The Evolved Campus

EVPN/VXLAN-Based Enterprise Networks

Challenge

Traditional campus networks are proprietary and too rigid to support the needs of endpoints in larger enterprises. These networks must also be flexible enough to accommodate IoT devices and provide consistent security at every layer, both within and across campuses.

Solution

Juniper's Evolved Campus solution, based on a VXLAN overlay with an EVPN control plane, offers an efficient and scalable way to build and interconnect multiple campuses, data centers, and public clouds.

Benefits

- Control plane-based L2/L3 information exchange
- Efficient host mobility
- Nonproprietary solution
- Scalability at all network layers
- Faster convergence
- Flexible and secure architecture

Enterprise networks around the world are adopting cloud and cloud-based applications to improve their competitiveness, lower IT costs, and provide users with anytime, anywhere access to resources and data. This trend, driven largely by the widespread use of mobile devices, social media, and collaboration tools, along with the growing number of Internet of Things (IoT) devices, is having a significant impact on enterprise campus networks. A growing number of network endpoints, coupled with rapidly evolving business needs, is driving demand for highly scalable networks that are not only simple, scalable, and programmable, but also built on a standards-based architecture that is common across both the campus and data center.

The Challenge

Most campus networks are based on conventional Layer 2 Ethernet-based architectures that eliminate the need for Spanning Tree Protocol. While these architectures work well in small and medium-sized campuses, where services are limited to a single network and cater to traditional campus requirements, they are simply too rigid to support the scalability needs of larger enterprises.

Cloud-based applications enable new business models, provide greater business agility, and support the adoption of key technologies such as unified communications, video, and other latency-sensitive applications. The increasing use of IoT devices also means that these same networks are expected to scale rapidly without adding complexity and resources. Since many of these IoT devices have limited networking capabilities, they require L2 adjacency across buildings or campuses. Traditionally, this problem was solved by extending VLANs across these areas using data plane flood and learn. This approach, however, is inefficient and hard to manage.

Security, which is no longer just a perimeter problem, also poses a unique challenge. Modern enterprises want security to be embedded into their network architectures—not just inside the campus, but through segmentation and policies extended across the entire organization, including data centers.

The Juniper Networks Evolved Campus Solution

Juniper's EVPN/VXLAN-based campus architecture decouples the overlay network from the underlay with technologies such as Virtual Extensible LAN (VXLAN) and Ethernet VPN (EVPN). This addresses the needs of the modern enterprise network by allowing network administrators to create logical L2 networks across different L3 networks.

VXLAN is an encapsulation/tunneling protocol and does not change the flood and learn behavior of the Ethernet protocol. Instead, it uses MP-BGP to allow the network to carry both L2 media access control (MAC) and L3 IP information in the control plane. By making the combined set of MAC and IP information available for forwarding decisions, VXLAN optimizes routing and switching, while the extension that allows BGP to transport L2 MAC and L3 IP information—EVPN—solves the flood-and-learn problem.

The standards-based EVPN solution offers the following benefits when operating as a campus control plane protocol.

- Greater network efficiency:
  - Reduces unknown unicast flooding with control plane MAC learning
  - Reduces Address Resolution Protocol (ARP) flooding by enabling MAC-to-IP binding in the control plane
  - Supports multipath traffic over multiple core switches (VXLAN entropy)
  - Supports multipath traffic to active/active dual-homed access layer switches
- Fast convergence:
  - Enables faster reconvergence when one of the links to multihomed access switches fail
  - Supports faster reconvergence when endpoints move
- Scalability:
  - Offers scalable BGP-based control plane
  - Allows seamless expansion of core, distribution, and access layers when needed
  - Supports seamless expansion of campuses as business needs grow
- Flexibility:
  - Enables easy integration with L3 and L2 VPNs
  - Delivers BGP-based control plane that allows application of fine-grained policies
- Nonproprietary:
  - Supports multivendor core, distribution, and access layers with standards-based protocols

With overlays, endpoints can be placed anywhere in the network and remain connected to the same logical L2 network, enabling a virtual topology to be decoupled from the physical topology. With an EVPN control plane, enterprises can easily add more core, distribution, and access layer devices as the business grows—without having to redesign the network or perform a forklift upgrade.

The EVPN/VXLAN-based architecture lets you deploy a common set of policies and services across campuses with support for L2 and L3 VPNs. Using a Layer 3 IP-based underlay coupled with an EVPN/VXLAN overlay, campus network operators can deploy much larger networks than would otherwise be possible with traditional L2 Ethernet-based architectures.

In an evolved campus architecture (see Figure 1), the core and distribution layers form a L3 fabric with an EVPN/VXLAN overlay. Ideally, the underlay would be deployed using the L3 Clos model with core and distribution switches, and the access layer switches would be multihomed to the distribution layer.

The Clos model provides an architecture that enables deterministic latency and horizontal scale at the core, distribution, and access layers. You can use either an interior gateway protocol (IGP) like OSPF as the underlay or external BGP (EBGP) as the underlay routing protocol. This solution uses an internal BGP (IBGP) overlay design with route reflection, where distribution devices within a given performance-optimized data center (POD) share endpoint information upstream as EVPN routes to the core devices that are acting as route reflectors. The core devices reflect the routes downstream to the other distribution devices. Using route reflectors eliminates the need for full-mesh BGP connections and simplifies configuration at the distribution layer with consistent configuration across all distribution layer switches.

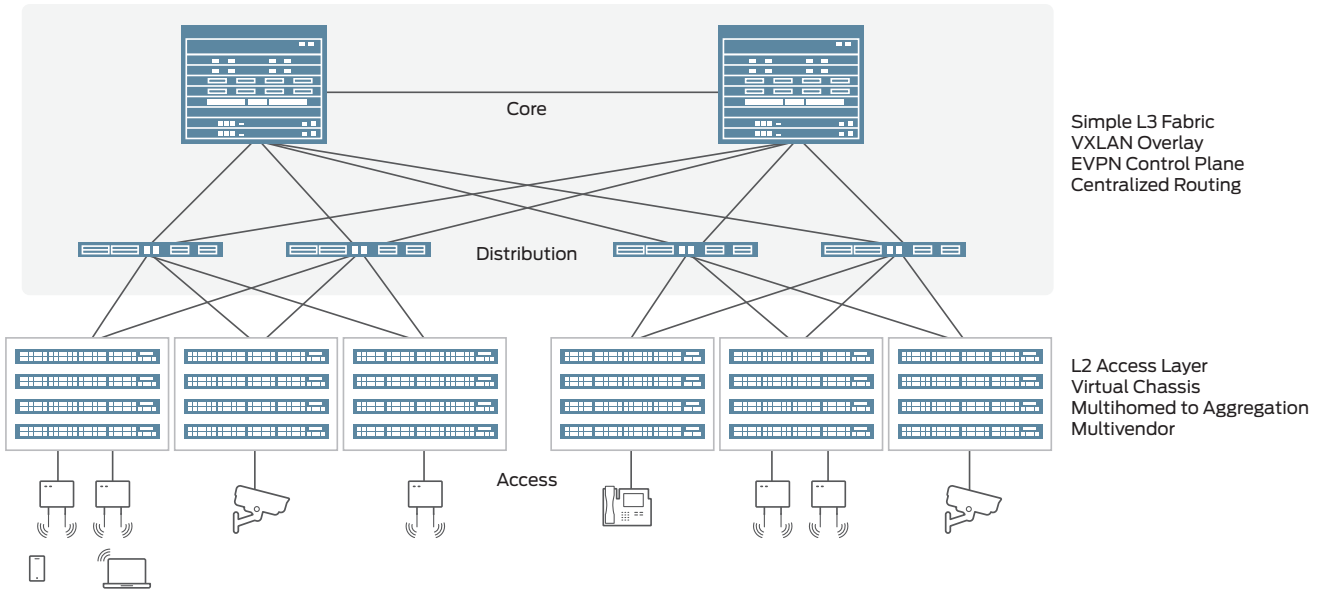

Figure 1: Evolved Campus high-level architecture

The access layer switches, typically deployed in a Virtual Chassis configuration that allows up to 10 interconnected platforms to operate as a single, logical device, are not part of the EVPN/VXLAN fabric. The access layer, which is L2 only, maps endpoints to VLANs, which are carried in trunk ports up to the distribution layer using the multihomed uplinks from the access layer to the distribution layer. This vendor-agnostic solution allows enterprises to use the existing access layer infrastructure and upgrade to access layer switches from Juniper or any other vendor.

VLANs are mapped to VXLANs at the distribution layer, while L3 Integrated Routing and Bridging (IRB) or switch virtual interface (SVI) for the VXLANs are located on the core switch with an anycast gateway address. Flexible and secure configuration options mean that IRBs can be placed in a common routing instance or, if segmentation is required, in separate routing instances. Similar to virtual routing and forwarding (VRF), routing instances enable the network to be segmented for multitenancy and/or security. Based on the enterprise security policy, some routes can be leaked between routing instances for inter-VRF communication, or inter-VRF traffic can be forced through a firewall for advanced security enforcement with network segmentation.

Like other Juniper architectures, the evolved campus architecture does not force customers to invest in new devices; the same devices used in other Juniper architectures can be used in an evolved campus deployment, as shown below.

- Core layer:
  - EX9204/EX9208/EX9214 Ethernet Switches
  - EX9251/EX9253 Ethernet Switches
- Distribution layer:
  - EX4600 Ethernet Switch
  - QFX5110 Switch
- Access layer:
  - EX4300/EX3400/EX2300 Ethernet Switches
  - EX4200/EX3300/EX2200 Ethernet Switches
  - Virtual Chassis technology
  - Non-Juniper access layer switches

The benefits of the EVPN/VXLAN-based fabric can be extended across campuses, data centers, and public cloud infrastructure with L2 and L3 VPN support in EVPN (see Figure 2). VXLAN is WAN underlay agnostic as long as the campuses, data centers, and the public cloud infrastructure have IP connectivity. The EVPN/VXLAN overlay can be deployed over a variety of WAN technologies, including private MPLS and IPsec over Internet.

Summary—Enterprises Must Embrace EVPN and VXLAN

Cloud-based resources are becoming an increasingly large part of the enterprise's IT strategy. This requires a network architecture that can accommodate cloud-based services without compromising security or performance. The demands of campus users for anytime, anywhere access and high levels of responsiveness are becoming harder and harder to achieve with traditional network architectures. The increasing prevalence of IoT devices in campus networks demands a network that is not rigid and can still maintain an architecture that is scalable, simple, programmable, open, and supports multivendor devices.

Juniper's Evolved Campus solution, based on a VXLAN overlay with EVPN control plane, is an efficient and scalable way to build campuses and interconnect multiple campuses, data centers, and public clouds. With a robust BGP/EVPN implementation on all platforms— QFX Series switches, EX Series switches— Juniper is uniquely positioned to bring EVPN technology to its full potential by providing optimized, seamless, and standards-compliant L2 or L3 connectivity, both within and across today's evolving campuses and data centers.

Next Steps

For more information, please contact your Juniper representative, or go to www.juniper.net.

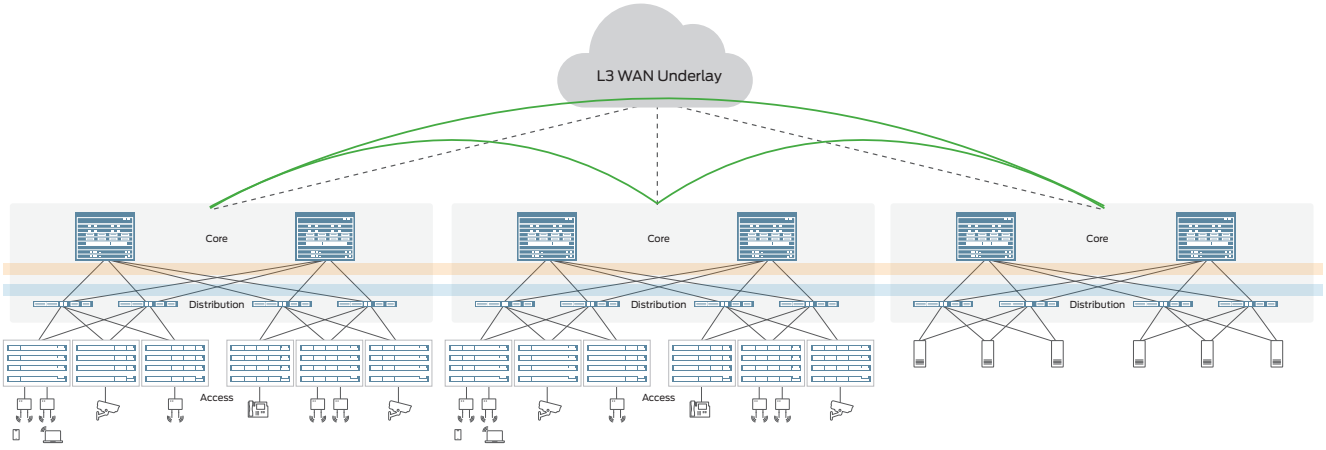

Figure 2: Interconnecting multiple campuses and data centers with an EVPN/VXLAN overlay

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3510643-001-EN June 2018