

Evolved Campus 솔루션

EVPN/VXLAN 기반 엔터프라이즈 네트워크

과제

기존의 캠퍼스는 독점 솔루션을 사용하기 때문에 대규모 엔터프라이즈의 엔드포인트 요구를 만족할 수 있는 유연성이 부족했습니다. 캠퍼스 네트워크는 IoT 디바이스를 수용할 수 있을 만큼 유연하고 캠퍼스 내외의 모든 레이어에서 일관된 보안을 제공해야 합니다.

솔루션

EVPN 컨트롤 플레인과 VXLAN 오버레이를 기반으로 하는 주니퍼의 Evolved Campus 솔루션은 여러 곳의 캠퍼스, 데이터센터 및 퍼블릭 클라우드를 구축하고 상호 연결하기 위한 효율적이고 확장 가능한 방법을 제공합니다.

이점

- 컨트롤 플레인 기반 L2/L3 정보 교환
- 효율적인 호스트 모빌리티
- 비독점 솔루션
- 모든 네트워크 레이어에서 확장 가능
- 빠른 컨버전스
- 유연하고 안전한 아키텍처

전 세계의 엔터프라이즈가 네트워크에 클라우드 및 클라우드 기반 애플리케이션을 도입하여 경쟁력을 개선하고 IT 비용을 절감하며 언제 어디서나 사용자가 리소스 및 데이터에 액세스할 수 있도록 지원하고 있습니다. 모바일 디바이스, 소셜 미디어 및 협업 툴과 더불어 사물 인터넷(IoT) 디바이스의 대중화에 따른 이러한 추세는 엔터프라이즈 캠퍼스 네트워크에 큰 영향을 주고 있습니다. 빠르게 진화하는 비즈니스 요구 사항과 점점 늘어나고 있는 네트워크 엔드포인트의 수로 인해 확장성이 뛰어난 네트워크에 대한 수요가 증가하고 있습니다. 네트워크는 단순하고 확장 가능하며 프로그래밍을 할 수 있어야 할 뿐 아니라 캠퍼스 및 데이터센터 전반에 걸쳐 일반적인 표준 기반의 아키텍처에 구축되어야 합니다.

과제

대부분의 캠퍼스 네트워크는 스페닝 트리 프로토콜(Spanning Tree Protocol)이 필요하지 않은 기존의 레이어 2 이더넷 기반 아키텍처를 기반으로 합니다. 이러한 아키텍처는 서비스가 단일 네트워크에 국한되는 중소 규모의 캠퍼스에서는 기존 캠퍼스 요구 사항을 충족하며 원활하게 작동하지만, 대규모 엔터프라이즈의 확장 요구를 지원할 수 있을 정도로 유연하지는 못합니다.

클라우드 기반 애플리케이션은 새로운 비즈니스 모델을 가능케 하며 비즈니스 민첩성을 높여줍니다. 또한, UC(unified communications)와 비디오 관련 애플리케이션을 비롯해 기타 지연 시간에 민감한 애플리케이션 등 핵심 기술을 도입할 수 있도록 지원합니다. IoT 디바이스 사용 증가는 또한 이러한 동일 네트워크에서 추가적인 복잡성이나 리소스 없이 빠르게 확장할 수 있어야 함을 의미합니다. 이러한 IoT 디바이스 중 상당수가 네트워크 기능이 제한되어 있어 건물이나 캠퍼스 전반에 걸쳐 L2 네트워크가 가까이 있어야 한다는 한계가 있습니다. 일반적으로, 이러한 문제는 데이터 플레인 플러드 앤 런(flood and learn)을 통해 이러한 영역 전반에서 VLAN을 확장하여 해결할 수 있었습니다. 그러나 이러한 방식은 비효율적이며 관리하기가 어렵습니다.

이제는 경계에 한정된 문제가 아닌 보안 역시 또 다른 문제를 야기합니다. 현대의 기업들은 캠퍼스와 데이터센터를 포함해 전체 조직에 확장되어 있는 세그멘테이션과 정책 전반에서 보안이 네트워크 아키텍처에 내장되어 기능하기를 바랍니다.

주니퍼 네트웍스 Evolved Campus 솔루션

주니퍼의 EVPN/VXLAN 기반 캠퍼스 아키텍처는 VXLAN(Virtual Extensible LAN) 및 EVPN(Ethernet VPN)과 같은 기술을 사용하여 언더레이어부터 오버레이 네트워크를 분리합니다. 이렇게 하면 네트워크 관리자가 서로 다른 L3 네트워크에 논리적 L2 네트워크를 생성할 수 있으므로 현대 엔터프라이즈 네트워크의 요구 사항을 충족할 수 있습니다.

VXLAN은 캡슐화/터널링 프로토콜로 이더넷 프로토콜의 플러드 앤 런 동작을 변경하지 않습니다. 대신, MP-BGP를 사용하여 네트워크가 컨트롤 플레인에 있는 L2 MAC(Media Access Control) 및 L3 IP 정보 모두를 처리하도록 허용합니다. 포워딩 결정을 위한 MAC 및 IP 정보를 결합함으로써 VXLAN은 라우팅 및 스위칭을 최적화하는 한편, 확장은 BGP가 L2 MAC 및 L3 IP 정보(EVPN)를 전송할 수 있도록 지원하여 플러드 앤 런 문제를 해결합니다.

표준 기반 EVPN 솔루션을 캠퍼스 컨트롤 플레인 프로토콜로 운영하는 경우 다음 이점을 얻을 수 있습니다.

- 향상된 네트워크 효율성:
 - 컨트롤 플레인 MAC 러닝으로 알 수 없는 유니캐스트 플러딩 감소
 - 컨트롤 플레인에서 MAC-to-IP 바인딩을 활성화함으로써 ARP(Address Resolution Protocol) 플러딩 감소
 - 여러 개의 코어 스위치를 통한 다중 경로 트래픽 지원(VXLAN 암호화)
 - 액티브/액티브 듀얼 호밍 액세스 레이어 스위치에 대한 다중 경로 트래픽 지원
- 빠른 커버전스:
 - 멀티 호밍 액세스 스위치에 대한 링크 중 하나에 오류가 있는 경우 보다 빠른 리커버전스 지원
 - 엔드포인트 이동 시 보다 빠른 리커버전스 지원
- 확장성:
 - 확장 가능한 BGP 기반 컨트롤 플레인 제공
 - 필요 시 원활한 코어 확장, 분배 및 액세스 레이어 허용
 - 비즈니스 요구 증가에 따른 원활한 캠퍼스 확장 지원
- 유연성:
 - L3 및 L2 VPN을 통한 손쉬운 통합 가능
 - 세분화된 정책 적용이 가능한 BGP 기반 컨트롤 플레인 제공
- 비獨점:
 - 표준기반 프로토콜을 통해 멀티 벤더 코어, 디스트리뷰션 및 액세스 레이어 지원

오버레이를 통해 네트워크 어디에나 엔드포인트를 배치하고 동일한 논리적 L2 네트워크와의 연결을 유지해 가상 토플로지를 물리적 토플로지에서 분리할 수 있습니다. EVPN 컨트롤 플레인을 사용하여, 기업에서는 비즈니스 성장에 따라 필요한 더 많은 코어, 디스트리뷰션 및 액세스 레이어 디바이스를 손쉽게 추가할 수 있습니다. 즉, 네트워크를 다시 설계하거나 막대한 비용이 드는 업그레이드를 수행하지 않아도 됩니다.

EVPN/VXLAN 기반 아키텍처를 사용하므로 L2 및 L3 VPN을 사용하여 캠퍼스 전체에 공통된 일련의 정책 및 서비스를 구축할 수 있습니다. EVPN/VXLAN 오버레이와 함께 레이어 3 IP 기반 언더레이어를 사용하여, 캠퍼스 네트워크 운영자는 기존 L2 언더레이어 기반 아키텍처로 가능했을 보다 대규모의 네트워크를 구축할 수 있습니다.

Evolved Campus 아키텍처(그림 1 참조)에서는 코어 및 디스트리뷰션 레이어가 EVPN/VXLAN 오버레이가 있는 L3 패브릭을 형성합니다. 이상적으로는 언더레이어가 코어 및 디스트리뷰션 스위치를 포함하는 L3 Clos 모델을 통해 구축되어야 하지만 액세스 레이어 스위치는 디스트리뷰션 레이어에 멀티 호밍됩니다.

Clos 모델은 코어, 디스트리뷰션 및 액세스 레이어에서 일률적인 지연 시간과 수평적 확장성을 제공합니다. 사용자는 언더레이어로 OSPF와 같은 IGP(Interior Gateway Protocol) 또는 언더레이어 라우팅 프로토콜로 외부 BGP(EBGP) 중 하나를 사용할 수 있습니다. 이 솔루션에서는 RFC(Route Reflection)이 포함된 내부 BGP(IBGP) 오버레이 설계를 사용합니다. 이때, 주어진 성능 최적화 데이터센터(POD) 내 디스트리뷰션 디바이스는 루트 리플렉터(Route Reflector)로 작동하고 있는 코어 디바이스에 대한 EVPN 루트로 엔드포인트 정보 업스트림을 공유합니다. 코어 디바이스는 루트 다운스트림을 다른 디스트리뷰션 디바이스에 반영합니다. 루트 리플렉터를 사용하면 풀 메시 BGP를 연결하지 않아도 되며, 모든 디스트리뷰션 레이어 스위치에 일관된 구성이 적용되므로 디스트리뷰션 레이어 구성이 간편합니다.

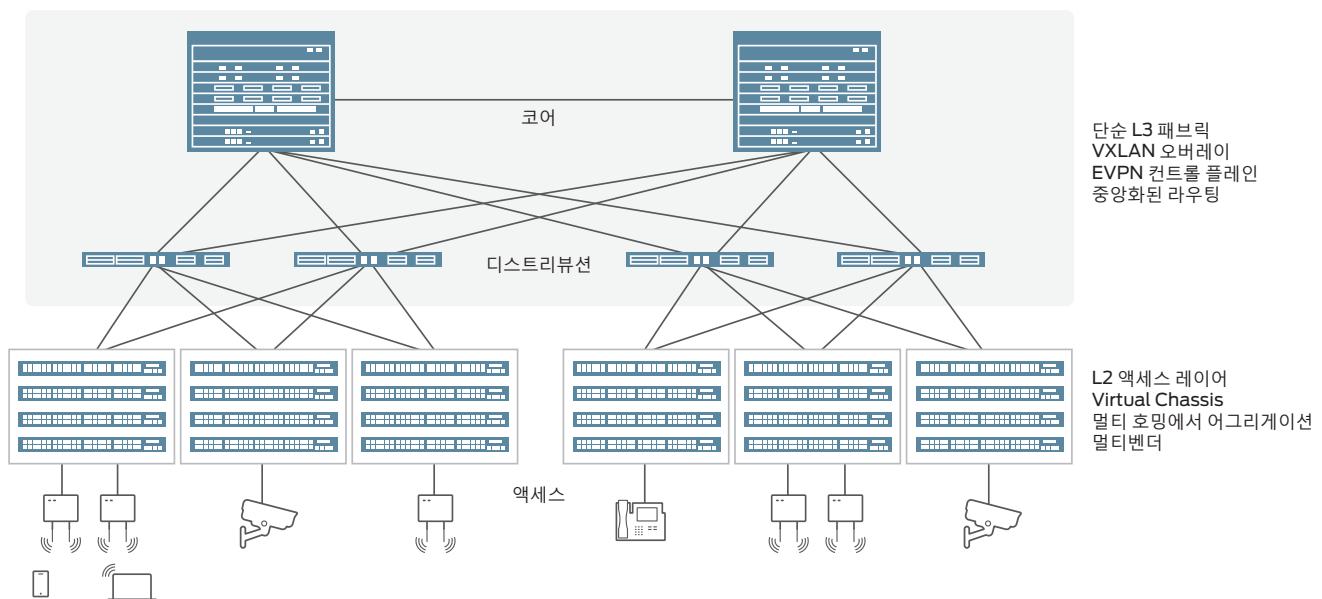


그림 1: Evolved Campus 상위 수준 아키텍처

최대 10개의 상호 연결된 플랫폼이 하나의 논리적 디바이스로 작동하도록 해주는 Virtual Chassis에 일반적으로 배포되는 액세스 레이어 스위치는 EVPN/VXLAN 패브릭의 일부가 아닙니다. L2 전용인 액세스 레이어는 엔드포인트를 VLAN에 매핑하며, 액세스 레이어에서 디스트리뷰션 레이어로의 멀티 호밍 업링크를 사용하여 디스트리뷰션 레이어까지 트렁크 포트로 이동합니다. 벤더의 제약을 받지 않는 이 솔루션은 엔터프라이즈가 기존 액세스 레이어 인프라를 사용하고 주니퍼나 다른 벤더로부터 액세스 레이어 스위치를 업그레이드할 수 있도록 지원합니다.

VLAN은 디스트리뷰션 레이어에서 VXLAN에 매핑되는 반면, L3 IRB(Integrated Routing and Bridging) 또는 VXLAN용 SVI(Switch Virtual Interface)는 앤리캐스트(anycast) 게이트웨어 주소가 있는 코어 스위치에 위치합니다. 유연하고 안전한 구성 옵션이란 IRB가 일반적인 라우팅 인스턴스(세그멘테이션이 필요한 경우에는 별도 라우팅 인스턴스)에서 배치될 수 있음을 의미합니다. 가상 라우팅 및 포워딩(VRF)과 마찬가지로, 라우팅 인스턴스는 네트워크가 멀티테넌시 및/또는 보안을 위해 세그먼트화되도록 해줍니다. 엔터프라이즈 보안 정책에 따라, 일부 루트는 인터 VRF 통신을 위해 라우팅 인스턴스 사이에서 누출될 수 있습니다. 또는 네트워크 세그멘테이션을 사용한 고급 보안 실행을 위해 인터 VRF 트래픽이 방화벽으로 강제 적용될 수 있습니다.

다른 주니퍼 아키텍처와 마찬가지로, Evolved Campus 아키텍처는 고객에게 새로운 디바이스에 투자하도록 강제하지 않습니다. 아래와 같이 다른 주니퍼 아키텍처에 사용된 동일한 디바이스를 Evolved Campus 구축 환경에서도 사용할 수 있습니다.

- 코어 레이어:
 - EX9204/EX9208/EX9214 이더넷 스위치
 - EX9251/EX9253 이더넷 스위치
- 디스트리뷰션 레이어:
 - EX4600 이더넷 스위치
 - QFX5110 스위치
- 액세스 레이어:
 - EX4300/EX3400/EX2300 이더넷 스위치
 - EX4200/EX3300/EX2200 이더넷 스위치
 - Virtual Chassis 기술
 - 비주니퍼 액세스 레이어 스위치

EVPN에서의 L2 및 L3 VPN 지원으로 EVPN/VXLAN 기반 패브릭의 이점을 캠퍼스, 데이터센터 및 퍼블릭 클라우드 전체에 확장할 수 있습니다(그림 2 참조). 캠퍼스, 데이터센터 및 퍼블릭 클라우드 인프라가 IP에 연결되어 있는 한 VXLAN은 WAN 언더레이와 무관합니다. EVPN/VXLAN 오버레이는 프라이빗 MPLS 및 인터넷을 통한 IPsec 등 다양한 WAN 기술을 사용하여 구축될 수 있습니다.

요약 - 엔터프라이즈의 EVPN 및 VXLAN 도입 필요성

엔터프라이즈의 IT 전략에 있어 클라우드 기반 리소스가 점점 더 많은 부분을 차지하고 있습니다. 이에 따라 보안이나 성능을 저하시키지 않으면서 클라우드 기반 서비스를 수용할 수 있는 네트워크 아키텍처가 필요합니다. 기존 네트워크 아키텍처로는 캠퍼스 사용자가 요구하는 시간 및 장소의 제약이 없는 상시 액세스와 높은 수준의 반응성을 충족하기가 점점 어려워질 것입니다. 캠퍼스 네트워크 내 IoT 디바이스 사용이 점점 늘어남에 따라 확장 및 프로그래밍이 가능하고 단순하며 멀티벤티 디바이스를 지원하는 개방형 아키텍처를 유지할 수 있는 네트워크가 필요해졌습니다.

EVPN 컨트롤 플레인과 VXLAN 오버레이를 기반으로 하는 주니퍼의 Evolved Campus 솔루션은 여러 곳의 캠퍼스, 데이터센터 및 퍼블릭 클라우드를 구축하고 상호 연결하기 위한 효율적이고 확장 가능한 방법을 제공합니다. 모든 플랫폼에 강력한 BGP/EVPN이 구축되어 있는 QFX 시리즈 스위치 및 EX 시리즈 스위치를 통해 주니퍼는 오늘날의 진화하는 캠퍼스 및 데이터센터 내외부 모두에 최적화된 원활한 표준 준수 L2 또는 L3 연결을 제공함으로써 EVPN 기술의 잠재력을 최대한 실현할 수 있도록 지원합니다.

다음 단계

자세한 정보는 주니퍼 담당자에게 문의하거나 www.juniper.net으로 이동하십시오.

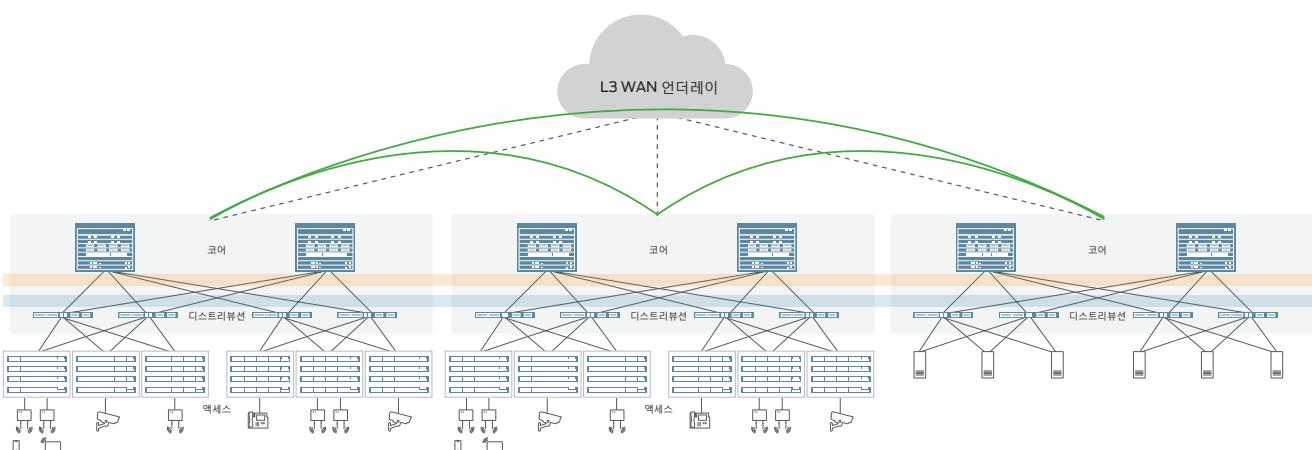


그림 2: EVPN/VXLAN 오버레이를 사용하여 여러 곳의 캠퍼스 및 데이터센터 상호 연결

주니퍼 네트웍스에 대하여

주니퍼 네트웍스는 세상을 연결하는 최고의 제품, 솔루션, 서비스를 통해 네트워킹 간소화를 지원합니다. 엔지니어링 혁신을 기반으로 클라우드 분야의 네트워킹 제약 조건 및 복잡성을 없앰으로써 고객들과 파트너들이 매일 마주하는 가장 까다로운 과제를 해결합니다. 주니퍼 네트웍스는 네트워크가 지식 공유는 물론 세상을 바꿀 인류의 진보를 위한 매개체라고 믿고 있으며, 비즈니스 성장 속도에 맞춰 확장 가능하고 자동화된 보안 네트워크를 구축하는 혁신적 방법을 찾아내기 위해 전념을 기울이고 있습니다.

본사

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
전화: 888.JUNIPER (888.586.4737)
또는 +1.408.745.2000
팩스: +1.408.745.2100
www.juniper.net

APAC 및 EMEA 본부

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
전화: +31.0.207.125.700
팩스: +31.0.207.125.701

Copyright 2018 Juniper Networks, Inc. All rights reserved. 주니퍼 네트웍스, 주니퍼 네트웍스 로고, 주니퍼 및 JUNOS는 미국과 기타 국가에서 주니퍼 네트웍스의 등록 상표입니다. 기타 모든 상표, 서비스 마크, 등록 상표 또는 등록 서비스 마크는 해당 소유 업체의 자산입니다. 주니퍼 네트웍스는 본 문서의 부정확성에 대해 일체의 책임을 지지 않습니다. 주니퍼 네트웍스는 예고 없이 본 문서의 내용을 변경, 수정, 이전 또는 개정할 권리를 보유합니다.

