Utilizing Software Defined Network to Ensure Agility in IT Service Delivery
Siddhesh Rane

Siddhesh Rane is a Technical Architect and part of the Software Defined Infrastructure (SDI) CoE team of the IT IS Converged Network Service (CNS) group at Tata Consultancy Services (TCS). With more than eight years of experience in the domain, Siddhesh has anchored several cloud solution implementations, and has worked as a consultant for infrastructure transformations for leading global enterprises. He has been closely involved in planning, designing, and implementation of network solutions for TCS’ clients across industries.
For enterprise architecture, most organizations focus on virtualization with two main objectives: efficient use of infrastructure and automated provisioning of application services. In traditional architecture, there is significant reliance on the IT team and several deployment cycles are required for provisioning application services. Virtualization in compute and storage domains has been shown to greatly improve the use of physical resources, but the dependence on physical network infrastructures still remains.

This white paper proposes a roadmap for IT organizations to adopt the Software Defined Network (SDN) technology. We also discuss some aspects that IT organizations need to consider while selecting an SDN solution from the ones available in the market.
## Contents

1. Overview 5
2. Business Challenges in a Complex IT Environment 5
3. How SDN Works 5
4. SDN Implementation Benefits in Enterprises 7
5. Adopting SDN for Greater Network Programmability 10
6. Conclusion 11
Overview

Most organizations have embraced storage and compute virtualization, enabling automated workload provisioning. However, these workloads still rely heavily on the rigid manual provisioning of network infrastructure, with the presence of a non-virtualized physical network layer. Software Defined Network (SDN) technology allows enterprises to create a flexible infrastructure that facilitates greater control over the network—with on-demand provisioning of networks and services—and ensures increased automation and IT agility.

Business Challenges in a Complex IT Environment

Accommodating application-related changes within legacy systems is a key limitation for most enterprises today. Manual configurations are required at multiple instances within the existing infrastructure, resulting in delayed provisioning of business applications and services, and lengthy application deployment cycles. The key challenges are:

Managing multiple stakeholders and addressing interdependencies in application deployment: The process for deploying infrastructure applications involves coordination among various domain-specific teams—compute, network, storage, UNIX, and data backup and recovery—often resulting in delayed application provisioning. For any infrastructure application deployment, the application team—providing server, network, and storage details—awaits infrastructure readiness, and is required to coordinate with other infrastructure teams, while creating an application.

Inefficient handling of network service chaining: Network services such as firewall, load balancing, and intrusion prevention systems (IPS) have to be manually configured as they are static in nature. They have to be pre-provisioned and cannot be deployed as per demand, based on application needs.

How SDN Works

Compute, network, and storage are the basic building blocks for creating business applications and services in existing data center infrastructures. In recent years, virtualization has mainly affected compute and storage resources, with only minor network virtualization features such as VLAN and VRF. Accommodating changes in applications within an inflexible infrastructure is difficult in the tightly integrated control and data planes in network devices. Non-virtualized network infrastructure prevents enterprises from harnessing the true potential of virtualization, automation, and quicker service deployment.

The SDN framework offers optimized, centralized, and programmable networks to enable agile enterprise computing. Virtualization of resources results in faster provisioning, increased uptime, and easy isolation of applications from physical hardware, as well as simplified workload movement on the cloud platform.

SDN works on the principle of decoupling of control and data planes. The control plane is centralized, whereas the data plane remains distributed in the network infrastructure. To efficiently configure and manage all network devices from a single console, a centralized control plane is used, while the data plane on each device is freed to provide optimized packet processing at high speeds.
SDN solutions integrate seamlessly with the cloud-orchestration tool to ensure:

- Automation in the data center
- Creation of a hybrid cloud
- Self-service catalogue based portal
- Multi-tenancy

The SDN controller uses northbound application programming interface (API) to interact with the application or orchestration layer, and southbound API for the underlay network.

SDN development started with the OpenFlow protocol in early 2007. The standard is now being defined by the Open Network Foundation (ONF). Different original equipment manufacturers (OEMs) started working on respective SDN solutions with underlay network supporting OpenFlow protocol. After OpenFlow, an overlay-based approach that operated independently was developed.

SDN deployment models (depicted in Figure 1) can be broadly categorized into the following:

**OpenFlow-based SDN:** As shown in Figure 1, OpenFlow protocol is used between a controller and a switch, this model is suitable for small to mid-scale deployments, new deployments, and instances where the existing infrastructure supports OpenFlow.

**Overlay-based SDN:** This model leverages the existing physical network, and the overlay is created using virtual switches inside hypervisors that set up tunnels in the underlying physical network. It operates irrespective of the hardware configuration and does not depend on the underlying network. There are two variants of overlay based SDN—hardware-based and software-based. Both types of overlay-based tunnels are shown in the Figure 1.

Hardware-based overlay is recommended in a heterogeneous compute environment, where there are multiple physical servers, or where visibility is required in the physical switching infrastructure. Software-based overlay is recommended when virtualization at the compute layer is at a minimum of 70 percent, physical servers are lesser as compared to the virtual environment, or in a non-heterogeneous environment.

Figure 1: SDN Deployment Models
SDN Implementation Benefits in Enterprises

SDN benefits organizations across industries like banking and financial services, insurance, telecom and IT services, government, and retail, by improving automation and reducing deployment cycles and configuration complexity.

Figures 2 and 3 depict the differences between traditional network architecture and software defined architecture. Provisioning requires corresponding changes in the overall infrastructure at multiple points, and the resultant manual interventions cause delays. SDN ensures automatic provisioning of network and single-pane configuration of multiple devices for new application or additional workload provisioning and up-scaling or down-scaling.
SDN is driven by:

Network Function Virtualization (NFV): NFV involves the abstraction of hardware appliance capabilities into software. Multiple physical hardware components or devices require more power, cooling, rack space, cabling cost, and more resources. Figure 4 illustrates how NFV technology routers, firewalls, and load balancers can be used as virtual appliances, thereby reducing operational overheads. Predominantly used in the telecom sector, NFV can also drive service component virtualization in data centers.

Service chaining: Load balancing and security services are key requirements for application deployment in data centers. Three-tier architectures require network administrators to manually redirect traffic between web, apps, and database zones through firewall and load balancers, and configure load balancing and security policies. Based on the number of application workloads, the corresponding changes in network devices take more time and effort, and are prone to human errors. Moreover, during periods of maintenance, replacement, or hardware appliance upgrades, the network administrator might be required to manually redirect traffic on redundant components—causing human-error related service disruptions.

An SDN controller can automate service chaining, thereby reducing the overall effort involved. After defining the workflow for traffic flow, the SDN controller communicates with the orchestration tool to create a virtual instance of the required service, for example, router, load balancer, and firewall. The SDN controller also defines and implements the load balancing and security policies for that traffic flow.

Using SDN, service components can be provisioned on demand. As shown in Figure 5, the cloud administrator can connect to an SDN controller and create a service instance for firewall and load balancer, along with the required policies. In case of malfunctioning components, SDN controllers can easily provision and replace the component with other virtual instances.
Multi-tenancy in data centers: SDN can create a secure multi-tenant environment as depicted in Figure 6. Separate tenants are created for each customer in the orchestration tool or SDN controller, and each tenant is associated with a separate virtual network, topology, and service chaining.
Stretched network across data centers: During disaster recovery, it is necessary to have infrastructure readiness when any application moves across the data center. SDN technology can ‘stretch’ the network by extending the logical domain across data centers, and the virtual workload can be easily moved to other data centers along with the corresponding network profile. It is also possible to have inter-data center communication by clustering the controllers across data centers.

Networking vendors such as Cisco, Juniper, VMware, HP, and Brocade offer unique SDN solutions that integrate effortlessly with the existing network infrastructure. Table 1 shows a comparison of SDN solutions.

### Table 1: Differentiating Features of Multi-vendor SDN solutions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Cisco (ACI)</th>
<th>VMWare (NSX)</th>
<th>Juniper (Contrail)</th>
<th>HP VAN SDN Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overlay or OpenFlow based</td>
<td>Overlay</td>
<td>Overlay</td>
<td>Overlay</td>
<td>OpenFlow</td>
</tr>
<tr>
<td>Heterogeneous environment support for multi-hypervisor</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Software or Hardware based overlay</td>
<td>Hardware</td>
<td>Software</td>
<td>Software</td>
<td>Hardware</td>
</tr>
<tr>
<td>Can work with Physical Workloads (x86)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dependency on underlying network infrastructure</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Any changes required in current network infrastructure for solution support</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Supports only Openflow enabled switches</td>
</tr>
</tbody>
</table>

Adopting SDN for Greater Network Programmability

SDN offers several benefits to users, including:

Faster application provisioning: The deployment cycle (for new services or applications, or changes in application) is drastically reduced with the adoption of SDN. In traditional infrastructure, new application deployment depends on infrastructure readiness. Orchestration tools enable centralized control and configurability over all infrastructure components.

Ease of operations: SDN offers a unified, single management view and console for infrastructure provisioning, ensuring quicker deployment and ease of operations. By centralizing management control, SDN reduces the dependence on multiple administrators for infrastructure component configuration.
Cloud-based service adoption: For the effective adoption of cloud-based service, enterprises require automation and single console management for overall infrastructure services spread within their premises, and on the cloud. Shifting to the cloud, along with SDN, ensures that enterprises can reach out to different business units for infrastructure and application provisioning. During the peak utilization period, application load can be shifted to a public cloud using SDN, to provide uninterrupted service.

Reduced CAPEX and OPEX: NFV enables virtualization of hardware appliances like routers, load balancers, and firewalls—optimizing cabling, rack-space, power consumption, and cooling costs. Elimination of human error and reduced resource usage leads to lower OPEX.

End-host security: SDN ensures both high speed and a secure connection between virtual machines through micro segmentation and virtual firewalls.

Conclusion

SDN technology drives network infrastructure virtualization and automation, providing cost benefits to customers by managing traffic explosion, simplifying operations, and reducing the need for manual interventions. The adoption of this technology promises increased scalability and agility in workload management, with greater control over the existing enterprise infrastructure. A host of SDN solutions that are available in the market necessitate a sound analysis of the existing infrastructure for readiness, prior to adoption. Based on the workload volume, the right solution should be identified to meet the business requirement. For a successful SDN implementation, it is not only important to select the apt SDN solution, but also to onboard people with requisite skillsets and deploy the right approach and methodology for a timely and error-free implementation.
About TCS’ IT Infrastructure Services Unit

Leading organizations across industries work with TCS to realize their business transformation and innovation objectives by enhancing the availability, performance and agility of their IT infrastructure. Leveraging a combination of the cloud, new generation delivery models such as IaaS, PaaS, and SaaS, virtualization, and managed services, our offerings deliver the secure, flexible, and reliable IT infrastructure needed to power critical business applications, services and data.

TCS infrastructure offerings encompass data center services, end-user computing (EUC), mobility services, cloud services and transformational solutions, converged network services, managed security services, application management services, enterprise systems management, IT service desk, and IT service management. Backed by our Assess-Build-Manage-Transform framework, extensive partner ecosystem, tools and automation frameworks, and technology Centers of Excellence (CoEs), analytics-led approach, to understand the ‘as-is’ state, and arrive at the ‘to-be’ state. As a result, you seamlessly transition from traditional infrastructure management services towards new generation delivery.

Contact
For more information about TCS’ IT Infrastructure Services, visit:
http://www.tcs.com/offerings/it_infrastructure/Pages/default.aspx
Email: itis.presales@tcs.com

Subscribe to TCS White Papers
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services (TCS)
Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

IT Services
Business Solutions
Consulting