配置DMVPN上的BGP第3阶段

目录

简介

本文档介绍使用BGP的DMVPN第3阶段的配置和操作，包括基于DMVPN隧道的IPsec的分层故障排除。

先决条件

对于本文档中的配置和调试命令，您需要两台运行Cisco IOS®版本15.3(3)M或更高版本的Cisco路由器。一般来说，基本动态多点VPN(DMVPN)第3阶段需要Cisco IOS版本12.4(6)T，尽管本文档中介绍的功能和调试不完全受支持。

要求

Cisco 建议您具有以下主题的基础知识：

- IKEV1/IKEV2和IPsec
- DMVPN组件：

- 下一跳解析协议(NHRP):创建所有分支的隧道到实际（公共接口）地址的分布式(NHRP)映射数据库
- 多点通用路由封装(mGRE)隧道接口:支持多个GRE/IPsec隧道的单个通用路由封装(GRE)接口

，简化了配置的大小和复杂性，并支持动态隧道创建
- IPsec隧道保护:动态创建并应用加密策略
- 路由:动态网络；几乎所有路由协议(增强型内部网关路由协议(EIGRP)、路由信息协议(RIP)、开放最短路径优先(OSPF)、BGP、ODR)都受支持

使用的组件

本文档中的信息基于Cisco ASR1000系列聚合服务路由器版本17.6.5(MD)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

什么是DMVPN?

DMVPN是一种Cisco IOS软件解决方案，用于轻松、动态和可扩展地构建IPsec+GRE VPN。这种解决方案无需静态配置所有设备，即可构建具有多个站点的VPN网络。它是“中心辐射型”网络，辐射型可以直接相互通信，而无需经过中心。IPsec支持加密，因此DMVPN成为使用常规互联网连接连接不同站点的常用选择。

DMVPN如何工作？

- 辐射点建立到集线器的动态永久GRE/IPsec隧道，但不建立到其他辐射点的隧道。它们注册为NHRP服务器（集线器）的客户端。
- 当分支需要将数据包发送到另一个分支后的目标（专用）子网时，它会通过NHRP查询目标分支的实际（外部）地址。
- 现在，始发分支可以发起到目标分支的动态GRE/IPsec隧道（因为它知道对等体地址）。
- 动态分支到分支隧道在mGRE接口上构建。
- 当流量停止时，将删除分支到分支隧道。

DMVPN有哪些不同类型？

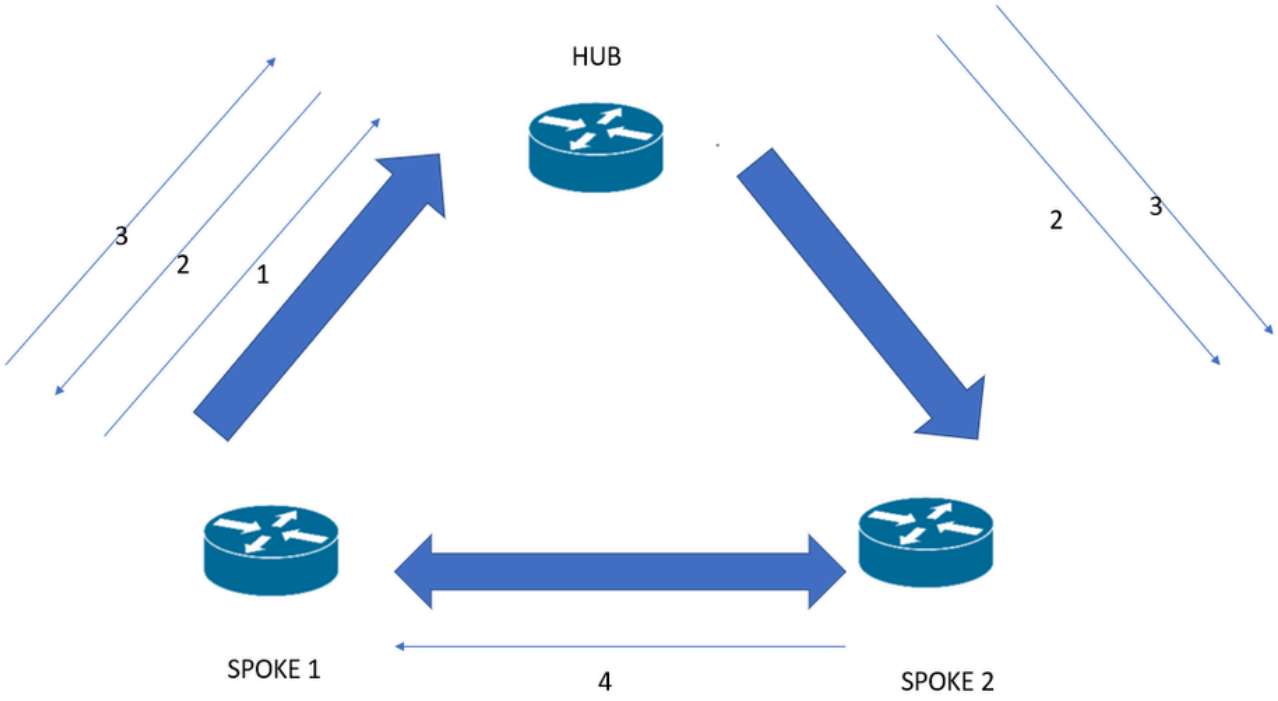
1. DMVPN阶段I:此阶段涉及中心上的单个mGRE接口，并且所有分支仍是静态隧道，因此您不会获得任何动态分支到分支连接。
2. DMVPN阶段II:此阶段涉及使用mGRE接口配置每个站点，以便您获得动态分支到分支连接。
3. DMVPN阶段III：此阶段扩展了DMVPN网络的可扩展性。这涉及到汇总到DMVPN云。配置NHRP重定向和NHRP快捷方式交换。NHRP重定向告知源设备找到通向它尝试到达的目的地的更佳路径。NHRP快捷方式允许DMVPN了解其他DMVPN路由器背后的其他网络。

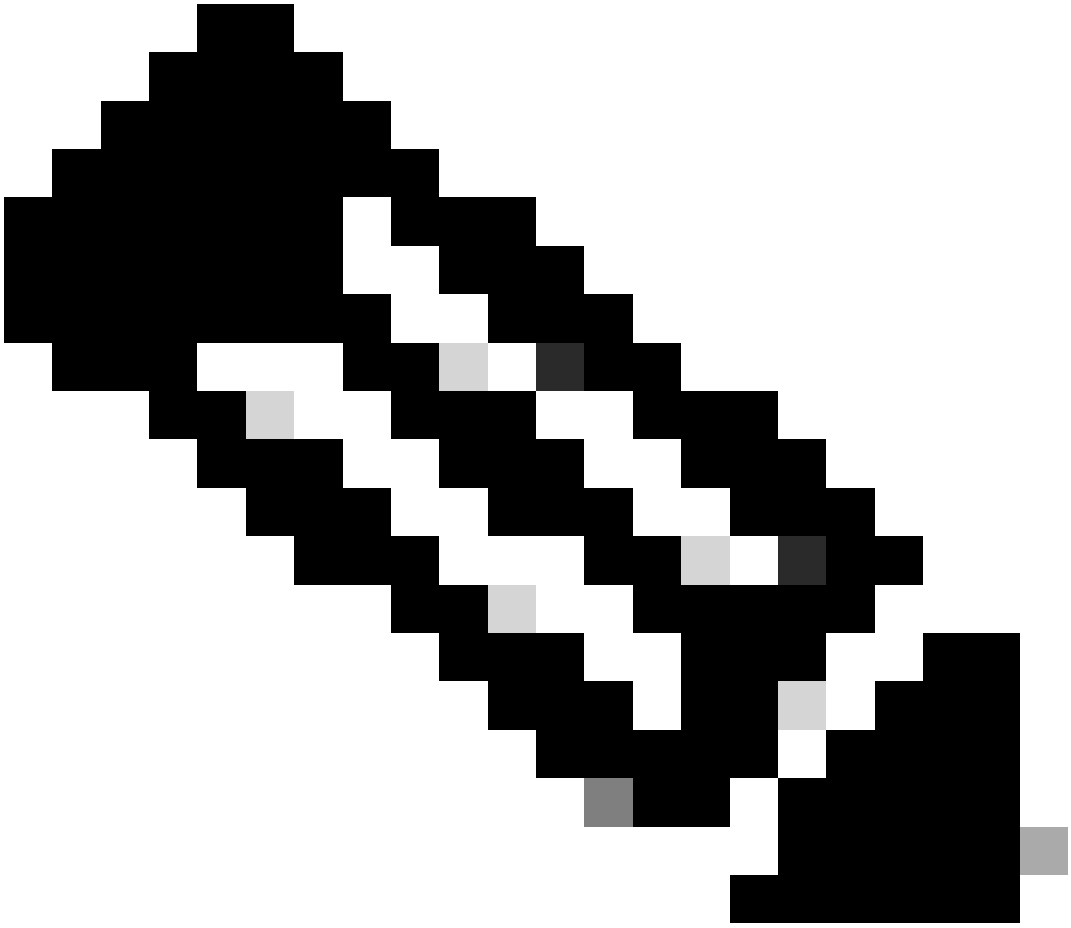
DMVPN第3阶段的流量

1. 数据包通过Hub（根据路由表）从Spoke的1个网络发送到Spoke的2个网络。
2. 中心路由器将数据包路由到Spoke2，但并行将NHRP重定向消息发送回Spoke1，其中包含有关到Spoke2的次优路径和Spoke2的隧道IP的信息。
3. 然后，Spoke1使用辐射点2隧道的目标IP向下一跳服务器(NHS)发出辐射点2非广播多路访问

(NBMA)IP地址的NHRP解析请求。此NHRP解析请求通过NHS发送到Spoke2(根据路由表) — 这是一个正常的逐跳NHRP转发过程。

4. Spoke2在收到包括Spoke1的NBMA IP的解析请求后，将NHRP解析应答直接发送到Spoke1 - 应答不会通过中心！
5. Spoke1在收到Spoke2的正确NBMA IP后重写目标前缀的CEF条目 — 此过程称为NHRP Shortcut。
6. 辐条不会通过收集邻接关系触发NHRP，但NHRP应答会更新CEF。



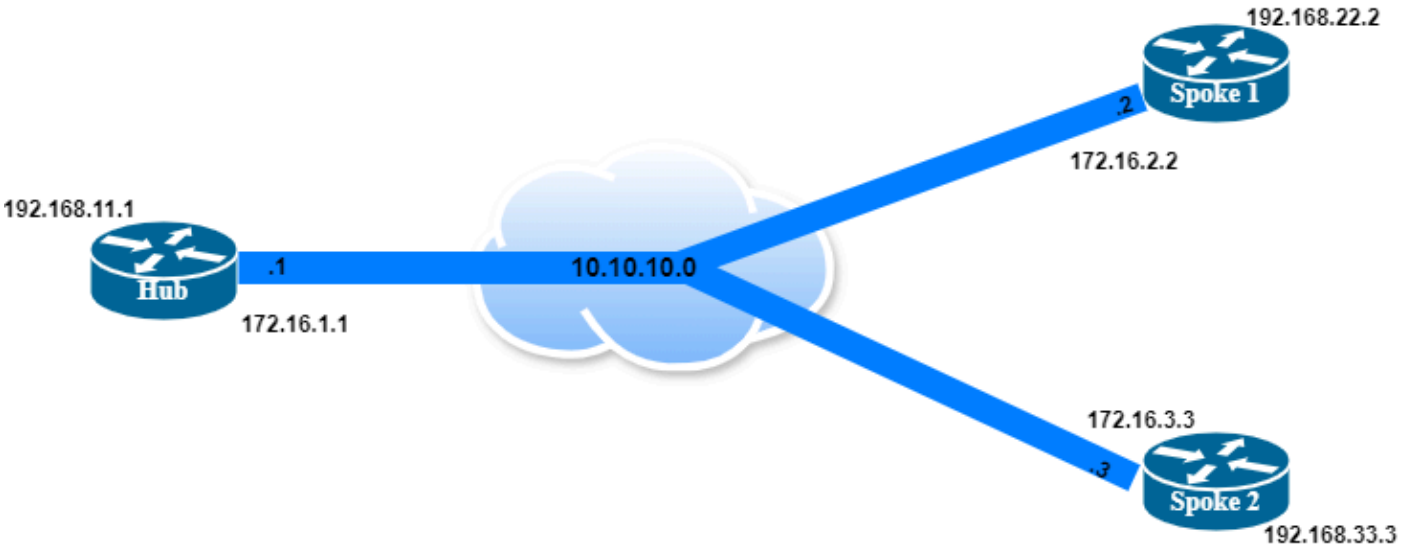


注意：

DMVPN第2阶段:在此阶段，初始分支到分支数据包确实是进程交换的，因为CEF邻接处于“聚集”状态。这意味着路由器没有足够的信息来使用CEF转发数据包，并且必须使用更加消耗资源的进程交换来使用NHRP（下一跳解析协议）解析下一跳。

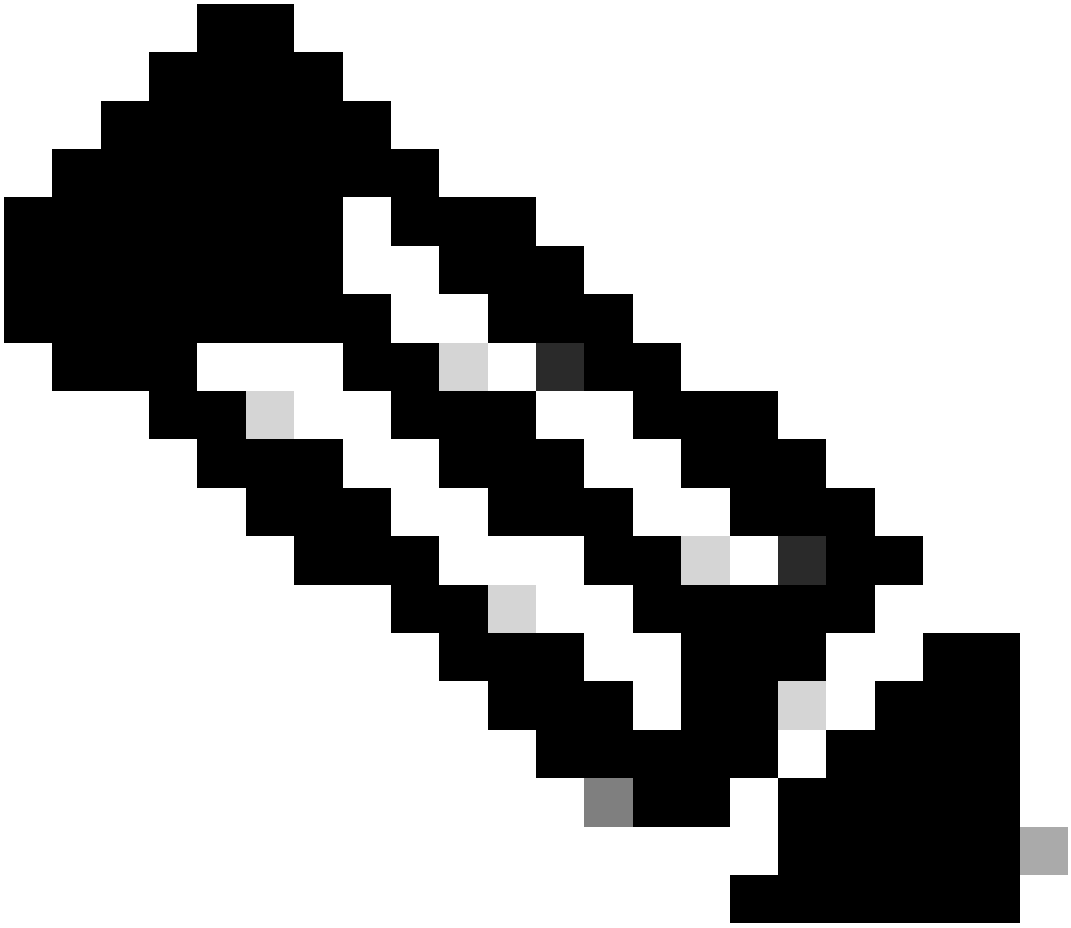
DMVPN第3阶段:此阶段在阶段2的基础上有所改进，它允许从开始使用CEF交换初始分支到分支数据包。这可通过使用NHRP重定向和NHRP快捷方式功能来实现，这些功能有助于快速建立直接的分支到分支隧道。因此，CEF的使用更加一致，减少对进程交换的依赖。

网络图


192.168.22.2
Spoke 1
.2
172.16.2.2
192.168.11.1
Hub
.1
10.10.10.0
172.16.1.1
172.16.3.3
.3
Spoke 2
192.168.33.3

配置

加密配置



注意：集线器和所有辐条上的情况相同。

1. 配置Ikev2建议和密钥环。

```
crypto ikev2 proposal DMVPN
encryption aes-cbc-256
integrity sha256
第 14 组
crypto ikev2 keyring IKEV2-KEYRING
peer any
地址0.0.0.0 0.0.0.0
预共享密钥CISCO123
!
```

2. 配置包含所有连接相关信息的Ikev2配置文件。

```
crypto ikev2 profile IKEV2-PROF
```

match address local interface GigabitEthernet0/0/0
match identity remote address 0.0.0.0
身份验证本地预共享
身份验证远程预共享
keyring local IKEV2-KEYRING

以下是ikev2配置文件中使用的命令的详细信息：

- match address local interface GigabitEthernet0/0/0:VPN终止的本地外部接口，在本例中为GigabitEthernet0/0/0
- match identity remote address 0.0.0.0：由于远程对等体可以是多个，因此使用0.0.0.0表示任何对等体
- 身份验证本地预共享:本地站点的身份验证模式是预共享的
- 身份验证远程预共享:本地站点的身份验证模式是预共享的
- 密钥环本地IKEV2-KEYRING:使用之前创建的相同密钥环。

3. 配置IPsec配置文件。

crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
模式隧道

crypto ipsec profile IPSEC-IKEV2

set transform-set T-SET
set ikev2-profile IKEV2-PROF

为IPsec隧道协商创建转换集，并在IPsec配置文件下调用转换集和Ikev2配置文件。

DMVPN 配置

1. 配置外部接口。

interface GigabitEthernet0/0/0

ip address 172.16.1.1 255.255.255.0
negotiation auto
cdp enable

2. 为mGRE和IPsec集成配置中心路由器（即，将隧道与在上一个过程中配置的IPsec配置文件相关联）

interface Tunnel0
ip address 10.10.10.1 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp redirect <--------在中心路由器上启用DMVPN第3阶段是必需的

tunnel source GigabitEthernet0/0/0
隧道模式gre多点
隧道保护ipsec配置文件IPSEC-IKEV2
!

以下命令用于隧道接口配置：

- ip nhrp authentication DMVPN:在这种情况下，“DMVPN”身份验证字符串在属于同一DMVPN网络的所有集线器和辐射点上必须具有相同的值。
- ip nhrp map multicast dynamic:允许NHRP向NHRP组播映射动态添加分支。
- ip nhrp network-id 1:在接口上启用NHRP的32位网络标识符。
- ip nhrp redirect:如果流量通过NHRP网络转发，则启用重定向流量指示。
- 隧道源GigabitEthernet0/0/0:设置隧道接口的源地址，此处您正在使用GigaEthernet 0/0/0 IP地址。
- 隧道模式gre multipoint:将此隧道接口的封装模式设置为mGRE。
- 隧道保护ipsec配置文件IPSEC-IKEV2:将隧道接口与已在加密配置中创建的IPsec配置文件关联。

3. 配置分支路由器以实现mGRE和IPsec集成，同时配置外部接口和环回以测试边界网关协议(BGP)连接。

辐射点X:（类似的配置可用于所有辐射点）

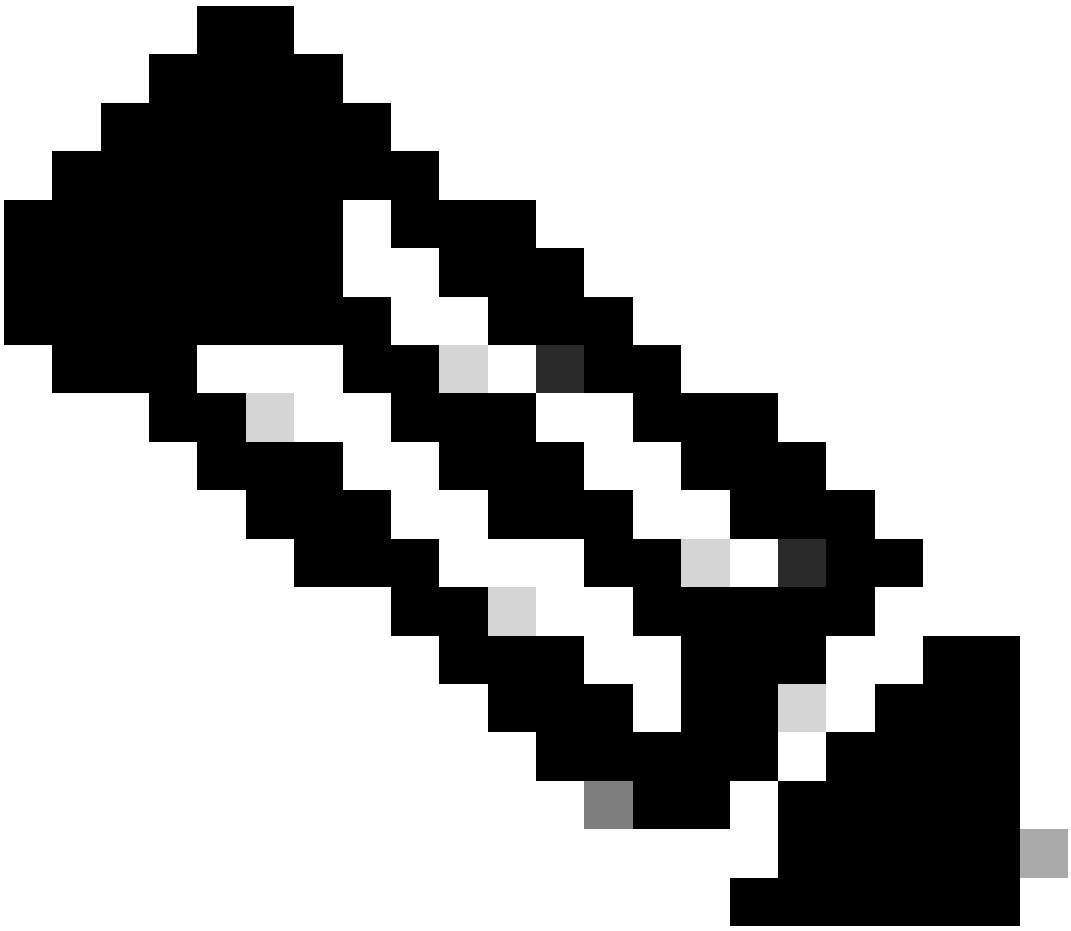
interface GigabitEthernet0/0/0
ip address 172.16.3.3 255.255.255.0
speed 1000
no negotiation auto

!

interface Loopback10
ip address 192.168.33.3 255.255.255.0
!
interface Tunnel0
ip address 10.10.10.3 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN
ip nhrp map 10.10.10.1 172.16.1.1
ip nhrp map multicast 172.16.1.1
ip nhrp network-id 1
ip nhrp nhs 10.10.10.1
ip nhrp shortcut <--------在分支路由器上启用DMVPN第3阶段是必需的
tunnel source GigabitEthernet0/0/0
隧道模式gre多点
隧道保护ipsec配置文件IPSEC-IKEV2

以下命令用于隧道接口配置：

- ip nhrp authentication DMVPN:在这种情况下，“DMVPN”身份验证字符串在属于同一DMVPN网络的所有集线器和辐射点上必须具有相同的值。
- ip nhrp map 10.10.10.1 172.16.1.1:手动将集线器NBMA IP地址与隧道接口IP地址映射。
- ip nhrp map multicast 172.16.1.1:将所有组播流量重定向到集线器。
- ip nhrp network-id 1:在接口上启用NHRP的32位网络标识符。
- ip nhrp nhs 10.10.10.1:使用此命令配置作为集线器的下一跳服务器。
- ip nhrp shortcut:在接口上启用NHRP快捷方式交换。
- 隧道源GigabitEthernet0/0/0:设置隧道接口的源地址，此处您正在使用GigaEthernet 0/0/0 IP地址。
- 隧道模式gre multipoint:将此隧道接口的封装模式设置为mGRE。
- 隧道保护ipsec配置文件IPSEC-IKEV2:将隧道接口与已在加密配置中创建的IPsec配置文件关联。



注意：ip nhrp redirect命令将消息发送到分支，消息中显示“有比通过集线器更好的路由到目标Spoke”，ip nhrp shortcut在分支的转发信息库(FIB)中强制安装此路由。

BGP配置

有多种变体可供选择：

- 每个分支上具有不同AS编号的eBGP
- 每个分支上具有相同AS编号的eBGP
- iBGP

解释所有三种场景均不在本文档的讨论范围之内。

在所有分支上配置了具有不同AS编号的eBGP，因此不能使用动态邻居。因此，您必须手动配置邻居。

辐射点上具有不同AS的eBGP

1. 集线器上的BGP配置：

Hub(config)#router bgp 65010

Hub(config-router)#bgp log-neighbor-changes

Hub(config-router)#network 192.168.11.1 mask 255.255.255.255

Hub(config-router)#neighbor 10.10.10.2 remote-as 65011

Hub(config-router)#neighbor 10.10.10.3 remote-as 65012

!

以下命令用于集线器上的BGP配置：

- router bgp 65010:配置BGP路由进程。使用向其他BGP扬声器标识设备的“autonomous-system-number”参数。
- 网络192.168.11.1掩码255.255.255.255:将网络指定为此自治系统的本地网络，并将其添加到BGP路由表。
- neighbor 10.10.10.2 remote-as 65011:将指定自治系统中邻居Spoke 1的IP地址添加到本地设备的IPv4多协议BGP邻居表。
- neighbor 10.10.10.3 remote-as 65012:将指定自治系统中邻居Spoke 2的IP地址添加到本地设备的IPv4多协议BGP邻居表。

2. 分支X上的BGP配置：

Spoke2(config)#router bgp 65012

Spoke2(config-router)#bgp log-neighbor-changes

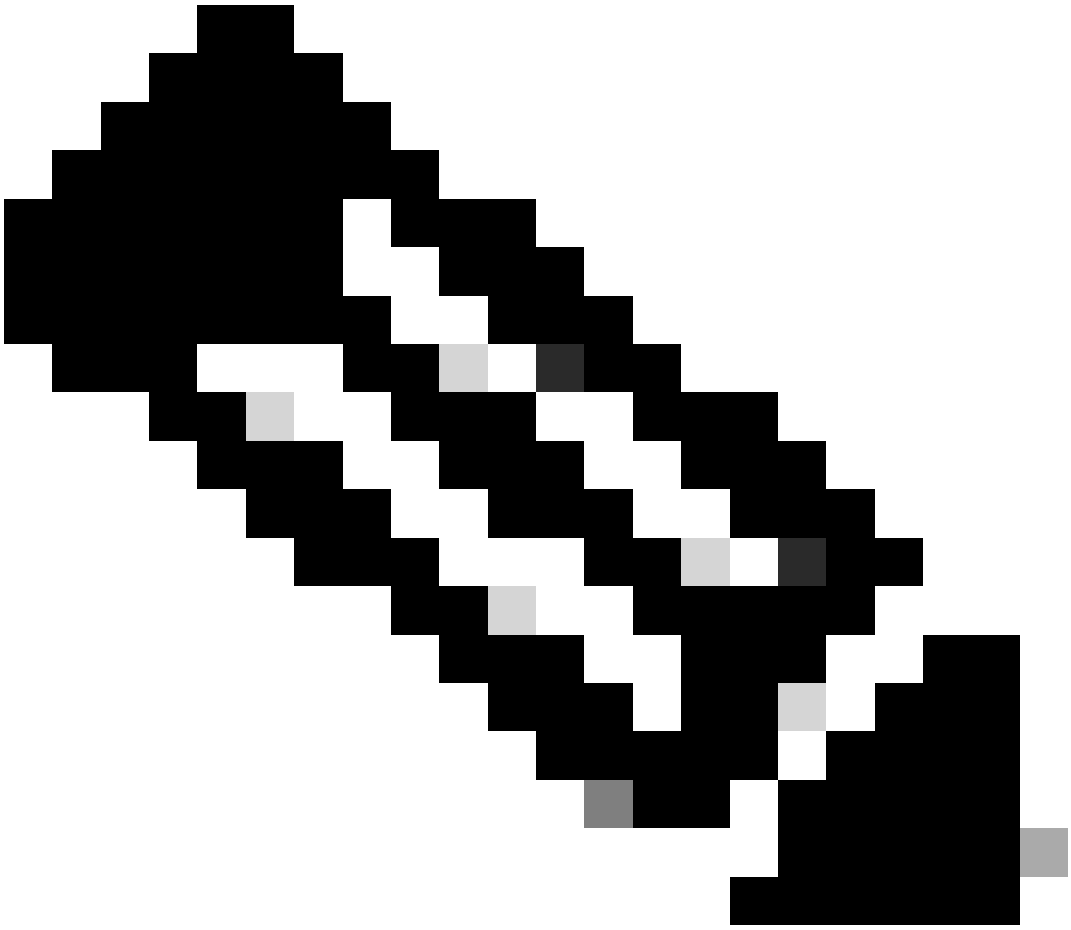
Spoke2(config-router)# network 192.168.33.3 mask 255.255.255

Spoke2(config-router)# neighbor 10.10.10.1 remote-as 65010

以下命令用于分支X上的BGP配置：

- router bgp 65012:配置BGP路由进程。使用向其他BGP扬声器标识设备的“autonomous-

system-number”参数。
- 网络192.168.33.3掩码255.255.255.255:将网络指定为此自治系统的本地网络，并将其添加到BGP路由表。
- neighbor 10.10.10.1 remote-as 65010:将指定自治系统中集线器的IP地址添加到本地设备的IPv4多协议BGP邻居表。



注意：必须在DMVPN网络中的所有分支上执行类似的配置。

验证

1. 集线器设备上的验证命令：

HUB#sh dmvpn

显示DMVPN特定会话信息。

说明：Attrb —> S — 静态，D — 动态，I — 不完整

N - NATed，L — 本地，X — 无套接字
T1 — 已安装路由，T2 — 下一跳覆盖
C — 支持CTS
Ent —>具有相同NBMA对等体的NHRP条目数
NHS状态：E —>期待回复，R —>回复，W —>等待
UpDn Time —>隧道的打开或关闭时间
==========

接口:Tunnel0、IPv4 NHRP详细信息
类型：集线器、NHRP对等点：2、<<<<<<<<<<<<<<<<<通知设备充当集线器，并且有两个NHRP对等点连接到此集线器。

#企业对等NBMA地址对等隧道添加状态UpDn Tm属性
----- --------------- --------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08 D <<<<<<<<<<<<<<<<<<<两个对等体都已动态注册到集线器，并且都处于UP状态。
1 172.16.3.3 10.10.10.3上升01:08:58

HUB#sh ip nhrp

显示连接到集线器的所有NHRP对等体的NBMA地址到隧道接口IP的映射。集线器维护所有辐射点的数据库。

经由 10.10.10.2 的 10.10.10.2/32
Tunnel0创建时间01:47:22，到期时间01:32:27
type：动态，标志：唯一注册的已使用nhop
NBMA地址：172.16.2.2
经由 10.10.10.3 的 10.10.10.3/32
Tunnel0创建时间01:09:11，到期时间01:29:58
type：动态，标志：唯一注册的已使用nhop
NBMA地址：172.16.3.3

HUB#sh ip nhrp multicast

显示NHRP组播映射信息。

I/F NBMA地址
Tunnel0 172.16.2.2标志：动态（已启用）
Tunnel0 172.16.3.3标志：动态（已启用）

HUB#sh crypto sockets

加密套接字连接数2

Tu0对等体（本地/远程）：172.16.1.1/172.16.2.2
本地标识（地址/掩码/端口/端口）：(172.16.1.1/255.255.255.255/0/47）
远程标识（地址/掩码/端口/端口）：(172.16.2.2/255.255.255.255/0/47）

IPSec 简档:"IPSEC-IKEV2"
套接字状态：Open（未解决）
客户端：“TUNNEL SEC”(客户端状态：活动)
Tu0对等体（本地/远程）：172.16.1.1/172.16.3.3
本地标识（地址/掩码/端口/端口）：(172.16.1.1/255.255.255.255/0/47）
远程标识（地址/掩码/端口/端口）：(172.16.3.3/255.255.255.255/0/47）
IPSec 简档:"IPSEC-IKEV2"
套接字状态：Open（未解决）
客户端：“TUNNEL SEC”(客户端状态：活动)
处于侦听状态的加密套接字：
客户端：“隧道安全”配置文件：“IPSEC-IKEV2”映射名称："Tunnel0-head-0"

HUB#sh cry ikev2 sa

IPv4加密IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.1/500 172.16.2.2/500 none/none就绪
加密：AES-CBC，密钥大小：256、PRF:SHA512，散列：SHA512,DH组：5，身份验证符号：PSK，身份验证验证：PSK
寿命/活动时间：86400/6524 秒

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.1.1/500 172.16.3.3/500 none/none就绪
加密：AES-CBC，密钥大小：256、PRF:SHA512，散列：SHA512,DH组：5，身份验证符号：PSK，身份验证验证：PSK
寿命/活动时间：86400/4234 秒

IPv6加密IKEv2 SA

HUB#sh ip bgp summary

显示BGP会话的当前状态/路由器从邻居或对等组接收的前缀数。

BGP路由器标识符192.168.11.1本地AS编号65010
BGP表版本为4，主路由表版本为4。
3个使用432字节内存的网络条目
3个使用252字节内存的路径条目
3/3使用480字节内存的BGP路径/最佳路径属性条目
2个使用48字节内存的BGP AS路径条目
0个使用0字节内存的BGP路由映射缓存条目
0个使用0字节内存的BGP过滤器列表缓存条目
使用1212总内存字节的BGP
BGP活动3/0前缀、3/0路径、扫描间隔60秒

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.2 4 65011 33 33 4 0 0 00:25:35 1
10.10.10.3 4 65012 21 25 4 0 0 00:14:58 1

Hub#sh ip route bgp

代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR、P — 定期下载的静态路由、H - NHRP、l - LISP
a — 应用路由
+ — 复制路由，% — 下一跳覆盖， p — 来自PfR的覆盖

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

192.168.0.0/16 is variably subnetted, 4 subnets, 2 masks
B 192.168.22.0/24 [20/0] via 10.10.10.2, 00:29:15 <<<<<<<<<<<<<分支1通告路由的条目
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<<分支2通告路由的条目

2. 分支1上的验证命令：

Spoke1#sh dmvpn

说明：Attrb —> S — 静态，D — 动态，I — 不完整
N - NATed，L — 本地，X — 无套接字
T1 — 已安装路由，T2 — 下一跳覆盖
C — 支持CTS，I2 — 临时
Ent —>具有相同NBMA对等体的NHRP条目数
NHS状态：E —>期待回复，R —>回复，W —>等待
UpDn Time —>隧道的打开或关闭时间
==========

接口:Tunnel0、IPv4 NHRP详细信息
类型：分支，NHRP对等体：2,

#企业对等NBMA地址对等隧道添加状态UpDn Tm属性
----- -------------- -------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:32:09 S <<<<<<<<<<Hub显示为S-static，因为我们已将其配置为隧道接口下的静态条目
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<将流量发送到分支2后创建的动态按需分支到分支隧道

Spoke1#sh ip bgp summary

BGP路由器标识符192.168.22.2，本地AS编号65011
BGP表版本为4，主路由表版本为4。
3个使用744字节内存的网络条目
3个使用432字节内存的路径条目

3/3使用864字节内存的BGP路径/最佳路径属性条目
2个使用64字节内存的BGP AS路径条目
0个使用0字节内存的BGP路由映射缓存条目
0个使用0字节内存的BGP过滤器列表缓存条目
使用2104总内存字节的BGP
BGP活动3/0前缀、3/0路径、扫描间隔60秒
3个网络在2022年6月2日08:16:54 UTC达到高峰（01:11:51.732之前）

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 4 65010 85 85 4 0 01:12:21 2 <<<<<<<<<<<<<<<<<我们已从集线器收到2个前缀，每个前缀用于集线器环回和Spoke2环回

Spoke1#sh ip route bgp

代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF外部类型1、E2 - OSPF外部类型2、m - OMP
n - NAT，Ni - NAT内部，No - NAT外部，Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP、G - NHRP注册、g - NHRP注册摘要
o - ODR、P — 定期下载的静态路由、l - LISP
a — 应用路由
+ — 复制路由，% — 下一跳覆盖， p — 来自PfR的覆盖

最后选用网关是172.16.2.10到网络0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.1, 01:13:16 >>>>>>>>>>>>>>通过集线器直接到达集线器网络

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 >>>>>>>>>>>>通过分支隧道IP直接到达分支网络。

Spoke1#sh ip route

代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF外部类型1、E2 - OSPF外部类型2、m - OMP
n - NAT，Ni - NAT内部，No - NAT外部，Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP、G - NHRP注册、g - NHRP注册摘要
o - ODR、P — 定期下载的静态路由、l - LISP
a — 应用路由
+ — 复制路由，% — 下一跳覆盖， p — 来自PfR的覆盖

最后选用网关是172.16.2.10到网络0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.10
172.16.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 172.16.2.0/24直接连接，GigabitEthernet2
L 172.16.2.2/32直接连接，GigabitEthernet2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24直接连接，Tunnel0
L 10.10.10.2/32直接连接，Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:21
192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.22.0/24直接连接，Loopback10
L 192.168.22.2/32直接连接，Loopback10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

说明：E=预期回复，R=响应，W=等待，D=动态
Tunnel0:
10.10.10.1 RE优先级= 0集群= 0 >>>>>>>>>仅配置一个下一跳服务器

Spoke1#sh ip nhrp traffic

Tunnel0:最大发送限制：10000数据包/10秒，使用率：0%
已发送：总计52
1解决请求0解决回复51注册请求<<<<<<<注册请求发送到集线器的次数
0注册回复0清除请求0清除回复
0错误指示0流量指示0重定向抑制
Rcvd:总计25
0 Resolution Request 1决议回复0注册请求<<<<<<<<我们收到对这些注册请求的回复的次数
24注册回复0清除请求0清除回复
0错误指示0流量指示0重定向抑制

Spoke1#sh ip nhrp multicast

I/F NBMA地址
Tunnel0 172.16.1.1标志：static(enabled)<<<<<<<<组播流量配置为转发到集线器NBMA

Spoke1#sh crypto sockets

加密套接字连接数2

Tu0对等体（本地/远程）：172.16.2.2/172.16.1.1
本地标识（地址/掩码/端口/端口）：(172.16.2.2/255.255.255.255/0/47）
远程标识（地址/掩码/端口/端口）：(172.16.1.1/255.255.255.255/0/47）

IPSec 简档:"IPSEC-IKEV2"
套接字状态：打开<<<<<<<<<<<<<<<<<<此对等设备的套接字状态
客户端：“TUNNEL SEC”(客户端状态：活动)
Tu0对等体（本地/远程）：172.16.2.2/172.16.3.3
本地标识（地址/掩码/端口/端口）：(172.16.2.2/255.255.255.255/0/47）
远程标识（地址/掩码/端口/端口）：(172.16.3.3/255.255.255.255/0/47）
IPSec 简档:"IPSEC-IKEV2"
套接字状态：Open（未解决）
客户端：“TUNNEL SEC”(客户端状态：活动)
处于侦听状态的加密套接字：
客户端：“隧道安全”配置文件：“IPSEC-IKEV2”映射名称："Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

IPv4加密IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.2.2/500 172.16.3.3/500 none/none就绪
加密：AES-CBC，密钥大小：256、PRF:SHA512，散列：SHA512,DH组：19，身份验证符号：PSK，身份验证验证：PSK
寿命/活动时间：86400/287 秒

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.2.2/500 172.16.1.1/500 none/none就绪
加密：AES-CBC，密钥大小：256、PRF:SHA512，散列：SHA512,DH组：19，身份验证符号：PSK，身份验证验证：PSK
寿命/活动时间：86400/4643 秒

IPv6加密IKEv2 SA

Spoke1#traceroute 192.168.33.3 source lo10

Type escape sequence to abort.
Tracing the route to 192.168.33.3
VRF信息：(vrf in name/id、vrf out name/id)
1 10.10.10.3 3毫秒4毫秒* <<<<<<<<<<<<流量直接流向辐条2路由器，而不通过集线器。

Spoke2#sh dmvpn

说明：Attrb —> S — 静态，D — 动态，I — 不完整
N - NATed，L — 本地，X — 无套接字
T1 — 已安装路由，T2 — 下一跳覆盖
C — 支持CTS，I2 — 临时
Ent —>具有相同NBMA对等体的NHRP条目数
NHS状态：E —>期待回复，R —>回复，W —>等待
UpDn Time —>隧道的打开或关闭时间
==========

接口:Tunnel0、IPv4 NHRP详细信息
类型：分支，NHRP对等体：2,

#企业对等NBMA地址对等隧道添加状态UpDn Tm属性
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1，南纬01:20:26
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. 分支2上的验证命令：

Spoke2#sh ip nhrp

经由 10.10.10.1 的 10.10.10.1/32
Tunnel0已创建01:36:06，永不过期
type：静态，标志：
NBMA地址：172.16.1.1
经由 10.10.10.2 的 10.10.10.2/32
Tunnel0创建时间00:08:09，到期时间00:01:50
type：动态，标志：路由器隐式
NBMA地址：172.16.2.2
经由 10.10.10.3 的 10.10.10.3/32
Tunnel0创建时间00:08:09，到期时间00:01:50
type：动态，标志：路由器唯一本地
NBMA地址：172.16.3.3
（无套接字）
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
I/F NBMA地址
Tunnel0 172.16.1.1标志：静态（已启用）
Spoke2#

Spoke2#sh crypto sockets

加密套接字连接数2

Tu0对等体（本地/远程）：172.16.3.3/172.16.1.1
本地标识（地址/掩码/端口/端口）：(172.16.3.3/255.255.255.255/0/47）
远程标识（地址/掩码/端口/端口）：(172.16.1.1/255.255.255.255/0/47）
IPSec 简档:"IPSEC-IKEV2"
套接字状态：打开<<<<<<<<<<<<<<<<<<<<<<<<<<<<此对等设备的套接字状态
客户端：“TUNNEL SEC”(客户端状态：活动)
Tu0对等体（本地/远程）：172.16.3.3/172.16.2.2
本地标识（地址/掩码/端口/端口）：(172.16.3.3/255.255.255.255/0/47）
远程标识（地址/掩码/端口/端口）：(172.16.2.2/255.255.255.255/0/47）
IPSec 简档:"IPSEC-IKEV2"
套接字状态：Open（未解决）
客户端：“TUNNEL SEC”(客户端状态：活动)

处于侦听状态的加密套接字：
客户端：“隧道安全”配置文件：“IPSEC-IKEV2”映射名称："Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

IPv4加密IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.3.3/500 172.16.2.2/500 none/none就绪
加密：AES-CBC，密钥大小：256、PRF:SHA512，散列：SHA512,DH组：19，身份验证符号：PSK，身份验证验证：PSK
寿命/活动时间：86400/509 秒

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.3.3/500 172.16.1.1/500 none/none就绪
加密：AES-CBC，密钥大小：256、PRF:SHA512，散列：SHA512,DH组：19，身份验证符号：PSK，身份验证验证：PSK
寿命/活动时间：86400/4866 秒

IPv6加密IKEv2 SA

Spoke2#sh ip bgp summary

BGP路由器标识符192.168.33.3，本地AS编号65012
BGP表版本为4，主路由表版本为4。
3个使用744字节内存的网络条目
3个使用432字节内存的路径条目
3/3使用864字节内存的BGP路径/最佳路径属性条目
2个使用64字节内存的BGP AS路径条目
0个使用0字节内存的BGP路由映射缓存条目
0个使用0字节内存的BGP过滤器列表缓存条目
使用2104总内存字节的BGP
BGP活动3/0前缀、3/0路径、扫描间隔60秒
3个网络在2022年6月2日08:16:54 UTC达到高峰（01:20:43.775之前）

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.1 465010 97 94 4 0 0 01:21:07 2 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>。我们从Hub收到2个前缀，每个前缀用于中心环回和Spoke2环回

Spoke2#sh ip route

代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF外部类型1、E2 - OSPF外部类型2、m - OMP
n - NAT，Ni - NAT内部，No - NAT外部，Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route

H - NHRP、G - NHRP注册、g - NHRP注册摘要
o - ODR、P — 定期下载的静态路由、l - LISP
a — 应用路由
+ — 复制路由，% — 下一跳覆盖， p — 来自PfR的覆盖

最后选用网关是172.16.3.10到网络0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.3.10
172.16.3.0/24/8 is variably subnetted, 2 subnets, 2 masks
C 172.16.3.0/24直接连接，GigabitEthernet3
L 172.16.3.3/32直接连接，GigabitEthernet3
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24直接连接，Tunnel0
L 10.10.10.3/32直接连接，Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:46:45
192.168.33.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.33.0/24直接连接，Loopback10
L 192.168.33.3/32直接连接，Loopback10

Spoke2#sh ip route bgp

代码：L — 本地，C — 连接，S — 静态，R - RIP，M — 移动，B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF外部类型1、E2 - OSPF外部类型2、m - OMP
n - NAT，Ni - NAT内部，No - NAT外部，Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP、G - NHRP注册、g - NHRP注册摘要
o - ODR、P — 定期下载的静态路由、l - LISP
a — 应用路由
+ — 复制路由，% — 下一跳覆盖， p — 来自PfR的覆盖

最后选用网关是172.16.3.10到网络0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.1, 01:21:11 >>>>>>>>>>>>>>>>>>通过集线器直接访问的集线器网络
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>>>通过分支隧道IP直接到达分支网络。

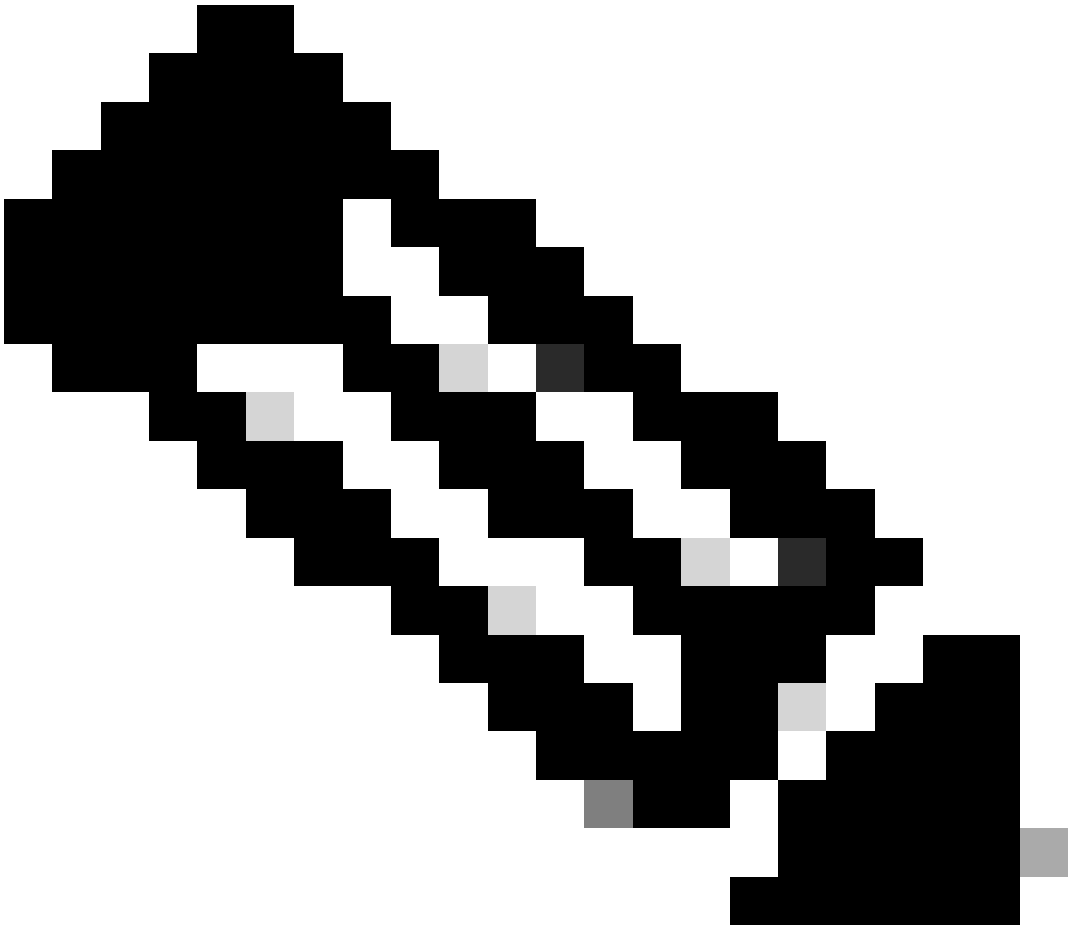
Spoke2#sh ip nhrp nhs

说明：E=预期回复，R=响应，W=等待，D=动态
Tunnel0:
10.10.10.1 RE优先级= 0集群= 0 >>>>>>>>>>>>>仅配置一个下一跳服务器

Spoke2#traceroute 192.168.22.2 source loopback 10

Type escape sequence to abort.
Tracing the route to 192.168.22.2
VRF信息：(vrf in name/id、vrf out name/id)
1 10.10.10.2 4毫秒4毫秒* <<<<<<<<<<<<流量直接流向辐条1路由器，而不通过集线器。

故障排除

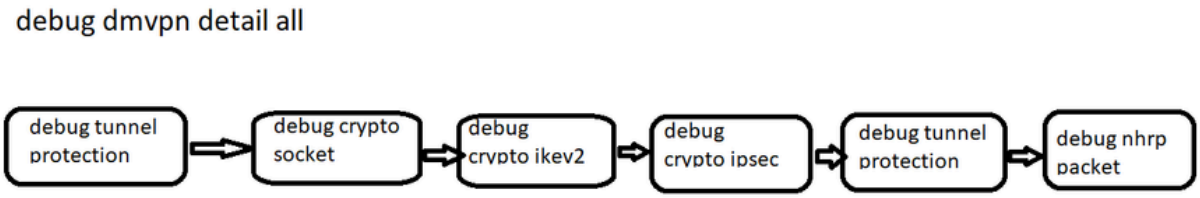


注意：始终建议使用条件调试，因为运行非条件调试可能会影响处理器，进而影响生产环境。NBMA地址对应于“外部IP地址”（用于提供隧道接口的IP地址），而隧道IP对应于“逻辑IP地址，即隧道接口的IP地址”。

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>
debug crypto condition peer ipv4 <对等体的WAN IP>

debug nhrp condition peer <nbma/tunnel> <NBMA or Tunnel IP address of Peer>

要对DMVPN进行故障排除，您必须采用分层方法：



1. 加密层：确认两个对等体之间的物理连接后，需要验证加密。此层加密/解密GRE数据包。

用于验证加密部分的常见Debug命令：

debug crypto condition peer ipv4 <WAN IP address of Peer>

debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

debug crypto ikev2 packet

debug crypto ipsec

debug crypto ipsec error

或者

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>

debug crypto condition peer ipv4 <对等体的WAN IP>

debug dmvpn detail crypto

要深入了解加密层故障排除，请参阅外部链接：

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html。

2. GRE/NHRP:一些常见问题包括NHRP注册失败以及分支中的动态NBMA地址更改，导致中心中的NHRP映射不一致。

用于验证NHRP映射的常见调试命令：

debug nhrp condition peer <nbma/tunnel> <NBMA or Tunnel IP address of Peer>

debug nhrp cache

debug nhrp packet

debug nhrp detail

debug nhrp error

要了解最常见的DMVPN故障排除解决方案，请参阅外部链接：

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html。

3. 路由：路由协议不监控按需辐射型隧道的状态。

IP路由更新和IP组播数据包仅通过集中星型隧道。

单播IP数据包通过中心辐射型和按需辐射型隧道。

调试:根据路由协议使用各种debug命令。

有关BGP路由的深入探讨，请参阅外部链路：

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。