# DMVPN Phase 1 Debugs Troubleshoot Guide

## Contents



## Introduction

This document describes the debug messages you would encounter on the hub and spoke of a Dynamic Multipoint Virtual Private Network (DMVPN) Phase 1 deployment.

## Prerequisites

For the configuration and debug commands in this document, you will need two Cisco routers which run Cisco IOS® Release 12.4(9)T or later. In general, a basic DMVPN Phase 1 requires Cisco IOS Release 12.2(13)T or later or Release 12.2(33)XNC for the Aggregation Services Router (ASR), although the features and debugs seen in this document might not be supported.

### Requirements

Cisco recommends that you have knowledge of these topics:

- Generic Routing Encapsulation (GRE)

- Next Hop Resolution Protocol (NHRP)
- Internet Security Association and Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE)
- Internet Protocol Security (IPSec)
- At least one of these routing protocols: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Border Gateway Protocol (BGP)

### Components Used

The information in this document is based on Cisco 2911 Integrated Services Routers (ISRs) which run Cisco IOS Release 15.1(4)M4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Significant Enhancements

These Cisco IOS versions introduced significant features or fixes for DMVPN Phase 1:

- Release 12.2(18)SXF5 - better support for ISAKMP when using Public Key Infrastructure (PKI)
- Release 12.2(33)XNE - ASR, IPSec Profiles, Tunnel Protection, IPSec Network Address Translation (NAT) Traversal
- Release 12.3(7)T - inside Virtual Routing and Forwarding (iVRF) support
- Release 12.3(11)T - front-door Virtual Routing and Forwarding (fVRF) support
- Release 12.4(9)T - support for various DMVPN related debugs and commands
- Release 12.4(15)T - Shared Tunnel Protection
- Release 12.4(20)T - IPv6 over DMVPN
- Release 15.0(1)M - NHRP Tunnel Health Monitoring

### Conventions

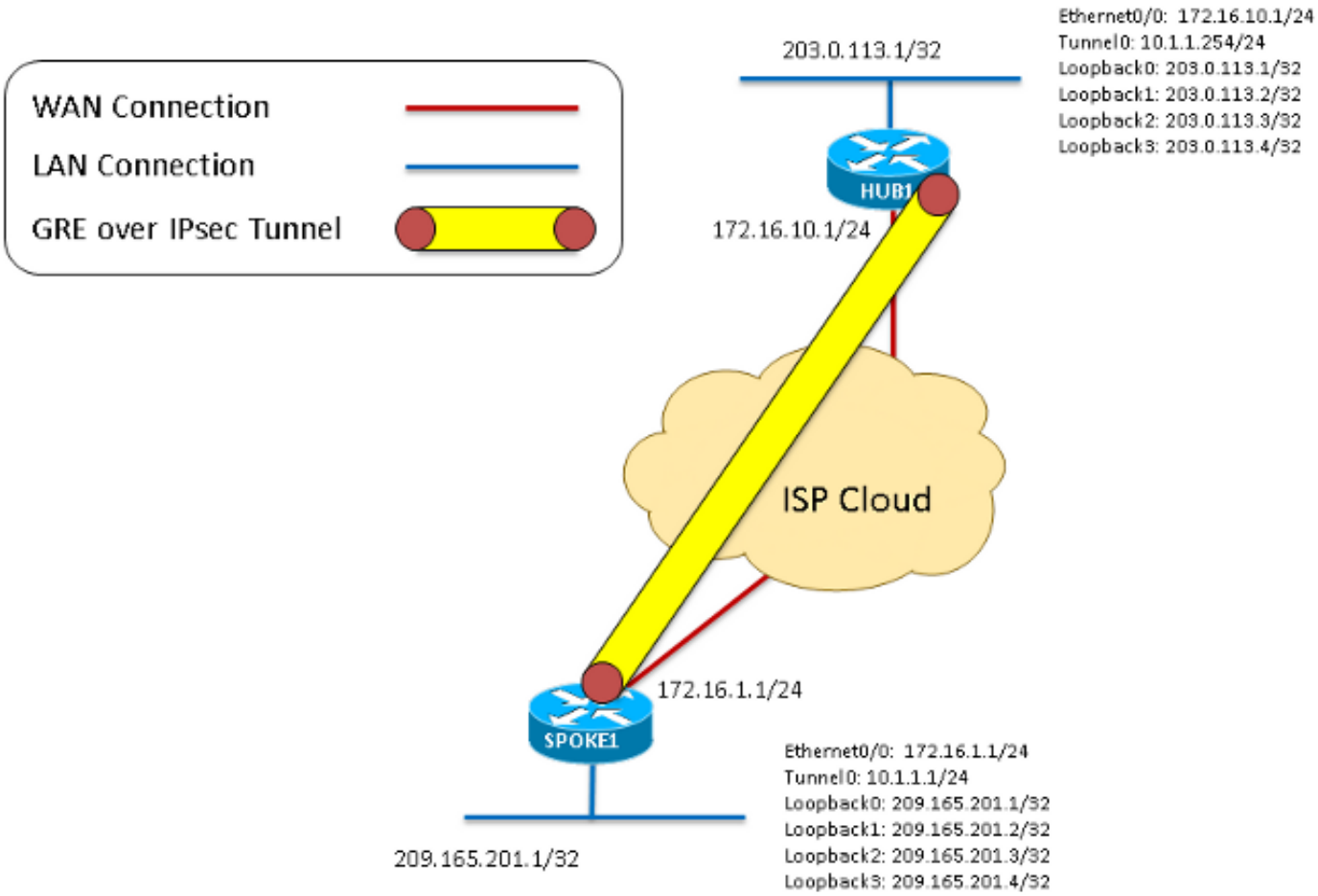
Refer to Cisco Technical Tips Conventions for information on document conventions.

## Relevant Configuration

### Topology Overview

For this topology, two 2911 ISRs which run Release 15.1(4)M4 were configured for DMVPN Phase 1: one as a hub and one as a spoke. Ethernet0/0 was used as the "internet" interface on each router. The four loopback interfaces are configured to simulate local area networks that live at the hub or spoke site. As this is a DMVPN Phase 1 topology with only one spoke, the spoke is configured with a point-to-point GRE tunnel rather than a multipoint GRE tunnel. The same crypto configuraton (ISAKMP and IPSec) was used on each router to ensure they matched exactly.

Diagram 1




## Crypto

This is the same on the hub and the spoke.

```
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
```

## Hub

```
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
```

### Spoke

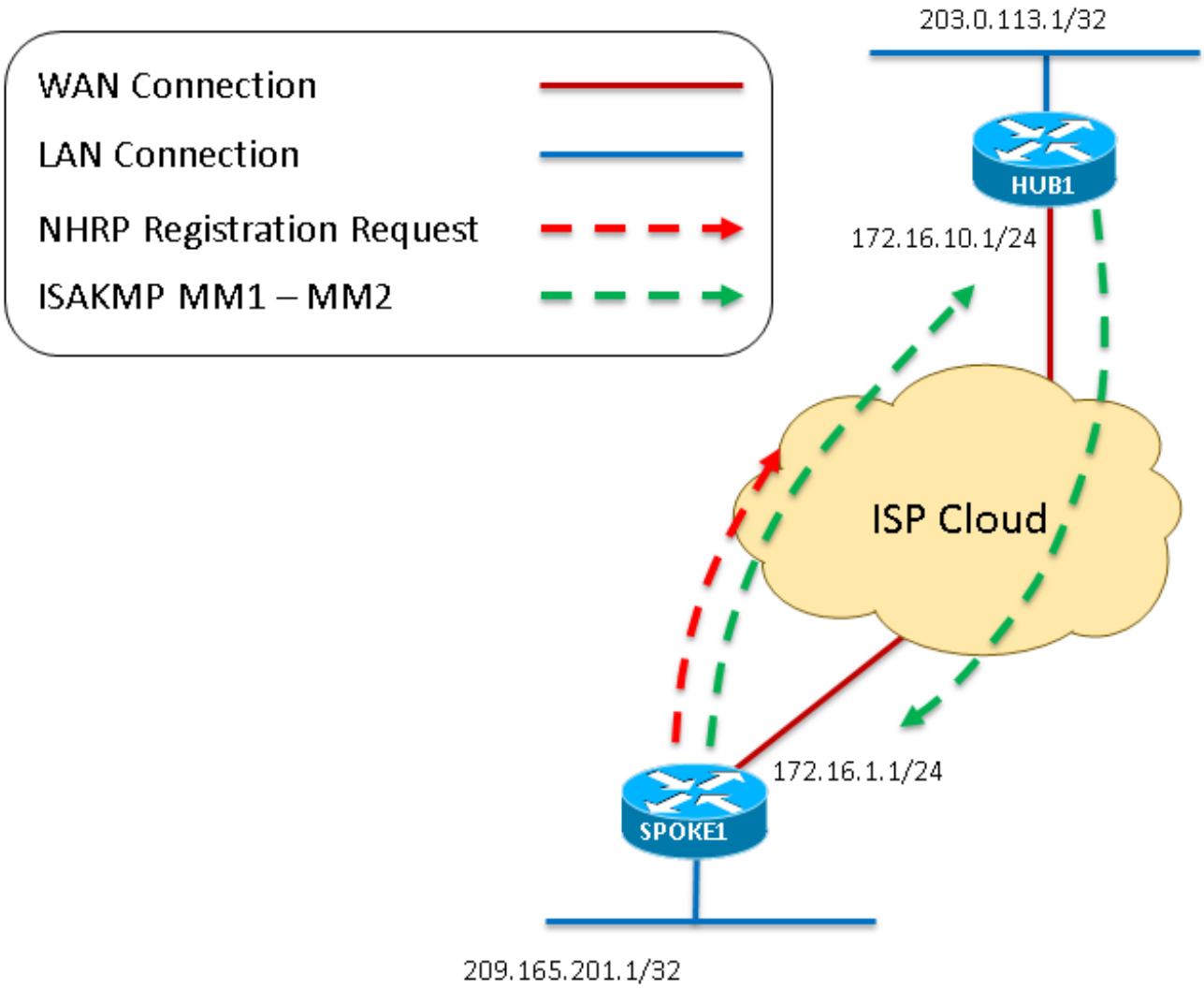
```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile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

# Debugs

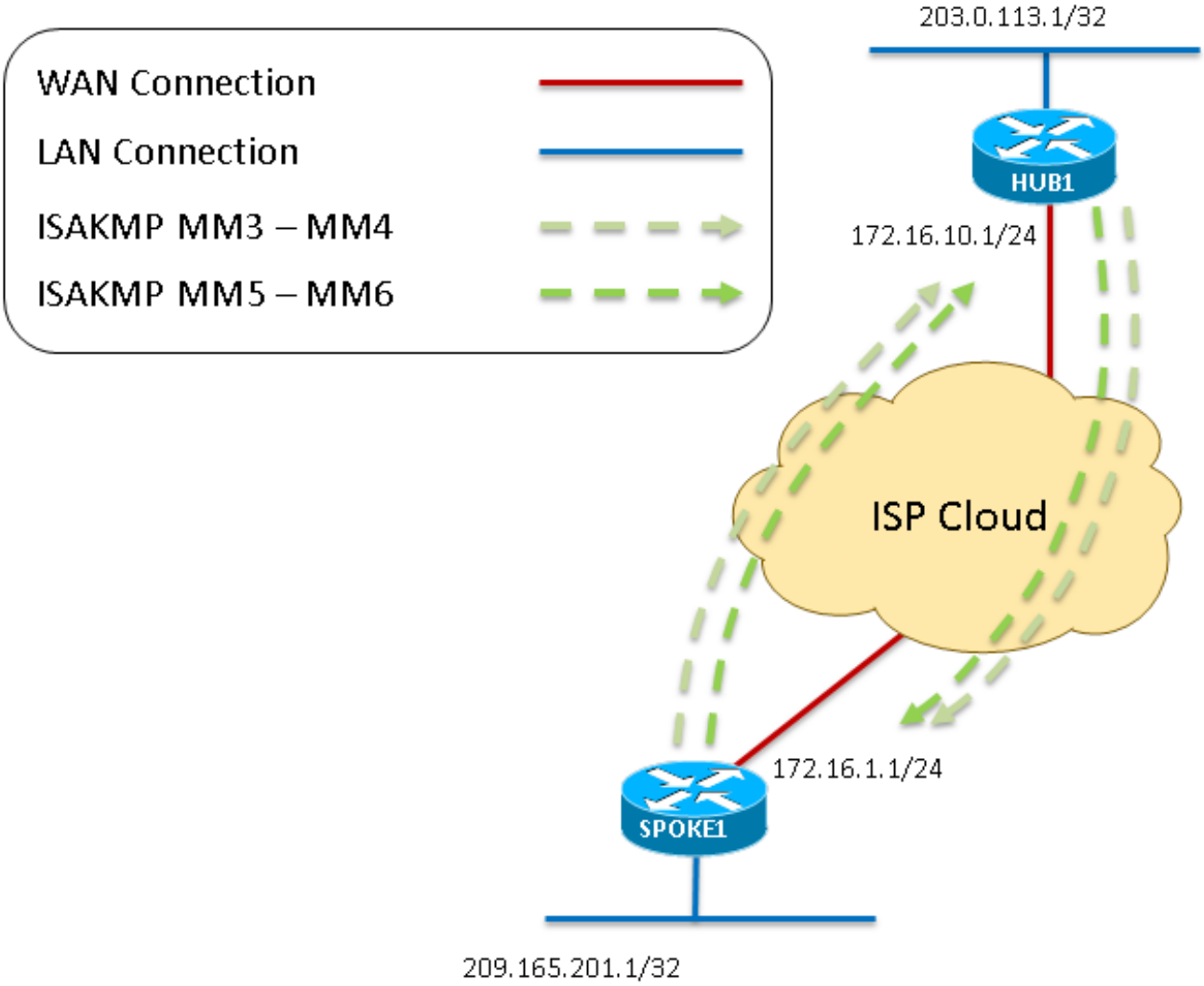
### Packet Flow Visualization

This is a visualization of the entire DMVPN packet flow as seen in this document. More detailed debugs that explain each of the steps are also included.

1. When the Tunnel on the Spoke is “no shutdown” it generates a NHRP Registration Request, which starts the DMVPN process. As the Hub’s configuration is completely dynamic, the Spoke must be the endpoint which initiates the connection.
2. The NHRP Registration Request is then encapsulated in GRE which triggers the crypto process to start.
3. At this point, the first ISAKMP Main Mode message – ISAKMP MM1 – is sent from the Spoke to the Hub on port UDP500.
4. The Hub receives and processes MM1 and responds with ISAKMP MM2, as it has a matching ISAKMP policy.
   Diagram 2 - refers to steps 1 to 4

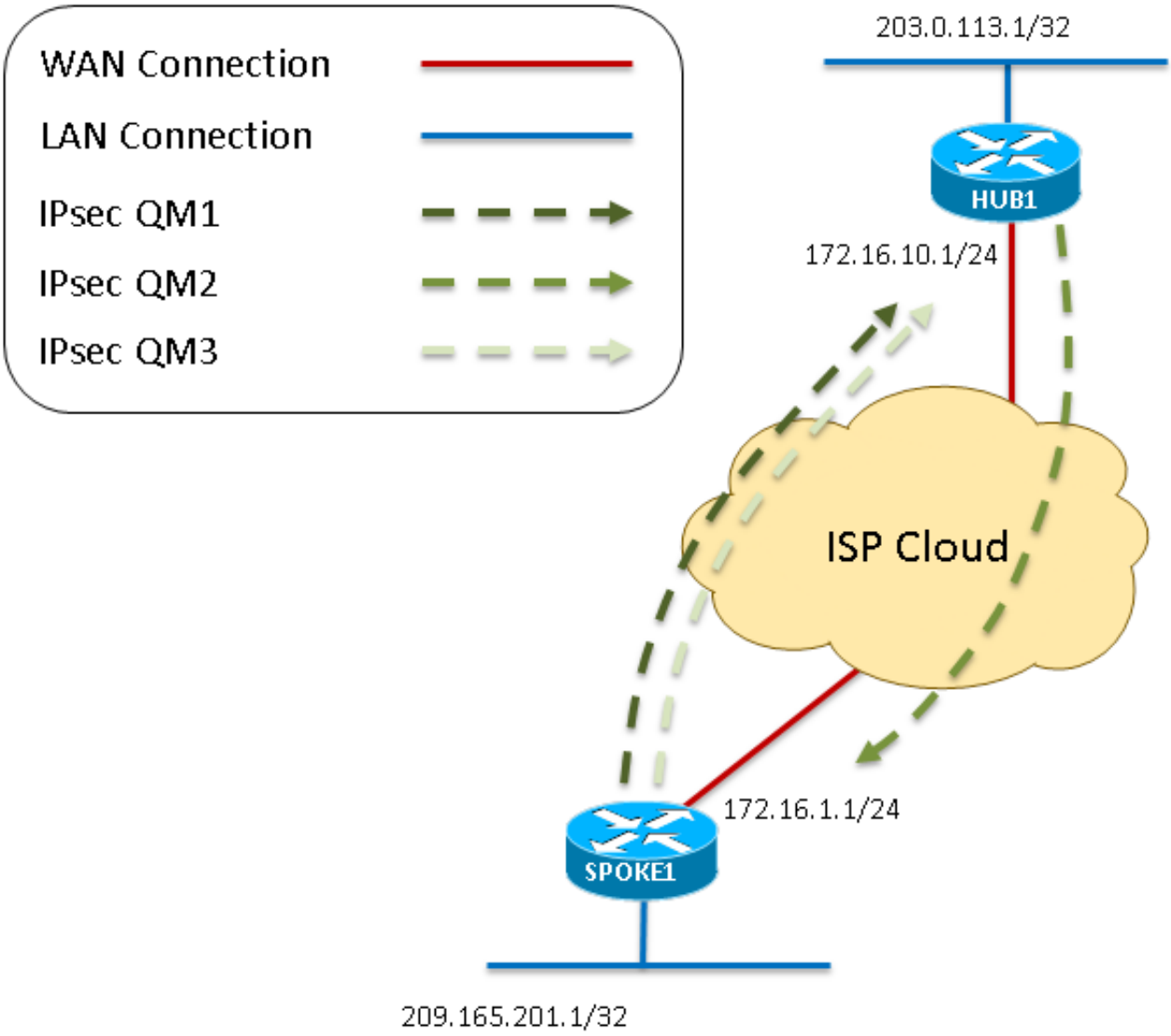



5. Once the Spoke receives the MM2, it responds with MM3. As with MM1, the Spoke confirms the received ISAKMP policy is valid.
6. The Hub receives MM3 and responds with MM4.
7. At this point in the ISAKMP negotiation, the Spoke might respond on port UDP4500 if NAT is detected in the transit path. However, if no NAT is detected the Spoke continues and sends MM5 on UDP500. Lastly, the Hub responds with MM6 in order to complete the Main Mode exchange.
   Diagram 3 - refers to steps 5 to 7

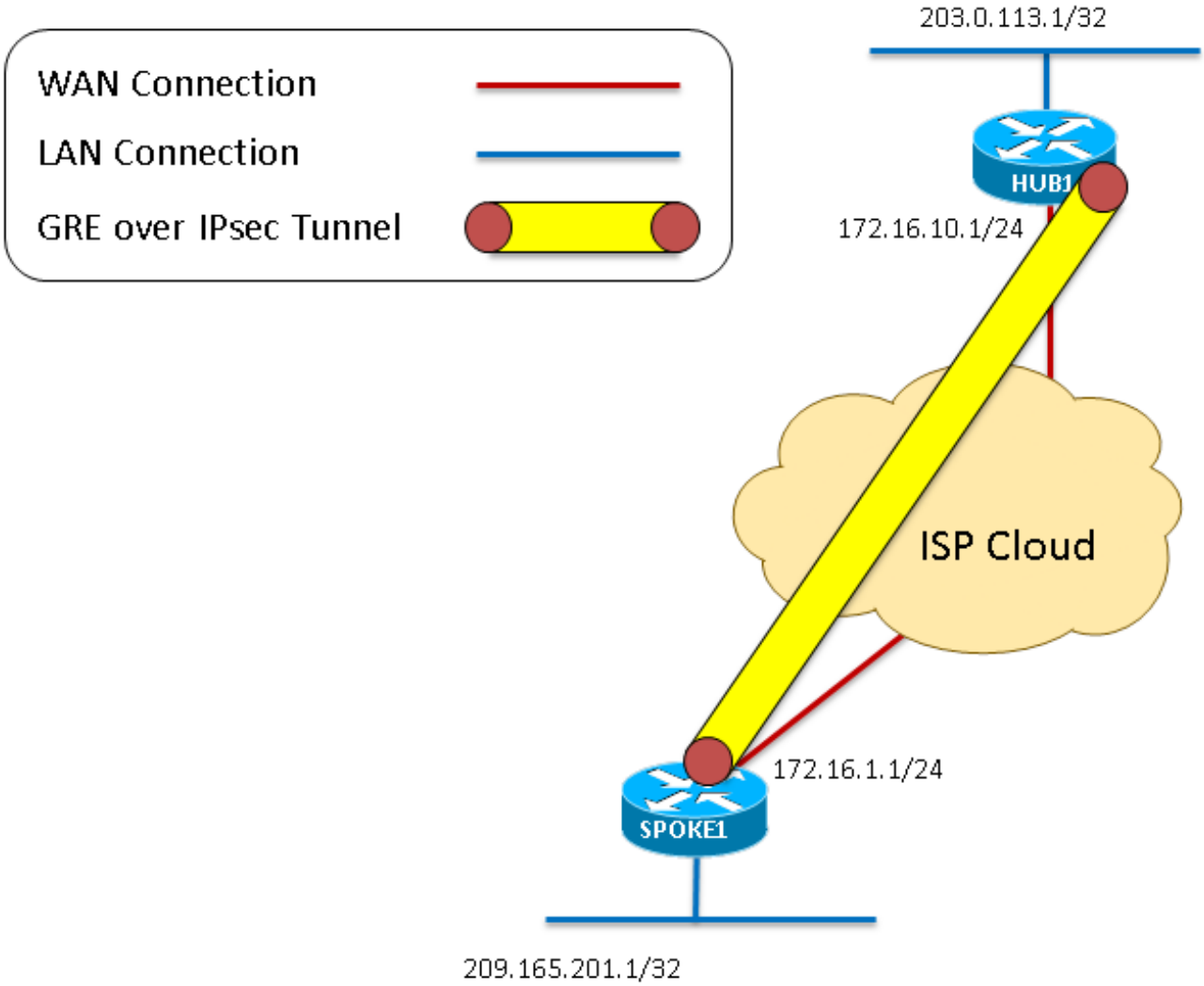



8. Once the Spoke receives MM6 from the Hub, it sends QM1 to the Hub on UDP500 in order to begin Quick Mode.
9. The Hub receives QM1 and responds with QM2, as all received attributes are accepted. At this point the Hub creates the Phase 2 SAs for this session.
10. As the last step of the Quick Mode negotiation, QM2 is received by the Spoke. The Spoke then creates its Phase 2 SAs and sends QM3 in response. This completes the ISAKMP and IPSec negotiation. There is now an IPSec session which encrypts GRE traffic between these two peers.

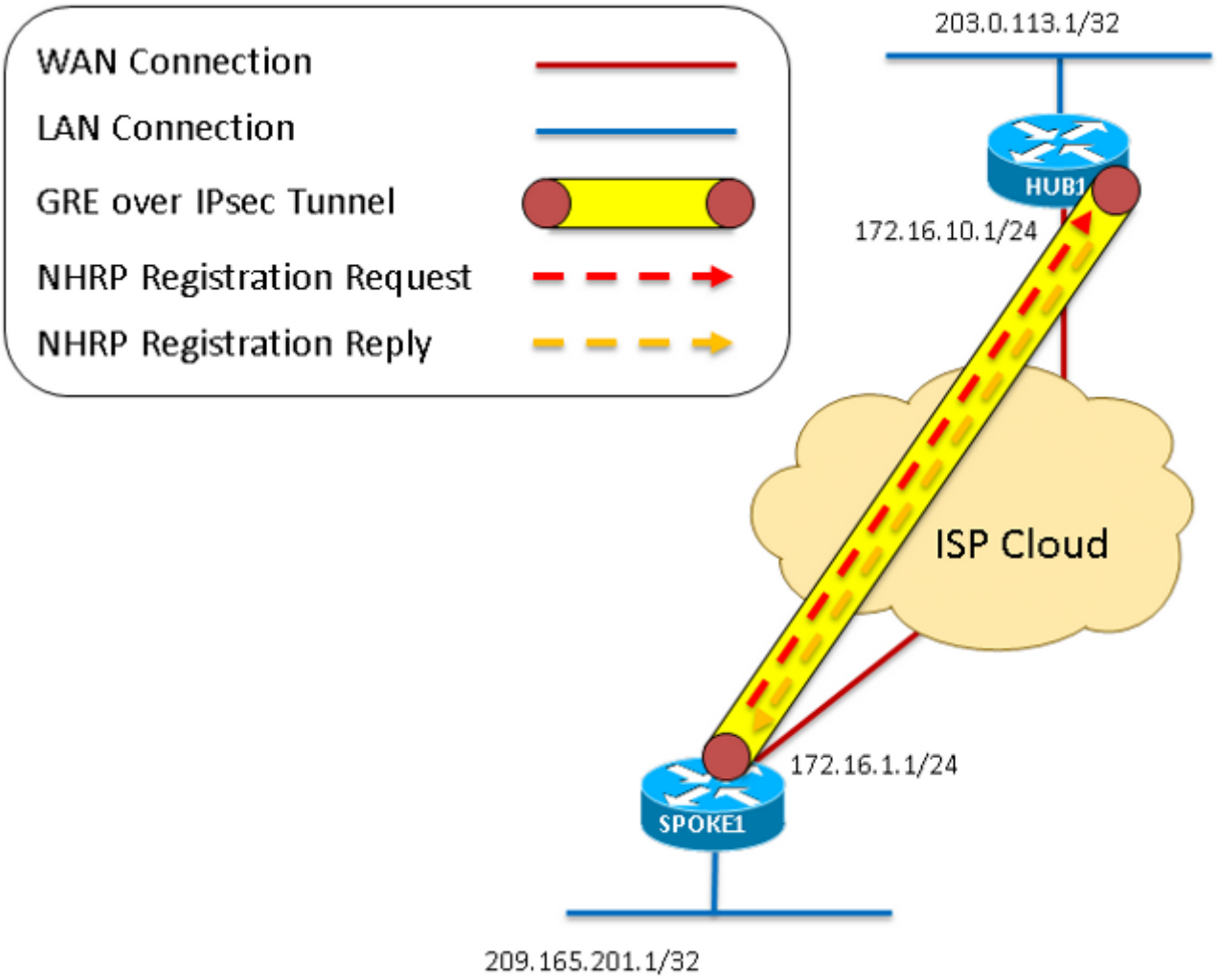
    Diagram 4 - refers to steps 8 to 10




11. Now that the crypto session is up and able to pass traffic, these packets are encapsulated within the GRE over IPSec tunnel.
    Diagram 5 - refers to step
    11




12. As was seen in the first steps, the Spoke generates an NHRP Registration Request which is sent across the GRE over IPSec tunnel.
13. The Hub receives the NHRP Registration Requests and sends an NHRP Registration Reply once it confirms the Spoke has a valid Tunnel and Nonbroadcast Multiaccess (NBMA) address. The Spoke receives this NHRP Registration Reply which completes the registration process.
    Diagram 6 - refers to steps 12 to
    13




These debugs are the result when the **debug dmvpn all all** command is entered on the hub and spoke routers. This particular command enables this set of debugs:

```
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
```

## Debugs with Explanation

As this is a configuraton where IPSec is implemented, the debugs show all of the ISAKMP and IPSec debugs. If no crypto is configured, ignore any debugs that start with "IPsec" or "ISAKMP."

| HUB DEBUG EXPLANATION | DEBUGS IN SEQUENCE | SPOKE DEBU EXPLANATIO |
|---|---|---|
| These first few debug messages are generated by a **no shutdown** command entered on the tunnel interface. Messages are generated by crypto, GRE, and NHRP services being initiated.<br>An NHRP registration error is seen on hub because it does not have a Next Hop Server (NHS) configured (the hub is the NHS for our DMVPN cloud). This is expected. | IPSEC-IFC MGRE/Tu0: Checking tunnel status.<br>**NHRP: if_up: Tunnel0 proto 0**<br>IPSEC-IFC MGRE/Tu0: tunnel coming up<br>IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start already listening<br>**%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON**<br>**NHRP: Unable to send Registration - no NHSes configured**<br>%LINK-3-UPDOWN: Interface Tunnel0, changed state to up<br>NHRP: if_up: Tunnel0 proto 0<br>NHRP: Unable to send Registration - no NHSes configured<br>IPSEC-IFC MGRE/Tu0: tunnel coming up<br>IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start already listening<br>**%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up**<br>IPSEC-IFC GRE/Tu0: Checking tunnel status.<br>IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 0<br>**IPSEC-IFC GRE/Tu0: crypto_ss_listen_start already listening**<br>**IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Opening a socket with profile DMVPN-IPSEC**<br>IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 0<br>IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Triggering tunnel immediately.<br>IPSEC-IFC GRE/Tu0: Adding Tunnel0 tunnel interface to shared list<br>**NHRP: if_up: Tunnel0 proto 0**<br>**NHRP: Tunnel0: Cache add for target 10.1.1.254/32 next-hop 10.1.1.254**<br>**172.16.10.1**<br>IPSEC-IFC GRE/Tu0: tunnel coming up<br>IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220 | These first few debu<br>messages are gene<br>a **no shutdown** com<br>entered on the tunne<br>interface. Messages<br>generated by crypto<br>and NHRP services<br>initiated.<br>Additionally, the spo<br>adds an entry to its<br>NHRP cache for its<br>NBMA and tunnel ad |

IPSEC-IFC GRE/Tu0: crypto_ss_listen_start already listening
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start already listening
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Opening a socket with profile DMVPN-IPSEC
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Socket is already being opened. Ignoring.
CRYPTO_SS(TUNNEL SEC): Application started listening
insert of map into mapdb AVL failed, map + ace pair already exists on the mapdb
**%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON**
CRYPTO_SS(TUNNEL SEC): Active open, socket info: local 172.16.1.1 172.16.1.1/255.255.255.255/0, remote 172.16.10.1 172.16.10.1/255.255.255.255/0, prot 47, ifc Tu0

**START OF ISAKMP (PHASE I) NEGOTIATION**

IPSEC(recalculate_mtu): reset sadb_root 94EFDC0 mtu to 1500
**IPSEC(sa_request): ,**
**(key eng. msg.) OUTBOUND local= 172.16.1.1:500, remote= 172.16.10.1:500,**
**local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),**
**remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),**
**protocol= ESP, transform= esp-3des esp-sha-hmac (Transport),**
**lifedur= 3600s and 4608000kb,**
**spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0**
ISAKMP:(0): SA request profile is (NULL)
ISAKMP: Created a peer struct for 172.16.10.1, peer port 500
ISAKMP: New peer created peer = 0x95F6858 peer_handle = 0x80000004
ISAKMP: Locking peer struct 0x95F6858, refcount 1 for isakmp_initiator
ISAKMP: local port 500, remote port 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP:(0):insert sa successfully sa = 8A26FB0
**ISAKMP:(0):Can not start Aggressive mode, trying Main mode.**
ISAKMP:(0):found peer pre-shared key matching 172.16.10.1
ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(0): constructed NAT-T vendor-07 ID
ISAKMP:(0): constructed NAT-T vendor-03 ID
ISAKMP:(0): constructed NAT-T vendor-02 ID
**ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM**

The first step once t
tunnel is “no shutdo
to start the crypto
negotiation. Here th
creates an SA reque
attempts to start Agg
Mode and fails back
Main Mode. Since
Aggressive Mode is
configured on either
this is expected.
The spoke begins M
Mode and sends the
ISAKMP message,
MM_NO_STATE. IS
state changes from
IKE_READY to
IKE_I_MM1.
The NAT-T vendor I
messages are used
detection and traver
NAT. These messag
expected during the
negotiation of ISAKM
regardless of whethe
not NAT is impleme
Like the Aggressive
messages, these ar
expected.

**ISAKMP:(0):Old State = IKE_READY  New State = IKE_I_MM1**

**ISAKMP:(0): beginning Main Mode exchange**
**ISAKMP:(0): sending packet to 172.16.10.1 my_port 500 peer_port 500 (I) MM_NO_STATE**
ISAKMP:(0):Sending an IKE IPv4 Packet.
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): good socket ready message

After the spoke's tunnel is "no shutdown," the hub receives the IKE NEW SA (Main Mode 1) message on port 500. As the Responder, the hub creates an ISAKMP Security Association (SA).
The ISAKMP state changes from IKE_READY to IKE_R_MM1.

**ISAKMP (0): received packet from 172.16.1.1 dport 500 sport 500 Global (N) NEW SA**
**ISAKMP: Created a peer struct for 172.16.1.1, peer port 500**
ISAKMP: New peer created peer = 0x8CACD00 peer_handle = 0x80000003
ISAKMP: Locking peer struct 0x8CACD00, refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500
**ISAKMP:(0):insert sa successfully sa = 6A5BDE8**
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
**ISAKMP:(0):Old State = IKE_READY  New State = IKE_R_MM1**

The received IKE Main Mode 1 message is processed. The hub determines that the peer has matching ISAKMP attributes and they are filled into the ISAKMP SA which was just created. The messages show that the peer uses 3DES-CBC for encryption, hashing of SHA, Diffie Hellman (DH) group 1, preshared key for authentication, and the default SA lifetime of 86400 seconds (0x0 0x1 0x51 0x80 = 0x15180 = 86400 seconds).
The ISAKMP state is still IKE_R_MM1 since a reply has not be sent to the spoke.
The NAT-T vendor ID messages are used in detection and traversal of NAT. These messages are expected during the negotiation of ISAKMP

ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
**ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch**
**ISAKMP (0): vendor ID is NAT-T RFC 3947**
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
ISAKMP (0): vendor ID is NAT-T v7
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
ISAKMP:(0): vendor ID is NAT-T v3
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
ISAKMP:(0): vendor ID is NAT-T v2
**ISAKMP:(0):found peer pre-shared key matching 172.16.1.1**
**ISAKMP:(0): local preshared key found**
ISAKMP : Scanning profiles for xauth ...
**ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy**
**ISAKMP: encryption 3DES-CBC**
**ISAKMP: hash SHA**
**ISAKMP: default group 1**
**ISAKMP: auth pre-share**
**ISAKMP: life type in seconds**

| | |
|---|---|
| regardless of whether or not NAT is implemented. Similar messages are seen for Dead Peer Detection (DPD). | **ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80**<br>**ISAKMP:(0):atts are acceptable. Next payload is 0**<br>**ISAKMP:(0):Acceptable atts:actual life: 0**<br>**ISAKMP:(0):Acceptable atts:life: 0**<br>**ISAKMP:(0):Fill atts in sa vpi_length:4**<br>**ISAKMP:(0):Fill atts in sa life_in_seconds:86400**<br>**ISAKMP:(0):Returning Actual lifetime: 86400**<br>**ISAKMP:(0)::Started lifetime timer: 86400.** |
| | ISAKMP:(0): processing vendor id payload<br>ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch<br>ISAKMP (0): vendor ID is NAT-T RFC 3947<br>ISAKMP:(0): processing vendor id payload<br>ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch<br>ISAKMP (0): vendor ID is NAT-T v7<br>ISAKMP:(0): processing vendor id payload<br>ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch<br>ISAKMP:(0): vendor ID is NAT-T v3<br>ISAKMP:(0): processing vendor id payload<br>ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch<br>ISAKMP:(0): vendor ID is NAT-T v2<br>ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE<br>ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM1 |
| MM_SA_SETUP (Main Mode 2) is sent to the spoke, which confirms that MM1 was received and accepted as a valid ISAKMP packet. ISAKMP state changes from IKE_R_MM1 to IKE_R_MM2. | ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID<br>**ISAKMP:(0): sending packet to 172.16.1.1 my_port 500 peer_port 500 (R) MM_SA_SETUP**<br>ISAKMP:(0):Sending an IKE IPv4 Packet.<br>ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE<br>**ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM2** |
| | **ISAKMP (0): received packet from 172.16.10.1 dport 500 sport 500 Global (I) MM_NO_STATE**<br>**ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH**<br>**ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2**<br><br>ISAKMP:(0): processing SA payload. message ID = 0<br>ISAKMP:(0): processing vendor id payload<br>**ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch**<br>ISAKMP (0): vendor ID is NAT-T RFC 3947<br>ISAKMP:(0):found peer pre-shared key matching 172.16.10.1<br>ISAKMP:(0): local preshared key found |
| | In response to the M message sent to the MM2 arrives which c that MM1 was receiv The received IKE M Mode 2 message is processed. The spo realizes that the pee has matching ISAKM attributes and these attributes are filled i ISAKMP SA that wa created. This packet that the peer uses 3 CBC for encryption, |

| | | |
|---|---|---|
| | ISAKMP : Scanning profiles for xauth ...<br>**ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy**<br>**ISAKMP: encryption 3DES-CBC**<br>**ISAKMP: hash SHA**<br>**ISAKMP: default group 1**<br>**ISAKMP: auth pre-share**<br>**ISAKMP: life type in seconds**<br>**ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80**<br>**ISAKMP:(0):atts are acceptable. Next payload is 0**<br>**ISAKMP:(0):Acceptable atts:actual life: 0**<br>**ISAKMP:(0):Acceptable atts:life: 0**<br>**ISAKMP:(0):Fill atts in sa vpi_length:4**<br>**ISAKMP:(0):Fill atts in sa life_in_seconds:86400**<br>**ISAKMP:(0):Returning Actual lifetime: 86400**<br>**ISAKMP:(0)::Started lifetime timer: 86400.** | hashing of SHA, Dif<br>Hellman (DH) group<br>preshared key for<br>authentication, and t<br>default SA lifetime o<br>seconds (0x0 0x1 0x<br>0x80 = 0x15180 = 8<br>seconds).<br>In addition to the NA<br>messages, there is a<br>exchange to determ<br>the session will use<br>The ISAKMP state c<br>from IKE_I_MM1 to<br>IKE_I_MM2. |
| | ISAKMP:(0): processing vendor id payload<br>ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch<br>ISAKMP (0): vendor ID is NAT-T RFC 3947<br>ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE<br>ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2 | |
| | **ISAKMP:(0): sending packet to 172.16.10.1 my_port 500 peer_port 500 (I) MM_SA_SETUP**<br>ISAKMP:(0):Sending an IKE IPv4 Packet.<br>ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE<br>**ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3** | MM_SA_SETUP (M<br>Mode 3) is sent to th<br>which confirms that<br>spoke received MM2<br>would like to procee<br>The ISAKMP state c<br>from IKE_I_MM2 to<br>IKE_I_MM3. |
| MM_SA_SETUP (Main Mode 3) is received by hub. The hub concludes that the peer is another Cisco IOS device and no NAT is detected for us or our peer. The ISAKMP state changes from IKE_R_MM2 to IKE_R_MM3. | **ISAKMP (0): received packet from 172.16.1.1 dport 500 sport 500 Global (R) MM_SA_SETUP**<br>ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH<br>**ISAKMP:(0):Old State = IKE_R_MM2 New State = IKE_R_MM3** | |
| | ISAKMP:(0): processing KE payload. message ID = 0<br>ISAKMP:(0): processing NONCE payload. message ID = 0<br>**ISAKMP:(0):found peer pre-shared key matching 172.16.1.1**<br>ISAKMP:(1002): processing vendor id payload<br>ISAKMP:(1002): vendor ID is DPD<br>ISAKMP:(1002): processing vendor id payload<br>**ISAKMP:(1002): speaking to another IOS box!**<br>ISAKMP:(1002): processing vendor id payload<br>ISAKMP:(1002): vendor ID seems Unity/DPD but major 225 mismatch<br>ISAKMP:(1002): vendor ID is XAUTH | |

ISAKMP:received payload type 20
**ISAKMP (1002): His hash no match - this node outside NAT**
ISAKMP:received payload type 20
**ISAKMP (1002): No NAT Found for self or peer**
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_R_MM3 New State = IKE_R_MM3

MM_KEY_EXCH (Main Mode 4) is sent by the hub. ISAKMP state changes from IKE_R_MM3 to IKE_R_MM4.

**ISAKMP:(1002): sending packet to 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH**
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
**ISAKMP:(1002):Old State = IKE_R_MM3 New State = IKE_R_MM4**
**ISAKMP (0): received packet from 172.16.10.1 dport 500 sport 500 Global (I) MM_SA_SETUP**
ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
**ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4**

MM_SA_SETUP (M
Mode 4) is received
spoke. The spoke
concludes that the p
another Cisco IOS d
and no NAT is detec
us or our peer.

ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
**ISAKMP:(0):found peer pre-shared key matching 172.16.10.1**
ISAKMP:(1002): processing vendor id payload
ISAKMP:(1002): vendor ID is Unity
ISAKMP:(1002): processing vendor id payload
ISAKMP:(1002): vendor ID is DPD
ISAKMP:(1002): processing vendor id payload
**ISAKMP:(1002): speaking to another IOS box!**
ISAKMP:received payload type 20
**ISAKMP (1002): His hash no match - this node outside NAT**
ISAKMP:received payload type 20
**ISAKMP (1002): No NAT Found for self or peer**
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_I_MM4 New State = IKE_I_MM4

The ISAKMP state c
from IKE_I_MM3 to
IKE_I_MM4.

ISAKMP:(1002):Send initial contact
**ISAKMP:(1002):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR**
ISAKMP (1002): ID payload
next-payload : 8
type : 1
address : 172.16.1.1
protocol : 17
port : 500
length : 12

MM_KEY_EXCH (M
Mode 5) is sent by t
spoke.

The ISAKMP state c
from IKE_I_MM4 to
IKE_I_MM5.

MM_KEY_EXCH (Main Mode 5) is received by the hub.
The ISAKMP state changes from IKE_R_MM4 to IKE_R_MM5.
Additionally, the “peer matches *none* of the profiles” is seen due to the lack of an ISAKMP profile. Because this is the case, ISAKMP does not use a profile.

```
ISAKMP:(1002):Total payload length: 12
ISAKMP:(1002): sending packet to 172.16.10.1
my_port 500 peer_port 500 (I) MM_KEY_EXCH
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
ISAKMP:(1002):Old State = IKE_I_MM4  New State =
IKE_I_MM5
ISAKMP (1002): received packet from 172.16.1.1
dport 500 sport 500 Global (R) MM_KEY_EXCH
ISAKMP:(1002):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
ISAKMP:(1002):Old State = IKE_R_MM4  New State
= IKE_R_MM5

ISAKMP:(1002): processing ID payload. message ID =
0
ISAKMP (1002): ID payload
        next-payload : 8
        type         : 1
        address      : 172.16.1.1
        protocol     : 17
        port         : 500
        length       : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1002): processing HASH payload. message
ID = 0
ISAKMP:(1002): processing NOTIFY
INITIAL_CONTACT protocol 1
        spi 0, message ID = 0, sa = 0x6A5BDE8
ISAKMP:(1002):SA authentication status:
        authenticated
ISAKMP:(1002):SA has been authenticated with
172.16.1.1
ISAKMP:(1002):SA authentication status:
        authenticated
ISAKMP:(1002): Process initial contact,
bring down existing phase 1 and 2 SA's with local
172.16.10.1 remote 172.16.1.1 remote port 500
ISAKMP: Trying to insert a peer
172.16.10.1/172.16.1.1/500/,  and inserted
successfully 8CACD00.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_R_MM5  New State =
IKE_R_MM5

IPSEC(key_engine): got a queue event with 1 KMI
message(s)
ISAKMP:(1002):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
ISAKMP (1002): ID payload
        next-payload : 8
```

type : 1
address : 172.16.10.1
protocol : 17
port : 500
length : 12
ISAKMP:(1002):Total payload length: 12

The final MM_KEY_EXCH packet (Main Mode 6) is sent by the hub. This completes the Phase 1 negotiation which signifies this device is ready for Phase 2 (IPSec Quick Mode).

**ISAKMP:(1002): sending packet to 172.16.1.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH**
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
**ISAKMP:(1002):Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE**

The ISAKMP state changes from IKE_R_MM5 to IKE_P1_COMPLETE.

ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1002):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

**ISAKMP (1002): received packet from 172.16.10.1 dport 500 sport 500 Global (I) MM_KEY_EXCH**
ISAKMP:(1002): processing ID payload. message ID = 0
ISAKMP (1002): ID payload
next-payload : 8
type : 1
address : 172.16.10.1
protocol : 17
port : 500
length : 12
**ISAKMP:(0):: peer matches *none* of the profiles**
ISAKMP:(1002): processing HASH payload. message ID = 0
ISAKMP:(1002):SA authentication status:
authenticated
ISAKMP:(1002):SA has been authenticated with 172.16.10.1
**ISAKMP: Trying to insert a peer 172.16.1.1/172.16.10.1/500/, and inserted successfully 95F6858.**
ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
**ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_I_MM6**

ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_I_MM6 New State = IKE_I_MM6

ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
**ISAKMP:(1002):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE**

The final MM_KEY_
packet (Main Mode
received by the spo
completes the Phas
negotiation which si
this device is ready
Phase 2 (IPSec Qui
Mode).
The ISAKMP state c
from IKE_I_MM5 to
IKE_I_MM6, and the
immediately to
IKE_P1_COMPLET
Additionally, the “pe
matches *none* of t
profiles” is seen due
lack of an ISAKMP p
Because this is the
ISAKMP does not us
profile.

**END OF ISAKMP (PHASE I) NEGOTATION, START OF IPSEC (PHASE II) NEGOTATION**

| | |
|---|---|
| | **ISAKMP:(1002):beginning Quick Mode exchange, M-ID of 3464373979**<br>ISAKMP:(1002):QM Initiator gets spi<br>**ISAKMP:(1002): sending packet to 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE**<br>ISAKMP:(1002):Sending an IKE IPv4 Packet.<br>ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_INTERNAL, IKE_INIT_QM<br>**ISAKMP:(1002):Old State = IKE_QM_READY New State = IKE_QM_I_QM1**<br>ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE<br>ISAKMP:(1002):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE |
| The hub receives the first Quick Mode (QM) packet which has the IPSec proposal. The attributes received specify that: encaps flag set to 2 (transport mode, flag of 1 would be tunnel mode), default SA lifetime of 3600 seconds and 4608000 kilobytes (0x465000 in hex), HMAC-SHA for authentication, and 3DES for encryption. As these are the same attributes set in the local configuration, the proposal is accepted and the shell of an IPSec SA is created. Since no Security Parameter Index (SPI) values are associated with these yet, this is just a shell of an SA that cannot be used to pass traffic yet. | **ISAKMP (1002): received packet from 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE**<br>**ISAKMP: set new node -830593317 to QM_IDLE**<br>ISAKMP:(1002): processing HASH payload. message ID = 3464373979<br>ISAKMP:(1002): processing SA payload. message ID = 3464373979<br>**ISAKMP:(1002):Checking IPSec proposal 1**<br>**ISAKMP: transform 1, ESP_3DES**<br>**ISAKMP: attributes in transform:**<br>**ISAKMP: encaps is 2 (Transport)**<br>**ISAKMP: SA life type in seconds**<br>**ISAKMP: SA life duration (basic) of 3600**<br>**ISAKMP: SA life type in kilobytes**<br>**ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0**<br>**ISAKMP: authenticator is HMAC-SHA**<br>**ISAKMP:(1002):atts are acceptable.**<br>IPSEC(validate_proposal_request): proposal part #1<br>IPSEC(validate_proposal_request): proposal part #1,<br>**(key eng. msg.) INBOUND local= 172.16.10.1:0, remote= 172.16.1.1:0,**<br>**local_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),**<br>**remote_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),**<br>**protocol= ESP, transform= NONE (Transport),**<br>**lifedur= 0s and 0kb,**<br>**spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0** |
| These are just general IPSec service messages that say it works properly. | IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): connection lookup returned 0<br>IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start already listening<br>**IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Opening a socket with profile DMVPN-IPSEC**<br>IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): connection lookup returned 0<br>IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): |

The Quick Mode (Ph
IPSec) exchange sta
the spoke send the f
message to the hub

Triggering tunnel immediately.
IPSEC-IFC MGRE/Tu0: Adding Tunnel0 tunnel interface to shared list
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnel_protection_start_pending_timer 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Good listen request

Pseudo-crypto map entry is created for IP protocol 47 (GRE) from 172.16.10.1 (hub public address) to 172.16.1.1 (spoke public address). An IPSec SA/SPI is created for both the inbound and outbound traffic with values from the accepted proposal.

insert of map into mapdb AVL failed, map + ace pair already exists on the mapdb
CRYPTO_SS(TUNNEL SEC): Passive open, socket info: local 172.16.10.1 172.16.10.1/255.255.255.255/0, remote 172.16.1.1 172.16.1.1/255.255.255.255/0, prot 47, ifc Tu0
Crypto mapdb : proxy_match
**src addr : 172.16.10.1**
**dst addr : 172.16.1.1**
**protocol : 47**
src port : 0
dst port : 0
ISAKMP:(1002): processing NONCE payload. message ID = 3464373979
ISAKMP:(1002): processing ID payload. message ID = 3464373979
ISAKMP:(1002): processing ID payload. message ID = 3464373979
ISAKMP:(1002):QM Responder gets spi
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
**ISAKMP:(1002):Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE**
**ISAKMP:(1002): Creating IPSec SAs**
**inbound SA from 172.16.1.1 to 172.16.10.1 (f/i) 0/ 0**
**(proxy 172.16.1.1 to 172.16.10.1)**
**has spi 0xDD2AC2B3 and conn_id 0**
**lifetime of 3600 seconds**
**lifetime of 4608000 kilobytes**
**outbound SA from 172.16.10.1 to 172.16.1.1 (f/i) 0/0**
**(proxy 172.16.10.1 to 172.16.1.1)**
**has spi 0x82C3E0C4 and conn_id 0**
**lifetime of 3600 seconds**
**lifetime of 4608000 kilobytes**

The second QM message sent by the hub. Message generated by IPSec service which confirms that tunnel protection is up on Tunnel0. Another SA creation message is seen which has the destination IPs, SPIs, transform set attributes, and lifetime in kilobytes and

**ISAKMP:(1002): sending packet to 172.16.1.1 my_port 500 peer_port 500 (R) QM_IDLE**
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_INTERNAL, IKE_GOT_SPI
**ISAKMP:(1002):Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2**
CRYPTO_SS(TUNNEL SEC): Completed binding of application to socket
IPSEC(key_engine): got a queue event with 1 KMI

seconds remaining.

message(s)
Crypto mapdb : proxy_match
src addr : 172.16.10.1
dst addr : 172.16.1.1
protocol : 47
src port : 0
dst port : 0
IPSEC(crypto_ipsec_sa_find_ident_head):
reconnecting with the same proxies and peer
172.16.1.1
IPSEC(policy_db_add_ident): src 172.16.10.1, dest
172.16.1.1, dest_port 0

**IPSEC(create_sa): sa created,**
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 3
sa_lifetime(k/sec)= (4536779/3600)
**IPSEC(create_sa): sa created,**
(sa) sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4
sa_lifetime(k/sec)= (4536779/3600)
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce):
updating Tunnel0 ident 8B6A0E8 with tun_decap_oce
6A648F0
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
connection lookup returned 8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): good
socket ready message
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
connection lookup returned 8C93888
**IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):**
**tunnel_protection_socket_up**
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
Signalling NHRP
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Got
MTU message mtu 1458
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):
connection lookup returned 8C93888
**ISAKMP (1002): received packet from 172.16.10.1**
**dport 500 sport 500 Global (I) QM_IDLE**
ISAKMP:(1002): processing HASH payload. message
ID = 3464373979
ISAKMP:(1002): processing SA payload. message ID =
3464373979
**ISAKMP:(1002):Checking IPSec proposal 1**
**ISAKMP: transform 1, ESP_3DES**
**ISAKMP: attributes in transform:**
**ISAKMP: encaps is 2 (Transport)**
**ISAKMP: SA life type in seconds**
**ISAKMP: SA life duration (basic) of 3600**
**ISAKMP: SA life type in kilobytes**

The spoke receives
second QM packet v
has the IPSec propo
This confirms that Q
received by the hub.
attributes received s
that: encaps flag set
(transport mode, flag
would be tunnel mo
default SA lifetime o
seconds and 46080
kilobytes (0x465000
hex), HMAC-SHA fo

**ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0**
**ISAKMP: authenticator is HMAC-SHA**
**ISAKMP:(1002):atts are acceptable.**
IPSEC(validate_proposal_request): proposal part #1
IPSEC(validate_proposal_request): proposal part #1,
**(key eng. msg.) INBOUND local= 172.16.1.1:0, remote= 172.16.10.1:0,**
**local_proxy= 172.16.1.1/255.255.255.255/47/0 (type=1),**
**remote_proxy= 172.16.10.1/255.255.255.255/47/0 (type=1),**
**protocol= ESP, transform= NONE (Transport),**
**lifedur= 0s and 0kb,**
**spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0**
**Crypto mapdb : proxy_match**
**src addr : 172.16.1.1**
**dst addr : 172.16.10.1**
**protocol : 47**
**src port : 0**
**dst port : 0**
ISAKMP:(1002): processing NONCE payload. message ID = 3464373979
ISAKMP:(1002): processing ID payload. message ID = 3464373979
ISAKMP:(1002): processing ID payload. message ID = 3464373979
**ISAKMP:(1002): Creating IPSec SAs**
**inbound SA from 172.16.10.1 to 172.16.1.1 (f/i) 0/ 0**
**(proxy 172.16.10.1 to 172.16.1.1)**
**has spi 0x82C3E0C4 and conn_id 0**
**lifetime of 3600 seconds**
**lifetime of 4608000 kilobytes**
**outbound SA from 172.16.1.1 to 172.16.10.1 (f/i) 0/0**
**(proxy 172.16.1.1 to 172.16.10.1)**
**has spi 0xDD2AC2B3 and conn_id 0**
**lifetime of 3600 seconds**
**lifetime of 4608000 kilobytes**
**ISAKMP:(1002): sending packet to 172.16.10.1 my_port 500 peer_port 500 (I) QM_IDLE**
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):deleting node -830593317 error FALSE reason "No Error"
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
**ISAKMP:(1002):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE**
IPSEC(key_engine): got a queue event with 1 KMI message(s)
Crypto mapdb : proxy_match
src addr : 172.16.1.1

authentication, and
encryption. As these
the same attributes
the local configuratio
proposal is accepted
the shell of an IPSec
created. Since no S
Parameter Index (SI
values are associate
these yet, this is just
of an SA that cannot
used to pass traffic
The pseudo-crypto
entry is created for I
protocol 47 (GRE) fr
172.16.10.1 (hub pu
address) to 172.16.1
(spoke public addres

An IPSec SA/SPI is
for both the inbound
outbound traffic with
from the accepted p

The spoke sends the
and final QM messa
the hub, which comp
the QM exchange. U
ISAKMP where each
goes through every
(MM1 through
MM6/P1_COMPLET
IPSec is a little diffe
there are only three
messages rather tha
The Initiator (our spo
this case, as signifie

dst addr : 172.16.10.1
protocol : 47
src port : 0
dst port : 0
IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer 172.16.10.1
IPSEC(policy_db_add_ident): src 172.16.1.1, dest 172.16.10.1, dest_port 0

**IPSEC(create_sa): sa created,**
(sa) sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 3
sa_lifetime(k/sec)= (4499172/3600)
**IPSEC(create_sa): sa created,**
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4
sa_lifetime(k/sec)= (4499172/3600)
**IPSEC(update_current_outbound_sa): get enable SA peer 172.16.10.1 current outbound sa to SPI DD2AC2B3**
**IPSEC(update_current_outbound_sa): updated peer 172.16.10.1 current outbound sa to SPI DD2AC2B3**
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce): updating Tunnel0 ident 94F2740 with tun_decap_oce 794ED30
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): tunnel_protection_socket_up
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Signalling NHRP
NHRP: NHS 10.1.1.254 Tunnel0 vrf 0 Cluster 0 Priority 0 Transitioned to 'E' from ' '

IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220
NHRP: Attempting to send packet via DEST 10.1.1.254

These final QM messages confirm that Quick Mode is complete and IPSec is up on both sides of the tunnel. Unlike ISAKMP where each peer goes through every state (MM1 through MM6/P1_COMPLETE), IPSec is a little different as there are only three messages rather than six. The Responder (our hub in

**ISAKMP (1002): received packet from 172.16.1.1 dport 500 sport 500 Global (R) QM_IDLE**
ISAKMP:(1002):deleting node -830593317 error FALSE reason "QM done (await)"
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
**ISAKMP:(1002):Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE**
IPSEC(key_engine): got a queue event with 1 KMI message(s)
IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP

the “I” in the
IKE_QM_**I**_QM1 me
goes from QM_REA
then to QM_I_QM1
to
QM_PHASE2_COM
The Responder (hub
QM_READY,
QM_SPI_STARVE,
QM_R_QM2,
QM_PHASE2_COM
Another SA creation
message is seen wh
the destination IPs,
transform set attribu
and lifetime in kiloby
seconds remaining.

| | | |
|---|---|---|
| this case, as signified by the “R” in the IKE_QM_**R**_QM1 message) goes QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE. The Initiator (spoke) goes from QM_READY, then to QM_I_QM1 directly to QM_PHASE2_COMPLETE. | **IPSEC(key_engine_enable_outbound): enable SA with spi 2193875140/50**<br>**IPSEC(update_current_outbound_sa): get enable SA peer 172.16.1.1 current outbound sa to SPI 82C3E0C4**<br>**IPSEC(update_current_outbound_sa): updated peer 172.16.1.1 current outbound sa to SPI 82C3E0C4** | |
| | **NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 108**<br>**src: 10.1.1.1, dst: 10.1.1.254**<br>(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1<br>shtl: 4(NSAP), sstl: 0(NSAP)<br>pktsz: 108 extoff: 52<br>(M) flags: "unique nat ", reqid: 65540<br>**src NBMA: 172.16.1.1**<br>**src protocol: 10.1.1.1, dst protocol: 10.1.1.254**<br>(C-1) code: no error(0)<br>prefix: 32, mtu: 17912, hd_time: 7200<br>addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0<br>Responder Address Extension(3):<br>Forward Transit NHS Record Extension(4):<br>Reverse Transit NHS Record Extension(5):<br>**Authentication Extension(7):**<br>**type:Cleartext(1), data:NHRPAUTH**<br>NAT address Extension(9):<br>(C-1) code: no error(0)<br>prefix: 32, mtu: 17912, hd_time: 0<br>addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0<br>**client NBMA: 172.16.10.1**<br>**client protocol: 10.1.1.254** | This is the NHRP registration requests the hub in attempt to register to the NHS hub). It is normal to multiples of these, a spoke continues to a to register with the N until it receives a “registration reply.”<br>**src,dst**: Tunnel sou (spoke) and destina (hub) IP addresses. are the source and destination of the GI packet sent by the r<br>**src NBMA**: the NBM (internet) address of spoke which sent th packet and tries to r with the NHS<br>**src protocol**: tunne address of the spok tries to register<br>**dst protocol**: tunne address of the NHS/<br>**Authentication Ext** data: NHRP authentication string<br>**client NBMA**: NBM/ address of the NHS/<br>**client protocol**: tun address of the NHS/ |
| | **NHRP-RATE: Sending initial Registration Request for 10.1.1.254, reqid 65540**<br>**%LINK-3-UPDOWN: Interface Tunnel0, changed state to up**<br>NHRP: if_up: Tunnel0 proto 0<br>**NHRP: Tunnel0: Cache update for target 10.1.1.254/32 next-hop 10.1.1.254 172.16.10.1**<br>IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): | More NHRP service messages that say t initial Registration R was sent to the NHS 10.1.1.254. There is confirmation that a c entry was added for IP 10.1.1.254/24 tha at NBMA 172.16.10. |

connection lookup returned 961D220
NHRP: Attempting to send packet via DEST 10.1.1.254

IPSEC-IFC GRE/Tu0: tunnel coming up
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start already listening
IPSEC-IFC GRE/Tu0: crypto_ss_listen_start already listening
**IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Opening a socket with profile DMVPN-IPSEC**
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): connection lookup returned 961D220
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1): Socket is already open. Ignoring.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

This is the NHRP registration requests received from the spoke in attempt to register to the NHS ( the hub). It is normal to see multiples of these, as the spoke continues to attempt to register with the NHS until it receives a “registration reply.”
**src NBMA**: the NBMA (internet) address of the spoke which sent this packet and tries to register with the NHS
**src protocol**: tunnel address of the spoke which tries to register
**dst protocol**: tunnel address of the NHS/hub
**Authentication Extension**, data: NHRP authentication string
**client NBMA**: NBMA address of the NHS/hub
**client protocol**: tunnel address of the NHS/hub

**NHRP: Receive Registration Request via Tunnel0 vrf 0, packet size: 108**
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: 108 extoff: 52
(M) flags: "unique nat ", reqid: 65540
**src NBMA: 172.16.1.1**
**src protocol: 10.1.1.1, dst protocol: 10.1.1.254**
(C-1) code: no error(0)
prefix: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Responder Address Extension(3):
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
**Authentication Extension(7):**
**type:Cleartext(1), data:NHRPAUTH**
NAT address Extension(9):
(C-1) code: no error(0)
prefix: 32, mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
**client NBMA: 172.16.10.1**
**client protocol: 10.1.1.254**

NHRP debug packets adding target network 10.1.1.1/32 available via next hop of 10.1.1.1 at NHRP of 172.16.1.1. 172.16.1.1 is also added to the list of addresses which the hub forwards multicast

NHRP: netid_in = 1, to_us = 1
**NHRP: Tunnel0: Cache add for target 10.1.1.1/32 next-hop 10.1.1.1**
**172.16.1.1**
**NHRP: Adding Tunnel Endpoints (VPN: 10.1.1.1, NBMA: 172.16.1.1)**
**NHRP: Successfully attached NHRP subblock for Tunnel Endpoints (VPN: 10.1.1.1, NBMA:**

delayed message sa
Tunnel has been “no
is seen here.
These are general I
service messages th
it works properly. He
where it is finally see
the Tunnel protocol

traffic to.
These messages confirm that the registration was successful, as was a resolution for the spokes Tunnel address.

**172.16.1.1)**
NHRP: Inserted subblock node for cache: Target
Inserted subblock node for cache: Target 10.1.1.1/32nhop 10.1.1.1
NHRP: Converted internal dynamic cache entry for 10.1.1.1/32 interface Tunnel0 to external
**NHRP: Tu0: Creating dynamic multicast mapping NBMA: 172.16.1.1**
**NHRP: Added dynamic multicast mapping for NBMA: 172.16.1.1**
NHRP: Updating our cache with NBMA: 172.16.10.1, NBMA_ALT: 172.16.10.1
NHRP: New mandatory length: 32
NHRP: Attempting to send packet via DEST 10.1.1.1
**NHRP: NHRP successfully resolved 10.1.1.1 to NBMA 172.16.1.1**
**NHRP: Encapsulation succeeded. Tunnel IP addr 172.16.1.1**

This is the NHRP Registration Reply sent by the hub to the spoke in response to the “NHRP Registration Request” received earlier. Like the other registration packets, the hub sends multiples of these in response to the multiple requests.
**src,dst**: Tunnel source (hub) and destination (spoke) IP addresses. These are the source and destination of the GRE packet sent by the router
**src NBMA**: NBMA (internet) address of the spoke
**src protocol**: tunnel address of the spoke which tries to register
**dst protocol**: tunnel address of the NHS/hub
**client NBMA**: NBMA address of the NHS/hub
**client protocol**: tunnel address of the NHS/hub
**Authentication Extension**, data: NHRP authentication string

**NHRP: Send Registration Reply via Tunnel0 vrf 0, packet size: 128**
**src: 10.1.1.254, dst: 10.1.1.1**
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)
pktsz: 128 extoff: 52
(M) flags: "unique nat ", reqid: 65540
**src NBMA: 172.16.1.1**
**src protocol: 10.1.1.1, dst protocol: 10.1.1.254**
(C-1) code: no error(0)
prefix: 32, mtu: 17912, hd_time: 7200
addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0
Responder Address Extension(3):
(C) code: no error(0)
prefix: 32, mtu: 17912, hd_time: 7200
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
**client NBMA: 172.16.10.1**
**client protocol: 10.1.1.254**
Forward Transit NHS Record Extension(4):
Reverse Transit NHS Record Extension(5):
**Authentication Extension(7):**
**type:Cleartext(1), data:NHRPAUTH**
NAT address Extension(9):
(C-1) code: no error(0)
prefix: 32, mtu: 17912, hd_time: 0
addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0
**client NBMA: 172.16.10.1**
**client protocol: 10.1.1.254**
**NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 128**
(F) afn: IPv4(1), type: IP(800), hop: 255, ver: 1
shtl: 4(NSAP), sstl: 0(NSAP)

This is the NHRP Registration Reply s
the hub to the spoke
response to the “NH

| | | |
|---|---|---|
| | pktsz: 128 extoff: 52<br>(M) flags: "unique nat ", reqid: 65541<br>**src NBMA: 172.16.1.1**<br>**src protocol: 10.1.1.1, dst protocol: 10.1.1.254**<br>(C-1) code: no error(0)<br>prefix: 32, mtu: 17912, hd_time: 7200<br>addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 0<br>Responder Address Extension(3):<br>(C) code: no error(0)<br>prefix: 32, mtu: 17912, hd_time: 7200<br>addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0<br>**client NBMA: 172.16.10.1**<br>**client protocol: 10.1.1.254**<br>Forward Transit NHS Record Extension(4):<br>Reverse Transit NHS Record Extension(5):<br>**Authentication Extension(7):**<br>**type:Cleartext(1), data:NHRPAUTH**<br>NAT address Extension(9):<br>(C-1) code: no error(0)<br>prefix: 32, mtu: 17912, hd_time: 0<br>addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 0<br>**client NBMA: 172.16.10.1**<br>**client protocol: 10.1.1.254**<br>NHRP: netid_in = 0, to_us = 1 | Registration Reques<br>received earlier. Like<br>other registration pa<br>the hub sends multip<br>these in response to<br>multiple requests.<br>**src NBMA**: NBMA<br>(internet) address of<br>spoke<br>**src protocol**: tunne<br>address of the spok<br>tries to register<br>**dst protocol**: tunne<br>address of the NHS<br>**client NBMA**: NBM<br>address of the NHS<br>**client protocol**: tun<br>address of the NHS<br>**Authentication Ext**<br>data: NHRP<br>authentication string |
| More general IPSec service messages that say it works properly. | IPSEC-IFC MGRE/Tu0: crypto_ss_listen_start already listening<br>IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Opening a socket with profile DMVPN-IPSEC<br>IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): connection lookup returned 8C93888<br>IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): Socket is already open. Ignoring.<br>IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1): tunnel_protection_stop_pending_timer 8C93888 | |
| | NHRP: NHS-UP: 10.1.1.254 | NHRP service mess<br>that say the NHS loc<br>10.1.1.254 is up. |
| System message that states the EIGRP adjacency is up with the neighbor spoke at 10.1.1.1. | %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.1 (Tunnel0) is up: new adjacency | |
| | %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.1.1.254 (Tunnel0) is up: new adjacency | System message th<br>states the EIGRP<br>adjacency is up with<br>neighbor hub at 10.1 |
| System message that confirms a successful NHRP resolution. | NHRP: NHRP successfully resolved 10.1.1.1 to NBMA 172.16.1.1 | |

# Confirm Functionality and Troubleshoot

This section has some of the most useful **show** commands used to troubleshoot both the hub and spoke. In order to enable more specific debugs, use these debug conditionals:

- 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:
```

# Related Information

- **IPsec Troubleshooting: Understanding and Using debug Commands**
- **Next Generation Encryption**
- **RFC3706: IKE Dead Peer Detection**
- **RFC3947: IKE NAT Traversal**
- **Technical Support & Documentation - Cisco Systems**