# DMVPN을 통한 BGP 구성 3단계

## 목차



## 소개

이 문서에서는 BGP를 사용하는 DMVPN 3단계의 컨피그레이션 및 작동, DMVPN 터널을 통한 IPsec에 대한 계층적 문제 해결에 대해 설명합니다.

## 사전 요구 사항

이 문서의 configuration 및 debug 명령을 사용하려면 Cisco IOS® Release 15.3(3)M 이상을 실행하는 Cisco 라우터 2개가 필요합니다. 일반적으로 기본 DMVPN(Dynamic Multipoint VPN) Phase 3에서는 Cisco IOS Release 12.4(6)T가 필요하지만, 이 문서에서는 기능 및 디버그가 완전히 지원되지 않습니다.

### 요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- IKEV1/IKEV2 및 IPsec
- DMVPN 구성 요소:

- NHRP(Next Hop Resolution Protocol): 실제(공용 인터페이스) 주소에 대한 모든 스포크 터널의 분산(NHRP) 매핑 데이터베이스를 생성합니다.

- mGRE(Multipoint Generic Routing Encapsulation) 터널 인터페이스: 여러 GRE/IPsec 터널을 지원하고 구성의 크기 및 복잡성을 간소화하며 동적 터널 생성을 지원하는 GRE(Single Generic Routing Encapsulation) 인터페이스
- IPsec 터널 보호: 암호화 정책을 동적으로 생성 및 적용
- 라우팅: 동적 네트워크, 거의 모든 라우팅 프로토콜(EIGRP, Enhanced Interior Gateway Routing Protocol, RIP, OSPF, BGP, ODR)이 지원됩니다

### 사용되는 구성 요소

이 문서의 정보는 Cisco ASR1000 Series Aggregation Services Router, 버전 17.6.5(MD)를 기반으로 합니다.

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

### DMVPN이란?

DMVPN은 IPsec+GRE VPN을 손쉽고 동적이며 확장 가능하게 구축하기 위한 Cisco IOS 소프트웨어 솔루션입니다. 모든 디바이스를 정적으로 구성할 필요 없이 여러 사이트를 사용하여 VPN 네트워크를 구축할 수 있는 솔루션입니다. 거점을 거치지 않고 거점이 직접 소통할 수 있는 '허브 앤 스포크' 네트워크다. 암호화는 IPsec을 통해 지원되므로 DMVPN은 일반 인터넷 연결을 사용하여 여러 사이트를 연결하는 데 널리 사용됩니다.

### DMVPN의 작동 방식

- 스포크는 허브에 대한 동적 영구 GRE/IPsec 터널을 구축하지만 다른 스포크에는 구축하지 않습니다. NHRP 서버(허브)의 클라이언트로 등록됩니다.
- 스포크가 다른 스포크 뒤에 있는 대상(프라이빗) 서브넷으로 패킷을 전송해야 할 경우, NHRP를 통해 대상 스포크의 실제(외부) 주소를 쿼리합니다.
- 이제 시작 스포크가 대상 스포크에 대한 동적 GRE/IPsec 터널을 시작할 수 있습니다(피어 주소를 알기 때문).
- 동적 스포크-투-스포크 터널은 mGRE 인터페이스를 통해 구축됩니다.
- 트래픽이 중단되면 스포크 투 스포크 터널이 제거됩니다.

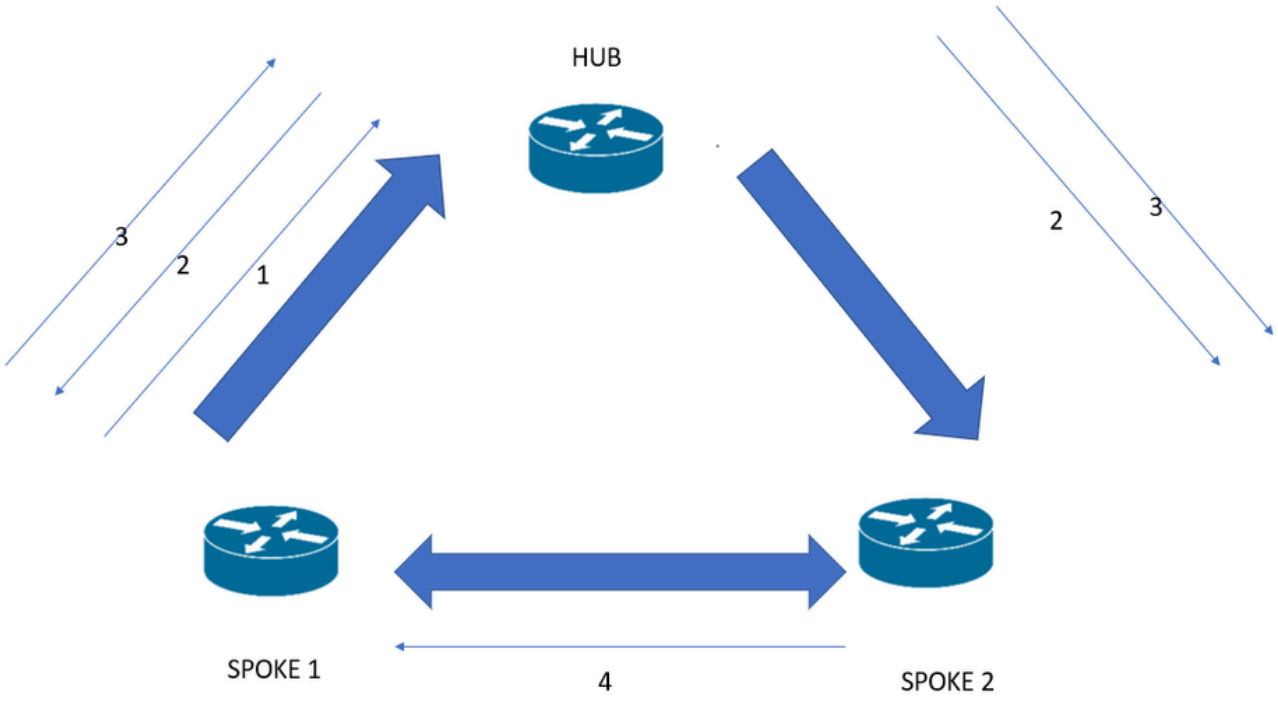
### DMVPN의 다양한 유형은 무엇입니까?

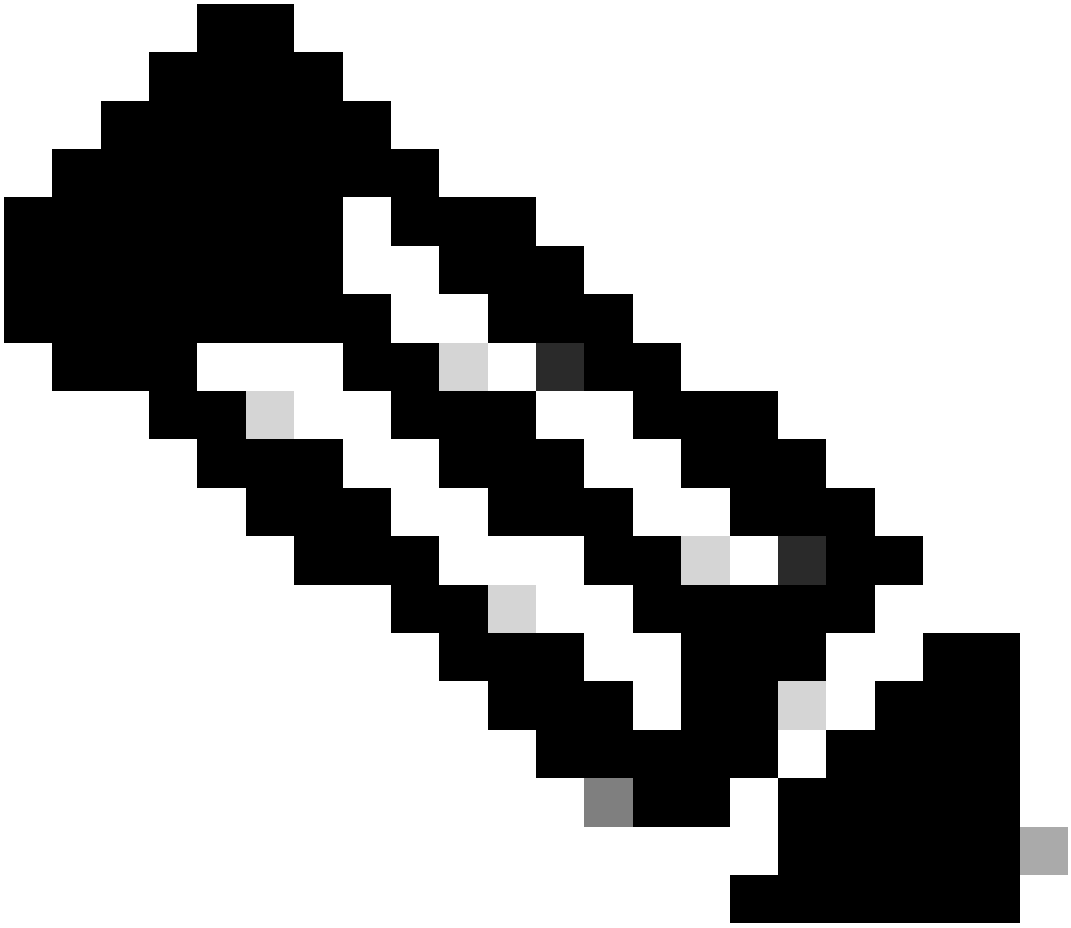
1. DMVPN 단계 I: 이 단계에서는 허브의 단일 mGRE 인터페이스가 포함되며, 모든 스포크는 여전히 고정 터널이므로 동적 스포크 대 스포크 연결을 얻을 수 없습니다.
2. DMVPN 단계 II: 이 단계에서는 모든 사이트가 mGRE 인터페이스로 구성되므로 동적 스포크 대 스포크 연결이 가능합니다.
3. DMVPN Phase III: 이 단계는 DMVPN 네트워크의 확장성에 따라 확장됩니다. 여기에는 DMVPN 클라우드로 요약하는 것이 포함됩니다. NHRP 리디렉션 및 NHRP 바로 가기 전환 구성과 함께. NHRP 리디렉션은 도달하려는 목적지로의 더 나은 경로를 찾기 위해 소스에 알립

니다. NHRP 바로 가기를 사용하면 DMVPN에서 다른 DMVPN 라우터 뒤의 다른 네트워크에 대해 알아볼 수 있습니다.

## DMVPN 3단계의 트래픽 흐름

1. 패킷은 (라우팅 테이블에 따라) Hub를 통해 Spoke의 1 네트워크에서 Spoke의 2 네트워크로 전송됩니다.
2. Hub는 패킷을 Spoke2로 라우팅하지만 Spoke2에 대한 최적이 아닌 경로 및 Spoke2의 터널 IP에 대한 정보를 포함하는 NHRP 리디렉션 메시지를 Spoke1로 병렬로 다시 전송합니다.
3. 그런 다음 Spoke1은 Spoke2의 NBMA(Nonbroadcast Multiaccess) IP 주소의 NHRP 확인 요청을 Spoke2의 목적지 IP가 있는 NHS(Next Hop Server)로 보냅니다. 이 NHRP 확인 요청은 NHS를 통해 Spoke2로 전송됩니다(라우팅 테이블에 따라). 일반적인 hop-by-hop NHRP 전달 프로세스입니다.
4. Spoke2가 Spoke1의 NBMA IP가 포함된 해결 요청을 받은 후 NHRP 해결 응답을 Spoke1에 직접 보냅니다. 응답이 허브를 통과하지 않습니다.
5. Spoke1이 Spoke2의 올바른 NBMA IP를 받은 후 대상 접두사에 대한 CEF 항목을 재작성합니다. 이 절차를 NHRP 바로가기라고 합니다.
6. 스포크는 인접성을 기울임으로써 NHRP를 트리거하지 않지만, NHRP 회신은 CEF를 업데이트합니다.



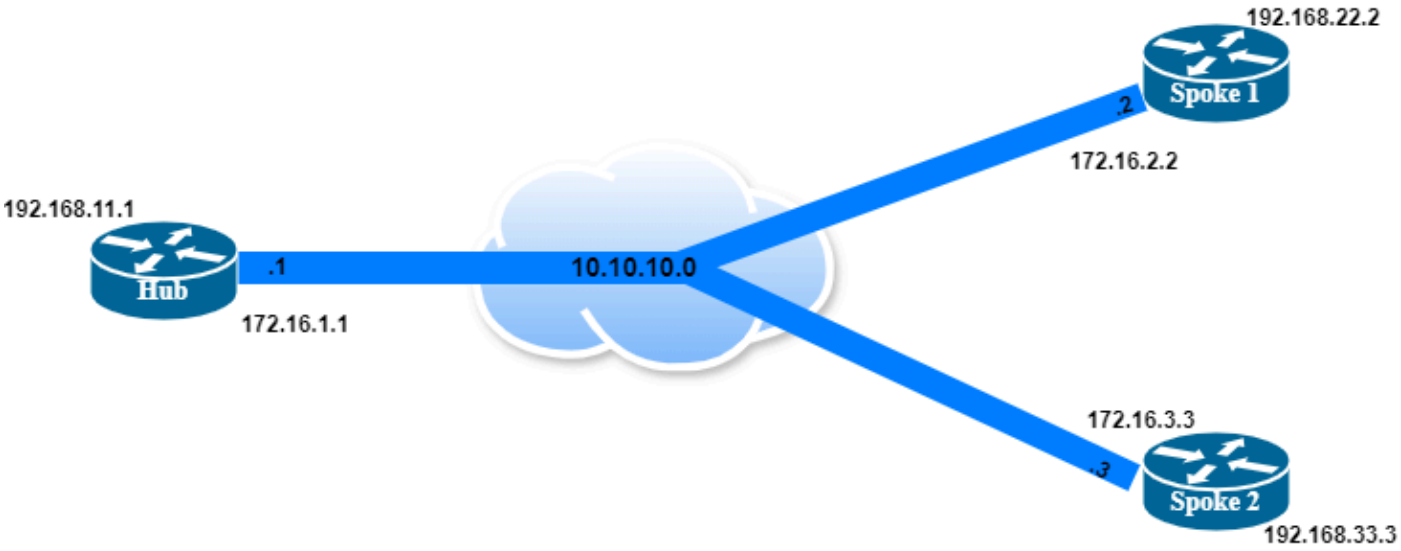


참고:

DMVPN 2단계: 이 단계에서는 CEF 인접성이 '병합' 상태이므로 초기 스포크-투-스포크 패킷이 실제로 프로세스 스위칭됩니다. 즉, 라우터에 CEF를 사용하여 패킷을 전달할 수 있는 충분한 정보가 없으며, NHRP(Next Hop Resolution Protocol)를 사용하여 다음 홉을 확인하기 위해 리소스 집약적인 프로세스 스위칭을 사용해야 합니다.

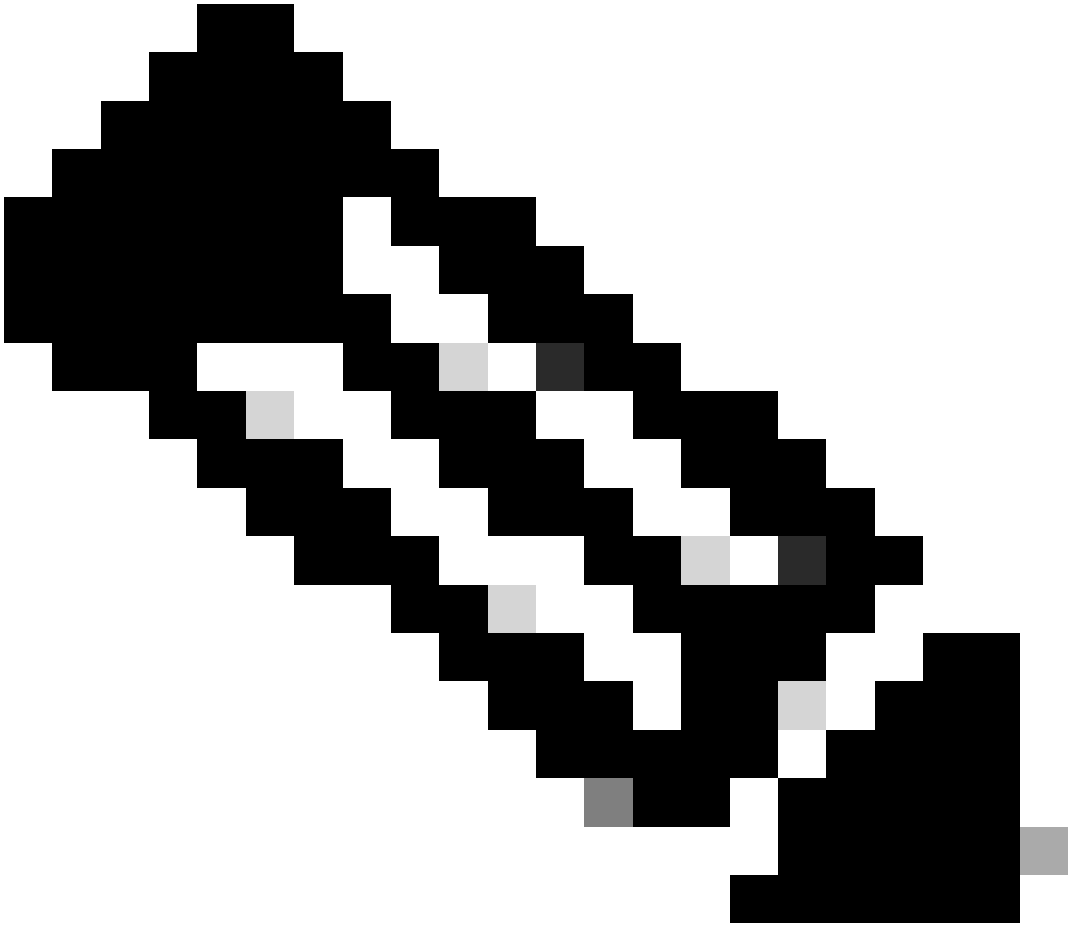
DMVPN 3단계: 이 단계는 시작 단계부터 CEF를 사용하여 초기 스포크-투-스포크 패킷을 스위칭할 수 있도록 함으로써 2단계에서 개선됩니다. 이는 NHRP Redirect 및 NHRP Shortcut 기능을 사용하여 구현되며, 이를 통해 직접 스포크 투 스포크 터널을 신속하게 설정할 수 있습니다. 그 결과, CEF가 보다 일관되게 사용되어 프로세스 스위칭에 대한 의존도가 줄어듭니다.

## 네트워크 다이어그램




# 설정

암호화 컨피그레이션



참고: 이것은 허브와 모든 스포크에서 동일합니다.

---

1. Ikev2 제안서 및 키링을 구성합니다.

```
crypto ikev2 제안 DMVPN
암호화 aes-cbc-256
무결성 sha256
그룹 14
crypto ikev2 keyring IKEV2-KEYRING
피어 any
주소 0.0.0.0 0.0.0
사전 공유 키 CISCO123
!
```

2. 모든 연결 관련 정보를 포함하는 Ikev2 프로필을 구성합니다.

```
crypto ikev2 프로필 IKEV2-PROF
```

match address 로컬 인터페이스 GigabitEthernet0/0/0
id 원격 주소 0.0.0.0 일치
인증 로컬 사전 공유
인증 원격 사전 공유
keyring 로컬 IKEV2-KEYRING

다음은 ikev2 프로필에 사용되는 명령의 세부 정보입니다.

- 주소 일치 로컬 인터페이스 GigabitEthernet0/0/0: VPN이 종료되는 로컬 외부 인터페이스(이 경우 GigabitEthernet0/0/0)
- match identity remote address 0.0.0.0: 원격 피어가 여러 개일 수 있으므로 모든 피어를 나타내는 0.0.0.0을 사용합니다.
- 인증 로컬 사전 공유: 로컬 사이트의 인증 모드는 사전 공유됨
- 인증 원격 사전 공유: 로컬 사이트의 인증 모드는 사전 공유됨
- 키링 로컬 IKEV2-KEYRING: 이전에 생성한 것과 동일한 키링을 사용합니다.

3. IPsec 프로필을 구성합니다.

crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
모드 터널

암호화 ipsec 프로필 IPSEC-IKEV2

set transform-set T-SET
ikev2-profile IKEV2-PROF 설정

IPsec 터널 협상에 대한 변형 집합을 생성하고 IPsec 프로필 아래에서 변형 집합 및 Ikev2 프로필을 호출합니다.

## DMVPN 컨피그레이션

1. 외부 인터페이스를 구성합니다.

인터페이스 GigabitEthernet0/0/0

ip 주소 172.16.1.1 255.255.255.0
자동 협상
cdp 활성화

2. mGRE 및 IPsec 통합을 위해 허브 라우터를 구성합니다(즉, 터널을 이전 절차에서 구성한 IPsec 프로필과 연결)

인터페이스 Tunnel0
ip 주소 10.10.10.1 255.255.255.0
no ip redirects
ip nhrp 인증 DMVPN
ip nhrp map multicast dynamic
ip nhrp network-id 1

```
ip nhrp 리디렉션 <-------- 허브 라우터에서 DMVPN Phase 3을 활성화하려면 필수
터널 소스 GigabitEthernet0/0/0
터널 모드 gre multipoint
터널 보호 ipsec 프로필 IPSEC-IKEV2
!
```

다음 명령은 터널 인터페이스 컨피그레이션에서 사용됩니다.

- ip nhrp 인증 DMVPN: 이 경우 'DMVPN' 인증 문자열은 동일한 DMVPN 네트워크에 속한 모든 허브 및 스포크에서 동일한 값을 가져야 합니다.
- ip nhrp 맵 멀티캐스트 동적: NHRP에서 동적으로 NHRP 멀티캐스트 매핑에 스포크를 추가할 수 있습니다.
- ip nhrp network-id 1: 인터페이스에서 NHRP를 활성화하는 32비트 네트워크 식별자입니다.
- ip nhrp 리디렉션: 트래픽이 NHRP 네트워크와 전달된 경우 리디렉션 트래픽 표시를 활성화합니다.
- 터널 소스 GigabitEthernet0/0/0: GigaEthernet 0/0/0 IP 주소를 사용하는 터널 인터페이스의 소스 주소를 설정합니다.
- 터널 모드 gre multipoint: 이 터널 인터페이스에 대해 캡슐화 모드를 mGRE로 설정합니다.
- 터널 보호 ipsec 프로필 IPSEC-IKEV2: 터널 인터페이스를 암호화 컨피그레이션에서 이미 생성된 IPsec 프로필과 연결합니다.

3. BGP(Border Gateway Protocol) 연결을 테스트하기 위해 외부 인터페이스 및 루프백과 함께 mGRE 및 IPsec 통합을 위한 스포크 라우터를 구성합니다.

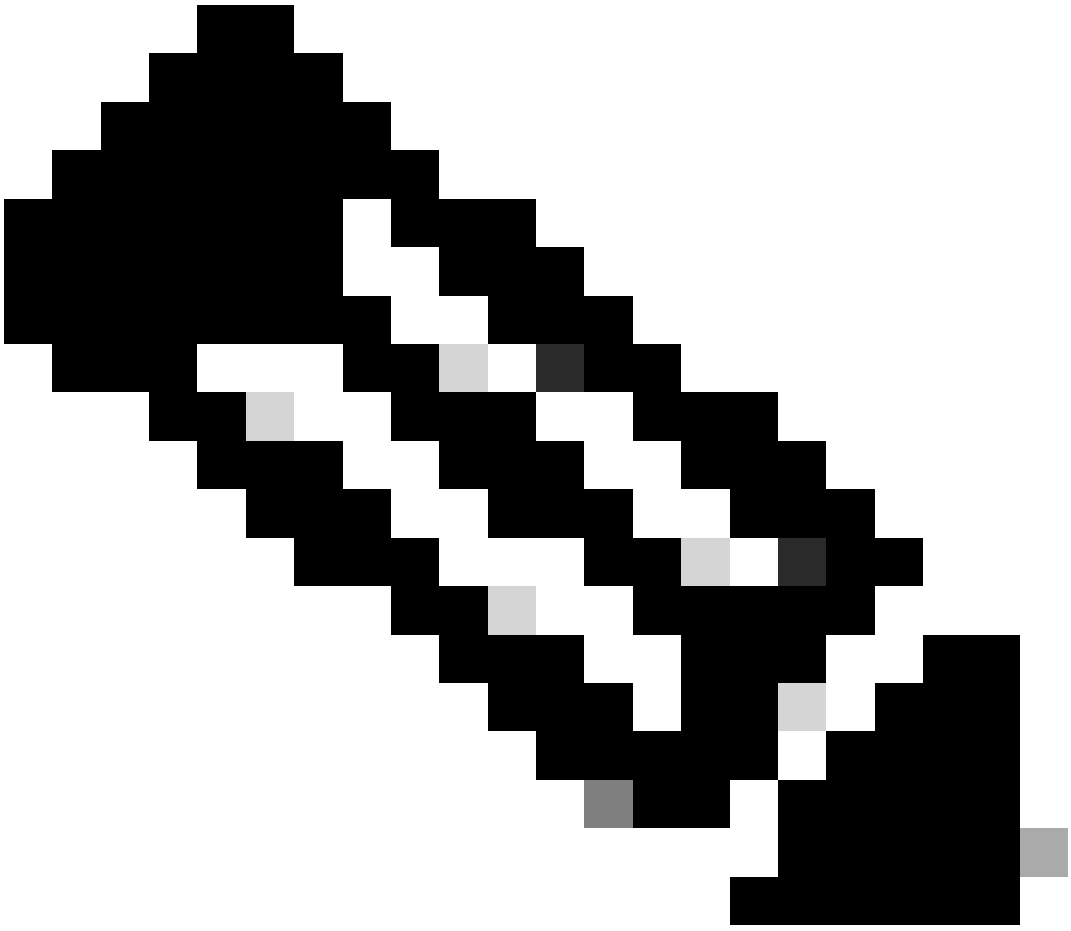
스포크 X: (모든 스포크에 유사한 컨피그레이션을 사용할 수 있음)

```
인터페이스 GigabitEthernet0/0/0
ip 주소 172.16.3.3 255.255.255.0
속도 1000
협상 자동 없음

!

인터페이스 루프백10
ip 주소 192.168.33.3 255.255.255.0
!
인터페이스 Tunnel0
ip 주소 10.10.10.3 255.255.255.0
no ip redirects
ip nhrp 인증 DMVPN
ip nhrp 맵 10.10.10.1 172.16.1.1
ip nhrp map multicast 172.16.1.1
ip nhrp network-id 1
ip nhrp nhs 10.10.10.1
ip nhrp 바로 가기 <-------- 스포크 라우터에서 DMVPN Phase 3을 활성화하는 데 필수
터널 소스 GigabitEthernet0/0/0
터널 모드 gre multipoint
터널 보호 ipsec 프로필 IPSEC-IKEV2
```

다음 명령은 터널 인터페이스 컨피그레이션에서 사용됩니다.

- ip nhrp 인증 DMVPN: 이 경우 'DMVPN' 인증 문자열은 동일한 DMVPN 네트워크에 속한 모든 허브 및 스포크에서 동일한 값을 가져야 합니다.
- ip nhrp 맵 10.10.10.1 172.16.1.1: 허브 NBMA IP 주소를 터널 인터페이스 IP 주소와 수동으로 매핑합니다.
- ip nhrp 맵 멀티캐스트 172.16.1.1: 모든 멀티캐스트 트래픽을 허브로 리디렉션합니다.
- ip nhrp network-id 1: 인터페이스에서 NHRP를 활성화하는 32비트 네트워크 식별자입니다.
- ip nhrp nhs 10.10.10.1: Hub인 다음 홉 서버는 이 명령을 사용하여 구성됩니다.
- ip nhrp 바로 가기: 인터페이스에서 NHRP 바로 가기 전환을 활성화합니다.
- 터널 소스 GigabitEthernet0/0/0: GigaEthernet 0/0/0 IP 주소를 사용하는 터널 인터페이스의 소스 주소를 설정합니다.
- 터널 모드 gre multipoint: 이 터널 인터페이스에 대해 캡슐화 모드를 mGRE로 설정합니다.
- 터널 보호 ipsec 프로필 IPSEC-IKEV2: 터널 인터페이스를 암호화 컨피그레이션에서 이미 생성된 IPsec 프로필과 연결합니다.

---



참고: ip nhrp redirect 명령은 "There is a better route to destination Spoke than via the Hub"(허브를 통하는 것보다 대상 스포크에 더 좋은 경로가 있습니다)라는 메시지를 스포크

---

에 전송하고 ip nhrp 바로 가기를 사용하면 스포크의 FIB(Forwarding Information Base)에 이 경로가 설치됩니다.

## BGP 컨피그레이션

다음과 같은 여러 가지 변형 중에서 선택할 수 있습니다.

- 각 스포크에 다른 AS 번호가 있는 eBGP
- 각 스포크에 동일한 AS 번호가 있는 eBGP
- iBGP

이 문서에서는 세 가지 시나리오를 모두 설명할 수 없습니다.

모든 스포크에서 다른 AS 번호를 가진 eBGP가 구성되었으므로 동적 인접 디바이스를 사용할 수 없습니다. 따라서 인접 디바이스를 수동으로 구성해야 합니다.

스포크에 다른 AS가 있는 eBGP

1. 허브의 BGP 컨피그레이션:

허브(config)#router bgp 65010

Hub(config-router)#bgp log-neighbor-changes

허브(config-router)#network 192.168.11.1 마스크 255.255.255.255

허브(config-router)#neighbor 10.10.10.2 remote-as 65011

허브(config-router)#neighbor 10.10.10.3 remote-as 65012

!

다음 명령은 허브의 BGP 컨피그레이션에서 사용됩니다.

- 라우터 bgp 65010: BGP 라우팅 프로세스를 구성합니다. 디바이스를 다른 BGP 스피커로 식별하는 'autonomous-system-number' 인수를 사용합니다.
- 네트워크 192.168.11.1 마스크 255.255.255.255: 네트워크를 이 자율 시스템에 대한 로컬로 지정하고 BGP 라우팅 테이블에 추가합니다.
- 인접 디바이스 10.10.10.2 remote-as 65011: 지정된 자동 시스템에 있는 인접 디바이스 스포크 1의 IP 주소를 로컬 디바이스의 IPv4 다중 프로토콜 BGP 인접 디바이스 테이블에 추가합니다.
- 인접 디바이스 10.10.10.3 remote-as 65012: 지정된 자동 시스템에 있는 인접 디바이스 스포크 2의 IP 주소를 로컬 디바이스의 IPv4 다중 프로토콜 BGP 인접 디바이스 테이블에 추가합니다.

2. 스포크 X의 BGP 컨피그레이션:

Spoke2(config)#router bgp 65012

Spoke2(config-router) #bgp 로그 인접 디바이스 변경

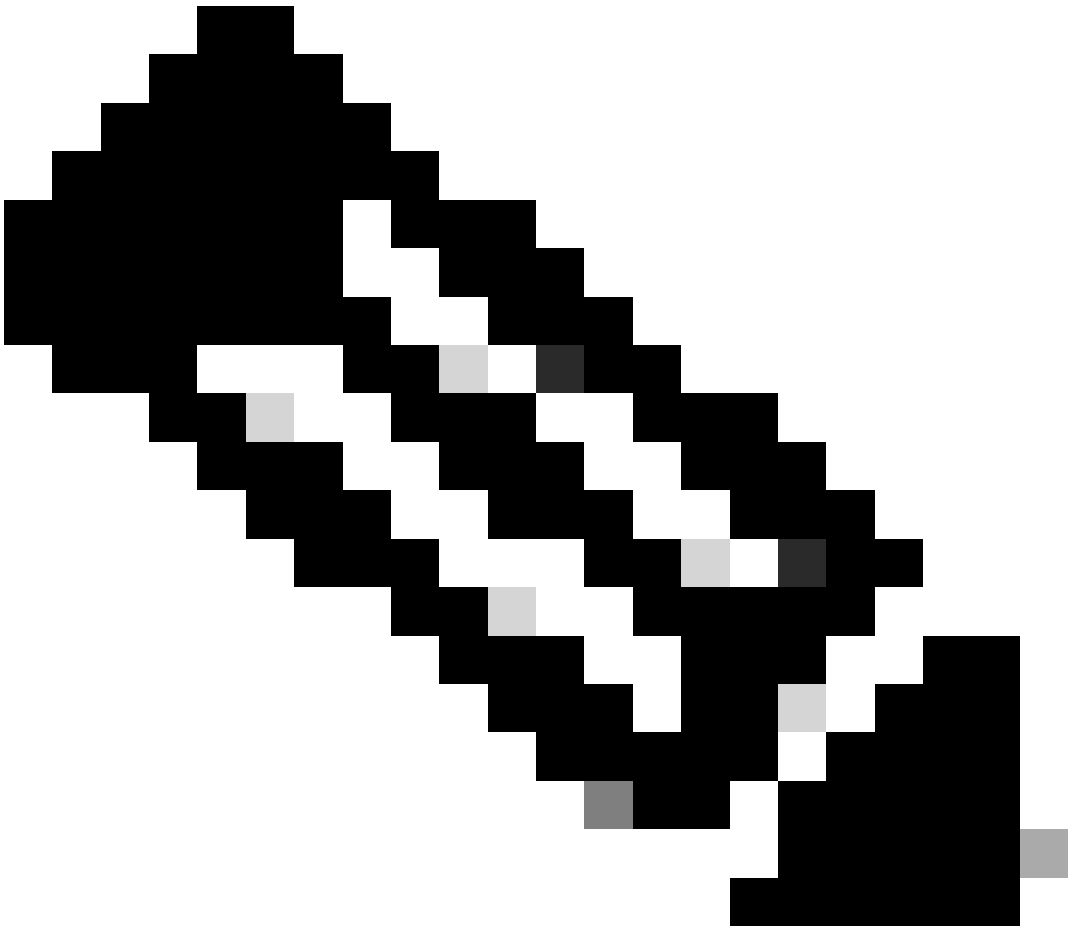
Spoke2(config-router)# 네트워크 192.168.33.3 마스크 255.255.255.255

Spoke2(config-router)# 인접 디바이스 10.10.10.1 remote-as 65010

다음 명령은 스포크 X의 BGP 컨피그레이션에서 사용됩니다.

- 라우터 bgp 65012: BGP 라우팅 프로세스를 구성합니다. 디바이스를 다른 BGP 스피커로 식별하는 'autonomous-system-number' 인수를 사용합니다.
- 네트워크 192.168.33.3 마스크 255.255.255.255: 네트워크를 이 자율 시스템에 대한 로컬로 지정하고 BGP 라우팅 테이블에 추가합니다.
- 인접 디바이스 10.10.10.1 remote-as 65010: 지정된 자동 시스템에 있는 허브의 IP 주소를 로컬 디바이스의 IPv4 다중 프로토콜 BGP 인접 디바이스 테이블에 추가합니다.

---



참고: DMVPN 네트워크의 모든 스포크에서 유사한 컨피그레이션을 수행해야 합니다.

---

# 다음을 확인합니다.

1. 허브 장치의 확인 명령:

HUB#sh dmvpn

DMVPN별 세션 정보를 표시합니다.

Legend: 속성 —> S - 정적, D - 동적, I - 불완전
N - NATed, L - 로컬, X - 소켓 없음
T1 - 설치된 경로, T2 - Nexthop-override
C - CTS 가능
# Ent —> NBMA 피어가 같은 NHRP 항목 수
NHS 상태: E —> Expected Replies, R —> Responding, W —> Waiting
터널의 UpDn 시간 —> Up 또는 Down 시간
==========

인터페이스: Tunnel0, IPv4 NHRP 세부사항
Type:Hub, NHRP Peers:2, <<<<<<<<<<<<<<<<<< 디바이스가 허브 역할을 하고 있음을 알려주며 NHRP 피어 2개가 이 허브에 연결되어 있습니다.

# Ent Peer NBMA 주소 피어 터널 상태 추가 UpDn Tm 속성
----- --------------- --------------- ----- -------- -----
1 172.16.2.2 10.10.10.2 UP 01:47:08D <<<<<<<<<<<<<<<<<<<<<<<<<<<<<< 두 피어가 모두 허브에 동적으로 등록되었으며 UP 상태입니다.
1 172.16.3.3 10.10.10.3 UP 01:08:58 D

HUB#sh ip nhrp

Hub에 연결된 모든 NHRP 피어의 터널 인터페이스 IP에 대한 NBMA 주소 매핑을 표시합니다. 허브는 모든 스포크의 데이터베이스를 유지 관리합니다.

10.10.10.2/32(10.10.10.2 경유)
Tunnel0가 생성됨 01:47:22, 만료됨 01:32:27
유형: 동적, 플래그: 고유 등록 사용 nhop
NBMA 주소: 172.16.2.2
10.10.10.3/32(10.10.10.3)
Tunnel0가 생성됨 01:09:11, 만료됨 01:29:58
유형: 동적, 플래그: 고유 등록 사용 nhop
NBMA 주소: 172.16.3.3

HUB#sh ip nhrp 멀티캐스트

NHRP 멀티캐스트 매핑 정보를 표시합니다.

NBMA 주소
Tunnel0 172.16.2.2 플래그: 동적(활성화됨)

Tunnel0 172.16.3.3 플래그: 동적(활성화됨)

HUB#sh 암호화 소켓

암호화 소켓 연결 수 2

Tu0 피어(로컬/원격): 172.16.1.1/172.16.2.2
로컬 Id(addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47 )
원격 ID(주소/마스크/포트/포트): (172.16.2.2/255.255.255.255/0/47 )
IPSec 프로필: "IPSEC-IKEV2"
소켓 상태: 열기
클라이언트: "TUNNEL SEC"(클라이언트 상태: 활성)
Tu0 피어(로컬/원격): 172.16.1.1/172.16.3.3
로컬 Id(addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47 )
원격 ID(주소/마스크/포트/포트): (172.16.3.3/255.255.255.255/0/47 )
IPSec 프로필: "IPSEC-IKEV2"
소켓 상태: 열기
클라이언트: "TUNNEL SEC"(클라이언트 상태: 활성)
수신 대기 상태의 암호화 소켓:
클라이언트: "TUNNEL SEC" 프로파일: "IPSEC-IKEV2" 맵 이름: "Tunnel0-head-0"

HUB#sh cry ikev2 sa

IPv4 암호화 IKEv2 SA

Tunnel-id 로컬 원격 fvrf/ivrf 상태
1 172.16.1.1/500 172.16.2.2/500 none/none READY
입력: AES-CBC, 키 크기: 256, PRF: SHA512, 해시: SHA512, DH Grp:5, 인증 기호: PSK, 인증 확인: PSK
수명/활성 시간: 86400/6524초

Tunnel-id 로컬 원격 fvrf/ivrf 상태
2 172.16.1.1/500 172.16.3.3/500 none/none READY
입력: AES-CBC, 키 크기: 256, PRF: SHA512, 해시: SHA512, DH Grp:5, 인증 기호: PSK, 인증 확인: PSK
수명/활성 시간: 86400/4234초

IPv6 암호화 IKEv2 SA

HUB#sh ip bgp 요약

BGP 세션의 현재 상태/라우터가 인접 디바이스 또는 피어 그룹에서 수신한 접두사 수를 표시합니다.

BGP 라우터 식별자 192.168.11.1 로컬 AS 번호 65010
BGP 테이블 버전은 4이고, 기본 라우팅 테이블 버전은 4입니다.
432바이트 메모리를 사용하는 네트워크 항목 3개
252바이트 메모리를 사용하는 경로 항목 3개

480바이트 메모리를 사용하는 3/3 BGP 경로/bestpath 특성 항목
48바이트 메모리를 사용하는 BGP AS-PATH 엔트리 2개
0바이트의 메모리를 사용하는 0개의 BGP route-map 캐시 항목
0바이트의 메모리를 사용하는 0개의 BGP filter-list 캐시 항목
총 메모리 1,212바이트를 사용하는 BGP
BGP 활동 3/0 접두사, 3/0 경로, 스캔 간격 60초

네이버 V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.2 4 65011 33 33 4 0 0 00:25:35 1
10.10.10.3 4 65012 21 25 4 0 0 00:14:58 1

Hub#sh ip 경로 bgp

코드: L - 로컬, C - 연결됨, S - 정적, R - RIP, M - 모바일, B - BGP
D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간
N1 - OSPF NSSA 외부 유형 1, N2 - OSPF NSSA 외부 유형 2
E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2
i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2
ia - IS-IS inter area, * - 후보 기본값, U - 사용자별 고정 경로
o - ODR, P - 정기적으로 다운로드되는 고정 경로, H - NHRP, I - LISP
a - 애플리케이션 경로
+ - 복제된 경로, % - 다음 홉 재정의, p - PfR에서 재정의

마지막 방법의 게이트웨이는 172.16.1.2에서 네트워크 0.0.0.0으로

192.168.0.0/16은 가변 서브넷으로, 서브넷 4개, 마스크 2개
B 192.168.22.0/24 [20/0] via 10.10.10.2, 00:29:15 <<<<<<<<<<<<<Spoke 1 알림 경로에 대한 항목

B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<<Spoke 2 알림 경로용 항목

2. 스포크 1의 확인 명령:

Spoke1#sh dmvpn

Legend: 속성 —> S - 정적, D - 동적, I - 불완전
N - NATed, L - 로컬, X - 소켓 없음
T1 - 설치된 경로, T2 - Nexthop-override
C - CTS 가능, I2 - 임시
# Ent —> NBMA 피어가 같은 NHRP 항목 수
NHS 상태: E —> Expected Replies, R —> Responding, W —> Waiting
터널의 UpDn 시간 —> Up 또는 Down 시간
==========

인터페이스: Tunnel0, IPv4 NHRP 세부사항
유형:스포크, NHRP 피어:2,

# Ent Peer NBMA 주소 피어 터널 상태 추가 UpDn Tm 속성
----- --------------- --------------- ----- -------- -----

1 172.16.1.1 10.10.10.10.1 UP 01:32:09 S <<<<<<<<<<<<<<Hub는 터널 인터페이스에 고정 항목으로 구성했으므로 S- static으로 표시됩니다.
1 172.16.3.3 10.10.10.10.3 UP 00:19:34 D <<<<<<<<<<<< 스포크 2로 트래픽을 전송한 후 생성된 동적 온디맨드 스포크 투 스포크 터널

Spoke1#sh ip bgp 요약

BGP 라우터 식별자 192.168.22.2, 로컬 AS 번호 65011
BGP 테이블 버전은 4이고, 기본 라우팅 테이블 버전은 4입니다.
744바이트 메모리를 사용하는 네트워크 항목 3개
432바이트 메모리를 사용하는 경로 항목 3개
864바이트 메모리를 사용하는 3/3 BGP 경로/bestpath 특성 항목
64바이트 메모리를 사용하는 BGP AS-PATH 엔트리 2개
0바이트의 메모리를 사용하는 0개의 BGP route-map 캐시 항목
0바이트의 메모리를 사용하는 0개의 BGP filter-list 캐시 항목
총 2104바이트의 메모리를 사용하는 BGP
BGP 활동 3/0 접두사, 3/0 경로, 스캔 간격 60초
3 networks peaked at 08:16:54 Jun 2 2022 UTC (01:11:51.732 전)

네이버 V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 4 65010 85 85 4 0 0 01:12:21 2 <<<<<<<<<<<<<<<<<<<< 허브 루프백과 Spoke2 루프백에 각각 해당하는 2개의 접두사를 Hub에서 받았습니다

Spoke1#sh ip 경로 bgp

코드: L - 로컬, C - 연결됨, S - 정적, R - RIP, M - 모바일, B - BGP
D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간
N1 - OSPF NSSA 외부 유형 1, N2 - OSPF NSSA 외부 유형 2
E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, m - OMP
n - NAT, Ni - NAT 내부, No - NAT 외부, Nd - NAT DIA
i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2
ia - IS-IS inter area, * - 후보 기본값, U - 사용자별 고정 경로
H - NHRP, G - NHRP 등록됨, G - NHRP 등록 요약
o - ODR, P - 정기적으로 다운로드되는 고정 경로, l - LISP
a - 애플리케이션 경로
+ - 복제된 경로, % - 다음 홉 재정의, p - PfR에서 재정의

마지막 방법의 게이트웨이는 172.16.2.10 - 네트워크 0.0.0.0입니다.

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 >>>>>>>>>>>>>>> 허브를 통해 직접 연결 가능한 허브 네트워크

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 >>>>>>>>>>>>>> Spoke network directly reachable via spoke tunnel IP.

Spoke1#sh ip 경로

코드: L - 로컬, C - 연결됨, S - 정적, R - RIP, M - 모바일, B - BGP
D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간
N1 - OSPF NSSA 외부 유형 1, N2 - OSPF NSSA 외부 유형 2
E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, m - OMP
n - NAT, Ni - NAT 내부, No - NAT 외부, Nd - NAT DIA
i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2
ia - IS-IS inter area, * - 후보 기본값, U - 사용자별 고정 경로
H - NHRP, G - NHRP 등록됨, G - NHRP 등록 요약
o - ODR, P - 정기적으로 다운로드되는 고정 경로, l - LISP
a - 애플리케이션 경로
+ - 복제된 경로, % - 다음 홉 재정의, p - PfR에서 재정의

마지막 방법의 게이트웨이는 172.16.2.10 - 네트워크 0.0.0.0입니다.

172.16.2.10을 통한 S* 0.0.0.0/0 [1/0]
172.16.2.0/24은 가변 서브넷으로, 서브넷 2개, 마스크 2개
C 172.16.2.0/24은 GigabitEthernet2로 직접 연결됩니다.
L 172.16.2.2/32은 직접 연결됨, GigabitEthernet2
10.0.0.0/8은 가변 서브넷입니다. 서브넷 2개, 마스크 2개
C 10.10.10.0/24은 Tunnel0으로 직접 연결됩니다.
L 10.10.10.2/32은 Tunnel0에 직접 연결되어 있습니다.
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:21
192.168.22.0/24은 가변 서브넷으로, 서브넷 2개, 마스크 2개
C 192.168.22.0/24은 직접 연결되어 있습니다. 루프백10
L 192.168.22.2/32은 직접 연결되어 있습니다. 루프백10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

Legend: E=응답 기대, R=응답, W=대기, D=동적
터널0:
10.10.10.1 RE 우선순위 = 0 클러스터 = 0 >>>>>>>> 다음 홉 서버가 하나만 구성됨

Spoke1#sh ip nhrp 트래픽

터널0: 최대 전송 제한: 10000Pkts/10Sec, 사용: 0%
보낸 날짜: 합계 52
1 해결 요청 0 해결 회신 51 등록 요청 <<<<<< < 허브로 등록 요청이 전송된 횟수
0 등록 응답 0 삭제 요청 0 삭제 응답
0 오류 표시 0 트래픽 표시 0 리디렉션 억제
수신: 합계 25
0 해결 요청 1 해결 회신 0 등록 요청 <<<<<<<<<<<< 해당 등록 요청에 대한 회신을 받은 횟수
24 등록 응답 0 삭제 요청 0 삭제 응답
0 오류 표시 0 트래픽 표시 0 리디렉션 억제

Spoke1#sh ip nhrp 멀티캐스트

NBMA 주소
터널0 172.16.1.1 플래그: 고정(활성화됨) <<<<<<<<<<< 허브 NBMA를 향해 멀티캐스트 트래픽이 전달되도록 구성됨

Spoke1#sh 암호화 소켓

암호화 소켓 연결 수 2

Tu0 피어(로컬/원격): 172.16.2.2/172.16.1.1
로컬 Id(addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47 )
원격 ID(주소/마스크/포트/포트): (172.16.1.1/255.255.255.255/0/47 )
IPSec 프로필: "IPSEC-IKEV2"
소켓 상태: 이 특정 피어에 대한 Socket의 <<<<<<<<<<<<< 상태를 엽니다.
클라이언트: "TUNNEL SEC"(클라이언트 상태: 활성)
Tu0 피어(로컬/원격): 172.16.2.2/172.16.3.3
로컬 Id(addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47 )
원격 ID(주소/마스크/포트/포트): (172.16.3.3/255.255.255.255/0/47 )
IPSec 프로필: "IPSEC-IKEV2"
소켓 상태: 열기
클라이언트: "TUNNEL SEC"(클라이언트 상태: 활성)
수신 대기 상태의 암호화 소켓:
클라이언트: "TUNNEL SEC" 프로파일: "IPSEC-IKEV2" 맵 이름: "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

IPv4 암호화 IKEv2 SA

Tunnel-id 로컬 원격 fvrf/ivrf 상태
2 172.16.2.2/500 172.16.3.3/500 none/none READY
입력: AES-CBC, 키 크기: 256, PRF: SHA512, 해시: SHA512, DH Grp:19, 인증 기호: PSK, 인증 확인: PSK
수명/활성 시간: 86400/287초

Tunnel-id 로컬 원격 fvrf/ivrf 상태
1 172.16.2.2/500 172.16.1.1/500 none/none READY
입력: AES-CBC, 키 크기: 256, PRF: SHA512, 해시: SHA512, DH Grp:19, 인증 기호: PSK, 인증 확인: PSK
수명/활성 시간: 86400/4643초

IPv6 암호화 IKEv2 SA

Spoke1#traceroute 192.168.33.3 소스 lo10

중단할 이스케이프 시퀀스를 입력합니다.
192.168.33.3에 대한 경로 추적
VRF 정보: (vrf in name/id, vrf out name/id)

1 10.10.10.3 3 msec 4 msec * <<<<<<<<<<<<<<<< 트래픽이 허브를 통과하지 않고 Spoke 2 라우터로 직접 이동합니다.

스포크2#sh dmvpn

Legend: 속성 —> S - 정적, D - 동적, I - 불완전
N - NATed, L - 로컬, X - 소켓 없음
T1 - 설치된 경로, T2 - Nexthop-override
C - CTS 가능, I2 - 임시
# Ent —> NBMA 피어가 같은 NHRP 항목 수
NHS 상태: E —> Expected Replies, R —> Responding, W —> Waiting
터널의 UpDn 시간 —> Up 또는 Down 시간
==========

인터페이스: Tunnel0, IPv4 NHRP 세부사항
유형:스포크, NHRP 피어:2,

# Ent Peer NBMA 주소 피어 터널 상태 추가 UpDn Tm 속성
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.1 UP 01:20:26 S
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. 스포크 2의 확인 명령:

Spoke2#sh ip nhrp

10.10.10.1/32(10.10.10.1 경유)
01:36:06에 생성된 Tunnel0, 만료되지 않음
유형: 정적, 플래그:
NBMA 주소: 172.16.1.1
10.10.10.2/32(10.10.10.2 경유)
Tunnel0가 생성됨 00:08:09, 만료됨 00:01:50
유형: 동적, 플래그: 라우터 암시적
NBMA 주소: 172.16.2.2
10.10.10.3/32(10.10.10.3)
Tunnel0가 생성됨 00:08:09, 만료됨 00:01:50
유형: 동적, 플래그: 라우터 고유 로컬
NBMA 주소: 172.16.3.3
(소켓 없음)
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp 멀티캐스트
NBMA 주소
Tunnel0 172.16.1.1 플래그: 고정(사용)
Spoke2#

Spoke2#sh 암호화 소켓

암호화 소켓 연결 수 2

Tu0 피어(로컬/원격): 172.16.3.3/172.16.1.1
로컬 Id(addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47 )
원격 ID(주소/마스크/포트/포트): (172.16.1.1/255.255.255.255/0/47 )
IPSec 프로필: "IPSEC-IKEV2"
소켓 상태: 특정 피어에 대한 Socket의 <<<<<<<<<<<<<<<<<<<< 상태를 엽니다.
클라이언트: "TUNNEL SEC"(클라이언트 상태: 활성)
Tu0 피어(로컬/원격): 172.16.3.3/172.16.2.2
로컬 Id(addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47 )
원격 ID(주소/마스크/포트/포트): (172.16.2.2/255.255.255.255/0/47 )
IPSec 프로필: "IPSEC-IKEV2"
소켓 상태: 열기
클라이언트: "TUNNEL SEC"(클라이언트 상태: 활성)
수신 대기 상태의 암호화 소켓:
클라이언트: "TUNNEL SEC" 프로파일: "IPSEC-IKEV2" 맵 이름: "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

IPv4 암호화 IKEv2 SA

Tunnel-id 로컬 원격 fvrf/ivrf 상태
2 172.16.3.3/500 172.16.2.2/500 none/none READY
입력: AES-CBC, 키 크기: 256, PRF: SHA512, 해시: SHA512, DH Grp:19, 인증 기호: PSK, 인증 확인: PSK
수명/활성 시간: 86400/509초

Tunnel-id 로컬 원격 fvrf/ivrf 상태
1 172.16.3.3/500 172.16.1.1/500 none/none READY
입력: AES-CBC, 키 크기: 256, PRF: SHA512, 해시: SHA512, DH Grp:19, 인증 기호: PSK, 인증 확인: PSK
수명/활성 시간: 86400/4866초

IPv6 암호화 IKEv2 SA

Spoke2#sh ip bgp 요약

BGP 라우터 식별자 192.168.33.3, 로컬 AS 번호 65012
BGP 테이블 버전은 4이고, 기본 라우팅 테이블 버전은 4입니다.
744바이트 메모리를 사용하는 네트워크 항목 3개
432바이트 메모리를 사용하는 경로 항목 3개
864바이트 메모리를 사용하는 3/3 BGP 경로/bestpath 특성 항목
64바이트 메모리를 사용하는 BGP AS-PATH 엔트리 2개
0바이트의 메모리를 사용하는 0개의 BGP route-map 캐시 항목
0바이트의 메모리를 사용하는 0개의 BGP filter-list 캐시 항목
총 2104바이트의 메모리를 사용하는 BGP
BGP 활동 3/0 접두사, 3/0 경로, 스캔 간격 60초
3 networks peaked at 08:16:54 Jun 2 2022 UTC (01:20:43.775 전)

네이버 V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.10.10.1 465010 97 94 4 0 0 01:21:07 2 >>>>>>>>>>>>>>> 허브 루프백 및 Spoke2 루프백에 각각 해당하는 2개의 접두사를 허브에서 받았습니다

Spoke2#sh ip 경로

코드: L - 로컬, C - 연결됨, S - 정적, R - RIP, M - 모바일, B - BGP
D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간
N1 - OSPF NSSA 외부 유형 1, N2 - OSPF NSSA 외부 유형 2
E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, m - OMP
n - NAT, Ni - NAT 내부, No - NAT 외부, Nd - NAT DIA
i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2
ia - IS-IS inter area, * - 후보 기본값, U - 사용자별 고정 경로
H - NHRP, G - NHRP 등록됨, G - NHRP 등록 요약
o - ODR, P - 정기적으로 다운로드되는 고정 경로, l - LISP
a - 애플리케이션 경로
+ - 복제된 경로, % - 다음 홉 재정의, p - PfR에서 재정의

마지막 방법의 게이트웨이는 172.16.3.10 - 네트워크 0.0.0.0입니다.

172.16.3.10을 통한 S* 0.0.0.0/0 [1/0]
172.16.3.0/24/8은 가변 서브넷으로, 서브넷 2개, 마스크 2개
C 172.16.3.0/24은 GigabitEthernet3으로 직접 연결됩니다.
L 172.16.3.3/32은 직접 연결됨, GigabitEthernet3
10.0.0.0/8은 가변 서브넷입니다. 서브넷 2개, 마스크 2개
C 10.10.10.0/24은 Tunnel0으로 직접 연결됩니다.
L 10.10.10.3/32은 Tunnel0에 직접 연결되어 있습니다.
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:46:45
192.168.33.0/24은 가변 서브넷으로, 서브넷 2개, 마스크 2개
C 192.168.33.0/24은 직접 연결되어 있습니다. 루프백10
L 192.168.33.3/32은 직접 연결되어 있습니다. 루프백10

Spoke2#sh ip 경로 bgp

코드: L - 로컬, C - 연결됨, S - 정적, R - RIP, M - 모바일, B - BGP
D - EIGRP, EX - EIGRP 외부, O - OSPF, IA - OSPF 영역 간
N1 - OSPF NSSA 외부 유형 1, N2 - OSPF NSSA 외부 유형 2
E1 - OSPF 외부 유형 1, E2 - OSPF 외부 유형 2, m - OMP
n - NAT, Ni - NAT 내부, No - NAT 외부, Nd - NAT DIA
i - IS-IS, su - IS-IS 요약, L1 - IS-IS 레벨 1, L2 - IS-IS 레벨 2
ia - IS-IS inter area, * - 후보 기본값, U - 사용자별 고정 경로
H - NHRP, G - NHRP 등록됨, G - NHRP 등록 요약
o - ODR, P - 정기적으로 다운로드되는 고정 경로, l - LISP
a - 애플리케이션 경로
+ - 복제된 경로, % - 다음 홉 재정의, p - PfR에서 재정의

마지막 방법의 게이트웨이는 172.16.3.10 - 네트워크 0.0.0.0입니다.

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 >>>>>>>>>>>>>>>>>>허브를 통해 직접 연결할 수 있는 허브 네트워크
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>>>> Spoke network directly reachable via spoke tunnel IP.

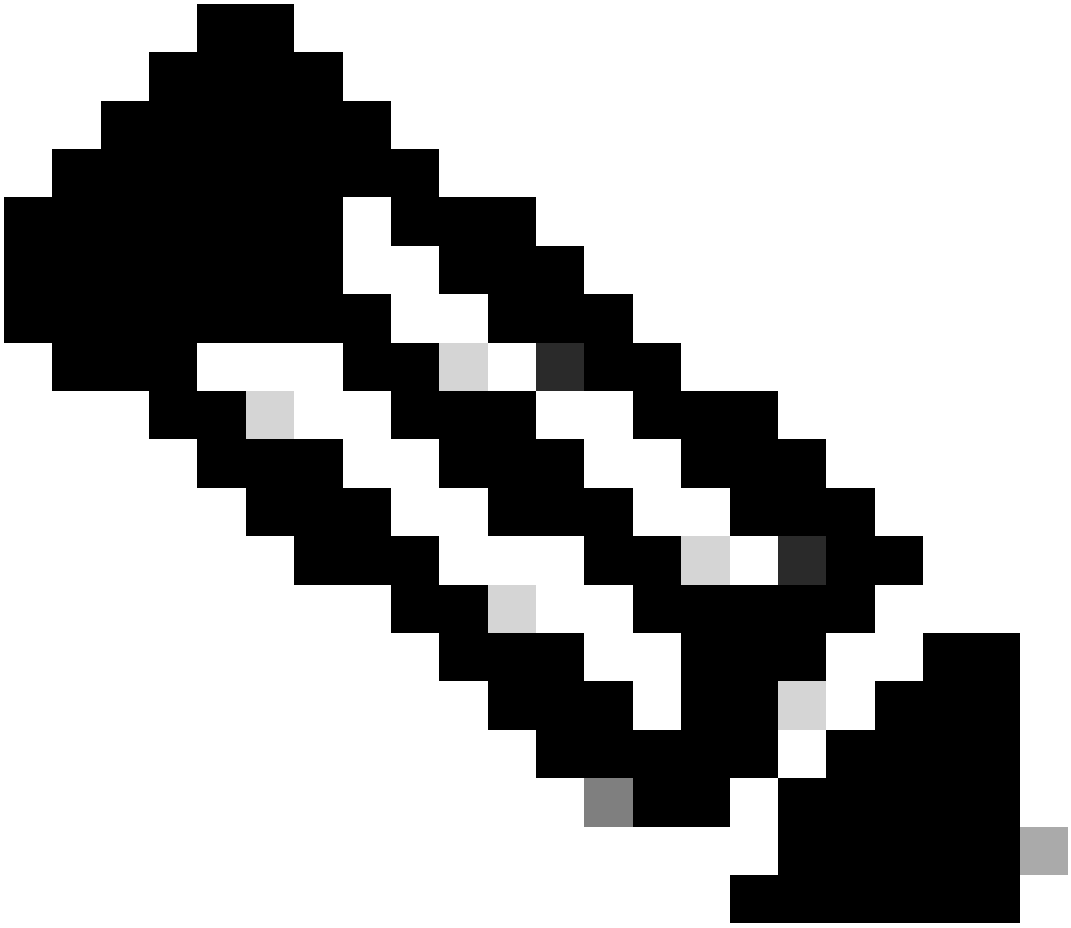
Spoke2#sh ip nhrp nhs

Legend: E=응답 기대, R=응답, W=대기, D=동적
터널0:
10.10.10.1 RE 우선순위 = 0 클러스터 = 0 >>>>>>>>>>>>> 다음 홉 서버가 하나만 구성됨

Spoke2#traceroute 192.168.22.2 소스 루프백 10

중단할 이스케이프 시퀀스를 입력합니다.
192.168.22.2에 대한 경로 추적
VRF 정보: (vrf in name/id, vrf out name/id)
1 10.10.10.2 4 msec * <<<<<<<<<<<<<<<<< 트래픽이 허브를 통과하지 않고 직접 Spoke 1 라우터로 이동합니다.

# 문제 해결



참고: 비조건부 디버그를 실행하면 프로세서와 프로덕션 환경에 영향을 줄 수 있으므로 항상 조건부 디버그를 사용하는 것이 좋습니다. NBMA 주소는 '외부 IP 주소'(터널 인터페이스의 소스에 사용되는 IP 주소)에 해당하고, 터널 IP는 '논리적 IP 주소, 즉 터널 인터페이스의 IP 주소'에 해당합니다.

---

디버그 dmvpn 조건 피어 <nmbma/tunnel> <NMBA IP 또는 피어의 터널 IP 주소>
디버그 암호화 조건 피어 ipv4 <피어의 WAN IP>
디버그 nhrp 조건 피어 <nbma/tunnel> <NBMA 또는 피어의 터널 IP 주소>

DMVPN 문제를 해결하려면 계층화된 접근 방식을 채택해야 합니다.

debug dmvpn detail all


1. 암호화 계층: 두 피어 간의 물리적 연결을 확인한 후 암호화를 확인해야 합니다. 이 레이어는 GRE 패킷을 암호화/해독합니다.

암호화 부분을 확인하는 데 사용되는 일반적인 디버그 명령:

디버그 암호화 조건 피어 ipv4 <피어의 WAN IP 주소>

crypto ikev2 디버그

디버그 crypto ikev2 오류

crypto ikev2 내부 디버그

crypto ikev2 패킷 디버그

암호화 ipsec 디버그

디버그 암호화 ipsec 오류

또는

디버그 dmvpn 조건 피어 <nmbma/tunnel> <NMBA IP 또는 피어의 터널 IP 주소>

디버그 암호화 조건 피어 ipv4 <피어의 WAN IP>

dmvpn 세부 정보 암호화 디버그

암호화 레이어 트러블슈팅에 대한 자세한 내용은 외부 링크를 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

2. GRE/NHRP: NHRP 등록에 실패하고 스포크의 동적 NBMA 주소 변경으로 인해 허브의 NHRP 매핑이 일관되지 않는 경우가 대표적인 문제입니다.

NHRP 매핑을 확인하는 데 사용되는 일반적인 디버그 명령:

디버그 nhrp 조건 피어 <nbma/tunnel> <NBMA 또는 피어의 터널 IP 주소>

nhrp 캐시 디버그

nhrp 패킷 디버그

nhrp 세부 정보 디버그

디버그 nhrp 오류

가장 일반적인 DMVPN 문제 해결 솔루션에 대한 이해는 외부 링크를 참조 하십시오.

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

3. 라우팅: 라우팅 프로토콜은 온디맨드 스포크-스포크 터널의 상태를 모니터링하지 않습니다.

IP 라우팅 업데이트 및 IP 멀티캐스트 데이터 패킷은 허브-앤-스포크 터널만 통과합니다.

유니캐스트 IP 데이터 패킷이 허브-스포크 및 온디맨드 스포크-스포크 터널을 모두 통과합니다.

디버그: 라우팅 프로토콜에 따라 다양한 debug 명령

BGP 라우팅 Deep Dive는 외부 링크를 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

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.