DMVPN スポークでの ISP 冗長性を VRF-Lite 機能で設定する

内容

概要

このドキュメントでは、Virtual Routing and Forwarding-Lite （ VRF-Lite ）機能を使用して Dynamic Multipoint VPN （ DMVPN ）スポーク上でインターネット サービス プロバイダー （ ISP ）の冗長性を設定する方法について説明します。

前提条件

要件

このドキュメントで説明する設定を開始する前に、次の項目に関する知識があることが推奨されます。

- VRF に関する基礎知識

- Enhanced Interior Gateway Routing Protocol（EIGRP）に関する基礎知識
- DMVPN に関する基礎知識

使用するコンポーネント

このドキュメントの情報は、Cisco IOS® バージョン 15.4(2)T 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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

VRF は IP ネットワーク ルータに含まれているテクノロジーであり、これによりルータ内にルーティング テーブルの複数のインスタンスを共存させ、それらを同時に使用できます。これにより、複数のデバイスを使用しなくてもネットワーク パスをセグメント化できるため、機能性が向上します。

冗長性のためにデュアル ISP を使用するのが一般的になりつつあります。管理者は、2 つの ISP のリンクを使用します。そのうちの 1 つはプライマリ接続として機能し、もう一方はバックアップ接続として機能します。

デュアル ISP を利用したスポーク上の DMVPN の冗長性にも同じ概念を実践できます。このドキュメントの目的は、*VRF-Lite を使用してスポークがデュアル ISP を持つ場合にルーティング テーブルを分離する方法を示すことです。*DMVPN トンネルを通過するトラフィックのパスの冗長性を提供するのにダイナミック ルーティングが使用されます。このドキュメントで説明している構成例は、この構成スキーマを使用しています。

インターフェイス	iSCSIポータルの	VRF	説明
Ethernet0/0	172.16.1.1	ISP1	プライマリ
Ethernet0/1	172.16.2.1	ISP2	セカンダリ

VRF-Lite 機能を使用すると、DMVPN スポーク上で複数の VPN ルーティング/転送インスタンスをサポートできます。VRF-Lite の機能は、複数の multipoint Generic Routing Encapsulation（mGRE）トンネル インターフェイスからのトラフィックに、それぞれの VRF ルーティング テーブルを使用するように強制します。たとえば、プライマリ ISP が *ISP1 VRF で終端し、セカンダリ ISP が ISP2 VRF で終端する場合、ISP2 VRF で生成されたトラフィックは ISP2 VRF ルーティング テーブルを使用する一方で、ISP1* VRF で生成されたトラフィックは ISP1 VRF ルーティング テーブルを使用します。

フロント ドア VRF（FVRF）を使用する利点は、主に、（トンネル インターフェイスが存在する）グローバル ルーティング テーブルから独立したルーティング テーブルを分割できる点です。 内部 *VRF（iVRF）を使用する利点は、DMVPN とプライベート ネットワークの情報を保持するためにプライベート空間を定義する点です。*これらの構成の両方は、ルーティング情報が分離されるので、インターネットからのルータに対する攻撃に対し、高度なセキュリティを提供します。

これらの VRF 構成は、DMVPN ハブとスポークの両方で使用できます。これは、両方の ISP がグローバル ルーティング テーブルで終端するようなシナリオに対して大幅な利点を提供します。

ISP の両方がグローバル VRF で終端すると、それらは同じルーティング テーブルを共有し、両方の mGRE インターフェイスは、グローバル ルーティング情報に依存します。その場合、プライマリ ISP に障害が発生すると、障害点が ISP のバックボーン ネットワーク内にあり、直接接続されていない場合、プライマリ ISP のインターフェイスがダウンしない可能性があります。これにより、mGRE トンネル インターフェイスの両方が引き続きプライマリ ISP を指すデフォルト ルートを使用する結果、DMVPN の冗長性が失敗してしまうようなシナリオになります。

VRF-Lite を使用せずにこの問題に対処するために、IP サービス レベル契約（IP SLA）または組み込みイベント マネージャ（EEM）のスクリプトを使用するような回避策がいくつかありますが、そのような回避策が常に最良の選択とは限りません。

導入方式

この項では、スプリット トンネリングおよびスポーク間トンネルの簡単な概要について説明します。

スプリット トンネリング

特定のサブネットまたは集約ルートが mGRE インターフェイス経由で学習されている場合、それは*スプリット トンネリング*と呼ばれます。デフォルト ルートが mGRE インターフェイス経由で学習される場合、それは *tunnel-all* と呼ばれます。

このドキュメントで説明している構成例は、スプリット トンネリングに基づいています。

スポーク間トンネル

このドキュメントで説明している構成例は、tunnel-all 導入方式（デフォルト ルートが mGRE インターフェイス経由で学習される）のための優れたデザインを示しています。

2 つの fVRF を使用することで、ルーティング テーブルを分離し、GRE カプセル化後のパケットがそれぞれの fVRF に転送されるので、スポーク間トンネルがアクティブな ISP を確実に提供するのに役立ちます。

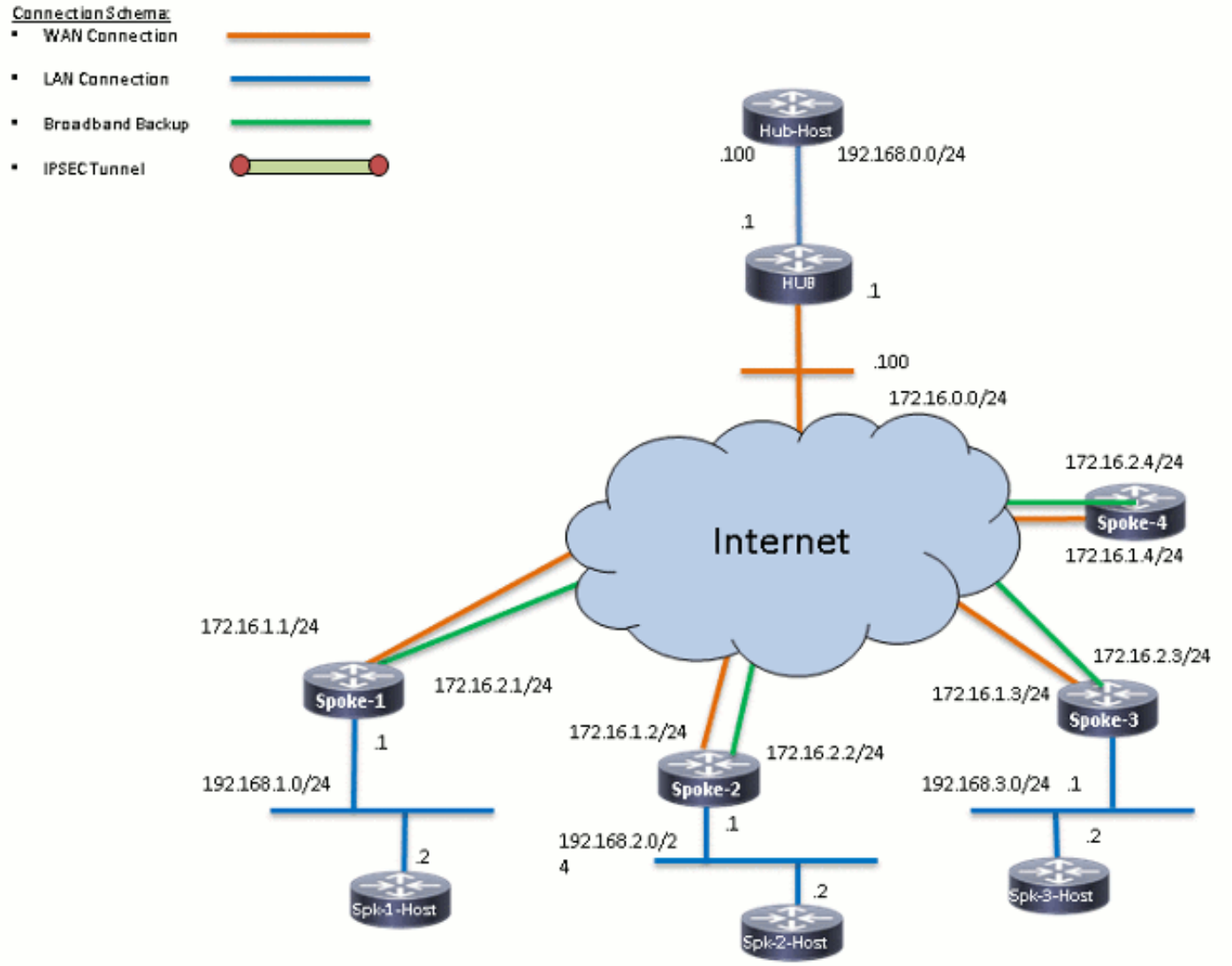
設定

この項では、VRF-Lite 機能経由で DMVPN スポーク上に ISP の冗長性を設定する方法について説明します。

> **注：**このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

次の図は、このドキュメントに含まれる例として使用されるトポロジです。



ハブ設定

ハブに関する設定についての いくつかの注意事項は、次のとおりです。

- *この構成例では、tunnel0 をプライマリ インターフェイスとして設定するために delay パラメータが変更されており、Tunnel0 から学習したルートを優先できるようになります。*

- **shared キーワードがトンネル保護で使用されます。さらに、mGRE インターフェイスは同じトンネル送信元 <インターフェイス> を使用するので、固有のトンネル キー**がすべての mGRE インターフェイスに追加されます。それ以外の場合、受信 Generic Routing Encapsulation （ GRE ）トンネル パケットは、復号後に不正なトンネル インターフェイスにパントされる可能性があります。

- すべてのスポークが mGRE トンネル（ **tunnel-all** ）経由でデフォルト ルートを確実に学習するために、ルート要約が実施されます。

  注：この例は、設定の関連するセクションのみを示しています。

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HUB1
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback0
 description LAN
 ip address 192.168.0.1 255.255.255.0
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile profile-dmvpn shared
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 no ip split-horizon eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 ip nhrp redirect
 ip summary-address eigrp 1 0.0.0.0 0.0.0.0
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile profile-dmvpn shared
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
```

```
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route 0.0.0.0 0.0.0.0 172.16.0.100
!
end
```

スポーク設定

スポークに関する設定についての いくつかの注意事項は、次のとおりです。

- スポークの冗長性のために、*Tunnel0 および Tunnel1 がそれぞれ Ethernet0/0 と Ethernet0/1 をトンネル送信元インターフェイスとして備えています。*Ethernet0/0 はプライマリ ISP に、Ethernet0/1 はセカンダリ ISP に接続されます。
- ISP を分離するために、VRF 機能が使用されます。プライマリ ISP は *ISP1 VRF を使用します。*セカンダリ ISP については、*ISP2 という名前の VRF が設定されます。*
- GRE 暗号化後のパケットの転送ルックアップが VRF ISP1 または ISP2 のいずれかで実行されることを示すために、*tunnel vrf ISP1 および tunnel vrf ISP2 がそれぞれインターフェイス Tunnel0 と Tunnel1 とに設定されます。*
- この構成例では、tunnel0 をプライマリ インターフェイスとして設定するために *delay* パラメータが変更されており、*Tunnel0 から学習したルートを優先できるようになります。*

  注：この例は、設定の関連するセクションのみを示しています。

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SPOKE1
!
vrf definition ISP1
 rd 1:1
 !
 address-family ipv4
 exit-address-family
!
vrf definition ISP2
 rd 2:2
 !
 address-family ipv4
 exit-address-family
!
crypto keyring ISP2 vrf ISP2
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring ISP1 vrf ISP1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 24
```

```
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set transform-dmvpn esp-aes 256 esp-sha256-hmac
 mode transport
!
!
crypto ipsec profile profile-dmvpn
 set transform-set transform-dmvpn
!
interface Loopback10
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 description Primary mGRE interface source as Primary ISP
 bandwidth 1000
 ip address 10.0.0.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.0.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel vrf ISP1
 tunnel protection ipsec profile profile-dmvpn
!
interface Tunnel1
 description Secondary mGRE interface source as Secondary ISP
 bandwidth 1000
 ip address 10.0.1.10 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp network-id 100001
 ip nhrp holdtime 360
 ip nhrp nhs 10.0.1.1 nbma 172.16.0.1 multicast
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 delay 1500
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel vrf ISP2
 tunnel protection ipsec profile profile-dmvpn
!
interface Ethernet0/0
 description Primary ISP
 vrf forwarding ISP1
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/1
 description Seconday ISP
 vrf forwarding ISP2
 ip address 172.16.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip route vrf ISP1 0.0.0.0 0.0.0.0 172.16.1.254
```

```
ip route vrf ISP2 0.0.0.0 0.0.0.0 172.16.2.254
!
logging dmvpn
!
end
```

確認

設定が適切に機能することを検証するためにこの項で説明されている情報を活用してください。

プライマリとセカンダリの ISP がアクティブ

この検証シナリオでは、プライマリとセカンダリの両方の ISP がアクティブです。このシナリオに関する追加の注意事項は次のとおりです。

- 両方の mGRE インターフェイスに対して、フェーズ 1 およびフェーズ 2 が動作しています。
- 両方のトンネルが起動しますが、Tunnel0 経由のルート（プライマリ ISP 経由で供給される）が優先されます。

このシナリオの設定を確認するのに使用できる、**show の関連コマンドは次のとおりです。**

```
SPOKE1#show ip route
<snip>
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 1w0d, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>
```

```
Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

プライマリ ISP がダウン/セカンダリ ISP がアクティブ

このシナリオでは、ISP1 リンクがダウンすると、ネイバーシップから Tunnel0 までの EIGRP *Hold タイマーの期限が切れ、ハブおよび他のスポークが Tunnel1（Ethernet0/1 によって供給される）を指すようになります。*

このシナリオの設定を確認するのに使用できる、**show の関連コマンドは次のとおりです。**

```
*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.1.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/3072000] via 10.0.1.1, 00:00:20, Tunnel1

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
```

```
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show ip route vrf ISP1

Routing Table: ISP1
<snip>

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.1.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0

SPOKE1#show ip route vrf ISP2

Routing Table: ISP2
<snip>

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.2.254
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Ethernet0/1
L        172.16.2.1/32 is directly connected, Ethernet0/1

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: DOWN
Peer: 172.16.0.1 port 500
 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

       Active SAs: 0, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel0
Session status: DOWN-NEGOTIATING
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive

!--- Tunnel0 is Inactive and the routes are preferred via Tunnel1.

 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Inactive
```

プライマリ ISP リンクの復旧

プライマリ ISP 経由の接続が復旧すると、Tunnel0 の暗号化セッションがアクティブになり、Tunnel0 インターフェイス経由で学習したルートが優先されます。

以下が一例です。

```
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency

SPOKE1#show ip route
<snip>

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

D*    0.0.0.0/0 [90/2944000] via 10.0.0.1, 00:00:45, Tunnel0

!--- This is the default route for all of the spoke and hub LAN segments.

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/24 is directly connected, Tunnel0
L        10.0.0.10/32 is directly connected, Tunnel0
C        10.0.1.0/24 is directly connected, Tunnel1
L        10.0.1.10/32 is directly connected, Tunnel1
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Loopback10
L        192.168.1.1/32 is directly connected, Loopback10

SPOKE1#show crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.1.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 172.16.0.1 port 500
 Session ID: 0
 IKEv1 SA: local 172.16.2.1/500 remote 172.16.0.1/500 Active

!--- Tunnel0 is Active and the routes are preferred via Tunnel0.

 IPSEC FLOW: permit 47 host 172.16.2.1 host 172.16.0.1
       Active SAs: 2, origin: crypto map
```

トラブルシュート

設定のトラブルシューティングを実施するには、**debug ip eigrp および logging dmvpn** を有効化します。

以下が一例です。

```
################## Tunnel0 Failed and Tunnel1 routes installed ####################

*Sep  2 14:07:33.374: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is down: holding time expired
*Sep  2 14:07:33.374: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:07:33.391: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:33.399: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
*Sep  2 14:07:36.686: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is DOWN
*Sep  2 14:07:36.686: %DMVPN-5-NHRP_NHS_DOWN: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1 ) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is DOWN, Reason:
External(NHRP: no error)

################## Tunnel0 came up and routes via Tunnel0 installed #################

*Sep  2 14:15:55.120: %DMVPN-5-CRYPTO_SS:  Tunnel0: local address : 172.16.1.1 remote
address : 172.16.0.1 socket is UP
*Sep  2 14:15:56.109: %DMVPN-5-NHRP_NHS_UP: Tunnel0: Next Hop Server : (Tunnel:
10.0.0.1 NBMA: 172.16.0.1) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is  UP
*Sep  2 14:15:59.128: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.0.0.1 (Tunnel0)
is up: new adjacency
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/3072000) origin(10.0.1.1)
*Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0
(90/2944000) origin(10.0.0.1)
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel0
*Sep  2 14:16:01.214: EIGRP-IPv4(1): table(default): 0.0.0.0/0 - do advertise
out Tunnel1
```

関連情報

- 最も一般的な DMVPN のトラブルシューティング方法
- Cisco MDS 9000 ファミリ トラブルシューティング ガイド、リリース 2.x：IPsec のトラブルシューティング
- テクニカル サポートとドキュメント – Cisco Systems