The 2015 Guide to SDN and NFV

Part 1: Software Defined Networking (SDN)

By Dr. Jim Metzler, Ashton Metzler & Associates
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Sponsored in part by:

Produced by:

Webtorials
# Table of Contents

**Executive Summary** ................................................................. 1

**Introduction** .................................................................................. 2
  - Definition of SDN ................................................................. 2
  - Context for SDN ................................................................. 3
  - Status of SDN Adoption .......................................................... 4
  - The SDN Architecture .......................................................... 4
  - The Northbound Interface ...................................................... 5
  - Architectural Distinctions between Approaches ...................... 6
  - The Overlay and the Underlay Model ....................................... 7
  - Service Chaining ................................................................. 8
  - The OpenDaylight Consortium .............................................. 9
  - The Relationship Between SDN and NFV ............................. 10

**SDN Use Cases** ........................................................................... 12
  - Drivers and Inhibitors .......................................................... 12
  - SDN Deployment Plans ......................................................... 13
  - Data Center ........................................................................ 14
  - WAN .................................................................................... 17
  - Campus ............................................................................... 17

**The Operational Implications** ..................................................... 20
  - Security ............................................................................. 20
  - Cloud Orchestration ............................................................ 21
  - Management ....................................................................... 23
  - Organizational Impact .......................................................... 26
Executive Summary

Over the last couple of years, the hottest topics in networking have been Software Defined Networking (SDN) and Network Functions Virtualization (NFV). While both enterprises and service providers have shown great interest in these topics, the vast majority of organizations are still either on the sidelines or in the analysis stage of adoption. The primary goals of The 2015 Guide to SDN & NFV (The Guide) are to eliminate the confusion that surrounds SDN and NFV and to accelerate the analysis and potential adoption of these new design and architectural approaches.

The Guide will be published both in its entirety and in a serial fashion. This document is the first of the serial publications and it will focus on SDN. The second publication will focus on NFV and the third on the SDN and NFV ecosystem. The fourth publication will include a complete copy of The Guide as well as an executive summary of the complete guide.

This document has three chapters:

1. Introduction
   Provides background on topics such as the current status of SDN deployment and the interest in both the fabric-based and the overlay based models.

2. Use Cases
   Discusses SDN use cases in the data center, WAN and campus and analyzes the factors that are currently limiting deployment.

3. Operational Considerations
   Identifies the security, management and organization issues relative to implementing SDN and analyzes how impactful these issues are likely to be in the near term.
Introduction

This chapter of The Guide is based in part on *The 2013 Guide to Network Virtualization and SDN* (The 2013 Guide). To limit the size of this chapter, some of the introductory SDN material that was contained in The 2013 Guide has been eliminated. That document, however, is still available online. Also with the goal of limiting the size of this chapter, detailed analyses of a number of topics are avoided and URLs are provided that point to relevant material. That material includes:

- An analysis of OpenFlow V1.3 and the use cases it enables;
- Criteria to evaluate a vendor's overall SDN solution as well as specific criteria to evaluate a SDN controller and the subtending network devices;
- A framework to plan for SDN;
- An analysis of the advantages and disadvantages of the overlay-based SDN model;
- Criteria to evaluate overlay-based SDN solutions.

This section contains the results of a survey that was distributed in September 2014 (The 2014 Survey). Throughout The Guide, the 176 network professionals who completed the survey will be referred to as The Survey Respondents. Where appropriate, the results of The 2014 Survey will be compared to the results of a similar survey given in 2013 (The 2013 Survey).

Thirty-two percent of The Survey Respondents indicated that they were either very familiar or extremely familiar with SDN. In response to The 2013 Survey, only twenty-one percent of the respondents indicated that they were either very familiar or extremely familiar with SDN.

*Over the last year, the familiarity with SDN has increased significantly.*

Definition of SDN

The Open Networking Foundation (ONF) is the group that is most associated with the development and standardization of SDN. According to the ONF, “Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow™ protocol is a foundational element for building SDN solutions.” Many vendors have announced support for OpenFlow V1.3. An overview of that protocol and the use cases it enables can be found in *An Overview of OpenFlow V1.3*.

The ONF states that the SDN architecture is:

- Directly programmable;
- Agile;
- Centrally managed;
- Programmatically configured;
- Open standards-based and vendor-neutral.
Context for SDN

As described later in this document, one of the key SDN use cases is the engineering of data traffic. A high level metaphor that both explains the value that SDN brings to engineering data traffic and that also provides insight into SDN’s overall value proposition stems from the world of vehicular traffic.

In terms of the engineering of vehicular traffic, things are largely the way they were upon the introduction of the traffic signal. A traffic signal is a good thing in that it helps vehicles to avoid a collision and it gives priority to higher volume roads. With the exception of HOV lanes and toll roads, until recently there has been very little else to assist in improving traffic flow. That situation changed several years ago with the introduction of GPS and real time maps which together provide a connected driver with the information that enables that driver to take a less congested route, which presumably results in a shorter travel time.

The metaphor is that in a computer network a packet is similar to a car in part because it has an origin and a destination and in part because the switches and routers along the end to end path from origin to destination play a role somewhat similar to traffic signals and road signs. The computer network also now has the equivalent of an HOV lane for important traffic and it is getting better at routing that traffic in ways that reduce travel times.

As mentioned, one of the key SDN use cases is traffic engineering. In addition, a defining characteristic of SDN is that it separates the control of the network from the process of forwarding the packets. Staying with the metaphor, one way to think about how SDN concepts could be applied to vehicular traffic involves thinking not of a traditional car, but of a Google-inspired, driverless car. Before it starts to move, the driverless car connects to a central control point that has a deep understanding of conditions that impact travel. The car informs the control point of its starting point and its destination, its status, (i.e. number of passengers, mission etc.) and in return, the control point sends the car a route. The route is based on factors such as the roads that are available and the other vehicles which are using those roads. The car merges onto a road, travels both at high speed and at a distance of only a few inches from other driverless cars - both front and back and side to side. Because the central control point has a deep level of understanding of the roads and the cars, openings are made for exiting and merging traffic and accidents are eliminated.

Centralized control points, driverless cars and cars traveling within a few inches of other cars may sound far-fetched. However, a subsequent section of this document details how Google applied SDN to its Wide Area Network and is now able to increase the utilization of that network to be 95%. A traditional WAN typically runs at a utilization rate between 60% and 65%. Increasing the utilization to 95% should cut the monthly cost of the WAN in half.
Status of SDN Adoption

The Survey Respondents in both 2013 and 2014 were given a set of alternatives and were asked to indicate the alternatives that described their company’s current approach to implementing SDN and were allowed to choose all that applied to their company. The responses of the two survey groups are shown in Table 1.

### Table 1: SDN Utilization

<table>
<thead>
<tr>
<th>Approach to Implementing SDN</th>
<th>Responses to The 2014 Survey</th>
<th>Responses to The 2013 Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have not made any analysis of SDN</td>
<td>16%</td>
<td>19%</td>
</tr>
<tr>
<td>We will likely analyze SDN sometime in the next year</td>
<td>22%</td>
<td>26%</td>
</tr>
<tr>
<td>We are currently actively analyzing the potential value that SDN offers</td>
<td>32%</td>
<td>36%</td>
</tr>
<tr>
<td>We expect that within a year that we will be running SDN either in a lab or in a limited trial</td>
<td>22%</td>
<td>19%</td>
</tr>
<tr>
<td>We are currently actively analyzing vendors’ SDN strategies and offerings</td>
<td>25%</td>
<td>20%</td>
</tr>
<tr>
<td>We currently are running SDN either in a lab or in a limited trial</td>
<td>18%</td>
<td>13%</td>
</tr>
<tr>
<td>We currently are running SDN somewhere in our production network</td>
<td>11%</td>
<td>6%</td>
</tr>
<tr>
<td>We looked at SDN and decided to not do anything with SDN over the next year</td>
<td>10%</td>
<td>5%</td>
</tr>
<tr>
<td>We expect that within a year that we will be running SDN somewhere in our production network</td>
<td>18%</td>
<td>10%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>2%</td>
<td>4%</td>
</tr>
</tbody>
</table>

The data in Table 1 indicates that while the utilization of SDN in production networks remains limited, it has increased somewhat significantly in the last year. In addition:

*The use of SDN in production networks should increase somewhat significantly in the next year.*

### The SDN Architecture

Figure 1 contains a graphical representation of the SDN architecture as envisioned by the ONF. One key component of a complete SDN solution that is missing from Figure 1 is cloud orchestration platforms such as OpenStack. The role that these platforms play in both SDN and NFV is described later in this document.
As is discussed below, in some implementations of the architecture depicted in Figure 1, the infrastructure layer is just the virtual switch in a hypervisor. This will be referred to as the overlay-based model. In other implementations, the infrastructure layer is a combination of virtual and physical network devices. This will be referred to as either the underlay-based model or the fabric-based model.

The white paper entitled How to Plan for SDN discusses criteria to evaluate a vendor’s overall SDN solution as well as specific criteria to evaluate a SDN controller and the subtending network devices. That white paper also contains a framework for how network organizations can plan for the adoption of SDN.

The Northbound Interface

The 2013 Guide contains definitions of the key terms and concepts that are embodied in Figure 1. One of those concepts is the North Bound Interface (NBI), which is the interface between the control layer and the application layer. When The 2013 Guide was published there were not any standards associated with the NBI and there was an ongoing debate in the industry about the viability of creating such standards. Proponents of standardizing the NBI argued that there were numerous controllers on the market, each with their own NBI and none of which had significant market share. Their argument was that the lack of standardization impeded the development of SDN because without standardization application developers wouldn’t be very motivated to develop applications for a controller with small market share knowing that they will likely have to modify their application to work on other controllers. The argument against standardization was that given where the industry was relative to the development of SDN it wasn’t possible to really know what should go into the NBI and hence it made no sense to standardize it.
After over a year of discussion, in late 2013 the ONF created the NBI working group and outlined the group's charter in a white paper. As part of their charter, the NBI working group intends to work with one or more open source initiatives to develop working code for the NBIs that the group standardizes. According to Sarwar Raza the chair of the NBI working group, the working group has a good relationship with both the OpenStack and the OpenDaylight initiatives but that when dealing with open source initiatives “there is no magic handshake”. Raza elaborated by saying that none of the open source initiatives are going to agree in advance to produce code for NBIs that are under development. He expects that what will happen is that after the standards have been developed the NBI working group will have detailed technical discussions with multiple open source communities and will see if there is a consensus about developing code.

The NBI working group has introduced the need for APIs at different latitudes. The idea is that a business application that uses the NBI should not require much detailed information about the underlying network. Hence, applications like this would require a high degree of abstraction. In contrast, network services such as load balancing or firewalls would require far more granular network information from the controller and hence, not need the same level of abstraction. One conclusion to be drawn from this approach is that the NBI working group won’t come out with one NBI that works for every type of application. It is also highly likely that there will be further segmentation of NBIs based on industry sector. For example, there may be different NBIs for enterprises than there are for service providers.

**Architectural Distinctions between Approaches**

Network virtualization isn’t a new topic. IT organizations have implemented various forms of network virtualization for years; i.e., VLANs, VPNs, VRF. However, in the context of SDN the phrase network virtualization refers to the creation of logical, virtual networks that are decoupled from the underlying network hardware to ensure the network can better integrate with and support increasingly virtual environments.

As previously noted, the predecessor to The Guide was entitled The 2013 Guide to Network Virtualization and SDN. The genesis of that title was that in 2013 there was disagreement in the industry about whether or not SDN and network virtualization were the same thing. Today most of that disagreement has gone away and there is general agreement that network virtualization is a critical SDN application and as described below, there are multiple ways to implement network virtualization.

In addition to having multiple ways of implementing network virtualization, other key architectural distinctions between the varying ways that vendors are implementing SDN include the:

- Role of dedicated hardware;
- Amount of control functionality that is centralized;
- Use of protocols such as OpenFlow.

As indicated above, there is a divergence of opinion relative to the role of dedicated hardware. One example of that divergence of opinion is that some vendors believe it is possible to fully support network virtualization in the data center without using dedicated hardware and some vendors believe that dedicated hardware is needed at least some times. The Survey Respondents were asked to indicate if they believed that with the current technologies and
products it’s possible to broadly support network virtualization in the data center without using any dedicated hardware? The no responses outnumbered the yes responses by almost a 2:1 ratio.

*IT organizations are highly skeptical that they can implement network virtualization in the data center without using at least some dedicated hardware.*

The Survey Respondents were also asked to indicate the likely role that the OpenFlow protocol will play in their company’s implementation of SDN. Their responses are shown in Table 2.

<table>
<thead>
<tr>
<th>Use of OpenFlow</th>
<th>Percentage of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our implementation of SDN will definitely include OpenFlow</td>
<td>18%</td>
</tr>
<tr>
<td>Our implementation of SDN will likely include OpenFlow</td>
<td>24%</td>
</tr>
<tr>
<td>Our implementation of SDN might include OpenFlow</td>
<td>24%</td>
</tr>
<tr>
<td>Our implementation of SDN will not include OpenFlow</td>
<td>4%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>29%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

One of the conclusions that can be drawn from the data in Table 2 is that IT organizations have a favorable view of OpenFlow. In addition:

*Very few IT organizations have ruled out the use of OpenFlow.*

**The Overlay and the Underlay Model**

As mentioned, there are two primary approaches that vendors are taking to implement the architecture depicted in Figure 1. These two approaches are the:

- Overlay-based model;
- Fabric-based or underlay model.

The overlay-based model focuses on the hypervisor and it uses tunneling and encapsulation. Since the overlay-based model focuses on the hypervisor, its use cases tend to be focused on responding to challenges and opportunities that are associated with virtualized servers. A discussion of the pros and cons of the overlay-based model is found in *The Advantages and Disadvantages of the Overlay-Based SDN Model*. A detailed set of criteria that IT organizations can use to evaluate some of the specific characteristics of the overlay-based model is found in *Architectural Criteria to Evaluate Overlay-Based SDN Solutions*.

Whereas the overlay-based model focuses on the hypervisor and uses tunneling and encapsulation, the underlay-based model focuses on a range of virtual and physical network elements and relies on the SDN controller manipulating flow tables in the network elements. In addition, whereas the use cases for the overlay-based model are focused on responding to challenges and opportunities that are associated with virtualized servers, the use cases that are
associated with the underlay-based model are broader in scope; i.e., ease the burden of configuring and provisioning both physical and virtual network elements.

One way that network virtualization can be implemented within an underlay solution is by having virtual networks be defined by policies that map flows to the appropriate virtual network based on the L1-L4 portions of the header. In line with the general philosophy of an underlay-based model, the SDN controller implements these virtual networks by configuring the forwarding tables in OpenFlow-based physical and virtual switches. However, another option is that an underlay solution manipulates the flow tables in OpenFlow-based physical and virtual switches in order to provide a range of functionality other than network virtualization, but that the underlay solution also uses an overlay-based approach to implement network virtualization.

The Survey Respondents were asked to indicate how their company sees the value that the overlay- and the underlay-based models will provide over the next two years. Their responses are shown in Table 3.

<table>
<thead>
<tr>
<th>Response</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>The overlay-based model will provide notably more value</td>
<td>22%</td>
</tr>
<tr>
<td>The fabric-based model will provide notably more value</td>
<td>28%</td>
</tr>
<tr>
<td>Each model will offer roughly equal value</td>
<td>12%</td>
</tr>
<tr>
<td>We don’t have an opinion on either model</td>
<td>31%</td>
</tr>
<tr>
<td>Other</td>
<td>7%</td>
</tr>
</tbody>
</table>

*By a small margin, IT organizations perceive the fabric-based SDN model will provide more value over the next two years than will the overlay model. However, many IT organizations are yet to form an opinion.*

Another step in the evolution of SDN is that a year ago the discussion of the overlay-based and underlay-based models was typically phrased as the overlay-based model vs. the underlay-based model. While that is still an interesting discussion, some providers of overlay-based solutions either have already started to ship products or have announced their intention to ship products based on federating their controllers with those of one or more providers of underlay-based solutions; a.k.a., an overlay/underlay solution. A large part of the motivation to deliver federated overlay/underlay solutions is that effective operations management requires that IT organizations have tools that give them clear visibility into the relationships between the virtual networks that are set up by the overlay solution and the physical networks and their component devices that are controlled and managed by the underlay solution. That is required because when performance or availability problems occur, both root cause analysis and impact analysis require bilateral mapping between the physical and virtual infrastructures.

**Service Chaining**

The phrase *service chaining* refers to the ability to steer virtual machine (VM)-VM traffic flows through a sequence of physical and/or virtual servers that provide network services, such as firewalls, IPS/IDS, DPI, or load balancers. In an underlay-based solution, the controller configures the forwarding plane switches to direct the flows along the desired paths. In an
overlay-based solution, the controller adjust the Forwarding Information Bases (FIBs) of the vSwitches/vRouters to force the traffic through the right sequence of VMs. The next section of The Guide focuses on Network Functions Virtualization (NFV). That section will discuss what the European Telecommunications Standards Institute (ETSI) refers to as VNF forwarding graphs, which are similar in concept to service chains.

The OpenDaylight Consortium

The OpenDaylight Consortium was founded in April 2013. The consortium’s stated mission is to facilitate a community-led, industry-supported open source framework, including code and architecture, to accelerate and advance a common, robust Software-Defined Networking platform. As of September 2014 the consortium had 41 members: 9 platinum members, 2 gold members and 30 silver members. Platinum members commit to dues of $500,000 a year for two years and to also provide at least ten developers a year. The financial commitment for Gold and Silver members is determined by a sliding scale based on the company’s revenues. Gold members pay annual dues that range between $50,000 and $250,000 and provide at least three developers while Silver members pay annual dues that range between $5,000 and $20,000 and provide at least one developer.

In February 2014 the consortium issued its first software release, called Hydrogen (Figure 2). A number of vendors have announced their intention to use Hydrogen as the basis of their SDN controller. A discussion of the functionality that Hydrogen provides can be found at the consortium’s Web site.
According to Neela Jacques, the Executive Director of OpenDaylight, the consortium’s next release of software, code named Helium, will likely be released in late 2014. He stated that some of the new functionality that may be included in Helium includes service chaining, the federation of SDN controllers, additional network virtualization options as well as more L4 – L7 functionality.

The Relationship Between SDN and NFV

Until recently, the conventional wisdom in the IT industry in general, and on the part of the ONF and the ETSI NFV ISG\(^1\) in particular, was that SDN and NFV were separate topics and didn’t need to be formally coordinated. That conventional wisdom officially changed in March 2014 when the ONF and the ETSI NFV ISG announced the signing of a Memorandum of Understanding (MOU).

As part of the announcing the MOU, the ONF and ETSI stated that “Together the organizations will explore the application of SDN configuration and control protocols as the base for the network infrastructure supporting NFV, and conversely the possibilities that NFV opens for virtualizing the forwarding plane functions.” Also as part of the announcement, the ONF released a document entitled the OpenFlow-enabled SDN and NFV Solution Brief. The solution brief showcases how operators are combining NFV and SDN to achieve the common goals of both technologies to achieve greater agility of the networks. The brief discusses the network challenges that operators will need to overcome to implement NFV, and it presents use cases that demonstrate how OpenFlow-enabled SDN can meet the need for automated, open, and programmable network connectivity to support NFV.

The Survey Respondents were asked to indicate the relationship that their company sees between SDN and NFV and they were allowed to check all that applied. Their answers are shown in Table 4.

<table>
<thead>
<tr>
<th>Relationship</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>They are totally independent activities</td>
<td>6%</td>
</tr>
<tr>
<td>They are complementary activities in that each can proceed without the other but the value of each activity may be enhanced by the other activity.</td>
<td>61%</td>
</tr>
<tr>
<td>In at least some instances, NFV requires SDN</td>
<td>25%</td>
</tr>
<tr>
<td>In at least some instances, SDN requires NFV</td>
<td>10%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>16%</td>
</tr>
</tbody>
</table>

Some of the conclusions that can be drawn from the data in Table 4 are:

The vast majority of IT organizations believe that SDN and NFV are complimentary activities.

A significant percentage of IT organizations believe that in at least some instances NFV requires SDN.

---

\(^1\) The role that this group plays in the development of NFV is explained in the next chapter of The Guide.
Only a small percentage of IT organizations believe that SDN and NFV are totally independent activities.
SDN Use Cases

Drivers and Inhibitors

The Survey Respondents were shown a number of challenges and opportunities and were asked to indicate which of them they thought that SDN could help them to respond to and they were allowed to check all that applied. Their responses are shown in Table 5.

<table>
<thead>
<tr>
<th>Challenge or Opportunity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better utilize network resources</td>
<td>55%</td>
</tr>
<tr>
<td>Perform traffic engineering with an end-to-end view of the network</td>
<td>54%</td>
</tr>
<tr>
<td>Ease the administrative burden of configuration and provisioning</td>
<td>53%</td>
</tr>
<tr>
<td>Support the dynamic movement, replication and allocation of virtual resources</td>
<td>52%</td>
</tr>
<tr>
<td>More easily scale network functionality</td>
<td>45%</td>
</tr>
<tr>
<td>Enable applications to dynamically request services from the network</td>
<td>45%</td>
</tr>
<tr>
<td>Have network functionality evolve more rapidly based on a software development lifecycle</td>
<td>41%</td>
</tr>
<tr>
<td>Reduce OPEX</td>
<td>40%</td>
</tr>
<tr>
<td>Implement more effective security functionality</td>
<td>35%</td>
</tr>
<tr>
<td>More easily implement QoS</td>
<td>33%</td>
</tr>
<tr>
<td>Reduce CAPEX</td>
<td>29%</td>
</tr>
<tr>
<td>Reduce complexity</td>
<td>24%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

One observation that can be drawn from the data in Table 5 is that IT organizations are optimistic that SDN can help them respond to a wide range of opportunities and challenges. However:

*Relatively few IT organizations believe that SDN will help them reduce CAPEX or reduce complexity.*

The Survey Respondents were also shown a set of impediments and were asked to indicate the two impediments that would be the biggest inhibitors to their company adopting SDN sometime in the next two years. Their responses are shown in Table 6.
Table 6: Inhibitors to the Adoption of SDN

<table>
<thead>
<tr>
<th>Impediment</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The immaturity of the current products</td>
<td>29%</td>
</tr>
<tr>
<td>Concerns about how we would integrate SDN into the rest of our infrastructure</td>
<td>23%</td>
</tr>
<tr>
<td>The immaturity of the enabling technologies</td>
<td>23%</td>
</tr>
<tr>
<td>The lack of a compelling business case</td>
<td>21%</td>
</tr>
<tr>
<td>The confusion and lack of definition in terms of vendors strategies</td>
<td>16%</td>
</tr>
<tr>
<td>Other technology and/or business priorities</td>
<td>14%</td>
</tr>
<tr>
<td>Concerns about how we would manage SDN</td>
<td>13%</td>
</tr>
<tr>
<td>Possible security vulnerabilities</td>
<td>12%</td>
</tr>
<tr>
<td>The lack of a critical mass of organizations that have deployed SDN</td>
<td>9%</td>
</tr>
<tr>
<td>No inhibitors to implementing SDN</td>
<td>7%</td>
</tr>
<tr>
<td>Concerns that the technology will not scale to support enterprise sized networks</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

Some of the inhibitors to SDN adoption, such as the immaturity of current products and the immaturity of enabling technologies, will naturally dissipate over time. However some on the key inhibitors won’t just naturally dissipate over time. These inhibitors need to be aggressively addressed by vendors and network organizations.

*Two of the major inhibitors to SDN adoption are concerns about how to integrate SDN into the rest of the infrastructure and the lack of a compelling business case.*

**SDN Deployment Plans**

While the use of SDN in data centers receives the majority of attention, it is also possible to implement SDN in branch and campus networks as well as in wide area networks (WANs). In order to understand where SDN will likely be implemented, The Survey Respondents were asked “If your organization is likely to implement SDN sometime over the next two years, where are you likely to implement it?” Their responses are summarized in Table 7.

Table 7: Focus of SDN Deployment

<table>
<thead>
<tr>
<th>Focus of SDN Deployment</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center</td>
<td>64%</td>
</tr>
<tr>
<td>WAN</td>
<td>26%</td>
</tr>
<tr>
<td>Branch and/or Campus</td>
<td>25%</td>
</tr>
<tr>
<td>We are unlikely to implement SDN within the next two years</td>
<td>12%</td>
</tr>
<tr>
<td>Don’t know/NA</td>
<td>10%</td>
</tr>
<tr>
<td>We are likely to implement a service from a WAN service provider that is based on SDN</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
</tbody>
</table>
One observation that can be made from the data in Table 7 is:

*Over the next two years, the primary focus of SDN deployment is likely to be in the data center. However, there is considerable interest in deploying SDN in the WAN as well as in branch and campus networks.*

The Survey Respondents were also asked to indicate how broadly they expected their campus, WAN and data centers networks would be based on SDN three years from now. Their responses are summarized in Table 8.

<table>
<thead>
<tr>
<th>Table 8: Planned SDN Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Exclusively based on SDN</td>
</tr>
<tr>
<td>Mostly SDN</td>
</tr>
<tr>
<td>Hybrid, with SDN and traditional coexisting about equally</td>
</tr>
<tr>
<td>Mostly traditional</td>
</tr>
<tr>
<td>Exclusively traditional</td>
</tr>
<tr>
<td>Don't know</td>
</tr>
</tbody>
</table>

Given the relatively low penetration of SDN currently, the data in Table 8 shows that:

*Network organizations are very optimistic that over the next three years that there will be a significant increase in SDN deployment.*

*Network organizations believe that three years from now that SDN deployment in data centers will be highly pervasive and that there will also be significant SDN deployment both in the WAN and in campus networks.*

The sections below describe possible SDN use cases in the data center, the WAN and the campus. In some instances the use cases are generic and in some instances the use cases reflect actual implementations. In many cases the placement of the use case is somewhat arbitrary. For example, most of the use cases that are included in the data center section could also be included in the campus networks section.

**Data Center**

**Virtual Machine Migration**

One of the advantages of server virtualization is that it enables moving VMs between physical servers. However, when a VM is moved between servers, the VM needs to be on the same VLAN after it was moved as it was on prior to the migration. Extending VLANS across a data center in order to support workload mobility adds to the operational cost and complexity and it adds time to the process because it requires that each switch in the end-to-end path be manually reconfigured.
Network virtualization resolves that challenge because with network virtualization when a VM changes location, even to a new subnet in the physical network, the switches at the edge of the overlay automatically update their mapping tables to reflect the new physical location of the VM. One of the advantages of network virtualization is that since the necessary changes are performed only at the network edge, nothing has to be done to the remainder of the network.

**Service Chaining**

In a traditional data center implementing L4 – L7 services such as firewalls and WAN optimization is cumbersome and time consuming as it requires acquiring the requisite network appliances and cabling them together in the correct order. Since each appliance has its own unique interface, configuring these appliances is a time consuming, error-prone task.

SDN overcomes the challenges of implementing L4 – L7 services by implementing two closely related techniques: service insertion and service chaining. The phrase *service insertion* refers to the ability to dynamically steer traffic flows to a physical or virtual server that provides one of the L4 – L7 services that were listed above. The phrase *service chaining* refers to the ability to dynamically steer traffic flows through a sequence of physical or virtual servers that provide the same type of L4 – L7 services.

**Security Services**

By virtue of Layer 2-4 flow matching capability, OpenFlow access switches can perform filtering of packets as they enter the network, acting as simple firewalls at the edge. With OpenFlow switches that support modification of packet headers, an OpenFlow-enabled controller will also be able to have the switch redirect certain suspicious traffic flows to higher-layer security controls, such as IDS/IPS systems, application firewalls, and Data Loss Prevention (DLP) devices. Other security applications built on OpenFlow controller can match suspicious flows to databases of malware signatures or divert DDoS attacks.

**Load Balancer Services**

OpenFlow with packet header modification will also allow the switch to function as a simple, cost-effective load-balancing device. With modification functionality, a new flow can result in a new flow table entry that includes an action to modify the destination MAC and IP addresses. The modified address can be used to direct traffic to the server selected by the controller load balancing application.

Indiana University (IU) has developed an OpenFlow-based, load-balancing application called FlowScale. According to the University, “FlowScale provides complex, distributed load balancing of network traffic using an OpenFlow-capable Top of Rack (ToR) switch. IU deployed the application into its Intrusion Detection System (IDS) to distribute traffic evenly to sensors. FlowScale is currently being deployed as part of the Intrusion Detection Systems operated by the Indiana University Information Security Office.

**New Software Defined Cloud model**

A national Cloud Leader is creating a new architecture that will allow all network and value-added services to be software defined, based on SDN. They are using OpenStack both for overall orchestration and also for its end user-friendly Horizon dashboard. While customers
interact with the system via the dashboard, their administrators leverage REST APIs to interact both with OpenStack and with the SDN. The SDN provides a virtual network overlay for a consistent, unified fabric over the entire network and all datacenters (planned expansion is 10 datacenters by 2018).

This use of SDN helps the Cloud Leader change how data center services are offered. New capabilities include:

- Full Datacenter Capabilities: Most public clouds offer compute and storage but do not systematically address networking. Their approach provides a complete datacenter approach that spans compute, network, and storage.
- Full UI-driven Self-service: Customers can control every aspect of their virtualized environment using their user interface. This capability both increases customer control and enables the cloud leader to handle huge volumes of customers and VMs – projected to be 1 million VMs at the end of the first year of operation.
- Full Network Programmability: SDN provides a coherent cloud network fabric that enables programmability from the datacenter endpoint all the way through the network. The fabric enables a number of new capabilities including consistent network service independent of underlying hardware, full workload portability among datacenters, and full programmability for future services.
- High Security within the Datacenter: Legacy security approaches focus on external threats rather than threats within the datacenter. The SDN's built-in security, including a default “Zero Trust” model, operates at the virtual machine level. These capabilities provide security and isolation within the rack, within each customer’s operations, and within the datacenter.

New Distributed Cloud Hosting model

A telecommunications service provider (TSP) in EMEA has created a virtual Platform Optimized Design (vPOD) architecture that provides Cloud efficiencies along with the flexibility of offering either shared or dedicated resources distributed among datacenters. SDN provides the interconnection within and among all vPODs and among all datacenters. Having a cohesive, unified cloud across datacenters enables consistent performance critical for SLAs, robust disaster recovery, and other value-added services.

New capabilities include:

- Precision SLAs for each Customer: Adding precise network controls to server virtualization and OpenStack orchestration, the TSP’s key customer demand of precise, end-to-end SLAs can be reliably delivered even on shared vPODs.
- Consistent Performance Across Datacenters: Similar to server virtualization, network virtualization provides consistent and predictable performance that is independent of each datacenter’s build-out, hardware configurations, and network architectures. This capability enables a range of new customer-centric capabilities such as load balancing workloads across datacenters.
- Fluid Disaster Recovery: Having consistent performance independent of datacenter build-out changes how disaster recovery is performed. Instead of having idle resources standing by in a dedicated datacenter, a customers’ implementation can be stretch-clustered across datacenters for truly fluid disaster recovery. In this fashion, loss of one or even multiple datacenters can be accommodated without disruption to operations.
- Effortless Datacenter Scalability: With this architecture, the TSP can scale-out to accommodate the needs of each customer just by adding vPODs or by adding racks to
a dedicated vPOD. They also can easily scale out to 100 times their initial rack count and up to millions of managed endpoints without having to change the architecture or the configuration.

- Fast and Non-disruptive Provisioning: Outside of physical racking and cabling, new vPODs can be added in an automated and non-disruptive manner — the entire installation or de-installation process takes only a few hours. New servers can be allocated to a vPOD nearly instantaneously via automation.

**WAN**

**The Google G-Scale WAN**

As is discussed in *An Overview of OpenFlow V1.3*, one of the primary benefits of OpenFlow is the centralized nature of the Forwarding Information Base (FIB). Centralization allows optimum routes to be calculated deterministically for each flow by leveraging a complete model of the end-to-end topology of the network. Based on an understanding of the service levels required for each type of flow, the centralized OpenFlow controller can apply traffic engineering principles to ensure each flow is properly serviced. Bandwidth allocations can be controlled dynamically to provide bandwidth on demand with changing traffic patterns. The result can be much better utilization of the network without sacrificing service quality. Centralized route processing also allows the pre-computation of a set of fail-over routes for each possible link or node failure.

The Google G-Scale WAN backbone links its various global data centers. G-Scale is a prime example of a production OpenFlow Layer 3 network that is realizing the benefits of FIB centralization. The G-Scale control plane is based on BGP and IS-to-IS and the OpenFlow-only switches are very simple 128 port 10 GbE switches built by Google using merchant silicon (when Google built these switches, 128 port 10 GbE switches had not yet been introduced in the commercial market). Google has identified a number of benefits that are associated with its G-Scale WAN backbone including that Google can run the network at utilization levels up to 95%.

**Campus**

Below are some popular use cases associated with deploying SDN in branch and campus networks.

**Dynamic QoS & Traffic Engineering**

The hop-by-hop routing and queuing techniques currently used in branch and campus networks yield a best effort network that results in poor quality for applications such as unified communications (UC). For the sake of example, consider the case of two users, User A and User B, of a popular UC application: Microsoft Lync. When User A asks Lync to make a call to User B, the Lync call controller converts User B’s contact information to an IP address. The Lync call controller sends this IP address to the Lync client running on User A’s laptop. A call is then started between the two users, but there is nothing in the call setup to indicate that the traffic for this call should have higher priority than other traffic.

In an SDN environment, as the Lync call controller is sending the IP address to the Lync client running on User A’s laptop, the Lync controller can be configured to also send it to an SDN application, whose function is to communicate with an SDN controller and have the priority set
to specified values for specific IP pairs in a network. A Lync call, for instance, could be set to a high priority. The SDN application communicates to the SDN controller that the priority level for traffic between a specific pair of IP addresses needs to be set to high and that this traffic should run over non-congested links. The SDN controller takes this information and determines the optimal path for the packets to flow through the network from User A to User B. This flow matching information, along with the required actions, are pushed out to each of the OpenFlow-enabled switches.

**Unified Wired and Wireless Networks**

Typically, wireless networks have been built as overlays to a wired network. As a result, in the vast majority of cases the wired and wireless networks in a campus operate as separate entities. This situation has a negative impact on users because it means that users will likely have different experiences based on whether they are using a wired or a wireless access device. This situation also negatively impacts IT organizations because maintenance and troubleshooting are unduly complex due to the fact there are two separate management systems, two separate sets of policies and two separate authentication processes.

One of the advantages of integrating the wireless and wired networks in a campus is that it results in a single-pane-of-glass management of the unified wired and wireless network. Using SDN technologies for this integration will make network provisioning more dynamic. For example, as wireless devices roam from AP (access point) to AP the policy associated with the user moves as well. Another advantage of the SDN architecture and related technologies is that they enable enforcing policy at a very granular level. This means, for example, that it is possible to set quality of service policies on a per user or per device basis. Another example of a granular policy option that is enabled by SDN is that if the IT organization trusts traffic from a specific SSID, it can decide to let that traffic bypass the firewall and hence not consume firewall resources needlessly.

**QoS Management for Microsoft Lync across wired and wireless networks**

This use case can be viewed as a combination of the preceding two use cases. As previously noted, enterprises are rapidly adopting Microsoft’s Lync as their unified communications solution of choice, but until recently a unifying Lync wired and wireless solution wasn’t available in the market. That is important because wireless has become the edge of the network and mobile users have a growing dependency on wireless services for performing critical job tasks. This situation creates a challenge relative to how wireless users can effectively and reliably access Lync services.

Recently an OpenFlow-based application that bridges wired and wireless networks to ensure a user the highest quality of experience with Microsoft’s Lync has entered the market. The solution can detect quality of service issues, identify resolutions and prioritize traffic across any OpenFlow-enabled network. The solution also enables the wireless and wired network to dynamically change in response to application traffic requirements.

**Personal Bonjour**

When Apple announced Bonjour, its zero-configuration application, it filled a void in the market. Users could simply access a network attached television or printer, as long as the device was on the same sub-net. Businesses quickly saw value in this class of application and commercial network centric solutions opened Bonjour up to more expansive networks. However, this
created a management challenge relative to user and device associations with larger populations of network users and devices.

Recently an OpenFlow-based application has been introduced to the market that implements the highest granularity policy management for Bonjour service access available. This application has functionality that enables IT organizations to ensure that individual users may be allowed to only access selected devices, in selected locations, at selected times of day. One way that this can be used is that a dormitory full of students, each with their own printer or TV, can be isolated from all other users without the network congestion often encountered with a standard Bonjour implementation.

**Role Based Access**

It is often useful to control what users can and cannot do on a network based on the role they play within the organization. One of the strengths of the SDN architecture and the OpenFlow protocol is that they offer a hardware- and software-independent abstraction model to access and manipulate resources. One way that the abstraction model can be leveraged to implement role-based resource allocation is by leveraging the authentication functionality that exists between the user and the NAC (Network Access Control) application in such a way that when the authentication process is complete, a message is sent to a role-based resource allocation SDN application. The message contains the MAC address of the user, the port of entry in the network, and the role of the user. The application then finds the user in a previously configured capabilities list. This list contains information such as which devices and other users this new user can communicate with; which VLAN the user should be assigned to; how much bandwidth the user can have assigned to its traffic; and what IP addresses are off limits. These capabilities are converted to a network resource message that is sent to the SDN controller. The SDN controller then communicates with the appropriate network device and configures the OpenFlow tables on that device to ensure the appropriate priority setting for the user’s traffic, the appropriate bandwidth as well as instructions to drop flows to restricted addresses.
The Operational Implications

One of the operational implications of adopting SDN is the movement to a DevOps operational model.

A detailed discussion of DevOps is contained in the subsequent chapter of The Guide.

Security

SDN creates security opportunities and security challenges.

The fact that SDN poses both security opportunities and security challenges was demonstrated by Table 5 and Table 6. Table 5 shows that 35% of network organizations believe that SDN will enable them to implement more effective security functionality. Table 6 shows that 12% of network organizations believe that concerns about how possible security vulnerabilities is a significant inhibitor to SDN deployment.

Two examples of how SDN can enhance security were already discussed. In one of those examples, security services were implemented based on OpenFlow-based access switches filtering packets as they enter the network. In the second example, role based access is implemented by deploying a role-based resource allocation application that leverages the control information and capability of the SDN controller. Other security related use cases include leveraging the control information and capability of the SDN controller to provide DDoS protection.

Some of the security challenges related to SDN are described in SDN Security Considerations in the Data Center. As pointed out in that document:

- The centralized controller emerges as a potential single point of attack and failure that must be protected from threats.
- The southbound interface between the controller and underlying networking devices (that is, OpenFlow), is vulnerable to threats that could degrade the availability, performance, and integrity of the network.
- The underlying network infrastructure must be capable of enduring occasional periods where the SDN controller is unavailable, yet ensure that any new flows will be synchronized once the devices resume communications with the controller.

Other security-related considerations include that IT organizations should:

1. Implement measures to deal with possible control flow saturation (controller DDOS) attacks;
2. Harden the SDN controller’s operating system to ensure availability of the controller function;
3. Implement effective authentication and authorization procedures that govern operator access to the controller.

Chapter 2 of The 2013 Guide to Network Virtualization and SDN contains a set of 5 key questions that network organizations can ask vendors about the security of their SDN solutions.
Cloud Orchestration

Cloud Orchestration platforms have evolved as a means of automating and facilitating the process of configuring pools of data center resources in order to provide a range of cloud or cloud-like services, such as Infrastructure as a Service (IaaS) solutions. The Orchestrator’s role is to manipulate the basic resources of the data center (i.e., VMs, networks, storage, and applications) at a very high level of abstraction to create the service. Orchestration is most effective when the data center is fully virtualized, facilitating software control/reconfiguration and automation. As a result, there is a natural affinity between Orchestration and SDN controllers.

OpenStack is a cloud computing orchestration project offering free open source software released under the terms of the Apache License. The project is managed by the OpenStack Foundation, a non-profit corporate entity established in September 2012 to promote OpenStack software and its community. Apache CloudStack is another open source Apache Licensed orchestration system. Eucalyptus is a third open source orchestrator with tight technical ties to Amazon Web Services (AWS).

In addition, there are a number of proprietary orchestrators that offer open APIs to allow integration across vendor boundaries. These include VMware’s vCloud Director and IBM’s SmartCloud Orchestrator.

Figure 3 shows a block diagram of the OpenStack system, including the OpenStack modules that are used to control resource pools in the data center, including Horizon and Neutron.

Horizon is the OpenStack Dashboard that provides administrators and users a graphical interface to access, provision and automate cloud-based resources. The dashboard is one of several ways users can interact with OpenStack resources. Developers can automate access or build tools to manage resources using the native OpenStack API or the EC2 compatibility API. The dashboard also provides a self-service portal for users to provision their own resources within set limits.

Neutron (formerly called Quantum) allows users to create their own networks, provide connectivity for servers and devices, and control traffic. With appropriate Neutron plug-ins, administrators can take advantage of various SDN solutions to allow for multi-tenancy and scalability. A number of drivers/plugins are included with the OpenStack source code. OpenStack networking also has an extension framework allowing additional network services,
such as intrusion detection systems (IDS), load balancing, firewalls and virtual private networks (VPN) to be deployed and managed. One example of the extension service is the Load Balancer as a Service (LBaaS) driver for Neutron available starting with the October 2013 Havana release. The driver enables ADC vendors to offer simple LBaaS plugins for Neutron, allowing their ADCs to be directly provisioned by OpenStack. Vendor-specific driver plug-ins that are contributed to the project are included in the OpenStack source code.

In conjunction with the Orchestrator, the role of the SDN controller is to translate the abstract model created on the Orchestrator into the appropriate configuration of the virtual and physical resources that will deliver the desired service. For example, the Orchestrator can instruct the controller to perform a variety of workflows, including:

- Create a VM;
- Assign a VM to a Virtual Network (VN);
- Connect a VM to an external network;
- Apply a security policy to a group of VMs or a VN;
- Attach Network Services to a VM or chain Network Services between VMs.

Figure 4 provides a high level depiction of how an orchestrator (OpenStack) and an overlay-based SDN controller might interact to place a VM into service within a VN.

The Nova compute module in OpenStack instructs the Nova Agent in the hypervisor to create the VM. The Nova agent communicates with the Neutron module in OpenStack to learn the network attributes of the VM. The Nova agent then informs the vSwitch agent to configure the virtual network for the VM and then the controller provides the route table entries needed by the vSwitch.

With the April 2014 Icehouse release of OpenStack the Heat Orchestration Service has been added. Heat is a template-driven engine that allows application developers to describe and automate the deployment of infrastructure through both an OpenStack-native REST API and a CloudFormation-compatible Query API. The flexible template language can specify compute, storage, and networking configurations to automate the full provisioning of infrastructure as well as services and applications. Through integration with the Celiometer Telemetry service, the Heat engine can also perform auto-scaling of certain infrastructure elements. Celiometer aggregates usage and performance data across the services deployed in an OpenStack cloud. This capability provides visibility and insight into the usage of the cloud across multiple data points and allows cloud operators to view service level metrics globally or by individual deployed resources. Usage data can be used for billing and charge back purposes.
The Survey Respondents were asked to indicate the approach that their company is taking relative to orchestration. Their responses are shown in Table 9.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>We have a well thought out strategy and we have begun to execute against that strategy</td>
<td>16%</td>
</tr>
<tr>
<td>We have a well thought out strategy but we have not yet begun to execute against that strategy</td>
<td>6%</td>
</tr>
<tr>
<td>We are in the process of developing a strategy and are optimistic that it will come together relatively quickly</td>
<td>21%</td>
</tr>
<tr>
<td>We are in the process of developing a strategy but have some concerns that the existing solutions are immature</td>
<td>30%</td>
</tr>
<tr>
<td>Don't know/NA</td>
<td>22%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

The vast majority of IT organizations don’t have a well thought out strategy for how they will implement orchestration.

Management

SDN creates management opportunities and security challenges.

The fact that SDN poses both management opportunities and management challenges was demonstrated by Table 5 and Table 6. Table 5 shows that 53% of network organizations believe that SDN will ease the administrative burden of management tasks such as configuration and provisioning. Table 6 shows that 13% of network organizations believe that concerns about how to manage SDN is a significant inhibitor to SDN deployment.

An architectural view of the key management challenges at each tier of the SDN architecture is depicted in Figure 5 which was published in the ONF document entitled SDN Architecture Overview. One of the conclusions that can be drawn from Figure 5 is that:

In SDN environments the challenges associated with end-to-end service performance management are more demanding than they are in traditional network environments.

This follows because in a SDN environment there is a need to monitor additional components, such as SDN controllers, in an environment that is a combination of physical and virtual resources and which is changing dynamically. From a service performance management perspective, the SDN controller can be viewed as a service enabler that needs to be instrumented and monitored just as any other application server. Whether it is OpenFlow or some other protocol that enables communications between the SDN controller and the network elements that protocol needs to be monitored the same way as any other protocol. In similar fashion, the combination of virtual and physical network elements need to be instrumented end-to-end and monitored across the entire infrastructure.
At the bottom of Figure 5, the data plane is comprised of network elements, whose SDN Datapaths expose their capabilities through the Control-Data-Plane Interface (CDPI) Agent. At the top of Figure 5, SDN Applications communicate their requirements via NBI Drivers. In the middle of the figure, the SDN Controller translates these requirements and exerts low-level control over the SDN Datapaths, while providing relevant information up to the SDN Applications.

One of the management challenges that applies across multiple tiers of the SDN architecture is the requirement to manage the messaging that goes between tiers; e.g., between the application tier and the control tier as well as between the control tier and the infrastructure tier. Another challenge that goes across tiers is the requirement to assign the SDN Datapaths to their SDN Controller and to configure policies that define the scope of control given to the SDN Controller or SDN Application.

At the infrastructure tier, one of the primary challenges is to perform element management potentially of both virtual and physical network elements. One of the management challenges at the control layer results from the fact that the controller is in the data path for new flows entering the network. During periods when many new flows are being created, the controller can potentially become a performance bottleneck adding significant latency for flow initiation. Performance management systems need visibility not only into application performance but also controller performance in processing flows.
As described in the preceding discussion of the North Bound Interface (NBI), one of the management challenges that occurs at the application tier is that based on the type of application (e.g., business application vs. a firewall) the service or application needs varying levels of visibility into the underlying network. Another set of management challenges that occurs at the application layer stem from the requirement to ensure acceptable performance. As described below, one thing this means is that network management organizations must have visibility into the SLA requirements of the application so that resources can be dynamically allocated to meet those requirements.

Looking at network virtualization as an application of SDN, another one of the performance management challenges stems from the fact that one of the primary benefits of overlay-based SDN solutions is the ability to support multiple virtual networks that run on top of a physical network. As previously mentioned, in order to perform management functions such as root cause analysis and impact analysis, network management organizations need the ability to see the bilateral mapping between the virtual networks and the physical network that supports them.

While understanding the mapping between the virtual networks and the physical infrastructure is necessary, it is not sufficient. For example, with the virtualization of L4 – L7 functions, software running on VMs can readily be moved among physical servers or replicated to run on newly created VMs in order to dynamically maintain availability, expand/shrink capacity, or balance the load across physical resources. Many of these changes in the infrastructure can be automated and programmatically activated to conform to configured policies under specific sets of circumstances. For example, consider the traffic of an important IP application flow that has a medium priority class. If congestion in the network results in excessive packet loss, it may be necessary to change the traffic classification to be high in order to continue to meet an established SLA.

**SDN holds the potential to enable IT organizations to dynamically change the environment in order to meet SLAs.**

However, due to the mobility of VMs or the need to change QoS settings, topology changes can occur in a matter of seconds rather than the days or weeks required for changing software/hardware relationships in traditional networks. In order to accommodate and leverage the virtualization technologies, network management organizations need tools that enable them to be able to dynamically discover, procure, allocate and reconfigure resources. In addition:

*Network management organizations need to be able to perform a two-way mapping between an application or service and all of the virtual services that support it and they must also be able to perform a two-way mapping between the virtual services that support a given service or application and the physical infrastructure that supports them.*

Given the challenges described above as well as the requirement to integrate the traditional legacy environment with the emerging software-centric environment:

*Applications and services need to be instrumented end-to-end.*

The physical and virtual environments should be instrumented independently and network management organizations should have the ability to contextually correlate and consolidate the two management datasets into one consistent and cohesive dataset which offers operational insight into the end-to-end service delivery.
Chapter 2 of The 2013 Guide to Network Virtualization and SDN contains a set of 5 key questions that network organizations can ask vendors about the management of their SDN solutions.

**Organizational Impact**

SDN can be viewed as being a part of a broader movement to implement all IT functionality in software, referred to as Software Defined Everything (SDE). The primary drivers of the SDE movement are the need to support a more agile IT operational model as well as increasingly more agile business processes.

As described in The Changing Role of the IT & Network Professional, because of the growing adoption of an SDE approach many organizations are implementing DevOps. DevOps is described in the next chapter of this e-book. As is also described in The Changing Role of the IT & Network Professional the adoption of an SDE approach is causing the role of network and IT infrastructure professionals to change. Some of the key characteristics of the emerging roles are:

- **An increased knowledge of other IT disciplines**

  In a recent blog, GE Capital’s CTO Eric Reed explained the need for all IT professionals to expand their area of expertise. According to Reed, “Our experience [GE Capital’s] on this journey to date has been that the small, self-directed teams required in a DevOps world require an amalgamation of skills spanning everything from IT security to database design and application architecture, plus everything in between. While each individual on the team has a particular strength (say, application design and coding), each one also needs to have working knowledge in other areas (maybe UX or network design).”

- **More focus on setting policy**

  Emerging technologies and architectures (e.g., Software Defined Networking, Network Functions Virtualization) enable IT organizations to implement a policy driven infrastructure in a more dynamic and granular fashion than was previously possible. It will take some time to adjust to these new capabilities, but the vast majority of IT organizations will adjust and will place more emphasis on setting policy.

- **More knowledge of the business**

  The need for more knowledge of the business is driven in part by the need for IT and network professionals to implement a policy driven infrastructure that is based on the specific requirements of the business. In addition, the ability of the IT organization to justify an investment in IT is increasingly tied to the ability of the organization to concretely demonstrate the business value of that investment.

- **More understanding of applications**

  While client server and n-tier applications are still common, as pointed out in The 2013 Application and Service Delivery Handbook, many applications are now based on a wide range of architectures; e.g., a Services Oriented Architecture (SOA). In addition, complex applications, such as Customer Relationship Management (CRM), are actually
comprised of several modules, with a range of network requirements. IT infrastructure and network professionals in particular need to better understand these new architectures and complex applications in order to ensure that the emerging set of technologies are designed and architected appropriately.

- **More emphasis on programming**

  While it is not true that all networking and data center professionals will become programmers, it is true that many senior level IT professionals will need an understanding of programming in order to better interact with the company’s software development organization. It is also true that some network organizations will want to leverage the API functionality that the emerging technologies provide by having network professionals write programs that utilize those APIs.

The Survey Respondents were told that SDN is part of a broader movement to implement all IT functionality in software, referred to as Software Defined Everything (SDE) and they were asked a number of questions about how the SDE movement has and would likely impact their organization as well as how it would likely impact their jobs. There were 122 responses from people who are involved with enterprise communications networks and 19 responses from people who work for a service provider that offers WAN services. Given that there are only 19 responses from service providers that is not a large enough sample size to be statistically significant. It is, however, large enough to provide insight into the organizational impact that the ongoing adoption of software based functionality is having on WAN service providers.

For example, The Survey Respondents were asked if within the last year the SDE movement had prompted their IT organization to do a re-org. Nine percent of enterprise respondents said yes and 32% of service provider respondents said yes. These responses make it appear as if service providers are further along relative to reorganizing the company to leverage software-based IT functionality.

The Survey Respondents were also asked how much of an impact they thought that the SDE movement will have on the structure of their company’s IT organization over the next two years? Their answers are shown in Table 10.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Percentage of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Significant Impact</td>
<td>4%</td>
</tr>
<tr>
<td>Significant Impact</td>
<td>16%</td>
</tr>
<tr>
<td>Moderate Impact</td>
<td>14%</td>
</tr>
<tr>
<td>Some Impact</td>
<td>18%</td>
</tr>
<tr>
<td>No Impact</td>
<td>23%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>25%</td>
</tr>
</tbody>
</table>

*Table 10: Impact of SDN on Organizational Structure*

*Over the next two years the ongoing adoption of software-based IT functionality is likely to have an impact on the structure of IT organizations.*
Some of the answers from service provider respondents when asked to indicate the type of organizational changes that had either already occurred or that they expected would occur include:

- The operations group is likely to be restructured;
- We now need to gather management from virtual devices;
- The company’s technical experts have been consolidated into a single group;
- The company has set up a subsidiary and are in the process of moving IT employees to that subsidiary;
- The organization’s OSS/BSSs need to be revamped.

When asked the same question, the answers from the enterprise respondents included:

- A shift from siloed specialists to service aligned generalists;
- A likely re-org around application development and network operations;
- An increase in cross functional teams and projects;
- Moving from a tower based organization to a DevOps model;
- An increased focus on software engineering;
- Team work will involve an enhanced mix of skills including programming, networking, virtualization and DevOps;

In addition, the Survey Respondents were asked how much of an impact they thought that the SDE movement will have on the nature of their jobs over the next two years? Their answers are shown in Table 11.

<table>
<thead>
<tr>
<th>Impact</th>
<th>Percentage of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Significant Impact</td>
<td>6%</td>
</tr>
<tr>
<td>Significant Impact</td>
<td>19%</td>
</tr>
<tr>
<td>Moderate Impact</td>
<td>16%</td>
</tr>
<tr>
<td>Some Impact</td>
<td>23%</td>
</tr>
<tr>
<td>No Impact</td>
<td>19%</td>
</tr>
<tr>
<td>Don't Know</td>
<td>18%</td>
</tr>
</tbody>
</table>

_Over the next two years the ongoing adoption of software-based IT functionality is likely to have an impact on the jobs of IT professionals._

Some of the answers from service provider respondents when asked to indicate the type of impact on their jobs that had either already occurred due to the ongoing adoption of software-based IT functionality or that they expected would occur include:

- The product development life cycle will change;
- The job will require new skills in general and more knowledge of software in particular;
- The customer demands are unknown;
• Product development needs to be able to provide tools to manage and monitor the environment;
• There will be new business models, new product offerings that must be supported.

When asked the same question, the answers from the enterprise respondents included:

• The way to design, implement and troubleshoot networks will change a lot;
• The job will require new skill sets in general and more programming knowledge in particular;
• There will be new security requirements;
• As we adopt DevOps, broad based skills are required;
• There will be less emphasis on technology silos;
• New architectures will need to be developed;
• There will be a lot of re-training and re-trenching.
About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division’s focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim’s current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.
Software-Defined Networking (SDN) and Network Virtualization (NV) are quickly becoming priorities because of the promise to dynamically manage traffic loads while lowering costs in response to changing business requirements...

Are you prepared for this evolution?

EMC understands these challenges. Designed to manage physical, virtual and cloud environments, the EMC Service Assurance Suite helps IT operations teams manage infrastructure across each phase of this evolution.

Empower your IT operations team to visualize, analyze, and optimize your service-delivery infrastructure. Learn more at www.emc.com/sa.

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, email us at asd@emc.com or call 866-438-3622.