

# DMVPN 3단계 다중 서브넷 설계 구현

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제](#)

[문제 세부 정보](#)

[솔루션](#)

[관련 정보](#)

## 소개

이 문서에서는 직접 스포크 투 스포크 터널이 올바르게 구축되도록 하기 위한 DMVPN Phase3 다중 서브넷 설계의 라우팅 고려 사항에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- [DMVPN\(Dynamic Multipoint VPN\)에 대한 기본 지식](#)
- [NHRP\(Next-Hop Resolution Protocol\)에 대한 기본 지식](#)

## 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

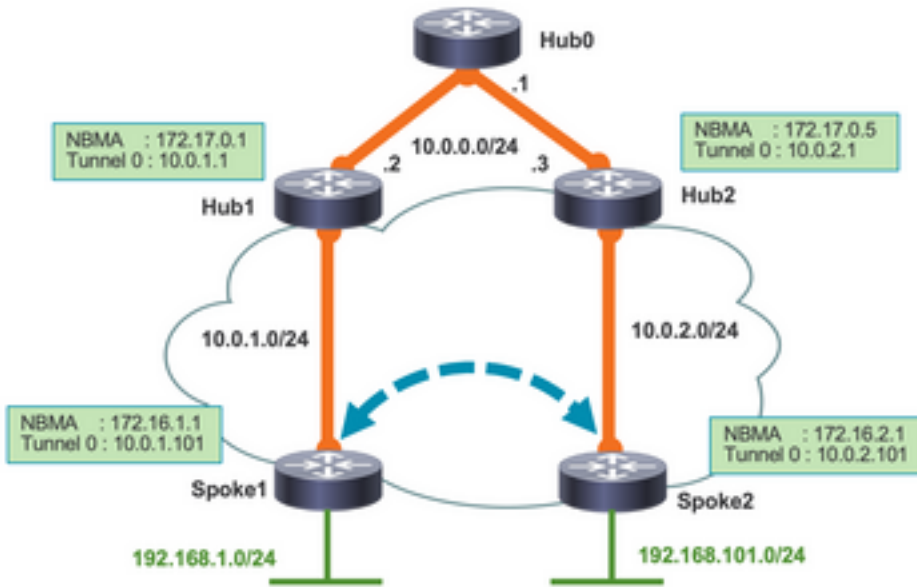
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

DMVPN phase2 및 phase3 구현에서는 스포크 디바이스에서 직접 스포크 터널을 구축하고 허브를 거치지 않아도 됩니다. 그러나 DMVPN Phase3는 스포크가 NHRP를 통해 원격 네트워크를 동적으로 검색하고 이후에 NHRP(H) 경로를 라우팅 테이블에 설치할 수 있도록 NHRP 리디렉션 메커니즘을 사용하여 훨씬 뛰어난 확장성을 제공합니다. 이렇게 하면 각 스포크에 라우팅 테이블의 원격 네트워크에 대한 특정 네트워크 접두사를 포함하도록 요구하는 2단계 제한이 제거됩니다. 3단계의 경우 대상 스포크의 NHRP 해결 응답(NBMA 종료 지점)은 직접 스포크-투-스포크 터널을 통과해야 합니다. 그러나 다중 서브넷 Phase3 설계에서는 Spoke-to-Spoke 터널을 올바르게 구성할 수 있도록 특별히 고려해야 합니다. 이 문서에서는 이러한 요구 사항에 대해 자세히 설명합니다.

# 문제

DMVPN Phase3는 단일 서브넷 오버레이 또는 다중 서브넷 오버레이에서 구현될 수 있다. 단일 서브넷 오버레이 토폴로지에서는 허브 및 모든 스포크 라우터 터널 주소가 단일 논리적 IP 서브넷에서 할당되지만, 다중 서브넷 설계에서는 다른 IP 서브넷에 있는 터널 주소를 가진 스포크에 대해 스포크 투 스포크 터널을 구축해야 합니다. 후자는 아래 이미지에 표시된 계층적 DMVPN 설계에서 사용되는 일반적인 시나리오입니다.



## DMVPN 3단계 다중 서브넷 토폴로지

### 문제 세부 정보

DMVPN phase3에서는 일반적으로 NHRP 확인 요청이 수신되면 대상 스포크가 소스 스포크에 대한 IPsec 터널을 시작하고, 그 후 해당 터널을 통해 확인 응답을 전송하는 것으로 알고 있습니다. 그러나 단일 서브넷 오버레이의 경우에만 해당됩니다. 스포크의 터널 인터페이스가 서로 다른 IP 논리 서브넷에 있는 경우, NHRP 제어 패킷은 스포크 투 스포크 터널을 사용하는 대신 스포크 허브 스포크 경로를 통과할 수 있습니다. 다음은 Spoke1이 Hub1에서 NHRP 리디렉션을 수신한 후 Spoke2에 해결 요청을 보낼 때의 이벤트 시퀀스입니다.

#### 1. Spoke2에서 해결 요청 수신

```
*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. Spoke2는 Resolution Request 패킷을 스누핑하여 10.0.1.101에 대한 암시적 NHRP 캐시 항목을 추가합니다.
3. Spoke2는 Spoke1의 NBMA 주소가 있는 Tunnel0에 대해 10.0.1.101에 인접성을 추가합니다.
4. Spoke2는 해결 회신(Resolution Reply)으로 응답합니다. 이때 요청 스포크 터널 주소의 경로가 Hub2를 가리킵니다.

```
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
```

NHRP 제어 패킷은 라우티드 경로를 따라 전달되므로 새로 생성된 스포크 투 스포크 터널이 아닌 Hub2로 Spoke1에 전송됩니다.

```
*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
```

이론적으로 모든 중간 허브가 NHRP 제어 패킷을 Spoke1의 터널로 다시 라우팅할 수 있는 한 모든 것이 작동해야 합니다. 그러나 반드시 그렇지는 않습니다. 해결 회신 스포크1로 다시 전달할 수 없는 경우 직접 스포크 투 스포크 터널을 작성할 수 없습니다.

단일 서브넷 오버레이의 경우 각 스포크에 터널 네트워크에 직접 연결된 경로가 있으므로 문제가 되지 않습니다. 그러면 해결 회신이 다시 전송되기 전에 요청 스포크 터널 주소에 대한 인접성 조회가 수행됩니다. 다중 서브넷 오버레이 네트워크에서는 스포크의 터널 주소가 동일한 IP 서브넷에 있지 않으므로 확인 응답 패킷이 직접 스포크 투 스포크 터널을 통해 전송되는 것은 보장되지 않습니다.

## 솔루션

다중 서브넷 DMVPN Phase3 설계의 경우 스포크에 직접 스포크 투 스포크 터널을 구축해야 하는 모든 원격 스포크 터널 서브넷의 터널 인터페이스를 가리키는 라우팅 항목을 사용하는 것이 좋습니다. 예를 들면 다음과 같습니다.

```
Spoke2#show run | in ip route  
ip route 10.0.101.0 255.255.255.0 Tunnel10
```

이렇게 하면 스포크가 요청한 스포크 터널 주소에 대한 인접성을 해결하려고 시도한 다음 스포크 터널을 통해 해결 응답을 보낼 수 있습니다.

또는 해결 회신은 스포크 허브 스포크 터널을 통과시킬 수 있습니다. 이러한 경우 모든 중간 허브는 NHRP 제어 패킷이 종단 간 전달될 수 있도록 요청하는 스포크 터널 서브넷에 대한 경로를 가져야 합니다.

**참고:** 명시적 고정 경로 없이 직접 터널을 통해 해결 회신을 전송하도록 하는 옵션을 탐색하기 위해 버그 개선 기능이 열렸습니다. Cisco 버그 ID [CSCvo02022](#) - 개선 사항: NHRP는 다중 서브넷 DMVPN에 대해 스포크 터널을 통해 해결 응답을 보내야 합니다.

**참고:** 등록된 Cisco 클라이언트만 내부 Cisco 버그 정보 및 툴에 액세스할 수 있습니다.

## 관련 정보

- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.