# Ten Important Facts about Evaluating SDN Solutions

# Ten Important Facts about Evaluating SDN Solutions

- ***Programming Rather than Managing Manually***

Programmability is a very important change compared to the traditional method of managing the network via command line interface or management GUI/console.

SDN programmability allows for greater flexibility, more sophisticated policies, and more agile networks overall.

**SDN doesn't necessarily require separation of the network control plane from the data plane as many originally defined it.**

Today there are a number of interrelated technologies, protocols, and architectures that lead to policy-based automation and achieve the original vision of SDN.

- ***Making for Easier Policy Implementation***

The SDN policies can reflect a sophisticated application, IT, or business policy objectives; whatever you can implement in software within the SDN framework.

By implementing policies in software, rather than through management tools of network devices, policies can more easily be aligned with business requirements, and be much easier to maintain and deploy.

- ***Supporting Multivendor Ecosystems***

For the SDN policy model to automate the entire application infrastructure, a large multivendor ecosystem across a large number of infrastructure device types must be supported by the SDN platform. One should consider what firewalls, application delivery controllers, and other security devices are supported by the proposed SDN architecture and standards.

This consideration also includes whether you can incorporate your existing network infrastructure into the SDN environment when it’s deployed, or to what extent you will have to upgrade your hardware to SDN-compliant devices.

- ***Understanding the Importance of the Controller***

The controller architecture is the key to many features of the SDN platform, how it is programmed, and what devices can be controlled. There may be a variety of controllers and platforms to consider when selecting an SDN strategy, so make sure you choose a controller that does everything you need. A proprietary controller or one that supports a limited SDN policy model will limit your capabilities down the road.

- ***Speaking the Right Language***

The language (or policy model) of the SDN policy/controller greatly determines how the infrastructure can be automated and the flexibility you have in programming it.

For example, Cisco ACI presents an application-centric policy model that represents the SDN policy in terms of application requirements and capabilities. This model allows a single policy to span the entire IT infrastructure, including network, security, application services, and so on.

With the right policy model in place, you can extend the advantages and methodology of SDN beyond the network to the entire application infrastructure and beyond the data center to the campus WAN and remote sites.

- ***Using the Northbound Lane***

Customized software programs written for an SDN environment usually run on top of the SDN controller through a northbound interface — an API running on the controller that hosts software applications. The specifications of this northbound API can also greatly influence the flexibility of how and what you can program the infrastructure to do, and what automation tasks your SDN platform can perform.

The northbound API should be open, flexible, and well integrated with the capabilities of the controller. It should also support the applications such as cloud orchestration tools that you will need to run.

- ***Making Use of Cloud Automation Tools***

Choose an SDN platform that gives you the greatest flexibility in cloud automation tools and platforms rather than being locked into one vendor's cloud stack. Many of the new generation of SDN applications that reside on the northbound API of the controller are themselves cloud automation tools, and they help to manage workflows and tasks for cloud application deployment and infrastructure management.

Some examples of cloud automation platforms that can sit on top of SDN controller northbound interfaces are OpenStack and Cisco UCS Director.

In addition to cloud management tools, any SDN platform should support a number of monitoring and performance tools that can help analyze, troubleshoot, and automate the tuning of the applications and the network.

- ***Choosing an Open Source SDN Platform Carefully***

Openness and interoperability are very important to any SDN strategy. Choice of open source SDN platform may provide a less expensive architecture initially, but may restrict integration to a more narrow policy that runs across multiple infrastructure components, or may require a lot of customization and integration for any particular cloud environment and policy requirements.

An open SDN platform should support all major server operating systems and hypervisor(VMM) platforms including VMware, Microsoft, and Linux KVM to provide maximum coverage and flexibility.

Another important requirement when considering an open source SDN controller, is the size of the vendor ecosystem that supports it.

- ***Keeping It Seamless***

Cloud environments are composed of both virtual and bare-metal applications, as well as virtual and physical infrastructures (networks, firewalls, service nodes).

The SDN platform, policies, and automation tools must operate seamlessly across this physical and virtual spectrum.

Too often the automation only applies to the virtual infrastructure, or a particular class of physical devices (a particular vendor's switches, for example).

A successful SDN strategy has to span everything, with a common set of policies, tools, and infrastructure if the IT automation strategy is to be successful.

- ***Considering an Extensible Architecture***

Because the SDN controller is the operational hub of all integration and automation efforts, it must be an open, extensible architecture in a number of important ways (such as an open, flexible northbound API to host multiple applications or cloud automation tools).

It must have an open way of communicating to a multivendor IT infrastructure of switches, routers, firewalls, application delivery controllers, and more.

It must be ensured that the SDN architecture meets all the open requirements to successfully navigate and simplify the deployments.

*Thank You*