動的 Ipsec マルチポイント VPN (IPsec VPN を測定するためにマルチポイント GRE/NHRP を使用する)

内容

概要

このドキュメントでは、Dynamic Multipoint IPsec VPN（DMVPN）について説明し、また企業がCiscoIOS® ソフトウェアでこの新しい IPsec VPN ソリューションを使用できるよう、ネットワークを設計または移行する必要性について説明します。

背景説明

企業はトラフィックを暗号化して保護しながら、インターネット上の多くのサイトをメイン サイトと接続し、またサイトどうしを相互接続する必要があります。たとえば、在庫や発注のため本社に接続する必要のある小売店舗は、製品の有無を確認するため社内の他の店舗にも接続する必要があります。これまですべてを相互接続するには、ISDN やフレーム リレーなどのレイヤ 2 ネットワークを使用するしか方法はありませんでした。社内 IP トラフィック用にこれらの有線接続を設定することは時間がかかり、コストもかかることでした。これらすべてのサイト（メイン サイトを含む）においてすでに比較的安価なインターネット アクセスができる場合、IPsec トンネルを使用してプライバシーとデータの整合性を確保することにより、このインターネット アクセスを店舗と本社間の社内 IP 通信にも使用できます。

企業がインターネットを介してサイトを相互接続する大規模な IPsec ネットワークを構築するには、IPsec ネットワークを拡張できる必要があります。IPsec は 2 つのエンドポイント（ピア）間のトラフィックを暗号化し、暗号化は共有「秘密」を使って 2 つのエンドポイントによって行われます。 この秘密はこれら 2 つのエンドポイント間でのみ共有されるため、暗号化されたネットワークは本質的にポイントツーポイント リンクの集合です。このため、IPsec は本質的にポイントツーポイント トンネル ネットワークです。大規模なポイントツーポイント ネットワークを拡張する最も現実的な方法は、ハブアンドスポークまたはフル（部分）メッシュ ネットワークに組み込むことです。多くのネットワークにおいて IP トラフィックの大部分はスポークとハブ間のもので、スポーク間のトラフィックは少ないため、ハブアンドスポークの設計がしばしば最適な選択になります。この設計は、古いフレーム リレー ネットワークにも適しています。なぜならこのようなネットワークにおいて、すべてのサイト間のリンクに対して支払う費用は非常に高かったためです。

ハブアンドスポーク間の相互接続としてインターネットを使用する場合、スポークどうしは追加コストなしで相互に直接アクセスすることもできますが、不可能ではないにしても、フル（部分）メッシュ ネットワークを設定、管理することは非常に難しいことでした。スポーク間トラフィックがハブ経由でなく直接接続できる場合、フルまたは部分メッシュ ネットワークが適していることがよくあります。ハブを通過するスポーク間トラフィックはハブのリソースを使用し、特に IPsec 暗号化を使用する場合、ハブは送信スポークからの着信パケットを復号化し、トラフィックを再暗号化し、受信スポークに送信する必要があるため、さらに遅延する場合があります。直接スポーク間トラフィックが有効なもう 1 つの例は、2 つのスポークが同じ都市にあり、ハブが全国にある場合です。

IPsec ハブアンドスポーク ネットワークが展開され、規模が拡大するにつれ、IP パケットを可能な限り動的にルーティングすることが求められるようになりました。古いフレーム リレーのハブアンドスポーク ネットワークでは、これはフレーム リレー リンク上で OSPF や EIGRP などのダイナミック ルーティング プロトコルを実行することで実現されました。これはスポーク ネットワークの到達可能性を動的にアドバタイズし、また IP ルーティング ネットワークの冗長性をサポートするうえで役立ちました。ネットワークがハブ ルータを失った場合、バックアップ ハブ ルータが自動的に引き継ぎ、このスポーク ネットワークへのネットワーク接続が維持されます。

IPsec トンネルとダイナミック ルーティング プロトコルには基本的な問題があります。ダイナミック ルーティング プロトコルは IP マルチキャスト パケットまたはブロードキャスト パケットを使用しますが、IPsec はマルチキャスト パケットまたはブロードキャスト パケットの暗号化をサポートしていません。この問題を解決する現在の方法は、IPsec 暗号化と組み合わせて Generic Routing Encapsulation（GRE）トンネルを使用することです。

GRE トンネルは、IP マルチキャストおよびブロードキャスト パケットを GRE トンネルの他端に転送することをサポートします。GRE トンネル パケットは IP ユニキャスト パケットのため、GRE パケットは IPsec を使用して暗号化できます。このシナリオでは、GRE がトンネリング作

業を行い、IPSec が VPN ネットワークをサポートし、暗号化を行います。GREトンネルを設定する場合、トンネルのエンドポイント(**tunnel source ..., tunnel destination ...)のIPアドレスは、他のエンドポイントが認識し、インターネット上でルーティング可能である必要があります。**これは、このネットワーク内のハブとすべてのスポーク ルータに、スタティックな非プライベート IP アドレスが必要であることを意味します。

インターネットへの小規模なサイト接続では、インターネットに接続するたびにスポークの外部IPアドレスが変更されることが一般的です。これは、Internet Service Provider（ISP；インターネットサービスプロバイダー）がスポークがオンラインになるたびに(DHCP(Dynamic Host Configuration Protocol)経由)外部インターフェイスアドレスを動的に提供するためです。 ルータが「外部アドレス」を動的に割り当てることにより、すべてのユーザが同時にオンラインになるわけではないため、ISP がインターネット アドレス空間の使用をオーバーサブスクライブすることができます。スポーク ルータにスタティック アドレスを割り当てるためのプロバイダーへの支払いは、かなり高額になる可能性があります。IPsec VPN 上でダイナミック ルーティング プロトコルを実行するには GRE トンネルを使用する必要がありますが、外部物理インターフェイスに動的に割り当てられた IP アドレスのスポークを持つという選択肢は失われます。

上記の制限事項およびその他の制限事項は、次の 4 つにまとめられます。

- IPsec は、アクセス コントロール リスト（ACL）を使用してどのデータを暗号化するかを定義します。したがって、新しい（サブ）ネットワークがスポークまたはハブの背後に追加されるたびに、顧客はハブとスポーク ルータの両方で ACL を変更する必要があります。SP がルータを管理している場合、IPsec ACL を変更するため SP に通知する必要があります。これにより、新しいトラフィックが暗号化されます。
- 大規模なハブアンドスポーク ネットワークでは、ハブ ルータ上の設定サイズが、使用不可になるほど巨大になることがあります。たとえばハブ ルータは、300 個のスポーク ルータをサポートするために、最大 3900 行の設定が必要です。これは設定を表示し、デバッグ中の現在の問題に関連する設定のセクションを見つけることが困難になるほど大きなサイズです。またこのサイズ設定は NVRAM に収まらないほど大きく、フラッシュ メモリに格納する必要があります。
- GRE+IPsec はエンドポイントのピア アドレスを認識している必要があります。スポークの IP アドレスはそれぞれの ISP 経由でインターネットに直接接続され、外部インターフェイスのアドレスが固定されないよう、設定されることがよくあります。この IP アドレスは、サイトがオンラインになるたびに（DHCP 経由で）変更できます。
- スポークが IPsec VPN を介して互いに直接やり取りする必要がある場合、ハブアンドスポーク ネットワークはフル メッシュになる必要があります。どのスポークが互いに直接やり取りする必要があるかがわからないため、各スポークが他のすべてのスポークと直接やり取りする必要がなくても、フル メッシュが必要です。また小さなスポーク ルータに IPsec を設定し、ネットワーク内の他のすべてのスポーク ルータと直接接続できるようにすることは現実的ではありません。したがってスポーク ルータはより強力なルータになる必要があります。

DMVPN ソリューション

DMVPN ソリューションは、マルチポイント GRE（mGRE）と Next Hop Resolution Protocol（NHRP）を、IPsec といくつかの新しい拡張機能とともに使用し、上記の問題をスケーラブルな方法で解決します。

IPsec 暗号化の自動開始

DMVPN ソリューションを使用しない場合、この IPsec トンネルの使用を必要とするデータ トラフィックが発生するまで、IPsec 暗号化トンネルは開始されません。IPsec トンネルの開始を完了するには 1 ~ 10秒ほどかかる場合があり、この期間データ トラフィックはドロップされます。IPsecでGREを使用する場合、GREトンネルの設定にはGREトンネルピア(**tunnel destination ...**)アドレス (IPsecピアアドレスでもある) がすでに含まれています。これらのアドレスは両方とも事前設定されています。

ハブ ルータでトンネル エンドポイント ディスカバリ (TED) とダイナミック暗号マップを使用する場合、ハブ上で IPsec ピア アドレスを事前に設定する必要はありませんが、ISAKMP ネゴシエーションを開始する前に TED プローブおよび応答を送受信する必要があります 。GRE を使用する場合、ピアの送信元アドレスと宛先アドレスはすでに認識されているため、これは必要ではありません。それらは設定にあるか、NHRP (マルチポイント GRE トンネル用) で解決されます。

DMVPN ソリューションを使用すると、IPsec はポイントツーポイントおよびマルチポイント GRE トンネルの両方に対して即座にトリガーされます。また暗号 ACL を設定する必要はありません。これらは GRE トンネルの送信元アドレスと宛先アドレスから自動的に取得されるためです。次のコマンドを使用して、IPsec 暗号化パラメータを定義します。この情報は関連する GRE トンネルまたは NHRP マッピングから直接取得されるため、**set peer ... または match address ... コマンドは必要ありません。**

```
crypto ipsec profile
```

```
 set transform-set
```

次のコマンドは、トンネル インターフェイスを IPsec プロファイルに関連付けます。

```
interface tunnel
```

```
 ...
 tunnel protection ipsec profile
```

「スポークとハブ間」リンクの ダイナミック トンネル作成

スポークに関する GRE または IPsec 情報は、DMVPN ネットワーク内のハブ ルータには設定さ

れていません。スポーク ルータの GRE トンネルは、（NHRP コマンドを使用して）ハブ ルータに関する情報が設定されます。上記のように、スポーク ルータが起動すると、ハブ ルータで IPsec トンネルを自動的に開始します。スポーク ルータは次に NHRP を使用して、ハブ ルータに現在の物理インターフェイス IP アドレスを通知します。これは、次の 3 つの理由により有用です。

- （ADSL または CableModem などにより）スポーク ルータに物理インターフェイス IP アドレスが動的に割り当てられている場合、スポーク ルータがリロードするたびに新しい物理インターフェイス IP アドレスを取得するため、この情報を使用してハブ ルータを設定することはできません。
- ハブ ルータの設定は短縮され、簡素化されています。これは、ピア ルータに関する GRE や IPsec 情報を持つ必要がないためです。この情報はすべて、NHRP を介して動的に学習されます。
- 新しいスポーク ルータを DMVPN ネットワークに追加した場合、ハブや現在のスポーク ルータの設定を変更する必要はありません。新しいスポーク ルータはハブ情報を使用して設定され、ルータの起動時に、ハブ ルータに動的に登録されます。ダイナミック ルーティング プロトコルは、このスポークのルーティング情報をハブへ伝搬します。このハブはこの新しいルーティング情報を他のスポークへ伝搬します。また他のスポークからこのスポークへのルーティング情報も伝搬します。

「スポーク間」トラフィックの ダイナミック トンネル作成

前述のように、現在メッシュ ネットワークでは、トンネルの一部が常に稼働していなくても、または必要ない場合でも、すべてのルータで、すべてのポイントツーポイント IPsec（または IPsec+GRE）トンネルを設定する必要があります。DMVPN ソリューションでは、1 つのルータがハブになり、他のすべてのルータ（スポーク）にはハブへのトンネルが設定されます。スポークとハブ間のトンネルは連続的に稼働しており、スポークには他のスポークへの直接トンネルを設定する必要はありません。代わりに、スポークが別のスポーク（別のスポークの背後にあるサブネットなど）にパケットを送信したい場合、スポークは NHRP を使用して、ターゲットのスポークに必要な宛先アドレスを動的に決定します。ハブ ルータは NHRP サーバとして動作し、送信元スポークへのこの要求を処理します。この 2 つのスポークは、それらの間に（1 つの mGRE インターフェイス経由で）IPsec トンネルを動的に作成し、データを直接転送することができます。この動的なスポーク間トンネルは、（設定可能な）非アクティブ期間後に自動的に切断されます。

ダイナミック ルーティング プロトコルのサポート

DMVPN ソリューションはトンネリング マルチキャスト/ブロードキャスト IP パケットをサポートする GRE トンネルに基づいているため、DMVPN ソリューションは IPsec+mGRE トンネル上で実行されるダイナミック ルーティング プロトコルもサポートしています。以前は、NHRP では、マルチキャストおよびブロードキャスト IP パケットの GRE トンネリングをサポートするため、トンネル宛先 IP アドレスのブロードキャスト/マルチキャスト マッピングを明示的に設定する必要がありました。たとえばハブでは、各スポークに対して **ip nhrp map multicast <spoke-n-addr> 設定行が必要です。**DMVPN ソリューションでは、スポークのアドレスは事前に認識できないため、この設定は不可能です。代わりに、NHRPは **ip nhrp map multicast dynamic コマンドを使用して、各スポークをハブ上のマルチキャスト宛先リストに自動的に追加するよう設定できます。**このコマンドを使用することで、スポーク ルータがユニキャスト NHRP マッピングを NHRP サーバ（ハブ）に登録すると、NHRP はこのスポークのブロードキャスト/マルチキャスト マッピングも作成します。これにより、事前にスポークのアドレスを認識する必要がなくなります。

mGRE の Cisco Express Forwarding ファスト スイッチング

現在、mGRE インターフェイスのトラフィックはプロセススイッチされているため、パフォーマンスが低下します。DMVPN ソリューションは、mGRE トラフィックに Cisco Express Forwarding スイッチングを追加することで、パフォーマンスが大幅に向上します。この機能を有効にするために必要な設定コマンドはありません。Cisco Express Forwarding スイッチングが GRE トンネル インターフェイスと発信/着信物理インターフェイスで許可されている場合、マルチポイント GRE トンネル パケットは Cisco Express Forwarding スイッチドになります。

IPsec で保護された VPN でのダイナミック ルーティングの使用

このセクションでは、現在の（DMVPN ソリューション以前の）状態について説明します。IPsec は、暗号化を定義する一連のコマンドと、ルータの外部インターフェイスに適用される **crypto map <map-name> コマンドを介して、Cisco ルータに実装されます。**この設計のため、また現在 IPsec を使用して IP マルチキャスト/ブロードキャスト パケットを暗号化する標準は存在しないため、IP ルーティング プロトコル パケットを IPsec トンネルを介して「転送」することはできず、ルーティングの変更を IPsec トンネルの反対側に動的に伝搬できません。

注：BGPを除くすべてのダイナミックルーティングプロトコルは、ブロードキャストまたはマルチキャストIPパケットを使用します。この問題を解決するには、GRE トンネルを IPsec と組み合わせて使用します。

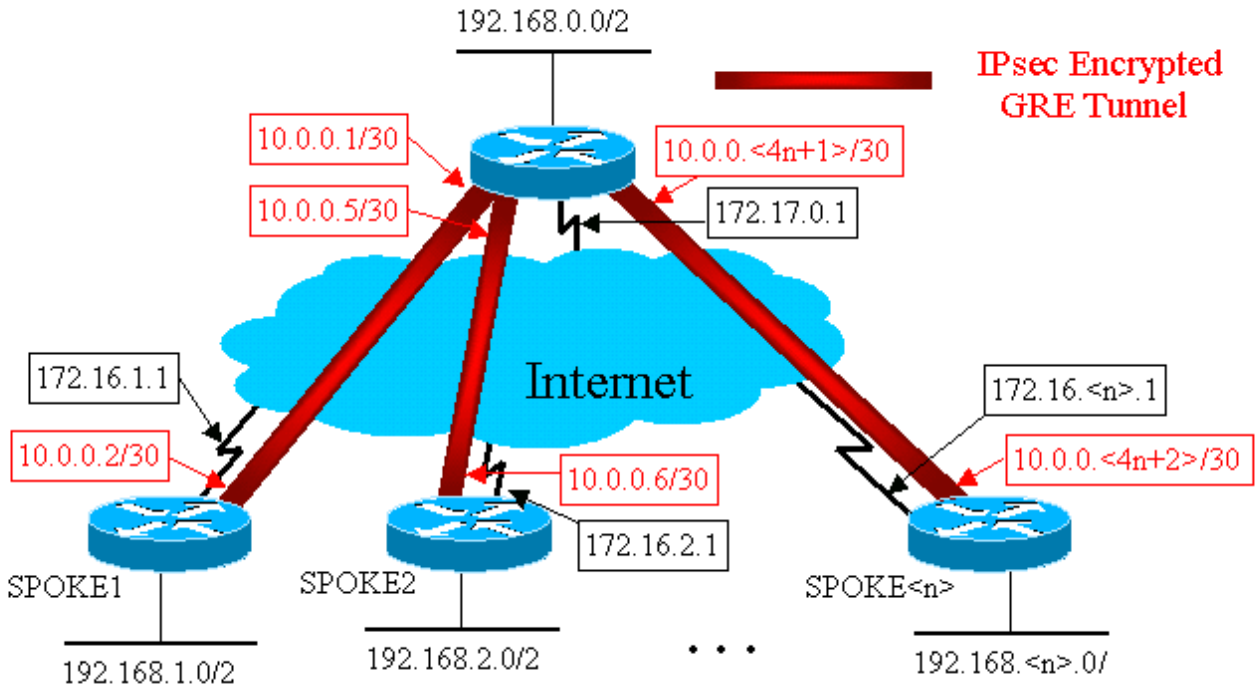
GRE トンネルは、仮想トンネル インターフェイス（**interface tunnel<#>**）を使用して Cisco ルータに実装されます。 GRE トンネリング プロトコルは、IP マルチキャスト/ブロードキャスト パケットを処理するよう設計されているため、ダイナミック ルーティング プロトコルを GRE トンネルで「実行」することができます。GRE トンネル パケットは、元の IP マルチキャスト/ユニキャスト パケットをカプセル化する IP ユニキャスト パケットです。その後、IPsec を使用して GRE トンネル パケットを暗号化できます。また GRE はすでに元のデータ パケットをカプセル化しているため、トランス ポート モードで IPsec を実行し、20 バイト節約することもできます。これにより、IPsec を使って、別の IP ヘッダーの GRE IP パケットをカプセル化する必要はありません。

IPsec をトランスポート モードで実行する場合、暗号化するパケットの IP 送信元アドレスと宛先アドレスが IPsec ピア アドレス（ルータ自体）と一致している必要があります。 この場合、これは、GRE トンネル エンドポイントと IPsec ピア アドレスが同じでなければならないことを意味します。同じルータが IPsec と GRE トンネル エンドポイントであるため、これは問題ではありません。GRE トンネルと IPsec 暗号化を組み合わせることにより、ダイナミック IP ルーティング プロトコルを使用して、暗号化トンネルの両端のルーティング テーブルを更新できます。暗号化トンネルを通して学習されたネットワークの IP ルーティング テーブル エントリは、トンネルの他端（GRE トンネル インターフェイスの IP アドレス）を IP ネクスト ホップとして保持します。したがって、トンネルのいずれかの側のネットワークが変更された場合、反対側は動的に変化を認識し、ルータ上で設定を変更することなく接続が継続されます。

基本設定

以下は、標準的なポイントツーポイント IPsec+GRE 設定です。この後、DMVPN のさまざまな機能を示すため、DMVPN ソリューションの特定の機能を段階的に追加した一連の設定例を示します。各例は前の例をベースにし、より複雑化するネットワーク設計において DMVPN ソリューションを使用する方法を示します。この一連の例は、現在の IPsec+GRE から DMVPN に移行するためのテンプレートとして使用できます。設定例が、求めるネットワーク設計の要件と一致する時点で、いつでも「移行」を停止できます。

IPsec + GRE ハブ アンド スポーク（n = 1、2、3、...）



Hub ルータ

```
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.




 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




!
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
```

Spoke1 ルータ

```
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
```

Spoke2 ルータ

```
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> ルータ

```
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.
```

上記の設定では、ACL を使用して、どのトラフィックを暗号化するかを定義します。ハブ ルータとスポーク ルータの両方で、この ACL のみは GRE トンネル IP パケットと一致させる必要があります。どちらかの側でネットワークがどのように変更されても、GRE IP トンネル パケットは変更されないため、この ACL を変更する必要はありません。

注：Cisco IOSソフトウェアバージョン12.2(13)Tより前を使用する場合は、GREトンネルインターフェイス(Tunnel<x>)と物理インターフェイス(Ethernet0)の両方に**crypto map vpnmap1設定コマンドを適用する必要があります。** Cisco IOS バージョン 12.2(13)T およびそれ以降では、**crypto map vpnmap1 設定コマンドを物理インターフェイス (Ethernet0) にのみ適用します。**

ハブ アンド スポーク ルータのルーティング テーブルの例

Hub ルータのルーティング テーブル

```
172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 C       10.0.0.4 is directly connected, Tunnel2
 ...
 C       10.0.0.<4n-4> is directly connected, Tunnel<n>
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.2,
18:28:19, Tunnel1
 D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
Tunnel2
 ...
 D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
2d05h, Tunnel<n>
```

Spoke1 ルータのルーティング テーブル

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
Tunnel0
 ...
 D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 C    192.168.1.0/24 is directly connected, Loopback0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
 ...
 D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
```

Spoke<n> ルータのルーティング テーブル

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.<n>.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 D       10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 ...
 C        10.0.0.<4n-4> is directly connected, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.1.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 ...
 C    192.168.<n>.0/24 is directly connected, Ethernet0
```

これは動作するための基本的な設定であり、DMVPN ソリューションを使用したより複雑な設定と比較するための開始点として使用します。最初の変更では、ハブ ルータの設定サイズを減らします。これは少数のスポーク ルータの場合は重要ではありませんが、50 ~ 100を超えるスポー

ク ルータがある場合は重要になります。

ハブ ルータ設定サイズの削減

次の例では、ハブ ルータにおいて、複数の GRE ポイントツーポイント トンネル インターフェイスから単一の GRE マルチポイント トンネル インターフェイスに最低限の変更がされています。これは DMVPN ソリューションの最初のステップです。

ハブ ルータには、各スポーク ルータの暗号マップ特性を定義するための固有の設定ライン ブロックがあります。この設定部分では、各スポーク ルータの暗号 ACL と GRE トンネル インターフェイスを定義します。これらの特性は、IP アドレス (**set peer …**、**tunnel destination …**) を除き、すべてのスポークでほぼ同じです。

ハブ ルータの上記の設定を見ると、スポーク ルータごとに設定行が最低 13 行あることがわかります。暗号マップに 4 行、暗号 ACL に 1 行、GRE トンネル インターフェイスに 8 行です。スポーク ルータが 300 個ある場合、設定行の総数は 3900 行です。また、各トンネル リンクのアドレッシングには、300 (/30) のサブネットも必要です。このサイズの設定は管理が非常に難しく、VPN ネットワークのトラブルシューティングはさらに困難です。この値を減らすには、ダイナミック暗号マップを使用します。これにより、上記の設定が 1200 行削減でき、300 のスポーク ネットワークでは 2700 行になります。

注：ダイナミック暗号マップを使用する場合、IPsec暗号化トンネルはスポークルータによって開始される必要があります。また、**ip unnumbered <interface> を使用して GRE トンネルに必要なサブネット数を削減することもできますが、後ほどトラブルシューティングをするのが難しくなる場合があります。**

DMVPN ソリューションにより、ハブ ルータ上で単一のマルチポイント GRE トンネル インターフェイスと単一の IPsec プロファイルを設定して、すべてのスポーク ルータを管理することができます。これにより、VPN ネットワークに追加されるスポーク ルータの数にかかわらず、ハブ ルータ上の設定サイズを一定に保つことができます。

DMVPN ソリューションでは、次の新しいコマンドが導入されました。

```
crypto ipsec profile
```

crypto ipsec profile <name> コマンドはダイナミック暗号マップのように使用され、トンネル インターフェイス専用に設計されています。このコマンドは、スポークとハブ間およびスポーク間の VPN トンネル上の IPsec 暗号化パラメータを定義するために使用されます。このプロファイルの下で必要な唯一のパラメータは、トランスフォーム セットです。IPsec ピア アドレスと IPsec プロキシの **match address ... 節は、GRE トンネルの NHRP マッピングから自動的に取得されます。**

tunnel protection ipsec profile <name> コマンドは、GRE トンネル インターフェイス配下で設定され、GRE トンネル インターフェイスを IPsec プロファイルに関連付けるために使用されます。また **tunnel protection ipsec profile <name> コマンドは、ポイントツーポイント GRE トンネルでも使用できます。**この場合、**tunnel source ... および tunnel destination ... 設定から IPsec のピ**

ア情報とプロキシ情報を取得します。これにより IPsec ピアと暗号 ACL が不要になるため、設定が簡素化されます。

注：tunnel **protection ...コマンド**は、GREカプセル化がパケットに追加された後にIPsec暗号化が行われることを指定します。

これらの最初の 2 つの新しいコマンドは、暗号マップを設定し、**crypto map <name> コマンドを使用して、暗号マップをインターフェイスに割り当てるのと似ています。**大きな違いは、新しいコマンドでは、暗号化するパケットに合わせて IPsec ピア アドレスまたは ACL を指定する必要がないことです。これらのパラメータは、mGRE トンネル インターフェイスへの NHRP マッピングから自動的に定義されます。

注：トンネルインターフェイスで**tunnel protection ...コマンドを使用する**と、物理的な発信インターフェイスで**crypto map ...コマンドが設定**されません。

最後の新しいコマンド、**ip nhrp map multicast dynamic** を使用することにより、スポーク ルータが mGRE+IPsec トンネルを開始し、ユニキャスト NHRP マッピングを登録すると、NHRP がマルチキャスト NHRP マッピングにスポーク ルータを自動的に追加することができます。これは、ダイナミック ルーティング プロトコルがハブとスポーク間の mGRE+IPsec トンネルで機能するために必要です。このコマンドを使用できなかった場合、ハブ ルータは各スポークへのマルチキャスト マッピングのために個別の設定行を持つ必要があります。

注：この設定では、ハブルータはスポークに関する情報を使用して設定されていないため、スポークルータはmGRE+IPsecトンネル接続を開始する必要があります。ただし DMVPN では、スポーク ルータの起動時に mGRE+IPsec トンネルが自動的に開始され、常に起動状態が維持されるため、これは問題にはなりません。

注：次の例は、スポークルータのポイントツーポイントGREトンネルインターフェイスと、ハブルータのmGREトンネルをサポートするためにハブルータとスポークルータの両方に追加されたNHRP設定行を示しています。設定変更は次のとおりです。

Hub ルータ (旧)

```
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.




 !
 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
```

Hub ルータ（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> ルータ（旧）

```
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> ルータ（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.




  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
 !
```

スポーク ルータでは、サブネット マスクが変更され、NHRP コマンドがトンネル インターフェイス配下に追加されました。これによりハブ ルータが NHRP を使用してスポーク トンネル インターフェイス IP アドレスをスポークの物理インターフェイス IP アドレスにマッピングするため、NHRP コマンドが必要になります。

ip address 10.0.0.

```
      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
```

サブネットは /30 の代わりに /24 になります。したがって、すべてのノードは別々のサブネットではなく同じサブネット上にあります。スポークはポイントツーポイント GRE トンネル インターフェイスを使用しているため、変わらずスポーク間トラフィックをハブ経由で送信します。**ip nhrp authentication ...、ip nhrp network-id ...、および tunnel key ... コマンドは、トンネル パケットと NHRP パケットがハブで受信されたときに、これらを正しいマルチポイント GRE トンネル インターフェイスと NHRP ネットワークにマッピングするために使用されます。ip nhrp map ...およびip nhrp nhs ...コマンド**は、スポークのNHRPマッピング(10.0.0.<n+1> —> 172.16.<n>.1)をハブにアドバタイズするために、スポーク上のNHRPによって使用されます。この 10.0.0.<n+1> アドレスはトンネル インターフェイスの **ip address ... コマンドから取得され、**

172.16.<n>.1 アドレスはトンネル インターフェイスの tunnel destination ... コマンドから取得されます。

スポーク ルータが 300 個ある場合、この変更により、ハブ上の設定行の数は 3900 行から 16 行に削減できます（3884 行の削減）。 各スポーク ルータの設定は 6 行増加します。

スポークでのダイナミック アドレスのサポート

Cisco ルータでは、IPsec トンネルを起動する前に、各 IPsec ピアに他の IPsec ピアの IP アドレスを設定する必要があります。スポーク ルータが物理インターフェイス上にダイナミック アドレスを持っている場合（DSL またはケーブル リンク経由で接続されているルータでは一般的）、これを行う際に問題が発生します。

TED は、暗号化が必要な元のデータ パケットの IP 宛先アドレスに特別な Internet Security Association and Key Management Protocol（ISAKMP）パケットを送信することによって、1 つの IPsec ピアが別の IPsec ピアを見つけられるようにします。前提条件は、このパケットが、IPsec トンネル パケットと同じ経路にあるネットワークを通過することです。このパケットは他端の IPsec ピアによってピックアップされ、それが最初のピアに応答します。この 2 つのルータは、ISAKMP と IPsec セキュリティ アソシエーション（SA）をネゴシエートし、IPsec トンネルを起動します。これは、暗号化されるデータ パケットがルーティング可能な IP アドレスを持つ場合にのみ機能します。

TED は、前のセクションで設定した GRE トンネルと組み合わせて使用できます。これはテスト済みで動作しますが、Cisco IOS ソフトウェアの以前のバージョンにはバグがありました。そのバグとは、TED が GRE トンネル パケットだけでなく、2 つの IPsec ピア間のすべての IP トラフィックを強制的に暗号化してしまうというものです。DMVPN ソリューションはこの機能と追加機能を提供しますが、ホストがインターネット ルーティング可能な IP アドレスを使用する必要がなく、またプローブ パケットと応答パケットを送信する必要もありません。わずかな変更を加えれば、最後のセクションの設定を使用して、外部物理インターフェイス上に動的な IP アドレスを持つスポーク ルータをサポートすることができます。

Hub ルータ（変更なし）

```
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> ルータ (旧)

```
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.
```

Spoke<n> ルータ (新)

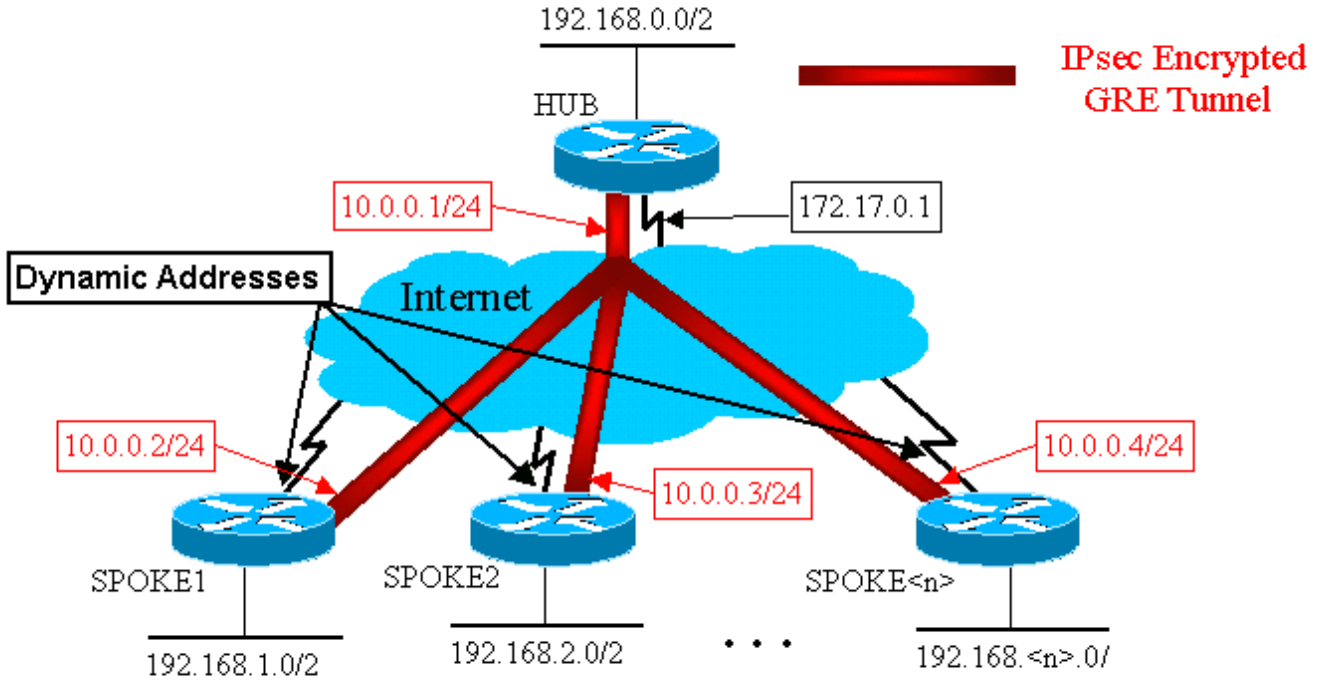
```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  set security-association level per-host
  match address 101
 !
 ...
 !
 access-list 101 permit gre any host 172.17.0.1
```

新しいスポーク設定で使用される機能は次のとおりです。

- GRE トンネル インターフェイスが起動すると、NHRP 登録パケットのハブ ルータへの送信が開始されます。これらの NHRP 登録パケットが IPsec の開始をトリガーします。スポーク ルータで、set peer <peer-address> および **match ip access-list <ACL> コマンドが設定されます。**ACL はプロトコルとして GRE を指定し、送信元に any を指定し、宛先に ハブ IP アドレスを指定します。**注：**ACLの送信元としてanyが使用されていることに注意してください。スポークルータのIPアドレスは動的であるため、物理インターフェイスがアクティブになる前には不明であるため、この場合もそうである必要があります。ダイナミック スポーク インターフェイス アドレスがそのサブネット内のアドレスに制限されている場合、IP サブネットを ACL の送信元として使用できます。
- **set security-association level per-host コマンドを使用し、スポーク IPsec プロキシの IP 送信先を、ACLの「any」ではなく、スポークの現在の物理インターフェイス アドレス (/32) にします。**ACL の「any」が IPsec プロキシの送信元として使用された場合、他のスポーク ルータもこのハブとの IPsec+GRE トンネルを設定できなくなります。これは、その結果ハブ上の IPsec プロキシが **permit gre host 172.17.0.1 any** と同等になるためです。これは、すべてのスポーク宛てのすべての GRE トンネル パケットが暗号化され、ハブとのトンネルを最初に確立したスポークに送信されることを意味します。これは、その IPsec プロキシがすべてのスポークの GRE パケットと一致するためです。
- IPsec トンネルが設定されると、NHRP 登録パケットが、スポーク ルータから設定されたネクスト ホップ サーバ (NHS) に送信されます。 NHS はこのハブアンドスポーク ネットワークのハブ ルータです。NHRP 登録パケットは、このスポーク ルータの NHRP マッピングを作成するためのハブ ルータの情報を提供します。このマッピングを使用すると、ハブ ルータは、このスポーク ルータへのユニキャスト IP データ パケットを mGRE+IPsec トンネル経由

で転送できます。また、ハブはスポーク ルータをその NHRP マルチキャスト マッピング リストに追加します。次にハブは、ダイナミック IP ルーティング マルチキャスト パケットのスポークへの送信を開始します（ダイナミック ルーティング プロトコルが設定されている場合）。 次にスポークはハブのルーティング プロトコル ネイバーになり、ルーティング更新を交換します。

IPsec + mGRE ハブ アンド スポーク



Hub ルータ

```
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
!
```

上記のハブの設定では、スポーク ルータの IP アドレスが設定されていないことに注意してください。スポークの外部物理インターフェイスとスポークのトンネル インターフェイス IP アドレスへのマッピングは、NHRP 経由でハブが動的に学習します。これにより、スポークの外部物理インターフェイス IP アドレスを動的に割り当てることができます。

Spoke1 ルータ

```
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
```

Spoke2 ルータ

```
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
```

スポークの設定について注意すべき主な事項は次のとおりです。

- 外部物理インターフェイス（ethernet0）の IP アドレスは DHCP 経由で動的です。**ip address dhcp hostname Spoke2**
- 暗号 ACL（101）は、サブネットを IPsec プロキシの送信元として指定します。**access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1**
- IPsec 暗号マップの次のコマンドは、セキュリティ アソシエーションがホストごとになるよう指定します。**set security-association level per-host**
- すべてのトンネルはハブ ルータ上の同じマルチポイント GRE インターフェイス経由で接続されているため、同じサブネットの一部です。**ip address 10.0.0.2 255.255.255.0**

これら 3 つのコマンドを組み合わせると、スポークの外部物理インターフェイス IP アドレスを設定する必要がなくなります。使用される IPsec プロキシは、サブネットベースではなくホストベースになります。

スポーク ルータは IPsec+GRE トンネルを開始する必要があるため、スポーク ルータの設定には、ハブ ルータの IP アドレスが設定されています。Spoke1 と Spoke2 の設定の類似点に注目してください。これら 2 つが似ているだけでなく、すべてのスポーク ルータの設定も似ています。ほとんどの場合、すべてのスポークはインターフェイス上で一意の IP アドレスを必要とし、残りの設定は同じになります。これにより、多くのスポーク ルータを即座に設定し、展開することができます。

NHRP データはハブとスポークで次のようになります。

Hub ルータ

```
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
```

Spoke1 ルータ

```
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
```

ダイナミック マルチポイント ハブ アンド スポーク

上記のスポーク ルータの設定は DMVPN ソリューションの機能に依存しないため、スポーク ルータはバージョン 12.2(13)T より前の Cisco IOS ソフトウェアを実行できます。ハブルータの設

定は DMVPN の機能に依存するため、Cisco IOS バージョン 12.2(13)T およびそれ以降を実行する必要があります。これにより、すでに展開されているスポーク ルータをいつの時点でアップグレードする必要があるかを柔軟に決めることができます。スポーク ルータで Cisco IOS バージョン 12.2(13)T またはそれ以降を実行している場合、次のようにスポークの設定を簡素化できます。

Spoke<n> ルータ（Cisco IOS 12.2(13)T より前）

```
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> ルータ（Cisco IOS 12.2(13)T 以降）

```
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>
 !
```

次の作業を実施済みであることに注意してください。

1. **crypto map vpnmap1 10 ipsec-isakmp コマンドを削除し、**crypto ipsec profile vpnprof で置き換えました。
2. Ethernet0 インターフェイスから **crypto map vpnmap1 コマンドを削除し、tunnel protection ipsec profile vpnprof コマンドを Tunnel0 インターフェイスに設定しました。**
3. 暗号 ACL、**access-list 101 permit gre any host 172.17.0.1** を削除しました。

この場合、IPsec ピア アドレスとプロキシは自動的に **tunnel source ... および tunnel destination ... 設定から取得されます。**ピアとプロキシは次のとおりです（**show crypto ipsec sa コマンドの出力に表示されます**）。

```
...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...
```

要約すると、以下のフル設定には、[基本設定（IPsec+GRE ハブ アンド スポーク）からここまでに行われたすべての変更が含まれます。]

Hub ルータ

```
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
!
```

ハブの設定に変更はありません。

Spoke1 ルータ

```
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
!
```

Spoke2 ルータ

```
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
!
```

ダイナミック マルチポイント IPsec VPN

このセクションの概念と設定では、DMVPN のすべての機能を示します。NHRP は、スポーク ルータが VPN ネットワーク内の他のスポーク ルータの外部物理インターフェイス アドレスを動的に学習する機能を提供します。これは、スポーク ルータが、他のスポーク ルータに直接 IPsec+mGRE トンネルを動的に構築するために十分な情報を持つことを意味します。このスポーク間データ トラフィックがハブ ルータ経由で送信された場合、暗号化/復号化する必要があり、ハブ ルータ上での遅延と負荷が 2 倍増えるため、これは有利です。この機能を使用するには、スポーク ルータをポイントツーポイント GRE (p-pGRE) からマルチポイント GRE (mGRE) トンネル インターフェイスに切り替える必要があります。また他のスポーク ルータのトンネル IP アドレスの IP ネクストホップを使用して、他のスポークの背後で利用可能な (サブ) ネットワークも学習する必要があります。スポーク ルータは、ハブとの IPsec+mGRE トンネルを介して実行されるダイナミック IP ルーティング プロトコル経由で、これらの (サブ) ネットワークを学習します。

このハブ ルータで実行されているダイナミック IP ルーティング プロトコルは、1 つのスポークから学習したルートを、他のすべてのスポークへの同じインターフェイスに反映し戻すように設定できますが、通常これらのルート上の IP ネクストホップは、ハブがこのルートを学習したスポーク ルータではなく、ハブ ルータになります。

注：ダイナミックルーティングプロトコルはハブアンドスポークリンクでのみ動作し、ダイナミックスポークツースポークリンクでは動作しません。

このダイナミック ルーティング プロトコル (RIP、OSPF、および EIGRP) は、ハブ ルータ上で、ルートを mGRE トンネル インターフェイスに戻すようアドバタイズします。またルートを他のスポークに戻すようアドバタイズされたときに、1 つのスポークから学習したそのルートの発信元スポーク ルータを IP ネクストホップに 設定する必要があります。

ルーティング プロトコルの設定要件は次のとおりです。

RIP

ハブの mGRE トンネル インターフェイス上で、スプリット ホライズンをオフにする必要があります。そうでない場合、RIP は mGRE インターフェイスを介して学習したルートを同じインターフェイスに戻すようアドバタイズしません。

```
no ip split-horizon
```

その他の変更は必要ありません。RIP は、これらのルートを学習したのと同じインターフェイスに戻すようアドバタイズするルートで、発信元の IP ネクストホップを自動的に使用します。

EIGRP

ハブの mGRE トンネル インターフェイス上で、スプリット ホライズンをオフにする必要があります。そうでない場合、EIGRP は mGRE インターフェイスを介して学習したルートを同じインターフェイスに戻すようアドバタイズしません。

```
no ip split-horizon eigrp
```

デフォルトの設定では、EIGRP は、ルートを学習したインターフェイスと同じインターフェイス上でルートをアドバタイズする場合でも、IP ネクストホップ値に、アドバタイズするルートのハブ ルータを設定します。この場合、これらのルートをアドバタイズするときに発信元の IP ネクストホップを使用するよう EIGRP に指示するには、次の設定コマンドが必要です。

```
no ip next-hop-self eigrp
```

注：no ip next-hop-self eigrp <as>コマンドは、Cisco IOSリリース12.3(2)以降で使用できます。12.2(13)T と 12.3(2) 間の Cisco IOS リリースでは、次の作業を行う必要があります。

- スポーク間ダイナミック トンネルを使用しない場合、上記のコマンドは不要です。
- spoke-to-spoke ダイナミック トンネルを使用する場合、スポーク ルータのトンネル インターフェイス上でプロセス スイッチングを使用する必要があります。
- それ以外の場合は、DMVPN で別のルーティング プロトコルを使用する必要があります。

OSPF

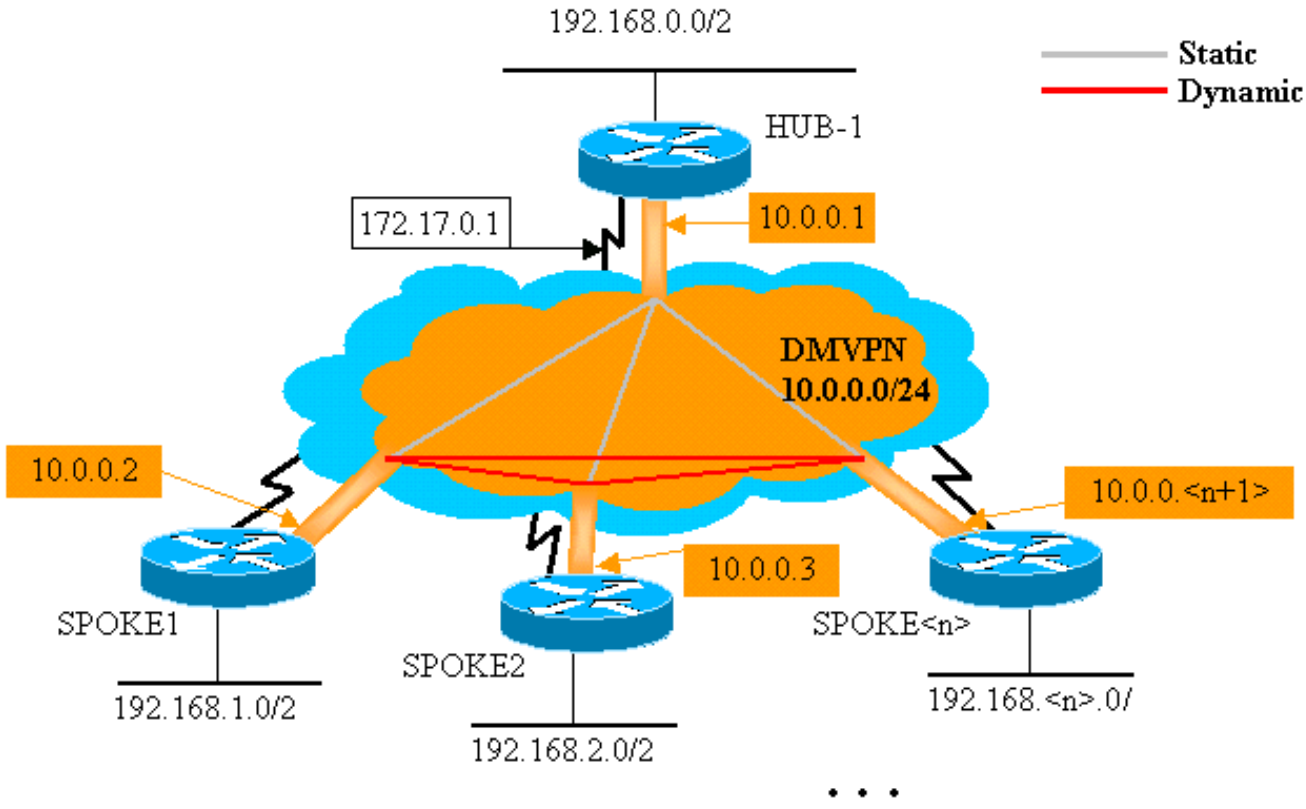
OSPF はリンクステート ルーティング プロトコルのため、スプリット ホライズンの問題はありません。通常マルチポイント インターフェイスの場合、OSPF ネットワーク タイプにポイントツーマルチポイントを設定しますが、これにより OSPF はスポーク ルータのルーティング テーブルにホスト ルートを追加します。これらのホスト ルートによって、他のスポーク ルータの背後にあるネットワーク宛てのパケットは、他のスポークに直接転送されず、ハブ経由で転送されます。この問題を回避するため、このコマンドを使用して、ブロードキャストする OSPF ネットワーク タイプを設定します。

```
ip ospf network broadcast
```

また、ハブ ルータが IPsec+mGRE ネットワークの代表ルータ（DR）になることを確認する必要があります。これは、OSPF プライオリティをハブ上では 1 より大きく、スポーク上では 0 より大きく設定することで実行できます。

- ハブ：ip ospf priority 2
- スポーク：ip ospf priority 0

DMVPN シングル ハブ



Hub ルータ

```
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
 !
```

ハブ設定の唯一の変更点は、ルーティング プロトコルが EIGRP ではなく OSPF であることです。OSPF ネットワーク タイプにブロードキャストが設定され、プライオリティに 2 が設定されていることに注意してください。OSPF ネットワーク タイプにブロードキャストを設定すると、OSPF は IP ネクストホップ アドレスを持つスポーク ルータの背後にあるネットワークのルートを、そのスポーク ルータの GRE トンネルとしてインストールします。

Spoke1 ルータ

```
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
!
```

このスポーク ルータの設定は、ハブの設定と非常によく似ています。違いは次のとおりです。

- OSPFプライオリティが0に設定されています。スポークルータは、mGRE非ブロードキャストマルチアクセス(NBMA)ネットワークのDRにすることはできません。ハブ ルータのみがすべてのスポーク ルータへの直接スタティック接続ができます。DR は NBMA ネットワークのすべてのメンバーにアクセスできる必要があります。
- ハブ ルータ用に設定された NHRP ユニキャスト マッピングとマルチキャスト マッピングがあります。

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

  以前の設定では、GRE トンネルがポイントツーポイントであったため、**ip nhrp map multicast dynamic... コマンドは必要ありませんでした。**その場合、マルチキャスト パケットは、1 つの可能な宛先へのトンネルを通して、自動的にカプセル化されます。スポーク GRE トンネルがマルチポイントに変更され、複数の可能な宛先が存在するため、現在はこのコマンドが必要になります。
- ハブ ルータにはスポーク ルータに関する情報が設定されておらず、スポーク ルータには IP アドレスが動的に割り当てられるため、スポーク ルータが起動したときに、ハブとのトンネル接続を開始する必要があります。スポーク ルータはまた、NHRP NHS としてハブが設定されています。

  ```
  ip nhrp nhs 10.0.0.1
  ```

上記のコマンドを使用すると、スポーク ルータは、NHRP 登録パケットをハブ ルータに mGRE+IPsec トンネルを通して定期的に送信します。これらの登録パケットは、ハブ ルータがスポーク ルータにパケットをトンネリングして戻すために必要な、スポーク NHRP マッピング情報を提供します。

Spoke2 ルータ

```
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> ルータ

```
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.




!
```

すべてのスポーク ルータの設定が非常に似ていることに注目してください。唯一の違いは、ローカル インターフェイス上の IP アドレスです。これは、多数のスポーク ルータを展開する場合に役立ちます。すべてのスポーク ルータを完全に同じように設定でき、ローカル IP インターフェイス アドレスだけを追加する必要があります。

この時点で、Hub、Spoke1、および Spoke2 ルータ上のルーティング テーブルと NHRP マッピング テーブルを参照し、初期状態 (Spoke1 と Spoke2 ルータを起動直後) 、および Spoke1 と Spoke2 によってその間のダイナミック リンクが作成された後の状態を確認します。

初期状態

Hub ルータの情報

```
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
```

Spoke1 ルータの情報

```
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
```

Spoke2 ルータの情報

```
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
```

この時点で、192.168.1.2から192.168.2.3にpingを実行します。これらのアドレスは、それぞれSpoke1ルータとSpoke2ルータの背後にあるホスト用です。直接スポーク間 mGRE+IPsec トンネルを構築するための、次の一連のイベントが発生します。

1. Spoke1ルータは、宛先192.168.2.3のpingパケットを受信します。ルーティングテーブルでこの宛先を検索し、このパケットをTunnel0インターフェイスからIPネクストホップ10.0.0.3に転送する必要があることを検出します。
2. Spoke1 ルータは宛先 10.0.0.3 への NHRP マッピング テーブルを確認し、エントリがないことがわかります。Spoke1 ルータは NHRP 解決要求パケットを作成し、NHS (ハブ ルータ) に送信します。
3. ハブルータは、宛先10.0.0.3に対するNHRPマッピングテーブルをチェックし、アドレス172.16.2.75にマッピングされていることを検出します。ハブルータはNHRP解決応答パケットを作成し、Spoke1ルータに送信します。
4. Spoke1ルータはNHRP解決応答を受信し、NHRPマッピングテーブルに10.0.0.3—>172.16.2.75マッピングを入力します。NHRP マッピングを追加すると、それがトリガーとなり、ピア 172.16.2.75 との IPsec トンネルが開始されます。
5. Spoke1 ルータは 172.16.2.75 で ISAKMP を開始し、ISAKMP と IPsec SA をネゴシエートします。IPsec プロキシは、Tunnel0 **tunnel source <address> コマンドと NHRP マッピングから取得します。**

   ```
   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. IPsec トンネルの構築が完了すると、192.168.2.0/24 サブネットへのすべてのデータ パケットは直接 Spoke2 に送信されます。
7. 192.168.2.3宛てのパケットがホストに転送された後、このホストは192.168.1.2に戻りパケットを送信します。Spoke2ルータは、192.168.1.2宛のこのパケットをルーティングテーブルで検索し、このパケットをIPネクストホップ10.0.0.2にTunnel0インターフェイスに転送する必要があります。
8. Spoke2 ルータは宛先 10.0.0.2 への NHRP マッピング テーブルを確認し、エントリがないことがわかります。Spoke2 ルータは NHRP 解決要求パケットを作成し、NHS (ハブ ルータ) に送信します。

9. ハブルータは、宛先10.0.0.2に対するNHRPマッピングテーブルをチェックし、アドレス172.16.1.24にマッピングされていることを検出します。ハブルータはNHRP解決応答パケットを作成し、Spoke2ルータに送信します。
10. Spoke2ルータはNHRP解決応答を受信し、NHRPマッピングテーブルに10.0.0.2 —> 172.16.1.24マッピングを入力します。NHRP マッピングを追加すると、それがトリガーとなり、ピア 172.16.1.24 との IPsec トンネルが開始されますが、すでにピア 172.16.1.24 との IPsec トンネルが存在するため、これ以上何もする必要はありません。
11. これにより、Spoke1 と Spoke2 はパケットを互いに直接転送できるようになりました。NHRP マッピングが、保留時間の間パケットの転送に使用されない場合、NHRP マッピングは削除されます。NHRP マッピング エントリを削除すると、IPsec はこの直接リンクへの IPsec SA を削除します。

Spoke1 と Spoke2 間にダイナミック リンクが作成された後の状態

Spoke1 ルータの情報

```
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
```

Spoke2 ルータの情報

```
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
```

上記の出力から、Spoke1 と Spoke2 がハブルータからお互いへの NHRP マッピングを取得し、mGRE+IPsec トンネルを構築し、使用したことがわかります。NHRP マッピングは 5 分後に無効になります（現在の NHRP 保留時間 = 300 秒）。 NHRP マッピングが無効になる直前に使用された場合、NHRP 解決要求と応答が送信され、エントリが削除される前に更新されます。そうでない場合、NHRP マッピングは削除され、IPsec によって IPsec SA がクリアされます。

デュアル ハブを備えたダイナミック マルチポイント IPSec VPN

スポーク ルータに数行の設定行を追加することで、冗長性のためのデュアル（または複数の）ハブ ルータを設定できます。デュアル ハブ DMVPN を設定するには、2 つの方法があります。

- 各スポークに 1 つのマルチポイント GRE トンネルインターフェイスを持ち、ネクストホップ サーバ（NHS）として 2 つの異なるハブを指すシングル DMVPN ネットワーク。ハブ ルータには、1 つのマルチポイント GRE トンネル インターフェイスしかありません。
- 各スポークに 2 つの GRE トンネル インターフェイス（ポイントツーポイントまたはマルチポイント）を持ち、それぞれの GRE トンネルが異なるハブ ルータに接続された、デュアル DMVPN ネットワーク。この場合も、ハブ ルータには、1 つのマルチポイント GRE トンネル インターフェイスしかありません。

次の例では、デュアル ハブ DMVPN のこれら 2 つの異なるシナリオの設定について説明します。どちらの場合も、ハイライトされた違いは、DMVPN のシングル ハブ設定に関連しています。

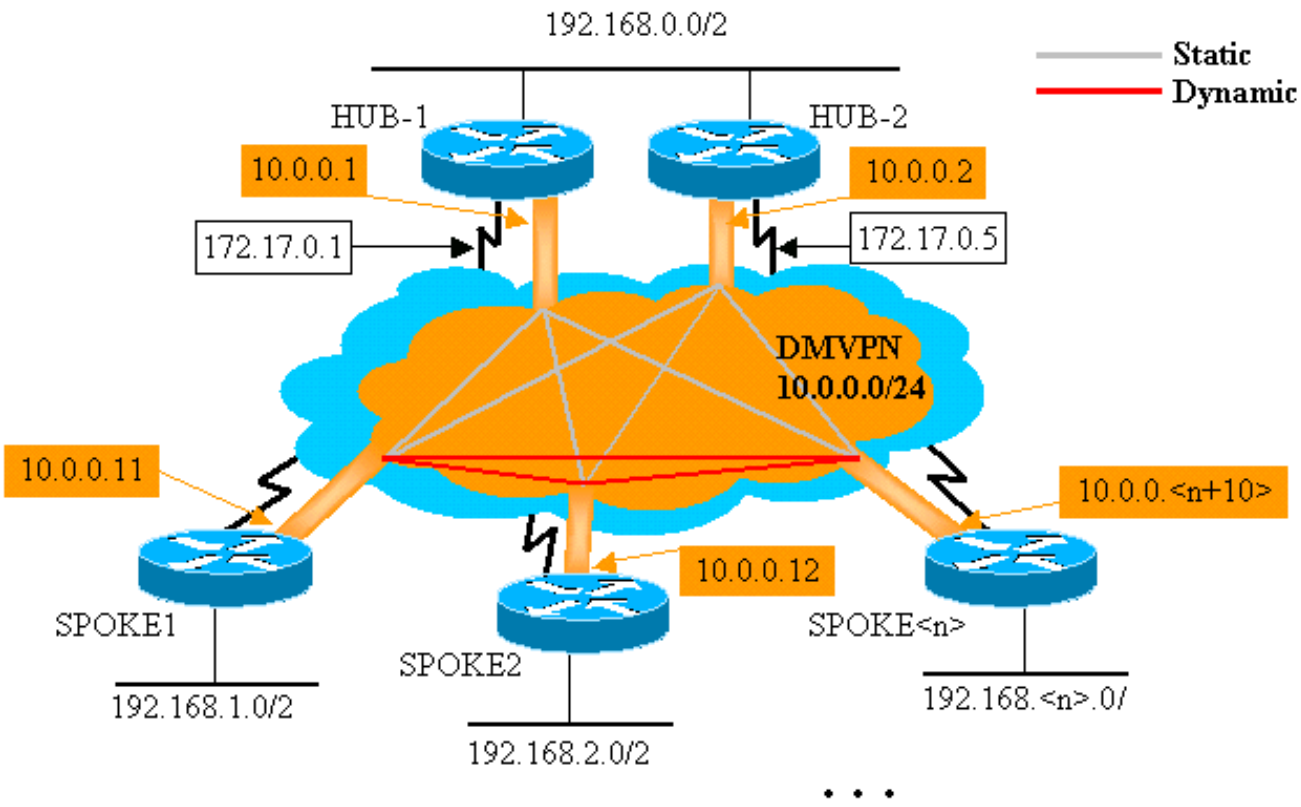
デュアル ハブ - シングル DMVPN レイアウト

シングル DMVPN レイアウトのデュアル ハブは設定が非常に簡単ですが、デュアル DMVPN レイアウトのデュアル ハブほど DMVPN を通るルーティングを制御できるわけではありません。この場合の考え方は、すべてのハブ（この場合 2 つ）とすべてのスポークがこの 1 つのサブネット（「クラウド」）に接続された、シングル DMVPN「クラウド」を持つことです。 このスポークからハブへのスタティック NHRP マッピングは、ダイナミック ルーティング プロトコルが実行されるスタティック IPsec+mGRE リンクを決定します。ダイナミック ルーティング プロトコルは、スポーク間のダイナミック IPsec+mGRE リンク上では実行されません。このスポーク ルータは、同じ mGRE トンネル インターフェイス上のハブ ルータでネイバーをルーティングしているため、リンクまたはインターフェイスの違い（メトリック、コスト、遅延、または帯域幅など）を使って、2 つのハブが起動しているときに 1 つのハブをもう 1 つのハブより優先するよう、ダイナミック ルーティング プロトコル メトリックを変更することはできません。このプリファレンスが必要な場合は、内部からルーティング プロトコルの設定へのテクニックを使用する必要があります。このため、ダイナミック ルーティング プロトコルには OSPF ではなく、EIGRP または RIP を使用した方がよい場合があります。

注：上記の問題は、通常、ハブルータが同じ場所に配置されている場合にのみ発生します。それらが同じ場所に配置されていない場合、ハブ ルータ経由で宛先ネットワークに到達できる場合で

も、通常のダイナミック ルーティングが正しいハブ ルータを優先する可能性が高くなります。

デュアル ハブ - シングル DMVPN レイアウト



Hub ルータ

```
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 ルータ

```
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
!
```

Hub1 の設定における唯一の変更点は、2 つのエリアを使用するよう OSPF を変更することです。エリア 0 は 2 つのハブの背後にあるネットワークに使用され、エリア 1 は DMVPN ネットワークと、スポーク ルータの背後にあるネットワークに使用されます。OSPF は 1 つのエリアを使用できますが、ここでは複数の OSPF エリアの設定を示すため、2 つのエリアを使用しています。

Hub2 の設定は基本的に Hub1 の設定と同じで、IP アドレスが適切に変更されています。主な違いの 1 つは、Hub2 が Hub1 のスポーク（またはクライアント）でもあり、Hub1 がプライマリ ハブに、Hub2 がセカンダリ ハブになることです。これが設定されると、Hub2 が mGRE トンネル上で Hub1 の OSPF ネイバーになります。Hub1 は OSPF DR であるため、mGRE インターフェイス（NBMA ネットワーク）上の他のすべての OSPF ルータと直接接続する必要があります。Hub1 と Hub2 間の直接リンクがないと、Hub1 も動作している場合に、Hub2 は OSPF ルーティングに参加しません。Hub1 がダウンすると、Hub2 は DMVPN（NBMA ネットワーク）の OSPF DR になります。 Hub1 が復旧すると、DMVPN の OSPF DR であることを引き継ぎます。

Hub1とHub2の背後にあるルータは、GREトンネルインターフェイスの帯域幅がHub1をスポークネットワークに送信するために使用します。これに対し、Hub2の900 Kb/secに設定されています。これは、ハブルータの背後にあるネットワークのパケットをHub1とHub2に送信します各スポークルータにトンネルインターフェイスがあり、2つの等コストルートがあります。パケットごとのロード バランシングが使用されている場合、これによりパケットの順序の乱れが起きる可能性があります。

Spoke1 ルータ

```
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
!
```

スポーク ルータの設定の違いは次のとおりです。

- 新しい設定では、スポークに Hub2 へのスタティック NHRP マッピングが設定され、Hub2 がネクストホップ サーバとして追加されます。オリジナル：

  ```
  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
  ```

  新しい：

  ```
  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
  ```

- スポーク ルータの OSPF エリアはエリア 1 に変更されました。

ハブのスポーク ルータでスタティック NHRP マッピングと NHS を定義することで、このトンネル上でダイナミック ルーティング プロトコルを実行することになります。これはハブ アンド スポーク ルーティングまたはネイバー ネットワークを定義します。Hub2はすべてのスポークのハブであり、Hub1のスポークでもあります。これにより、DMVPNソリューションを使用する際に、マルチレイヤハブアンドスポークネットワークの設計、設定、および変更が容易になります。

Spoke2 ルータ

```
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> ルータ

```
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.




!
```

この時点で、Hub1、Hub2、Spoke1、Spoke2 ルータ上のルーティング テーブル、NHRP マッピング テーブル、および IPsec 接続を参照し、初期状態 (Spoke1 と Spoke2 ルータを起動直後) を確認できます。

初期状態と変更

Hub1 ルータの情報

```
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 ルータの情報

```
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
```

Spoke1 ルータの情報

```
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
```

Spoke2 ルータの情報

```
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
```

Hub1、Hub2、Spoke1、および Spoke2 のルーティング テーブルには、いくつかの興味深い問題があります。

- 両ハブ ルータは、スポーク ルータの背後にあるネットワークと同等のコスト ルートを持っています。Hub1：

  ```
  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
  ```

  Hub2：

  ```
  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
  ```

  これは、Hub1 と Hub2 がスポーク ルータの背後にあるネットワークと同じコストを、ハブ ルータの背後にあるネットワークのルータにアドバタイズすることを意味します。たとえば、192.168.0.0/24 LAN に直接接続されているルータ、R2 のルーティング テーブルは次のようになります。R2:

  ```
  O     IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3
                          [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3O
  O     IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
                          [110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3
  ```

- スポーク ルータは、両方のハブ ルータ経由で、ハブ ルータ背後のネットワークと同じコスト ルートを持ちます。Spoke1：

  ```
  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
  ```

  Spoke2：

  ```
  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
  ```

  スポーク ルータがパケットごとのロード バランシングを行っている場合、順序が正しくないパケットを受け取る可能性があります。

2 つのハブへのリンク間で、非対称ルーティングまたはパケットごとのロード バランシングが行われないようにするには、両方向で 1 つのスポークとハブ間のパスを優先するよう、ルーティング プロトコルを設定する必要があります。Hub1 をプライマリに、Hub2 をバックアップにするには、ハブ トンネル インターフェイスの OSPF コストを異なる値に設定します。

Hub1：

```
interface tunnel0
...
ip ospf cost 10
...
```

Hub2：

```
interface tunnel0
```

```
...
ip ospf cost 20
...
```
ルートは次のように表示されます。

Hub1：

```
O     192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O     192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```
Hub2：

```
O     192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O     192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```
R2:

```
O     IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O     IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```
これで、2 つのハブ ルータは、スポーク ルータの背後にあるネットワークへのルートで異なるコストを持つようになります。これは、ルータR2で確認できるように、Hub1がスポークルータにトラフィックを転送するために優先されることを意味します。これは、上記の最初の箇条書きで説明されている非対称ルーティングの問題に対処します。

上記 2 番目の箇条書きで説明した、他方向の非対称ルーティングはまだ存在します。ダイナミック ルーティング プロトコルとして OSPF を使用する場合、スポークの **router ospf 1 配下で distance ... コマンドを使用し、Hub2 経由で学習したルートより Hub1 経由で学習したルートを優先させることで、これを回避できます。**

Spoke1：

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```
Spoke2：

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```
ルートは次のように表示されます。

Spoke1：

```
O     192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```
Spoke2：

```
O     192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```
上記のルーティング設定により、非対称ルーティングから保護し、同時に Hub1 がダウンすると Hub2 にフェールオーバーすることができます。これは、両方のハブが起動しているときは、Hub1 だけが使用されることを意味します。フェールオーバー保護を使用し、非対称ルーティン

グを使用せずに、ハブ間のスポークのバランスをとりながら両方のハブを使用する場合、ルーティング設定が複雑になる場合があります。OSPF を使用する場合は特に複雑になります。このため、次のデュアル DMVPN レイアウトのデュアル ハブが適しています。

デュアル ハブ - デュアル DMVPN レイアウト

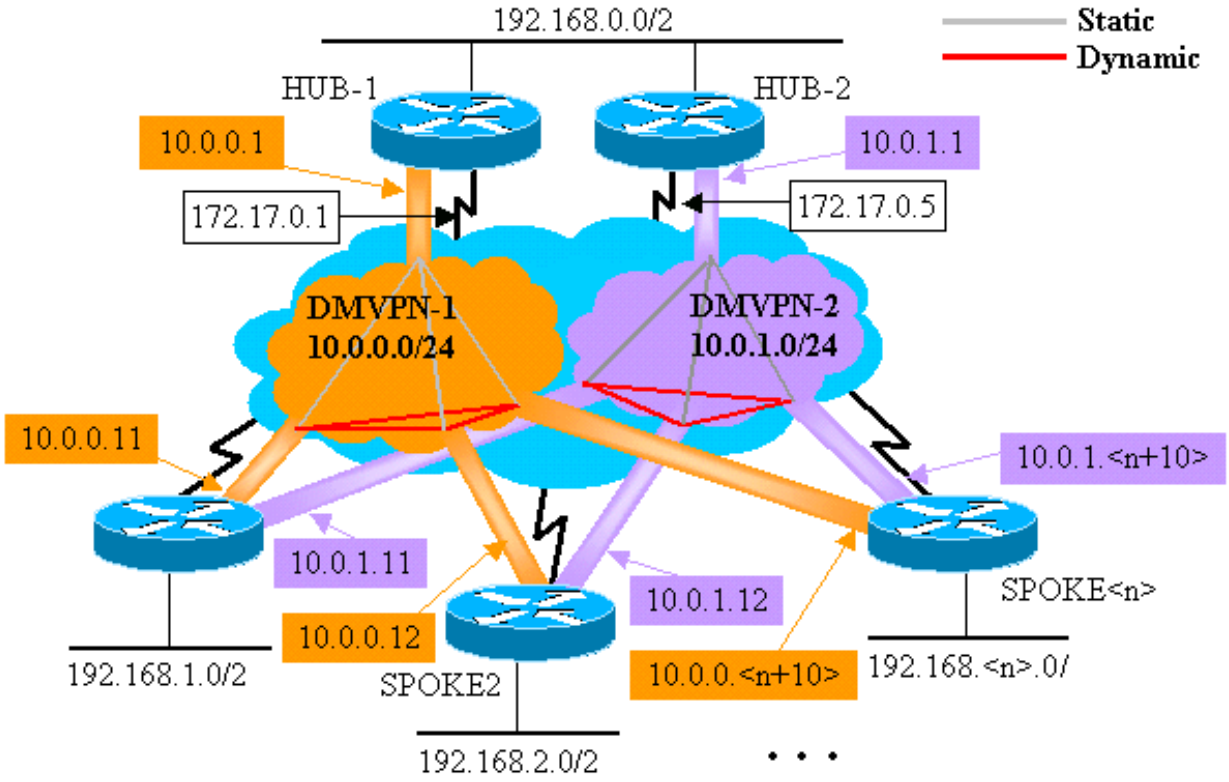
デュアル DMVPN レイアウトのデュアル ハブは設定が少し難しいですが、DMVPN を通るルーティングをより適切に制御できます。考え方は、2 つの別々の DMVPN 「クラウド」を持つことです。 各ハブ (この場合 2 つ) は 1 つの DMVPN サブネット (「クラウド」) に接続され、スポークは両方の DMVPN サブネット (「クラウド」) に接続されます。 このスポーク ルータは、2 つの GRE トンネル インターフェイス上の両方のハブ ルータでネイバーをルーティングしているため、インターフェイス設定の違い (帯域幅、コスト、遅延など) を使って、2 つのハブが起動しているときに 1 つのハブをもう 1 つのハブより優先するよう、ダイナミック ルーティング プロトコル メトリックを変更できます。

注：上記の問題は、通常、ハブルータが同じ場所に配置されている場合にのみ関連します。それらが同じ場所に配置されていない場合、ハブ ルータ経由で宛先ネットワークに到達できる場合でも、通常のダイナミック ルーティングが正しいハブ ルータを優先する可能性が高くなります。

このスポーク ルータでは、p-pGRE または mGRE トンネル インターフェイスのいずれかを使用できます。スポークルータ上の複数のp-pGREインターフェイスは、同じトンネルソ**ースを使用できます。**IPアドレスですが、スポークルータ上の複数のmGREインターフェイスには、一意のトンネルソ**ースが必要です。**IP アドレス。これは、IPsec の開始時の最初のパケットが、mGRE トンネルの 1 つと関連付ける必要がある ISAKMP パケットのためです。ISAKMP パケットには、この関連付けを行う宛先 IP アドレス (リモート IPsec ピア アドレス) しかありません。このアドレスは **tunnel source ... アドレスと照合されますが、両方のトンネルは同じ tunnel source ... アドレスを持つため、常に最初の mGRE トンネル インターフェイスと合致します。**これは、受信するマルチキャスト データ パケットが誤った mGRE インターフェイスに関連付けられ、ダイナミック ルーティング プロトコルを破ってしまう可能性があることを意味します。

GRE パケット自体には、この 2 つの mGRE インターフェイスを区別するための **tunnel key ... 値があるため、この問題は生じません。**Cisco IOS ソフトウェア リリース 12.3(5) および 12.3(7)T より、この制限を解決するため、追加パラメータが導入されました：**トンネル保護....shared**この **shared キーワードは、複数の mGRE インターフェイスが、同じ 送信元 IP アドレスを持つ IPSec 暗号化を使用することを示します。**これ以前のリリースの場合、このデュアル DMVPN レイアウトのデュアル ハブで p-pGRE トンネルを使用できます。p-pGREトンネルの場合、トンネルの**送信元とトンネルの宛先**の両方**が**...IPアドレスを照合に使用できます。この例では、p-pGREトンネルがこのデュアル DMVPN レイアウトのデュアル ハブで使用され、**shared 修飾子は使用されません。**

デュアル ハブ - デュアル DMVPN レイアウト



次のハイライトされている変更点は、本書の前半で説明したダイナミック マルチポイント ハブおよびスポークの設定に関連しています。

Hub1 ルータ

```
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 ルータ

```
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
!
```

この場合、Hub1 と Hub2 の設定は似ています。主な違いは、それぞれが異なる DMVPN のハブであることです。各 DMVPN は異なる次のものを使用します。

- IP サブネット (10.0.0.0/24、10.0.0.1/24)
- NHRP ネットワーク ID (100000、100001)
- トンネル キー (100000、100001)

ダイナミック ルーティング プロトコルは OSPF から EIGRP に切り替えられました。本書の後半で説明するように、EIGRP を使用して NBMA ネットワークを設定、管理する方が簡単なためです。

Spoke1 ルータ

```
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
!
```

各スポーク ルータでは 2 つの p-GRE トンネル インターフェイスが、2 つの DMVPN のそれぞれに 1 つずつ設定されています。この **ip address ...、ip nhrp network-id ...、tunnel key ...、および tunnel destination ... の値は、この 2 つのトンネルを区別するために使用されます。**ダイナミック ルーティング プロトコルの EIGRP は、両方の p-pGRE トンネル サブネットで実行され、1 つの p-pGRE インターフェイス (DMVPN) を他のものの中から選択するために使用されます。

Spoke2 ルータ

```
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> ルータ

```
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.




  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.




  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
!
```

この時点で、Hub1、Hub2、Spoke1、Spoke2 ルータ上のルーティング テーブル、NHRP マッピング テーブル、および IPsec 接続を参照し、初期状態 (Spoke1 と Spoke2 ルータを起動直後) を確認してみましょう。

初期状態と変更

Hub1 ルータの情報

```
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 ルータの情報

```
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
```

Spoke1 ルータの情報

```
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
```

Spoke2 ルータの情報

```
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
```

ここでも、Hub1、Hub2、Spoke1、および Spoke2 のルーティング テーブルには、いくつかの興味深い点があります。

- 両ハブ ルータは、スポーク ルータの背後にあるネットワークと同等のコスト ルートを持っています。Hub1：

```
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
```

Hub2：

```
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
```

これは、Hub1 と Hub2 がスポーク ルータの背後にあるネットワークと同じコストを、ハブ ルータの背後にあるネットワークのルータにアドバタイズすることを意味します。たとえば、192.168.0.0/24 LAN に直接接続されているルータ、R2 のルーティング テーブルは次のようになります。R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
                                [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                    [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3
```

- スポーク ルータは、両方のハブ ルータ経由で、ハブ ルータ背後のネットワークと同じコスト ルートを持ちます。Spoke1：

```
D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1
                                [90/3097600] via 10.0.0.1, 00:26:30, Tunnel0
```

Spoke2：

```
D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1
                                [90/3097600] via 10.0.0.1, 00:38:04, Tunnel0
```

スポーク ルータがパケットごとのロード バランシングを行っている場合、順序が正しくないパケットを受け取る可能性があります。

2 つのハブへのリンク間で、非対称ルーティングまたはパケットごとのロード バランシングが行われないようにするには、両方向で 1 つのスポークとハブ間のパスを優先するよう、ルーティング プロトコルを設定する必要があります。Hub1 をプライマリに、Hub2 をバックアップにするには、ハブ トンネル インターフェイスの遅延を異なる値に設定します。

Hub1：

```
interface tunnel0
...
delay 1000
...
```

Hub2：

```
interface tunnel0
...
delay 1050
...
```

注：この例では、Hub2のトンネルインターフェイスの遅延に50が追加されました。これは、2つのハブ(100)間のEthernet1インターフェイスの遅延よりも小さいためです。 これにより、Hub2はスポークルータにパケットを直接転送しますが、Hub1よりも望ましくないルートをHub1とHub2の背後にあるルータにアドバタイズします。遅延が100以上増加した場合、Hub1とHub2の背後にあるルータはHub1を介して転送しますスポークルータに送信します。

ルートは次のように表示されます。

Hub1：

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

Hub2：

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

2つのハブルータは、スポークルータの背後にあるネットワークルートのコストが異なるため、この場合は、R2で確認できるように、Hub1がスポークルータへのトラフィック転送に優先されます。これは、上記の最初の箇条書きで説明した問題に対処します。

上記 2 番目の箇条書きで説明した問題はまだ存在しますが、2 つの p-pGRE トンネル インターフェイスがあるため、このトンネル インターフェイスに個別に **delay ... を設定し、EIGRP メトリックを Hub1 と Hub2 から学習したルートに変更できます。**

Spoke1：

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Spoke2：

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

ルートは次のように表示されます。

Spoke1：

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

Spoke2：

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

上記のルーティング設定により、非対称ルーティングから保護し、同時に Hub1 がダウンすると Hub2 にフェールオーバーすることができます。これは、両方のハブが起動しているときは、Hub1 だけが使用されることを意味します。

フェールオーバー保護を使用し、非対称ルーティングを使用せずに、ハブ間のスポークのバランスをとりながら両方のハブを使用する場合、ルーティング設定はより複雑になりますが、EIGRP を使用する場合にこれが可能です。これを達成するには、ハブ ルータのトンネル インターフェイスの **delay ... を等しくするように設定してから、スポーク ルータで offset-list <acl> out <offset>**

<interface> コマンドを使用し、GRE トンネル インターフェイスからバックアップ ハブにアドバタイズされたルートの EIGRP メトリックを増やします 。スポークの Tunnel0 と Tunnel1 のインターフェイス間の等しくない **delay ... は引き続き使用されるため、スポーク ルータはプライマリ ハブ ルータを優先します。**スポーク ルータの変更点は次のとおりです。

Spoke1 ルータ

```
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
 !
```

Spoke2 ルータ

```
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
!
```

注：オフセット値12800(50*256)は、25600(100*256)よりも小さいため、EIGRPメトリックに追加されました。 この値 (25600) は、ハブ ルータ間で学習されたルートの EIGRP メトリックに追加されるものです。**Offset-list コマンドで 12800 を使用すると、バックアップ ハブ ルータは、これらのパケットをスポークのプライマリ ハブ ルータを通り、イーサネット経由で転送するのではなく、パケットをスポーク ルータに直接転送します。**ハブ ルータによってアドバタイズされたルートのメトリックは、正しいプライマリ ハブ ルータが優先されるものになります。スポークの半分は Hub1 をプライマリ ルータとして使用し、残りの半分は Hub2 をプライマリ ルータとして使用します。

注：オフセット値が25600(100*256)以上に増加した場合、ハブは、ハブの背後にあるルータがスポークルータにパケットを送信するために正しいハブを優先する場合でも、もう一方のハブを経由経由ででスポークルータにパケットを転送転送します。

注：スポーク上の1つのトンネルインターフェイスを介して1つのハブルータから学習したルート

を、もう1つのトンネルを介して別のハブにアドバタイズできるため、distribute-list 1 outコマンドも追加されました。distribute-list ... コマンドは、スポーク ルータが自身のルートだけをアドバタイズできることを保証します。

注：スポークルータではなくハブルータでルーティングアドバタイズメントを制御する場合**は、スポークではなくハブルータでoffset-list <acl1> in <value> <interface>コマンドとdistribute-list <acl2>コマンドを設定できます**。<acl2> access-list にはすべてのスポークの背後からのルートがリストされ、<acl1> access-list には別のハブ ルータがプライマリ ハブになるスポークからのルートだけがリストされます。

これらの変更により、ルートは次のようになります。

Hub1：

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

Hub2：

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

Spoke1：

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

Spoke2：

```
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

結論

DMVPN ソリューションは、大小さまざまな IPsec VPN ネットワークに合わせて拡大縮小するため、次の機能を提供します。

- DMVPN により、フル メッシュまたは部分メッシュ IPsec VPN のより良いスケーリングが可能になります。これは、スポーク間トラフィックが散発的な場合（たとえば、全スポークが常に他の全スポークにデータを送信しているわけではないなど）、特に有用です。 スポーク間の直接 IP 接続がある限り、どのスポークも他のスポークに直接データを送信できます。
- DMVPN は、動的に割り当てられたアドレスを持つ IPsec ノード（ケーブル、ISDN、DSL など）をサポートします。これは、ハブアンドスポークおよびメッシュ ネットワークに適用されます。DMVPN が常に稼働しているためにはハブからスポークへのリンクが必要です。
- DMVPN は VPN ノードの追加を簡素化します。新しいスポーク ルータを追加する場合は、スポーク ルータを設定し、ネットワークに接続するだけで済みます（ただし、ハブ上で新しいスポークの場合、ISAKMP 認証情報を追加する必要があります）。 ハブは新しいスポークについて動的に学習し、ダイナミック ルーティング プロトコルは、ハブおよび他のすべての

スポークへのルーティングを伝播します。
- DMVPN は、VPN 内のすべてのルータで必要な設定のサイズを削減します。GRE+IPsec ハブアンドスポーク専用 VPN ネットワークの場合も同様です。
- DMVPN は GRE を使用するため、VPN 間の IP マルチキャストおよびダイナミック ルーティング トラフィックをサポートします。これは、ダイナミック ルーティング プロトコルを使用でき、冗長な「ハブ」をこのプロトコルでサポートできることを意味します。マルチキャスト アプリケーションもサポートされています。
- DMVPN はスポークでのスプリット トンネリングをサポートします。

関連情報

- Dynamic Multipoint VPN（DMVPN）
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems