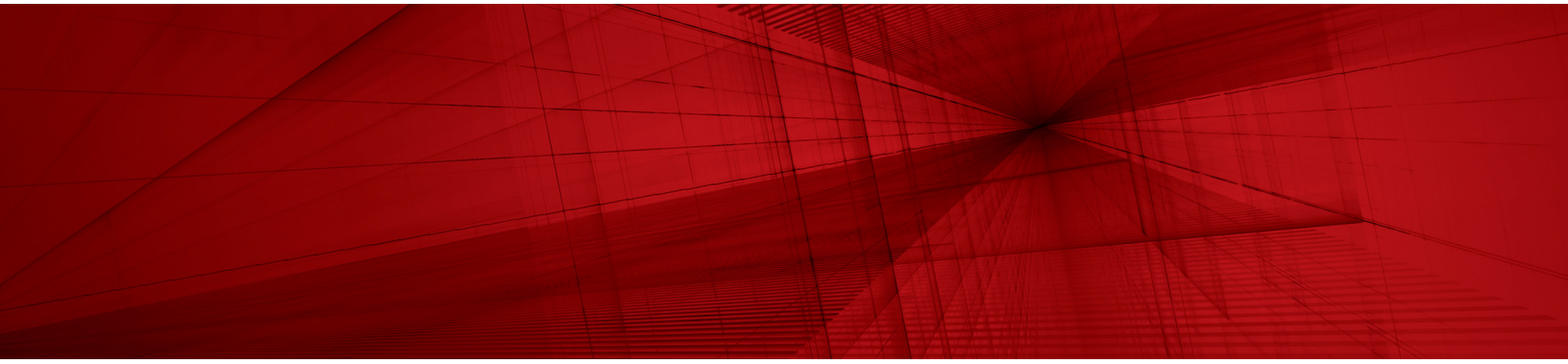
BROCADE



MIGRATING TO SDN: PLANNING FOR A SMOOTH TRANSITION

With 2014 shaping up to be the year of Proof-of-Concept (PoC) testing for Software-Defined Networking (SDN), many organizations are stepping up initiatives to migrate to a software-centric model. For most, the question no longer revolves around the merits of an SDN paradigm shift, but rather how best to navigate the transition to a more automated network architecture. Though it might seem daunting at first, migrating to an automated, virtualized network architecture should be a smooth and gradual process.

PoC: Playing with the Trial Version

There's a plethora of resources for organizations to leverage in exploring the benefits of SDN. For those who prefer to evaluate new technology by watching it in action rather than discussing it in the abstract, a PoC demonstration is a great first step.

Many SDN components are available for free or at substantially reduced cost on a 60-day trial basis. This allows network administrators to jump right in and test the ways SDN can benefit their network operations. For instance, some of the world's largest telcos have been testing the waters with PoC demos over the past couple years, including:

- **Deutsche Telekom:** Known in the US for its T-Mobile subsidiary, Deutsche Telekom was co-host at a meeting of the European Telecommunications Standard Institute (ETSI) where the telco discussed a PoC currently underway to test a virtualized IP multimedia subsystem platform.
- **Orange:** The Paris-based telco's San Francisco office is building a test bed to evaluate a virtual Evolved Packet Core (vEPC).

- **Verizon:** In collaboration with Intel, Hewlett Packard, ADARA networks, and others, Verizon has been testing various use cases for SDN solutions for more than three years. In 2012, the four companies jointly hosted an SDN demonstration that focused on using the OpenFlow protocol to address the cost of implementing complex consumer services, as well as optimizing the flow of information between data centers.

What to Do Before Starting

Organizations should have a clear idea of the benefits they hope to realize by implementing SDN. In many cases, a software-defined solution won't necessarily look different than a conventional network. To fully leverage the benefits, some users (such as Cloud Service Providers [CSPs]) may need to deploy a Network Functions Virtualization (NFV) strategy alongside SDN.

Through the course of any major shift in networking, one of the more terrifying prospects is a continuity gap during the migration process. This should be confronted head-on prior to the start of migration. The IT team must determine the impact of an SDN model on existing services and in instances where the possibility of a gap exists, administrators should always have a failsafe mechanism in place. To this end, they should work from a list of sample applications that will be used for connectivity and service continuity checks before and after migration. This will help not only to guard against service interruptions, but also weed out any issues that are unrelated to the migration.

But no matter how much preparation is conducted beforehand, not all circumstances can be foreseen. For this reason, it is essential to have a mitigation plan that enables administrators to revert back to the previous network configuration.

Migrating to SDN: Great Leap or Baby Steps?

For many organizations, a network overlay is the first step in virtualization. Overlays allow for data to travel along the physical network without the need to reconfigure switches along the way. While this serves as a great initial foray, organizations looking to shift toward OpenFlow-based SDN will need to adopt a more holistic view.

First, administrators need to provision network management and traffic monitoring tools to function on the migrated network. This allows organizations to keep an eye on several critical elements during migration, such as OpenFlow compatibility across the network.

Another important point to keep in mind is network segmentation. Many network administrators are rightly apprehensive at the prospect of network virtualization in that it introduces a new threat to IT infrastructure in the form of the hypervisor. Like any software, the hypervisor represents a potential security risk that could compromise every virtual machine running under a given hardware system. To mitigate this risk, administrators should segment their network between applications. This can be accomplished either through software or additional hardware, though the latter approach might be more costly.

When virtualizing servers, it's also critical to consider the associated networking functions and to virtualize them where appropriate. This is where NFV begins to complement SDN.

Migration can vary greatly depending on the size and complexity of the network and the experience of the IT team. In some cases, new skill sets and additional training may be required. Still, transitioning to an architecture that embraces software is not as difficult as many would assume. With proper planning, most organizations can quickly and easily leverage the benefits of an SDN solution.

Get the facts at *Brocade.com/NetworkFacts*.