



پایاده سازی DMVPN

برای پایاده سازی DMVPN مهمترین ابزار تکنولوژی mGRE است که قابلیت ایجاد اینترفیس های از نوع Multipoint را فراهم می کند. در اینترفیس های تونل Multipoint برخلاف اینترفیس های تونل Point-to-Point آدرس مقصد تونل نامعلوم است

روتر با بکارگیری ابزار دیگری به نام NHRP آدرس فیزیکی روتر مقصد را تشخیص داده و به صورت اتوماتیک و dynamic با مقصد تونل ایجاد می کند. امکان اجرای پروتکل های مسیریابی نیز روی بستر DMVPN وجود دارد که مسیر را به صورت dynamic بین سایت ها جابجا می کند. همچنین می توان از پروتکل IPsec برای امن سازی بستر DMVPN استفاده نمود. بنابراین چهار تکنولوژی mGRE، NHRP، IGP و IPsec در کنار یکدیگر بستری ایده آل و multipoint برای ایجاد ارتباط بین دفاتر یک سازمان با انواع توپولوژی فراهم می کند. در ذیل تعریفی کوتاه از هر یک از تکنولوژی های فوق ارائه شده است.

mGRE اینترفیس تونل از نوع Multipoint که در آن مقصد تونل نامعلوم است. تونل های Point-to-Point به صورت اتوماتیک بعد از استخراج آدرس فیزیکی مقصد ایجاد می گردد.

NHRP: پروتکلی از نوع Client-Server است که آدرس تونل را به آدرس فیزیکی تبدیل می کند. روتر ها در DMVPN با بکارگیری این پروتکل، آدرس فیزیکی مقصد را استخراج نموده و به صورت اتوماتیک تونل از نوع Point-to-Point ایجاد می کنند

IGP: تکنولوژی DMVPN از IGP مستقل است اما با ایجاد IGP روی بستر DMVPN مسیرها به صورت dynamic بین سایت ها جابجا می شود که منجر به مدیریت ساده تر می شود.

IPsec: تکنولوژی DMVPN از IPsec مستقل است. هدف از این پروتکل اختیاری امن سازی بستر DMVPN است که در این فصل به آن پرداخته نمی شود. معمولا بهتر است از این پروتکل استفاده شود

DMVPN انواع توپولوژی ها را در اختیار شما قرار می دهد. توپولوژی Hub-and-Spoke و Spoke-to-Spoke از مهمترین توپولوژی های DMVPN به شمار می آیند. البته در سازمانهای بزرگ پیشنهاد می شود DMVPN را به صورت سلسله مراتبی پایاده سازی نماییم. همچنین پیشنهاد می شود راه حل های افزونگی نیز برای DMVPN دیده شود dual HUB dual و dual HUB single



DMVPN مهمترین راه حل های افزونگی به شمار می آیند. در ادامه همه توپولوژی ها و تکنولوژی های فوق به تفکیک مورد بررسی قرار می گیرند.

طراحی و پیاده سازی Hub-and-Spoke phase 1 DMVPN

در اولین گام در DMVPN به توپولوژی Hub-and-Spoke می پردازیم که اصطلاحاً DMVPN phase 1 نیز نامیده می شود. همانطور که از نام آن پیداست در این روش ارتباطات بین Spoke ها از طریق HUB انجام می گیرد. مزیت اصلی این روش نسبت به مکانیزم Point-to-Point GRE کاهش تعداد تونل در نقطه HUB است.

با توجه به شکل بعد، در طراحی اولیه این روش نکات زیر قابل توجه می باشد:

۱. برای پیاده سازی DMVPN Phase 1 در HUB از GRE و در Spoke ها از Point-to-Point GRE استفاده می شود. تفاوت GRE با mGRE در این است که در GRE مبدا و مقصد تونل مشخص است اما در mGRE مقصد تونل نامعلوم است. آدرس فیزیکی Spoke ها توسط خود mGRE و با کمک NHRP استخراج می شود. بعد از استخراج آدرس فیزیکی Spoke ها، تونل های Point-to-Point به صورت dynamic توسط HUB ایجاد می گردد.
۲. آدرس اینترفیس Tunnel در HUB و Spoke ها از محدوده آدرس ۱۶,۱,۰/۲۴ انتخاب شده است. از آنجایی که دفتر مرکزی و دفاتر تابعه از طریق یک ابر مشترک DMVPN به هم متصل هستند، بنابراین محدوده آدرس اینترفیس Tunnel در همه روترها یکسان است.
۳. روتر HUB را به عنوان NHRP Server و روترهای Spoke را به عنوان NHRP Client معرفی می کنیم. وظیفه پروتکل NHRP تبدیل آدرس Tunnel به آدرس فیزیکی روتر است. نگاشت آدرس اینترفیس Tunnel به آدرس فیزیکی روتر HUB را به صورت دستی روی روترهای Spoke وارد می نماییم. روترهای Spoke نیز هر یک مستقلاً آدرس فیزیکی و آدرس اینترفیس Tunnel خود را به NHRP Server اعلام می کنند. بنابراین در روتر HUB جدولی به نام **NHRP Table** ایجاد خواهد شد که معادل آدرس فیزیکی آدرس تونل روترهای Spoke در آن ذخیره می گردد. کاربرد این جدول را در ادامه متوجه خواهیم شد. نمونه ای از جدول NHRP در ذیل نشان داده است که در آن معادل آدرس ۱۶,۱,۱ آدرس فیزیکی ۱۲,۱,۱,۲ و معادل آدرس ۱۷۲,۱۶,۱,۲ آدرس فیزیکی ۱۲,۱,۲,۲ تعیین شده است.



172.16.1.1/32 via 172.16.1.1

Tunnel0 created 00:00:27, expire 01:59:56

Type: dynamic, Flags: unique registered used nhop

NBMA address: 12.1.1.2

!

172.16.1.2/32 via 172.16.1.2

Tunnel0 created 00:11:09, expire 01:48:50

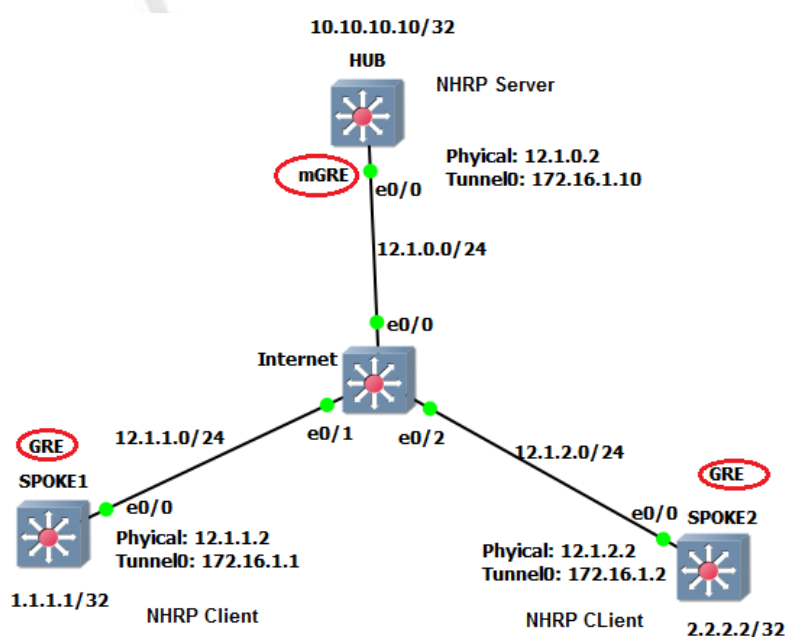
Type: dynamic, Flags: unique registered used nhop

NBMA address: 12.1.2.2

۴. پیکربندی 1- Error! No text of specified style in document. خروجی جدول

NHRP برای تبدیل آدرس تونل به آدرس فیزیکی

۵. پروتکل DMVPN به پروتکل مسیریابی وابسته نیست و استفاده از هر یک از پروتکل های مسیریابی از جمله Static، پروتکل های IGP و یا پروتکل BGP در DMVPN مجاز است. روش پیشنهادی سیستم پروتکل EIGRP است. در ادامه ابتدا به روش Static و سپس به ترتیب EIGRP و OSPF را در DMVPN محک خواهیم زد.



پایاده سازی 1 DMVPN Phase 1 با توپولوژی Hub-and-Spoke



جریان برقراری ارتباط در DMVPN چگونه است؟

۱. ابتدا مسیر شبکه های متصل به هر Spoke توسط روتر Spoke و روی اینترنت فیس Tunnel به روتر HUB یاد داده می شود. اگر به خاطر داشته باشید از قبل روی روترهای Spoke تونل GRE با مقصد HUB ایجاد شده است. پروتکل های مسیریابی در روترهای Spoke مسیر شبکه متصل به خود را روی تونل ایجاد شده به روتر HUB یاد می دهند. بنابراین روتر HUB مسیر شبکه متصل به روترهای Spoke را از طریق تونل یاد می گیرد. تاکید می شود که آدرس next-hop در روتر HUB برای شبکه های متصل به Spoke، آدرس اینترنت فیس تونل روتر Spoke است. ما در این سناریو و در گام اول مسیرها را به صورت دستی در روتر HUB و Spoke ایجاد کرده ایم. در مراحل بعدی EIGRP و OSPF را نیز اجرا خواهیم نمود

!!! HUB

```
ip route 1.1.1.1 255.255.255.255 172.16.1.1
```

```
ip route 2.2.2.2 255.255.255.255 172.16.1.2
```

۲. آدرس next-hop مسیر شبکه های متصل به Spoke به آدرس تونل روترهای Spoke اشاره می کند

۳. روتر HUB با توجه به جدول NHRP آدرس فیزیکی معادل آدرس تونل روترهای Spoke را استخراج می کند. حتما به خاطر دارید که هر روتر Spoke، نگاشت بین آدرس فیزیکی و آدرس تونل خود را قبلا در اختیار روتر HUB قرار داده است. در ذیل خروجی جدول NHRP در روتر HUB نشان داده شده است. همانطور که مشاهده می کنید روتر HUB معادل آدرس فیزیکی آدرس تونل هر یک از Spoke ها را در جدول NHRP در اختیار دارد.

```
172.16.1.1/32 via 172.16.1.1
```

```
Tunnel0 created 00:00:27, expire 01:59:56
```

```
Type: dynamic, Flags: unique registered used nhop
```

```
NBMA address: 12.1.1.2
```

!

```
172.16.1.2/32 via 172.16.1.2
```

```
Tunnel0 created 00:11:09, expire 01:48:50
```



Type: dynamic, Flags: unique registered used nhop

NBMA address: 12.1.2.2

۴. جدول NHRP در روتر HUB

۵. ساختار بسته nhrp request و nhrp reply در شکل زیر نشان داده شده است. بسته nhrp روی تونل GRE سوار می شود. همانطور که مشاهده می کنید در بسته nhrp request آدرس تونل داده می شود و آدرس فیزیکی درخواست می گردد.

No.	Time	Source	Destination	Protocol	Length	Info
28	48.9132110	12.1.1.2	12.1.0.2	NHRP	121	NHRP Registration Request, ID=3
29	49.0467280	12.1.0.2	12.1.1.2	NHRP	141	NHRP Registration Reply, ID=3, Code=Success

Frame 28: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface 0

- Cisco HDLC
- Internet Protocol Version 4, Src: 12.1.1.2 (12.1.1.2), Dst: 12.1.0.2 (12.1.0.2)
- Generic Routing Encapsulation (NHRP)
- Next Hop Resolution Protocol (NHRP Registration Request)
 - NHRP Fixed Header
 - NHRP Mandatory Part
 - Source Protocol Len: 4
 - Destination Protocol Len: 4
 - Flags: 0x8000
 - Request ID: 0x00000003 (3)
 - Source NBMA Address: 12.1.1.2 (12.1.1.2)
 - Source Protocol Address: 172.16.1.2 (172.16.1.2)
 - Destination Protocol Address: 172.16.1.10 (172.16.1.10)
 - Client Information Entry
 - Responder Address Extension
 - Forward Transit NHS Record Extension
 - Reverse Transit NHS Record Extension
 - NHRP Authentication Extension
 - End of Extension

۶.

۷. ساختار بسته NHRP Request و NHRP Reply

۸. روتر HUB با توجه به آدرس فیزیکی روتر Spoke که از جدول NHRP استخراج شده است، به صورت اتوماتیک تونل GRE از نوع Point-to-Point به مقصد آدرس فیزیکی روتر های Spoke ایجاد می کند. همانطور که می دانید روی روتر HUB قبلاً تونل از نوع GRE ایجاد شده است که مقصد آن نامعلوم است. در پایان این فاز روتر Hub با تمام روتر های Spoke تونل Point-to-Point GRE ایجاد می کند. تونل های ایجاد شده توسط دستور show dmvpn قابل مشاهده است که در ذیل نشان داده شده است.



```
HUB#sh 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:2,

```
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
```

```
-----
```

```
1 12.1.1.2          172.16.1.1  UP 00:00:39  D
```

```
1 12.1.2.2          172.16.1.2  UP 00:11:45  D
```

۹. تونل های ایجاد شده به صورت dynamic در روتر HUB

۱۰. روتر HUB مسیر یاد گرفته شده از هر یک از روترهای Spoke را به دیگر روترهای Spoke روی تونل GRE که در مرحله قبل ایجاد شده است، یاد می دهد. از دید Spoke مسیر رسیدن به شبکه های متصل به دیگر روترهای Spoke روتر HUB است. بنابراین ترافیک بین روترهای Spoke از طریق روتر HUB جابجا می شود. در اولین بخش از اجرای این سناریو مسیریابی به صورت دستی انجام شده است اما در ادامه پروتکل OSPF و EIGRP را جایگزین روش دستی خواهیم نمود.

```
!!! SPOKE1
```

```
ip route 2.2.2.2 255.255.255.255 tunnel0 172.16.1.10
```

```
ip route 10.10.10.10 255.255.255.255 tunnel0 172.16.1.10
```

```
!
```


**!!! SPOKE2**

```
ip route 1.1.1.1 255.255.255.255 tunnel0 172.16.1.10  
ip route 10.10.10.10 255.255.255.255 tunnel0 172.16.1.10
```

۱۱. مسیر روترهای Spoke به یکدیگر با واسطه روتر HUB

۱۲. در ذیل نشان داده شده است که ترافیک ما بین روترهای Spoke از HUB عبور می کند.

SPOKE1#traceroute 10.10.10.10

```
Type escape sequence to abort.  
Tracing the route to 10.10.10.10  
VRF info: (vrf in name/id, vrf out name/id)  
 1 172.16.1.10 12 msec 6 msec 5 msec  
!
```

SPOKE1#traceroute 2.2.2.2

```
Type escape sequence to abort.  
Tracing the route to 2.2.2.2  
VRF info: (vrf in name/id, vrf out name/id)  
 1 172.16.1.10 13 msec 7 msec 5 msec  
 2 172.16.1.2 7 msec 9 msec 4 msec
```

۱۳. در 1 DMVPN Phase ترافیک بین Spoke ها از HUB عبور می کند

با توجه به شکل و توضیحات فوق، چگونگی پیاده سازی 1 DMVPN Phase در ذیل آمده است.

۱. ابتدا روی روتر HUB ایتترفیس Tunnel از نوع mGRE و روی روترهای Spoke ایتترفیس Tunnel از نوع GRE پیاده سازی می شود. همانطور که قبلاً گفته شده است در mGRE مقصد Tunnel نامعلوم است اما در GRE مقصد Tunnel از قبل توسط مدیر شبکه تنظیم می شود. در این سناریو tunnel checksum و tunnel key روی ایتترفیس Tunnel فعال شده است و به همین دلیل مقدار MTU معادل ۱۴۶۸ در نظر گرفته شده است. امکان فعال سازی tunnel sequence و



keepalive روی اینترنت فیس های mGRE وجود ندارد. Keepalive روی روترهای Spoke فعال شده است.

۲. ویژگی های اختیاری authentication و checksum با دستورات tunnel key و tunnel checksum در اینترنت فیس Tunnel در همه روترهای HUB و Spoke فعال می گردد. بدین ترتیب با احتساب ۲۰ بایت سر بار IP و ۴ بایت سر بار ثابت GRE، مجموعاً ۳۲ بایت سر بار به ترافیک IP اضافه می گردد. بنابراین MTU اینترنت فیس های Tunnel عددی ۱۴۶۸ در نظر گرفته شده است. لازم به ذکر است با توجه به اینکه tunnel sequence قابل فعال سازی روی اینترنت فیس mGRE نیست این ویژگی روی هیچ یک از روترهای Hub و یا Spoke فعال نشده است.

۳. روی روترهای Spoke با دستور **keepalive 5 15** ویژگی keep-alive را روی اینترنت فیس Tunnel فعال می کنیم. بنابراین چنانچه اینترنت فیس Tunnel در روتر HUB با مشکلی مواجه شود، به صورت اتوماتیک اینترنت فیس Tunnel در روترهای Spoke به down تغییر حالت خواهند داد. در خصوص چگونگی مکانیزم keepalive در GRE به اندازه کافی بحث شده است. ویژگی keep-alive نمی توان روی اینترنت فیس های mGRE در Hub فعال نمود که البته خیلی هم مهم نیست که روتر Hub، down شدن تونل spoke را متوجه شود.

!!! HUB

```
interface Tunnel0
ip address 172.16.1.10 255.255.255.0
no ip redirects
ip mtu 1468
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 123
tunnel checksum
```

!

!!! Spoke1

```
interface Tunnel0
ip address 172.16.1.1 255.255.255.0
```




```
ip mtu 1468
```

```
keepalive 5 15
```

```
tunnel source Ethernet0/0
```

```
tunnel destination 12.1.0.2
```

```
tunnel key 123
```

```
tunnel checksum
```

۱. پیاده سازی mGRE Tunnel در HUB و GRE Tunnel در روترهای Spoke در Phase 1 DMVPN

۲. در مرحله دوم روتر HUB را به عنوان NHRP Server و روترهای Spoke را به عنوان NHRP Client معرفی می کنیم. پیاده سازی NHRP Server و NHRP Client در ذیل نشان داده شده است. دستور **ip nhrp authentication** برای احراز هویت nhrp server و nhrp client به یکدیگر است. دستور **ip nhrp network-id** محدوده عملکردی پروتکل NHRP را تعیین می کند و باید بین همه server ها و client های یک دامنه یکسان باشد. دستور **ip nhrp map multicast dynamic** مهمترین دستور nhrp server است که باعث ایجاد جدول NHRP به صورت dynamic در روتر nhrp server می شود. در روترهای nhrp client علاوه بر فعال کردن nhrp authentication و nhrp network-id نگاشت آدرس فیزیکی به آدرس Tunnel روتر nhrp server را روی روترهای nhrp client ایجاد می کنیم. دستور **ip nhrp nhs** آدرس nhrp server را تعیین می کند. با دستور **ip nhrp map** نگاشت آدرس تونل به آدرس فیزیکی روتر HUB را به صورت دستی انجام می دهیم. دستور **ip nhrp map multicast** آدرس فیزیکی روتر hub را تعیین می کند که ترافیک broadcast و multicast ارسالی به مقصد hub به این آدرس ارسال می گردد.

!!! HUB

```
interface Tunnel0
```

```
ip nhrp authentication Javan
```

```
ip nhrp map multicast dynamic
```

```
ip nhrp network-id 1234
```

```
!
```



!!! SPOKE

```
interface Tunnel0
ip nhrp authentication Javan
ip nhrp map 172.16.1.10 12.1.0.2
ip nhrp map multicast 12.1.0.2
ip nhrp network-id 1234
ip nhrp nhs 172.16.1.10
```

۳. پیاده سازی NHRP Server در HUB و NHRP Client در Spoke ها

۲. DMVPN مستقل از پروتکل مسیریابی است. به همین دلیل در اولین گام پیاده سازی DMVPN با ایجاد مسیرهای Static نشان داده شده است.

!!! HUB

```
ip route 1.1.1.1 255.255.255.255 tunnel0 172.16.1.1
ip route 2.2.2.2 255.255.255.255 tunnel0 172.16.1.2
```

!

!!! SPOKE

```
ip route 2.2.2.2 255.255.255.255 tunnel0 172.16.1.10
ip route 10.10.10.10 255.255.255.255 tunnel0 172.16.1.10
```

!

!!! SPOKE2

```
ip route 1.1.1.1 255.255.255.255 tunnel0 172.16.1.10
ip route 10.10.10.10 255.255.255.255 tunnel0 172.16.1.10
```

۳. چگونگی ایجاد مسیر Static در DMVPN Phase 1

۴. پیکربندی نهایی روترهای HUB و Spoke با توجه به شکل قبل در ذیل آمده است.

!!! HUB

```
interface Loopback0
ip address 10.10.10.10 255.255.255.255
```



```
!  
interface eth0/0  
  no shut  
  ip address 12.1.0.2 255.255.255.0  
!  
ip route 0.0.0.0 0.0.0.0 12.1.0.1  
!  
interface Tunnel0  
  ip address 172.16.1.10 255.255.255.0  
  no ip redirects  
  ip mtu 1468  
  ip nhrp authentication Javan  
  ip nhrp map multicast dynamic  
  ip nhrp network-id 1234  
  no ip route-cache  
  tunnel source Ethernet0/0  
  tunnel mode gre multipoint  
  tunnel key 123  
  tunnel checksum  
!  
ip route 1.1.1.1 255.255.255.255 172.16.1.1  
ip route 2.2.2.2 255.255.255.255 172.16.1.2  
!  
!!! SPOKE1  
interface Tunnel0  
  ip address 172.16.1.1 255.255.255.0  
  ip mtu 1468
```



```
ip nhrp authentication Javan
ip nhrp map 172.16.1.10 12.1.0.2
  ip nhrp map multicast 12.1.0.2
ip nhrp network-id 1234
  ip nhrp nhs 172.16.1.10
  no ip route-cache
keepalive 5 15
  tunnel source Ethernet0/0
  tunnel destination 12.1.0.2
  tunnel key 123
tunnel checksum
!
ip route 2.2.2.2 255.255.255.255 172.16.1.10
ip route 10.10.10.10 255.255.255.255 172.16.1.10
!
!!! SPOKE2
interface Loopback0
  ip address 2.2.2.2 255.255.255.255
!
interface eth0/0
  no shut
  ip address 12.1.2.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 12.1.2.1
!
interface Tunnel0
  ip address 172.16.1.2 255.255.255.0
```



```
ip mtu 1468
ip nhrp authentication Javan
ip nhrp map 172.16.1.10 12.1.0.2
ip nhrp map multicast 12.1.0.2
ip nhrp network-id 1234
ip nhrp nhs 172.16.1.10
no ip route-cache
keepalive 5 15
tunnel source Ethernet0/0
tunnel destination 12.1.0.2
tunnel key 123
tunnel checksum
!
ip route 1.1.1.1 255.255.255.255 172.16.1.10
ip route 10.10.10.10 255.255.255.255 172.16.1.10
```

۵. پیکربندی نهایی 1 DMVPN Phase

۶. در سناریوی فوق 1 DMVPN Phase با روش مسیریابی Static پیاده سازی شده است. به این دلیل که خواستیم نشان دهیم DMVPN به پروتکل مسیریابی وابسته نیست. اما قصد داریم در ادامه نشان دهیم که در صورت اجرای پروتکل EIGRP و یا OSPF روی 1 DMVPN Phase چه نکاتی را باید مورد توجه قرار دهیم. توجه کنید که این نکات لزوماً در 2 DMVPN phase و یا 3 DMVPN phase صحیح نیستند.

۷. در صورت اجرای پروتکل EIGRP در 1 DMVPN phase فقط کافی است به نکته زیر توجه کنید.

- روتر HUB روی همان اینترفیسی که مسیر شبکه های متصل به Spoke را یاد می گیرد (اینترفیس mGRE)، مجدداً روی همان اینترفیس مسیر یاد گرفته شده را به دیگر روترهای Spoke یاد می دهد. برای محقق شدن این سناریو لازم است تا Split Horizon را روی اینترفیس mGRE در روتر HUB غیر فعال نماییم.



پیاده سازی EIGRP در 1 phase DMVPN به همراه نتایج آن در ذیل نشان داده شده است. خروجی جدول مسیریابی Spoke نشان می دهد که ترافیک به مقصد Spoke دوم از روتر HUB عبور می کند.

```
!  
!!! HUB  
router eigrp 1  
network 10.10.10.10 0.0.0.0  
network 172.16.1.0 0.0.0.255  
!  
interface Tunnel0  
no ip split-horizon eigrp 1  
!  
!!! SPOKE1  
router eigrp 1  
network 1.1.1.1 0.0.0.0  
network 172.16.1.0 0.0.0.255  
!  
!!! SPOKE2  
router eigrp 1  
network 2.2.2.2 0.0.0.0  
network 172.16.1.0 0.0.0.255  
!  
HUB(config-if)#do sh ip eigrp neigh  
EIGRP-IPv4 Neighbors for AS(1)  
H  Address                Interface          Hold Uptime  SRTT  RTO  Q  Seq  
                                (sec)         (ms)          Cnt  Num  
1  172.16.1.2              Tu0               11 00:00:11   9 1464 0 3  
0  172.16.1.1              Tu0               10 00:00:44  44 1464 0 4
```




```
!
SPOKE1(config-router)#do sh ip eigrp neigh
EIGRP-IPv4 Neighbors for AS(1)
H  Address          Interface          Hold Uptime  SRTT  RTO  Q  Seq
                               (sec)         (ms)    Cnt  Num
0  172.16.1.10        Tu0                13 00:01:13  17  1464  0  6
!
SPOKE1(config-router)#do sh ip route eigrp
!!! بخشی از خروجی حذف شده است
    2.0.0.0/32 is subnetted, 1 subnets
D      2.2.2.2 [90/28288000] via 172.16.1.10, 00:00:51, Tunnel0
    10.0.0.0/32 is subnetted, 1 subnets
D     10.10.10.10 [90/27008000] via 172.16.1.10, 00:01:24, Tunnel0
```

پیکربندی پیاده سازی EIGRP در DMVPN Phase 1

برای پیاده سازی OSPF در DMVPN phase 1 ضروری است تا از OSPF با نوع شبکه broadcast و non-broadcast استفاده نشود. به این دلیل که در DMVPN phase 1 حتما روترهای Spoke باید ترافیک را از طریق روتر HUB به دیگر روترهای Spoke ارسال نمایند. در صورت استفاده از یکی از دو نوع broadcast و یا non-broadcast روتر HUB نقش DR را خواهد داشت و روتر DR مسیر Spoke ها را به دیگر Spoke ها بدون تغییر next-hop می دهد که در این صورت ترافیک بین Spoke ها از روتر HUB جابجا نخواهد شد. در DMVPN phase 2 خواهیم دید که بر خلاف phase 1 باید از نوع شبکه broadcast و یا non-broadcast استفاده شود تا Spoke ها به طور مستقیم با هم در ارتباط باشند. در این سناریو نوع شبکه پروتکل OSPF، point-to-multipoint، ایترنیتیس Tunnel روترهای HUB و Spoke در نظر گرفته شده است.

!!! HUB

```
router ospf 1
router-id 10.10.10.10
```



```
network 10.10.10.10 0.0.0.0 area 0
network 172.16.0.0 0.0.255.255 area 0
!
HUB(config)#interface tunnel 0
HUB(config-if)#ip ospf network point-to-multipoint
!
!!! SPOKE1
router ospf 1
router-id 1.1.1.1
network 1.1.1.1 0.0.0.0 area 0
network 172.16.0.0 0.0.255.255 area 0
!
SPOKE1(config)#interface tunnel 0
SPOKE1(config-if)#ip ospf network point-to-multipoint
!
!!! SPOKE2
router ospf 1
router-id 2.2.2.2
network 2.2.2.2 0.0.0.0 area 0
network 172.16.0.0 0.0.255.255 area 0
!
SPOKE1(config)#interface tunnel 0
SPOKE1(config-if)#ip ospf network point-to-multipoint
```

پایاده سازی OSPF در DMVPN Phase 1 که حتما باید از نوع point-to-multipoint باشد خروجی جدول مسیریابی روتر Spoke نشان می دهد که ترافیک به مقصد دیگر Spoke ها از روتر HUB عبور می کند.

```
HUB#sh ip ospf neighbor
```



```
Neighbor ID  Pri  State          Dead Time  Address    Interface
2.2.2.2      0    FULL/ -        00:01:58   172.16.1.2  Tunnel0
1.1.1.1      0    FULL/ -        00:01:46   172.16.1.1  Tunnel0
!
```

```
SPOKE1#sh ip route ospf
```

!!! بخشی از خروجی حذف شده است

2.0.0.0/32 is subnetted, 1 subnets

O 2.2.2.2 [110/2001] via 172.16.1.10, 00:01:04, Tunnel0

10.0.0.0/32 is subnetted, 1 subnets

O 10.10.10.10 [110/1001] via 172.16.1.10, 00:01:29, Tunnel0

172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks

O 172.16.1.2/32 [110/2000] via 172.16.1.10, 00:01:04, Tunnel0

O 172.16.1.10/32 [110/1000] via 172.16.1.10, 00:01:29, Tunnel0

خروجی OSPF و جدول مسیریابی در Phase 1 DMVPN

نکته مهمی که در مسیریابی Phase 1 DMVPN وجود دارد اینکه روترهای Spoke همواره ترافیک را از مسیر HUB به دیگر Spoke ها ارسال می کنند. این بدان معنی است که روتر HUB می تواند به جای ارسال مسیر شبکه های متصل به همه روترهای Spoke فقط مسیر خلاصه شده و یا مسیر default را به روترهای Spoke ارسال نماید.