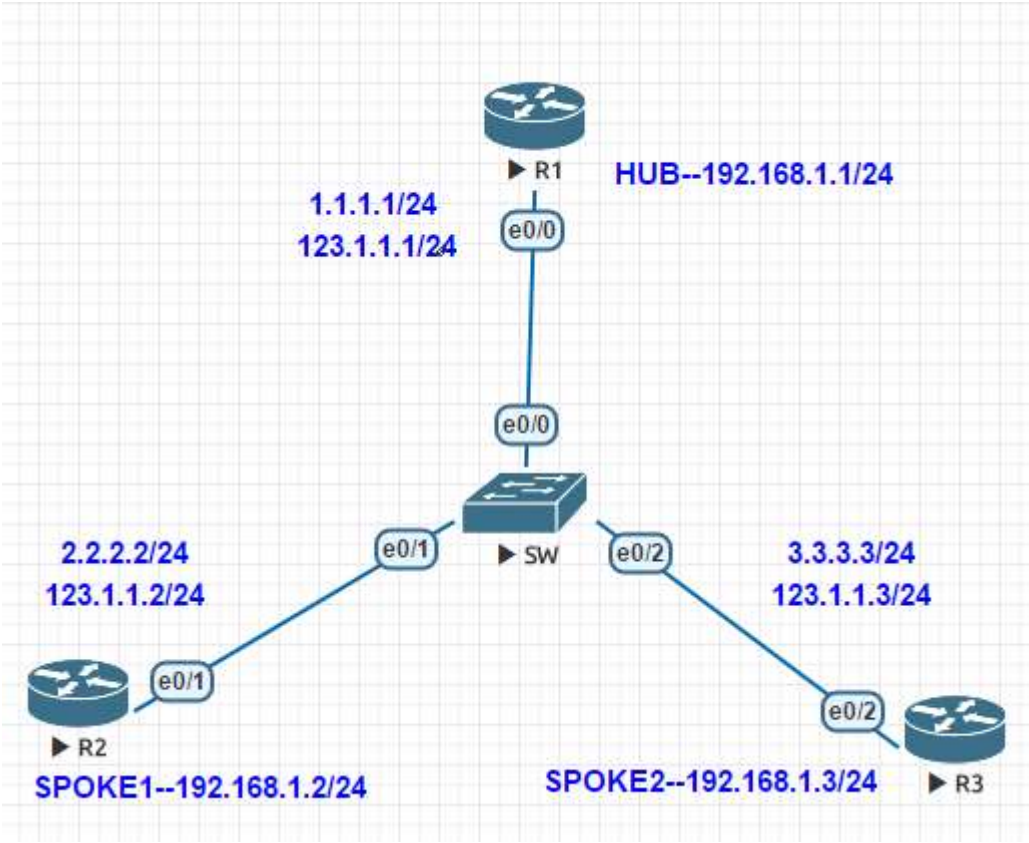
DMVPN 配置和原理分析

一、拓扑



要求:

1.按图中要求，在 R1、R2、R3 上配置 MGRE，其中 MGRE 的 IP 地址为 192.168.1.0/24。

2.在 MGRE 上运行 IGP 协议，使 R1、R2、R3 背后的环回口可以通过 IGP 相通。

3.在 MGRE 的基础上配置 IPSEC VPN，即 DMVPN，并且分析其工作过程。

二、配置

1.基本 IP 地址配置(省略)。

2.配置 MGRE

```
R1(config)#interface tunnel 123
R1(config-if)#tunnel
*Mar 20 07:57:05.549: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1
R1(config-if)#tunnel mode gre multipoint
R1(config-if)#tunnel source 123.1.1.1
R1(config-if)#t
*Mar 20 07:57:28.832: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1
R1(config-if)#tunnel key 123
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

其中第一句是修改 Gre 的工作模式为多点 GRE，即 MGRE。

接着在 R2、R3 上完成相同的配置，并且 MGRE 的 IP 地址分别为 192.168.1.2/24、192.168.1.3/24，在下图中没有贴出 IP 地址的配置，但实质已经配过了

```
R2(config)#interface tunnel 123
R2(config-if)#tunnel mode gre m
*Mar 20 07:58:44.989: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel123
R2(config-if)#tunnel mode gre multipoint
R2(config-if)#tunnel source 123.1.1.2
R2(config-if)#tun
*Mar 20 07:58:52.874: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel123
R2(config-if)#tunnel key 123
R2(config-if)#no shutdown
```

```
R3(config)#interface tunnel 123
R3(config-if)#tunnel mode gre
*Mar 20 08:00:03.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1
R3(config-if)#tunnel mode gre multipoint
R3(config-if)#tunnel source 123.1.1.3
R3(config-if)#
*Mar 20 08:00:15.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1
R3(config-if)#tunnel key 123
R3(config-if)#no shutdown
```

配置完成后，我们可以从 R2 上访问另外 R1、R3，看能否成功?

```
R2#ping 192.168.1.1 source 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.2
.....
Success rate is 0 percent (0/5)
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES TFTP   administratively down down
Ethernet0/1            123.1.1.2       YES TFTP   up                    up
Ethernet0/2            unassigned      YES TFTP   administratively down down
Ethernet0/3            unassigned      YES TFTP   administratively down down
Loopback0              2.2.2.2         YES TFTP   up                    up
Tunnel123              192.168.1.2     YES manual up                    up
R2#
```

明显看到 R2 不能访问 R1，同样 R2 也不能访问 R3，其质上，此时 MGRE 的三个端口都没法互访，分析原因，这是因为 R2 要发包给 R1，必须知道 R1 上的 MGRE 地址 192.168.1.1/24 对应的 MAC 地址是多少，如果不知道这个 MAC 地址，那么根本不可能完成访问。

因此在 MGRE 的基础上还要配置 NHRP，即下一跳解析协议，

3.NHRP 配置

①Hub 节点——即中心节点 R1 的配置

```
R1(config)#interface tunnel 123
R1(config-if)#ip nhrp network-id 10
R1(config-if)#ip nhrp authentication cisco
R1(config-if)#ip nhrp map multicast dynamic
R1(config-if)#
```

②Spoke 节点——即分支节点 R2、R3 的配置

```
R2(config)#interface tunnel 123
R2(config-if)#ip nhrp network-id 10
R2(config-if)#ip nhrp authentication cisco
R2(config-if)#ip nhrp map 192.168.1.1 123.1.1.1
R2(config-if)#ip nhrp map multicast 123.1.1.1
R2(config-if)#ip nhrp nhs 192.168.1.1
R2(config-if)#no shutdown
R2(config-if)#
```

```
R3(config)#interface tunnel 123
R3(config-if)#ip nhrp network-id 10
R3(config-if)#ip nhrp authentication cisco
R3(config-if)#ip nhrp map 192.168.1.1 123.1.1.1
R3(config-if)#ip nhrp map multicast 123.1.1.1
R3(config-if)#ip nhrp nhs 192.168.1.1
R3(config-if)#no shutdown
```

其中命令解释如下:

Ip nhrp map 192.168.1.1 123.1.1.1：让 SPOKE 知道 HUB 的虚拟地址(tunnel 口地址)和其物理地址(Tunnel 源的物理地址)之间的对应关系。

Ip nhrp map multicast 123.1.1.1：即让 SPOKE 向物理地址为 123.1.1.1 的接口发组播包，因为此时的 MGRE 是一个 NBMA 网络。

Ip nhrp nhs 192.168.1.1：让 SPOKE 知道 nhrp 服务器的地址，即向该服务器进行注册。

配置完成后，我们可以在 HUB 和 SPOKE 上进行互访测试

```
R1#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

```
R2#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R2#
```

```
R3#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R3#
```

明显可以看到现在 R1、R2、R3 可以通过 MGRE 相通。

4.在 MGRE 上配置动态路由协议，这里选择 EIGRP

```
R1(config)#router eigrp 90
R1(config-router)#eigrp router-id 1.1.1.1
R1(config-router)#eigrp log-neighbor-changes
R1(config-router)#no auto-summary
R1(config-router)#network 1.1.1.1 0.0.0.0
R1(config-router)#network 192.168.1.1 0.0.0.0
```

```
R2(config)#router eigrp 90
R2(config-router)#eigrp router-id 2.2.2.2
R2(config-router)#eigrp log-neighbor-changes
R2(config-router)#network 2.2.2.2 0.0.0.0
R2(config-router)#network 192.168.1.2 0.0.0.0
```

```
R3(config)#router eigrp 90
R3(config-router)#eigrp router-id 3.3.3.3
R3(config-router)#eigrp log-neighbor-changes
R3(config-router)#no auto-summary
R3(config-router)#network 3.3.3.3 0.0.0.0
R3(config-router)#network 192.168.1.3 0.0.0.0
```

查看 R1 即 HUB 上的 EIGRP 邻居

```
R1#show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(90)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   192.168.1.3             Tu123                    13 00:00:43    5  1470  0  3
0   192.168.1.2             Tu123                    13 01:02:15   21  1470  0  3
R1#
```

明显可以看到 R1 和 R2、R3 分别建立了 EIGRP 邻居。

同时也可以看到 R1 即 HUB 上已获得了去往两个 SPOKE 节点 R2、R3 的 EIGRP 路由

```
R1#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/24 is subnetted, 1 subnets
D        2.2.2.0 [90/27008000] via 192.168.1.2, 01:03:17, Tunnel123
      3.0.0.0/24 is subnetted, 1 subnets
D        3.3.3.0 [90/27008000] via 192.168.1.3, 00:01:47, Tunnel123
R1#
```

再查看两个 SPOKE 节点上的 EIGRP 邻居及路由

```
R2#show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(90)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   192.168.1.1             Tu123                    11 01:05:07   27  1470  0  6
R2#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/27008000] via 192.168.1.1, 01:05:08, Tunnel123
R2#
```

```
R3#show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(90)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   192.168.1.1             Tu123                    11 00:04:11   16  1470  0  6
R3#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/27008000] via 192.168.1.1, 00:04:15, Tunnel123
R3#
```

可以看到两个 SPOKE 节点彼此间并没有建立 EIGRP 邻居关系，仅仅和 HUB 即 R1 建立了 EIGRP 邻居，并且没有学到彼此的环回口路由，这个现象是由 EIGRP 的水平分割引起的，现在 HUB 节点即 R1 上关闭 EIGRP 的水平分割

```
R1(config)#interface tunnel 123
R1(config-if)#no ip split-horizon eigrp 90
R1(config-if)#no shutdown
```

再查看两个 SPOKE 节点 R2、R3 上的 EIGRP 邻居和路由表

```
R2#show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(90)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   192.168.1.1             Tu123                    11 01:09:34   27  1470  0  7
R2#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/27008000] via 192.168.1.1, 01:09:36, Tunnel123
      3.0.0.0/24 is subnetted, 1 subnets
D        3.3.3.0 [90/28288000] via 192.168.1.1, 00:02:24, Tunnel123
R2#
```

```
R3#show ip eigrp neighbor
EIGRP-IPv4 Neighbors for AS(90)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   192.168.1.1             Tu123                    11 00:08:35   17  1470  0  8
R3#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/27008000] via 192.168.1.1, 00:08:39, Tunnel123
      2.0.0.0/24 is subnetted, 1 subnets
D        2.2.2.0 [90/28288000] via 192.168.1.1, 00:02:57, Tunnel123
R3#
```

可以看到，虽然两个 SPOKE 节点 R2、R3 间没有直接建立 EIGRP 邻居，但是学习到了去往对方环回口的路由，但该路由的下一跳地址是 HUB 节点的 Tunnel 口地址，而不是对方的 Tunnel 口地址，现我们再配置如下

```
R1(config)#interface tunnel 123
R1(config-if)#no ip next-hop eigrp 90
R1(config-if)#no shutdown
```

该句的作用是:HUB 节点即 R1 上的 Tunnel 口不能成为 Eigrp 路由的下一跳地址，再查看 R2、R3 的路由表

```
R2#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/27008000] via 192.168.1.1, 00:00:28, Tunnel123
      3.0.0.0/24 is subnetted, 1 subnets
D        3.3.3.0 [90/28288000] via 192.168.1.3, 00:00:28, Tunnel123
R2#
```

发现 SPOKE 节点 R2 上去往另一 SPOKE 节点 R3 的环回口的路由，其下一跳已经由 HUB 节点 R1 的 Tunnel 地址变成了 R3 的 Tunnel 地址。查看 R3，有相同的变化。

```
R3#show ip route eigrp 90
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/27008000] via 192.168.1.1, 00:00:56, Tunnel123
      2.0.0.0/24 is subnetted, 1 subnets
D        2.2.2.0 [90/28288000] via 192.168.1.2, 00:00:56, Tunnel123
R3#
```

5.在 MGRE 的基础上完成 IPSEC 的配置，

①HUB 节点 R1 上的配置

```
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 2
R1(config-isakmp)#exit
R1(config)#
R1(config)#crypto isakmp key cisco address 0.0.0.0
R1(config)#crypto ipsec transform-set DMVPN esp-aes esp-md5-hmac
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#crypto ipsec profile DMVPN_PROFILE
R1(ipsec-profile)#set transform-set DMVPN
R1(ipsec-profile)#exit
R1(config)#interface tunnel 123
R1(config-if)#tunnel protection ipsec profile DMVPN_PROFILE
R1(config-if)#n
*Mar 21 07:09:45.650: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#no shutdo
```

②SPOKE 节点 R2、R3 上的配置

```
R2(config)#crypto isakmp enable
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#encryption aes
R2(config-isakmp)#hash md5
R2(config-isakmp)#group 2
R2(config-isakmp)#exit
R2(config)#crypto isakmp key cisco address 0.0.0.0
R2(config)#crypto ipsec transform-set DMVPN esp-aes esp-md5-hmac
R2(cfg-crypto-trans)#mode transport
R2(cfg-crypto-trans)#exit
R2(config)#crypto ipsec profile DMVPN_PROFILE
R2(ipsec-profile)#set transform-set DMVPN
R2(ipsec-profile)#exit
R2(config)#interface tunnel 123
R2(config-if)#tunnel protection ipsec profile DMVPN_PROFILE
R2(config-if)#no shutdown
```

```
R3(config)#crypto isakmp enable
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption aes
R3(config-isakmp)#hash md5
R3(config-isakmp)#group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key cisco address 0.0.0.0
R3(config)#crypto ipsec transform-set DMVPN esp-aes esp-md5-hmac
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit
R3(config)#crypto ipsec profile DMVPN_PROFILE
R3(ipsec-profile)#set transform-set DMVPN
R3(ipsec-profile)#exit
R3(config)#interface tunnel 123
R3(config-if)#tunnel protection ipsec profile DMVPN_PROFILE
R3(config-if)#no shut
```

注意：在这里采用了 GRE Over IPSEC 的第二种配法，即新式配法。

6.查看 ISAKMP SA 和 IPSEC SA

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
123.1.1.3       123.1.1.1       QM_IDLE           1004 ACTIVE
123.1.1.2       123.1.1.1       QM_IDLE           1002 ACTIVE
123.1.1.1       123.1.1.2       QM_IDLE           1001 ACTIVE
123.1.1.1       123.1.1.3       QM_IDLE           1003 ACTIVE
```

```
R1#show crypto ipsec sa

interface: Tunnel123
    Crypto map tag: Tunnel123-head-0, local addr 123.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (123.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (123.1.1.3/255.255.255.255/47/0)
   current_peer 123.1.1.3 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 123.1.1.1, remote crypto endpt.: 123.1.1.3
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0xDD51140(232067392)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x5C16999B(1544984987)
        transform: esp-aes esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 7, flow_id: SW:7, sibling_flags 80000000, crypto map: Tunnel123-head-0
        sa timing: remaining key lifetime (k/sec): (4304438/3496)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x4D8C0C06(1301023750)
        transform: esp-aes esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 9, flow_id: SW:9, sibling_flags 80004000, crypto map: Tunnel123-head-0
        sa timing: remaining key lifetime (k/sec): (4216947/3501)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

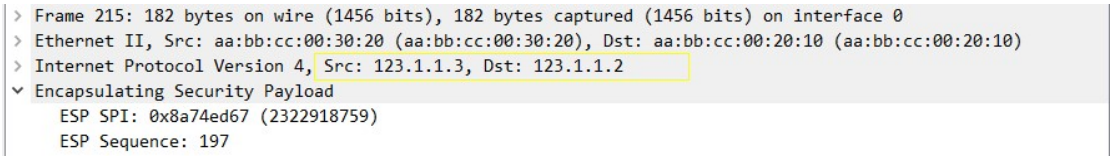
直接测试，并抓包

```
R1#ping 2.2.2.2 source 1.1.1.1 repeat 10000000
Type escape sequence to abort.
Sending 10000000, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

17423	41.926314	123.1.1.2	123.1.1.1	ESP	182	ESP (SPI=0x9c91f24d)
17424	41.930739	123.1.1.1	123.1.1.2	ESP	182	ESP (SPI=0x958ada54)
17425	41.931241	123.1.1.2	123.1.1.1	ESP	182	ESP (SPI=0x9c91f24d)
17426	41.935661	123.1.1.1	123.1.1.2	ESP	182	ESP (SPI=0x958ada54)
17427	41.936147	123.1.1.2	123.1.1.1	ESP	182	ESP (SPI=0x9c91f24d)
17428	41.940560	123.1.1.1	123.1.1.2	ESP	182	ESP (SPI=0x958ada54)
17429	41.941056	123.1.1.2	123.1.1.1	ESP	182	ESP (SPI=0x9c91f24d)
17430	41.945482	123.1.1.1	123.1.1.2	ESP	182	ESP (SPI=0x958ada54)
17431	41.945995	123.1.1.2	123.1.1.1	ESP	182	ESP (SPI=0x9c91f24d)

```
> Frame 22702: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
> Ethernet II, Src: aa:bb:cc:00:10:00 (aa:bb:cc:00:10:00), Dst: aa:bb:cc:00:20:10 (aa:bb:cc:00:20:10)
> Internet Protocol Version 4, Src: 123.1.1.1, Dst: 123.1.1.2
v Encapsulating Security Payload
    ESP SPI: 0x958ada54 (2508905044)
    ESP Sequence: 13197
```

```
R2#ping 3.3.3.3 source 2.2.2.2 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/4/7 ms
R2#
```



明显可以看到三个节点在互访时，都进行了加密，即 DMVPN 配置成功。