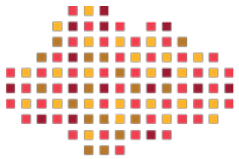
The 2013 Guide to Network Virtualization and SDN

Part 2: The What, Why and How of SDN

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

Sponsored in part by:



nuagenetworks

Produced by:

Webtorials

Table of Contents

Executive Summary

Over the last year, the hottest topics in networking have been Network Virtualization (NV) and Software Defined Networking (SDN). There is, however, considerable confusion amongst enterprise IT organizations relative to these topics. There are many sources of that confusion, including the sheer number of vendors who have solutions that solve different problems using different solution architectures and technologies, all of whom claim to be offering SDN and/or NV solutions.

The primary goal of the ***2013 Guide to Software Defined Networking & Network Virtualization*** (**The Guide**) is to eliminate that confusion and accelerate the adoption of NV and/or SDN. The guide will achieve that goal by walking the readers through the following set of topics:

1. What are the problems and opportunities that NV and SDN help to address?
2. What are the primary characteristics of NV and SDN solutions?
3. How does NV and SDN help IT organizations respond to problems and opportunities?
4. How are IT organizations approaching the evaluation and deployment of NV and/or SDN?
5. What is the role of organizations such as the ONF and the OpenDayLight consortium?
6. What approach are the key vendors taking relative to NV and SDN?
7. What should IT organizations do to get ready for NV and SDN?

The Guide will be published both in its entirety and in a serial fashion. This is the second of the serial publications. The first publication[1] focused on NV and this publication will focus on SDN. The two subsequent publications will focus on:

1. The Vendor Ecosystem
2. Planning for NV and SDN

In August and September of 2013 a survey was given to the subscribers of Webtorials. Throughout this document, the IT professionals who responded to the surveys will be referred to as *The Survey Respondents*.

1 webtorials.com/Metzler

Background

In the traditional approach to networking, most network functionality is implemented in a dedicated appliance; i.e., switch, router, application delivery controller. In addition, within the dedicated appliance, most of the functionality is implemented in dedicated hardware such as an ASIC (Application Specific Integrated Circuit).

Some of the key characteristics of this approach to developing network appliances are:

- The ASICs that provide the network functionality evolve slowly;
- The evolution of ASIC functionality is under the control of the provider of the appliance;
- The appliances are proprietary;
- Each appliance is configured individually;
- Tasks such as provisioning, change management and de-provisioning are very time consuming and error prone.

Networking organizations are under increasing pressure to be more efficient and agile. One source of that pressure results from the widespread adoption of server virtualization. As part of server virtualization, virtual machines (VMs) are dynamically moved between servers in a matter of seconds or minutes. However, if the movement of a VM crosses a Layer 3 boundary, it can take days or weeks to reconfigure the network to support the VM in its new location. It can sometimes be difficult to define exactly what it means for a network to be agile. That said, if it takes weeks to reconfigure the network to support the movement of a VM, that network isn't agile.

The bottom line is that a traditional network evolves slowly; is limited in functionality by what is provided by the vendors of the network appliances; has a relatively high level of OPEX and is relatively static in nature. The majority of the potential SDN use cases (see below) are intended to overcome those characteristics of traditional networks.

Potential SDN Use Cases

There is scene in the novel *Alice in Wonderland* that is directly relevant to the adoption of NV and SDN solutions. That scene is comprised of the following dialogue between Alice and the Cheshire cat.

Alice: "Would you tell me, please, which way I ought to go from here?"

Cheshire Cat: 'That depends a good deal on where you want to get to."

Alice: "I don't much care where."

Cheshire Cat: "Then it doesn't matter which way you go."

The relevance of that dialogue to SDN is that an analysis of SDN solution architectures and subtending protocols is totally irrelevant until IT organizations identify which use cases they are hoping to address with SDN.

The left hand column of **Table 1** contains some of the primary challenges & opportunities facing the typical IT organization. The Survey Respondents were shown those challenges & 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. Each row of the right hand column of **Table 1** contains the percentage of The Survey Respondents that indicated that they thought that SDN could help them to respond to the challenge or opportunity in the corresponding left hand column.

Table 1: Opportunities & Challenges that SDN Can Address	
Challenge or Opportunity	**Percentage**
Better utilize network resources	51%
Ease the administrative burden of configuration and provisioning QoS and Security	47%
Perform traffic engineering with an end-to-end view of the network	44%
More easily scale network functionality	39%
Support the dynamic movement, replication and allocation of virtual resources	38%
Establish virtual Ethernet networks without the limitations and configuration burden of VLANs	35%
Reduce Complexity	34%
Enable applications to dynamically request services from the network	32%
Reduce OPEX	30%
Have network functionality evolve more rapidly based on a software development lifecycle	27%
More easily implement QoS	27%
Implement more effective security functionality	26%
Reduce CAPEX	25%
We don't see any challenges or opportunities that SDN can help us with	3%
Don't know	3%
Other	3%

One observation that can be drawn from the data in **Table 1** is that there is a wide range of challenges and opportunities that The Survey Respondents believe that SDN can help with and conversely very few IT organizations believe that SDN won't be beneficial. Having a wide range of potential challenges and opportunities to respond to bodes well for the long-term adoption of SDN. However, having so many challenges and opportunities to respond to can create confusion in the short term and can possibly delay SDN adoption.

To exemplify the relationship between the opportunities & challenges and the two types of solutions analyzed in The Guide (i.e., NV and SDN), assume that the opportunity that a hypothetical IT organization is attempting to respond to is the need to support the dynamic movement, replication and allocation of virtual workloads. The hypothetical IT organization can respond to this challenge using any of the NV solutions that were discussed in the preceding chapter; e.g., solutions from Nuage Networks, Netsocket, Avaya and NEC. As a reminder to the reader, the NV solutions from Nuage Networks, Netsocket and Avaya are based on overlay technologies and the NV solution from NEC is based on manipulating the flow tables in NEC's SDN solution.

The situation is quite different if the opportunity that the hypothetical IT organization is trying to respond to is the need to make it easier to implement QoS or the need to enable applications to dynamically request services from the network. The hypothetical IT organization can potentially respond to both of these challenges by implementing an SDN solution whereas that organization couldn't respond to those challenges by just implementing one of the controller based NV solutions that were discussed in the

preceding chapter. As will be pointed out in the following discussion of a federated overlay/underlay model, it would potentially be possible for the hypothetical IT organization to respond to those challenges using a federation of NV overlay solutions and SDN solutions.

The challenges and opportunities that are identified in **Table 1** aren't dependent on any particular technology. For example, there are a number of technologies that can be implemented in order to ease the burden of configuration management. That said, a subsequent sub-section of this document identifies some of the specific use cases and benefits that are associated with the OpenFlow protocol.

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 2**.

Table 2: Focus of SDN Deployment

Focus of SDN Deployment	Percentage
Data Center	54%
Branch and/or Campus	26%
WAN	23%
We are likely to implement a service from a WAN service provider that is based on SDN	12%
We are unlikely to implement SDN within the next two years	11%
Don't know	11%
Other	7%

One observation that can be made from the data in **Table 2** is that while the primary interest in deploying SDN is focused on the data center, there is strong interest in deploying SDN broadly throughout an organization's entire network.

A Working Definition of SDN

Within the IT industry, there is not a universally agreed to definition of SDN. While **The Guide** will identify the primary characteristics of an SDN, it won't make any attempt to define SDN. It is, however, helpful to have a working definition of SDN. The working definition of SDN that will be used in this publication is the one created by the Open Networking Foundation (ONF).

The ONF is the group that is most associated with the development and standardization of SDN. According to the ONF[2], "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."

According to the ONF, the SDN architecture is:

- **Directly programmable**: Network control is directly programmable because it is decoupled from forwarding functions.
- **Agile**: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.
- **Centrally managed**: Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.
- **Programmatically configured**: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.
- **Open standards-based and vendor-neutral**: When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

Part of the confusion that surrounds SDN is that many vendors don't buy in totally to the ONF definition of SDN. For example, while the vast majority of vendors do include the centralization of control in their definition of SDN, there isn't agreement as to how much control should be centralized. In addition, while some vendors are viewing OpenFlow as a foundational element of their SDN solutions, other vendors are taking a wait and see approach to OpenFlow.

Another source of confusion is the relationship between NV and SDN. It's possible to implement an SDN that resembles the ONF definition of SDN and use that SDN to implement network virtualization. For example, the OpenDayLight foundation recently accepted a contribution from NEC, referred to as Virtual Tenant Networking (VTN), which enables an SDN to implement network virtualization by manipulating the flow tables that are associated with the OpenFlow protocol. It is also possible, however, to implement network virtualization without implementing an SDN as defined by the ONF. For

[2] https://www.opennetworking.org/sdn-resources/sdn-definition

example, as described in the previous section of The Guide, Avaya offers an NV solution that doesn't rely on a controller. In addition, both Nuage Networks and VMware/Nicira implement network virtualization using an overlay model and a controller. To add to the confusion, Nuage Networks refers to their solution as SDN while VMware is adamant that their solution is network virtualization and not SDN.

The Survey Respondents were given a set of characteristics that are often associated with SDN and were asked to indicate which two characteristics would provide the most value to their company's network. Their responses are shown in **Table 3**.

Table 3: Value of SDN Characteristics

Characteristic	Percentage
Centralization of configuration and policy management	45%
Programmability of network elements	31%
Automation of administrative tasks	28%
Centralization of control	28%
The development of network functionality on a software development cycle vs. a hardware cycle	27%
Open up the network to innovation by the entire ISV community	17%
The use of open protocols	10%
The use of open source solutions	8%
Other	2%
Don't Know	1%

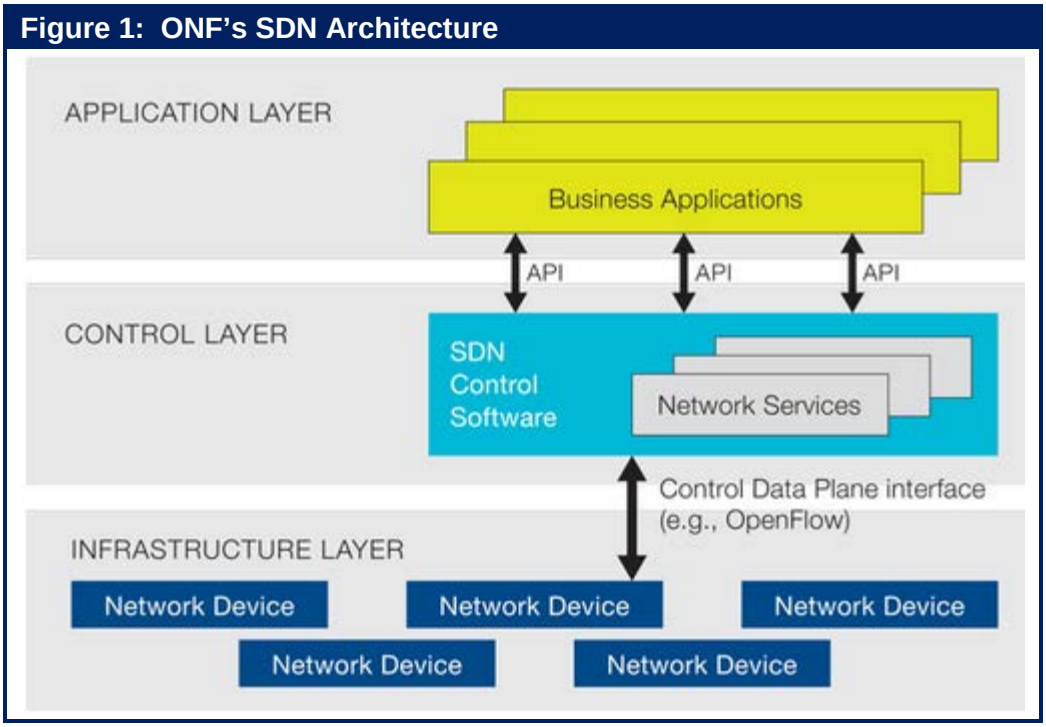
One observation that can be drawn from **Table 3** is that the characteristic of SDN that offers the most value to The Survey Respondents is tactical: The centralization of configuration and policy management. However, the second most important characteristic, the programmability of network elements, is strategic. That characteristic is strategic because the programmability of network elements is a key component of the overall functionality that is required in order to enable applications to dynamically request the network services they need.

Another observation that can be drawn from **Table 3** is that in spite of all of the discussion in the industry about open networking, The Survey Respondents were not very enthusiastic about the value that open protocols would bring to their networks.

The SDN Solution 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 NV and SDN solutions was described in the preceding section of The Guide.

Figure 1: ONF's SDN Architecture



Below are definitions of some terms that are commonly associated with SDN, some of which appear in **Figure 1**.

- **Business Applications**
  This refers to applications that are directly consumable by end users. Possibilities include video conferencing, supply chain management and customer relationship management.

- **Network Services**
  This refers to functionality that enables business applications to perform efficiently and securely. Possibilities include a wide range of L4 – L7 functionality including load balancing and security capabilities such as firewalls, IDS/IPS and DDoS protection.

- **Open Protocol**
  An open protocol is a protocol whose specification a company, or group of companies, has made public.

- **Standards Based Protocol**
  A standards based protocol is an open protocol that was created by a recognized standards body such as the ONF, the IEEE or the IETF.

- **Pure SDN Switch**
  In a pure SDN switch, all of the control functions of a traditional switch (i.e., routing protocols that are used to build forwarding information bases) are run in the central controller. The functionality in the switch is restricted entirely to the data plane.

- **Hybrid Switch**
  In a hybrid switch, SDN technologies and traditional switching protocols run simultaneously on a given switch. A network manager can configure the SDN controller to discover and control certain traffic flows while traditional, distributed networking protocols continue to direct the rest of the traffic on the network.

- **Hybrid Network**
  A hybrid network is a network in which traditional switches and SDN switches, whether they are pure SDN switches or hybrid switches, operate in the same environment.

- **Southbound API**
  Relative to **Figure 1**, the southbound API is the API that enables communications between the control layer and the infrastructure layer.

- **Service Chaining**[3]
  Service chaining is the ability to steer VM-VM traffic flows through a sequence of physical or virtual servers that provide network services, such as firewalls, IPS/IDS, DPI, or load balancers.

Figure 1 shows an API between the SDN control layer and the business applications. This API is commonly referred to as *the Northbound API*. The role of the northbound API is to enable communications between the control layer and the application layer. Currently there isn't a standard for the Northbound API, although the ONF has recently begun a process that could lead to a standards based API. While it isn't possible to state how the development of the northbound API will evolve, it is likely that there won't be a single northbound API, but multiple northbound APIs. One viable alternative is that there will be a northbound API between the SDN control software and each of the following entities:

- Network services
- Business applications
- Cloud management/orchestration systems

3 Service chaining was described in greater detail in the preceding section of The Guide.

Criteria to Evaluate SDN Solution Architectures

Below is a set of 7 questions that IT organizations should ask vendors who provide all or the majority of the SDN solution architecture that is shown in **Figure 1**. These questions focus on key criteria that IT organizations should use relative to evaluating alternative SDN solutions. A more complete set of criteria can be found in *A Mock RFI for SDN Solutions*[4].

As highlighted in the preceding discussion of Alice in Wonderland, SDN solutions need to be evaluated relative to their ability to respond to the specific challenges and opportunities facing an IT organization. For the sake of example, assume that one of the opportunities that an IT organization is hoping to respond to is enabling applications to dynamically request services from the network. Given that, then one question that the IT organization should ask vendors of SDN solutions is:

1. How does your SDN solution enable applications to dynamically request services from the network?

Other questions that IT organizations should ask SDN solution vendors include:

2. Describe the SDN solution that you are proposing and include in that description how the SDN architecture for the solution you are proposing is similar to the architecture shown in **Figure 1** and also describe how it is different. In your answer, identify the southbound protocols that you support and provide the rationale for supporting those protocols.

3. Identify the aspects of your solution architecture that enable high availability; that enable scalability of performance; that enable extensibility of functionality.

4. Which components of the solution architecture do you provide yourself? Which components do partners provide? If the solutions you are proposing includes components from partners, is there a single point of accountability for the solutions?

5. In your SDN solution, what control functions reside in the control layer and which control functions reside in the infrastructure layer?

6. Describe the Northbound protocol(s)/API(s) you support between the control layer and:

    - Network services
    - Enterprise applications
    - Cloud management/orchestration systems

7. How does your proposed solution implement network virtualization? Include in your answer whether overlays are used; what protocols are supported; how the tunneling control function is implemented. If virtual networks are defined by flow partitioning, describe which header fields are used and how the partitioning is accomplished.

4 Will be published at: webtorials.com/Metzler

The Inhibitors to SDN Adoption

The left hand column of **Table 4** contains some of the primary impediments to the adoption of SDN. The Survey Respondents were shown these 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. Each row of the right hand column of **Table 4** contains the percentage of The Survey Respondents that indicated that the impediment in the corresponding left column was one of the two primary inhibitors.

Table 4: Inhibitors to the Adoption of SDN

Impediment	Percentage
The immaturity of the current products	30%
The immaturity of the enabling technologies	29%
Other technology and/or business priorities	24%
The confusion and lack of definition in terms of vendors' strategies	22%
The lack of resources to evaluate SDN	21%
The lack of a critical mass of organizations that have deployed SDN	14%
Concerns that the technology will not scale to support enterprise sized networks	12%
We don't see a compelling value proposition	7%
Concern that this is just a passing fad	7%
Other	5%
The confusion around the impact of consortiums such as OpenDayLight	4%
We don't see any inhibitors to implementing SDN	3%
Don't know	3%

One clear observation that can be drawn from **Table 4** is that immaturity, broadly defined, is the primary inhibitor to the adoption of SDN. That includes the immaturity of the current products, the immaturity of the enabling technologies and the confusion and lack of definition in terms of vendor strategies.

The role that a compelling business case plays relative to driving and inhibiting the adoption of SDN is somewhat subtle. As shown in **Table 4**, only 7% of *The Survey Respondents* indicated that the lack of a compelling value proposition was an inhibitor to their adoption of SDN. It would be easy to conclude from that metric that business cases that demonstrate the compelling value of SDN exist and that these business cases are widely understood. Drawing the conclusion would be a mistake.

Arguing against that conclusion is the fact that 24% of *The Survey Respondents* indicated that "other technology and/or business priorities" was an inhibitor and that 21% of *The Survey Respondents* indicated that "the lack of resources to evaluate SDN" was an inhibitor. If indeed, there were compelling, well-understood SDN business cases, these organizations would rearrange their priorities and find the resources to evaluate SDN solutions.

The Overlay/Underlay Model

The preceding chapter of The Guide discussed ways to implement multiple virtual network topologies overlaid on a common physical network; a.k.a., an overlay model. That chapter also discussed some of the benefits and limitations of an overlay model. Some of those limitations were:

- Virtual and physical networks are separate entities, possibly with separate service assurance solutions, policy management, provisioning, and control points.

- As the virtual networks grow and evolve, the physical network does not automatically adapt to the changes. As a result, overlay NV requires a lightly oversubscribed or non-oversubscribed physical underlay network.

- Some value-added features in existing networks cannot be leveraged due to encapsulation. For example, the physical network loses its ability to provide differentiated services based on the content of the packet header.

An emerging approach to overcome the limitations of the overlay model is referred to as an overlay/underlay model. The cornerstone of this approach is a federation between the overlay network virtualization controller and the underlay SDN controller. In August 2013, HP and VMware announced their intention to work together to create an overlay/underlay solution[5]. As part of that announcement, HP stated their intention to develop a new application called ConvergedControl that will enable HP's Intelligent Management Center (IMC) to share information about the network with both the HP and the VMware controllers. As part of the announced solution, VMware's NSX controller will continue to provision the virtual network overlay and HP's SDN controller will continue to provision physical network flows on its switches. The solution is intended to enable the two controllers to work together to ensure that the virtual network gets the physical flows it needs. The solution is also intended to provide visibility across the virtual and physical environment so that, for example, if there is congestion or a failure on the physical network, the virtual environment is aware of the issue and can respond accordingly.

Network Function Virtualization

A concept that often gets discussed in conjunction with SDN is Network Function Virtualization (NFV). Strictly speaking, NFV is being driven primarily by telecommunications service providers to meet their specific requirements. Their interest in NFV stems from the fact that in the current environment, telecommunications and networking software is being run on three types of platforms:

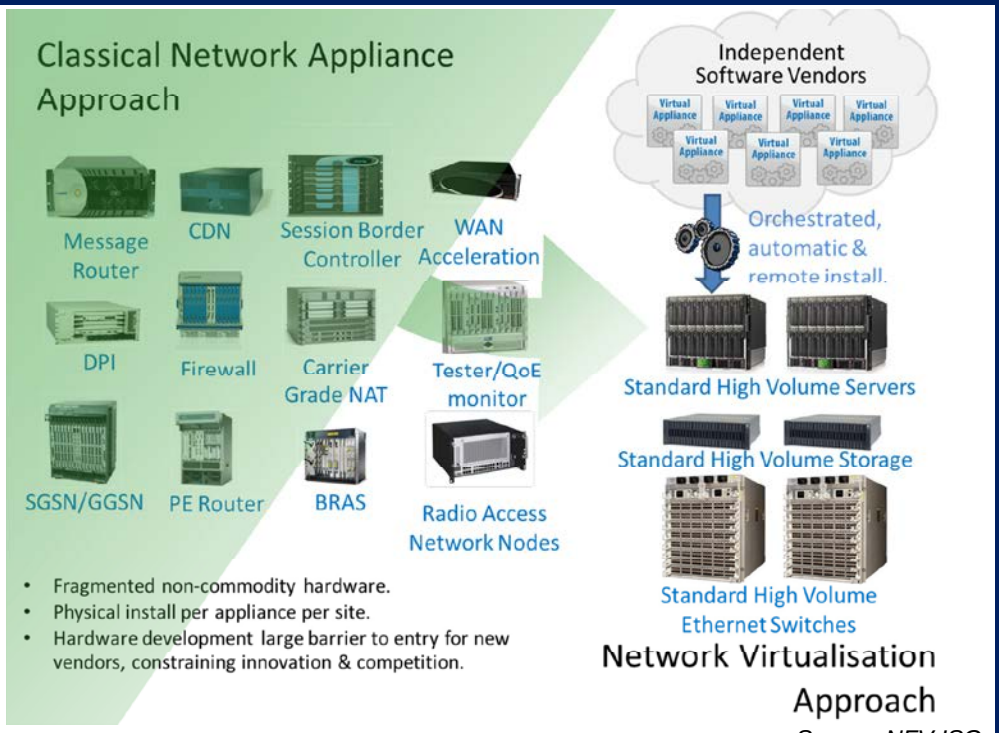
- Industry standard servers running Linux or Windows;
- Virtual appliances running over hypervisors on industry standard hardware servers;
- Proprietary hardware appliances.

Telecommunications service providers feel that they can greatly simplify their operations and reduce capital expense if all network functions were available as virtual appliances that can be easily provisioned and integrated regardless of the vendor who provided the appliance or the hypervisor(s) on which it runs.

5 http://searchsdn.techtarget.com/news/2240204281/HP-and-VMware-NSX-Joint-management-for-virtual-and-physical-networks

In order to bring this vision to fruition, an Industry Specifications Group for Network Functions Virtualization (NFV ISG) has been formed under the auspices of the European Telecommunications Standards Institute (ETSI). Their vision for the transition from hardware appliances of today to a fully virtualized appliance environment is depicted in **Figure 2**.

Figure 2: The Virtualization of Network Appliances



Source: NFV ISG

The approach that the NFV ISG is taking is that the virtualization of network functionality is applicable to any data plane packet processing and control plane function in both fixed and mobile networks. As shown in **Figure 2**, examples of these functions include:

- Switching elements;
- Tunneling gateway elements: IPSec/SSL VPN gateways;
- Traffic analysis: DPI, QoE measurement;
- Service Assurance, SLA monitoring, Test and Diagnostics;
- Application-level optimization: ADCs, WOCs;
- Security functions: Firewalls, virus scanners, intrusion detection systems;
- Multi-function home routers and set top boxes;
- Mobile network nodes.

The initial members of the NFV ISG were service providers such as AT&T, Deutsche Telekom and NTT. Its membership[6] has since grown and now includes a number of equipment vendors, but currently relatively few of the top vendors of virtual appliances are members.

6 http://portal.etsi.org/NFV/NFV_List_members.asp

The first meeting of the group was held in January 2013 and a number of smaller working groups were created in April 2013. In October 2013, ETSI published the first five specifications relative to NFV[7]. According to ETSI[8], "The five published documents include four ETSI Group Specifications (GSs) designed to align understanding about NFV across the industry. They cover NFV use cases, requirements, the architectural framework, and terminology. The fifth GS defines a framework for co-ordinating and promoting public demonstrations of Proof of Concept (PoC) platforms illustrating key aspects of NFV. Its objective is to encourage the development of an open ecosystem by integrating components from different players."

While the development of SDN and the development of NFV can proceed independently, there are some areas of possible overlap and cooperation. For example, one of the primary challenges the NFV group is facing is that the Operational Support Systems/Business Support Systems (OSS/BSS) that telecommunications service providers use must be able to automate the orchestration and provisioning of NFV appliances. While the NFV group believes its goals can be achieved using non-SDN mechanisms, the group is looking closely to see if standards coming from SDN consortia, such as the ONF and the OpenDaylight consortium, apply to NFV. As such, one possibility is that standards coming from the development of NV and SDN may facilitate the development of NFV. Alternatively, the development of NFV may result in technologies that facilitate the provisioning of virtual appliances in a NV or SDN solution.

7 http://www.etsi.org/technologies-clusters/technologies/nfv

8 http://www.etsi.org/index.php/news-events/news/700-2013-10-etsi-publishes-first-nfv-specifications

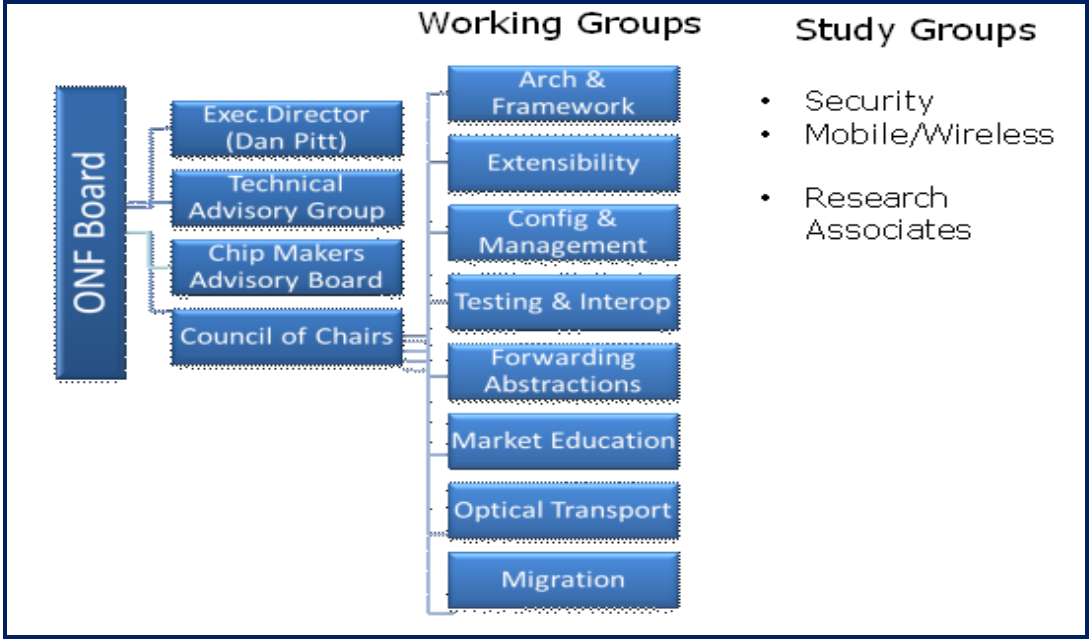
The Open Networking Foundation and OpenFlow

The Open Networking Foundation

The Open Networking Foundation was launched in 2011 and its vision is to make OpenFlow-based SDN the new norm for networks. To help achieve that vision, the ONF has taken on the responsibility of driving the standardization of the OpenFlow protocol. Unlike most IT standards groups or industry consortiums, the ONF was not by founded by suppliers of the underlying technologies, but by Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo! As such, the ONF is one of the very few IT standards groups or industry consortiums that was launched by potential users of the technologies on which the consortium focused.

Figure 3 shows the ONF organizational model. More information on the ONF working and study groups as well as the activities that the ONF is sponsoring can be found at the ONF web site[9].

Figure 3: The ONF Organizational Model



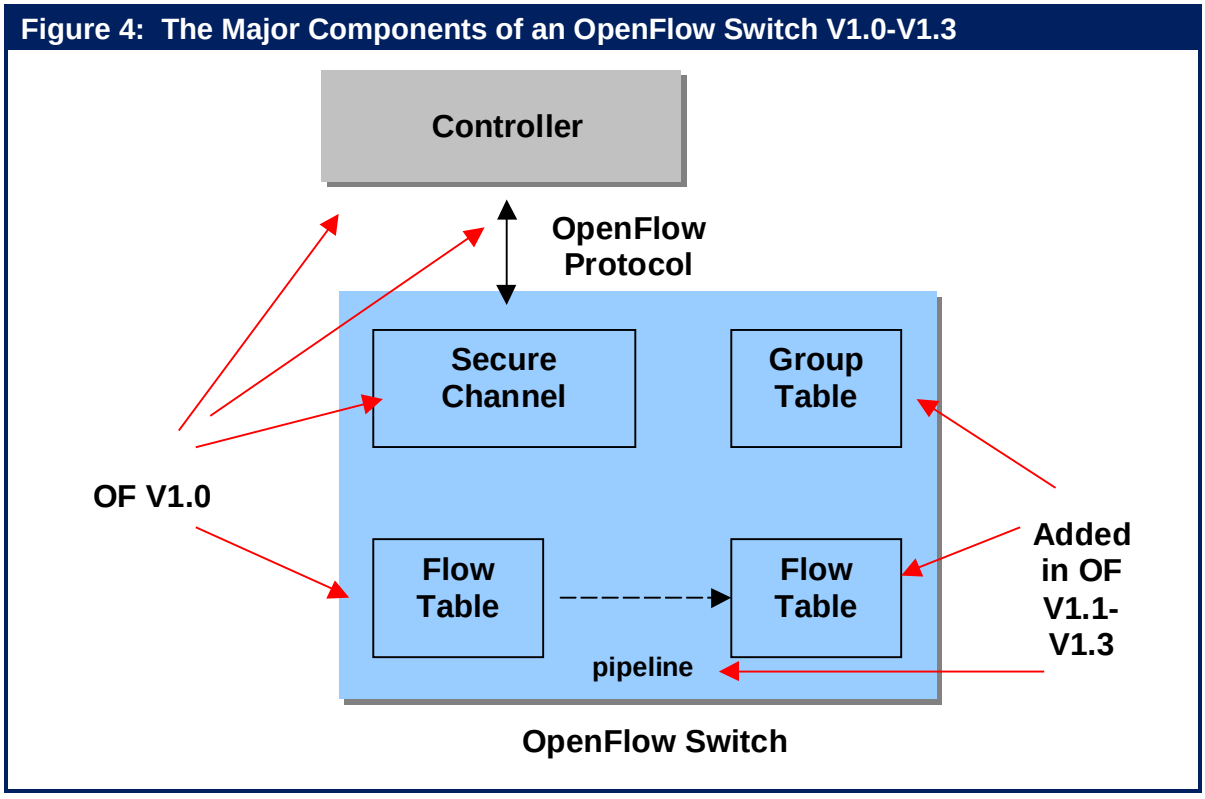
The OpenFlow Protocol

Referring back to **Figure 1** (ONF's SDN Architecture), OpenFlow is a standards-based protocol that enables an SDN controller to program the behavior of an OpenFlow-enabled switch. OpenFlow V1.0 was developed by Stanford University and was published in December 2009. The basic elements of an OpenFlow V1.0 network are shown on the left hand side of **Figure 4**. The central controller communicates with the switch's OpenFlow agent over a secure TLS (Transport Layer Security) channel. This channel could be either in-band or out-of-band. The OpenFlow agent on the switch populates the flow table as directed by the controller. Note that within **Figure 4**, OpenFlow is referred to as OF.

[9] https://www.opennetworking.org/

Subsequent to the publication of OpenFlow V1.0, the development of OpenFlow became the responsibility of the ONF. This OpenFlow specification has been enhanced three times. Version 1.1 was published in February 2011; V1.2 was published in December of 2011 and V1.3 was published in June of 2012. While few vendors adopted v1.1 or v1.2 of OpenFlow, many vendors have either already adopted v1.3 or have indicated that they will. In addition, V1.4 of OpenFlow is currently awaiting ratification.

Figure 4: The Major Components of an OpenFlow Switch V1.0-V1.3



Throughout most of 2012, SDN and OpenFlow were tightly linked in the trade press as if they were either the same thing, or as if OpenFlow was required in order to implement an SDN. Neither statement is true. OpenFlow is one possible protocol that can be used to implement an SDN. In order to understand how IT organizations currently view OpenFlow, The Survey Respondents were given a set of options and were asked to indicate which option best describes the role that the OpenFlow protocol will play in their company's implementation of SDN. Their possible options and the percentage of the respondents who indicated that option are shown in **Table 5**.

Table 5: Planned Use of OpenFlow

Planned use of OpenFlow	Percentage
Will definitely include OpenFlow	16%
Will likely include OpenFlow	27%
Might include OpenFlow	31%
Will not include OpenFlow	3%
Don't know	24%
Other	1%

The data in **Table 5** indicates that there is strong interest in using the OpenFlow protocol as part of implementing an SDN. The data also shows, however, that there is still a high level of uncertainty and whether or not OpenFlow will be used.

Potential Use Cases and Benefits of OpenFlow

There are a number of possible ways for the control centralization, programmability, and flow forwarding characteristics of OpenFlow to be exploited by innovative users and vendors of network devices and software. This includes the following examples.

Centralized FIB/Traffic Engineering
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. This model can be build using a discovery protocol, such as the Link Layer Discovery Protocol (LLDP). 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. Centralized processing also can take advantage of the virtually unlimited processing power of multi-core processors and cluster computing for calculating routes and processing new flows. As shown in **Table 1**, being able to do end-to-end traffic engineering is one of the top three opportunities that The Survey Respondents associate with SDN.

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%[10]. As shown in **Table 1**, being able to increase resource utilization is the primary opportunity that The Survey Respondents associate with SDN.

Other WAN Optimizations
WAN traffic can be dynamically rerouted to reduce/control latency for VoIP and other latency sensitive applications. Traffic can also be load balanced over parallel paths of differing costs.

QoS Optimization
With OpenFlow V 1.3, per flow meters can be used for rate limiting or to provide real time visibility of application performance allowing the controller to modify forwarding behavior to maximize application performance. For example, the controller can configure an OpenFlow switch to modify the QoS markings to change the priority received over the remainder of the end-to-end path.

OpenFlow-Based Virtual Networking
With OpenFlow V1.3 virtual ports, an OpenFlow switch can be programmed to perform tunnel encapsulation and de-capsulation. Therefore, an OpenFlow switch can be programmed to be a overlay NV VTEP/NVE or gateway, as described in the section on overlay NV. As also described in that section, OpenFlow can provide another type of network virtualization for isolating network traffic based on flows segregation or segmentation. Flows are separated based on a subset of the match fields listed earlier in the section.

[10] https://www.opennetworking.org/images/stories/downloads/sdn-resources/customer-case-studies/cs-googlesdn.pdf

OpenFlow-Based Multi-Pathing
Most networking vendors offer data center fabric solutions featuring some form of Layer 2 multi-pathing to improve the networks capacity to handle "east-west" traffic flow characteristic of server virtualization, converged storage networking, and cluster computing. OpenFlow offers another approach to multi-pathing that does not rely on standards such as TRILL or SPB. As noted earlier, the OpenFlow Controller (OFC) can use LLDP to discover the entire network topology via discovering switches and switch adjacencies. Using this topological model, OFC can compute all the parallel physical paths, including paths that share some network nodes and other paths that are entirely disjoint (and therefore offer higher reliability). OFC can then assign each flow across the network fabric to a specific path and configure the OpenFlow switches' flow tables accordingly. The OFC can then offer shared and disjoint multi-pathing as network services that can be delivered to applications. With appropriate processing power, the OFC can support very large scale networks and high availability via path redundancy and fast convergence following link or node failures.

OpenFlow Security Services and Load Balancer 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, the OpenFlow 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 an OpenFlow controller can match suspicious flows to databases of malware signatures or divert DDoS attacks. Another possible security application of OpenFlow would be in Network Access Control (NAC). Examples of security-oriented services that have already been announced are included in the security sub-section of this document.

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 has developed an OpenFlow-based, load-balancing application called FlowScale. According to the University[11], "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. When fully deployed, the system will span the IU Bloomington and IUPUI networks and have the capability to distribute traffic at rates exceeding 500Gb/s."

Network Taps
With OpenFlow virtual ports, the functionality of a network tap can be programmed into the OpenFlow switch, allowing selected traffic to be monitored without deploying physical taps. Traffic can also be replicated and redirected to any monitoring device in the network. Big Switch networks has announced such a network monitoring application referred to as Big Tap[12].

Service Insertion/Chaining
OpenFlow's ability to dynamically reroute flows allows network services provided by physical or virtual appliances (e.g., firewalls, NATs, load balancers, and WOCs) to be inserted in the path of the flow.

[11] http://incntre.iu.edu/research/flowscale
[12] http://www.bigswitch.com/blog/2013/07/26/network-monitoring-with-big-tap-your-first-sdn-application

Redirecting the flow to the next service can be based on encapsulation or rewrite of the destination MAC address.

Circuit Provisioning

With extensions in V1.3 and V1.4, OpenFlow can support circuit-switched paradigms, including CWDM, DWDM, and MPLS with specific path selection and requested levels of CBR and priority. Circuits can be provisioned on a dynamic, scheduled, or permanent basis. Recovery from failed circuits can be via predetermined backup paths or by dynamic path selection. Circuit provisioning can take into account performance metrics, port states, and endpoint utilization.

The OpenDaylight Consortium

The OpenDaylight Consortium[13] 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 shown in **Figure 5** the consortium currently has eight platinum members, two gold members and seventeen silver members. Platinum members pay an annual fee of $500K and provide at least ten developers for a period of two years. While the commitment of the gold members and silver members is less, with the current membership the Open Daylight consortium has significant resources including annual revenues of roughly five million dollars and the full time equivalent of over eighty developers.

Figure 5: Members of the OpenDaylight Consortium

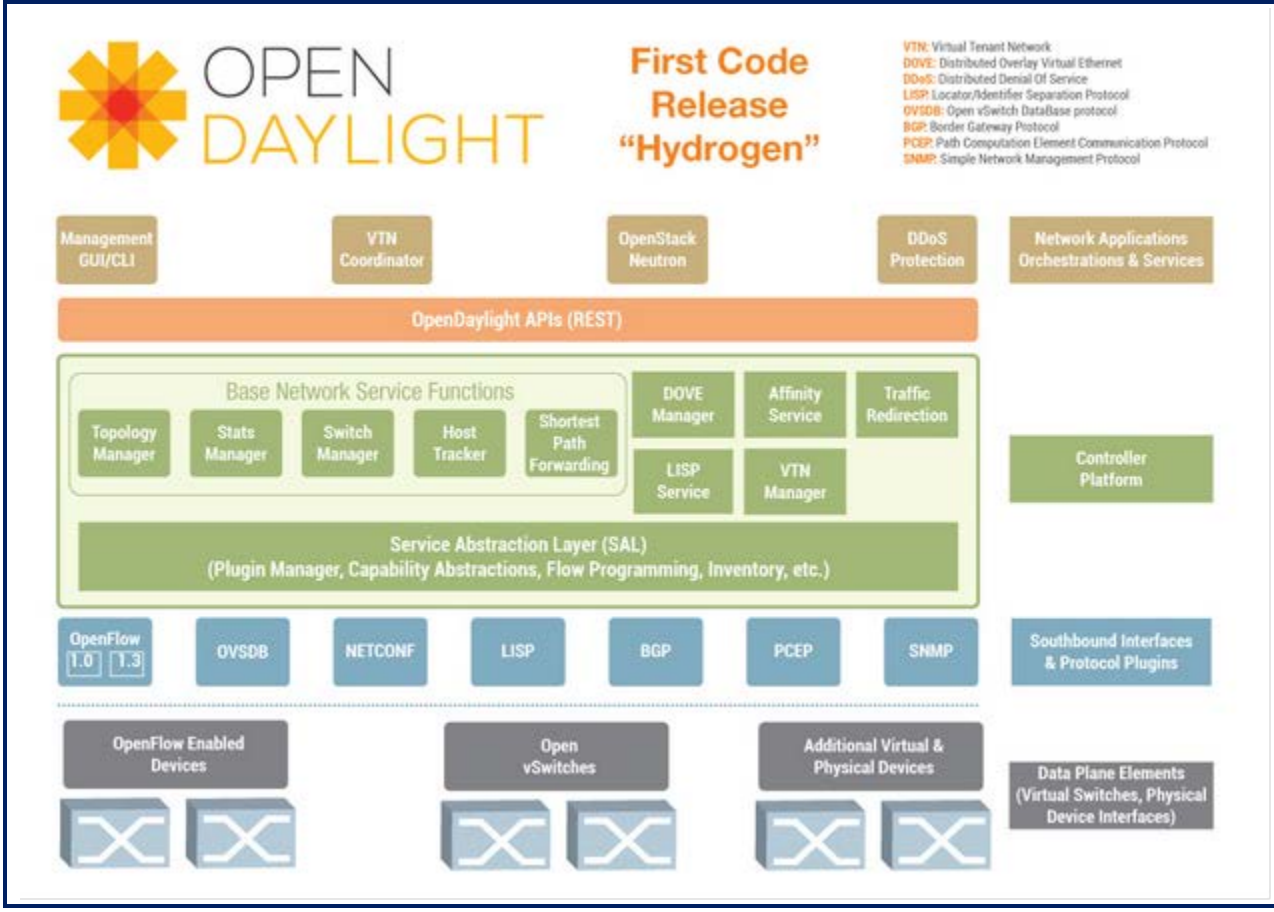
The approach that the consortium is taking to the base architecture for the OpenDaylight controller is to combine two code bases that were brought together through a collaborative proposal by Colin Dixon of IBM and David Erickson of Stanford. In addition, while the expectation is that the platinum members will make significant contributions of intellectual property, anybody can contribute code and a lot of code that has already been contributed. For example, Radware has contributed code that can be used for the detection and mitigation of Distributed Denial of Service (DDoS) attacks and IBM has contributed a version of its established network virtualization technology, called Distributed Overlay Virtual Ethernet (DOVE). Plexxi contributed code that allows both the Open Daylight controller and higher-level applications to create and share an abstract, topology and implementation independent description of the infrastructure needs, preferences and behaviors of workloads. NEC has contributed software that enables network virtualization.

The OpenDaylight Consortium has announced its intention for the first release of code. That code release is called *Hydrogen* and is expected to occur in December 2014. **Figure 6** depicts the

[13] http://www.opendaylight.org/

OpenDaylight SDN Architecture and indicates some of the functionality that will be included in the first code release.

Figure 6: OpenDaylight SDN Architecture



Some vendors, such as Cisco, have announced that they will use the code produced by the OpenDaylight Consortium as the basis for their SDN controller. Other vendors are taking a wait and see attitude.

Security

SDN poses both security challenges and security opportunities. The primary security challenge is to ensure that an attacker cannot compromise the central controller and hence have access to all of the subtending network elements. In addition to securing the controller itself, all communication between the controller and other devices including switches, network services platforms and management systems must be secured.

A preceding sub-section of this document contained a set of 7 questions that IT organizations should ask SDN vendors relative to their overall SDN solution architecture. Below is a set of 5 questions that IT organizations should ask SDN vendors relative to the security of their proposed SDN solutions.

1. For the controller, describe the measures that have been taken to harden its operating system and to ensure availability of the controller function.

2. Describe the authentication and authorization procedures that govern operator access to the controller. What additional physical and logical security measures are recommended?

3. Describe how communications between the controller and other devices is secured by authentication and encryption (e.g., SSL/TLS).

4. What measures are available to deal with possible control flow saturation (controller DDOS) attacks?

5. What tests have been run to verify the effectiveness of the security measures that have been taken? Is it possible to see those test results?

As noted, in addition to creating security challenges, SDN also presents opportunities to improve security by implementing security related applications that leverage the control information that has been centralized in the SDN controller. One example of such an application is DefenseFlow that was recently announced by Radware[14]. Relative to the terminology of **Figure 1**, DefenseFlow is a network service that provides DDoS protection. Another such example is HP's Sentinel application[15] that was designed to combat the security challenges that are associated with BYOD by leveraging the HP TippingPoint Repudiation Digital Vaccine data base.

To quantify the concern that IT organization have relative to security, The Survey Respondents were given the following question. "Some in the industry suggest that the implementation of SDN will make organizations less secure because if the SDN controller is hacked, the hacker has access to all of the subtending switches. Others argue that new security-oriented applications will be developed that take advantage of the SDN controller and make organizations more secure. What is the overall impact that you believe that SDN will have on network security? (Choose only one.)" Their responses are shown in **Table 6**.

[14] http://www.radware.com/Products/DefenseFlow/
[15] http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA4-7496ENW.pdf

Table 6: Perceived Impact of SDN on Security	
Impact	**Percentage**
Networks will be much more secure	7%
Networks will be somewhat more secure	31%
It will have no impact on network security	20%
Networks will be somewhat less secure	20%
Networks will be much less secure	3%
Don't know	19%

One observation that can be drawn from the data in **Table 6** is that overall The Survey Respondents believe that SDN will have a positive impact on security.

Management

As is the case with security, SDN presents both management opportunities and management challenges. One of the primary opportunities was highlighted in **Table 3**. That table showed the characteristic of SDN that The Survey Respondents stated would provide the most value to their company's network was the centralization of configuration and policy management. In addition, as previously described, new network management applications, such as network taps, that leverage SDN functionality are now coming to market.

SDN does, however, create some new management challenges. For example, one of the primary benefits of both the overlay NV solutions that were described in the preceding chapter of The Guide and the SDN solutions that were described in this chapter of The Guide is the ability to support multiple virtual isolated networks that run on top of the physical network. Effective operations management requires tools that give operators clear visibility into the relationships between the virtual and physical networks and their component devices. In particular, when performance or availability problems occur, both root cause analysis and impact analysis require bilateral mapping between the physical and virtual infrastructures.

With SDN, the flows between a pair of VMs can be distributed among a number of alternate paths through the network. Mapping a flow to the physical path it takes can be a challenge unless the flow monitoring solution can involve the controller's end-to-end view of the network

With SDN solutions, 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. With overlay NV solutions, the controller, even if one is present, is not in the data path and does not represent a potential bottleneck. However, the overlay forwarding table must be updated frequently as VMs are created or moved

As was previously mentioned, one of the characteristics of NV and SDN is that network functions such as load balancing and firewalls are increasingly implemented in software as network services that can integrated with virtual networks or SDN flows under programmatic control; a.k.a., service chaining. Implementing these functions in software both increases the delay associated with performing these functions and it also increases the variability of that delay. The result is an increased need for insight into the performance of each component of the overall SDN solution.

Preceding sub-sections of this document contained questions that IT organizations should ask SDN vendors relative to their overall SDN solution architecture as well as questions that IT organizations should ask SDN vendors relative to the security of their proposed SDN solutions. Below is a set of 5 questions that IT organizations should ask SDN vendors relative to SDN management.

1. Describe the extent of your management solution. For example, does it manage just the SDN solution you provide? Does the same tool also manage any traditional network components that you also provide? To what degree will it manage networks (SDN or traditional) that are provided by other vendors?

2. Describe the ability of your solution to monitor the SDN controller. Include in that description your ability to monitor functionality such as CPU utilization as well as flow throughput and latency. Also describe the statistics you collect on ports, queues, groups and meters; and the

error types, codes and descriptors you report on. Also, does your solution monitor the number of flow set-ups being performed by the SDN controller?

3. How does your SDN management solution learn the end-to-end physical topology of the network? Is it possible for service assurance solutions, such root cause analysis to access this topology? Can virtual networks that have been defined be mapped to the underlying physical network elements for root cause analysis and performance analysis?

4. Describe how your SDN management solution can monitor the messages that go between the SDN controller and the SDN switches.

5. Describe the visualization functionality that your solution provides for a hybrid SDN network that is comprised of both physical network elements and virtual network elements.

The Survey Respondents were asked to indicate how much of an impact they thought that SDN will have on network management. Their responses are shown in **Table 7**.

Table 7: Perceived Impact of SDN on Management

Impact	Percentage
Networks will be much easier to manage	30%
Networks will be somewhat easier to manage	52%
SDN will have no impact on management	3%
Networks will be somewhat more difficult to manage	7%
Networks will be much more difficult to manage	4%
Don't know	4%

One observation that can be drawn from the data in **Table 7** is that the vast majority of The Survey Respondents believe that SDN will have a positive impact on management.

Appendix

The data path of an OpenFlow V1.0 switch is comprised of a single Flow Table that includes the rules for matching flows to table entries, an action associated with each flow entry, and counters recording the number of packets and bytes received per flow and other port and table statistics, as shown in **Figure 7.**

Figure 7: The OpenFlow V1.0 Flow Table Fields		
Header Fields	**Counters**	**Actions**

Figure 8 shows the 12-tuple of header fields that are used to match flows in the flow table,

Figure 8: The OpenFlow V1.0 Header Fields											
Ingress Port	Ether Source	Ether Dest	Ether Type	VLAN ID	VLAN Prior	IP Source	IP Dest	IP Proto	IP TOS	Source Port	Dest Port

OpenFlow V1.0 switches are required to support two basic types of actions: Forward and Drop. Forwarding is either directed to a physical port or to one of the following virtual ports:

- ALL: Send the packet out all interfaces, not including the incoming interface.
- CONTROLLER: Encapsulate and send the packet to the controller.
- LOCAL: Send the packet to the switch's local networking stack.
- TABLE: Perform actions in the flow table. Applies for only packet-out messages.
- IN PORT: Send the packet out the input port.

For OpenFlow V1.0 there are also a number of optional/recommended actions:

- NORMAL: Process the packet using the traditional forwarding path supported by the switch (for OpenFlow-hybrid switches)
- FLOOD: Flood the packet along the spanning tree
- ENQUEUE: Forward a packet through a specific port queue to provide QoS
- MODIFY FIELD: Change the content of header fields, including set VLAN ID and priority, strip VLAN, modify Ethernet or IPV4 source and destination addresses, modify IPV4 TOS, modify transport souce and destination ports

When a packet arrives at the OpenFlow V1.0 switch, the header fields are compared to flow table entries. If a match is found, the packet is either forwarded to specified port(s) or dropped depending on the action stored in the flow table. When an OpenFlow Switch receives a packet that does not match the flow table entries, it encapsulates the packet and sends it to the controller. The controller then decides how the packet should be handled and notifies the switch to either drop the packet or make a new entry in the flow table to support the new flow.

Over the last year and a half extensive enhancements have been made to the OpenFlow specification under of the auspices of the ONF. A complete listing of the enhancements included in OpenFlow V1.1-V1.3 is well beyond the scope of this document. However, some of the major changes include:

- Additional components of a flow entry in the flow table as shown below. In addition to the match and counter fields, the following fields are included in the entry:
  - Instructions to execute actions or to modify the action set or pipeline processing
  - Priority: matching precedence of the flow entry

- Timeouts: maximum amount of time or idle time before flow expiration
- Cookie: opaque data value chosen and used by the controller to process flows

Match Fields	Counters	Instructions/Actions	Priority

- Flexible pipeline processing through multiple flow tables, as shown in the right hand side of **Figure 4**. As a packet is processed through the pipeline, it is associated with a set of accumulating actions and metadata. The action set is resolved and applied at the end of the pipeline. The metadata allows a limited amount of state to be passed down the pipeline.

- The new group table abstraction and group action enable OpenFlow to represent a set of ports as a single entity for forwarding packets. Different types of groups are provided, to represent different forwarding abstractions, such as multicasting or multi-pathing.

- Support for virtual ports, which can represent complex forwarding abstractions such as Link Aggregation Groups (LAGs) or tunnels. Encapsulation/Decapsulation of packets supports Network Virtualization tunnels, including PBB, QinQ VLAN stacking, and Push/Pop/Rewrite of MPLS headers.

- OpenFlow Extensible Match (OXM) uses a TLV (Type Link Value) structure to give a unique type to each header field increasing the flexibility of the match process.

- Basic support for IPv6 match and header rewrite has been added, via OXM.

- Routing emulation (Time to Live (TTL) decrement)

- Per flow meters which can be used to measure and control the rate of packet forwarding—including rate limiting packets sent to controller

- Support for multiple controllers to improve reliability

With V 1.4, OpenFlow will provide enhanced extensibility of the OpenFlow wire protocol and a new set of port properties to provide support for optical ports. This will allow Ethernet optical ports or optical ports on circuit switches to be configured and monitored.

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.

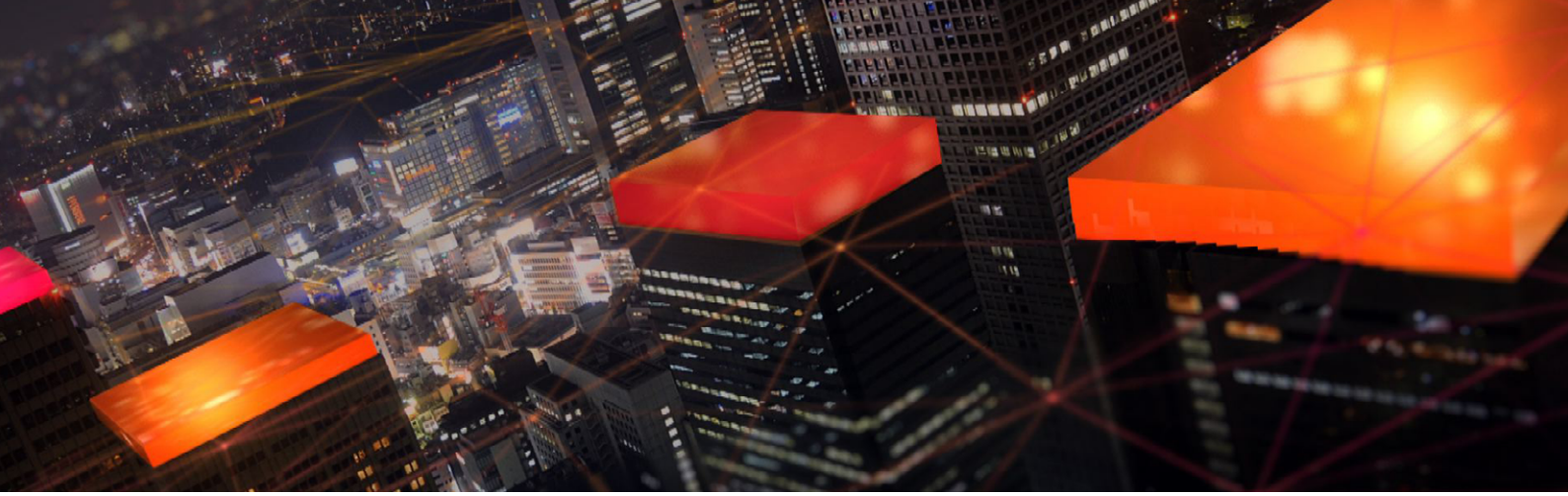
Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting 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 at *jim@webtorials.com* or Steven Taylor at *taylor@webtorials.com*.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.



The Consumable Datacenter Network

Taking cloud computing to the next level

The move to cloud computing and storage has changed the way Enterprise users access and consume data. Unfortunately, today's data communications networks aren't keeping pace with this dynamic business environment, and they're struggling to deliver consistent, on-demand connectivity.

That's where we come in. Nuage Networks™ closes the gap between the network and the cloud-based consumption model, creating an infrastructure in which network resources are as readily consumable as compute and storage resources. Our approach enables enterprises to transform the way they build and use their networks, which has a profound effect inside and across multiple datacenters. The transformation is also felt at the critical remote working environment, through a seamless connection to the Enterprise's Wide Area Network.

WOULDN'T IT BE NICE IF...

- Datacenter infrastructures were so simple and standards-based that you could break the vendor lock and work with whichever suppliers offered you the best solutions for your business?
- The network could expand and evolve transparently with the needs of applications, bypassing the datacenter's arbitrary boundaries?
- The datacenter network team could set up controlled, secure templates that application teams could use to deploy applications on the network for and by themselves — without manual transactions or unnecessary project overhead?

Before the move to the cloud, enterprises had to purchase large compute systems to meet the peak processing needs of a limited set of specific events, such as financial milestones (month end or year end), or annual retail events (holiday shopping). Outside of the specific events, the systems were underutilized. This approach was therefore expensive, both in terms of CAPEX and OPEX, requiring significant outlay for power, space and air-conditioning.

Cloud-based datacenters have unshackled the IT environment, making it possible for applications to request additional compute and storage on an as-needed basis. Peak demands can be provisioned "just in time", which lowers operational costs and provides the ability to share compute resources across applications.

The term "cloud" means many things to many people. We focus on two key benefits that cloud computing delivers to Enterprises:

Abstraction of the application from the infrastructure. Cloud computing separates the application from the physical compute and storage infrastructure. This allows workloads to be consistently configured remotely, and templated for mass deployment. End users don't need to worry about the location and specifications of individual hosts. Virtualization and cloud management tools abstract those details to make the infrastructure more readily consumable.

Customer self-fulfillment. Cloud Management Systems (CMS) like Alcatel-Lucent CloudBand™ and the abstraction layer enabled by server virtualization allow IT departments to minimize the tedious and cumbersome processing of application-to-network transactions. For example, IT can provision end customer access policies in the CMS to govern who is authorized to create virtual machine instances, in which location, how many are allowed, and who is the funding department. Users and work groups get instant application deployment, which in turn, makes the business more agile and responsive — critical

attributes in today's enterprise environment. At the same time, operational expenses associated with the handling of work orders is greatly reduced.

As a result of these innovations, Enterprises enjoy a powerful new IT environment in which applications can consume compute resources easily. However as the dynamic nature of cloud computing becomes mainstream, the underlying datacenter network is struggling to match the flexibility of the applications. In fact, most often the network is the weak link, inhibiting the enterprise's ability to profit from the benefits that moving to the cloud should provide.

While virtual compute resources can be instantiated in seconds, it often takes days for network connectivity to be configured and established. Furthermore, the static configurations used by today's networks do not provide the efficiencies and flexibility needed to drive maximum server utilization and application availability.

Consuming the Network

Nuage Networks ensures your network elements are as efficient and flexible as your cloud computing. The result is a choreographed datacenter environment where the compute resources and network work seamlessly.

Imagine the possibilities when network resources are easily consumable. A Nuage Networks datacenter network is as dynamic, automated and virtualized as the server infrastructure, and supports the needs of applications with instantaneous network connectivity.

Nuage Networks eliminates the constraints that have been limiting the datacenter network as it scales out to meet growing demand. With Nuage Networks, you can:

- Define the network service design per application
- Optimize your workload placement across datacenter zones or even across geo-diverse datacenters
- Maximize efficiency of your compute and storage resources

Nuage Networks paves the way for datacenters of the future to be the heartbeat of a powerful cloud infrastructure. Enterprises and user groups could conceive and consume their own secure slices of a robust multi-tenant infrastructure, with appropriate operational visibility and control.

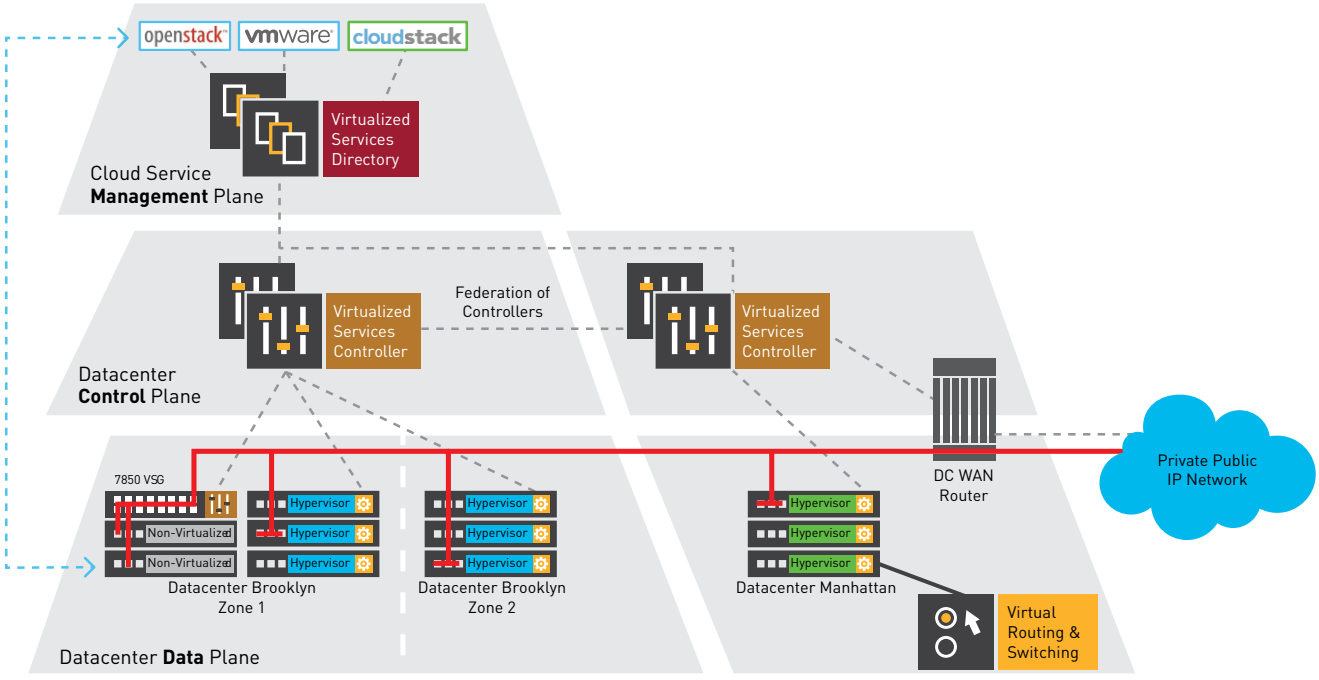
Nuage Networks Virtualized Services Platform

Nuage Networks Virtualized Services Platform (VSP) is the first network virtualization platform that addresses modern datacenter requirements for multi-tenancy, full-featured routing and security at scale. It also integrates seamlessly with wide area business VPN services. It is a software solution that transforms the physical network into a simple to manage, rack-once and wire-once, vendor-independent IP backplane. As a result, network resources within and across datacenters can be treated as an elastic resource pool of capacity that can be consumed and repurposed on demand. Nuage Networks enables unconstrained datacenter networks for the cloud era.

Nuage Networks delivers virtualization and automation of business networks through the three key elements in the Nuage Networks VSP:

Virtualized Services Directory (VSD). Configuration of networks is complex. To eliminate unnecessary complexity while leaving full control and visibility of applications with the IT administrator, the VSD abstracts networking constructs down to their base primitives in four categories: Connectivity Domains, Security, Quality of Service, and Analytics. This allows the requirements for network services to be expressed simply,

FIGURE 1. Nuage Networks Virtualized Services Platform



consistently, and in a repeatable manner. The critical need for mobility is also addressed, ensuring network services adjust gracefully and instantly as application endpoints and workloads move from virtual machines within or across datacenters.

The VSD also provides a rich permission-based multi-tenant interface to enable end user provisioning by application owners. Through its role-based hierarchy of permissions, the VSD eliminates operational delays and minimizes transactions between organizations while providing visibility and control of the network "slices" that each group is given in support of their application requirements.

Virtualized Services Controller (VSC). The VSC is an advanced SDN controller that manages the provisioning of virtual network services by programming the edges of the network using OpenFlow™. The VSC ensures that the network follows the application instantaneously. Parting with cumbersome and error-prone device-by-device manual provisioning, Nuage Networks introduces an event-triggered and pull-based configuration model. Once application events such as moves, adds or changes are detected, appropriate policy-based configurations are instantaneously applied. Leveraging Alcatel-Lucent's proven Service Router Operating System, which has been deployed in over 400 service provider networks worldwide for over a decade, the VSC runs a full and robust IP routing stack that allows it to communicate and seamlessly integrate into existing networks.

Virtual Routing and Switching (VRS) is a true hypervisor for the network. The first of its kind in the industry, the VRS fully virtualizes network offerings ranging from distributed virtual Layer 2, Layer 3 forwarding and Layer 4 security. These virtual network services leverage the existing network infrastructure and are offered in a standards-based manner compliant with IETF NVO3. Operators can use whatever servers, hypervisors, and cloud management systems they choose; the Nuage Networks solution abstracts and automates the cloud-networking infrastructure.

In many real-world installations, datacenter environments are a mix of virtualized and non-virtualized assets. To help all datacenters benefit from automation and network virtualization, Nuage Networks supports the full range of options. Software gateways such as the Nuage VRS-G are ideal for environments with relatively low density of bare metal servers and appliances, just as hardware VTEPs from our ecosystem partners provide a viable alternative for certain use cases and environments. For environments with significant investment in bare metal servers and appliances, a new breed of high performance gateway is needed.

The **Nuage Networks 7850 Virtualized Services Gateway (VSG)** is a high-performance gateway that extends Nuage Networks SDN 2.0 functionality seamlessly between virtualized and non-virtualized assets in the datacenter. Working in concert with the Nuage Networks VSP, policies devised for applications automatically extend across virtualized and non-virtualized assets for a fully automated network infrastructure.

FIGURE 2. Nuage Networks datacenter network benefits

	Status Quo	NUAGE NETWORKS DELIVERS What is Needed
Virtualization of network services	LAYER 2 VIRTUALIZATION	FULL NETWORK VIRTUALIZATION, L2 THROUGH L4
Breadth of application models	SIMPLE SCENARIOS	HYBRID CLOUD SERVICES, SEAMLESS VPN CONNECTIVITY
Availability & scale	FRAGILE, NOT MULTI-TENANT	ROBUST, THOUSANDS OF TENANTS
Reach & mobility of network resources	ISLANDS, WITHIN RACKS OR CLUSTERS	SEAMLESS VIRTUALIZED FABRIC, THROUGHOUT & ACROSS DATACENTERS
Network service turn-up time	SLOW, MANUAL, CONFIGURATION DRIVEN	INSTANTANEOUS, AUTOMATED POLICY-DRIVEN
Openness	SPECIFIC TO VENDOR IMPLEMENTATIONS	INDEPENDENCE FROM HARDWARE CHOICES
Breadth of assets automated	VIRTUALIZED ASSETS, LIMITED OPTIONS FOR NON-VIRTUALIZED	ALL DATACENTER ASSETS, VIRTUALIZED & NON-VIRTUALIZED

NU•ÂHJ: FROM FRENCH, MEANING "CLOUD"

The cloud can be more than what it is. In fact, it needs to be. When we founded Nuage Networks, it was with the idea that it's time for the cloud to come of age. From the beginning we recognized the unique challenges that cloud service providers and large enterprises face delivering and managing large, multi-tenant clouds. While the virtualization of compute and storage has evolved quickly, the network simply has not kept up. The result is that today your cloud is being held back. And so is your business.

When we started Nuage Networks, it was with the mission that we could empower our customers to finally deliver on the true promise of the cloud. We envision a world in which IT and IP are no longer in conflict, but rather work in concert to propel your business and elevate the cloud for every one of your customers. We see a world where innovation isn't hampered by infrastructure, and network resources are as effortlessly consumable as compute and storage.

To make this vision a reality, Nuage Networks brings a unique combination of groundbreaking technologies and unmatched networking expertise. This enables us to create solutions that do more than provide incremental improvement. It allows us to introduce radically new thinking and pick up where others have left off, delivering a massively scalable SDN solution that makes the datacenter network able to respond instantly to demand and boundary-less.

Visit us on the web

Our mission is to help you harness the full value of the cloud.

nuagenetworks

www.nuagenetworks.net