排除DMVPN第3階段NHRP重定向問題

目錄

簡介

本文檔介紹DMVPN第3階段，NHRP重定向如何是一個關鍵功能，它允許分支路由器發現到另一個分支裝置的直接路徑。

背景資訊

若要建立輻射點到輻射點通道，動態多點虛擬私人網路(DMVPN)集線器必須能夠從資料平面產生下一個躍點解析通訊協定(NHRP)重新導向控制封包，然後將此重新導向傳送到輻射點裝置。在某些情況下，必須執行一些調整才能在大型DMVPN部署中正常工作，本文討論了其中一些注意事項。

問題

NHRP控制資料包限制

在大規模環境中，DMVPN中心需要處理大量NHRP重定向資料包。由於資料平面或控制平面上的限制，NHRP重定向資料包可能會被丟棄。如果DMVPN分支在可以傳送解析請求之前未收到NHRP重定向資料包，您可以首先檢查以確保NHRP重定向資料包在集線器上未被丟棄。有三個地方可能會發生這種情況。

1.使用Cisco IOS®-XE時，重定向請求需要經過從資料平面到Cisco IOSd的轉發路徑。如果有大量資料平面資料包需要重定向，則這些資料包可能會在分流路徑中被丟棄。必須檢查此點策略器：

```
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重新導向是受速率限制的，因此傳入的每個資料平面封包都不會觸發重新導向。預設速率限制間隔為8秒，可以使用以下命令調整該間隔：

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

3.所有NHRP控制資料包的速率均受隧道介面nhrp max-send配置的限制，您可以使用**show ip nhrp traffic**命令檢查利用率是否高：

```
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#
```

解決方案

識別重新導向的來源

緩解NHRP重新導向捨棄問題的第一個也是最重要的步驟是首先識別在特定DMVPN設計的情況下是否預期這些重新導向封包。對於大多數DMVPN網路，NHRP重定向可以觸發源分支以構建直接分支到分支隧道。因此，具有網路首碼的NHRP路由可以安裝在路由表中，而且任何前往相同首碼的流量都不能觸發額外的重新導向，直到通道因為不活動而中斷。如果由於某種原因，無法建立直接分支到分支隧道，則資料流量可以繼續觸發這些重定向。要瞭解觸發重定向的流量，請在集線器上使用以下命令：

```
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#
```

如果觸發這些重定向的所有資料流量都是合法的，但由於網路規模龐大，集線器上仍有大量重定向需要保證，則可以調整點監察器和NHRP最大傳送閾值以滿足要求。

調整punt-policer閾值

預設情況下，DMVPN NHRP重定向使用點路徑中的高隊列。要調整此特定原因的點策略器速率，請使用以下命令：

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

調整NHRP最大傳送閾值

使用思科錯誤ID CSCux,NHRP最大傳送速率從100Pkts/10Sec增加到10000Pkts/10Sec58299（可以調整ip NHRP max-send的預設限制）。此閾值可通過以下方式進一步提高：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。