# Troubleshoot DMVPN Phase3 NHRP Redirect Issues

## Contents



## Introduction

This document describes how DMVPN Phase3, NHRP Redirect is a key function that allows a spoke router to discover direct path to another spoke device.

## Background Information

In order for the spoke to spoke tunnel to be built, the Dynamic Mulitpoint Virtual Private Network (DMVPN) hub must be able to generate an Next Hop Resolution Protocol (NHRP) redirect control packet from the data plane, and subsequently send this redirect to the spoke device. In some situations, some tuning must be performed for this to work in a large DMVPN deployment, and this article discusses some of these considerations.

## Problem

### NHRP control packets throttling

In a large scale environment, a DMVPN hub needs to handle a lot of NHRP redirect packets. NHRP redirect packets can be dropped due to throttling on either the data plane or control plane. If a DMVPN spoke is not receiving an NHRP redirect packet before it can send a resolution request, you can first check to make sure the NHRP redirect packets are not dropped on the hub. There are 3 places where this can happen.

1. With Cisco IOS®-XE, the redirect request needs to go through the punt path from the data plane to Cisco IOSd. If there are a lot of data plane packets that need to be redirected, then these packets could be dropped in the punt path. This punt policer must be checked:

```
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. On Cisco IOSd, NHRP redirects are rate-limited, so that a redirect is not triggered for every data plane packet that comes in. The default rate-limit interval is 8 seconds, and this can be adjusted with the command:

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

3. All NHRP control packets are rate-limited by the tunnel interface nhrp max-send configuration, and you can check for high utilization with the **show ip nhrp traffic** command:

```
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

## Identify source of the redirect

The first and most important step to mitigate the NHRP redirect drop issue is to first identify if these redirect packets are expected given the particular DMVPN design. For most DMVPN network, an NHRP redirect can trigger the source spoke to build a direct spoke to spoke tunnel. As a result, an NHRP route with a network prefix can be installed in the routing table, and any traffic going to the same prefix can not trigger additional redirects until the tunnel gets torn down due to inactivity. If for some reason, the direct spoke to spoke tunnel cannot be built, then the data traffic can continue to trigger these redirects. To understand what traffic is triggering the redirects, use this command on the 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#
```

If all the data traffic that triggers these redirects are legitimate, but a high volume of redirects is still warranted on the hub due to the scale of the network, then the punt-policer and NHRP max-send thresholds can be tuned to accommodate the requirements.

## Tuning the punt-policer threshold

By default, the DMVPN NHRP redirects use the high queue in the punt path. To adjust the punt-policer rate for this particular cause, use this command:

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

## Tuning the NHRP max-send threshold

The NHRP max-send rate was increased from 100Pkts/10Sec to 10000Pkts/10Sec with Cisco bug ID CSCux58299 (default limit of ip NHRP max-send can be adjusted). This threshold can further be increased with:

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