Konfigurieren der ISP-Redundanz auf einem DMVPN-Spoke mit der VRF-Lite-Funktion

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Redundanz von Internet Service Providern (ISP) auf einem Dynamic Multipoint VPN (DMVPN) konfiguriert wird, das über die Virtual Routing and Forwarding-Lite (VRF-Lite)-Funktion gesprochen wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, vor dem Versuch der in diesem Dokument beschriebenen Konfiguration über Kenntnisse dieser Themen zu verfügen:

- Grundkenntnisse der VRF-Instanzen

- Grundkenntnisse des Enhanced Interior Gateway Routing Protocol (EIGRP)
- Grundkenntnisse von DMVPN

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IOS® Version 15.4(2)T.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die VRF-Instanz ist eine in den IP-Netzwerk-Routern enthaltene Technologie, die es ermöglicht, mehrere Instanzen einer Routing-Tabelle gleichzeitig in einem Router zu existieren und gleichzeitig zu arbeiten. Dies erhöht die Funktionalität, da die Netzwerkpfade ohne die Verwendung mehrerer Geräte segmentiert werden können.

Die Verwendung dualer ISPs für Redundanz ist zu einer gängigen Praxis geworden. Administratoren verwenden zwei ISP-Links: eine dient als primäre Verbindung und die andere als Backup-Verbindung.

Das gleiche Konzept kann für die DMVPN-Redundanz in einem Spoke mit Verwendung von zwei ISPs implementiert werden. Dieses Dokument soll zeigen, wie *VRF-Lite* zur Trennung der Routing-Tabelle verwendet werden kann, wenn ein Spoke über zwei ISPs verfügt. Dynamisches Routing wird verwendet, um Pfadredundanz für den Datenverkehr bereitzustellen, der den DMVPN-Tunnel passiert. Die in diesem Dokument beschriebenen Konfigurationsbeispiele verwenden das folgende Konfigurationsschema:

Schnittstelle	IP-Adresse	VRF	Beschreibung
Ethernet0/0	172,16,1,1	ISP1 VRF	Primäre ISP
Ethernet0/1	172,16,2,1	ISP2-VRF	Sekundärer ISP

Mit der VRF-Lite-Funktion können mehrere VPN-Routing-/Weiterleitungsinstanzen im DMVPN-Spoke unterstützt werden. Die VRF-Lite-Funktion zwingt den Datenverkehr von mehreren mGRE-Tunnelschnittstellen (Multipoint Generic Routing Encapsulation) zur Verwendung der entsprechenden VRF-Routing-Tabellen. Wenn beispielsweise der primäre ISP in der *ISP1*-VRF terminiert und der sekundäre ISP in der *ISP2*-VRF terminiert, wird der im *ISP2*-VRF generierte Datenverkehr in der *ISP2*-VRF-Routing-Tabelle verwendet, während der in der in der *ISP1-VRF-VRF*–––-ISP-*ISPISP-VRF--VRF*V

Ein Vorteil, der sich aus der Verwendung eines VRF (*Front Door* VRF) ergibt, besteht in erster Linie darin, eine separate Routing-Tabelle von der globalen Routing-Tabelle zu erstellen (wo Tunnelschnittstellen vorhanden sind). Der Vorteil bei der Verwendung einer *internen* VRF-Instanz (iVRF) besteht in der Definition eines privaten Raums, um DMVPN- und private Netzwerkinformationen zu speichern. Beide Konfigurationen bieten zusätzliche Sicherheit vor Angriffen auf den Router vom Internet, wo die Routing-Informationen getrennt sind.

Diese VRF-Konfigurationen können sowohl auf dem DMVPN-Hub als auch in den Spoke-Sitzungen verwendet werden. Dies bietet einen großen Vorteil gegenüber einem Szenario, in dem beide ISPs in der globalen Routing-Tabelle enden.

Wenn beide ISPs in der globalen VRF-Instanz terminieren, verwenden sie dieselbe Routing-Tabelle, und beide mGRE-Schnittstellen basieren auf den globalen Routing-Informationen. Wenn in diesem Fall der primäre ISP ausfällt, fällt die primäre ISP-Schnittstelle möglicherweise nicht aus, wenn sich der Fehlerpunkt im Backbone-Netzwerk von ISPs befindet und nicht direkt verbunden ist. Dies führt zu einem Szenario, in dem beide mGRE-Tunnelschnittstellen weiterhin die Standardroute verwenden, die auf den primären ISP verweist, was zum Ausfall der DMVPN-Redundanz führt.

Obwohl es einige Problemumgehungen gibt, die IP Service Level Agreements (IP SLA) oder Embedded Event Manager (EEM)-Skripts verwenden, um dieses Problem ohne VRF-Lite zu beheben, sind diese möglicherweise nicht immer die beste Wahl.

Bereitstellungsmethoden

Dieser Abschnitt bietet eine kurze Übersicht über Split-Tunneling und Spoke-to-Spoke-Tunnel.

Split Tunneling

Wenn bestimmte Subnetze oder zusammengefasste Routen über eine mGRE-Schnittstelle erfasst werden, wird dies als *Split-Tunneling* bezeichnet. Wenn die Standardroute über eine mGRE-Schnittstelle abgerufen wird, wird sie als *tunnel-all* bezeichnet.

Das Konfigurationsbeispiel in diesem Dokument basiert auf Split-Tunneling.

Spoke-to-Spoke-Tunnel

Das in diesem Dokument bereitgestellte Konfigurationsbeispiel ist ein gutes Design für die Bereitstellungsmethode für Tunnel (die Standardroute wird über die mGRE-Schnittstelle erfasst).

Die Verwendung von zwei fVRFs trennt die Routing-Tabellen und stellt sicher, dass die gekapselten Post-GRE-Pakete an die jeweilige fVRF-Instanz weitergeleitet werden. Dadurch wird sichergestellt, dass der Spoke-to-Spoke-Tunnel über einen aktiven ISP verfügt.

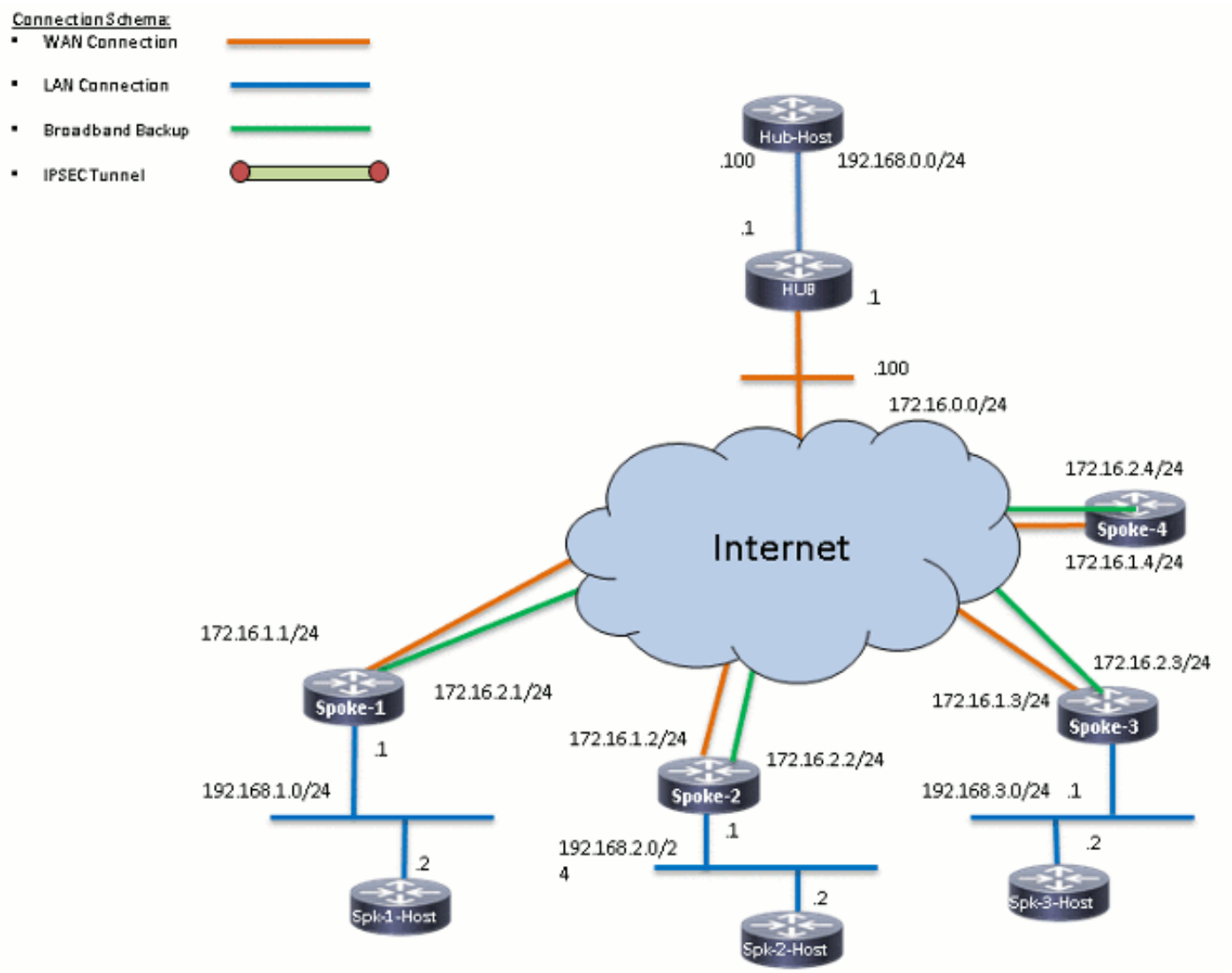
Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie die ISP-Redundanz auf einem DMVPN-Spoke über die VRF-Lite-Funktion konfigurieren.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Dies ist die Topologie, die für die Beispiele in diesem Dokument verwendet wird:



Hub-Konfiguration

Im Folgenden finden Sie einige Hinweise zur entsprechenden Konfiguration auf dem Hub:

- Um *Tunnel0* als primäre Schnittstelle in diesem Konfigurationsbeispiel festzulegen, wurde der *Verzögerungsparameter* geändert, wodurch die Routen, die von *Tunnel0* gelernt wurden, bevorzugt werden.

- Das **shared**-Schlüsselwort wird mit Tunnelschutz verwendet, und auf allen mGRE-Schnittstellen wird ein eindeutiger *Tunnelschlüssel* hinzugefügt, da sie dieselbe *Tunnelquelle <Schnittstelle>* verwenden. Andernfalls werden die eingehenden GRE-Tunnelpakete (Generic Routing Encapsulation) nach der Entschlüsselung an die falsche Tunnelschnittstelle weitergeleitet.

- Es wird eine Routenzusammenfassung durchgeführt, um sicherzustellen, dass alle Stationen

die Standardroute über die mGRE-Tunnel (**Tunnel-all**) erfassen.

Hinweis: In diesem Beispiel sind nur die relevanten Abschnitte der Konfiguration enthalten.

```
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
```

Spoke-Konfiguration

Im Folgenden finden Sie einige Hinweise zur relevanten Konfiguration in den Spokes:

- Für die Spoke-Redundanz haben *Tunnel0* und *Tunnel1 Ethernet0/0* und *Ethernet0/1* als Tunnelquellenschnittstellen. Ethernet0/0 ist mit dem primären ISP verbunden, und Ethernet0/1 ist mit dem sekundären ISP verbunden.

- Zur Trennung der ISPs wird die VRF-Funktion verwendet. Der primäre ISP verwendet die *ISP1*-VRF-Instanz. Für den sekundären ISP wird eine VRF-Instanz mit dem Namen *ISP2* konfiguriert.

- Der *Tunnel-VRF ISP1* und der *Tunnel-VRF-ISP2* werden auf den Schnittstellen Tunnel0 bzw. Tunnel1 konfiguriert, um anzuzeigen, dass die Weiterleitungssuche für das gekapselte Paket nach GRE entweder im VRF-ISP1 oder im ISP2 durchgeführt wird.

- Um Tunnel0 als primäre Schnittstelle in diesem Konfigurationsbeispiel festzulegen, wurde der *Verzögerungsparameter* geändert, wodurch die Routen, die von Tunnel0 gelernt werden, bevorzugt werden.

Hinweis: In diesem Beispiel sind nur die relevanten Abschnitte der Konfiguration enthalten.

```
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
```

Überprüfen

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Aktive primäre und sekundäre ISPs

In diesem Überprüfungsszenario sind sowohl die primären als auch die sekundären ISPs aktiv. Hier einige zusätzliche Hinweise zu diesem Szenario:

- Phase 1 und Phase 2 für beide mGRE-Schnittstellen sind aktiv.
- Beide Tunnel sind verfügbar, aber die Routen über Tunnel0 (über den primären ISP bezogen) werden bevorzugt.

Hier sind die relevanten **show**-Befehle, die Sie verwenden können, um Ihre Konfiguration in diesem Szenario zu überprüfen:

```
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
```

Primärer ISP inaktiv/sekundärer ISP aktiv

In diesem Szenario laufen die EIGRP-*Hold*-Timer für die Nachbarschaft über Tunnel0 ab, wenn die ISP1-Verbindung ausfällt, und die Routen zum Hub und den anderen Stationen zeigen jetzt auf Tunnel1 (mit Ethernet0/1).

Hier sind die relevanten **show**-Befehle, die Sie verwenden können, um Ihre Konfiguration in diesem Szenario zu überprüfen:

```
*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
```

Primäre Wiederherstellung der ISP-Verbindung

Wenn die Verbindung über den primären ISP wiederhergestellt wird, wird die Crypto-Sitzung für Tunnel0 aktiviert, und die Routen, die über die Tunnel0-Schnittstelle abgerufen werden, werden bevorzugt.

Hier ein Beispiel:

```
*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
```

Fehlerbehebung

Um eine Fehlerbehebung für Ihre Konfiguration durchzuführen, aktivieren Sie **debug ip eigrp** und **logging dmvpn**.

Hier ein Beispiel:

```
****************** 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
```

Zugehörige Informationen

- Häufigste DMVPN-Fehlerbehebungslösungen
- Cisco MDS 9000-Produktfamilie - Leitfaden zur Fehlerbehebung, Version 2.x - Â IPsec-Fehlerbehebung
- Technischer Support und Dokumentation - Cisco Systems