VXLAN and the BIG-IP Platform

BYOD, cloud computing, big data, and converged communications are rapidly forcing networks beyond the abilities to scale and manage efficiently that are provided by current standards and best practices. VXLAN is a result of SDN and network virtualization efforts that strive to shift the burden from operations to technology. F5 BIG-IP platform support for VXLAN enables organizations to seamlessly transition from traditional to virtual network architectures, providing the scale and agility necessary to meet today's operational and business challenges.

by Lori MacVittie
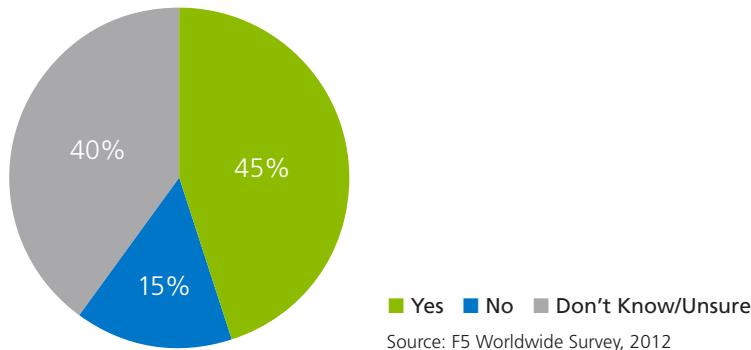Senior Product Manager, Emerging Technologies

Contents

Introduction

The pressure on network operations to support a growing, dynamic, and volatile set of technologies continues to increase. IT organizations are adopting technologies like cloud computing to realize the operational benefits of economies of scale and more effectively manage the explosive growth of data, devices, and applications. As organizations undertake the transformation required to support the more fluid and agile environment associated with the cloud, they are finding that current data center networking architectures are a limiting factor. Mobility of workloads is assumed to be a core capability of a dynamic data center, but traditional network constraints can impede this mobility, limiting it to layer 2 domains defined by standard protocols such as VLAN.

VLAN and switching boundaries are not flexible or easily extended. As requirements expand and contract, compute and storage resources need to be provisioned without excessive operational overhead. Virtual machine mobility and fault tolerance solutions are generally designed to operate best with flat, layer 2 networks, but managing such an architecture at scale is operationally difficult. On top of these core networking challenges come the limitations inherent in traditional VLAN and IP address management techniques. As resources are provisioned, de-provisioned, and moved throughout the network domain, simply maintaining the core network becomes a challenge, especially when strong isolation is required.

To address these challenges, VMware, in partnership with leading networking and silicon vendors, has created the VXLAN technology. VXLAN is a virtual networking protocol that enables the creation of dynamic, virtual layer 2 domains atop an existing switched network. VXLAN uses standard Ethernet technology, giving organizations the ability to extend existing networks by creating virtual overlay networks that can be isolated from each other as well as from the underlying network. Virtual networking is an increasingly attractive solution to the challenges imposed by the need for agility and elasticity in the underlying network.

Organizations Planning to Deploy Network Virtualization
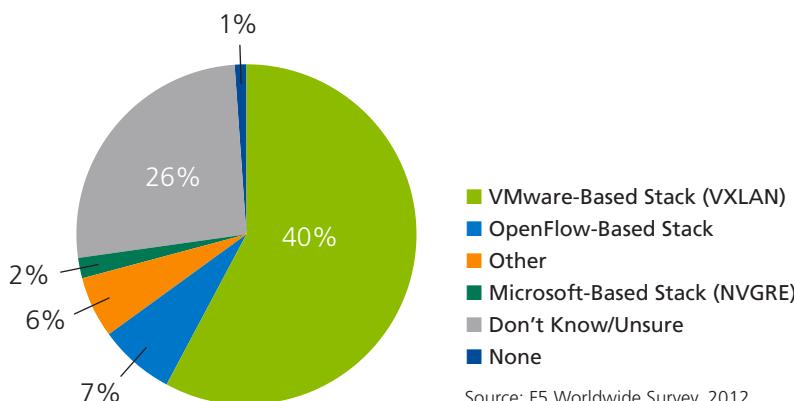

■ Yes ■ No ■ Don't Know/Unsure
Source: F5 Worldwide Survey, 2012

Figure 1: In a 2012 F5 worldwide survey with 1,361 respondents, 45 percent indicated plans to deploy network virtualization technologies.

VXLAN continues to gain traction in the market, eliciting interest and implementation plans alike. In an F5 worldwide survey of over a thousand IT professionals, 58 percent of respondents who were planning to deploy network virtualization indicated they intended to take advantage of VXLAN—more than all other virtual network protocol stacks combined.

This is unsurprising. VXLAN offers organizations a solution to the challenges of cloud and elastic scale without requiring a completely new network architecture. This is particularly important for enterprises required to support applications that rely on traditional networking alongside those needing the dynamic and flexible networking of elastic application and software-defined data center initiatives.

Stacks/Protocols That Organizations Plan to Use in Network Virtualization Environments

■ VMware-Based Stack (VXLAN)
■ OpenFlow-Based Stack
■ Other
■ Microsoft-Based Stack (NVGRE)
■ Don't Know/Unsure
■ None

Source: F5 Worldwide Survey, 2012

Figure 2: Respondents in a 2012 F5 worldwide survey indicated a strong preference for VXLAN over other virtual networking technologies.

Networking with VXLAN

VXLAN provides the ability to create isolated, multi-tenant broadcast domains across data center networks, enabling organizations to define elastic, logical networks able to span physical network boundaries. It accomplishes this by creating logical, layer 2 networks encapsulated in standard layer 3 IP packets.

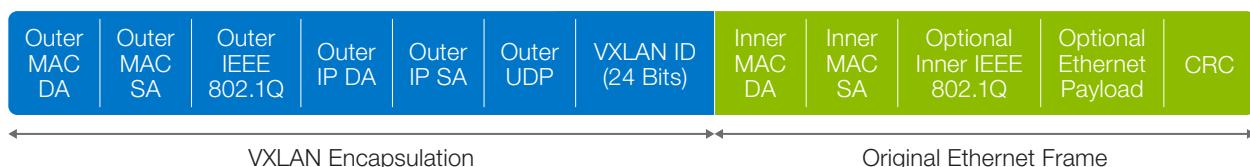| Outer MAC DA	Outer MAC SA	Outer IEEE 802.1Q	Outer IP DA	Outer IP SA	Outer UDP	VXLAN ID (24 Bits)	Inner MAC DA	Inner MAC SA	Optional Inner IEEE 802.1Q	Optional Ethernet Payload	CRC

VXLAN Encapsulation   Original Ethernet Frame

Figure 3: VXLAN extends standard Ethernet frames, enabling the coexistence of virtual networks with traditional IP networks.

A segment ID in every frame designates which VXLAN logical network the packet belongs to and eliminates the need for VLAN tags. The segment ID is significantly longer than traditional VLAN tag IDs, allowing for much larger logical networks; VXLAN can support up 4 million network segments versus a VLAN network's 4,096 segments.

The use of a separate segment ID also ensures coexistence with existing network architectures.

VXLAN 1
VXLAN 2
IP Network
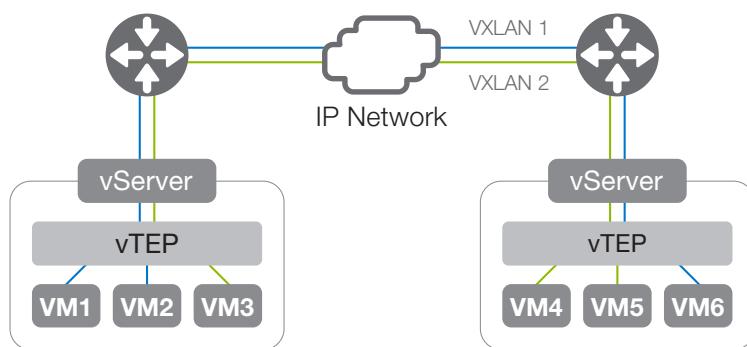vServer
vTEP
VM1 VM2 VM3
vServer
vTEP
VM4 VM5 VM6

Figure 4: VXLAN creates tunnels between two virtual tunnel end points (vTEPs), allowing physically dislocated resources to communicate as though they were on the same network segment.

Compatibility with Traditional Networks

While coexistence of a VXLAN-based virtual network with traditional networks is ensured because of its foundation on existing Ethernet standards, compatibility with traditional networking requires additional capabilities. This is especially true when hosts on a VXLAN virtual network need to communicate with hosts on a non-VXLAN network, such as one based on VLAN.

In the virtual network architecture, VXLAN encapsulation is performed on the host between a virtual machine's virtual network interface controller (NIC) and its logical port on the associated virtual switch. This end point is referred to as a virtual tunnel end point (vTEP), and it forms the basis for the logical, layer 2 virtual network. The tunnels provide isolation of traffic and the vTEP offers a measure of protection by allowing only traffic with the appropriate VXLAN segment ID to traverse the logical network.

While this model can coexist with a traditional IP network, it does not provide for compatibility with hosts residing on a traditional IP network segment. Compatibility requires a VXLAN gateway to translate between VXLAN and VLAN segments and allow traffic to traverse both networks.

The BIG-IP Platform and VXLAN

F5® BIG-IP® products deliver native support for VXLAN as well as offering vTEP capabilities. This means BIG-IP products, in any form factor, can act as a gateway, bridging VXLAN and non-VXLAN networks with equal alacrity and enabling organizations to consistently apply Application Delivery Networking services across both virtual and traditional networks.

It also means that organizations can take a transitory approach to migration of resources and systems, avoiding the disruption otherwise required. This is particularly important for maintaining existing infrastructure in the layer 2 network, where VXLAN requires an increase in the size of packets to accommodate the additional information necessary to create and properly route the virtual network. While increasing the maximum transmission unit (MTU) of a network is generally considered a boon for throughput and performance, failure to do so across the entire network can be devastating to performance. An organization unwilling or unable to make such a change across the data center will benefit from the ability to deploy BIG-IP devices as a gateway and avoid the disruption of VXLAN's underlying technical requirements.
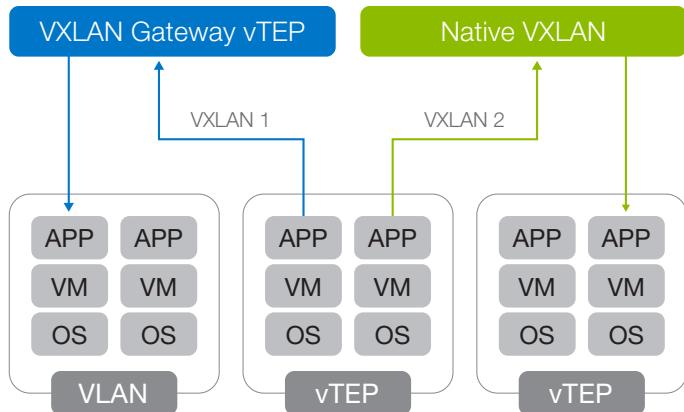
Figure 5: A VXLAN gateway permits virtual and physical networks to communicate.

The support provided by the BIG-IP platform for both native VXLAN and gateway vTEP services enables organizations to make all application network services available to all application workloads, irrespective of the underlying network topology. Organizations with heterogeneous networks find that a unified gateway approach to providing services offers more consistent and predictable results for application delivery.

Additionally, cross-environment portability is made possible by eliminating the need to change IP addresses during migrations. This requirement, which is necessary in traditional network environments, has hampered the mobility of IP-dependent applications. VXLAN-based networks, offering functional isolation, eliminate this requirement and enable the migration of enterprise-class, IP-dependent applications, improving the success of business continuity and disaster recovery initiatives.

Conclusion

Applications running across networks encounter a wide range of performance, security, and availability challenges. Many of these challenges are made more complex by the introduction of cloud computing and the drive toward software-defined data centers. Virtual networking technology attempts to address some of these challenges by introducing the ability to separate logical from physical networks with protocols such as VXLAN, thus freeing applications from constraints imposed by a more fixed network architecture.

The need to support both traditional IP networks and virtual VXLAN-based networks, however, introduces its own challenges both at the network and application layers.

BIG-IP products in both physical and virtual form factors support the native VXLAN and vTEP capabilities required to seamlessly interoperate and transition between traditional IP and VXLAN-based virtual networks.

By taking advantage of the BIG-IP platform, organizations can approach this virtual network technology with a transitional strategy, avoiding the disruption caused by technical requirements while reaping the benefits of a more agile, dynamic application infrastructure. Furthermore, they can achieve this benefit without compromising their ability to consistently apply and enforce the application network services critical to meeting the business expectations of performance, security, and application scalability.

F5 Networks, Inc.   401 Elliott Avenue West, Seattle, WA 98119   888-882-4447   www.f5.com