Dépannage des problèmes de redirection NHRP phase3 DMVPN

Table des matières

Introduction

Ce document décrit comment DMVPN Phase3, NHRP Redirect est une fonction clé qui permet à un routeur en étoile de découvrir le chemin direct vers un autre périphérique en étoile.

Informations générales

Pour que le tunnel satellite à satellite soit construit, le concentrateur DMVPN (Dynamic Mulitpoint Virtual Private Network) doit être capable de générer un paquet de contrôle de redirection NHRP (Next Hop Resolution Protocol) à partir du plan de données, puis d'envoyer cette redirection au périphérique satellite. Dans certaines situations, un certain réglage doit être effectué pour que cela fonctionne dans un déploiement DMVPN de grande envergure, et cet article traite de certaines de ces considérations.

Problème

Limitation des paquets de contrôle NHRP

Dans un environnement à grande échelle, un concentrateur DMVPN doit gérer un grand nombre de paquets de redirection NHRP. Les paquets de redirection NHRP peuvent être abandonnés en raison de la limitation sur le plan de données ou le plan de contrôle. Si un satellite DMVPN ne reçoit pas de paquet de redirection NHRP avant de pouvoir envoyer une demande de résolution, vous pouvez d'abord vérifier que les paquets de redirection NHRP ne sont pas abandonnés sur le concentrateur. Il y a 3 endroits où cela peut se produire.

1. Avec Cisco IOS®-XE, la requête de redirection doit passer par le chemin de point du plan de données à Cisco IOSd. S'il y a beaucoup de paquets de plan de données qui doivent être redirigés, alors ces paquets pourraient être abandonnés dans le chemin punt. Ce régulateur de point doit être vérifié :

```
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. Sur Cisco IOSd, les redirections NHRP sont limitées en débit, de sorte qu'une redirection n'est pas déclenchée pour chaque paquet de plan de données entrant. L'intervalle rate-limit par défaut est de 8 secondes, et ceci peut être ajusté avec la commande :

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

3. Tous les paquets de contrôle NHRP sont limités en débit par la configuration nhrp max-send de l'interface de tunnel, et vous pouvez vérifier l'utilisation élevée avec la commande **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#
```

Solution

Identifier la source de la redirection

La première et la plus importante étape pour atténuer le problème de suppression de redirection NHRP consiste à identifier d'abord si ces paquets de redirection sont attendus compte tenu de la conception DMVPN particulière. Pour la plupart des réseaux DMVPN, une redirection NHRP peut déclencher le rayon source pour construire un tunnel direct de rayon à rayon. Par conséquent, une route NHRP avec un préfixe de réseau peut être installée dans la table de routage, et tout trafic allant au même préfixe ne peut pas déclencher de redirections supplémentaires jusqu'à ce que le tunnel soit désactivé en raison de l'inactivité. Si, pour une raison quelconque, le tunnel rayon à rayon direct ne peut pas être construit, alors le trafic de données peut continuer à déclencher ces redirections. Pour comprendre le trafic qui déclenche les redirections, utilisez cette commande sur le concentrateur :

```
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#
```

Si tout le trafic de données qui déclenche ces redirections est légitime, mais qu'un volume élevé de redirections est toujours justifié sur le concentrateur en raison de l'échelle du réseau, alors le régulateur de point et les seuils NHRP max-send peuvent être réglés pour répondre aux exigences.

Réglage du seuil de punt-policer

Par défaut, les redirections NHRP DMVPN utilisent la file d'attente haute dans le chemin de pontage. Pour régler le débit du régulateur de point pour cette cause particulière, utilisez cette commande :

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

Réglage du seuil d'envoi maximal NHRP

Le taux d'envoi maximal NHRP a été augmenté de 100Pkts/10Sec à 10000Pkts/10Sec avec l'ID de bogue Cisco CSCux58299 (la limite par défaut de ip NHRP max-send peut être ajustée). Ce seuil peut encore être augmenté avec :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.