Fehlerbehebung bei Problemen mit der DMVPN Phase3 NHRP-Umleitung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die DMVPN Phase 3, NHRP-Umleitung, eine Schlüsselfunktion darstellt, mit der ein Spoke-Router den direkten Pfad zu einem anderen Spoke-Gerät erkennen kann.

Hintergrundinformationen

Damit der Spoke-to-Spoke-Tunnel erstellt werden kann, muss der DMVPN-Hub (Dynamic Multipoint Virtual Private Network) ein Next Hop Resolution Protocol (NHRP)-Umleitungspaket von der Datenebene generieren und diese Umleitung anschließend an das Spoke-Gerät senden können. In einigen Situationen muss eine Optimierung durchgeführt werden, damit dies in einer umfangreichen DMVPN-Bereitstellung funktioniert. In diesem Artikel werden einige dieser Aspekte erläutert.

Problem

Drosselung von NHRP-Steuerungspaketen

In einer groß angelegten Umgebung muss ein DMVPN-Hub eine Vielzahl von NHRP-Umleitungspaketen verarbeiten. NHRP-Umleitungspakete können aufgrund einer Drosselung auf der Daten- oder der Kontrollebene verworfen werden. Wenn eine DMVPN-Spoke kein NHRP-Umleitungspaket empfängt, bevor sie eine Auflösungsanfrage senden kann, können Sie zunächst überprüfen, ob die NHRP-Umleitungspakete auf dem Hub verworfen werden. Es gibt 3 Orte, an denen dies geschehen kann.

1. Bei Cisco IOS®-XE muss die Umleitungsanforderung den Punktpfad von der Datenebene zu Cisco IOSd durchlaufen. Wenn eine große Anzahl an Datenebenenpaketen umgeleitet werden muss, können diese Pakete im Punt-Pfad verworfen werden. Dieser Kontrollpunkt muss überprüft werden:

```
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. Auf Cisco IOSd sind NHRP-Umleitungen ratenbegrenzt, sodass nicht für jedes eingehende Datenebenenpaket eine Umleitung ausgelöst wird. Das Standardintervall für die Ratenbegrenzung ist 8 Sekunden. Dies kann mithilfe des folgenden Befehls angepasst werden:

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

3. Alle NHRP-Steuerungspakete werden durch die Konfiguration der Tunnelschnittstelle "nhrp max-send" auf die Durchsatzrate begrenzt, und Sie können mit dem Befehl **show ip nhrp traffic** überprüfen, ob die Pakete **hochausgelastet sind**:

```
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#
```

Lösung

Identifizieren der Quelle der Umleitung

Der erste und wichtigste Schritt zur Minimierung des Problems mit dem NHRP-Redirect-Drop besteht darin, zunächst festzustellen, ob diese Redirect-Pakete im Hinblick auf das jeweilige DMVPN-Design erwartet werden. Bei den meisten DMVPN-Netzwerken kann eine NHRP-Umleitung dazu führen, dass die Source-Spoke einen direkten Spoke-to-Spoke-Tunnel erstellt. Dadurch kann eine NHRP-Route mit einem Netzwerkpräfix in der Routing-Tabelle installiert werden, und Datenverkehr, der an dasselbe Präfix weitergeleitet wird, kann erst dann zusätzliche Umleitungen auslösen, wenn der Tunnel aufgrund von Inaktivität abgebaut wird. Wenn aus irgendeinem Grund kein Direct-Spoke-to-Spoke-Tunnel erstellt werden kann, kann der Datenverkehr diese Umleitungen weiterhin auslösen. Um zu ermitteln, welcher Datenverkehr die Umleitungen auslöst, verwenden Sie folgenden Befehl auf dem 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#
```

Wenn der gesamte Datenverkehr, der diese Umleitungen auslöst, legitim ist, aber aufgrund der Größe des Netzwerks immer noch eine große Anzahl von Umleitungen auf dem Hub erforderlich ist, können die Grenzwerte für Punt-Policer und NHRP Max-Send an die Anforderungen angepasst werden.

Optimieren des Grenzwerts für Punt-Policer

Standardmäßig verwenden die DMVPN-NHRP-Umleitungen die Warteschlange "high" im Punt-Pfad. Verwenden Sie den folgenden Befehl, um die Punktvergabe-Rate für diesen bestimmten Grund anzupassen:

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

Einstellen des NHRP-Grenzwerts für den max. Sendevorgang

Die maximale NHRP-Sendegeschwindigkeit wurde mit der Cisco Bug-ID CSCux58299 von 100 Pkte/10 Sek auf 10000 Pkte/10 Sek. erhöht. (Der Standardwert für "ip NHRP max-send" kann angepasst werden.) Diese Schwelle kann weiter erhöht werden mit:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.