SDN 101: An Introduction to Software Defined Networking

CITRIX®

Over the last year, the hottest topics in networking have been software defined networking (SDN) and Network Virtualization (NV). 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 this white paper is to eliminate that confusion. In order to accomplish that goal, this white paper will put SDN into the context of a broad movement to have more of a focus on software based solutions and it will identify the key opportunities that SDN can address. This white paper will also discuss both SDN and NV and will describe the relationship between these two emerging approaches to networking.

Background

Traditional Data Network

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 than is possible with the traditional approach to networking. 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 ASICs and the vendors of the network appliances; has a relatively high level of OPEX and is relatively static in nature. SDN holds the promise of overcoming those limitations.

The Shift to Software

As noted, the traditional data network has been largely hardware-centric. However, over the last few years the adoption of virtualized network appliances and the burgeoning interest in software defined data centers (SDDCs) have lead a movement towards an increased reliance on software-based network functionality. For example, in the mid to late 2000s, network appliances such as WAN Optimization Controllers (WOCs) and Application Delivery Controllers (ADCs) were purpose-built, hardware appliances. That means that functions such as encryption/decryption and the processing of TCP flows were performed in hardware that was designed specifically for those functions. Driven largely by the need for increased agility, it is now common to have WOC or ADC functionality provided by software running on a general purpose server or on a VM.

A SDDC can be looked at as the complete opposite of the traditional data center network that was previously described. For example, one of the key characteristics of a software-defined data center is that all of the data center infrastructure is virtualized and delivered as a service. Another key characteristic is that the automated control of data center applications and services is provided by a policy-based management system.

Possible Opportunities

One of the characteristics that is often associated with any fundamentally new approach to technology is that there is confusion about the opportunities that can be addressed by that new approach. In order to successfully evaluate and adopt a new approach to technology such as SDN, IT organizations need to identify which opportunity or opportunities that are important to the organization are best addressed by that new approach.

After all of the SDN-related discussions that have occurred over the last couple of years, the following have emerged as the most likely set of opportunities that SDN can address.

- Support the dynamic movement, replication and allocation of virtual resources;
- Ease the administrative burden of the configuration and provisioning of functionality such as QoS and security;

- More easily deploy and scale network functionality;
- Perform traffic engineering with an end-to-end view of the network;
- Better utilize network resources;
- Reduce OPEX;
- Have network functionality evolve more rapidly based on a software development lifecycle;
- Enable applications to dynamically request services from the network;
- Implement more effective security functionality;
- Reduce complexity.

Software Defined Networking

The Open Networking Foundation (ONF) is the group that is most associated with the development and standardization of SDN. According to the ONF[1], "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.

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

Figure 1 contains a graphical representation of the SDN architecture as envisioned by the ONF.

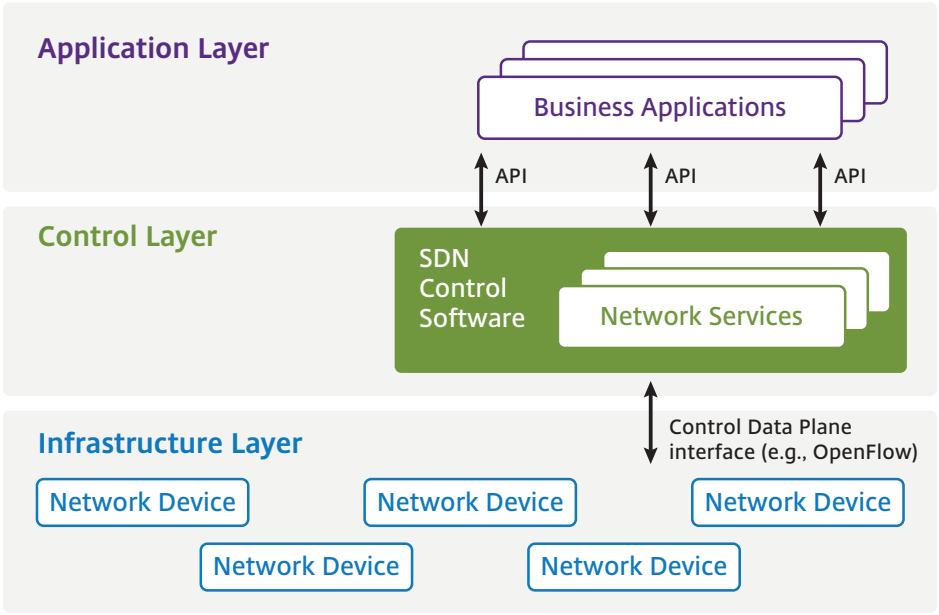

Figure 1: The SDN System Architecture
Source: ONF

Below is a description of some of the key concepts that are part of the SDN system architecture that is shown in Figure 1.

Business Applications

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

Network & Security Services

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

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. 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.

Northbound API
Relative to Figure 1, the northbound API is the API that enables communications between the control layer and the business application layer. There is currently not a standards-based northbound API.

Southbound API
Relative to Figure 1, the southbound API is the API that enables communications between the control layer and the infrastructure layer. Protocols that can enable this communications include OpenFlow, the extensible messaging and presence protocol (XMPP) and the network configuration protocol.

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 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 disagreement relative to what constitutes the infrastructure layer. To the ONF, the infrastructure layer is a broad range of physical and virtual switches and routers. As described below, one of the current approaches to implementing network virtualization relies on an architecture that looks similar to the one shown in Figure 1, but which only includes virtual switches and routers.

Network Virtualization

Network virtualization isn't a new topic as network organizations have a long history implementing techniques such as virtual LANs (VLANs), virtual routing and forwarding (VRF) and virtual private networks (VPNs). However, throughout this white paper, the phrase *network virtualization* refers to the capability shown in the right half of Figure 2. In particular, network virtualization refers to the ability to provide end-to-end networking that is abstracted away from the details of the underlying physical network in a manner similar to how server virtualization provides compute resources that are abstracted away from the details of the underlying x86 based servers.

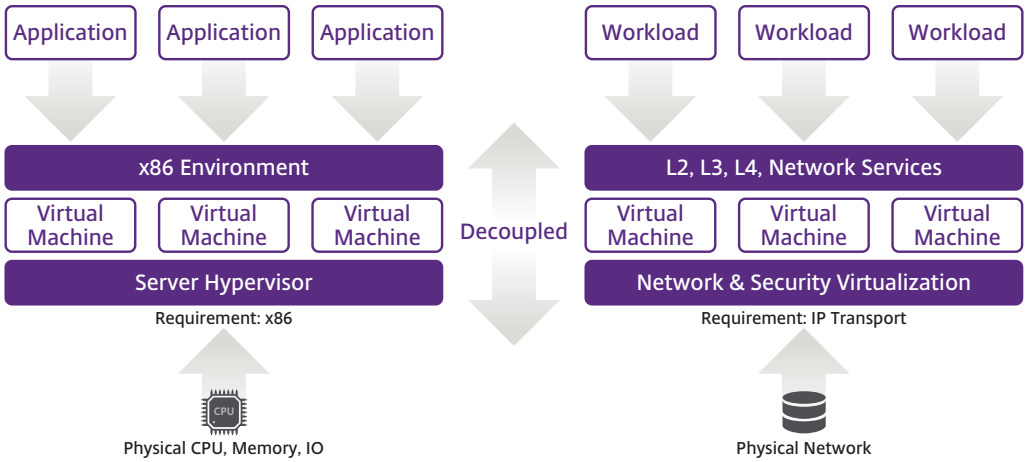

Figure 2: Network Virtualization
Source: VMware

One way to implement network virtualization is as an application that runs on a SDN controller, leverages the OpenFlow protocol and defines virtual networks based on policies that map flows to the appropriate virtual network using the L1-L4 portions of the header. This approach is often referred to as fabric-based network virtualization.

Another way to implement network virtualization is to use encapsulation and tunneling to construct multiple virtual network topologies overlaid on a common physical network. This approach is often referred to as overlay-based network virtualization. IT organizations have been implementing network virtualization via overlays for the last few years based on protocols such as VXLAN. However, the initial wave of these solutions didn't feature a controller. Since these controller-less solutions typically used flooding as a way to disseminate information about the end systems, these solutions didn't scale well.

Figure 3 shows a more recent approach to implementing network virtualization. This approach features a controller and has an architecture similar to the one shown in Figure 1 except that the network elements are either vSwitches or vRouters. One of the primary roles of the controller in Figure 3 is to provide tunnel control plane functionality. This functionality allows the ingress device to implement a mapping operation that determines where the encapsulated packet should be sent to reach its intended destination VM.

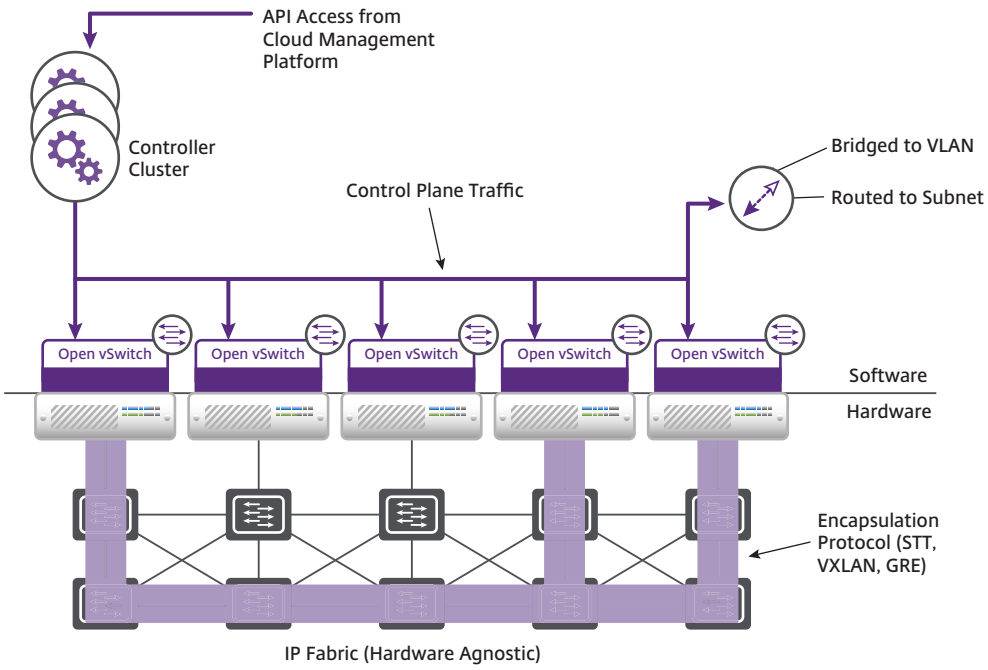

Figure 3: Overlay-Based Network Virtualization
Source: VMware

In the approach to network virtualization that is shown in Figure 3, a virtual network 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 header includes a field that is generally 24 bits in length and these 24 bits can be used to identify roughly 16 million virtual networks. However, practical limits are often in the range of 16,000 to 32,000 virtual networks. In the approach shown in Figure 3, virtualization is performed at the network edge, while the remainder of the physical L2/L3 network remains unchanged and doesn't need any configuration modifications in order to support the virtualization of the network.

The primary benefit of an overlay-based network virtualization solution is that it provides support for virtual machine mobility independent of the physical network. If a VM changes location, even to a new subnet, the switches at the edge of the overlay simply update their mapping tables to reflect the new location of the VM.

Summary

While a SDN is comprised of many enabling technologies, SDN is not a technology, but an architecture. Whether it is fabric or overlay-based, network virtualization can be viewed as a SDN application. The primary benefit of a network virtualization solution is that it provides support for virtual machine mobility independent of the physical network. SDN, however, has other potential benefits including easing the administrative burden of provisioning functionality such as QoS and security.

While some of the characteristics of a SDN, such as the increased reliance on software, are already widely adopted in the marketplace, vendors have only recently begun to ship SDN solutions and SDN adoption is just beginning. Given all of the potential benefits that SDN is likely to provide, IT organizations need to develop a plan for how they will evolve their networks to incorporate SDN. Chapter 4 of The 2013 Guide to Network Virtualization and Software Defined Networking outlines such a plan[2].

For more information visit: citrix.com/sdn

[2] http://www.webtorials.com/content/2014/01/2013-guide-to-network-virtualization-sdn-3.html

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com