实施DMVPN第3阶段多子网设计

目录

简介

本文档介绍DMVPN第3阶段多子网设计中的路由注意事项，以确保正确构建直接分支到分支隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- 动态多点VPN(DMVPN)基础知识
- 下一跳解析协议(NHRP)基础知识

使用的组件

本文档不限于特定的软件和硬件版本。

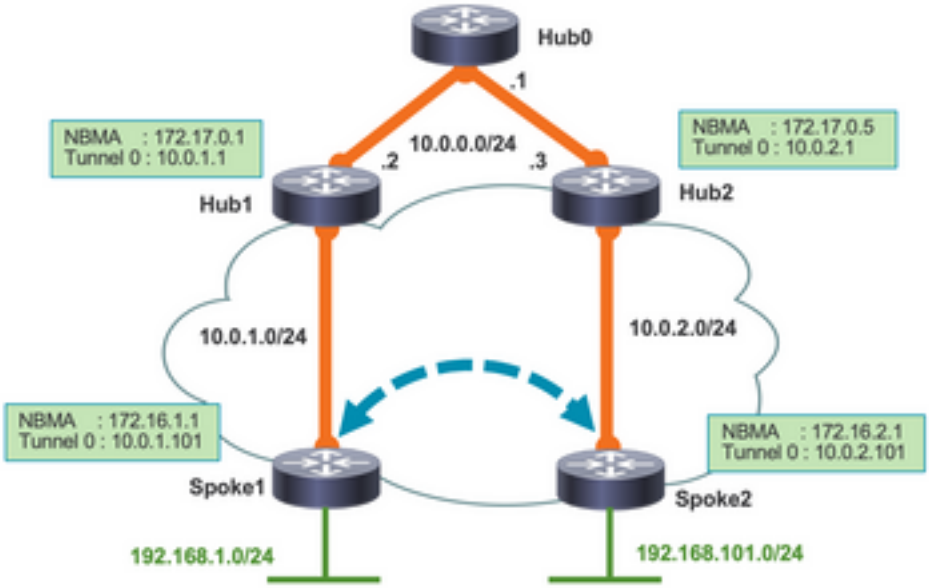
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

DMVPN第2阶段和第3阶段都允许分支设备建立到分支的直接分支隧道，而无需通过中心。但是，DMVPN第3阶段提供了更好的可扩展性，通过分支的NHRP重定向机制，通过NHRP动态发现远程网络，然后将NHRP(H)路由安装到路由表中。这消除了第2阶段限制，即要求每个分支在其路由表中具有远程网络的特定网络前缀。对于第3阶段，来自目标分支（NBMA出口点）的NHRP解析应答必须通过直接分支到分支隧道。但是，必须特别考虑多子网阶段3设计，以便可以正确建立分支到分支隧道。本文详细讨论了这些要求。

问题

DMVPN阶段3可以在单子网重叠或多子网重叠中实施。在单子网重叠拓扑中，中心路由器和所有分支路由器隧道地址都从单个逻辑IP子网中分配；而在多子网设计中，分支到分支隧道需要针对其隧道地址位于不同IP子网中的分支而构建。后者是下图所示的分层DMVPN设计中使用的常见场景。



DMVPN第3阶段多子网拓扑

问题详细资料

在DMVPN阶段3中，通常可以理解，当收到NHRP解析请求时，目标分支发起到源分支的IPsec隧道，然后通过该隧道发送解析应答。但是，这仅适用于单个子网重叠。当分支的隧道接口处于不同的IP逻辑子网中时，NHRP控制数据包可以通过分支中心分支路径而不是直接分支到分支隧道。以下是Spoke1收到来自Hub1的NHRP重定向后，向Spoke2发送解析请求时的事件序列：

1. Spoke2收到解析请求

```
*Feb  7 20:57:22.272: NHRP: Receive Resolution Request via Tunnel0 vrf global(0x0), packet
size: 144
*Feb  7 20:57:22.272:  (F) afn: AF_IP(1), type: IP(800), hop: 252, ver: 1
*Feb  7 20:57:22.272:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb  7 20:57:22.272:      pktsz: 144 extoff: 52
*Feb  7 20:57:22.272:  (M) flags: "router auth src-stable nat ", reqid: 5
*Feb  7 20:57:22.272:      src NBMA: 172.16.1.1
*Feb  7 20:57:22.272:      src protocol: 10.0.1.101, dst protocol: 192.168.101.1
*Feb  7 20:57:22.272:  (C-1) code: no error(0)
*Feb  7 20:57:22.272:        prefix: 32, mtu: 17912, hd_time: 900
*Feb  7 20:57:22.272:        addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref:
255
```

2. Spoke2通过监听Resolution Request数据包，为10.0.1.101添加一个隐式NHRP缓存条目。
3. Spoke2使用Spoke1的NBMA地址为Tunnel0添加10.0.1.101的邻接关系。
4. Spoke2使用解析回复做出响应。请注意，此时，请求分支隧道地址的路由指向Hub2:

```
Spoke2#show ip route 10.0.1.101
Routing entry for 10.0.1.0/24
```

```
  Known via "eigrp 1", distance 90, metric 3609600, type internal
  Redistributing via eigrp 1
  Last update from 10.0.2.1 on Tunnel0, 00:17:44 ago
  Routing Descriptor Blocks:
  * 10.0.2.1, from 10.0.2.1, 00:17:44 ago, via Tunnel0
      Route metric is 3609600, traffic share count is 1
      Total delay is 41000 microseconds, minimum bandwidth is 1000 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 3
Spoke2#
Spoke2#
Spoke2#show ip cef 10.0.1.101
10.0.1.0/24
  nexthop 10.0.2.1 Tunnel0
```

由于NHRP控制数据包沿路由路径转发，因此它被发送到Hub2，而不是发送到Spoke1的新创建分支到分支隧道：

```
*Feb  7 20:57:22.360: NHRP: Send Resolution Reply via Tunnel0 vrf global(0x0), packet size:
172
*Feb  7 20:57:22.360:  src: 10.0.2.101, dst: 10.0.1.101
*Feb  7 20:57:22.360:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb  7 20:57:22.360:      shtl: 4(NSAP), sstl: 0(NSAP)
*Feb  7 20:57:22.360:      pktsz: 172 extoff: 60
*Feb  7 20:57:22.360:  (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 5
*Feb  7 20:57:22.360:      src NBMA: 172.16.1.1
*Feb  7 20:57:22.360:      src protocol: 10.0.1.101, dst protocol: 192.168.101.1
*Feb  7 20:57:22.360:  (C-1) code: no error(0)
*Feb  7 20:57:22.360:        prefix: 24, mtu: 17912, hd_time: 900
*Feb  7 20:57:22.360:        addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref:
255
*Feb  7 20:57:22.360:        client NBMA: 172.16.2.1
*Feb  7 20:57:22.360:        client protocol: 10.0.2.101
*Feb  7 20:57:22.360: NHRP: Encapsulation succeeded.  Sending NHRP Control Packet  NBMA
Address: 172.17.0.5
```

理论上，只要所有中间集线器都能将NHRP控制数据包路由回Spoke1的隧道，那么一切都必须仍然有效。但情况并非总是如此。如果解析应答无法转发回Spoke1，则无法建立直接辐射到辐射隧道。

对于单个子网重叠，这不是问题，因为每个分支都有到隧道网络的直接连接路由。这将导致在发送回解析应答之前为请求辐射隧道地址执行邻接查找。在多子网重叠网络中，由于分支的隧道地址不在同一IP子网上，因此不保证通过直接分支到分支隧道发送解析应答数据包。

解决方案

对于多子网DMVPN第3阶段设计，建议分支具有一个路由条目，指出其需要建立分支到分支的直接隧道的所有远程分支隧道子网的隧道接口。例如：

```
Spoke2#show run | in ip route
ip route 10.0.101.0 255.255.255.0 Tunnel0
```

这允许分支尝试解析请求分支隧道地址的邻接，然后通过分支向分支隧道发送解析应答。

或者，解析应答可以遍历分支中心分支隧道。在这种情况下，所有中间集线器必须具有通往请求分

支隧道子网的路由，以确保NHRP控制数据包可以端到端传送。

> **注意**：漏洞增强功能已打开，用于探索即使没有显式静态路由，也可以在直接隧道上发送解析应答的选项。Cisco Bug ID CSCvo02022 — 增强功能：NHRP必须通过分支向多子网DMVPN的分支隧道发送解析应答。

> **注意**：只有注册的思科客户端可以访问内部思科漏洞信息和工具。

相关信息

- **思科技术支持和下载**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。