

排除DMVPN第3阶段NHRP重定向问题

目录

[简介](#)

[背景信息](#)

[问题](#)

[NHRP控制数据包限制](#)

[解决方案](#)

[确定重定向的来源](#)

[调整punt-policer阈值](#)

[调整NHRP最大发送阈值](#)

简介

本文档介绍DMVPN第3阶段，NHRP重定向如何是允许分支路由器发现到另一个分支设备的直接路径的关键功能。

背景信息

要建立分支到分支隧道，动态多点虚拟专用网络(DMVPN)中心必须能够生成来自数据平面的下一跳解析协议(NHRP)重定向控制数据包，然后将此重定向发送到分支设备。在某些情况下，必须执行一些调整才能在大型的DMVPN部署中正常工作，本文讨论其中一些注意事项。

问题

NHRP控制数据包限制

在大规模环境中，DMVPN中心需要处理大量NHRP重定向数据包。由于数据平面或控制平面上的限制，NHRP重定向数据包可能会被丢弃。如果DMVPN分支在发送解析请求之前未收到NHRP重定向数据包，您可以首先进行检查以确保NHRP重定向数据包未在中心上丢弃。这有3个地方可以实现。

1.使用Cisco IOS®-XE时，重定向请求需要通过从数据平面到Cisco IOSd的传送路径。如果有大量数据平面数据包需要重定向，则这些数据包可能会被丢弃在传送路径中。必须检查此强制转发器：

```
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.在Cisco IOSd上，NHRP重定向受到速率限制，因此不会为每个传入的数据平面数据包触发重定向。默认速率限制间隔为8秒，可以使用以下命令调整此值：

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

3.所有NHRP控制数据包都受隧道接口nhrp max-send配置的速率限制，您可以使用show ip nhrp traffic命令检查利用率是否较高：

```
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#
```

解决方案

确定重定向的来源

缓解NHRP重定向丢弃问题的第一个也是最重要的步骤是首先确定在特定DMVPN设计下是否期望这些重定向数据包。对于大多数DMVPN网络，NHRP重定向可以触发源分支以构建直接分支到分支隧道。因此，可以在路由表中安装带有网络前缀的NHRP路由，并且流向相同前缀的所有流量在隧道因不活动而中断之前无法触发其他重定向。如果由于某种原因，无法建立直接分支到分支隧道，则数据流量可以继续触发这些重定向。要了解哪些流量触发了重定向，请在集线器上使用此命令：

```
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#
```

如果触发这些重定向的所有数据流量都是合法的，但由于网络规模庞大，集线器上仍然需要大量重定向，则可以调整punt-policer和NHRP max-send阈值以满足要求。

调整punt-policer阈值

默认情况下，DMVPN NHRP重定向使用分支路径中的高队列。要为此特定原因调整punt-policer速率，请使用以下命令：

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

调整NHRP最大发送阈值

使用Cisco Bug ID [CSCux](#),NHRP最大发送速率从100Pkts/10Sec增加到10000Pkts/10Sec[58299](#)
(可以调整ip NHRP max-send的默认限制)。此阈值可通过以下方式进一步增加 :

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。