DMVPN フェーズ 1 のデバッグ トラブルシューティング ガイド

内容

概要

このドキュメントでは、Dynamic Multipoint Virtual Private Network（DMVPN）フェーズ 1 導入のハブとスポークで表示されることがあるデバッグ メッセージについて説明します。

前提条件

このドキュメントの設定コマンドおよびデバッグ コマンドを実行するには、Cisco IOS® Release 12.4(9)T 以降が稼働している 2 台の Cisco ルータが必要です。一般に、基本 DMVPN フェーズ 1 では Cisco IOS リリース 12.2(13)T 以降またはリリース 12.2(33)XNC（アグリゲーション サービス ルータ（ASR）の場合）が必要ですが、このドキュメントに示されている機能とデバッグがサポートされていない可能性があります。

要件

次の項目に関する知識があることが推奨されます。

- 総称ルーティング カプセル化（GRE）
- Next Hop Resolution Protocol（NHRP）
- Internet Security Association and Key Management Protocol（ISAKMP）
- ンターネット キー交換（IKE）
- IPSec（Internet Protocol Security）
- 次のルーティング プロトコルのうち、1 つ以上。Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Routing Information Protocol（RIP）、Border Gateway Protocol（BGP）

使用するコンポーネント

このドキュメントの情報は、Cisco IOS リリース 15.1(4)M4 が稼働する Cisco 2911 サービス統合型ルータに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

重要な機能拡張

次の Cisco IOS バージョンでは、DMVPN フェーズ 1 の重要な機能またはフィックスが導入されています。

- リリース 12.2(18)SXF5：Public Key Infrastructure（PKI）使用時の ISAKMP のサポートが強化されました
- リリース 12.2(33)XNE：ASR、IPSec プロファイル、トンネル保護、 IPSec ネットワーク アドレス変換（NAT）トラバーサル
- リリース 12.3(7)T：Inside Virtual Routing and Forwarding（iVRF）サポート
- リリース 12.3(11)T：Front-door Virtual Routing and Forwarding（fVRF）サポート
- リリース 12.4(9)T：各種 DMVPN 関連デバッグおよびコマンドのサポート
- リリース 12.4(15)T：共有トンネル保護
- リリース 12.4(20)T： IPv6 over DMVPN
- リリース 15.0(1)M - NHRP トンネル ヘルス モニタリング

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

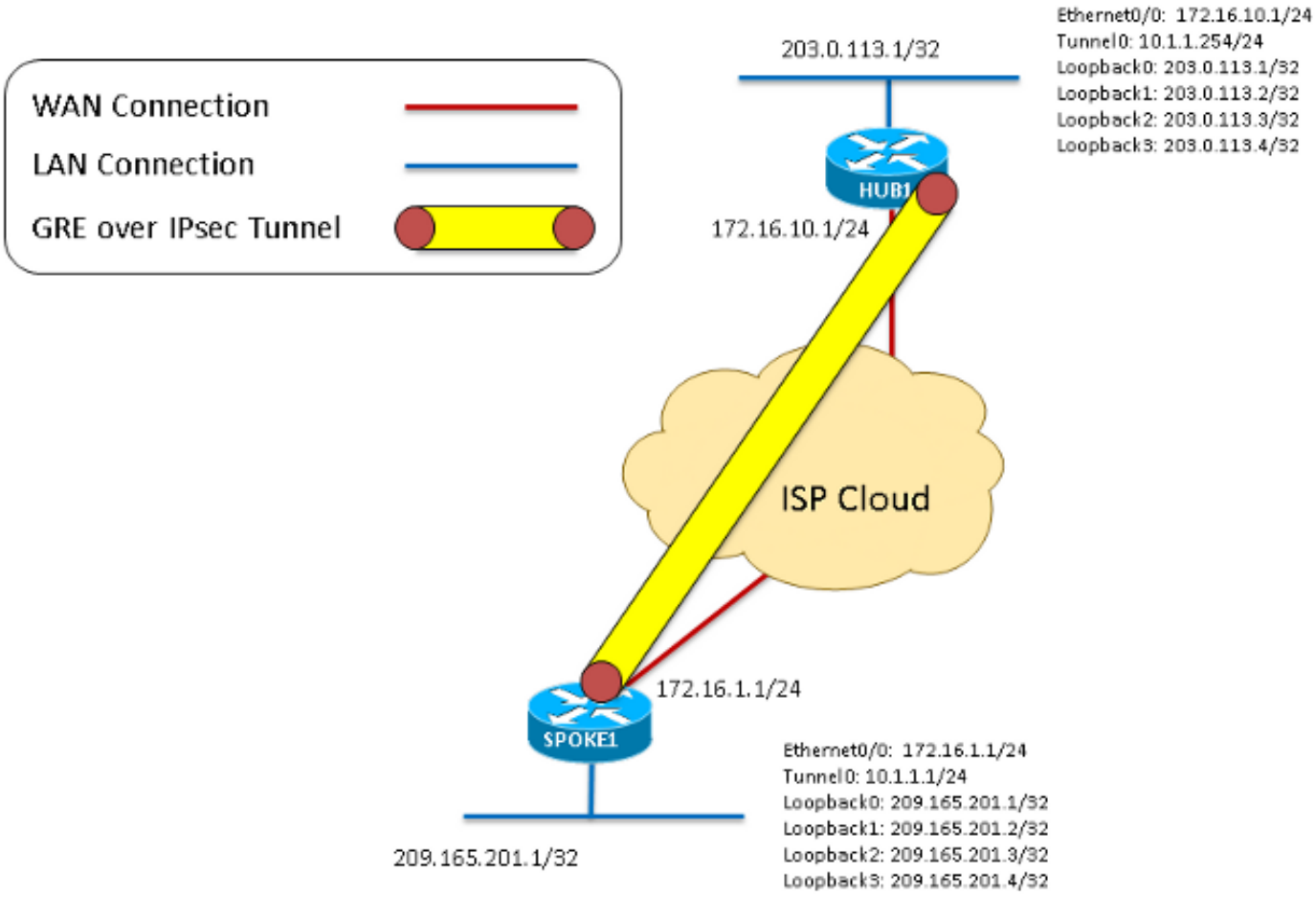
関連コンフィギュレーション

トポロジの概要

このトポロジでは、リリース 15.1(4)M4 が稼働する 2 台の 2911 ISR が、DMVPN フェーズ 1 用に設定されています（ハブとして 1 台、スポークとして 1 台）。各ルータで「インターネット」インターフェイスとして Ethernet0/0 が使用されています。4 つのループバック インターフェイ

スが、ハブ サイトまたはスポーク サイトで稼働しているローカル エリア ネットワークをシミュレーションするように設定されています。これはスポークが 1 つだけの DMVPN フェーズ 1 トポロジーであるため、このスポークはマルチポイント GRE トンネルではなく、ポイントツーポイント GRE トンネルを使用して設定されています。厳密に一致するように、各ルータで同じ暗号化設定 (ISAKMP および IPSec) が使用されています。

図 1



暗号化

これは、ハブとスポークで同一です。

```
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
```

ハブ

```
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
```

スポーク

```
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
```

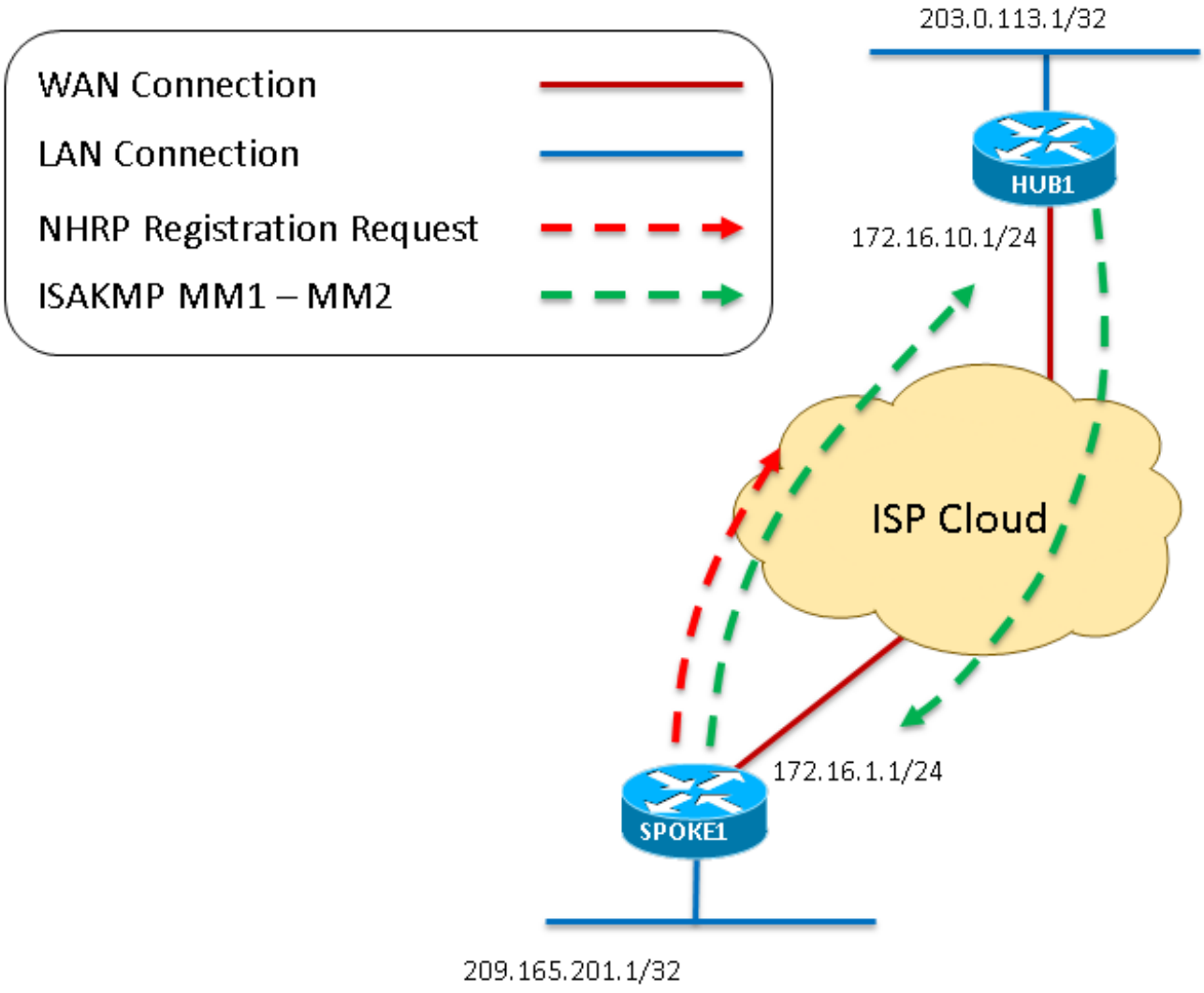
```
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

デバッグ

パケット フロー全体図

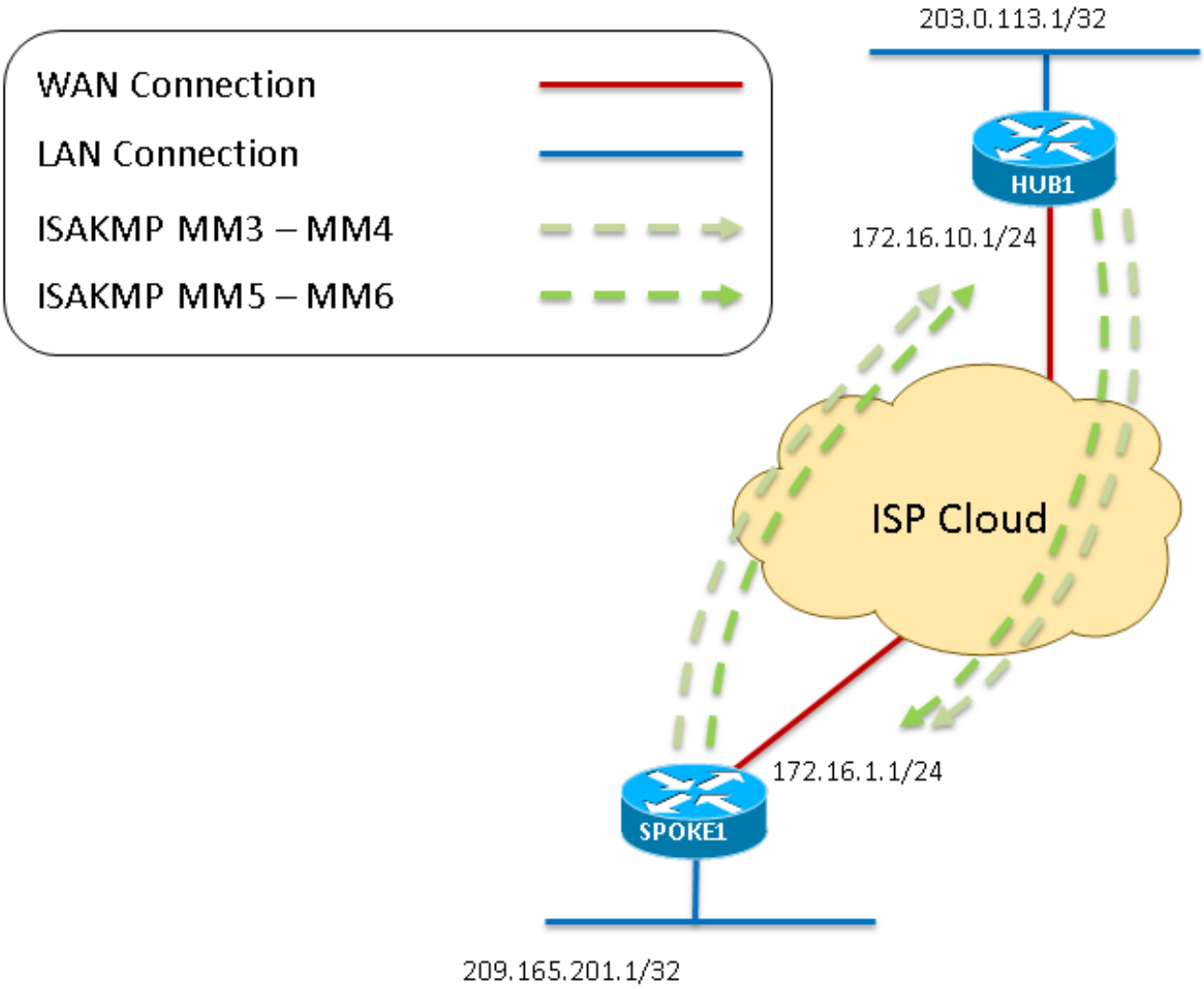
これは、このドキュメントに示す DMVPN パケット フロー全体を示す図です。各ステップを説明する詳細なデバッグも収録されています。

1. スポークのトンネルが「no shutdown」の場合、NHRP登録要求が生成され、DMVPNプロセスが開始されます。ハブの設定は完全に動的であるため、スポークは接続を開始するエンドポイントである必要があります。
2. その後 NHRP 登録要求が GRE でカプセル化され、これにより暗号プロセスの開始がトリガーされます。
3. この時点で、最初のISAKMPメインモードメッセージ(ISAKMP MM1)がスポークからハブにポートUDP500で送信されます。
4. ハブは MM1 を受信して処理し、一致する ISAKMP ポリシーがあるため ISAKMP MM2 で応答します。
   図 2：ステップ 1 から 4 を参照

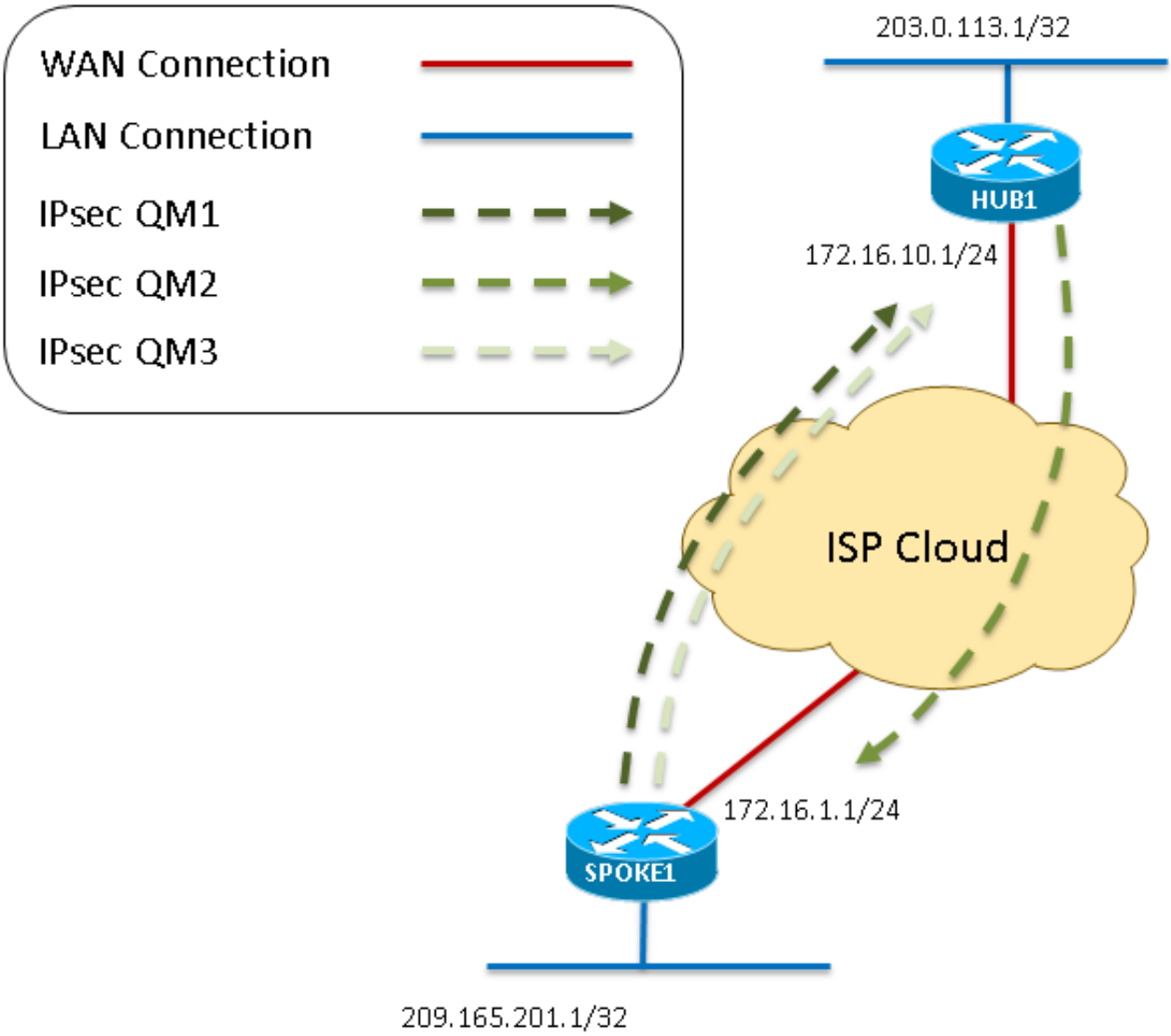


5. スポークがMM2を受信すると、MM3で応答します。MM1と同様に、スポークは受信したISAKMPポリシーが有効であることを確認します。

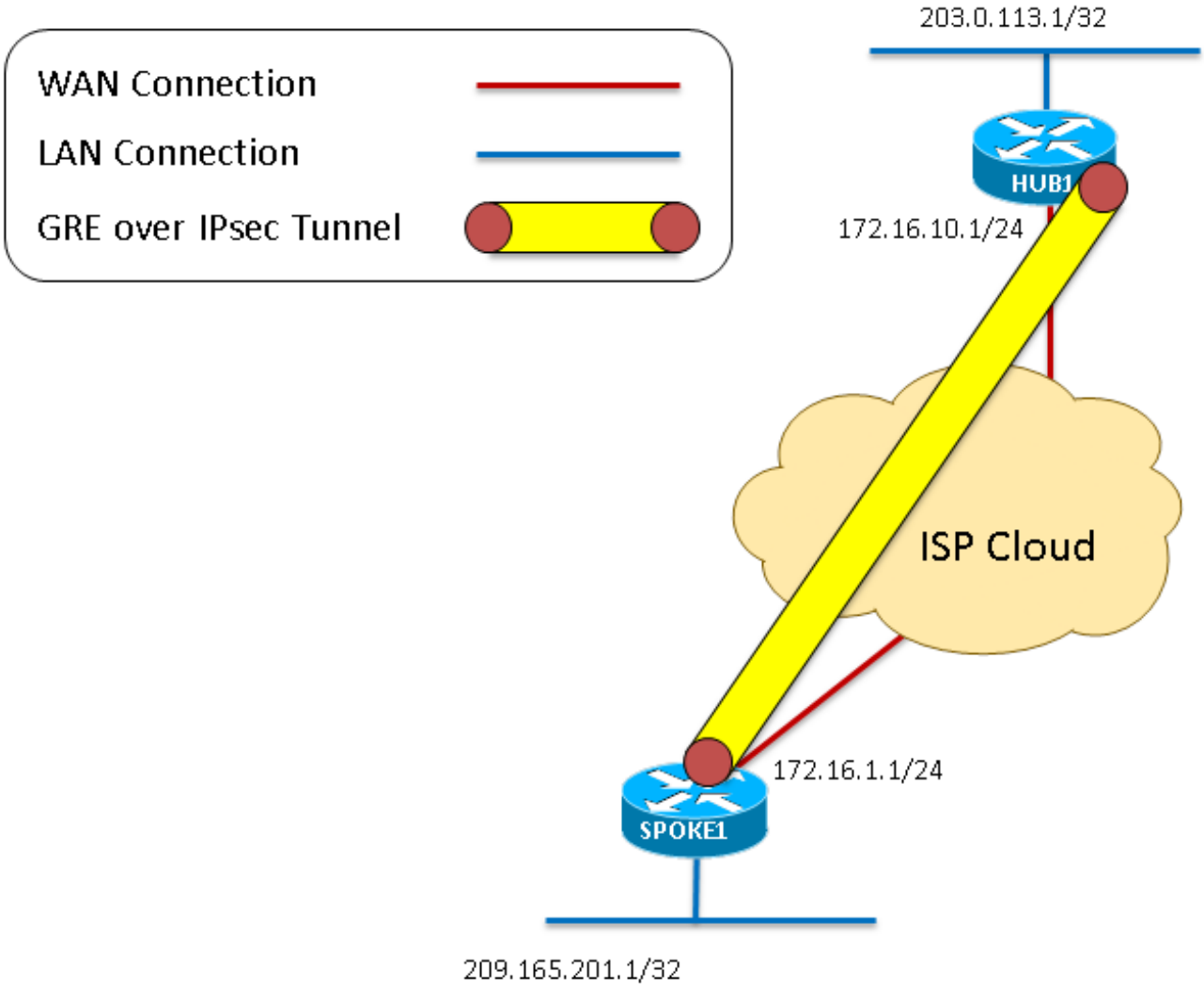
6. ハブは MM3 を受信し、MM4 で応答します。
7. ISAKMP ネゴシエーションのこの時点で、遷移パスで NAT が検出されると、スポークがポート UDP 4500 で応答することがあります。ただし、NATが検出されない場合、スポークは続行し、UDP500でMM5を送信します。最後に、ハブはメインモード交換を完了するためにMM6で応答します。
   図 3：ステップ 5 から 7 を参照



8. スポークはハブから MM6 を受信すると、クイック モードを開始するため UDP500 からハブに QM1 を送信します。
9. ハブは QM1 を受信し、受信した属性がすべて受け入れられるため QM2 で応答します。この時点で、ハブはこのセッションのためのフェーズ 2 SA を作成します。
10. クイック モード ネゴシエーションの最終ステップとして、スポークが QM2 を受信します。その後スポークは、フェーズ 2 SA を作成し、応答として QM3 を送信します。これにより ISAKMP と IPSec のネゴシエーションが完了します。これで、この 2 つのピア間の GRE トラフィックを暗号化する IPSec セッションが確立しました。
    図 4：ステップ 8 から 10 を参照

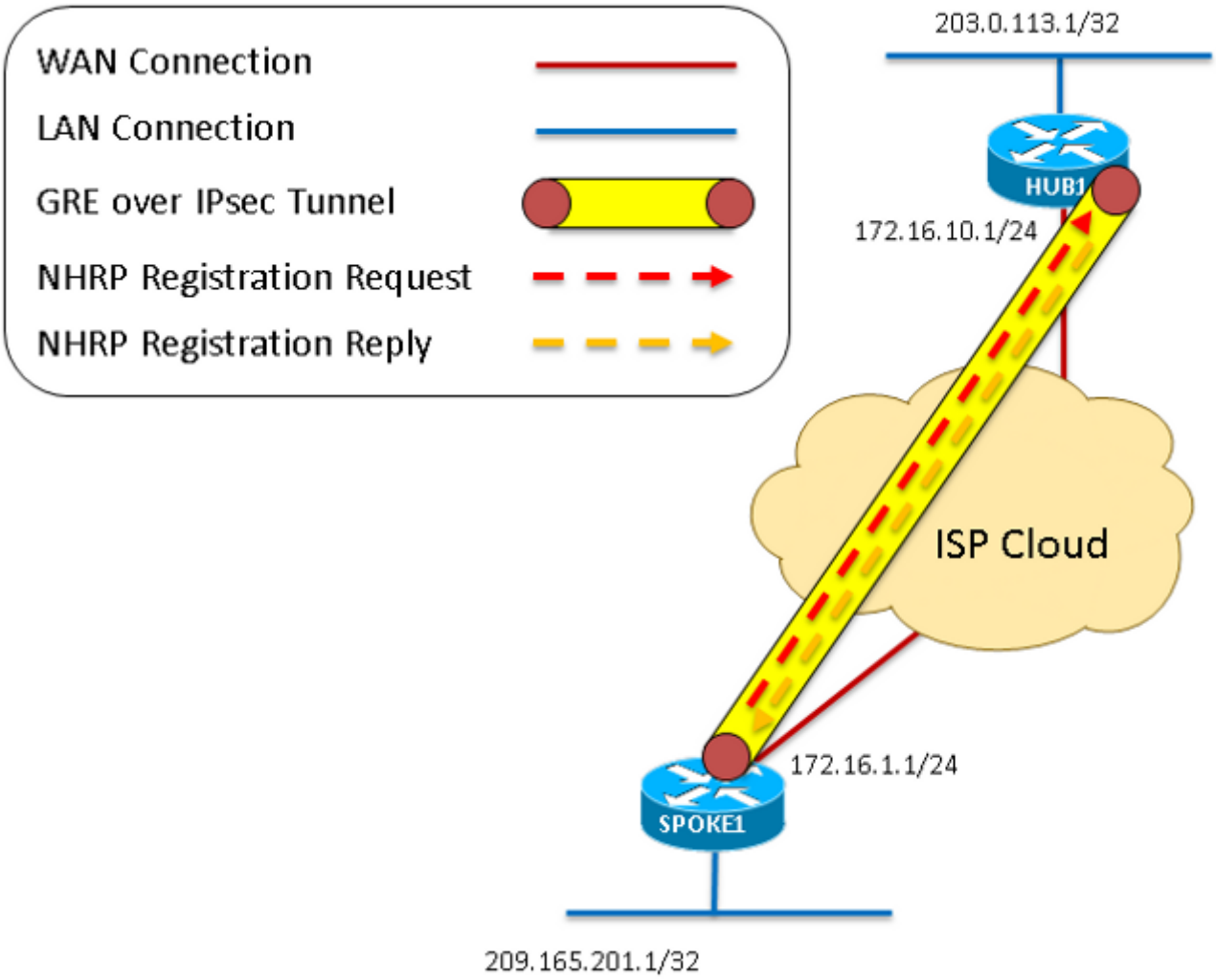


11. 暗号化セッションが確立され、トラフィックを渡すことができるようになったため、これらのパケットは GRE over IPSec トンネル内にカプセル化されています。
    図 5：ステップ 11 を参照



12. 1 番目のステップで示したように、スポークにより NHRP 登録要求が生成され、この要求が GRE over IPSec トンネル経由で送信されます。
13. ハブが NHRP 登録要求を受信します。スポークに有効なトンネルおよびノンブロードキャスト マルチアクセス (NBMA) アドレスがあることを確認すると、NHRP 登録応答を送信します。スポークがこの NHRP 登録応答を受信します。これにより登録プロセスが完了します。

図 6：ステップ 12 から 13 を参照



次に示すデバッグは、ハブ ルータとスポーク ルータで **debug dmvpn all all コマンドを入力した結果です。**この特殊なコマンドは、次の一連のデバッグを有効にします。

```
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
```

デバッグと説明

この構成では IPSec が実装されているため、デバッグによりすべての ISAKMP および IPSec デバッグが表示されます。暗号化が設定されていない場合は、「IPsec」または「ISAKMP」で始まるデバッグは無視してください。

最初のいくつかのデバッグ メッセージは、トンネル インターフェイスで入力された **no shutdown コマン**
す。
ハブではネクストホップ サーバ（NHS）が設定されていないため（このハブは DMVPN クラウドの NH

スポークのトンネルが「no shutdown」になると、ハブはポート500でIKE NEW SA（メインモード1）メ
ISAKMP の状態が IKE_READY から IKE_R_MM1 に変更されます。

受信した IKE メイン モード 1 メッセージが処理されます。ハブは、ピアに一致する ISAKMP 属性がある
号化用 3DES-CBC 、SHA のハッシュ、Diffie-Hellman（DH）グループ 1、認証用事前共有キー、および
応答がスポークに送信されていないため、ISAKMP の状態はまだ IKE_R_MM1 です。
NAT-T ベンダー ID メッセージが NAT の検出とトラバーサルで使用されます。これらのメッセージは、
Detection（DPD; デッドピア検出）でも同様のメッセージが 表示されます。

MM_SA_SETUP (メイン モード 2) がスポークに送信されます。これにより、MM1 が受信され、有効な
ISAKMP の状態が IKE_R_MM1 から IKE_R_MM2 に変更されます。

ハブが MM_SA_SETUP (メイン モード 3) を受信します。ハブは、ピアが別の Cisco IOS デバイスであ
ISAKMP の状態が IKE_R_MM2 から IKE_R_MM3 に変更されます。

ハブが MM_KEY_EXCH (メイン モード 4) を送信します。
ISAKMP の状態が IKE_R_MM3 から IKE_R_MM4 に変更されます。

ハブが MM_KEY_EXCH (メイン モード 5) を受信します。
ISAKMP の状態が IKE_R_MM4 から IKE_R_MM5 に変更されます。
また、ISAKMPプロファイルがないため、「peer matches *none* of the profiles」が表示されます。この

ハブが最終 MM_KEY_EXCH パケット（メイン モード 6）を送信します。これで、フェーズ 1 ネゴシエ
ISAKMP の状態が IKE_R_MM5 から IKE_P1_COMPLETE に変更されます。

ハブが最初のクイック モード（QM）パケットを受信します。このパケットには IPSec プロポーザルが含
ォルト SA ライフタイム 3600 秒および 4608000 キロバイト（16 進数値では 0x465000）、認証に HMA
け入れられ、IPSec SA のシェルが作成されます。セキュリティ パラメータ インデックス（SPI）の値が

これらは、IPSec サービスが適切に機能していることを示す IPSec サービスの一般メッセージです。

172.16.10.1 (ハブのパブリック アドレス) から 172.16.1.1 (スポークのパブリック アドレス) までの I
と発信とトラフィックの両方に対して IPSec SA/SPI が作成されます。

ハブが送信する 2 番目の QM メッセージ。Tunnel0 でトンネル保護が有効であることを示す、IPSec サ
宛先 IP、SPI、トランスフォーム セット属性、および残りのライフタイム (キロバイト数および秒数) を

これらの最終 QM メッセージにより、クイック モードが完了し、トンネルの両側で IPSec が稼働してい
各ピアがすべての状態（MM1 から MM6/P1_COMPLETE まで）を変遷する ISAKMP とは異なり、IPSe
QM_READY、QM_SPI_STARVE、QM_R_QM2、QM_PHASE2_COMPLETEになります。発信側（スポ

これは、NHS（ハブ）への登録のためにスポークから受信した NHRP 登録要求です。 スポークは「登録
src NBMA:このパケットを送信し NHS への登録を試行するスポークの NBMA（インターネット）アドレ
src protocol:登録を試行するスポークのトンネル アドレス。
dst protocol：NHS/ハブのトンネル アドレス
認証拡張、データ&コロン；NHRP 認証ストリング
client NBMA:NHS/ハブの NBMA アドレス
client protocol:NHS/ハブのトンネル アドレス

172.16.1.1のNHRPで10.1.1.1のネクストホップ経由で使用可能なターゲットネットワーク10.1.1.1/32を
これらのメッセージは、登録が成功し、スポーク トンネル アドレスが解決されたことを確認するメッセ

これは、先に受信した「NHRP登録要求」に応答して、ハブからスポークに送信されたNHRP登録応答で
src,dst：トンネルの送信元（ハブ）と宛先（スポーク）の IP アドレス。これらは、ルータが送信する G
src NBMA:スポークの NBMA（インターネット）アドレス
src protocol:登録を試行するスポークのトンネル アドレス。
dst protocol：NHS/ハブのトンネル アドレス
client NBMA:NHS/ハブの NBMA アドレス

client protocol:NHS/ハブのトンネル アドレス
認証拡張、データ&コロン；NHRP 認証ストリング

IPSec サービスが適切に機能していることを示すその他の一般的な IPSec サービス メッセージです。

10.1.1.1 の隣接スポークとの EIGRP 隣接関係が有効であることを示すシステム メッセージ。

NHRP 解決が成功したことを確認するシステム メッセージ。

機能の確認とトラブルシューティング

ここでは、ハブとスポークの両方のトラブルシューティングに使用される最も有用な show コマンドの一部について説明します。より具体的なデバッグを有効にするには、次のデバッグ条件を使用します。

- 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:
```

関連情報

- IPSec のトラブルシューティング：debug コマンドの説明と使用
- 次世代暗号化
- RFC3706：IKE デッドピア検出
- RFC3947：IKE NAT トラバーサル
- テクニカル サポートとドキュメント – Cisco Systems