

Resolución de Problemas de Redirección NHRP DMVPN Phase3

Contenido

[Introducción](#)

[Antecedentes](#)

[Problema](#)

[Límite de paquetes de control NHRP](#)

[Solución](#)

[Identificar el origen de la redirección](#)

[Ajuste del umbral del regulador de punt](#)

[Ajuste del umbral de envío máximo NHRP](#)

Introducción

Este documento describe cómo DMVPN Phase3, NHRP Redirect es una función clave que permite que un router spoke detecte la trayectoria directa a otro dispositivo spoke.

Antecedentes

Para que se cree el túnel de radio a radio, el hub de red privada virtual multipunto dinámica (DMVPN) debe ser capaz de generar un paquete de control de redirección del protocolo de resolución de próximo salto (NHRP) desde el plano de datos y, a continuación, enviar esta redirección al dispositivo de radio. En algunas situaciones, se deben realizar algunos ajustes para que esto funcione en una implementación DMVPN grande, y este artículo trata algunas de estas consideraciones.

Problema

Límite de paquetes de control NHRP

En un entorno de gran escala, un hub DMVPN necesita gestionar una gran cantidad de paquetes de redirección NHRP. Los paquetes de redirección NHRP se pueden descartar debido a la aceleración en el plano de datos o en el plano de control. Si un radio DMVPN no recibe un paquete de redirección NHRP antes de poder enviar una solicitud de resolución, primero puede comprobar que los paquetes de redirección NHRP no se descartan en el hub. Hay 3 lugares donde esto puede suceder.

1. Con Cisco IOS®-XE, la solicitud de redirección debe pasar a través de la trayectoria de punt desde el plano de datos a Cisco IOSd. Si hay muchos paquetes de plano de datos que necesitan ser redirigidos, entonces estos paquetes podrían ser descartados en la trayectoria de punt. Este regulador de punt debe ser verificado:

```
Router#show platform software punt-policer
```

Punt	Cause	Description	Config Rate(pps)		Config Burst(pkts)		Config Alert		Conform Packets	
			Normal	High	Normal	High	Normal	High	Normal	High
High		Normal	High	Normal	High					

<snip>										
51		DMVPN NHRP redirect		2000	1000		0		0	0
0			2000	1000	Off	Off				
<snip>										

2. En Cisco IOSd, las redirecciones NHRP están limitadas por velocidad, de modo que no se activa una redirección para cada paquete de plano de datos que entra. El intervalo de límite de velocidad predeterminado es de 8 segundos, y esto se puede ajustar con el comando:

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

3. La configuración nhrp max-send de la interfaz de túnel limita la velocidad de todos los paquetes de control NHRP, y puede verificar la alta utilización con el 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#
```

Solución

Identificar el origen de la redirección

El primer paso y el más importante para mitigar el problema de caída de redirección NHRP es identificar primero si se esperan estos paquetes de redirección dado el diseño DMVPN particular. Para la mayoría de las redes DMVPN, una redirección NHRP puede activar el spoke de origen para crear un túnel de spoke directo a spoke. Como resultado, se puede instalar una ruta NHRP con un prefijo de red en la tabla de ruteo, y cualquier tráfico que vaya al mismo prefijo no puede desencadenar redirecciones adicionales hasta que el túnel se interrumpa debido a la inactividad. Si por alguna razón, no se puede construir el túnel de radio a radio directo, entonces el tráfico de datos puede continuar activando estas redirecciones. Para comprender qué tráfico está activando las redirecciones, utilice este comando en el 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#				

Si todo el tráfico de datos que activa estas redirecciones es legítimo, pero se sigue garantizando un alto volumen de redirecciones en el hub debido a la escala de la red, se pueden ajustar los umbrales de máximo envío NHRP y el regulador de puertos para adaptarse a los requisitos.

Ajuste del umbral del regulador de punt

De forma predeterminada, las redirecciones NHRP de DMVPN utilizan la cola alta en la ruta de punteo. Para ajustar la velocidad del regulador de punt para esta causa en particular, utilice este comando:

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

Ajuste del umbral de envío máximo NHRP

La velocidad máxima de envío de NHRP se aumentó de 100 paquetes/10 segundos a 10000 paquetes/10 segundos con la identificación de error de Cisco [CSCux58299](#) (se puede ajustar el límite predeterminado de ip NHRP max-send). Este umbral se puede aumentar aún más con:

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).