DMVPN第1阶段调试故障排除指南

目录

简介

本文档介绍在动态多点虚拟专用网络(DMVPN)第1阶段部署中在中心辐射点上会遇到的调试消息。

先决条件

对于本文档中的配置和debug命令，您需要运行Cisco IOS® 12.4(9)T版或更高版本的两台Cisco路由器。一般来说，基本DMVPN第1阶段需要Cisco IOS版本12.2(13)T或更高版本或12.2(33)XNC用于聚合服务路由器(ASR)，尽管本文档中显示的功能和调试可能不受支持。

要求

Cisco 建议您了解以下主题：

- 通用路由封装 (GRE)
- 下一跳解析协议 (NHRP)

- Internet 安全关联和密钥管理协议 (ISAKMP)
- Internet 密钥交换 (IKE)
- 互联网协议安全(IPSec)
- 至少以下路由协议之一：增强型内部网关路由协议(EIGRP)、开放最短路径优先(OSPF)、路由信息协议(RIP)和边界网关协议(BGP)

使用的组件

本文档中的信息基于运行Cisco IOS版本15.1(4)M4的Cisco 2911集成多业务路由器(ISR)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

显着增强

这些Cisco IOS版本为DMVPN第1阶段引入了重要功能或修复：

- 版本12.2(18)SXF5 — 使用公钥基础设施(PKI)时更好地支持ISAKMP
- 版本12.2(33)XNE - ASR、IPSec配置文件、隧道保护、IPSec网络地址转换(NAT)穿越
- 版本12.3(7)T — 内部虚拟路由和转发(iVRF)支持
- 版本12.3(11)T — 前门虚拟路由和转发(fVRF)支持
- 版本12.4(9)T — 支持各种与DMVPN相关的调试和命令
- 版本12.4(15)T — 共享隧道保护
- 版本12.4(20)T - IPv6 over DMVPN
- 版本15.0(1)M - NHRP隧道运行状况监控

规则

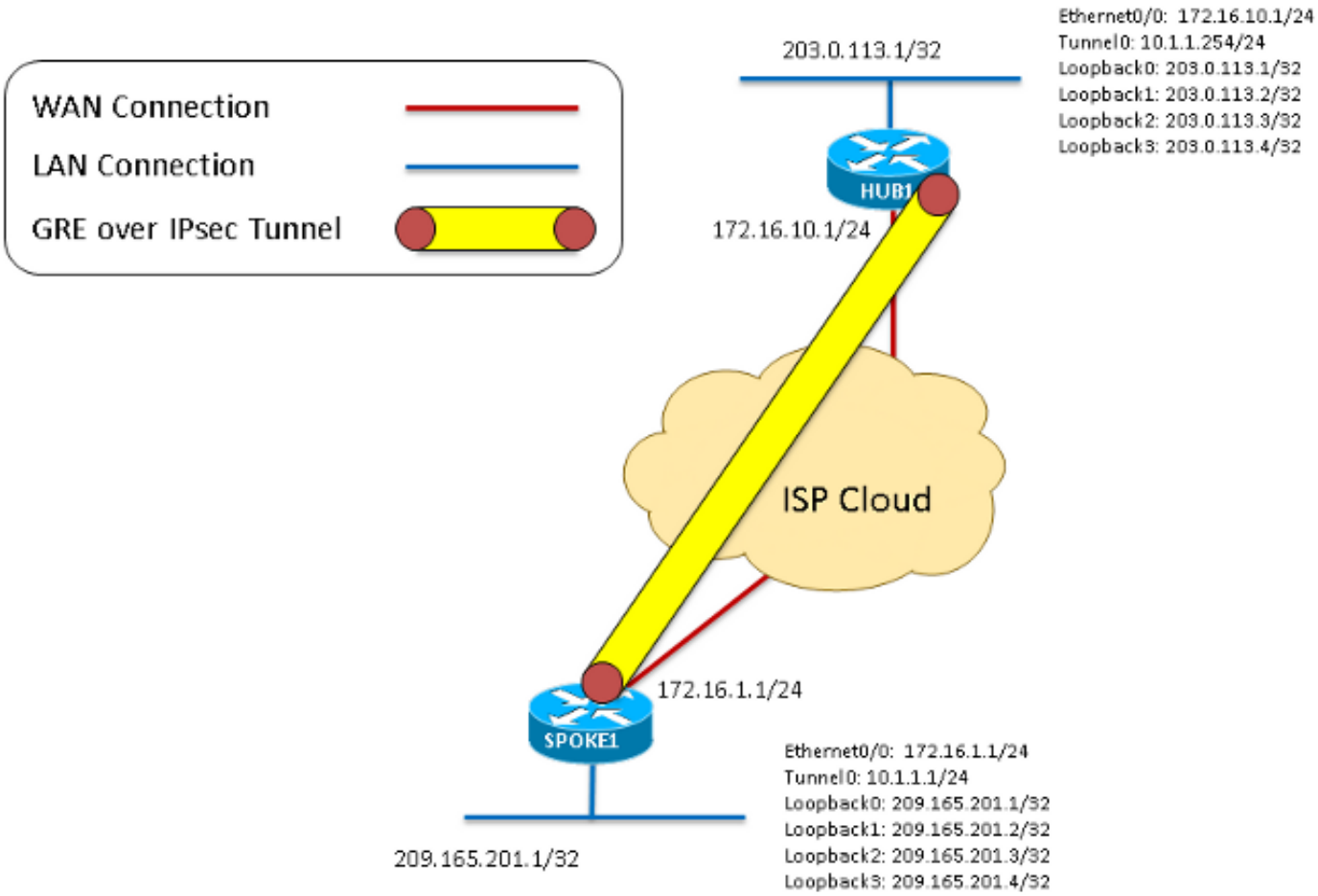
有关文档规则的信息，请参阅 Cisco 技术提示规则。

相关配置

拓扑概述

对于此拓扑，为DMVPN第1阶段配置了两个运行版本15.1(4)M4的2911 ISR:一个作为中心，一个作为分支。以太网接口0/0用作每台路由器的“internet”接口。四个环回接口配置为模拟位于中心或分支站点的局域网。由于这是仅包含一个分支的DMVPN第1阶段拓扑，因此该分支配置了点对点GRE隧道，而不是多点GRE隧道。每台路由器上使用相同的加密配置（ISAKMP和IPSec）来确保它们完全匹配。

图 1



加密

中心和辐条上的情况相同。

```
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
```

集线器

```
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
```

辐射

```
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
```

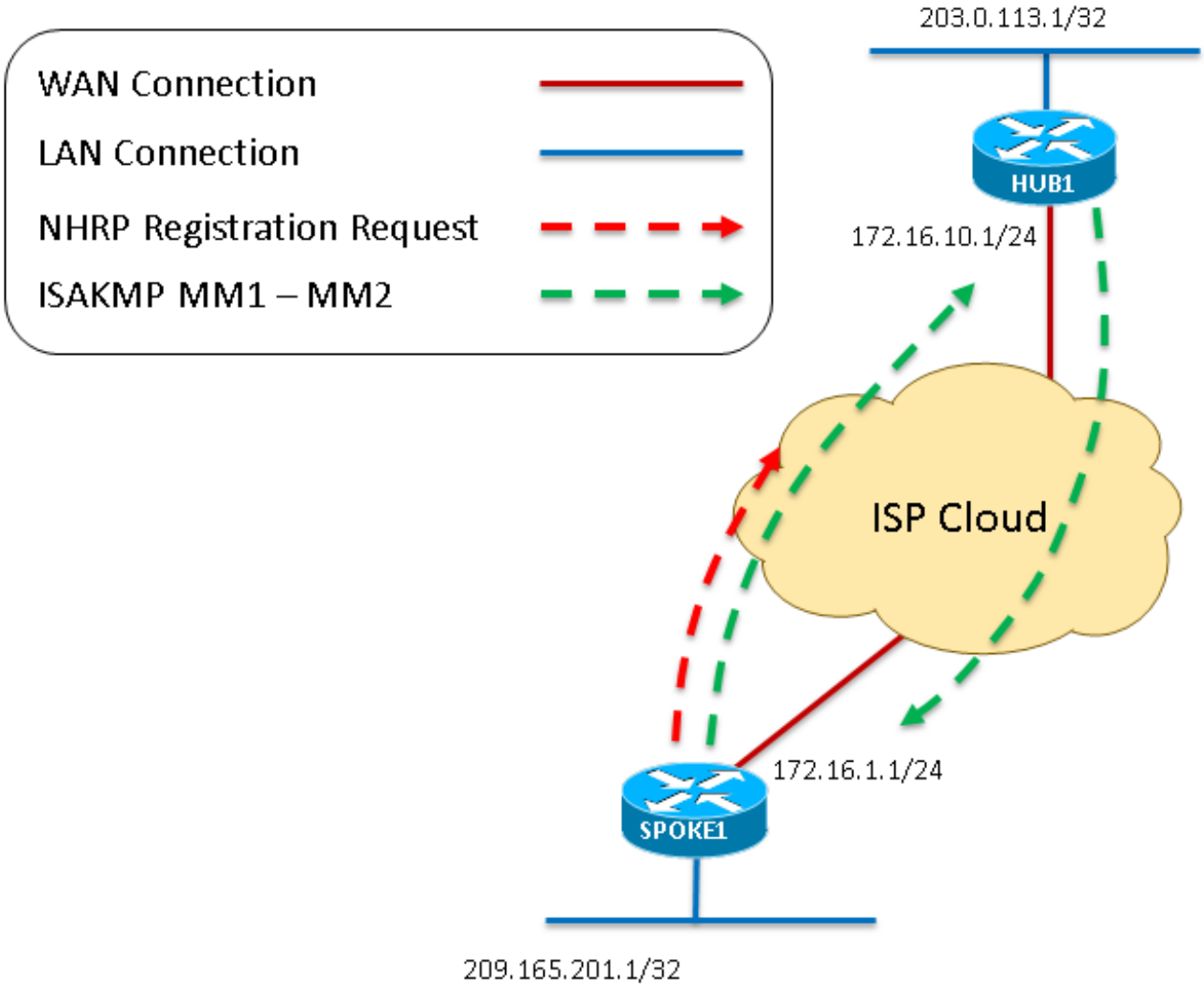
调试

数据包流可视化

这是整个DMVPN数据包流的可视化，如本文档所示。此外还包含更详细的调试，解释每个步骤。

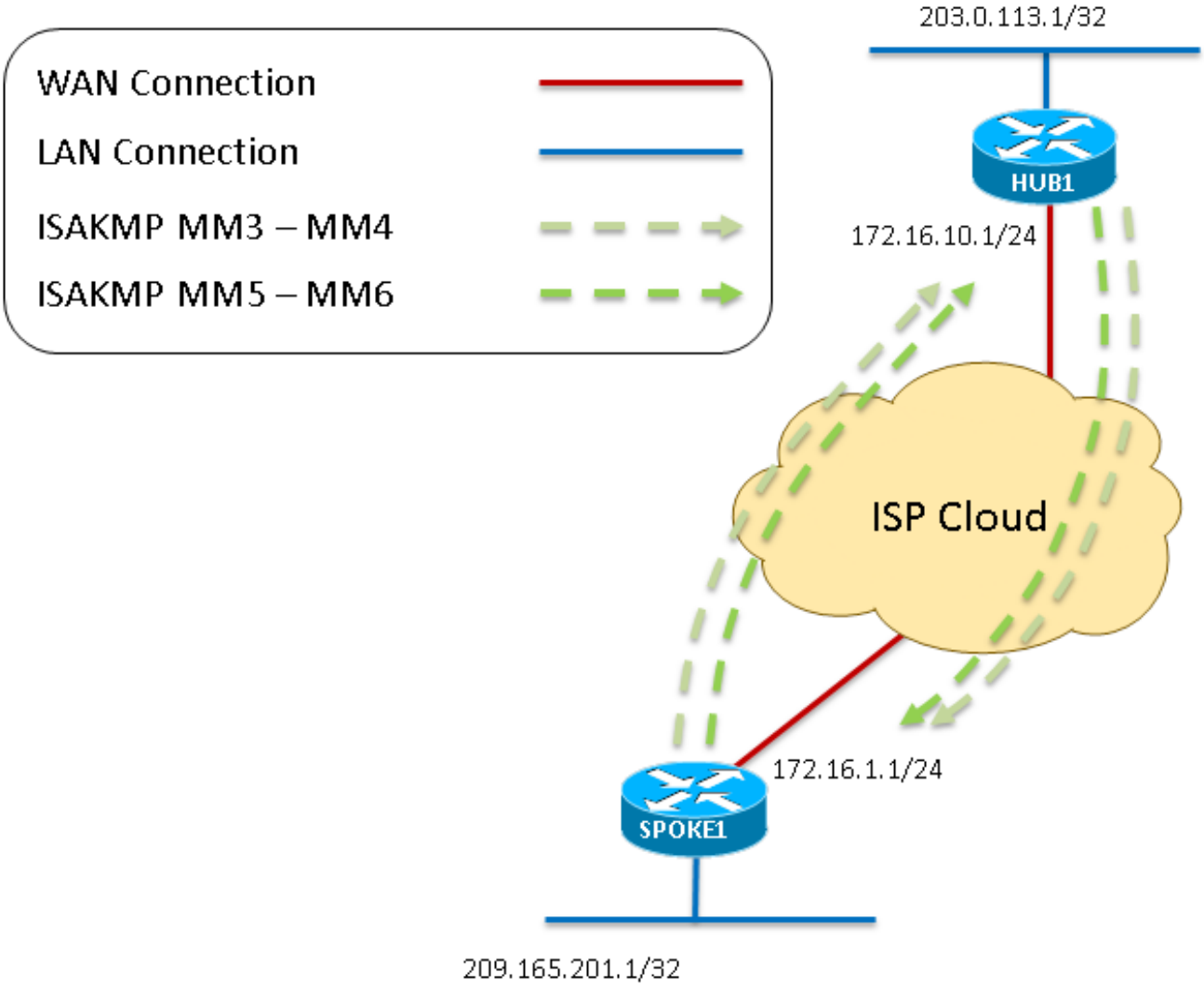
1. 当分支上的隧道为“no shutdown”时，会生成NHRP注册请求，该请求将启动DMVPN进程。由于集线器的配置是完全动态的，因此辐条必须是发起连接的终端。
2. 然后，NHRP注册请求封装在GRE中，GRE会触发加密进程启动。
3. 此时，第一条ISAKMP主模式消息ISAKMP MM1从分支发送到端口UDP500上的集线器。
4. 集线器接收并处理MM1，并以ISAKMP MM2作出响应，因为它具有匹配的ISAKMP策略。

图2 — 指步骤1至4



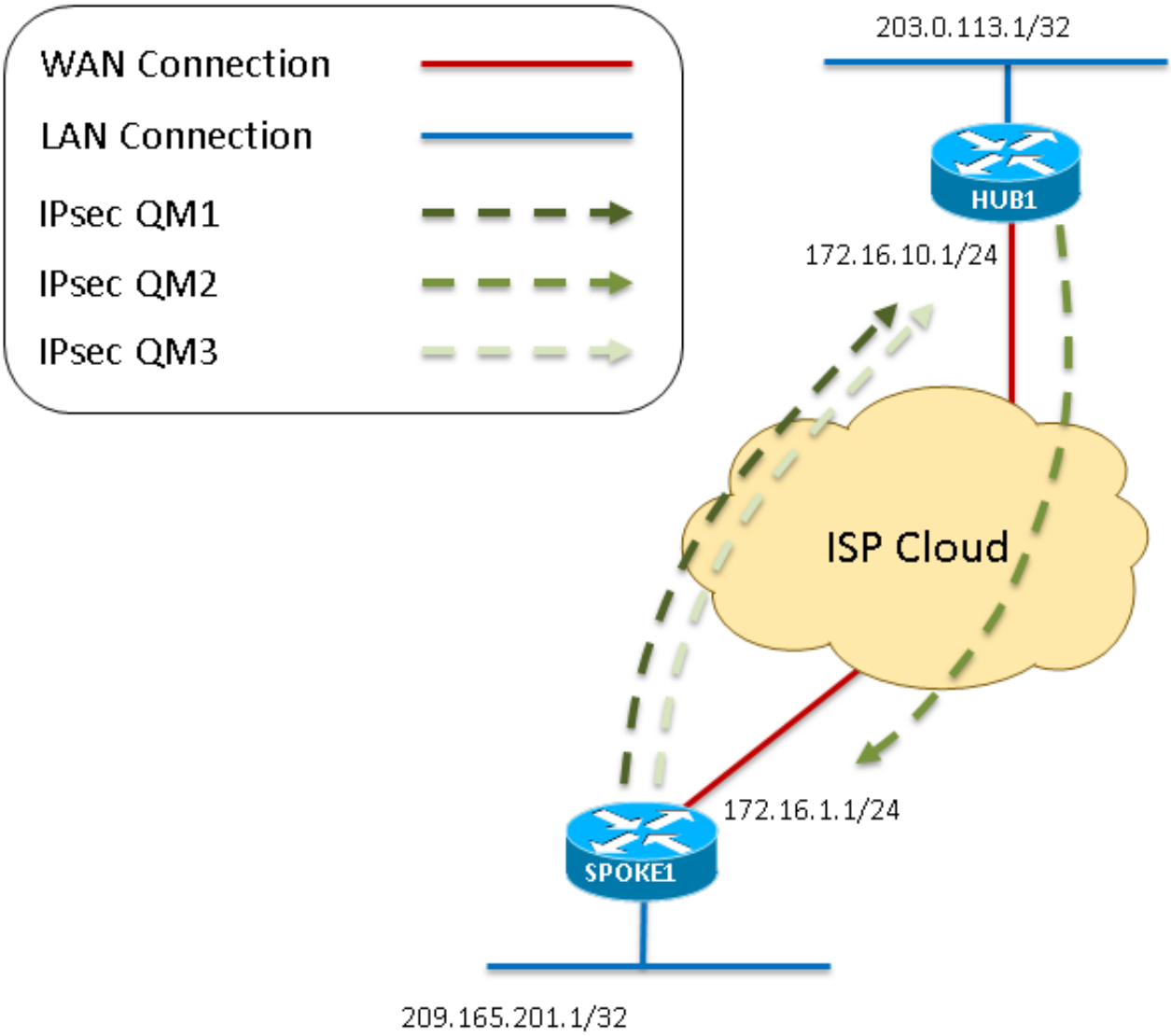
5. 辐条收到MM2后，会用MM3做出响应。与MM1一样，辐条会确认收到的ISAKMP策略有效。
6. 集线器接收MM3并以MM4作出响应。
7. 此时，在ISAKMP协商中，如果在传输路径中检测到NAT，分支可能会在端口UDP4500上做出响应。但是，如果未检测到NAT，则辐条继续并在UDP500上发送MM5。最后，集线器以MM6响应以完成主模式交换。

图3 — 指步骤5至7



8. 辐条从集线器收到MM6后，会将QM1发送到UDP500上的集线器以开始快速模式。
9. 集线器接收QM1并以QM2响应，因为所有接收的属性都被接受。此时，集线器会为此会话创建第2阶段SA。
10. 作为快速模式协商的最后一步，分支接收QM2。然后，辐条会创建其第2阶段SA并发送QM3作为响应。ISAKMP和IPSec协商完成。现在有一个IPSec会话，用于加密这两个对等体之间的GRE流量。

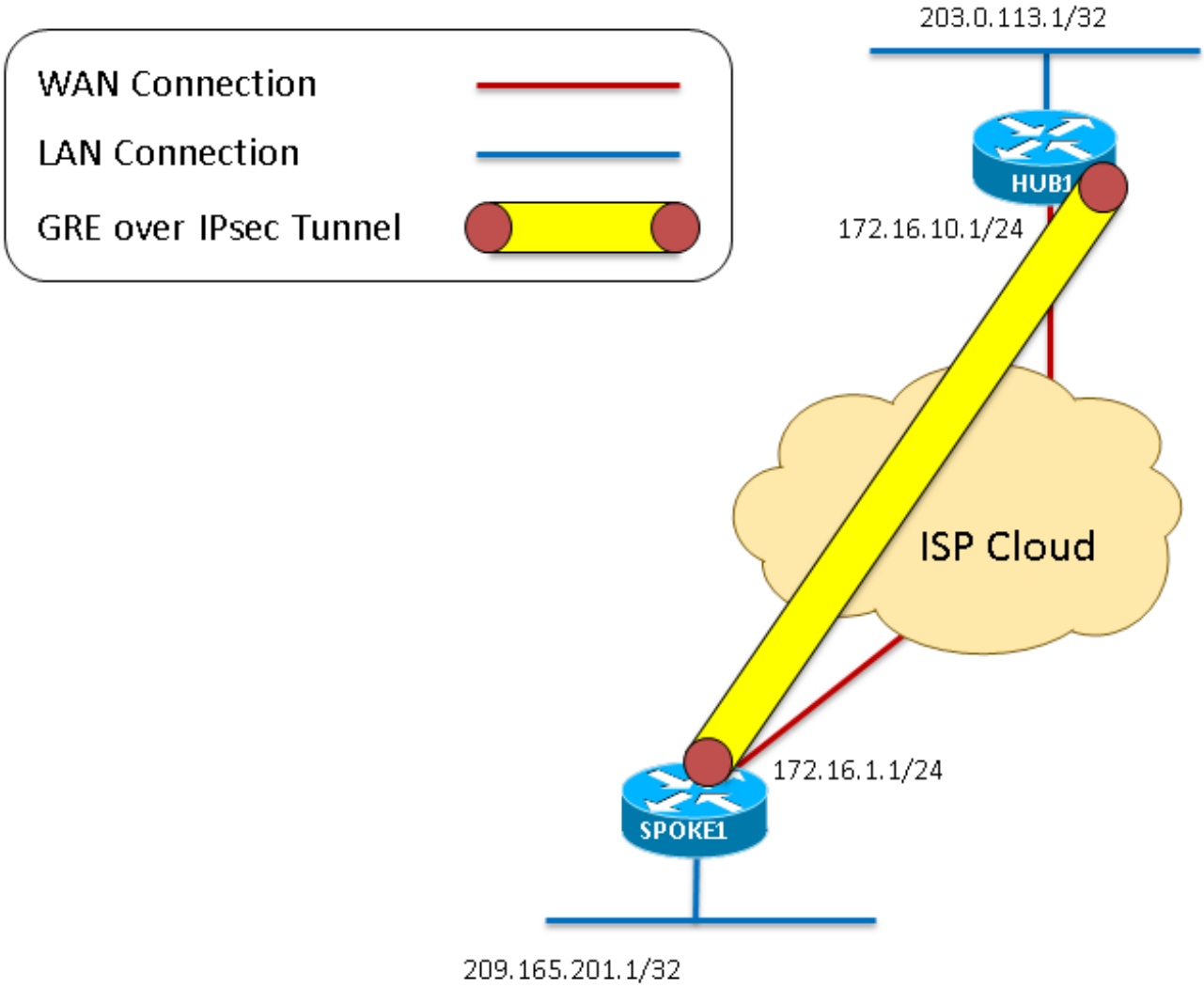
图4 — 指步骤8至10



11. 现在加密会话已启用并能够传递流量，这些数据包将封装在GRE over IPSec隧道中。

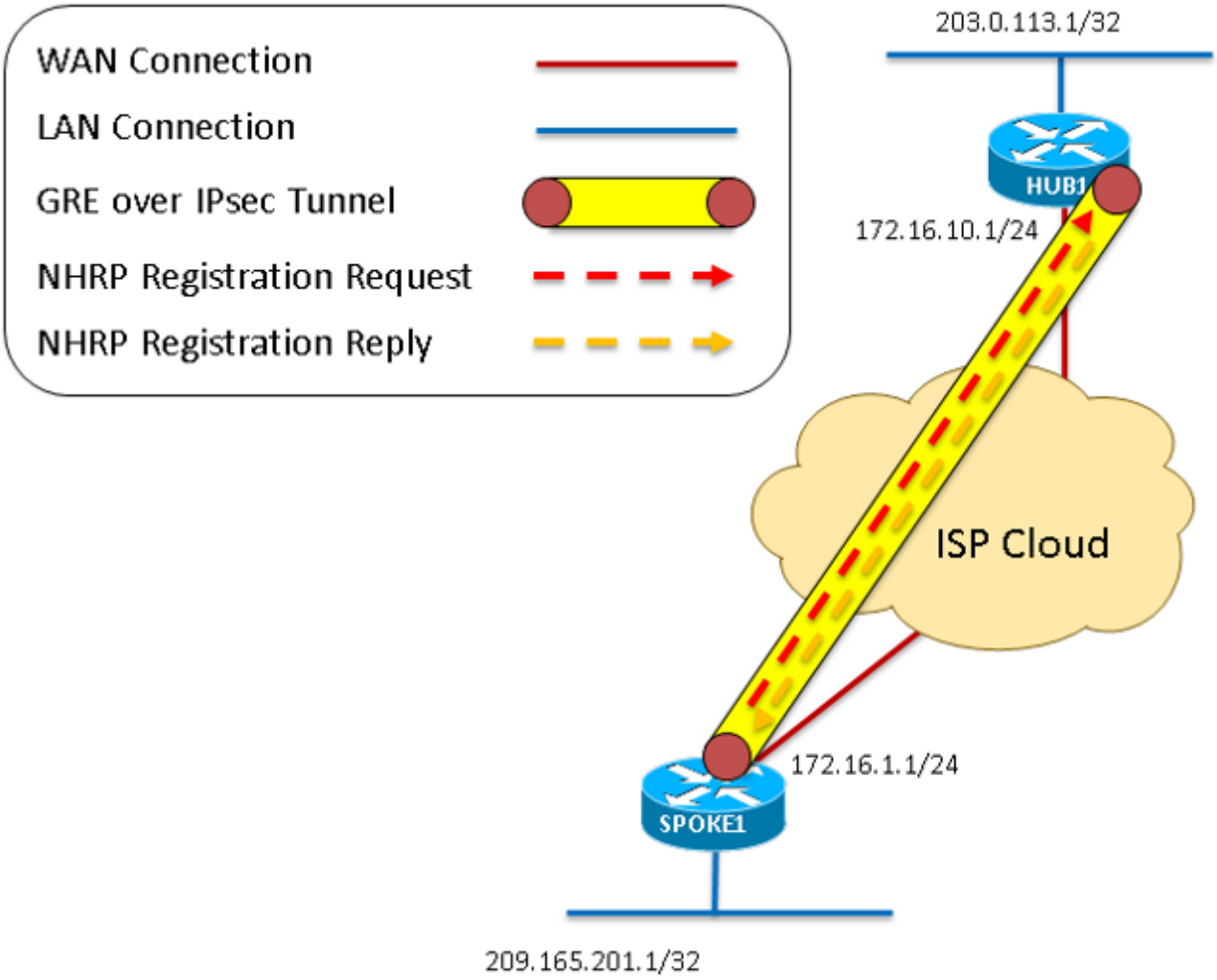
图5 — 指步骤

11



12. 如前面的步骤所示，辐条生成NHRP注册请求，该请求通过GRE over IPSec隧道发送。
13. 中心收到NHRP注册请求，并在确认分支具有有效隧道和非广播多路访问(NBMA)地址后发送NHRP注册应答。辐条收到此NHRP注册回复，完成注册过程。

图6 — 指步骤12至13



在中心和分支路由器上输入**debug dmvpn all** 命令时，会产生这些调试。此特定命令可启用以下调试集：

```
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
```

带说明的调试

由于这是实施IPSec的配置，因此调试显示所有ISAKMP和IPSec调试。如果未配置加密，请忽略以“IPsec”或“ISAKMP”开头的所有调试。

前几条调试消息由在隧道接口上**输入的**no shutdown命令生成。消息由正在启动的加密、GRE和NHRP服务集线器上出现NHRP注册错误，因为它未配置下一跳服务器(NHS)（集线器是DMVPN云的NHS）。 这是预

在分支的隧道为“no shutdown”后，集线器在端口500上收到IKE NEW SA（主模式1）消息。作为响应器，
ISAKMP状态从IKE_READY更改为IKE_R_MM1。

接收的IKE主模式1消息将被处理。集线器确定对等体具有匹配的ISAKMP属性，并且这些属性已填充到刚创
ISAKMP状态仍为IKE_R_MM1，因为回复尚未发送到辐条。
NAT-T供应商ID消息用于检测和遍历NAT。无论是否实施NAT，在ISAKMP协商期间都会收到这些消息。对

MM_SA_SETUP（主模式2）被发送到辐条，这确认MM1已接收并被接受为有效的ISAKMP数据包。ISAKMP状态从IKE_R_MM1更改为IKE_R_MM2。

集线器接收MM_SA_SETUP（主模式3）。集线器得出结论，对等体是另一台Cisco IOS设备，未为我们或
ISAKMP状态从IKE_R_MM2更改为IKE_R_MM3。

MM_KEY_EXCH（主模式4）由集线器发送。
ISAKMP状态从IKE_R_MM3更改为IKE_R_MM4。

集线器接收MM_KEY_EXCH（主模式5）。
ISAKMP状态从IKE_R_MM4更改为IKE_R_MM5。
此外，由于缺少ISAKMP配置文件，“对等匹配*none* of the profiles”被发现。因为这种情况下，ISAKMP不

最终MM_KEY_EXCH数据包（主模式6）由集线器发送。这将完成第1阶段协商，表示此设备已准备好进入
ISAKMP状态从IKE_R_MM5更改为IKE_P1_COMPLETE。

集线器接收第一个具有IPSec建议的快速模式(QM)数据包。收到的属性指定：encaps标志设置为2（传输模

联，因此这只是SA的外壳，尚不能用于传递流量。

这些只是一般的IPSec服务消息，说它工作正常。

为从172.16.10.1（集线器公有地址）到172.16.1.1（辐条公有地址）的IP协议47(GRE)创建伪加密映射条目

集线器发送的第二条QM消息。IPSec服务生成的消息，确认隧道保护在Tunnel0上处于启用状态。另一条SA创建消息将显示，其中以千字节和秒为单位，包含目标IP、SPI、转换集属性和生存期。

这些最终的QM消息确认快速模式已完成，且隧道两端均启用IPSec。
与ISAKMP不同，IPSec只有三条消息，而不是六条，而ISAKMP中每个对等体都经历每种状态（MM1到MM

这是从辐条收到的NHRP注册请求，用于向NHS（中心）注册。 看到这些数字的倍数很正常，因为辐条在
源NBMA:发送此数据包并尝试向NHS注册的分支的NBMA(internet)地址
src协议:尝试注册的辐条的隧道地址
dst协议:NHS/集线器的隧道地址
身份验证扩展，数据和冒号；NHRP 验证字符串
客户端NBMA:NHS/集线器的NBMA地址
客户端协议:NHS/集线器的隧道地址

NHRP调试数据包添加目标网络10.1.1.1/32，可通过下一跳10.1.1.1（NHRP为172.16.1.1）获得。172.16.
这些消息确认注册成功，分支隧道地址的解析也成功。

这是集线器为响应之前收到的“NHRP注册请求”而向辐条发送的NHRP注册回复。与其他注册数据包一样，
src，dst:隧道源（中心）和目标（分支）IP地址。这些是路由器发送的GRE数据包的源和目标
源NBMA:分支的NBMA（互联网）地址
src协议:尝试注册的辐条的隧道地址

dst协议:NHS/集线器的隧道地址
客户端NBMA:NHS/集线器的NBMA地址
客户端协议:NHS/集线器的隧道地址
身份验证扩展，数据和冒号；NHRP 验证字符串

更常见的IPSec服务消息，说它工作正常。

表示EIGRP邻接关系与位于10.1.1.1的邻居辐条处于启用状态的系统消息。

确认NHRP解析成功的系统消息。

确认功能并排除故障

本部分提供一些最有用的**show**命令，用于对中心辐射型和辐射型进行故障排除。要启用更具体的调试，请使用以下调试条件：

- 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:
```

相关信息

- IPSec故障排除：了解和使用debug命令
- 下一代加密
- RFC3706:IKE失效对等体检测
- RFC3947:IKE NAT穿越
- 技术支持和文档 - Cisco Systems