

MDS VPN Phase3 multi-subnetontwerp implementeren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Probleemgegevens](#)

[Oplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft routingsoverwegingen in een DMVPN fase3 multi-subnetontwerp om ervoor te zorgen dat direct spraaktunnels correct worden gebouwd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- [Basiskennis van Dynamic Multipoint VPN \(DMVPN\)](#)
- [Basiskennis van Next-Hop Resolution Protocol \(NHRP\)](#)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

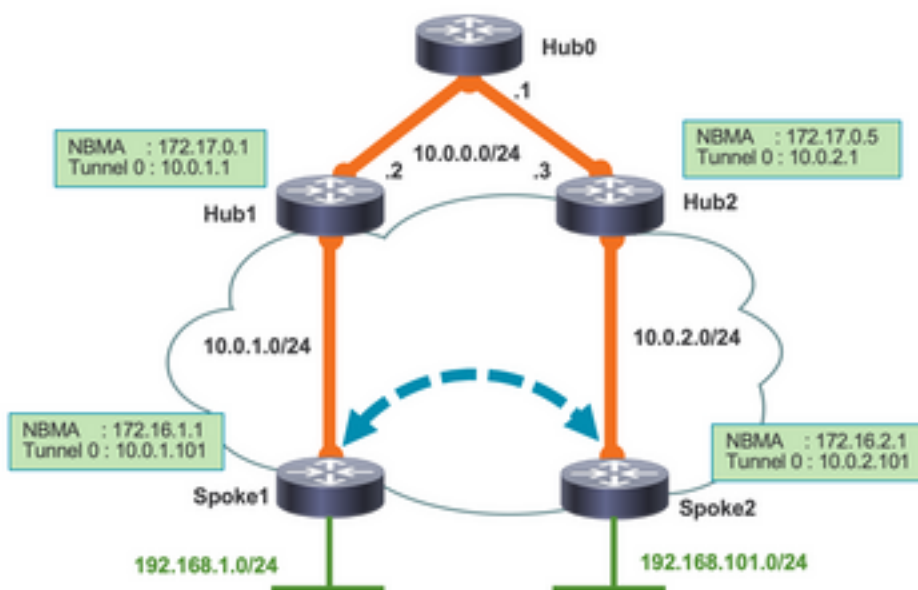
Achtergrondinformatie

Zowel DMVPN fase2 als fase3 implementaties laten een spraakapparaat toe om een directe spraaktunnel te bouwen en hoeven niet door de hub te gaan. Echter, DMVPN fase3 biedt veel betere schaalbaarheid door met het NHRP omleiden mechanisme voor de spaak om de externe netwerken dynamisch te ontdekken via NHRP, en vervolgens te installeren NHRP (H) routes in de routing tabel. Dit verwijdert de fase2 beperking van het vereisen van elke spoke om specifieke

netwerkprefixes te hebben voor de externe netwerken in zijn Routing Table. Bij fase 3 moet het NHRP Resolution Reply van de target spoke (NBMA exit point) over de directe spoke-to-spoke-tunnel gaan. Echter, speciale aandacht moet worden gegeven aan een multi-subnetfase3 ontwerp, zodat de spaak-spaak tunnel correct kan worden gebouwd. In dit artikel worden deze vereisten in detail besproken.

Probleem

DMVPN fase3 kan worden geïmplementeerd in één subnetoverlay of in multi-subnetoverlay. In een single-subnetoverlay-topologie worden de hub en alle spraakroutertunneladressen toegewezen uit één logische IP-subnetverbinding; terwijl in een multi-subnetontwerp spaaktunnelverbindingen moeten worden gemaakt voor spaken met hun tunneladressen in verschillende IP-subnetten. Dit laatste is een veelvoorkomend scenario dat wordt gebruikt in een hiërarchisch DMVPN-ontwerp dat in de onderstaande afbeelding wordt getoond.



DMVPN Phase3 multi-subnettopologie

Probleemgegevens

Met DMVPN fase3, wordt algemeen begrepen dat wanneer het NHRP Resolutieverzoek wordt ontvangen, het doel spaak de IPsec tunnel aan de bron spaak in werking stelt, en daarna, verzendt het Resolutiereactie over die tunnel. Dit is echter alleen het geval bij één subnetoverlay. Wanneer de spokes' tunnelinterfaces in verschillende IP logische subnetten zijn, kunnen de NHRP controlepakketten via de spaak-hub-spaak weg in plaats van met de directe spaak-spaak tunnel oversteken. Dit is de volgorde van gebeurtenissen wanneer Spoke1 een Resolutieverzoek naar Spoke2 stuurt nadat het een NHRP-doorverwijzing van Hub1 ontvangt:

1. Spoke2 ontvangt een verzoek voor een oplossing

```
*Feb 7 20:57:22.272: NHRP: Receive Resolution Request via Tunnel0 vrf global(0x0), packet size: 144
*Feb 7 20:57:22.272: (F) afn: AF_IP(1), type: IP(800), hop: 252, ver: 1
*Feb 7 20:57:22.272: sht1: 4(NSAP), sst1: 0(NSAP)
```

```

*Feb 7 20:57:22.272:      pktsz: 144 extoff: 52
*Feb 7 20:57:22.272: (M) flags: "router auth src-stable nat ", reqid: 5
*Feb 7 20:57:22.272:      src NBMA: 172.16.1.1
*Feb 7 20:57:22.272:      src protocol: 10.0.1.101, dst protocol: 192.168.101.1
*Feb 7 20:57:22.272: (C-1) code: no error(0)
*Feb 7 20:57:22.272:      prefix: 32, mtu: 17912, hd_time: 900
*Feb 7 20:57:22.272:      addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref:
255

```

2. Spoke2 voegt een impliciete NHRP cacheingang voor 10.0.1.101 toe door het pakket van het Resolutieverzoek te snuiven.
3. Spoke2 voegt een nabijheid toe voor 10.0.1.101 voor Tunnel0 met het NBMA-adres van Spoke1.
4. Spoke2 reageert met Resolutiereactie. Bericht op dit punt, de route voor de het vragen spraaktunneladressen aan Hub2:

```

Spoke2#show ip route 10.0.1.101
Routing entry for 10.0.1.0/24
  Known via "eigrp 1", distance 90, metric 3609600, type internal
  Redistributing via eigrp 1
  Last update from 10.0.2.1 on Tunnel0, 00:17:44 ago
  Routing Descriptor Blocks:
  * 10.0.2.1, from 10.0.2.1, 00:17:44 ago, via Tunnel0
    Route metric is 3609600, traffic share count is 1
    Total delay is 41000 microseconds, minimum bandwidth is 1000 Kbit
    Reliability 255/255, minimum MTU 1400 bytes
    Loading 1/255, Hops 3
Spoke2#
Spoke2#
Spoke2#show ip cef 10.0.1.101
10.0.1.0/24
  nexthop 10.0.2.1 Tunnel0

```

Aangezien het NHRP Control Packet wordt doorgestuurd langs het gerouteerde pad, wordt het verzonden naar Hub2 in plaats van de nieuw gecreëerde spaak-spaak-tunnel naar Spoke1:

```

*Feb 7 20:57:22.360: NHRP: Send Resolution Reply via Tunnel0 vrf global(0x0), packet size:
172
*Feb 7 20:57:22.360:      src: 10.0.2.101, dst: 10.0.1.101
*Feb 7 20:57:22.360: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 7 20:57:22.360:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 7 20:57:22.360:      pktsz: 172 extoff: 60
*Feb 7 20:57:22.360: (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 5
*Feb 7 20:57:22.360:      src NBMA: 172.16.1.1
*Feb 7 20:57:22.360:      src protocol: 10.0.1.101, dst protocol: 192.168.101.1
*Feb 7 20:57:22.360: (C-1) code: no error(0)
*Feb 7 20:57:22.360:      prefix: 24, mtu: 17912, hd_time: 900
*Feb 7 20:57:22.360:      addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref:
255
*Feb 7 20:57:22.360:      client NBMA: 172.16.2.1
*Feb 7 20:57:22.360:      client protocol: 10.0.2.101
*Feb 7 20:57:22.360: NHRP: Encapsulation succeeded. Sending NHRP Control Packet NBMA
Address: 172.17.0.5

```

In theorie, zolang alle tussenliggende hub(s) het NHRP-regelpakket terug kan leiden naar de

tunnel van Spoke1, dan moet alles nog werken. Maar dit is niet altijd het geval. Als het antwoord op de resolutie niet kan worden doorgestuurd naar Spoke1, dan kan de directe spaak-spraak-tunnel niet worden gebouwd.

Met één subnetoverlay is dit geen probleem omdat elke spaak een direct verbonden route heeft naar het tunnelnetwerk. Dit resulteert in een nabijheidsraadpleging voor het vragende spraaktunneladres alvorens het Resolutiereactie wordt teruggestuurd. In een multi-subnetoverlay-netwerk, omdat de spokes-tunneladressen niet op hetzelfde IP-subnetnummer staan, is het niet gegarandeerd dat het Resolution Reply-pakket wordt verzonden over de directe spaak-to-spraak-tunnel.

Oplossing

Voor een multi-subnet DMVPN fase3 ontwerp, wordt het aanbevolen voor een spoke om een routingingang te hebben die de tunnelinterface aanwijst voor om het even welke ver spraaktunnelsubnet waaraan het moet bouwen direct spraaktunnel. Voorbeeld:

```
Spoke2#show run | in ip route
ip route 10.0.101.0 255.255.255.0 Tunnel0
```

Hierdoor kan de spaak proberen de nabijheid voor het vragende spraaktunneladres op te lossen en vervolgens de resolutie antwoord over de spraaktunnel sturen.

Een andere mogelijkheid is dat het antwoord op de resolutie de spaak-spraak-tunnels kan doorkruisen. In een dergelijk geval moeten alle tussenliggende hub(s) een route naar het vragende spraaktunnelsubnet hebben om te garanderen dat de NHRP-controlepakketten van begin tot eind kunnen worden geleverd.

Opmerking: er is een bugverbetering geopend om de mogelijkheden te verkennen om het Resolutiereactie over de directe tunnel te laten versturen, zelfs zonder een expliciete statische route. Cisco bug-id [CSCvo0202](#) - Verbetering: NHRP moet oplossingsantwoord sturen via spraaktunnelondersteuning voor multi-subnet DMVPN.

Opmerking: alleen geregistreerde Cisco-clients hebben toegang tot interne Cisco-bug-informatie en -tools.

Gerelateerde informatie

- [Cisco technische ondersteuning en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.