White Paper

SDN Unlocks New Opportunities for Cloud Service Providers

Prepared by

Caroline Chappell
Senior Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.juniper.net

March 2014
Executive Summary

The market for enterprise cloud services is buoyant and set to experience rapid growth over the next few years, driving data center demand. Companies that own data centers have an excellent opportunity to cut out “middleman” cloud service providers and expand into infrastructure-as-a-service (IaaS) delivery themselves.

But cloud service providers need to differentiate themselves in the IaaS market. Cloud compute and storage solutions may be commoditizing, but there is still a large amount of variation in cloud service providers’ networking and security capabilities. Traditional data center networking technologies are inflexible and require time-consuming manual management, which has an impact on virtual machine (VM) provisioning times, scaling dynamics and the types of complex cloud models, such as hybrid cloud, cloud service providers can support.

Cloud service providers are turning to software-defined networking (SDN) technology to address networking issues within their data centers. SDN provides an overlay on top of the physical network so that virtual connections between VMs can be configured quickly, automatically and at scale. This makes it far easier for cloud service providers to manage the dynamism of VM creation and migration in the cloud and to support hybrid cloud approaches, where workloads may move seamlessly between the service provider’s data center and the enterprise private cloud. Such capabilities enable cloud service providers to offer a superior IaaS experience to enterprise customers.

However, the proliferation of SDN solutions entering the market is bewildering. Cloud service providers need to consider the pros and cons of different SDN approaches carefully. To future-proof themselves, cloud service providers will want to benchmark the degree to which different vendors’ products are open, for example. They will also need to evaluate the performance, security and resilience advantages associated with Layer 3-based SDN solutions that use Border Gateway Protocol (BGP) routing, which is tried and tested in the largest service provider networks worldwide. Enabling data center networks to implement carrier-grade networking technology is a key advantage of SDN and one that can help to differentiate cloud service providers delivering IaaS.

This white paper discusses the IaaS opportunity for data center owners and the requirement for improved network management and agility, which can be met through SDN.

Section II looks at the enterprise requirements driving demand for IaaS and the attributes data center owners can leverage to become cloud service providers.

Section III describes how SDN can address data center networking challenges and the advantages of a Layer 3-based SDN approach.
Taking Advantage of the Cloud Opportunity

Data Center Providers Are Well Positioned to Exploit IaaS Growth

As the enterprise cloud market gathers pace, data center owners have a major opportunity to upsell cloud services to existing colocation and managed services customers, becoming cloud service providers. Enterprises that outsource their IT infrastructure needs are proving highly receptive to IaaS solutions, according to Heavy Reading research. Cloud service providers can also target IaaS services at software-as-a-service (SaaS) providers, which want to deliver applications from the cloud but don’t have the means to invest in data center infrastructure themselves.

Compared with IT infrastructure outsourcing, IaaS further cuts the time and cost for companies wanting to provision and deliver new applications. Enterprises see IaaS as a cost-effective way of addressing business needs, including handling the growth in big data, bringing new services to users and customers and supporting business continuity. Enterprises and SaaS providers are attracted to IaaS because they don’t have to dimension in-house or outsourced infrastructure for peak usage. This typically results in under-utilization of resources. With IaaS, infrastructure capacity can scale in line with demand and customers pay only for what they consume. Increasingly, enterprise customers want to maintain a certain IT capacity in-house, as a private cloud, but be able to “burst” into a cloud service provider’s IaaS service when they need more resources.

This “hybrid cloud” model can be a powerful business accelerator if implemented in the right way. For example, it can allow companies to add low-cost storage capacity in the cloud service provider’s cloud to applications that remain in their private cloud or to experiment with new applications, services and service development tools without having to bring them in-house first. Hybrid cloud also supports the migration of workloads between the enterprise private and cloud service provider’s IaaS cloud for resilience and performance reasons.

Data center owners are well-positioned to become IaaS providers. They have physical footprint in trusted locations and existing enterprise customer relationships to build upon. By offering IaaS on top of traditional colocation and IT outsourcing services, data center owners can differentiate themselves from their competition, and stand out from the crowd as cloud service providers.

New Capabilities Are Required

To succeed in the highly competitive IaaS market, however, cloud service providers need strong security and networking capabilities to ensure they can offer enterprise customers a state-of-the-art cloud service at a compelling price point. Ubiquitous security capabilities are particularly important given that enterprises cite security as their largest barrier to adopting third-party cloud services. But the following are also critical from an IaaS operational cost perspective:

- A standardized and cost-efficient data center switching fabric that simplifies devices management and reduces overhead
- SDN to simplify networking and the provisioning of virtualized workloads

SDN gives cloud service providers the ability to connect VMs with each other and with users, rapidly and automatically. It significantly reduces the cost and limitations imposed by current manual processes for configuring virtual local-area networks (VLANs) within data centers. This paper will focus on SDN as a key enabler of a cloud service provider’s IaaS strategy.
SDN: What Do Cloud Service Providers Need?

How Does SDN Address Data Center Networking Challenges?

If enterprises are to trust IaaS services, cloud service providers need to make such services look as though they are a seamless part of an on-premise cloud. In other words, any workload running in the provider’s IaaS and delivered across the wide-area network (WAN) should appear to be executing locally in the enterprise’s private cloud from a security, privacy, availability and performance perspective.

So the first challenge cloud service providers face is how to provide enterprises with seamless, virtual private connectivity to their IaaS cloud. Asking enterprise customers to use the Internet is not a solution here, and it certainly won’t differentiate a cloud service provider from Amazon, for example. But making virtual private connectivity work end-to-end across the network today, from the customer premises to a VM in the cloud service provider’s cloud, requires manual processes to stitch it together. This takes time, adds cost and risks the introduction of human error.

The second problem is internal to the data center itself. IaaS is highly dynamic. Enterprise customers sign up for IaaS because of this – they want to be able to scale VMs when they need to and such scalability is, by definition, unpredictable in a hybrid “cloud-bursting” scenario. This means that the data center cloud is in a constant state of change due to:

- **Customers** spinning up new VMs and moving them between the cloud service provider’s and their own private clouds
- **Operations staff** moving VMs between servers for maintenance/upgrade reasons, e.g., adding blades and storage devices to increase capacity
- The **virtualization platform** autonomically moving VMs, for example, when it detects usage on a particular server is increasing/decreasing and needs to protect a workload’s performance or switch off a server to save power

Each time a VM moves, its connectivity needs to be reconfigured so that users can still reach the applications running in the VM. Presently, re-establishing network links to VMs when they migrate is typically a manual process. As the market moves beyond simple and relatively static cloud scenarios to more complex situations involving VM migration across hybrid clouds and the highly dynamic scaling of workloads, current approaches to IaaS networking are becoming increasingly human-intensive and costly to support.

Cloud service providers often use VLAN technology as the foundation for IaaS networks. However, VLANs have well-known limitations and they must be set up manually in the physical network. These issues are becoming barriers to the business agility and flexibility enterprise customers want from IaaS.

In contrast, SDN provides a means of virtualizing, and automating the configuration of, both data center networks and the end-to-end connectivity from the data center across the WAN to the customer premises. SDN provides a layer of abstraction (virtualization) on top of the physical network, which makes it simple, quick and cost-effective to set up connectivity between VMs, wherever they are located in the IaaS/hybrid cloud.

When SDN is in place, the same IaaS orchestration system that orders the creation of new VMs can simultaneously request new connectivity for those VMs (see Figure 1).
By integrating a virtual router resource with the hypervisor, VMs and their connectivity can be spun up together to fulfill the orchestration system’s request. The SDN abstraction layer automatically creates the required virtual network tunnels across the physical network infrastructure. Enterprise customers don’t have to wait while a network engineer manually creates a physical network connection to a new VM. Because all SDN connections are virtual, there are no restrictions on the number that can be created, so VM scaling is not a problem. This contrasts with VLAN technology, which does have an upper limit on the number of virtual networks it can support.

Virtualizing the network helps cloud service providers support multiple tenants (enterprise customers) more easily. SDN can be used to define a secure “virtual private” IaaS domain for each customer within which they are free to use their own IP addressing schemes and security policies, without creating conflicts with other customers. The SDN controller secures each virtual connection, both through the protocol it uses to create virtual network tunnels and through the integral security services it can provide at either end of a connection, on a per-VM basis, such as policy-driven firewalling.

This gives enterprise customers peace of mind when using a third-party IaaS service: wherever their VMs are in a hybrid cloud, they are subject to the same,
customer-specified security policies and from an IP addressing perspective, the enterprise’s private cloud and its virtual private domain within the cloud service provider’s IaaS cloud appear as one, seamless environment.

Attributes to Look for in a Data Center SDN Solution

New SDN solutions are entering the market thick and fast. Cloud service providers should evaluate candidates carefully, taking into consideration:

The openness of the SDN solution. Cloud technology is evolving rapidly and in time, a cloud service provider may want to swap out critical components of an IaaS stack, such as hypervisor/virtualization platform or orchestration system as these technologies mature and/or their business requirements change. SDN solutions that are tightly coupled with a specific hypervisor or vendor cloud stack may prevent cloud service providers from using new best-of-breed/open-source components in the future. The SDN solution should support:

- Industry-standard protocols to set up virtual network tunnels and route traffic across them
- REST-based open application programming interfaces (APIs) northbound for integration with orchestration and other cloud service provider management systems
- Self-service portals through which enterprise customers can set policies/gain visibility into their virtual network domains.

The robustness of the networking protocols supported by SDN. One of the advantages of SDN is that a virtualized networking approach can mask the complexity of Layer 3 routing while enabling cloud service providers to leverage the many benefits of networking at this level. Cloud service providers have traditionally used Layer 2 (Ethernet) networking because it is simpler, but it has its drawbacks, for example, around IP address handling.

SDN solutions that use BGP routing bring highly resilient, high-performing and secure networking technology – tried and tested in the world’s largest service provider networks – into the data center as the basis for connectivity between VMs. Not only do data center networks benefit from the robustness that Layer 3-based virtual networks confer, but this approach also makes it easier for cloud service providers to offer secure end-to-end connectivity to the customer premises. This is because both data center and WAN use the same routing technology.

The scalability of the SDN solution. Cloud service providers that are successfully selling IaaS today have often been taken by surprise by the rapid growth of their cloud services. To be future-proof, an SDN solution should support millions of concurrent virtual networking sessions and the ability to rapidly scale out connections – that is to add new connections on a massive scale.

The SDN solution’s support for security. Although security for data flows is an inherent feature of Layer 3 networking, an SDN solution should go further to address this key concern for enterprise customers. The SDN solution should help secure VMs by setting up, as part of a virtual connection, a virtual gateway (virtual firewall appliance) on a per-VM basis. The SDN solution should provide a means by which enterprise customers can apply their security policies to these virtual firewalls in a simple and automated way.
Conclusion

Cloud service providers that wish to move up the value chain and add IaaS to the portfolio of services they can offer enterprise customers will need to address the networking and security challenges associated with the cloud.

Current approaches to data center networking – which require the manual configuration of the physical network to create connectivity between VMs – are inflexible, time-consuming and costly. They make it difficult for IaaS providers to support complex cloud scenarios, such as hybrid cloud, and limit the scalability and dynamism of cloud services.

But cloud service providers that implement SDN do have an opportunity to differentiate themselves by providing enterprise customers with a superior IaaS experience. SDN enables the network to be manipulated, simply and cost-effectively, at a high level of abstraction and supports the automated creation of virtual network tunnels between VMs, wherever they are located in a hybrid cloud service provider/enterprise private cloud infrastructure. SDN can enable cloud service providers to leverage mature, resilient and secure Layer 3 networking protocols for seamless connectivity across data center and WANs.

Cloud service providers have considerable choice of SDN solution at this stage of the market. New entrants are flooding in, many with new and untried technologies. Cloud service providers will need to evaluate such solutions carefully, particularly with regard to their openness, robustness, scalability and security capabilities. Making the right SDN choice will be a key factor in achieving competitive success in the IaaS market.
About Juniper

Juniper Networks (NYSE: JNPR) delivers innovation across routing, switching and security. From the network core down to consumer devices, Juniper Networks' innovations in software, silicon and systems transform the experience and economics of networking. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on Twitter and Facebook.