設定BGP over DMVPN第3階段

目錄

簡介

本檔案介紹使用BGP的DMVPN第3階段的設定和運作，包括透過DMVPN通道進行的IPsec的分層疑難排解。

必要條件

對於本文檔中的配置和debug命令，您需要兩台運行Cisco IOS®版本15.3(3)M或更高版本的Cisco路由器。一般情況下，基本動態多點VPN(DMVPN)第3階段需要Cisco IOS版本12.4(6)T，不過不完全支援本文所述的功能和調試。

需求

思科建議您瞭解以下主題的基本知識：

- IKEV1/IKEV2和IPsec
- DMVPN元件：

- 下一個躍點解析通訊協定(NHRP):建立所有分支的隧道到實際（公共介面）地址的分散式(NHRP)對映資料庫
- 多點通用路由封裝(mGRE)通道介面:單個通用路由封裝(GRE)介面支援多個GRE/IPsec隧道

，簡化了配置的大小和複雜性，並支援動態隧道建立
- IPsec通道保護:動態建立並應用加密策略
- 路由:動態網路；幾乎所有路由協定(增強型內部網關路由協定(EIGRP)、路由資訊協定(RIP)、開放最短路徑優先(OSPF)、BGP、ODR)都受支援

採用元件

本文檔中的資訊基於Cisco ASR1000系列聚合服務路由器版本17.6.5(MD)。

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

背景資訊

什麼是DMVPN?

DMVPN是一種Cisco IOS軟體解決方案，用於輕鬆、動態和可擴展地構建IPsec+GRE VPN。這種解決方案無需靜態配置所有裝置，即可構建具有多個站點的VPN網路。它是「中心輻射型」網路，輻射型網路可以直接相互通訊，而無需經過中心。通過IPsec支援加密，因此DMVPN成為使用常規Internet連線連線不同站點的常用選擇。

DMVPN的工作原理？

- 輻條會建立到集線器的動態永久GRE/IPsec隧道，但不會建立到其他輻條的隧道。它們註冊為NHRP伺服器（集線器）的客戶端。
- 當分支需要將資料包傳送到另一個分支後面的目標（專用）子網時，它通過NHRP查詢目標分支的實際（外部）地址。
- 現在，始發分支可以發起到目標分支的動態GRE/IPsec隧道（因為它知道對等體地址）。
- 動態輻條到輻條隧道是通過mGRE介面構建的。
- 當流量停止時，將刪除分支到分支隧道。

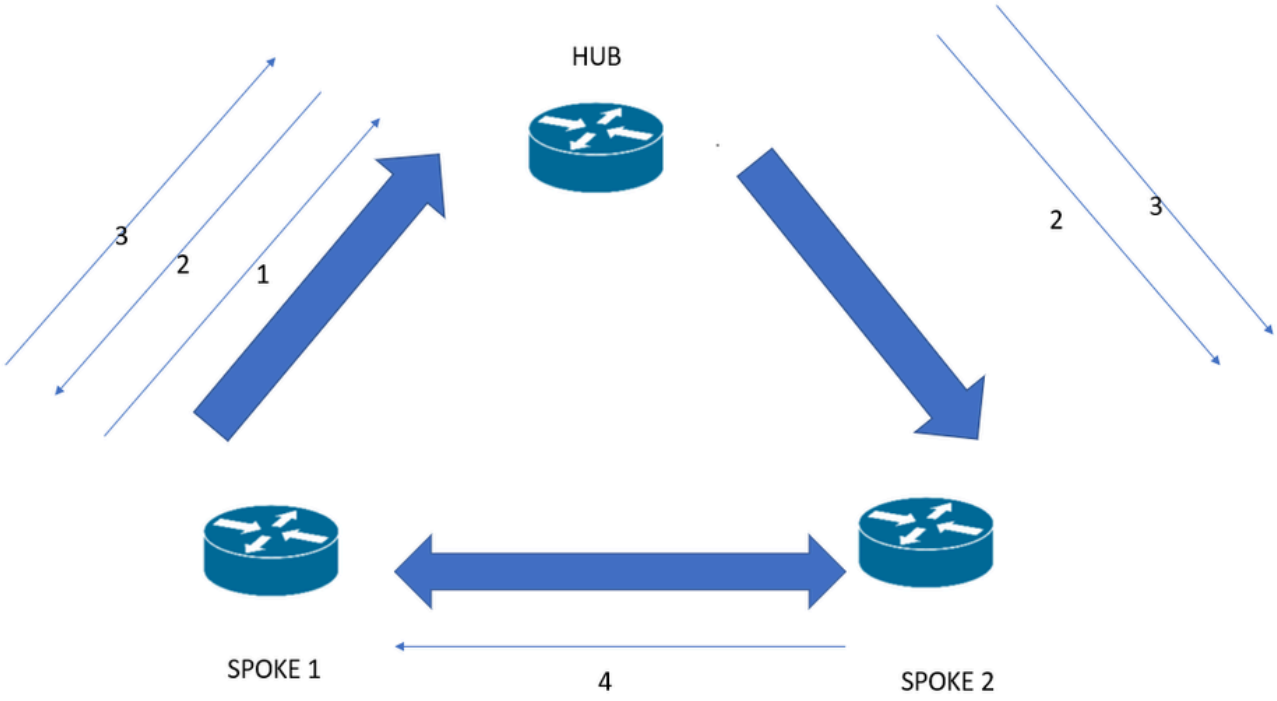
DMVPN有哪些不同型別？

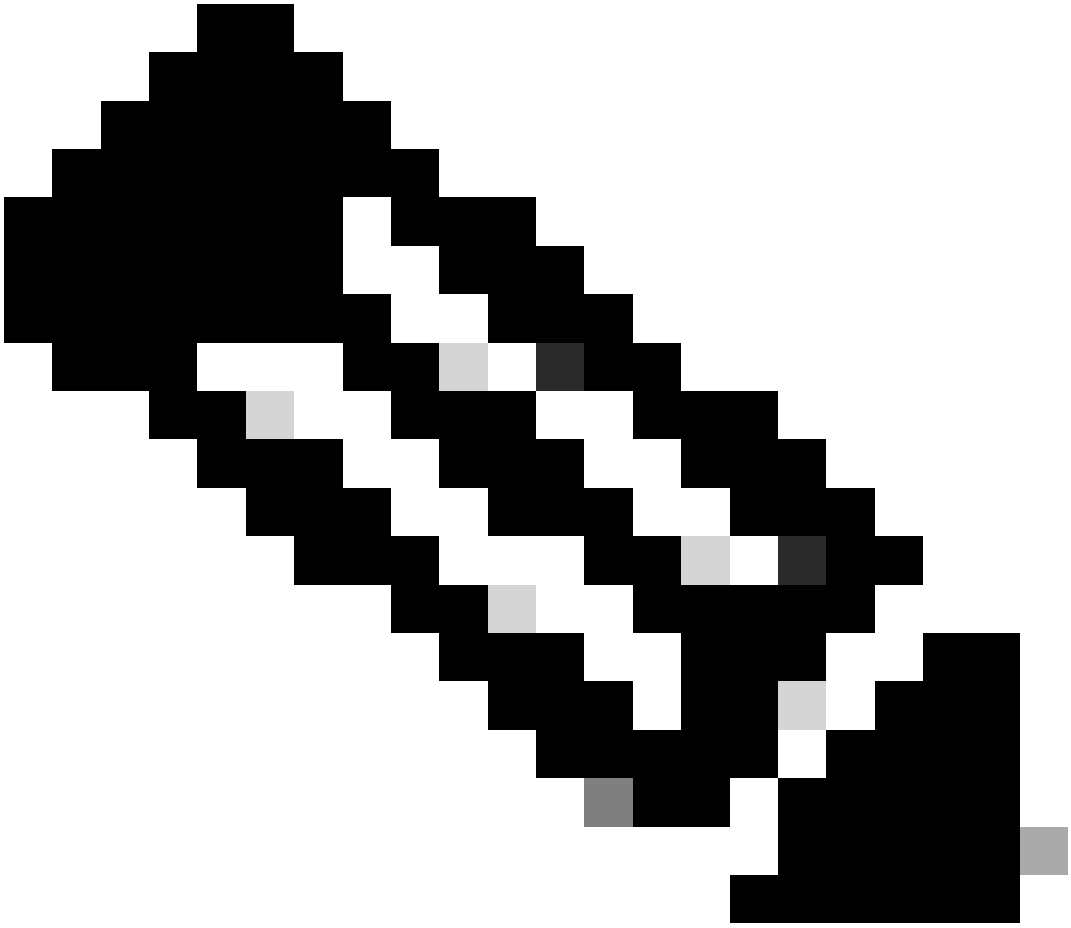
1. DMVPN第I階段:此階段涉及集線器上的單個mGRE介面，並且所有輻條仍是靜態隧道，因此您不會獲得任何動態輻條到輻條連線。
2. DMVPN第II階段:此階段涉及每個站點配置一個mGRE介面，以便您獲得動態輻條到輻條連線。
3. DMVPN第III階段：此階段擴展了DMVPN網路的可擴充性。這涉及總結到DMVPN雲。以及配置NHRP重定向和NHRP快捷方式交換。NHRP重新導向會告訴來源找到通向它嘗試到達的目的地的更好路徑。NHRP快捷方式允許DMVPN瞭解其他DMVPN路由器背後的其他網路。

DMVPN第3階段的流量

1. 資料包通過Hub（根據路由表）從Spoke的1個網路傳送到Spoke的2個網路。
2. 中心路由器將資料包路由到Spoke2，但並行將NHRP重定向消息傳送回Spoke1，該消息包含有關通往Spoke2的次優路徑以及Spoke2的隧道IP的資訊。

3. 然後，Spoke1向Spoke的2條隧道的目標IP為下一跳伺服器(NHS)發出Spoke的2個非廣播多路訪問(NBMA)IP地址的NHRP解析請求。此NHRP解析請求通過NHS以Spoke2為目標（根據路由表）傳送 — 這是一個普通的逐跳NHRP轉發過程。
4. Spoke2在收到包括Spoke1的NBMA IP的解析請求後，將NHRP解析應答直接傳送到Spoke1 - 應答不會遍歷中心！
5. Spoke1收到Spoke2的正確NBMA IP後，重寫目標字首的CEF條目 — 此過程稱為NHRP快捷方式。
6. 輻條不會通過收集鄰接觸發NHRP，但NHRP回覆會更新CEF。



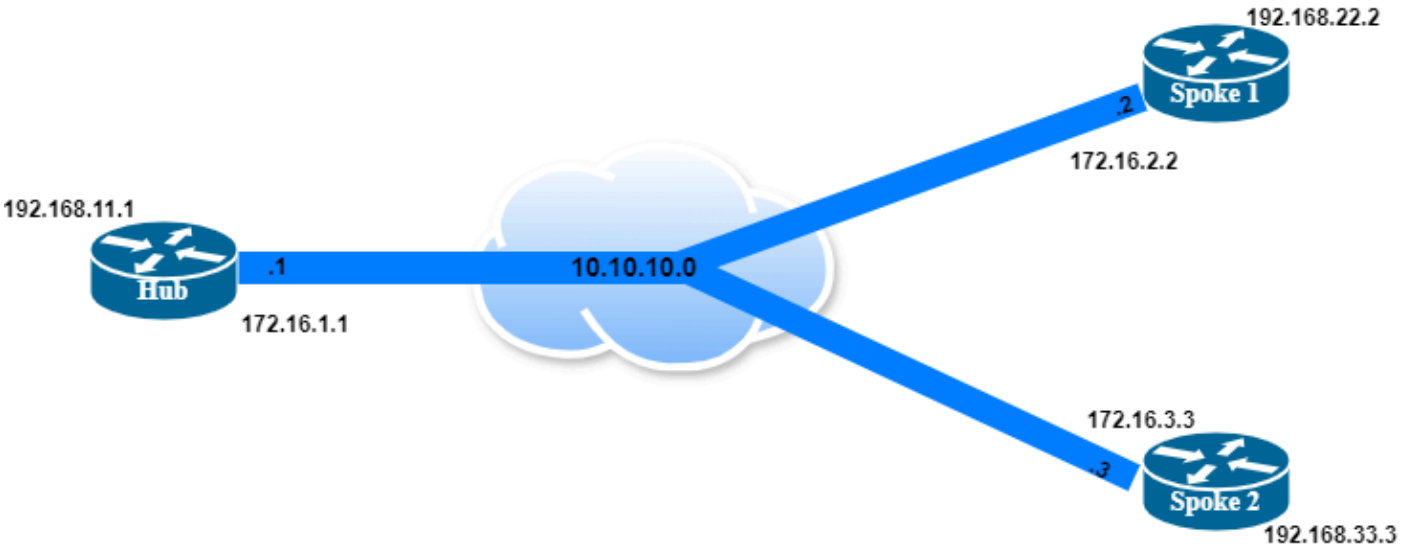


附註：

DMVPN第2階段:在這個階段，初始的輻條到輻條資料包確實是進程交換的，因為CEF鄰接處於'glean'狀態。這表示路由器沒有足夠的資訊來使用CEF轉送封包，且必須使用更為資源密集的處理序交換來使用NHRP（下一個躍點解析通訊協定）解析下一個躍點。

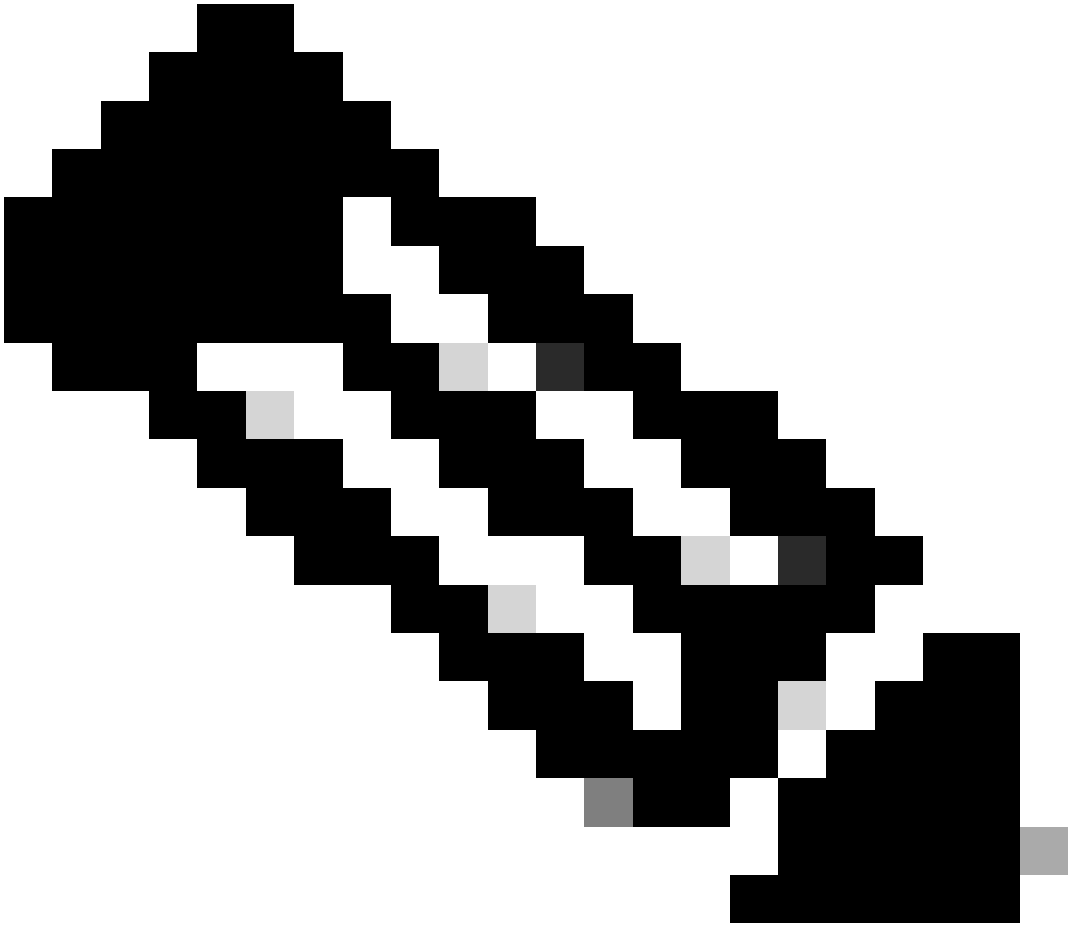
DMVPN第3階段:此階段在階段2的基礎上進行了改進，允許從開始使用CEF交換初始輻條到輻條資料包。這是通過使用NHRP重定向和NHRP快捷方式功能實現的，這些功能可幫助快速建立直接輻條到輻條隧道。因此，CEF的使用更加一致，減少對進程交換的依賴。

網路圖表


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

組態

加密配置



附註：集線器和所有輻條上都是相同的。

1. 配置Ikev2建議和金鑰環。

```
crypto ikev2 proposal DMVPN
加密aes-cbc-256
完整性sha256
組14
crypto ikev2 keyring IKEV2-KEYRING
peer any
地址0.0.0.0 0.0.0.0
預共用金鑰CISCO123
!
```

2. 配置包含所有連線相關資訊的Ikev2配置檔案。

```
crypto ikev2配置檔案IKEV2-PROF
```

match address local interface GigabitEthernet0/0/0
match identity remote address 0.0.0.0
身份驗證本地預共用
身份驗證遠端預共用
金鑰環本地IKEV2-KEYRING

以下是ikev2配置檔案中使用的命令的詳細資訊：

- match address local interface GigabitEthernet0/0/0:VPN終止的本地外部介面（在本例中為GigabitEthernet0/0/0）
- match identity remote address 0.0.0.0：由於遠端對等體可以是多個，因此使用0.0.0.0表示任何對等體
- 身份驗證本地預共用:本地站點上的身份驗證模式是預共用的
- 身份驗證遠端預共用:本地站點上的身份驗證模式是預共用的
- 金鑰環本地IKEV2-KEYRING:使用之前建立的相同金鑰環。

3. 配置IPsec配置檔案。

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

為IPsec隧道協商建立轉換集，並在IPsec配置檔案下呼叫轉換集和Ikev2配置檔案。

DMVPN配置

1. 配置外部介面。

interface GigabitEthernet0/0/0

ip address 172.16.1.1 255.255.255.0
自動交涉
cdp enable

2. 為mGRE和IPsec整合配置中心路由器（即，將隧道與在上一個過程中配置的IPsec配置檔案相關聯）

interface Tunnel0
ip address 10.10.10.1 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN
ip nhrp map組播動態
ip nhrp network-id 1
ip nhrp redirect <-------- Mandatory to enable DMVPN Phase 3 on Hub Router

隧道源GigabitEthernet0/0/0
通道模式gre多點
隧道保護ipsec配置檔案IPSEC-IKEV2
!

以下命令用於通道介面組態：

- ip nhrp authentication DMVPN:在這種情況下，「DMVPN」身份驗證字串在屬於同一DMVPN網路的所有集線器和輻條上必須具有相同的值。
- ip nhrp map multicast dynamic:允許NHRP向NHRP組播對映動態新增分支。
- ip nhrp network-id 1:在介面上啟用NHRP的32位網路識別符號。
- ip nhrp redirect:如果流量通過NHRP網路轉發，則啟用重定向流量指示。
- 隧道源GigabitEthernet0/0/0:設定隧道介面的源地址，此處您正在使用GigaEthernet 0/0/0 IP地址。
- 通道模式gre多點:為此通道介面將封裝模式設定為mGRE。
- 隧道保護ipsec配置檔案IPSEC-IKEV2:將通道介面與已在加密配置中建立的IPsec配置檔案相關聯。

3. 配置分支路由器以整合mGRE和IPsec以及外部介面和環回，以測試邊界網關協定(BGP)連線。

輻射點X:（所有輻條中均可使用類似的配置）

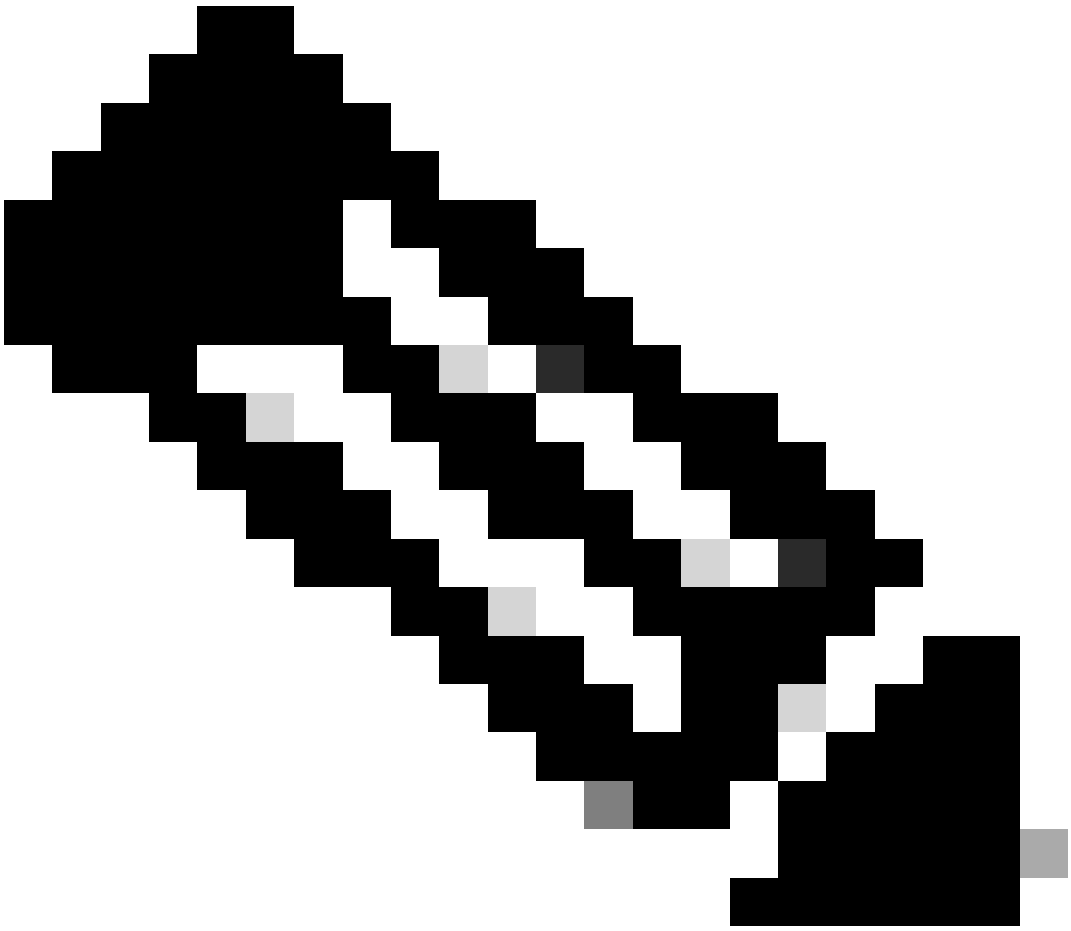
interface GigabitEthernet0/0/0
ip address 172.16.3.3 255.255.255.0
速度1000
no negotiation auto

!

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--------輻路由器上啟用DMVPN第3階段
隧道源GigabitEthernet0/0/0
通道模式gre多點
隧道保護ipsec配置檔案IPSEC-IKEV2

以下命令用於通道介面組態：

- ip nhrp authentication DMVPN:在這種情況下，「DMVPN」身份驗證字串在屬於同一DMVPN網路的所有集線器和輻條上必須具有相同的值。
- ip nhrp map 10.10.10.1 172.16.1.1:手動將集線器NBMA IP地址與隧道介面IP地址對映。
- ip nhrp map multicast 172.16.1.1:將所有組播流量重定向到集線器。
- ip nhrp network-id 1:在介面上啟用NHRP的32位網路識別符號。
- ip nhrp nhs 10.10.10.1:使用此命令配置作為中心伺服器的下一跳伺服器。
- ip nhrp快捷方式:在介面上啟用NHRP快捷方式交換。
- 隧道源GigabitEthernet0/0/0:設定隧道介面的源地址，此處您正在使用GigaEthernet 0/0/0 IP地址。
- 通道模式gre多點:為此通道介面將封裝模式設定為mGRE。
- 隧道保護ipsec配置檔案IPSEC-IKEV2:將通道介面與已在加密配置中建立的IPsec配置檔案相關聯。



附註：ip nhrp redirect命令將消息傳送到分支，該消息顯示「有比通過集線器更好的路由到目標分支」，ip nhrp快捷方式強制在分支上的轉發資訊庫(FIB)中安裝此路由。

BGP組態

有幾種變體可供選擇：

- 每個分支上具有不同AS編號的eBGP
- 每個分支上具有相同AS編號的eBGP
- iBGP

解釋所有三種情況均超出本檔案的範圍。

在所有輻條上配置了具有不同AS編號的eBGP，因此不能使用動態鄰居。因此，您必須手動配置鄰居。

輻射點上具有不同AS的eBGP

1. HUB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

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

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

!

以下命令用於集線器上的BGP配置中：

- 路由器bgp 65010:配置BGP路由進程。使用向其他BGP揚聲器標識裝置的「autonomous-system-number」引數。
- 網路192.168.11.1掩碼255.255.255.255:將網路指定為此自治系統的本地網路，並將其新增到BGP路由表中。
- neighbor 10.10.10.2 remote-as 65011:將指定自治系統中鄰居Spoke 1的IP地址新增到本地裝置的IPv4多協定BGP鄰居表中。
- neighbor 10.10.10.3 remote-as 65012:將指定自治系統中鄰居Spoke 2的IP地址新增到本地裝置的IPv4多協定BGP鄰居表中。

2. 分支X上的BGP配置：

Spoke2(config)#router bgp 65012

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

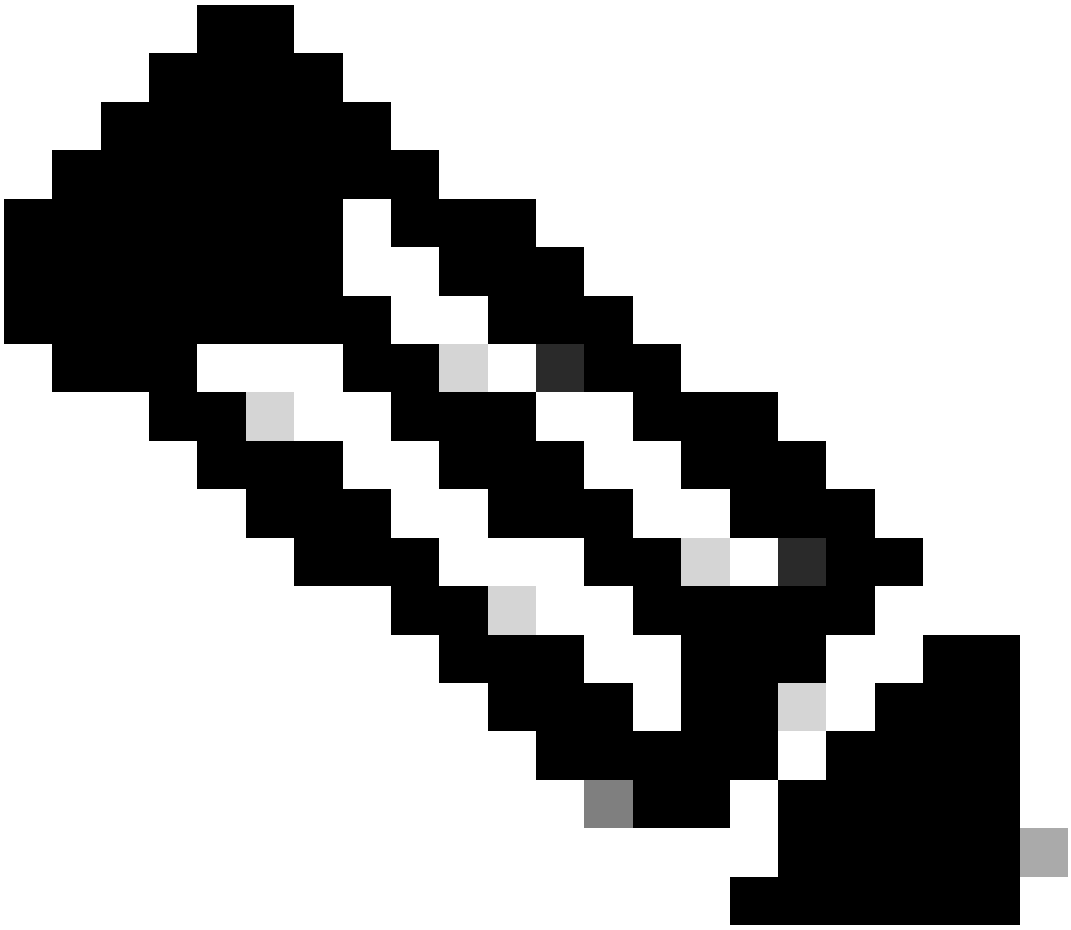
Spoke2(config-router)# network 192.168.33.3 mask 255.255.255

Spoke2(config-router)# neighbor 10.10.1 remote-as 65010

在分支X上的BGP配置中使用以下命令：

- 路由器bgp 65012:配置BGP路由進程。使用向其他BGP揚聲器標識裝置的「autonomous-

system-number」引數。
- 網路192.168.33.3掩碼255.255.255.255:將網路指定為此自治系統的本地網路，並將其新增到BGP路由表中。
- neighbor 10.10.1 remote-as 65010:將指定自治系統中集線器的IP地址新增到本地裝置的IPv4多協定BGP鄰居表。



附註：必須在DMVPN網路中的所有分支上執行類似的配置。

驗證

1. 集線器裝置上的驗證命令：

HUB#sh dmvpn

顯示DMVPN特定的會話資訊。

圖例：Attrb —> S — 靜態、D — 動態、I — 不完整

N - NATed，L — 本地，X — 無套接字
T1 — 已安裝路由，T2 — 下一跳覆蓋
C — 支援CTS
#企業 — >具有相同NBMA對等體的NHRP條目數
NHS狀態：E —>等待回覆，R —>響應，W —>等待
UpDn Time —>通道的開啟或關閉時間
==========

Interface:Tunnel0, IPv4 NHRP詳細資訊
鍵入：Hub， NHRP Peers:2, <<<<<<<<<<<<<<<<<<<<<<<<通知裝置充當集線器，並且有兩個NHRP對等體連線到此集線器。

#企業對等NBMA地址對等隧道新增狀態UpDn Tm屬性
----- --------------- --------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08 D <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<兩個對等體都已在集線器上動態註冊並處於UP狀態。
1 172.16.3.3 10.10.10.3 UP 01:08:58 D

HUB#sh ip nhrp

顯示連線到集線器的所有NHRP對等點的NBMA地址到隧道介面IP的對映。集線器維護所有輻條的資料庫。

通過10.10.10.2訪問10.10.10.2/32
Tunnel0建立時間01:47:22，終止時間01:32:27
Type:動態，標誌：唯一註冊已使用的nhop
NBMA地址：172.16.2.2
通過10.10.10.3訪問10.10.10.3/32
Tunnel0建立時間01:09:11，到期時間01:29:58
Type:動態，標誌：唯一註冊已使用的nhop
NBMA地址：172.16.3.3

HUB#sh ip nhrp multicast

顯示NHRP組播對映資訊。

I/F NBMA地址
Tunnel0 172.16.2.2標誌：動態（已啟用）
Tunnel0 172.16.3.3標誌：動態（已啟用）

HUB#sh加密套接字

加密套接字連線數2

Tu0 Peers（本地/遠端）：172.16.1.1/172.16.2.2
本地Ident(addr/mask/port/port):(172.16.1.1/255.255.255.255/0/47）
遠端標識(addr/mask/port/port):(172.16.2.2/255.255.255.255/0/47）

IPSec配置檔案："IPSEC-IKEV2"
套接字狀態：未解決
用戶端:"TUNNEL SEC"(使用者端狀態：活動)
Tu0 Peers（本地/遠端）：172.16.1.1/172.16.3.3
本地Ident(addr/mask/port/port):(172.16.1.1/255.255.255.255/0/47）
遠端標識(addr/mask/port/port):(172.16.3.3/255.255.255.255/0/47）
IPSec配置檔案："IPSEC-IKEV2"
套接字狀態：未解決
用戶端:"TUNNEL SEC"(使用者端狀態：活動)
處於偵聽狀態的加密套接字：
用戶端:"TUNNEL SEC"配置檔案：「IPSEC-IKEV2」對映名稱："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就緒
加密：AES-CBC，金鑰大小：256, PRF:SHA512，雜湊：SHA512,DH組：5，身份驗證符號：PSK，身份驗證驗證：PSK
壽命/活動時間：86400/6524秒

Tunnel-id Local Remote fvrf/ivrf Status
2 172.16.1.1/500 172.16.3.3/500無/無就緒
加密：AES-CBC，金鑰大小：256, PRF:SHA512，雜湊：SHA512,DH組：5，身份驗證符號：PSK，身份驗證驗證：PSK
壽命/活動時間：86400/4234秒

IPv6加密IKEv2 SA

HUB#sh ip bgp summary

顯示BGP會話的當前狀態/路由器從鄰居或對等組接收的字首數。

BGP路由器識別符號192.168.11.1本地AS編號65010
BGP表版本為4，主路由表版本為4。
3個使用432位元組記憶體的網路條目
3個使用252位元組記憶體的路徑條目
3/3使用480位元組記憶體的BGP路徑/bestpath屬性專案
2使用48位元組記憶體的BGP AS-PATH專案
0 BGP路由對映快取條目，使用0位元組的記憶體
0 BGP filter-list cache entries using 0 bytes of memory
BGP使用1212總記憶體位元組
BGP活動3/0字首、3/0路徑、掃描間隔60秒

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

Hub#sh ip route bgp

代碼：L — 本地， C — 連線， S — 靜態， R - RIP， M — 移動， B - BGP
D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF內部區域
N1 - OSPF NSSA外部型別1,N2 - OSPF NSSA外部型別2
E1 - OSPF外部型別1,E2 - OSPF外部型別2
i - IS-IS， su - IS-IS SUMMARY， L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS內部區域， * — 候選預設值， U — 每使用者靜態路由
o - ODR， P — 定期下載靜態路由， H - NHRP， l - LISP
a — 應用路由
+ — 複製路由，% — 下一跳覆蓋， p — 來自PfR的覆蓋

最後選用網關是172.16.1.2到網路0.0.0.0

192.168.0.0/16進行了可變子網劃分，4個子網，2個掩碼
B 192.168.22.0/24 [20/0] (通過10.10.10.2, 00:29:15) <<<<<<<<<<<<<<<<分支1通告的路由)
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<<<<<分支2通告的路由

2. 分支1上的驗證命令：

Spoke1#sh dmvpn

圖例：Attrb —> S — 靜態、D — 動態、I — 不完整
N - NATed，L — 本地，X — 無套接字
T1 — 已安裝路由，T2 — 下一跳覆蓋
C — 支援CTS，I2 — 臨時
#企業 — >具有相同NBMA對等體的NHRP條目數
NHS狀態：E —>等待回覆，R —>響應，W —>等待
UpDn Time —>通道的開啟或關閉時間
==========

Interface:Tunnel0, IPv4 NHRP詳細資訊
型別：分支，NHRP對等體：2,

#企業對等NBMA地址對等隧道新增狀態UpDn Tm屬性
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:32:09 S <<<<<<<<<<<<<集線器顯示為S-static，因為我們已將其配置為隧道介面下的靜態條目
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<< <將流量傳送到分支2後建立的動態按需分支到分支隧道

Spoke1#sh ip bgp summary

BGP路由器識別符號192.168.22.2，本地AS編號65011
BGP表版本為4，主路由表版本為4。
3個使用744位元組記憶體的網路條目
3個使用432位元組記憶體的路徑條目

3/3使用864位元組記憶體的BGP路徑/bestpath屬性專案
2使用64位元組記憶體的BGP AS-PATH專案
0 BGP路由對映快取條目，使用0位元組的記憶體
0 BGP filter-list cache entries using 0 bytes of memory
BGP使用2104總記憶體位元組
BGP活動3/0字首、3/0路徑、掃描間隔60秒
3個網路在2022年6月2日08:16:54 UTC達到高峰（01:11:51.732之前）

鄰居V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.1 4 65010 85 85 4 0 001:12:21 2 <<<<<<<<<<<<<<<<<<<<<<<<我們已從集線器收到2個字首，每個字首用於集線器環回和Spoke2環回

Spoke1#sh ip route bgp

代碼：L — 本地， C — 連線， S — 靜態， R - RIP， M — 移動， B - BGP
D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF內部區域
N1 - OSPF NSSA外部型別1,N2 - OSPF NSSA外部型別2
E1 - OSPF外部型別1,E2 - OSPF外部型別2,m - OMP
n - NAT，Ni - NAT內部，否 — 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內部區域， * — 候選預設值， U — 每使用者靜態路由
H - NHRP，G - NHRP註冊，g - NHRP註冊摘要
o - ODR， P — 定期下載靜態路由， l - LISP
a — 應用路由
+ — 複製路由，% — 下一跳覆蓋， p — 來自PfR的覆蓋

最後選用網關是172.16.2.10到網路0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.1, 01:13:16 >>>>>>>>>>>>>>通過集線器直接到達集線器網路

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 >>>>>>>>>>>>>>通過分支隧道IP直接到達分支網路。

Spoke1#sh ip route

代碼：L — 本地， C — 連線， S — 靜態， R - RIP， M — 移動， B - BGP
D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF內部區域
N1 - OSPF NSSA外部型別1,N2 - OSPF NSSA外部型別2
E1 - OSPF外部型別1,E2 - OSPF外部型別2,m - OMP
n - NAT，Ni - NAT內部，否 — 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內部區域， * — 候選預設值， U — 每使用者靜態路由
H - NHRP，G - NHRP註冊，g - NHRP註冊摘要
o - ODR， P — 定期下載靜態路由， l - LISP
a — 應用路由
+ — 複製路由，% — 下一跳覆蓋， p — 來自PfR的覆蓋

最後選用網關是172.16.2.10到網路0.0.0.0

S* 0.0.0.0/0 [1/0]（通過172.16.2.10）
172.16.2.0/24進行了可變子網劃分，2個子網，2個掩碼
C 172.16.2.0/24是直連的，GigabitEthernet2
L 172.16.2.2/32直接連線，GigabitEthernet2
10.0.0.0/8進行了可變子網劃分，2個子網，2個掩碼
C 10.10.10.0/24直接連線，Tunnel0
L 10.10.10.2/32直接連線，Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.1, 01:13:21
192.168.22.0/24進行了可變子網劃分，2個子網，2個掩碼
C 192.168.22.0/24直接連線，Loopback10
L 192.168.22.2/32直接連線，Loopback10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

圖例：E=Expected replies， R=Responding， W=Waiting， D=Dynamic
Tunnel0:
10.10.10.1 RE priority = 0 cluster = 0 >>>>>>>>>僅配置一個下一跳伺服器

Spoke1#sh ip nhrp traffic

Tunnel0:Max-send limit:10000Pkts/10Sec， Usage:0%
已傳送：總計52
1 Resolution Request 0 Resolution Reply 51 Registration Request <<<<<<<<註冊請求傳送到集線器的次數
0登記回覆0清除請求0清除回覆
0 Error Indication 0 Traffic Indication 0重定向抑制
Rcvd:總計25
0 Resolution Request 1 Resolution Reply 0 Registration Request <<<<<<<<<<我們收到對這些註冊請求的回覆的次數
24登記回覆0清除請求0清除回覆
0 Error Indication 0 Traffic Indication 0重定向抑制

Spoke1#sh ip nhrp multicast

I/F NBMA地址
Tunnel0 172.16.1.1標志：靜態（啟用）<<<<<<<<<<<組播流量配置為轉發到中心NBMA

Spoke1#sh crypto sockets

加密套接字連線數2

Tu0 Peers（本地/遠端）：172.16.2.2/172.16.1.1

本地Ident(addr/mask/port/port):(172.16.2.2/255.255.255.255/0/47）
遠端標識(addr/mask/port/port):(172.16.1.1/255.255.255.255/0/47）
IPSec配置檔案："IPSEC-IKEV2"
套接字狀態：開啟<<<<<<<<<<<<<<<<<<<<此特定對等點的套接字狀態
用戶端:"TUNNEL SEC"(使用者端狀態：活動)
Tu0 Peers（本地/遠端）：172.16.2.2/172.16.3.3
本地Ident(addr/mask/port/port):(172.16.2.2/255.255.255.255/0/47）
遠端標識(addr/mask/port/port):(172.16.3.3/255.255.255.255/0/47）
IPSec配置檔案："IPSEC-IKEV2"
套接字狀態：未解決
用戶端:"TUNNEL SEC"(使用者端狀態：活動)
處於偵聽狀態的加密套接字：
用戶端:"TUNNEL SEC"配置檔案：「IPSEC-IKEV2」對映名稱："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無/無就緒
加密：AES-CBC，金鑰大小：256, PRF:SHA512，雜湊：SHA512,DH組：19，身份驗證符號：PSK，身份驗證驗證：PSK
壽命/活動時間：86400/287秒

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.2.2/500 172.16.1.1/500 none/none就緒
加密：AES-CBC，金鑰大小：256, PRF:SHA512，雜湊：SHA512,DH組：19，身份驗證符號：PSK，身份驗證驗證：PSK
壽命/活動時間：86400/4643秒

IPv6加密IKEv2 SA

Spoke1#traceroute 192.168.33.3源lo10

鍵入要中止的轉義序列。
跟蹤到192.168.33.3的路由
VRF資訊：(vrf in name/id， vrf out name/id)
1 10.10.10.3 3 msec 4 msec * <<<<<<<<<<<<<流量直接流向分支2路由器，而不通過集線器。

Spoke2#sh dmvpn

圖例：Attrb —> S — 靜態、D — 動態、I — 不完整
N - NATed，L — 本地，X — 無套接字
T1 — 已安裝路由，T2 — 下一跳覆蓋
C — 支援CTS，I2 — 臨時
#企業 — >具有相同NBMA對等體的NHRP條目數
NHS狀態：E —>等待回覆，R —>響應，W —>等待

UpDn Time —>通道的開啟或關閉時間
==========

Interface:Tunnel0, IPv4 NHRP詳細資訊
型別：分支，NHRP對等體：2,

#企業對等NBMA地址對等隧道新增狀態UpDn Tm屬性
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1南緯01:20:26
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. 分支2上的驗證命令：

Spoke2#sh ip nhrp

通過10.10.10.1訪問10.10.10.1/32
Tunnel0建立時間01:36:06，永不過期
Type:靜態，標誌：
NBMA地址：172.16.1.1
通過10.10.10.2訪問10.10.10.2/32
Tunnel0建立時間00:08:09，到期時間00:01:50
Type:動態，標誌：router implicit
NBMA地址：172.16.2.2
通過10.10.10.3訪問10.10.10.3/32
Tunnel0建立時間00:08:09，到期時間00:01:50
Type:動態，標誌：路由器唯一本地
NBMA地址：172.16.3.3
（無套接字）
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
I/F NBMA地址
Tunnel0 172.16.1.1標誌：靜態（已啟用）
輻條2#

Spoke2#sh crypto sockets

加密套接字連線數2

Tu0 Peers（本地/遠端）：172.16.3.3/172.16.1.1
本地Ident(addr/mask/port/port):(172.16.3.3/255.255.255.255/0/47）
遠端標識(addr/mask/port/port):(172.16.1.1/255.255.255.255/0/47）
IPSec配置檔案："IPSEC-IKEV2"
套接字狀態：開啟<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<此特定對等點的套接字狀態
用戶端:"TUNNEL SEC"(使用者端狀態：活動)
Tu0 Peers（本地/遠端）：172.16.3.3/172.16.2.2
本地Ident(addr/mask/port/port):(172.16.3.3/255.255.255.255/0/47）
遠端標識(addr/mask/port/port):(172.16.2.2/255.255.255.255/0/47）

IPSec配置檔案："IPSEC-IKEV2"
套接字狀態：未解決
用戶端:"TUNNEL SEC"(使用者端狀態：活動)
處於偵聽狀態的加密套接字：
用戶端:"TUNNEL SEC"配置檔案：「IPSEC-IKEV2」對映名稱："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無/無就緒
加密：AES-CBC，金鑰大小：256, PRF:SHA512，雜湊：SHA512,DH組：19，身份驗證符號：PSK，身份驗證驗證：PSK
壽命/活動時間：86400/509秒

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.3.3/500 172.16.1.1/500 none/none就緒
加密：AES-CBC，金鑰大小：256, PRF:SHA512，雜湊：SHA512,DH組：19，身份驗證符號：PSK，身份驗證驗證：PSK
壽命/活動時間：86400/486秒

IPv6加密IKEv2 SA

Spoke2#sh ip bgp summary

BGP路由器識別符號192.168.33.3，本地AS編號65012
BGP表版本為4，主路由表版本為4。
3個使用744位元組記憶體的網路條目
3個使用432位元組記憶體的路徑條目
3/3使用864位元組記憶體的BGP路徑/bestpath屬性專案
2使用64位元組記憶體的BGP AS-PATH專案
0 BGP路由對映快取條目，使用0位元組的記憶體
0 BGP filter-list cache entries using 0 bytes of memory
BGP使用2104總記憶體位元組
BGP活動3/0字首、3/0路徑、掃描間隔60秒
3個網路在2022年6月2日08:16:54 UTC達到高峰（01:20:43.775前）

鄰居V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.1.1 465010 97 94 4 0 0 01:21:07 2 >>>>>>>>>>>>>>>>>>>>>>。我們已經從集線器收到2個字首，每個字首用於集線器環回和Spoke2環回

Spoke2#sh ip route

代碼：L — 本地， C — 連線， S — 靜態， R - RIP， M — 移動， B - BGP
D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF內部區域
N1 - OSPF NSSA外部型別1,N2 - OSPF NSSA外部型別2
E1 - OSPF外部型別1,E2 - OSPF外部型別2,m - OMP

n - NAT，Ni - NAT內部，否 — 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內部區域， * — 候選預設值， U — 每使用者靜態路由
H - NHRP，G - NHRP註冊，g - NHRP註冊摘要
o - ODR， P — 定期下載靜態路由， l - LISP
a — 應用路由
+ — 複製路由，% — 下一跳覆蓋， p — 來自PfR的覆蓋

最後選用網關是172.16.3.10到網路0.0.0.0

S* 0.0.0.0/0 [1/0]（通過172.16.3.10）
172.16.3.0/24/8進行了可變子網劃分，2個子網，2個掩碼
C 172.16.3.0/24直接連線，GigabitEthernet3
L 172.16.3.3/32直接連線，GigabitEthernet3
10.0.0.0/8進行了可變子網劃分，2個子網，2個掩碼
C 10.10.10.0/24直接連線，Tunnel0
L 10.10.10.3/32直接連線，Tunnel0
B 192.168.11.0/24 [20/0] via 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進行了可變子網劃分，2個子網，2個掩碼
C 192.168.33.0/24直接連線，Loopback10
L 192.168.33.3/32直接連線，Loopback10

Spoke2#sh ip route bgp

代碼：L — 本地， C — 連線， S — 靜態， R - RIP， M — 移動， B - BGP
D - EIGRP、EX - EIGRP外部、O - OSPF、IA - OSPF內部區域
N1 - OSPF NSSA外部型別1,N2 - OSPF NSSA外部型別2
E1 - OSPF外部型別1,E2 - OSPF外部型別2,m - OMP
n - NAT，Ni - NAT內部，否 — 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內部區域， * — 候選預設值， U — 每使用者靜態路由
H - NHRP，G - NHRP註冊，g - NHRP註冊摘要
o - ODR， P — 定期下載靜態路由， l - LISP
a — 應用路由
+ — 複製路由，% — 下一跳覆蓋， p — 來自PfR的覆蓋

最後選用網關是172.16.3.10到網路0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.1, 01:21:11 >>>>>>>>>>>>>>>>>>通過集線器直接訪問的集線器網路
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>>>>通過分支隧道IP直接到達分支網路。

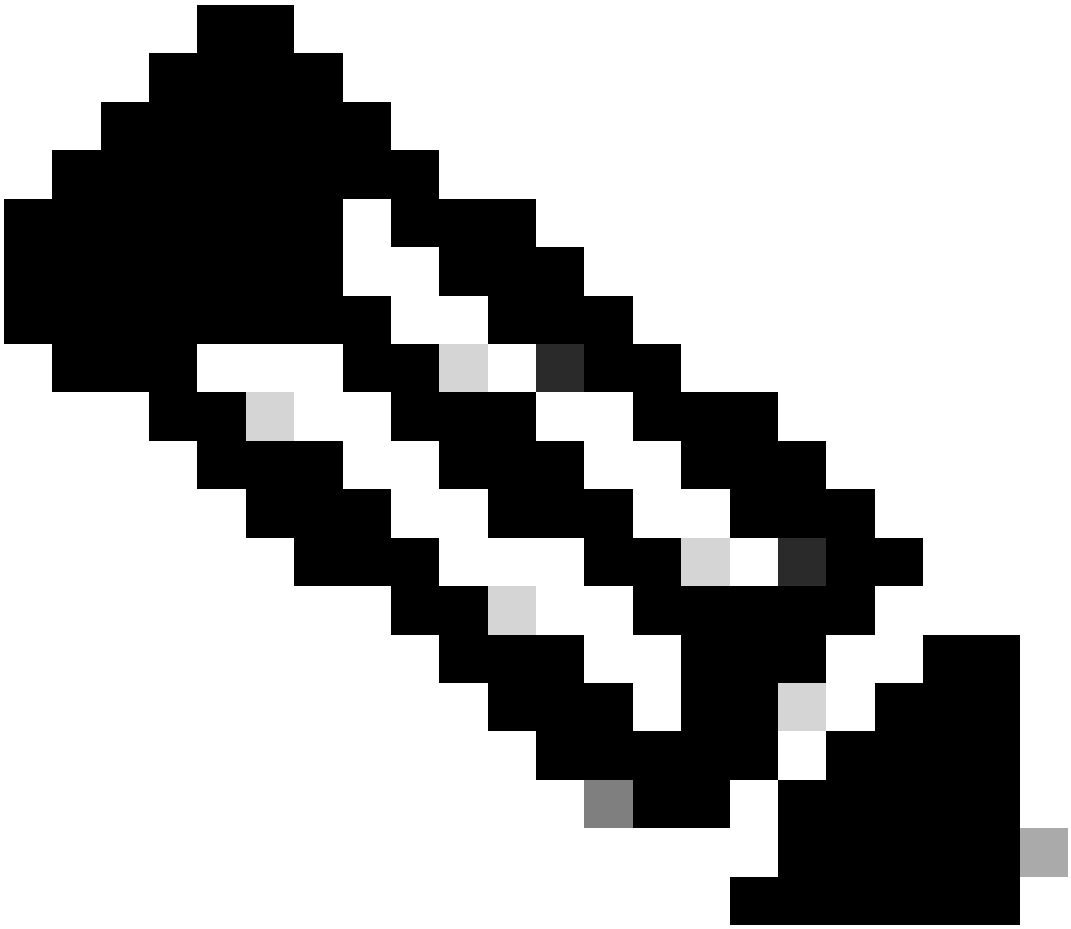
Spoke2#sh ip nhrp nhs

圖例：E=Expected replies， R=Responding， W=Waiting， D=Dynamic
Tunnel0:
10.10.10.1 RE優先順序= 0集群= 0 >>>>>>>>>>>>>僅配置一個下一跳伺服器

Spoke2#traceroute 192.168.22.2來源回送10

鍵入要中止的轉義序列。
跟蹤到192.168.22.2的路由
VRF資訊：(vrf in name/id， vrf out name/id)
1 10.10.10.2 4 msec 4 msec * <<<<<<<<<<<<<流量直接流向輻條1路由器，而不通過集線器。

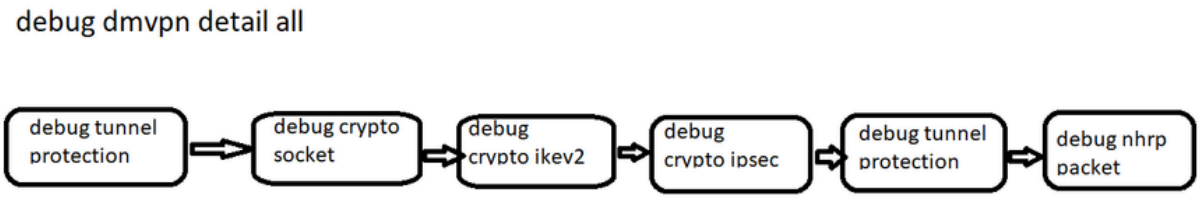
疑難排解



附註：建議始終使用條件調試，因為運行非條件調試可能會影響處理器，從而影響生產環境。NBMA位址對應於「外部IP位址」（用於來源通道介面的IP位址），而通道IP對應於「邏輯IP位址，也就是通道介面的IP位址」。

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>
debug crypto condition peer ipv4 <對等體的WAN IP>
debug nhrp condition peer <nbma/tunnel> <NBMA or Tunnel IP address of Peer>

為了對DMVPN進行故障排除，您必須採用分層方法：



1. 加密層：確認兩個對等體之間的物理連線後，需要驗證加密。此層加密/解密GRE資料包。

用於驗證加密部分的常見Debug命令：

debug crypto condition peer ipv4 <對等體的WAN IP地址>

debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

debug crypto ikev2 packet

debug crypto ipsec

debug crypto ipsec error

或

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

debug crypto condition peer ipv4 <對等體的WAN IP>

debug dmvpn detail crypto

要深入瞭解加密層故障排除，請參閱外部連結：

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

2. GRE/NHRP:一些常見問題包括NHRP註冊失敗以及輻條中動態NBMA地址更改，導致中心點中的NHRP對映不一致。

用於驗證NHRP對映的常見Debug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

要瞭解最常見的DMVPN故障排除解決方案，請參閱外部連結：

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

3. 路由：路由協定不監控按需輻射型通道的狀態。

IP路由更新和IP組播資料包僅通過星型隧道。

單播IP資料包同時通過中心輻射型和按需輻射型隧道。

調試：根據路由協定的不同，有不同的debug命令。

有關BGP路由的深入探討，請參閱外部連結：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。