

IOS XR L2VPN 서비스 및 기능

목차

[소개](#)

[1. Point-to-Point 및 Multipoint 서비스](#)

[1.1 포인트-투-포인트 서비스](#)

[1.2 멀티포인트 서비스](#)

[2. 부착회로](#)

[2.1 ASR 9000 Ethernet Virtual Circuit](#)

[2.1.1 수신 인터페이스 일치](#)

[2.1.2 VLAN 조작](#)

[2.2 Cisco IOS XR 비EVC 라우터 동작\(CRS 및 XR12000\)](#)

[3. 포인트-투-포인트 서비스](#)

[3.1 로컬 스위칭](#)

[3.1.1 주 인터페이스](#)

[3.1.2 하위 인터페이스 및 VLAN 조작](#)

[3.2 Virtual Private Wire 서비스](#)

[3.2.1 개요](#)

[3.2.2 PW 및 AC 연결 상태](#)

[3.2.3 유형 4 및 유형 5 PW](#)

[3.2.4 멀티세그먼트 PW](#)

[3.2.5 이중화](#)

[3.3 CDP](#)

[3.3.1 L2VPN PE의 주 인터페이스에서 CDP가 활성화되지 않음](#)

[3.3.2 L2VPN PE의 주 인터페이스에서 CDP 활성화](#)

[3.4 스페닝 트리](#)

[4. 다중 지점 서비스](#)

[4.1 로컬 스위칭](#)

[4.2 전체 MST](#)

[4.3 BVI](#)

[4.4 VPLS](#)

[4.4.1 개요](#)

[4.4.2 PW 유형 및 전송된 태그](#)

[4.4.3 자동 검색 및 신호 처리](#)

[4.4.4 MAC 플러시 및 인출](#)

[4.4.5 H-VPLS](#)

[4.4.6 SHG\(Split Horizon Group\)](#)

[4.4.7 이중화](#)

[4.5 트래픽 스톱 제어](#)

[4.6 MAC 이동](#)

[4.7 IGMP 및 MLD 스누핑](#)

[5. 추가 L2VPN 항목](#)

[5.1 로드 밸런싱](#)

[5.2 로깅](#)

[5.3 이더넷 서비스 액세스 목록](#)

[5.4 이더넷 이그레스 필터](#)

소개

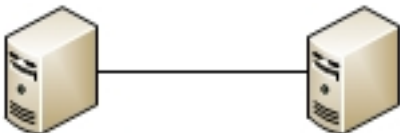
이 문서에서는 기본 L2(Layer 2) VPN(L2VPN) 토폴로지에 대해 설명합니다. 디자인, 서비스, 기능 및 구성을 보여주기 위해 기본적인 예를 제시하는 것이 유용합니다. 자세한 내용은 [Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide, Release 4.3.x](#)를 참조하십시오.

1. Point-to-Point 및 Multipoint 서비스

L2VPN 기능은 Point-to-Point 및 Multipoint 서비스를 제공하는 기능을 제공합니다.

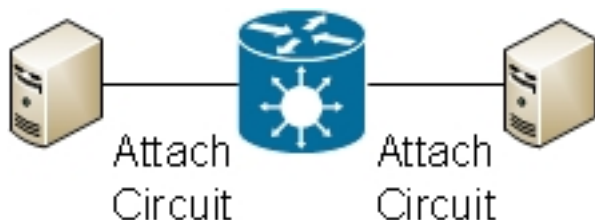
1.1 포인트-투-포인트 서비스

Point-to-Point 서비스는 기본적으로 두 엔드 노드 간의 전송 회로를 에뮬레이트하므로 엔드 노드가 Point-to-Point 링크를 통해 직접 연결된 것처럼 보입니다. 두 사이트를 연결하는 데 사용할 수 있습니다.

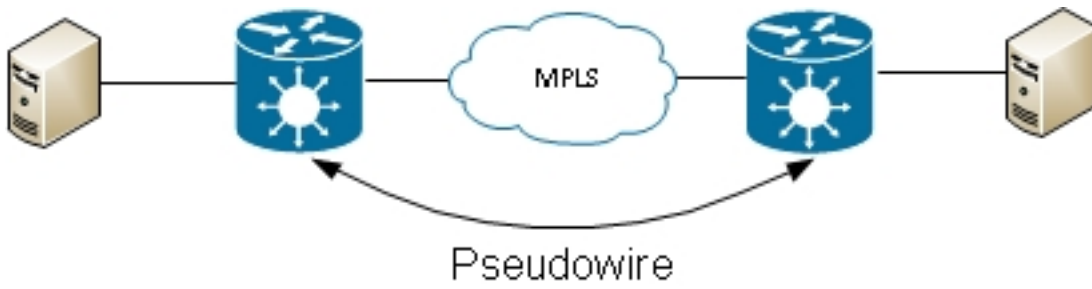


실제로 두 엔드 노드 사이에 여러 라우터가 있을 수 있으며, 포인트 투 포인트 서비스를 제공하기 위한 여러 설계가 있을 수 있습니다.

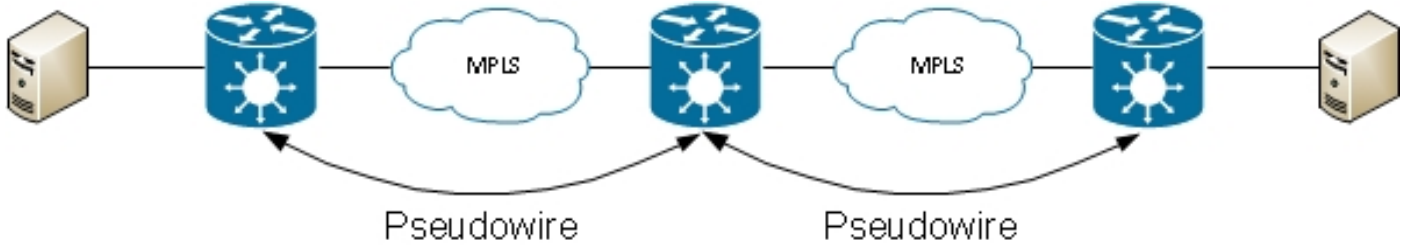
하나의 라우터가 두 인터페이스 간에 로컬 스위칭을 수행할 수 있습니다.



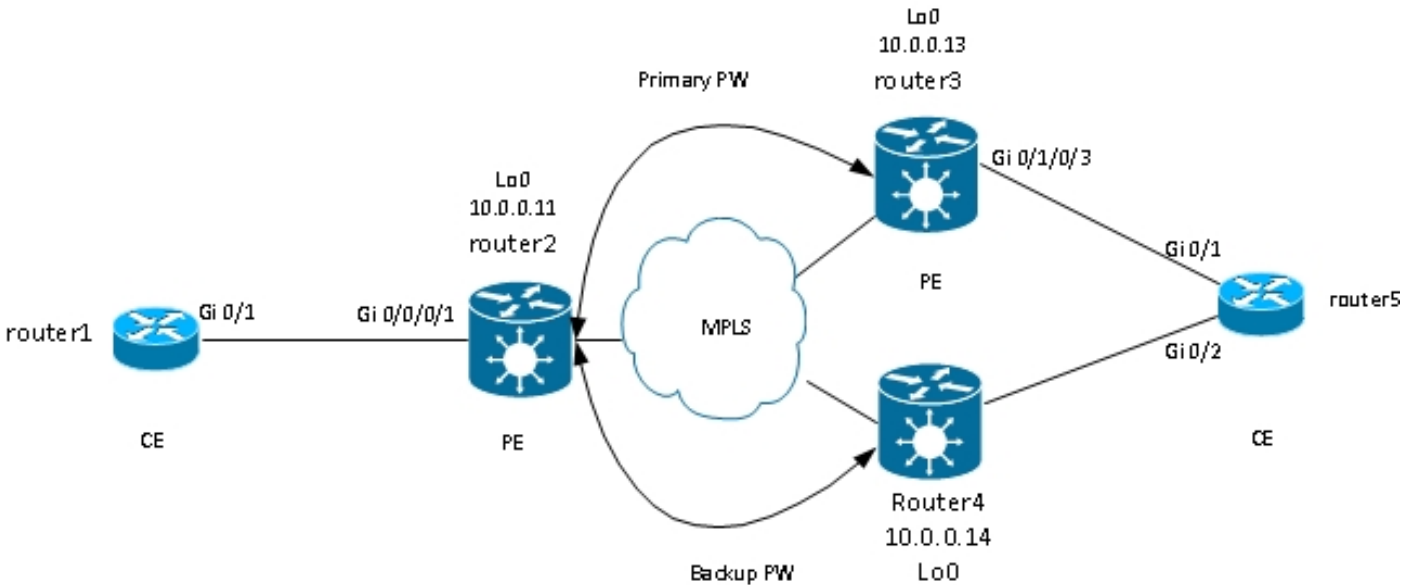
두 라우터 간에는 MPLS(Multiprotocol Label Switching) PW(pseudowire)가 있을 수도 있습니다.



라우터는 두 PW 간에 프레임을 전환할 수 있습니다. 이 경우 다중 세그먼트 PW입니다.



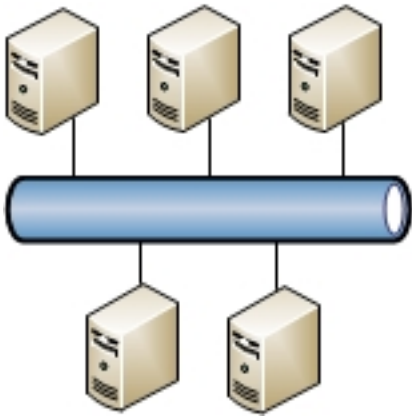
이중화는 PW 이중화 기능을 통해 사용할 수 있습니다.



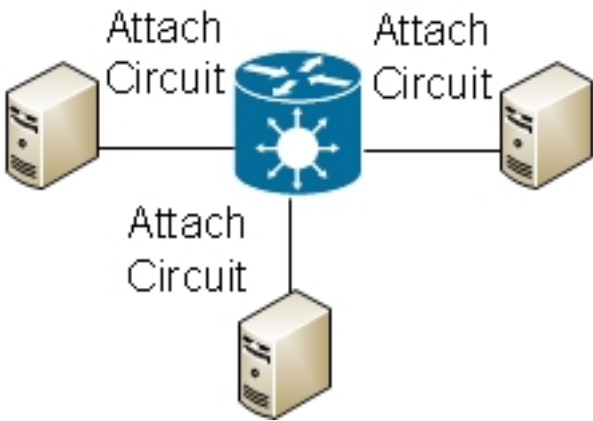
다른 디자인도 가능하지만, 모두 여기에 나열할 수는 없습니다.

1.2 멀티포인트 서비스

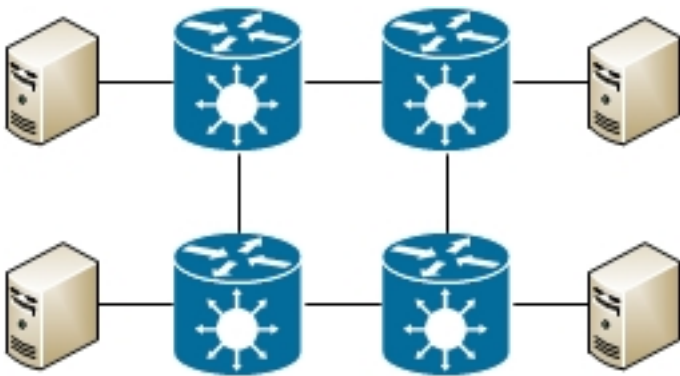
멀티포인트 서비스는 브로드캐스트 도메인을 에뮬레이트하므로 해당 브리지 도메인에 연결된 모든 호스트는 동일한 이더넷 세그먼트에 논리적으로 연결된 것처럼 보입니다.



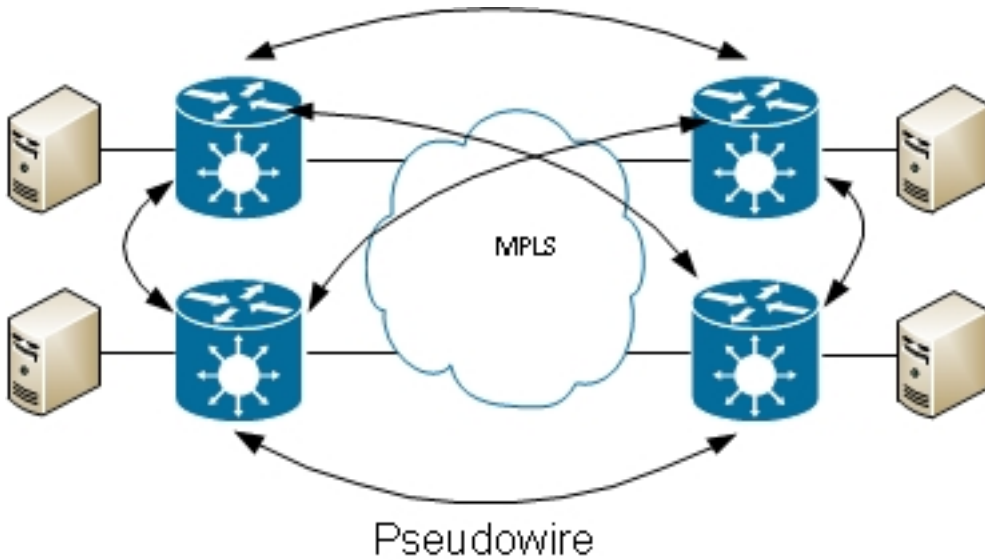
모든 호스트를 동일한 라우터/스위치에 연결할 수 있습니다.



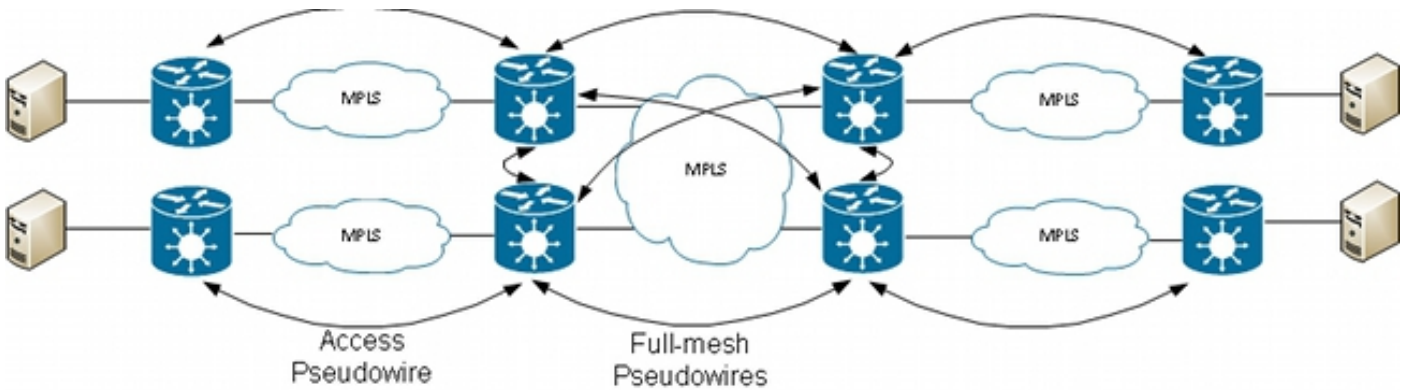
여러 스위치로 기존 이더넷 스위칭을 수행할 수 있습니다. 루프를 끊으려면 스패닝 트리를 사용해야 합니다.



VPLS(Virtual Private LAN Services)를 사용하면 MPLS PW를 사용하여 여러 사이트 간에 브로드캐스트 도메인을 확장할 수 있습니다.



계층적 VPLS를 사용하여 확장성을 높일 수 있습니다.



2. 부착회로

2.1 ASR 9000 Ethernet Virtual Circuit

2.1.1 수신 인터페이스 일치

AC(Attachment Circuit)에 대한 기본 규칙은 다음과 같습니다.

- L2VPN 기능에서 처리하려면 *I2transport* 키워드로 구성된 인터페이스에서 패킷을 수신해야 합니다.
- 이 인터페이스는 ***I2transport* 명령**이 인터페이스 컨피그레이션 모드에서 구성되는 주 인터페이스일 수도 있고, 하위 인터페이스 뒤에 *I2transport* 키워드가 구성되는 하위 인터페이스일 수도 있습니다.
- 가장 긴 일치 조회는 패킷의 수신 인터페이스를 결정합니다. 가장 긴 일치 조회는 수신 패킷을 하위 인터페이스에 일치시키기 위해 다음 조건을 순서대로 확인합니다.

1. 들어오는 프레임에는 두 개의 dot1q 태그가 있으며 동일한 두 개의 dot1q 태그(802.1Q 터널링 또는 QinQ)로 구성된 하위 인터페이스와 일치합니다. 가능한 한 가장 긴 일치입니다.
2. 들어오는 프레임에는 두 개의 dot1q 태그가 있으며 동일한 dot1q 첫 번째 태그와 두 번째 태

그에 대해 *any*로 구성된 하위 인터페이스와 일치합니다.

3. 들어오는 프레임에는 dot1q 태그가 하나씩 있으며 동일한 dot1q 태그 및 *exact* 키워드로 구성된 하위 인터페이스와 일치합니다.
4. 들어오는 프레임에는 하나 이상의 dot1q 태그가 있으며 dot1q 태그 중 하나로 구성된 하위 인터페이스와 일치합니다.
5. 들어오는 프레임에는 dot1q 태그가 없으며 *encapsulation untagged* 명령으로 구성된 하위 인터페이스와 일치합니다.
6. 수신 프레임은 다른 하위 인터페이스와 일치하지 않으므로 *encapsulation default* 명령으로 구성된 하위 인터페이스와 일치합니다.
7. 수신 프레임은 다른 하위 인터페이스와 일치하지 않으므로 *I2transport*에 대해 구성된 기본 인터페이스와 일치합니다.

- EVC(Ethernet Virtual Connection) 모델을 사용하지 않는 기존 라우터에서는 하위 인터페이스에 구성된 VLAN 태그가 L2VPN 기능에 의해 전송되기 전에 프레임에서 제거(팝업)됩니다.
- EVC 인프라를 사용하는 Cisco ASR 9000 Series Aggregation Services Router에서 기본 작업은 기존 태그를 보존하는 것입니다. 기본값을 수정하려면 **rewrite** 명령을 사용합니다.
- 브리지 도메인에 BVI(Bridge Virtual Interface)가 있는 경우 BVI는 태그가 없는 라우터드 인터페이스이므로 모든 수신 태그가 팝업되어야 합니다. 자세한 내용은 [BVI](#) 섹션을 참조하십시오.

다음은 이러한 규칙을 보여 주는 몇 가지 예입니다.

1. 기본 예는 VLAN 태그가 있는지 여부에 관계없이 물리적 포트에서 수신된 모든 트래픽을 전송해야 하는 경우입니다. 기본 인터페이스에서 **I2transport**를 구성할 경우 해당 물리적 포트에서 수신된 모든 트래픽이 L2VPN 기능에 의해 전송됩니다.

```
interface GigabitEthernet0/0/0/2
I2transport
```

해당 기본 인터페이스의 하위 인터페이스가 있는 경우, 기본 인터페이스는 하위 인터페이스가 매칭하지 않은 프레임을 catch합니다. 이는 가장 긴 일치 규칙입니다.

2. 번들 인터페이스 및 하위 인터페이스는 **I2transport**로 구성할 수 있습니다.

```
interface Bundle-Ether1
I2transport
```

3. **I2transport** 하위 인터페이스 아래에서 캡슐화 기본값을 사용하여 가장 긴 일치 항목을 가진 다른 하위 인터페이스에 의해 매칭되지 않은 태그되거나 태그되지 않은 모든 트래픽을 매칭합니다. (예 4 참조). **I2transport** 키워드는 기본 인터페이스에서처럼 하위 인터페이스 아래에 구성되지 않고 하위 인터페이스 이름에 구성됩니다.

```
interface GigabitEthernet0/1/0/3.1 I2transport
encapsulation default
```

태그 없는 프레임만 일치시키려면 캡슐화 태그 없는 프레임을 구성합니다.

4. 여러 하위 인터페이스가 있는 경우 수신 인터페이스를 확인하기 위해 수신 프레임에 대해 가장 긴 일치 테스트를 실행합니다.

```
interface GigabitEthernet0/1/0/3.1 I2transport
encapsulation default
```

```
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 2 second-dot1q 3
```

이 컨피그레이션에서는 다음 사항에 유의하십시오.

- 외부 VLAN 태그 2 및 내부 VLAN 태그 3이 있는 QinQ 프레임은 .1, .2 또는 .3 하위 인터페이스와 일치할 수 있지만 가장 긴 일치 규칙 때문에 .3 하위 인터페이스에 할당됩니다. .3의 태그 2개는 .2의 태그 1개보다 길고 .1의 태그가 없는 태그 1개보다 깁니다.
- 외부 VLAN 태그 2 및 내부 VLAN 태그 4가 있는 QinQ 프레임은 .2 하위 인터페이스에 할당됩니다. 캡슐화 **dot1q 2**는 dot1q 프레임을 VLAN 태그 2로만 매칭할 수 있지만 외부 태그 2로도 매칭할 수 있기 때문입니다. QinQ 프레임과 일치하지 않으려는 경우 예제 5(*exact* 키워드)를 참조하십시오.
- 외부 VLAN 태그 3이 있는 QinQ 프레임은 .1 하위 인터페이스와 일치합니다.
- VLAN 태그 2가 있는 dot1q 프레임은 .2 하위 인터페이스와 일치합니다.
- VLAN 태그 3이 있는 dot1q 프레임은 .1 하위 인터페이스와 일치합니다.

5. QinQ 프레임이 아닌 dot1q 프레임과 일치하려면 *exact* 키워드를 사용합니다.

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2 exact
```

이 컨피그레이션은 정확히 하나의 VLAN 태그가 있는 프레임만 일치하므로 외부 VLAN 태그가 2인 QinQ 프레임과 일치하지 않습니다.

6. CDP(Cisco Discovery Protocol) 패킷 또는 MST(Multiple Spanning Tree) BPDU(Bridge Protocol Data Units)와 같이 태그가 지정되지 않은 프레임만 일치시키려면 태그가 지정되지 않은 키워드를 사용합니다.

```
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation default
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```

이 컨피그레이션에서는 다음 사항에 유의하십시오.

- VLAN 태그 3이 있는 Dot1q 프레임 또는 외부 태그 3이 있는 QinQ 프레임은 .3 하위 인터페이스와 일치합니다.
- 다른 모든 dot1q 또는 QinQ 프레임은 .1 하위 인터페이스와 일치합니다.
- VLAN 태그가 없는 프레임은 .2 하위 인터페이스와 일치합니다.

7. *any* 키워드는 와일드카드로 사용할 수 있습니다.

```
interface GigabitEthernet0/1/0/3.4 l2transport
encapsulation dot1q 4 second-dot1q any
```

```
!  
interface GigabitEthernet0/1/0/3.5 l2transport  
encapsulation dot1q 4 second-dot1q 5
```

하위 인터페이스 .4와 .5 모두 QinQ 프레임과 태그 4 및 5를 일치시킬 수 있지만, 보다 구체적이므로 .5 하위 인터페이스에 프레임이 할당됩니다. 가장 긴 일치 규칙입니다.

8. VLAN 태그의 범위를 사용할 수 있습니다.

```
interface GigabitEthernet0/1/0/3.6 l2transport  
encapsulation dot1q 6-10
```

9. 첫 번째 또는 두 번째 dot1q 태그에 대해 여러 VLAN 태그 값 또는 범위를 나열할 수 있습니다.

```
interface GigabitEthernet0/1/0/3.7 l2transport  
encapsulation dot1q 6 , 7 , 8-10  
!  
interface GigabitEthernet0/1/0/3.11 l2transport  
encapsulation dot1q 11 second-dot1q 1 , 2 , 3 , 4-6 , 10
```

최대 9개의 값을 나열할 수 있습니다. 더 많은 값이 필요한 경우 다른 하위 인터페이스에 할당해야 합니다. 목록의 길이를 줄이기 위해 범위 내의 값을 그룹화합니다.

10. encapsulation dot1q second-dot1q 명령은 QinQ 프레임을 캡슐화하는 Cisco 방법이므로 외부 및 내부 태그에 Ethertype 0x8100을 사용합니다. 그러나 IEEE에 따르면, 이더 타입 0x8100은 하나의 VLAN 태그가 있는 802.1q 프레임용으로 예약되어야 하며, 이더 타입 0x88a8이 있는 외부 태그는 QinQ 프레임용으로 사용되어야 합니다. Ethertype 0x88a8의 외부 태그는 dot1ad 키워드로 구성할 수 있습니다.

```
interface GigabitEthernet0/1/0/3.12 l2transport  
encapsulation dot1ad 12 dot1q 100
```

11. QinQ 외부 태그에 기존 Ethertype 0x9100 또는 0x9200을 사용하려면 QinQ 하위 인터페이스의 주 인터페이스 아래에서 dot1q tunneling ethertype 명령을 사용합니다.

```
interface GigabitEthernet0/1/0/3  
dot1q tunneling ethertype [0x9100|0x9200]  
!  
interface GigabitEthernet0/1/0/3.13 l2transport  
encapsulation dot1q 13 second-dot1q 100
```

외부 태그의 이더 타입은 0x9100 또는 0x9200이고, 내부 태그의 이더 타입은 dot1q 이더 타입 0x8100입니다.

12. 수신 프레임은 소스 MAC 주소를 기반으로 하위 인터페이스에 할당할 수 있습니다.

```
interface GigabitEthernet0/1/0/3.14 l2transport  
encapsulation dot1q 14 ingress source-mac 1.1.1
```

2.1.2 VLAN 조작

EVC 기반 플랫폼의 기본 동작은 수신 프레임에 VLAN 태그를 유지하는 것입니다.


```
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```

이 컨피그레이션에서는 VLAN 태그 3이 있는 수신 dot1q 프레임이 프레임이 전달될 때 VLAN 태그 3을 유지합니다. 외부 VLAN 태그 3 및 내부 태그 100을 가진 들어오는 QinQ 프레임은 프레임이 전달될 때 두 태그를 변경하지 않고 유지합니다.

그러나 EVC 인프라를 사용하면 **rewrite 명령**으로 태그를 조작할 수 있으므로 수신 VLAN 태그 스택에 태그를 팝업(제거), 변환 또는 푸시(추가)할 수 있습니다.

다음은 몇 가지 예입니다.

- **pop** 키워드를 사용하면 들어오는 dot1q 프레임에서 QinQ 태그를 제거할 수 있습니다. 다음 예에서는 들어오는 QinQ 프레임의 외부 태그(13)를 제거하고 dot1q 태그(100)가 위에 있는 프레임을 전달합니다.

```
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
rewrite ingress tag pop 1 symmetric
```

거동은 항상 대칭적인데, 이는 외부 태그(13)가 인그레스 방향으로 팝업되고 이그레스 방향으로 푸시됨을 의미한다.

- **translate** 키워드를 사용하면 하나 또는 두 개의 수신 태그를 하나 또는 두 개의 새 태그로 대체할 수 있습니다.

```
RP/0/RSP0/CPU0:router2(config-subif)#interface GigabitEthernet0/1/0/3.3
l2transport
RP/0/RSP0/CPU0:router2(config-subif)# encapsulation dot1q 3
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate ?
1-to-1 Replace the outermost tag with another tag
1-to-2 Replace the outermost tag with two tags
2-to-1 Replace the outermost two tags with one tag
2-to-2 Replace the outermost two tags with two other tags
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1 ?
dot1ad Push a Dot1ad tag
dot1q Push a Dot1Q tag
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1
dot1q 4
RP/0/RSP0/CPU0:router2(config-subif)#show config
Building configuration...
!! IOS XR Configuration 4.3.0
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag translate 1-to-1 dot1q 4 symmetric
!
end
```

symmetric 키워드는 지원되는 유일한 모드이므로 자동으로 추가됩니다.

- **push** 키워드를 사용하면 들어오는 dot1q 프레임에 QinQ 태그를 추가할 수 있습니다.

```
interface GigabitEthernet0/1/0/3.4 l2transport
encapsulation dot1q 4
rewrite ingress tag push dot1q 100 symmetric
```

외부 QinQ 태그(100)가 dot1q 태그(4)를 갖는 착신 프레임에 추가된다. 이그레스 방향에서는 QinQ

태그가 팝업됩니다.

2.2 Cisco IOS XR 비EVC 라우터 동작(CRS 및 XR12000)

비 EVC 플랫폼에서 VLAN 일치를 위한 구문은 encapsulation 키워드를 사용하지 않습니다.

```
RP/0/RP0/CPU0:router1#config
RP/0/RP0/CPU0:router1(config)#int gig 0/0/0/2.3 l2transport
RP/0/RP0/CPU0:router1(config-subif)#dot1q ?
vlan Configure a VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan ?
<1-4094> Configure first (outer) VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 ?
<1-4094> Configure second (inner 802.1Q) VLAN ID on the subinterface
any Match frames with any second 802.1Q VLAN ID
```

```
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 100
```

dot1q 또는 dot1ad 명령에 지정된 모든 태그를 팝업하는 동작만 가능하므로 VLAN 태그 조작을 구성할 수 없습니다. 이 작업은 기본적으로 수행되므로 rewrite 명령이 없습니다.

3. 포인트-투-포인트 서비스

참고:

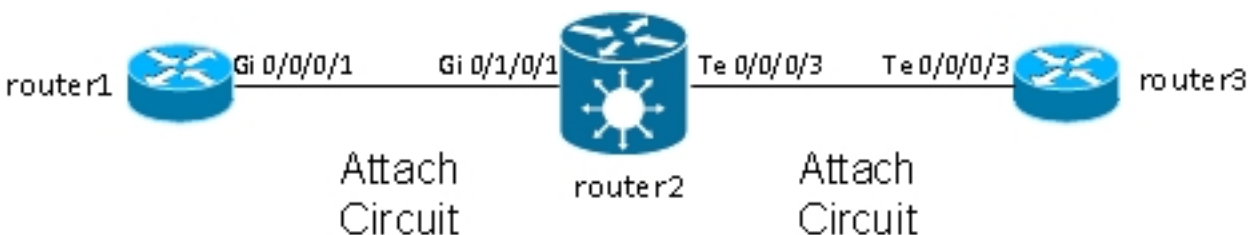
이 섹션에 사용된 명령에 대한 자세한 내용을 가져오려면 [명령 조회 툴\(등록 고객 전용\)](#)을 사용하십시오.

[아웃풋 인터프리터 툴\(등록 고객 전용\)](#)은 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

3.1 로컬 스위칭

3.1.1 주 인터페이스

기본 토폴로지는 두 기본 인터페이스 간의 로컬 교차 연결입니다.



Router2는 Gi 0/1/0/1에서 수신된 모든 트래픽을 가져와서 Te 0/0/0/3으로 전달하거나 그 반대로 전달합니다.

이 토폴로지에서는 router1과 router3이 직접 백-투-백 케이블을 사용하는 것처럼 보이지만, router2가 실제로 TenGigE와 GigabitEthernet 인터페이스 간에 전환되기 때문에 그렇지 않습니다. 라우터2는 이 두 인터페이스에서 기능을 실행할 수 있습니다. 예를 들어 ACL(Access Control List)은 낮은 우선순위 트래픽의 형태를 정하거나 속도를 제한하기 위해 특정 유형의 패킷 또는 정책 맵을 삭제할 수 있습니다.

기본 Point-to-Point 교차 연결은 라우터2에서 l2transport로 구성된 두 개의 기본 인터페이스 사이에 구성됩니다.

```
interface GigabitEthernet0/1/0/1
l2transport
!
!
interface TenGigE0/0/0/3
l2transport
!
!
l2vpn
xconnect group test
p2p p2p1
interface TenGigE0/0/0/3
interface GigabitEthernet0/1/0/1
!
```

router1 및 router3에서 기본 인터페이스는 CDP 및 IPv4 주소로 구성됩니다.

```
RP/0/RP0/CPU0:router1#sh run int Gi 0/0/0/1
interface GigabitEthernet0/0/0/1
cdp
ipv4 address 10.1.1.1 255.255.255.0
!
```

```
RP/0/RP0/CPU0:router1#
RP/0/RP0/CPU0:router1#sh cdp nei Gi 0/0/0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
```

```
Device ID Local Intrfce Holdtme Capability Platform Port ID
router3.cisco.c Gi0/0/0/1 132 R ASR9K Ser Te0/0/0/3
```

```
RP/0/RP0/CPU0:router1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/32 ms
```

Router1은 router3을 CDP 네이버로 간주하며 두 라우터가 직접 연결된 것처럼 10.1.1.2(router3의 인터페이스 주소)를 ping할 수 있습니다.

라우터 2에 구성된 하위 인터페이스가 없으므로 dot1q 하위 인터페이스가 라우터 1과 라우터 3에 구성된 경우 VLAN 태그가 있는 수신 프레임이 투명하게 전송됩니다.

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2
ipv4 address 10.1.2.1 255.255.255.0
dot1q vlan 2
!
```

```
RP/0/RP0/CPU0:router1#ping 10.1.2.2
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms

router1에서 router3으로 10,000번의 ping을 수행한 후에는 **show interface** 및 **show l2vpn** 명령을 사용하여 한 AC에서 router2가 수신한 ping 요청이 다른 AC에서 전달되고 ping 응답이 반대 방향으로 동일하게 처리되도록 할 수 있습니다.

```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 1000Mb/s, SXFD, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:01:07
5 minute input rate 28000 bits/sec, 32 packets/sec
5 minute output rate 28000 bits/sec, 32 packets/sec
10006 packets input, 1140592 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 6 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10007 packets output, 1140832 bytes, 0 total output drops
Output 0 broadcast packets, 7 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

```
RP/0/RSP0/CPU0:router2#sh int ten 0/0/0/3
TenGigE0/0/0/3 is up, line protocol is up
Interface state transitions: 3
Hardware is TenGigE, address is 0024.98ea.038b (bia 0024.98ea.038b)
Layer 1 Transport Mode is LAN
Description: static lab connection to putin 0/0/0/3 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, LR, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:06
Last clearing of "show interface" counters 00:01:15
5 minute input rate 27000 bits/sec, 30 packets/sec
5 minute output rate 27000 bits/sec, 30 packets/sec
10008 packets input, 1140908 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 8 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10006 packets output, 1140592 bytes, 0 total output drops
Output 0 broadcast packets, 6 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
```

0 carrier transitions

RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test

Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2

Group Name ST Description ST Description ST

test p2p1 UP Te0/0/0/3 UP Gi0/1/0/1 UP

RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p1, state is up; Interworking none

AC: TenGigE0/0/0/3, state is up

Type Ethernet

MTU 1500; XC ID 0x1080001; interworking none

Statistics:

packets: received 10008, sent 10006

bytes: received 1140908, sent 1140592

AC: GigabitEthernet0/1/0/1, state is up

Type Ethernet

MTU 1500; XC ID 0x1880003; interworking none

Statistics:

packets: received 10006, sent 10008

bytes: received 1140592, sent 1140908

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface gigabitEthernet 0/1/0/1
hardware ingress detail location 0/1/CPU0

Local interface: GigabitEthernet0/1/0/1, Xconnect id: 0x1880003, Status: up
Segment 1

AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound

Statistics:

packets: received 10022, sent 10023

bytes: received 1142216, sent 1142489

packets dropped: PLU 0, tail 0

bytes dropped: PLU 0, tail 0

Segment 2

AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound

Platform AC context:

Ingress AC: Local Switch, State: Bound

Flags: Remote is Simple AC

XID: 0x00580003, SHG: None

Ingress uIDB: 0x0003, Egress uIDB: 0x0003, NP: 3, Port Learn Key: 0

NP3

Ingress uIDB:

Flags: L2, Status

Stats Ptr: 0x0d842c, uIDB index: 0x0003, Wire Exp Tag: 0

BVI Bridge Domain: 0, BVI Source XID: 0x01000000

VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000

L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0

QOS ID: 0, QOS Format ID: 0

Local Switch dest XID: 0x00000001

UIDB IF Handle: 0x00000000, Source Port: 1, Num VLANs: 0

Xconnect ID: 0x00580003, NP: 3

Type: AC, Remote type: AC

Flags: Learn enable

uIDB Index: 0x0003, LAG pointer: 0x0000

Split Horizon Group: None

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface Te 0/0/0/3 hardware egress
detail location 0/0/CPU0

```

Local interface: TenGigE0/0/0/3, Xconnect id: 0x1080001, Status: up
Segment 1
AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound
Statistics:
packets: received 10028, sent 10027
bytes: received 1143016, sent 1142732
packets dropped: PLU 0, tail 0
bytes dropped: PLU 0, tail 0
Segment 2
AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound

```

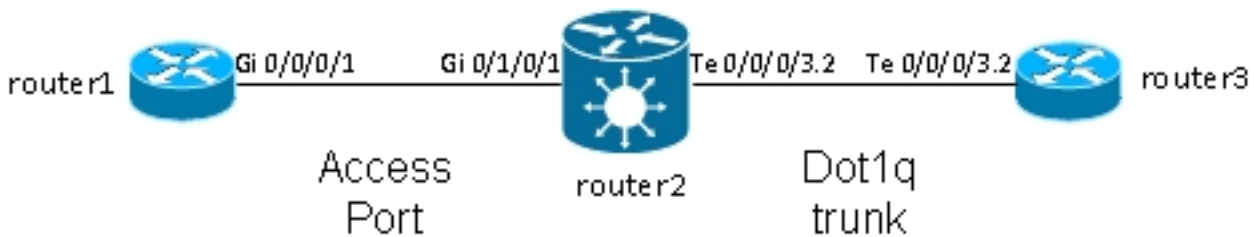
```

Platform AC context:
Egress AC: Local Switch, State: Bound
Flags: Remote is Simple AC
XID: 0x00000001, SHG: None
Ingress uIDB: 0x0007, Egress uIDB: 0x0007, NP: 0, Port Learn Key: 0
NP0
Egress uIDB:
Flags: L2, Status, Done
Stats ptr: 0x000000
VPLS SHG: None
L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0
VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000
UIDB IF Handle: 0x04000240, Search VLAN Vector: 0
QOS ID: 0, QOS format: 0
Xconnect ID: 0x00000001, NP: 0
Type: AC, Remote type: AC
Flags: Learn enable
uIDB Index: 0x0007, LAG pointer: 0x0000
Split Horizon Group: None

```

3.1.2 하위 인터페이스 및 VLAN 조작

Cisco IOS® 소프트웨어 용어에서 이 예에는 switchport 모드 액세스 인터페이스와 같은 하나의 AC와 트렁크와 같은 dot1q 하위 인터페이스가 있습니다.



일반적으로 이 토폴로지에서는 브리지 도메인을 사용합니다. VLAN에 포트가 두 개 이상 있지만 두 포트만 있는 경우 지점 간 교차 연결을 사용할 수 있습니다. 이 섹션에서는 유연한 재작성 기능을 통해 VLAN을 조작하는 여러 가지 방법을 제공하는 방법을 설명합니다.

3.1.2.1 주 인터페이스 및 Dot1q 하위 인터페이스

이 예에서 기본 인터페이스는 한 쪽에 있고 dot1q 하위 인터페이스는 다른 쪽에 있습니다.

다음은 router1의 기본 인터페이스입니다.

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1
```

```
interface GigabitEthernet0/0/0/1
description static lab connection to router2 0/1/0/1
cdp
ipv4 address 10.1.1.1 255.255.255.0
!
```

다음은 router2의 dot1q 하위 인터페이스입니다.

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/1
interface GigabitEthernet0/1/0/1
description static lab connection to router1 0/0/0/1
l2transport
```

```
RP/0/RSP0/CPU0:router2#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
```

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p2
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1
```

이제 하위 인터페이스 이름인 *TenGigE0/0/0/3.2*에 l2transport 키워드가 있습니다. Router3은 tag 2가 포함된 dot1q 프레임을 전송하며, 이는 router2의 TenGigE0/0/0/3.2 하위 인터페이스와 일치합니다.

인커밍 태그 2는 **rewrite ingress tag pop 1 symmetric** 명령에 의해 이그레스 방향으로 제거됩니다. TenGigE0/0/0/3.2에서 이그레스 방향으로 태그가 제거되었으므로 패킷은 GigabitEthernet0/1/0/1에서 이그레스 방향으로 태그가 지정되지 않은 상태로 전송됩니다.

Router1은 태그되지 않은 프레임을 전송하며, 이는 기본 인터페이스인 GigabitEthernet0/1/0/1과 일치합니다.

GigabitEthernet0/1/0/1에는 **rewrite** 명령이 없으므로 태그가 팝업, 푸시 또는 변환되지 않습니다.

TenGigE0/0/0/3.2에서 패킷을 전달해야 하는 경우, dot1q 태그 2는 **rewrite ingress tag pop 1** 명령의 **symmetric** 키워드로 인해 푸시됩니다. 이 명령은 이그레스 방향으로 하나의 태그를 팝업하지만 이그레스 방향으로 하나의 태그를 대칭적으로 푸시합니다. 다음은 router3의 예입니다.

```
RP/0/RSP0/CPU0:router3#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2
ipv4 address 10.1.1.2 255.255.255.0
encapsulation dot1q 2
```

동일한 **show interface** 및 **show l2vpn** 명령으로 하위 인터페이스 카운터를 모니터링합니다.

```
RP/0/RSP0/CPU0:router2#clear counters
Clear "show interface" counters on all interfaces [confirm]
RP/0/RSP0/CPU0:router2#clear l2vpn forwarding counters
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#sh int TenGigE0/0/0/3.2
TenGigE0/0/0/3.2 is up, line protocol is up
Interface state transitions: 1
Hardware is VLAN sub-interface(s), address is 0024.98ea.038b
```

```
Layer 2 Transport Mode
MTU 1518 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability Unknown, txload Unknown, rxload Unknown
Encapsulation 802.1Q Virtual LAN,
Outer Match: Dot1Q VLAN 2
Ethertype Any, MAC Match src any, dest any
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:00:27
1000 packets input, 122000 bytes
0 input drops, 0 queue drops, 0 input errors
1002 packets output, 122326 bytes
0 output drops, 0 queue drops, 0 output errors
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect detail
```

```
Group test, XC p2p2, state is up; Interworking none
AC: TenGigE0/0/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1080001; interworking none
Statistics:
packets: received 1001, sent 1002
bytes: received 118080, sent 118318
drops: illegal VLAN 0, illegal length 0
AC: GigabitEthernet0/1/0/1, state is up
Type Ethernet
MTU 1500; XC ID 0x1880003; interworking none
Statistics:
```

```
packets: received 1002, sent 1001
bytes: received 114310, sent 114076
```

예상대로 TenGigE0/0/0/3.2에서 수신된 패킷 수는 GigabitEthernet0/1/0/1에서 전송된 패킷 수와 일치하며, 그 반대의 경우도 마찬가지입니다.

3.1.2.2 캡슐화가 포함된 하위 인터페이스

GigabitEthernet0/1/0/1의 기본 인터페이스 대신, 모든 프레임을 catch하기 위해 encapsulation default를 사용하는 하위 인터페이스를 사용하거나 태그 없는 프레임만 일치시키기 위해 encapsulation untagged를 사용하는 하위 인터페이스를 사용할 수 있습니다.

```
RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged
```

```
RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
```

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

3.1.2.3 GigabitEthernet0/1/0/1.1의 인그레스 방향

TenGigE0/0/0/3.2의 인그레스 방향으로 태그 2를 팝업하는 대신 GigabitEthernet0/1/0/1.1의 인그레스 방향으로 태그 2를 푸시할 수 있으며 TenGigE0/0/0/3.2에서는 아무것도 수행하지 않습니다.

```
RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
```

```
RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged
rewrite ingress tag push dot1q 2 symmetric
```

```
RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
```

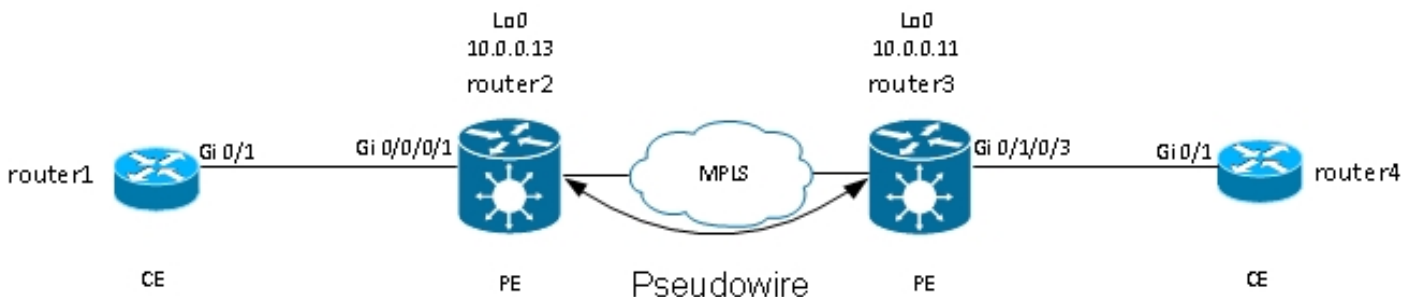
```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

따라서 encapsulation and rewrite 명령을 사용하는 EVC 모델에서 VLAN 태그를 확인하고 조작할 수 있는 뛰어난 유연성을 제공합니다.

3.2 Virtual Private Wire 서비스

3.2.1 개요

EoMPLS(Ethernet over MPLS)라고도 하는 VPWS(Virtual Private Wire Services)는 두 개의 L2VPN PE(Provider Edge) 디바이스가 MPLS 클라우드를 통해 L2VPN 트래픽을 터널링할 수 있도록 합니다. 두 L2VPN PE는 일반적으로 서로 다른 두 사이트에서 MPLS 코어를 사이에 두고 연결됩니다. 각 L2VPN PE에 연결된 2개의 AC는 MPLS 네트워크(MPLS PW)를 통해 PW로 연결됩니다.



원격 PE의 루프백에 도달하려면 각 PE에 MPLS 레이블이 있어야 합니다. 일반적으로 IGP(Interior Gateway Protocol) 레이블이라고 하는 이 레이블은 MPLS LDP(Label Distribution Protocol) 또는 MPLS TE(Traffic Engineering)를 통해 학습할 수 있습니다.

두 PE는 PW의 상태를 설정하고 제어할 수 있도록 PE 간에 대상 MPLS LDP 세션을 설정합니다. 한 PE는 PW 식별을 위해 MPLS 레이블을 다른 PE에 광고합니다.

참고: BGP는 시그널링에 사용될 수 있지만 이 문서에서는 다루지 않습니다.

로컬 AC에서 router2가 수신한 트래픽은 MPLS 레이블 스택에서 캡슐화됩니다.

- 외부 MPLS 레이블은 router3의 루프백에 연결하기 위한 IGP 레이블입니다. 레이블이 직접 연결된 경우 암시적-null 레이블일 수 있습니다. 즉, IGP 레이블이 추가되지 않습니다.
- 내부 MPLS 레이블은 대상 LDP 세션을 통해 라우터3에서 광고하는 PW 레이블입니다.
- 컨피그레이션 및 캡슐화 유형에 따라 MPLS 레이블 뒤에 PW 제어 단어가 있을 수 있습니다. 제어 단어는 이더넷 인터페이스에서 기본적으로 사용되지 않으며 필요할 때 명시적으로 구성해야 합니다.
- 전송된 L2 프레임은 패킷 내에서 뒤따릅니다.
- 일부 VLAN 태그는 컨피그레이션 및 PW 유형에 따라 PW를 통해 전송됩니다.

MPLS 코어의 router3 바로 앞의 Penultimate 홉은 IGP 레이블을 팝업하거나 명시적 null 레이블로 대체합니다. 따라서, 라우터3에 의해 수신된 프레임 상의 최상위 의미 있는 라벨은 라우터3이 PW를 위해 라우터2에 시그널링한 PW 라벨이다. 따라서 router3는 해당 MPLS 레이블로 수신된 트래픽을 router4에 연결된 AC로 전환해야 함을 알고 있습니다.

[이전](#) 예에서는 각 L2VPN에 원격 PE의 루프백에 대한 MPLS 레이블이 있는지 먼저 확인해야 합니다. 다음은 router2에서 레이블을 확인하는 방법의 예입니다.

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding prefix 10.0.0.11/32
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
-----
16008 16009 10.0.0.11/32 Te0/0/0/1 10.0.23.2 681260
```

AC 컨피그레이션은 여전히 동일합니다.

```
RP/0/RSP1/CPU0:router2#sh run int gig 0/0/0/1.2
Wed May 1 13:56:07.668 CEST
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
```

다시 쓰기 인그레스 pop 명령이 없으므로 들어오는 VLAN 태그 2가 PW를 통해 전송됩니다. 자세한 내용은 [유형 4 및 5 PW](#)를 참조하십시오.

L2VPN 컨피그레이션은 로컬 AC 및 원격 L2VPN PE를 PW ID로 지정합니다. PW ID는 각 측면에서 일치해야 하며 각 네이버에 대해 고유해야 합니다.

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 222
```

router3의 해당 컨피그레이션은 다음과 같습니다.

```
RP/0/RSP0/CPU0:router3#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
```

```
RP/0/RSP0/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
```

```
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
```

교차 연결에 대한 세부사항을 보려면 show l2vpn xconnect detail 명령을 사용합니다.

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail
```

```
Group test, XC p2p4, state is up; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38448
bytes: received 12644, sent 2614356
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
```

```
-----
Label 16026                               16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2       GigabitEthernet0/1/0/3.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
```

```
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (21:31:00 ago)
Last time status changed: 30/04/2013 16:36:42 (21:25:16 ago)
Statistics:
packets: received 38448, sent 186
bytes: received 2614356, sent 12644
```

이 컨피그레이션에서는 다음 사항에 유의하십시오.

- AC의 수신 태그가 팝업되지 않으므로 AC의 MTU(최대 전송 단위)는 1504입니다. MTU가 양쪽에서 일치해야 합니다. 그렇지 않으면 PW가 나타나지 않습니다.
- 186개의 패킷이 AC에서 수신되었고 예상대로 PW에서 전송되었습니다.
- 38448 패킷은 PW에서 수신되었으며 예상대로 AC에서 전송되었습니다.
- router2의 로컬 레이블은 16026이며 router3에서 내부 레이블로 사용하는 레이블입니다. 패킷이 라우터2에서 상위 레이블로 수신되는데, 이는 IGP 레이블이 중간 MPLS 홉에 의해 팝업되었기 때문입니다. Router2는 해당 PW 레이블의 수신 프레임을 AC Gi 0/0/0/1.2로 전환해야 함을 알고 있습니다.

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding labels 16026
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
-----
16026 Pop PW(10.0.0.11:222) Gi0/0/0/1.2 point2point 2620952
```

3.2.2PW 및 AC 연결 상태

접대점 교차 연결에서, AC와 PW가 결합된다. 따라서 AC가 다운되면 L2VPN PE는 LDP를 통해 원격 PE에 PW 상태가 다운되어야 함을 알립니다. 이렇게 하면 PW 이중화가 구성된 경우 컨버전스가 트리거됩니다. 자세한 내용은 [Redundancy](#) 섹션을 참조하십시오.

이 예에서 AC는 router2에서 다운되어 'AC Down' PW 상태를 router3으로 전송합니다.

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail
Wed May 1 23:38:55.542 CEST
```

```
Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is down
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38544
bytes: received 12644, sent 2620884
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is down ( remote standby )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```
PW Status TLV in use
MPLS Local Remote
```

```
-----
Label 16026 16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2 GigabitEthernet0/1/0/3.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
```

```
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (1d07h ago)
Last time status changed: 01/05/2013 14:05:07 (09:33:47 ago)
Statistics:
packets: received 38544, sent 186
bytes: received 2620884, sent 12644
```

라우터3은 원격 AC가 다운되었기 때문에 PW가 다운되어야 함을 알고 있습니다.

```
RP/0/RSP0/CPU0:router3#sh l2vpn xconnect group test xc-name p2p4 detail
```

```
Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 38545, sent 186
bytes: received 2620952, sent 12644
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```
PW Status TLV in use
```

```
MPLS Local Remote
```

```
-----
Label 16031 16026
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
```

```
Incoming Status (PW Status TLV):
```

```
Status code: 0x6 (AC Down) in Notification message
```

```
Outgoing Status (PW Status TLV):
```

```
Status code: 0x0 (Up) in Notification message
```

```
MIB cpwVcIndex: 3221225477
```

```
Create time: 30/04/2013 16:37:57 (1d07h ago)
```

```
Last time status changed: 01/05/2013 14:11:33 (09:35:50 ago)
```

```
Statistics:
```

```
packets: received 186, sent 38545
```

```
bytes: received 12644, sent 2620952
```

3.2.3 유형 4 및 유형 5 PW

두 가지 유형의 PW를 사용할 수 있습니다(유형 4 및 유형 5).

- 타입 4 PW를 VLAN 기반 PW라고 합니다. 인그레스 PE는 PW를 통해 전송할 수신 VLAN 태그를 제거해서는 안 됩니다.

ASR 9000과 같은 EVC 기반 플랫폼에서는 들어오는 AC에 들어오는 VLAN 태그를 팝업하는 **rewrite 명령**이 있을 수 있으므로 PW를 통해 전송할 VLAN 태그가 없을 수 있습니다. 이러한 가능성을 해결하기 위해 EVC 플랫폼은 유형 4 PW용 프레임 위에 더미 VLAN 태그 0을 삽입합니다. Type 4 PW는 **transport-mode vlan 명령**으로 구성됩니다. 원격 PE는 EVC 기반이어야 하며

최상위 VLAN 태그가 제거할 더미 태그임을 이해해야 합니다.

그러나 EVC 플랫폼과 비 EVC 플랫폼 간에 유형 4 PW를 사용하는 경우 상호 운용성 문제가 발생할 수 있습니다. 비 EVC 플랫폼은 상위 VLAN 태그를 더미 VLAN 태그로 간주하지 않고 더미 VLAN 태그 0이 포함된 프레임의 외부 태그로 전달합니다. EVC 플랫폼에는 rewrite 명령으로 수신 프레임에 수신된 VLAN 태그를 조작할 수 있는 기능이 있습니다. 해당 VLAN 조작의 결과는 Type 4 PW를 통해 전송되며 그 위에 여분의 더미 태그 0이 있습니다.

최근 Cisco IOS XR 소프트웨어 릴리스에서는 **transport-mode vlan passthrough** 명령으로 더미 태그 0을 사용하지 않고 유형 4 PW를 사용할 수 있는 기능을 제공합니다. EFP(Ethernet Flow Point)에서 VLAN 태그를 조작하려면 적어도 하나의 태그가 남아 있어야 합니다. 이는 유형 4 PW에서 전송되는 VLAN 태그가 있어야 하며 이 경우 해당 요구 사항을 충족하는 더미 태그가 없기 때문입니다. 수신 인터페이스 태그 재작성 후 프레임에 남아 있는 태그는 PW를 통해 투명하게 전송됩니다.

- 타입 5 PW는 이더넷 포트 기반 PW라고 합니다. 인그레스 PE는 메인 인터페이스에서 수신된 프레임 또는 서브 인터페이스에서 패킷이 수신될 때 서브 인터페이스 태그가 제거된 후 프레임을 전송한다. 타입 5 PW를 통해 태그가 지정된 프레임을 전송할 필요는 없으며, EVC 기반 플랫폼에 의해 더미 태그가 추가되지 않습니다. EVC 기반 플랫폼에는 rewrite 명령으로 수신 프레임에 수신된 VLAN 태그를 조작할 수 있는 기능이 있습니다. 이러한 VLAN 조작의 결과는 태그가 지정되었거나 지정되지 않은 유형 5 PW를 통해 전송됩니다.

기본적으로 L2VPN PE는 다음 예에서 볼 수 있는 것처럼 유형 5 PW를 협상하려고 합니다.

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"  
PW type Ethernet, control word disabled, interworking none  
PW type Ethernet Ethernet
```

PW type Ethernet은 type 5 PW를 나타낸다.

이는 PW를 통해 라우터1에서 보내고 라우터2에서 라우터3에 캡슐화한 ARP 요청의 스니퍼 캡처입니다.

```
Frame 38: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)  
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50  
(00:24:f7:1e:93:50)  
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251  
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast  
(ff:ff:ff:ff:ff:ff)  
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2  
Address Resolution Protocol (request)
```

MPLS 레이블 16031은 라우터3에서 광고하는 PW 레이블입니다. Penultimate 홉과 router3 사이에서 스니퍼 캡처를 가져왔으므로 IGP 레이블이 없습니다.

PW 레이블 바로 다음에 캡슐화된 이더넷 프레임이 시작됩니다. PW 제어 단어가 있을 수 있지만 이 예에서는 구성되지 않습니다.

Type 5 PW인 경우에도 라우터2가 AC에서 수신한 수신 VLAN 태그 2는 AC에서 팝업하는 재작성 명령이 없으므로 전송됩니다. EVC 기반 플랫폼에는 자동 태그가 팝업되지 않으므로 재작성 처리 후 AC에서 발생하는 결과가 전송됩니다. 유형이 5 PW인 더미 VLAN 태그 0은 없습니다.

rewrite ingress tag pop 1 symmetric 명령으로 구성한 경우 PW를 통해 전송되는 VLAN 태그가 없습

니다.

다음은 router2 및 router3에서 pw-class를 구성한 유형 4 PW의 예입니다.

참고: 한쪽에서만 유형 4를 구성하면 PW가 계속 작동 중지되고 '오류: PW 유형 불일치'로 보고됩니다.

```
l2vpn
pw-class VLAN
encapsulation mpls
transport-mode vlan
!
!
xconnect group test
p2p p2p4
neighbor 10.0.0.11 pw-id 222
pw-class VLAN
!
!
!
!
```

PW type Ethernet VLAN은 type 4 PW를 나타낸다.

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
```

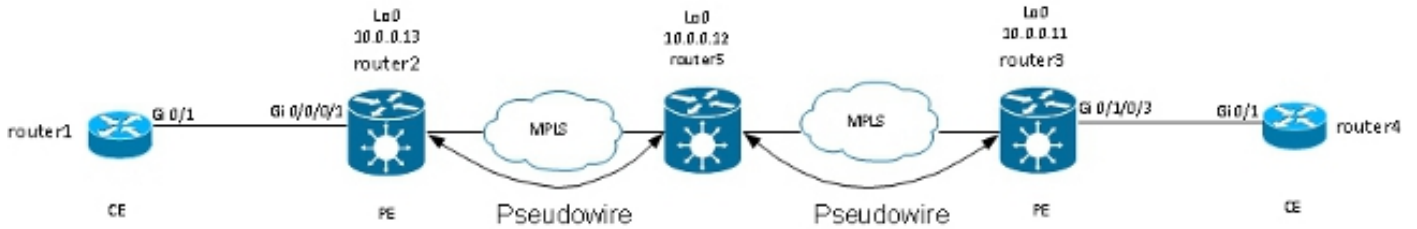
이제 전송되는 프레임 위에 더미 태그 0이 삽입되었습니다.

```
Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50
(00:24:f7:1e:93:50)
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 0
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
Address Resolution Protocol (request)
```

이그레스 EVC 기반 PE는 더미 태그를 제거하고 로컬 AC에 태그 2가 있는 프레임을 포워딩한다. 이그레스 PE는 PW에 수신된 프레임에서 AC에 구성된 로컬 태그 조작을 적용합니다. 로컬 AC가 인그레스 태그 POP 1 대칭으로 재작성되도록 구성된 경우, 구성된 태그는 이그레스 방향으로 푸시되어야 하므로 새 태그가 PW에서 수신된 태그 2의 위에 푸시됩니다. rewrite 명령은 매우 유연하지만 PW의 각 측면에서 달성하고자 하는 내용을 신중하게 평가해야 합니다.

3.2.4 멀티세그먼트 PW

물리적 인터페이스 대신 PW가 있는 L2VPN PE를 AC로 사용할 수 있습니다.



Router5는 PW의 패킷을 router2에서 수신하고 다른 PW의 패킷을 router3으로 전환합니다. 따라서 router5는 router2와 router3 간에 다중 세그먼트 PW를 생성하기 위해 PW 사이를 전환합니다.

이제 router2의 컨피그레이션이 라우터5를 원격 PE로 가리킵니다.

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.12 pw-id 222
!
```

라우터 5의 컨피그레이션은 기본입니다.

```
RP/0/RSP0/CPU0:router5#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
neighbor 10.0.0.11 pw-id 223
!
neighbor 10.0.0.13 pw-id 222
!
description R2-R5-R3
!
```

description 명령은 선택 사항이며, router5가 각 원격 PE(router2 및 router3)로 전송하는 PW TLV(Switching Type Length Value)에 삽입됩니다. 이 설명은 중간에 PW 스위칭을 수행하는 라우터가 있을 때 PW 문제를 해결해야 할 때 유용합니다.

PW 스위칭 TLV를 검토하려면 sh l2vpn xconnect 명령을 입력합니다.

```
RP/0/RSP0/CPU0:router5#sh l2vpn xconnect group test det

Group test, XC p2p5, state is down; Interworking none
Description: R2-R5-R3
PW: neighbor 10.0.0.11, PW ID 223, state is down ( provisioned )
PW class not set, XC ID 0xc0000002
Encapsulation MPLS, protocol LDP
Source address 10.0.0.12
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
```

Label 16042 unknown
Group ID 0x4000280 0x0
Interface GigabitEthernet0/0/0/1.2 unknown
MTU 1504 unknown
Control word disabled unknown
PW type Ethernet unknown
VCCV CV type 0x2 0x0
(none)
(LSP ping verification)
VCCV CC type 0x4 0x0
(none)
(TTL expiry)

Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.13, PW ID: 222

Description: R1-R5-R3

Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 3221225474
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:30 (00:00:06 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)
PW: neighbor 10.0.0.13, PW ID 222, state is up (established)
PW class not set, XC ID 0xc0000001
Encapsulation MPLS, protocol LDP
Source address 10.0.0.12
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16043 16056
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x4 0x6
(router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.11, PW ID: 223

Description: R2-R5-R3

Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 0
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:35 (00:00:01 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)

라우터5는 PW 스위칭 TLV를 라우터3로 보내고 PW에 대한 세부 정보를 라우터2로 보내고 PW 스위칭 TLV를 라우터3으로 보냅니다.

3.2.5 이중화

두 사이트를 연결하는 데 포인트-투-포인트 PW를 사용할 수 있지만 PE 또는 AC 장애 시 이 두 사이트는 연결된 상태로 유지되어야 합니다.

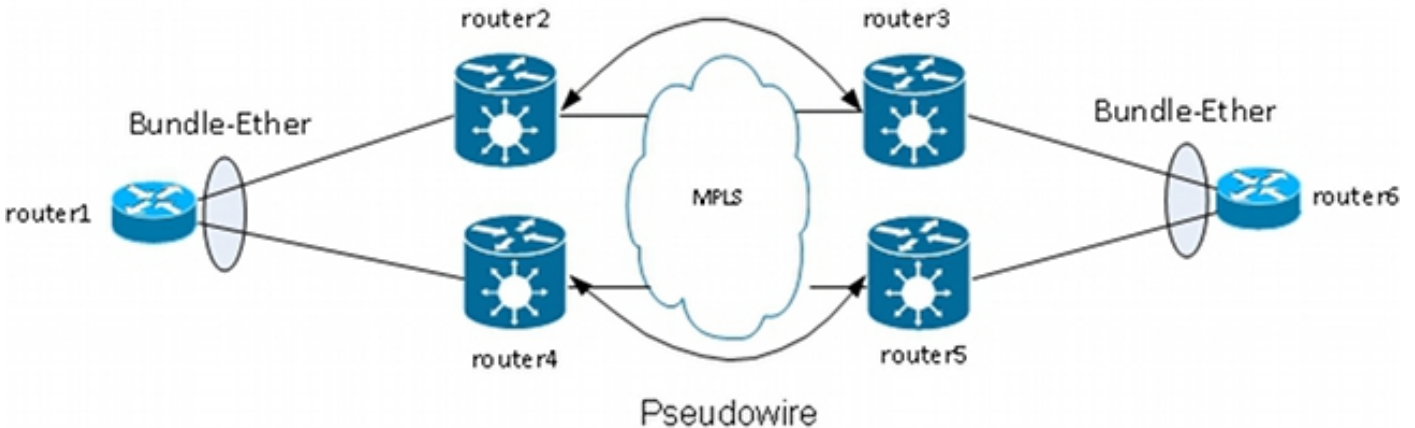
3.2.5.1 코어 리던던시

MPLS 코어의 리라우팅에 영향을 주는 토폴로지 변경을 수행하면 MPLS PW가 새 경로를 즉시 상속합니다.

3.2.5.2 Bundle Over PWs

CE(Customer Edge) 디바이스와 PE 간에 번들 멤버 링크 장애가 있는 경우 링크 이중화를 제공하기 위해 CE 디바이스는 이더넷 번들을 통해 PE에 연결될 수 있습니다. 하나의 번들 링크 멤버가 다운되더라도 번들은 계속 업됩니다. PE 장애가 전체 번들을 다운시키기 때문에 PE 이중화를 제공하지 않습니다.

리던던시를 위한 하나의 방법은, 포인트-투-포인트(point-to-point) PW들에 의해 전송되는 다수의 회로들을 갖는 것이다. 각 회로는 두 CE 간의 이더넷 번들에 속합니다.



PE는 번들을 종료하지 않고 대신 CE가 서로 교환하는 LACP(Link Aggregation Control Protocol) 프레임에 포함하여 PW를 통해 투명하게 프레임을 전송합니다.

이 설계에서는 AC 또는 PE가 손실되면 번들 멤버가 다운되지만 번들은 계속 업됩니다.

참고: LACP BPDU는 Cisco IOS XR 소프트웨어 릴리스 4.2.1 이전 릴리스에서 ASR 9000에 의해 L2VPN을 통해 전송되지 않았습니다.

CE는 여전히 이 설계에서 단일 장애 지점입니다. CE에서 사용할 수 있는 기타 이중화 기능은 다음과 같습니다.

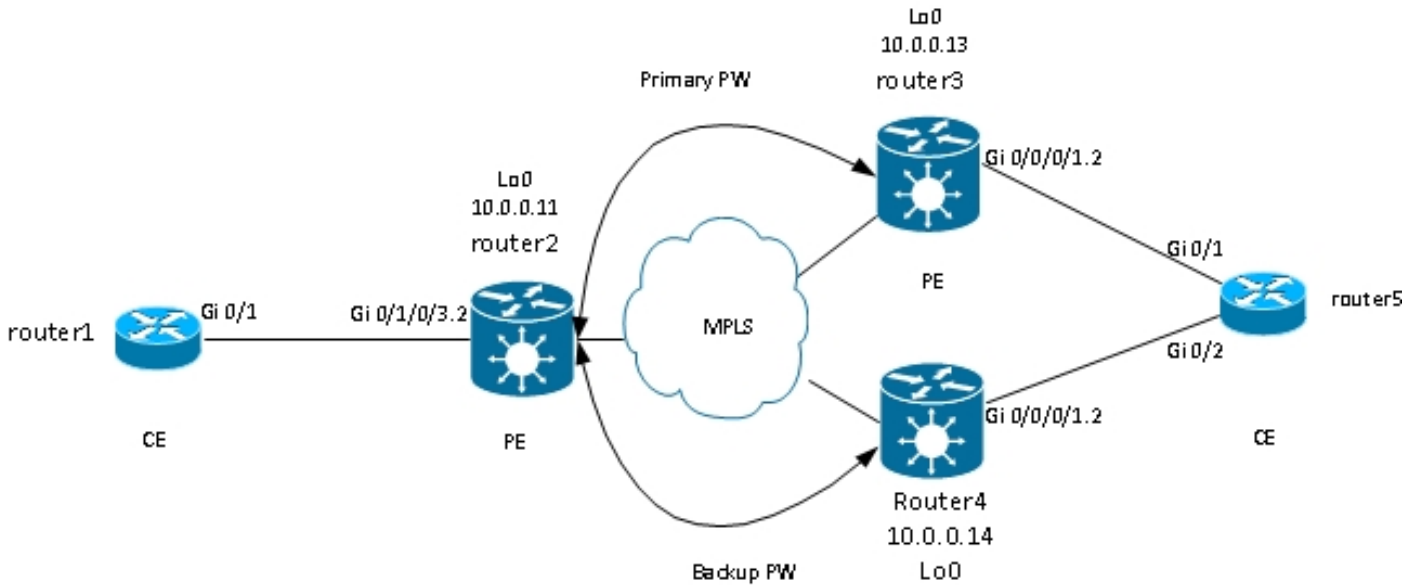
- MC-LAG(Multichassis Link Aggregation Group)

- ASR 9000 nV(Network Virtualization) 클러스터링
- Cisco IOS 스위치의 VSS(Virtual Switching System)
- Cisco Nexus 스위치의 vPC(Virtual Port Channel)

PE의 관점에서 보면 AC와 MPLS PW 사이에 간단한 포인트-투-포인트 연결이 있습니다.

3.2.5.3PW 이중화

PE는 또한 PW Redundancy라는 기능으로 이중화를 제공할 수 있습니다.



Router2에는 router3에 대한 기본 PW가 있습니다. 라우터1에서 라우터6로의 트래픽은 정상적인 상황에서 기본 PW를 통해 이동합니다. 또한 라우터2는 핫 스탠바이 상태에서 라우터4에 대한 백업 PW를 가지고 있지만, 정상적인 상황에서는 해당 PW를 지나는 트래픽이 발생하지 않습니다.

기본 PW, 기본 PW의 원격 PE(router3) 또는 원격 PE의 AC(router3)에 문제가 있는 경우 router2는 백업 PW를 즉시 활성화하고 트래픽이 백업 PW를 통과하기 시작합니다. 문제가 해결되면 트래픽이 기본 PW로 다시 이동합니다.

router2의 컨피그레이션은 다음과 같습니다.

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p6
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
backup neighbor 10.0.0.14 pw-id 222
!
```

router3 및 router4의 표준 컨피그레이션은 다음과 같습니다.

```
RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
```

```
xconnect group test
p2p p2p6
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 222
!
!
!
!
```

안정적인 조건에서 PW-to-router3은 활성 상태이고 PW-to-router4는 대기 상태입니다.

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
-----
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 UP
Backup
10.0.0.14 222 SB
-----
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det
```

```
Group test, XC p2p6, state is up; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 51412, sent 25628
bytes: received 3729012, sent 1742974
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```
PW Status TLV in use
MPLS Local Remote
```

```
-----
Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
```

```
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
```

MAC withdraw message: send 0 receive 0
Statistics:
packets: received 25628, sent 51412
bytes: received 1742974, sent 3729012

Backup PW:
PW: neighbor 10.0.0.14, PW ID 222, state is standby (all ready)
Backup for neighbor 10.0.0.13 PW ID 222 (inactive)
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16050 289971
Group ID 0x6000180 0x4000100
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x20 (Standby) in Notification message
MIB cpwVcIndex: 3221225478
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
MAC withdraw message: send 0 receive 0
RP/0/RSP0/CPU0:router2#

AC 상태와 PW 상태가 연결되므로, router3의 AC가 중단될 때 router3은 'AC down'을 router2에 알립니다. Router2는 기본 PW를 종료하고 백업 PW를 활성화합니다.

RP/0/RSP0/CPU0:May 3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.13, id 222, state is Down
RP/0/RSP0/CPU0:May 3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.14, id 222, state is Up

RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST

test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP

RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p6, state is up; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1

VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 51735, sent 25632
bytes: received 3752406, sent 1743230
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down (local ready)
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x6 (**AC Down**) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0

Backup PW:
PW: neighbor 10.0.0.14, PW ID 222, state is up (established)
Backup for neighbor 10.0.0.13 PW ID 222 (active)
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16050 289971
Group ID 0x6000180 0x4000100
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message

```

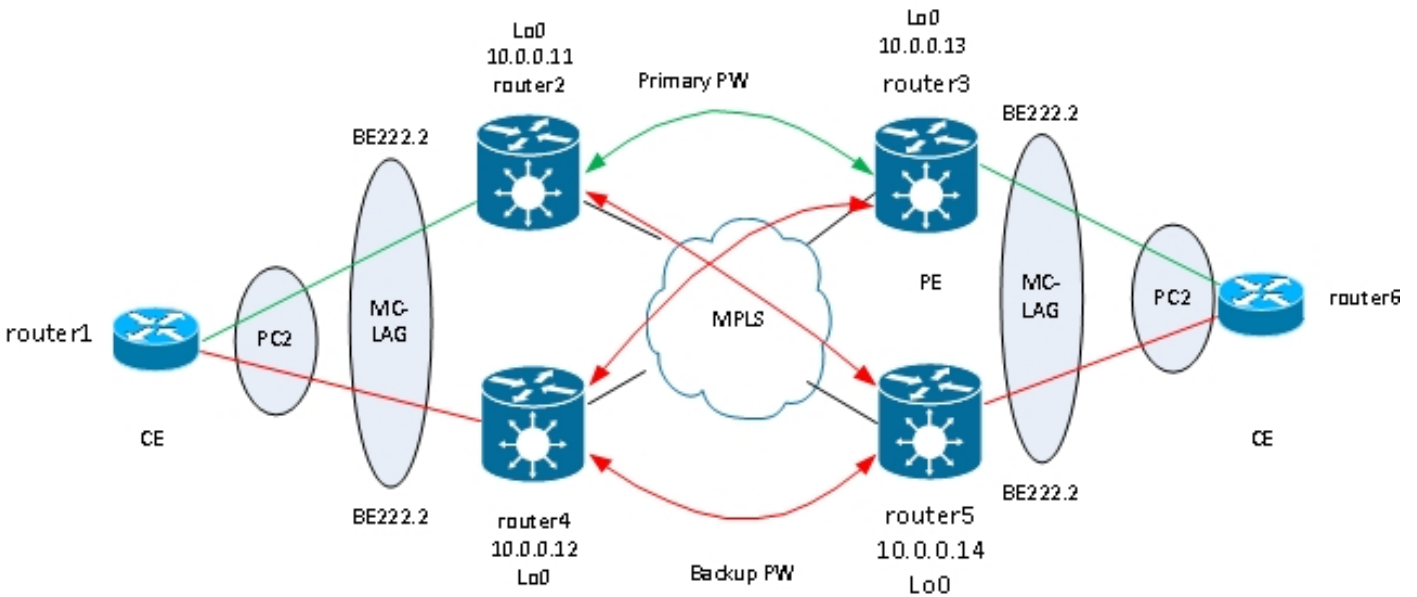
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225478
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0
Statistics:
packets: received 25632, sent 51735
bytes: received 1743230, sent 3752406
RP/0/RSP0/CPU0:router2#

```

라우터 3의 AC가 다시 작동하면 router2는 기본 PW를 라우터 3으로 재활성화하고 라우터 4의 PW는 대기 상태로 돌아갑니다.

또한 백업 PW는 라우터3이 다운되고 라우터2가 루프백에 대한 경로를 잃을 때 활성화됩니다.

다음 논리적 단계는 각 사이트에 2개의 PE로 양방향 PW 이중화를 도입하는 것입니다.



그러나 PW의 이 풀 메시(full mesh)는 두 개의 PW가 동시에 활성화되어 있을 때 네트워크에 루프가 유입될 때 문제가 발생합니다. 일반적으로 STP(Spanning Tree Protocol)를 사용하여 루프를 끊어야 합니다. 그러나 한 사이트의 스페닝 트리 불안정성이 다른 사이트로 전파되는 것은 원하지 않습니다. 따라서 이러한 PW에서 스페닝 트리를 실행하지 않고 두 사이트 간에 스페닝 트리를 병합하지 않는 것이 좋습니다. 두 사이트 사이에 하나의 논리적 링크만 있으면 스페닝 트리가 필요하지 않으므로 더 간단합니다.

한 가지 해결 방법은 한 사이트의 두 PE와 해당 로컬 CE 간에 MC-LAG 번들을 사용하는 것입니다. 두 PE 중 하나에만 해당 번들 멤버가 활성 상태이므로 원격 사이트에 대한 PW가 활성 상태입니다. 다른 PE는 스탠바이 상태에 있는 번들 멤버를 가지고 있으며 원격 사이트에 대한 PW를 가지고 있습니다. 두 사이트 사이에 하나의 PW만 활성화되어 있으면 루프가 도입되지 않습니다. 활성 PW가 있는 PE는 원격 사이트의 두 번째 PE에 대한 대기 PW도 갖습니다.

안정적인 상태에서 활성 번들 멤버는 router2와 router3에 있으며, 활성 PW는 그 사이에 있습니다. 라우터3의 컨피그레이션입니다.

```

RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2

```

```
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
```

```
RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!
```

```
RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
backup neighbor 10.0.0.12 pw-id 222
!
!
!
!
!
```

```
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
-----
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
-----
```

```
RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
```



```
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured
```

```
Port Device State Port ID B/W, kbps
```

```
-----
Gi0/0/0/1 Local Active 0x8001, 0x9001 1000000
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8002, 0xa002 1000000
Link is marked as Standby by mLACP peer
```

router5에서 로컬 번들 멤버와 기본 PW-to-router2는 대기 상태이며, 백업 PW-to-router4는 작동 중
지됩니다.

```
RP/0/RSP1/CPU0:router5#sh run redundancy
redundancy
iccp
group 2
mlacp node 2
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.13
!
backbone
interface TenGigE0/1/0/0
interface TenGigE0/1/0/1
!
isolation recovery-delay 300
!
!
!
```

```
RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!
```

```
RP/0/RSP1/CPU0:router5#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
backup neighbor 10.0.0.12 pw-id 222
!
```

!
!
!
!

```
RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
-----
test p2p7 DN BE222.2 UP 10.0.0.11 222 SB
Backup
10.0.0.12 222 DN
-----
```

```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222
```

```
Bundle-Ether222
Status: mLACP hot standby
Local links : 0 / 1 / 1
Local bandwidth : 0 (0) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Standby
Foreign links : 1 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured
```

```
Port Device State Port ID B/W, kbps
-----
Gi0/0/0/1 Local Standby 0x8002, 0xa002 1000000
mLACP peer is active
Gi0/0/0/1 10.0.0.13 Active 0x8001, 0x9001 1000000
Link is Active
```

router6에서 router3에 대한 번들 멤버는 활성 상태이고 router5에 대한 번들 멤버는 대기 상태입니다.

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
```

```
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
```

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports

-----+-----+-----+-----
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)

router3의 번들 멤버가 다운되면 router6에 router5에 대한 활성 멤버가 있습니다.

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
```

```
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
```

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports

-----+-----+-----+-----
2 Po2(SU) LACP Gi0/1(D) Gi0/2(P)

bundle-ether222가 router5에서 다운되었으므로 라우터2에 연결된 PW가 동시에 다운됩니다.

```
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
```

```
-----
test p2p7 DN BE222.2 DN 10.0.0.11 222 DN
Backup
10.0.0.12 222 DN
-----
```

Router2는 라우터3에 대한 PW가 다운되었음을 감지하고 라우터5에 대한 백업 PW를 활성화합니다.

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
```

```
-----
test p2p7 UP BE222.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
-----
```

Router5에는 번들 멤버가 활성 상태이고 기본 PW가 Router2에 연결되어 있습니다.

```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222
```

```

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

```

```

Port Device State Port ID B/W, kbps
-----
Gi0/0/0/1 Local Active 0x8002, 0xa002 1000000
Link is Active
Gi0/0/0/1 10.0.0.13 Configured 0x8003, 0x9001 1000000
Link is down
RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

```

```

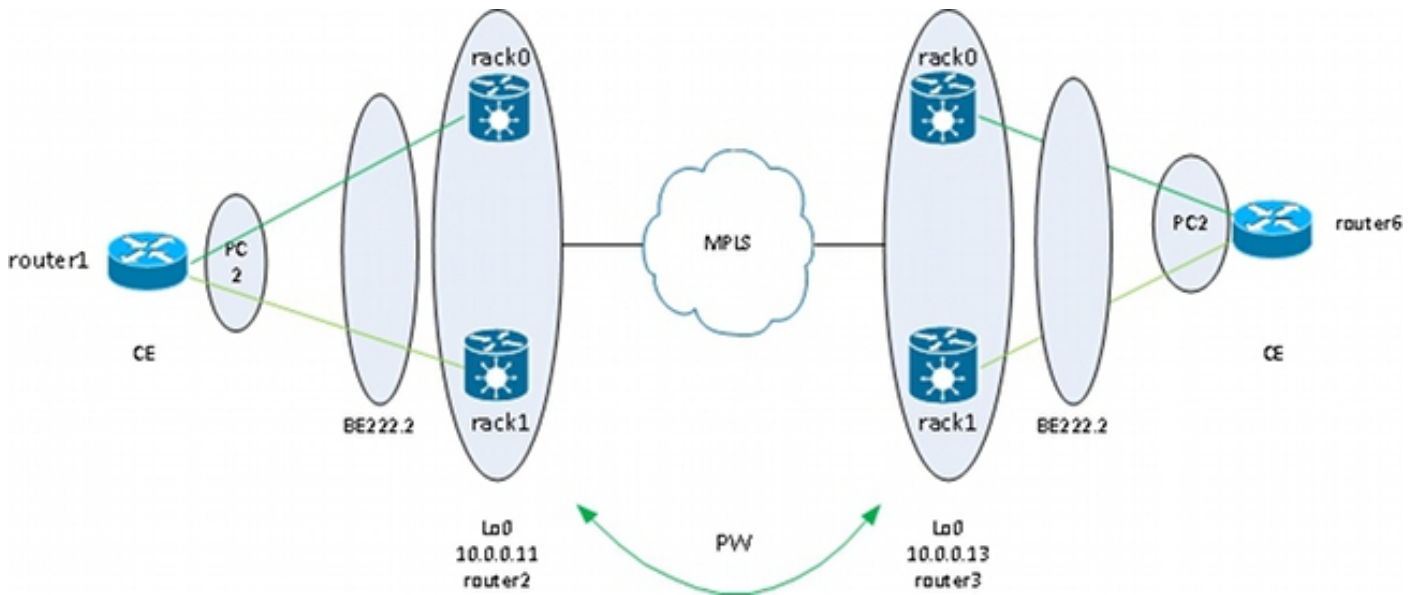
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
-----
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
-----

```

3.2.5.4 ASR 9000 nV 에지 클러스터

MC-LAG 및 PW 이중화를 기반으로 한 [이전 설계는 이중화](#)에 적합하지만, 일부 번들 멤버가 대기 상태이므로 안정된 조건에서 트래픽을 전달하지 않습니다.

모든 번들 멤버를 활성화하려는 경우, 안정적인 조건에서도 PE의 각 랙에 연결된 CE의 번들 멤버와 함께 ASR 9000 클러스터를 사용할 수 있습니다.



이 설계에서는 클러스터가 MPLS 코어에 이중으로 연결되어 있고 코어에 이중화가 있는 한 CE와 PE 간의 번들 멤버 링크 오류, 랙 오류 및 코어 링크 오류에 대해 이중화를 제공합니다. 두 랙은 같은 장소에 배치할 필요가 없으며 서로 다른 위치에 배치될 수 있습니다. 랙 간 링크는 이 다이어그램에 표시되지 않습니다.

CE에 이중화를 구현하려는 경우 CE에 대해 멀티 샴시 솔루션을 사용할 수 있습니다.

- MC랙
- ASR 9000 nV 클러스터링
- VSS
- vPC

ASR 9000 클러스터의 구성은 매우 기초적입니다.

```
interface TenGigE0/0/0/8
bundle id 222 mode on
!
interface TenGigE1/0/0/8
bundle id 222 mode on
!
interface Bundle-Ether222
!
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface Bundle-Ether222.2
neighbor 10.0.0.13 pw-id 8
!
!
!
!
```

지정된 셸프 컨트롤러 전환으로 인한 MAC 주소 변경을 방지하기 위해 고정 LACP 시스템 MAC 주소 및 번들 MAC 주소를 구성하는 것이 좋습니다. 다음 예에서는 주소를 찾는 방법을 보여 줍니다.

```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
```

```

Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address 0024.f71e.d309
RP/1/RSP0/CPU0:router2(config-if)#commit
RP/1/RSP0/CPU0:router2(config-if)#end
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#sh l2vpn system-id

```

```

Priority MAC Address
-----
0x8000 00-24-f7-1e-d3-05
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#l2vpn system mac 0024.f71e.d305
RP/1/RSP0/CPU0:router2(config)#commit
RP/1/RSP0/CPU0:router2(config)#end

```

요약하면, 이는 각 랙에 멤버가 포함된 번들-에테르 222(랙 0의 경우 0/0/8, 랙 1의 경우 1/0/0/8)이며 포인트-투-포인트 교차 연결을 위해 구성된 번들 하위 인터페이스입니다.

```

RP/1/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

```

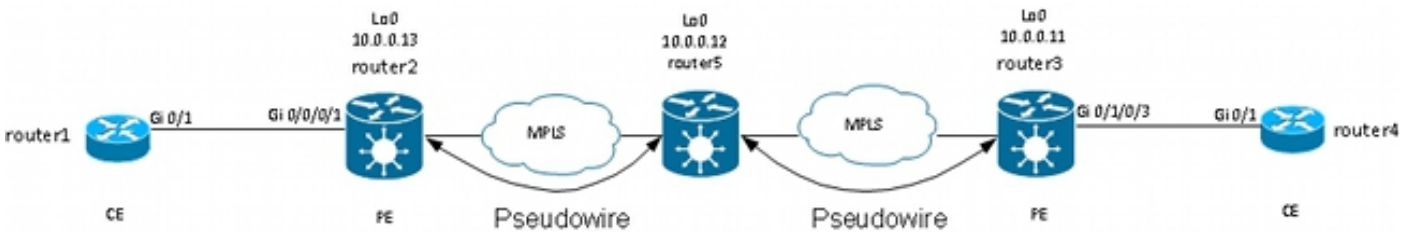
```

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
-----
test p2p8 UP BE222.2 UP 10.0.0.13 8 UP
-----

```

3.3 CDP

Cisco 라우터 및 스위치는 일반적으로 dot1q 태그 없이 CDP 패킷을 전송합니다. 교차 연결용으로 구성된 IOS XR 라우터에서 이러한 CDP 패킷을 수신할 때 어떤 일이 발생하는지 결정하는 시나리오가 여러 가지가 있습니다.



이 토폴로지에서 router1은 컨피그레이션에 따라 로컬 PE 라우터2를 CDP 인접 디바이스 또는 원격 CE 라우터4로 볼 수 있습니다.

3.3.1 L2VPN PE의 주 인터페이스에서 CDP가 활성화되지 않음

L2VPN CE의 CDP 패킷은 교차 연결을 통해 전송됩니다. 두 L2VPN CE는 주 인터페이스가 l2transport로 구성되거나 태그가 지정되지 않은 CDP 프레임과 일치하는 하위 인터페이스가 있는 경우 `show cdp neighbors` 명령을 사용하여 서로를 확인합니다.

다음은 기본 인터페이스의 예입니다.

```

interface GigabitEthernet0/0/0/1
l2transport
!
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1
neighbor 10.0.0.11 pw-id 8
!
!
!
!

```

다음은 태그가 지정되지 않은 하위 인터페이스의 예입니다.

```

interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 8
!
!
!
!

```

이 두 가지 예에서 CDP 패킷은 교차 연결을 통해 전송되며 CE는 서로를 CDP 네이버로 간주합니다. CE는 PE를 CDP 네이버로 보지 않습니다.

```

router1#sh cdp nei gigabitEthernet 0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
router4 Gig 0/1 168 R S ME-3400G- Gig 0/1

```

3.3.2 L2VPN PE의 주 인터페이스에서 CDP 활성화

PE는 태그가 지정되지 않은 CDP 패킷을 처리하며, PE와 CE는 서로를 네이버로 간주합니다. 그러나 L2VPN PE의 주 인터페이스에서 CDP가 활성화된 경우 CE는 원격 CE를 확인하지 않습니다.

다음 사항에 유의하십시오.

- l2transport로 구성된 기본 인터페이스에서는 CDP를 구성할 수 없습니다.
- PE는 기본 non-l2transport 인터페이스에 CDP가 구성된 경우 CDP 패킷을 인터셉트합니다. 이는 태그 없는 CDP 패킷과 일치하도록 구성된 l2transport 하위 인터페이스가 있는 경우에도 발생합니다(캡슐화 태그 없는 또는 캡슐화 기본 명령 사용). 이 경우 CDP 패킷은 원격 사이트로 전송되지 않습니다.

3.4 스페닝 트리

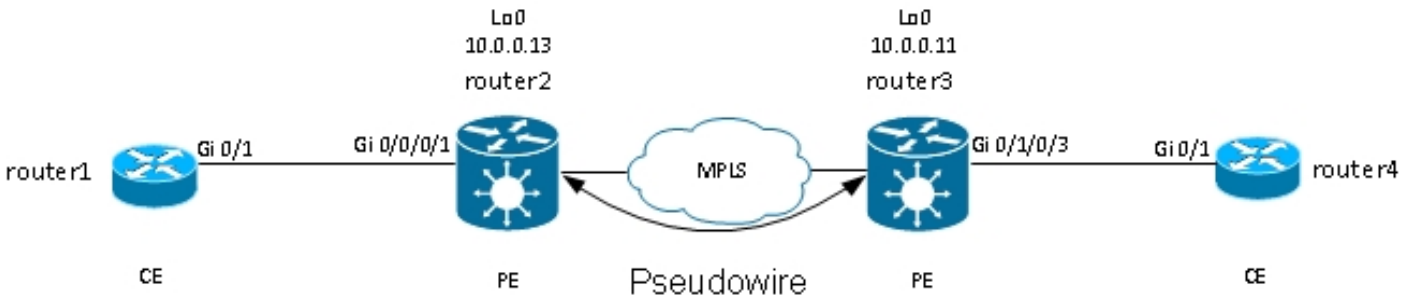
L2VPN CE가 이더넷 스위치이고 스페닝 트리 BPDU를 L2VPN PE로 전송하는 경우, 이러한

BPDU는 일반 트래픽으로 처리되며 L2VPN 컨피그레이션에 따라 전송됩니다.

주 인터페이스가 l2transport로 구성되어 있거나 캡슐화 태그 없음 또는 캡슐화 기본 명령으로 구성된 l2transport 하위 인터페이스가 있는 경우 STP 또는 MST BPDU는 태그 없이 전송되며 포인트-투-포인트 교차 연결을 통해 전송됩니다.

PVST+(Per VLAN Spanning Tree Plus) 또는 PVRST+(Rapid PVST+)는 BPDU의 dot1q 태그와 일치하는 l2transport 하위 인터페이스가 있는 경우 전송되는 태그가 지정된 BPDU를 전송합니다.

다음은 토폴로지의 예입니다.



Router2 및 router3은 dot1q 태그 2가 있는 태그가 지정되지 않은 프레임 및 프레임을 전송합니다.

```
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 8
!
!
p2p p2p9
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 9
!
!
!
```

스위치 1은 VLAN 1의 태그가 지정되지 않은 BPDU를 수신하고 VLAN 2의 태그가 지정된 BPDU를 스위치 4에서 수신합니다. 루트 포트는 Gi0/1에서 스위치 4로 향합니다.

```
switch1#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 8
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```



```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
```

```
Gi0/1 Root FWD 4 128.1 P2p
```

```
switch1#sh spanning-tree vlan 2
```

```
VLAN0002
```

```
Spanning tree enabled protocol ieee
```

```
Root ID Priority 32770
```

```
Address 0019.552b.b580
```

```
Cost 4
```

```
Port 1 (GigabitEthernet0/1)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
```

```
Address 001d.4603.1f00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 15
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
```

```
Gi0/1 Root FWD 4 128.1 P2p
```

이 구성에서는 사이트 A의 스페닝 트리 도메인이 사이트 B의 스페닝 트리 도메인과 병합됩니다. 한 사이트의 스페닝 트리 불안정성이 다른 사이트로 전파될 수 있다는 문제가 발생할 수 있습니다.

한 사이트가 하나의 PW를 통해서만 다른 사이트에 연결되어 있고 물리적 루프를 발생시킬 수 있는 백도어 링크가 없다고 확신하는 경우 두 사이트 위에 스페닝 트리를 실행하지 않는 것이 좋습니다. 이렇게 하면 두 스페닝 트리 도메인이 격리됩니다. 이를 위해 CE에 스페닝 트리 bpdu필터를 구성하거나 PE에 이더넷 서비스 액세스 목록을 구성하여 BPDU에서 사용하는 대상 MAC 주소의 프레임을 삭제합니다. PE의 이더넷 서비스 액세스 목록을 사용하여 BPDU 대상 MAC 또는 PW를 통해 전달하지 않으려는 다른 종류의 L2 프로토콜로 프레임을 삭제할 수 있습니다.

두 사이트 간에 전송 중인 각 l2transport(sub) 인터페이스에서 사용할 수 있는 액세스 목록입니다.

```
ethernet-services access-list block-invalid-frames
```

```
10 deny any 0180.c200.0000 0000.0000.000f
```

```
20 deny any host 0180.c200.0010
```

```
30 deny any host 0100.0c00.0000
```

```
40 deny any host 0100.0ccc.cccc
```

```
50 deny any host 0100.0ccc.cccd
```

```
60 deny any host 0100.0ccd.cdce
```

```
70 permit any any
```

```
!
```

```
RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.1
```

```
interface GigabitEthernet0/0/0/1.1 l2transport
```

```
encapsulation untagged
```

```
ethernet-services access-group block-invalid-frames ingress
```

```
ethernet-services access-group block-invalid-frames egress
```

```
!
```

```
RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.2
```

```
interface GigabitEthernet0/0/0/1.2 l2transport
```

```
encapsulation dot1q 2
```

```
rewrite ingress tag pop 1 symmetric
ethernet-services access-group block-invalid-frames ingress
ethernet-services access-group block-invalid-frames egress
!
```

이더넷 서비스 ACL에서 BPDU를 삭제하기 시작합니다.

```
RP/0/RSP1/CPU0:router2#sh access-lists ethernet-services block-invalid-frames
hardware ingress location 0/0/CPU0
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f (41 hw matches)
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
50 deny any host 0100.0ccc.cccd (63 hw matches)
60 deny any host 0100.0ccd.cdce
70 permit any any (8 hw matches)
```

Switch1은 더 이상 switch4에서 BPDU를 수신하지 않으므로 이제 switch1이 루트가 됩니다.

```
switch1#sh spanning-tree vlan 1
```

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Desg FWD 4 128.1 P2p
```

```
switch1#sh spanning-tree vlan 2
```

```
VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32770
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Desg FWD 4 128.1 P2p
```

링크에서 스페닝 트리를 비활성화할 경우 사이트 간에 백도어 연결이 생성되면 물리적 루프가 발생하고 스페닝 트리가 루프를 끊을 수 없다는 위험이 있습니다. 따라서 PW에서 스페닝 트리를 비활성화할 때는 사이트 간에 이중 링크가 없고 PW가 사이트 간의 유일한 연결로 유지되어야 합니다.

사이트 간에 여러 연결이 있는 경우 MSTAG(MST Access Gateway) 또는 PVSTAG(PVST+ Access Gateway) 같은 스페닝 트리의 액세스 게이트웨이 버전과 함께 VPLS와 같은 솔루션을 사용합니다.

자세한 내용은 Multipoint [Service](#)에 대한 섹션을 참조하십시오.

4. 다중 지점 서비스

참고:

이 섹션에 사용된 명령에 대한 자세한 내용을 가져오려면 [명령 조회 툴\(등록 고객 전용\)](#)을 사용하십시오.

[아웃풋 인터프리터 툴\(등록 고객 전용\)](#)은 특정 `show` 명령을 지원합니다. `show` 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

멀티포인트 L2 [기능](#)에 대한 자세한 설명은 Implementing Multipoint Layer 2 Services를 참조하십시오.

L2VPN 스위치는 두 개의 인터페이스만 지점 간 교차 연결로 제공하므로, 측면에서 수신한 모든 내용을 L2VPN 스위치에서 받아 반대쪽으로 전달합니다.

브리지 도메인에 두 개 이상의 인터페이스가 있는 경우 이더넷 스위치는 대상 MAC 주소를 기반으로 프레임을 전달할 위치를 결정하기 위해 스위칭 결정을 내려야 합니다. 스위치는 수신한 프레임의 소스 MAC 주소를 기반으로 MAC 학습을 수행하고 `mac-address-table`을 작성합니다.

스위치는 다음과 같은 방법으로 프레임을 전달합니다.

- 브로드캐스트 프레임이 모든 포트에 플러딩됩니다. 브로드캐스트 플러딩 비율을 제한하려면 `storm control`을 사용합니다.
- 멀티캐스트 프레임은 IGMP(Internet Group Management Protocol) 또는 MLD(Multicast Listener Discovery) 스누핑이 구성된 경우를 제외하고 브리지 도메인의 모든 포트에 플러딩됩니다. 멀티캐스트 플러딩 속도를 제한하려면 `storm control`을 사용합니다.
- 브리지 도메인의 `mac-address-table`(알 수 없는 유니캐스트)에 속하지 않는 대상 MAC 주소의 유니캐스트 프레임은 브리지 도메인의 모든 포트에서 플러딩됩니다. 알 수 없는 유니캐스트 플러딩 속도를 제한하려면 `storm control`을 사용합니다.
- 브리지 도메인의 `mac-address-table`에 속하는 대상 MAC 주소의 유니캐스트 프레임은 대상 MAC 주소가 학습된 포트에 전달됩니다.

Cisco IOS XR 소프트웨어에서 브로드캐스트 도메인 또는 에뮬레이트된 LAN을 브리지 도메인이라고 합니다. 이는 IOS의 VLAN이 트렁크에서 dot1q 태그로 사용되는 VLAN 번호에 링크된다는 점을 제외하면 Cisco IOS 소프트웨어 용어의 VLAN과 유사합니다. Cisco IOS XR 소프트웨어의 브리지 도메인은 dot1q VLAN 태그 번호에 연결되지 않습니다. EVC 모델을 사용하여 dot1q 태그를 조작하고 동일한 브리지 도메인에 서로 다른 dot1q VLAN 번호가 있는 dot1q 하위 인터페이스를 포함하거나 태그가 지정되지 않은 인터페이스를 포함할 수 있습니다.

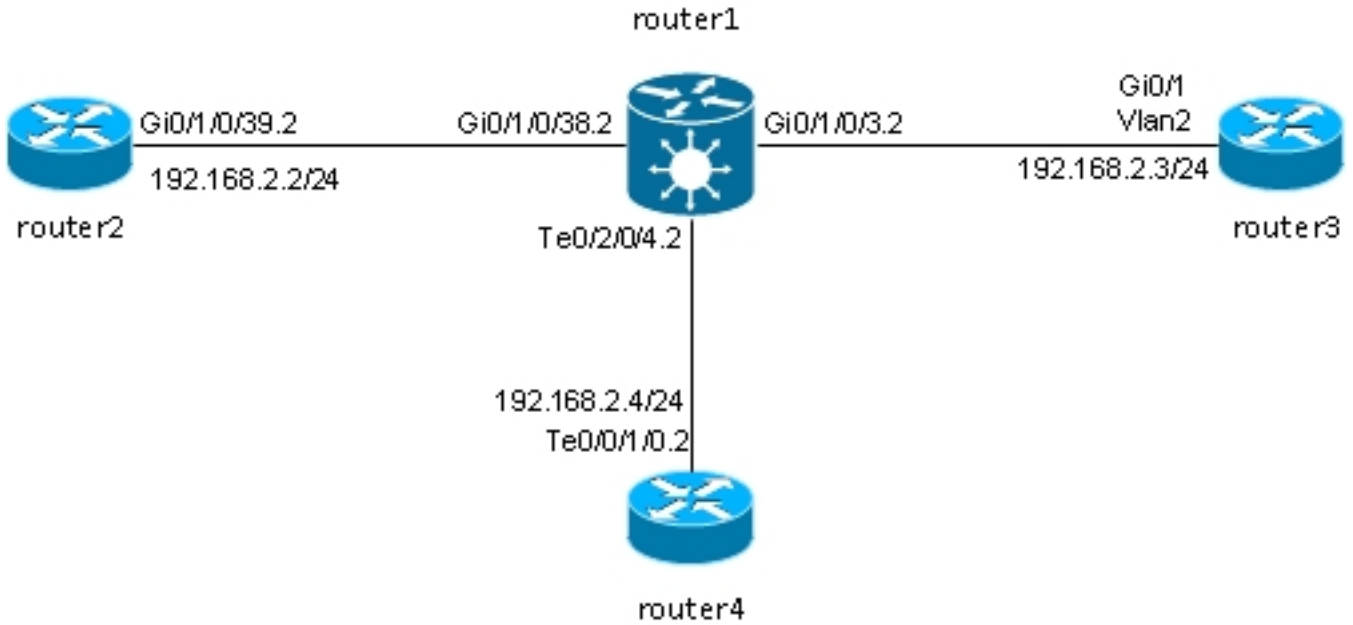
브리지 도메인은 기본적으로 브로드캐스트 및 멀티캐스트 프레임이 플러딩되는 하나의 브로드캐스트 도메인입니다. 각 브리지 도메인에 하나의 `mac-address-table`이 연결됩니다(매우 드물지만 컨피그레이션에 의해 MAC 학습이 수동으로 비활성화되지 않는 한). 이는 일반적으로 브리지 도메인의 모든 호스트가 직접 연결되는 하나의 IPv4 또는 IPv6 서브넷에 해당합니다.

브리지 도메인은 브리지 그룹 내에서 그룹화할 수 있습니다. 이렇게 하면 컨피그레이션을 쉽게 확인할 수 있습니다. 각 브리지 도메인에 대해 하나의 `show` 명령 대신 브리지 그룹에 대해 하나의 `show` 명령을 실행할 수 있습니다. 브리지 그룹에는 `mac-address-table` 또는 기타 연결이 없습니다.

컨피그레이션 및 show 명령에만 사용됩니다.

4.1 로컬 스위칭

이는 매우 기본적인 예입니다.



라우터2, 라우터3 및 라우터4는 ASR 9000을 통해 연결되며, 이 ASR 9000은 이 세 라우터 간의 LAN을 시뮬레이션합니다.

이 세 라우터의 인터페이스 컨피그레이션은 다음과 같습니다.

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/39.2
interface GigabitEthernet0/1/0/39.2
ipv4 address 192.168.2.2 255.255.255.0
encapsulation dot1q 2
!
```

```
router3#sh run int gig 0/1
Building configuration...

Current configuration : 203 bytes
!
interface GigabitEthernet0/1
port-type nni
switchport access vlan 2
switchport trunk allowed vlan 1,2
switchport mode trunk
end
```

```
router3#sh run int vlan 2
Building configuration...

Current configuration : 61 bytes
!
interface Vlan2
ip address 192.168.2.3 255.255.255.0
end
```

```
router3#
```

```
RP/0/RSP0/CPU0:router4#sh run int ten 0/0/1/0.2
interface TenGigE0/0/1/0.2
ipv4 address 192.168.2.4 255.255.255.0
encapsulation dot1q 2
```

!
패킷은 dot1q 태그 2가 있는 router1에서 수신되며 dot1q 태그 2가 있는 다른 라우터로 전달됩니다.

이 기본 시나리오에서는 AC에 두 가지 옵션이 있습니다.

1. 모든 AC에서 dot1q 태그 2를 사용하므로 프레임에 유지하고 이그레스 인터페이스에서 받은 것과 동일한 dot1q 태그를 사용하여 이그레스 인터페이스의 프레임을 전달할 수 있습니다. **rewrite ingress tag pop 1 symmetric** 명령은 필요하지 않습니다.
2. 수신 dot1q 태그 2를 인그레스 방향으로 팝업하고 dot1q 태그 2를 이그레스 방향으로 대칭적으로 푸시할 수 있습니다. 이 기본 시나리오에서는 이러한 과정이 필요하지 않지만, 처음부터 브리지 도메인을 이러한 방식으로 구성하는 것이 좋습니다. 미래에 더 많은 유연성을 제공하기 때문입니다. 다음은 초기 컨피그레이션 이후에 발생할 수 있는 두 가지 변경 예입니다.
 - 라우티드 BVI 인터페이스가 나중에 브리지 도메인에 추가된 경우 패킷이 태그 없이 BVI에서 처리되어야 합니다. 자세한 내용은 섹션을 참조하십시오.
 - 다른 dot1q 태그를 사용하는 새 AC가 나중에 추가됩니다. dot1q 태그 2는 인그레스 방향으로 팝업되고 다른 dot1q 태그는 이그레스 방향으로 새 인터페이스에 푸시되며 그 반대의 경우도 마찬가지입니다. [BVI](#)

router1의 각 AC에 dot1q 태그를 팝업합니다.

```
RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/38.2
interface GigabitEthernet0/1/0/38.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP0/CPU0:router1#sh run int TenGigE0/2/0/4.2
interface TenGigE0/2/0/4.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

다음 3가지 AC로 브리지 도메인의 컨피그레이션을 확인합니다.

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain engineering
interface TenGigE0/2/0/4.2
!
interface GigabitEthernet0/1/0/3.2
!
```

```
interface GigabitEthernet0/1/0/38.2
!  
!  
!  
!
```

브리지 도메인은 브리지 그룹 아래에 구성해야 합니다. 이 고객의 다른 브리지 도메인이 필요한 경우 동일한 브리지 그룹인 customer1에서 구성할 수 있습니다. 새 브리지 도메인이 다른 고객에 속하는 경우 새 브리지 그룹을 생성할 수 있습니다. 이 예에서는 고객을 사용하여 브리지 도메인을 그룹화하지만, 브리지 도메인은 임의의 기준으로 그룹화할 수 있습니다.

show run l2vpn bridge group customer1 bridge-domain engineering 명령을 사용하여 bridge-domain의 컨피그레이션을 표시합니다.

모든 브리지 도메인의 컨피그레이션을 보려면 **show run l2vpn bridge group customer1** 명령을 사용합니다.

show l2vpn bridge-domain bd-name engineering 명령 또는 **show l2vpn bridge-domain group customer1** 명령을 사용하여 브리지 도메인에 대한 정보를 표시합니다.

```
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name engineering
```

Legend: pp = Partially Programmed.

Bridge group: customer1, bridge-domain: engineering, id: 5, state: up, ShgId: 0, MSTi: 0

Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog

Filter MAC addresses: 0

ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)

List of ACs:

Gi0/1/0/3.2, state: up, Static MAC addresses: 0

Gi0/1/0/38.2, state: up, Static MAC addresses: 0

Te0/2/0/4.2, state: up, Static MAC addresses: 0

List of Access PWs:

List of VFIs:

```
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name engineering det
```

Legend: pp = Partially Programmed.

Bridge group: customer1, bridge-domain: engineering, id: 5, state: up, ShgId: 0, MSTi: 0

Coupled state: disabled

MAC learning: enabled

MAC withdraw: enabled

MAC withdraw for Access PW: enabled

MAC withdraw sent on bridge port down: disabled

Flooding:

Broadcast & Multicast: enabled

Unknown unicast: enabled

MAC aging time: 300 s, Type: inactivity

MAC limit: 4000, Action: none, Notification: syslog

MAC limit reached: no

MAC port down flush: enabled

MAC Secure: disabled, Logging: disabled

Split Horizon Group: none

Dynamic ARP Inspection: disabled, Logging: disabled

IP Source Guard: disabled, Logging: disabled

DHCPv4 snooping: disabled

IGMP Snooping profile: none

Bridge MTU: 1500

MIB cvplsConfigIndex: 6

Filter MAC addresses:

Create time: 28/05/2013 17:17:03 (00:18:06 ago)

No status change since creation
ACs: 3 (3 up), VFIs: 0, PWS: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 185066, sent 465
bytes: received 13422918, sent 34974
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
AC: GigabitEthernet0/1/0/38.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40005; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 8, sent 12287
bytes: received 770, sent 892418
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
AC: TenGigE0/2/0/4.2, state is up

```

Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1040001; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 463, sent 11839
bytes: received 35110, sent 859028
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:

```

각 AC에서 패킷이 수신 및 전송되는지 확인하려면 **show l2vpn bridge-domain group customer1 bd-name engineering det** 명령을 사용합니다.

mac-address-table을 확인하려면 **show l2vpn forwarding bridge-domain** 명령에 **mac-address** 키워드를 추가합니다.

```

RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

```

```

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A

```

MAC 학습은 브리지 도메인에서 프레임이 수신될 때마다 라인 카드에 의해 하드웨어에서 실행됩니다. 또한 **mac-address-table**의 소프트웨어 캐시가 있지만 이 소프트웨어 테이블은 하드웨어 항목과 일치하도록 지속적으로 업데이트할 수 없습니다. **show** 명령을 최근 코드에 입력하면 소프트웨어 테이블을 하드웨어 테이블과 재동기화하려고 시도합니다. 최대 15초 후에 재동기화가 완료되지 않은 경우(예: 테이블이 큰 경우) 소프트웨어 **mac-address-table**의 현재 상태를 인쇄합니다. 소프트웨어 및 하드웨어 테이블을 수동으로 재동기화하려면 **l2vpn resynchronize forwarding mac-address-table** 명령을 사용합니다.

```

RP/0/RSP0/CPU0:router1#term mon
RP/0/RSP0/CPU0:router1#l2vpn resynchronize forwarding mac-address-table

```



```
location 0/1/CPU0
RP/0/RSP0/CPU0:router1#LC/0/1/CPU0:May 28 18:25:35.734 : vkg_l2fib_mac_cache[357]
%PLATFORM-
PLAT_L2FIB_MAC_CACHE-6-RESYNC_COMPLETE : The resynchronization of the MAC
address table is complete
0/1/CPU0
```

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

syslog 메시지는 재동기화 프로세스가 완료되는 시기를 나타내므로, 메시지를 보기 위해 터미널 모니터를 활성화하는 것이 유용합니다.

Resync Age(재동기화 기간) 옆에는 MAC 주소가 하드웨어 테이블에서 마지막으로 재동기화된 시간이 표시됩니다.

location 키워드는 수신 또는 발신 라인 카드의 위치입니다. MAC 주소는 하드웨어에서 라인 카드 간에 교환되므로 AC 또는 PW가 있는 각 라인 카드에서 MAC 주소를 알아야 합니다. detail 키워드는 소프트웨어 테이블의 최신 버전을 제공할 수 있습니다.

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address detail location 0/1/CPU0
```

```
Bridge-domain name: customer1:engineering, id: 5, state: up
MAC learning: enabled
MAC port down flush: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC Secure: disabled, Logging: disabled
DHCPv4 snooping: profile not known on this node
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
IGMP snooping: disabled, flooding: enabled
Bridge MTU: 1500 bytes
Number of bridge ports: 3
Number of MAC addresses: 4
Multi-spanning tree instance: 0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
GigabitEthernet0/1/0/3.2, state: oper up
Number of MAC: 2
Statistics:
packets: received 187106, sent 757
bytes: received 13571342, sent 57446
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
```

Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 0019.552b.b581, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local

Mac Address: 0019.552b.b5c3, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local

GigabitEthernet0/1/0/38.2, state: oper up
Number of MAC: 1
Statistics:
packets: received 18, sent 14607
bytes: received 1950, sent 1061882
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 0024.986c.6417, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local

TenGigE0/2/0/4.2, state: oper up
Number of MAC: 1
Statistics:
packets: received 0, sent 0
bytes: received 0, sent 0
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 6c9c.ed3e.e484, LC learned: 0/2/CPU0
Resync Age: 0d 0h 0m 0s, Flag: remote

명령의 세부 버전에서는 브리지 도메인에서 학습된 총 MAC 주소 수와 각 AC에서 학습된 MAC 주소 수를 제공합니다.

hardware 키워드는 인그레스 또는 이그레스 포워딩 엔진에서 직접 하드웨어 mac-address-table을 폴링합니다.

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware ingress location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

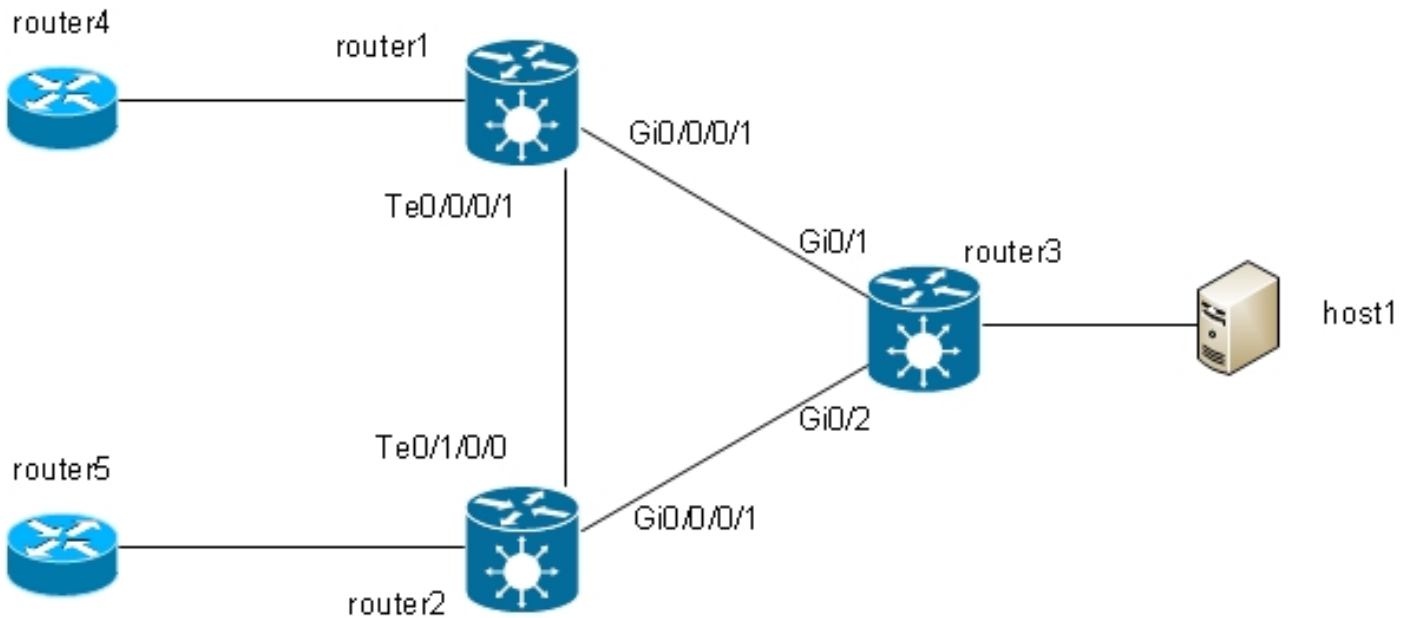
```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
```

```
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware egress location 0/2/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 14s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 1s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 10s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 13s N/A
RP/0/RSP0/CPU0:router1#
```

4.2 전체 MST

이전의 [로컬 스위칭](#)은 라우터만 브리지 도메인에 연결되었기 때문에 기본이었습니다. 그러나 L2 스위치를 연결하기 시작하면 루프가 발생할 수 있으며 루프를 끊으려면 STP가 필요합니다.



이 토폴로지에서는 router1, router2 및 router3가 각각 다이어그램에 있는 모든 인터페이스가 포함된 브리지 도메인으로 구성됩니다. router4가 브로드캐스트(예: ARP 요청)를 router1로 전송하면 router1은 이를 router2 및 router3으로 플러딩하고, router2는 이를 router3으로 플러딩하고, router3은 이를 router2로 플러딩합니다. 이것은 반복과 폭풍을 초래한다.

루프를 끊으려면 STP를 사용합니다. STP는 여러 유형이 있지만 Cisco IOS XR 소프트웨어는 MST라는 하나의 전체 구현만 제공합니다.

또한 PVSTAG 및 MSTAG와 같은 Cisco IOS XR 소프트웨어에서 지원되는 프로토콜의 액세스 게이트웨이 버전이 있습니다. 이는 일반적으로 VPLS를 사용하는 특정 토폴로지에서 사용할 수 있는 프로토콜의 제한된 정적 버전이며, MSTAG 및 PVSTAG [섹션에 설명되어](#) 있습니다. Cisco IOS XR 소프트웨어에서 MST는 여러 스위치가 있는 토폴로지가 있고 전체 스페닝 트리 구현이 필요한 경우에만 사용할 수 있습니다.

각 라우터에 2개의 하위 인터페이스가 구성되고 브리지 도메인에 추가됩니다. router1의 컨피그레이션은 다음과 같습니다.

```
interface GigabitEthernet0/0/0/1.2 l2transport
```

```

encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
!
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
!
!
!

```

MST가 기본 인터페이스에 구성되어 있습니다. 이 예에서 VLAN 2는 인스턴스 1에 할당되고 다른 모든 VLAN은 기본 인스턴스 0으로 유지됩니다. (좀 더 현실적인 컨피그레이션에서는 VLAN을 인스턴스 간에 균등하게 분할합니다.)

STP 네트워크 내에서 루트 브리지의 선택은 각 디바이스의 구성된 우선순위 및 임베디드 브리지 ID에 의해 결정됩니다. 우선순위가 가장 낮거나, 우선순위가 똑같이 가장 낮지만 브리지 ID가 가장 낮은 디바이스가 루트 브리지로 선택됩니다. 이 예에서 router3은 인스턴스 0의 경우 router1보다 낮은 우선 순위로 구성되므로 router3은 인스턴스 0의 루트입니다. 라우터1은 인스턴스 1의 경우 라우터3보다 우선순위가 낮으므로 라우터1은 인스턴스 1의 루트입니다.

다음은 router1의 컨피그레이션입니다.

```

spanning-tree mst customer1
name customer1
revision 1
instance 0
priority 28672
!
instance 1
vlan-ids 2
priority 24576
!
interface TenGigE0/0/0/1
!
interface GigabitEthernet0/0/0/1
!
!
!

```

라우터3의 컨피그레이션입니다.

```
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
```

```
spanning-tree mst 0 priority 24576
spanning-tree mst 1 priority 28672
```

이름, 개정 및 VLAN-인스턴스 매핑은 모든 스위치에서 동일해야 합니다.

이제 router1의 스패닝 트리 상태를 확인합니다.

```
RP/0/RSP1/CPU0:router1#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed
```

Operating in dot1q mode

MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

```
CIST Root Priority 24576
Address 001d.4603.1f00
Ext Cost 0
```

```
Root ID Priority 24576
Address 001d.4603.1f00
Int Cost 20000
Max Age 20 sec, Forward Delay 15 sec
```

```
Bridge ID Priority 28672 (priority 28672 sys-id-ext 0)
Address 4055.3912.f1e6
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6
```

```
Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
```

```
-----
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.1
Te0/0/0/1 128.1 2000 DSGN FWD 28672 4055.3912.f1e6 128.1
```

MSTI 1:

VLANS Mapped: 2

```
Root ID Priority 24576
Address 4055.3912.f1e6
This bridge is the root
Int Cost 0
Max Age 20 sec, Forward Delay 15 sec
```

```
Bridge ID Priority 24576 (priority 24576 sys-id-ext 0)
```

Address 4055.3912.f1e6
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6

```
Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
-----
Gi0/0/0/1 128.2 20000 DSGN FWD 24576 4055.3912.f1e6 128.2
Te0/0/0/1 128.1 2000 DSGN FWD 24576 4055.3912.f1e6 128.1
```

Router3은 예를 들어 0의 루트이므로 router1은 Gi0/0/0/1에서 router3으로 향하는 루트 포트를 가집니다. Router1은 인스턴스 1의 루트이므로, router1은 해당 인스턴스의 모든 인터페이스에서 지정된 브리지입니다.

라우터2는 Te0/1/0/0에서 0에 대해 차단됩니다.

```
RP/0/RSP1/CPU0:router2#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed
```

Operating in dot1q mode

MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

```
CIST Root Priority 24576
Address 001d.4603.1f00
Ext Cost 0
```

```
Root ID Priority 24576
Address 001d.4603.1f00
Int Cost 20000
Max Age 20 sec, Forward Delay 15 sec
```

```
Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address f025.72a7.b13e
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6
```

```
Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
-----
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.2
Te0/1/0/0 128.1 2000 ALT BLK 28672 4055.3912.f1e6 128.1
```

MSTI 1:

VLANS Mapped: 2

```
Root ID Priority 24576
Address 4055.3912.f1e6
Int Cost 2000
Max Age 20 sec, Forward Delay 15 sec
```

```
Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
```

Address f025.72a7.b13e
 Max Age 20 sec, Forward Delay 15 sec
 Max Hops 20, Transmit Hold count 6

```
Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
-----
Gi0/0/0/1 128.2 20000 DSGN FWD 32768 f025.72a7.b13e 128.2
Te0/1/0/0 128.1 2000 ROOT FWD 24576 4055.3912.f1e6 128.1
RP/0/RSP1/CPU0:router2#
```

Te0/1/0/0.2가 포워딩되고 Te0/1/0/0.3은 차단됩니다. STP Blocked 값이 0x0이면 조건이 false이므로 인터페이스가 전달됩니다. STP Blocked 값이 0x1이면 조건이 true이므로 인터페이스가 차단됩니다.

이를 확인하고 네트워크 프로세서에 있는 인터페이스 데이터를 표시하려면 **show uidb data** 명령을 사용합니다.

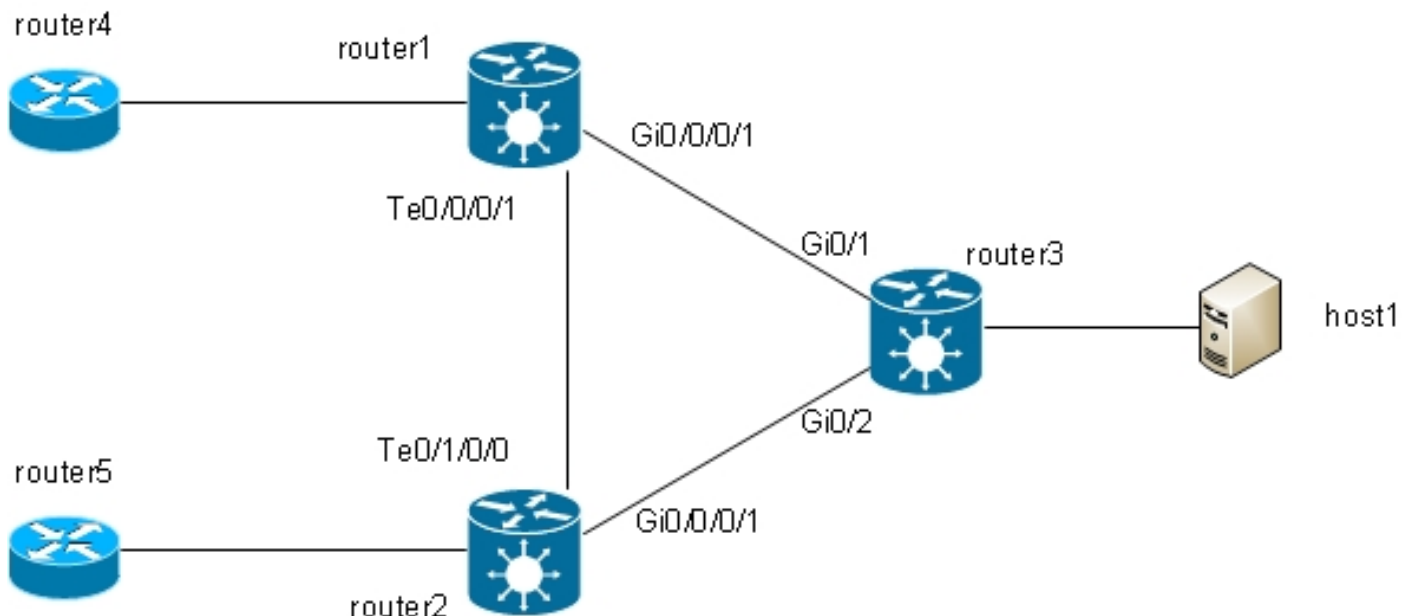
```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked                                0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked                                0x1
```

4.3BVI

브리지 도메인을 구성하면 L2 도메인이 생성됩니다. 해당 L2 도메인을 종료하려면 브리지 도메인 내의 호스트와 외부 환경 간에 라우팅하는 L3 라우터를 연결합니다. [이전](#) 다이어그램에서 host1은 로컬 서브넷을 종료하고 인터넷에 연결하기 위해 router4 또는 router5를 사용할 수 있습니다.

브리지 도메인이 구성된 라우터 1 및 라우터 2는 ASR 9000 라우터이며, IPv4 및 IPv6 트래픽을 라우팅할 수 있습니다. 따라서 이 두 라우터는 L3 라우터에 의존하는 대신 브리지 도메인에서 IP 트래픽을 가져와 인터넷으로 직접 라우팅할 수 있습니다. 이렇게 하려면 브리지 도메인에 패킷을 보내고 받을 수 있도록 브리지 도메인에 연결되는 L3 인터페이스인 BVI를 구성해야 합니다.

논리적으로 보면 다음과 같습니다.



이는 다음과 같은 컨피그레이션입니다.

```
RP/0/RSP1/CPU0:router1#sh run int bvi 2
interface BVI2
ipv4 address 192.168.2.1 255.255.255.0
!

RP/0/RSP1/CPU0:router1#sh run int bvi 3
interface BVI3
ipv4 address 192.168.3.1 255.255.255.0
!

RP/0/RSP1/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
!
routed interface BVI3
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
routed interface BVI2
!
!
!
RP/0/RSP1/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

BVI는 태그가 지정되지 않은 L3 인터페이스입니다. 따라서 BVI에서 브리지 도메인의 AC에 수신된 패킷을 처리하게 하려면 들어오는 모든 태그를 팝업하도록 AC를 구성해야 합니다. 그렇지 않으면 BVI가 태그를 인식할 수 없어 패킷을 삭제합니다. BVI에서는 dot1q 하위 인터페이스를 구성할 수 없으므로 [이전 예](#)의 Gi0/0/0/1.2에서와 같이 AC에서 태그를 팝업으로 인그레스(ingress)해야 [합니](#)
[다](#).

BVI 인터페이스는 가상 인터페이스이므로 활성화할 수 있는 기능에 몇 가지 제한이 있습니다. 이러한 제한 사항은 [Cisco ASR 9000 Series 라우터에 통합 라우팅 및 브리징 구성: IRB 구성에 대한 제한 사항에 설명되어 있습니다](#). ASR 9000의 BVI 인터페이스에서는 다음 기능이 지원되지 않습니다.

- ACL(Access Control List). 그러나 브리지 도메인의 각 L2 포트에 L2 ACL을 구성할 수 있습니다
- IP FRR(빠른 경로 재지정)
- Netflow
- MoFRR(멀티캐스트 전용 빠른 재라우팅)
- MPLS 레이블 스위칭
- mVPNv4
- QoS(Quality of Service)
- 트래픽 미러링

- BVI의 번호가 지정되지 않은 인터페이스
- 비디오 모니터링(Vidmon)

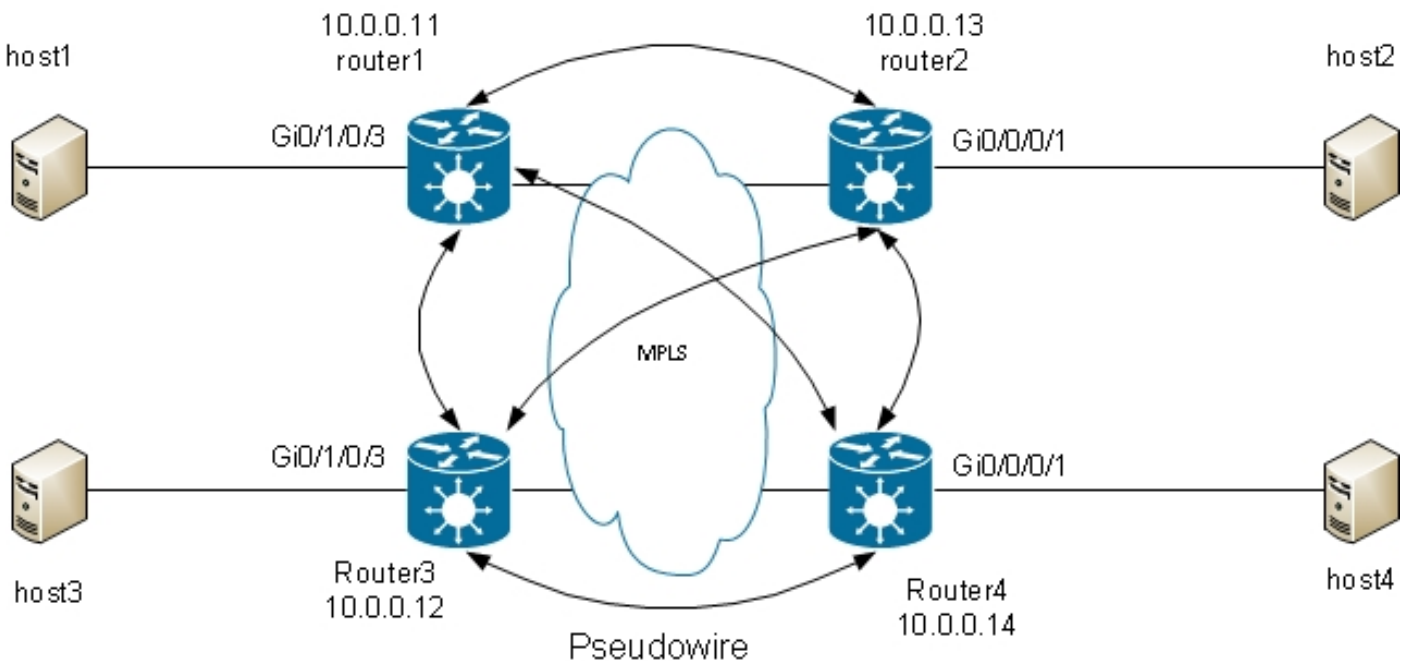
BVI는 VRF(Virtual Routing and Forwarding) 컨피그레이션일 수 있으므로 BVI에 수신된 트래픽은 MPLS를 통해 전달되지만 *per-vrf label-allocation-mode*를 사용해야 합니다.

이러한 제한된 기능 중 하나가 필요한 경우 BVI를 사용할 수 없습니다. 또 다른 해결 방법은 라우터의 두 포트 간에 외부 루프백 케이블을 사용하는 것입니다. 여기서 한 포트는 브리지 도메인에 있고 한 포트는 모든 기능을 구성할 수 있는 일반 라우터 인터페이스로 구성됩니다.

4.4 VPLS

4.4.1 개요

VPLS는 MPLS PW를 통해 여러 사이트의 브리지 도메인을 하나의 큰 브리지 도메인으로 결합할 수 있는 기능을 제공합니다. 서로 다른 사이트의 호스트는 L2VPN PE 간에 MPLS PW의 전체 메쉬를 통해 투명하게 캡슐화되므로 동일한 L2 세그먼트에 직접 연결된 것으로 보입니다.



각 호스트가 다른 모든 호스트의 트래픽을 수신할 수 있도록 하려면 PW의 전체 메시가 필요합니다. 따라서 L2VPN PE는 VPLS PW에서 수신된 프레임을 다른 VPLS PW를 통해 전달하지 않습니다. PW의 풀 메시가 있어야 합니다. 즉, 각 PE는 트래픽을 직접 수신하며 포워딩을 하면 루프가 발생하므로 PW 간에 트래픽을 포워딩할 필요가 없습니다. 이를 split horizon 규칙이라고 합니다.

라우터에서 MAC 학습을 실행하고 있습니다. MAC 주소가 mac-address-table에 있으면 PW를 통해 대상 MAC 주소에 대한 프레임만 이 MAC 주소가 학습된 L2VPN PE로 전달합니다. 따라서 코어에서 불필요한 트래픽 중복이 방지됩니다. 모든 호스트에서 브로드캐스트 및 멀티캐스트를 수신할 수 있도록 하기 위해 모든 PW에서 브로드캐스트 및 멀티캐스트를 풀러딩합니다. IGMP 스누핑과 같은 기능은 수신기 또는 멀티캐스트 라우터가 있는 경우에만 멀티캐스트 프레임을 PE에 전송할 수 있으므로 유용합니다. 이 경우 코어에 있는 트래픽의 양이 줄어들지만, 동일한 패킷의 여러 복사본이 각 PE에 전송되어야 하지만 해당 그룹에 대한 관심이 있을 때 이 복사본을 전송해야 합니다.

PW의 전체 메시는 VFI(Virtual Forwarding Instance) 아래에서 구성해야 합니다.

```

RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
!

```

VFI 아래에 구성된 PW는 코어에서 완전히 메싱되는 PW입니다. 이러한 프레임은 한 PW에서 수신된 프레임이 다른 PW로 전달되지 않도록 하기 위해 동일한 SHG(Split Horizon Group)의 일부입니다.

AC의 한 유형으로 간주되고 VFI 아래에 구성되지 않는 액세스 PW를 구성할 수 있습니다. 자세한 내용은 섹션을 참조하십시오.

router2, router3 및 router4의 컨피그레이션은 매우 유사하며, 나머지 3개의 라우터는 모두 VFI 아래의 네이버로 존재합니다.

```

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled

```

DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (23:06:02 ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up [H-VPLS](#)
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 234039, sent 7824
bytes: received 16979396, sent 584608
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up (established)
PW class not set, XC ID 0xc0000009
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16049 16042
Group ID 0x5 0x1
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225481
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 15:57:36 (00:25:29 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 555, sent 285
bytes: received 36308, sent 23064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up (established)
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16050 16040
Group ID 0x5 0x3
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225482
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:00:56 (00:22:09 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 184, sent 158
bytes: received 12198, sent 14144
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 2, state is up (established)
PW class not set, XC ID 0xc000000b
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16051 289974
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled

```

PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225483
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:02:38 (00:20:27 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 137
bytes: received 0, sent 12064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0

```

10.0.0.12까지의 PW에 대한 로컬 레이블은 16049이며, 이는 레이블 16049과 함께 이더넷 프레임이 수신됨을 의미합니다. 최종 MPLS 홉에서 IGP 레이블을 팝업했어야 하므로, 스위칭 결정은 이 MPLS 레이블을 기반으로 합니다. 명시적 null 레이블이 남아 있을 수 있지만 스위칭 결정은 PW 레이블을 기반으로 합니다.

```

RP/0/RSP0/CPU0:router1#sh mpls forwarding labels 16049
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
-----
16049 Pop PW(10.0.0.12:2) BD=5 point2point 58226

```

레이블에 대한 **show mpls forwarding labels** 명령은 브리지 도메인 번호를 제공하며, 이 번호를 사용하여 패킷이 수신된 대상 mac-address 및 PW(neighbor 및 pw-id)를 찾을 수 있습니다. 그런 다음 해당 네이버를 가리키는 mac-address-table에 항목을 생성할 수 있습니다.

```

RP/0/RSP0/CPU0:router1#sh l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-----
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.985e.6a01 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/1/CPU0 0d 0h 0m 0s N/A

```

4.4.2 PW 유형 및 전송된 태그

VPLS PW는 기본적으로 유형 5(이더넷) PW로서 협상됩니다. VLAN 태그 조작 후(rewrite 명령이 구성된 경우) AC에 들어오는 것은 무엇이든 PW를 통해 전송됩니다.

Cisco IOS XR Software Release 4.1.0 for LDP signaling and Release 4.3.1 with BGP에서는 인접 디바이스 아래에 pw-class를 구성하고 pw-class 아래에 **전송 모드 vlan passthrough**를 구성할 수 있습니다. 그러면 rewrite 명령이 구성된 경우 VLAN 태그 조작 후 AC에서 나오는 모든 것을 전송하는 VC(virtual connection)-type 4(이더넷 VLAN) PW가 협상됩니다.

VC-type 4 PW가 있는 경우 프레임에 dot1q 태그가 필요하므로 EFP에서 VLAN 태그를 조작하면 프레임에 하나 이상의 VLAN 태그가 남아 있습니다. 전송 모드 vlan 패스스루 모드를 사용할 때 프레임에 더미 태그 0이 추가되지 않습니다.

동일한 VFI에서 유형 4와 유형 5 PW를 혼합하는 것은 지원되지 않습니다. 모든 PW는 같은 유형이어야 합니다.

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
pw-class VC4-PT
!
neighbor 10.0.0.13 pw-id 2
pw-class VC4-PT
!
neighbor 10.0.0.14 pw-id 2
pw-class VC4-PT
!
!
!
!
```

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail |
i "PW:|PW type"
MAC withdraw for Access PW: enabled
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
```

4.4.3 자동 검색 및 신호 처리

는 VFI에 속한 모든 네이버의 수동 컨피그레이션을 기반으로 했습니다. MPLS LDP는 인접 디바이스와의 PW 시그널링에 사용되었습니다.[이전 예](#)

네트워크에 새 VPLS PE를 추가할 때 각 로컬 브리지 도메인의 모든 기존 PE에 대한 PW를 갖도록 PE를 구성합니다. 그러면 모든 PE가 완전히 메싱되어야 하므로 새 PE에 대한 PW를 보유하기 위해 모든 기존 PE를 재구성해야 합니다. 이는 PE 및 브리지 도메인의 수가 증가함에 따라 운영상의 문제가 될 수 있습니다.

한 가지 해결 방법은 PE가 BGP를 통해 자동으로 다른 PE를 검색하도록 하는 것입니다. IBGP에는 풀 메시(full-mesh) 요구 사항도 있지만 경로 리플렉터를 사용하면 풀 메시(full-mesh) 요구 사항을 해결할 수 있습니다. 따라서 새 PE는 일반적으로 적은 수의 경로 리플렉터로 피어링하도록 구성되며, 다른 모든 PE는 해당 업데이트를 수신하고, 새 PE는 다른 PE로부터 업데이트를 수신합니다.

BGP를 통해 다른 PE를 검색하기 위해 각 PE는 vpls-vpws 주소군에 대해 구성되며, 참여하려는 브리지 도메인을 BGP에 광고합니다. 동일한 브리지 도메인에 속한 다른 PE가 검색되면 각 PE에 대해 PW가 설정됩니다. BGP는 이 자동 검색에 사용되는 프로토콜입니다.

자동 검색된 PE에 대한 PW의 신호에는 BGP와 LDP의 두 가지 옵션이 있습니다. 이 예에서는 BGP 신호 및 LDP [신호](#)를 사용하여 [이전](#) 토폴로지를 BGP 자동 검색으로 변환합니다.

4.4.3.1 BGP 자동 검색 및 BGP 시그널링

라우터 bgp 및 인접 디바이스(다른 PE 또는 route-reflector) 아래에 주소군 l2vpn vpls-vpws를 구성합니다.

```
router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
```

새 주소 패밀리가 네이버와 함께 활성화되지만 어떤 PE도 아직 브리지 도메인에 대한 참여를 알리지 않았습니다.

```
RP/0/RSP0/CPU0:router1#sh bgp neighbor 10.0.0.3 | i Address family L2VPN
Address family L2VPN VPLS: advertised and received
```

```
P/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 77
BGP scan interval 60 secs
```

BGP is operating in STANDALONE mode.

```
Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 77 77 77 77 77 77
```

```
Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 252950 53252 77 0 0 1w0d 0
10.0.0.10 0 65000 941101 47439 77 0 0 00:10:18 0
```

L2VPN 브리지 도메인 컨피그레이션 모드에서 자동 검색 bgp 및 신호 프로토콜 bgp를 구성합니다. router1의 컨피그레이션은 다음과 같습니다.

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
```

```

!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 11
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 11
!
!
!
!
!
!
!

```

router2의 컨피그레이션은 다음과 같습니다.

```

RP/0/RSP1/CPU0:router2#sh run l2vpn bridge group customer1
Thu May 30 15:25:55.638 CEST
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 13
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 13
!
!
!
!

```


!
!

vpn-id와 route-target은 각 브리지 도메인에 대해 서로 다른 PE에서 동일하지만 각 PE에는 고유한 VE-ID(Virtual Edge Identifier)가 있습니다. 각 PE는 BGP를 통해 VPN의 다른 PE를 검색하고 PW에 신호를 보내기 위해 BGP를 사용합니다. 그 결과 PW의 전체 메시지가 생성됩니다.

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 103
BGP scan interval 60 secs
```

BGP is operating in STANDALONE mode.

```
Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 103 103 103 103 103 103
```

```
Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 254944 53346 103 0 0 1w0d 6
10.0.0.10 0 65000 944859 47532 103 0 0 01:40:22 6
```

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 103
BGP scan interval 60 secs
```

Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Rcvd Label Local Label

Route Distinguisher: 10.0.0.11:32769 (default for vrf customer1:finance)

*> 11:10/32 0.0.0.0 nolabel 16060

*>i12:10/32 10.0.0.12 16060 nolabel

*>i13:10/32 10.0.0.13 16060 nolabel

*>i14:10/32 10.0.0.14 289959 nolabel

Route Distinguisher: 10.0.0.11:32770 (default for vrf customer1:engineering)

*> 11:10/32 0.0.0.0 nolabel 16075

*>i12:10/32 10.0.0.12 16075 nolabel

*>i13:10/32 10.0.0.13 16075 nolabel

*>i14:10/32 10.0.0.14 289944 nolabel

Route Distinguisher: 10.0.0.12:32768

*>i12:10/32 10.0.0.12 16060 nolabel

* i 10.0.0.12 16060 nolabel

Route Distinguisher: 10.0.0.12:32769

*>i12:10/32 10.0.0.12 16075 nolabel

* i 10.0.0.12 16075 nolabel

Route Distinguisher: 10.0.0.13:32769

*>i13:10/32 10.0.0.13 16060 nolabel

* i 10.0.0.13 16060 nolabel

Route Distinguisher: 10.0.0.13:32770

*>i13:10/32 10.0.0.13 16075 nolabel

* i 10.0.0.13 16075 nolabel

Route Distinguisher: 10.0.0.14:32768

*>i14:10/32 10.0.0.14 289959 nolabel

* i 10.0.0.14 289959 nolabel

Route Distinguisher: 10.0.0.14:32769

```
*>i14:10/32 10.0.0.14 289944 nolabel
* i 10.0.0.14 289944 nolabel
```

Processed 14 prefixes, 20 paths

이는 router1에서 볼 수 있듯이 router3(10.0.0.13)에서 광고하는 접두사입니다. 접두사는 두 개의 route-reflector(10.0.0.3 및 10.0.0.10)를 통해 수신됩니다.

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32770 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32770
Versions:
Process bRIB/RIB SendTblVer
Speaker 92 92
Last Modified: May 30 15:10:44.100 for 01:23:38
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, best, group-best,
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 92
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32769 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32769
Versions:
Process bRIB/RIB SendTblVer
Speaker 93 93
Last Modified: May 30 15:10:44.100 for 01:25:02
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, best, group-best,
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 93
Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
```

Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10

라우터1에서 몇 가지 PW를 설정했습니다.

RP/0/RSP0/CPU0:router1#sh l2vpn discovery bridge-domain

Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3, signaling
protocol: BGP
List of Local Edges (1 Edges):
Local Edge ID: 11, Label Blocks (1 Blocks)
Label base Offset Size Time Created

16060 10 10 05/30/2013 15:07:39
List of Remote Edges (3 Edges):
Remote Edge ID: 12, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created

16060 10 10 10.0.0.12 05/30/2013 15:09:53
Remote Edge ID: 13, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created

16060 10 10 10.0.0.13 05/30/2013 15:10:43
Remote Edge ID: 14, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created

289959 10 10 10.0.0.14 05/30/2013 15:11:22

Bridge group: customer1, bridge-domain: engineering, id: 5, signaling
protocol: BGP
List of Local Edges (1 Edges):
Local Edge ID: 11, Label Blocks (1 Blocks)
Label base Offset Size Time Created

16075 10 10 05/30/2013 15:08:54
List of Remote Edges (3 Edges):
Remote Edge ID: 12, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created

16075 10 10 10.0.0.12 05/30/2013 15:09:53
Remote Edge ID: 13, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created

16075 10 10 10.0.0.13 05/30/2013 15:10:43
Remote Edge ID: 14, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created

289944 10 10 10.0.0.14 05/30/2013 15:11:22

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain autodiscovery bgp
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0

```
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1 detail
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
```

MIB cvplsConfigIndex: 4
Filter MAC addresses:
Create time: 29/05/2013 15:36:17 (1d01h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [3, 3]
MTU 1500; XC ID 0xc40006; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 10120, sent 43948
bytes: received 933682, sent 2989896
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32769
Import Route Targets:
0.0.0.1:3
Export Route Targets:
0.0.0.1:3
Signaling protocol: BGP
Local VE-ID: 11 , Advertised Local VE-ID : 11
VE-Range: 10
PW: neighbor 10.0.0.12, PW ID 3, state is up (established)
PW class not set, XC ID 0xc000000c
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote

Label 16062 16061
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 12

MIB cpwVcIndex: 3221225484
Create time: 30/05/2013 15:09:52 (01:29:44 ago)
Last time status changed: 30/05/2013 15:09:52 (01:29:44 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 2679, sent 575
bytes: received 171698, sent 51784
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 3, state is up (established)
PW class not set, XC ID 0xc000000e
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote

Label 16063 16061
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 13

MIB cpwVcIndex: 3221225486
Create time: 30/05/2013 15:10:43 (01:28:54 ago)
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 11, sent 574
bytes: received 1200, sent 51840
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 3, state is up (established)
PW class not set, XC ID 0xc0000010
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote

Label 16064 289960
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 14

MIB cpwVcIndex: 3221225488
Create time: 30/05/2013 15:11:22 (01:28:15 ago)
Last time status changed: 30/05/2013 15:11:22 (01:28:15 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 561
bytes: received 0, sent 50454
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:

drops: illegal VLAN 0, illegal length 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1d23h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 243532, sent 51089
bytes: received 17865888, sent 3528732
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32770

Import Route Targets:
0.0.0.1:2
Export Route Targets:
0.0.0.1:2
Signaling protocol: BGP
Local VE-ID: 11 , Advertised Local VE-ID : 11
VE-Range: 10
PW: neighbor 10.0.0.12, PW ID 2, state is up (established)
PW class not set, XC ID 0xc000000d
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote

Label 16077 16076
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 12

MIB cpwVcIndex: 3221225485
Create time: 30/05/2013 15:09:52 (01:29:45 ago)
Last time status changed: 30/05/2013 15:09:52 (01:29:45 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 2677, sent 574
bytes: received 171524, sent 51670
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up (established)
PW class not set, XC ID 0xc000000f
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote

Label 16078 16076
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 13

MIB cpwVcIndex: 3221225487
Create time: 30/05/2013 15:10:43 (01:28:54 ago)
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 17, sent 572
bytes: received 1560, sent 51636
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 2, state is up (established)
PW class not set, XC ID 0xc0000011
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none


```
PW backup disable delay 0 sec
Sequencing not set
```

```
MPLS Local Remote
```

```
-----
Label 16079 289945
```

```
MTU 1500 1500
```

```
Control word disabled disabled
```

```
PW type VPLS VPLS
```

```
VE-ID 11 14
-----
```

```
MIB cpwVcIndex: 3221225489
```

```
Create time: 30/05/2013 15:11:22 (01:28:16 ago)
```

```
Last time status changed: 30/05/2013 15:11:22 (01:28:16 ago)
```

```
MAC withdraw message: send 0 receive 0
```

```
Static MAC addresses:
```

```
Statistics:
```

```
packets: received 0, sent 559
```

```
bytes: received 0, sent 50250
```

```
DHCPv4 snooping: disabled
```

```
IGMP Snooping profile: none
```

```
VFI Statistics:
```

```
drops: illegal VLAN 0, illegal length 0
```

4.4.3.2 BGP 자동 검색 및 LDP 신호

address-family l2vpn vpls-vpws 명령을 사용한 BGP 컨피그레이션은 BGP 시그널링과 정확히 동일합니다. L2VPN 컨피그레이션은 **signaling-protocol ldp** 명령으로 LDP 신호 처리를 사용하도록 수정되었습니다.

동일한 컨피그레이션이 4개의 PE 모두에서 사용됩니다.

```
router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol ldp
vpls-id 65000:3
!
!
!
!
```

```

bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol ldp
    vpls-id 65000:2
!
!
!
!
!
!

```

vpls-id는 BGP AS(Autonomous System) 번호 및 vpn-id로 구성됩니다.

router1의 세 가지 show 명령은 검색된 PE로 PW가 설정되었음을 보여줍니다.

```
RP/0/RSP0/CPU0:router1#sh l2vpn discovery
```

```

Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3,
signaling protocol: LDP
VPLS-ID: 65000:3
Local L2 router id: 10.0.0.11
List of Remote NLRI (3 NLRIs):
Local Addr Remote Addr Remote L2 RID Time Created
-----
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46

```

```

Bridge group: customer1, bridge-domain: engineering, id: 5,
signaling protocol: LDP
VPLS-ID: 65000:2
Local L2 router id: 10.0.0.11
List of Remote NLRI (3 NLRIs):
Local Addr Remote Addr Remote L2 RID Time Created
-----
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46

```

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1
```

```

Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 65000:3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 65000:3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 65000:3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,

```

ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 65000:2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 65000:2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 65000:2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#**sh l2vpn bridge-domain group customer1 det**

Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 4
Filter MAC addresses:
Create time: 29/05/2013 15:36:17 (1d01h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [3, 3]
MTU 1500; XC ID 0xc40006; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 10362, sent 45038

bytes: received 956240, sent 3064016
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32769
Import Route Targets:
0.0.0.1:3
Export Route Targets:
0.0.0.1:3
Signaling protocol: LDP
AS Number: 65000
VPLS-ID: 65000:3
L2VPN Router ID: 10.0.0.11
PW: neighbor 10.0.0.12, PW ID 65000:3, state is up (established)
PW class not set, XC ID 0xc0000003
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use

MPLS Local Remote

Label 16006 16033
BGP Peer ID 10.0.0.11 10.0.0.12
LDP ID 10.0.0.11 10.0.0.12
AII 10.0.0.11 10.0.0.12
AGI 65000:3 65000:3
Group ID 0x3 0x0
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):

Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225475
Create time: 30/05/2013 17:10:18 (00:06:32 ago)
Last time status changed: 30/05/2013 17:10:24 (00:06:25 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 190, sent 40
bytes: received 12160, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 65000:3, state is up (established)
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP

Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16016 16020
BGP Peer ID 10.0.0.11 10.0.0.13
LDP ID 10.0.0.11 10.0.0.13
AII 10.0.0.11 10.0.0.13
AGI 65000:3 65000:3
Group ID 0x3 0x4
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/05/2013 17:10:18 (00:06:32 ago)
Last time status changed: 30/05/2013 17:10:27 (00:06:22 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 40
bytes: received 0, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 65000:3, state is up (established)
PW class not set, XC ID 0xc0000009
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16049 289970
BGP Peer ID 10.0.0.11 10.0.0.14
LDP ID 10.0.0.11 10.0.0.14
AII 10.0.0.11 10.0.0.14
AGI 65000:3 65000:3
Group ID 0x3 0x4
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):

Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225481
Create time: 30/05/2013 17:11:46 (00:05:04 ago)
Last time status changed: 30/05/2013 17:11:51 (00:04:59 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 31
bytes: received 0, sent 2790
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1d23h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 243774, sent 52179
bytes: received 17888446, sent 3602852
Storm control drop counters:

packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned (Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32770
Import Route Targets:
0.0.0.1:2
Export Route Targets:
0.0.0.1:2
Signaling protocol: LDP
AS Number: 65000
VPLS-ID: 65000:2
L2VPN Router ID: 10.0.0.11
PW: neighbor 10.0.0.12, PW ID 65000:2, state is up (established)
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote

Label 16027 16042
BGP Peer ID 10.0.0.11 10.0.0.12
LDP ID 10.0.0.11 10.0.0.12
AII 10.0.0.11 10.0.0.12
AGI 65000:2 65000:2
Group ID 0x5 0x1
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 0
Create time: 30/05/2013 17:10:18 (00:06:33 ago)
Last time status changed: 30/05/2013 17:10:24 (00:06:26 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 190, sent 41
bytes: received 12160, sent 3690
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 65000:2, state is up (established)
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec

Sequencing not set

PW Status TLV in use

MPLS Local Remote

Label 16043 16021
BGP Peer ID 10.0.0.11 10.0.0.13
LDP ID 10.0.0.11 10.0.0.13
AII 10.0.0.11 10.0.0.13
AGI 65000:2 65000:2
Group ID 0x5 0x3
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 0
Create time: 30/05/2013 17:10:18 (00:06:33 ago)
Last time status changed: 30/05/2013 17:10:27 (00:06:23 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 40
bytes: received 0, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 65000:2, state is up (established)
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use

MPLS Local Remote

Label 16050 289974
BGP Peer ID 10.0.0.11 10.0.0.14
LDP ID 10.0.0.11 10.0.0.14
AII 10.0.0.11 10.0.0.14
AGI 65000:2 65000:2
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)

Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225482
Create time: 30/05/2013 17:11:46 (00:05:05 ago)


```
Last time status changed: 30/05/2013 17:11:51 (00:05:00 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 31
bytes: received 0, sent 2790
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

4.4.4 MAC 플러시 및 인출

VPLS에서 포워딩은 수신하는 프레임의 소스 MAC 주소를 학습하여 동적으로 구성되는 mac-address-table을 기반으로 합니다. 브리지 도메인에 토폴로지가 변경되면 호스트가 다른 AC 또는 VPLS 인접 디바이스를 통해 도달할 수 있습니다. 기존 mac-address-table에 따라 프레임이 계속 포워딩되는 경우 해당 호스트의 트래픽이 대상에 도달하지 못할 수 있습니다.

L2VPN PE의 경우 여러 가지 방법으로 토폴로지 변경을 탐지할 수 있습니다.

- 브리지 도메인의 포트가 작동 또는 중단됩니다.
- L2VPN PE가 전체 MST 구현 또는 스페닝 트리 액세스 게이트웨이 프로토콜을 실행할 경우 TCN(Spanning Tree Topology Change Notification) BPDU가 처리됩니다. 장애가 발생한 링크는 PE에서 로컬이 아닐 수 있지만 토폴로지에서 더 멀리 떨어져 있을 수 있습니다. PE가 TCN을 인터셉트합니다.

L2VPN PE가 토폴로지 변경을 탐지하면 두 가지 작업을 수행합니다.

1. PE는 토폴로지 변경의 영향을 받는 브리지 도메인의 mac 주소 테이블을 플러시합니다. PE가 PVSTAG 또는 PVRSTAG(Per-VLAN Rapid Spanning Tree Access Gateway)에 대해 구성된 경우, 하나의 VLAN 하위 인터페이스에서 탐지된 TCN BPDU는 해당 물리적 인터페이스의 모든 VLAN 및 브리지 도메인에 영향을 줍니다.
2. PE는 MPLS LDP MAC 회수 메시지를 통해 VPLS 인접 디바이스에 mac-address-table을 플러시해야 한다는 신호를 보냅니다. MAC 회수 LDP 메시지를 수신하는 모든 원격 L2VPN PE는 mac-address-tables를 플러시하고 트래픽이 다시 플러시됩니다. mac-address-tables는 새 토폴로지를 기반으로 재구축됩니다.

포트 플랩의 경우 MAC 수신 거부 메시지의 기본 동작이 시간이 지남에 따라 변경되었습니다.

- 전통적으로 Cisco IOS XR 소프트웨어에서 L2VPN PE는 AC가 중단될 때 MAC 철회 메시지를 보냈습니다. 원격 PE가 영향을 받는 브리지 도메인에 대한 MAC 주소 테이블을 플러시하도록 하여 다운된 포트 뒤에 있는 MAC 주소를 다른 포트에서 학습하도록 하려는 의도였습니다.
- 그러나 이로 인해 RFC 4762를 따르는 일부 원격 PE에서 상호 운용성 문제가 발생했으며 MAC 철회 메시지를 전송하는 PE를 제외한 모든 PE에서 해당 MAC 주소를 삭제합니다. RFC 4762에서는 AC가 가동될 때는 PE가 MAC 철회 메시지를 전송하지만 AC가 가동될 때는 보내지 않는다고 가정합니다. Cisco IOS XR Software Release 4.2.1 이후의 기본 동작은 RFC를 더 잘 준수하기 위해 브리지 도메인 포트가 나타날 때만 LDP MAC 철회 메시지를 전송하는 것입니다. 이전 동작으로 되돌리기 위해 configuration 명령이 추가되었습니다.

Cisco IOS XR 소프트웨어 릴리스 4.2.1 이후의 기본 동작이 포함된 show 명령입니다.

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain bd-name engineering det |
i "PW:|VFI|neighbor|MAC w"
MAC withdraw: enabled
```

```

MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 4
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 2
VFI Statistics:

```

중요한 행은 '브리지 포트 다운에서 전송된 MAC 철회'이며, 이제 Cisco IOS XR 소프트웨어 릴리스 4.2.1 이후에 기본적으로 비활성화됩니다. 이 명령은 또한 브리지 도메인에서 보내고 받은 MAC 수신 거부 메시지의 수를 제공합니다. 철회 메시지 수가 많으면 브리지 도메인이 불안정함을 나타냅니다.

이는 이전 동작으로 되돌아가는 컨피그레이션입니다.

```

l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
!
!
!

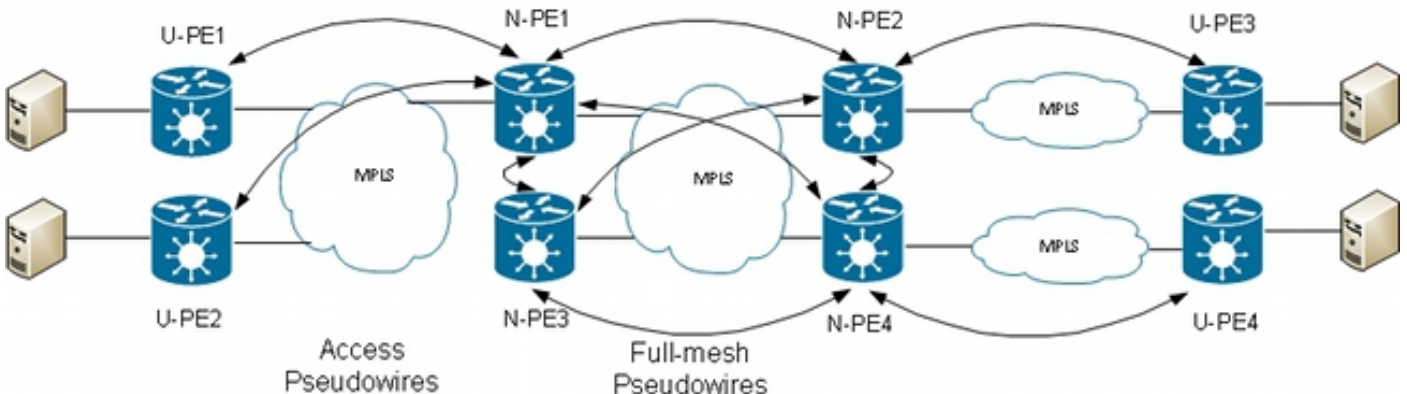
```

4.4.5 H-VPLS

VPLS는 L2VPN PE 간에 완전한 PW 메시가 있어야 어떤 PE가 어떤 PW에서 다른 PW로의 프레임 을 반영할 필요 없이 어떤 PE가 어떤 다른 PE 뒤의 호스트에 한 홉으로 도달할 수 있습니다. 이는 PE가 프레임을 한 PW에서 다른 PW로 포워딩하는 것을 방지하는 스플릿 호라이즌 규칙의 기초입 니다. mac-address-table의 목적지 MAC 주소가 다른 PW를 가리키는 특별한 경우에도 프레임이 삭 제됩니다.

PW의 풀 메시(full mesh)는 PE의 수가 증가함에 따라 PW의 수가 매우 많아질 수 있다는 의미이므 로 확장성 문제가 발생할 수 있습니다.

PE의 계층 구조를 사용하여 이 토폴로지에서 PW의 수를 줄일 수 있습니다.



이 토폴로지에서는 다음 사항에 유의하십시오.

- U-PE(User Provider Edge) 디바이스에는 CE에 대한 AC가 있습니다.
- U-PE 디바이스는 MPLS 포인트-투-포인트 PW를 통해 CE 트래픽을 N-PE(Network Provider Edge) 디바이스로 전송합니다.
- N-PE는 다른 N-PE와 완전히 메시(mesh)되는 코어 VPLS PE입니다.
- N-PE에서 U-PE에서 오는 PW는 AC와 매우 유사한 액세스 PW로 간주됩니다. U-PE는 다른 N-PE와 함께 메시의 일부가 아니므로 N-PE는 액세스 PW를 AC로 간주하고 해당 액세스 PW에서 VPLS 풀 메시의 일부인 코어 PW로 트래픽을 전달할 수 있습니다.
- N-PE 사이의 코어 PW는 VFI 아래에 구성된 모든 코어 PW에 split horizon 규칙이 적용되도록 하기 위해 VFI 아래에 구성됩니다.
- U-PE의 액세스 PW는 VFI 아래에 구성되지 않으므로 VFI PW와 동일한 SHG에 속하지 않습니다. 트래픽은 액세스 PW에서 VFI PW로 또는 그 반대로 전달될 수 있습니다.
- U-PE는 PW 이중화 기능을 사용하여 기본 N-PE에 대한 기본 PW와 대기 N-PE에 대한 대기 PW를 가질 수 있습니다. 기본 PW가 다운되면 스탠바이가 이 역할을 수행합니다.

다음은 U-PE1(10.0.0.15)이 N-PE1(10.0.0.11) 및 N-PE2(10.0.0.12)에 대한 PW 이중화로 구성된 예입니다.

```
RP/0/RP0/CPU0:U-PE1#sh run int ten 0/1/0/5.2
interface TenGigE0/1/0/5.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RP0/CPU0:U-PE1#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p engineering-0-1-0-5
interface TenGigE0/1/0/5.2
neighbor 10.0.0.11 pw-id 15
backup neighbor 10.0.0.12 pw-id 15
!
!
!
!
!
```

```
RP/0/RP0/CPU0:U-PE1#sh l2vpn xconnect group customer1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
-----
customer1 engineering-0-1-0-5
UP Te0/1/0/5.2 UP 10.0.0.11 15 UP
Backup
10.0.0.12 15 SB
-----
```

10.0.0.12에 대한 PW는 대기 상태입니다. N-PE1에는 10.0.0.15에 대한 액세스 PW와 VFI 아래에 없는 AC가 있습니다.

N-PE1은 액세스 PW 및 VFI PW를 통해 몇 가지 MAC 주소를 학습합니다.

```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
```

```

bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
neighbor 10.0.0.15 pw-id 15
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
Neighbor 10.0.0.15 pw-id 15, state: up, Static MAC addresses: 0
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
RP/0/RSP0/CPU0:N-PE1#sh l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

```

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to

```

-----
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A

```

N-PE2(10.0.0.12)에서 액세스 PW는 대기 상태입니다.

```

RP/0/RSP0/CPU0:N-PE2#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
neighbor 10.0.0.15 pw-id 15
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!

```

```

!
!
!
!
RP/0/RSP0/CPU0:N-PE2#sh l2vpn bridge-domain bd-name engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 1, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
Neighbor 10.0.0.15 pw-id 15, state: standby, Static MAC addresses: 0
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

```

4.4.6 SHG(Split Horizon Group)

스플릿 호라이즌 규칙은 하나의 VFI PW에서 수신된 프레임이 다른 VFI PW를 통해 전달될 수 없음을 지시합니다. VFI N-PE는 완전히 메시징되어야 합니다.

이 분할 기간은 SHG를 통해 시행됩니다.

- 한 SHG의 멤버는 서로 프레임을 전달할 수 없지만 다른 SHG의 멤버에게는 프레임을 전달할 수 있습니다.
- 모든 VFI PW는 기본적으로 SHG 1에 할당됩니다. 이렇게 하면 VFI PW 간에 포워딩이 없어 split horizon 규칙이 시행됩니다. VFI PW에서 수신된 패킷은 동일한 SHG의 일부가 아니므로 AC 및 액세스 PW에 전달될 수 있습니다.
- 모든 AC 및 액세스 PW는 기본적으로 SHG 그룹에 속하지 않습니다. 즉, AC 또는 액세스 PW에서 수신된 패킷을 동일한 브리지 도메인의 다른 AC 또는 액세스 PW로 전달할 수 있습니다.
- AC와 액세스 PW는 SHG 2에서 **split-horizon group** 명령을 사용하여 둘 사이의 전달을 방지하는 것이 목적이라면 SHG 2에 할당할 수 있습니다.

```

RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
split-horizon group
!
interface GigabitEthernet0/1/0/3.2
split-horizon group
!
neighbor 10.0.0.15 pw-id 15
split-horizon group
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!

```

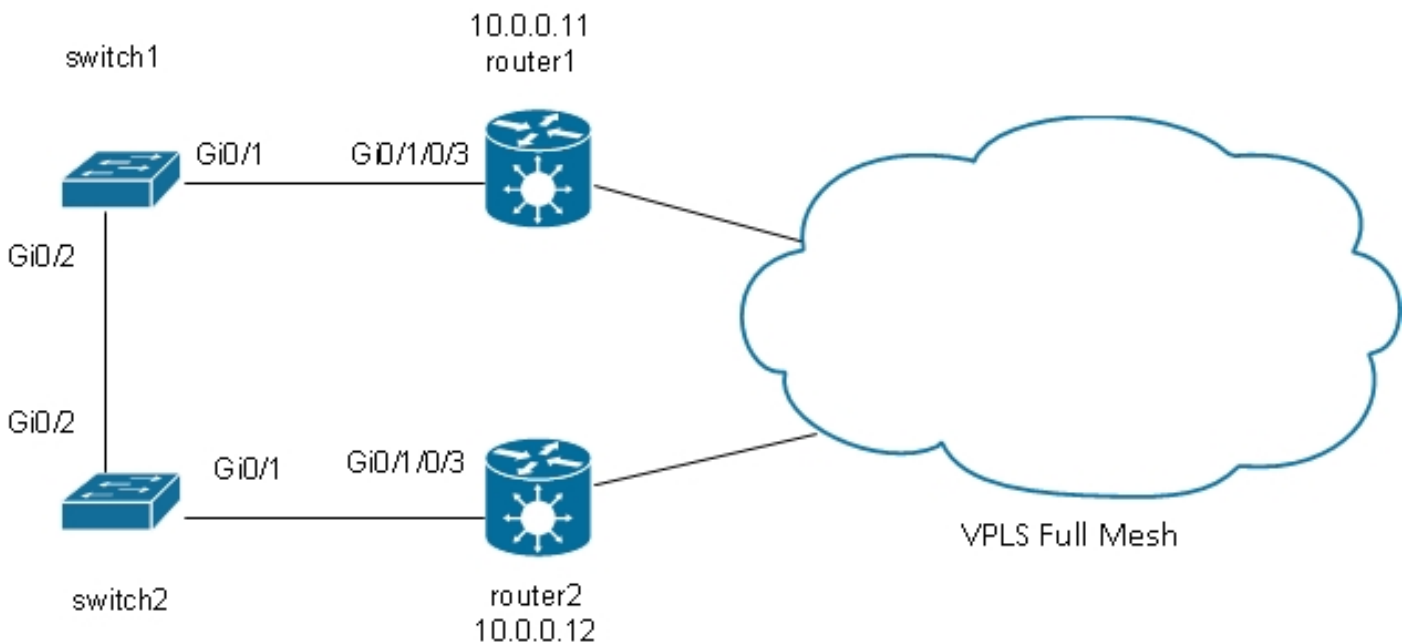
```
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

이 구성에서는 Gi 0/0/1.2와 Gi 0/1/0/3.2, Gi 0/0/0/1.2와 10.0.0.15 또는 Gi 0/1/0/3.2와 10.0.0.15 사이에 포워딩이 없습니다. 그러나 AC와 VFI PW는 서로 다른 SHG(1과 2)의 일부이므로 여전히 트래픽 포워딩이 있을 수 있습니다.

```
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering detail |
i "state is|List of|VFI|Split"
Split Horizon Group: none
ACs: 2 (1 up), VFIs: 1, PWS: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/0/0/1.2, state is unresolved
Split Horizon Group: enabled
AC: GigabitEthernet0/1/0/3.2, state is up
Split Horizon Group: enabled
List of Access PWS:
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )
Split Horizon Group: enabled
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
VFI Statistics:
```

4.4.7 이중화

이중화를 도입하려는 경우 VPLS 도메인에 이중으로 연결된 사이트가 있을 수 있습니다.



switch1에 연결된 호스트가 브로드캐스트를 전송하면 switch1은 이를 router1과 switch2로 전달합니다. Router1은 PW의 전체 메시지를 가지므로 router2에 대한 PW가 있으며, router1은 해당 PW를 통해 브로드캐스트를 전달합니다. Router2는 브로드캐스트를 switch2로 전달하며, switch2는 이를 switch1로 전달합니다. 이 경우 물리적 루프가 발생합니다.

4.4.7.1 스페닝 트리

VPLS에서는 [전체](#) MST 구현이 작동하지 않습니다. 이 구현에서는 주 인터페이스에 MST BPDU를 보내 해당 인터페이스에 있는 모든 VLAN의 포워딩 상태를 제어하기 때문입니다. VPLS에서는 각 브리지 도메인에 대한 VFI가 있으므로 이러한 모든 VFI에 대한 주 인터페이스에서 BPDU를 전송할 수 없습니다.

스패닝 트리 BPDU는 기본적으로 VPLS 및 포인트-투-포인트 PW를 통해 전송됩니다.

스위치 1과 스위치 2가 VLAN별 BPDU 또는 태그가 지정되지 않은 MST BPDU를 전송하는 경우 BPDU가 라우터 1과 라우터 2의 I2transport 하위 인터페이스와 일치하면 BPDU가 VPLS를 통해 전송됩니다. 스위치는 Gi 0/1 인터페이스에서 서로의 BPDU를 보고 스페닝 트리가 루프를 끊고 하나의 포트를 차단합니다.

스위치 2는 VLAN 2의 루트입니다.

```
switch2#sh spanning-tree vlan 2

MST0
Spanning tree enabled protocol mstp
Root ID Priority 32768
Address 0024.985e.6a00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Desg FWD 20000 128.1 P2p Bound(PVST)
Gi0/2 Desg FWD 20000 128.2 P2p Bound(PVST)
```

Switch1은 Gi 0/1에 루트 포트를 가지며 Gi 0/2를 차단하고 있습니다.

```
switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Root FWD 4 128.1 P2p
Gi0/2 Altn BLK 4 128.2 P2p
```

문제는 BPDU가 원격 사이트에도 전송되며 한 사이트의 스페닝 트리 불안정성이 VPLS 도메인에

연결된 모든 사이트에 전파된다는 것입니다. VPLS를 통해 BPDU를 전송하지 않고 각 사이트를 격리하는 것이 안전합니다.

한 가지 해결책은 STP의 액세스 게이트웨이 버전을 사용하는 것입니다. 이는 프로토콜의 제한된 구현이며, L2VPN PE는 스페닝 트리 루트에 연결된 것처럼 보이기 위해 일부 고정 BPDU를 전송하도록 구성됩니다. L2VPN PE는 CE에서 수신한 BPDU를 원격 사이트로 전송하지 않으므로 각 사이트에는 자체 스페닝 트리 도메인이 있습니다.

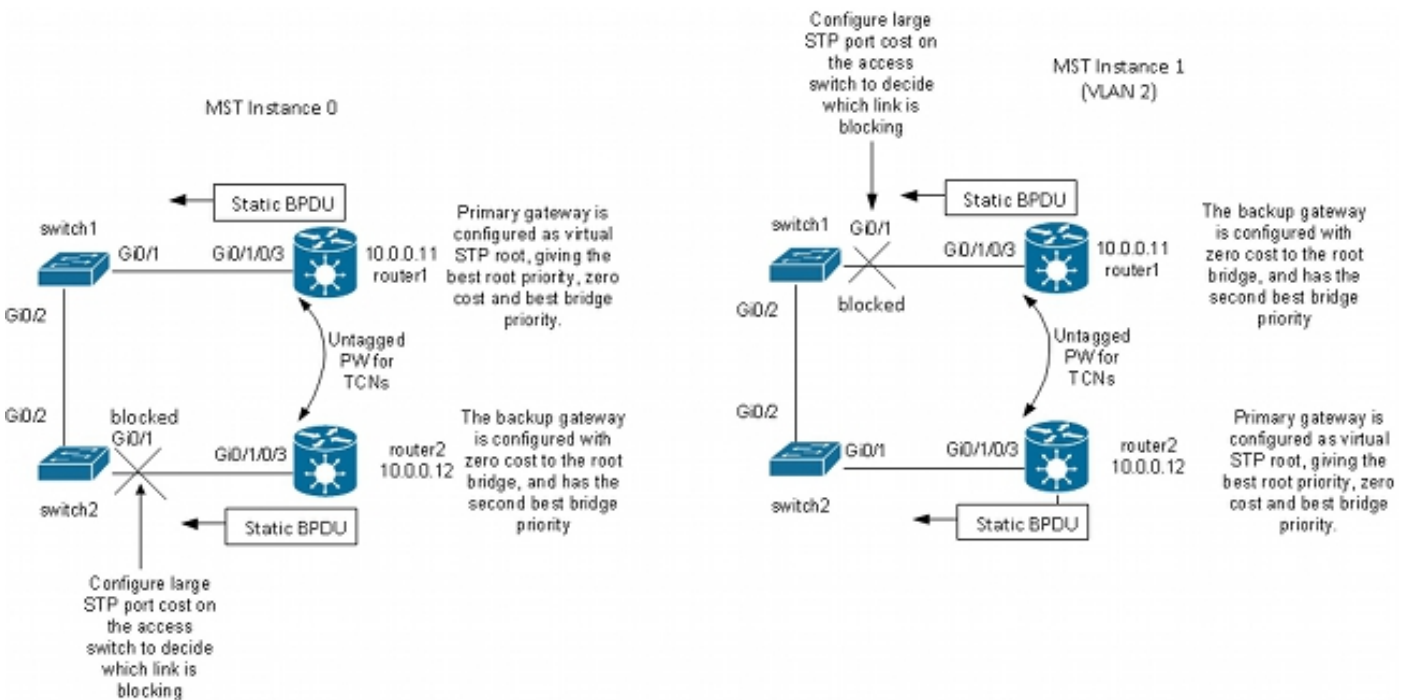
4.4.7.2메가와트

스패닝 트리 섹션에서 설명한 것처럼 MST는 태그되지 않은 BPDU를 전송하지만, 이러한 BPDU는 인터페이스에 있는 모든 VLAN의 포워딩 상태를 제어합니다.

VLAN은 여러 인스턴스로 그룹화될 수 있으며, 각 인스턴스는 자체 포워딩 상태를 갖습니다.

VLAN은 일반적으로 트래픽이 여러 경로 간에 균등하게 분산될 수 있도록 그룹화됩니다. 경로가 2개인 경우 트래픽의 절반은 첫 번째 경로에서 포워딩하고 두 번째 경로에서 차단하는 인스턴스에 속합니다. 트래픽의 나머지 절반은 첫 번째 경로에서 차단하고 두 번째 경로에서 포워딩하는 인스턴스에 속합니다. 따라서 안정적인 조건에서 두 경로 간의 로드 밸런싱이 가능합니다. 그렇지 않으면 일반적으로 완전히 차단되고 기본 경로가 중단된 경우에만 활성화되는 하나의 경로가 있습니다.

다음은 일반적인 MSTAG 토폴로지입니다.



이 실습 예에서는 인스턴스 1에 VLAN 2가 있고 인스턴스 0에 다른 VLAN이 있습니다. (좀 더 현실적인 시나리오에서는 VLAN이 여러 인스턴스 간에 분산되어 인스턴스 간의 트래픽 로드 밸런싱을 원활하게 수행할 수 있도록 합니다.) 일부 VLAN은 다른 VLAN보다 훨씬 많은 트래픽을 가지므로 각 인스턴스에 항상 같은 수의 VLAN이 있는 것은 아닙니다.

다음은 MST 인스턴스 0의 컨피그레이션입니다.

- 라우터1과 라우터2는 MSTAG 컨피그레이션을 기반으로 일부 고정 BPDU를 전송합니다. 이들은 네트워크에서 들어오는 BPDU를 처리하지 않거나 전체 구현을 실행하려고 하지 않습니다.

MSTAG에서는 두 L2VPN PE가 MSTAG 컨피그레이션에 따라 고정 BPDU만 전송합니다.

- Router1은 해당 인스턴스의 루트로 간주되어 인스턴스 0의 트래픽을 끌어오기 위해 구성됩니다.
- 라우터2는 라우터1에 장애가 발생하거나 스위치1과 라우터1 간의 AC 장애가 발생할 경우 새로운 루트가 되도록 인스턴스 0의 두 번째 최상의 루트 우선 순위로 구성됩니다.
- Switch2는 루트에 대한 기본 경로가 switch1 및 router1을 통해 Gig 0/2에 있는지 확인하기 위해 포트 Gi 0/1에서 router2로의 높은 스페닝 트리 비용으로 구성됩니다.
- Switch2는 Gi 0/2를 instance0의 루트 포트로 선택하고 루트가 손실된 경우 Gi 0/1을 대체 포트로 선택합니다.
- 따라서 인스턴스 0에 속하는 VLAN에 있는 해당 사이트의 트래픽은 router1을 통해 VPLS를 통해 다른 사이트에 도달합니다.

MST 인스턴스 1(VLAN 2)의 경우 컨피그레이션이 반전됩니다.

- Router2는 해당 인스턴스의 루트로 간주되어 인스턴스 1의 트래픽을 가져오도록 구성됩니다.
- 라우터1은 인스턴스 1의 두 번째 최상의 루트 우선 순위로 구성되므로 스위치2와 라우터2 간의 라우터2 장애 또는 AC 장애 시 새 루트가 됩니다.
- Switch1은 루트에 대한 기본 경로가 switch2 및 router2를 통해 Gig 0/2에 있도록 하기 위해 포트 Gi 0/1에서 router1로의 높은 스페닝 트리 비용으로 구성됩니다.
- Switch1은 인스턴스 1의 루트 포트로 Gi 0/2를 선택하고 루트가 손실된 경우 대체 포트로 Gi 0/1을 선택합니다.
- 따라서 인스턴스 1에 속하는 VLAN(이 예에서는 VLAN 2)에 있는 해당 사이트의 트래픽은 router2를 통해 VPLS를 통해 다른 사이트에 도달합니다.
- 태그가 지정되지 않은 TCN을 포착하여 포인트-투-포인트 PW를 통해 다른 라우터로 전달하려면 router1 및 router2에 하위 인터페이스가 있어야 합니다. 스위치1과 스위치2가 직접 링크를 잃고 서로 격리될 수 있으므로 라우터1과 라우터2는 포인트-투-포인트 PW를 통해 서로 간의 TCN을 전달해야 합니다.
- PE는 또한 TCN을 가로채고 mac-address-tables를 플러시하며 원격 PE에 LDP MAC 철회를 보냅니다.

라우터 1의 컨피그레이션입니다.

```
RP/0/RSP0/CPU0:router1#sh run int gigabitEthernet 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
```

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
```

```
!  
neighbor 10.0.0.13 pw-id 3  
!  
neighbor 10.0.0.14 pw-id 3  
!  
!  
bridge-domain engineering  
interface GigabitEthernet0/1/0/3.2  
!  
vfi customer1-engineering  
neighbor 10.0.0.12 pw-id 2  
!  
neighbor 10.0.0.13 pw-id 2  
!  
neighbor 10.0.0.14 pw-id 2  
!  
!  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router1#sh run l2vpn xconnect group customer1  
l2vpn  
xconnect group customer1  
p2p mstag-gi-0-1-0-3  
interface GigabitEthernet0/1/0/3.1  
neighbor 10.0.0.13 pw-id 103  
!  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router1#sh run spanning-tree mstag customer1-0-1-0-3  
spanning-tree mstag customer1-0-1-0-3  
interface GigabitEthernet0/1/0/3.1  
name customer1  
revision 1  
bridge-id 0000.0000.0001  
instance 0  
root-id 0000.0000.0001  
priority 4096  
root-priority 4096  
!  
instance 1  
vlan-ids 2  
root-id 0000.0000.0002  
priority 8192  
root-priority 4096  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router1#sh spanning-tree mstag customer1-0-1-0-3  
GigabitEthernet0/1/0/3.1  
Pre-empt delay is disabled  
Name: customer1  
Revision: 1  
Max Age: 20  
Provider Bridge: no  
Bridge ID: 0000.0000.0001  
Port ID: 1  
External Cost: 0  
Hello Time: 2
```

```
Active: yes
BPDUs sent: 3048
MSTI 0 (CIST):
VLAN IDs: 1,3-4094
Role: Designated
Bridge Priority: 4096
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0001
Root Priority: 4096
Topology Changes: 369
MSTI 1
VLAN IDs: 2
Role: Designated
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 322
```

이 컨피그레이션에서는 다음 사항에 유의하십시오.

- MST 인스턴스 0에서 루트 브리지는 router1의 브리지 ID인 0000.0000.0001입니다.
- MST 인스턴스 1에서 루트 브리지는 router2의 브리지 ID인 0000.0000.0002입니다.
- router1의 브리지 우선순위는 인스턴스 0의 경우 4096(루트가 됨)이고 인스턴스 1의 경우 8192(차상위 루트가 됨)입니다.
- router1의 브리지 우선순위는 인스턴스 0의 경우 8192이고(차상위 루트가 됨) 인스턴스 1의 경우 4096입니다(루트가 됨).
- GigabitEthernet0/1/0/3.1의 포인트-투-포인트 교차 연결에서는 태그가 지정되지 않은 MST TCN을 다른 라우터로 전달합니다.

아직 MST로 마이그레이션되지 않은 다른 사이트에서 전송할 수 있는 VLAN별 BPDU를 삭제하기 위해 dot1q 하위 인터페이스에 이그레스 ACL이 구성되었습니다. 이 컨피그레이션은 MST용으로 구성된 인터페이스에서 VLAN별 BPDU를 수신할 때 CE 스위치에서 인터페이스가 일관성이 없다고 선언하는 것을 방지합니다.

router2의 컨피그레이션은 다음과 매우 유사합니다.

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!

RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
```

```
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
```

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p mstag-gi-0-1-0-3
interface GigabitEthernet0/1/0/3.1
neighbor 10.0.0.13 pw-id 103
!
!
!
!
```

```
RP/0/RSP0/CPU0:router2#sh run spanning-tree mstag customer1-0-1-0-3
spanning-tree mstag customer1-0-1-0-3
interface GigabitEthernet0/1/0/3.1
name customer1
revision 1
bridge-id 0000.0000.0002
instance 0
root-id 0000.0000.0001
priority 8192
root-priority 4096
!
instance 1
vlan-ids 2
root-id 0000.0000.0002
priority 4096
root-priority 4096
!
!
!
```

```
RP/0/RSP0/CPU0:router2#sh spanning-tree mstag customer1-0-1-0-3
GigabitEthernet0/1/0/3.1
Pre-empt delay is disabled
Name: customer1
Revision: 1
Max Age: 20
Provider Bridge: no
Bridge ID: 0000.0000.0002
Port ID: 1
```

External Cost: 0
Hello Time: 2
Active: yes
BPDUs sent: 3186
MSTI 0 (CIST):
VLAN IDs: 1,3-4094
Role: Designated
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0001
Root Priority: 4096
Topology Changes: 365
MSTI 1
VLAN IDs: 2
Role: Designated
Bridge Priority: 4096
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 177

스위치 1의 기본 컨피그레이션입니다.

```
switch1#sh run | b spanning-tree
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
switch1#sh run int gig 0/1 | i spanning
spanning-tree mst 1 cost 100000
```

```
switch1#sh spanning-tree
```

```
MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

```
MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 40000
```

```
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Gi0/1 Altn BLK 100000 128.1 P2p
Gi0/2 Root FWD 20000 128.2 P2p
```

따라서 인스턴스 0의 트래픽은 router1을 통해 전달되고 인스턴스 1의 트래픽은 switch2 및 router2를 통해 전달됩니다.

switch2의 컨피그레이션에서는 switch1과 동일한 명령을 사용합니다.

```
switch2#sh run | b spanning
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
switch2#sh run int gig 0/1 | i spanning
spanning-tree mst 0 cost 100000
```

```
switch2#sh spanning-tree
```

```
MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Gi0/1 Altn BLK 100000 128.1 P2p
Gi0/2 Root FWD 20000 128.2 P2p
```

```
MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 20000
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Gi0/1 Root FWD 20000 128.1 P2p
```

```
Gi0/2 Desg FWD 20000 128.2 P2p
```

Switch2는 switch1 및 router1(예: 0)을, router2(예: 1)를 거칩니다.

한 인스턴스는 router1을 통해 사이트를 나가고 다른 인스턴스는 router2를 통해 사이트를 나가기 때문에 트래픽이 로드 밸런싱됩니다.

router1과 switch1 간의 링크가 다운되면 두 인스턴스 모두 router2를 통해 이동합니다.

```
switch1#sh spanning-tree
```

```
MST0
```

```
Spanning tree enabled protocol mstp
```

```
Root ID Priority 4096
```

```
Address 0000.0000.0001
```

```
Cost 0
```

```
Port 2 (GigabitEthernet0/2)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
```

```
Address 0019.552b.b580
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Gi0/2 Root FWD 20000 128.2 P2p
```

```
MST1
```

```
Spanning tree enabled protocol mstp
```

```
Root ID Priority 4097
```

```
Address 0000.0000.0002
```

```
Cost 40000
```

```
Port 2 (GigabitEthernet0/2)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
```

```
Address 0019.552b.b580
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Gi0/2 Root FWD 20000 128.2 P2p
```

```
switch2#sh spanning-tree
```

```
MST0
```

```
Spanning tree enabled protocol mstp
```

```
Root ID Priority 4096
```

```
Address 0000.0000.0001
```

```
Cost 0
```

```
Port 1 (GigabitEthernet0/1)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
```

```
Address 0024.985e.6a00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```

Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Root FWD 100000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p

```

```

MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 20000
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```

```

Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p

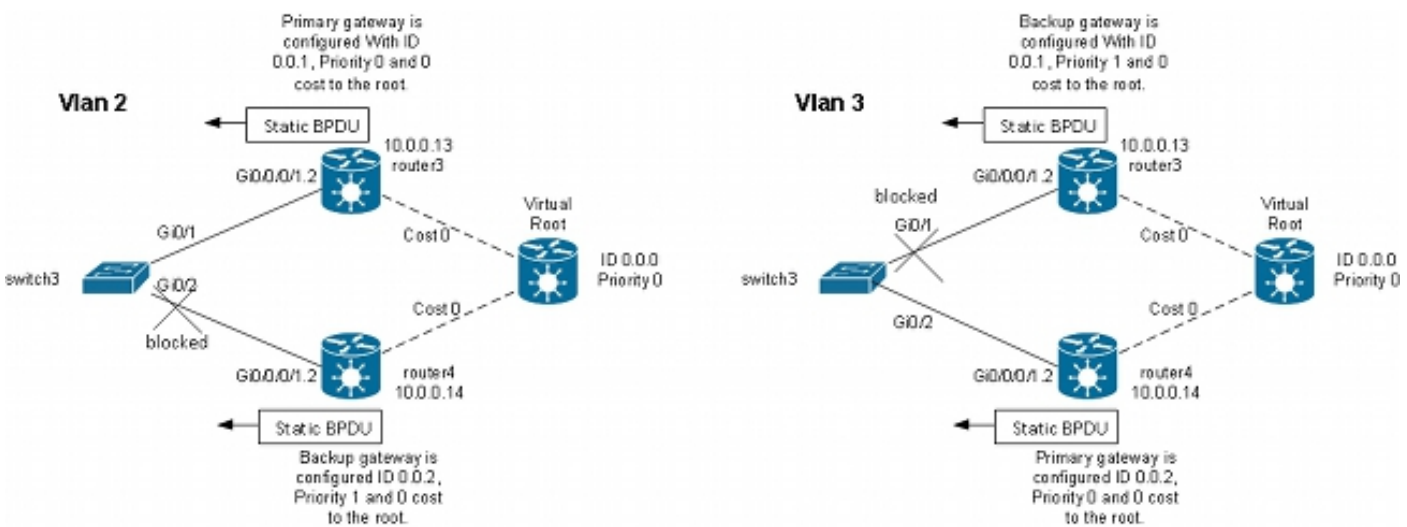
```

차상위 루트를 통과하는 경로가 이미 대체 경로로 선택되었기 때문에 이러한 유형의 장애에 신속한 컨버전스를 구현할 수 있습니다. MSTAG에서는 MST BPDU가 VPLS를 통해 전송되지 않으므로 사이트가 다른 사이트의 불안정성과 격리됩니다.

4.4.7.3 PVSTAG 또는 PVRSTAG

MSTAG는 고속 스페닝 트리를 사용하며 각 VLAN의 BPDU가 아닌 인스턴스를 사용하여 확장 가능하기 때문에 VPLS에서 선호하는 액세스 게이트웨이 프로토콜입니다.

사이트를 MST로 마이그레이션할 수 없고 PVST+ 또는 PVRST를 계속 실행하는 것만이 해결책인 경우 PVSTAG 또는 PVRSTAG를 사용할 수 있지만 구현은 하나의 특정 토폴로지로 제한됩니다.



이 토폴로지에서는 CE 스위치가 하나만 있을 수 있다는 점이 가장 중요합니다. MSTAG 토폴로지에서와 같이 두 개의 스위치를 가질 수 없습니다. MSTAG에서는 사이트가 두 부분으로 분할된 경우 태그가 지정되지 않은 트래픽(BPDU TCN 포함)을 한 PE에서 다른 PE로 전송하기 위해 포인트-투-포인트 PW를 구성할 수 있습니다. PVST 및 PVRST를 사용하면 TCN에 태그가 지정되어 VPLS를

통해 전송할 데이터 트래픽과 동일한 하위 인터페이스와 일치합니다. 라우터는 TCN을 다른 쪽에 전달하기 위해 MAC 주소 및 프로토콜 유형에 따라 BPDU를 식별해야 합니다. 현재 지원되지 않으므로 CE 디바이스를 하나만 보유해야 합니다.

Cisco IOS XR 소프트웨어 릴리스 4.3.0 이전 릴리스의 또 다른 요구 사항은 번들 인터페이스를 AC로 사용할 수 없다는 것입니다. Cisco IOS XR 소프트웨어 릴리스 4.3.0에서는 이러한 제한이 해제되었습니다.

그 원리는 MSTAG와 매우 비슷하다. PVSTAG 라우터는 CE가 비용 0으로 (가상) 루트에 직접 연결된 스위치에 연결된 것처럼 보이도록 고정 BPDU를 전송합니다. 트래픽의 로드 밸런싱을 위해 일부 VLAN은 router3의 루트로 구성하고 다른 VLAN은 router4의 루트로 구성할 수 있습니다.

다음은 라우터3의 컨피그레이션 예입니다.

```
RP/0/RSP1/CPU0:router3#sh run int gigabitEthernet 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP1/CPU0:router3#sh run spanning-tree pvstag customer1-0-0-0-1
spanning-tree pvstag customer1-0-0-0-1
interface GigabitEthernet0/0/0/1
vlan 2
root-priority 0
root-id 0000.0000.0000
```

```
root-cost 0
priority 0
bridge-id 0000.0000.0001
!
vlan 3
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 1
bridge-id 0000.0000.0001
!
!
!
```

```
RP/0/RSP1/CPU0:router3#sh spanning-tree pvstag customer1-0-0-0-1
GigabitEthernet0/0/0/1
```

```
VLAN 2
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
```

```
VLAN 3
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
```

다음은 라우터 4의 컨피그레이션 예입니다.

```
RP/0/RSP1/CPU0:router4#sh run int gig 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP1/CPU0:router4#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
```

```
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
```

```
RP/0/RSP1/CPU0:router4#sh run spanning-tree pvstag customer1-0-0-0-1
spanning-tree pvstag customer1-0-0-0-1
interface GigabitEthernet0/0/0/1
vlan 2
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 1
bridge-id 0000.0000.0002
!
vlan 3
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 0
bridge-id 0000.0000.0002
!
!
!
```

```
RP/0/RSP1/CPU0:router4#sh spanning-tree pvstag customer1-0-0-0-1
GigabitEthernet0/0/0/1
VLAN 2
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0002
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202799
Topology Changes: 0
VLAN 3
```

```
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0002
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202799
Topology Changes: 0
```

다음은 CE 스위치3의 구성 예입니다.

```
switch3#sh spanning-tree vlan 2
```

```
VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 0000.0000.0000
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Gi0/1 Root FWD 4 128.1 P2p
Gi0/2 Altn BLK 4 128.2 P2p
```

```
switch3#sh spanning-tree vlan 3
```

```
VLAN0003
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 0000.0000.0000
Cost 4
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32771 (priority 32768 sys-id-ext 3)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Gi0/1 Altn BLK 4 128.1 P2p
Gi0/2 Root FWD 4 128.2 P2p
```

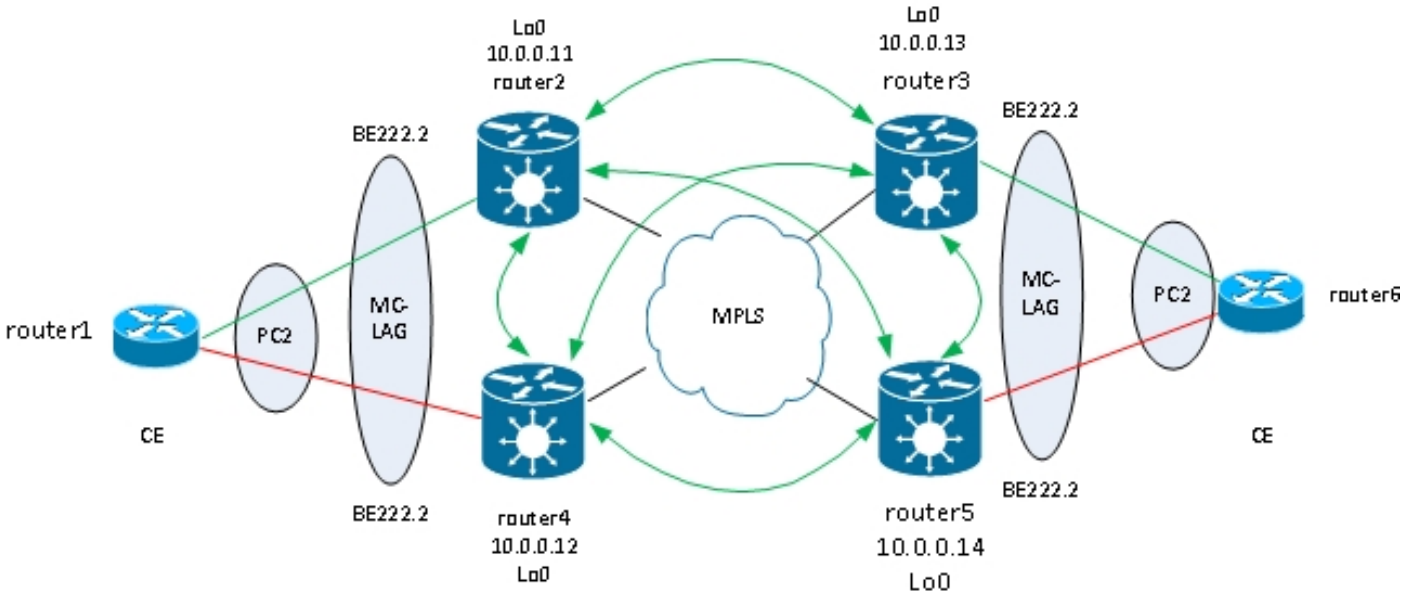
PVSTAG에 대한 구성은 MSTAG와 매우 유사하지만, MSTAG 예에서 기본 게이트웨이의 루트 우선 순위와 우선 순위가 4096으로 구성되고 백업 게이트웨이의 우선 순위가 8192로 구성된다는 점이 다릅니다.

도메인의 다른 모든 스위치는 PVSTAG 또는 PVRSTAG에 구성된 스위치보다 우선순위가 더 높아야 합니다.

어떤 포트가 루트 포트가 되고 어떤 포트가 차단되는지 영향을 주기 위해 CE 스위치에서 인터페이스 비용을 조정할 수 있습니다.

4.4.7.4 MC-LAG

VPLS를 사용하는 MC-LAG 컨피그레이션은 양방향 PW 이중화를 사용하는 포인트투포인트 PW보다 간단합니다. 기본 PW 하나와 대기 PW 세 개 대신 PE는 VPLS에서 표준인 VPLS PW의 전체 메시지만 필요합니다.



이 토폴로지에서는 다음 사항에 유의하십시오.

- MC-LAG는 왼쪽의 두 VPLS PE(router2 및 router4) 사이에서 실행됩니다.
- 정상 상태에서 번들 멤버는 router1과 router2 사이에서 활성 상태이고 router1과 router4 사이에서 대기 상태입니다.
- Router2에는 VPLS 브리지 도메인에 구성된 번들 하위 인터페이스가 있으므로 router2는 트래픽을 원격 VPLS PE로 전달합니다. 토폴로지 다이어그램에는 두 개의 사이트가 나와 있지만 더 많은 사이트가 있을 수 있습니다.
- 원격 PE는 라우터1의 MAC 주소와 라우터2를 통한 디바이스 뒤의 MAC 주소를 학습하므로, PE는 라우터2를 통해 이러한 대상 MAC 주소에 대한 트래픽을 전달합니다.
- router1과 router2 간의 링크가 다운되거나 router2가 다운되면 router1과 router4 간의 번들 멤버가 활성화됩니다.
- 라우터 2와 마찬가지로 router4는 VPLS 브리지 도메인 아래에 번들 하위 인터페이스가 구성되어 있습니다.
- 번들 하위 인터페이스가 router4에 나타나면 router4는 원격 VPLS PE에 LDP MAC 회수 메시지를 보내 토폴로지 변경이 있음을 알립니다.

라우터3의 컨피그레이션입니다.

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
```

```
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!
```

```
RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!
```

```
RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222.*
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
```

!
!
!

MC-LAG 번들이 구성되면 다른 AC와 마찬가지로 VPLS 컨피그레이션 아래에 추가합니다.

라우터5의 해당 컨피그레이션입니다.

```
RP/0/RSP1/CPU0:router5#sh run redundancy
redundancy
iccp
group 2
mlacp node 2
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.13
!
backbone
interface TenGigE0/1/0/0
interface TenGigE0/1/0/1
!
isolation recovery-delay 300
!
!
!
```

```
RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222
interface Bundle-Ether222
lACP switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!
```

```
RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222.*
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP1/CPU0:router5#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
```

```

!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!
!
!

```

정상적인 상황에서는 router3과 router6 간의 번들 멤버가 활성 상태이고 router5와 router6 간의 멤버가 대기 상태입니다.

```
RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222
```

```

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

```

```
Port Device State Port ID B/W, kbps
```

```

-----
Gi0/0/0/1 Local Active 0x0001, 0x9001 1000000
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8000, 0xa002 1000000
Link is marked as Standby by mLACP peer
RP/0/RSP1/CPU0:router3#

```

```

router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

```


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports

-----+-----+-----+-----
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)

router6#

CE의 트래픽은 라우터3에서 수신되어 원격 PE로 전달됩니다.

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 4, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

```
RP/0/RSP1/CPU0:router3#sh l2vpn forwarding bridge-domain customer1:
engineering mac location 0/0/CPU0
```

To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to

```
-----  
001d.4603.1f01 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f42 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A  
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

마지막 명령은 router3이 해당 번들에서 일부 MAC 주소를 학습하고 있으며 활성 멤버가 router3에 있음을 보여줍니다. 라우터 5에서는 로컬 멤버가 대기 상태이므로 번들을 통해 학습된 MAC 주소가 없습니다.

```
RP/0/RSP1/CPU0:router5#sh l2vpn forwarding bridge-domain customer1:engineering
mac location 0/0/CPU0
```

To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to

```
-----  
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f01 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

router3과 router6 간의 번들 멤버가 다운되면 라우터5에서 번들 멤버가 활성화됩니다. MC-LAG VPLS PE는 원격 PE가 mac 주소 테이블을 삭제하고 새로운 활성 MC-LAG PE 라우터5를 통해 MAC 주소를 학습할 수 있도록 LDP MAC 탈퇴 메시지를 전송합니다.

활성 MC-LAG 번들 멤버가 router3에서 router5로 이동할 때 Router2는 router3 및 router5로부터 MAC 회수 메시지를 수신합니다.

```
RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1 detail |  
i "state is|withd|bridge-domain"  
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,  
ShgId: 0, MSTi: 0  
MAC withdraw: enabled  
MAC withdraw for Access PW: enabled  
MAC withdraw sent on bridge port down: disabled  
AC: GigabitEthernet0/1/0/3.3, state is up  
PW: neighbor 10.0.0.12, PW ID 3, state is up ( established )  
MAC withdraw message: send 0 receive 0  
PW: neighbor 10.0.0.13, PW ID 3, state is up ( established )  
MAC withdraw message: send 0 receive 1  
PW: neighbor 10.0.0.14, PW ID 3, state is up ( established )  
MAC withdraw message: send 0 receive 1  
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,  
ShgId: 0, MSTi: 0  
MAC withdraw: enabled  
MAC withdraw for Access PW: enabled  
MAC withdraw sent on bridge port down: disabled  
AC: GigabitEthernet0/0/0/1.2, state is unresolved  
AC: GigabitEthernet0/1/0/3.2, state is up  
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )  
MAC withdraw message: send 2 receive 0  
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )  
MAC withdraw message: send 0 receive 0  
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )  
MAC withdraw message: send 0 receive 1  
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )  
MAC withdraw message: send 0 receive 1
```

router2의 MAC 주소가 router3(10.0.0.13)에서 router5(10.0.0.14)로 이동합니다.

```
RP/0/RSP0/CPU0:router2#sh l2vpn forwarding bridge-domain customer1:  
engineering mac-address location 0/0/CPU0  
To Resynchronize MAC table from the Network Processors, use the command...  
l2vpn resynchronize forwarding mac-address-table location
```

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to

```
-----  
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A  
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f02 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f42 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

MC-LAG를 사용하면 사이트에서 단일 번들을 사용하여 VPLS를 통해 다른 사이트에 연결할 수 있습니다. MC-LAG는 링크 및 PE 이중화를 제공하지만 논리적으로 보면 여전히 하나의 번들 인터페이스로 다른 사이트에 연결할 수 있습니다. 해당 번들에는 스페닝 트리가 필요하지 않으며, VPLS를

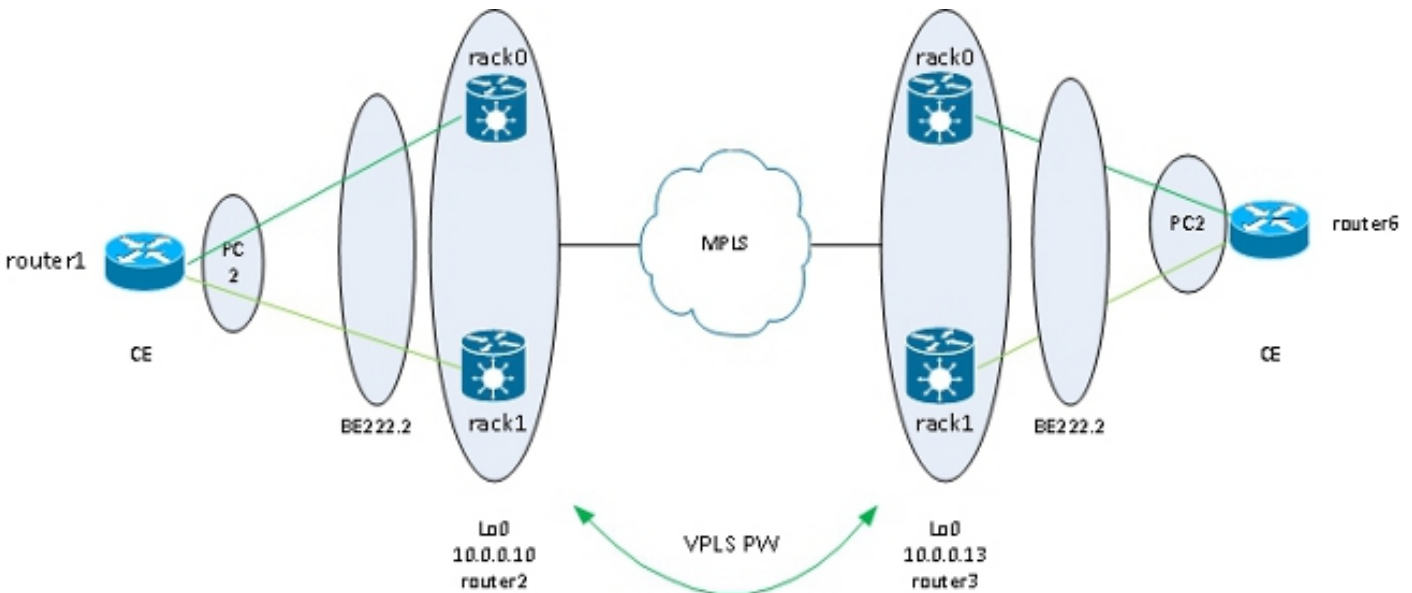
통해 사이트 간에 BPDU가 교환되지 않도록 CE에 BPDU 필터를 구성할 수 있습니다.

또 다른 옵션은 사이트 간에 BPDU가 전송되지 않도록 BPDU의 대상 MAC 주소를 삭제하기 위해 번들에 있는 AC에 이더넷 서비스 액세스 목록을 구성하는 것입니다. 그러나 사이트 간에 백도어 링크가 도입되면 스페닝 트리가 MC-LAG 번들에서 실행되고 있지 않으므로 루프를 끊을 수 없습니다. 따라서 MC-LAG 번들에서 스페닝 트리를 비활성화할지 신중하게 평가합니다. 사이트 간 토폴로지를 신중하게 유지하면 스페닝 트리가 필요 없이 MC-LAG를 통해 이중화를 구현하는 것이 좋습니다.

4.4.7.5 ASR 9000 nV 에지 클러스터

MC-LAG 솔루션은 스페닝 트리를 사용할 필요 없이 이중화를 제공했습니다. 한 가지 단점은 하나의 MC-LAG PE에 대한 번들 멤버가 대기 상태이므로 링크 사용량을 최대화하지 않는 액티브-스탠바이 솔루션입니다.

또 다른 설계 옵션은 CE가 동시에 활성화되는 각 클러스터 랙에 번들 멤버를 포함할 수 있도록 ASR 9000 nV Edge 클러스터를 사용하는 것입니다.



이 솔루션의 또 다른 이점은 각 사이트의 각 클러스터에 대해 클러스터당 하나의 PW만 존재하기 때문에 PW의 수가 감소된다는 것입니다. 사이트당 2개의 PE가 있는 경우 각 PE는 각 사이트에서 2개의 PE에 대한 PW를 가져야 합니다.

구성이 단순해지는 것도 장점입니다. 컨피그레이션은 번들 AC 및 VFI PW가 있는 브리지 도메인을 사용하는 매우 기본적인 VPLS 컨피그레이션처럼 보입니다.

```
RP/1/RSP0/CPU0:router2#sh bundle bundle-ether 222
```

```
Bundle-Ether222
Status: Up
Local links : 2 / 0 / 2
Local bandwidth : 20000000 (20000000) kbps
MAC address (source): 0024.f71e.d309 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 64
Wait while timer: 2000 ms
Load balancing: Default
LACP: Not operational
```

Flap suppression timer: Off
Cisco extensions: Disabled
mLACP: Not configured
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps

Te0/0/0/8 Local Active 0x8000, 0x0005 10000000

Link is Active

Te1/0/0/8 Local Active 0x8000, 0x0001 10000000

Link is Active

```
RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.2
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.3
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
```

```
RP/1/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
```

```
RP/1/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1
```

Legend: pp = Partially Programmed.

Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0

Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog

Filter MAC addresses: 0

```
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
```

```
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
```

```
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

번들 AC 듀얼 홈(dual homed)을 통해 2개의 랙에 이중화가 제공되므로, 번들 구성 요소에 장애가 발생하거나 랙에 장애가 발생할 경우에도 번들이 계속 작동합니다.

사이트가 클러스터를 통해서만 VPLS 도메인에 연결되는 경우, 토폴로지는 스페닝 트리와 관련하여 MC-LAG와 유사합니다. 따라서 해당 번들에는 스페닝 트리가 필요하지 않으며, VPLS를 통해 사이트 간에 BPDU가 교환되지 않도록 CE에 BPDU 필터를 구성할 수 있습니다.

또 다른 옵션은 사이트 간에 BPDU가 전송되지 않도록 BPDU의 대상 MAC 주소를 삭제하기 위해 번들에 있는 AC에 이더넷 서비스 액세스 목록을 구성하는 것입니다. 그러나 사이트 간에 백도어 링크가 도입되면 스페닝 트리가 CE-PE 번들에서 실행되지 않으므로 루프를 끊을 수 없습니다. 따라서 해당 CE-PE 번들에서 스페닝 트리를 비활성화할지 신중하게 평가합니다. 사이트 간 토폴로지를 신중하게 유지하면 스페닝 트리가 필요 없이 클러스터를 통해 이중화를 수행하는 것이 좋습니다.

4.4.7.6 ICCP-SM(ICCP-Based Service Multi-Homing)(PMCLAG(Pseudo MCLAG) 및 액티브/액티브)

MC-LAG의 한계를 극복하기 위해 버전 4.3.1에 새로운 기능이 도입되었습니다. 일부 번들 링크는 대기 모드에 남아 있으므로 사용되지 않습니다. Pseudo MCLAG라는 새로운 기능에서 DHD에서 PoA(Points of Attachments)까지의 모든 링크가 사용 중이지만 VLAN은 서로 다른 번들 간에 분할됩니다.

ICCP-SM (Pseudo MCLAG)

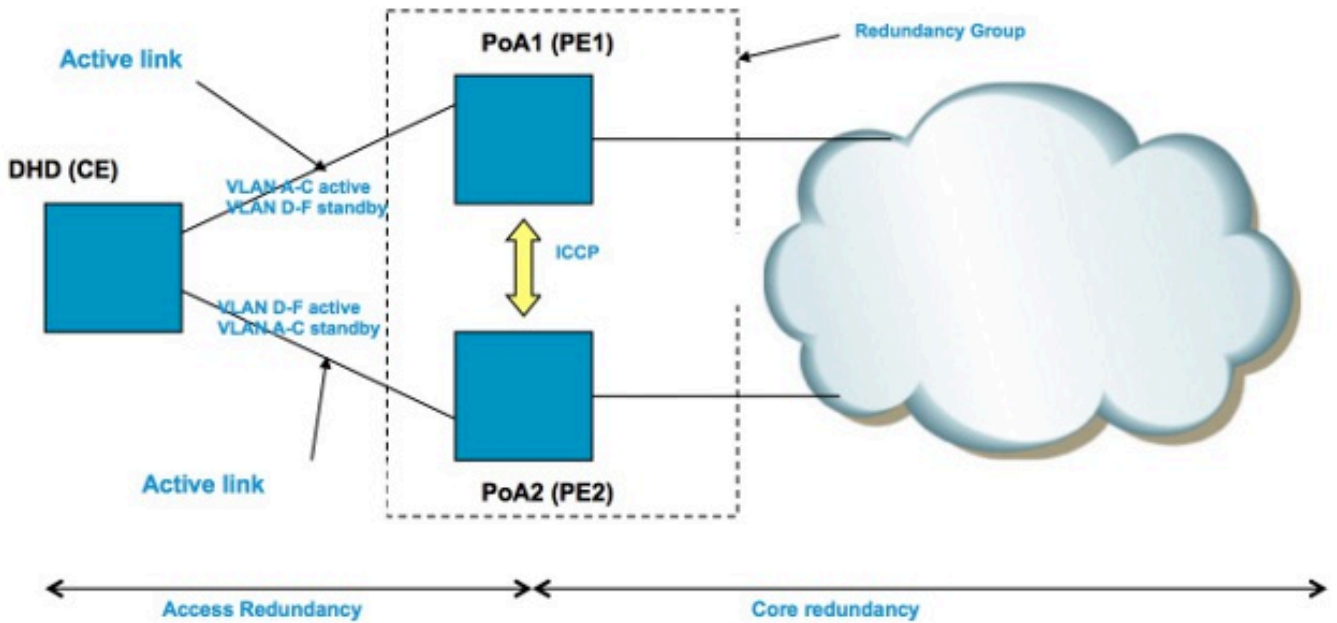


Figure 2 Pseudo MCLAG

DHD has two separate bundles – one to PoA1 and the other to PoA2.
Both bundles are active for some VLANs and standby for others.
Active VLANs on one bundle = standby VLANs for other bundle.
PoAs communicate over ICCP.
Only VPLS is supported in core (first release.)

4.5 트래픽 스톰 제어

L2 브로드캐스트 도메인에서는 호스트가 잘못 행동하여 브리지 도메인의 모든 영역에 플러딩되어야 하는 높은 비율의 브로드캐스트 또는 멀티캐스트 프레임을 전송할 위험이 있습니다. 또 다른 위험은 L2 루프(스패닝 트리에 의해 중단되지 않음)를 생성하는 것이며, 이로 인해 브로드캐스트 및 멀티캐스트 패킷이 반복됩니다. 브로드캐스트 및 멀티캐스트 패킷의 비율이 높으면 브로드캐스트 도메인의 호스트 성능에 영향을 미칩니다.

네트워크의 스위칭 디바이스의 성능은 브리지 도메인의 여러 이그레스 포트에 대한 하나의 입력 프레임(브로드캐스트, 멀티캐스트 또는 알 수 없는 유니캐스트 프레임)의 복제에 의해서도 영향을 받을 수 있습니다. 패킷을 복제해야 하는 디바이스 내부의 위치에 따라, 동일한 패킷의 여러 복사본을 만드는 데 리소스를 많이 사용할 수 있습니다. 예를 들어, 패브릭의 멀티캐스트 복제 기능 때문에 서로 다른 여러 슬롯에 브로드캐스트를 복제하는 것은 문제가 되지 않습니다. 네트워크 프로세서가 처리하는 일부 포트에서 전송할 동일 패킷의 여러 사본을 생성해야 할 경우 네트워크 프로세서의 성능에 영향을 미칠 수 있습니다.

스톰 시 디바이스를 보호하기 위해 트래픽 스톰 제어 기능을 사용하면 브리지 도메인 AC에서 허용되는 브로드캐스트, 멀티캐스트 및 알 수 없는 유니캐스트의 최대 속도를 구성할 수 있습니다. 자세한 내용은 [Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide, Release 4.3.x: Implementing Traffic Storm Control under a VPLS Bridge](#)를 참조하십시오.

트래픽 스톰 제어는 번들 AC 인터페이스 또는 VFI PW에서는 지원되지 않지만, 비번들 AC 및 액세스 PW에서는 지원됩니다. 이 기능은 기본적으로 비활성화되어 있습니다. 스톰 제어를 설정하지 않는 한 브로드캐스트, 멀티캐스트 및 알 수 없는 유니캐스트의 모든 속도를 허용합니다.

다음은 컨피그레이션의 예입니다.

```
RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
neighbor 10.0.0.15 pw-id 15
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
vfi customer1-engineering
neighbor 10.0.0.10 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1w1d ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 5 (5 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
```

```
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
```

Storm Control:

```
Broadcast: enabled(1000)
Multicast: enabled(10000)
Unknown unicast: enabled(10000)
```

Static MAC addresses:

Statistics:

```
packets: received 251295, sent 3555258
bytes: received 18590814, sent 317984884
```

Storm control drop counters:

```
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
```

Dynamic ARP inspection drop counters:

```
packets: 0, bytes: 0
```

IP source guard drop counters:

```
packets: 0, bytes: 0
```

<snip>

스톰 제어 삭제 카운터는 항상 **show l2vpn bridge-domain detail** 명령의 출력에 있습니다. 이 기능은 기본적으로 비활성화되어 있으므로 기능이 구성된 경우에만 카운터에서 삭제를 보고하기 시작합니다.

구성된 속도는 한 네트워크에서 다른 네트워크로의 트래픽 패턴에 따라 달라질 수 있습니다. Cisco에서는 속도를 구성하기 전에 일반적인 상황에서는 브로드캐스트, 멀티캐스트 또는 알 수 없는 유니캐스트 프레임의 속도를 이해하는 것이 좋습니다. 그런 다음 구성된 속도의 마진을 일반 속도보다 높게 추가합니다.

4.6 MAC 이동

인터페이스 플랩과 같이 네트워크가 불안정한 경우 새 인터페이스에서 MAC 주소를 학습할 수 있습니다. 이는 정상적인 네트워크 컨버전스이며 mac-address-table이 동적으로 업데이트됩니다.

그러나 지속적인 MAC 이동은 L2 루프 중에 심각한 불안정과 같은 네트워크 불안정을 나타내는 경우가 많습니다. MAC 주소 보안 기능을 사용하면 MAC 이동을 보고하고 위반 포트를 종료하는 등의 시정 조치를 취할 수 있습니다.

해결 조치가 구성되지 않은 경우에도 MAC 이동 메시지를 통해 네트워크 불안정에 대한 알림을 받도록 logging 명령을 구성할 수 있습니다.

```
l2vpn
bridge group customer1
bridge-domain engineering
mac
```



```
secure
action none
logging
!
```

이 예에서는 작업이 none으로 구성되므로 MAC 이동이 탐지될 때 syslog 메시지가 로깅되는 경우를 제외하고는 아무 작업도 수행되지 않습니다. 다음은 예제 메시지입니다.

```
LC/0/0/CPU0:Dec 13 13:38:23.396 : l2fib[239]:
%L2-L2FIB-5-SECURITY_MAC_SECURE_VIOLATION_AC : MAC secure in AC
GigabitEthernet0_0_0_4.1310 detected violated packet - source MAC:
0000.0000.0001, destination MAC: 0000.0001.0001; action: none
```

4.7 IGMP 및 MLD 스누핑

기본적으로 멀티캐스트 프레임은 브리지 도메인의 모든 포트에 플러딩됩니다. IP TV(IPTV) 서비스와 같은 고속 스트림을 사용할 경우 모든 포트에서 상당한 양의 트래픽이 전달되고 여러 PW를 통해 복제될 수 있습니다. 모든 TV 스트림이 하나의 인터페이스를 통해 전달되는 경우 포트가 혼잡해질 수 있습니다. 유일한 옵션은 IGMP 또는 MLD 스누핑과 같은 기능의 컨피그레이션이며, 이 기능은 적절한 경우에만 포트와 멀티캐스트 라우터를 추적하고 포트의 스트림을 포워딩하기 위해 멀티캐스트 제어 패킷을 인터셉트합니다.

이러한 기능에 대한 자세한 내용은 [Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide, Release 4.3.x](#)를 참조하십시오.

5. 추가 L2VPN 항목

참고:

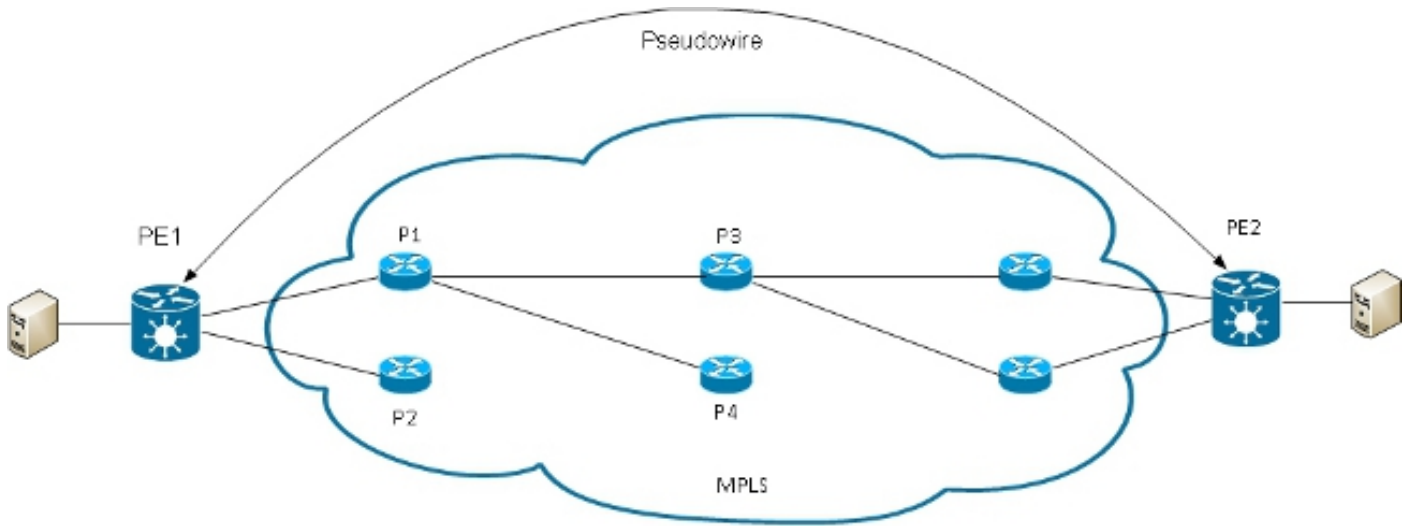
이 섹션에 사용된 명령에 대한 자세한 내용을 가져오려면 [명령 조회 툴\(등록 고객 전용\)](#)을 사용하십시오.

[아웃풋 인터프리터 툴\(등록 고객 전용\)](#)은 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

5.1 로드 밸런싱

L2VPN PE가 MPLS PW를 통해 프레임을 전송해야 하는 경우 이더넷 프레임은 하나 이상의 MPLS 레이블을 사용하여 MPLS 프레임으로 캡슐화됩니다. 원격 PE에 연결하기 위해 하나 이상의 PW 레이블과 IGP 레이블이 있을 수 있습니다.

MPLS 프레임은 MPLS 네트워크에 의해 원격 L2VPN PE로 전송됩니다. 일반적으로 대상 PE에 도달하기 위한 여러 경로가 있습니다.



참고: 일부 링크는 이 다이어그램에 표시되지 않습니다.

PE1은 PE2를 향하는 첫 번째 MPLS P 라우터로 P1과 P2 중에서 선택할 수 있습니다. P1이 선택되면, PE1은 P3과 P4 사이에서 선택하는 등. 사용 가능한 경로는 IGP 토폴로지 및 MPLS TE 터널 경로를 기반으로 합니다.

MPLS 통신 사업자는 활용률이 낮은 다른 링크와 함께 혼잡한 링크 하나보다는 모든 링크를 균등하게 활용하는 것을 선호합니다. 일부 PW는 다른 PW보다 훨씬 많은 트래픽을 전달하며 PW 트래픽이 사용하는 경로는 코어에서 사용되는 해싱 알고리즘에 의존하기 때문에 이 목표를 달성하기가 항상 쉬운 것은 아닙니다. 여러 개의 고대역폭 PW가 동일한 링크로 해시될 수 있으며, 이로 인해 혼잡이 발생합니다.

매우 중요한 요구 사항은 한 흐름의 모든 패킷이 동일한 경로를 따라야 한다는 것입니다. 그렇지 않으면 프레임 순서가 잘못되어 애플리케이션의 품질이나 성능에 영향을 줄 수 있습니다.

Cisco 라우터의 MPLS 네트워크에서의 로드 밸런싱은 일반적으로 맨 아래 MPLS 레이블에 따르는 데이터를 기반으로 합니다.

- 하단 레이블 바로 뒤의 데이터가 0x4 또는 0x6으로 시작하는 경우 MPLS P 라우터는 MPLS 패킷 내에 IPv4 또는 IPv6 패킷이 있다고 가정하고 프레임에서 추출된 소스 및 대상 IPv4 또는 IPv6 주소의 해시를 기반으로 로드 밸런싱을 시도합니다. 이론적으로 이는 대상 MAC 주소가 하단 레이블을 따르기 때문에 캡슐화되어 PW를 통해 전송되는 이더넷 프레임에는 적용되지 않습니다. 그러나 최근에 0x4 및 0x6으로 시작하는 일부 MAC 주소 범위가 할당되었습니다. MPLS P 라우터는 이더넷 헤더가 실제로 IPv4 헤더라고 잘못 간주하여 IPv4 소스 및 대상 주소라고 가정하는 내용에 따라 프레임을 해시할 수 있습니다. PW의 이더넷 프레임은 MPLS 코어의 서로 다른 경로를 통해 해시될 수 있으며, 이로 인해 PW 및 애플리케이션 품질 문제가 시퀀스가 잘못된 프레임으로 이어집니다. 해결책은 포인트-투-포인트 또는 VPLS PW에 연결할 수 있는 pw 클래스 아래에 제어 단어를 구성하는 것입니다. 제어 단어는 MPLS 레이블 바로 뒤에 삽입됩니다. 제어 단어는 0x4 또는 0x6로 시작하지 않으므로 문제가 발생하지 않습니다.

```
RP/1/RSP0/CPU0:router#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
pw-class control-word
encapsulation mpls
control-word
```

```

!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class control-word
!
<snip>
RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class control-word, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
-----
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----

```

- MPLS 레이블 스택의 맨 아래 바로 뒤에 있는 데이터가 0x4 또는 0x6으로 시작하지 않으면 P 라우터가 맨 아래 레이블을 기준으로 로드 밸런싱을 수행합니다. 한 PW의 모든 트래픽은 동일한 경로를 따르므로 무순서 패킷이 발생하지 않지만, 고대역폭 PW의 경우 일부 링크에서 혼잡이 발생할 수 있습니다. Cisco IOS XR 소프트웨어 릴리스 4.2.1에서 ASR 9000은 FAT(Flow Aware Transport) PW 기능을 지원합니다. 이 기능은 L2VPN PE에서 실행되며, 여기서 Point-to-Point 또는 VPLS PW의 두 끝 간에 협상됩니다. 인그레스 L2VPN PE는 AC 및 L2VPN 컨피그레이션의 플로우를 감지하고 MPLS 레이블 스택의 맨 아래에 있는 PW MPLS 레이블 아래에 새 MPLS 흐름 레이블을 삽입합니다. 인그레스 PE는 소스 및 목적지 MAC 주소(기본값) 또는 소스 및 목적지 IPv4 주소(구성 가능)를 기반으로 플로우를 탐지합니다. MAC 주소의 사용이 기본값입니다. IPv4 주소의 사용이 권장되지만 수동으로 구성해야 합니다.

FAT PW 기능을 사용하면 인그레스 L2VPN PE는 src-dst-mac 또는 src-dst-ip당 하단 MPLS 레이블 하나를 삽입합니다. MPLS P 라우터(PE 간)는 사용 가능한 경로를 통해 해시 프레임을 생성한 다음 MPLS 스택 하단의 FAT PW 흐름 레이블을 기준으로 대상 PE에 연결합니다. 이는 일반적으로 PW가 소수의 src-dst-mac 또는 src-dst-ip 대화만 전달하지 않는 한 코어에서 훨씬 뛰어난 대역폭 활용률을 제공합니다. Cisco에서는 흐름 레이블 바로 뒤에 0x4 및 0x6으로 시작하는 MAC 주소가 있는 것을 피하려면 제어 단어를 사용하는 것이 좋습니다. 이렇게 하면 해시가 흐름 레이블이 아닌 의사 IP 주소를 기반으로 올바르게 설정됩니다.

이 기능을 사용하면 하나의 PW에서 제공되는 트래픽이 사용 가능한 경우 코어의 여러 경로를 통해 로드 밸런싱됩니다. 동일한 소스(MAC 또는 IP)에서 동일한 목적지(MAC 또는 IP)로의 모든 트래픽이 동일한 경로를 따르므로 애플리케이션 트래픽은 무순서 패킷을 겪지 않습니다. 다음은 컨피그레이션을 보여주는 예입니다:

```
l2vpn
pw-class fat-pw
encapsulation mpls
control-word
load-balancing
flow-label both
!
!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class fat-pw
```

```
RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class fat-pw, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set
Load Balance Hashing: src-dst-ip
Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=1,Rx=1)
```

```
PW Status TLV in use
MPLS Local Remote
-----
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
```

5.2 로깅

L2VPN 컨피그레이션 모드에서 다른 유형의 로깅 메시지를 구성할 수 있습니다. L2VPN 이벤트에 대한 syslog 알림을 받으려면 l2vpn 로깅을 구성하고, PW 상태가 변경되는 시점을 확인하려면

logging pseudowire를 구성합니다.

```
l2vpn
logging
bridge-domain
pseudowire
nsr
!
```

많은 PW가 구성된 경우 메시지가 로그를 플러딩할 수 있습니다.

5.3 이더넷 서비스 액세스 목록

이더넷 서비스 액세스 목록을 사용하여 특정 호스트에서 트래픽을 삭제하거나 라우터가 l2transport 인터페이스의 호스트에서 패킷을 가져오는지 확인할 수 있습니다.

```
RP/0/RSP0/CPU0:router#sh run ethernet-services access-list count-packets
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3
20 permit any any
!
```

```
RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group count-packets egress
!
```

```
RP/0/RSP0/CPU0:router#sh access-lists ethernet-services count-packets
hardware egress location 0/1/CPU0
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3 (5 hw matches)
20 permit any any (30 hw matches)
```

하드웨어 일치는 *hardware* 키워드에서만 볼 수 있습니다. access-group의 방향에 따라 ingress 또는 egress 키워드를 사용합니다. access-list가 적용되는 인터페이스의 라인 카드 위치도 지정됩니다.

l2transport 인터페이스에 보안 또는 문제 해결 기능으로 ipv4 access-list를 적용할 수도 있습니다.

```
RP/0/RSP0/CPU0:router#sh run ipv4 access-list count-pings
ipv4 access-list count-pings
10 permit icmp host 192.168.2.1 host 192.168.2.2
20 permit ipv4 any any
!
```

```
RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ipv4 access-group count-pings ingress
!
```

```
RP/0/RSP0/CPU0:router#sh access-lists ipv4 count-pings hardware ingress
location 0/1/CPU0
ipv4 access-list count-pings
```

```
10 permit icmp host 192.168.2.1 host 192.168.2.2 (5 hw matches)
20 permit ipv4 any any (6 hw matches)
```

5.4 이더넷 이그레스 필터

AC의 이그레스 방향에서 이그레스 VLAN 태그를 결정하는 **rewrite ingress tag pop <> symmetric** 명령이 없다고 가정합니다. 이 경우 encapsulation 명령에 따라 발신 프레임에 올바른 VLAN 태그가 있는지 확인하기 위한 검사가 이루어지지 않습니다.

다음은 컨피그레이션을 보여주는 예입니다:

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
!
interface GigabitEthernet0/1/0/39.2 l2transport
encapsulation dot1q 2
!
l2vpn
bridge group customer2
bridge-domain test
interface GigabitEthernet0/1/0/3.2
!
interface GigabitEthernet0/1/0/3.3
!
interface GigabitEthernet0/1/0/39.2
!
!
!
!
```

이 컨피그레이션에서는 다음 사항에 유의하십시오.

- GigabitEthernet0/1/0/39.2에서 dot1q 태그 2와 함께 수신된 브로드캐스트에는 **rewrite ingress 명령이 없으므로** 수신 태그가 유지됩니다.
- 해당 브로드캐스트는 dot1q 태그 2로 GigabitEthernet0/1/0/3.2에서 플러딩되지만, GigabitEthernet0/1/0/3.2도 dot1q 태그 2로 구성되어 있으므로 문제가 발생하지 않습니다.
- 이 브로드캐스트는 GigabitEthernet0/1/0/3.3에서도 플러딩되므로 GigabitEthernet0/1/0/3.3에 **rewrite 명령이 없으므로** 원래 태그 2가 유지됩니다. GigabitEthernet0/1/0/3.3의 캡슐화 **dot1q 3** 명령은 이그레스 방향으로 확인되지 않습니다.
- 그 결과, GigabitEthernet0/1/0/39에서 태그 2와 함께 수신된 하나의 브로드캐스트에는 GigabitEthernet0/1/0/3에서 태그 2가 나가는 두 개의 브로드캐스트가 있습니다. 이러한 중복 트래픽은 일부 애플리케이션 문제를 일으킬 수 있습니다.
- 이 솔루션은 패킷이 올바른 VLAN 태그가 있는 하위 인터페이스를 떠날 수 있도록 엄격한 **이더넷 이그레스 필터** 컨피그레이션입니다. 그렇지 않으면 패킷이 전달되지 않고 삭제됩니다.

```
interface GigabitEthernet0/1/0/3.2 l2transport
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/3.3 l2transport
ethernet egress-filter strict
!
```

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.