DMVPN阶段1调试排除故障指南

目录

简介

本文描述您在一动态多点虚拟专用网络的调试消息(DMVPN)阶段1部署的星型网会遇到。

先决条件

对于配置和调试in命令本文，您将需要运行Cisco IOS版本12.4(9)T或以上的两个Cisco路由器。一般来说，一基本DMVPN阶段1要求Cisco IOS版本12.2(13)T或以上或版本聚合服务路由器的(ASR) 12.2(33)XNC，虽然功能，并且也许不支持在本文看到的调试。

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)
- Internet协议安全性(IPSec)
- 至少这些路由协议之一：增强的内部网关路由选择协议(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

本文档中的信息根据Cisco运行Cisco IOS版本15.1(4)M4的2911集成服务路由器(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。

重要的增强功能

这些Cisco IOS版本介绍重大的功能或修正DMVPN阶段1的：

- 当曾经公共密钥基础设施(PKI)时，版本12.2(18)SXF5 -请改善ISAKMP的支持
- 版本12.2(33)XNE - ASR， IPSec简档，通道保护， IPSec网络地址转换(NAT)穿越
- 版本12.3(7)T -里面虚拟路由和转发(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 -多种DMVPN的支持涉及调试和命令
- 版本12.4(15)T -共享通道保护
- 版本12.4(20)T -在DMVPN的IPv6
- 版本15.0(1)M - NHRP通道健康监控

规则

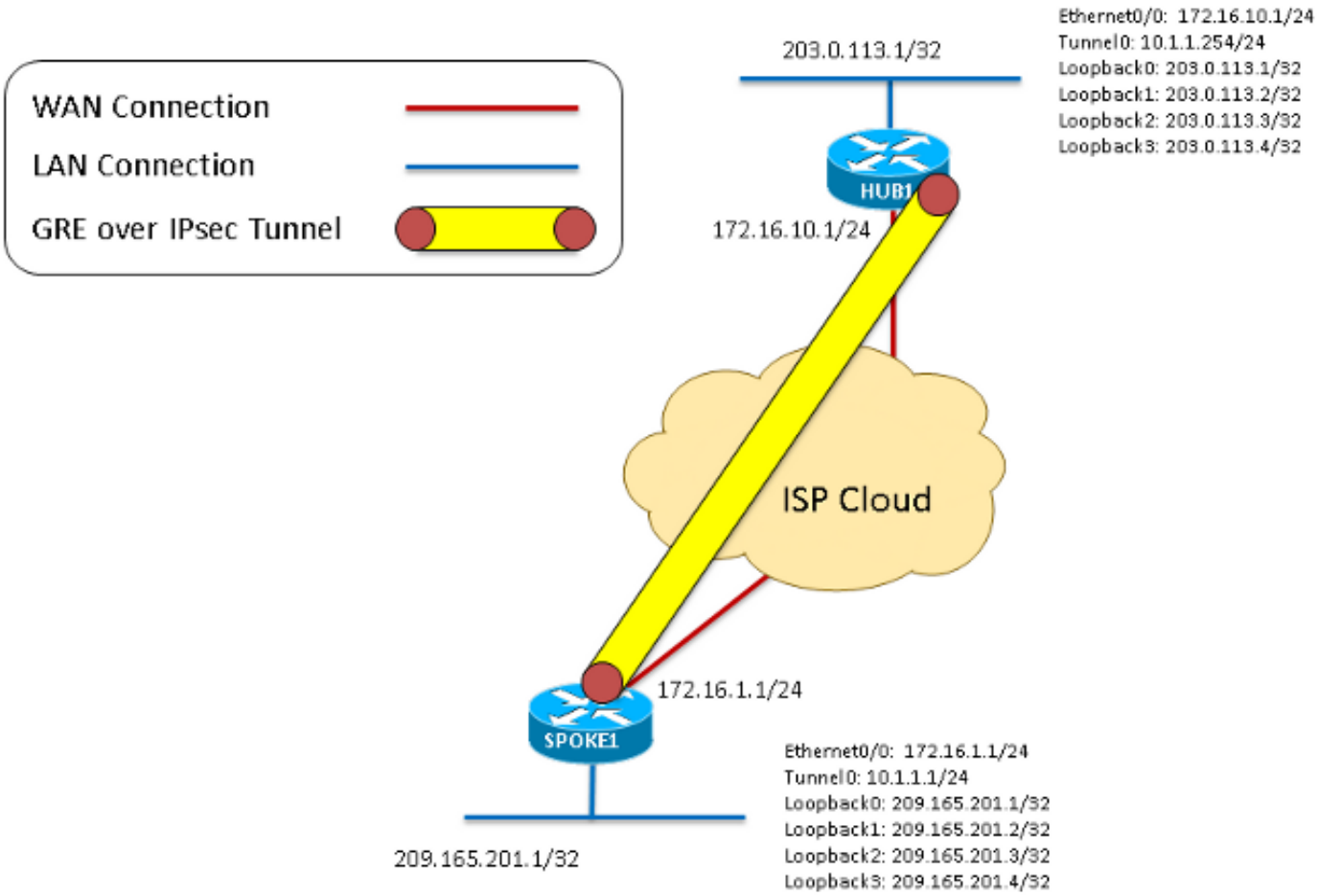
有关文档规则的信息，请参阅 Cisco 技术提示规则。

相关配置

拓扑概述

对于此拓扑，运行的两2911 ISR版本15.1(4)M4为DMVPN阶段1配置：一作为集线器和一个作为分支。使用了Ethernet0/0，在每个路由器的“互联网”接口。四回环接口配置模拟在集线器或轮幅站点居住的局域网。因为这是一DMVPN阶段1拓扑与仅一个发言，分支用一点到点GRE隧道配置而不是多点GRE通道。同一crypto configuraton (ISAKMP和IPSec)在每个路由器用于保证他们正确地匹配。

图 1



crypto

这是相同的在集线器和分支。

```
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
```

分支

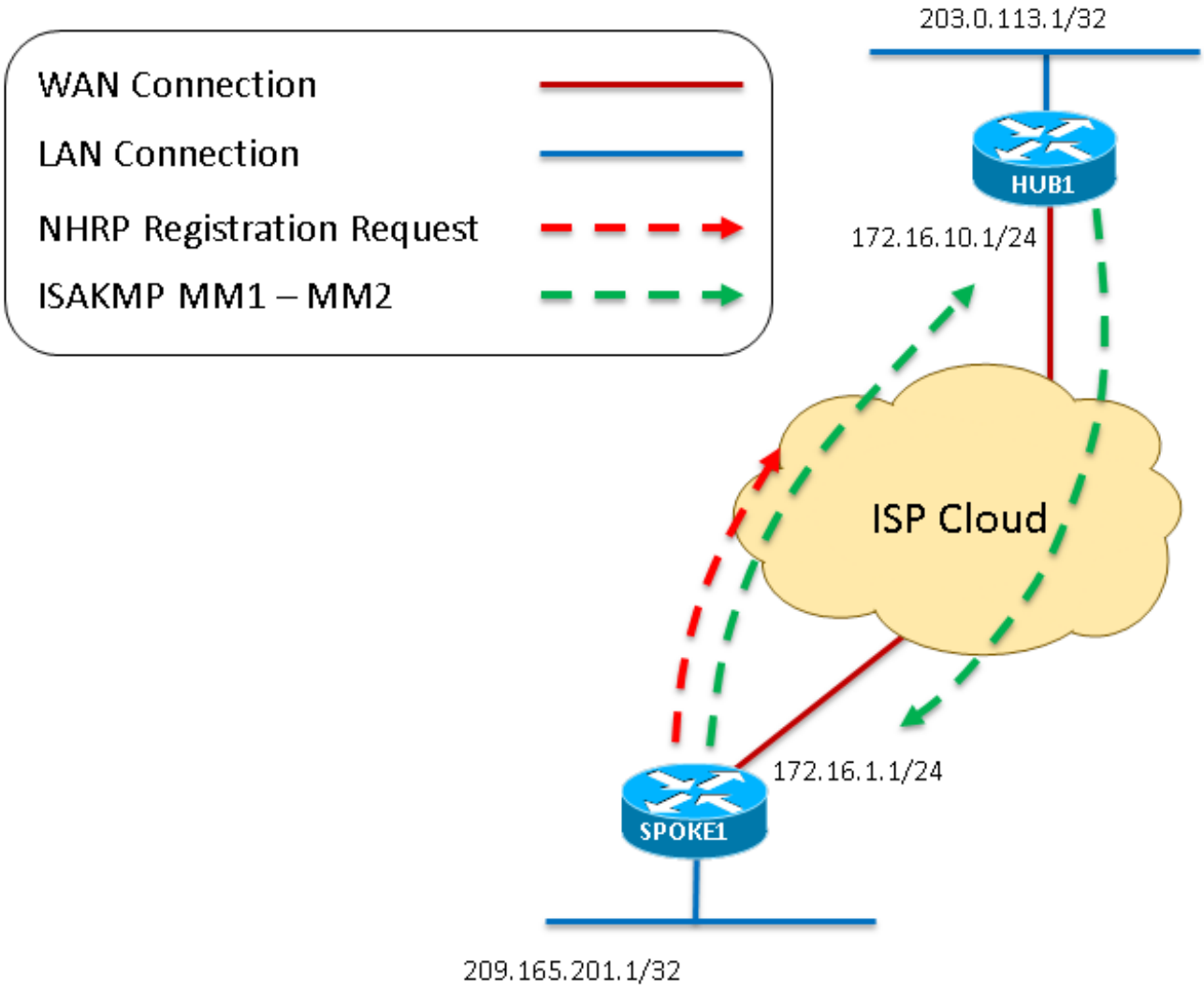
```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile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

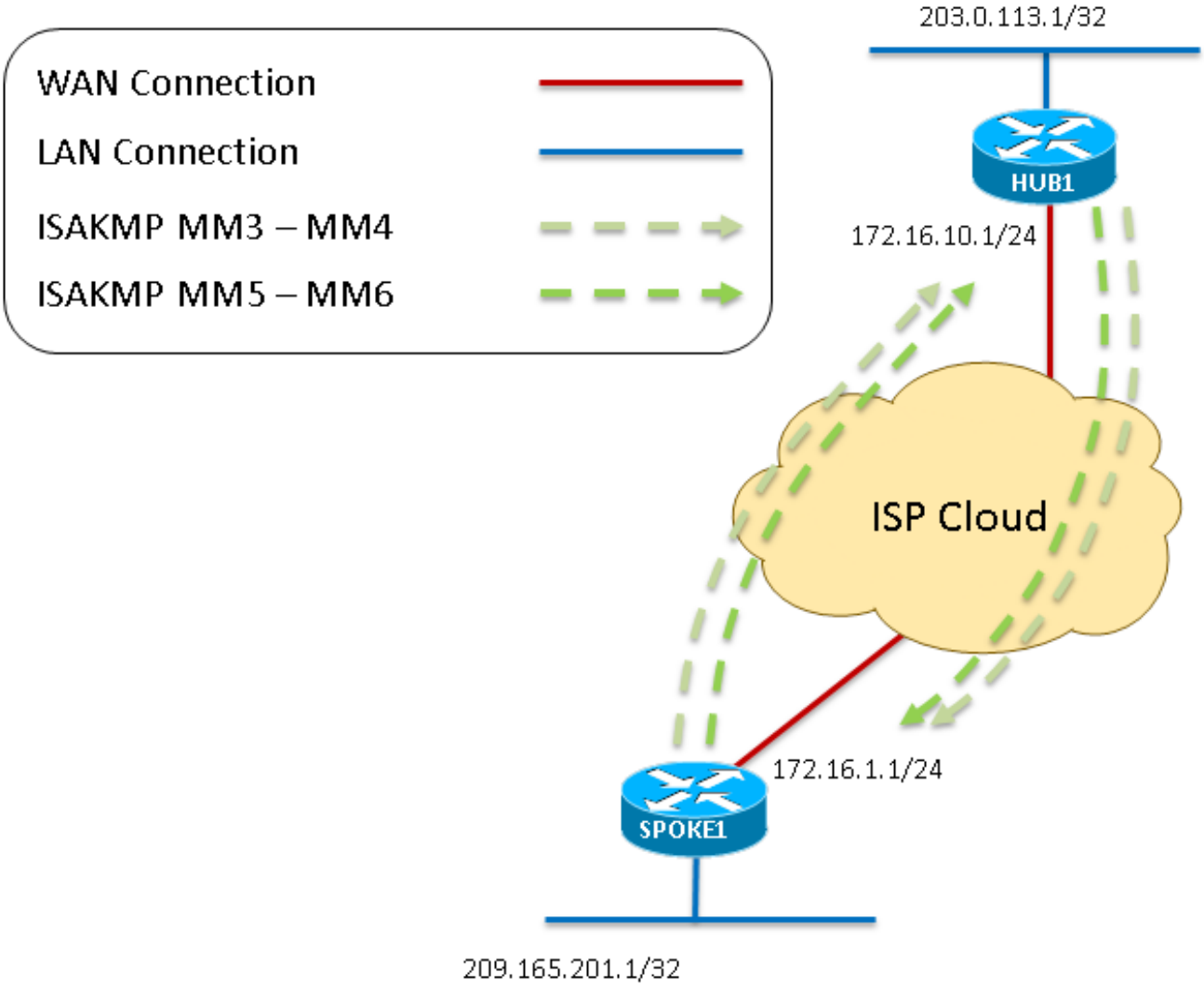
数据包流流可视化

这是整个DMVPN数据包流的可视化如在本文中看到的。解释其中每一个步骤的更多详细的调试也包括。

1. 当在分支的通道是"no shutdown"时生成NHRP注册请求，开始DMVPN进程。因为集线器的配置完全动态，分支必须是首次连接的终端。
2. 触发加密进程开始的NHRP注册请求在GRE然后被封装。
3. 这时，第一ISAKMP主模式信息- ISAKMP MM1 -从传送发言到在端口UDP500的集线器。
4. 因为有一个匹配的ISAKMP策略，集线器接收并且处理MM1并且回应ISAKMP MM2。
   图表2 -是指步骤1到
   4

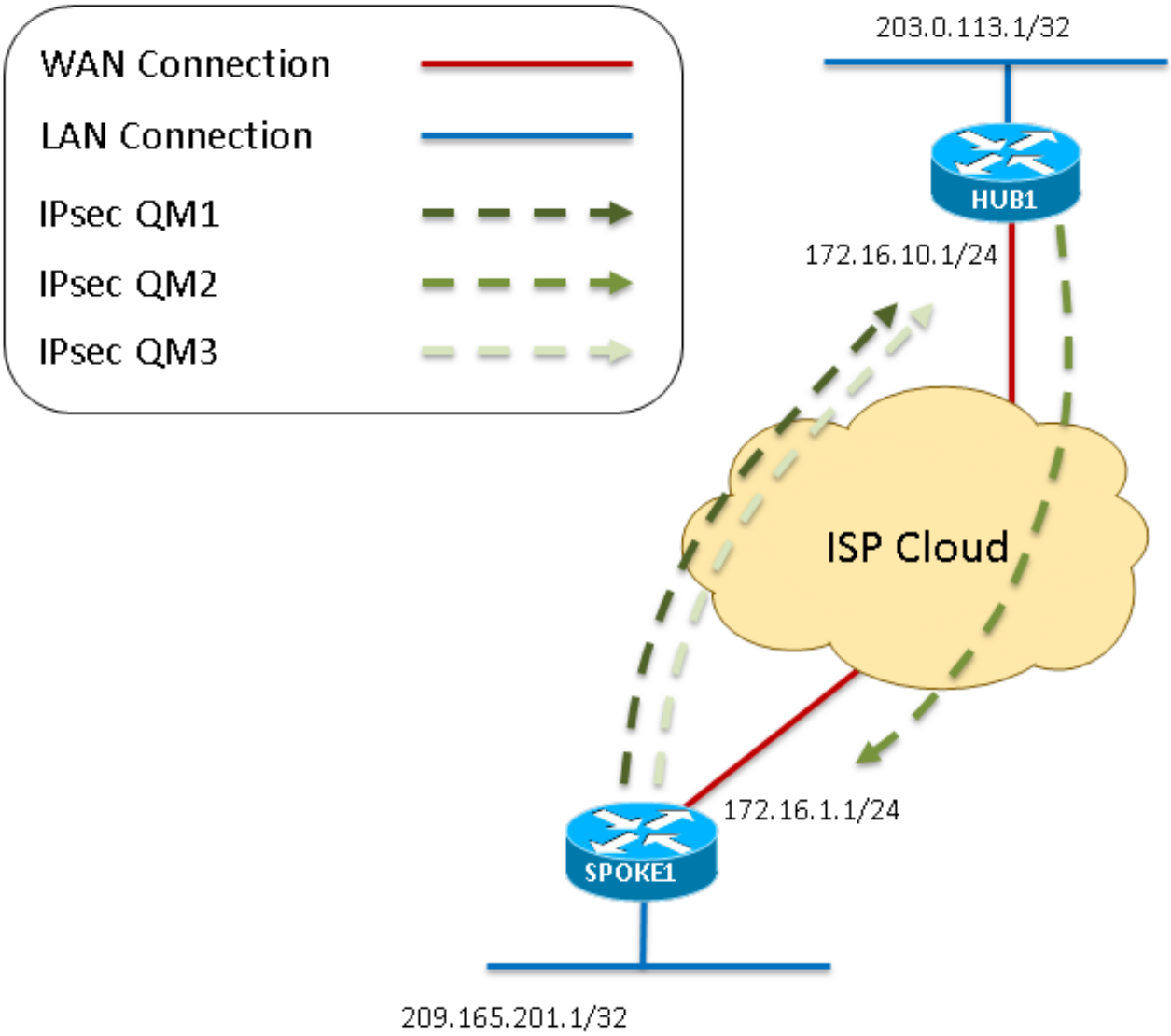


5. 一旦分支接收MM2，回应MM3。如同MM1，分支确认已接收ISAKMP策略有效。
6. 集线器接收MM3并且回应MM4。
7. 在这一点上，如果NAT在转接路径，检测ISAKMP协商，分支在端口UDP4500也许响应。然而，如果NAT没有检测分支继续并且发送在UDP500的MM5。最后，集线器回应MM6为了完成主模式交换。
   图表3 -是指步骤5到
   7

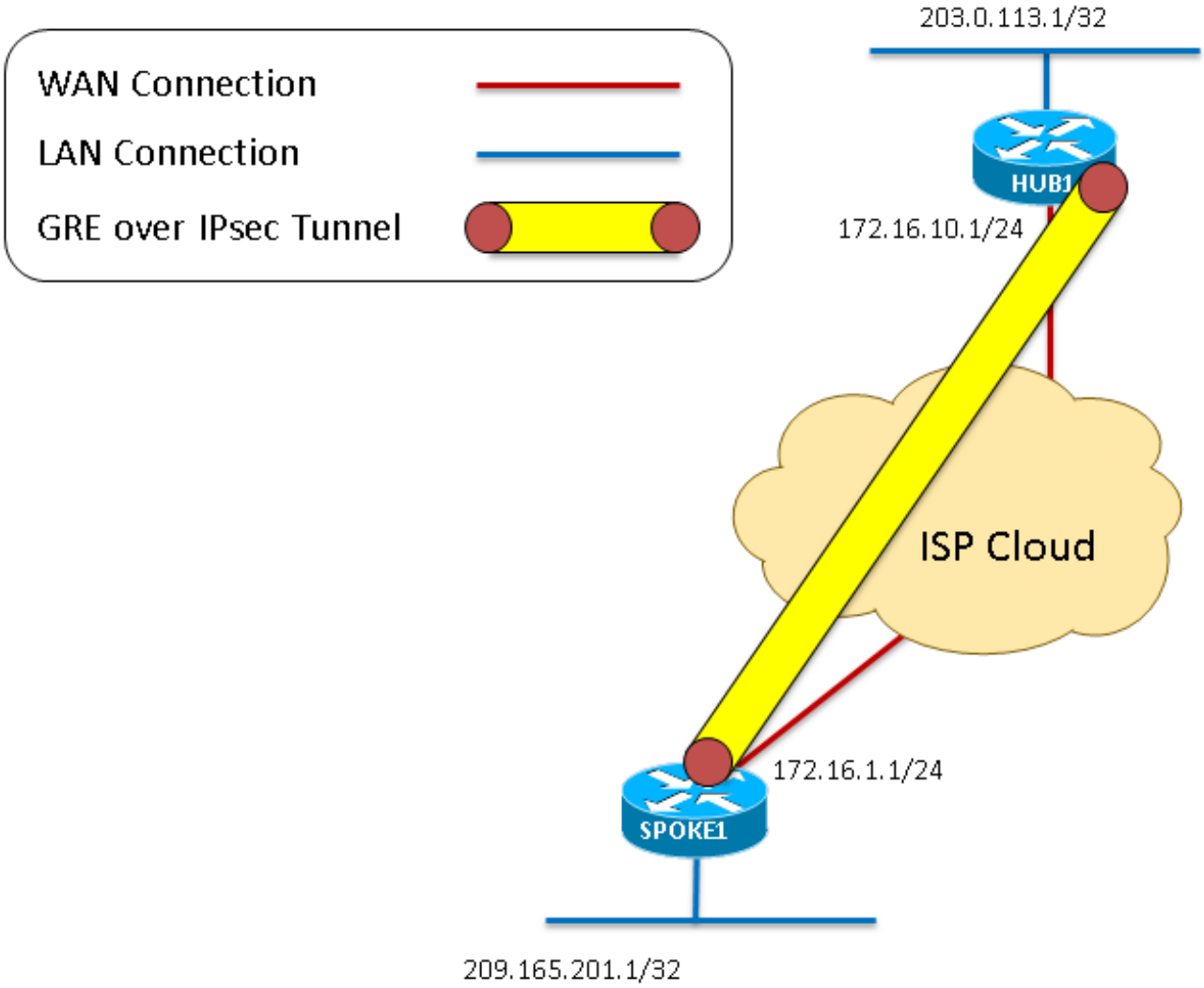


8. 一旦分支接收从集线器的MM6，发送QM1到在UDP500的集线器为了开始快速模式。
9. 集线器接收QM1并且回应QM2，和所有已接收属性接受。这时集线器创建此会话的第2阶段SAS。
10. 作为快速模式协商的最后一步， QM2由分支接收。分支然后创建其第2阶段SAS并且发送在答复的QM3。这完成ISAKMP和IPSec协商。当前有加密在这两对等体之间的GRE流量的IPSec会话。

图表4 -是指步骤8到10

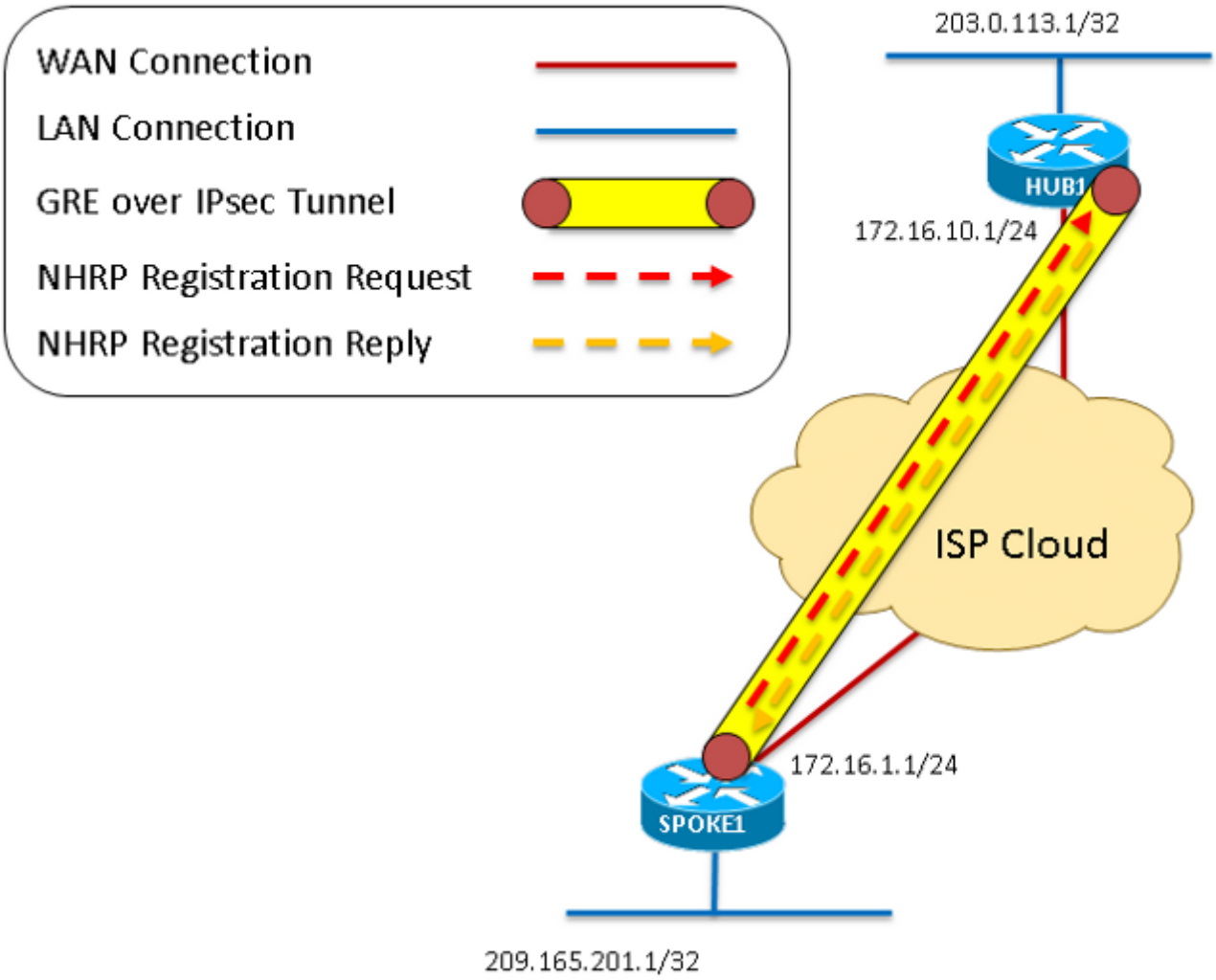


11. 即然crypto会话启用和能通过流量，这些数据包在IPSec的GRE通道内被封装。
    图表5 -是指步骤
    11



12. 象在第一步被看到了，分支生成在IPSec的GRE通道间发送的NHRP注册请求。
13. 集线器收到NHRP注册请求并且发送NHRP注册回复，一旦确认分支有一个有效通道和非广播多路访问(NBMA)地址。分支收到完成注册过程的此NHRP注册回复。

图表6 -是指步骤12到
13



当所有all命令调试的dmvpn在星型网路由器时，被输入这些调试是结果。此特定命令启用此套调试：

```
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
```

与说明的调试

因为这是IPSec实现的configuraton，调试显示所有ISAKMP和IPSec调试。如果没有crypto配置，忽略从“IPsec”或“ISAKMP开始的所有调试”。

HUB调试说明
这些最初的少数调试消息由在隧道接口输入的**no shutdown命令**生成。消息由启动的crypto， GRE和NHRP NHRP注册错误在集线器被看到，因为不安排一个下一跳服务器(NHS)配置(集线器是我们的DMVPN网云的

在spoke的通道是“未关闭后”，集线器接收IKE新建的SA (在端口500的主模式1)消息。作为响应方，集线器
ISAKMP状态变换从IKE_READY到IKE_R_MM1。

已接收IKE主模式1消息处理。集线器确定对等体有创建的匹配ISAKMP属性，并且他们被填装到ISAKMP S
Hellman (DH) group1、预共享密匙验证的和SA默认寿命86400秒(0x0 0x1 0x51 0x80 = 0x15180 = 86400
因为回复有不被发送到分支， ISAKMP状态仍然是IKE_R_MM1。
NAT-T厂商ID消息用于NAT检测和穿越。不论NAT实现，这些消息在ISAKMP的协商时预计。相似的消息为

MM_SA_SETUP (主模式2)发送对分支，确认MM1接收并且接受作为一个有效ISAKMP信息包。
ISAKMP状态变换从IKE_R_MM1到IKE_R_MM2。

MM_SA_SETUP (主模式3)由集线器接收。集线器认为，对等体是另一个Cisco IOS设备，并且NAT没有为 ISAKMP状态变换从IKE_R_MM2到IKE_R_MM3。
MM_KEY_EXCH (主模式4)由集线器发送。 ISAKMP状态变换从IKE_R_MM3到IKE_R_MM4。

MM_KEY_EXCH (主模式5)由集线器接收。
ISAKMP状态变换从IKE_R_MM4到IKE_R_MM5。
另外，配置文件的“对等体匹配*none*”被看到的归结于缺乏ISAKMP简档。由于这是实际情形， ISAKMP不

最终MM_KEY_EXCH数据包(主模式6)由集线器发送。这完成表示此设备为第2阶段的阶段1协商(IPSec快速
ISAKMP状态变换从IKE_R_MM5到IKE_P1_COMPLETE。

集线器收到有IPSec建议的第一快速模式数据包。接收的属性指定那：encaps标志设置到2 (传输模式，标志
节(在十六进制的0x465000)，加密的HMAC-SHA和3DES。因为这些是在本地配置里设置的同样属性，建议
(SPI)值没有关联与这些，这是不能使用通过流量SA的shell。

这些是说的将军IPSec服务服务消息适当地运作。

假crypto映射条目为从172.16.10.1 (集线器公共地址)的IP协议47 (GRE)创建对172.16.1.1 (分支公共地址)。
建议。

由集线器的第二QM发送的消息。确认的IPSec服务生成的消息通道保护是UP在隧道0。
有目的地IP、斯皮、转换设置的属性和寿命在千字节和秒钟保持的另一个SA创建消息被看到。

这些最终QM消息确认快速模式完成，并且IPSec是UP在通道的两边。
不同于每对等体通过每状态的ISAKMP (MM1通过MM6/P1_COMPLETE)， IPSec有点不同的，尽管只有三
示由“R”在IKE_QM_R_QM1消息)去QM_READY， QM_SPI_STARVE， QM_R_QM2， QM_PHASE2_CO
QM_I_QM1直接地QM_PHASE2_COMPLETE。

这是从在尝试的分支接收的NHRP注册请求注册到NHS (集线器)。发现这些的多个是正常的，当分支继续尝 **src NBMA** ：发送此数据包并且设法向NHS登记分支的NBMA (互联网)地址 **src协议**：建立隧道设法注册分支的地址 **dst协议**：NHS/hub的通道地址 **验证分机**，数据：NHRP认证字符串 **客户端NBMA** ：NHS/hub的NBMA地址 **客户端协议**：NHS/hub的通道地址
NHRP添加目标网络10.1.1.1/32联机的调试数据包通过10.1.1.1下一跳在172.16.1.1 NHRP。172.16.1.1也被 这些消息确认注册是成功的，象spoke的一解决方法请建立隧道地址。

这是集线器发送的NHRP注册回复对分支以回应”接收的“NHRP注册请求前。类似其他注册信息包，集线器
src， dst ：隧道源(集线器)和目的地(分支) IP地址。这些是路由器发送的GRE数据包的源和目的
src NBMA ：分支的NBMA (互联网)地址
src协议：设法注册分支的通道地址
dst协议：NHS/hub的通道地址
客户端NBMA ：NHS/hub的NBMA地址
客户端协议：NHS/hub的通道地址
验证分机，数据：NHRP认证字符串

说的更加将军的IPSec服务服务消息它适当地运作。
陈述的系统消息EIGRP邻接是邻接发言在10.1.1.1。
确认一成功的NHRP解决方法的系统消息。

确认功能并且排除故障

此部分有用于的某些多数有用的show命令排除故障两星型网。为了启用更多特定调试，请使用这些调试conditionals ：

- debug dmvpn condition对等体nbma *NBMA_ADDRESS*
- debug dmvpn condition对等体通道*TUNNEL_ADDRESS*
- debug crypto condition对等体ipv4 *NBMA_ADDRESS*

显示crypto插槽

```
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"
```

显示crypto会话详细信息

```
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详细信息

```
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 encryptionIPv4 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详细信息

```
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
```

显示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)
```

显示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：了解和使用调试指令
- 下一代加密
- RFC3706 ：IKE对端死机检测
- RFC3947 ：IKE NAT横越

- 技术支持和文档 - Cisco Systems