ASR 1000을 사용한 오버레이 전송 가상화 구성

목차

소개

이 문서에서는 ASR1000 및 Catalyst 8300/8500 시리즈 라우터에서 지원되는 OTV(Overlay Transport Virtualization) 네트워크 토폴로지에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASR1000, IOS® XE 버전 16.10.1a 이상
- Catalyst 8300, IOS® XE 버전 17.5.1a 이상
- Catalyst 8500, IOS® XE 버전 17.6.1a 이상

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

ASR1000은 Cisco IOS® XE 릴리스 3.5 이후 OTV를 지원합니다. Catalyst 8300 Series 라우터는 IOS® XE17.5.1a로 지원을 시작하고 Catalyst 8500 Series 경로는 IOS® XE 버전 17.6.1a로 지원을 시작합니다.

OTV는 전송 네트워크의 MAC 주소 기반 라우팅 및 MAC-in-IP(IP-encapsulated forwarding)를 통해 원격 네트워크 사이트 간에 레이어 2 연결을 제공하여 클러스터 및 가상화와 같이 레이어 2 인접성이 필요한 애플리케이션을 지원합니다. OTV는 오버레이 컨트롤 플레인 프로토콜을 사용하여 오버레이 네트워크 전반에 MAC 라우팅 정보를 학습하고 전파합니다. OTV 컨트롤 플레인 프로토콜은 IS-IS(Intermediate-System-to-Intermediate-System) 메시지를 사용하여 원격 사이트에 대한 인접성을 구축하고 원격 사이트에 MAC 경로 업데이트를 전송합니다. OTV는 원격 OTV 디바이스를 자동으로 검색하여 오버레이 네트워크의 원격 사이트에 대한 레이어 2 인접성을 구축합니다.

레이어 2 확장을 위한 OTV의 이점은 다음과 같습니다.

- MPLS 요구 사항 없음
- 메시에 대한 복잡한 EoMPLS(Ethernet over Multiprotocol Label Switching) 컨피그레이션 없음
- 레이어 2 확장을 위한 복잡한 VPLS(Virtual Private LAN Services) 구축 없음
- 네이티브 스패닝 트리 격리
    - 브리지 BPDU(Data Protocol Unit) 필터를 명시적으로 구성할 필요 없음
    - 스패닝 트리 문제를 지정된 데이터 센터로 기본 격리
- 네이티브 알 수 없는 유니캐스트 플러딩 격리
    - 알 수 없는 유니캐스트 MAC 패킷은 전달되지 않습니다
    - mac별 알 수 없는 유니캐스트 착신 전환 지원이 허용됩니다.
- OTV ARP 캐싱을 통한 ARP(Address Resolution Protocol) 최적화
    - 불필요한 WAN 트래픽 감소
- FHRP(First Hop Redundancy Protocol) 격리의 간소화된 프로비저닝
- 사이트 추가 간소화
- 간소화된 이중화 구성
- 임시 서비스가 필요한 경우 마이그레이션을 위한 "어플라이언스 삭제" 가능

요구 사항

후속 항목은 OTV 구축을 설계할 때 유의해야 할 기본 규칙입니다. 이러한 규칙을 준수하면 설계 및 구축이 간소화됩니다.

- 구성된 모든 OTV 오버레이 인터페이스에 대해 OTV 캡슐화된 트래픽(조인 인터페이스라고

함)을 전송하는 데 하나의 인터페이스만 사용할 수 있습니다
- OTV 사이트 VLAN에 대한 데이터 센터 L2 서비스 인스턴스 및 구성된 모든 OTV 오버레이 인터페이스에 대해 데이터 센터 간에 확장된 VLAN을 구성하는 데 하나의 인터페이스만 사용할 수 있습니다
- 포트 채널은 인터페이스 이중화 및 VSS 또는 VPC 스위치와의 연결에 사용할 수 있으며 연결을 위한 "단일" 인터페이스로 지원됩니다.
- 모든 OTV 라우터는 조인 인터페이스를 통해 연결할 수 있어야 합니다
- 데이터 센터를 가리키는 OTV 라우터에 스패닝 트리를 구성해야 합니다
- 데이터 센터 멀티캐스트 트래픽을 올바르게 전달하도록 IGMP 스누핑 및 쿼리를 구성해야 합니다.
- 지정된 데이터 센터는 1개 또는 2개의 OTV 라우터로 구성할 수 있습니다. 두 개의 라우터를 사용하면 VLAN 번호에 따라 홀수/짝수 방식으로 VLAN 포워딩을 분배합니다. 데이터 센터의 각 OTV 라우터는 다른 라우터에 대한 백업 역할을 합니다.
- 멀티홈 쌍은 동일한 OTV 사이트 식별자로 구성해야 합니다.
- ASR1000/Catalyst 8300/Catalyst 8500 및 Nexus 7000은 동일한 OTV 네트워크에 참여할 수 있습니다
    - Nexus 7000은 OTV 단편화 또는 암호화를 지원하지 않으므로 "하이브리드" 구축에서는 이러한 기능을 사용할 수 없습니다.

명시된 규칙을 준수하지 않는, 지원되는 특정 백투백 연결 설계가 있습니다. 이러한 컨피그레이션은 지원되지만 권장되지 않습니다. 이에 대한 자세한 내용은 이후 섹션 "Special case unicast topology(특수 케이스 유니캐스트 토폴로지)"에서 확인할 수 있습니다.

OTV에 대한 조인 및 L2 액세스 인터페이스의 컨피그레이션을 수행할 때 현재 OTV 소프트웨어에서 "단일" 인터페이스 제한이 있다는 점을 강조할 수 없습니다. 이중화를 위해 포트 채널 인터페이스를 사용할 수 있습니다. VPC에서 Nexus 7000에 대한 포트 채널 연결이 지원됩니다. 단일 스위치에 대한 기본 포트 채널 연결도 지원됩니다.

OTV 구현 유형

OTV에는 단일 조인 인터페이스 및 단일 L2 인터페이스가 필요합니다. 각 OTV 라우터당 하나만 지원할 수 있습니다. 또한 OTV에서는 멀티홈 OTV 라우터가 로컬 네트워크를 통해 서로 통신할 수 있도록 사이트 VLAN을 구성해야 합니다. 싱글 홈 OTV 라우터도 OTV 사이트 VLAN을 구성해야 합니다. 또한 각 사이트 또는 데이터 센터에는 고유한 사이트 식별자가 구성되어 있어야 합니다. 듀얼 홈 OTV 라우터는 동일한 사이트 식별자를 사용하고 동일한 VLAN을 통해 통신할 수 있어야 합니다.

후속 컨피그레이션에서는 OTV에 필요한 기본 컨피그레이션을 제공합니다. 그러나 유니캐스트 또는 멀티캐스트 코어 컨피그레이션을 추가해야 하므로 완료되지 않습니다. 이러한 내용은 이 문서의 후속 섹션에 자세히 설명되어 있습니다.

```
otv site bridge-domain 100
otv site-identifier 0000.0000.1111
!
interface Overlay1
  no ip address
  otv join-interface GigabitEthernet0/0/0
  service instance 99 ethernet
```

```
    encapsulation dot1q 99
    bridge-domain 99
  !
  service instance 90 ethernet
    encapsulation dot1q 90
    bridge-domain 90
!
interface GigabitEthernet1/0/1
  no ip address
  negotiation auto
  service instance 100 ethernet
    encapsulation dot1q 100
    bridge-domain 100
  !
  service instance 99 ethernet
    encapsulation dot1q 99
    bridge-domain 99
  !
  service instance 98 ethernet
    encapsulation dot1q 98 second-dot1q 1098
    rewrite ingress tag trans 2-to-1 dot1q 90 symmetric
    bridge-domain 90
```

서비스 인스턴스 컨피그레이션은 OTV를 사용하는 모든 L2 인터페이스 컨피그레이션에 사용됩니다.

L2 인터페이스의 각 서비스 인스턴스는 특정 단일 또는 이중 태그 캡슐화와 연결되어야 합니다.

차례로, 이러한 각 서비스 인스턴스는 브리지 도메인과 연결되어야 합니다.

이 브리지 도메인은 오버레이 인터페이스에 구성된 서비스 인스턴스에서 사용됩니다.

bridge-domain은 오버레이 서비스 인스턴스를 L2 인터페이스 서비스 인스턴스에 연결하는 접착제입니다.

오버레이 인터페이스의 트래픽 캡슐화는 L2 인터페이스의 인그레스(ingress)를 재작성한 후 트래픽의 캡슐화와 일치해야 합니다.

이 예에서 Gig1/0/1 서비스 인스턴스 99에 인그레스되는 트래픽은 단일 802.1Q VLAN 99와 브리지 도메인 99를 가집니다. 오버레이 인터페이스에 브리지 도메인 99가 있는 해당 서비스 인스턴스는 단일 802.1Q VLAN 99에 대해서도 구성됩니다. 이 경우가 가장 간단합니다.

이 예에서 Gig1/0/1 서비스 인스턴스 98에 인그레스되는 트래픽의 이중 802.1Q VLAN은 99 및 1098이고 브리지 도메인 90입니다. 오버레이 인터페이스에 브리지 도메인 90이 있는 해당 서비스 인스턴스는 90의 단일 802.1Q VLAN에 대해 구성됩니다. 이는 확실히 동일하지 않습니다. rewrite ingress 명령은 트래픽이 인그레스 인터페이스를 통해 이동할 때 태그가 올바르게 변환되도록 합니다. L2 인터페이스에 들어오는 트래픽에는 98/1098 802.1Q VLAN이 있습니다. 대칭 키워드는 L2 인터페이스를 나가는 트래픽에 90의 단일 802.1Q VLAN이 있는지 확인합니다.

OTV에서 확장되는 여러 802.1Q VLAN이 있는 서비스 인스턴스는 rewrite ingress 명령을 사용해야 합니다. OTV 캡슐화는 단일 VLAN 식별자만 지원합니다. 따라서 L2 인터페이스의 이중 VLAN 컨피그레이션은 오버레이 인터페이스 서비스 인스턴스의 단일 태그에 다시 기록해야 합니다. 이 경

우 모호한 VLAN 컨피그레이션을 지원하지 않습니다.

태그 재작성에 대한 자세한 내용은 다음 문서를 참조하십시오.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

이 예에서 OTV 사이트 bridge-domain은 100입니다.

- OTV 사이트 브리지 도메인은 L2 인터페이스에서만 구성됩니다.
- OTV 사이트 브리지 도메인은 OTV 구축을 불안정하게 하므로 오버레이 인터페이스에서 구성하지 않아야 합니다.
- OTV 사이트 VLAN은 OTV 라우터에만 연결해야 하며 다른 데이터 센터/사용자 트래픽을 전달해서는 안 됩니다.
- OTV 사이트 VLAN은 OTV 확장 VLAN과 동일한 물리적 인터페이스에 있어야 합니다.

멀티홈

데이터 센터는 단일 OTV 호스트로 연결하거나 이중화를 위해 최대 2개를 멀티홈으로 연결할 수 있습니다. 멀티홈은 복원력 및 로드 밸런싱에 사용됩니다. 사이트에 둘 이상의 에지 디바이스가 있고 둘 다 동일한 오버레이 네트워크에 참여하는 경우 해당 사이트는 멀티홈(multihomed)으로 간주됩니다. OTV Multihome은 VLAN 번호를 기반으로 홀수/짝수 방식으로 동일한 사이트에 속하는 두 OTV 라우터 간의 VLAN을 분할합니다. 하나의 에지 장치는 모든 홀수 VLAN의 AED로 선택되고 다른 OTV 라우터는 모든 짝수 VLAN의 AED로 선택됩니다. 각 AED는 다른 라우터에서 활성 상태인 VLAN에 대한 대기 상태입니다. AED 중 하나에서 링크 또는 노드 장애가 발생하면 대기 AED는 모든 VLAN에 대해 액티브 상태가 됩니다.

두 ASR1000을 동일한 데이터 센터에 연결하여 멀티홈을 수행하는 경우 두 ASR1000 간에 전용 링크가 필요하지 않습니다. OTV는 내부 인터페이스를 통해 전파되고 조인 인터페이스를 통해 통신하는 OTV 사이트 VLAN을 사용하여 짝수 및 홀수 VLAN을 담당하는 라우터를 결정합니다.

ASR1000 및 Nexus 7000은 동일한 데이터 센터에서 다른 라우터에 대한 백업으로 두 라우터에 구성된 OTV와 혼합할 수 없습니다. 특정 데이터 센터의 멀티홈은 일치하는 플랫폼(ASR1000 또는 Nexus 7000)에 대해 지원됩니다. 한 데이터 센터에는 ASR1000을, 다른 데이터 센터에는 Nexus 7000을 포함할 수 있습니다. 이 두 플랫폼 간의 상호 운용성이 테스트 및 지원되었습니다. 일부 데이터 센터는 멀티홈 방식이지만 다른 데이터 센터는 싱글홈 방식입니다.

멀티홈 ASR1000 라우터 쌍은 동일한 버전의 Cisco IOS® XE 소프트웨어를 실행해야 합니다.

Multihome을 사용하는 경우 OTV 라우터에서 TCN(Topology Change Notification)을 전송할 수 있으므로 OTV 라우터에서 스패닝 트리를 활성화하는 것이 좋습니다. 그러면 인접한 L2 스위치 디바이스가 스패닝 트리의 다른 스위치와 함께 에이징 타이머를 기본값에서 15초로 줄입니다. 이렇게 하면 멀티홈 쌍 간에 장애 또는 복구가 있을 때 속도 컨버전스가 크게 증가합니다. 전역 컨피그레이션에 후속 행을 추가하여 구성된 모든 서비스 인스턴스(OTV 등에 연결됨)에 대해 스패닝 트리를 활성화할 수 있습니다.

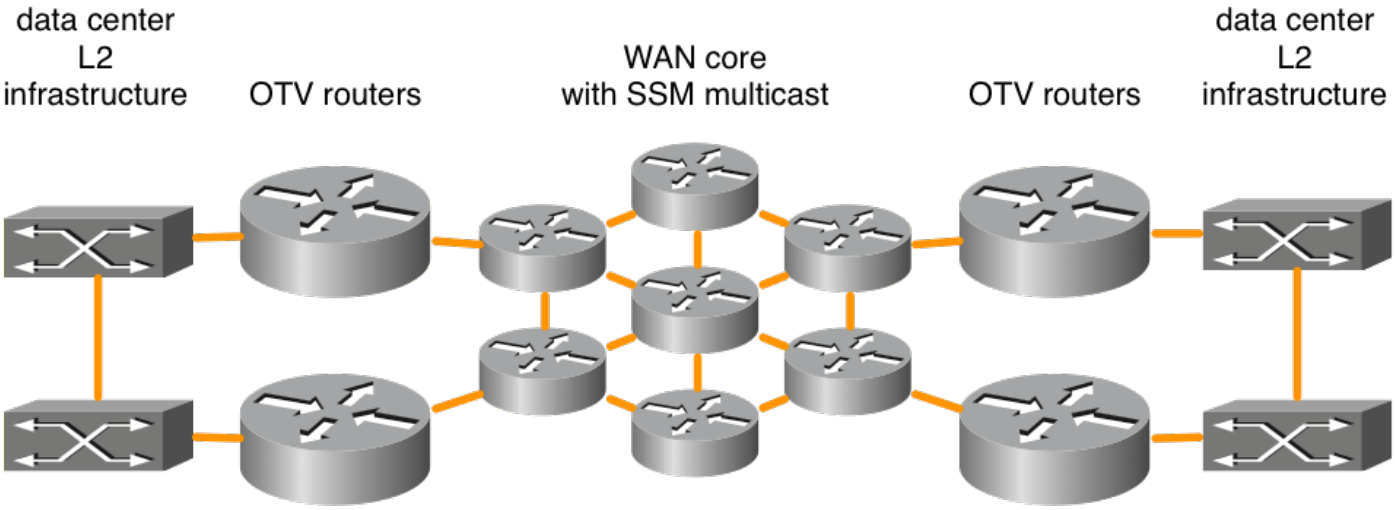
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

VLAN 또는 서비스 인스턴스 컨피그레이션별 특정 작업은 필요하지 않습니다.

멀티캐스트 코어

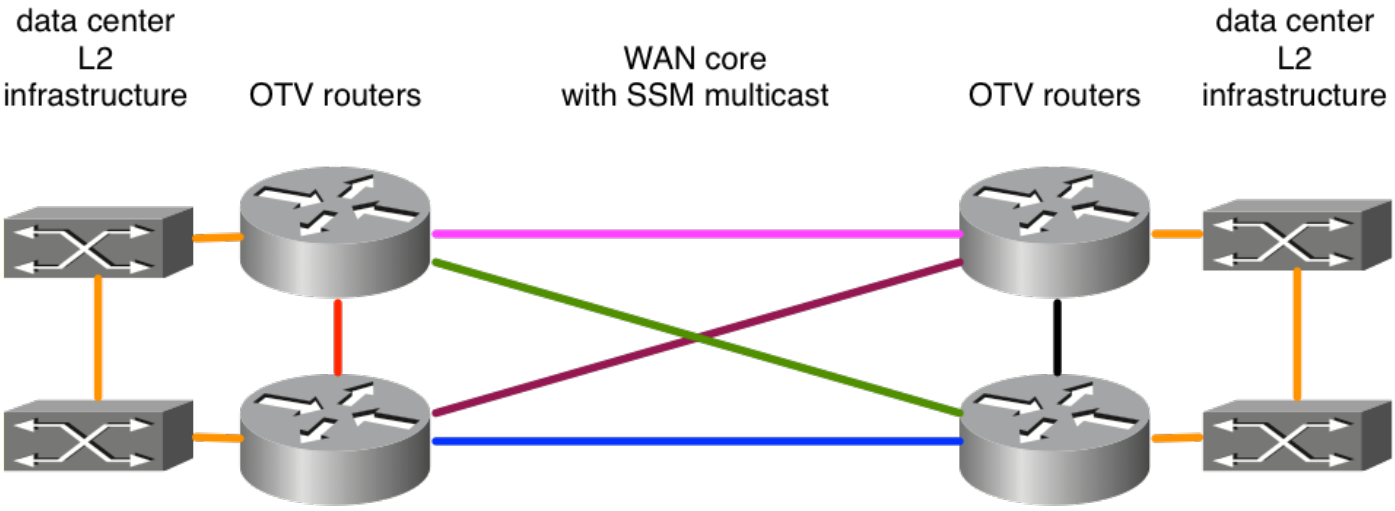
멀티캐스트 네트워크에는 WAN 전체에서 풀 메시 연결이 필요합니다. 모든 OTV 라우터는 조인 인터페이스를 통해 함께 연결해야 합니다.

그림 1. 지원되는 멀티캐스트 네트워크 토폴로지



이 그림에서는 풀 메시 형태의 코어를 통해 연결된 두 데이터 센터의 예를 보여줍니다. OTV 라우터와 WAN 코어 라우터 간에 SSM(Source Specific Multicast) PIM(Protocol Independent Multicast)이 실행됩니다. 풀 메시 연결이 가능한 경우 코어 라우터의 수에 제한이 없습니다. WAN 코어 전체에서 OTV 연결을 위해 명시적인 최대 레이턴시 요건은 없습니다.

그림 2. 지원되지 않는 멀티캐스트 네트워크 토폴로지



ASR1000/OTV는 모든 피어에서 단일 조인 인터페이스에서 멀티캐스트 메시지를 수신할 것으로 예상하므로, 예를 들어 OTV 구축이 불안정해질 수 있습니다. 분홍색과 파란색의 동-서 링크가 조인 인터페이스로 구성되었다고 가정합니다. 분홍색 링크가 실패하면 라우터는 더 이상 해당 인터페이스에서 OTV 업데이트를 수신할 수 없습니다. 조인 인터페이스가 명시적으로 구성되어 있으므로 녹색 또는 보라색 링크를 통한 대체 경로는 허용되지 않습니다. 해당 인터페이스에서 업데이트를 수

신해야 합니다. 루프백 인터페이스를 조인 인터페이스로 사용하는 것은 현재 지원되지 않습니다.

사용자가 백본을 소유하지 않은 경우 서비스 공급자가 자신의 코어에서 멀티캐스트를 지원하고 서비스 공급자가 IGMP(Internet Group Management Protocol) 쿼리 메시지에 응답할 수 있는지 확인해야 합니다. ASR1000의 OTV는 코어 WAN 멀티캐스트 토폴로지에 대한 멀티캐스트 라우터가 아니라 멀티캐스트 호스트(IGMP 조인 메시지 전달)의 역할을 합니다.

OTV 라우터 간의 전송 네트워크는 사업자 멀티캐스트 그룹에 대한 PIM 스파스 모드(ASM[Any Source Multicast])와 전달 그룹에 대한 SSM을 지원해야 합니다.

멀티캐스트 코어는 제어 그룹 및 데이터 전달에 사용되는 데이터 멀티캐스트 그룹 범위에 대한 오버레이 인터페이스의 일부 특정 컨피그레이션을 필요로 합니다.

```
ip multicast-routing distributed
ip pim ssm default
!
interface Port-channel60
 encapsulation dot1Q 30
 ip address 10.0.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
!
interface Overlay99
 no ip address
 otv control-group 239.1.1.1
 otv data-group 232.192.1.0/24
 otv join-interface Port-ch60
```

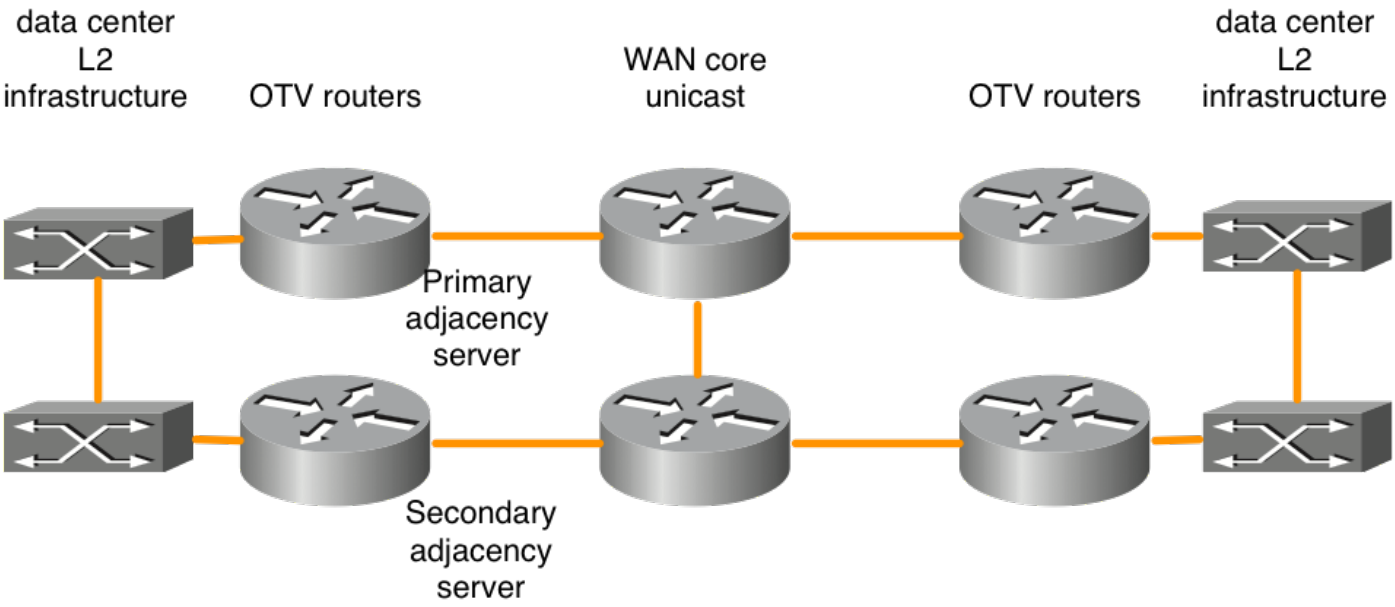
멀티캐스트 OTV 구축에서는 조인 인터페이스를 PIM 패시브 인터페이스로 구성해야 합니다. 필요에 따라 다른 버전에 대해 IGMP를 구성할 수 있습니다. 오버레이 인터페이스에는 control-group 및 data-group이 구성되어 있어야 합니다. 제어 그룹은 OTV 관리에 사용되는 단일 멀티캐스트 그룹입니다. 데이터 그룹은 데이터 센터 간에 사용자 데이터를 전송하는 데 사용되는 멀티캐스트 주소의 범위입니다. 데이터 그룹이 232.0.0.0/8 IP 공간에 없는 경우 추가 명령 "ip pim ssm range"는 OTV에 필요한 범위를 포함하도록 구성해야 합니다.

OTV 라우터 간의 전송 네트워크는 사업자 멀티캐스트 그룹에 대한 PIM 스파스 모드(ASM[Any Source Multicast])와 전달 그룹에 대한 SSM(Source Specific Multicast)을 지원해야 합니다.

인접성 서버가 있는 유니캐스트 코어

Cisco IOS® XE 3.9에는 유니캐스트 코어가 있는 OTV에 대한 지원이 추가되었습니다. OTV용 유니캐스트 및 멀티캐스트 코어 모두 모든 ASR1000 플랫폼 및 Cisco IOS® XE 3.9의 향후 릴리스에서 계속 지원됩니다.

그림 3. 유니캐스트 네트워크 토폴로지



OTV Adjacency Server 기능은 OTV 에지 간의 유니캐스트 전용 전송을 활성화합니다. 인접성 서버 역할로 구성된 OTV 라우터는 알려진 모든 OTV 라우터 목록을 유지합니다. 이 목록은 모든 등록된 OTV 라우터에 제공되므로 복제된 브로드캐스트 및 멀티캐스트 트래픽을 수신해야 하는 디바이스 목록이 있습니다.

유니캐스트 전용 전송에 대한 OTV 제어 평면은 멀티캐스트 코어를 사용하는 OTV와 정확히 같은 방식으로 작동합니다. 단, 유니캐스트 코어 네트워크에서는 각 OTV 에지 디바이스가 각 제어 평면 패킷의 여러 복사본을 생성하고 동일한 논리적 오버레이에서 각 원격 에지 디바이스에 유니캐스트 해야 합니다.

동일한 관점에서 데이터 센터의 모든 멀티캐스트 트래픽은 로컬 OTV 라우터에 복제되고 여러 복사본이 각 원격 데이터 센터로 전송됩니다. 이는 복제를 수행하기 위해 WAN 코어에 의존하는 것보다 효율적이기는 하지만 코어 멀티캐스트 네트워크의 컨피그레이션 및 관리가 필요하지 않습니다. 데이터 센터 멀티캐스트 트래픽의 양이 적거나 데이터 센터 위치가 적은 경우(4개 이하), 일반적으로 OTV 포워딩을 위한 유니캐스트 코어가 최상의 선택입니다. 전반적으로 유니캐스트 전용 모델의 운영 간소화를 통해 LAN 확장 연결이 4개 이하의 데이터 센터 사이에서만 필요한 시나리오에서 유니캐스트 코어 구축 옵션을 선호합니다. 둘 이상의 인접 서버, 즉 기본 서버와 백업 서버를 구성하는 것이 좋습니다. 액티브/액티브 인접성 서버 컨피그레이션에는 옵션이 없습니다.

OTV 라우터를 적절하게 식별하고 적절한 인접성 서버에 등록하도록 적절하게 구성해야 합니다.

	기본 인접성 서버	보조 인접성 서버	기타 OTV 라우터
OTV 조인 인터페이스 IP 주소	10.0.0.1	10.2.2.24	기타 IP 주소
설정	인터페이스 오버레이 1 otv 인접성 서버 유니캐스트 전용	인터페이스 오버레이 1 otv 인접성 서버 유니캐스트 전용 otv use-adjacency-server	인터페이스 오버레이 1 otv use-adjacency-server 10.0.0.1 10.2.2.24 유니캐스트 전용

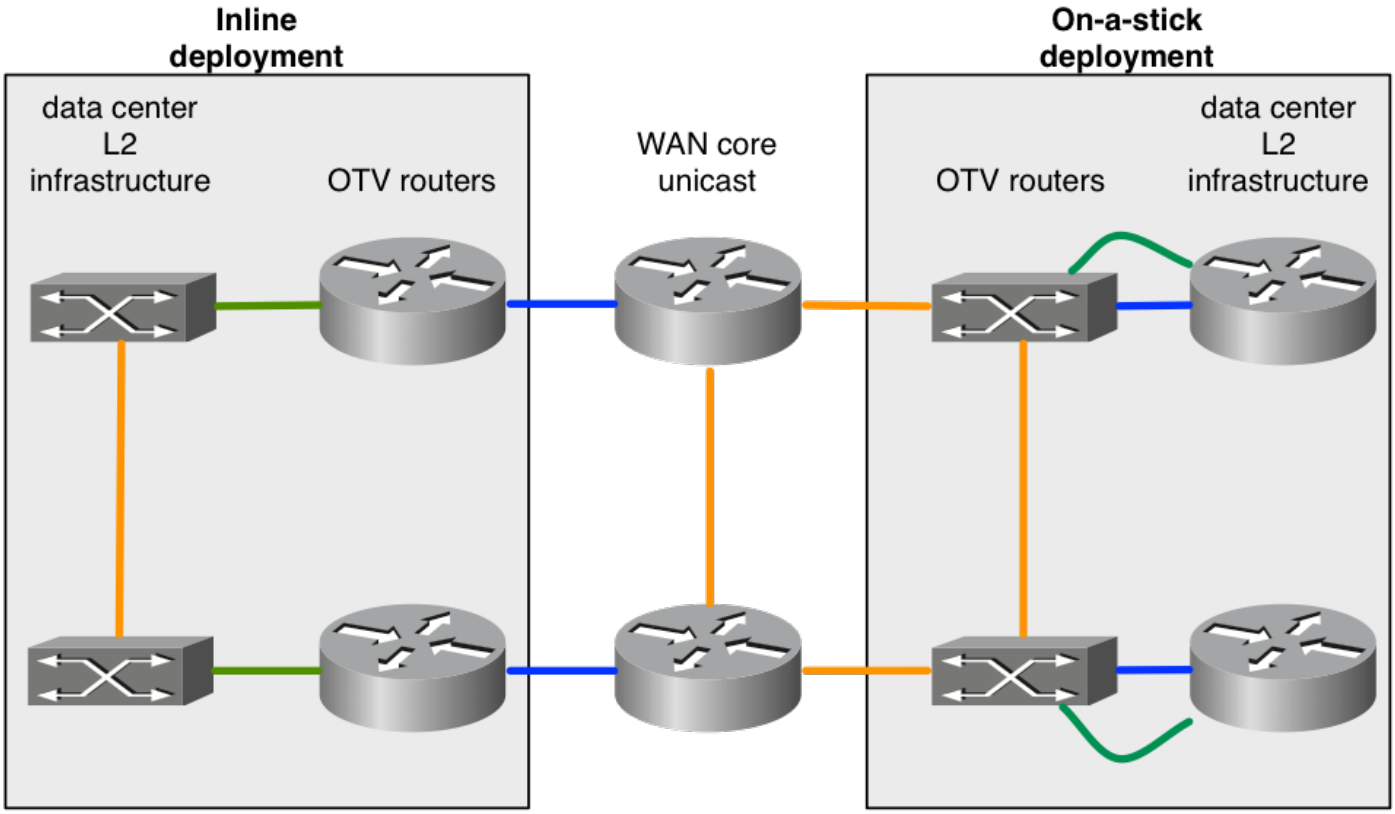
	기본 인접성 서버	보조 인접성 서버	기타 OTV 라우터
		10.0.0.1 유니캐스트 전용	

"풀 메시" 규칙을 준수하지 않는 유니캐스트 OTV 전달에서 지원되는 백투백 연결을 위한 특정 설계가 있습니다. 이러한 컨피그레이션은 지원되지만 권장되지 않습니다. 이러한 구축 유형은 데이터 센터가 다크 파이버(dark fiber)를 통해 연결된 경우 가장 일반적입니다. 이 컨피그레이션 옵션에 대한 자세한 내용은 이후 섹션 "Special case unicast topology(특수 케이스 유니캐스트 토폴로지)"에서 확인할 수 있습니다.

OTV on a Stick 대 Inline

데이터 센터에 OTV를 구축하는 모델에는 스틱과 인라인이라는 두 가지가 있습니다. 이전에 제시된 설계 시나리오에서 OTV 라우터는 데이터 센터와 통신 사업자 코어 네트워크 간에 인라인으로 연결되어 있었습니다. 그러나 모든 트래픽의 전송 경로에 없는 어플라이언스로 OTV 라우터를 추가하는 것이 더 바람직할 수 있습니다. 때로는 현재 장비를 통해 서비스 공급업체에 연결하기 위해 현재 토폴로지를 변경하지 않는 것이 요구됩니다(예: OTV를 지원하지 않는 Catalyst 6000 스위치 또는 Nexus 스위치 하드웨어가 있는 브라운필드 구축). 따라서 OTV 어플라이언스로서 스틱으로 ASR1000에 OTV를 구축하는 것이 좋습니다.

그림 4. 인라인 토폴로지 대 스틱 토폴로지



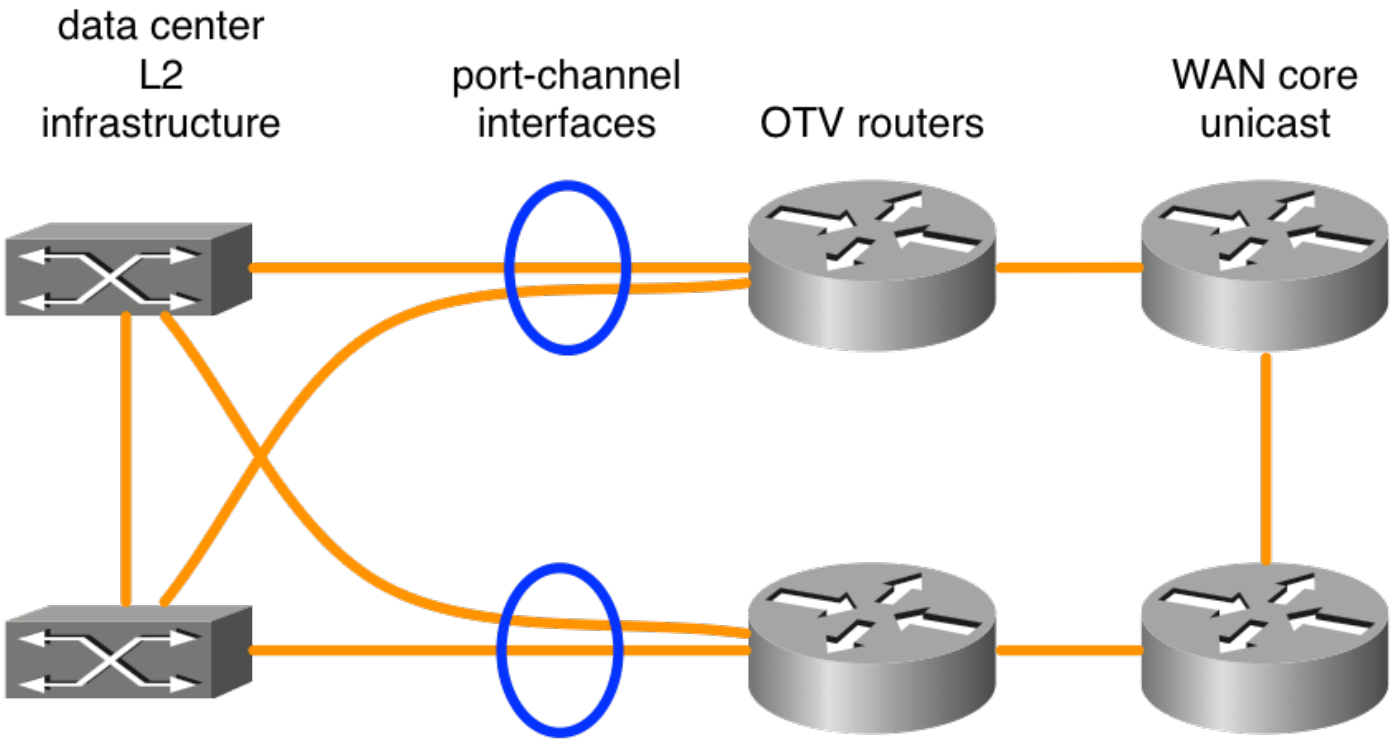
이 다이어그램에서는 동일한 오버레이에 포함될 수 있는 두 가지 구축 모델을 보여 줍니다. OTV 라우터에 연결된 녹색 링크는 L2 액세스 인터페이스로 구성되어 VLAN 트래픽을 허용합니다. OTV 라우터에 연결된 파란색 링크는 OTV 캡슐화된 VLAN 트래픽을 전달하는 조인 인터페이스입니다.

OTV에서 지원되지 않는 기능을 구성해야 할 수 있습니다. 예를 들어, OTV와 MPLS는 같은 상자에 구성할 수 없습니다. 따라서 스틱에 ASR1000/OTV를 사용하고 OTV 라우터 앞에 있는 라우터에 MPLS를 구성하는 것이 좋습니다.

레이어 2 및 레이어 3의 포트 채널

ASR1000용 Cisco IOS® XE 3.10 코드에는 OTV를 통한 레이어 2 및 레이어 3 포트 채널 구성이 추가되었습니다. 레이어 2 포트 채널을 내부 인터페이스로 사용할 수 있습니다. 포트 채널은 최대 4개의 물리적 인터페이스로 구성되어야 합니다. 레이어 3 포트 채널을 조인 인터페이스로 사용할 수 있습니다.

그림 5. L2 연결에 사용되는 포트 채널



이 다이어그램은 VSS(Catalyst 6000 Series) 또는 VPC(Nexus 7000 Series)에서 2개의 스위치를 사용하는 일반적인 포트 채널 시나리오를 보여줍니다. 이러한 유형의 설계는 듀얼 OTV 라우터와 데이터 센터 인프라에 대한 듀얼 연결을 통해 이중화를 제공합니다. OTV 라우터 옆의 L2 스위칭 장비에서 VSS 또는 VPC를 사용하는 경우 기본 포트 채널 컨피그레이션 외에 OTV에 대한 특별한 컨피그레이션이 필요하지 않습니다.

기본 게이트웨이

정의상 OTV는 여러 위치에 동일한 L3 서브넷을 생성합니다. 이를 위해서는 확장 VLAN으로 L3 트래픽을 라우팅할 때 몇 가지 특별한 고려가 필요합니다. L3 라우팅은 OTV 라우터 자체에서 구성할 수도 있고, 확장 VLAN에 연결된 다른 디바이스에서 구성할 수도 있습니다. 또한 각 시나리오에서 이중화를 위해 HSRP(Hot Standby Redundancy Protocol) 또는 VRRP(Virtual Router Redundancy Protocol)와 같은 FHRP(First Hop Redundancy Protocol)를 구축할 수 있습니다. HSRP는 지정된 데이터 센터에서 로컬로 실행하거나 데이터 센터 간에 확장할 수 있습니다(일반적이지 않음).

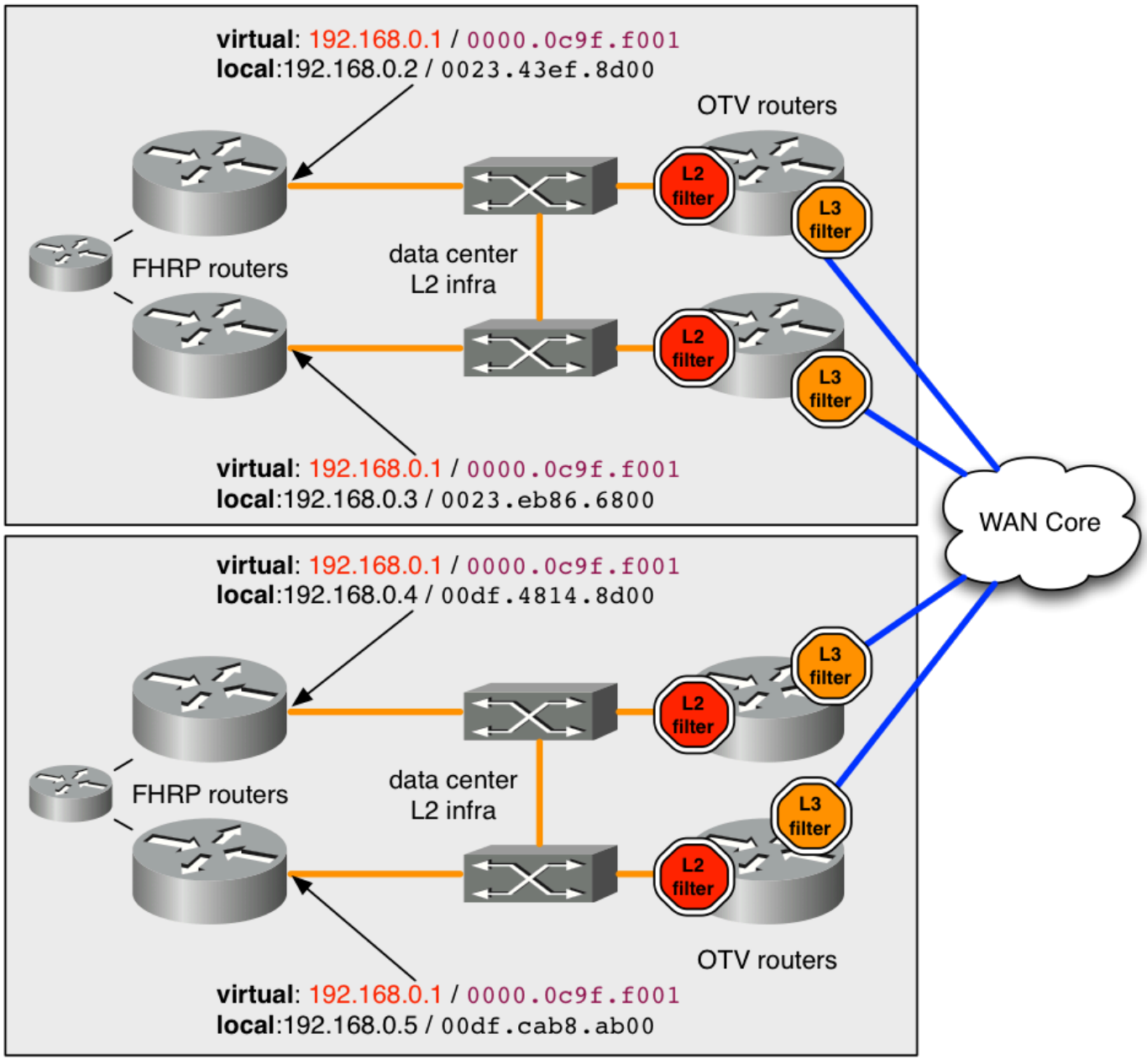
FHRP를 활용하는 OTV 구축의 모범 사례는 각 데이터 센터에서 FHRP의 로컬 인스턴스를 실행하

는 것입니다. 이러한 FHRP 인스턴스는 동일한 가상 MAC 주소와 IP 주소를 사용하므로 VM(가상 머신)이 데이터 센터 간에 이동할 때 중단 없는 연결을 갖게 됩니다. 기본 라우터의 MAC 주소가 데이터 센터 간에 변경되는 경우 VM의 기본 게이트웨이 ARP 항목 시간이 초과될 때까지 VM이 서브넷에서 통신할 수 없습니다.

OTV를 사용하여 FHRP를 제대로 구축하려면 OTV에서 필터링 및 격리해야 하는 L2 및 L3 트래픽을 고려해야 합니다. L2 수준에서 OTV가 여러 위치에서 FHRP에서 사용하는 동일한 L2 가상 MAC을 놓치지 않도록 해야 합니다. 활성/수신/대기 선택이 각 데이터 센터로 현지화되도록 HSRP 및 VRRP 광고를 각 데이터 센터로 격리하려면 L3 레벨에서 필터가 필요합니다.

OTV가 활성화된 경우 기본적으로 FHRP 필터가 활성화됩니다. 설계상 데이터 센터 간에 FHRP를 확장해야 하는 경우 비활성화할 수 있습니다. 가상 MAC 주소의 L2 필터링은 기본적으로 활성화되지 않으며 수동으로 구성해야 합니다.

그림 6. FHRP에 권장되는 구축의 예



이 예에서 가상 MAC 주소 0000.0c9f.f001은 서브넷의 연결을 위해 확장 VLAN에 호스팅하는 IP 주

소 192.168.0.1에 사용됩니다. 두 데이터 센터에서 동일한 가상 MAC 및 IP를 사용하면 호스트가 데이터 센터 간에 전송할 때 서브넷에서 원활하게 연결됩니다.

OTV에서 MAC 주소 0000.0c9f.f001을 여러 위치에서 숨기려면 VLAN을 서비스하는 각 OTV 라우터의 VLAN에 대해 인그레스 L2 필터(다이어그램의 빨간색 중지)를 배포해야 합니다. ACL 필터에서 인그레스 L2 서비스 인스턴스에 구성된 필터 ACL을 사용하면 ASR1000의 OTV 프로세스에서 해당 MAC에서 제공된 모든 패킷이 해당 패킷을 볼 수 있기 전에 삭제됩니다. 따라서 OTV는 MAC에 대해 전혀 알지 못하며 이를 원격 데이터 센터에 알리지 않습니다.

모든 잘 알려진/기본 FHRP 가상 MAC 트래픽을 잡기 위한 권장 컨피그레이션이 여기에 제공됩니다.

```
mac access-list extended otv_filter_fhrp
 deny 0000.0c07.ac00 0000.0000.00ff any
 deny 0000.0c9f.f000 0000.0000.0fff any
 deny 0007.b400.0000 0000.0000.00ff any
 deny 0000.5e00.0100 0000.0000.00ff any
 permit any any
```

이 ACL은 HSRP 버전 1 및 2, GLBP(Gateway Load Balancing Protocol) 및 VRRP(순서대로)와 연결된 잘 알려진 MAC 주소 공간과 일치합니다. 가상 MAC이 FHRP 그룹 번호를 기반으로 하지 않는 비표준 값을 사용하도록 구성된 경우 ACL 예에 명시적으로 추가해야 합니다. ACL은 L2 서비스 인스턴스(여기에 표시됨)에 추가해야 합니다.

```
interface Port-channel10
  description *** OTV internal interface ***
  no ip address
  no negotiation auto
!
  service instance 800 ethernet
    encapsulation dot1q 800
    mac access-group otv_filter_fhrp in
    bridge-domain 800
```

또한 L3 레벨에서 FHRP 호스트 간의 통신을 관리할 필요가 있습니다. 다이어그램에는 단일 확장 서브넷에 구성된 4개의 FHRP 라우터가 있습니다. 어느 정도의 L3 필터가 없으면 4개의 모든 라우터가 서로를 확인하고 단일 활성 디바이스를 선택하며 다양한 대기 상태에서 3을 갖습니다. 따라서 한 데이터 센터에는 두 개의 로컬 대기 FHRP 라우터가 있지만 이전에 설명한 L2 필터로 인해 원격 활성 라우터에 대한 L2 연결이 없을 수 있습니다.

원하는 결과는 각 데이터 센터에 활성 FHRP 라우터와 대기 FHRP 라우터가 하나씩 있는 것입니다. 선택 프로세스에서 라우터의 실제 IP 및 MAC 주소를 사용하므로 앞에서 설명한 인그레스 L2 필터에서는 이 선택 트래픽을 catch하지 않습니다. 기본적으로 후속 ACL은 오버레이 인터페이스에서 이그레스(egress)로 적용됩니다. 오버레이 인터페이스의 이그레스(egress)는 WAN 코어를 향하는 트래픽일 수 있습니다. 실행 중인 컨피그레이션에서는 ACL이 표시되지 않지만 "show ip

access-list"에서는 관찰할 수 있습니다. UDP 포트 번호를 기반으로 FHRP 선택 트래픽을 필터링합니다.

```
Extended IP access list otv_fhrp_filter_acl
    10 deny udp any any eq 1985 3222
    20 deny 112 any any
    30 permit ip any
```

이 필터를 비활성화하는 유일한 이유는 VLAN의 모든 FHRP 라우터가 활성 상태의 동일한 선택에 참여하게 하려는 경우입니다. 이 필터를 비활성화하려면 오버레이 인터페이스에서 "no otv filter-fhrp"를 구성합니다.

알 수 없는 유니캐스트 트래픽

기본적으로 원격 OTV 위치에 존재하는 것으로 알려지지 않은 MAC 주소로 향하는 OTV 라우터가 LAN에서 수신한 유니캐스트 트래픽은 삭제됩니다. 이 트래픽은 알 수 없는 유니캐스트라고 합니다. 이 삭제 작업은 WAN에서 사용되는 대역폭의 양을 브로드캐스트 트래픽으로 제한하는 WAN 코어로 이동합니다. 일반적으로 LAN의 모든 호스트는 OTV 라우터가 항상 확인하고 광고하며 "알려진" 브로드캐스트 트래픽(ARP, 프로토콜 브로드캐스트 등)을 충분히 발생시킵니다.

일부 애플리케이션은 무음 호스트를 활용합니다. 일반적인 스위칭 인프라에서는 LAN에서 알 수 없는 유니캐스트 MAC 주소를 L2 브로드캐스트하면 무음 호스트가 트래픽을 볼 수 있으므로 이 문제는 발생하지 않습니다. 그러나 OTV 환경에서는 OTV 라우터가 데이터 센터 간의 트래픽을 차단합니다.

이를 보완하기 위해 Selective Unicast Forwarding이라고 하는 기능이 Cisco IOS® XE 3.10.6, XE3.13.3, XE 3.14.1, XE3.15에 통합되었으며 이후 모든 릴리스에서 선택적 유니캐스트 포워딩을 지원합니다.

오버레이 인터페이스의 MAC 주소당 단일 명령을 추가하여 구성합니다. 예를 들면 다음과 같습니다.

```
interface Overlay1
  service instance 100 ethernet
    encapsulation dot1q 100
    otv mac flood 0000.0000.0001
    bridge-domain 100
```

0000.0001.0001로 향하는 모든 트래픽은 이 예에서 VLAN 100이 있는 모든 원격 OTV 라우터에 플러딩되어야 합니다. 이는 후속 명령에서 확인할 수 있습니다.

<#root>

```
OTV_router_1#
```

```
show otv route


Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood
```

해당 MAC 주소가 원격 사이트에서 학습된 경우 플러드 항목보다 우선하는 항목을 전달 테이블에 추가해야 합니다.

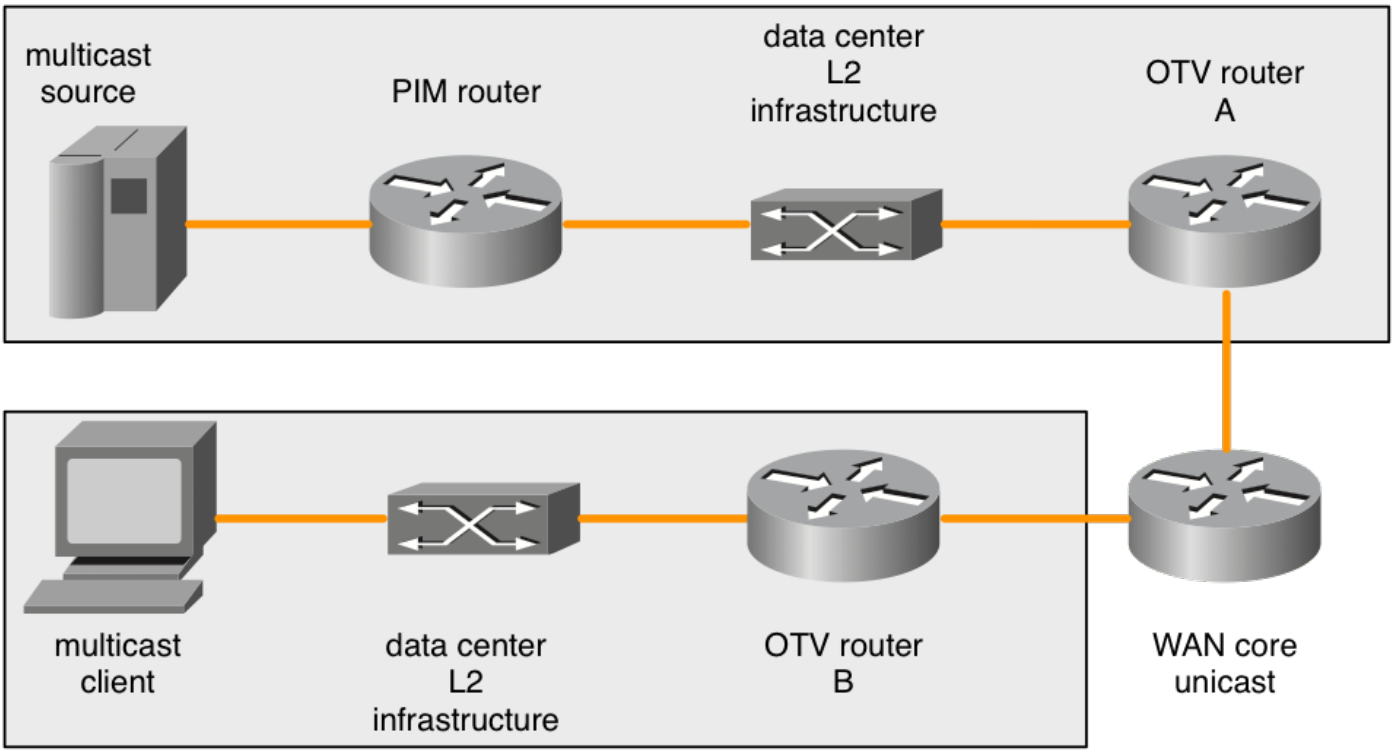
```
<#root>

OTV_router_1#

show otv route


Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood
 0    100  100    0000.0000.0001 50    ISIS   OTV_router_3
```

일반적으로 특정 MAC 주소에 대한 플러딩 항목은 해당 VLAN이 있는 모든 OTV 라우터에서 구성해야 합니다.

원격 멀티캐스트 소스

OTV 라우터가 LAN에서 수신한 멀티캐스트 IGMP 가입 요청을 전달하지 않는 ASR1000입니다. 후속 다이어그램에서는 문제가 될 수 있는 토폴로지를 자세히 설명합니다.

그림 7. 원격 멀티캐스트 소스



멀티캐스트 클라이언트가 멀티캐스트 IGMP 참가를 전송하면 ASR1000(OTV 라우터 B)이 이를 관찰하고 멀티캐스트 그룹에 대한 관심을 알립니다. 원격 OTV 라우터(OTV 라우터 A)는 모든 트래픽을 로컬 L2 브로드캐스트 도메인에 있는 해당 멀티캐스트 그룹으로 전달해야 합니다. 그러나 원격 ASR1000(OTV 라우터 A)은 클라이언트의 OTV 라우터(OTV 라우터 B)에서 멀티캐스트 그룹에 대한 관심을 알릴 때 멀티캐스트 IGMP 조인 요청을 다시 생성하지 않습니다.

멀티캐스트 소스가 OTV 라우터와 동일한 L2 브로드캐스트 도메인에 있는 경우 이 문제는 발생하지 않습니다. OTV 라우터는 IGMP 쿼리 발송자로 구성해야 합니다. 이는 L2 브로드캐스트 도메인에 있는 모든 멀티캐스트 트래픽에서 표시됩니다. 그러나 PIM 가입 요청만 있으면 PIM 라우터가 멀티캐스트 소스를 다른 L2 브로드캐스트 도메인에서 OTV 라우터가 있는 L2 브로드캐스트 도메인으로 전달합니다.

원격 IGMP 가입 요청이 전달되거나 다시 생성되지 않습니다. OTV 라우터도 PIM 라우터가 아닙니다. 따라서 OTV 라우터가 있는 L2 브로드캐스트 도메인에 직접 있지 않은 멀티캐스트 소스의 토폴로지에서는 원격 클라이언트가 관심을 가질 때 소스 트래픽을 전달하기 위해 PIM 라우터를 수신할 방법이 없습니다.

이 문제는 두 가지 해결 방법이 있습니다.

먼저 로컬 IGMP 클라이언트를 OTV 라우터(OTV 라우터 A)에 연결된 L2 브로드캐스트 도메인에 배포할 수 있습니다. 이 IGMP 클라이언트는 원격 클라이언트가 가입할 수 있는 멀티캐스트 그룹에 가입해야 합니다. 그러면 PIM 라우터가 멀티캐스트 트래픽을 OTV 라우터 A에 인접한 브로드캐스트 도메인으로 전달합니다. 그런 다음 IGMP 쿼리는 모든 멀티캐스트 트래픽을 가져오고 오버레이를 통해 전송됩니다.

다른 해결 방법은 원격 클라이언트가 구독할 수 있는 모든 그룹에 대해 "ip igmp static-join"을 구성하는 것입니다. 그러면 PIM 라우터가 멀티캐스트 트래픽을 OTV 라우터 A에 인접한 브로드캐스트 도메인으로 전달합니다.

이 제한은 알려진 것이며 설계 사양의 일부입니다. 현재 지원되는 토폴로지에서는 버그로 간주되지 않지만 제한됩니다.

QoS 고려 사항

기본적으로 ASR1000에서는 추가된 OTV 헤더의 TOS 값이 L2 패킷의 802.1p 비트에서 복사됩니다. L2 패킷에 태그가 지정되지 않은 경우 0 값이 사용됩니다.

Nexus 7000은 5.2.1 소프트웨어 이상에서 다른 기본 동작을 수행합니다. 원하는 동작이 내부 패킷 TOS 값을 외부로 복사하는 것이라면 추가 QoS 컨피그레이션을 통해 이를 달성할 수 있습니다. 이는 최신 Nexus 7000 소프트웨어와 동일한 동작을 제공합니다.

L2 패킷 L3 TOS 값을 OTV 패킷의 가장 바깥쪽 헤더에 복사하는 컨피그레이션은 다음과 같습니다.

```
class-map dscp-af11
 match dscp af11
!
class-map dscp-af21
 match dscp af21
!
class-map qos11
 match qos-group 11
!
class-map qos21
 match qos-group 21
!
policy-map in-mark
 class dscp-af11
  set qos-group 11
 class dscp-af21
  set qos-group 21
!
policy-map out-mark
 class qos11
  set dscp af11
 class qos21
  set dscp af21
!
interface Gig0/0/0
 ! L2 interface
 service instance 100 ethernet
  encapsulation dot1q 100
  service-policy in-mark
  bridge-domain 100
!
interface Gig0/0/1
 ! OTV join interface
 service-policy out-mark
```

제공된 컨피그레이션은 인그레스의 다양한 DSCP 값에 대한 트래픽과 일치해야 합니다. 로컬에서 중요한 qos-group 태그는 라우터를 통과하는 동안 트래픽을 내부적으로 표시하는 데 사용됩니다. 이그레스 인터페이스에서 qos-group을 확인한 다음 가장 바깥쪽 TOS 바이트가 그에 따라 업데이

트됩니다.

WAN MTU 고려 사항/단편화

OTV는 기본적으로 GRE 헤더를 사용하여 WAN을 통해 L2 트래픽을 전송합니다. 이 GRE 헤더의 크기는 42바이트입니다. 이상적인 네트워크 구축에서 WAN 링크는 OTV가 처리할 것으로 예상되는 최대 패킷보다 최소 42바이트 큰 MTU(최대 전송 단위)를 가져야 합니다.

L2 인터페이스의 MTU가 1500바이트이면 조인 인터페이스의 MTU는 1542바이트 이상이어야 합니다. L2 인터페이스의 MTU가 2000바이트이지만 패킷이 1500바이트까지만 처리되어야 하는 경우에는 1542바이트의 WAN MTU로도 충분하지만 2000에 42를 기본적으로 추가하는 것이 좋습니다.

```
interface GigabitEthernet0/0/0
  mtu 1600
!
interface Overlay 1
  otv join-interface GigabitEthernet0/0/0
!
interface GigabitEthernet0/0/1
  mtu 1500
  service instance 100 ethernet
    encapsulation dot1q 100
    bridge-domain 100
  service instance 101 ethernet
    encapsulation dot1q 101
    bridge-domain 101
```

일부 통신 사업자는 WAN 회로에 더 큰 MTU 값을 제공할 수 없습니다. 이 경우 ASR1000은 OTV 전송 데이터의 단편화를 수행할 수 있습니다. Nexus 7000에는 이 기능이 없습니다. ASR1000에서 단편화가 활성화된 혼합 ASR1000 및 Nexus 7000 OTV 네트워크는 지원되지 않습니다.

OTV 프래그먼트화를 위한 컨피그레이션은 다음과 같습니다.

```
otv fragmentation join-interface GigabitEthernet0/0/0
!
interface Overlay 1
  otv join-interface GigabitEthernet0/0/0
```

global level 명령은 Overlay interface join-interface 명령보다 먼저 구성해야 합니다. Overlay 인터페이스의 otv join-interface 명령이 먼저 구성된 경우 Overlay 인터페이스에서 otv join-interface 명령을 제거하고 otv fragmentation join-interface 명령을 구성한 다음 Overlay 인터페이스의 otv join-interface 명령을 다시 구성합니다.

OTV 프래그먼트화가 활성화되지 않은 경우, 캡슐화된 L2 데이터를 전달하는 모든 OTV 패킷이 전송 중에 프래그먼트화되지 않도록 DF 비트 세트와 함께 전송됩니다. fragmentation 명령이 추가되면 DF 비트가 0으로 설정됩니다. OTV 라우터 자체는 패킷을 프래그먼트화할 수 있으며, 다른 라우

터가 전송 중에 프래그먼트화할 수 있습니다.

ASR1000 플랫폼에서는 패킷 리어셈블리 버퍼의 양이 제한적이므로 전송을 위해 패킷을 잘게 썰어야 하는 프래그먼트의 수가 적습니다. 따라서 효율성이 높아지고 문제가 있는 경우 WAN에서 전반적인 대역폭 소모가 줄어듭니다. OTV 프래그먼트화를 활성화하는 성능 관련 사항이 있습니다. 프래그먼트화가 있고 1Gb/sec 이상의 OTV 트래픽을 처리할 것으로 예상되는 경우, OTV 성능을 추가로 조사해야 합니다.

특수 케이스 유니캐스트 토폴로지

OTV를 위한 현장 구축은 종종 두 데이터 센터의 OTV 라우터 간에 직접 백투백 파이버 연결을 제공합니다.

단일 홈 토폴로지의 경우 OTV 및 비 OTV 트래픽이 조인 인터페이스를 공유하는 표준 구축에 사용됩니다. 이 설정이 적용되지 않도록 특별히 고려할 필요가 없습니다.

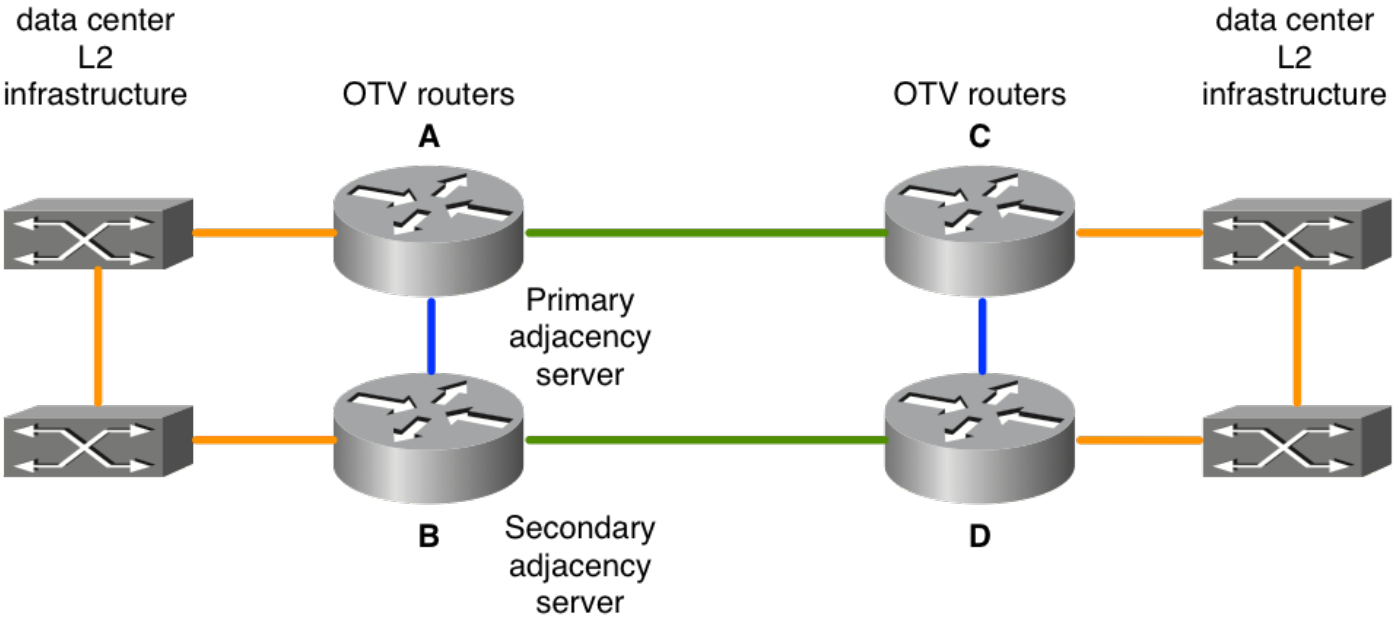
그러나 구축에 두 데이터 센터에 멀티홈 OTV 라우터가 있는 경우 몇 가지 특별한 고려 사항이 있습니다. 추가 컨피그레이션이 필요합니다.

두 개 이상의 데이터 센터가 관련된 경우 이 특수 컨피그레이션은 적용되지 않습니다.

단일 또는 멀티홈 OTV 라우터가 있는 데이터 센터가 두 개 이상인 시나리오에서는 표준 유니캐스트 또는 멀티캐스트 OTV 구축을 사용해야 합니다.

지원되는 다른 대안은 없습니다.

그림 8. 특수 케이스 유니캐스트



제시된 토폴로지에서 녹색 링크는 두 데이터 센터 간의 다크 파이버 링크입니다. 이러한 다크 파이버(dark fiber)는 OTV 라우터에 직접 연결됩니다. OTV 라우터 간의 파란색 링크는 녹색 링크에 장애가 발생할 경우 비 OTV 트래픽을 재라우팅하는 데 사용됩니다. 맨 위 녹색 링크가 실패하면 (A~C) 맨 위 OTV 라우터를 기본 경로로 사용하는 비 OTV 트래픽은 north-south 파란색 링크(A~B,

C~D)를 통해 맨 아래 OTV 라우터 쌍(B~D) 사이의 작동 중인 녹색 링크로 라우팅됩니다.

OTV 컨피그레이션은 물리적 인터페이스를 조인 인터페이스로 지정하므로 이러한 기본 트래픽 리라우팅은 OTV 트래픽에서 작동하지 않습니다. OTV 라우터 A의 "녹색 인터페이스"가 다운되면 대체 인터페이스 OTV 라우터 B에서 OTV 트래픽을 소싱할 수 없습니다. 또한 WAN 코어를 통한 전체 연결이 없기 때문에 장애가 발생한 경우 모든 OTV 라우터에 알림을 보낼 수 없습니다. 이 문제를 해결하기 위해 EEM(Embedded Event Manager) 스크립팅과 함께 BFD(Bidirectional Forwarding Detection)가 사용됩니다.

BFD는 동-서 OTV 라우터 쌍(A/C 및 B/D) 간의 WAN 링크를 모니터링해야 합니다. 원격 라우터에 대한 연결이 끊기면 OTV 오버레이 인터페이스가 동-서 OTV 라우터 쌍의 EEM 스크립트를 통해 종료됩니다. 그러면 페어링된 멀티홈 라우터가 모든 VLAN에 대한 포워딩을 가정합니다. BFD에서 링크가 복구되었음을 탐지하면 EEM 스크립트가 트리거되어 오버레이 인터페이스가 다시 활성화됩니다.

BFD를 사용하여 링크 장애를 탐지하는 것은 매우 중요합니다. 이는 오버레이 인터페이스가 동-서 쌍은 물론 "장애가 발생한" 측 모두에서 종료되어야 하기 때문입니다. 통신 사업자가 제공하는 연결 유형에 따라 하나의 물리적 링크가 중단되고(OTV 라우터 A의 녹색 인터페이스) 해당 east-west 쌍 라우터의 인터페이스가 가동 상태를 유지할 수 있습니다(OTV 라우터 C의 녹색 인터페이스). BFD는 인터페이스 중 하나에서 장애가 발생하거나 전송 중인 다른 문제를 감지하여 두 쌍에 동시에 즉시 알립니다. 라우터에 복구 링크에 대한 알림을 보내야 하는 경우에도 마찬가지입니다.

이 구축에 대한 컨피그레이션은 후속 항목을 추가하여 다른 구축과 동일합니다.

- WAN 인터페이스의 BFD 컨피그레이션
- 후속 EEM 스크립트
- 짝수/홀수 VLAN 배포와 일치하는 OTV ISIS ID

OTV 조인 인터페이스의 BFD 컨피그레이션은 이 문서의 범위를 벗어납니다. ASR1000에서 BFD를 구성하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-3s/irb-xe-3s-book.html

BFD 장애 탐지가 조인 인터페이스 쌍(다이어그램의 녹색 링크) 간에 올바르게 작동하면 EEM 스크립트를 구축해야 합니다. EEM 스크립트는 특정 라우터에 맞게 조정되어야 올바른 오버레이 인터페이스를 수정할 수 있으며, BFD 오류 및 복구에 대한 로그에서 더 정확한 문자열을 모니터링할 수 있습니다.

```
event manager environment _OverlayInt Overlay1
!
event manager applet WatchBFDdown
description "Monitors BFD status, if it goes down, bring OVERLAY int down"
event syslog pattern "BFD peer down notified" period 1
action 1.0 cli command "enable"
action 2.0 cli command "config t"
action 2.1 syslog msg "EEM: WatchBFDdown will shut int $_OverlayInt"
action 3.0 cli command "interface $_OverlayInt"
action 4.0 cli command "shutdown"
action 5.0 syslog msg "EEM WatchBFDdown COMPLETE ..."
```

```
!
event manager applet WatchBFDup
description "Monitors BFD status, if it goes up, bring OVERLAY int up"
event syslog pattern "new adjacency" period 1
action 1.0 cli command "enable"
action 2.0 cli command "config t"
action 2.1 syslog msg "EEM: WatchBFDup bringing up int $_OverlayInt"
action 3.0 cli command "interface $_OverlayInt"
action 4.0 cli command "no shutdown"
action 5.0 syslog msg "EEM WatchBFDup COMPLETE ..."
!
```

이러한 구축 유형에서는 odd 및 even vlan을 전달할 때 east-west 라우터 쌍(A/C 및 B/D)이 일치해야 합니다.

예를 들어 A와 C는 짝수 VLAN을 포워딩하고 B와 D는 홀수 VLAN을 정상 상태 공칭 연산으로 포워딩해야 합니다.

홀수/짝수 분포는 "show otv site" 명령으로 관찰할 수 있는 OTV 서수에 따라 결정됩니다.

두 사이트 라우터 간의 서수는 OTV ISIS net ID를 기반으로 결정됩니다.

```
OTV_router_A#show otv site
Site Adjacency Information (Site Bridge-Domain: 99)
Overlay99 Site-Local Adjacencies (Count: 2)
  Hostname       System ID      Last Change Ordinal    AED Enabled Status
* OTV_router_A   0021.D8D4.F200 19:32:02    0          site       overlay
  OTV_router_B   0026.CB0C.E200 19:32:46    1          site       overlay
```

OTV ISIS net 식별자는 모든 OTV 라우터에서 구성해야 합니다. 모든 OTV 라우터가 서로를 인식할 수 있도록 식별자를 구성할 때는 주의해야 합니다.

<#root>

```
OTV router A:
otv isis Site
 net
```

49

.

0001

.

0001

.

0001

.

000a

.

00

OTV router B:
otv isis Site
 net

49

.

0001

.

0001

.

0001

.

000b

.

00

OTV router C:
otv isis Site
 net

49

.

0001

.

0001

.

0001

.

000c

.

00

OTV router

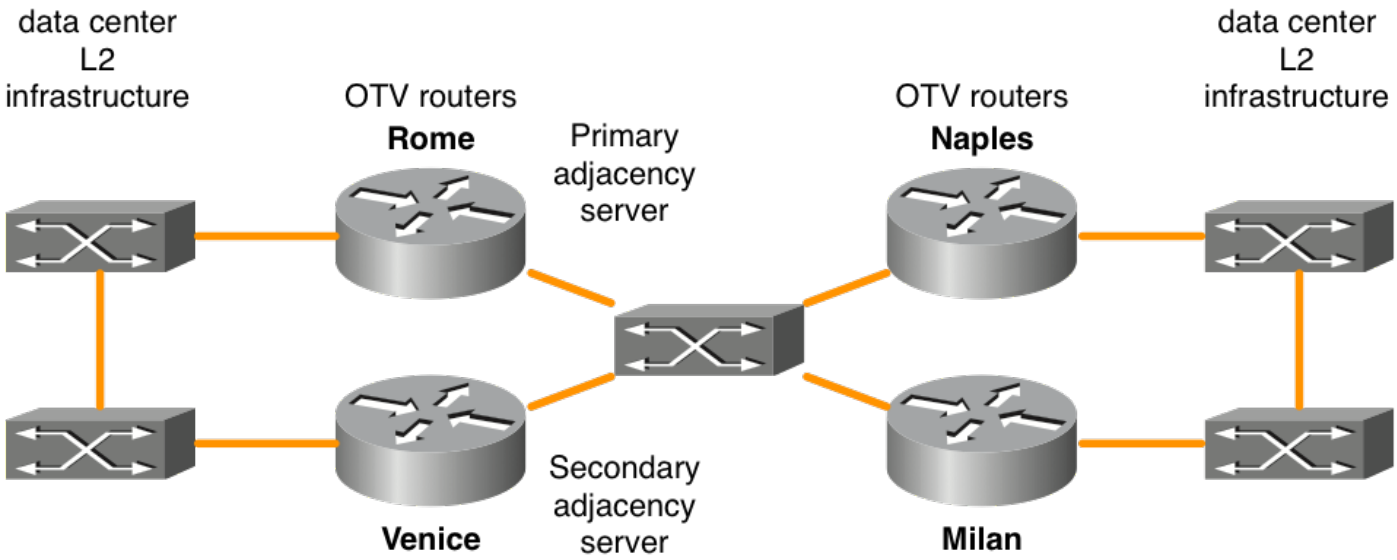
```
      D:
otv isis Site
 net

49

.

0001

.

0001

.

0001

.

000d

.

00
```

검은색 식별자 부분은 오버레이에 참여하는 모든 OTV 라우터에서 일치해야 합니다. 빨간색 식별자 부분은 수정할 수 있습니다. 사이트에서 가장 낮은 네트워크 식별자는 서수 0을 얻고 짝수 번호의 VLAN을 전달합니다. 사이트의 가장 높은 네트워크 식별자는 서수 1을 얻고 홀수 VLAN을 전달합니다.

컨피그레이션 예

유니캐스트

그림 9. 유니캐스트 컨피그레이션 예



Rome 구성:

```
!
hostname Rome
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet1/0/0
 otv adjacency-server unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
interface GigabitEthernet1/0/0
 ip address 172.16.0.1 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet1/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Venice 구성:

```
!
hostname Venice
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
```

```
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv adjacency-server unicast-only
 otv use-adjacency-server 172.16.0.1 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.2 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Naples 구성:

```
!
hostname Naples
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv use-adjacency-server 172.16.0.1 172.16.0.2 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
```

```
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.3 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

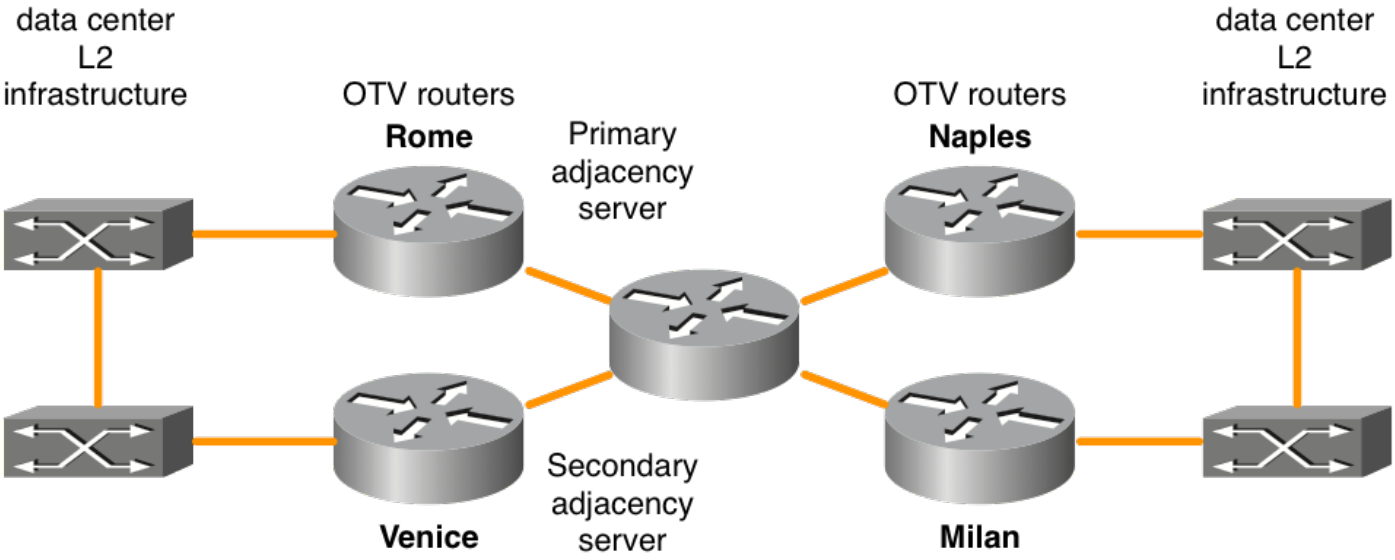
Milan 구성:

```
!
hostname Milan
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv use-adjacency-server 172.16.0.1 172.16.0.2 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
```

```
 ip address 172.16.0.4 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

멀티캐스트

그림 10. 멀티캐스트 컨피그레이션 예



Rome 구성:

```
!
hostname Rome
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
```

```
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet1/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet1/0/0
 ip address 192.168.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet1/0/1
 no ip address
 negotiation auto
 cdp enable
!
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Venice 구성:

```
!
hostname Venice
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
```

```
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.17.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
!
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Naples 구성:

```
!
hostname Naples
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
```

```
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.18.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Milan 구성:

```
!
hostname Milan
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
```

```
 otv join-interface GigabitEthernet0/0/0
otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
  service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.19.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

자주 묻는 질문(FAQ)

Q) 프라이빗 VLAN은 OTV와 함께 지원됩니까?

A) 예, OTV에 특수 구성이 필요하지 않습니다. 프라이빗 VLAN 구성에서 OTV L2 인터페이스에 연결된 스위치 포트가 프로미스큐어스 모드로 구성되었는지 확인하십시오.

Q) OTV는 IPSEC 암호화에서 지원됩니까?

A) 예. join-interface의 암호화 맵 컨피그레이션이 지원됩니다. OTV가 암호화를 지원하기 위해 특별한 컨피그레이션이 필요하지 않습니다. 그러나 암호화 컨피그레이션은 추가 오버헤드를 추가하므로 WAN MTU가 LAN MTU에 비해 증가함에 따라 이를 보완해야 합니다. 이것이 불가능한 경우 OTV 단편화가 필요합니다. OTV 성능은 IPSEC 하드웨어의 성능으로 제한됩니다.

Q) MACSEC에서 OTV를 지원합니까?

A) 예. ASR1001-X에는 내장 인터페이스에 대한 MACSEC 지원이 포함됩니다. OTV는 LAN 및/또

는 WAN 인터페이스에 구성된 MACSEC과 함께 작동합니다. OTV 성능은 MACSEC 하드웨어의 성능으로 제한됩니다.

Q) 루프백 인터페이스를 조인 인터페이스로 사용할 수 있습니까?

A) 아니요, 이더넷, Portchannel 또는 POS 인터페이스만 OTV 조인 인터페이스로 사용할 수 있습니다. OTV 루프백 가입 인터페이스가 로드맵에 있지만 현재 릴리스에 예약되어 있지 않습니다.

Q) 터널 인터페이스를 조인 인터페이스로 사용할 수 있습니까?

A) 아니요, GRE 터널, DMVPN 터널 또는 기타 터널 유형은 조인 인터페이스로 지원되지 않습니다. 이더넷, Portchannel 또는 POS 인터페이스만 OTV 조인 인터페이스로 사용할 수 있습니다.

Q) 서로 다른 오버레이 인터페이스에서 서로 다른 L2 및/또는 조인 인터페이스를 사용할 수 있습니까?

A) 모든 오버레이 인터페이스는 동일한 조인 인터페이스를 가리켜야 합니다. 모든 오버레이는 데이터 센터로의 L2 연결을 위해 동일한 물리적 인터페이스에 연결되어야 합니다.

Q) OTV 사이트 VLAN이 OTV 확장 VLAN과 다른 물리적 인터페이스에 있을 수 있습니까?

A) OTV 사이트 VLAN과 확장 VLAN은 동일한 물리적 인터페이스에 있어야 합니다.

Q) OTV에는 어떤 기능 세트가 필요합니까?

A) OTV에는 AIS(Advanced IP Services) 또는 AES(Advanced Enterprise Services)가 필요합니다.

Q) 고정 구성 플랫폼의 OTV에는 별도의 라이센스가 필요합니까?

A) 아니요. ASR1000이 Advispservices 또는 Adventuprise 부팅 수준을 구성한 상태로 실행되면 OTV를 사용할 수 있습니다.

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.