Solucionar problemas de redirecionamento de NHRP da fase 3 do DMVPN

Contents

[Introduction](#)
[Informações de Apoio](#)
[Problema](#)
[Limitação de pacotes de controle NHRP](#)
[Solução](#)
[Identificar a origem do redirecionamento](#)
[Ajustando o limite do punt-policer](#)
[Ajuste do limite máximo de envio de NHRP](#)

Introduction

Este documento descreve como a Fase 3 do DMVPN, Redirecionamento de NHRP, é uma função-chave que permite que um roteador spoke descubra o caminho direto para outro dispositivo spoke.

Informações de Apoio

Para que o túnel spoke-to-spoke seja construído, o hub DMVPN (Dynamic Mulitpoint Virtual Private Network) deve ser capaz de gerar um pacote de controle de redirecionamento NHRP (Next Hop Resolution Protocol) a partir do plano de dados e, subsequentemente, enviar esse redirecionamento para o dispositivo spoke. Em algumas situações, algum ajuste deve ser executado para que isso funcione em uma implantação DMVPN grande, e este artigo discute algumas dessas considerações.

Problema

Limitação de pacotes de controle NHRP

Em um ambiente de larga escala, um hub DMVPN precisa lidar com muitos pacotes de redirecionamento de NHRP. Os pacotes de redirecionamento NHRP podem ser descartados devido à limitação no plano de dados ou no plano de controle. Se um spoke DMVPN não estiver recebendo um pacote de redirecionamento de NHRP antes de enviar uma solicitação de resolução, você poderá primeiro verificar se os pacotes de redirecionamento de NHRP não foram descartados no hub. Há 3 lugares onde isso pode acontecer.

1. Com o Cisco IOS®-XE, a solicitação de redirecionamento precisa passar pelo caminho punt do plano de dados para o Cisco IOSd. Se houver muitos pacotes de plano de dados que precisam ser redirecionados, esses pacotes poderão ser descartados no caminho de punt. Este vigilante de punt deve ser verificado:

```
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. No Cisco IOSd, os redirecionamentos NHRP têm taxa limitada, de modo que um redirecionamento não seja acionado para cada pacote de plano de dados recebido. O intervalo de limite de taxa padrão é de 8 segundos e pode ser ajustado com o comando:

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

3. Todos os pacotes de controle NHRP têm taxa limitada pela configuração tunnel interface nhrp max-send e você pode verificar a alta utilização com o comando **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#
```

Solução

Identificar a origem do redirecionamento

A primeira e mais importante etapa para mitigar o problema de queda de redirecionamento de NHRP é primeiro identificar se esses pacotes de redirecionamento são esperados devido ao projeto de DMVPN específico. Para a maioria das redes DMVPN, um redirecionamento NHRP pode disparar o spoke de origem para criar um túnel spoke-to-spoke direto. Como resultado, uma rota NHRP com um prefixo de rede pode ser instalada na tabela de roteamento, e qualquer tráfego que vá para o mesmo prefixo não pode disparar redirecionamentos adicionais até que o túnel seja interrompido devido à inatividade. Se, por algum motivo, o túnel spoke-to-spoke direto não puder ser criado, o tráfego de dados poderá continuar a disparar esses redirecionamentos. Para entender qual tráfego está disparando os redirecionamentos, use este comando no 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#
```

Se todo o tráfego de dados que aciona esses redirecionamentos for legítimo, mas um alto volume de redirecionamentos ainda for garantido no hub devido à escala da rede, os limiares punt-policer e NHRP max-send poderão ser ajustados para acomodar os requisitos.

Ajustando o limite do punt-policer

Por padrão, os redirecionamentos de NHRP DMVPN usam a fila alta no caminho de punt. Para ajustar a taxa punt-policer para essa causa específica, use este comando:

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

Ajuste do limite máximo de envio de NHRP

A taxa máxima de envio de NHRP foi aumentada de 100Pkts/10Sec para 10000Pkts/10Sec com a ID de bug Cisco CSCux58299 (o limite padrão de ip NHRP max-send pode ser ajustado). Este limiar pode ainda ser aumentado com:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.