The 2015 Guide to SDN and NFV

Executive Summary

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

Sponsored in part by:

CISCO
Executive Summary

Software Defined Networking (SDN)

Introduction

This e-book is based in part on two surveys that were administered in September and October of 2014. One of the surveys focused on SDN and the other on NFV. Throughout this executive summary, the respondents to those surveys will be referred to respectively as The SDN Survey Respondents and The NFV Survey Respondents.

The responses to the SDN survey indicated that the general familiarity with SDN has increased significantly over the last year and that while the percentage of IT organizations that have implemented SDN in production is still small, it has increased somewhat significantly over the last year. The SDN Survey Respondents also indicated that the percentage of IT organizations who have SDN in production will likely increase somewhat over the next year, but the percentage will remain small.

The e-book identified a number of changes that have occurred with SDN over the last year. One thing that has changed is that most of the discussion around whether or not an overlay network virtualization solution is indeed SDN has gone away. Today, most IT professionals regard an overlay solution as being a form of SDN. The e-book discusses the pros and cons of the overlay and the underlay SDN models and presents market research that indicates that by a small margin that The SDN Survey Respondents believe that the underlay model will provide more value over the next two years.

Another change that has occurred in the SDN landscape within the last year is that the Open Networking Foundation (ONF) established the Northbound Interface (NBI) working group with the goal of eventually standardizing SDN’s northbound interface. Sarwar Raza, the chairman of the working group, is quoted as saying that standardization was not a short term goal of the group and that “Our goal in the next year is to formalize the framework along with the information and data models and then iterate some with code before we even start a standards discussion.” The NBI working group intends to work with one or more open source initiatives to develop working code for the NBIs and the group aims to work on standardization at an appropriate time in the future.

Another change in the SDN landscape that is discussed in the e-book is that in February 2014 the OpenDaylight community issued its first software release, called Hydrogen and in September 2014 issued its second software release called Helium. A number of vendors have announced their intention to use the OpenDaylight solution as the basis of their SDN controller. This creates the potential for SDN solutions based on OpenDaylight solutions to reach critical mass in the near term and hence accelerate the adoption of SDN.

The majority of The SDN Survey Respondents indicated that they thought that SDN and NFV are complimentary activities and a quarter of the respondents indicated that they thought that in at least some instances that NFV requires SDN. That second school of thought is in line with the ONF who in March of 2014 published a white paper that included uses cases that the ONF believes demonstrate how OpenFlow-enabled SDN can meet the need for automated, open, and programmable network connectivity to support NFV.
SDN Use Cases

The SDN Survey Respondents indicated that a wide range of factors were driving their interest in SDN including the desire to better utilize network resources and to perform traffic engineering with an end-to-end view of the network. However, very few of the respondents indicated that they thought that SDN would help them reduce CAPEX or reduce complexity. The SDN Survey Respondents also indicated that a wide range of factors were inhibiting their interest in SDN. Some of the inhibitors to SDN adoption, such as the immaturity of current products and the immaturity of enabling technologies, will naturally dissipate over time. However some of the key inhibitors, such as the lack of a compelling business case, need to be addressed or they will continue to impede SDN adoption.

The SDN Survey Respondents indicated that over the next two years that the primary focus of their SDN deployment will likely to be in the data center. However, they expressed considerable interest in deploying SDN in the WAN as well as in branch and campus networks. In addition, when asked to look forward three years, The SDN Survey Respondents indicated that three years from now that they will have deployed SDN pervasively in their data centers and that they will also have made significant SDN deployment both in their WAN and in their campus networks.

The e-book discussed a number of SDN use cases. The WAN use case that was discussed was how Google has deployed SDN to connect its data centers and as a result of that deployment, has driven its network utilization to 95%. The campus use cases that were discussed were:

- Dynamic QoS and traffic engineering;
- Unified wired and wireless networks;
- QoS management for Microsoft Lync across wired and wireless networks;
- Personal Bonjour;
- Roll based access.

The data center use cases that were discussed were:

- Virtual machine migration;
- Service chaining;
- Security services;
- Load balancer services;
- Software defined clouds;
- Cloud hosting.

The Operational Implications

Thirty five percent of The SDN Survey Respondents indicated that SDN will enable them to implement more effective security functionality and 12% of The SDN Survey Respondents indicated that concerns about possible security vulnerabilities is a significant inhibitor to SDN deployment. As the e-book discusses, one of the ways that SDN can enhance security is by implementing security services on OpenFlow-based access switches that can filter packets as they enter the network. Another such example is role based access that is implemented by deploying a role-based resource allocation application that leverages the control information and capability of the SDN controller.
The e-book discusses some of the security challenges including:

- The centralized controller emerges as a potential single point of attack and failure that must be protected from threats.
- The southbound interface between the controller and underlying networking devices is vulnerable to threats that could degrade the availability, performance, and integrity of the network.

The e-book describes OpenStack and points out that orchestration engines such as OpenStack are important to both SDN and NFV. As explained in the e-book, in conjunction with the orchestration engine, the role of the SDN controller is to translate the abstract model created on the orchestration engine into the appropriate configuration of the virtual and physical resources that will deliver the desired service. For example, the orchestration engine can instruct the controller to perform a variety of workflows including:

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

In spite of the importance of orchestration, only a small minority of The SDN Survey Respondents indicated that their organization had a well thought out strategy for how they would do orchestration.

Similar to the situation with security, the e-book shows how management is a double edged sword. Fifty three percent of network organizations believe that SDN will ease the administrative burden of management tasks such as configuration and provisioning while 13% of network organizations believe that concerns about how to manage SDN is a significant inhibitor to SDN deployment.

The e-book highlights the fact that in SDN environments the challenges associated with end-to-end service performance management are more demanding than they are in traditional network environments. Some of the reasons for that are that in an SDN environment:

- The combination of physical and virtual infrastructure and dynamically changing resources requires a more holistic approach to instrumentation, consolidation of individual datasets, and analysis of the consolidated dataset in a service contextual fashion.
- The SDN controller needs to be instrumented and monitored just as any other application server and the southbound protocol needs to be monitored the same way as any other protocol.
- Network management organizations need tools that enable them to be able to dynamically discover, procure, allocate and reconfigure resources.
- Network management organizations need to be able to perform a two-way mapping between an application or service and all of the virtual services that support it and they must be able to perform a two-way mapping between the virtual services that support a given service or application and the physical infrastructure that supports them.

The e-book positions SDN as being a part of a broader movement to implement all IT functionality in software, referred to as Software Defined Everything (SDE) and points out that the adoption of an SDE approach is causing the role of network and IT infrastructure professionals to change. Some of the key characteristics of the emerging roles are:
• An increased knowledge of other IT disciplines;
• More focus on setting policy;
• More knowledge of the business;
• More understanding of applications;
• More emphasis on programming.

The Survey Respondents were asked how they thought that the SDE movement would likely impact their organization. Their answers included:

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

The Survey Respondents were also asked how they thought that the SDE movement would likely impact their jobs. Their answers included:

• The way to design, implement and troubleshoot networks will change a lot;
• The job will require new skill sets in general and more programming knowledge in particular;
• There will be new security requirements;
• New architectures will need to be developed;
• There will be a lot of re-training and re-trenching.
Network Functions Virtualization (NFV)

Introduction

NFV is being driven by a number of different types of players who are described in the e-book. This includes industry organizations such as the TM Forum and ETSI, open source communities such as OPNFV and traditional standards development organizations such as IETF.

As described in the e-book, early in 2014 the TM Forum announced its Zero-touch Orchestration, Operations and Management (ZOOM) project. According to the Forum, the goal of Zoom is to define a vision of the new virtualized operations environment and a management architecture based on the seamless interaction between physical and virtual components that can easily and dynamically assemble personalized services. As of November 2014, the ZOOM team has delivered an assessment of how virtualization impacts SLAs and is currently working on information and policy models, NFV preparedness, and a set of operational support system (OSS) design principles needed for NFV adoption to become widespread.

The ETSI NFV ISG has identified nine NFV use cases and is currently driving 25 POCs. The ETSI NFV ISG was established with a two year life span that expires in January 2015. In late July and early August 2014 the NFV ISG met in Santa Clara, CA. At that meeting the primary objectives of NFV Phase 2 were identified. Whereas ETSI characterizes Phase 1 as being the Requirements Phase, ETSI characterizes Phase 2 as being the Implementation Phase. The objectives of Phase 2 include building on the achievements that were made in the first two years of the ISG and consist of an enhanced focus on interoperability, formal testing, as well as working closer with projects developing open source NFV implementations. In addition, the NFV ISG also released nine draft NFV documents for industry comments and published a publically available document that summarizes the key concepts that are contained in those documents.

In September 2014 the Linux Foundation announced the founding of the Open Platform for NFV Project (OPNFV). As part of the announcement the Linux Foundation declared that OPNFV will establish a carrier-grade, integrated, open source reference platform that industry peers will build together to advance the evolution of NFV and ensure consistency, performance and interoperability among multiple open source components. The Foundation also stated that because multiple open source NFV building blocks already exist, OPNFV will work with upstream projects to coordinate continuous integration and testing while filling development gaps.

Although their efforts are just getting started, the IETF can be expected to play a significant role in the evolution of standards for SDN and NFV. For example, the IETF Service Function Chaining (SFC) Work Group (WG) currently has over forty active Internet drafts on the topic of delivering traffic along predefined logical paths incorporating a number of service functions. As described in one of those Internet drafts, the basic concept of SFC is similar to ETSI NFV ISG’s Virtualized Network Function (VNF)-Forwarding Graphs.

In spite of the fact that the vast majority of The NFV Survey Respondents believe that NFV is applicable in both an enterprise and a service provider environment, only a modest number of IT organizations have implemented NFV in a production network. However, driven primarily by the belief that NFV will enable them to reduce the amount of time it takes to deploy new services, a large percentage of IT organizations are currently in varying stages of analyzing NFV.
The NFV Survey Respondents indicated that the primary impediments that would keep their organization from broadly implementing NFV are:

- Concerns about end-to-end provisioning;
- The lack of a compelling business case;
- The immaturity of the current products.

**Use Cases and Proof of Concept (POC)**

The e-book discusses some of the use cases and POCs being sponsored by ETSI and by the TM Forum. The ETSI use cases are:

- **NFV Infrastructure as a Service (NFVIaaS)**
  NFVIaaS is analogous to a cloud IaaS that is capable of orchestrating virtual infrastructures that span a range of virtual and physical network, compute, and storage functions.

- **Virtual Network Functions as a Service (VNFaaS)**
  Many enterprises are deploying numerous network service appliances at their branch offices; e.g., access routers, WAN optimization controllers, stateful firewalls and intrusion detection systems. Virtual Network Functions delivered as a Service (VNFaaS) is an alternative solution for enterprise branch office networks whereby VNFs are hosted on servers in the network service provider’s access network PoP.

- **Virtualization of the Home Environment (VoHE)**
  Virtualization of the Home Environment is analogous to VNFaaS. In this case the residential gateway (RGW) and the set top box (STB) are virtualized as VNFs residing on servers in the network service provider’s PoP.

- **VNF Forwarding Graph (FG)**
  IT organizations need to be able to orchestrate and manage traffic flows between virtualized service platforms (e.g., VNFs) and physical devices in order to deliver a complete service to the end user.

  The VNF Forwarding Graph (VNF FG) is a service that provides flow mapping (a.k.a., service stacking or chaining) from a management and orchestration system that may or may not be part of an SDN infrastructure.

- **Virtual Network Platform as a Service (VNPaaS)**
  VNPaaS is similar to an NFVIaaS that includes VNFs as components of the virtual network infrastructure. The primary differences are the programmability and development tools of the VNPaaS that allow the subscriber to create and configure custom ETSI NFV-compliant VNFs to augment the catalog of VNFs offered by the service provider.

- **Virtualization of Mobile Core Network and IP Multimedia Subsystem**
  The 3GPP is the standards organization that defines the network architecture and specifications for Network Functions (NFs) in mobile and converged networks. Each NF typically is run on a dedicated appliance in the mobile network PoP. Running the NFs as VNFs on virtualized industry standard servers is expected to bring a number of benefits in terms of CAPEX, OPEX, as well as flexibility and dynamic scaling of the network to meet spikes in demand.
• **Virtualization of the Mobile Base Station**
  3GPP LTE provides the Radio Access Network (RAN) for the Evolved Packet System (EPS). There is the possibility that a number of RAN functions can be virtualized as VNFs running on industry standard infrastructure.

• **Virtualization of Content Delivery Networks (CDNs)**
  Some ISPs are deploying proprietary CDN cache nodes in their networks to improve delivery of video and other high bandwidth services to their customers. Cache nodes typically run on dedicated appliances running on custom or industry standard server platforms. Both CDN cache nodes and CDN control nodes can potentially be virtualized.

• **Virtualization of Fixed Access Network Functions**
  NFV offers the potential to virtualize remote functions in the hybrid fiber/copper access network as well as PON fiber to the home and hybrid fiber/wireless access networks. In a DSL access network some of the functions that can potentially be virtualized include the DSLAM and Message Display Unit (MDU) forwarding functions, while control functions remain centralized at the central office.

The POCs that are being driven by the TM Forum that are discussed in this e-book are:

• **Closing the Loop: Data-driven network performance optimization for NFV & SON**
  In this context closing the loop means collecting and analyzing data to identify how the network can be optimized and then implement those changes. This POC showed how network operators can use Self-Organizing Networks (SON) and Network Functions Virtualization (NFV) in tandem to automate closing the loop and improve performance for customers.

• **CloudNFV: Dynamic, data-driven management and operations Catalyst**
  This POC builds on TM Forum’s Information Framework to create a meta-data model using active virtualization, a term coined by the CloudNFV™ consortium. The specific challenge this POC is addressing is that without these connections, services like dynamic quality of service likely won’t work at scale.

• **Orchestrating Software-Defined Networking (SDN) and NFV while Enforcing Service Level Agreements (SLAs) over Wide Area Networks (WANs)**
  One set of challenges that this POC addressed are the challenges that service providers face when offering private clouds to enterprises and managing SLAs in a virtualized environment. Another set of challenges are the challenges that geographically diversified enterprises encounter when integrating data centers.

• **Service bundling in a B2B2X marketplace**
  This POC showed how a buyer can bundle a collection of services sourced from different suppliers and deliver them seamlessly to a customer in a business-to-business or business-to-business-to-consumer arrangement. These components could include traditional network access products, as well as NFV and infrastructure-as-a-service products.
The Operational Implications

The majority of The NFV Survey Respondents indicated that they believe that even if a NFV-related POC is successful, it will take between a significant and a tremendous amount of effort to broadly implement that solution in production. One of the operational challenges that can make it difficult to move from POC to production is performance. As discussed in the e-book, in order to move VNFs into production, it must be possible to achieve the same or greater performance in a software-based environment as is possible in a traditional hardware-based environment. However, that isn’t possible without an enabling software architecture because of the bottlenecks that are associated with the hypervisors, virtual switches and virtual machines that are the foundation of the emerging software-based approach to IT.

The adoption of NFV poses a number of other significant challenges that must be overcome in order to ensure the ability to continue to implement effective end-to-end management. These challenges include:

- **Dynamic relationships between software and hardware components.** With NFV, software running on virtual machines (VMs) can readily be moved among physical servers or replicated to run on newly created VMs in order to dynamically maintain availability, expand/shrink capacity, or balance the load across physical resources.

- **Dynamic changes to physical/virtual device configurations.** To accommodate the dynamic nature of virtualized networks, end-to-end management systems will need to be able to adjust the configuration of devices to react to changing conditions in the network.

- **Many-to-Many relationships between network services and the underlying infrastructure.** In a virtualized infrastructure a network service can be supported by a number of VNFs which may be running on one or several VMs. A single VNF may also support a number of distinct network services. In addition, the group of VNFs supporting a single network service could possibly be running on a number of distinct physical servers.

- **Hybrid physical/virtual infrastructures.** As virtualization is gradually adopted, service providers will need to be able to integrate virtual environments into their existing end-to-end traditional/legacy monitoring infrastructures.

- **Network services spanning multiple service providers.** Some of the VNFs comprising a virtualized network service may be hosted in the clouds of multiple collaborating providers.

- **IT and Network Operations collaboration.** These organizations will need to cooperate effectively to establish new operational processes that meet the demands of end-to-end management of hybrid physical/virtual infrastructures.

Roughly a third of IT The NFV Survey Respondents believe that over the next two years that the adoption of NFV is likely to have a significant or very significant impact on the structure of their organization. When asked what type of changes they expected, a number of The NFV Survey Respondents commented that it would require them to change how they implemented SLAs, how they developed a business case and it would cause them to rethink their business models. Other comments included:

- We will need to adopt a new approach to service provisioning and management;
• It will cause us to consolidate our physical platforms;
• It will change how we do network planning;
• We will need to determine how we are going to orchestrate end-to-end systems.

Almost half of The NFV Survey Respondents indicated that over the next two years that the adoption of NFV will likely have a significant or very significant impact on the skill base of IT professionals. When asked to indicate the type of impact, the answers included:

• We will need to know multiple technologies;
• We will need to think in software and end-to-end terms rather than in component terms;
• It will require the skills to drive the integration between legacy equipment and management systems and NFV management systems;
• We will need to modify our change management, incident and problem management processes.

An additional hurdle that has to be overcome before the full benefits of NFV can be realized is that IT organizations must take a DevOps-like approach to network operations. The e-book describes the key principles that characterize DevOps and also describes how a DevOps approach has to be modified in order to be applied to network operations.
The SDN and NFV Ecosystem

The e-book identifies the primary classes of vendors that either currently do, or can be expected to provide either parts or all of a SDN solution. Included in the discussion is the value proposition of this class of vendor as well as a set of representative vendors. The classes of SDN vendors included in the e-book are:

- Merchant Silicon/Chip Vendors;
- HyperScale Data Centers;
- Telecom Service Providers;
- Switch Vendors;
- Network and Service Monitoring, Management and Automation;
- Providers of Network Services;
- Testing Vendors and Services;
- Standards Bodies and Related Communities;
- Providers of SDN Controllers;
- Providers of Telcom Service Provider's Infrastructure/ Optical Networking;
- Server Virtualization Vendors.

The e-book also identifies the primary classes of vendors that either currently do, or can be expected to provide either parts or all of a NFV solution. Included in the discussion is the value proposition of this class of vendor as well as a set of representative vendors. The classes of NFV vendors included in the e-book are:

- Telecom Service Providers;
- Merchant Silicon/Chip Vendors;
- Network Systems and Electronic Equipment Vendors;
- Virtualized Network Service and Cloud Service Vendors;
- SDN Controller Software Vendors;
- NFVI Providers;
- Orchestration Software Vendors;
- Network Monitoring, Management and OSS/BSS Vendors;
- Hypervisor Vendors;
- Test Equipment Vendors and Test Services;
- Standards Bodies and Related Communities.
About the Webtorials® Editorial/Analyst Division

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

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

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.
Cisco ACI: An Application Centric Approach to SDN

IT Trends and the Advent of Software Defined Networking
IT departments and lines of business are looking at cloud automation tools and software-defined networking (SDN) architectures to accelerate application delivery, reduce operating costs, and increase business agility. The success of an IT or cloud automation solution depends largely on the business policies that can be carried out by the infrastructure through the SDN architecture.

The emergence of SDN promised a new era of centrally managed, software-based automation tools that could accelerate network management, optimization, and remediation. Gartner has defined SDN as “a new approach to designing, building and operating networks that focuses on delivering business agility while lowering capital and operational costs.” (Source: “Ending the Confusion About Software-Defined Networking: A Taxonomy”, Gartner, March 2013)

The Cisco Application Centric Infrastructure (ACI) architecture, Cisco’s expanded vision of SDN that encompasses the entire data center infrastructure, supports a more business-relevant application policy language than alternative software overlay solutions or traditional SDN designs. What makes the Cisco SDN policy model application-centric? And what are the benefits? First we need a comparison of ACI to traditional SDN designs.

A Comparison of ACI to Traditional SDN Architectures
Although traditional SDN and Cisco ACI have important differences, both have essentially the same architectural components and concepts for policy-based IT infrastructure automation:

- A centralized policy store and infrastructure controller: In SDN and Cisco ACI, this feature is generally known as the controller (Cisco Application Policy Infrastructure Controller [APIC] for Cisco ACI).
- Programmable, or automated, network devices: All infrastructure devices, such as switches, application delivery controllers and firewalls, must be able to respond to and implement policies according to commands from the controller. This feature may involve agents running on the device, APIs in the devices themselves, or management hooks to the devices that are implemented in the controller.
- A controller southbound protocol to communicate with the managed or controlled devices and to communicate policy information: Initially, the OpenFlow protocol was used in SDN architecture, and vendors released OpenFlow-compliant switches. In Cisco ACI, OpFlex is the primary protocol used, although other mechanisms for integrating devices into the Cisco ACI policy model are supported.
- Northbound controller interfaces for integrating higher-level automation solutions on top of the policy and controller framework, including workflow automation tools and analytics: Modern SDN controllers, as does Cisco APIC, include northbound APIs allowing for the integration of OpenStack or other vendor-specific cloud automation tools (e.g., Cisco UCS Director).
What's unique about ACI is that the policy language (the rules that tell your cloud infrastructure what to do) is not modeled on arcane networking concepts like VLAN's and IP addresses, but on application requirements, and especially how application workloads can and can't communicate, and what kind of services they are entitled to. Policies are applied to classes of applications or workloads (e.g., the web tier of an application), also called endpoint groups (EPG), which can be either physical or virtual workloads (or containers).

An application policy will consist of the EPG’s that make up the application, and the contracts and services between the EPG’s. This is fundamentally all we need to automate the deployment, provisioning and optimization of our application network anywhere, on any cloud resources we want.

The result is an SDN-automated infrastructure that extends beyond just network devices, to include layer 4-7 application services like load balancers, as well as security devices and policies for IPS and firewall components. Because applications are the best reflection of business activity, an application-centric policy is ideal to align IT with business policies, and to automate policies that reflect real business and application requirements.

Figure – Cisco ACI provisions the entire network infrastructure through application polices managed in a centralized SDN controller, the APIC.

For More Information

For more information, please visit http://cisco.com/go/aci.

For More Information