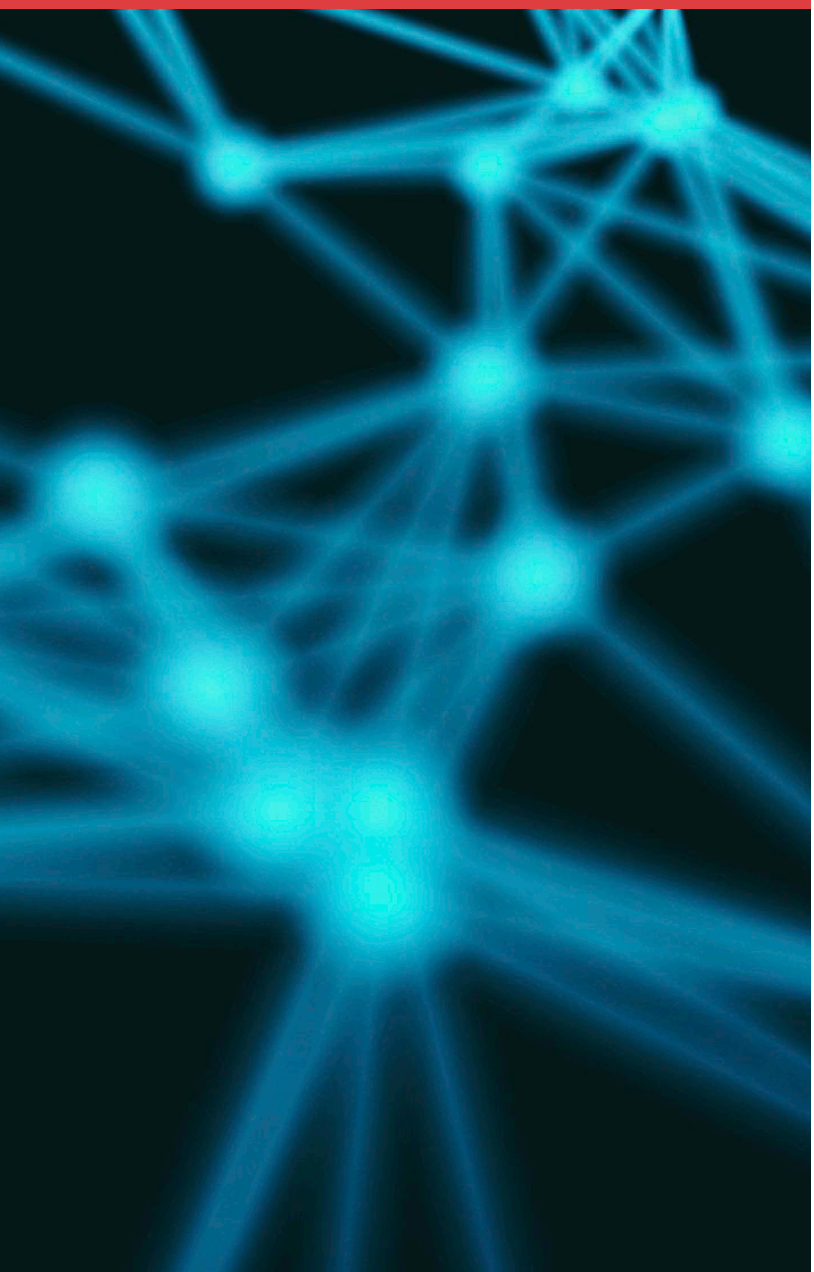
Understanding White Box Networking and Open Network Operating Systems

By George Crump

Storage Switzerland, LLC

Pluribus NETWORKS

CHAPTER 1: Understanding White Box Networking and Open Network Operating Systems



For decades, an organization bought its network switching products from a single vendor such as Cisco. In most cases, that organization's data center became 100% dedicated to that networking vendor and it was almost impossible for another vendor to gain a foothold in the data center. Traditional networking today faces challenges from white box networking, open network operating systems, and software defined networking. All the industry sometimes uses these terms interchangeably, however there are important differences that IT needs to understand in order to implement a more open network strategy.

The Rise of Merchant Silicon

In the traditional networking model, the vendor's switch hardware came with a proprietary network operating system that only worked on the vendor's specific hardware. In the early days, most switch vendors developed their own custom switching ASICs (Application Specific Integrated Circuit) to deliver the features needed and to differentiate themselves from other vendors. However, in the past 5 years, Broadcom has built a powerful family of general purpose switching ASICs, known as "merchant silicon", that have radically simplified the process of building network switches.

Over the past five years, the switching market has also evolved significantly and merchant silicon has become as powerful as the early custom ASICs. In fact, so much so, that it has become more cost-effective to build next generation switches with these merchant silicon chips rather than developing custom ASICs. These powerful ASICs deliver the important networking capabilities that many modern high-performance networks require.

Today most vendors that offer network switches use merchant silicon from Broadcom. In fact, these ASICs are so powerful and feature rich that many of the traditional switching vendors also use the Broadcom chips to build their branded switching hardware. Most switches on the market today have a common chip set, and when combined with a common network operating system, customers can mix and match switches from various vendors.

What is Disaggregation?

Traditionally, data center products were a combination of hardware and software that customers had to buy together as an integrated solution. Disaggregation decouples those components and enables IT to mix and match them. Disaggregation enables organizations to drive down data center costs while increasing flexibility. In the compute segment, disaggregation's starting point, IT can select a variety of operating systems like Linux, Windows or VMware and run it on server hardware from a multitude of vendors.

The disaggregation phenomenon is also taking hold in the network switching market, commonly referred to as "Open Networking" or White Box Switches. A number of companies now offer "bare metal" switches which they build from the same standard components with similar capabilities to traditional networking switches. Contract manufacturers are also building networking switches, even though the logos are different, with the same components and same merchant silicon.

Why White Box Networking

The white box networking concept offers a significant costs savings over traditional networking devices. White box switches typically cost 50-60% less than a comparative traditional switch, a delta large enough to capture the attention of even the most skeptical IT planner, especially given the relative equality in features and capabilities. In addition to cost savings, white box networking also provides the potential for vendors to bring additional innovations to market.

The Network Operating System Enables Open Networking

As organizations move from just the cost savings of white box switches, to the complete hardware flexibility offered by Open Networking, those organizations need to create or acquire a network operating system to run the various switches in the environment. Similar to how an IT planner will decide on an operating system to install on its various server hardware platforms, they also need to decide on a single network operating system (NOS) for their various white box network switches. The NOS enables the organization to customize the solution to meet its needs.

In many cases, the white box switch hardware companies provide a rudimentary NOS with their switch. The design of these basic NOS options essentially allow them to manage just one switch or only manage switches with that vendor's logo on it, which breaks the Open Networking concept. Increasingly, white box switch vendors provide the basic NOS for single switch management and offer a number of NOS software vendor's solutions, which can work with multiple switches. Still other white box switch vendors sell only the hardware and assume the customer will supply software.

The Open Networking business model parallels the server business model. There is a variety of ways to purchase the product but in the end, while the hardware is important, the software (NOS) is critical. NOS vendors compete for IT attention and they use features like ease of management, ease of aggregation, automation and other features to differentiate themselves from each other. The competition, which drives innovation, means that data centers built on Open Networking can expect a more feature rich networking environment at significantly lower prices.

Selecting the Right Network Operating System

All NOS solutions deliver basic layer 2 and layer 3 switching and routing. The differences between solutions lies in the advance features that each provide. Most data centers for example, will find it important for the NOS to stay up and operational through various outages but not all NOSs provide enterprise class resiliency. Data Centers may also want to evolve into a software-defined network (SDN), in which case those organizations will want the integration of advanced networking services, like automation and integrated monitoring. Only a few of the Open Networking (or white box) NOS solutions can evolve into SDN.

Other key features to consider are

- *Fabric Architecture to enable multiple switches to act as one*
- *Network Virtualization to segment and secure the network*
- *Integrate network operations and services with virtualization platforms like VMware*
- *API driven Network Automation*

—

IT planners looking to modernize their network need to aim for a network experience that is more flexible and automated. For many, the eventual end goal is a software-defined networking architecture. The first step for those IT planners is white box networking and the network operating system is the most critical aspect of that step. White box networking promises to drive down networking costs significantly but if IT planners don't place the right amount of attention on the network operating system then the strategy may end up hitting a brick wall. The right NOS selection brings not only the cost savings of white box switches but also assures optimal network operation with future innovation and automation previously thought impossible.

CHAPTER 2: Defining SDN in the Open Networking Era

Software-defined networking (SDN) represents the future of networking. A "software-defined" network enables an organization to virtualize their network, automate operations to enable efficient network configuration, and integrate network functions across dozens of switches creating a unified network architecture that is programmable and dynamically definable. The goal of SDN is to create a network that is easier to manage and is automated to accelerate the roll out of services as IT stands up new applications and adds new users. SDN should also help IT simplify the operational model and the movement and sharing of applications, resources and users to various locations across the organization.

When initially created, the spirit of SDN was to separate the control plane and the data plane functions. The separation enables programmability and also enables the use of low-cost, less intelligent network switches. For years SDN was commonly associated with the OpenFlow protocol and controllers with the purpose of determining the path for network packets across network switches and centralizing management of the network.

While SDN protocols and architectures have evolved, the notion of the SDN controller has remained. Even today most SDN architectures still use controllers to support the separation of the control plane functions from the physical switches to enable programmability, allow centralized and automated control over the network.

What's Not SDN?

Vendors now use the term "software-defined" to describe everything, including networking. Unfortunately, some networking vendors use the SDN term more liberally than they should. Stated simply, today's SDN is creating a "fabric" of network switches that operate together as a single logical switch that through the SDN software is programmable and automated.

A common term used along with SDN and Open Networking is disaggregation. Disaggregation decouples switch hardware from the networking operating system and enables IT to mix and match the hardware and software components. SDN though is not always about disaggregation and disaggregation is not always an SDN solution. There are SDN solutions that are available from traditional networking vendors. These are the closed hardware and software offerings that use a controller to enable their ability for programming and automation. There are also disaggregated SDN solutions from Open Networking OS vendors as well. These use open networking hardware switches and a Network OS that enables the SDN functionality. With Open Networking SDN, some SDN architectures use a controller, while others do not. But not all Open Networking OSes are capable of implementing SDN.

Our last chapter established the value of Open Networking and disaggregation, but the benefits of Open Networking translate through to SDN deployments as well. To see those benefits, one needs to understand the evolution of SDN.

SDN - The First Generation

The first generation SDN architectures have two common elements – they are dependent on a controller for operation, and they use an SDN related communication protocol such as Open Flow between the controller and switches.

The SDN controller is the “brains” of the network. It holds the configurations, tells the switches what to do and is the point of programming and control for the switches that are in the SDN fabric. The controller enables centralized control, automation and programmability. The use of a controller has a significant downside though, the network will not function without the controller.

SDN controllers also add complexity and impede resiliency. Since the network is dependent on them for operation, they are a single-point-of-failure and can become a performance bottleneck. In the event of controller failures, fail-over to a redundant controller can cause network reconvergence impacting network operations. A reconverging network can interrupt applications and create user experience issues as the network resets itself through the controller.

In addition to resiliency considerations, SDN controllers inhibit the ability to extend the SDN fabric across physical locations. Some first-generation SDN vendors can interconnect SDN islands, but each island still has its group of controllers that are overseeing the local fabric of switches.

SDN can significantly improve network functionality, agility and business value, but the complexity of controllers and dependency on new protocols like Open Flow, has been cited as a common inhibitor to widespread SDN adoption.

Next Generation SDN

The next generation of SDN addresses the fundamental challenges created by first-generation controller-bound SDN architectures. It is still software-defined, and programmable, but it eliminates the complexities that are common with controllers and SDN protocols. Next-Generation SDN is a fully distributed fabric architecture that operates without a controller. Many IT professionals find it easier to manage and easier to automate. It is also considered more resilient since it isn’t dependent on a controller architecture. IT can deploy next generation SDN more easily into an existing networking infrastructure allowing IT organizations to orchestrate a more graceful migration to SDN.

The next generation of SDN removes the complexities that have inhibited SDN adoption by building the controller function into the operating system. The controller functionality then operates within the distributed network devices. The peer-to-peer approach shares the controller functionality across all of the network’s switches. The distribution of the controller function across switches is similar to how computing and storage cluster technologies work.

With next-generation SDN there is still the separation of control plane functions that was the intent of the initial SDN definitions. The distribution of the control plane instead of isolating on a few servers makes the network switches more intelligent and more integrated with the rest of the network.

Next-generation SDN simplifies the operational model and should lead to increasing adoption for several reasons. First, automation is now integrated into the network and is not dependent on a controller. This means that you can manage and program the network from any device in the network. The switches in a next-generation SDN network are intelligent and understand the state

of the network – not only for the local switch, but for all switches across the network. The network awareness of each switch increases resiliency, eliminates reconvergance and makes the network inherently smarter.

Second, next-generation SDN virtualizes the network, like how a hypervisor virtualizes a server, which means you can segment the network for security and multi-tenant operations, but you can also virtualize network services. Through network virtualization IT can segment networks for better security control to reduce the attack surface and prevent attack movements.

Third, next-generation SDN enables IT to build a geographically distributed SDN fabric to simplify Data Center Interconnection. Data Center Interconnection via SDN means organizations can have a single logical switch that can be distributed to many physically separate places. Even in the geographically disperse configuration IT still has the control and programmability over the environment as if all of the distributed switches were one logical switch.

Finally, the next-generation SDN is also is important for virtualized applications and hyper-converged infrastructure environments because it allows distributed locations to operate as if they are located in a single data center. Next-generation SDN improves application resiliency, optimizes resource sharing, speeds application mobility and supports business continuity requirements.

In our last chapter, we discussed the importance of the Network Operating Systems when implementing White Box Switches. Open Networking changes the economics of networking in the data center and beyond. However, not all White Box OS options are SDN, and not all SDN systems are built on white boxes. There are two steps to consider. The first is taking the journey to white box architectures, and then considering adoption of SDN for your network.

An Open Networking enabled SDN architecture can lower costs by leveraging the cost efficiencies and flexibility of white box switches. The operational value of SDN is of equal importance. It will improve network efficiency and organizational agility through automation and programmability. The next-generation of SDN can remove the obstacles associated with first generation SDN implementations and enable the organization to undertake a staged migration to SDN and all its benefits.

CHAPTER 3: What is Intent Based Networking?

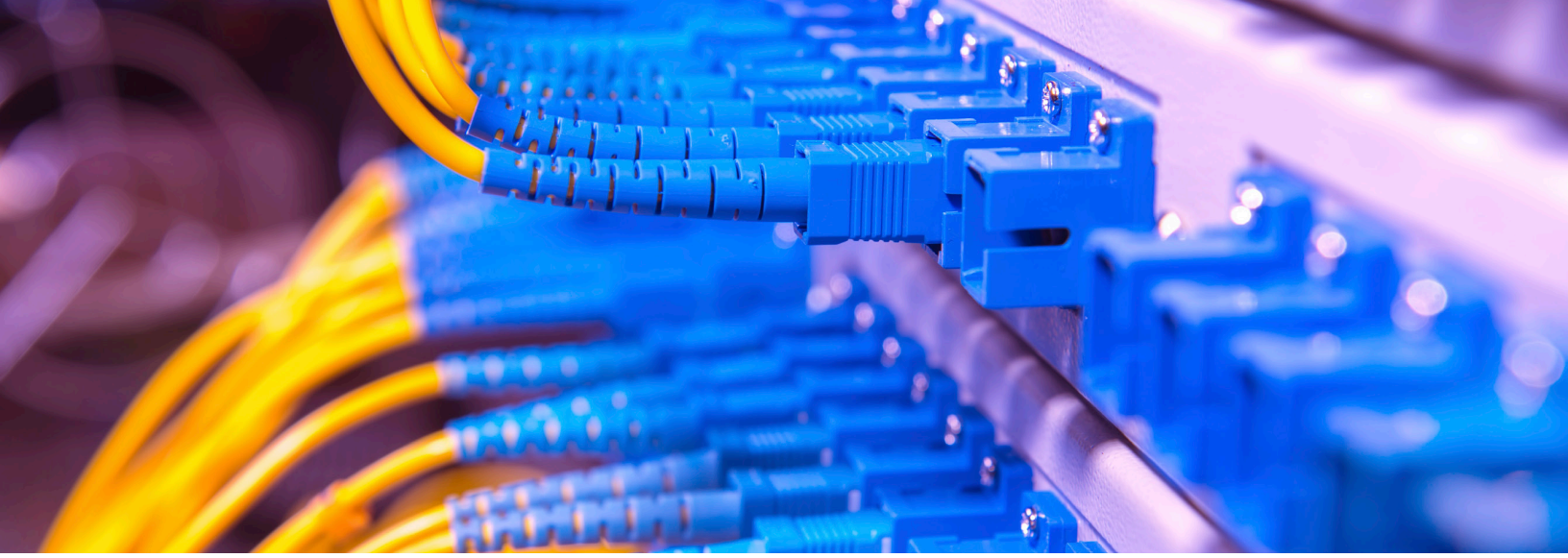
Intent-Based Networking moves organizations from reactive networking where everything that happens on a network is in response to something, to proactive networking where everything that happens on a network is to deliver the business goal or the intent. Intent-based networking requires the networking software to collect the appropriate telemetry data, analyze that data, and take actions so that the network can meet the businesses objectives. Intent-based networking is not software-defined networking, but software-defined networking (SDN) is a logical path to intent-based networking.

Intent-based networking is how IT will manage networks in the future but the concept is still in its infancy. The network team can't wait for an intent-based networking future, they have to improve the way they manage networks today. IT should, however, make sure that the steps they take to improve today's network, like leveraging open networking, lay the foundation for intent-based networking. If organizations are not careful intent-based networking can make them even more susceptible to vendor lock-in.

Next generation SDN solutions make managing networks of massive scale and multiple physical locations possible, but at some point, even the best networking team can't stay on top of every aspect of the network. The idea behind intent-based networking is to leverage analytics to enable the network to take self-correcting actions so that the networking team doesn't need to be involved in every single detail of the data center's network.

The most obvious required addition to SDN solutions is the ability to capture the various "intents" or business objectives of the organization. An intent-based solution needs these as a baseline to which it compares current network operations.

SDN vendors, in most cases, collect telemetry data on all network operations that their software controls. The SDN vendor also has to add an analytics engine which is different than network diagnostics, a common SDN feature. Network diagnostics informs the networking team what is wrong. Analytics advises the networking team not only of a problem but also how to correct it. More importantly, an analytics engine predicts future problems and allows their correction before users or application owners notice a performance drop or application outage.



In addition to analytics, the SDN solution has to provide autonomic operation. Most SDN solutions have some form of automation or programmability as features. Autonomic operation leverages automation and combines it with the knowledge gained from the analytics engine. With this combination intact, the network can now proactively make adjustments to its configuration based on how those results line up with the various “intents” of the business.

There are several approaches to delivering intent based networking, and the capability is not exclusive to SDN solutions. Proprietary vendors are quickly moving to deliver “Intent” based solutions. Proprietary solutions, of course, have all the challenges listed in the prior two entries in this series, most notably vendor lock-in, high cost and lack of flexibility. There are also third-party approaches that layer on top of the networking environment and pull telemetry data from the various components. The problem with this approach is that in most cases these solutions also only work with a “short-list” of proprietary solutions. These solutions suffer from the same lack of hardware flexibility as proprietary solutions. They also are entirely dependent on the proprietary vendors sharing access to their telemetry data.

Getting Ready for Intent-based Networking

As organizations improve their networks responsiveness and attempt to lower costs, there are key capabilities they should look for in their SDN solution to make sure it is ready for an intent-based future. First, it needs to leverage a REST API that provides full parity with a command line interface. Comprehensive API’s are required so when intent-based networking is layered in it can manipulate the network configuration to align with the established intents.

Second, the SDN solution needs to provide complete telemetry data and capture that data in fine detail. This enables the intent-based networking component to mine that data to ensure correct configuration decisions are made when maintaining intent coherency.

Third, the SDN solution needs to provide single point of control so that when the intent based component initiates a network change it has a single interface that executes this. The single point of control can be through a centralized controller or a controller-less fabric. The controller-less fabric has an advantage since the changes can be made in parallel across the network.

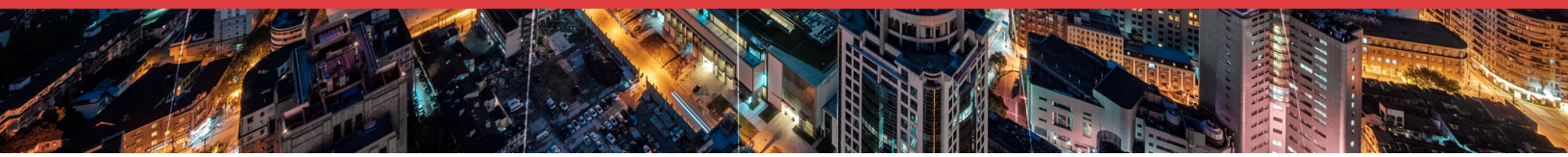
Finally, the network needs to maintain its openness. The organization needs to avoid getting even further locked-in to a particular vendor in order to gain intent-based networking. To maintain an open network in the future the organization needs to select an SDN solution that not only provides open networking today but can maintain its openness as intent based capabilities are added to it.

SDN, assuming the vendor adds the above capabilities, has a clear advantage. The SDN vendor can integrate intent based networking directly into their software, which lowers the overhead and provides full access to the telemetry information. Integrating intent-based networking into SDN should also reduce implementation complexity.

—

SDN removes network cost and operational roadblocks to data center scale. SDN with integrated intent-based networking enables the organization to accelerate scale with the full confidence that current IT staffing levels are enough to meet application service levels continuously.

CHAPTER 4: How Data Centers Can Implement Open Networking Now



The use of Open Networking promises operational value, data center flexibility and a reduction in the cost of network infrastructure. Next Generation SDN (Software Defined Networking) promises automation, increased agility and a reduction in operational costs of data center networking in single site and multi-site data centers. With adequately designed open network solutions, gaining these values is possible without a complete, disruptive refresh of existing network infrastructure. Now, Network Operations can start IT on a journey that progresses from using an open Network Operating System (NOS) leveraging cost-effective white-box switches that continues on to a complete software-defined network (SDN). This approach provides the ultimate in automation, while also integrating with existing proprietary networking hardware. The challenge facing organizations is not when these technologies are enterprise-ready (they are now) but how to start the journey.

All The Pieces Are Already in Place

Before starting on any journey, an organization needs to confirm that all the components are in place to complete that journey. In the case of Open Networking, they are: Network Operating Systems (NOSs), which are available now from several vendors and that can work with currently available white box switches. Some of the NOS offerings enable the organization to create a network fabric that resembles their virtual server infrastructure. In a virtual server infrastructure, the critical component is the hypervisor, while in a white box virtualized network, a capable NOS is the critical component. With the proper NOS selected, the organization can use and manage a variety of different white box switches from different vendors while achieving a consistent operational model and single pane of glass for management.

As the organization continues the journey, both controller-based and controllerless SDN solutions are available either from the same vendors that provide the NOS or from dedicated SDN controller vendors. In the data center these SDN solutions should provide a VXLAN overlay fabric for the spine/leaf architecture, some sort of network slicing/segmentation and also provide an increased level of automation. The controllerless solutions are becoming popular, especially in multi-site scenarios as they distribute the networking automation and management functions across all switches at all sites.

Additionally, controllerless solutions do not suffer the cost burden of multiple redundant controllers, the

latency penalties for establishing new flows or network re-convergence, or the single point of failure with out-of-band management seen with traditional controller-based solutions. These SDN solutions also provide advanced telemetry that enables the organization to troubleshoot their network proactively. The deep telemetry capture provided by SDN paves the way for future use cases like intent-based networking (IBN). IBN enables the organization to create application-level service agreements with which the network automatically conforms.

Why Introduce Open Networking?

The “why” is often as important as the “can.” As stated in our prior entries (chapters) the reasons for open networking and SDN are compelling. First, open networking with white box switches should provide significant cost savings to the organization. Some studies claim that companies can reduce the cost of their network infrastructure by as much as 50% or more.

Second, open networking provides much greater flexibility and feature velocity. The organization can easily change hardware vendors if another vendor provides better service or better pricing. The flexibility also enables the organization to adopt new technology sooner, like higher bandwidth switches and switches with greater port densities. Third, open networking enables increased management efficiency. The current networking staff is likely overwhelmed by requests, and they take days or weeks to respond. With Open Networking and SDN, many of the required tasks can be automated and pre-programmed.

How To Get Started

At some point, the research and study of open networking should end, and implementation needs to begin. The first step is to understand which of the organization’s workloads are migrating to the cloud and which are staying in the data center.

The next step is to determine if the organization can consolidate data centers or if the organization wants to migrate all or some of their infrastructure to one or more carrier-neutral colocation facilities. During data center consolidation or migration to colocation facilities, the right Open Networking NOS can make the transition easier by unifying the multiple sites into one logical SDN-controlled fabric and automate network configurations to adapt to applications as they move to their new location.

Within each data center, organizations should examine their current (brownfield) networking infrastructure for components that are going to stay in place as well as those that are either reaching the end of life or can no longer meet the performance demands. Instead of upgrading to a switch from the same proprietary vendor, use Open Networking with NOS and SDN to introduce white box switches into the environment. Again, some white box switches and SDN can easily coexist with proprietary switch vendor hardware in a brownfield environment while other open networking and SDN solutions may require a complete rip and replace.

New (greenfield) initiatives are an obvious candidate for introducing Open Networking concepts. Over time IT can gradually integrate open networking into the existing proprietary backbone. However, a brownfield scenario is more-often-than-not the typical environment.

One additional consideration is for the organization to understand their edge compute strategy. If the data center operator is looking at deploying mini or micro-data centers closer to their end-users then more weight should be put on the multi-site capabilities of the offering – the ability to deploy an SDN controlled fabric across multiple sites with low latency becomes more and more important.

Once the open networking switches and NOS are selected, they should go through a proof of concept in one data center or across multiple data centers in a multi-site scenario. Once the POC is proven out for the environment, full deployment can occur.

—

Open Networking, Network Operating Systems, White Box Network switches, and Software Defined Networking are all mature and ready for the enterprise. They are no longer solutions exclusively for cloud providers and hyper-scalers. The financial justification for Open Networking is beyond compelling as are the gains in operational efficiency. The only remaining piece is for organizations and IT planners within those organizations, to start taking the first steps on the open networking journey. In particular they must carefully examine the capabilities of the NOS and SDN control implementation to ensure the right solution is selected for the data center operator's environment.

Storage Switzerland, LLC

The Firm

Storage Switzerland is the leading storage analyst firm focused on the emerging storage categories of memory-based storage (Flash), Big Data, virtualization, and cloud computing. The firm is widely recognized for its blogs, white papers and videos on current approaches such as all-flash arrays, deduplication, SSD's, software-defined storage, backup appliances and storage networking. The name "Storage Switzerland" indicates a pledge to provide neutral analysis of the storage marketplace, rather than focusing on a single vendor approach.

Pluribus NETWORKS

About Our Partner

Pluribus Networks is delivering the next generation software defined network fabric for multi-site data center and Distributed Cloud environments. The Linux-based Netvisor® ONE operating system and the Adaptive Cloud Fabric™ have been purpose built to deliver radically simplified networking along with white box economics by leveraging open networking hardware from our partners Dell EMC, D-Link Systems and Edgecore as well as Pluribus' own Freedom Series of switches. The Adaptive Cloud Fabric controllerless SDN architecture distributes state and intelligence throughout the network fabric and is optimized to deliver rich and highly secure per-tenant services across data center sites with simple operations and no single point of failure. Pluribus Networks is also embedded within Ericsson's Software Defined Infrastructure (SDI), Network Function Virtualization Infrastructure (NFVi) and Distributed Cloud solutions which are being deployed in the networks of the world's largest 5G service providers. Pluribus Networks is a founding member of the Linux Foundation's LF Edge organization. Visit pluribusnetworks.com to learn more.

The Analyst

George Crump is the founder of Storage Switzerland, the leading storage analyst firm focused on the subjects of big data, solid state storage, virtualization, cloud computing and data protection. He is widely recognized for his articles, white papers, and videos on such current approaches as all-flash arrays, deduplication, SSDs, software-defined storage, backup appliances, and storage networking. He has over 25 years of experience designing storage solutions for data centers across the U.S.