# DMVPN第1階段調試故障排除指南

## 目錄


[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[重大改進](#)
[慣例](#)
[相關配置](#)
[拓撲概述](#)
[加密](#)
[中心](#)
[輻條](#)
[調試](#)
[封包流視覺化](#)
[調試及說明](#)
[確認功能和疑難排解](#)
[show crypto sockets](#)
[show crypto session detail](#)
[show crypto isakmp sa detail](#)
[show crypto ipsec sa detail](#)
[show ip nhrp](#)
[show ip nhs](#)
[show dmvpn [detail]](#)
[相關資訊](#)


## 簡介

本檔案介紹您會在集線器上遇到的偵錯訊息，並提到動態多點虛擬私人網路(DMVPN)第1階段部署。

## 必要條件

對於本文檔中的配置和調試命令，您需要兩台運行Cisco IOS®版本12.4(9)T或更高版本的Cisco路由器。一般來說，基本DMVPN第1階段要求用於聚合服務路由器(ASR)的Cisco IOS版本12.2(13)T或更新版本或12.2(33)XNC版本，但可能不支援本文檔中所述的功能和調試。

### 需求

思科建議您瞭解以下主題：

- 通用路由封裝(GRE)

- 下一個躍點解析通訊協定(NHRP)
- 網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)
- 網際網路金鑰交換(IKE)
- 網際網路通訊協定安全(IPSec)
- 這些路由協定中至少有一個協定：增強型內部閘道路由通訊協定(EIGRP)、開放最短路徑優先(OSPF)、路由資訊通訊協定(RIP)和邊界閘道通訊協定(BGP)

### 採用元件

本檔案中的資訊是根據執行Cisco IOS版本15.1(4)M4的Cisco 2911整合式服務路由器(ISR)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### 重大改進

以下Cisco IOS版本為DMVPN第1階段引入了重要的功能或修復：

- 版本12.2(18)SXF5 — 使用公開金鑰基礎架構(PKI)時更好地支援ISAKMP
- 版本12.2(33)XNE - ASR、IPSec配置檔案、隧道保護、IPSec網路地址轉換(NAT)遍歷
- 版本12.3(7)T — 內部虛擬路由和轉送(iVRF)支援
- 版本12.3(11)T — 前門虛擬路由和轉發(fVRF)支援
- 版本12.4(9)T — 支援各種與DMVPN相關的調試和命令
- 版本12.4(15)T — 共用通道保護
- 版本12.4(20)T — 使用DMVPN的IPv6
- 版本15.0(1)M - NHRP通道健康狀況監控

### 慣例

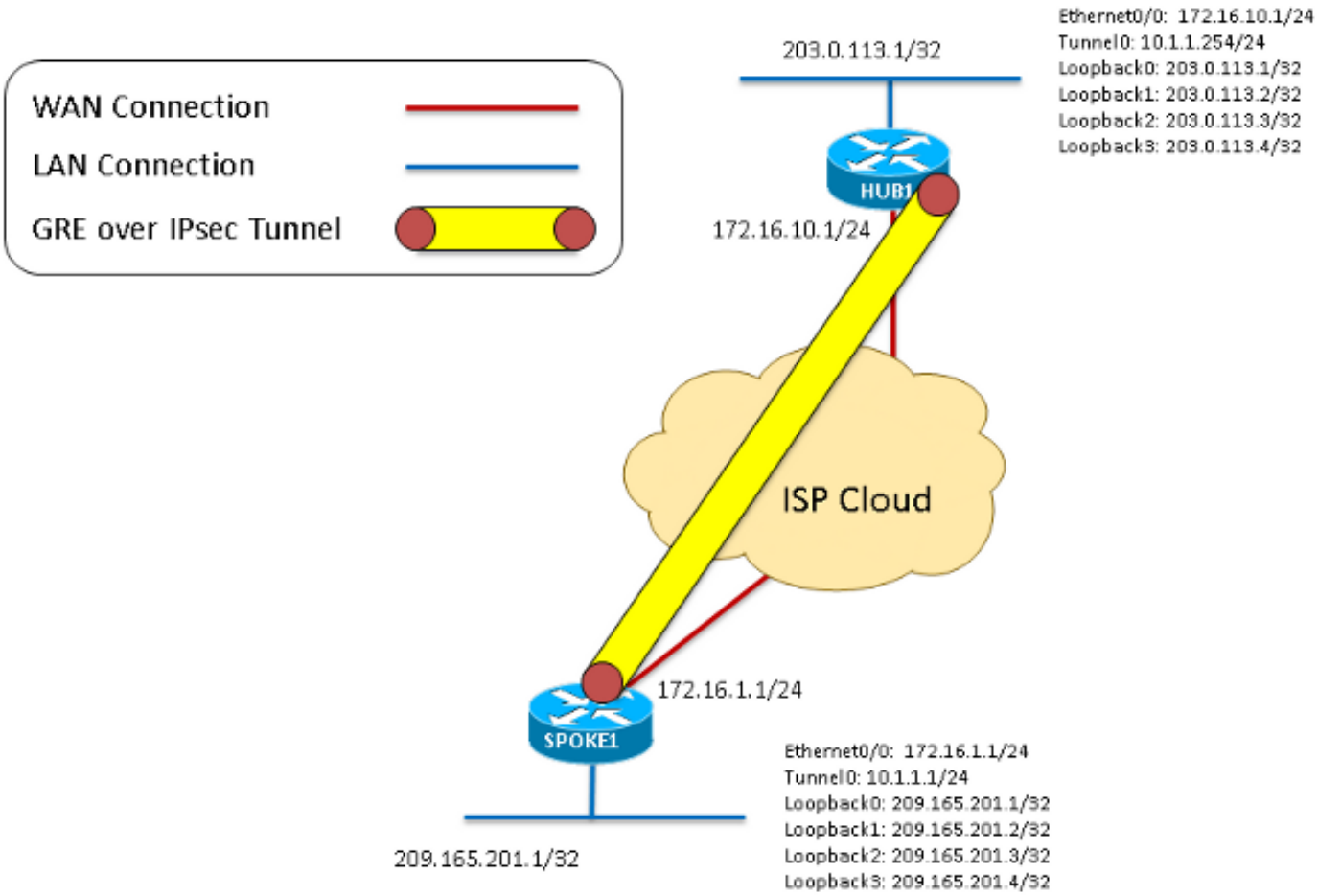
如需檔案慣例的相關資訊，請參閱思科技術提示慣例。

## 相關配置

### 拓撲概述

對於此拓撲，為DMVPN第1階段配置了兩個運行版本15.1(4)M4的2911 ISR:一個作為中心，一個作為分支。Ethernet0/0被用作每台路由器的「internet」介面。四個環回介面配置為模擬位於中心站點或分支站點的區域網。由於這是只有一個分支的DMVPN第1階段拓撲，因此該分支配置了點對點GRE隧道而不是多點GRE隧道。每台路由器上使用相同的加密配置（ISAKMP和IPSec）以確保它們完全匹配。

圖表1




## 加密

中心和分支上的情况相同。

```
crypto isakmp policy 1
encr 3des
hash sha
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set DMVPN-TSET esp-3des esp-sha-hmac
mode transport
crypto ipsec profile DMVPN-IPSEC
set transform-set DMVPN-TSET
```

## 中心

```
interface Tunnel0
ip address 10.1.1.254 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip tcp adjust-mss 1360
no ip split-horizon eigrp 1
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
```

```
end

interface Ethernet0/0
ip address 172.16.10.1 255.255.255.0
end

interface Loopback0
ip address 203.0.113.1 255.255.255.255
interface Loopback1
ip address 203.0.113.2 255.255.255.255
interface Loopback2
ip address 203.0.113.3 255.255.255.255
interface Loopback3
ip address 203.0.113.4 255.255.255.255

router eigrp 1
network 10.1.1.0 0.0.0.255
network 203.0.113.1 0.0.0.0
network 203.0.113.2 0.0.0.0
network 203.0.113.3 0.0.0.0
network 203.0.113.4 0.0.0.0
```

### 輻條

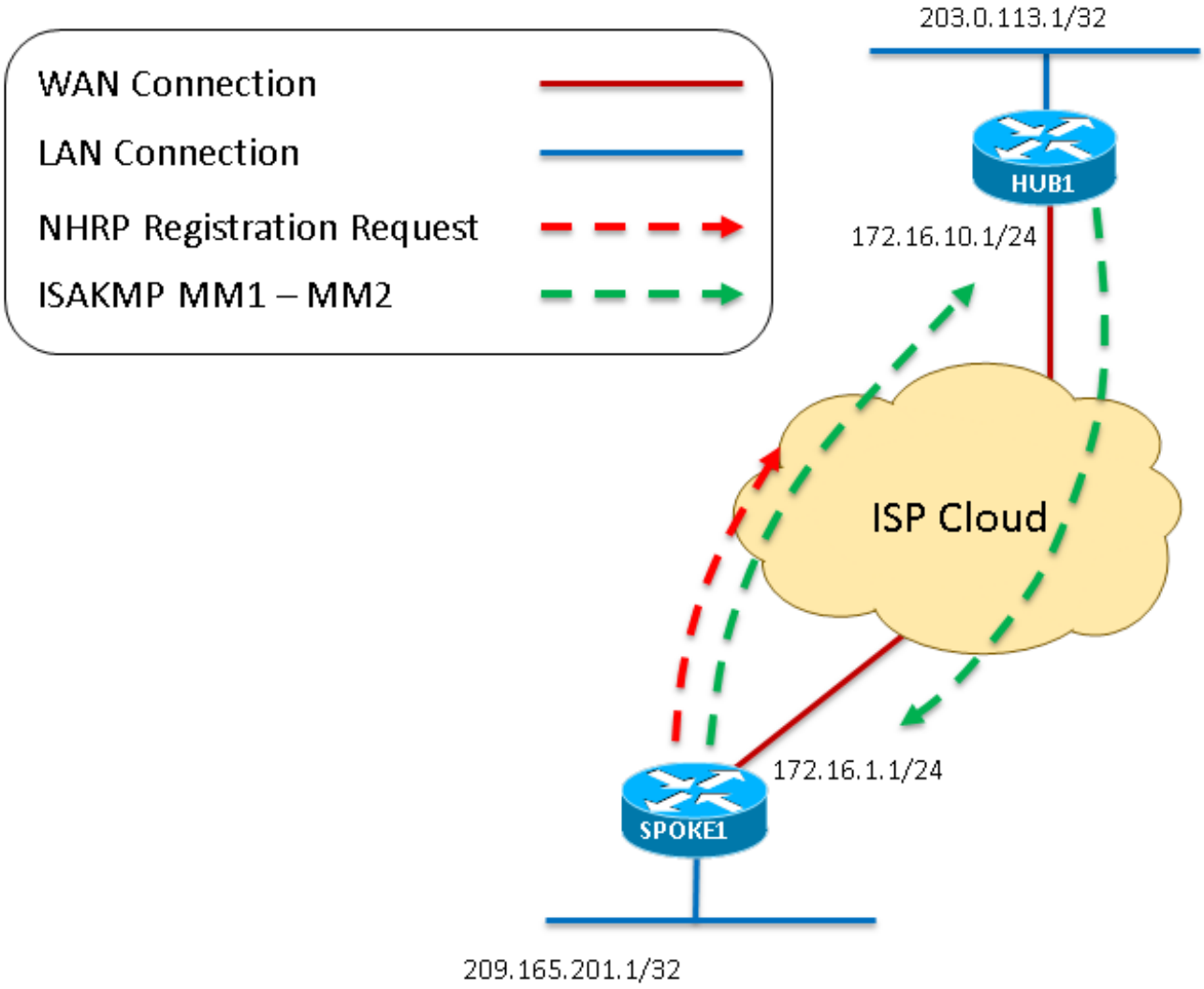
```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
end

interface Loopback0
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

router eigrp 1
network 209.165.201.1 0.0.0.0
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

# 調試

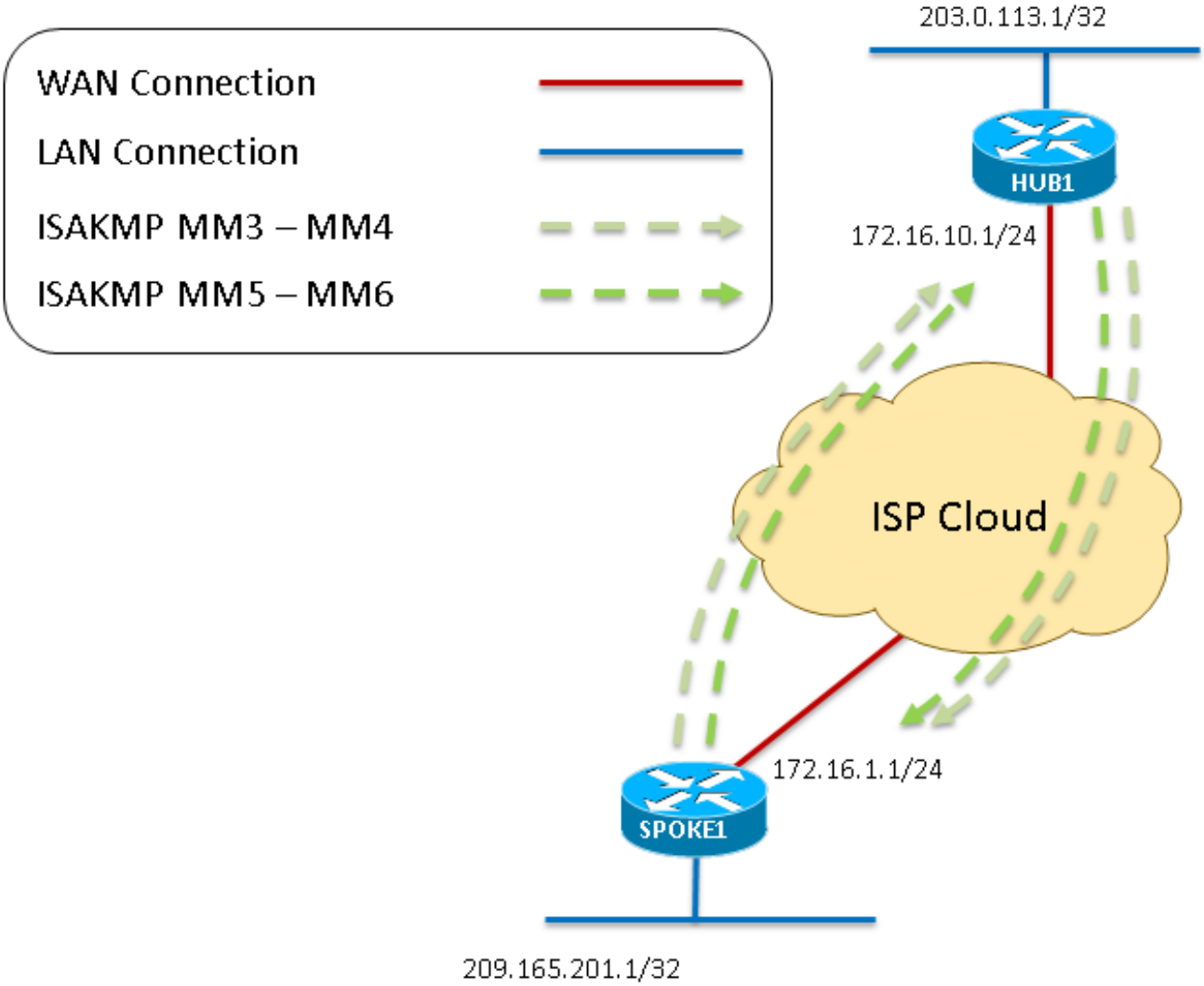
## 封包流視覺化

如本檔案所示，這是整個DMVPN封包流程的視覺化。還包括解釋每個步驟的更詳細的調試。

1. 當分支上的隧道為「no shutdown」時，它將生成NHRP註冊請求，該請求將啟動DMVPN進程。由於集線器的配置完全是動態的，分支必須是發起連線的端點。
2. 然後，NHRP註冊請求將封裝在GRE中，從而觸發加密過程啟動。
3. 此時，第一個ISAKMP主模式消息 — ISAKMP MM1 — 從分支傳送到埠UDP500上的集線器。
4. 集線器接收並處理MM1並使用ISAKMP MM2進行響應，因為它具有匹配的ISAKMP策略。
   圖2 — 指步驟1至
   4

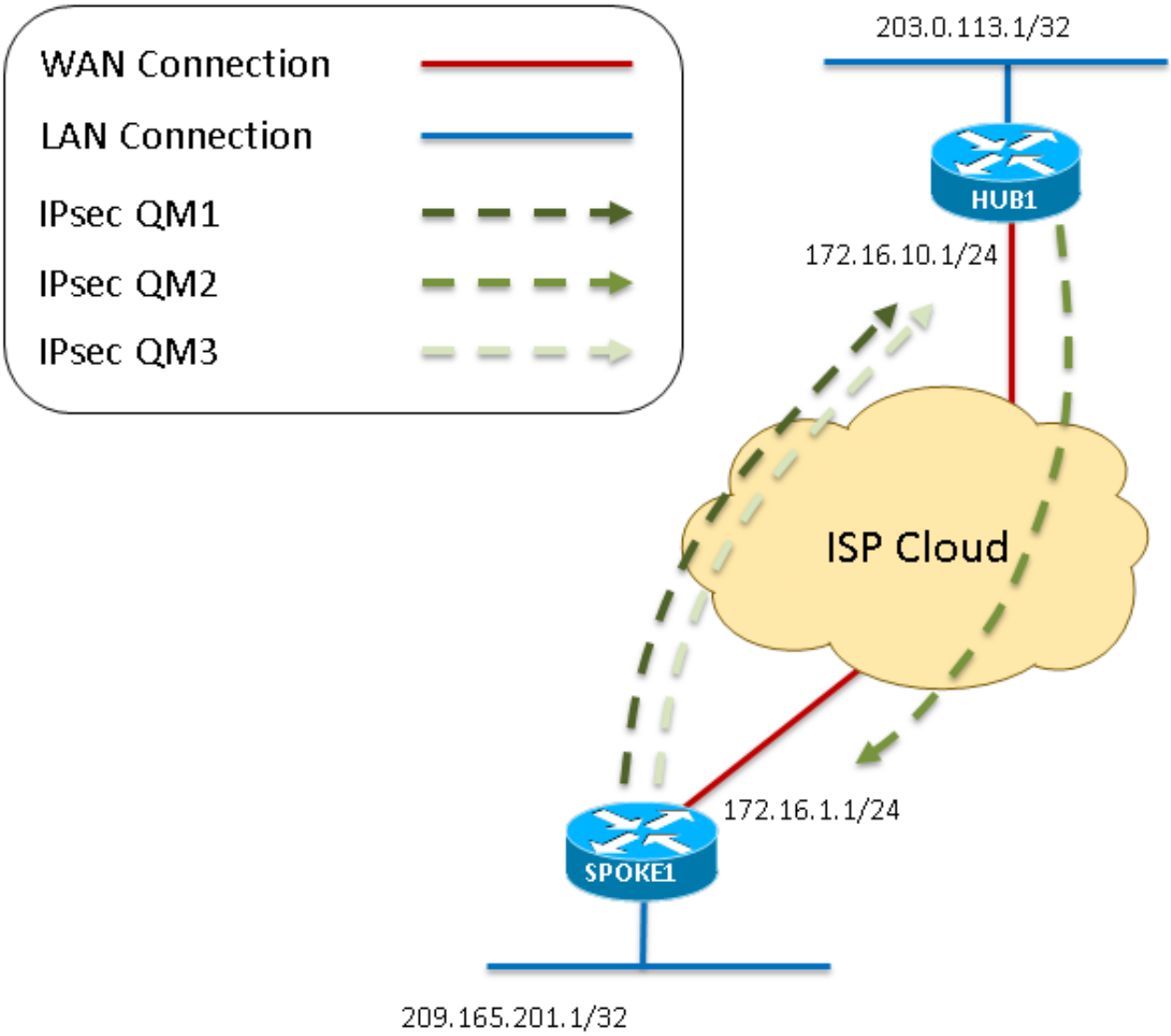



5. 輻條收到MM2後，會使用MM3做出響應。與MM1一樣，輻條會確認收到的ISAKMP策略有效。
6. 集線器收到MM3並響應MM4。
7. 在ISAKMP協商的此時點，如果在傳輸路徑中檢測到NAT，分支可能會在埠UDP4500上響應。但是，如果未檢測到NAT，分支會繼續在UDP500上傳送MM5。最後，集線器使用MM6響應，以完成主模式交換。
   圖3 — 指步驟5至
   7

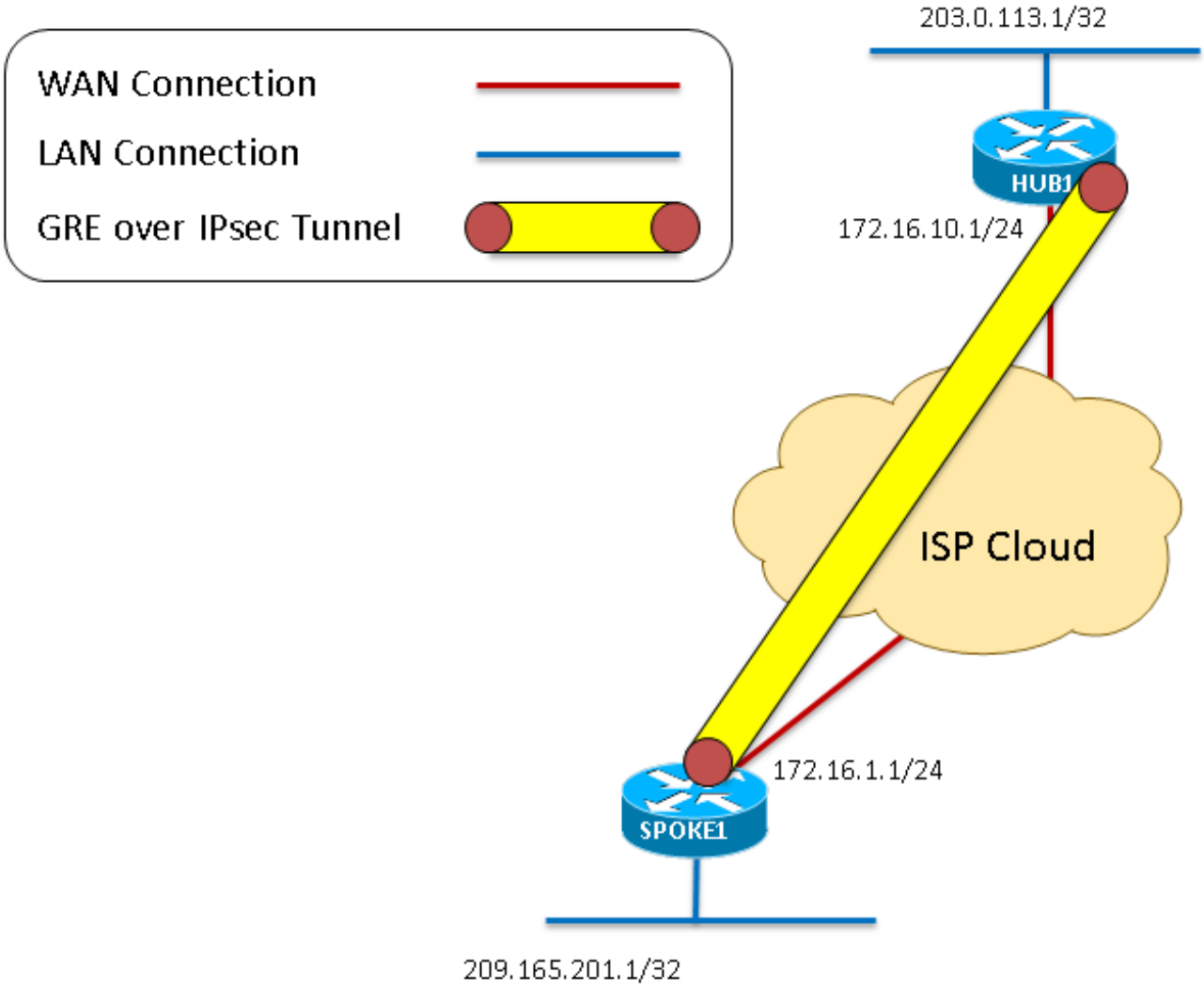



8. 分支從集線器收到MM6後，會將QM1傳送到UDP500上的集線器，以開始快速模式。
9. 中心收到QM1並使用QM2進行響應，因為接收的所有屬性都被接受。此時，集線器會為此會話建立第2階段SA。
10. 作為快速模式協商的最後一步，分支接收到QM2。然後，分支建立其第2階段SA並傳送QM3作為響應。這樣就完成了ISAKMP和IPSec協商。現在有一個IPSec會話用於加密這兩個對等體之間的GRE流量。

圖4 — 涉及步驟8至10

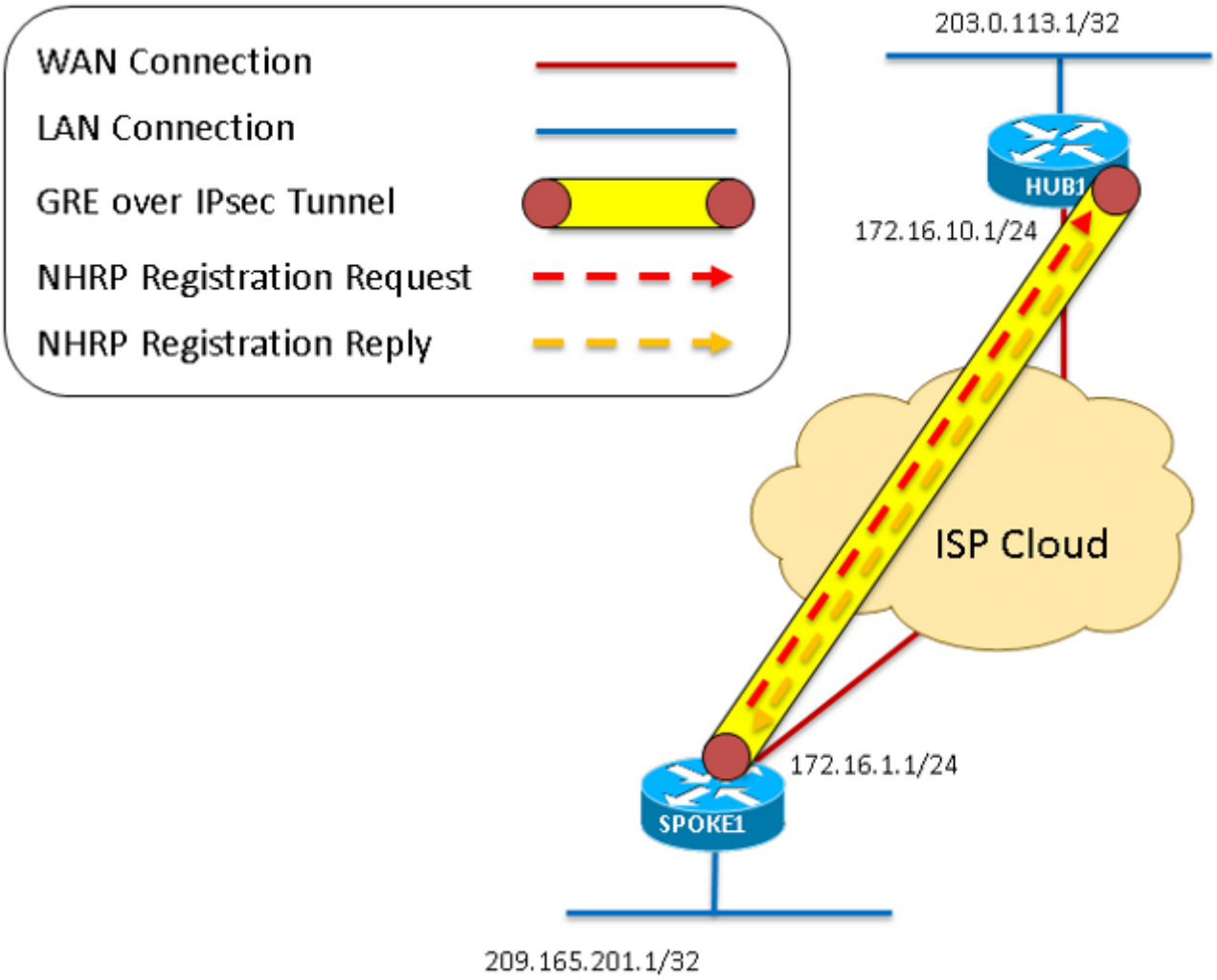



11. 由於加密作業階段已啟動且能夠傳遞流量，因此這些封包將封裝在GRE over IPSec通道中。
    圖5 — 表示步驟
    11




12. 如第一步所示，輻條會生成一個NHRP註冊請求，該請求通過GRE over IPSec隧道傳送。
13. 中心收到NHRP註冊請求，並在確認分支具有有效的隧道和非廣播多路訪問(NBMA)地址後傳送NHRP註冊應答。分支收到此NHRP註冊回覆，該回覆將完成註冊過程。

圖6 — 涉及步驟12至13




在中心和分支路由器上輸入**debug dmvpn all**命令時，將會出現這些調試。此特定命令啟用這組調試：

```
Spoke1#debug dmvpn all all
DMVPN all level debugging is on
Spoke1#show debug


NHRP:
NHRP protocol debugging is on
NHRP activity debugging is on
NHRP extension processing debugging is on
NHRP cache operations debugging is on
NHRP routing debugging is on
NHRP rate limiting debugging is on
NHRP errors debugging is on
IKEV2:
IKEV2 error debugging is on
IKEV2 terse debugging is on
IKEV2 event debugging is on
IKEV2 packet debugging is on
IKEV2 detail debugging is on



Cryptographic Subsystem:
Crypto ISAKMP debugging is on
Crypto ISAKMP Error debugging is on
Crypto IPSEC debugging is on
```

```
Crypto IPSEC Error debugging is on
Crypto secure socket events debugging is on
Tunnel Protection Debugs:
Generic Tunnel Protection debugging is on
DMVPN:
DMVPN error debugging is on
DMVPN UP/DOWN event debugging is on
DMVPN detail debugging is on
DMVPN packet debugging is on
DMVPN all level debugging is on
```

## 調試及說明

由於這是實施IPSec的配置，因此調試顯示所有ISAKMP和IPSec調試。如果未配置加密，則忽略任何以「IPsec」或「ISAKMP」開頭的調試。

**集線器調試說明**

這些前幾個調試消息是通過在隧道介面上輸入的**no shutdown**命令生成的。消息由正在啟動的加密、GRE和
在集線器上出現NHRP註冊錯誤，因為它沒有配置下一跳伺服器(NHS)（集線器是DMVPN雲的NHS）。 這

在分支的隧道為「no shutdown」後，集線器在埠500上收到IKE新SA（主模式1）消息。作為響應方，集線
ISAKMP狀態從IKE_READY更改為IKE_R_MM1。

處理收到的IKE主模式1消息。集線器確定對等體具有匹配的ISAKMP屬性，並將其填充到剛建立的ISAKMP
Diffie Hellman(DH)組1、預共用金鑰進行身份驗證，以及預設SA生存時間為86400秒(0x0 0x1 0x51 0x80 =
ISAKMP狀態仍為IKE_R_MM1，因為回覆尚未傳送到分支。
NAT-T供應商ID消息用於檢測和穿越NAT。無論是否實施NAT，在ISAKMP協商過程中都預期會出現這些消

MM_SA_SETUP（主模式2）被傳送到分支，這確認已接收MM1並將其作為有效的ISAKMP資料包接受。ISAKMP狀態從IKE_R_MM1更改為IKE_R_MM2。

MM_SA_SETUP（主模式3）由集線器接收。集線器斷定對等點是另一個Cisco IOS裝置，並且沒有為我們
ISAKMP狀態從IKE_R_MM2更改為IKE_R_MM3。

MM_KEY_EXCH（主模式4）由集線器傳送。
ISAKMP狀態從IKE_R_MM3更改為IKE_R_MM4。

MM_KEY_EXCH（主模式5）由集線器接收。
ISAKMP狀態從IKE_R_MM4更改為IKE_R_MM5。
此外，由於缺少ISAKMP配置檔案，出現「peer matches *none* of the profiles」。由於這種情況，ISAKM

最終MM_KEY_EXCH封包（主模式6）由集線器傳送。這完成了階段1協商，表示此裝置已為階段2（IPSe
ISAKMP狀態從IKE_R_MM5更改為IKE_P1_COMPLETE。

集線器收到第一個具有IPSec方案的快速模式(QM)資料包。接收的屬性指定：encaps標誌設定為2（傳輸模
KB(十六進製為0x465000),HMAC-SHA用於身份驗證，3DES用於加密。由於這些屬性是在本地配置中設定
安全引數索引(SPI)值，因此這只是一個SA的外殼，還不能用於傳遞流量。

這些只是一般的IPSec服務消息，表示它工作正常。

偽加密對映條目是為從172.16.10.1（中心公共地址）到172.16.1.1（分支公共地址）的IP協定47(GRE)建立
議中的值。

集線器傳送的第二條QM消息。由IPSec服務生成的消息，用於確認Tunnel0上已啟用隧道保護。
還會顯示另一條SA建立消息，其中包含目標IP、SPI、轉換集屬性和生存期（以千位元組和剩餘秒為單位）

這些最後的QM消息確認「快速模式」已完成，通道的兩端均已啟動IPSec。
與ISAKMP不同，每個對等體都經歷每個狀態（MM1到MM6/P1_COMPLETE），IPSec略有不同，因為只
IKE_QM_**R**_QM1消息中的「R」表示)將執行QM_READY、QM_SPI_STARVE、QM_R_QM2、QM_PHAS
QM_I_QM1到QM_PHASE2_COMPLETE。

這是從輻條收到的NHRP註冊請求，它嘗試向NHS（中心）註冊。 通常，可以看到這些分支的倍數，因為
**src NBMA**:傳送此資料包並嘗試向NHS註冊的分支節點的NBMA(internet)地址
**src protocol**:嘗試註冊的輻條的隧道地址
**dst協定**:NHS/集線器的隧道地址
**身份驗證擴**展、資料冒號(&C);NHRP身份驗證字串
**客戶端NBMA**:NHS/集線器的NBMA地址
**客戶端協定**:NHS/集線器的隧道地址

NHRP debug packets adding target network 10.1.1.1/32 available via next hop of 10.1.1.1 at NHRP of 17
中。
這些消息確認註冊成功，輻條隧道地址的解析也是如此。

這是由中心向輻射點傳送的NHRP註冊回覆，該回覆響應了之前收到的「NHRP註冊請求」。與其他註冊資
**src，dst**:通道來源（集線器）和目的地（分支）IP位址。以下是路由器傳送的GRE封包的來源和目的地
**src NBMA**:輻條的NBMA（網際網路）地址
**src protocol**:嘗試註冊的輻條的隧道地址
**dst協定**:NHS/集線器的隧道地址
**客戶端NBMA**:NHS/集線器的NBMA地址
**客戶端協定**:NHS/集線器的隧道地址
**身份驗證擴**展、資料冒號(&C);NHRP身份驗證字串

更一般的IPSec服務消息，表示它工作正常。

表示EIGRP鄰接關係與10.1.1.1上的鄰居分支已啟動的系統消息。

確認成功解決NHRP的系統消息。

# 確認功能和疑難排解

本節包含一些最有用的用於排除中心輻射和輻射點故障的**show**命令。若要啟用更具體的調試，請使用以下調試條件：

- debug dmvpn condition peer nbma *NBMA_ADDRESS*
- debug dmvpn condition peer tunnel *TUNNEL_ADDRESS*
- debug crypto condition peer ipv4 *NBMA_ADDRESS*

## show crypto sockets

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.1.1/172.16.10.1
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"
```

```
Hub#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.10.1/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"
```

## show crypto session detail

```
Spoke1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538

Hub#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:47
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none)
ivrf: (none)
Phase1_id: 172.16.1.1
Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:12
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 35 drop 0 life (KB/Sec) 4576682/3492
Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4576682/3492
```

## show crypto isakmp sa detail

```
Spoke1#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.1.1 172.16.10.1 ACTIVE 3des sha psk 1 23:59:10
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

Hub#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
```

```
psk - Preshared key, rsig - RSA signature
renc - RSA encryption IPv4 Crypto ISAKMP SA
C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 172.16.10.1 172.16.1.1 ACTIVE 3des sha psk 1 23:58:20
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

## show crypto ipsec sa detail

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.10.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xA259D71(170237297)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport,}
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:
```

```
Hub#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
#pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x8D538D11(2371063057)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas: spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
outbound pcp sas:
```

## show ip nhrp

```
Spoke1#show ip nhrp
10.1.1.254/32 via 10.1.1.254
Tunnel0 created 00:00:55, never expire
Type: static, Flags:
```

```
NBMA address: 172.16.10.1

Hub#show ip nhrp
10.1.1.1/32 via 10.1.1.1
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: unique registered
NBMA address: 172.16.1.1
```

## show ip nhs

```
Spoke1#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.254 RE priority = 0 cluster = 0

Hub#show ip nhrp nhs (As the hub is the only NHS for this DMVPN cloud,
it does not have any servers configured)
```

## show dmvpn [detail]

```
"show dmvpn detail" returns the output of show ip nhrp nhs, show dmvpn,
and show crypto session detail

Spoke1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.10.1 10.1.1.254 UP 00:00:39 S

Spoke1#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==============================================================================

Interface Tunnel0 is up/up, Addr. is 10.1.1.1, VRF ""
Tunnel Src./Dest. addr: 172.16.1.1/172.16.10.1, Tunnel VRF ""
Protocol/Transport: "GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled

IPv4 NHS:
10.1.1.254 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1 172.16.10.1 10.1.1.254 UP 00:00:41 S 10.1.1.254/32


Crypto Session Details:
```

```
------------------------------------------------------------------------------
Interface: Tunnel0
Session: [0x08D513D0]
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:59:18
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.10.1
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4596088/3558
Outbound: #pkts enc'ed 21 drop 3 life (KB/Sec) 4596088/3558
Outbound SPI : 0x A259D71, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:

Hub#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details Type:Hub, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.1.1.1 UP 00:01:30 D

Hub#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket # Ent --> Number of NHRP entries with same NBMA peer NHS
Status: E --> Expecting Replies, R --> Responding, W --> Waiting UpDn Time --> Up or Down Time
for a Tunnel ==========================================================================
Interface Tunnel0 is up/up, Addr. is 10.1.1.254, VRF "" Tunnel Src./Dest. addr:
172.16.10.1/MGRE, Tunnel VRF "" Protocol/Transport: "multi-GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled Type:Hub, Total NBMA Peers (v4/v6): 1
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network ----- --------------- --
------------- ----- -------- ----- ----------------- 1 172.16.1.1 10.1.1.1 UP 00:01:32 D
10.1.1.1/32

Crypto Session Details:
------------------------------------------------------------------------------ Interface:
Tunnel0
Session: [0x08A27858]
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:26
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.1.1
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound SPI : 0x8D538D11, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:
```

# 相關資訊

- [IPsec 疑難排解：瞭解和使用偵錯指令]
- [下一代加密]

- RFC3706:IKE失效對等體偵測
- RFC3947:IKE NAT遍歷
- 技術支援與文件 - Cisco Systems