Configurazione della ridondanza ISP su uno spoke DMVPN con funzione VRF-Lite

Sommario

Introduzione

In questo documento viene descritto come configurare la ridondanza del provider di servizi Internet (ISP) su una VPN DMVPN (Dynamic Multipoint VPN) tramite la funzionalità Virtual Routing and Forwarding-Lite (VRF-Lite).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti prima di provare la configurazione descritta in questo documento:

- Conoscenze base di VRF

- Conoscenze base di Enhanced Interior Gateway Routing Protocol (EIGRP)
- Conoscenze base di DMVPN

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco IOS® versione 15.4(2)T.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il VRF è una tecnologia inclusa nei router di rete IP che consente a più istanze di una tabella di routing di coesistere in un router e funzionare contemporaneamente. In questo modo la funzionalità aumenta, in quanto i percorsi di rete possono essere segmentati senza l'utilizzo di più dispositivi.

L'uso di due ISP per la ridondanza è diventata una pratica comune. Gli amministratori utilizzano due collegamenti ISP: una funge da connessione primaria, l'altra da connessione di backup.

Lo stesso concetto può essere implementato per la ridondanza DMVPN su uno spoke con l'uso di ISP doppi. L'obiettivo di questo documento è dimostrare come *VRF-Lite* può essere usato per segregare la tabella di routing quando un spoke ha due ISP. Il routing dinamico viene usato per fornire ridondanza dei percorsi per il traffico che attraversa il tunnel DMVPN. Gli esempi di configurazione descritti in questo documento utilizzano lo schema seguente:

Interfaccia	Indirizzo IP	VRF	Descrizione
Ethernet 0/0	172.16.1.1	ISP1 VRF	ISP primario
Ethernet 0/1	172.16.2.1	ISP2 VRF	ISP secondario

Con la funzione VRF-Lite, è possibile supportare più istanze di routing/inoltro VPN sullo spoke DMVPN. La funzionalità VRF-Lite forza il traffico proveniente da più interfacce del tunnel GRE (Multipoint Generic Routing Encapsulation) a usare le rispettive tabelle di routing VRF. Ad esempio, se l'ISP primario termina nel VRF dell'ISP1 e l'ISP secondario termina nel VRF dell'ISP2, il traffico generato nel VRF dell'*ISP2* utilizza la tabella di routing del VRF dell'*ISP2*, mentre il traffico generato nel VRF dell'*ISP1* utilizza la tabella di routing del *VRF dell'ISP1*.

Un vantaggio che deriva dall'uso di un VRF (fVRF) della *porta anteriore* è principalmente quello di creare una tabella di routing separata dalla tabella di routing globale (dove esistono interfacce tunnel). Il vantaggio dell'utilizzo di un VRF (iVRF) *interno* consiste nel definire uno spazio privato in cui memorizzare le informazioni sulla rete privata e sulla VPN DMVPN. Entrambe queste configurazioni offrono una maggiore sicurezza dagli attacchi al router provenienti da Internet, dove le informazioni di routing sono separate.

Queste configurazioni VRF possono essere utilizzate sia sull'hub che sullo spoke DMVPN. Questo

offre un grande vantaggio rispetto a uno scenario in cui entrambi gli ISP terminano nella tabella di routing globale.

Se entrambi gli ISP terminano nel VRF globale, condividono la stessa tabella di routing e entrambe le interfacce GRE si basano sulle informazioni di routing globali. In questo caso, se si verifica un errore nell'ISP primario, l'interfaccia dell'ISP primario potrebbe non interrompersi se il punto di errore si trova nella rete backbone degli ISP e non è connesso direttamente. Il risultato è uno scenario in cui entrambe le interfacce del tunnel GRE utilizzano ancora il percorso predefinito che punta all'ISP primario, che causa il mancato funzionamento della ridondanza DMVPN.

Sebbene esistano soluzioni alternative che utilizzano gli script IP Service Level Agreements (IP SLA) o Embedded Event Manager (EEM) per risolvere questo problema senza VRF-Lite, non sempre rappresentano la scelta migliore.

Metodi di distribuzione

In questa sezione vengono fornite brevi panoramiche del tunneling suddiviso e dei tunnel spoke-to-spoke.

Tunneling ripartito

Quando si apprendono subnet specifiche o route riepilogate tramite un'interfaccia GRE, il processo viene chiamato *tunneling suddiviso*. Se il percorso predefinito viene individuato tramite un'interfaccia mGRE, viene denominato *tunnel-all*.

L'esempio di configurazione fornito in questo documento si basa sul tunneling suddiviso.

Tunnel spoke-to-spoke

L'esempio di configurazione fornito in questo documento è un buon progetto per il metodo di distribuzione tunnel-all (il percorso predefinito viene appreso tramite l'interfaccia mGRE).

L'uso di due fVRF segrega le tabelle di routing e assicura che i pacchetti incapsulati post-GRE vengano inoltrati al rispettivo fVRF, assicurando che il tunnel spoke-to-spoke disponga di un ISP attivo.

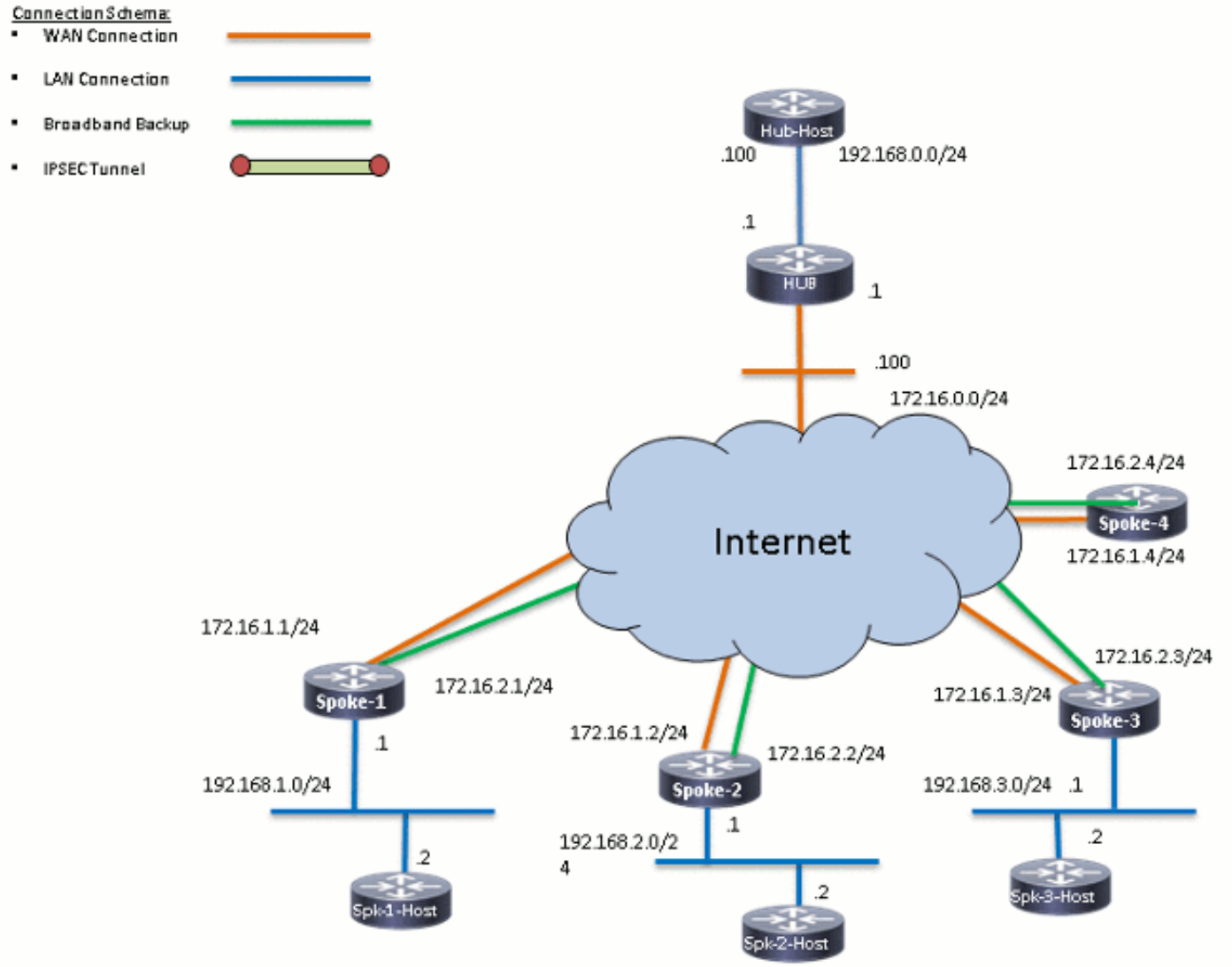
Configurazione

In questa sezione viene descritto come configurare la ridondanza ISP su una VPN DMVPN tramite la funzione VRF-Lite.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Questa è la topologia utilizzata per gli esempi in questo documento:



Configurazione hub

Di seguito sono riportate alcune note sulla configurazione rilevante nell'hub:

- Per impostare *Tunnel0* come interfaccia primaria nell'esempio di configurazione, è stato modificato il parametro *delay*, che consente di preferire i percorsi appresi dal parametro *Tunnel0*.

- La parola chiave **shared** viene usata con la protezione del tunnel e una *chiave tunnel* univoca viene aggiunta su tutte le interfacce GRE perché usano la stessa *origine tunnel <interface>*. In caso contrario, i pacchetti del tunnel GRE (Generic Routing Encapsulation) in entrata potrebbero essere indirizzati all'interfaccia del tunnel errata dopo la decrittografia.

- Viene eseguito un riepilogo del percorso per garantire che tutti i raggi imparino il percorso predefinito tramite i tunnel GRE (**tunnel-all**).

  Nota: In questo esempio vengono incluse solo le sezioni rilevanti della configurazione.

```
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
```

Configurazione spoke

Di seguito sono riportate alcune note relative alla configurazione rilevante in spoke:

- Per la ridondanza spoke, *Tunnel0* e *Tunnel1* hanno rispettivamente *Ethernet0/0* e *Ethernet0/1*come interfacce di origine del tunnel. Ethernet0/0 è collegato all'ISP primario ed Ethernet0/1 all'ISP secondario.
- Per isolare gli ISP, viene utilizzata la funzione VRF. L'ISP primario utilizza il protocollo *ISP1* VRF. Per l'ISP secondario è configurato un VRF denominato *ISP2*.
- Il *tunnel vrf ISP1* e il *tunnel vrf ISP2* sono configurati rispettivamente sulle interfacce Tunnel0 e Tunnel1, in modo da indicare che la ricerca di inoltro per il pacchetto incapsulato post-GRE viene eseguita in VRF ISP1 o ISP2.
- Per impostare Tunnel0 come interfaccia primaria nell'esempio di configurazione, è stato modificato il parametro *delay*, per rendere più preferibili le route che vengono apprese da Tunnel0.

Nota: In questo esempio vengono incluse solo le sezioni rilevanti della configurazione.

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni descritte in questa sezione.

ISP principali e secondari attivi

In questo scenario di verifica, sono attivi sia l'ISP primario che quello secondario. Di seguito sono riportate alcune note aggiuntive relative a questo scenario:

- La fase 1 e la fase 2 per entrambe le interfacce mGRE sono attive.
- Entrambi i tunnel arrivano, ma sono preferibili i percorsi tramite Tunnel0 (originato dall'ISP primario).

Di seguito sono elencati i comandi **show** pertinenti che è possibile utilizzare per verificare la configurazione in questo scenario:

```
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
```

ISP primario inattivo/ISP secondario attivo

In questo scenario, i timer di *attesa* EIGRP scadono per il router adiacente tramite Tunnel0 quando il collegamento ISP1 diventa inattivo e i percorsi all'hub e agli altri raggi ora puntano a Tunnel1 (originato con Ethernet0/1).

Di seguito sono elencati i comandi **show** pertinenti che è possibile utilizzare per verificare la configurazione in questo scenario:

```
*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
```

Ripristino collegamento ISP primario

Quando la connettività tramite l'ISP primario viene ripristinata, la sessione crittografica Tunnel0 diventa attiva e si preferiscono le route individuate tramite l'interfaccia Tunnel0.

Di seguito è riportato un esempio:

```
*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
```

Risoluzione dei problemi

Per risolvere i problemi relativi alla configurazione, abilitare **debug ip eigrp** e **registrare** il **comando dmvpn**.

Di seguito è riportato un esempio:

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

Informazioni correlate

- Soluzioni più comuni per la risoluzione dei problemi DMVPN
- Guida alla risoluzione dei problemi della famiglia Cisco MDS 9000, versione 2.xÂ Risoluzione dei problemi IPsec
- Documentazione e supporto tecnico – Cisco Systems