



I D C E X E C U T I V E I N S I G H T S

Transitioning Toward a Software-Defined Industry

February 2016

By Shiv Putchu

Sponsored by Ciena

The ICT industry is making a transformation from one that has been largely defined by hardware and capex investments to one determined by software and services. Enterprise buyers are looking at network virtualization technology as a potential replacement for purpose-built appliances and extending virtualization from islands of storage, server and compute to one that encompasses network resources from switching and routing to areas such as firewalls and optimization. This provides alternatives to premise-based physical equipment. The end result is moving towards a software-defined industry that extends from the desktop (or device), to the datacenter across the wide area network. This software-defined network will be orchestrated to deliver an overall ICT environment which is more agile, programmable and responsive to business needs. According to the annual IDC C-Suite Barometer survey, software-defined infrastructure is the most appealing technology for 2015-16 for future investment. The survey also shows that the single biggest IT priority for CXOs is in creating an environment in which innovation can be used for competitive advantage.

This document takes a closer look at the investment plans and views of enterprises around software-defined networking (SDN) and network function virtualization (NFV), two complementary concepts that are being developed by the IT and telecoms industry. In the next 24 months, enterprises are going to focus on ways to virtualize the network by service providers to improve the overall delivery of ICT software and services to enterprises.

Aligning to Business Outcomes

How do we get there from here? The results of the IDC Asia/Pacific WAN and Communications Survey, 2015, show that enterprises see the network as becoming more aligned with business objectives and outcomes. The top reasons for network investments are to:

- Improve business process
- Increase employee productivity
- Enhance security and data governance
- Improve customer experience

The role of the datacenter is undergoing its own transformation. The average enterprise currently utilizes between three and five cloud providers. This figure is likely to triple by the end of the decade. In the not-too-distant future, the average enterprise will have more data in the cloud than on-site. This, in turn, is putting more pressure on the network to secure and transport data, and driving further investments into the datacenter.

According to the same research, the top three factors driving network investment into the datacenter are:

- Improve business continuity and disaster recovery
- Support a technology expansion
- Replace legacy infrastructure

Connected Clouds: North-South versus East-West Traffic

Today, there is an increasing trend towards convergence of datacenters and networks. For example, the proliferation of clouds and increased focus in business continuity/disaster recovery (BC/DR) has meant that the network must now not only be provisioned to support north-south (typically client-server) traffic as it has done for many years, but also east-west traffic, allowing data to move both within and between datacenters for areas such as backup, archiving and data recovery. In large hyperscale deployments, there is more focus on resiliency between clouds to the point where there should be no measurable downtime in the event an entire facility goes offline. Google, for example, is one company that has articulated this view.

The trends from BC/DR to interconnected hyperscale clouds are driving the requirement for high-capacity fiber and Ethernet links. Networks will also be able to secure and transport data between clouds, move data more quickly, and support more enterprises around various recovery points and recovery time objectives for their data, which is often determined by local governance and regulatory compliance requirements. IDC estimates that the amount of east-west traffic is 10-fold greater than north-south in overall volumes.

Datacenter Interconnect (DCI) for Connected Clouds

Datacenter interconnect network infrastructure and services are undergoing a significant transformation, as the demand for more DCI services increases because of the exponential growth in bandwidth, Big Data and low-latency applications, and the use of more distributed datacenter resources.

Connected clouds in the Asia/Pacific region are also driving the requirement for more datacenter interconnects (DCIs). The most important considerations when investing in DCI solutions are ease of management, cost and scalability. These factors point to the fact that datacenter owners are looking for scalable and low-cost DCI solutions that can be programmed to cater to their specific needs.

Internet of Things Driving Changes in Network Infrastructure

The networks will not only need to have the agility to support east-west traffic, but there is also an increasing requirement from the network to support compute, storage and connectivity at the core and edge of the network. This will be driven by the Internet of Things (IOT) which is projected to reach 9.8 billion connected devices by 2019 in the Asia/Pacific region, including Japan (APJ), representing a US\$618 billion opportunity. Each minute, there are 4,000 connected devices added to a network somewhere in the world. Without significant improvements to the ability for networks to support core and edge computing at scale, IOT will be difficult to deploy and manage. According to the IDC Internet of Things Survey 2015, the average enterprise undergoing IOT deployment has about 28,000 devices under management and plans to increase this to almost 58,000 connected devices during the next implementation. The survey also showed that Asia is leading the world in terms of deployments. As such, the requirements for core-edge compute will likely be driven in Asia first.

The Case for SDN for Agile, Scalable and Programmable Networks

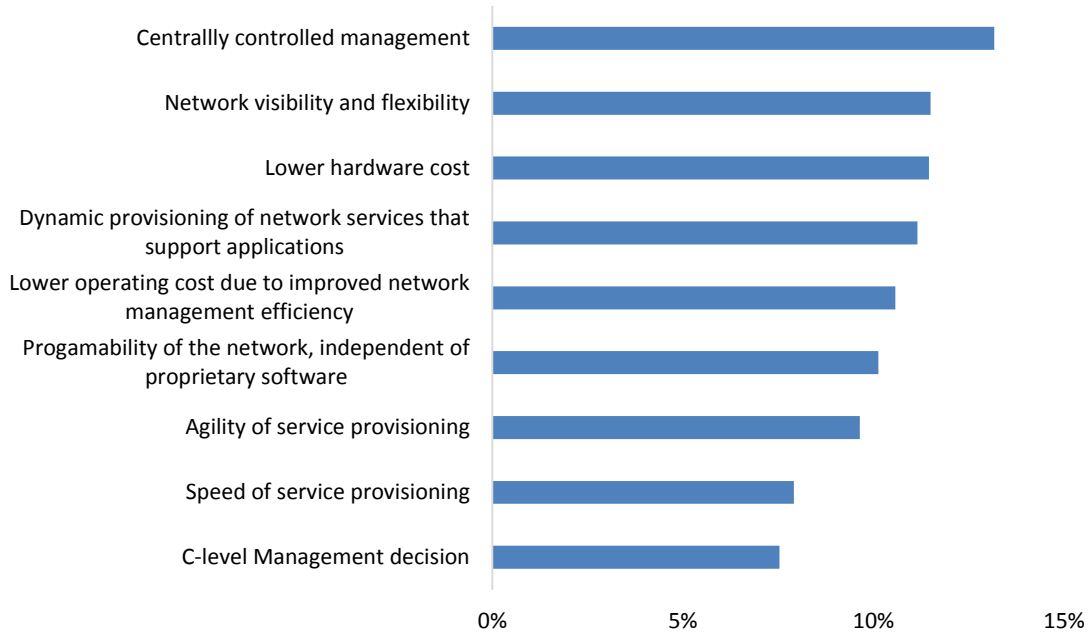
IDC maintains that given the direction of the industry combined with the current and future requirements for networks, SDN discussions are becoming prevalent especially in the context of digital transformation. In interviews with IT heads, IDC has found that enterprises consider adopting SDN for a few key reasons:

- **Agility:** While virtualization has come to storage, applications and servers, for example, very little has happened at the network layer. Networks have always been manually configured, which has proven to be costly, takes a lot of time, and is one of the leading causes of an outage. Manual configuration is also not dynamic enough to factor in changes in traffic with the pervasiveness of video, proliferation of mobile devices and consumerization of IT. Network configurations can often become obsolete quickly and unable to match the workloads. SDN, however, promises improved provisioning through automated processes and better overall management and control. This can free up resources and save considerably on opex.
- **Speed of provisioning:** Manual processes associated with building networks have also prolonged provisioning times to weeks and months, and this is another pain point that businesses are looking to address. Better capabilities, such as ability to templatize IT policies into hardware devices, is dramatically accelerating provisioning times and allowing IT managers the option to create and take down networks to meet specific requirements within minutes or hours. This is attractive for enterprises looking to build networks to support specific workloads, such as backup, videoconferencing and/or test-dev environments. Accelerated provisioning puts an enterprise on course to building a network that is cloud-ready.
- **Programmability:** The promise of having a network that can be programmed to support specific types of workloads which need to be supported on a particular day. Latency sensitive enterprise applications could be treated different than batch processing. If networks could be programmed to support applications, it can then be tuned to provide deterministic routing. Moving to solutions that provide deterministic routing (over existing heuristic routing) can also be important for business continuity and disaster recovery, especially for improving recovery time objectives (RTO).

IDC's research reveals the primary motivations (Figure 1) and inhibitors (Figure 2) of SDN implementation.

Figure 1

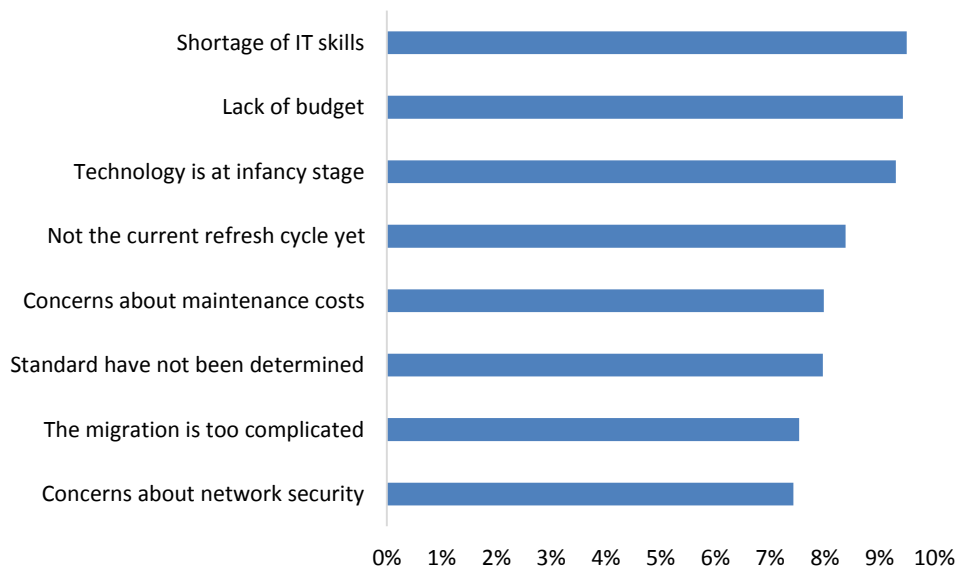
Motivations for Considering or Implementing SDN



Source: IDC Asia/Pacific WAN and Communications Survey, 2015

Figure 2

Primary Inhibitors for Implementing SDN Today



Source: IDC Asia/Pacific WAN and Communications Survey, 2015

There are a number of challenges that enterprises have with an SDN implementation, and they are not different from previous technology upgrades. Most enterprises do not know where to start, lack the skill sets, and do not have a dedicated budget line item for SDN. Other concerns have to do with a technology at an infancy stage, the uncertainty of when to start their deployments given product refresh cycles, and the underlying business case of establishing the starting point for potential savings. There are other trade-offs to consider such as capabilities available today versus waiting for industry standards tomorrow.

IDC research shows that the majority of Asian businesses are aware of SDN. Some 30% of enterprises in the Asia/Pacific region are planning, testing or actively deploying the technology. Some 55% of enterprises have an annual budget ranging between US\$500,000 and US\$2 million just for SDN. Other IDC research shows that within five years, over 85% of datacenters and campus environments will be SDN-enabled.

Motivations for NFV for Application Delivery

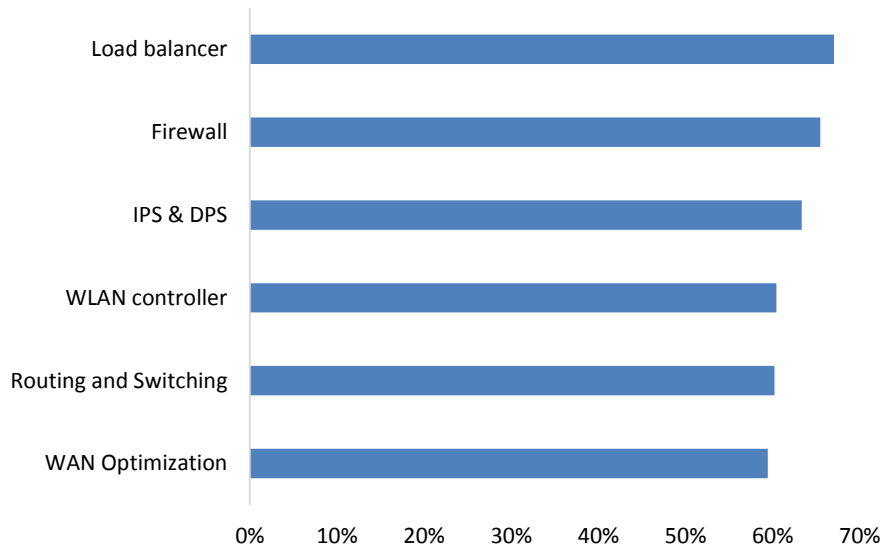
There is a premise in the industry that appliance-based technologies that are housed in customer premises, such as firewalls, will be virtualized and provisioned from the cloud (see Figure 3). IDC has found that some 64% of businesses are currently evaluating NFV technologies. The top three value propositions that businesses seek from their service providers are:

- Network performance
- Using the network to support hybrid cloud
- Improving network security

The level of interest, acceptance and likeliness of adoption is currently higher for NFV than SDN. Reasons are likely to vary from the fact that this is ETSI-based and carrier-backed, to an overall perception that this is the first place where software-defined services are likely to be available to the mass market. The question is often not whether services will be available, but where a service provider needs to start and what an enterprise would be willing to buy. The data shows that there is broad-based demand for NFV.

Figure 3

Types of Appliances or Functions Considered for Virtualization



Source: IDC Asia/Pacific WAN and Communications Survey, 2015

The Security Imperative

Like every technology, especially coming from the 3rd Platform (e.g., social, mobile, big data, and cloud), security continues to be of paramount importance. IDC defines the 3rd platform technologies to include cloud, big data, mobility and social. Businesses are increasingly being built on a combination of all these foundational pillars. In fact, many companies now focused on digital transformation (DX) are assessing how they can leverage these 3rd platform technologies and innovation accelerators like IOT and robotics to deliver additional value. To this end, security continues to be one of the best use cases for SDN/NFV. There are many ways to address this challenge such as looking at it from an application programming interface (API) layer, and considering it from the data and control plane angles.

In the case of NFV, an overwhelming majority of enterprises believe that it will improve security and it is currently not seen as a major inhibitor.

- 29% believe NFV will improve network security
- 52% see marginal improvements in security
- 14% see no difference in security
- Only 4% see networks as becoming less secure

SDN and NFV is a decision that impacts the overall network architecture. Security should be considered and will continue to be a horizontal play and important for all areas of ICT. As part of the migration, it will be an imperative for service providers and vendors to educate the market accordingly.

Conclusion

The network is moving from one based on rigid physical infrastructure to a more software-defined virtual infrastructure that is more closely linked with the targeted services and capabilities. This will enable new capabilities such as NFV. Networks will continue to be a platform for intelligence and play a lead role in providing next-gen security. As networks become more intelligent, they will align to focus more on business outcomes. Network discussions are moving away from static measurements such as availability and latency to improving business outcomes and employee productivity. Instead of provisioning network and cloud resources separately, IT managers will begin to provision them together and build networks that understand applications, and applications that are network-aware. By 2017, IDC predicts that 65% of organizations will have implemented hybrid environments leveraging in-house and external IT resources. The implications are networks and cloud will start to converge and the focus will shift to end-user experience. By 2016, 15% of organizations will have started the journey to SD-WAN. Other factors that will contribute to the movement towards a software defined infrastructure are:

- Shifts to east-west traffic driven the by interconnection of clouds
- Requirement for compute and connectivity to be processed on both the core and edge.
- Security to move from a model that is preventative to one that is policy and context-aware
- Service providers adopting platforms for managing virtualized network, compute and storage

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the Custom Solutions information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document require an additional license from IDC.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserve/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com