Using Software-Defined Data Centers to Enable Cloud Adoption

Juniper-VMware Areas of Collaboration

By:
Daniel McGinniss, Juniper Networks
Scott Lowe, VMware

Table of Contents

Executive Summary

Customers looking to cloud technologies for better application agility and more efficient support of their entire IT operations are finding that broader use of virtualization across hardware is fundamental to achieving these goals. Not only is virtualization a method of unifying capabilities across a varying set of hardware and software components, it is also an enabler for enhanced features such as orchestration, automated provisioning, workload mobility and multitenancy. By creating a hardware abstraction layer and employing virtualization, technology companies like VMware and Juniper Networks have long been able to mask the complexity of disparate hardware. As a result, customers have realized increased levels of efficiency and accelerated time to market.

Many IT professionals, however, will argue that most of these enhancements have remained within their respective silos of storage, compute, and network, thereby making provisioning and orchestration across these silos far too complex and disjointed. There are certainly some pieces of software that can glue the different components together, but the underlying silos are not truly integrated at the most fundamental levels.

This is why Juniper and VMware are expanding their long-standing partnership. Working in tandem, VMware and Juniper will collaborate to extend the capabilities of virtualization to deliver a tightly integrated solution using standards-based protocols and open APIs. This will make it possible to break through silos, and customers will benefit by being able to take advantage of the flexibility of network overlays and Network Functions Virtualization (NFV) while maintaining the same levels of performance and reliability their businesses require.

Introduction: New Technology, New Challenges

To understand the need for a joint solution and why it is critical to our customers' success, it's important to recognize the challenge presented as customers look to take advantage of new technologies to build next-generation cloud networks.

First, let's consider the three different classifications of resources found in most data centers today:

1. **Non-virtualized servers** (sometimes referred to as bare metal machines) such as non-x86 servers (UNIX, mainframes), storage (NAS, iSCSI SANs), and certain database and high-performance compute instances (financial trading applications, big data)

2. **Virtualized servers** running vSphere, Hyper-V, KVM, or Xen

3. **Layer 4-7 appliances** such as firewalls, load balancers, or Network Address Translation (NAT) devices

When these resources need to communicate with each other, they typically rely on ASIC-based routers and switches to facilitate this connectivity. The protocols these resources use are very mature and well understood by these devices. The maturity of these protocols is a good thing, but we also realize that there isn't a good handoff from the resources to the networks and services.

As customers begin to take advantage of cloud computing operational models and cloud management platforms, they find that network virtualization is key to success in these initiatives. While network virtualization is often used interchangeably with other terms like SDN, network overlays, and NFV, network virtualization encompasses all of these various forms of innovation within the networking space. And when customers implement a technology such as VMware NSX to support their cloud computing initiative, they introduce a fourth classification of resources into the network:

4. **SDN-enabled cloud servers** running a network virtualization solution like VMware NSX

When customers create this new type of resource, it not only introduces new protocols into the network, but it also creates an entirely new set of methods for provisioning resources, automating tasks, applying security, and enabling communication between resources.

Although a network virtualization solution like VMware NSX is hardware-independent, a physical network that openly integrates with the network virtualization platform can allow customers to more fully realize the benefits of network virtualization. Working hand-in-hand, Juniper and VMware are committed to innovating around the tight integration of the network virtualization solution and the underlying physical network through standards-based protocols, open APIs, and open source projects. This innovation will enable Juniper and VMware customers to address the challenges that arise from the use of new technologies as they adjust their infrastructure to meet business needs.

The Partnership

Juniper and VMware agree that network virtualization is a fundamental ingredient to enabling cohesive management and orchestration across entire IT infrastructures. This, in turn, will enable customers to achieve their goals of efficient IT operations and application agility through cloud computing operational models.

The key to realizing the promise of the cloud is having a tight integration across all the technology silos to which it is applied. Implemented correctly, network virtualization can offer significant opportunities to instantiate applications and services faster than ever before with fewer manual processes. Removing manual processes also inherently reduces risk, lowers costs, and decreases time to market.

Most software tools that attempt to stitch the IT silos together do so from the top down, which can simplify the user experience but often at the expense of network or even application visibility. With network virtualization, we approach the problem from the bottom up. While this may offer a much more powerful solution, the challenge in this bottom-up approach is that there needs to be an increased level of collaboration during the entire development process—it cannot be an afterthought. Working closely throughout the development process ensures that the solution is interoperable and takes an end-to-end approach.

This is why Juniper and VMware are working strategically to develop a tightly integrated joint solution—one that is tested and validated, and will be easy to build and operate.

Together, Juniper and VMware are focused on four key areas of collaboration to help overcome the obstacles without compromise and move the industry innovation forward:

1. Smart forwarding across physical and virtual infrastructure
2. End-to-end visibility and management for simplified operations
3. Telemetry and analytics that help proactively detect and auto-correct anomalies
4. Application/flow-based traffic handling that maximizes application efficiency and performance

1. Smart Forwarding Across Physical and Virtual Infrastructure

When we look at the four classifications of resources in customer data centers, we can assume that each type will have to talk to every other type at some point. Web servers hosted in a network virtualization-powered cloud will have to talk to bare metal database servers, and resources in one data center will need to connect to resources in another data center or in a remote cloud. How do we ensure that a cloud host running VMware NSX and using an overlay protocol, such as VXLAN, can communicate with resources outside VMware NSX that don’t understand an overlay protocol?

We can look to MPLS for our answer. Customers building MPLS-enabled WANs today leverage the concept of a provider edge (PE) router. The PE router handles all encapsulation and decapsulation so that resources outside the MPLS network don’t need to understand MPLS. That same concept can be leveraged for overlay protocols and network virtualization. A gateway serves the same purpose in VMware NSX environments: it handles the encapsulation and decapsulation so that resources outside the VMware NSX logical networks don’t need to understand VMware NSX or an overlay protocol.

VMware does offer an x86-based solution that can handle this function, but also recognizes that just as some customers are reliant on hardware-based routers and switches with purpose-built ASICs to deliver consistent results at wire speed, some customers will look for hardware-based solutions to provide the functionality of a gateway.

This is where Juniper’s universal SDN gateway complements VMware NSX by offering the most flexible set of VXLAN Tunnel Endpoint (VTEP) gateways that perform at line rate and are highly redundant. By utilizing both best-in-class merchant silicon and their programmable ASICs, Juniper can help provide seamless, high-performance connectivity between resources inside and outside of VMware NSX logical networks.

For connectivity inside the data center, Juniper’s universal SDN gateway offers three potential use cases:

1. **Layer 2 Gateway** provides connectivity within the same broadcast domain, as if the devices were connected to the same physical switch. This provides simple and easy connectivity between workloads attached to a VMware NSX logical network and bare-metal workloads, traditional virtualized workloads, and network appliances.
2. **Layer 3 Gateway** enables connectivity between different broadcast domains where a router would traditionally be needed to communicate. This allows customers to connect subnets inside a VMware NSX logical network with subnets outside of VMware NSX.
3. **SDN-to-SDN Gateway** supplies connectivity between workloads in different VMware NSX domains that are managed by different VMware NSX controllers. The SDN-to-SDN gateway functionality seamlessly stitches together the data planes and federates the control planes of these “islands of SDN.”

Additionally, for connectivity between data centers or to remote clouds, Juniper offers an additional use case:

4. **WAN Gateway** connects VMware NSX logical networks directly to the WAN via MPLS, VPLS, Ethernet VPN (EVPN), IPsec, generic routing encapsulation (GRE), or the Internet.

By integrating these hardware gateway capabilities with features like in-service software upgrades (ISSU) and multichassis link aggregation group (MC-LAG), Juniper will help customers feel confident in their deployment strategy as they migrate their workloads to an NSX cloud.

2. End-to-End Visibility and Management for Simplified Operations

To help guarantee the success of any new technology, it needs to be simple to consume by those deploying it. In highly virtualized data centers running workloads using hypervisors like vSphere, KVM, or Xen, end-to-end visibility and management of those virtualized workloads can be challenging. Traditionally, the connection between the physical network and the virtual network has either not been possible or has been an afterthought. Users have been able to tolerate not having a strong linkage between physical and virtual networks, despite the challenges that this can create in providing operational and management simplicity and efficiency. But as network overlays are integrated into our solutions, the industry is quickly realizing that there is an almost mandatory requirement that the physical and virtual networks be in sync.

A fundamental characteristic of an overlay is that it is provisioned atop an existing physical network; this physical network is typically referred to as the underlay network. This essentially creates a blind spot that can hinder an operator's ability to manage or visualize what this virtual network looks like and to what it connects. Similar to other networking encapsulation mechanisms like GRE or MPLS, logical network traffic is now encapsulated across the physical network. Underlay networks no longer need to know about things like Layer 2 host information or IP routing for logical networks; when it pertains to routing and switching, their role is limited to providing reachability so the tunnel (or label-switched path, to borrow an MPLS term) can be formed between two endpoints.

For all of the possibilities that network virtualization offers—such as multitenancy, enhanced orchestration, and increased logical scale—the use of an overlay can disrupt the operational model to which we have become accustomed. For anyone who has worked in an environment using an overlay (GRE or MPLS are good examples), they understand that without the proper tools, the ability to understand and troubleshoot these networks is quite difficult. This includes things like determining the path of a particular flow, knowing if the tunnel is or isn't operable, or knowing the location of the endpoints and the devices or subnets reachable from within those endpoints. These are all things that can easily be taken for granted in a traditional IP network, but must be taken under serious consideration when the physical and logical networks are decoupled.

To prevent this from happening, Juniper and VMware believe it is essential for there be an intelligent exchange of information between the hardware and software elements that comprise the end-to-end solution. Furthermore, we believe this should be achieved by adhering to open standards. VMware NSX offers a RESTful API for management solutions that provides programmatic access to all of the information contained within—information such as host and VM details, current and trended traffic statistics, and overlay endpoints. Together, Juniper and VMware are working to create a loosely coupled but tightly integrated management tool for physical and logical (virtual) network topologies. Juniper Networks® Junos® Space Network Director will be fully NSX-aware and capable of being the "single pane of glass" that will allow customers to deploy cloud technologies without sacrificing operational control or visibility. This integration and awareness will take a couple of different forms:

- Junos Space Network Director will interact with the NSX API to retrieve the virtualized data center and logical network information.
- VMware NSX will provide flow-level information via IPFIX, and Network Director will digest and analyze this flow-level information.

Sharing data between the VMware NSX management layer and Junos Space Network Director enables customers to use correlated analytics for virtual/physical topology visibility, dynamic threshold detection, trending analysis, root cause detection, and automated resource placement. Currently, hypervisors such as VMware vSphere offer automated resource placement on the basis of compute-centric properties (such as RAM or CPU capacity); this joint Juniper-VMware integration at the networking layer enables network-aware automated resource placement.

Junos Space Network Director will offer comprehensive and unified visibility across virtual and physical networks through a new dashboard. This new dashboard will allow customers to monitor, troubleshoot, and report, and will allow the user to drill down into the underlay network, the overlay network, applications, and tenant networks to view inventory and performance information in a correlated fashion.

3. Telemetry and Analytics that Help Proactively Detect and Auto-Correct Anomalies

One of the promises of the software-defined data center (SDDC) is for enterprise IT and cloud builders to deliver application-driven service-level agreements (SLAs). Application-driven SLAs are notoriously difficult to enforce because different applications present different demands to the network. Further, the lack of a strong connection between the virtualized workloads in the hypervisor and the physical network complicates the challenge of application-driven SLAs. So how can Juniper and VMware work together to solve this on behalf of customers?

The Juniper-VMware joint telemetry solution will enable robust SLAs through the following areas of collaboration:

- Hardware telemetry support in Juniper products will enable very fine-grained visibility of physical network traffic statistics and latency (with nanosecond levels of accuracy). This will also provide per-hop atomic counters for the physical underlay network, information that could be used to help determine the best path through the network for a particular application.
- The VMware EPSEC and NSX APIs enable overlay monitoring and application-level visibility provided by the hypervisor (when workloads are running on VMware vSphere). These APIs will allow the joint solution to integrate and understand application requirements.

Together, the joint Juniper-VMware solution will provide application-level visibility of VXLAN traffic by keying off a common attribute across compute, storage, and network. The solution will collect data from the underlay and the overlay, detect issues, and give feedback to orchestrate and place workloads in the optimal location. For example, the solution could detect a single tenant exhibiting high network I/O behavior in a multitenant environment, and modify the equal-cost multipath (ECMP) algorithm or adjust the quality of service (QoS) for this errant tenant.

4. Application/Flow-Based Traffic Handling that Maximizes Application Efficiency and Performance

Different types of network traffic have different needs from the physical underlay network. One example is network flows that are very short-lived, bursty, and latency sensitive. These flows are often referred to as “mice flows.” There are also network flows that are long-lived and quite bandwidth intensive; these flows are often called “elephant flows.” If not identified and addressed, elephant flows can overwhelm mice flows in the data center, causing application performance problems. Traditional protocols and techniques such as ECMP can’t and don’t identify elephant flows or handle them differently.

However, virtual switches in the hypervisors at the edge of a network virtualization solution are well-positioned to identify elephant flows, and provide signaling to the physical underlay network to handle such flows differently and in a way that doesn’t impact smaller mice flows.

Working together, the Juniper and VMware joint solution will identify elephant and mice flows at the virtual switch layer, and then uniquely tag them for identification by the physical network. The physical network will then use one of two methods to ensure that elephant flows don’t squash mice flows:

- Elephant flows will be queued differently, or
- Elephant flows will be dynamically load-balanced and moved to different network paths to reduce congestion.

By leveraging the tagging provided by VMware NSX in the hypervisor, Juniper physical network equipment can use this information to intelligently direct traffic flows across the data center in the most efficient manner possible, and in a manner that ensures each type of flow—both the short-lived latency-sensitive flows as well as the long-lived bandwidth intensive flows—is given appropriate consideration and handling. The end result for customers is a more efficient data center network. Further, the identification of elephant flows can be passed up to management systems for additional fine-tuning of applications, the overlay network, workload placement, and the physical underlay network.

This capability is not limited to just elephant and mice flows. Customers can also take advantage of NSX’s ability to pass DiffServ code point (DSCP) markings to the physical network, where Juniper will utilize those markings to deliver end-to-end QoS within the data center and across the wide area network.

Conclusion

Juniper and VMware are committed to expanding their relationship and will continue to extend the capability of network virtualization and deliver a solution that is open and tightly integrated. We look forward to helping our customers realize the benefits of these new technologies by jointly focusing on the following key areas:

1. Smart forwarding across physical and virtual infrastructure
2. End-to-end visibility and management for simplified operations
3. Telemetry and analytics that help proactively detect and auto-correct anomalies
4. Application/flow-based traffic handling that maximizes application efficiency and performance

VMware and Juniper believe that by collaborating in these four key areas, we can deliver greater value to our shared customers that are deploying VMware NSX in conjunction with Juniper's routing, switching, and security solutions.

About VMware

VMware is the leader in virtualization and cloud infrastructure solutions that enable businesses to thrive in the Cloud Era. Customers rely on VMware to help them transform the way they build, deliver and consume Information Technology resources in a manner that is evolutionary and based on their specific needs. With 2013 revenues of $5.21 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

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