Introduction

Mobility, cloud, and consumerization of IT are all major themes playing out in the IT industry today—all of which are fundamentally changing the way we think about managing IT infrastructure. Mobility is driving significant productivity gains. Users, devices and indeed applications are all mobile. Users today access their applications, data, and content from whatever location they are at—be it from the office or from a hotel lobby or from an airport, using whatever device they have at their disposal such as their laptop, smartphone or tablet, and leveraging whatever technology is available—from wired Ethernet, to WiFi to 3G/4G. Today applications also move from server to server in the form of virtual machines—under administrative control, or in a completely automated way using tools that do resource management for example. While mobility is driving significant productivity gains, it is also making the IT environment very complex. In such a dynamic environment, it is becoming difficult to determine whether a user, or an application, or the underlying infrastructure itself is performing as desired and whether the security, compliance, and audit requirements are being met.

Consumerization of IT is often associated with BYOD (Bring Your Own Device). However, it is far more impacting than that. The fundamental expectation of IT is changing where IT is expected to embrace a consumer-like behavior. IT is expected to now support consumer devices on the corporate infrastructure. Along with that consumer applications are now running and competing for resources on the same IT infrastructure as enterprise applications. For example, smartphones constantly synchronize consumer applications in the background and now users of the corporate IT infrastructure are actively using consumer applications as part of their productivity suite. IT is expected to respond, accommodate, and indeed fully embrace this shift with 24x7 support. Unfortunately, today IT and the management, monitoring, and security tools that they use are lacking the visibility they need to be able to accurately determine the stability, the security, and the performance of this evolving environment.

In the midst of all of these changes, the way networking has been implemented has remained fundamentally unchanged. Even though the network speeds and the protocols that are used to keep the network operational have evolved, the fundamental nature of the network has not changed. The network today is still run as a set of interconnected devices each of which operate as individual entities having their own local control plane and forwarding or data plane (see Figure 1 on the next page). The control plane determines where traffic is to be sent, and the data plane takes care of forwarding the traffic at very high speeds and progressively lower latency. Both the control plane and the data plane today are co-resident on each networking device, making the large network a complex distributed computing problem that has to respond and react to dynamic changes at very high speeds and with large traffic volumes. To compound the challenge further, each networking component or attached device has only a partial view of what is going on in the network and piecing together the whole picture becomes a complex exercise.
Addressing Network Complexity through SDN

SDN changes the fundamental nature of networking. With SDN, the control plane or the intelligence functions of the network are centralized on a controller. The SDN controller maintains a centralized view of all the networking switches, and programs each switch with the knowledge it needs to correctly forward traffic. By centralizing the control plane, the SDN model provides a simplified operational model for large networks that are characterized by highly dynamic workloads, user/device/application mobility, and policy driven connectivity (see Figure 1).

A secondary effect of this approach is that by removing the intelligence out from the network appliances such as switches and routers, the software and hardware for these switches and routers could be simplified, thereby driving down costs for the individual devices. In fact there is a growing momentum around leveraging “white boxes” —bare metal switches/routers sourced directly from manufacturers, along with an open-source network OS, in conjunction with an open source controller to put together an SDN solution.

However, the promise of “white box” networking has yet to bear fruit as there are significant barriers to making the white box approach a true working solution for mainstream deployment in the near term. The challenges range from lack of maturity of software, to lack of interoperability, to a DIY (Do It Yourself) type approach required to make the solution successful. Still, the promise of the SDN model of centralizing the network intelligence, and the operational simplification it can bring to complex networks holds promise.

While SDN is still in its nascent stages, several different technologies and applications of SDN are emerging. OpenFlow is one such technology. OpenFlow is being standardized through the Open Networking Foundation (ONF) and is one example of how a centralized controller programs and manages distributed network switches. OpenFlow provides a standardized way to program forwarding tables in network switches based on the intelligence and applications running on the controller. While OpenFlow provides a standardized approach for a controller to program network switches, it does not specify how the controller addresses specific challenges associated with mobility or BYOD or other such challenges. In other words, OpenFlow is simply a protocol between the controller and the network switches. The function of that protocol to solving network challenges is left to the controller and the applications residing on that controller, and will differ from implementation to implementation and from vendor to vendor. This provides an opportunity for differentiation as well as innovation in this space.

OpenFlow is just one embodiment of SDN. Several other technologies, mainly vendor driven, are now emerging under the SDN umbrella. Unlike OpenFlow, many of the other emerging technologies under the SDN umbrella are targeted and purpose built for solving specific problems. One such area that is being targeted for SDN deployments is network virtualization. Network virtualization effectively builds dynamic network overlays over an underlying physical network infrastructure and addresses key challenges around mobility and multi-tenancy in cloud, data center, and campus environments (see Figure 2 on the next page). These dynamic overlays create logical tunnels between different endpoints belonging to a common logical network service, or to a tenant using some form of traffic encapsulation. A key technology that is gaining traction to address network virtualization is VXLAN. With VXLAN, virtual extensible overlay
networks are built using VXLAN encapsulation or tunnels. In cloud deployments these tunnels can originate and terminate within the hypervisor, making the physical network oblivious and independent of the overlay (see Figure 2). The tunnels can be dynamically instantiated based on mobility events or based on spinning up capacity in various segments of the network.

While network virtualization addresses some of the challenges around multi-tenancy and mobility, it creates a different set of issues from the perspective of monitoring, management, and security. By creating separate logical overlays which are abstracted from the physical underlying network, it creates two planes of troubleshooting, monitoring, and management—the physical underlay and the logical overlay. Both planes can be subject to security threats and breaches.

Many other applications of SDN are also emerging. These include, among others, traffic engineering over WAN links, policy-based access control, and centralized routing.

**Monitoring, Managing, and Securing in an SDN World**

While SDN holds the promise of operationally simplifying dynamic environments such as those with large volumes of traffic, mobility, and cloud deployments, SDN deployments will be characterized by an increased need for tools that do security, performance, and user experience monitoring. There are several reasons for this. For example, separating the data and control plane could lead to synchronization issues between these two components. The deployment of network virtualization solutions that use encapsulation or tunneling also create separate planes for management and control for the overlay and underlay networks, thereby increasing the need for monitoring. These are explored in the following sections in more detail.

Typically tools rely on one of three types of techniques for monitoring and management.

1. SNMP style based monitoring
2. Flow-based monitoring and analysis
3. Packet-based monitoring and analysis

SNMP style monitoring is typically used for device status monitoring as well as aggregate traffic monitoring based on counters and statistics is an example of this. Flow-based and packet-based techniques rely on actual traffic information. In flow-based techniques actual traffic is sampled, flow records are gathered from the sampled traffic, and the flow information is then presented to the tools. The greater the sampling rate, the more accurate the tools analysis. In packet-based techniques, the actual packets are presented to the tools which may then look anywhere within the packet, for example using DPI (Deep Packet Inspection) techniques to perform their analysis. Many Network Performance Management (NPM), security, Application Performance Management (APM), and Customer Experience Management (CEM) tools today use either flow-based techniques, packet-based inspection, or even a combination thereof.

With SDN, it is conceivable that the need for SNMP style monitoring of individual devices diminishes as much of the status information for the individual devices may now be available at the centralized controller. The controller may choose to export this using a variety of different APIs. However, in an SDN world, the need for flow- and packet-based monitoring (i.e. traffic-based monitoring) will actually increase and in fact will become an integral component of the SDN deployment. This is primarily because of two reasons.

1. The need to monitor and manage the SDN deployment itself
2. The need to monitor and manage the dynamic IT infrastructure that SDN will enable
1. Monitoring SDN Deployment Challenges

SDN breaks apart the traditional network switch/router/appliance by abstracting the control plane and centralizing it at a controller while leaving the data or forwarding plane on the individual network switches. This brings operational simplicity by not having to manage every switch/router individually, and having the controller act as the central point of management and control. However, it brings about a new set of challenges that will need to be addressed through increased traffic-based monitoring solutions. Some of these challenges are outlined below:

Controller and Switch Synchronization

In a large SDN deployment, ensuring all devices in the deployment stay synchronized with the controller can be a challenge. The state information associated with a large number of devices that is centrally maintained at the controller may get out of synchronization with the actual devices. This can be due to a variety of factors such as latency issues between the controller and the devices, packet loss in the network, the complexity associated with dealing with disparate devices each having different capabilities and different internal resources such as table sizes, or even software or hardware issues including software bugs or programming errors. Depending on the implementation, the devices may re-synchronize with the controller or may not be able to re-synchronize back with the controller. In either case, the state of the network while the situation persists may be unpredictable. In order to rapidly detect and correct such situations, it will be necessary to monitor traffic from the network switches and ensure that the network is performing as expected within the bounds of what is considered normal.

Further, being able to correlate network traffic activity to what the controller expects the network switches to be doing is going to be a critical aspect of ensuring the success of SDN deployments without which it will become exceedingly difficult to troubleshoot and identify root cause problems in SDN deployments. In fact, being able to provide a closed loop solution where a set of “always-on” network traffic-based monitoring solutions (for security, for network performance management, for customer and application experience management, etc.) are constantly monitoring and auditing for anomalies and then working with the controller to tune or optimize the SDN deployment may be necessary both for optimal performance, as well as rapid troubleshooting. In other words traffic-based visibility will need to become an integral part of the SDN deployment in order to ensure its success.

Network Virtualization Monitoring

The adoption of new technologies like VXLAN and network virtualization makes it challenging for packet-based analysis tools for a few reasons. The first is that they add additional packet header information which tools are unable to recognize easily. The additional headers also add processing overhead to the tools which are now required to not just understand the new header, but be able to parse the packets beyond the new headers, strip the new headers, etc. The issue at hand is not limited to VXLAN, but is rather indicative of the rapid change in technologies taking place rendering it difficult for tools to keep up with the different forms of encapsulation and packet formats being put in play for SDN.

Secondly, in many cases network virtualization technologies such as VXLAN tend to be hypervisor-oriented technologies i.e., the tunnel encapsulation/origination and termination may occur within the hypervisor making the physical network completely unaware of when tunnels and virtual overlays are being created and torn down. This makes troubleshooting and network performance management very difficult. For example, if a data packet was sent from one virtual machine to another using a VXLAN overlay, but did not make it to the other end, it becomes difficult to determine whether the packet was lost in the hypervisor, in the underlying physical network, or as a consequence of the overlay tunnel not routing traffic correctly or because the destination dropped the packet. Finally, by creating two logical forwarding planes—the overlay and the underlay, the need to monitor both the planes independently, as well as to correlate what’s happening in one plane with the impact to other plane will be important.

These kinds of issues will require new types of traffic analysis tools that enable rapid correlation and troubleshooting of issues in both the physical underlay as well as the virtual overlay networks. And serving up the traffic to the tools in a form that the tools can understand will become an important piece of the monitoring solution. This type of functionality can readily be done in the Gigamon Visibility Fabric™ which can serve up traffic to the tools from both the logical overlay and the physical underlay, along with normalizing the traffic to what the tools can decipher. Gigamon’s Visibility Fabric is a solution that delivers traffic from the production network, to the tools that are used to monitor and manage the network, and along the way perform traffic optimization functions such as stateful de-duplication, or flow record generation to help offload tools.
Hybrid Deployments

Most SDN deployments will need to function in conjunction with traditional network deployments for several years to come. In many cases traffic will need to straddle both these environments. For example, client-server traffic may originate from a client in a traditional network but may be served up by applications/servers in an SDN environment. Ensuring that the traffic bridged between the traditional and the SDN environments does not suffer a performance impact, or a security breach, or at its basic level is simply getting forwarded correctly, will require traffic-based monitoring across the boundaries of the traditional and SDN worlds. In other words, visibility of traffic traversing the physical and SDN worlds will be important both from a performance as well as from a security perspective. Once again, this can be readily accomplished by leveraging a Visibility Fabric that delivers traffic from both the SDN and traditional worlds to the set of tools that are used to monitor and secure the two environments. This topic has also been covered by analyst Lee Doyle who writes,

“What’s more, integration of SDN/virtual networks with legacy physical networks will require tools to model and measure performance and latency, as well as provide comprehensive network mapping that reflects both environments.”

Figure 3 below captures how traffic-based monitoring in the previous scenarios may be accomplished using a single Unified Visibility Fabric to drive traffic-based visibility to tools.

2. Monitoring the Dynamic IT Infrastructure Enabled By SDN

The promise of SDN is that it will enable very dynamic network environments characterized by mobility, policy, and elasticity of compute, storage, and applications. In effect, networks which until recently were a bottleneck in the enablement of key trends, such as virtualization, cloud, and mobility, will now become an enabler. This will open up a whole new breed of applications, deployment models, along with new services and service level agreements. Environments characterized by mobility, dynamic, and virtual networks, as well as

Figure 3: A Gigamon Visibility Fabric™ platform can drive traffic-based visibility to tools for monitoring

1 Covered by principal analyst Lee Doyle of Doyle Research who writes “SDN, networking monitoring: Challenge or a change for the better?”
http://searchsdn.techtarget.com/tip/SDN-networking-monitoring-Challenge-or-a-change-for-the-better, (2013, December)
policy-driven networks, all enabled through SDN, will require increased investment in newer traffic-based monitoring and analysis solutions that previously did not exist or were not as essential. This in turn will require more intelligent control over the access and visibility to network traffic.

The Gartner report “Introducing the Network Performance Monitoring and Diagnostics Market” states:

“Future demand from virtualized networks and SDN, and the increased complexity and volatility this will introduce, indicate further development of NPMD tools to cater to the increased need for crossdomain diagnosis and troubleshooting aids.”

For instance, in environments driven by user or application mobility, even though SDN may dynamically reconfigure and adapt the network for example using VXLAN, the actual performance of the application will depend on various conditions such as network congestion, server performance, storage latencies, etc. In a more traditional static network environment, one could more easily engineer and predict the performance based on application requirements and network speeds at that location. Additionally, tools could be inserted at very specific tap points in the network to monitor traffic related to specific applications. However with applications moving dynamically from server to server, and the network getting dynamically reconfigured through SDN, it becomes very difficult to engineer and predict performance and user experience since the dynamic instantiation of overlays fundamentally changes the effective topology and connectivity of applications, compute, and storage.

Having traffic-based monitoring tools becomes critical in these environments to constantly, and in real time, evaluate how the applications are performing in such a dynamic environment.

However, unlike the traditional model, tapping at specific locations to insert monitoring tools no longer works, as the traffic for that application may no longer be visible at that tap point if the application has moved. As such the need to tap and deliver traffic to analysis tools almost becomes ubiquitous across the SDN deployment. In such environments the Visibility Fabric that can ubiquitously and pervasively deliver traffic from across the network to a set of centralized tools that rely on traffic-based analysis becomes an effective approach and indeed almost a requirement to enabling instrumentation.

Securing the Dynamic IT Infrastructure Enabled by SDN

Security is a challenge in the dynamic environments that SDN enables. With users, devices, and applications moving almost at will and the network dynamically getting reconfigured through SDN, addressing security, compliance, and audit becomes a challenge. Pinpointing the source of security threats in such a highly mobile environment will require not only rapid detection, but also location awareness of traffic and traffic sources, along with a comprehensive network-wide view of who is accessing the network, what is the user, device, or application doing on the network, where is the network being accessed from, along with a knowledge of when the network is being accessed. In fact, the source of an attack or the capture point of a hacker could easily be as mobile as the very applications they are sniffing. This will require enhanced traffic-based analysis (both flow- and packet-based) and again with almost ubiquitous coverage across the network. Once again, the most comprehensive way to achieve this type of traffic visibility is through the Gigamon Visibility Fabric that enables traffic delivery across the network to a set of tools that are used for security, performance, or user experience management.

Mobility and network virtualization are not the only deployment environments that will be enabled by SDN networks. As indicated earlier, SDN can be applied to address a variety of challenges including policy driven networks and traffic engineering, among others. Here too, for example in the case of policy driven networks, the controller may function as a centralized policy manager determining who is allowed to access the network, what is the user allowed to do, etc. However, while the policy controller may determine and push policy to the individual network switches, the ultimate enforcement of the policy will be done by the individual switches in the network. And with cheaper white box solutions coming from a variety of different sources with different implementations and capabilities, the only reliable way to determine if the policy is actually being enforced accurately or adequately is to monitor traffic and correlate that to the policy. Especially since the policy may change dynamically. In other words there needs to exist a closed loop mechanism to ensure that what the controller expects is happening, and what is really happening stay in synchronization. And the function that closes that loop needs to reside outside the SDN controller and network.

---

2 NPMD – Network Performance Monitoring and Diagnostics

3 Gartner Report, "Introducing the Network Performance Monitoring and Diagnostics Market", 29 July 2013
i.e., some form of an out-of-band tool otherwise the tool itself may become subject to the issues it is trying to monitor and manage. For example, it is conceivable that in cases where infrastructure is offered as a service, as users sign on for those services, the SLAs associated with different users would need to get updated/changed and enforced as users sign on and off. These SLAs would be implemented in an SDN world in the form of dynamic policy updates. This type of an environment is a stark contrast to the traditional static network environments we see today. Ensuring that the SLAs are being met through policy enforcement will require a set of tools that monitor the actual traffic to ensure compliance with the policies defined by the controller and implicitly the SLAs associated with those policies. In fact these types of deployments may give rise to a new breed of tools that do both traffic-based monitoring, and also interact with the controller to correlate traffic with policy. Without these types of monitoring and correlation tools, SDN deployments will be plagued with unpredictability, lack of accountability, and ultimately stalled acceptance.

Summary
As the applications of SDN take on broader deployment use cases and scenarios, one thing is clear. The fundamental nature of how networks are architected and deployed will change, enabling dynamic on-demand networking, greater policy-based control, and an increased interaction across departmental silos. The need for traffic-based visibility solutions in such an environment, along with increased correlation of traffic with controller policies and state will become an integral part of the SDN solution. Further, the dynamic nature of the network, compute and storage, will drive the need for delivering traffic pervasively across all segments of the network to a centralized set of tools responsible for the monitoring and correlation of performance, security analysis, and user experience. The Gigamon Visibility Fabric that works in conjunction with the SDN deployment to pervasively deliver relevant traffic to the monitoring tools, while normalizing the traffic to what the tools can interpret, becomes the most effective and reliable way to enable instrumentation for the SDN world.

About the Visibility Fabric
The Gigamon Visibility Fabric is an out-of-band network that delivers traffic from the production network to the tools required to monitor and manage IT infrastructure such as security, application and network performance, and user experience monitoring tools. A Visibility Fabric is very different from a traditional network. The Fabric taps into the production network (be it SDN or traditional) or connects to the SPAN/mirror ports of the network switches (white box or otherwise) to receive a copy of the traffic traversing the production network. That traffic is then forwarded to the tools based on the type of traffic that is relevant to the tools. There is a fundamental difference between how network switches and Visibility Fabric nodes forward traffic. Traffic within the Visibility Fabric is forwarded based on the content that is relevant to the tools.

Traditional network switches are highly optimized for address-based forwarding where traffic is forwarded based on address information in the headers of the packets. Within the Visibility Fabric, traffic is forwarded based on the content of the packets, as well as based on correlated traffic flows that straddle multiple packets. And furthermore, those traffic streams may need to be replicated within the Visibility Fabric so as to deliver them to multiple sets of tools. That packet replication is also based on the content of the packet as well as based on correlated traffic streams so as to ensure that just the relevant traffic is delivered to the tools. This makes the Visibility Fabric a highly specialized function that is very unique and different from traditional network switches. As we look to the future, this specialized capability of the Visibility Fabric will make it an integral but distinct component in ensuring the successful deployment of SDN solutions.

About Gigamon
Gigamon provides an intelligent Visibility Fabric architecture to enable the management of increasingly complex networks. Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies, centralized management and a portfolio of high availability and high density fabric nodes, network traffic is intelligently delivered to management, monitoring and security systems. Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.

For more information about the Gigamon Visibility Fabric architecture visit: www.gigamon.com