VRF-Lite 기능으로 DMVPN 스포크에서 ISP 이중화 구성

목차

소개

이 문서에서는 VRF-Lite(Virtual Routing and Forwarding-Lite) 기능을 통해 DMVPN(Dynamic Multipoint VPN) 스포크에서 ISP(Internet Service Provider) 이중화를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 설명된 컨피그레이션을 시도하기 전에 이러한 주제에 대해 알고 있는 것이 좋습니다.

- VRF에 대한 기본 지식
- EIGRP(Enhanced Interior Gateway Routing Protocol)에 대한 기본 지식

- DMVPN에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® 버전 15.4(2)T를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

VRF는 라우팅 테이블의 여러 인스턴스가 라우터에 공존하고 동시에 작동할 수 있도록 하는 IP 네트워크 라우터에 포함된 기술입니다.이렇게 하면 여러 디바이스를 사용하지 않고도 네트워크 경로를 분할할 수 있으므로 기능이 향상됩니다.

이중화를 위해 이중 ISP를 사용하는 것이 일반적인 관행이 되었습니다.관리자는 두 개의 ISP 링크를 사용합니다.하나는 기본 연결 역할을 하고 다른 하나는 백업 연결 역할을 합니다.

이중 ISP를 사용하여 스포크의 DMVPN 이중화에 동일한 개념을 구현할 수 있습니다.이 문서의 목적은 스포크에 이중 ISP가 있는 경우 라우팅 테이블을 분리하기 위해 VRF-*Lite*를 사용하는 방법을 시연하는 것입니다.동적 라우팅은 DMVPN 터널을 통과하는 트래픽에 대한 경로 이중화를 제공하기 위해 사용됩니다.이 문서에 설명된 구성 예제는 다음 구성 스키마를 사용합니다.

인터페이스	IP 주소	VRF	설명
이더넷0/0	172.16.1.1	ISP1 VRF	기본 ISP
이더넷0/1	172.16.2.1	ISP2 VRF	보조 ISP

VRF-Lite 기능을 사용하면 DMVPN 스포크에서 여러 VPN 라우팅/포워딩 인스턴스를 지원할 수 있습니다.VRF-Lite 기능은 여러 mGRE(Multipoint Generic Routing Encapsulation) 터널 인터페이스의 트래픽이 해당 VRF 라우팅 테이블을 사용하도록 강제합니다.예를 들어, 기본 ISP가 *ISP1 VRF에서 종료되고 보조 ISP가 ISP2* VRF에서 종료되는 경우 *ISP2* VRF에서 생성된 트래픽은 ISP2 VRF 라우팅 테이블을 사용하고 *ISP1 VRF에서 생성된 트래픽은 ISP1 VRF 라우팅 테이블을 사용합니다.*

전면 도어 VRF(fVRF)를 사용할 때 얻을 수 있는 이점은 주로 전역 라우팅 테이블(터널 인터페이스가 있는 경우)에서 별도의 라우팅 테이블을 분할하는 것입니다. iVRF(*내부* VRF)를 사용할 때의 이점은 DMVPN 및 프라이빗 네트워크 정보를 저장하기 위해 전용 공간을 정의하는 것입니다.이 두 컨피그레이션 모두 라우팅 정보가 분리된 인터넷으로부터 라우터에 대한 공격으로부터 추가적인 보안을 제공합니다.

이러한 VRF 컨피그레이션은 DMVPN 허브와 스포크 모두에서 사용할 수 있습니다.이렇게 하면 글로벌 라우팅 테이블에서 두 ISP가 모두 종료되는 시나리오보다 훨씬 유리합니다.

두 ISP가 모두 전역 VRF에서 종료되면 동일한 라우팅 테이블을 공유하고 mGRE 인터페이스 모두 전역 라우팅 정보를 사용합니다.이 경우 기본 ISP에 장애가 발생하면 장애 지점이 ISP의 백본 네트워크에 있고 직접 연결되지 않은 경우 기본 ISP 인터페이스가 다운되지 않을 수 있습니다.따라서

mGRE 터널 인터페이스 두 인터페이스가 여전히 기본 ISP를 가리키는 기본 경로를 사용하므로 DMVPN 이중화가 실패합니다.

VRF-Lite 없이 이 문제를 해결하기 위해 IP SLA(IP Service Level Agreements) 또는 EEM(Embedded Event Manager) 스크립트를 사용하는 몇 가지 해결 방법이 있지만, 이러한 방법이 항상 최선의 선택은 아닐 수 있습니다.

배포 방법

이 섹션에서는 스플릿 터널링 및 스포크 투 스포크 터널에 대한 간략한 개요를 제공합니다.

스플릿 터널링

mGRE 인터페이스를 통해 특정 서브넷 또는 요약 경로를 학습하면 *스플릿 터널링이라고 합니다* .mGRE 인터페이스를 통해 기본 경로를 학습하면 이를 tunnel-all이라고 *합니다*.

이 문서에서 제공되는 구성 예제는 스플릿 터널링을 기반으로 합니다.

스포크 투 스포크 터널

이 문서에서 제공하는 컨피그레이션 예는 tunnel-all 구축 방법을 위한 좋은 설계입니다(기본 경로는 mGRE 인터페이스를 통해 학습됨).

2개의 fVRF를 사용하면 라우팅 테이블을 분리하고, GRE 이후 캡슐화된 패킷이 각 fVRF에 전달되도록 할 수 있습니다. 따라서 스포크 투 스포크 터널이 활성 ISP를 제공하는지 확인할 수 있습니다.

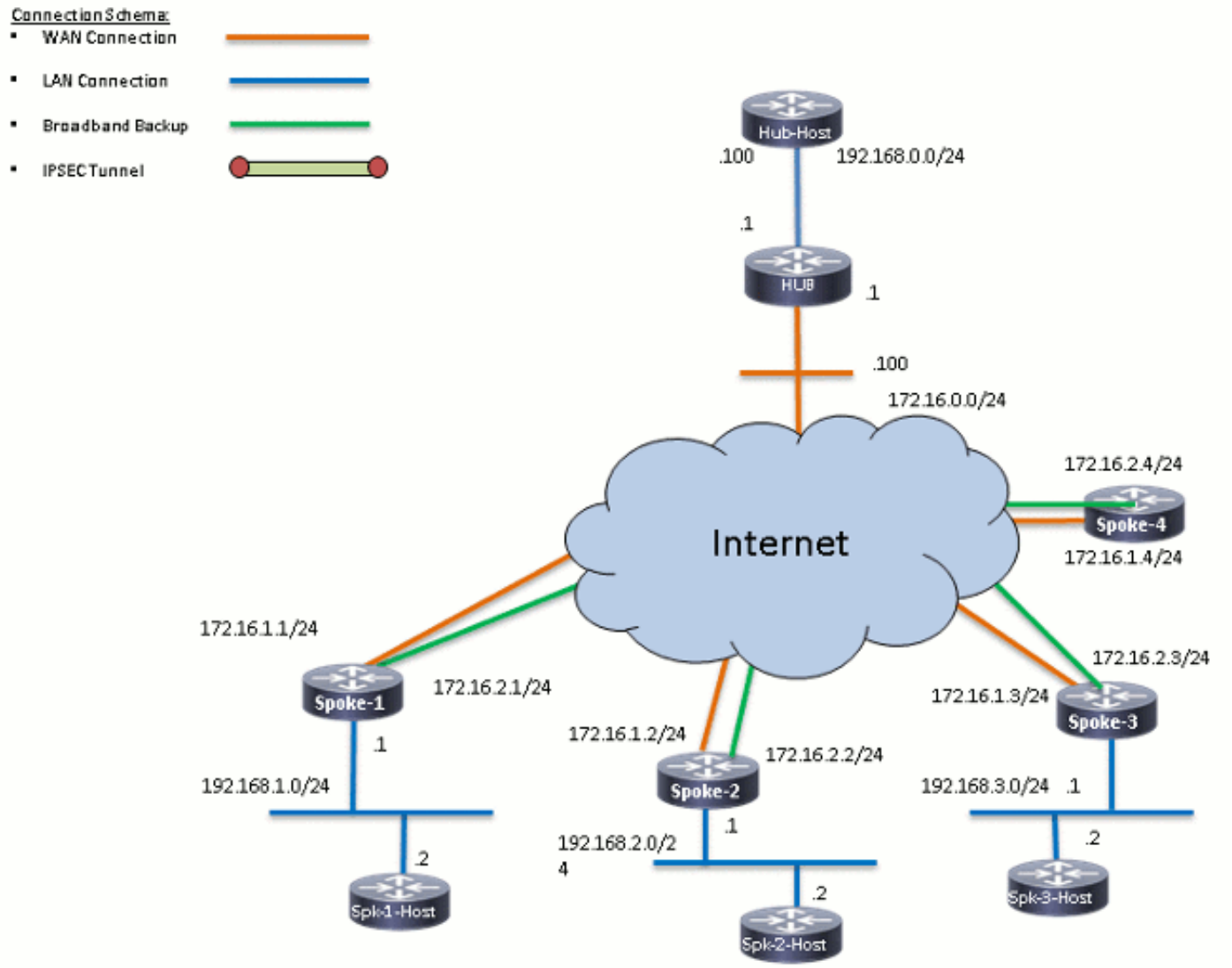
구성

이 섹션에서는 VRF-Lite 기능을 통해 DMVPN 스포크에서 ISP 이중화를 구성하는 방법에 대해 설명합니다.

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

이 문서 내의 예제에 사용되는 토폴로지입니다.



허브 구성

다음은 허브의 관련 컨피그레이션에 대한 몇 가지 참고 사항입니다.

- 이 컨피그레이션 예에서 *Tunnel0*을 기본 인터페이스로 설정하기 위해 *delay* 매개 변수가 변경되어 Tunnel0에서 학습된 경로가 더 선호됩니다.
- shared 키워드는 터널 보호와 함께 사용되며 모든 mGRE 인터페이스에서 동일한 *터널 소스 <interface>*를 사용하므로 고유한 *터널 키*가 *추가됩니다*.그렇지 않으면 암호 해독 후 인바운드 GRE(Generic Routing Encapsulation) 터널 패킷이 잘못된 터널 인터페이스에 펀딩될 수 있습니다.
- 모든 스포크가 mGRE 터널(**tunnel-all**)을 통해 기본 경로를 학습하도록 경로 요약이 수행됩니다.

  참고:이 예에는 컨피그레이션의 관련 섹션만 포함됩니다.

```
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
```

스포크 구성

다음은 스포크의 관련 구성에 대한 몇 가지 참고 사항입니다.

- 스포크 리던던시의 경우 *Tunnel0* 및 *Tunnel1*은 *Ethernet0/0* 및 *Ethernet0/1*을 각각 터널 소스 인터페이스로 사용합니다.Ethernet0/0은 기본 ISP에 연결되고 Ethernet0/1은 보조 ISP에 연결됩니다.

- ISP를 분리하기 위해 VRF 기능이 사용됩니다.기본 ISP는 *ISP1* VRF를 사용합니다.보조 ISP의 경우 *ISP2*라는 VRF*가* 구성됩니다.

- VRF *ISP1* 및 *터널 vrf ISP2*는 각각 Tunnel0 및 Tunnel1 인터페이스에 구성되어 VRF ISP1 또는 ISP2에서 GRE 캡슐화된 패킷에 대한 포워딩 조회가 수행됨을 나타냅니다.

- 이 컨피그레이션 예에서 Tunnel0을 기본 인터페이스로 설정하기 위해 *지연* 매개 변수가 변경되었으며, 이를 통해 Tunnel0에서 학습된 경로가 더 선호됩니다.

  참고:이 예에는 컨피그레이션의 관련 섹션만 포함됩니다.

```
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
```

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션에 설명된 정보를 사용하십시오.

기본 및 보조 ISP 활성

이 확인 시나리오에서는 기본 및 보조 ISP가 모두 활성 상태입니다.이 시나리오에 대한 몇 가지 추가 참고 사항이 있습니다.

- 두 mGRE 인터페이스의 1단계와 2단계가 모두 작동합니다.
- 두 터널 모두 작동하지만 Tunnel0(기본 ISP를 통해 제공)을 통한 경로가 우선합니다.

이 시나리오에서 컨피그레이션을 확인하기 위해 사용할 수 있는 관련 **show** 명령은 다음과 같습니다.

```
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
```

기본 ISP 다운/보조 ISP 활성

이 시나리오에서는 ISP1 링크가 다운되면 Tunnel0을 통해 인접 디바이스에 대해 EIGRP 보류 타이머가 만료되고 허브 및 다른 스포크에 대한 경로가 Tunnel1을 가리킵니다(Ethernet0/1을 통해 제공).

이 시나리오에서 컨피그레이션을 확인하기 위해 사용할 수 있는 관련 **show** 명령은 다음과 같습니다.

```
*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
```

기본 ISP 링크 복원

기본 ISP를 통한 연결이 복원되면 Tunnel0 암호화 세션이 활성화되고 Tunnel0 인터페이스를 통해 학습된 경로가 우선합니다.

예를 들면 다음과 같습니다.

```
*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
```

문제 해결

컨피그레이션 문제를 해결하려면 debug ip eigrp 및 **logging dmvpn을 활성화합니다**.

예를 들면 다음과 같습니다.

```
################### 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
```

관련 정보

- 가장 일반적인 DMVPN 문제 해결 솔루션
- Cisco MDS 9000 제품군 문제 해결 가이드, 릴리스 2.x 문제 해결 IPsec
- 기술 지원 및 문서 – Cisco Systems