Unified MPLS 기능, 기능 및 구성 예

목차

소개

이 문서에서는 배율에 대한 MPLS(Unified Multiprotocol Label Switching)에 대해 설명합니다.기존의 세분화된 인프라 전반에 걸쳐 간단한 엔드 투 엔드 트래픽 및/또는 서비스를 제공하는 기술 솔루션 프레임워크를 제공합니다.계층적 인프라의 이점을 모두 활용하면서 확장성과 네트워크 설계의 단순성을 개선합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

구성

네트워크 진화

네트워크 패킷 기반 서비스의 기록을 살펴보면 네트워크 비즈니스 가치의 변화를 확인할 수 있습니다.이는 애플리케이션을 최대한 유창하게 만들기 위해 개별 연결 개선 사항에서 모바일 협업을 지원하기 위한 협업 기술로 이어집니다.마지막으로, 조직에서 사용하는 툴을 최적화하고 안정성 및 소유 비용을 개선하기 위해 애플리케이션 서비스와 함께 온디맨드 클라우드 서비스가 도입되었습니다.

그림 1

이러한 지속적인 가치와 기능 개선을 통해 네트워크 간소화, 관리 용이성, 통합, 안정성에 대한 필요성이 더욱 보편화되었습니다. 이 경우 운영 환경이 서로 분리되고 실제 엔드 투 엔드 경로 제어가 이루어지지 않아 네트워크가 분할되었습니다.이제 관리하기 쉬운 단일 아키텍처와 100,000개의 노드까지 확장성과 최신 고가용성 및 빠른 통합 기술을 모두 통합해야 합니다.이것이 Unified MPLS가 테이블에 제공하는 기능입니다. 이 테이블은 분할된 네트워크를 단일 컨트롤 플레인 및 엔드 투 엔드 경로 가시성입니다.

최신 네트워크 요구 사항

- 대역폭 수요 증가(비디오)
- 애플리케이션 복잡성 증가(클라우드 및 가상화)
- 컨버전스의 필요성 증가(모빌리티)

더 복잡한 애플리케이션 요구 사항으로 점점 더 규모가 큰 네트워크에서 MPLS 운영을 간소화하려면 어떻게 해야 합니까?

다양한 액세스 기술을 통한 기존 MPLS 과제

- TE FRR(Traffic Engineering Fast Reroute)을 통해 50ms의 컨버전스를 실현하기 위한 복잡성
- 정교한 라우팅 프로토콜 및 레이어 2 프로토콜과의 상호 작용 필요성
- 서비스를 엔드 투 엔드 방식으로 제공하는 동안 대규모 네트워크를 도메인으로 분할
- 일반적인 엔드 투 엔드 통합 및 복원력 메커니즘
- 여러 도메인에서 엔드 투 엔드 문제 해결 및 프로비저닝

Unified MPLS 어트랙션은 다음 목록에 요약되어 있습니다.

- 운영 지점 수 감소. 일반적인 전송 플랫폼에서는 운영 지점을 통해 모든 네트워크 요소에 서비스를 구성해야 합니다.관리 시스템은 토폴로지를 알아야 합니다.Unified MPLS에서는 모든 MPLS 섬과의 통합을 통해 최소 운영 지점 수를 달성합니다.
- 손쉽게 서비스를 프로비저닝할 수 있는 가능성:레이어 3(L3) VPN, VPWS(Virtual Private Wire Service), VPLS(Virtual Private LAN Service), PW-스티칭(pw-stitching) 또는 InterAS 메커니즘 없음.어그리게이션 내에 MPLS가 도입되면서 일부 정적 컨피그레이션은 MPLS 아일랜드를 생성하는 것이 방지됩니다.
- 엔드 투 엔드 MPLS 전송을 제공합니다.
- IGP(Interior Gateway Protocol) 영역을 구분하여 작은 라우팅 테이블을 유지합니다.
- 신속한 통합.
- 구성 및 문제 해결이 간편합니다.
- 모든 액세스 기술과 통합할 수 있습니다.
- IPv6 준비도.

Cisco Unified MPLS

Unified MPLS는 기존/기존 MPLS에 추가 기능을 추가하여 정의되며 확장성, 보안, 단순성 및 관리 용이성을 향상시킵니다.MPLS 서비스를 엔드 투 엔드, 엔드 LSP(Labeled Switches Path)를 제공해야 합니다.목표는 MPLS 서비스(MPLS VPN, MPLS L2VPN)를 그대로 유지하면서 더 큰 확장성을 도입하는 것입니다.이를 위해 일부 IGP 접두사를 BGP(Border Gateway Protocol)(PE(Provider Edge) 라우터의 루프백 접두사)로 이동한 다음 접두사를 종단간 배포합니다.

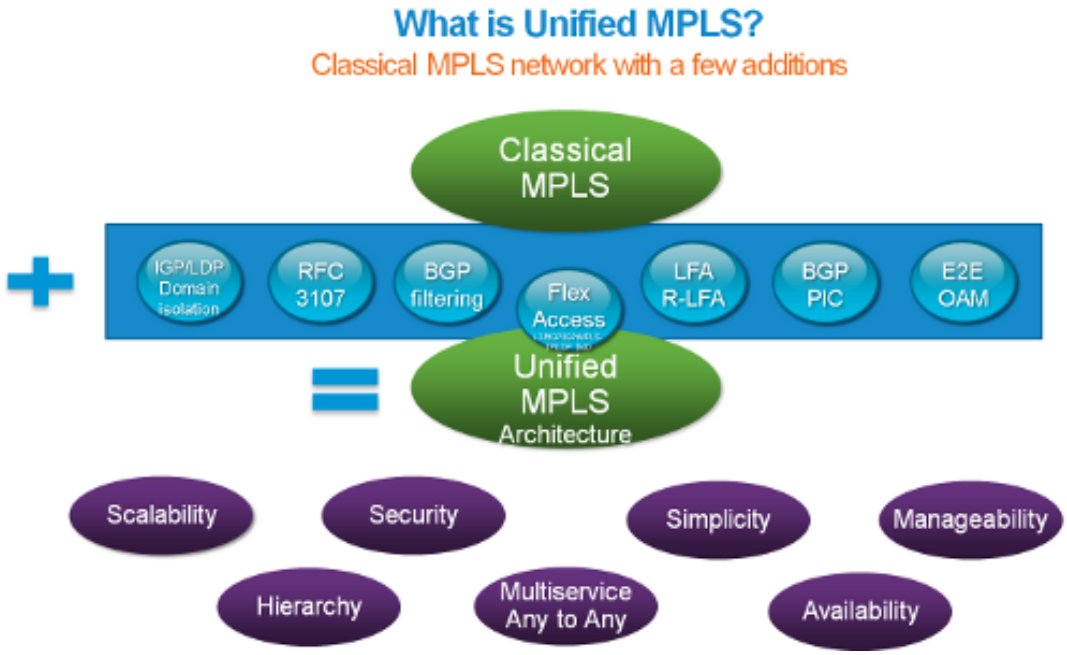

그림 2

Cisco Unified MPLS 아키텍처에 대해 논의하기 전에 이를 실현하기 위해 사용되는 주요 기능을 이해하는 것이 중요합니다.

기능 및 구성 요소

BGP-4에서 레이블 정보 전달(RFC 3107)

네트워크 세그먼트 간에 접두사를 교환하기 위해 확장 가능한 방법이 있어야 합니다 .IGP(OSPF(Open Shortest Path First), IS-IS(Intermediate System-to-Intermediate System) 또는 EIGRP(Enhanced Interior Gateway Routing Protocol)를 단일 도메인으로 간단히 병합할 수 있습니다.그러나 IGP는 100,000의 접두사를 전달하도록 설계되지 않았습니다.이러한 목적으로 선택한 프로토콜은 BGP입니다.이 프로토콜은 100,000개의 라우트와 수백만 개의 엔트리가 있는 MPLS-VPN 환경에서 인터넷을 지원하는 검증된 프로토콜입니다.Cisco Unified MPLS는 레이블 정보 교환과 함께 BGP-4를 사용합니다(RFC3107). BGP가 경로를 분배할 때 해당 경로에 매핑된 MPLS 레이블을 배포할 수도 있습니다.경로에 대한 MPLS 레이블 매핑 정보는 경로에 대한 정보가 포함된 BGP 업데이트 메시지에서 전달됩니다.다음 홉이 변경되지 않으면 레이블이 유지되고 다음 홉이 변경되면 레이블이 변경됩니다.Unified MPLS에서 ABR(Area Border Router)에서 다음 홉이 변경됩니다.

두 BGP 라우터에서 RFC 3107을 활성화하면 라우터는 서로 알리고 MPLS 레이블을 경로와 함께 전송할 수 있습니다.라우터가 MPLS 레이블을 전송하는 기능을 성공적으로 협상하면 라우터는 모든 발신 BGP 업데이트에 MPLS 레이블을 추가합니다.

세그먼트 간의 엔드 투 엔드 경로 정보를 유지하려면 레이블 교환이 필요합니다.그 결과, 각 세그먼트는 운영자가 관리할 수 있을 만큼 작아지고 동시에 서로 다른 두 IP 스피커 간의 경로 인식을 위해 회로 정보가 배포됩니다.

작동 방식

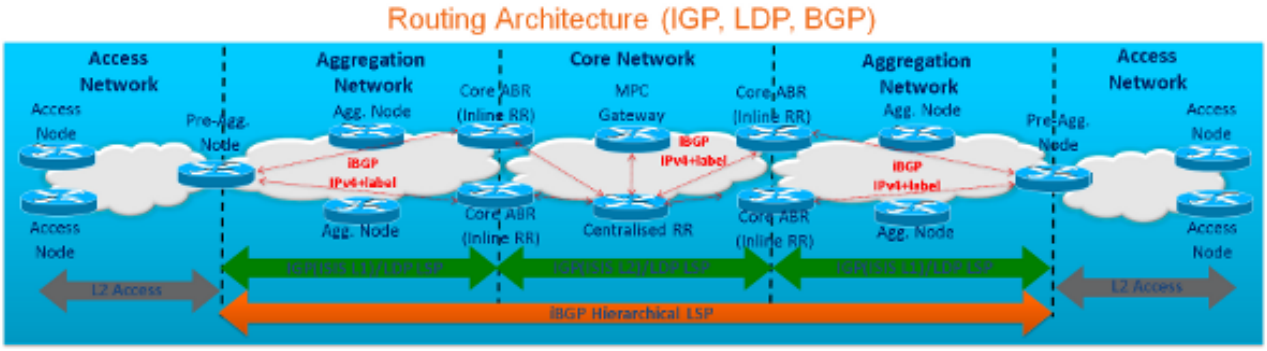

그림 3

그림 3에서 LDP(Label Discovery Protocol Labeled Switches Path)가 있고 액세스 네트워크에 LDP가 활성화되지 않은 세 개의 세그먼트가 있음을 확인할 수 있습니다.목표는 사전 어그리게이션(Pre-Aggregation) 노드 간에 단일 MPLS 경로(iBGP(Internal BGP) 계층 LSP)가 있도록 이들을 함께 결합하는 것입니다.네트워크는 단일 BGP AS(Autonomous System)이므로 모든 세션은 iBGP 세션입니다.각 세그먼트는 IGP 도메인 내에서 고유한 IGP(OSPF, IS-IS 또는 EIGRP) 및 LDP LSP 경로를 실행합니다.Cisco Unified MPLS 내에서 세그먼트에 조인하는 라우터(ABR)는 세션에 구성된 IPv4 + 레이블을 전달하려면 Next-Hop-Self 및 RFC 3107과 함께 BGP 인라인 경로 리플렉터여야 합니다.이러한 BGP 스피커는 ABR로 참조되는 Cisco Unified MPLS 아키텍처 내에 있습니다.

ABR이 인라인 경로 리플렉터인 이유는 무엇입니까?

Unified MPLS의 목표 중 하나는 확장성이 뛰어난 엔드 투 엔드 인프라를 구축하는 것입니다.따라서 각 세그먼트는 간편하게 운영되어야 합니다.모든 피어링은 iBGP 피어이므로 전체 네트워크 내의 모든 iBGP 스피커 간에 풀 메쉬의 피어링이 필요합니다.따라서 수천 개의 BGP 스피커가 있는 경우 매우 비실용적인 네트워크 환경이 조성됩니다.ABR이 경로 리플렉터로 만들어진 경우 전체 AS의 'all' BGP 스피커 사이에 있는 'all' 대신 iBGP 피어링 수가 '세그먼트당' BGP 스피커 수로 줄어듭니다.

Next-Hop-Self를 선택해야 하는 이유

BGP는 재귀 라우팅 조회의 기반에서 작동합니다.이는 활용되는 기본 IGP 내에서 확장성을 수용하기 위해 수행됩니다.재귀 조회의 경우 BGP는 각 BGP 경로 항목에 연결된 Next-Hop을 사용합니다.예를 들어, Source-Node가 패킷을 Destination-Node로 전송하려는 경우 패킷이 BGP 라우터에 도달하면 BGP 라우터는 BGP 라우팅 테이블에서 라우팅 조회를 수행합니다.Destination-Node로 향하는 경로를 찾은 다음 단계로 Next-Hop을 찾습니다.이 Next-Hop은 기본 IGP에서 알고 있어야 합니다.마지막 단계로, BGP 라우터는 해당 Next-Hop에 연결된 IP 및 MPLS 레이블 정보를 기반으로 패킷을 계속 전달합니다.

각 세그먼트 내에서 IGP에서 Next-Hop만 알아야 함을 확인하려면 BGP 항목에 연결된 Next-Hop이 네트워크 세그먼트 내에 있어야 하며 인접 또는 더 멀리 떨어진 세그먼트 내에 있어야 합니다.Next-Hop-Self 기능으로 BGP Next-Hop을 재작성할 경우 Next-Hop이 로컬 세그먼트 내에 있는지 확인합니다.

모두 통합

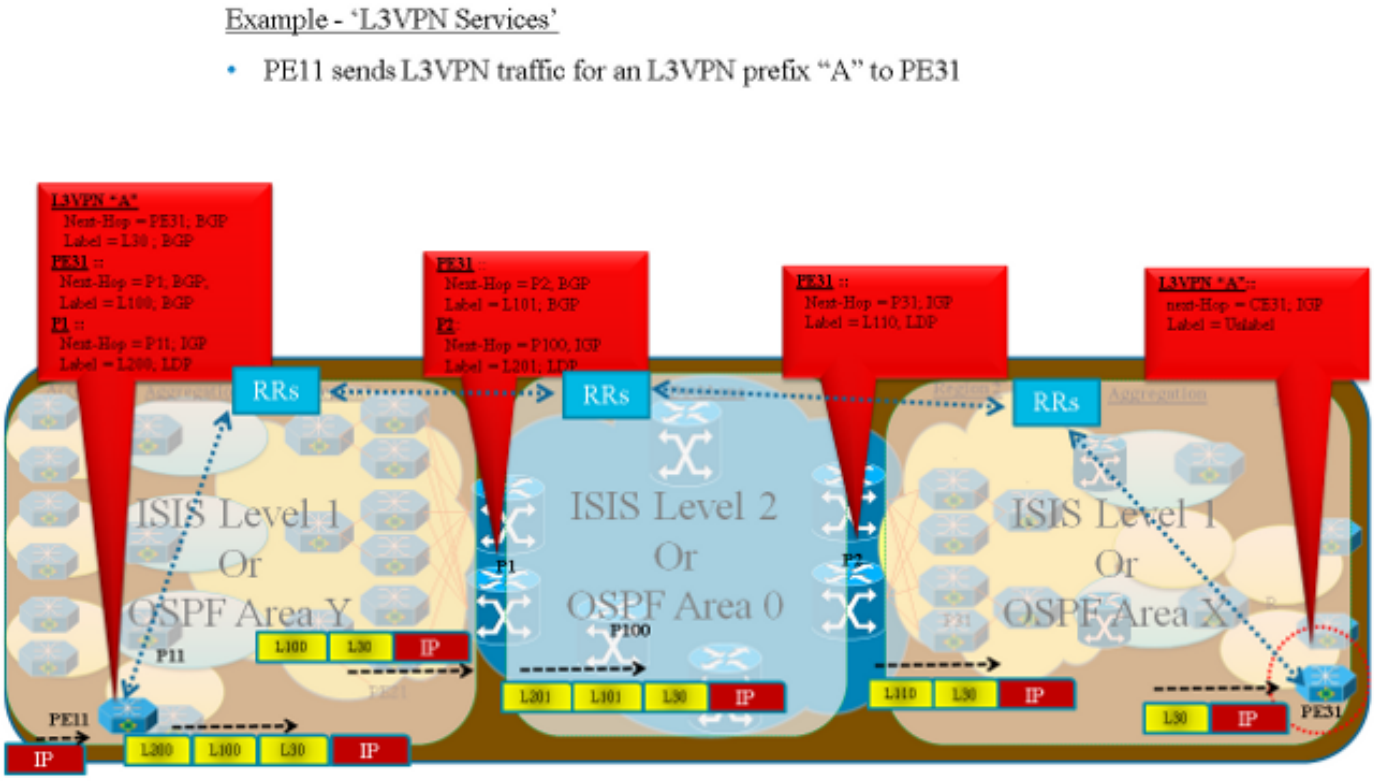

그림 4

그림 4는 L3 VPN 접두사 'A'와 레이블 교환이 작동하는 방식 및 두 PE 간의 트래픽 흐름에 대한 엔드 투 엔드 경로 정보를 제공하기 위해 MPLS 레이블 스택이 생성되는 방식의 예를 보여줍니다.

네트워크는 3개의 독립적인 IGP/LDP 도메인으로 분할됩니다.라우터의 라우팅 및 포워딩 테이블 크기가 줄어들기 때문에 안정성과 컨버전스 속도가 향상됩니다.LDP는 도메인 내에서 내부 도메인 LSP를 구축하는 데 사용됩니다.RFC 3107 BGP IPv4+ 레이블은 도메인 간에 계층적 BGP LSP를

구축하기 위해 도메인 간 레이블 배포 프로토콜로 사용됩니다.BGP3107은 Unified MPLS 아키텍처의 포워딩 레이블 스택에 하나의 추가 레이블을 삽입합니다.

인트라도메인 - LDP LSP

도메인 간 - BGP 계층적 LSP

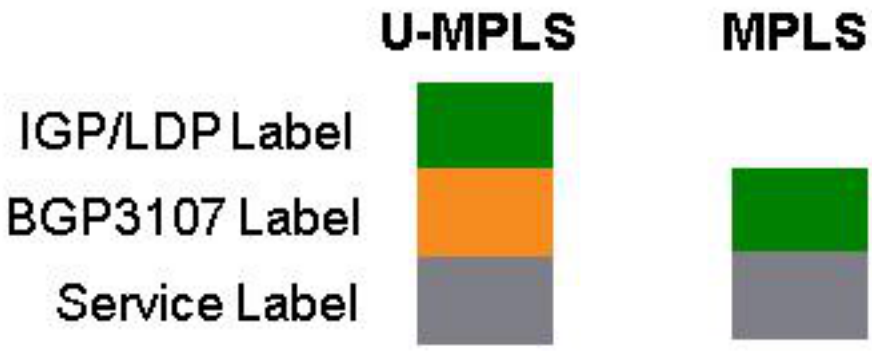

그림 5

VPN 접두사 'A'는 PE31에서 L3VPN 서비스 레이블 30을 사용하는 PE11로, next hop은 엔드 투 엔드 도메인 간 계층적 BGP LSP를 통해 PE31의 루프백으로 광고됩니다.이제 PE11에서 PE31까지 VPN 접두사 'A'의 포워딩 경로를 확인합니다.

- PE11에서 접두사 A는 PE31을 사용하는 BGP 세션을 통해 알려지며 next-hop PE31은 BGP 레이블 100을 사용하는 P1을 통해 재귀적으로 연결할 수 있습니다. PE11은 RFC 3107 기능을 사용하여 IPv4 + IPv4로 보내기 위해 IP레이블 기능을 활성화했기 때문에 P1에서 BGP 업데이트로 IPv4 + 레이블 정보를 받았습니다. 정보를 제공합니다.
- P1은 내부 LDP LSP를 통해 PE11에서 연결할 수 있으며 BGP 레이블 위에 또 다른 LDP 레이블을 추가합니다.마지막으로, 패킷은 3개의 레이블이 있는 PE11 노드에서 벗어납니다.예를 들어, 30개의 L3VPN 서비스 레이블, 100개의 BGP 레이블 및 200개의 LDP IGP 레이블.
- LDP 상위 레이블은 계속해서 내부 LDP LSP에서 교체되고 패킷은 Penultimate Hop Popting(PHP) 이후 두 개의 레이블로 P1에 도달합니다.
- P1은 next-hop self를 사용하여 인라인 RR(Route Reflector)로 구성되며 두 IGP 도메인 또는 LDP LSP에 조인합니다.
- P1에서 PE31의 다음 홉이 P2로 변경되고 IPv4 + Label(RFC3107)이 있는 BGP를 통해 업데이트가 수신됩니다. next-hop이 변경되고 IGP 레이블이 맨 위에 푸시되므로 BGP 레이블이 새 레이블로 교체됩니다.
- 3개의 레이블과 서비스 레이블 30이 있는 패킷이 P1 노드에서 나가는 경우 그대로 유지됩니다.즉, 30개의 L3VPN 서비스 레이블, 101개의 BGP 레이블 및 201 LDP 레이블입니다.
- LDP 상위 레이블은 내부 LDP LSP에서 교체되고 패킷은 PHP 뒤에 두 개의 레이블이 있는 P2에 도달합니다.
- P2에서 PE31의 다음 홉이 다시 변경되고 IGP를 통해 연결할 수 있습니다.PHP용 PE31에서 암시적 null BGP 레이블을 수신하면 BGP 레이블이 제거됩니다.
- 패킷이 두 개의 레이블로 나갑니다.예를 들어, 30 L3VPN 서비스 레이블 및 110 LDP 레이블.
- PE31에서 패킷은 LDP 레이블의 PHP 뒤에 서비스 레이블 30에 따라 하나의 레이블로 도착합니다. 레이블이 지정되지 않은 패킷은 VRF(Virtual Routing and Forwarding) 아래의 CE31 대상으로 전달됩니다.

MPLS 레이블 스택을 보면 MPLS 스위칭 환경에서 이전 접두사 및 레이블 교환을 기반으로 소스 디바이스와 대상 디바이스 간의 패킷 스위칭이 관찰됩니다.

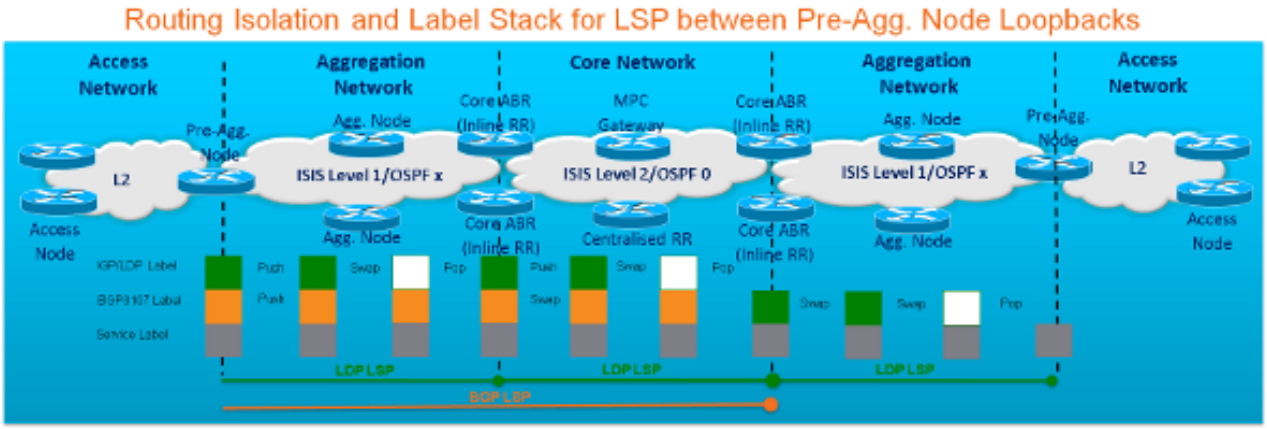

그림 6

BGP PIC(Prefix-Independent Convergence)

이는 BGP 장애 시나리오에서 사용되는 Cisco 기술입니다.네트워크는 BGP 재컨버전스의 기존 초 단위 손실 없이 통합됩니다.BGP PIC를 사용하면 대부분의 장애 시나리오를 100msec 미만의 재통합 시간으로 줄일 수 있습니다.

어떻게 된 거죠?

일반적으로 BGP에서 실패를 탐지하면 최적의 경로를 위해 각 BGP 항목에 대해 다시 계산됩니다.수천 개의 경로 엔트리가 있는 라우팅 테이블이 있는 경우 이 작업에는 상당한 시간이 소요될 수 있습니다.또한 이 BGP 라우터는 변경된 네트워크 토폴로지 및 변경된 최적 경로를 알려주기 위해 각각의 인접 디바이스에 이러한 새로운 최상의 경로를 모두 배포해야 합니다.마지막 단계로 각 수신자 BGP 스피커는 새로운 최상의 경로를 찾기 위해 최적의 경로 계산을 수행해야 합니다.

첫 번째 BGP 스피커가 잘못된 것을 탐지할 때마다 모든 인접 BGP 스피커가 다시 계산을 수행할 때까지 최상의 경로 계산을 시작합니다. 트래픽 흐름이 삭제될 수 있습니다.

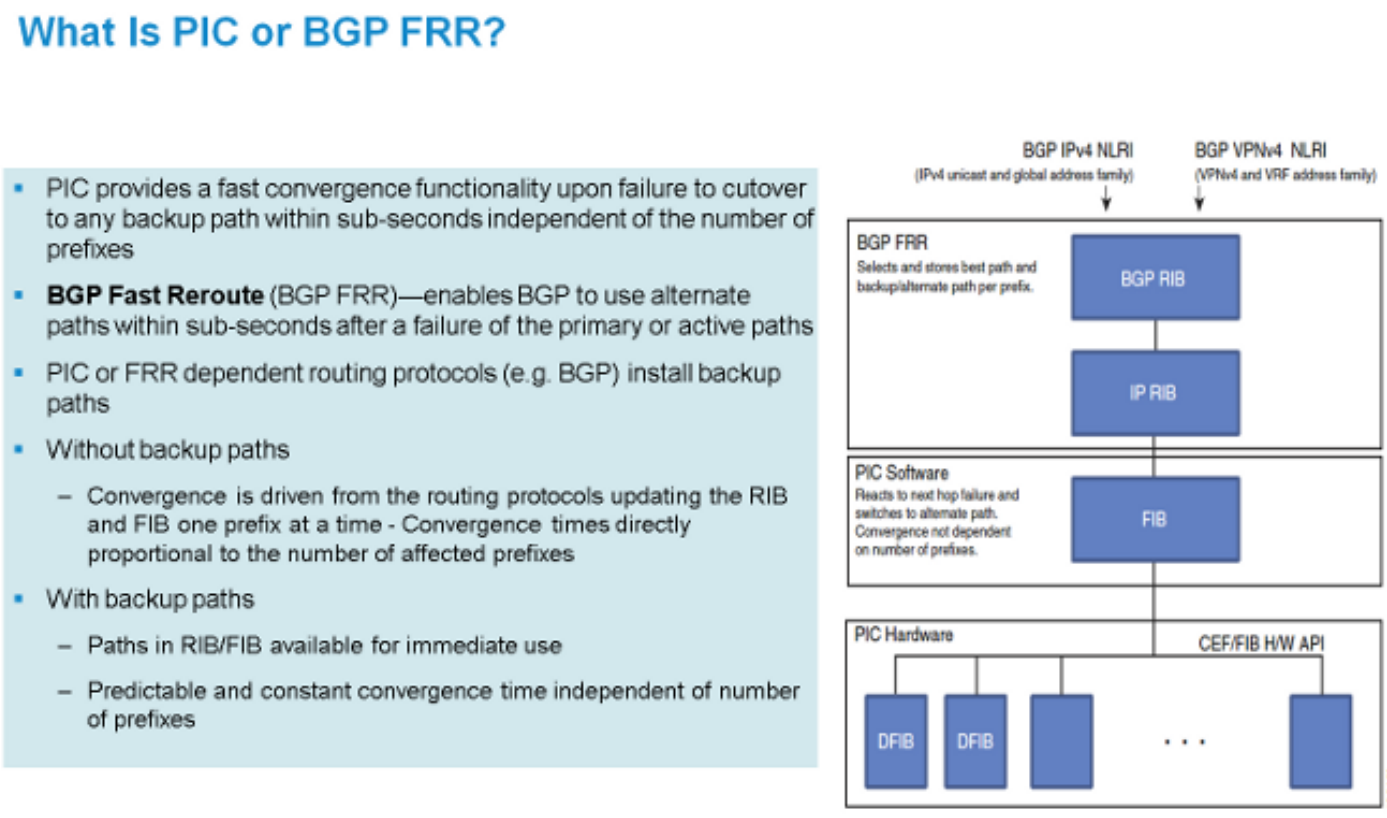

그림 7

IP 및 MPLS VPN용 BGP PIC 기능은 네트워크 장애 후 BGP 컨버전스를 개선합니다.이러한 컨버전스는 코어 및 에지 장애 모두에 적용되며 IP 및 MPLS 네트워크 모두에서 사용할 수 있습니다.IP용 BGP PIC 및 MPLS VPN 기능은 RIB(Routing Information Base), FIB(Forwarding Information Base) 및 CEF(Cisco Express Forwarding)에 백업/대체 경로를 생성하여 저장하여 장애가 감지되면 백업/대체 경로가 즉시 대체될 수 있으므로 신속한 장애 조치가 가능합니다.

next-hop 정보를 단일 재작성하면 트래픽 흐름이 복원됩니다.또한 네트워크 BGP 컨버전스는 백그라운드에서 발생하지만 트래픽 흐름은 더 이상 영향을 받지 않습니다.이 재작성은 50밀리초 이내에 수행됩니다.이 기술을 사용하면 네트워크 컨버전스가 초 단위 50msec에서 IGP 컨버전스로 축소됩니다.

BGP 추가 경로

BGP Add-Path는 BGP 스피커 간에 BGP 항목이 전달되는 방식을 개선합니다.특정 BGP 스피커에 특정 목적지에 단일 항목 이상이 있는 경우, 해당 BGP 스피커는 해당 목적지에 대한 최상의 경로인 항목만 인접 디바이스로 전송합니다.따라서 동일한 대상에 대해 여러 경로를 광고할 수 있도록 어떤 규정도 만들어지지 않습니다.

BGP Add-Path는 최상의 경로만 허용하는 BGP 기능이며, 이전 경로를 암시적으로 대체하지 않고 새 경로가 동일한 대상에 대해 여러 경로를 허용합니다.BGP 경로 리플렉터를 사용하는 경우 BGP PIC를 지원하기 위해 이 BGP 확장은 특히 중요합니다. 따라서 AS 내의 다른 BGP 스피커가 경로 리플렉터에 따라 '최상의 BGP 경로'처럼 더 많은 BGP 경로에 액세스할 수 있습니다.

IGP Fast-Convergence용 루프 프리 대안 및 LFA

링크 또는 노드 장애 후 50ms의 복구를 수행하는 작업은 LFA(Loop-Free Alternative)라는 새로운 기술을 도입하여 대폭 간소화할 수 있습니다.LFA는 루프 프리 방식으로 대체 라우팅 경로를 찾기 위해 링크 상태 라우팅 프로토콜(IS-IS 및 OSPF)을 개선합니다.LFA를 사용하면 인접성(네트워크 노드 또는 링크)이 실패할 경우 각 라우터가 미리 정의된 백업 경로를 정의하고 사용할 수 있습니다.링크 또는 노드 장애 시 50msec의 복원 시간을 제공하기 위해 MPLS TE FRR을 구축할 수 있습니다.그러나 이렇게 하려면 TE 터널의 설정 및 관리를 위해 다른 프로토콜(Resource Reservation Protocol 또는 RSVP)을 추가해야 합니다.대역폭 관리에 필요할 수 있지만 보호 및 복원 작업에는 대역폭 관리가 필요하지 않습니다.따라서 RSVP TE 추가와 관련된 오버헤드는 링크 및 노드를 간단하게 보호하기 위해 높은 수준으로 간주됩니다.

LFA는 이러한 시나리오에서 RSVP TE를 구축하지 않고도 간단하고 쉬운 기술을 제공할 수 있습니다.이러한 기술을 통해 대규모 네트워크에 연결된 오늘날의 상호 연결된 라우터는 운영자에 대한 구성 요구 사항 없이 링크 및 노드 장애에 대해 50msec의 복원을 제공할 수 있습니다.

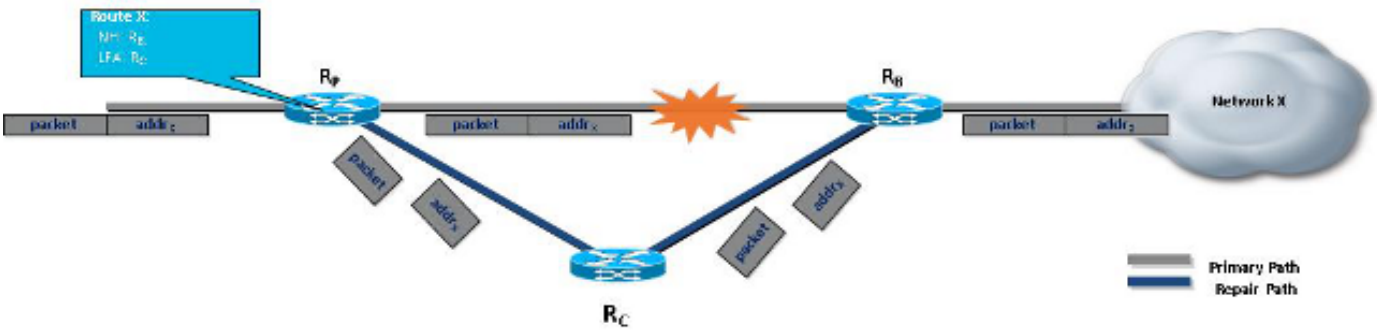

그림 8

LFA-FRR은 IP, MPLS, EoMPLS(Ethernet Over MPLS), MPLS를 통한 IMA(Inverse Multiplexing over ATM), CESoPSN(Circuit Emulation Service over Packet Switched Network) 및 MPLS를 통한 Structure-Agnostic Time Division Multiplexplexing(Multiplexing)에 대한 로컬 보호를 제공하는 메커니즘입니다. MPLS 네트워크를 통해 구축할 수 있습니다.그러나 일부 토폴로지(예: 링 토폴로지)에는 LFA-FRR에서만 사용할 수 없는 보호가 필요합니다.Remote LFA-FRR 기능은 이러한 상황에서 유용합니다.

Remote LFA-FRR은 LFA-FRR의 기본 동작을 모든 토폴로지로 확장합니다.장애가 발생한 노드 주위의 트래픽을 둘 이상의 홉이 떨어진 원격 LFA로 전달합니다.그림 9에서 C1과 C2 간의 링크가 A1에 도달하지 못하면 C2는 A1에 연결할 수 있는 C5로 직접 LDP 세션을 통해 패킷을 전송합니다.

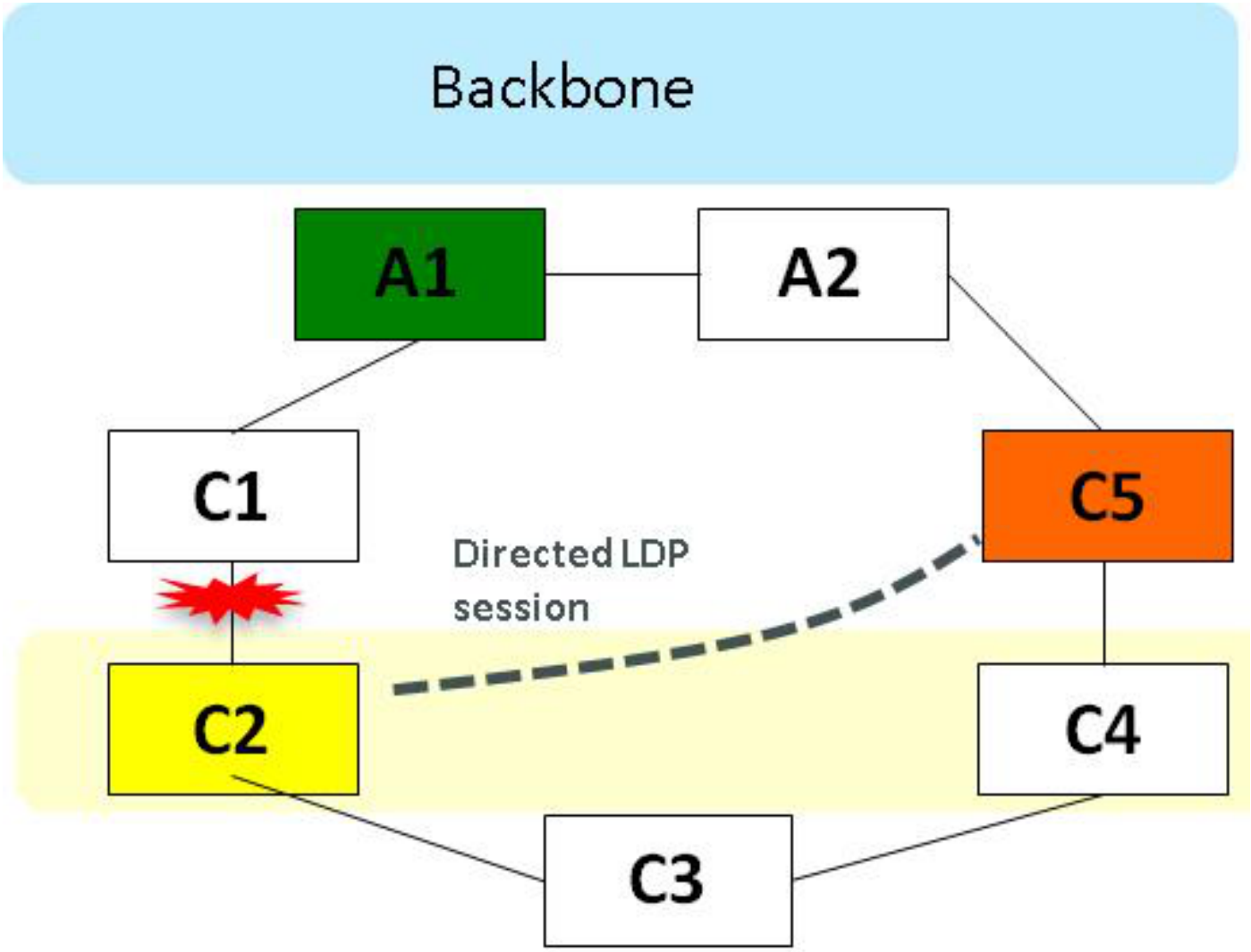

그림 9

원격 LFA-FRR에서 노드는 LFA 노드를 동적으로 계산합니다.대체 노드가 확인되면(직접 연결되지 않음) 노드는 자동으로 대체 노드에 대한 지정 LDP(Label Distribution Protocol) 세션을 설정합니다.직접 LDP 세션은 특정 전달 오류 수정(FEC)에 대한 레이블을 교환합니다.

링크가 실패하면 노드는 트래픽을 목적지로 전달하기 위해 원격 LFA 노드로 트래픽을 터널링하기 위해 레이블 스태킹을 사용합니다.원격 LFA 노드에 대한 모든 레이블 교환 및 터널링은 기본적으로 동적이며 사전 프로비저닝이 필요하지 않습니다.전체 레이블 교환 및 터널링 메커니즘은 동적이며 수동 프로비저닝은 포함되지 않습니다.

내부 도메인 LSP의 경우 원격 LFA FRR은 링 토폴로지의 유니캐스트 MPLS 트래픽에 사용됩니다

.원격 LFA FRR은 IGP 라우팅 테이블의 모든 접두사에 대한 백업 경로를 미리 계산합니다. 이렇게 하면 오류가 발생할 때 노드가 백업 경로로 빠르게 전환할 수 있습니다.이렇게 하면 50msec의 순서대로 복구 시간이 제공됩니다.

Cisco Unified MPLS 아키텍처 예

이전의 모든 툴과 기능이 네트워크 환경 내에 통합되면 Cisco Unified MPLS 네트워크 환경이 생성됩니다.이는 대규모 통신 사업자를 위한 아키텍처 예입니다.

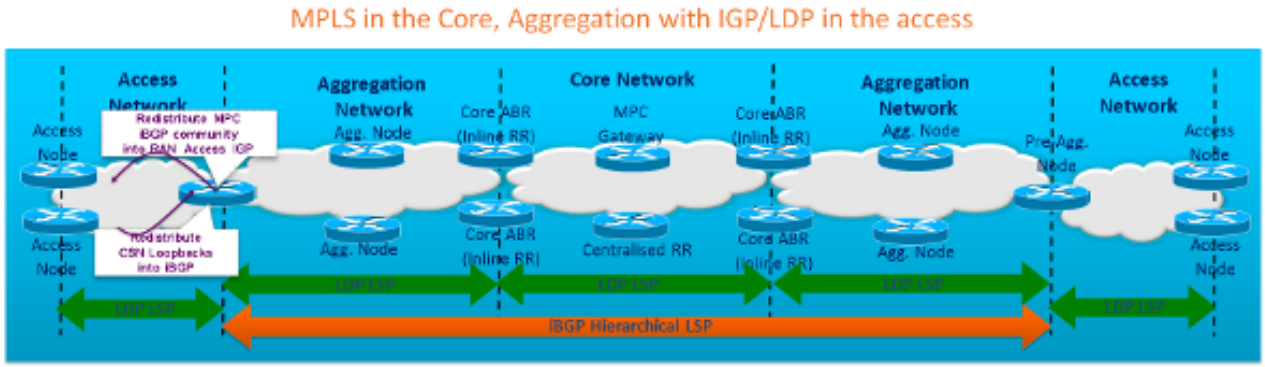

그림 10

- 코어 및 어그리게이션은 고유한 IGP/LDP 도메인으로 구성됩니다.
- RFC 3107 기반의 도메인 간 계층적 LSP, 프리agg로 확장된 BGP IPv4+ 레이블
- LDP를 기반으로 하는 내부 도메인 LSP입니다.
- 도메인 간 코어/어그리게이션 LSP는 RAN(Radio Access Networks Interior Gateway Protocol)를 도메인 간 iBGP로 배포하여 액세스 네트워크에서 확장되며, 필요한 레이블이 지정된 iBGP 접두사(MPC(Mobile Packet Core) 게이트웨이를 RAN IGP(BGP 커뮤니티)를 통해 배포합니다.

Unified MPLS 컨피그레이션 예

다음은 Unified MPLS의 간소화된 예입니다.

Core Area Border Router - Cisco IOS® XR

사전 어그리게이션 및 셀 사이트 게이트웨이 라우터 - Cisco IOS

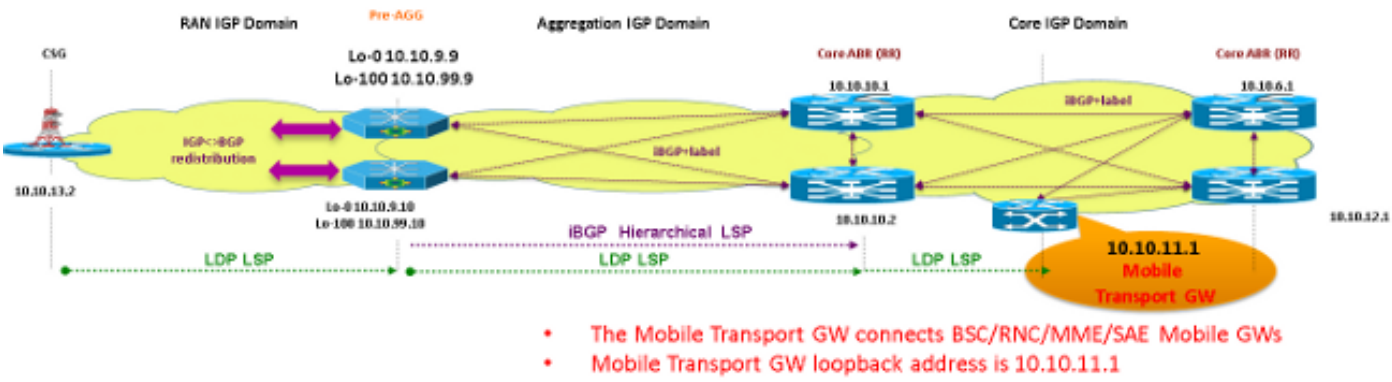

그림 11

200:200 MPC 커뮤니티

300:300 집계 커뮤니티
코어 IGP 도메인 ISIS 레벨 2
어그리게이션 IGP 도메인 ISIS 레벨 1
IGP 도메인 액세스 OSPF 0 영역

코어 영역 경계 라우터 컨피그레이션

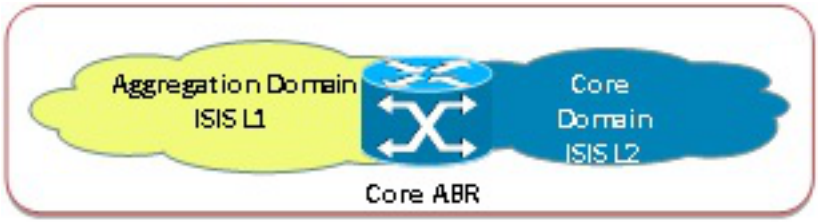

그림 12

```
! IGP Configuration
router isis core-agg
net 49.0100.1010.0001.0001.00
address-family ipv4 unicast
metric-style wide
propagate level 1 into level 2 route-policy drop-all  ! Disable L1 to L2 redistribution
!
interface Loopback0
ipv4 address 10.10.10.1 255.255.255.255
passive
!
interface TenGigE0/0/0/0
!
interface TenGigE0/0/0/1
circuit-type level-2-only                    ! Core facing ISIS L2 Link

!
interface TenGigE0/0/0/2
circuit-type level-1                         ! Aggregation facingis ISIS L1 Link

  !
route-policy drop-all
drop
end-policy

! BGP Configuration

router bgp 100
ibgp policy out enforce-modifications
bgp router-id 10.10.10.1
address-family ipv4 unicast
allocate-label all                           ! Send labels with BGP routes
!
session-group infra
remote-as 100
cluster-id 1001
update-source Loopback0
!
neighbor-group agg
use session-group infra
address-family ipv4 labeled-unicast
  route-reflector-client

   route-policy BGP_Egress_Filter out        ! BGP Community based Egress filtering
```

```
   next-hop-self
!
neighbor-group mpc
use session-group infra
address-family ipv4 labeled-unicast
  route-reflector-client
   next-hop-self
!
neighbor-group core
use session-group infra
address-family ipv4 labeled-unicast
  next-hop-self

community-set Allowed-Comm
200:200,
 300:300,
!
route-policy BGP_Egress_Filter
if community matches-any Allowed-Comm then
  pass
```

사전 집계 컨피그레이션

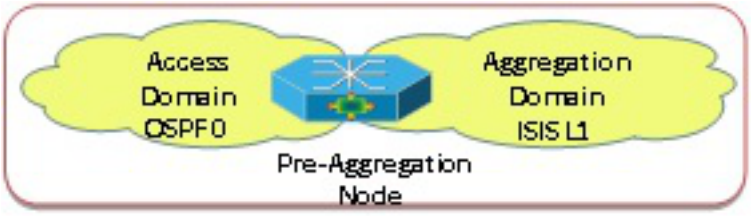

그림 13

```
interface Loopback0
ipv4 address 10.10.9.9 255.255.255.255
!
interface Loopback1
ipv4 address 10.10.99.9 255.255.255.255

! Pre-Agg IGP Configuration

router isis core-agg
net 49.0100.1010.0001.9007.00
is-type level-1                                  !  ISIS L1 router
metric-style wide
passive-interface Loopback0                      !  Core-agg IGP loopback0

!RAN Access IGP Configuration

router ospf 1
router-id 10.10.99.9
redistribute bgp 100 subnets route-map BGP_to_RAN     !  iBGP to RAN IGP redistribution
network 10.9.9.2 0.0.0.1 area 0
network 10.9.9.4 0.0.0.1 area 0
network 10.10.99.9 0.0.0.0 area 0
distribute-list route-map Redist_from_BGP in          !  Inbound filtering to prefer
     labeled BGP learnt prefixes

ip community-list standard MPC_Comm permit 200:200
!
route-map BGP_to_RAN permit 10                        ! Only redistribute prefixes
     marked with MPC community
```

```
 match community MPC_Comm
 set tag 1000
route-map Redist_from_BGP deny 10
match tag 1000
!
route-map Redist_from_BGP permit 20


! BGP Configuration
router bgp 100
ibgp policy out enforce-modifications
bgp router-id 10.10.9.10
bgp cluster-id 909
neighbor csr peer-group
neighbor csr remote-as 100
neighbor csr update-source Loopback100                ! Cell Site - Routers RAN IGP
     loopback100 as source
neighbor abr peer-group
neighbor abr remote-as 100
neighbor abr update-source Loopback0                  ! Core POP ABRs - core-agg IGP
     loopback0 as source
neighbor 10.10.10.1 peer-group abr
neighbor 10.10.10.2 peer-group abr
neighbor 10.10.13.1 peer-group csr
!
address-family ipv4
bgp redistribute-internal
network 10.10.9.10 mask 255.255.255.255 route-map AGG_Comm   ! Advertise with
     Aggregation Community (300:300)
redistribute ospf 1                                   !  Redistribute RAN IGP prefixes
neighbor abr send-community
neighbor abr next-hop-self

 neighbor abr send-label                              !  Send labels with BGP routes
neighbor 10.10.10.1 activate
neighbor 10.10.10.2 activate
exit-address-family
!
route-map AGG_Comm permit 10
set community 300:300
```

CSG(Cell Site Gateway) 구성

그림 14

```
interface Loopback0
ip address 10.10.13.2 255.255.255.255

! IGP Configuration
router ospf 1
router-id 10.10.13.2
network 10.9.10.0 0.0.0.1 area 0
network 10.13.0.0 0.0.255.255 area 0
network 10.10.13.3 0.0.0.0 area 0
```

MTG 컨피그레이션

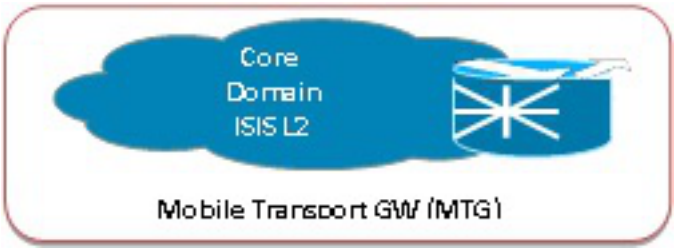

그림 15

```
Interface lookback0
ip address 10.10.11.1 255.255.255.255

! IGP Configuration
router isis core-agg
is-type level-2-only                          !  ISIS L2 router
net 49.0100.1010.0001.1001.00
address-family ipv4 unicast
metric-style wide

! BGP Configuration
router bgp 100
ibgp policy out enforce-modifications
bgp router-id 10.10.11.1
address-family ipv4 unicast
network 10.10.11.1/32 route-policy MPC_Comm   ! Advertise Loopback-0 with MPC Community
allocate-label all                            ! Send labels with BGP routes
!
session-group infra

remote-as 100
update-source Loopback0
!
neighbor-group abr
use session-group infra
address-family ipv4 labeled-unicast
  next-hop-self
!
neighbor 10.10.6.1
use neighbor-group abr
!
neighbor 10.10.12.1
use neighbor-group abr

community-set MPC_Comm
200:200
end-set
!
route-policy MPC_Comm
set community MPC_Comm
end-policy
```

다음을 확인합니다.

MPG(Mobile Packet Gateway)의 루프백 접두사는 10.10.11.1/32이므로 해당 접두사는 중요합니다.이제 패킷이 CSG에서 MPG로 전달되는 방법을 살펴봅니다.

MPC 접두사 10.10.11.1은 경로 태그 1000이 포함된 사전 에이전트에서 CSG 라우터에 알려지며, 이 접두사는 나가는 LDP 레이블 31(도메인 내 LDP LSP)이 포함된 레이블이 지정된 패킷으로 전달할 수 있습니다. 재배포가 OSPF에 있는 동안 MPC 커뮤니티 200:200은 Pre-agg 노드에서 경로 태

그 1000으로 매핑되었습니다.

CSG 노드 출력

```
CSG#sh mpls forwarding-table 10.10.11.1 detail
Local      Outgoing    Prefix           Bytes Label  Outgoing    Next Hop
Label      Label       or Tunnel Id     Switched     interface
34          31         10.10.11.1/32    0            Vl40        10.13.1.0
      MAC/Encaps=14/18, MRU=1500, Label Stack{31}
```

Pre-Agg 노드 출력

Pre-agg 노드에서 MPC 접두사가 커뮤니티 기반 필터링을 사용하여 BGP에서 RAN 액세스 OSPF 프로세스로 재배포되고 OSPF 프로세스가 BGP로 재배포됩니다.이러한 제어된 재배포는 엔드 투 엔드 IP 연결성을 제공하기 위해 필요한 동시에 각 세그먼트가 필요한 최소 경로를 가지고 있습니다 .

10.10.11.1/32 접두사는 MPC 200:200 커뮤니티가 연결된 계층 BGP 100을 통해 알려져 있습니다 .코어 ABR(Area Border Router)에서 수신한 16020 BGP 3107 레이블과 LDP 레이블 22는 다음 홉의 재귀 조회 후 내부 포워딩에 대해 맨 위에 추가됩니다.

```
Pre-AGG1#sh ip route 10.10.11.1
Routing entry for 10.10.11.1/32
Known via "bgp 100", distance 200, metric 0, type internal
Redistributing via ospf 1
Advertised by ospf 1 subnets tag 1000 route-map BGP_TO_RAN
Routing Descriptor Blocks:
* 10.10.10.2, from 10.10.10.2, 1d17h ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
    MPLS label: 16020

Pre-AGG1#sh bgp ipv4 unicast 10.10.11.1
BGP routing table entry for 10.10.11.1/32, version 116586
Paths: (2 available, best #2, table default)
Not advertised to any peer
Local
  <SNIP>
Local
  10.10.10.2 (metric 30) from 10.10.10.2 (10.10.10.2)
    Origin IGP, metric 0, localpref 100, valid, internal, best
    Community: 200:200
    Originator: 10.10.11.1, Cluster list: 0.0.3.233, 0.0.2.89
    mpls labels in/out nolabel/16020

Pre-AGG1#sh bgp ipv4 unicast labels
  Network          Next Hop     In label/Out label
  10.10.11.1/32 10.10.10.1   nolabel/16021
                 10.10.10.2   nolabel/16020

Pre-AGG1#sh mpls forwarding-table 10.10.10.2 detail
Local      Outgoing  Prefix           Bytes Label   Outgoing    Next Hop
Label      Label     or Tunnel Id     Switched      interface
79          22         10.10.10.2/32 76109369     Vl10        10.9.9.1
      MAC/Encaps=14/18, MRU=1500, Label Stack{22}

Pre-AGG#sh mpls forwarding-table 10.10.11.1 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing    Next Hop
```

```
Label      Label      or Tunnel Id     Switched      interface
530        16020      10.10.11.1/32 20924900800   Vl10        10.9.9.1
      MAC/Encaps=14/22, MRU=1496, Label Stack{22 16020}
```

코어 ABR 노드 출력

접두사 10.10.11.1은 ISIS-L2(intradomain IGP)를 통해 그리고 MPLS 포워딩 테이블에 따라 알려져 있습니다.LDP LSP를 통해 연결할 수 있습니다.

```
ABR-Core2#sh ip route 10.10.11.1
Routing entry for 10.10.11.1/32
Known via "isis core-agg", distance 115, metric 20, type level-2
Installed Sep 12 21:13:03.673 for 2w3d
Routing Descriptor Blocks
  10.10.1.0, from 10.10.11.1, via TenGigE0/0/0/0, Backup
    Route metric is 0
  10.10.2.3, from 10.10.11.1, via TenGigE0/0/0/3, Protected
    Route metric is 20
No advertising protos.
```

세그먼트화된 영역 간에 접두사를 배포할 경우 레이블이 있는 BGP(RFC 3107)가 사용됩니다 .IGP의 세그먼트화된 영역 내에 상주해야 하는 것은 중앙 인프라와 관련된 PE와 주소의 루프백입니다.

서로 다른 영역을 함께 연결하는 BGP 라우터는 BGP 경로 리플렉터 역할을 하는 ABR입니다.이러한 디바이스는 PE와 중앙 인프라의 IP 주소 대신 IGP에 완전한 자동 시스템의 모든 Next-Hop-Self 기능을 사용할 필요가 없도록 Next-Hop-Self 기능을 사용합니다.루프 탐지는 BGP Cluster-ID를 기반으로 완료됩니다.

네트워크 복원력을 위해 BGP 경로 추가 기능이 있는 BGP PIC를 IGP가 있는 BGP 및 LFA와 함께 사용해야 합니다.이러한 기능은 이전 예제에서 사용되지 않습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 원활한 MPLS 아키텍처
- Cisco Unified MPLS 백서
- Cisco CPT(Carrier Packet Transport) 시스템
- 기술 지원 및 문서 – Cisco Systems