Hub1 ：

```
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
!
```

Hub2 ：

```
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
 !
```

R2 ：

```
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
!
```

分支1 ：

```
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
 !
```

分支2 ：

```
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
 !
```

结论

DMVPN解决方案提供以下功能更好扩展大和小的IPSec VPN网络。

- DMVPN允许更好的比例缩放在全网状连接或在部分网状IPsec VPN。是特别有用的，当spoke-to-spoke数据流是间歇的时(例如，每分支不经常发送数据到其他分支)。它允许任何讲话发送数

据直连到所有其他分支，象长期spoke之间的直接IP连通性。
- DMVPN支持与动态地分配的地址的IPsec节点(例如电缆、ISDN和DSL)。这适用于星型网以及网状网络。DMVPN能要求hub-to-spoke链路经常是UP。
- DMVPN简化VPN节点的添加。当添加一新的分支路由器时，您必须只配置分支路由器和把它插入网络(虽则，您可能需要添加ISAKMP新的发表演讲授权信息关于集线器)。集线器将动态地得知新的分支，并且动态路由协议将传播路由对集线器和其他spoke。
- DMVPN减少在所有路由器需要的配置的大小在VPN。这也是GRE+IPsec仅仅是集中星型的VPN网络的盒。
- DMVPN使用GRE，并且，因此，支持IP组播和动态路由数据流在VPN间。这意味着可以使用一个动态路由协议，并且冗余"集线器"可以由协议支持。也支持组播应用。
- DMVPN在spoke的支持分割隧道。

Related Information

- 动态多点 VPN (DMVPN)
- IPSec 支持页面
- Technical Support - Cisco Systems