

Problemen met omleiding van DMVPN Phase3 NHRP oplossen

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Probleem](#)

[NHRP controle pakketten throttling](#)

[Oplossing](#)

[Identificeer de bron van de doorverwijzing](#)

[Afstemming van de punt-policer-drempel](#)

[De NHRP max-verzenddrempel instellen](#)

Inleiding

Dit document beschrijft hoe DMVPN Phase3, NHRP Redirect een sleutelfunctie is die een spaak router toestaat om directe weg aan een ander spaak apparaat te ontdekken.

Achtergrondinformatie

Om de spoke to spoke-tunnel te kunnen bouwen, moet de Dynamic Multipoint Virtual Private Network (DMVPN) hub een Next Hop Resolution Protocol (NHRP) kunnen genereren die de besturingspakket vanuit het dataplatform omleidt, en dit vervolgens doorsturen naar het spoke-apparaat. In sommige situaties, moet sommige tuning worden uitgevoerd voor dit om in een grote DMVPN plaatsing te werken, en dit artikel bespreekt sommige van deze overwegingen.

Probleem

NHRP controle pakketten throttling

In een grootschalige omgeving moet een DMVPN-hub veel NHRP-omleidingspakketten verwerken. NHRP redirect pakketten kunnen worden gedropt vanwege gaspedaal op ofwel het dataplatform of het besturingsplane. Als een DMVPN spaak ontvangt geen NHRP redirect pakket voordat het een resolutie aanvraag kan verzenden, kunt u eerst controleren om ervoor te zorgen dat de NHRP redirect pakketten niet worden gelaten vallen op de hub. Er zijn 3 plekken waar dit kan gebeuren.

1. Met Cisco IOS®-XE moet de aanvraag voor omleiding door het puntpad van het gegevensvlak naar Cisco IOSd. Als er veel dataplatformpakketten zijn die moeten worden omgeleid, dan kunnen deze pakketten in het puntpad worden gedropt. Dit punt policer moet gecontroleerd worden:

```
Router#show platform software punt-policer
```

Per Punt-Cause Policer Configuration and Packet Counters

```

Punt                               Config Rate(pps)   Conform Packets
Dropped Packets                    Config Burst(pkts) Config Alert
Cause Description                  Normal   High   Normal           High           Normal
High                               Normal   High   Normal   High
-----
<snip>
 51  DMVPN NHRP redirect           2000    1000    0               0               0
0    2000    1000    Off           Off
<snip>

```

2. Op Cisco IOSd zijn NHRP-omleidingen beperkt tot het aantal snelheden, zodat een omleiding niet wordt geactiveerd voor elk gegevensplatform dat wordt ontvangen. Het standaard snelheidsinterval is 8 seconden, en dit kan met de opdracht worden aangepast:

```

Spoke(config-if)#ip nhrp redirect timeout ?
 <2-30> Interval in seconds

```

3. Alle NHRP besturingspakketten zijn snelheidsbeperkt door de tunnelinterface nhrp max-send configuratie, en u kunt controleren op hoog gebruik met de opdracht **show ip NHRP traffic**:

```

Hub#show ip nhrp traffic
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
  Sent: Total 18740
        0 Resolution Request  3 Resolution Reply  7734 Registration Request
        0 Registration Reply  3 Purge Request  0 Purge Reply
        0 Error Indication  11000 Traffic Indication  0 Redirect Suppress
  Rcvd: Total 7737
        3 Resolution Request  0 Resolution Reply  0 Registration Request
        7728 Registration Reply  0 Purge Request  3 Purge Reply
        0 Error Indication  3 Traffic Indication  0 Redirect Suppress
Spoke2#

```

Oplossing

Identificeer de bron van de doorverwijzing

De eerste en belangrijkste stap om het NHRP omleiden drop probleem te verlichten is om eerst te identificeren of deze omleiden pakketten worden verwacht gezien het bijzondere DMVPN ontwerp. Voor de meeste DMVPN-netwerken kan een NHRP-omleiding de spraakbron activeren om een spraaktunnel te bouwen. Dientengevolge, kan een route NHRP met een netwerkprefix in de routerlijst worden geïnstalleerd, en om het even welk verkeer dat naar de zelfde prefix gaat kan geen extra omleidingen teweegbrengen tot de tunnel wordt afgebroken wegens inactiviteit. Als om de een of andere reden de direct spoke to spoke tunnel niet kan worden gebouwd, dan kan het dataverkeer deze omleidingen blijven activeren. Om te begrijpen welk verkeer de omleidingen activeert, gebruikt u deze opdracht op de hub:

```

Hub#show ip nhrp redirect
  I/F      NBMA address      Destination      Drop Count      Expiry
Tunnel0   172.16.1.1        192.168.101.1   16              00:00:00
Tunnel1   172.17.0.9        192.168.1.2    16              00:00:00

```

Hub#

Als al het dataverkeer dat deze omleidingen activeert legitiem is, maar een hoog volume omleidingen is nog steeds gewettigd op de hub vanwege de schaal van het netwerk, dan kunnen de punt-policer en NHRP max-send drempels worden afgestemd om aan de vereisten te voldoen.

Afstemming van de punt-policer-drempel

Standaard wordt de DMVPN NHRP omgeleid naar de hoge wachtrij in het punt pad. Gebruik deze opdracht om het punt-policer-tarief voor deze specifieke oorzaak aan te passen:

```
Hub(config)#platform punt-policer dmvpn-redir-pkt 20000 20000 high
```

De NHRP max-verzenddrempel instellen

De maximale NHRP-verzendsnelheid is verhoogd van 100Pkts/10Sec naar 10000Pkts/10Sec met Cisco bug ID [CSCux58299](#) (De standaardlimiet van ip NHRP max-send kan worden aangepast). Deze drempel kan verder worden verhoogd met:

```
Hub(config-if)#ip nhrp max-send 20000 every 10
```

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.