The 2013 Guide to
Network Virtualization and SDN

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

Sponsored in part by:

AVAYA
The Power of We™

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 was published both in its entirety and in a chapter-by-chapter fashion.

Chapter one of The Guide is focused on NV and it discusses:

- The primary NV use cases;
- Various ways that overlay NV solutions can be implemented and the benefits and limitations of those solutions;
- The drivers and inhibitors of NV adoption;
- The role of orchestration and service chaining;
- A canonical architecture for a controller based NV solution;
- A comparison of current NV solutions;
- How to create NV solutions by manipulating OpenFlow tables.

The second chapter focuses on SDN and it discusses:

- Potential SDN use cases;
- The ONF definition of SDN and the ONF solution architecture;

- Criteria to evaluate SDN solution architectures;
- The drivers and inhibitors of SDN adoption;
- The overlay/underlay model;
- Network function virtualization;
- Potential use cases and benefits of OpenFlow;
- The OpenDaylight consortium;
- The impact of SDN on security and on management.

The third chapter focuses on the NV and SDN ecosystem. The chapter identifies the primary classes of vendors in the ecosystem, their value proposition and also identifies some of the key players in each class of vendor. The classes of vendors discussed in chapter 3 are:

- Merchant silicon/chip vendors;
- Hyperscale data centers;
- Telecom service providers;
- Switch vendors;
- Network management and automation vendors;
- Providers of network services;
- Providers of test equipment or testing services;
- Standards bodies;
- Providers of controllers;
- Providers of Telecom Service Provider’s infrastructure/optical equipment;
- Networking vendors;
- Server virtualization vendors.

Chapter 3 also profiles some of the major players in the NV and SDN ecosystem. Included in each profile is the focus each vendor is taking, a discussion of their value proposition and the identification of some proof points that demonstrate their creditability. The following vendors are profiled in chapter 3:

- Avaya;
- QualiSystems;

- Cisco;
- NEC;
- Nuage Networks;
- HP;
- Ciena;
- A10;
- Pica8;
- Packet Design;
- Netsocket;
- EMC.

Chapter 4 presents some market research that describes the current state of planning for NV and SDN. In addition, the chapter presents an outline that IT organizations can modify to use in their environment to plan for NV and SDN. That outline suggests that IT organizations that are interested in NV and SDN should:

- Create definitions of NV and SDN that are agreed to and well understood within their organization;
- Identify the primary opportunities that the organization is hoping to address and identify the key business metrics associated with each opportunity;
- Evaluate viable solutions;
- Determine how to integrate the solutions into the current environment;
- Educate the organization;
- Evaluate professional services;
- Eliminate organizational resistance;
- Perform a POC;
- Obtain management buy-in.

Chapter 1: The what, why and how of Network Virtualization

Introduction

Over the last couple of years a number of approaches to NV have emerged that are focused on addressing the limitations of the traditional techniques for network virtualization (e.g., 802.1Q VLANs and Virtual Routing and Forwarding (VRFs)). All of these approaches are based on creating a number of virtual Layer 2 or Layer 3 networks that are supported by a common physical infrastructure. The basic idea is to virtualize the network in a manner analogous to compute server virtualization. As a result of these developments, network designers will have the opportunity to choose among the following NV alternatives.

1. Traditional NV
2. Overlay Network Virtualization via Tunneling
3. Software Defined NV via Flow Table Segmentation
4. A combination of the above alternatives

The Survey Respondents were asked to indicate how their organization defines network virtualization and multiple answers were allowed. The survey question focused on the emerging forms of network virtualization – bullets 2 and 3 in the preceding list. As indicated in **Table 1**, some of the emerging forms of network virtualization are based on a device referred to as a controller. As is described below, one of the key roles of a controller is to serve as a central repository of address mappings.

The responses to this question are shown in **Table 1**.

Table 1: Characterization of NV Solutions

Definition of Network Virtualization	Percentage of Respondents
It is based on overlays using protocols such as VXLAN, NVGRE or STT but it does not involve a controller	21.0%
It is based on overlays and a controller. It may or may not use protocols such as VXLAN, NVGRE or STT	39.1%
It is part of a software defined network and may be based on segregating traffic flows	36.2%
Don’t know	17.7%
Other	4.5%

The data in **Table 1** indicates that of the emerging forms of network virtualization, the controller-based approaches to NV are by a wide margin the most popular.

VXLAN, NVGRE and STT are all draft IETF standards. To understand the role that standards play in the selection of NV solutions, The Survey Respondents were asked how important it was to their organization that NV solutions are based on open standards. Their responses are shown in **Table 2**.

Table 2: Importance of Open Standards

Level of Importance	Percentage of Respondents
Extremely important	16.0%
Very important	32.1%
Moderately important	24.7%
Somewhat important	14.4%
Not important	7.4%
Don’t know	5.3%

The data in Table 2 indicates that NV solutions that are built on open standards are either very or extremely important to roughly half of The Survey Respondents.

Traditional NV & The NV Use Case

One-to-many virtualization of network entities is not a new concept. The most common traditional applications of the virtualization concept to networks are VRF instances and VLANs.

VRF is a form of Layer 3 network virtualization in which a physical router supports multiple virtual router (VR) instances, each running its own routing protocol instance and maintaining its own forwarding table. Unlike VLANs, VRF does not use a tag in the packet header to designate the specific VRF to which a packet belongs. The appropriate VRF is derived at each hop based on the incoming interface and information in the frame. An additional requirement is that each intermediate router on the end-to-end path traversed by a packet needs to be configured with a VRF instance that can forward that packet.

VLANs partition the standard Ethernet network into as many as 4,096 broadcast domains as designated by a 12 bit VLAN ID tag in the Ethernet header. VLANs have been a convenient means of isolating different types of traffic that share a common switched LAN infrastructure. In data centers making extensive use of server virtualization, the limited number of available VLAN IDs can present problems, especially in cases where a large number of tenants need to be supported, each of whom requires multiple VLANs. In contrast to this limitation of VLANs, part of the use case for the NV approaches that are described in The Guide is that these approaches enable IT organizations to establish virtual Ethernet networks without being constrained to only having 4,096 VLAN IDs.

Server virtualization is another factor that is driving the adoption of the approaches to NV that are described in this sub-section of The Guide. Due to server virtualization, virtual machines (VMs) can be dynamically created and moved, both within a data center and between data centers. Extending VLANs across a data center via 802.1Q trunks to support VM mobility adds operational cost and complexity due to the fact that each switch in end-to-end path has to be manually reconfigured. In data centers based on Layer 2 server-to-server connectivity, large numbers of VMs, each with its own MAC address, can also place a burden on the forwarding tables capacities of Layer 2 switches. A major component of the value proposition for the NV approaches that are described in The Guide is that they support the dynamic movement, replication and allocation of virtual resources without manual intervention. Another component of the value proposition for these approaches is that they avoid the issue of needing more MAC addresses than data center LAN switches can typically support.

The value proposition of network overlay solutions is expanded upon in the following sub-section. As is also described below, one characteristic of NV solutions that IT organizations need to understand is whether the solution enables the dynamic movement of virtual resources within a data center; between data centers; or between a data center and a branch or campus facility. A related characteristic that IT organizations need to understand is whether the solution leverages standards based protocols to federate with other NV solutions.

Network Overlays via Tunneling: Benefits & Limitations

A number of approaches to network virtualization leverage tunneling and encapsulation techniques to construct multiple virtual network topologies overlaid on a common physical network. A virtual network (VN) can be a Layer 2 network or a Layer 3 network, while the physical network can be Layer 2, Layer 3 or a combination depending on the overlay technology. With overlays, the outer (encapsulating) header includes a field (generally up to 24 bits wide) that carries a virtual network instance ID (VNID) that specifies the virtual network designated to forward the packet.

Virtual network overlays can provide a wide range of benefits, including:

- Virtualization is performed at the network edge, while the remainder of the L2/L3 network remains unchanged and doesn't need any configuration change in order to support the virtualization of the network. The most common approach is to perform the encapsulation at the hypervisor vSwitch, which acts as the virtual tunnel endpoint (VTEP) or network virtualization edge (NVE). As a result, overlay NV solutions can generally be implemented over existing networks as either an enhancement to the conventional distributed network architecture, or as a step toward an SDN architecture.

- Support for essentially unlimited numbers of VNs as the 24 bits that are typically used by network overlays to identify VNs can identify slightly more than 16 million VN IDs. While theoretically NV solutions can support 16 million VNs, practical limits are often in the range of 16,000 to 32,000 VNs.

- Decoupling of the virtual network topology from the physical network Infrastructure and decoupling of the "virtual" MAC and/or IP addresses used by VMs from the infrastructure IP addresses used by the physical data center core network. The decoupling avoids issues such as limited MAC table size in physical switches.

- Support for VM mobility independent of the physical network. If a VM changes location, even to a new subnet in the physical network, the switches at the edge of the overlay simply update mapping tables to reflect the new physical location of the VM. The network for a new VM can be be provisioned entirely at the edge of the network.

- Ability to manage overlapping IP addresses between multiple tenants.

- Support for multi-path forwarding within virtual networks.

- Ease of provisioning virtual appliances in the data path. Network services resident on VMs can be chained together (a.k.a., service chaining) with point-and-click simplicity under the control of NV software.

- For controller-based NV solutions, the controller is not in the data path, and so it does not present a potential bottleneck.

The Survey Respondents were given a set of 15 possible challenges and opportunities and were asked to indicate which challenges and opportunities they thought that NV solutions could help them to respond to. The Survey Respondents were allowed to indicate multiple challenges and opportunities. The top 5 challenges and opportunities are shown in **Table 3.**

Table 3: Use Cases for NV Solutions

Challenge/Opportunity	Percentage of Respondents
Better utilize network resources	44.0%
Support the dynamic movement, replication and allocation of virtual resources	39.1%
Establish virtual Ethernet networks without the limit and configuration burden of VLANs	32.5%
More easily scale network functionality	31.7%
Reduce OPEX	30.5%

Given the similarity of the second and third entries in **Table 3**, it follows that the primary value that IT organizations see in NV solutions is the ability to dynamically implement virtual Ethernet networks that can support the dynamic movement, replication and allocation of virtual resources.

Some of the limitations of overlay NV solutions include:

- 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.

- Gateways between the virtual network and systems and network service points on the physical network may need to pass high volumes of traffic. If a software gateway running on a VM or a dedicated appliance has insufficient processing power, hardware support for the gateway functionality may be required in physical switches or network service appliances. Some of the more recent merchant silicon switching chips support gateway functionality for VXLAN which is the most popular encapsulation protocol.

- 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.

NV solutions also create some management challenges. For example, one of the primary benefits of overlay solutions is the ability to support multiple VNs running on top of the physical network. Effective operations management requires that IT organizations have tools that give them clear visibility into the relationships between virtual and physical networks and their component devices. When performance or availability problems occur, both root cause analysis and impact analysis require bilateral mapping between the physical and virtual infrastructures.

Both increasing and complicating the need for the visibility described in the preceding paragraph is the ability of NV solutions to do service chaining. The phrase *service chaining* refers to 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. The primary focus of service chaining is on services provided by virtual appliances. Most SDN or NV solutions provide service chaining. For SDN, the controller configures the forwarding plane switches to direct the flows along the desired paths, For NV, the controller adjust the FIBs of the vSwitches/vRouters to force the traffic through the right sequence of VMs. Network Function Virtualization, discussed in the next section of The Guide, is basically service chaining that focuses on network services/functions provided by virtual appliances, but isn't necessarily dependent on SDN or NV.

The bottom line is that IT organizations need visibility not just into the overlay NV solution but into the complete solution and all of its components; e.g., firewalls, load balancers.

The Survey Respondents were given a set of 12 inhibitors to the adoption of NV and were asked to indicate the two biggest inhibitors to their company adopting NV sometime in the next two years. The top 5 inhibitors are shown in **Table 4**.

Table 4: Inhibitors to the Adoption of NV Solutions

Inhibitor	% of Respondents
The immaturity of the current products	29.6%
The lack of resources to evaluate NV	29.2%
Other technology and/or business priorities	28.8%
The immaturity of the enabling technologies	29.6%
The confusion and lack of definition in terms of vendors' strategies	18.1%

One interesting observation that can be drawn from the data in **Table 4** is that IT organizations are not avoiding implementing NV solutions because they don't see value in them. Rather, the key factors inhibiting the adoption of NV solutions are the same factors that typically inhibit the adoption of any new technology or way of implementing technology: Immaturity of products and strategies; confusion; and lack of resources.

The Survey Respondents were asked to indicate the impact they thought that NV would have on security and network management. Their responses are shown in **Table 5** and **Table 6**.

Table 5: Impact of NV on Security

Impact on Security	% of Respondents
Networks will be much more secure	6.2%
Networks will be somewhat more secure	33.7%
NV will have no impact on network security	23.5%
Networks will be somewhat less secure	14.0%
Networks will be much less secure	2.5%
Don't know	20.2%

Table 6: Impact of NV on Management

Impact on Management	% of Respondents
Networks will be much easier to manage	21.8%
Networks will be somewhat easier to manage	52.3%
NV will have no impact on management	4.5%
Networks will be somewhat more difficult to manage	9.9%
Networks will be much more difficult to manage	4.5%
Don't know	7.0%

One conclusion that can be drawn from the data in **Table 5** and **Table 6** is that The Survey Respondents generally think that implementing NV solutions will make their networks more secure and easier to manage. As such, security and ease of management can potentially be looked at as benefits of implementing NV solutions.

Cloud Orchestration

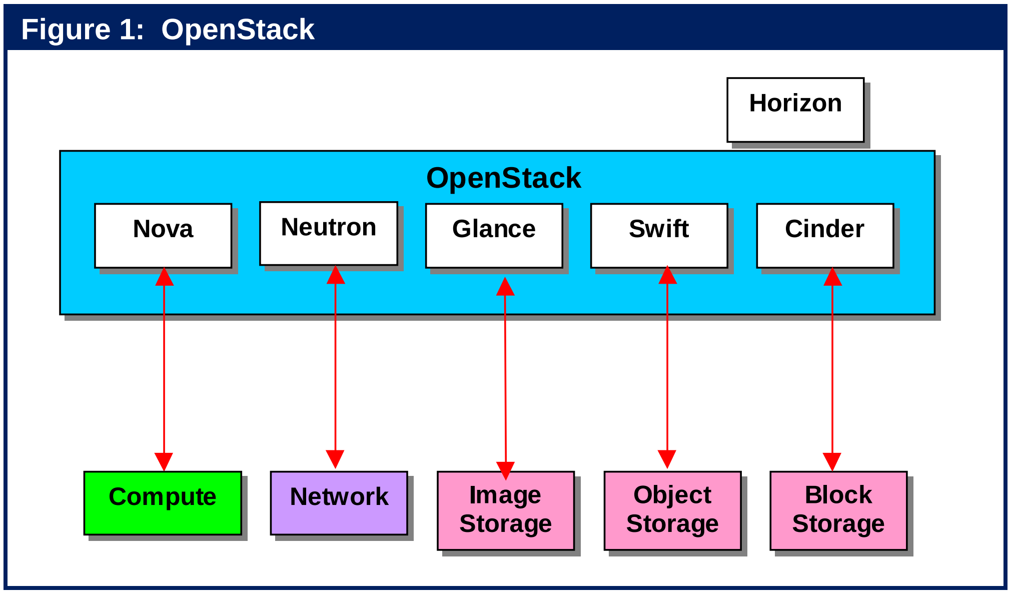
Cloud Orchestration platforms have evolved as a means of automating and facilitating the process of configuring pools of data center resources in order to provide a range of cloud or cloud-like services, such as Infrastructure as a Service (IaaS) solutions. The Orchestrator's role is to manipulate the 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 naturally affinity between Orchestration and software-based network controllers, such as NV controllers or 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 1 shows a block diagram of the OpenStack system, including the OpenStack modules that are used to control resource pools in the data center. Horizon is the OpenStack Dashboard that provides administrators and users a graphical interface to access, provision and automate cloud-based resources.

Figure 1: OpenStack



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 NV and SDN solutions to allow for multi-tenancy and scalability. 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.

In conjunction with the Orchestrator, the role of the SDN or NV 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 Virtual Network
- Attach Network Services to a VM or chain Network Services between VMs

Figure 2: VM Creation Workflow with OpenStack

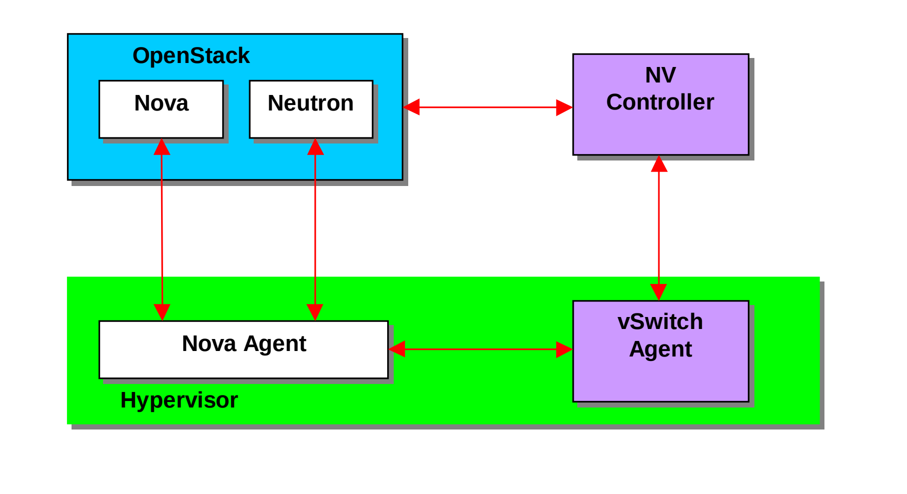


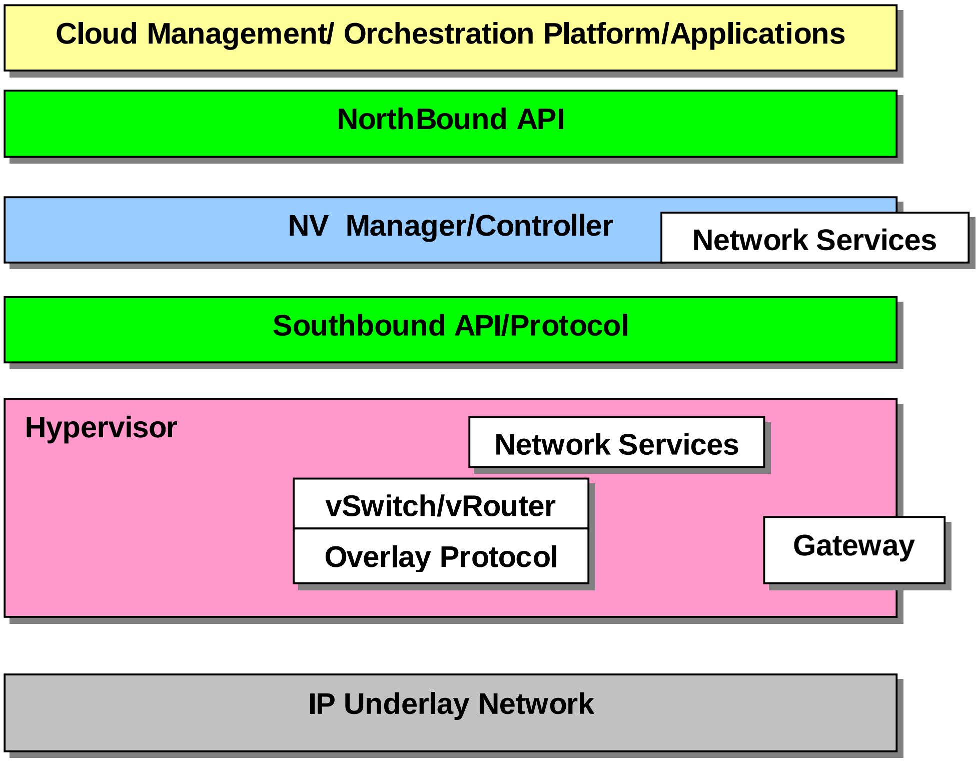
Figure 2 provides a high level depiction of how an orchestrator (OpenStack) and a NV controller might interact to place a VM into service within a VN.

The Nova 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.

Controller Based NV Solution Architecture

A Network Virtualization Solution typically has an architecture similar to the one shown in **Figure 3**. The main components are typically the NV Controller, hypervisor-resident vSwitches/vRouters, and gateways that provide connectivity from virtual networks to traditional network segments; e.g., VLANs, non-virtualized servers, or Internet routers. The controller function is generally supported by a high availability (HA) cluster or another HA configuration. Controller functionality may be comprised of a number of sub-functions running on different servers. Cloud Management/Orchestration is typically obtained from a third party and network services may be integrated with the controller, integrated via virtual appliances, or possibly integrated via physical appliances through the gateway.

Figure 3: Network Virtualization Architecture



Criteria to Evaluate Overlay NV Solutions

One of the primary criterion that IT organizations should use relative to evaluating overlay network virtualization solutions is how well it solves the problem(s) that the IT organization is looking to solve. For example, can the solution enable the IT organization to move workloads between data centers? Between a data center and a branch office?

Other solution level criteria that IT organizations should evaluate include:

- Does the solution federate and hence interoperate with other solutions?
- What interaction, if any, is there between the virtual networks and the physical networks?
- What management functionality is provided into both the virtual and physical networks?
- Does the solution support service chaining?

The main technical differences between the various overlay NV solutions that IT organizations should evaluate fall into the following categories:

- **Encapsulation formats**. Some of the tunneling/encapsulation protocols that provide network virtualization of the data center include VXLAN, NVGRE, STT, and SPB MAC-in-MAC (SPBM). Both the IEEE and the IETF have already standardized SPB. It is unclear as to whether or not all of the other proposals will become standards.

- **Tunnel control plane functionality** that allows ingress (encapsulating) devices to map a frame to the appropriate egress (decapsulating) device. The first-hop overlay device implements a mapping operation that determines where the encapsulated packet should be sent to reach its intended destination VM. Specifically, the mapping function maps the destination address (either L2 or L3) of a packet received from a VM into the corresponding destination address of the egress NVE device. The main differences here are whether a controller is used and the functionality of the controller.

  Some of the initial, controller-less approaches to network virtualization relied on IP multicast as a way to disseminate address mappings. A more common solution is based on a central repository of address mappings housed in a controller. Vendors frequently refer to controller-based overlay NV solutions as SDN, while a more descriptive terminology might be Software Defined Overlay Network Virtualization.

- **vSwitches supported.** A number of vSwitches are based to some degree on the open source Open vSwitch (OVS)[1], while other vSwitches are of proprietary design. Another point of differentiation is whether the vSwitch is a virtual router as well as being an encapsulating Layer 2 switch. With Layer 3 functionality, a vSwitch can forward traffic between VMs on the same hypervisor that are in different subnets and can be used to implement Layer 3 VNs. Where the tunneling vSwitch has full Layer 3 functionality, the majority of intelligence can be implemented at the edge of network, allowing the underlay network to be implemented as a simple Layer 2 fabric.

[1] While based on OVS, many vSwitches have implemented proprietary extensions to OVS.

- **Broadcast/Multicast delivery** within a given virtual network. NVEs need a way to deliver multi-destination packets to other NVEs with destination VMs. There are three different approaches that can be taken:

    - The multicast capabilities of the underlay network can be used
    - The NVEs can replicate the packets and unicast a copy across the underlay network to each NVE currently participating in the VN.
    - The NVE can send the packet to a distribution server which replicates and unicasts the packets on the behalf of the NVEs.

- **Protocols.** Another characteristic of centralized controller solutions is the choice of Southbound protocols/APIs employed between the NV controller and the NVE and the choice of Northbound protocols/APIs used between the NV controller and cloud management systems and hypervisor management systems. If the southbound protocols are standardized, the NVE can potentially communicate with different types of NV controllers or controllers from different vendors. Some the alternatives here include OpenFlow, BGP, and CLI shell scripts.

  If the northbound protocols are standardized, the controller can be integrated with network services from ISVs or different types of third party orchestration systems. Most overlay NV controllers support a RESTful Web API for integration with cloud management and orchestration systems. With both southbound and northbound APIs the most important question becomes which third party switches, applications, virtual appliances, and orchestration systems have been certified and are supported by the overlay NV vendor.

- **VN Extension over the WAN.** VN extension over the WAN can generally be accomplished with most NV solutions. However, in some cases the encapsulation used over the wide area may differ from that used within the data center. Some of the encapsulation techniques used for VN extension over the WAN include MPLS VPNs and two proprietary protocols from Cisco: Overlay Transport Virtualization (OTV) and Locator/ID Separation Protocol (LISP). OTV is optimized for inter-data center VLAN extension over the WAN or Internet using MAC-in-IP encapsulation. It prevents flooding of unknown destinations across the WAN by advertising MAC address reachability using IS-IS routing protocol extensions. LISP is an encapsulating IP-in-IP technology that allows end systems to keep their IP address (ID) even as they move to a different subnet within the network (Location). By using LISP VM-Mobility, IP endpoints such as VMs can be relocated anywhere regardless of their IP addresses while maintaining direct path routing of client traffic. LISP also supports multi-tenant environments with Layer 3 virtual networks created by mapping VRFs to LISP instance-IDs. Inter-data center network virtualization could also potentially be based on Layer 3 vSwitches that support MPLS VPNS and implement network virtualization using RFC 4023 MPLS over IP/GRE tunnels through an IP enterprise network to connect to an MPLS VPN service. SPBM is unique in that it offers extensions over the WAN natively without requiring additional protocols such as OTV or MPLS VPNs.

The remainder of this sub-section of The Guide focuses on the primary differentiating features of Overlay NV solutions: tunnel encapsulation and tunnel control.

Tunnel Encapsulation

VXLAN: Virtual eXtensible LAN (VXLAN)[2] virtualizes the network by creating a Layer 2 overlay on a Layer 3 network via MAC-in-UDP encapsulation. The VXLAN segment is a Layer 3 construct that replaces the VLAN as the mechanism that segments the data center LAN for VMs. Therefore, a VM can only communicate or migrate within a VXLAN segment. The VXLAN segment has a 24-bit VXLAN Network identifier. VXLAN is transparent to the VM, which still communicates using MAC addresses. The VXLAN encapsulation is performed through a function known as the VXLAN Tunnel End Point (VTEP), typically a hypervisor vSwitch or a possibly a physical access switch. The encapsulation allows Layer 2 communications with any end points that are within the same VXLAN segment even if these end points are in a different IP subnet. This allows live migrations to transcend Layer 3 boundaries. Since MAC frames are encapsulated within IP packets, there is no need for the individual Layer 2 physical switches to learn MAC addresses. This alleviates MAC table hardware capacity issues on these switches. Overlapping IP and MAC addresses are handled by the VXLAN ID, which acts as a qualifier/identifier for the specific VXLAN segment within which those addresses are valid.

As noted, VXLANs use a MAC-in-UDP encapsulation. One of the reasons for this is that modern Layer 3 devices parse the 5-tuple (including Layer 4 source and destination ports). While VXLAN uses a well-known destination UDP port, the source UDP port can be any value. As a result, a VTEP can spread all the flows from a single VM across many UDP source ports. This allows for efficient load balancing across link aggregation groups (LAGs) and intermediate multi-pathing fabrics even in the case of multiple flows between just two VMs.

Where VXLAN nodes on a VXLAN overlay network need to communicate with nodes on a legacy (i.e., VLAN) portion of the network, a VXLAN gateway can be used to perform the required tunnel termination functions including encapsulation/decapsulation. The gateway functionality could be implemented in either hardware or software.

VXLAN is supported by a number of vendors including Cisco Systems, VMware, IBM, and Nuage Networks. Avaya's SPBM implementation (Fabric Connect) can also support a VXLAN deployment, acting as a transport layer providing optimized IP Routing and Multicast for VXLAN-attached services.

STT: Stateless Transport Tunneling (STT)[3] is a second overlay technology for creating Layer 2 virtual networks over a Layer 2/3 physical network within the data center. Conceptually, there are a number of similarities between VXLAN and STT. The tunnel endpoints are typically provided by hypervisor vSwitches, the VNID is 24 bits wide, and the transport source header is manipulated to take advantage of multipathing. STT encapsulation differs from VXLAN in two ways. First, it uses a stateless TCP-like header inside the IP header that allows tunnel endpoints within end systems to take advantage of TCP segmentation offload (TSO) capabilities of existing TOE server NICs. The benefits to the host include lower CPU utilization and higher utilization of 10 Gigabit Ethernet access links. STT generates a source port number based on hashing the header fields of the inner packet to ensure efficient load balancing over LAGs and multi-pathing fabrics. STT also allocates more header space to the per-packet metadata, which provides added flexibility for the virtual network tunnel control plane. With these features, STT is

[2] http://searchservervirtualization.techtarget.com/news/2240074318/VMware-Cisco-propose-VXLAN-for-VM-mobility

[3] http://tools.ietf.org/html/draft-davie-stt-01

optimized for hypervisor vSwitches as the encapsulation/decapsulation tunnel endpoints. The initial implementations of Network Virtualization using STT from Nicira Networks are based on OpenFlow-like hypervisor vSwitches (Open vSwitches) and a centralized control plane for tunnel management via downloading mapping tables to the vSwitches.

NVGRE: Network Virtualization using Generic Router Encapsulation (NVGRE)[4] uses the GRE tunneling protocol defined by RFC 2784 and RFC 2890. NVGRE is similar in most respects to VXLAN with two major exceptions. While GRE encapsulation is not new, most network devices do not parse GRE headers in hardware, which may lead to performance issues and issues with 5-tuple hashes for traffic distribution in multi-path data center LANs. With GRE hashing generally involves the GRE key. One initial implementation of NVGRE from Microsoft relies on Layer 3 vSwitches whose mapping tables and routing tables are downloaded from the vSwitch manager. Downloads are performed via a command-line shell and associated scripting language.

SPBM[5]: IEEE 802.1aq/IETF 6329 Shortest Path Bridging MAC-in-MAC uses IEEE 802.1ah MAC-in-MAC encapsulation and the IS-IS routing protocol to provide Layer 2 network virtualization and VLAN extension in addition to a loop-free equal cost multi-path Layer 2 forwarding functionality. VLAN extension is enabled by the 24-bit Service IDs (I-SIDs) that are part of the outer MAC encapsulation. Unlike other network virtualization solutions, no changes are required in the hypervisor vSwitches or NICs and switching hardware already exists that supports IEEE 802.1ah MAC-in-MAC encapsulation. For SPBM, the control plane is provided by the IS-IS routing protocol.

SPBM can also be extended to support Layer 3 forwarding and Layer 3 virtualization as described in the IP/SPB IETF draft using IP encapsulated in the outer SPBM header. This specification identifies how SPBM nodes can perform Inter-ISID or inter-VLAN routing. IP/SPB also provides for Layer 3 VSNs by extending VRF instances at the edge of the network across the SPBM network without requiring that the core switches also support VRF instances. VLAN-extensions and VRF-extensions can run in parallel on the same SPB network to provide isolation of both Layer 2 and Layer 3 traffic for multi-tenant environments. With SPBM, only those Switches that define the SPBM boundary need to be SPBM-capable. Switches not directly involved in mapping services to SPB service IDs don’t require special hardware or software capabilities. SPBM isn’t based on special vSwitches, data/control plane separation, or centralized controllers. SPBM hardware Switches are currently available from several vendors, including Avaya and Alcatel-Lucent.

Tunnel Control

As previously mentioned, initial implementations of VXLAN by Cisco and VMware use flooding as a distributed control solution based on Any Source Multicast (ASM) to disseminate end system location information. Because flooding requires processing by all the vSwitches in the multicast group, this type of control solution will not scale to support very large networks.
.
A more recent approach is to implement tunnel control as a centralized controller function. A control plane protocol that carries both MAC and IP addresses can eliminate the need for ARP. One controller-based solution for VXLAN control, championed by IBM’s Distributed Overlay

[4] http://datatracker.ietf.org/doc/draft-sridharan-virtualization-nvgre/
[5] http://tools.ietf.org/html/draft-allan-l2vpn-spbm-evpn-00

Virtual Ethernet (DOVE) initiative, is to use a DNS-like network service to map the VM's IP address to the egress VTEP's IP address. IBM's solution does not require Multi Cast enablement in the physical network. IBM's Controller based solution has built-in IP routing capability.

In another controller-based approach, used by Nicira Networks, the controller maintains a data base of Open vSwitches (OVS) in the network and proactively updates OVS mapping tables via OpenFlow to create new tunnels when VMs are created or moved. The Nicira controller focuses on the virtual network topology and is oblivious to the topology of the core physical network. The controller is integrated with hypervisor and cloud management systems to learn of changes in the population of VMs.

A third controller approach, used by Nuage Networks and Netsocket, involves the controller maintaining a full topology of the virtual and physical network and maintaining the full address mapping and routing tables derived from standard routing protocols, such as OSPF, IS-IS, or BGP. The portion of the table needed by the vSwitch is disseminated from the controller to the vSwitches via the OpenFlow protocol. The Nuage Networks' vSwitches use VXLAN to encapsulate L2 traffic and GRE to encapsulate L3 traffic.

Comparison of Network Overlay Virtualization Solutions

The following table (**Table 7**) provides a high level summary of the primary features of some of the Network Virtualization solutions that are available or have been recently announced. Note that the solutions described in columns two and three (Cisco, VMware) are not based on a controller.

Table 7: Network Overlay Virtualization features

	Cisco	VMware	IBM	VMware/ Nicira	Nuage Networks	Avaya	Netsocket	Juniper
Product	**Nexus 1000v**	**VSphere DS**	**SDN-VE**	**NSX**	**VSP**	**Fabric Connect**	**NVN**	**Contrail**
Overlay	VXLAN	VXLAN	VXLAN	VXLAN STT?	VXLAN	SPBM	GRE	MPLS/GRE MPLS/UDP VXLAN
VM-NVE Address Learning	VTEP Multicast flooding	VTEP Multicast flooding	Pull From Controller's Directory	Push From Controller's Data Base	Push From Controller's Map Table	IS-IS SPB on physical switch	Push From Controller's Map Table	Push From Controller's Map Table
Broadcast / Multicast within VN	via underlay Multicast	via underlay Multicast	distribution server replication	distribution server replication	dVRS packet replication	via SPB multicast		VRouter packet replication or proxy
Controller Topology Awareness	na	na	Virtual Networks	Virtual Networks	Entire Network	Entire Network	Entire Network	Entire Network
Controller to NVE Protocol	NX-OS CLI	VMware API	Open source submitted to OpenDaylight	OpenFlow NSX API	OpenFlow	IS-IS	vFlow or OpenFlow	XMPP
vSwitch	Nexus 1000v	VDS	SDN-VE vSwitch	VDS, Open vSwitch**	dVRS (Open vSwitch**)	Native to Hypervisor	vFlowSwitch	v Contrail vRouter
vSwitch L3	no	no	yes	yes	yes	na	yes	yes
Gateway Support in Physical Switches				Arista 7150s Brocade ADX	Nuage Networks 7850 VSG	na		
Hypervisors	ESXi, Hyper-V, XEN, KVM	ESXi	ESXi KVM	vSphere. ESXi, XEN, KVM	ESXi, Hyper-V, XEN, KVM	ESXi, Hyper-V, XEN, KVM	Hyper-V ESXi Xen, KVM	KVM, XEN
Controller Federation					via MP-BGP			BGP
DC-DC encapsulation	OTV	OTV	VXLAN	GRE	MPLS over GRE to PE router	Over an SPBM WAN	GRE	MPLS/GRE
	OpenStack vCloud	OpenStack vCloud	OpenStack	OpenStack CloudStack vCloud	OpenStack CloudStack vCloud	OpenStack Integration in controller	OpenStack System Ctr.	OpenStack.

na = not applicable ***** = with proprietary extensions***

Software Defined NV via Flow Table Segmentation

Network virtualization can also be implemented as an application that runs on an SDN controller. Virtual networks are defined by policies that map flows to the appropriate virtual network based on L1-L4 portions of the header. With this type of SDN-based NV, there is no need for tunnels and encapsulation protocols. One example of an NV application is the Big Virtual Switch that runs on the Big Network Controller from Big Switch Networks. The Big Network Controller implements VNs by configuring forwarding tables in OpenFlow physical and virtual switches. The OpenFlow switches can be from a variety of traditional switch vendors. Another alternative is to use Big Switch Switch Light OpenFlow thin software agent running on bare metal Ethernet switches based on Broadcom merchant silicon or on virtual switches.

By exploiting the capability of OpenFlow to deal with encapsulation and de-encapsulation, the SDN controller NV application can also be used to implement overlay VNs running over a conventional L2/L3 network, or a hybrid network based partially on pure SDN VNs and partially on SDN NVs with OpenFLow virtual switches and a conventional core network.

Another slightly different approach to an NV application for SDN controllers is the Virtual Tenant Network (VTN) application developed by NEC and recently accepted as an application by the OpenDaylight consortium. The VTN solution provides a layer of abstraction between the virtual network and the physical network. In the event of a failed link, the VTN can detect and redirect the affected flows within milliseconds. This avoids the re-convergence delay associated with traditional network protocols. The VTN also supports redirection, which enables use cases related to traffic steering and service chaining. In addition, the VTN physical control of the network supports flow based traffic engineering as well as 8-way ECMP.

VTN is based on a logical abstraction that decouples the VTN from the physical network. A virtual network can be designed and deployed using the following set of logical network elements:

• vBridge	L2 switch function.
• vRouter	router function.
• vTEP	virtual Tunnel End Point.
• vTunnel	Tunnel.
• vBypass	connectivity between controlled networks.
• vInterface	end point on the virtual node.
• vLink	L1 connectivity between virtual interfaces.

Using these elements allows the user can define a logical network with the look and feel of conventional L2/L3 network. VTN can also by used to implement an overlay network, an OpenFlow network, or a hybrid overlay/OpenFlow network. Once the network is designed on VTN, it can automatically be mapped onto the underlying physical network, and configured on the individual switches leveraging an SDN control protocol, Typically this would be OpenFlow. Mapping is used to identify the VTN to which each packet transmitted or received by an OpenFlow switch belongs, as well as which interfaces on the OpenFlow switch can transmit or receive that packet. Flows are mapped to a VTN vBridge based on the ingress port on the OpenFlow switch, the source MAC address or the VLAN ID.

Enterprise Plans for NV Adoption

The Survey Respondents were asked a series of questions about their current position relative to evaluating and adopting NV solutions and how that position might change over the next two to three years. In the first of those questions, The Survey Respondents were given a set of alternatives and were asked to indicate the alternatives that described their company's current approach to implementing NV solutions. Their responses are shown in **Table 8**.

Table 8: Current Approaches to Adopting NV Solutions

Approach to Adoption NV Solutions	% of Respondents
We have not made any analysis of NV	25.5%
We will likely analyze NV sometime in the next year	25.5%
We are currently actively analyzing the potential value that NV offers	24.7%
We expect that within a year that we will be running NV either in a lab or in a limited trial	13.6%
We are currently actively analyzing vendors' NV strategies and offerings	11.5%
We currently are running NV either in a lab or in a limited trial	9.9%
We currently are running NV somewhere in our production network	7.4%
We looked at NV and decided to not do anything with NV over the next year	6.2%
We expect that within a year that we will be running NV somewhere in our production network	5.8%
Don't know	4.9%

The data in **Table 8** indicates that while there is currently little deployment of NV, there is a lot of activity and interest relative to analyzing NV solutions. The data in Table 8 also suggests that over the next year the percentage of IT organizations that are either running NV somewhere in their production network, or in a lab or limited trial, will double.

The Survey Respondents were given a two-year time frame and were asked to indicate where in their infrastructure their organization was likely to implement NV solutions. (Multiple responses were allowed) Their responses are shown in **Table 9**.

Table 9: Likely Deployment of NV Solutions

Focus of Future NV Implementation	% of Respondents
Data Center	58.0%
Branch and/or Campus	25.1%
WAN	18.5%
We are unlikely to implement NV in the next two years	15.6%
Don't know	10.7%
We are likely to acquire a WAN service that is based on NV	9.5%

The data in **Table 9** indicates that IT organizations will primarily implement NV solutions within a data center. However, the data also indicates that a sizeable percentage of IT organizations want to extend their NV solutions over the WAN and to also implement NV solutions in their branch and campus networks.

In the final question about their potential future use of NV solutions, The Survey Respondents were asked to indicate how broadly their data center networks will be based on NV three years from now. Their responses are shown in **Table 10**.

Table 10: Data Center Design in Three Years

Balance of NV and Traditional Approach	% of Respondents
Exclusively based on NV	3.3%
Mostly based on NV	25.1%
NV and traditional networking coexisting about equally	37.9%
Mostly traditional	16.9%
Exclusively traditional	4.1%
Don't know	12.8%

The data in **Table 10** indicates that the vast majority of The Survey Respondents expect that in three years that at least half of their data center networks will be based on NV.

Chapter 2: The what, why and how of SDN

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 11** 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 11** 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 11: 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 11** 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 11** 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 12**.

Table 12: 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 12** 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[6], "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

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

implementing an SDN as defined by the ONF. For 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 13**.

Table 13: 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%

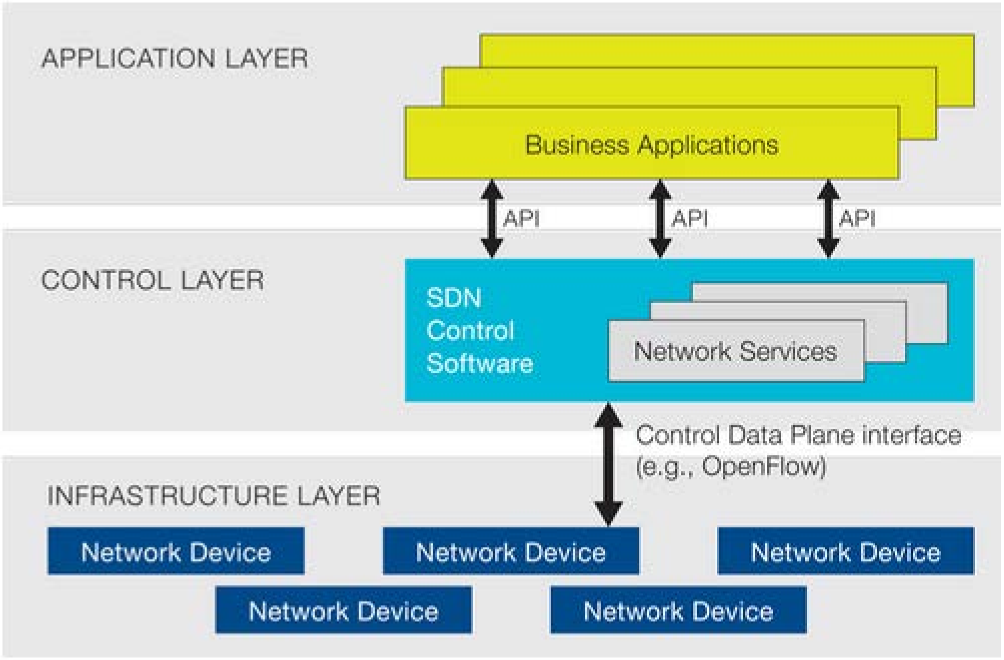
One observation that can be drawn from **Table 13** is that the characteristic of SDN that offers the most value to The Survey Respondents is tactical: The centralization of configuration and policy management. However, the second most important characteristic, the programmability of network elements, 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 13** 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 4 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 4** 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 4: ONF's SDN Architecture



Below are definitions of some terms that are commonly associated with SDN, some of which appear in **Figure 4**.

- **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 4**, the southbound API is the API that enables communications between the control layer and the infrastructure layer.

- **Service Chaining**[7]
  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 4 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

[7] 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 4**. 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*[8].

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 4** 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.

[8] Will be published at: webtorials.com/Metzler

The Inhibitors to SDN Adoption

The left hand column of **Table 14** 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 14** 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 14: 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 14** 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 14**, 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[9]. 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:

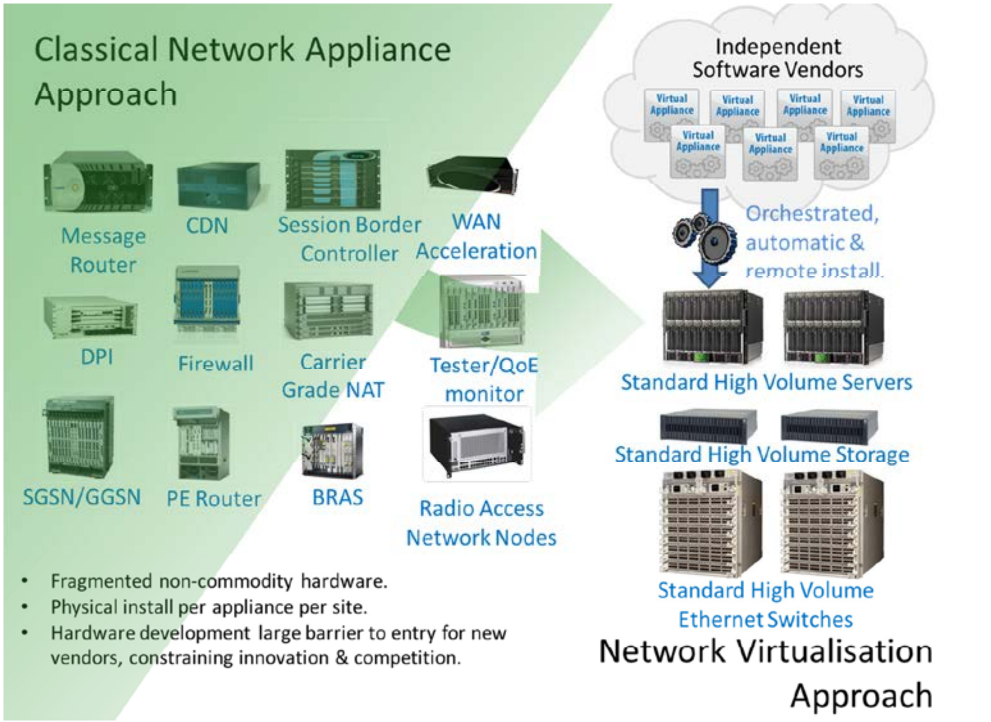
- Industry standard servers running Linux or Windows;
- Virtual appliances running over hypervisors on industry standard hardware servers;
- Proprietary hardware appliances.

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

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.

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 5**.

Figure 5: The Virtualization of Network Appliances


Classical Network Appliance Approach
Message Router
CDN
Session Border Controller
WAN Acceleration
DPI
Firewall
Carrier Grade NAT
Tester/QoE monitor
SGSN/GGSN
PE Router
BRAS
Radio Access Network Nodes
Fragmented non-commodity hardware.
Physical install per appliance per site.
Hardware development large barrier to entry for new vendors, constraining innovation & competition.
Independent Software Vendors
Virtual Appliance
Orchestrated, automatic & remote install.
Standard High Volume Servers
Standard High Volume Storage
Standard High Volume Ethernet Switches
Network Virtualisation Approach

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 5**, 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[10] has since grown and now includes a number of equipment vendors, but currently relatively few of the top vendors of virtual appliances are members.

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[11]. According to ETSI[12], "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.

[10] http://portal.etsi.org/NFV/NFV_List_members.asp
[11] http://www.etsi.org/technologies-clusters/technologies/nfv
[12] http://www.etsi.org/index.php/news-events/news/700-2013-10-etsi-publishes-first-nfv-specifications

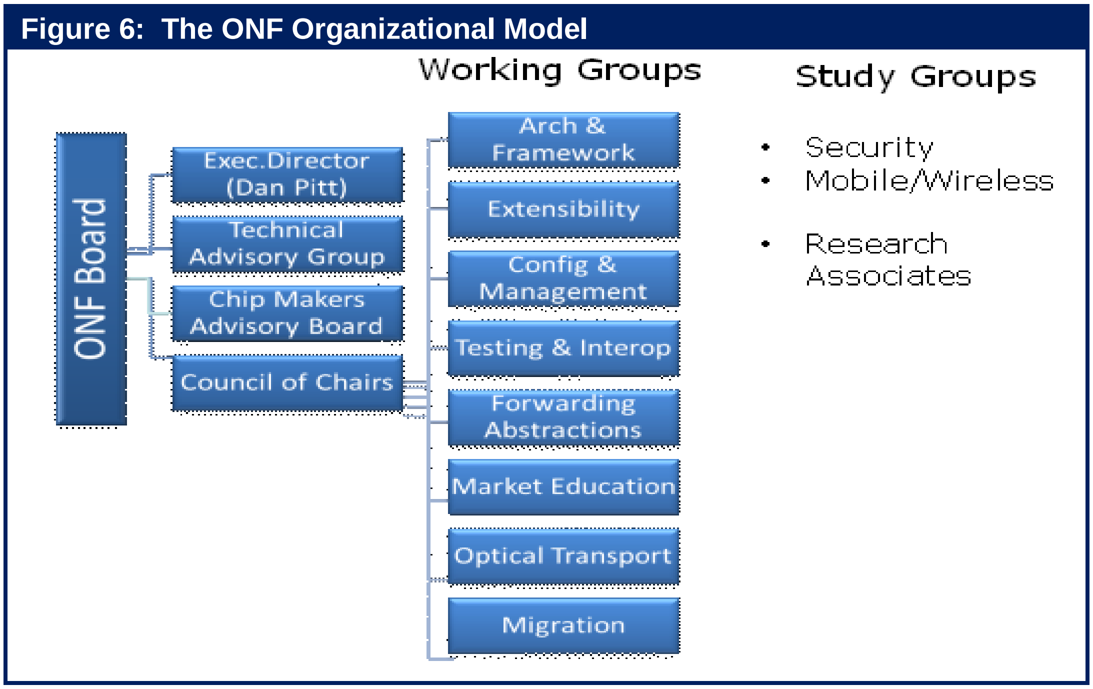
The Open Networking Foundation and OpenFlow

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 6 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[13].

Figure 6: The ONF Organizational Model



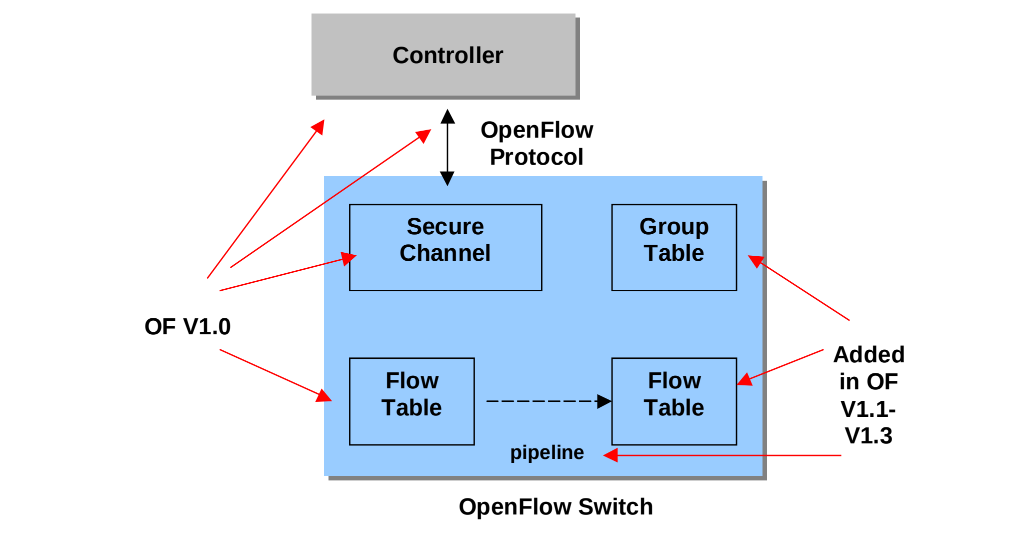
The OpenFlow Protocol

Referring back to **Figure 4** (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 7**. 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 7**, OpenFlow is referred to as OF.

[13] 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 7: 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 15**.

Table 15: 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 15 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 11**, 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%[14]. As shown in **Table 11**, 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

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

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.

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[15], “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[16].

[15] http://incntre.iu.edu/research/flowscale

[16] http://www.bigswitch.com/blog/2013/07/26/network-monitoring-with-big-tap-your-first-sdn-application

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

Circuit Provisioning

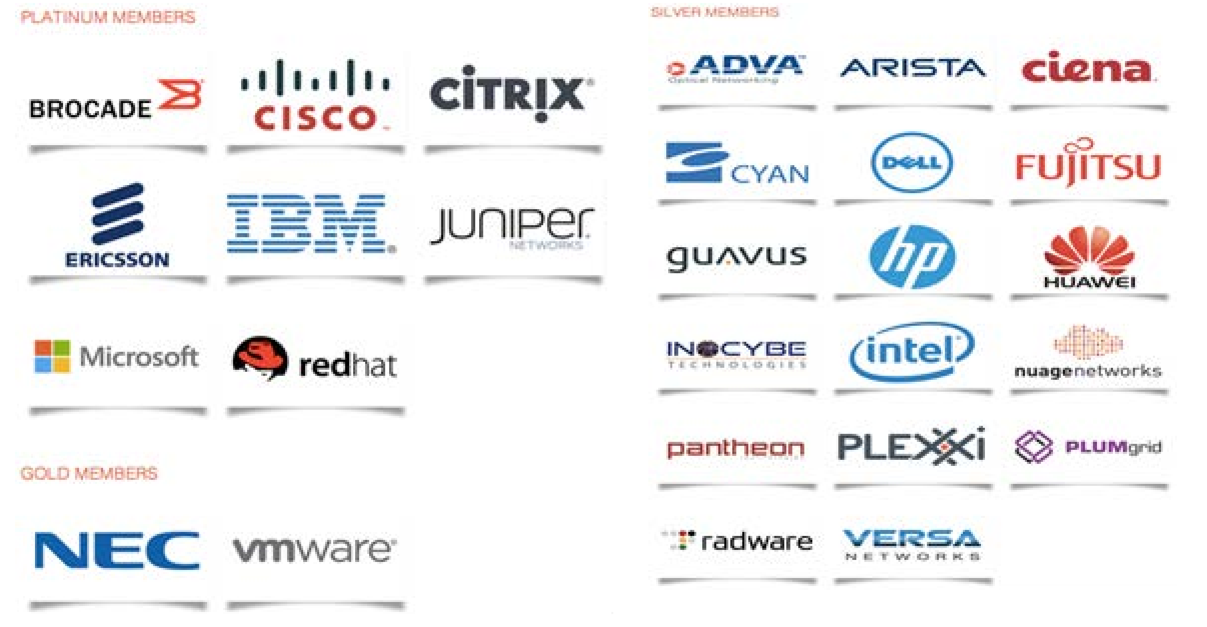
With extensions in V1.3 and V1.4, OpenFlow can support circuit-switched paradigms, including CWDM, DWDM, and MPLS with specific path selection and requested levels of CBR and priority. Circuits can be provisioned on a dynamic, scheduled, or permanent basis. Recovery from failed circuits can be via predetermined 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[17] 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

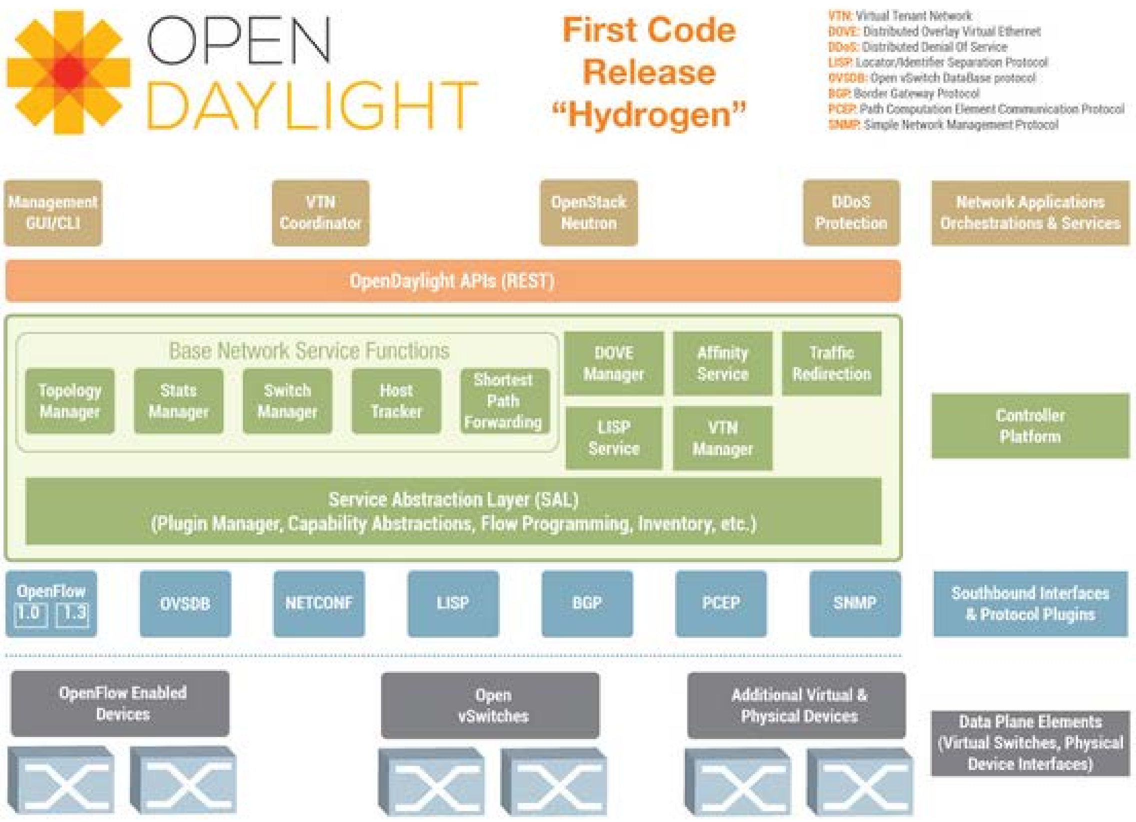


The approach that the consortium is taking to the base architecture for the OpenDaylight controller is to combine two code bases that were brought together through a collaborative proposal by Colin Dixon of IBM and David Erickson of Stanford. In addition, while the expectation is that the platinum members 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.

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

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

Figure 6: OpenDaylight SDN Architecture


OPEN DAYLIGHT
First Code Release "Hydrogen"
VTN: Virtual Tenant Network
DOVE: Distributed Overlay Virtual Ethernet
DDoS: Distributed Denial Of Service
LISP: Locator/Identifier Separation Protocol
OVSDB: Open vSwitch DataBase protocol
BGP: Border Gateway Protocol
PCEP: Path Computation Element Communication Protocol
SNMP: Simple Network Management Protocol
Management GUI/CLI
VTN Coordinator
OpenStack Neutron
DDoS Protection
Network Applications Orchestrations & Services
OpenDaylight APIs (REST)
Base Network Service Functions
Topology Manager
Stats Manager
Switch Manager
Host Tracker
Shortest Path Forwarding
DOVE Manager
Affinity Service
Traffic Redirection
LISP Service
VTN Manager
Controller Platform
Service Abstraction Layer (SAL)
(Plugin Manager, Capability Abstractions, Flow Programming, Inventory, etc.)
OpenFlow 1.0 1.3
OVSDB
NETCONF
LISP
BGP
PCEP
SNMP
Southbound Interfaces & Protocol Plugins
OpenFlow Enabled Devices
Open vSwitches
Additional Virtual & Physical Devices
Data Plane Elements (Virtual Switches, Physical Device Interfaces)

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[18]. Relative to the terminology of **Figure 4**, DefenseFlow is a network service that provides DDoS protection. Another such example is HP's Sentinel application[19] 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 16**.

[18] http://www.radware.com/Products/DefenseFlow/

[19] http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA4-7496ENW.pdf

Table 16: 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 16** 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 13**. 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 17**.

Table 17: 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 17 is that the vast majority of The Survey Respondents believe that SDN will have a positive impact on management.

Appendix – Chapter 2

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

Error! Objects cannot be created from editing field codes.

- Flexible pipeline processing through multiple flow tables, as shown in the right hand side of **Figure 7**. 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.

Chapter 3: The NV and SDN Ecosystem

Overview of the NV and SDN Ecosystem

One measure of the extent of the NV and SDN ecosystem is that there are currently more than 100 members of the Open Networking Foundation[20] (ONF). This subsection of The Guide identifies the major categories of organizations that are part of the NV and SDN ecosystem and briefly discusses the value proposition of each of the categories.

This subsection of The Guide also identifies representative members of each category of organizations that are part of the NV and SDN ecosystem. The representative members that are identified either currently provide the indicated functionality or can be expected to provide the indicated functionality in the near term. As is explained below, in some instances there can be a very wide range in terms of the functionality provided by the members of a given category.

Merchant Silicon/Chip Vendors

Value Proposition: These vendors are in a position to provide hardware support in switching chips for protocols such as OpenFlow and VXLAN. This will have the effect of increasing the speed and scalability of solutions. Longer term there is also the possibility of at least some of these vendors developing cost-effective switch silicon that is optimized for OpenFlow and other controller/switch protocols.

Representative Members:

- Broadcom
- Intel
- Marvell
- Mellanox

HyperScale Data Centers

Value Proposition: Part of their value proposition is that these high-profile vendors either already are or are likely to be early adopters of SDN. As a result, these vendors are having a significant indirect impact on the development of SDN. In addition, vendors such as Google, Yahoo and Facebook are board members of the ONF. As such, these vendors directly influence the work of the ONF in general and of the evolution of the OpenFlow protocol and the northbound API in particular.

It is possible that some of these vendors will also influence the development of NV. However, some of the major players in this segment of vendors, such as Facebook and Google, currently make little use of NV.

Representative Members:

- Yahoo
- Google
- Facebook

[20] https://www.opennetworking.org/blog/tag/open-networking-foundation

Telecom Service Providers

Value Proposition: Part of the value proposition of this class of vendors is similar to the value proposition of hyper-scale data center providers. For example, these vendors either already are, or are likely to be early adopters of SDN and/or NV in order to support their cloud offerings. In addition, vendors such as Deutsche Telekom, NTT Communications and Verizon are also board members of the ONF.

The preceding chapter of The Guide discussed the interest that IT organizations have in either using SDN in the WAN or in acquiring a service from a WAN service provider that is based on SDN. Responding to that interest, vendors like Pertino[21] are currently using SDN and Network Function Virtualization (NFV)[22] to enable them to offer a new generation of WAN services and Verizon[23] has announced a trial based on using SDN to enable a new generation of data center to data center WAN services.

Representative Members:

- Pertino
- Deutsche Telekom
- NTT Communications
- Verizon

Switch Vendors

Value Proposition: Relative to SDN, the majority of these vendors takes at least some of the control functionality that has typically resided in their switches and now relies on that functionality being provided by an SDN controller. In addition, these vendors implement protocols in their switches that enable those switches to communicate with an SDN controller. These vendors are increasing reliant on merchant silicon as the basis for major portions of their switching product lines.

Most of the vendors in this category represent traditional switch vendors. An exception to that is Pica8. Pica8 provides a switch that is comprised of its network operating system loaded onto commodity white box, bare-metal switches.

Representative Members:

- Alcatel-Lucent
- Avaya
- Cisco
- Dell
- Extreme Networks
- HP
- NEC
- PICA8
- IBM

[21] http://www.pcmag.com/article2/0,2817,2415354,00.asp
[22] NFV was explained in the preceding chapter of The Guide
[23] http://searchsdn.techtarget.com/news/2240182264/Intel-DPDK-switch-and-server-ref-designs-push-SDN-ecosystem-forward

Network Management and Automation

Value Proposition: Most, if not all of the providers of NV and SDN solutions will provide at least some ability for the consumers of those solutions to manage the solutions that they provide. The members of this category of the ecosystem don't provide NV and/or SDN solutions themselves. The vendors listed below either currently provide, or soon will provide management functionality that isn't offered by the providers of the NV or SDN and solutions and/or they integrate the management of these solutions into a broader management structure. The breadth of management functionality provided by the members of this category is illustrated in the next sub-section of The Guide - the sub-section entitled *Representative Vendors*.

Representative Members:

- Packet Design
- QualiSystems
- EMC
- NetScout
- CA

Providers of Network Services

Value Proposition: The members of this category provide network services such as security and optimization that are part of NV and SDN solutions[24]. Some of these services were described in the preceding section of this report. There is the possibility that over time that a large number of independent software vendors (ISVs) will also provide these services.

Representative Members:

- Embrane
- A10
- Radware
- HP
- Riverbed
- Citrix
- Cisco
- Extreme Networks
- NEC

[24] The preceding section of The Guide discussed service chaining/Insertion

Testing

Value Proposition: The members of this category either provide products that enable equipment manufacturers and others to test NV and SDN solutions or they provide the testing themselves.

Representative Members:

- QualiSystems
- InCNTRE
- Ixia
- Spirent

Standards Bodies

Value Proposition: The members of this category create standards for protocols such as OpenFlow or VXLAN. These standards form the basis for enabling products from disparate vendors to interoperate.

Representative Members:

- ONF[25]
- IEEE
- IETF
- Network Function Virtualization (NFV) – under the auspices of ETSI[26]

Providers of SDN or Network Virtualization Controllers

Value Proposition: These vendors provide the controllers that are part of any SDN solution and which are part of many NV and SDN solutions.

Representative Members:

- Big Switch Networks
- NEC
- Nuage Networks
- Netsocket
- HP
- Cisco
- Open Daylight Consortium[27]
- VMware/Nicira

[25] The role of the ONF was discussed in the preceding section of The Guide

[26] The relationship between SDN and NFV was discussed in the preceding section of The Guide

[27] The Open Daylight Consortium was discussed in the preceding section of The Guide.

Providers of Telcom Service Provider’s Infrastructure/ Optical Networking

Value Proposition: These vendors are providing the infrastructure that enables telecom providers to leverage SDN in their service offerings.

Representative Members:

- ADVA Optical Networking
- Ciena
- Cyan
- Infinera
- ZTE Corporation

Server Virtualization Vendors

Value Proposition: These vendors provide the vSwitches and the hypervisor vSwitch APIs for third party vSwitches that are a key component of NV and SDN solutions.

Representative Members:

- Citrix
- Microsoft
- VMware

Representative Vendor - Avaya

The Opportunity that Avaya is Targeting

Avaya's SDN objective is to automate service delivery for applications and users across any combination of physical and virtual components – taking both human-induced error and delay out of the process.

Avaya's SDN Strategy

The key components of Avaya's SDN strategy are to:

1. Leverage OpenStack to enable rapid service creation via a common orchestration interface

- OpenStack provides an integration layer that sits above the virtualized components within the Data Center and orchestrates those resources to deliver a service through a set of APIs and a common dashboard.
- An Avaya OpenStack Horizon-based Management Platform, used to deliver, via a common GUI interface, orchestration for compute (Nova), storage (Cinder/Swift) and Avaya VENA Fabric Connect network virtualization technology (Neutron).

2. Deploy Avaya Fabric Connect (an enhanced implementation of Shortest Path Bridging) to link virtual/physical infrastructure and enable flexible network services at any scale

- Eliminates protocol overlays to deliver all services with a single protocol – making it much easier to design, manage, provision, and troubleshoot the network.
- Replaces complex network-wide provisioning practices with simple edge-only provisioning.
- Simplifies virtual machine mobility. Virtual LANs and connectivity can be extended anywhere - across Layer 3 domains and geographically dispersed Data Centers.
- Automates the provisioning of Fabric Connect through an OpenStack Neutron interface.

3. Provide public access (APIs) allowing customized interaction and integration with Avaya Fabric Connect

- Avaya is developing public access APIs directly into its Fabric Connect technology to allow for customized interaction directly with the virtualized network.

4. Extend orchestration and Fabric Connect to deliver end-to-end service creation and delivery from Data Center to Desktop

- Avaya is extending its service orchestration and network virtualization technology to the network edge in order to extend the service chain from Data Center to Desktop.
- This allows for new levels of network simplicity as services are driven top-down, by the end-point, with provisioning automated where the applications and users connect to the network.

5. Integrate policy control to automate service delivery through interaction with the application layer

- Policy controller detects users / applications and then coordinates with the orchestration system to allocate the necessary resources to support that application.

Avaya Customer Deployments

Avaya VENA Fabric Connect technology has been widely adopted by businesses across the globe. Many of these customers are also evaluating the OpenStack cloud orchestration platform as a means to enable automation and coordinated orchestration of Data Center resources. Specific customer examples include:

Sochi 2014 Olympic Winter Games

- Will be the first “Fabric-enabled” Games; providing ease of management, provisioning and deployment, simplified adds, moves and changes, and increased stability / robustness.
- This will be the first Olympics to combine video with voice and data on a single, IP-based network. Sharing the same fabric architecture will reduce the costs for video, simplify network administration and significantly boost throughput and reliability.

InteropNet 2013

- First time that the Interop organizers deployed a network fabric.
- Backbone for the entire event was staged by only three individuals, and in only a matter of days (1/10th the burden of previous years).
- Ran flawlessly for both North American Interop 2013 events (Las Vegas and NYC).

Leeds Metropolitan University

- Leverages Fabric Connect first to provide seamless L2 extensions between geographically dispersed Data Centers.
- Migrated OSPF core to Fabric Connect’s Shortest Path Bridging to reduce inter-site failover times from seconds to ~20 milliseconds.
- Set up an isolated IP network across the corporate backbone to secure credit card transactions to help meet PCI DSS compliance for the banks. Provisioning at the edge only and done without adding overlay protocols or complexity.

Oslo University Hospital

- Using Fabric Connect to interconnect 40 locations.
- Leveraging the integrated VRF functionality of Fabric Connect to create secure zones for important traffic like imaging from medical devices.
- Ability to do adds, moves, and changes to the network easily without risk.
- Zero downtime environment; Fabric Connect offers a streamlined network solution – fully load balanced – with lightning fast recoveries.

Franciscan Alliance

- Leveraging Fabric Connect to provide a simplified, higher capacity network that supports increased, imaging-driven traffic requirements.
- Carrier issues no longer impact the entire network – where previously topology changes (planned or unplanned) would cause network-wide re-convergence delays – Fabric Connect instantaneously converges, delivering superior experience for both end-users and IT.

Chapter 4: Planning for NV and SDN

Introduction

As noted in the executive summary, there is considerable confusion in the industry relative to NV and SDN. This confusion is understandable given the breadth of problems that these solutions are supposed to address combined with the variety of approaches that vendors are proposing. Further adding to the confusion is the embryonic nature of most of the solutions that are available in the marketplace, the current limited adoption of these solutions and the overall level of hype associated with NV and SDN.

Given this confusion, it would be understandable if an enterprise IT organization decided to take a wait and see attitude about NV and SDN. While that response would be understandable, it isn't the right approach to take either from the perspective of the IT organization or the IT professional. That follows in part because even though no reasonable person would claim to know in detail how SDN and network virtualization will evolve over the next several years, there is no doubt that:

- IT organizations need to solve the problems (e.g., support the dynamic movement of virtual machines, reduce operational complexity) that NV and SDN are designed to solve.

- Many of the characteristics of NV and SDN solutions (e.g., more reliance on software, increased use of automation) are already being broadly adopted within IT organizations.

There is also no doubt that implementing NV and/or SDN presents risk, but that ignoring NV and SDN presents significant risk to both enterprise IT organizations and to IT professionals. The risk to enterprise IT organizations is that by ignoring NV and SDN they remain unable to solve the problems that NV and SDN are designed to solve and this puts their company at a competitive disadvantage. The risk to IT professionals is that ignoring NV and SDN delays their coming up the learning curve on these new approaches which would result in a diminishment of the value they could provide either to their current employer or to a future employer.

Market Research: The Current State of Planning

This subsection of The Guide presents recent market research that quantifies:

- How IT organizations are approaching analyzing and implementing NV and SDN;
- The plans that IT organizations have for open source solutions and open protocols;
- The expectations that IT organizations have for how broadly they will implement NV and SDN.

How IT organizations are Approaching NV and SDN

The Survey Respondents were asked to indicate the approach that their company is taking relative to adopting NV and SDN. The Survey Respondents were allowed to indicate multiple approaches and a summary of their responses is shown in **Table 18**.

Table 18: Approach to Implementing NV and SDN

Approach	NV	SDN
We have not made any analysis of it	26%	19%
We will likely analyze it sometime in the next year	26%	26%
We looked at it and decided to not do anything with it over the next year	6%	5%
We are currently actively analyzing the potential value that it offers	25%	36%
We are currently actively analyzing vendors' strategies and offerings for it	12%	20%
We expect that within a year that we will be running it either in a lab or in a limited trial	14%	19%
We currently are running it either in a lab or in a limited trial	10%	13%
We expect that within a year that we will be running it somewhere in our production network	6%	10%
We currently are running it somewhere in our production network	7%	6%
Don't know	5%	4%
Other	1%	4%

The way to read the data in **Table 18** is that 26% of The Survey Respondents work for companies that haven't made any analysis of NV and 19% of The Survey Respondents work for companies that haven't made any analysis of SDN.

While there are some differences between the overall approach that IT organizations are taking to NV and the overall approach that IT organizations are taking to SDN, there are more similarities than there are differences. The high level story told by the data in **Table 18** is that today there is a lot of interest in both NV and SDN, but very little deployment of either in production networks. If The Survey Respondents are correct, there will be a modest increase in the production use of both NV and SDN in 2014.

The Expected Role of Open Source and Open Protocols

Given that the phrase *open networking* is often associated with SDN, The Survey Respondents were asked to indicate the type of SDN solution that their organization was likely to implement within the next two years and the possible responses focused on open protocols and open source solutions. The respondents were only allowed one choice. Their responses are shown in **Table 19**.

Table 19: Likely SDN Solutions

Selection	% of Respondents
Open source, open protocols, multiple vendors	21%
Open source, open protocols, single vendor with an ecosystem of partners	12%
A mix of open and proprietary protocols based on a single vendor with its ecosystem of partners	22%
Most attractive solution regardless of openness or number of vendors	17%
It is unlikely that we will implement SDN within two years	15%
Don’t know	12%

One conclusion that can be drawn from **Table 19** is that in spite of all of the discussion of open networking on the part of press and analysts, less that half of The Survey Respondents who work for a company that will likely implement SDN within the next two years are currently committed to SDN solutions based on open source and open protocols[28].

[28] The Survey Respondents who answered “don’t know” were excluded from the calculation.

Anticipated NV and SDN Deployment

The Survey Respondents were asked to indicate how broadly they expected that their campus, WAN and data center networks would be based on SDN and/or NV three years from now. The question didn't make any attempt to define how network virtualization would be implemented; e.g., as part of an overlay solution or through manipulating OpenFlow tables. Their responses are shown in **Table 20** and **Table 21**.

Table 20: Expected Deployment of NV

	Exclusively Based on NV	Mostly NV	Hybrid – NV and Traditional about Equal	Mostly Traditional	Exclusively Traditional	Don't know
Campus Networks	1%	12%	40%	24%	10%	14%
WAN	0%	7%	35%	32%	11%	14%
Data Center Networks	3%	25%	38%	17%	4%	13%

Table 21: Expected Deployment of SDN

	Exclusively Based on SDN	Mostly SDN	Hybrid – SDN and Traditional about Equal	Mostly Traditional	Exclusively Traditional	Don't know
Campus Networks	2%	14%	42%	26%	7%	10%
WAN	2%	10%	35%	35%	10%	8%
Data Center Networks	3%	28%	39%	18%	5%	7%

Some of the conclusions that can be drawn from the data in **Table 20** and **Table 21** include:

- Although The Survey Respondents expressed the strongest interest in deploying NV and SDN in their data centers, they also expressed significant interest in deploying NV and SDN in both campus and wide area networks.

- Only a small percentage of The Survey Respondents indicated that in three years that their networks would be either based exclusively on traditional techniques or exclusively on NV and/or SDN.

- The Survey Respondents' most common response was that three years from now that each type of network would be comprised roughly equally of a traditional approach and an approach based on NV and/or SDN.

Crafting an NV and/or SDN Plan

This section of The Guide outlines a process that a hypothetical company, that will be referred to in this section as *GottaChange,* can use to plan for the implementation of NV and/or SDN. The intention is that IT organizations will customize this process for use in their environments.

Define NV and SDN

As described in previous chapters of The Guide, there isn't uniform agreement in the industry as to the precise definition of NV and/or SDN. *GottaChange* can't wait for the brouhaha surrounding the definition of NV and SDN to sort itself out. As part of developing an implementation plan, *GottaChange* must develop a definition of NV and/or SDN that is well understood and agreed to within their organization.

Identify the Primary Opportunities

In order to intelligently choose vendors, architectures and enabling technologies, *GottaChange* needs to first identify the primary opportunities that they are hoping to address by implementing NV and/or SDN. To assist with this process, Chapter 1 of The Guide identified the primary use cases for NV and also presented market research that showed the interest that The Survey Respondents had in each of the use cases. Chapter 2 did the same for SDN.

To exemplify the relationship between the opportunities and the various solutions being proposed by vendors, consider the fact that if the primary opportunity that is driving an IT organization is the need to support the dynamic movement, replication and allocation of virtual workloads, then an overlay-based NV solution from a vendor such as Nuage Networks or Netsocket is a viable candidate, as is a solution from a company such as NEC that implements NV by manipulating OpenFlow tables. An overlay-based NV solution unto itself, however, doesn't make it easier to respond to other opportunities such as making it easier to implement QoS, nor does it enable applications to dynamically request services from the network[29].

Identify the Key Metrics

Having identified the primary opportunities, *GottaChange* needs to identify the key business-related metrics that are associated with each opportunity. The principal use of these metrics is to enable the IT organization to create a business case for implementing NV and/or SDN. However, *GottaChange* should use these metrics throughout the evaluation process; i.e., evaluating solution architectures and performing a proof of concept.

In some cases the key business metrics may be obvious. For example, if one of the primary opportunities that *GottaChange* is trying to address is the centralization of configuration management and provisioning, then one of the key business metrics associated with that opportunity is likely to be labor savings. In contrast, if one of the primary opportunities is to enable business agility, it may be more difficult for *GottaChange* to identify one or more IT-related metrics that, if NV and/or SDN improve them, lead to measurable business value.

[29] Chapter 2 of The Guide discussed an overlay/underlay model that can address these opportunities.

Define the Scope of Possible Solutions

As some point in the planning process *GottaChange* needs to define how broad of an NV and/or SDN solution they are seriously considering implementing. This could come after the first phase of the evaluation process (see below). It should come prior to *GottaChange* moving forward with performing a proof of concept (POC). As described below, the broader *GottaChange* defines the potential solution, the more risk and the more organizational resistance they will encounter.

In addition, based on how *GottaChange* defines what they mean by a NV and/or SDN solution, it may or may not be possible for them to acquire a complete solution from a single vendor. For example, it is reasonable to consider a NV solution based on overlays to be a complete solution unto itself. Analogously, it is reasonable to think of one or more SDN controllers and the underlying network elements as being a complete solution. If *GottaChange* uses one or both of these approaches as their definition of an NV and/or SDN solution, then it is possible for *GottaChange* to buy a complete solution from a single vendor.

However, if *GottaChange* has an expanded definition of *solution*, it is less likely that they will be able to acquire a complete solution from a single vendor. An expanded definition of what *GottaChange* means by solution could include functionality such as orchestration; the L4 to L7 functions that are inserted into the service that is consumed by users; and the business applications that access the control information in the SDN controller.

Decide: Best of Breed vs. Systems Solution

As described above, based on how *GottaChange* defines what they mean by an NV and/or SDN solution, it may be possible for them to acquire a complete NV and/or SDN solution from a single vendor; a.k.a., a systems solution. However, even if it is possible for GottaChange to buy a systems solution they may decide to at least explore the option of buying best of breed components from varying vendors. If *GottaChange* determines that they are willing to acquire components from varying vendors, *GottaChange* must evaluate the testing that was done on both the individual components as well as the complete solution; how the solution will be updated and tested over time; and whether or not there is a *single throat to choke*.

It's reasonable for *GottaChange* to think that if they are acquiring a complete NV and/or SDN solution from a single vendor, that the solution won't have interoperability issues. While that is a reasonable thought, IT organizations still need to request details of the testing that was performed by the vendor themselves, as well as the results of any third party testing that was performed. This testing is important both to demonstrate interoperability of the components of the solution as well as to identify the performance limits of the solution.

Evaluate NV and/or SDN Solutions

The process that *GottaChange* uses to evaluate NV and/or SDN solutions should be cyclical. As part of the first stage of the evaluation process, *GottaChange* should perform a cursory evaluation of numerous vendors. The primary goal of the first stage of the evaluation process is to enable *GottaChange* to determine which solutions correspond to the opportunities that they are seeking to respond to and it also makes *GottaChange* aware of the varying approaches to SDN that the vendors have, each with their own value add. Upon completion of the first stage of the evaluation process, *GottaChange* is in a position to eliminate vendors from consideration and to begin a more detailed analysis on a small set of vendors. As described below, the result of this detailed analysis may well be the recommendation to go forward with a POC.

When evaluating a vendor's SDN solution, IT organizations need to understand the following aspects of those solutions.

- **The Solution Architecture**

  This includes topics such as which components of the solution are provided by the vendor and which are provided by a partner; what functionality is done in hardware vs. in software; how much control is centralized in the SDN controller; what protocols are used within the solution; how the solution supports high availability and the level of abstraction that is provided by the controller's northbound API.

  In addition, *GottaChange* must evaluate the various NV and/or SDN solutions based on their ability to respond to the opportunities that the IT organization has identified. For example, assume that one of the opportunities that the *GottaChange* has identified is being able to support the dynamic movement of VMs. Given that, then as part of the evaluation of solution architectures, *GottaChange* has to identify how each solution accomplishes this.

  Chapter 2 of The Guide contains a set of 7 key questions that *GottaChange* can ask vendors about the architecture of their SDN solutions.

- **The Controller**

  GottaChange must evaluate the architecture of a number of NV and/or SDN controllers. For example, does the controller have a modular architecture that will enable the addition of new functionality over time? *GottaChange* also needs to understand how the controller's architecture enables scalability, high availability and performance. At the author's web site[30] is a white paper that discusses ten criteria that IT organization should use to evaluate SDN controllers[31].

- **The Network Elements**

  Most overlay-based NV solutions are network agnostic. If that is the type of solution that *GottaChange* is evaluating, then it is highly likely that there isn't a need for them to evaluate the network elements on which the potential NV solutions run.

  However, if *GottaChange* is evaluating solutions that closely resemble the ONF definition of SDN that was presented in Chapter 2, then *GottaChange* should ask the vendors questions such as:

  1. Which switches, both virtual and physical, support your SDN solution? For OpenFlow-enabled switches, identify whether the switch is a pure OpenFlow switch or a hybrid OpenFlow switch.

[30] www.ashtonmetzler.com
[31] Ibid.

2. What protocols do you support between the control layer and the infrastructure layer of your proposed solution? What network behaviors are enabled by these protocols and what types of services can be constructed using those behaviors?

3. If Open Flow is supported, what versions have been implemented? What required features of the supported version are not included in the implementation? Indicate which of the optional features it supports. Describe any significant vendor-specific extensions that have been made.

4. If one of the switches in your proposed solution is in SDN mode, are there any types of traffic that must be processed partially in software before being forwarded?

5. If one of the switches in your proposed solution is in hybrid mode, does that have any impact on the behavior of the traditional component of the switch? If yes, explain.

- **Management**

  There are two aspects of NV and/or SDN management that *GottaChange* needs to evaluate. One aspect is the ability of the vendor's solution to alleviate the management challenges created by NV and/or SDN. Based on the type of solution that *GottaChange* is considering, this may include monitoring the performance of the controller; providing end-to-end visualization of the virtual networks; configuring the SDN switches and monitoring the physical and logical networks between switches. The second aspect of management that *GottaChange* needs to evaluate is the integration of the management of NV and/or SDN into a broader management solution.

  Chapter 2 of The Guide contains a set of 5 key questions that *GottaChange* can ask vendors about the management of their SDN solutions.

- **Security**

  There are also two aspects of security that GottaChange needs to evaluate. One aspect is what functionality the vendor provides in order to secure their NV and/or SDN solution. One of the reasons this is important is because the NV and SDN controllers are new attack surfaces. The other aspect of security that needs to be evaluated is the ability of the solution to enhance the overall security of the IT infrastructure. An example of how SDN can potentially improve security is Radware's recent contribution to the Open DayLight consortium's SDN controller of a toolset that can be used for the detection and mitigation of DDoS attacks.

  Chapter 2 of The Guide contains a set of 5 key questions that GottaChange can ask vendors about the security of their SDN solutions.

- **Additional Functionality**

  There are two approaches that an IT organization can take relative to implementing network functions that ride on the SDN controller. One approach is to acquire the network functions from a vendor. Two examples of vendor provided network functions were already discussed. One is Radware's DDoS application and the other is NEC's Virtual Tenant Networking functionality. Since most IT organizations will acquire network functions from vendors, evaluating vendor supplied network functions is a key component of the overall process of evaluating SDN solutions.

The second approach is for the IT organization to develop some or all of the required network functionality itself. The primary advantage of this approach is that it enables the IT organization to customize the network functions to meet the organization's specific requirements. One of the disadvantages of this approach is that it requires the IT organization to have the base of skills that are necessary both to develop the network functions and to maintain those functions over their life cycle.

GottaChange should use the process of evaluating NV and/or SDN solutions to determine if it can acquire all of the network functions it needs to respond to the opportunities that it has identified or if it has to develop some or all of those functions itself.

Test and Certify Solutions

As previously discussed, even if all of the components of an NV or SDN solution come from a single vendor, as part of evaluating those solutions *GottaChange* needs to understand the testing that was done to ensure both the smooth operation and the performance of the solution. Particularly in those situations in which the components of the SDN solution come from multiple vendors, *GottaChange* needs to understand if the solution is certified. By that is meant, if *GottaChange* implements the solution, will it have a single point of contact to resolve any problems that develop.

There may be instances in which *GottaChange* has to either do testing itself or to commission a third party to do testing on its behalf. For example, if *GottaChange* were to develop one or more network functions, it would need to test the operation of those functions on the controller(s) that it had selected and it would need to redo that testing prior to implementing new versions of the controller or new versions of the network functions. If *GottaChange* anticipates facing a situation like this then as part of the evaluation process, *GottaChange* needs to evaluate both the tools that are available to enable the organization to do the testing itself as well as the functionality provided by external test labs.

Integrate with the Existing Environment

It is certainly possible for *GottaChange* to evaluate NV and/or SDN solutions in isolation from the IT organization's current environment. However, given that the NV and/or SDN solution might at some time be implemented in *GottaChange's* production network, then as part of the evaluation process *GottaChange* should examine how the SDN solution would fit into the existing infrastructure. For example, what mechanisms exist to enable traffic to flow between the SDN solution and the traditional network? Is it possible to extend the SDN solution so that it operates both in a data center and in a branch office? So that the solution operates in multiple data centers?

Educate the Organization

Both NV and SDN are both embryonic and rapidly evolving. Hence, in order to create and update a plan to potentially implement one or both of these architectures, *GottaChange* must continually educate itself as to what is happening in the broad NV and/or SDN ecosystem. This certainly includes analyzing what is being said in the industry about the relevant use cases and the techniques that can be used to justify deployment. It also includes reviewing product announcements; the announcement of enabling technologies that are either new or have evolved; the results of plugfests that are intended to test the interoperability of SDN solutions; and the work of organizations such as the Open DayLight consortium.

Much of the education discussed in the preceding paragraph can be accomplished by reading articles and white papers and by attending seminars and workshops. *GottaChange* should also consider downloading some of the open source products that are readily available and playing with those solutions to gain deeper insight into their capabilities and weaknesses. In addition, by yearend 2013 the author will publish a mock RFI for SDN solutions that will be hosted at the author's web site (www.ashtonmetzler.com). *GottaChange* can use this document to structure a dialogue with selected vendors.

Evaluate Professional Services

Given that SDN is a new way of implementing networking, *GottaChange* may choose to use a professional services organization to help with one or more stages in the overall Plan, Design, Implement and Operations (PDIO) lifecycle. The relevant services that *GottaChange* might use could be technology centric (e.g., developing SDN designs, testing SDN solutions), organization centric (e.g., evaluating the skills of the current organization, identifying the skills that are needed and creating a way to develop those skills) or process centric; e.g., evaluating the current processes and developing new ones. These services could be light-weight (i.e., the professional services organization provides limited support) or heavy-weight. They may also be consumed just as part of an initial rollout of NV and/or SDN or they could be consumed over an extended period of time as The Company extends its deployment of NV and/or SDN.

If *GottaChange* is considering leveraging professional services from a third party, then as part of the overall evaluation process, *GottaChange* needs to evaluate the professional services that are provided, both by the potential providers of the NV and/or SDN solution as well as from independent providers of professional services.

Eliminate Organizational Resistance

Organizations tend to resist change and typically the amount of resistance is directly proportional to the extent of the change. Hence, if *GottaChange* is looking at a narrowly defined SDN solution, such as one that implements a network tap application, it can expect minimum organizational resistance. Conversely, if *GottaChange* is looking at a broadly defined SDN solution, then it must anticipate significant organizational resistance.

Organizations are particularly resistant to change if that change is likely to have a significant impact on jobs. Both NV and SDN have the potential to impact the jobs of network professionals. For example, the deployment of NV and/or SDN is likely to reduce the amount of manual labor that *GottaChange* has to perform and is likely to increase the amount of programming that *GottaChange* chooses to perform. As part of planning for NV and/or SDN, *GottaChange* needs to anticipate resistance from the network organization and respond accordingly. For example, *GottaChange* may sponsor members of its network organization achieving some of the new certifications that various NV and/or SDN vendors have recently announced.

However, a number of other factors are also impacting the jobs of IT professionals. This includes mobility, the virtualization of servers and desktops, the convergence of technologies (i.e. networks, servers, compute) and the broad and growing adoption of varying forms of cloud computing. As a result, *GottaChange's* VN and/or SDN initiatives may be just one more factor contributing to the need for *GottaChange's* IT organization to take a broad look at the skills it will need on a going forward basis and to implement a plan to develop those skills. As previously noted, *GottaChange* has the option of leveraging a professional services provider to perform a skills assessment of *GottaChange*'s IT organization.

Perform a POC

Assuming that the previous steps in their plan have produced positive results, *GottaChange* may well elect to perform a POC. The breadth of the POC is directly related to how *GottaChange* has scoped the proposed NV and/or SDN solution and the length of the POC is directly related to the criticality of the tasks that the solution is intended to support.

One goal of a POC is to determine if indeed the proposed solution works and if so, how well it performs. Another goal is to quantify the previously defined key metrics that are associated with each opportunity that *GottaChange* is hoping to address.

Obtain Management Buy-In

GottaChange's network organization needs varying levels of management buy-in at the various stages of their NV and/or SDN plan. For example, little if any management buy-in is needed just for members of *GottaChange's* network organization to attend a seminar or workshop and in many cases, little buy-in is needed in order for them to download open source solutions and to spend a modest amount of time coming to understand the functionality and the limitations of those solutions. Increasing levels of management buy-in are typically needed to engage vendors in detailed discussions of NV and/or SDN, to conduct a POC or to implement an NV or SDN solution.

GottaChange is more likely to get management buy-in if the members of the project team that is evaluating NV and/or SDN anticipate management's concerns and work to resolve those concerns over the entire planning cycle. For example, like virtually all organizations, *GottaChange* will likely face management resistance to implementing any technology or new way of delivering technology if the associated security and compliance concerns are not thoroughly addressed. In addition, *GottaChange* will likely face management resistance if any of *GottaChange's* key processes are impacted.

Like virtually all IT organizations, *GottaChange* will need to develop some form of business case to justify implementing NV and/or SDN. There are three primary components to the business case that *GottaChange* has to develop. One component is the identification and quantification of the benefits that will occur if *GottaChange* implements the proposed NV and/or SDN solution. As noted, one of the primary reasons for performing a POC is to quantify those benefits. Another component of the business case is a multi-year financial analysis that details all of the costs as well as the benefits that are associated with implementing the proposed solution. The third component of the business case is an analysis of what *GottaChange's* IT organization will do to mitigate the risk that is associated with implementing the proposed solution. In addition to mitigating the risk associated with the solution not performing well, this includes mitigating the previously mentioned concerns that management has about issues such as security, compliance and existing processes.

Summary and Conclusions

There is no doubt that over the next few years that NV and SDN will have a significant impact both on enterprise networks and on the role of network professionals. Because of that, IT organizations and IT professionals need to develop a plan to evaluate and potentially implement NV and/or SDN.

Given the embryonic and rapidly changing nature of NV and SDN, any implementation plan will likely evolve over time. The process that a company such as *GottaChange* should take to evaluate solutions and possibly implement one or more solutions should include most if not all of the following steps:

1. Define NV and SDN
2. Identify the Primary Opportunities
3. Identify the Key Metrics
4. Define the Scope of Possible Solutions
5. Evaluate NV and/or SDN Solutions
6. Test and Certify Solutions
7. Integrate with the Existing Environment
8. Educate the Organization
9. Evaluate Professional Services
10. Eliminate Organizational Resistance
11. Perform a POC
12. Obtain Management Buy-In

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.

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.

AVAYA
The Power of We™

Agile, Automated Cloud Services

Avaya's Software-Defined Data Center (SDDC) framework offers a simple five-step process for deploying cloud-based services in a matter of minutes. This framework breaks-down the frustration, complexity, and lack of agility that's typically been the norm when building and deploying business applications. Avaya replaces the complicated, independent provisioning steps between the compute, storage, and networking teams with our simplified, orchestrated, and automated workflow. With the SDDC, compute, storage, and network components are automatically combined, customized, and commissioned through a common orchestration layer.

The Avaya SDDC framework is based on the following components:

- **Avaya Fabric Connect technology** as the virtual backbone to interconnect resource pools within and between Data Centers with increased flexibility and scale
- **An Avaya OpenStack Horizon-based Management Platform**, delivering orchestration for compute (Nova), storage (Cinder/Swift) and Avaya Fabric Connect networking (Neutron)
- **Open APIs into Avaya Fabric Connect** for ease of integration, customization and interoperability with other SDN architectures

Traditional methods of configuring network, storage, and virtualized servers could take months and involve several complicated independent steps. Avaya's SDDC framework leverages OpenStack, an open-source cloud operating system. Now Data Center administrations can spin up virtual machines, assign storage, and configure networks through a single GUI. OpenStack provides a control layer that sits above all the virtualized resources within the Data Center, allowing these to be orchestrated – as a single service entity – through a set of common interfaces and a common dashboard.

Avaya Fabric Connect enhances and complements the OpenStack environment by removing the restrictions of traditional Ethernet Virtual LAN/Spanning Tree-based networks. Fabric Connect turns a complex, rigid, and un-scalable model of building network services into a dynamic, flexible, and scalable one. It facilitates the unrestricted movement of virtual machines inside the OpenStack orchestration environment, within and between Data Centers. It also enables the interconnection of old and new resources across the service chain with greater speed and agility.

In summary, with a combination of its Fabric Connect and intelligent orchestration software, based on OpenStack, Avaya is enabling simple and agile **automated** service delivery for applications and users across any combination of physical and virtual components in an evolutionary manner.

Learn more at avaya.com/sdn

Advantages of the Avaya Software-Defined Data Center Architecture

- **Reduced Time-to-Service**: Cloud services enabled in minutes, in a few simple steps.
- **Simplified Virtual Machine Mobility**: End-point provisioning to enable Virtual Machine mobility within and between geographically dispersed Data Centers.
- **Multi-Vendor Orchestration**: Coordinated allocation of compute, storage, and networking resources via a single interface to streamline the deployment of applications.
- **Openness**: APIs ease integration and customization with Fabric Connect, and interoperability with other Software-Defined Networking architectures.
- **Scale-Out Connectivity**: Services scale to more than 16 million unique services, up from the four thousand limitation of traditional Ethernet networks.
- **Improved Network Flexibility**: Overcomes the current Virtual LAN challenges to deliver a load-balanced, loop-free network where any logical topology can be built with simple end-point provisioning.

AVAYA
The Power of We™

Top 10 things you **need to know** about Avaya Fabric Connect

(An enhanced implementation of Shortest Path Bridging)

A completely new way to build networks, Avaya Fabric Connect delivers a simplified, agile and resilient infrastructure that makes network configuration and deployment of new services faster and easier. A standards-based network virtualization technology based on an enhanced implementation of IEEE 802.1aq Shortest Path Bridging and IETF RFC 6329, Avaya Fabric Connect combines decades of experience with Ethernet and Intermediate System-to-Intermediate System (IS-IS) to deliver a next-generation technology that combines the best of Ethernet with the best of IP. Avaya Fabric Connect creates a multi-path Ethernet network that leverages IS-IS routing to build a topology between nodes dynamically. Traffic always takes the shortest path from source to destination, increasing performance and efficiency.

Avaya Fabric Connect is an industry unique solution that offers a number of characteristics that set it apart from competing offers. The following Top 10 list below will give you a sneak peek of the advantages Fabric Connect offers:

1 It is more than just a Spanning Tree Replacement

Avaya's dynamic, real-time, service-based Fabric Connect technology is one of the most advanced network virtualization solution on the market today. Going beyond simple L2 multi-pathing capabilities, Avaya Fabric Connect delivers the full breadth of desired integrated services including Layer 2 virtualized services, Layer 3 virtualized services (with multiple Virtual Routing and Forwarding instances), and fully optimized routing and multicast services.

As a result, Fabric Connect enables businesses to gradually migrate away from a host of legacy overlay technologies (such as STP, OSPF, RIP, BGP and PIM) and to enable all services with a single technology – delivering unprecedented levels of network simplification.

2 It's for more than just the Data Center

While many network virtualization technologies are designed exclusively as Data Center technologies, Avaya Fabric Connect extends network-wide, providing a single service end-to-end delivery model. With Fabric Connect you can extend the power of virtualization into the campus and into geographically dispersed branch offices. Services can then easily be deployed via simple end-point provisioning where servers attach and where users attach, thereby increasing speed and agility.

3 It accelerates time-to-service through edge-only provisioning

Fabric Connect allows new services or changes to services to be implemented at the edge of the network – eliminating error-prone and time-consuming network wide configuration practices. Now, add new services or make changes to existing services in days rather than weeks or months. Fabric Connect also offers new levels of flexibility in network design. It allows any logical topology to be built, whether it is Layer 2, Layer 3, or a combination of the two – anywhere where there is Ethernet connectivity. Eliminate design constraints and have the freedom to build services wherever and whenever needed on demand.

4 It offers inherent Data Center Interconnect capabilities

Customers are demanding network virtualization solutions that are not confined to the four walls of the Data Center. Avaya Fabric Connect offers a single end-to-end service construct that can extend between multiple geographically dispersed Data Centers without requiring any overlay protocols or complex protocol stitching. This allows for resource sharing, seamless VM mobility and true active, active connectivity between Data Centers and any other Ethernet-connected enterprise location.

5 It delivers PIM-free IP Multicast that is scalable, resilient and easy to manage

IP Multicast is making a come-back. Many technologies such as next-generation video surveillance, IPTV, digital signage, desktop imaging, financial applications and some network overlays are reliant on Multicast protocols. Avaya Fabric Connect offers a scalable, reliable and efficient way of supporting IP Multicast Routing, without the onerous requirement of configuring, deploying, and maintaining a complex PIM overlay.

Imagine a Multicast network without RPF checks, rendezvous points and complex configuration. Enable Multicast at the edge of the network only, while offering increased scale and performance of the multicast applications. Eliminate your PIM induced headaches forever!

6 It offers inherent multi-tenant capabilities

Avaya Fabric Connect offers integrated Virtual Routing and Forwarding Instances. This allows for private IP networks to be set up quickly and easily across the fabric-enabled network without requiring any overlay protocols. These IP networks can reflect anything from different departments or entities in a traditional multi-tenant environment to separating different types of users (wireless guests, executive access) and even isolating traffic types for security and/or regulatory compliance (i.e. banking transactions for PCI DSS compliance, medical imaging devices in a hospital). The best part is rather than complex configuration, these isolated networks can be deployed quickly and easy at the network edges with just a couple of lines of configuration.

7 It offers “lightening fast” recovergence times (sub-second)

The elimination of overlay protocols has a profound impact on the ability for the network to reconverge. Avaya Fabric Connect customers are experiencing recovery times of less than 50 milliseconds - network-wide - for core, link, or node failures. This represents a vast improvement over large OSPF routed cores and massive improvement when compared to average recovery times in PIM-based Multicast networks.

8 It scales to 16 million unique services

Many network virtualization technologies are based on VLAN virtualization which limits them to the 4096 ceiling. Avaya Fabric Connect, based on the Shortest Path Bridging standard, utilizes a 24-bit header allowing it to scale up to 16 million unique services.

9 It offers proven interoperability with other vendors SPB implementations

Avaya is committed to delivering an open and interoperable solution to market. We have been actively participating with other vendors to demonstrate Shortest Path Bridging interoperability through a series of public tests. The most recent interoperability test was conducted at Interop 2013 in Las Vegas with major industry vendors Alcatel Lucent, HP, and Spirent.

10 It is an important foundation to your SDN strategy

When it comes to SDN, Avaya’s strategy is to first eliminate network complexity in order to provide a simple and flexible network foundation. Rather than adding overlays or additional protocols, and creating even more complexity than what we have today, Fabric Connect first streamlines the network then automates it though OpenStack-based orchestration functionality (via a Neutron plug-in). It provides a simplified and proven way to automate the service delivery process and evolve to the Software Defined Network of the future.

Learn more about Avaya Fabric Connect:
Avaya Fabric Connect - video on YouTube, Considerations for turning your network into a Fabric - Packet Pushers podcast, Network Virtualization Using Shortest Path Bridging and IP/SPB – White Paper