تكوين تكرار ISP على DMVPN يتم التحدث عنه باستخدام ميزة VRF-Lite

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين تكرار موفر خدمة الإنترنت (ISP) على شبكة VPN (DMVPN) ديناميكية متعددة النقاط يتم التحدث بها من خلال ميزة التوجيه الظاهري وإعادة التوجيه Virtual Routing and Forwarding-Lite (VRF-Lite)).

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من هذا موضوع قبل أن أنت تحاول التشكيل أن يكون موضح في هذا وثيقة:

- معرفة أساسية ب VRF
- معرفة أساسية ببروتوكول توجيه البوابة الداخلية المحسنة (EIGRP)

- معرفة أساسية بـ DMVPN

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 15.4(2)T من Cisco IOS®.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

ال VRF هي تقنية مضمنة في موجهات شبكة IP التي تسمح للمثيلات المتعددة لجدول التوجيه بالتعايش في موجه والعمل في وقت واحد. وهذا يزيد من الوظائف لأنه يسمح بتقسيم مسارات الشبكة دون إستخدام أجهزة متعددة.

وقد أصبح إستخدام موفري خدمات الإنترنت المزدوجين للتكرار ممارسة شائعة. يستخدم المسؤولون ارتباطين ل ISP، يعمل أحدهما كوصلة أساسية ويعمل الآخر كوصلة إحتياطية.

يمكن تنفيذ نفس المفهوم لوحدة DMVPN المتكررة على أي طريقة يتم التحدث بها باستخدام مزودي خدمة الإنترنت (ISPs) المزدوجين. الهدف من هذا المستند هو توضيح كيف يمكن إستخدام *VRF-Lite* لفصل جدول التوجيه عندما يكون لدى أحد المتحدثين موجهات خدمات مدمجة (ISPs) مزدوجة. يتم إستخدام التوجيه الديناميكي لتوفير تكرار المسار لحركة المرور التي تجتاز نفق DMVPN. تستخدم أمثلة التكوين الموضحة في هذا المستند مخطط التكوين هذا:

الواجهة	عنوان IP	VRF	الوصف
Ethernet0/0	172.16.1.1	ISP1 VRF	مزود خدمة الإنترنت (ISP) الأساسي
Ethernet0/1	172.16.2.1	ISP2 VRF	مزود خدمة الإنترنت (ISP) الثانوي

باستخدام ميزة VRF-Lite، يمكن دعم مثيلات متعددة لتوجيه/إعادة توجيه VPN على شبكة DMVPN التي يتم التحدث بها. تفرض ميزة VRF-Lite حركة المرور من واجهات نفق تضمين التوجيه العام متعدد النقاط (mGRE) لاستخدام جداول توجيه VRF الخاصة بها. على سبيل المثال، إذا انتهى مزود خدمة الإنترنت (ISP) الأساسي في ISP1 VRF وISP الثانوي في ISP2 VRF، فإن حركة المرور التي تم إنشاؤها في ISP2 VRF تستخدم جدول توجيه *ISP2* VRF، بينما تستخدم حركة المرور التي يتم إنشاؤها في *ISP1* VRF جدول *توجيه* VRF *ISP1*.

إحدى الميزات التي تأتي مع إستخدام VRF *للباب الأمامي* (fVRF) هي بشكل أساسي تخصيص جدول توجيه منفصل من جدول التوجيه العام (حيث توجد واجهات النفق). والميزة مع إستخدام VRF *داخلي* (iVRF) هي تحديد مساحة خاصة لاحتجاز معلومات شبكة DMVPN وشبكة خاصة. يوفر كلا التكوينين أمانا إضافيا من الهجمات على الموجه من الإنترنت، حيث يتم فصل معلومات التوجيه.

يمكن إستخدام تكوينات VRF هذه على كل من محور DMVPN والكلمة. وهذا يعطي ميزة كبيرة على السيناريو الذي ينتهي فيه كل من مزودي خدمة الإنترنت (ISPs) في جدول التوجيه العالمي.

إذا تم إنهاء كل من موفري خدمة الإنترنت (ISPs) في التردد اللاسلكي العام، فسيتشاركون في نفس جدول التوجيه وتعتمد كلا واجهات mGRE على معلومات التوجيه العالمية. في هذه الحالة، إذا فشل مزود خدمة الإنترنت (ISP) الرئيسي، فقد لا تنخفض واجهة مزود خدمة الإنترنت (ISP) الأساسية إذا كانت نقطة الفشل في الشبكة الأساسية لمزود خدمة الإنترنت (ISP) وغير متصلة مباشرة. وهذا ينتج عنه سيناريو حيث لا تزال كل من واجهات نفق mGRE تستخدم المسار الافتراضي الذي يشير إلى ISP الأساسي، والذي يتسبب في فشل تكرار DMVPN.

على الرغم من وجود بعض الحلول التي تستخدم نصوص إتفاقيات مستوى خدمة IP (IP SLA) أو البرامج النصية لإدارة الأحداث المضمنة (EEM) لمعالجة هذه المشكلة بدون VRF-Lite، إلا أنها قد لا تكون دائما الخيار الأفضل.

طرق النشر

يوفر هذا القسم نظرة عامة مختصرة على أنفاق الأنفاق المنفصلة والأنفاق التي يتم التحدث إليها.

تقسيم الاتصال النفقي

عند تعلم شبكات فرعية معينة أو مسارات ملخصة عبر واجهة mGRE، يطلق عليها بعد ذلك *تقسيم الاتصال النفقي*. إذا تم تعلم المسار الافتراضي عبر واجهة mGRE، فيطلق عليه اسم *tunnel-all*.

يعتمد مثال التكوين الذي يتم توفيره في هذا المستند على الاتصال النفقي المنقسم.

أنفاق تتحدث

يعد مثال التكوين الذي يتم توفيره في هذا المستند تصميما جيدا لطريقة النشر tunnel-all (يتم تعلم المسار الافتراضي عبر واجهة mGRE).

يعمل إستخدام إثنين من أطر تكرار الخطوة الأولى (FVRF) على الفصل بين جداول التوجيه ويضمن إعادة توجيه الحزم التي تم تغليفها بعد بروتوكول الشجرة المتفرعة (GRE) إلى إطار التردد اللاسلكي (fVRF) الخاص، مما يساعد على ضمان أن يخرج النفق الذي يتحدث إليه بمزود خدمة إنترنت (ISP) نشط.

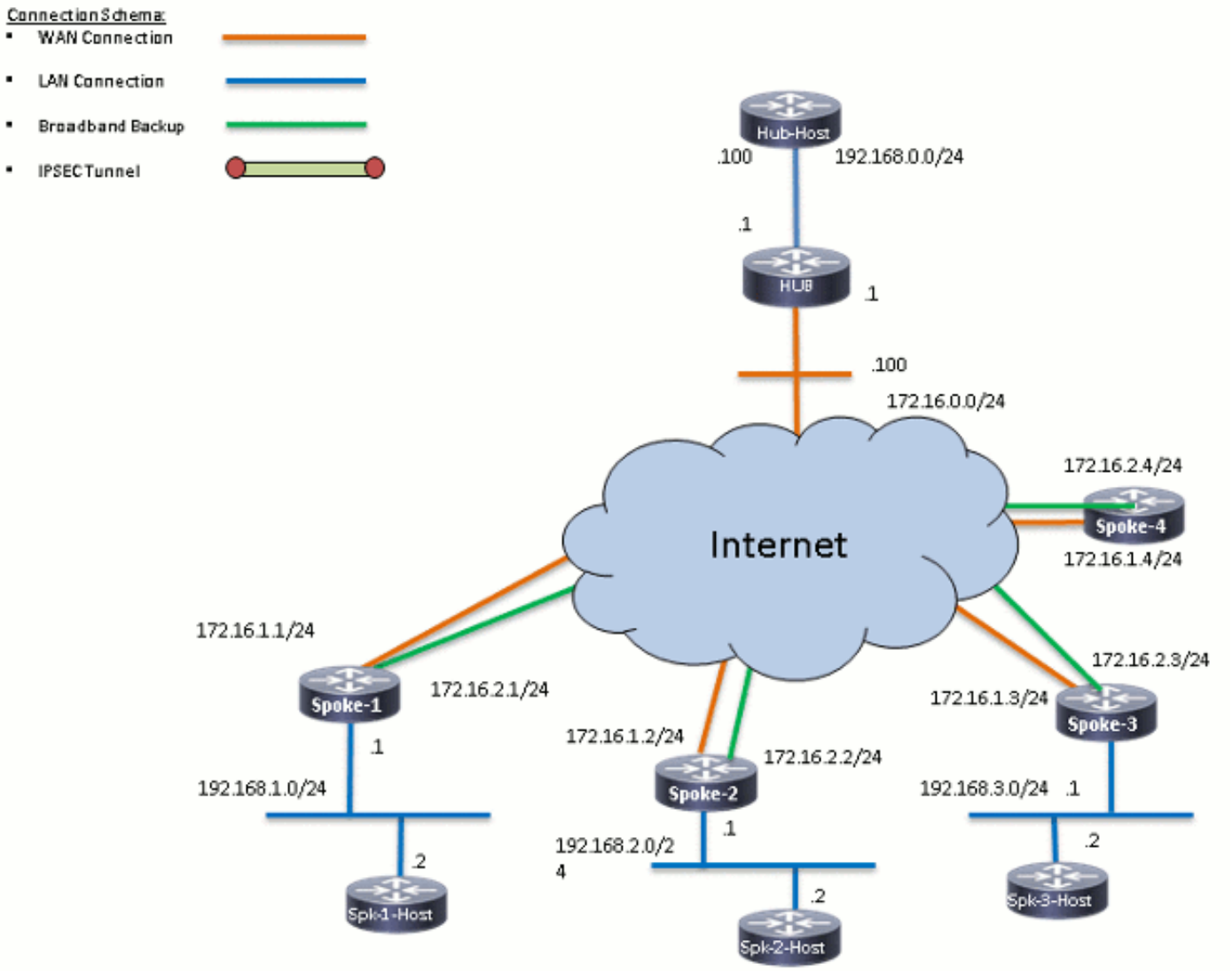
التكوين

يصف هذا القسم كيفية تكوين تكرار ISP على DMVPN يتم التحدث به عبر ميزة VRF-Lite.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

هذا هو المخطط الذي يتم إستخدامه للأمثلة ضمن هذا المستند:



تكوين الموزع

هنا بعض ملاحظات حول التشكيل مناسب على الصرة:

- من أجل تعيين *Tunnel0* كالواجهة الأساسية في مثال التكوين هذا، تم تغيير المعلمة *delay*، والتي تتيح للمسارات التي يتم التعرف عليها من *Tunnel0* أن تصبح أكثر تفضيلا.

يتم إستخدام الكلمة الأساسية **المشتركة** مع حماية النفق وتتم إضافة *مفتاح نفق* فريد على جميع واجهات mGRE لأنها تستخدم نفس *مصدر النفق <interface>*. وإلا، فقد يتم توقيع حزم نفق تضمين التوجيه العام الوارد (GRE) على واجهة النفق غير الصحيحة بعد فك التشفير.

- يتم إجراء تلخيص المسار لضمان أن جميع الخوادم تتعرف على المسار الافتراضي عبر أنفاق mGRE (**tunnel-all**).

ملاحظة: يتم تضمين الأقسام ذات الصلة فقط من التكوين في هذا المثال.

```
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
```

التكوين الذي تم التحدث به

فيما يلي بعض الملاحظات حول التكوين ذي الصلة على المحادثة:

- بالنسبة للتكرار الصوتي، يحتوي *Tunnel0* و*Tunnel1* على *Ethernet0/0* و*Ethernet0/1* كواجهات مصدر النفق، على التوالي. يتصل Ethernet0/0 ب ISP أساسي ويتصل Ethernet0/1 ب ISP الثانوي.

- in order to فصلت ال isp، ال VRF استعملت سمة. يستخدم ISP الأساسي VRF *ISP1*. بالنسبة إلى ISP الثانوي، يتم تكوين VRF باسم *ISP2*.

- يتم تكوين *النفق isp1 vrf* و*tunnel vrf isp2* على الواجهات Tunnel0 و Tunnel1، على التوالي، للإشارة إلى أنه يتم إجراء بحث إعادة التوجيه للحزمة التي تم تغليفها بعد GRE في ISP1 VRF أو ISP2.

- لتعيين Tunnel0 كواجهة أساسية في مثال التكوين هذا، تم تغيير معلمة *التأخير*، والتي تتيح للمسارات التي يتم التعرف عليها من Tunnel0 أن تصبح أكثر تفضيلا.

ملاحظة: يتم تضمين الأقسام ذات الصلة فقط من التكوين في هذا المثال.

```
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
```

التحقق من الصحة

أستخدم المعلومات الموضحة في هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

موجهات الخدمات المتكاملة (ISP) الأساسية والثانوية النشطة

في سيناريو التحقق هذا، يكون كل من موفري خدمة الإنترنت الأساسيين والثانويين نشطا. فيما يلي بعض الملاحظات الإضافية حول هذا السيناريو:

- تم الانتهاء من المرحلة الأولى والمرحلة الثانية لكل من واجهات بروتوكول MGRE.
- يتم إنشاء كلا النفقين، ولكن يتم تفضيل المسارات عبر Tunnel0 (التي يتم الحصول عليها من خلال ISP الأساسي).

وفيما يلي أوامر **العرض** ذات الصلة التي يمكنك إستخدامها للتحقق من التكوين الخاص بك في هذا السيناريو:

```
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 ---!

is variably subnetted, 4 subnets, 2 masks 10.0.0.0/8
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
is variably subnetted, 2 subnets, 2 masks 192.168.1.0/24
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
is variably subnetted, 2 subnets, 2 masks 172.16.0.0/16
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
is variably subnetted, 2 subnets, 2 masks 172.16.0.0/16
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
```

مزود خدمة الإنترنت (ISP) الأساسي لأسفل/الثانوي نشط

في هذا السيناريو، تنتهي صلاحية مؤقتات *إحتجاز* EIGRP للسفينة المجاورة عبر النفق0 عند تعطل إرتباط ISP1، وتشير الموجهات إلى الوصل والأقسام الأخرى الآن إلى النفق 1 (يتم الحصول على مصدر مع Ethernet0/1).

وفيما يلي أوامر **العرض** ذات الصلة التي يمكنك إستخدامها للتحقق من التكوين الخاص بك في هذا السيناريو:

```
(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 ---!

                          is variable subnetted, 4 subnets, 2 masks 10.0.0.0/8
                               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
                    is variable subnetted, 2 subnets, 2 masks 192.168.1.0/24
                          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
                    is variable subnetted, 2 subnets, 2 masks 172.16.0.0/16
                          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
is variably subnetted, 2 subnets, 2 masks 172.16.0.0/16
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
```

إستعادة إرتباط ISP الأساسي

عندما يتم إستعادة الاتصال من خلال ISP الأساسي، تصبح جلسة تشفير Tunnel0 نشطة، ويفضل المسارات التي يتم التعرف عليها عبر واجهة Tunnel0.

فيما يلي مثال:

```
(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 ---!

     is variable subnetted, 4 subnets, 2 masks 10.0.0.0/8
          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
  is variable subnetted, 2 subnets, 2 masks 192.168.1.0/24
      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
```

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء التكوين وإصلاحها، قم بتمكين **debug ip eigrp** و**logging dmvpn**.

فيما يلي مثال:

```
##################### 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*
                                                          (origin(10.0.1.1 (90/3072000)
      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*
:NBMA: 172.16.0.1 ) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is DOWN, Reason 10.0.0.1
```

```
(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*
           NBMA: 172.16.0.1) for (Tunnel: 10.0.0.10 NBMA: 172.16.1.1) is  UP 10.0.0.1
   (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*
                                                          (origin(10.0.1.1 (90/3072000)
   Sep  2 14:16:01.197: EIGRP-IPv4(1): table(default): route installed for 0.0.0.0/0*
                                                          (origin(10.0.0.1 (90/2944000)
        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
```

معلومات ذات صلة

- حلول أستكشاف أخطاء DMVPN وإصلاحها الأكثر شيوعا
- دليل أستكشاف أخطاء العائلة وإصلاحها Cisco MDS 9000، الإصدار xaÂ.2 أستكشاف أخطاء IPsec وإصلاحها
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).