# DMVPNフェーズ3でのBGPの設定

## 内容



## はじめに

このドキュメントでは、IPsec over DMVPNトンネルの階層型トラブルシューティングを含め、BGPを使用したDMVPNフェーズ3の設定と動作について説明します。

## 前提条件

このドキュメントの設定コマンドとdebugコマンドを実行するには、Cisco IOS®リリース15.3(3)M以降が稼働している2台のCiscoルータが必要です。一般に、基本的なDynamic Multipoint VPN(DMVPN)フェーズ3にはCisco IOSリリース12.4(6)Tが必要ですが、このドキュメントに記載されている機能とデバッグは完全にはサポートされていません。

### 要件

次の項目に関する基本的な知識が推奨されます。

- IKEV1/IKEV2およびIPsec
- DMVPNコンポーネント：

- Next Hop Resolution Protocol(NHRP)：スポークのすべてのトンネルから実際の（パブリックインターフェイス）アドレスへの分散(NHRP)マッピングデータベースを作成します。

- Multipoint Generic Routing Encapsulation(mGRE)トンネルインターフェイス：複数のGRE/IPsecトンネルをサポートする単一の総称ルーティングカプセル化(GRE)インターフェイスにより、設定のサイズと複雑さが簡素化され、ダイナミックトンネルの作成がサポートされます。
- IPSecトンネル保護：暗号化ポリシーを動的に作成して適用
- ルーティング：ダイナミックネットワーク。ほぼすべてのルーティングプロトコル(Enhanced Interior Gateway Routing Protocol(EIGRP)、Routing Information Protocol(RIP)、Open Shortest Path First(OSPF)、BGP、ODR)がサポートされています。

### 使用するコンポーネント

このドキュメントの情報は、Cisco ASR1000シリーズアグリゲーションサービスルータ、バージョン17.6.5(MD)に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

### DMVPNとは

DMVPNは、IPsec+GRE VPNを簡単、動的、スケーラブルに構築するためのCisco IOSソフトウェアソリューションです。すべてのデバイスを静的に設定することなく、複数のサイトを持つVPNネットワークを構築するソリューションです。これは、スポークがハブを経由せずに相互に直接通信できる「ハブアンドスポーク」ネットワークです。暗号化はIPSecを介してサポートされるため、通常のインターネット接続を使用して異なるサイトに接続する場合は、DMVPNが一般的な選択肢となります。

### DMVPNの仕組み

- スポークはハブへのダイナミックな永続的GRE/IPsecトンネルを構築しますが、他のスポークへのトンネルは構築しません。NHRPサーバ（ハブ）のクライアントとして登録する
- スポークが別のスポークの背後にある宛先（プライベート）サブネットにパケットを送信する必要がある場合、NHRP経由で宛先スポークの実際の（外部）アドレスを照会します。
- この時点で、発信側スポークはターゲットスポークへのダイナミックGRE/IPsecトンネルを開始できます（ピアアドレスを認識しているため）。
- 動的なスポーク間トンネルは、mGREインターフェイス上に構築されます。
- トラフィックが停止すると、スポーク間トンネルは削除されます。

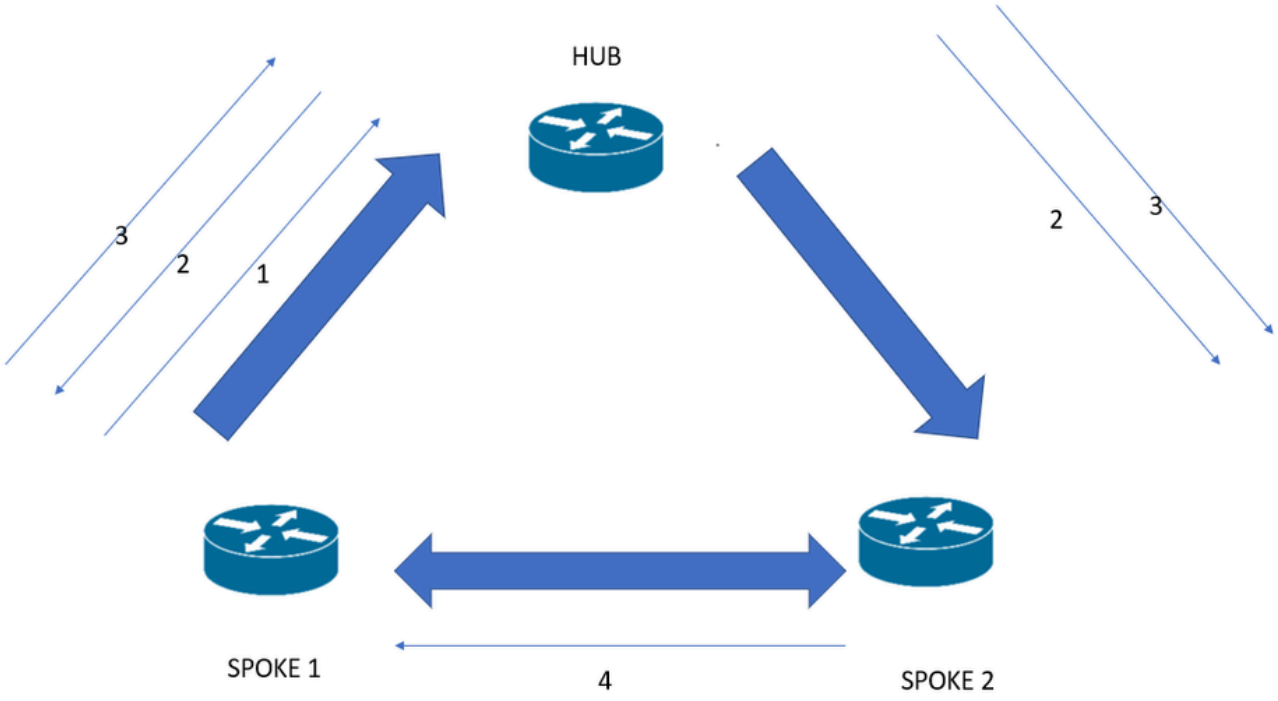
### DMVPNのタイプにはどのようなものがありますか。

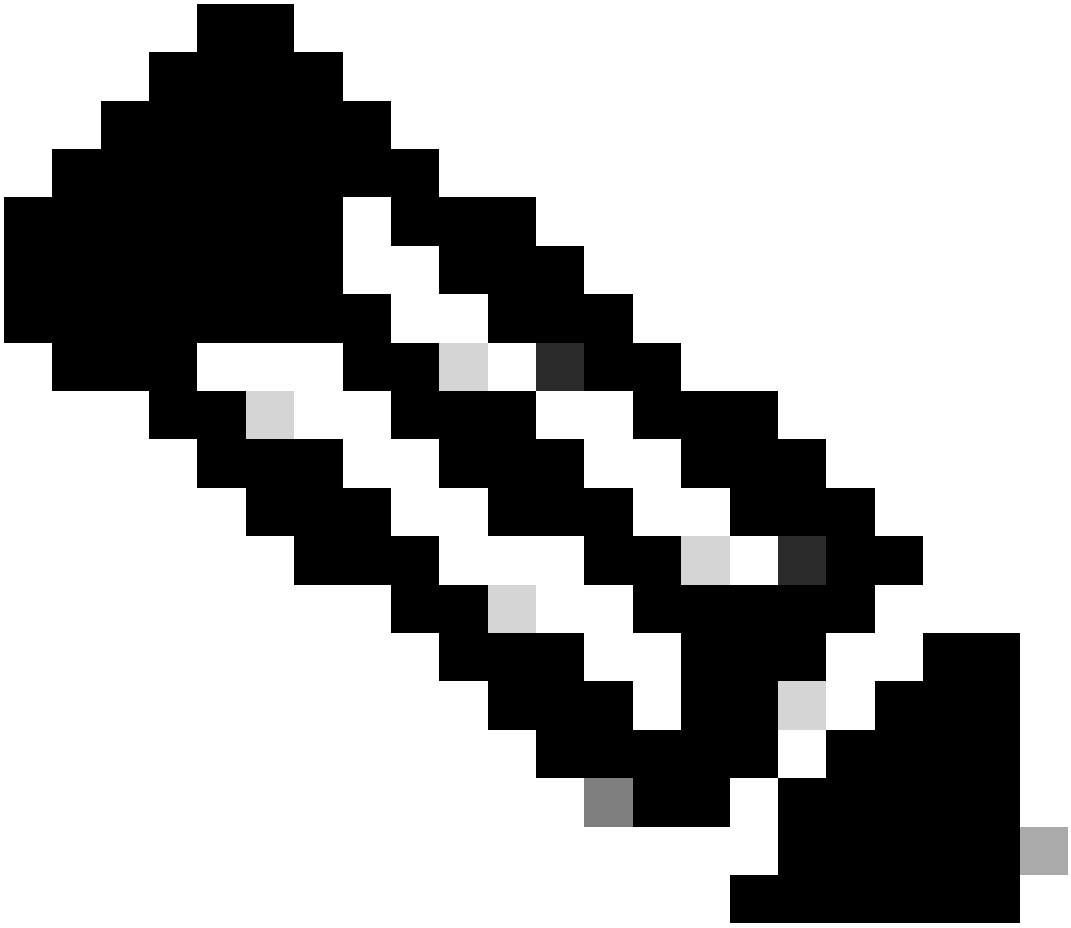
1. DMVPNフェーズI：このフェーズでは、ハブ上の単一のmGREインターフェイスが使用され、すべてのスポークはまだスタティックトンネルであるため、スポーク間で動的な接続を取得することはできません。

2. DMVPNフェーズII：このフェーズでは、動的なスポーク間接続を取得できるように、mGREインターフェイスを使用して設定されているすべてのサイトが含まれます。
3. DMVPNフェーズIII：このフェーズは、DMVPNネットワークのスケーラビリティをさらに拡大します。これには、DMVPNクラウドへの集約が含まれます。NHRPリダイレクトおよびNHRPショートカットスイッチングの設定に加えて、NHRPリダイレクトは、到達しようとしている宛先へのより良いパスを見つけるように送信元に指示します。NHRPショートカットを使用すると、DMVPNは、他のDMVPNルータの背後にある他のネットワークについて学習できます。

## DMVPNフェーズ3のトラフィックフロー

1. パケットは、ハブを介してスポーク1のネットワークからスポーク2のネットワークに送信されます（ルーティングテーブルに従います）。
2. ハブはパケットをSpoke2にルーティングしますが、Spoke2への最適でないパスとSpoke2のトンネルIPに関する情報を含むNHRPリダイレクトメッセージをSpoke1に同時に返信します。
3. 次に、Spoke1は、Spokeの2つのNonbroadcast Multiaccess(NBMA)IPアドレスのNHRP解決要求を、Spokeの2つのトンネルの宛先IPを使用して、ネクストホップサーバ(NHS)に発行します。このNHRP解決要求は、NHS経由でSpoke2に送信されます（ルーティングテーブルに従います）。これは通常のホップバイホップNHRP転送プロセスです。
4. Spoke1のNBMA IPを含む解決要求を受信した後、Spoke2はNHRP解決応答をSpoke1に直接送信：応答はハブを通過しない
5. Spoke2の正しいNBMA IPを受信した後、Spoke1は宛先プレフィックスのCEFエントリを書き換えます。この手順はNHRPショートカットと呼ばれます。
6. スポークは隣接関係を取得することによってNHRPをトリガーしませんが、NHRP応答はCEFを更新します。



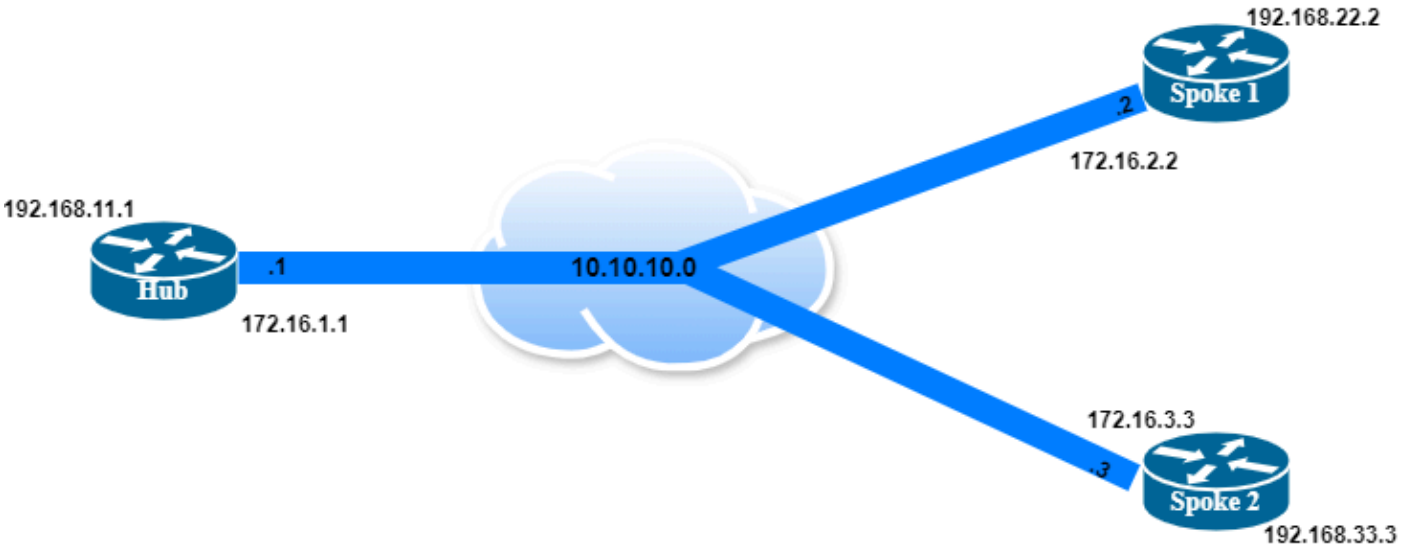


注：

DMVPNフェーズ2：このフェーズでは、CEF隣接関係が「グリーニング」状態であるため、最初のスポーク間パケットは実際にプロセススイッチングされます。つまり、ルータにはCEFを使用してパケットを転送するための十分な情報がないため、NHRP(Next Hop Resolution Protocol)を使用してネクストホップを解決するために、よりリソースの多いプロセススイッチングを使用する必要があります。

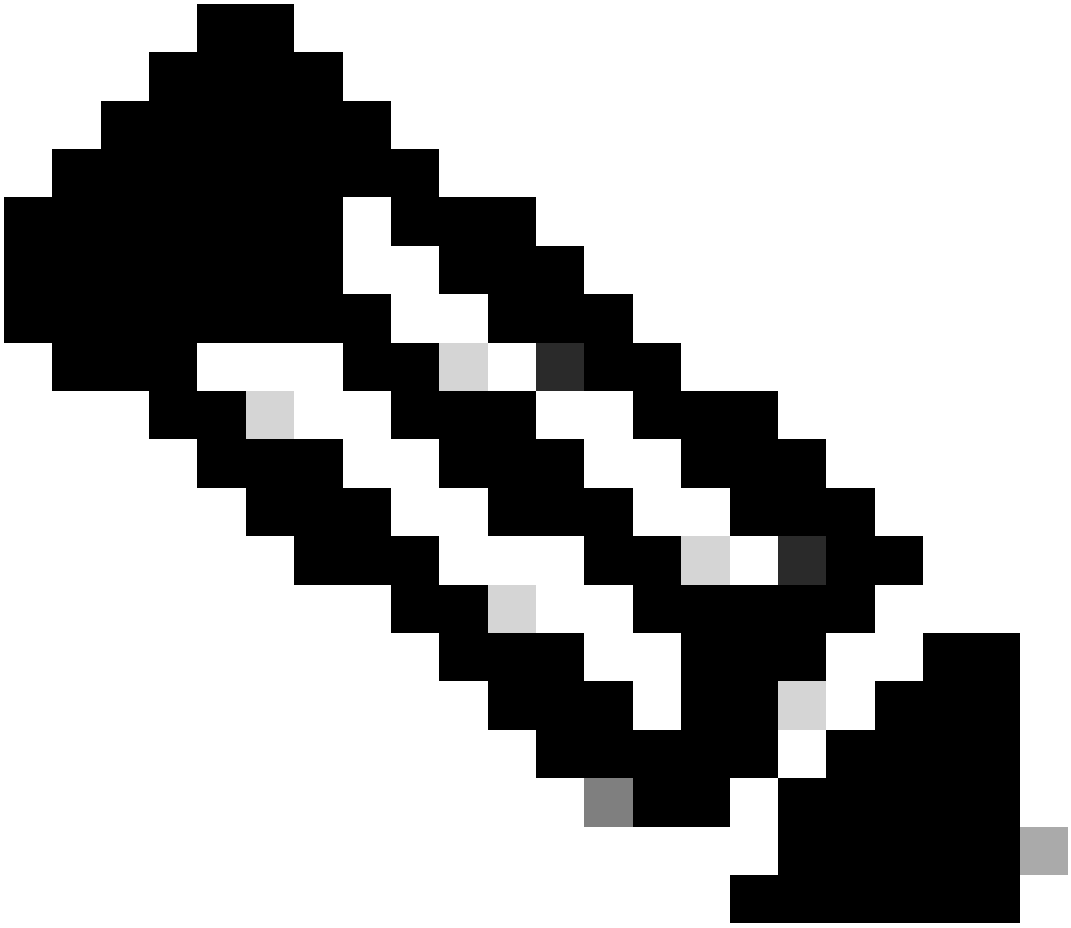
DMVPNフェーズ3：このフェーズは、フェーズ2で改善され、最初からCEFを使用してスポークツースポークパケットをスイッチングできるようになっています。これは、直接のスポークツースポークトンネルを迅速に確立するのに役立つNHRPリダイレクトおよびNHRPショートカット機能を使用して実現されます。その結果、CEFはより一貫して使用され、プロセススイッチングへの依存が軽減されます。

## ネットワーク図




# コンフィギュレーション

暗号設定



注：これはハブ上でも、すべてのスポーク上でも同じです。

1. Ikev2プロポーザルとキーリングを設定します。

```
crypto ikev2プロポーザルDMVPN
encryption aes-cbc-256
整合性sha256
group 14
crypto ikev2 keyring IKEV2-KEYRING
ピアany
アドレス0.0.0.0 0.0.0.0
事前共有キーCISCO123
!
```

2. すべての接続関連情報を含むIkev2プロファイルを設定します。

```
crypto ikev2プロファイルIKEV2-PROF
```

一致アドレスローカルインターフェイスGigabitEthernet0/0/0
idリモートアドレス0.0.0.0と一致
認証ローカル事前共有
認証リモート事前共有
キーリングローカルIKEV2-KEYRING

ikev2プロファイルで使用されるコマンドの詳細を次に示します。

- match address local interface GigabitEthernet0/0/0:VPNが終端するローカル外部インターフェイス（この場合はGigabitEthernet0/0/0）
- match identity remote address 0.0.0.0：リモートピアは複数にすることができるため、すべてのピアを示す0.0.0.0を使用します
- authentication local pre-share：ローカルサイトの認証モードは事前共有されます
- 認証リモート事前共有：ローカルサイトの認証モードは事前共有されます
- keyring local IKEV2-KEYRING：前に作成したキーリングを使用します。

3. IPSecプロファイルを設定します。

crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
モードトンネル

crypto ipsec profile IPSEC-IKEV2（IPSEC認証）

set transform-set T-SET（トランスフォームセットT – セット）
set ikev2-profile IKEV2-PROF

IPSecトンネルネゴシエーション用のトランスフォームセットを作成し、IPSecプロファイルの下でトランスフォームセットとIkev2プロファイルを呼び出します。

## DMVPN のコンフィギュレーション

1. 外部インターフェイスを設定します。

interface GigabitEthernet0/0/0

ip address 172.16.1.1 255.255.255.0
negotiation auto
cdp enable

2. mGREとIPsecを統合するようにハブルータを設定します（つまり、前の手順で設定したIPsecプロファイルにトンネルを関連付けます）

interface Tunnel0
ip address 10.10.10.1 255.255.255.0
no ip redirects
ip nhrp認証DMVPN
ip nhrp map multicast dynamic
ip nhrp network-id 1

ip nhrp redirect <--------ハブルータでDMVPNフェーズ3を有効にするには必須
トンネル発信元GigabitEthernet0/0/0
トンネルモードGREマルチポイント
トンネル保護ipsecプロファイルIPSEC-IKEV2
!

次のコマンドは、トンネルインターフェイス設定で使用されます。

- ip nhrp authentication DMVPN：この場合、同じDMVPNネットワークに属するすべてのハブとスポークでは、「DMVPN」認証文字列の値が同じである必要があります。
- ip nhrp map multicast dynamic:NHRPがスポークをNHRPマルチキャストマッピングに動的に追加できるようにします。
- ip nhrp network-id 1：インターフェイスでNHRPを有効にする32ビットネットワーク識別子。
- ip nhrp redirect：トラフィックがNHRPネットワークで転送される場合、リダイレクトトラフィック表示を有効にします。
- tunnel source GigabitEthernet0/0/0：トンネルインターフェイスの送信元アドレスを設定します。ここでは、GigaEthernet 0/0/0 IPアドレスを使用しています。
- tunnel mode gre multipoint：このトンネルインターフェイスのカプセル化モードをmGREに設定します。
- tunnel protection ipsec profile IPSEC-IKEV2：トンネルインターフェイスを、暗号設定ですでに作成されているIPsecプロファイルに関連付けます。

3. mGREとIPsecの統合のためのスポークルータの設定、およびBorder Gateway Protocol(BGP)接続をテストするための外部インターフェイスとループバックの設定

スポークX:（すべてのスポークで同様の設定を使用できます）

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

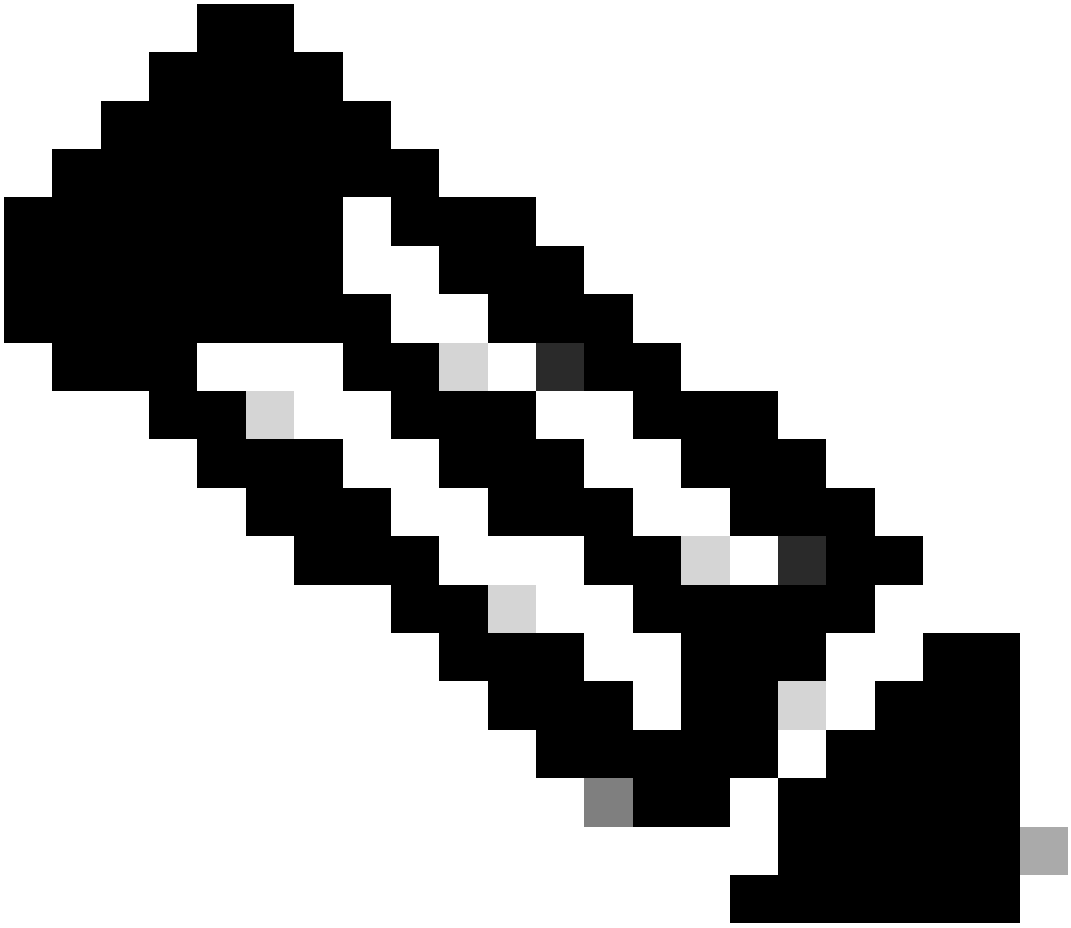
!

インターフェイスループバック10
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認証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 <--------スポークルータでDMVPNフェーズ3を有効にするには必須
トンネル発信元GigabitEthernet0/0/0

トンネルモードGREマルチポイント
トンネル保護ipsecプロファイルIPSEC-IKEV2

次のコマンドは、トンネルインターフェイス設定で使用されます。

- ip nhrp authentication DMVPN：この場合、同じDMVPNネットワークに属するすべてのハブとスポークでは、「DMVPN」認証文字列の値が同じである必要があります。
- ip nhrp map 10.10.10.1 172.16.1.1：ハブのNBMA IPアドレスをトンネルインターフェイスのIPアドレスに手動でマッピングします。
- ip nhrp map multicast 172.16.1.1：すべてのマルチキャストトラフィックをハブにリダイレクトします。
- ip nhrp network-id 1：インターフェイスでNHRPを有効にする32ビットネットワーク識別子。
- ip nhrp nhs 10.10.10.1：ハブであるネクストホップサーバは、このコマンドを使用して設定します。
- ip nhrp shortcut：インターフェイスでNHRPショートカットスイッチングを有効にします。
- tunnel source GigabitEthernet0/0/0：トンネルインターフェイスの送信元アドレスを設定します。ここでは、GigaEthernet 0/0/0 IPアドレスを使用しています。
- tunnel mode gre multipoint：このトンネルインターフェイスのカプセル化モードをmGREに設定します。
- tunnel protection ipsec profile IPSEC-IKEV2：トンネルインターフェイスを、暗号設定ですでに作成されているIPsecプロファイルに関連付けます。



注:ip nhrp redirectコマンドは、「ハブ経由よりも宛先スポークへのより良いルートがある」というメッセージをスポークに送信し、ip nhrp shortcutはスポーク上の転送情報ベース(FIB)にこのルートのインストールを課します。

## BGPの設定

次のバリエーションから選択できます。

- 各スポークで異なるAS番号を使用したeBGP
- 各スポーク上で同じAS番号を持つeBGP
- iBGP

この3つのシナリオすべてを説明することは、このドキュメントの適用範囲外です。

すべてのスポークで異なるAS番号を持つeBGPが設定されているため、ダイナミックネイバーは使用できません。したがって、ネイバーを手動で設定する必要があります。

スポーク上の異なるASを使用したeBGP

1. ハブでのBGPの設定：

Hub(config)#router bgp 65010

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

ハブ(config-router)#network 192.168.11.1マスク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

!

ハブのBGP設定では、次のコマンドを使用します。

- router bgp 65010:BGPルーティングプロセスを設定します。他のBGPスピーカーにデバイスを示す「autonomous-system-number」引数を使用します。
- network 192.168.11.1 mask 255.255.255.255：この自律システムのローカルなネットワークを指定し、BGPルーティングテーブルに追加します。
- neighbor 10.10.10.2 remote-as 65011：指定された自律システム内のネイバースポーク1のIPアドレスを、ローカルデバイスのIPv4マルチプロトコルBGPネイバーテーブルに追加します。
- neighbor 10.10.10.3 remote-as 65012：指定された自律システム内のネイバースポーク2のIPアドレスを、ローカルデバイスのIPv4マルチプロトコルBGPネイバーテーブルに追加します。

2. スポークXのBGP設定：

Spoke2(config)#router bgp 65012

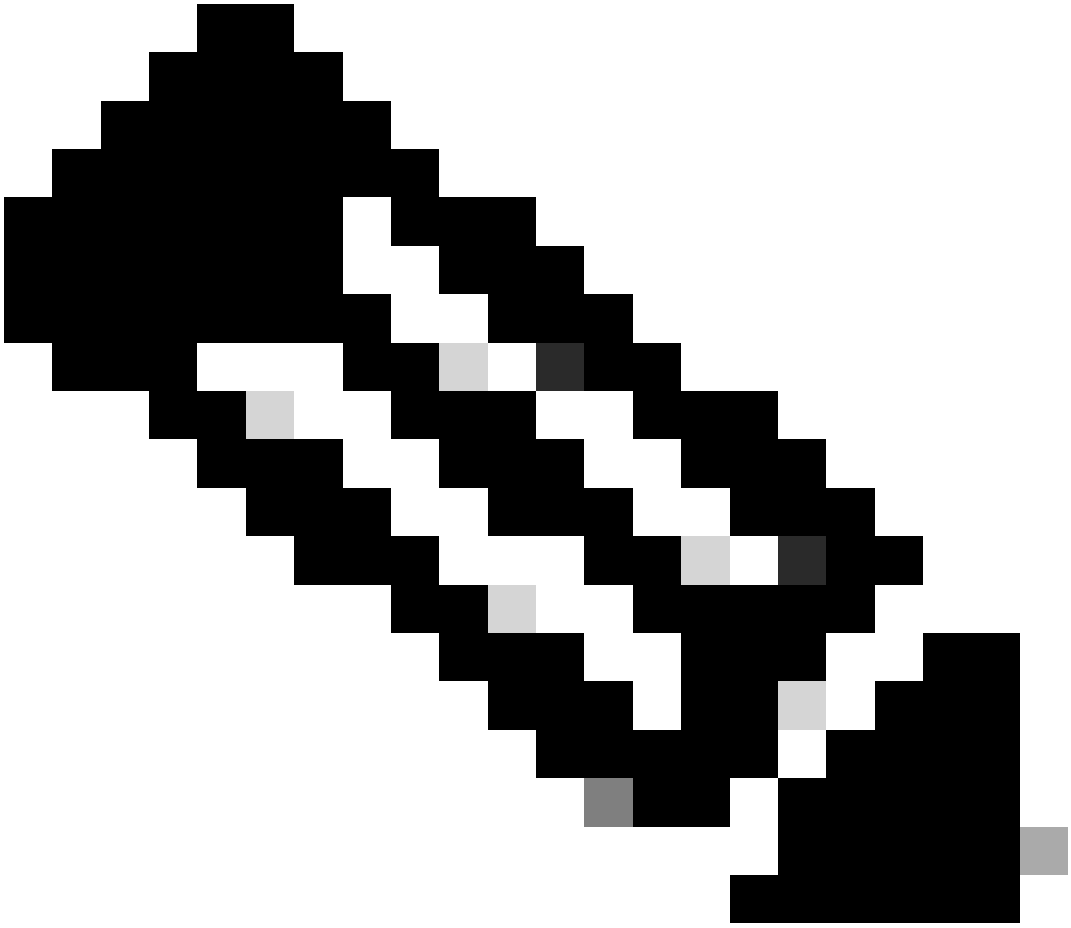
Spoke2(config-router)#bgp log-neighbor-changes

Spoke2(config-router)# network 192.168.33.3 mask 255.255.255.255

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

スポークXのBGP設定では、次のコマンドが使用されます。

- router bgp 65012:BGPルーティングプロセスを設定します。他のBGPスピーカーにデバイスを示す「autonomous-system-number」引数を使用します。
- network 192.168.33.3 mask 255.255.255.255：この自律システムのローカルなネットワークを指定し、BGPルーティングテーブルに追加します。
- neighbor 10.10.10.1 remote-as 65010：指定された自律システム内のハブのIPアドレスを、ローカルデバイスのIPv4マルチプロトコルBGPネイバーテーブルに追加します。



注:DMVPNネットワーク内のすべてのスポークで同様の設定を行う必要があります。

## 確認

1. ハブデバイスの検証コマンド：

ハブ#sh dmvpn

DMVPN固有のセッション情報を表示します。

凡例： Attrb —> S – 静的、D – 動的、I – 不完全
N - NAT対応、L – ローカル、X – ソケットなし
T1 – インストールされたルート、T2 – ネクストホップ上書き
C - CTS対応
# Ent —>同じNBMAピアを持つNHRPエントリの数
NHSステータス： E —>応答を予期しています、R —>応答しています、W —>待機中
UpDn Time —>トンネルのアップまたはダウン時間

==========

インターフェイス：Tunnel0、IPv4 NHRPの詳細
Type:Hub, NHRP Peers:2, <<<<<<<<<<<<<<<<<<<デバイスがハブとして動作していることを通知し、2つのNHRPピアがこのハブに接続されている。

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08 D <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<両方のピアがハブに動的に登録され、UP状態になっています。
1 172.16.3.3 10.10.10.3 UP 01:08:58 D

ハブ#sh ip nhrp

ハブに接続されているすべてのNHRPピアのトンネルインターフェイスIPへのNBMAアドレスマッピングを表示します。ハブは、すべてのスポークのデータベースを維持します。

10.10.10.2/32経由10.10.10.2
Tunnel0が01:47:22を作成し、01:32:27が期限切れになりました。
タイプ：ダイナミック、フラグ：一意の登録済み使用されるホップ
NBMAアドレス：172.16.2.2
10.10.10.3/32経由10.10.10.3
Tunnel0が01:09:11を作成し、01:29:58が期限切れになりました。
タイプ：ダイナミック、フラグ：一意の登録済み使用されるホップ
NBMAアドレス：172.16.3.3

ハブ#sh ip nhrp multicast

NHRPマルチキャストマッピング情報を表示します。

I/F NBMAアドレス
Tunnel0 172.16.2.2フラグ：ダイナミック（有効）
Tunnel0 172.16.3.3フラグ：ダイナミック（有効）

HUB#sh crypto sockets

暗号化ソケット接続の数2

Tu0ピア（ローカル/リモート）:172.16.1.1/172.16.2.2
ローカルID（アドレス/マスク/ポート/ポート）: (172.16.1.1/255.255.255.255/0/47)
リモートID（アドレス/マスク/ポート/ポート）: (172.16.2.2/255.255.255.255/0/47)
IPSecプロファイル：「IPSEC-IKEV2」
ソケットの状態：開く
クライアント：「TUNNEL SEC」（クライアントの状態：アクティブ）
Tu0ピア（ローカル/リモート）:172.16.1.1/172.16.3.3
ローカルID（アドレス/マスク/ポート/ポート）: (172.16.1.1/255.255.255.255/0/47)
リモートID（アドレス/マスク/ポート/ポート）: (172.16.3.3/255.255.255.255/0/47)

IPSecプロファイル：「IPSEC-IKEV2」
ソケットの状態：開く
クライアント：「TUNNEL SEC」（クライアントの状態：アクティブ）
リッスン状態の暗号化ソケット：
クライアント：「TUNNEL SEC」プロファイル：「IPSEC-IKEV2」マップ名：「Tunnel0-head-0」

HUB#sh cry ikev2 sa

IPv4暗号化IKEv2 SA

トンネルIDローカルリモートFVRF/IVRFステータス
1 172.16.1.1/500 172.16.2.2/500 none/none READY
暗号化：AES-CBC、キーサイズ：256、PRF:SHA512、ハッシュ：SHA512、DHグループ：5、
認証記号：PSK、認証検証：PSK
寿命/アクティブ時間： 86400/6524秒

トンネルIDローカルリモートFVRF/IVRFステータス
2 172.16.1.1/500 172.16.3.3/500 none/none準備完了
暗号化：AES-CBC、キーサイズ：256、PRF:SHA512、ハッシュ：SHA512、DHグループ：5、
認証記号：PSK、認証検証：PSK
寿命/アクティブ時間： 86400/4234秒

IPv6暗号化IKEv2 SA

HUB#sh ip bgp summary

BGPセッションの現在の状態、およびネイバーまたはピアグループからルータが受信したプレフィックスの数を表示します。

BGPルータID 192.168.11.1ローカルAS番号65010
BGPテーブルバージョンは4、メインルーティングテーブルバージョンは4です。
3 network entries using 432 bytes of memory
3 path entries using 252 bytes of memory
3/3 BGPパス/最適パス属性エントリ（480バイトのメモリを使用）
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1212 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs

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

ハブ#sh ip route bgp

コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、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外部タイプ1、E2:OSPF外部タイプ2
i - IS-IS、su - IS-ISサマリー、L1 - IS-ISレベル1、L2 - IS-ISレベル2
ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート
o - ODR、P – 定期的にダウンロードされたスタティックルート、H - NHRP、l - LISP
a：アプリケーションルート
+ – 複製されたルート、% – ネクストホップオーバーライド、 p - PfRからのオーバーライド

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 <<<<<<<<<<<<<<<Spoke 1のアドバタイズされたルートのエントリ
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<<<<Spoke 2のアドバタイズされたルートのエントリ

2. スポーク1での確認コマンド：

スポーク1#sh dmvpn

凡例： Attrb —> S – 静的、D – 動的、I – 不完全
N - NAT対応、L – ローカル、X – ソケットなし
T1 – インストールされたルート、T2 – ネクストホップ上書き
C - CTS対応、I2 – 一時
# Ent —>同じNBMAピアを持つNHRPエントリの数
NHSステータス： E —>応答を予期しています、R —>応答しています、W —>待機中
UpDn Time —>トンネルのアップまたはダウン時間
==========

インターフェイス：Tunnel0、IPv4 NHRPの詳細
タイプ：スポーク、NHRPピア：2、

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 UP 01:32:09 S <<<<<<<<<<<<<<<ハブは、トンネルインターフェイスでスタティックエントリとして設定されているため、S-staticと表示されています
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<<<<スポーク2にトラフィックを送信した後に作成されたダイナミックオンデマンドスポーク間トンネル

スポーク1#sh ip bgp summary

BGP router identifier 192.168.22.2, local AS number 65011
BGPテーブルバージョンは4、メインルーティングテーブルバージョンは4です。
3 network entries using 744 bytes of memory
3 path entries using 432 bytes of memory
3/3 BGPパス/最適パス属性エントリ（864バイトのメモリを使用）

2 BGP AS-PATH entries using 64 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2104 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs
3つのネットワークがピークに達した日時：2022年6月2日08:16:54 UTC（01:11:51.732前）

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ
Up/Down State/PfxRcd
10.10.10.1 4 65010 85 85 4 0 0 01:12:21 2 <<<<<<<<<<<<<<<<<<<<<<<<<<<< ハブから2つのプレフィックス（それぞれハブループバックとSpoke2ループバック）を受信しました

スポーク1#sh ip route bgp

コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、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外部タイプ1、E2 - OSPF外部タイプ2、m - OMP
n - NAT、Ni - NAT内部、No - NAT外部、Nd - NAT DIA
i - IS-IS、su - IS-ISサマリー、L1 - IS-ISレベル1、L2 - IS-ISレベル2
ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート
H - NHRP、G - NHRP登録、g - NHRP登録の概要
o - ODR、P – 定期的にダウンロードされたスタティックルート、l - LISP
a：アプリケーションルート
+ – 複製されたルート、% – ネクストホップオーバーライド、 p - PfRからのオーバーライド

ラストリゾートゲートウェイは172.16.2.10からネットワーク0.0.0.0です。

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 >>>>>>>>>>ハブを介して直接ハブに到達可能なハブネットワーク

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 >>>>>>>>>>スポークトンネルIPを介して直接到達可能なスポークネットワーク。

スポーク1#sh ip route

コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、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外部タイプ1、E2 - OSPF外部タイプ2、m - OMP
n - NAT、Ni - NAT内部、No - NAT外部、Nd - NAT DIA
i - IS-IS、su - IS-ISサマリー、L1 - IS-ISレベル1、L2 - IS-ISレベル2
ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート
H - NHRP、G - NHRP登録、g - NHRP登録の概要
o - ODR、P – 定期的にダウンロードされたスタティックルート、l - LISP
a：アプリケーションルート
+ – 複製されたルート、% – ネクストホップオーバーライド、 p - PfRからのオーバーライド

ラストリゾートゲートウェイは172.16.2.10からネットワーク0.0.0.0です。

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は直接接続されています。GigabitEthernet2
L 172.16.2.2/32は直接接続され、GigabitEthernet2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24は直接接続されています。Tunnel0
L 10.10.10.2/32は直接接続され、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 is directly connected, Loopback10（直接接続されている場合）
L 192.168.22.2/32は直接接続されています。Loopback10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

スポーク1#sh ip nhrp nhs

凡例：E=応答を期待、R=応答、W=待機、D=動的
Tunnel0:
10.10.10.1 REプライオリティ= 0クラスタ= 0 >>>>>>>> ネクストホップサーバが1つだけ設定されている

Spoke1#sh ip nhrp traffic

Tunnel0: Max-send limit:10000Pkts/10Sec、使用量：0%
送信済み：合計52
1解決要求0解決応答51登録要求<<<<<<<ハブに登録要求が送信された回数
0登録応答0パージ要求0パージ応答
0エラー表示0トラフィック表示0リダイレクト抑制
Rcvd：合計25
0解決要求1解決応答0登録要求<<<<<<<<<<<<これらの登録要求に対する応答を受信した回数
24 Registration Reply 0 Purge Request 0 Purge Reply
0エラー表示0トラフィック表示0リダイレクト抑制

Spoke1#sh ip nhrp multicast

I/F NBMAアドレス
Tunnel0 172.16.1.1フラグ：スタティック（有効）<<<<<<<<<<<ハブNBMAに向けてマルチキャストトラフィックを転送するように設定されている

Spoke1#sh crypto sockets

暗号化ソケット接続数2

Tu0ピア（ローカル/リモート）:172.16.2.2/172.16.1.1

ローカルID（アドレス/マスク/ポート/ポート）: (172.16.2.2/255.255.255.255/0/47)
リモートID（アドレス/マスク/ポート/ポート）: (172.16.1.1/255.255.255.255/0/47)
IPSecプロファイル：「IPSEC-IKEV2」
Socket State: Open <<<<<<<<<<<<<<<<<<<この特定のピアのソケットのステータス
クライアント：「TUNNEL SEC」（クライアントの状態：アクティブ）
Tu0ピア（ローカル/リモート）:172.16.2.2/172.16.3.3
ローカルID（アドレス/マスク/ポート/ポート）: (172.16.2.2/255.255.255.255/0/47)
リモートID（アドレス/マスク/ポート/ポート）: (172.16.3.3/255.255.255.255/0/47)
IPSecプロファイル：「IPSEC-IKEV2」
ソケットの状態：開く
クライアント：「TUNNEL SEC」（クライアントの状態：アクティブ）
リッスン状態の暗号化ソケット：
クライアント：「TUNNEL SEC」プロファイル：「IPSEC-IKEV2」マップ名：「Tunnel0-head-0」

スポーク1#sh cry ikev2 sa

IPv4暗号化IKEv2 SA

トンネルIDローカルリモートFVRF/IVRFステータス
2 172.16.2.2/500 172.16.3.3/500 none/none準備完了
暗号化：AES-CBC、キーサイズ：256、PRF:SHA512、ハッシュ：SHA512、DH Grp:19、認証記号：PSK、認証検証：PSK
寿命/アクティブ時間：86400/287秒

トンネルIDローカルリモートFVRF/IVRFステータス
1 172.16.2.2/500 172.16.1.1/500 none/none READY
暗号化：AES-CBC、キーサイズ：256、PRF:SHA512、ハッシュ：SHA512、DH Grp:19、認証記号：PSK、認証検証：PSK
寿命/アクティブ時間： 86400/4643秒

IPv6暗号化IKEv2 SA

スポーク1#traceroute 192.168.33.3送信元lo10

中止するにはエスケープ文字列を入力します
Tracing the route to 192.168.33.3
VRF情報：(vrf in name/id、vrf out name/id)
1 10.10.10.3 3ミリ秒4ミリ秒* <<<<<<<<<<<<<トラフィックはハブを通過せずにスポーク2ルータに直接送信される。

スポーク2#sh dmvpn

凡例： Attrb —> S – 静的、D – 動的、I – 不完全
N - NAT対応、L – ローカル、X – ソケットなし
T1 – インストールされたルート、T2 – ネクストホップ上書き
C - CTS対応、I2 – 一時

# Ent —>同じNBMAピアを持つNHRPエントリの数
NHSステータス： E —>応答を予期しています、R —>応答しています、W —>待機中
UpDn Time —>トンネルのアップまたはダウン時間
==========

インターフェイス：Tunnel0、IPv4 NHRPの詳細
タイプ：スポーク、NHRPピア：2、

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1を01:20:26 Sまで上昇
1 172.16.2.2 10.10.10.2アップ00:07:51 D

3. スポーク2での確認コマンド：

スポーク2#sh ip nhrp

10.10.10.1/32経由10.10.10.1
Tunnel0 created 01:36:06, never expire（トンネル0が作成されました。期限が切れません）
タイプ：static、フラグ：
NBMAアドレス：172.16.1.1
10.10.10.2/32経由10.10.10.2
Tunnel0が00:08:09を作成し、00:01:50が期限切れになりました。
タイプ：ダイナミック、フラグ：ルータの暗黙的
NBMAアドレス：172.16.2.2
10.10.10.3/32経由10.10.10.3
Tunnel0が00:08:09を作成し、00:01:50が期限切れになりました。
タイプ：ダイナミック、フラグ：ルータユニークローカルアドレス
NBMAアドレス：172.16.3.3
（ソケットなし）
スポーク2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
I/F NBMAアドレス
Tunnel0 172.16.1.1フラグ：static（有効）
スポーク2#

Spoke2#sh crypto sockets

暗号化ソケット接続の数2

Tu0ピア（ローカル/リモート）:172.16.3.3/172.16.1.1
ローカルID（アドレス/マスク/ポート/ポート）: (172.16.3.3/255.255.255.255/0/47)
リモートID（アドレス/マスク/ポート/ポート）: (172.16.1.1/255.255.255.255/0/47)
IPSecプロファイル：「IPSEC-IKEV2」
ソケットの状態：オープン<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<この特定のピアのソケットの状態
クライアント：「TUNNEL SEC」（クライアントの状態：アクティブ）

Tu0ピア（ローカル/リモート）:172.16.3.3/172.16.2.2
ローカルID（アドレス/マスク/ポート/ポート）: (172.16.3.3/255.255.255.255/0/47)
リモートID（アドレス/マスク/ポート/ポート）: (172.16.2.2/255.255.255.255/0/47)
IPSecプロファイル：「IPSEC-IKEV2」
ソケットの状態：開く
クライアント：「TUNNEL SEC」（クライアントの状態：アクティブ）
リッスン状態の暗号化ソケット：
クライアント：「TUNNEL SEC」プロファイル：「IPSEC-IKEV2」マップ名：「Tunnel0-head-0」

スポーク2#sh cry ikev2 sa

IPv4暗号化IKEv2 SA

トンネルIDローカルリモートFVRF/IVRFステータス
2 172.16.3.3/500 172.16.2.2/500 none/none準備完了
暗号化：AES-CBC、キーサイズ：256、PRF:SHA512、ハッシュ：SHA512、DH Grp:19、認証記号：PSK、認証検証：PSK
寿命/アクティブ時間：86400/509秒

トンネルIDローカルリモートFVRF/IVRFステータス
1 172.16.3.3/500 172.16.1.1/500 none/none READY
暗号化：AES-CBC、キーサイズ：256、PRF:SHA512、ハッシュ：SHA512、DH Grp:19、認証記号：PSK、認証検証：PSK
寿命/アクティブ時間： 86400/4866秒

IPv6暗号化IKEv2 SA

スポーク2#sh ip bgp summary

BGP router identifier 192.168.33.3, local AS number 65012
BGPテーブルバージョンは4、メインルーティングテーブルバージョンは4です。
3 network entries using 744 bytes of memory
3 path entries using 432 bytes of memory
3/3 BGPパス/最適パス属性エントリ（864バイトのメモリを使用）
2 BGP AS-PATH entries using 64 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2104 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs
3つのネットワークがピークに達した日時：2022年6月2日08:16:54 UTC（01:20:43.775前）

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ
Up/Down State/PfxRcd
10.10.10.1 465010 97 94 4 0 0 01:21:07 2 >>>>>>>>>>>>>>>>>>>>。ハブから2つのプレフィックスを受信しました。それぞれハブループバックとスポーク2ループバック用です

スポーク2#sh ip route

コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、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外部タイプ1、E2 - OSPF外部タイプ2、m - OMP
n - NAT、Ni - NAT内部、No - NAT外部、Nd - NAT DIA
i - IS-IS、su - IS-ISサマリー、L1 - IS-ISレベル1、L2 - IS-ISレベル2
ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート
H - NHRP、G - NHRP登録、g - NHRP登録の概要
o - ODR、P – 定期的にダウンロードされたスタティックルート、l - LISP
a：アプリケーションルート
+ – 複製されたルート、% – ネクストホップオーバーライド、 p - PfRからのオーバーライド

ラストリゾートゲートウェイは172.16.3.10からネットワーク0.0.0.0です。

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 is directly connected, GigabitEthernet3（直接接続されているCポート、GigabitEthernet3）
L 172.16.3.3/32は直接接続、GigabitEthernet3
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24は直接接続されています。Tunnel0
L 10.10.10.3/32は直接接続され、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 is directly connected, Loopback10（直接接続されている場合）
L 192.168.33.3/32は直接接続されています。Loopback10

スポーク2#sh ip route bgp

コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、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外部タイプ1、E2 - OSPF外部タイプ2、m - OMP
n - NAT、Ni - NAT内部、No - NAT外部、Nd - NAT DIA
i - IS-IS、su - IS-ISサマリー、L1 - IS-ISレベル1、L2 - IS-ISレベル2
ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート
H - NHRP、G - NHRP登録、g - NHRP登録の概要
o - ODR、P – 定期的にダウンロードされたスタティックルート、l - LISP
a：アプリケーションルート
+ – 複製されたルート、% – ネクストホップオーバーライド、 p - PfRからのオーバーライド

ラストリゾートゲートウェイは172.16.3.10からネットワーク0.0.0.0です。

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 >>>>>>>>>>>>>>ハブを介して直接ハブネットワークに到達可能

B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>スポークトンネルIPを介して直接到達可能なスポークネットワーク。

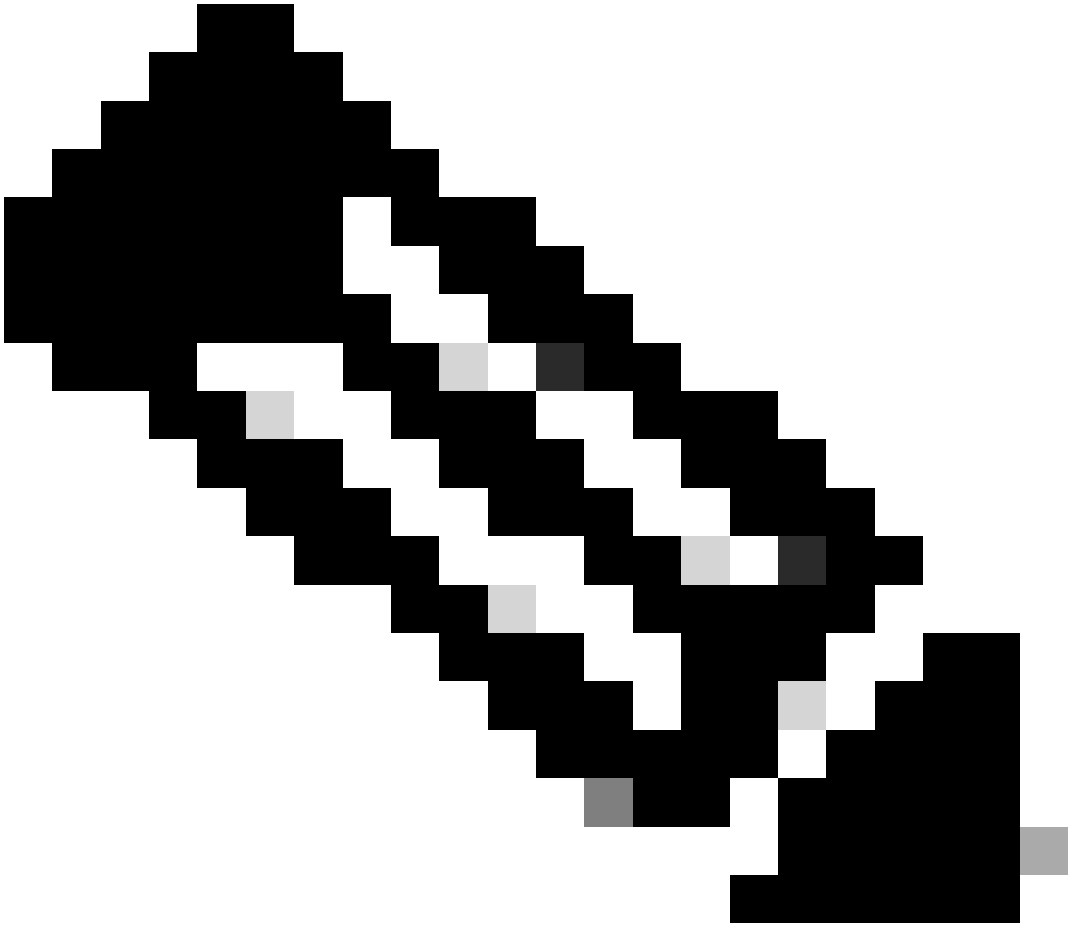
スポーク2#sh ip nhrp nhs

凡例：E=応答を期待、R=応答、W=待機、D=動的
Tunnel0:
10.10.10.1 REプライオリティ= 0クラスタ= 0 >>>>>>>>>>>>> ネクストホップサーバは1つだけ設定されます

Spoke2#traceroute 192.168.22.2 source loopback 10

中止するにはエスケープ文字列を入力します
Tracing the route to 192.168.22.2
VRF情報：(vrf in name/id、vrf out name/id)
1 10.10.10.2 4ミリ秒4ミリ秒* <<<<<<<<<<<<<トラフィックはハブを通過せずにスポーク1ルータに直接送信される。

# トラブルシュート



注：非条件付きデバッグを実行するとプロセッサおよび実稼働環境に影響を与える可能性があるため、常に条件付きデバッグの使用を推奨します。NBMAアドレスは「外部IPアドレス」（トンネルインターフェイスの発信元として使用されるIPアドレス）に対応し、トンネルIPは「論理IPアドレス、つまりトンネルインターフェイスのIPアドレス」に対応します。

---

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>
debug crypto condition peer ipv4 <ピアのWAN IP>
debug nhrp condition peer <nbma/tunnel> <NBMAまたはピアのトンネルIPアドレス>

DMVPNのトラブルシューティングを行うには、次のように階層化アプローチを採用する必要があります。

debug dmvpn detail all


1. 暗号化層：2つのピア間の物理接続を確認した後、暗号化を確認する必要があります。この層は、GREパケットを暗号化/復号化します。

暗号化の部分を確認するために使用される一般的なdebugコマンドは次のとおりです。

debug crypto condition peer ipv4 <ピアのWAN IPアドレス>

debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

debug crypto ikev2 packet

debug crypto ipsec

debug crypto ipsec error

または

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

debug crypto condition peer ipv4 <ピアのWAN IP>

debug dmvpn detail crypto

暗号化レイヤのトラブルシューティングの詳細については、外部リンクを参照してください。

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html にアクセスしてください。

2. GRE/NHRP：一般的な問題には、NHRP登録の失敗や、ハブでのNHRPマッピングの不整合につながるスポークでのダイナミックNBMAアドレスの変更などがあります。

NHRPマッピングの確認に使用される一般的なdebugコマンド

debug nhrp condition peer <nbma/tunnel> <NBMAまたはピアのトンネルIPアドレス>

debug nhrp cache

NHRPパケットのデバッグ

デバッグNHRPの詳細

debug nhrpエラー

最も一般的なDMVPNのトラブルシューティング方法については、外部リンクを参照してください。

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html にアクセスしてください。

3. ルーティング：ルーティングプロトコルは、オンデマンドのスポーク間トンネルの状態を監視しません。

IPルーティングアップデートとIPマルチキャストデータパケットは、ハブアンドスポークトンネルのみを通過します。

ユニキャストIPデータパケットは、ハブアンドスポークとオンデマンドのスポーク間トンネルの両方を通過します。

Debug：ルーティングプロトコルに応じて、さまざまなdebugコマンドを使用できます。

BGPルーティングの詳細については、外部リンクを参照してください。

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html にアクセスしてください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。