```
outbound ah sas:

outbound pcp sas:
```

Erase the startup configuration of the routers and reload them before proceeding to the next lab.

Lab 13-4: Protecting DMVPN Tunnels

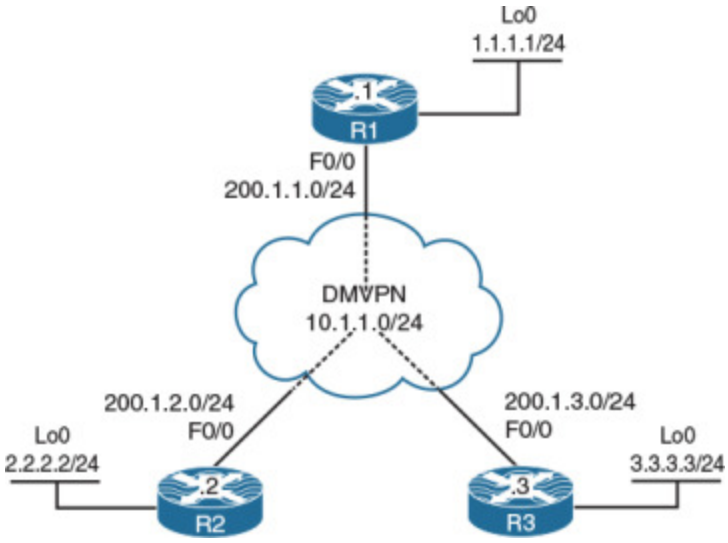

Figure 13-4 *Configuring Protecting DMVPN Tunnels*

Figure 13-4 illustrates the topology that will be used in the following lab.

Task 1

SW1 represents the Internet; configure the ports on the switch based on the following and then enable IP routing:

- **F0/1**: 200.1.1.10/24
- **F0/2**: 200.1.2.10/24
- **F0/3**: 200.1.3.10/24

On SW1:

```
SW1(config)# interface FastEthernet 0/1
SW1(config-if)# no switchport
SW1(config-if)# ip address 200.1.1.10 255.255.255.0
SW1(config-if)# no shutdown

SW1(config)# interface FastEthernet 0/2
SW1(config-if)# no switchport
SW1(config-if)# ip address 200.1.2.10 255.255.255.0
SW1(config-if)# no shutdown
SW1(config)# interface FastEthernet 0/3
SW1(config-if)# no switchport
SW1(config-if)# ip address 200.1.3.10 255.255.255.0
```

```
SW1(config-if)# no shutdown

SW1(config)# ip routing
```

Task 2

Configure the F0/0 and loopback0 interfaces of R1, R2, and R3 based on the configurations shown in Table 13-4.

Table 13-4 *Configurations for Task 2*

Router	Interfaces
R1	loopback0: 1.1.1.1/24 F0/0: 200.1.1.1/24
R2	loopback0: 2.2.2.2/24 F0/0: 200.1.2.2/24
R3	loopback0: 3.3.3.3/24 F0/0: 200.1.3.3/24

Ensure that these routers have full reachability to each other using static routes:

On R1:

```
R1(config)# interface loopback0
R1(config-if)# ip address 1.1.1.1 255.255.255.0

R1(config)# interface FastEthernet 0/0
R1(config-if)# ip address 200.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# ip route 200.1.2.0 255.255.255.0 200.1.1.10
R1(config)# ip route 200.1.3.0 255.255.255.0 200.1.1.10
```

On R2:

```
R2(config)# interface loopback0
R2(config-if)# ip address 2.2.2.2 255.255.255.0

R2(config)# interface FastEthernet 0/0
R2(config-if)# ip address 200.1.2.2 255.255.255.0
R2(config-if)# no shutdown
R2(config)# ip route 200.1.1.0 255.255.255.0 200.1.2.10
R2(config)# ip route 200.1.3.0 255.255.255.0 200.1.2.10
```

On R3:

```
R3(config)# interface loopback 0
R3(config-if)# ip address 3.3.3.3 255.255.255.0
```

```
R3(config)# interface FastEthernet 0/0
R3(config-if)# ip address 200.1.3.3 255.255.255.0
R3(config-if)# no shutdown

R3(config)# ip route 200.1.1.0 255.255.255.0 200.1.3.10
R3(config)# ip route 200.1.2.0 255.255.255.0 200.1.3.10
```

Let's verify the configuration:

On R1:

```
R1# ping 200.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1# ping 200.1.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

On R2:

```
R2# ping 200.1.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Task 3

Configure DMVPN Phase 2 such that R1 is the hub. R2 and R3 should be configured as the spokes. You should use 10.1.1.*x*/24, where *x* is the router number. If this configuration is performed correctly, these routers should have full reachability to all loopback interfaces and tunnel endpoints. You should *not* configure static mappings on the hub router to accomplish this task. Use EIGRP to provide reachability.

On R1:

```
R1(config)# interface tunnel123
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source FastEthernet 0/0
```

```
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# ip nhrp network-id 111
R1(config-if)# ip nhrp map multicast dynamic
```

On R2:

```
R2(config)# interface tunnel123
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source FastEthernet 0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# ip nhrp network-id 222
R2(config-if)# ip nhrp nhs 10.1.1.1
R2(config-if)# ip nhrp map 10.1.1.1 200.1.1.1
```

On R3:

```
R3(config)# interface tunnel123
R3(config-if)# ip address 10.1.1.3 255.255.255.0
R3(config-if)# tunnel source FastEthernet 0/0
R3(config-if)# tunnel mode gre multipoint
R3(config-if)# ip nhrp network-id 333
R3(config-if)# ip nhrp nhs 10.1.1.1
R3(config-if)# ip nhrp map 10.1.1.1 200.1.1.1
```

Let's verify the configuration:

On R1:

```
R1# show ip nhrp

10.1.1.2/32 via 10.1.1.2
  Tunnel123 created 00:03:43, expire 01:56:16
  Type: dynamic, Flags: unique registered
  NBMA address: 200.1.2.2
10.1.1.3/32 via 10.1.1.3
  Tunnel123 created 00:02:18, expire 01:57:41
  Type: dynamic, Flags: unique registered
  NBMA address: 200.1.3.3

R1# 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 Tunnel123 is up/up, Addr. is 10.1.1.1, VRF ""
  Tunnel Src./Dest. addr: 200.1.1.1/MGRE, Tunnel VRF ""
  Protocol/Transport: "multi-GRE/IP", Protect ""
  Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb  Target Network
----- --------------- --------------- ----- -------- ----- ---------------
   1     200.1.2.2       10.1.1.2    UP 00:04:47    D     10.1.1.2/32
   1     200.1.3.3       10.1.1.3    UP 00:03:22    D     10.1.1.3/32

Crypto Session Details:
--------------------------------------------------------------------

Pending DMVPN Sessions:
```

```
R1# ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R1# ping 10.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Now we can run EIGRP:

```
R1(config)# router eigrp 100
R1(config-router)# network 1.1.1.1 0.0.0.0
R1(config-router)# network 10.1.1.1 0.0.0.0

R1(config)# interface tunnel123
R1(config-if)# no ip split-horizon eigrp 100
R1(config-if)# no ip next-hop-self eigrp 100
```

On R2:

```
R2(config)# router eigrp 100
R2(config-router)# network 2.2.2.2 0.0.0.0
R2(config-router)# network 10.1.1.2 0.0.0.0
```

You should see the following console message:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up:
new adjacency

R2(config)# interface tunne123
R2(config-if)# ip nhrp map multicast 200.1.1.1
```

On R3:

```
R3(config)# router eigrp 100
R3(config-router)# network 3.3.3.3 0.0.0.0
R3(config-router)# network 10.1.1.3 0.0.0.0
```

You should also see this console message:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up:  new adjacency

R3(config)# interface tunnel123
R3(config-if)# ip nhrp map multicast 200.1.1.1
```

Let's verify the configuration:

On R2:

```
R2# show ip route eigrp | begin Gate
Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
D       1.1.1.0 [90/27008000] via 10.1.1.1, 00:02:19, Tunnel123
    3.0.0.0/24 is subnetted, 1 subnets
D       3.3.3.0 [90/28288000] via 10.1.1.3, 00:01:31, Tunnel123

R2# ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2# ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Task 4

Protect the traffic between 1.1.1.0/24, 2.2.2.0/24, and 3.3.3.0/24 using an IPSec VPN based on the policy shown in Table 13-5.

Table 13-5 *Policy Guidelines for Configuring Task 4*

ISAKMP Policy	IPSec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Hash: MD5	Hash: ESP-MD5-HMAC
DH Group: 2	Proxy-ID/Crypto ACL: 1.1.1.1 .... 2.2.2.2
Encryption: 3DES	
PSK: cisco	

Let's go through the steps.

First, we begin by configuring IKE Phase 1:

On R1:

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# encryption 3des
```

NOTE The address is set to 0.0.0.0 because the edge devices may acquire different IP addresses, and/or spoke-to-spoke communication may occur between any spokes. Therefore, the IP address *must* be set to 0.0.0.0:

```
R1(config)# crypto isakmp key cisco address 0.0.0.0
```

Now with that done, we can create a transform set based on the requirement in the task:

```
R1(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R1(cfg-crypto-trans)# mode transport
```

Next, we configure crypto ipsec profile to reference the transform set:

```
R1(config)# crypto ipsec profile TST
R1(ipsec-profile)# set transform-set TSET
```

The crypto ipsec profile is configured in the tunnel to protect all traffic traversing the tunnel interface:

```
R1(config)# interface tunnel123
R1(config-if)# tunnel protection ipsec profile TST
```

Once this is configured on R1, you will see that ISAKMP is enabled. Because this is the only site configured, EIGRP neighbor adjacency will be lost to R2 and R3:

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.2 (Tunnel123) is down:
holding time expired

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.3 (Tunnel123) is down:
holding time expired
```

You will also see the following console messages stating that you are receiving packets that are not encrypted:

%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip) vrf/dest_addr= /200.1.1.1, src_addr= 200.1.2.2, prot= 47

On R2:

```
R2(config)# crypto isakmp policy 10
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# encryption 3des

R2(config)# crypto isakmp key cisco address 0.0.0.0

R2(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R2(cfg-crypto-trans)# mode transport

R2(config)# crypto ipsec profile TST
R2(ipsec-profile)# set transform-set TSET

R2(config)# interface tunnel 123
R2(config-if)# tunnel protection ipsec profile TST
```

You should see the following console message:

%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up: new adjacency

On R3:

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# encryption 3des

R3(config)# crypto isakmp key cisco address 0.0.0.0

R3(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R3(cfg-crypto-trans)# mode transport

R3(config)# crypto ipsec profile TST
R3(ipsec-profile)# set transform-set TSET
```

```
R3(config)# interface tunnel 123
R3(config-if)# tunnel protection ipsec profile TST

%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up:
new adjacency
```

Let's verify the configuration:

On R2:

```
R2# show crypto ipsec sa

interface: Tunnel123
    Crypto map tag: Tunnel123-head-0, local addr 200.1.2.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (200.1.1.1/255.255.255.255/47/0)
   current_peer 200.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    # pkts encaps: 176, # pkts encrypt: 176, # pkts digest: 176
    # pkts decaps: 178, # pkts decrypt: 178, # pkts verify: 178
    # 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.: 200.1.2.2, remote crypto endpt.: 200.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0x97BEF376(2545873782)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x7AC150C4(2059489476)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Transport, }
        conn id: 2003, flow_id: NETGX:3, sibling_flags 80000006, crypto map: Tunnel123-head-0
        sa timing: remaining key lifetime (k/sec): (4428305/2843)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
```

```
 inbound pcp sas:

 outbound esp sas:
  spi: 0x97BEF376(2545873782)
    transform: esp-des esp-md5-hmac ,
   in use settings ={Transport, }
    conn id: 2004, flow_id: NETGX:4, sibling_flags 80000006, crypto map: Tunnel123-head-0
    sa timing: remaining key lifetime (k/sec): (4428305/2843)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

 outbound ah sas:

 outbound pcp sas:

protected vrf: (none)
local  ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (200.1.3.3/255.255.255.255/47/0)
current_peer 200.1.3.3 port 500
  PERMIT, flags={origin_is_acl,}
 # pkts encaps: 0, # pkts encrypt: 0, # pkts digest: 0
 # pkts decaps: 0, # pkts decrypt: 0, # pkts verify: 0

 # 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.: 200.1.2.2, remote crypto endpt.: 200.1.3.3
  path mtu 1500, ip mtu 1500, ip mtu idb (none)
  current outbound spi: 0x539AB1EC(1402647020)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0xCC3D2892(3426560146)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Transport, }
    conn id: 2007, flow_id: NETGX:7, sibling_flags 80000006, crypto map: Tunnel123-head-0
    sa timing: remaining key lifetime (k/sec): (4529448/2854)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

  inbound ah sas:
```

```
    inbound pcp sas:

    outbound esp sas:
     spi: 0x539AB1EC(1402647020)
       transform: esp-des esp-md5-hmac ,
       in use settings ={Transport, }
       conn id: 2008, flow_id: NETGX:8, sibling_flags 80000006, crypto map: Tunnel123-head-0
       sa timing: remaining key lifetime (k/sec): (4529448/2854)
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

R2# **show crypto isakmp sa**

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
200.1.2.2       200.1.3.3       QM_IDLE           1003 ACTIVE
200.1.2.2       200.1.1.1       QM_IDLE           1002 ACTIVE
200.1.1.1       200.1.2.2       QM_IDLE           1001 ACTIVE
200.1.3.3       200.1.2.2       QM_IDLE           1004 ACTIVE

IPv6 Crypto ISAKMP SA
```

R2# **ping 3.3.3.3 source loopback0**

```
Type escape sequence to abort.
Sending 5, 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 (5/5), round-trip min/avg/max = 4/4/4 ms
```

R2# **show crypto ipsec sa | include local|remote|#pkts**

```
    Crypto map tag: Tunnel123-head-0, local addr 200.1.2.2
   local  ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (200.1.1.1/255.255.255.255/47/0)
    # pkts encaps: 304, # pkts encrypt: 304, # pkts digest: 304
    # pkts decaps: 306, # pkts decrypt: 306, # pkts verify: 306
    # pkts compressed: 0, # pkts decompressed: 0
    # pkts not compressed: 0, # pkts compr. failed: 0
    # pkts not decompressed: 0, # pkts decompress failed: 0
     local crypto endpt.: 200.1.2.2, remote crypto endpt.: 200.1.1.1
```

```
local  ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (200.1.3.3/255.255.255.255/47/0)
 # pkts encaps: 5, # pkts encrypt: 5, # pkts digest: 5
 # pkts decaps: 5, # pkts decrypt: 5, # pkts verify: 5
 # pkts compressed: 0, # pkts decompressed: 0
 # pkts not compressed: 0, # pkts compr. failed: 0
 # pkts not decompressed: 0, # pkts decompress failed: 0
  local crypto endpt.: 200.1.2.2, remote crypto endpt.: 200.1.3.3
```

Erase the startup configuration of the routers and reload them before proceeding to the next lab.
