WHITE PAPER | FEBRUARY 2015

Managing the Software Defined World

Managing Your Infrastructure in the Highly Agile World of Software Defined Networks

Mike Shevenell and Tim Diep

Infrastructure Management Solutions, CA Technologies

Table of Contents

Executive Summary

Challenge

In today's application-driven business, IT can operate at a competitive speed only if services, applications, systems and networks become more agile. Virtualization and the cloud have decreased the speed of application and system deployments to minutes and seconds. Software Defined Networking (SDN) and Network Function Virtualization (NFV) bring agility to the network domain but will stretch network processes. Legacy management solutions, which rely heavily on manual processes, will not be adequate in next-generation networks.

Opportunity

IT management software must seize the opportunity to completely redefine infrastructure management to make it as agile as SDN/NFV-based networks. This situation demands infrastructure management solutions that not only keep up, but stay ahead of the highly dynamic environment. Current opportunities to couple provisioning and the monitoring as well as the analytical and notification aspects of management provide the possibility for great network stability and service delivery—even in the face of dynamic changes.

Benefits

Next-generation infrastructure management tools will be as agile as the software-defined world. The tools will have the ability to keep up with the pace of frequent infrastructure changes. These new tools will redefine the role that management plays in business operations. This new role will assure network service where the management systems not only report but also help prevent problems by capturing a clearer and more current view on the state of networked resources.

Section 1:

Dynamic Infrastructures Challenge Existing IM Tools

Highly dynamic environments composed of SDN-enabled components present numerous challenges to current tools. The frequency, scope and scale of configuration changes enabled by SDN exceed anything the network industry has seen to this point. Additionally, NFV-based components add to the challenge by permitting ephemeral network components to go into and out of existence dynamically—based on rapidly changing business and user requirements.

The current state of SDN and NFV is not unlike server and compute virtualization several years ago. Server technology broke new ground with virtualization, enabling dynamic and automated resource allocation in line with the business demand, thereby improving resource utilization and contributing directly to the bottom line with an improved return on investment (ROI). At this point, server virtualization is a relatively mature technology and is widely used in modern IT infrastructures and business strategies.

Until recently, the networks supporting these dynamic servers remained relatively static in configuration. Complex network devices created vendor-specific proprietary silos and added to network complexity, inflexibility and management challenges. However, in the last several years, network virtualization efforts have gained momentum as an extension to the virtualization of computing resources. VPNs, virtual switches (VS) and distributed switches (DS) try to enable networking for the virtual machine, optimization of resources and centralized management. At the same time, SDN has emerged as a new network paradigm, transforming networks by abstracting the physical network devices from the programmable software solutions. Separation of forwarding and control capabilities with SDN is designed to enable network flow that is indifferent to the vendor-specific physical devices and proprietary protocols. One of the prime benefits of this separation and centralization of the control plane is to enable a more global view of the network. This approach permits more intelligent traffic management policies to be developed.

The Challenges of Managing Agility

IT agility is necessary to drive success in today's application economy. New applications and business services, and the new infrastructure to support them are now deployed at an incredibly rapid rate, and with increased customization. Until recently, it was not possible to satisfy rapidly changing network requirements, and to change them again. Requirements change, as they are driven by an ever-changing business landscape. Traditional networks services were offered with the goals of predictability, reliability and stability. These goals are more important than ever and will be more difficult to retain in the new agile SDN/NFV environment.

However, increased agility has its challenges, as Rajesh Rajamani of Spirent aptly stated at a recent SDN conference: "Agility without predictability is just chaos."[1]

Indeed, the potential for chaos is overwhelming because legacy tools were not designed to keep up with the dynamic nature of SDN/NFV networks. The current business climate requires all the benefits of agile SDN and NFV environments without losing all the attributes of predictability, reliability and stability that we strived for in the currently pervasive, static network paradigm.

Additionally, great network agility can render conventional monitoring tools ineffective.[2] With SDN/NFV, the network devices and services that current-generation IM tools are monitoring can quickly change underneath them. This leads to the problem of "stale state" in the management and monitoring systems.

One example is the monitoring of an interface that has a specific utilization threshold set. If a major service is added to, or removed from, this interface, utilization could dramatically change, which leads to an unnecessary event or alarm. A worse problem might involve a newly provisioned service that is not yet monitored by monitoring tools because the tools are not aware of the new service.

The Challenges of Managing Diversity

While the transition to the highly agile SDN/NFV environments is progressing rapidly, industry leaders expect the coexistence period with legacy technologies to last a decade or more.[3] During this transition, infrastructure management solutions must offer the ability to manage the following matrix of possibilities in multi-vendor deployments:

- SDN/NFV and traditionally provisioned devices and services[4]
- SNMP and non-SNMP manageable network devices
- Physical and virtual assets (switches, firewalls, network function servers, etc.)

Consequently, infrastructure management solutions must manage all legacy equipment and services seamlessly with the emerging agile environments for the foreseeable future.

The relative immaturity of SDN/NFV products makes managing these environments more difficult. Standards are emerging slowly, and there are a wide range of vendor proprietary tools and Application Programming Interfaces (APIs). The brisk pace of mergers and acquisitions continues as vendors of major network software and equipment position themselves in this vigorous market.

One wild card in the discussion is the very strong position of open-source software options in the market. One leader in this effort is the OpenDaylight Project (ODL), a Linux Foundation collaborative project. With the number of open source options growing quickly, the development community has almost too many choices.

There are a wide array of choices, approaches, APIs, vendors and offerings. Everyone is claiming some aspect of software-defined “something”; the acronym “SDx” referring to networks, data centers, security, etc. is increasingly common. Consequently, one of the biggest challenges of embracing this emerging technology is knowing where to start.

The Challenges of Limited Visibility

Today’s monitoring and management tools lack the visibility into software defined network and network function virtualization environments that network operations teams require. These blind spots are caused by:

- Fragmented controller market (numerous vendors and open-source software)
- Competing proprietary control approaches (OpenFlow, Cisco onePK, Path Computation Element Protocol and others)
- Controllers are often isolated to specific network segments or areas (optical, core, edge or access) with little visibility for end-to-end operations[5]
- Controllers are isolated to newer SDN enabled components, and have little awareness of legacy devices

Consequently, these blind-spot conditions lead to a patchwork of domains or segments with limited visibility.

The Challenges of Scale in Next-Generation Networks

In addition to the dynamic network landscape, network scale is increasing rapidly. One element of the application economy is an exponential growth in users interacting with organizations via mobile access and applications. web-scale computing is no longer confined to the major consumer websites such as Google, Amazon and eBay, but affects nearly all organizations that interact with customers via mobile devices. The Internet of Things (IoT) will increase the number of manageable objects by an order of magnitude in the near future. Networks of the future (powered by SDN/NFV) will be expected to handle unprecedented amounts of data in real time from an enormous variety of sources. These data sources will include all of the traditional IT devices, as well as health sensors, home and traffic automation, and municipal resource monitoring, just to name a few. The requirements of web-scale computing and IoT will become "Agility at Scale."

The Challenges of Using SNMP in SDN Networks

The dominant network monitoring approach today is through the Simple Network Management Protocol (SNMP). While network management tools have utilized SNMP for more than 20 years, emerging environments driven by SDN and NFV present significant challenges to continued use of SNMP for management. Device complexity and the associated Management Information Bases (MIBs) have grown dramatically. For some time, industry observers have been concerned about the future of SNMP, some predicting its decline and even its demise.[6] This sentiment is due to the inefficiency of extracting large volumes of data via SNMP, which can lead to performance problems for both the device and the management system. The dynamic nature of SDN/NFV exacerbates this situation because of the amount and frequency of configuration change expected in the more virtualized and dynamic network environment.

Several years ago, it became "best practice" to perform a network discovery operation once a week. This was typically a resource intensive operation for both the network management system and the monitored devices. Consequently, discoveries were run infrequently to limit impact on network resources and services. In some environments, discovery cycles have been increased to once a day due to more frequent network configuration changes. SDN and NFV create a need for much more frequent updates on network discovery and configuration. Executing discovery as often as once an hour could become inadequate, if that is even possible or advisable.

In addition to the basic discovery operations, an integral part of SNMP is its polling paradigm. Using the current approach, network performance attributes are queried periodically—typically every 5 to 15 minutes. This represents an unacceptably long delay for many circumstances and use cases. Increasing the poll rate to one—minute intervals can improve the "responsiveness" of management and monitoring, but it comes at a high cost of increased resource utilization for both the device and the management solution. Another impact on resources can be real-time SNMP notifications. Notifications (traps) afforded in SNMP are utilized to provide near real-time indications, but they can cause network resource issues due to the high volume of what can be low-level events. Imagine a major network topology change: this could result in thousands of traps flooding the management system in a very short period.

Section 2:

A New Paradigm for Managing Dynamic Networks

It is no longer adequate for operations teams to reactively monitor networks; monitoring must be current, near real-time and proactive. One expert in the field commented that, “SDN makes Network Management a first class citizen.”[6] Indeed, things have changed because so much in the network is changing.

The new vision for infrastructure management is defined by the following required attributes:

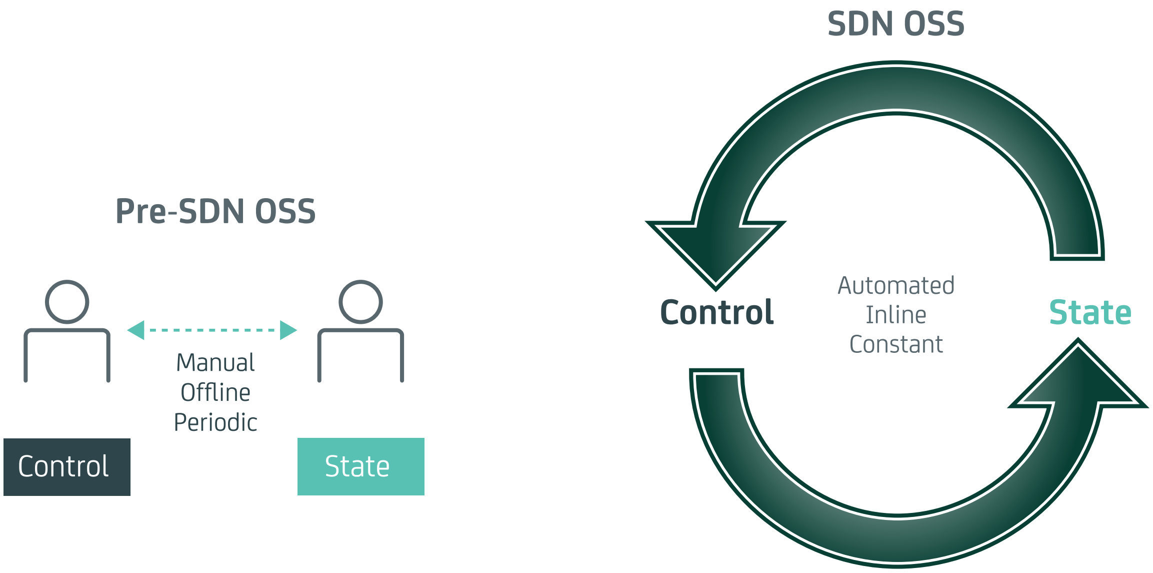
- Tightly coupled to network operations, orchestration and provisioning
- Agility as dynamic as the network it manages
- Real-time response to configuration changes

Historically, infrastructure management was responsible for managing hardware-centric, relatively static networks. This has changed dramatically in the software-defined world. Networks have to be as agile as the services they power; “service velocity” is now the ultimate Key Performance Indicator (KPI). In evolving infrastructures, “service velocity” describes the speed with which services can be configured, deployed, modified and retired.

Figure A depicts the contrast between the management models of legacy environments and emerging SDN-based environments. Many legacy OSS tools (Operational Support Systems, as shown on the left) separate control and state (orchestration/provisioning and monitoring).

Figure A.

Comparing Legacy (left) and SDN (right) Solutions

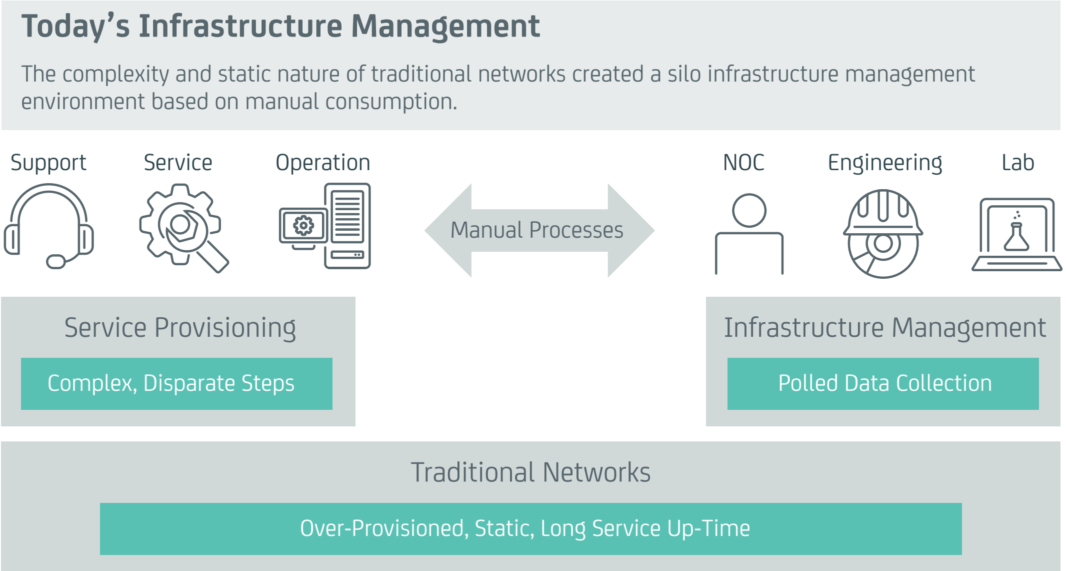


Legacy management is often performed in silos by disparate tools and teams. The coupling between tools and teams is weak, and often requires manual interactions and processes to achieve cooperation. These complex and frequently manual interactions are the source of errors and decreased efficiency. Conversely, modern, flexible networks based on SDN and NFV (shown on the right) require tight coupling (between orchestration and monitoring) and closed-loop control to achieve their promised benefits at scale.

Figure B illustrates how the complexity and static nature of traditional networks created a management environment of silos based on manual configuration.

Figure B.

Today's Networks Requiring Manual Processes



Today's Infrastructure Management

The complexity and static nature of traditional networks created a silo infrastructure management environment based on manual consumption.

In agile, software defined networks, the interaction between control and state must have the following qualities:

- Automated: Not requiring manual intervention or processes
- Instantaneous: Not relying on delayed communications
- Continuous: Not based on batched or polled operations

Active infrastructure management solutions for the next generation bring the additional capabilities of:

- Mapping and correlating virtual-to-physical domains
- Correlating network policies based on service changes
- Authorizing change requests using network intelligence on capacity and state

Architecture for Agility

Provisioning and monitoring have often existed as separate entities within network tools, operational and engineering teams. To meet the needs of SDN/NFV, provisioning and monitoring must come together in a unified architecture to manage today's software defined, agile networks. Tight coupling between network control (provisioning/configuration) and state (monitoring) will provide the visibility for assuring the required service levels.

An example of this type of architecture is shown in Figure C.

Figure C.

Infrastructure Management Architecture Showing Closed Loop Control

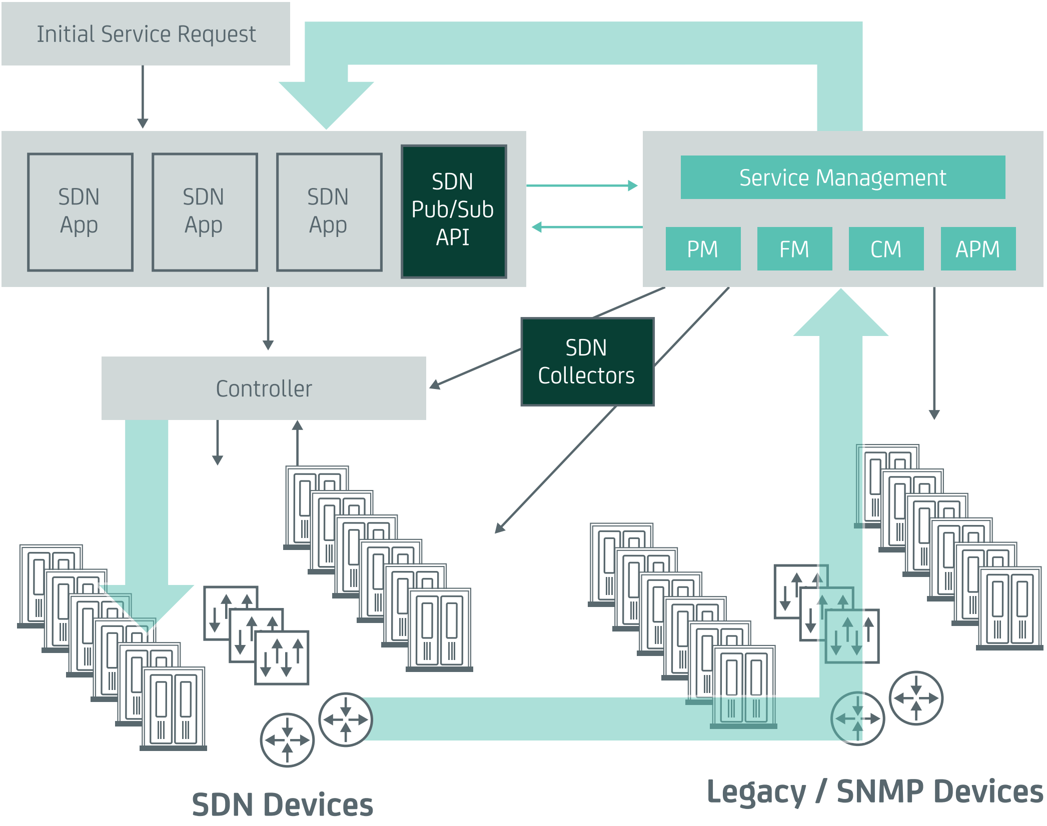


Figure C shows a tight, closed-loop control approach with continuous feedback, which operates bi-directionally. The feedback is:

- From provisioning to monitoring—communication of control changes
- From monitoring to provisioning—communication of state and state changes (fault and performance)

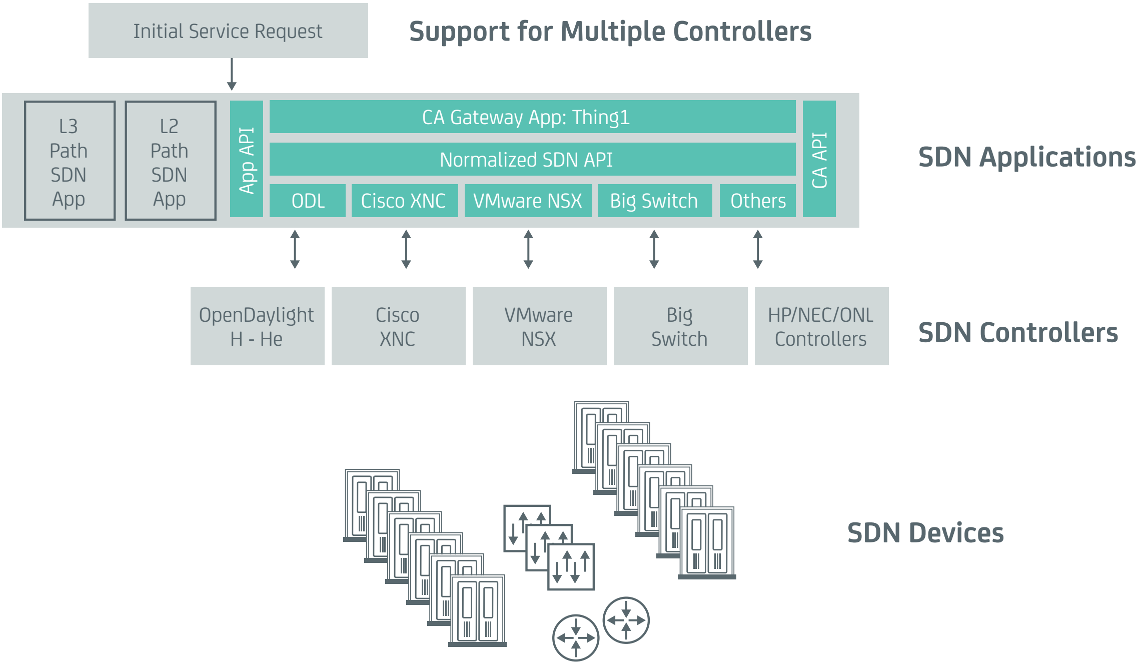
The provisioning/orchestration entities provide real-time communications of configuration changes to the network monitoring system, and enable a solution to today's problem of stale state information. Without this modification, today's monitoring systems have little or no way to know the network underneath them has changed so dramatically.

Open Architecture for Flexibility

Although early adopters in the communication service provider, cloud service provider and financial services industries are deploying SDN and NFV in production networks, these deployments have not converged around a single SDN controller or deployment architecture. Additionally, the SDN controller market is relatively immature, and significant developments are frequent. Consequently, the infrastructure management architecture must recognize this fact and adapt easily to various solutions and architectures. Figure D shows an architecture that provides management for many of the top SDN controllers, and the ability to adapt to new ones.

Figure D.

Architecture for Adaptability Using Modular Approach



The modular approach presented here creates an abstraction between the communications and services of multiple controllers and the applications responsible for managing these resources.

Architecture for Application Visibility – Application Performance Management

In addition to managing the resources orchestrated by SDN (like devices and NFV instances), it is essential to manage the complex ecosystem of applications that provide this orchestration. This ecosystem includes both SDN controllers and the numerous applications and interconnects that form this system. These foundational applications include name resolution, path computation, QoS guaranteed calculations and security verification. These applications are instrumental in providing the commonly known services, such as firewalls, load balancers, WAN accelerators, deep packet inspection solutions, etc.

Service chaining of NFV-based functions presents a new and compelling use case for Application Performance Management (APM). APM is used to manage the applications (elements of the service chain), as well as the interconnections between applications. This is used to ensure end-to-end system throughput and to identify any bottlenecks in performance along the entire service chain. Traditionally, service chains were made up of interconnected physical (purpose-built) appliances (firewalls, intrusion detection systems, load balancers, etc.). As service providers and large enterprises adopt NFV-based services, these may now be instrumented for APM. This combination of NFV and APM provides greater insight and visibility into the overall application ecosystem than ever before.

The Role of the Open-Source Software in SDN/NFV

One may draw a parallel between today's SDN open source environment and the Linux open source movement of the late 1990s. There is a lot of activity and an array of choices. The scope and capabilities of SDN open-source software tools is significant, and portends to become a de facto standard in many segments.[7] One participant at the 2014 Open Daylight Summit noted:

> "You can't keep the same standards process in place once you become more software based." [8]
>
> Guru Parulkar of Stanford University and Open Networking Lab

While the number of open source options continues to grow, the OpenDaylight (ODL) Project has emerged as a clear leader. Although many of the major IT equipment vendors and players are members, there are very few service providers currently enrolled. One possible challenger to the dominance of ODL is the Open Networking Laboratory (ON.LAB), which is attracting more service provider members.

The rapidly expanding open source movement creates challenges for infrastructure management because it must keep up with the frequently changing management and monitoring landscape. Continuously evolving immature interfaces complicate matters further. Multiple approaches and emerging technologies from multiple vendors require a new breed of management tools that can evolve and adapt along with the resources they monitor.

Section 3:

Management That Keeps Up With Your Network

The new generation of SDN/NFV networks require a new generation of infrastructure management solutions to deliver the value in the software-defined world. Components of next generation infrastructure management solutions include:

- Tight coupling of monitoring to orchestration, provisioning and configuration changes
- Support for multi-vendor, multi-technology, multi-state deployments
- Co-existence of SDN/NFV and legacy technologies for the foreseeable future

Tight Coupling of Monitoring with Orchestration, Provisioning and Configuration Changes

To achieve the high quality of service that business requires, organizations need to monitor the appropriate infrastructure components at the appropriate time. Tight coupling of monitoring with orchestration, provisioning and configuration changes can reduce the typical delays between monitoring and control. This coupling will become a critical requirement as components and services provisioning becomes more dynamic. The reduction of latency between orchestration, provisioning and change with monitoring to near zero will help ensure continuous service quality from the moment the service is activated to its retirement.

Support for Multi-Vendor, Multi-Technology and Multi-State Deployments

SDN is a rapidly maturing technology, which attracts significant interest in both service provider and large data center environments. While many organizations may have a dominant network equipment vendor in certain network segments, there is a wide variety of equipment when considering end-to-end operations.

These environments are:

- **Multi-vendor**: Cisco, Juniper, VMware, Alcatel-Lucent, Huawei, HP, Dell, Brocade, Intel, Extreme Networks, etc.
- **Multi-technology**: routed, L2 switched, optical, MPLS, MPLS LSP, VxLAN, NvGRE, STT, etc.
- **Multi-state**: physical, virtual and hybrid versions of these technologies

Infrastructure management solutions to support dynamic, multi-faceted environments must be designed to adapt, adjust and advance with the changing ecosystem. In a word, the solutions must be agile.

Coexistence of the Future with the Present

While the transition to the highly agile SDN/NFV environments is progressing rapidly, experts expect a coexistence period with legacy technologies to last a decade or more. During this transition, infrastructure management solutions must be able to manage both legacy (traditional) and SDN/NFV-based networks simultaneously and seamlessly. Network-based services will typically traverse both legacy and agile, software defined entities as well as physical and virtual components. Infrastructure management solutions must provide an end-to-end view of the composite network environment.

Enabling the Future

The new role for infrastructure management goes beyond the monitoring of systems in response to changes. The role now includes acting as a trusted advisor when planning and deciding how and where to deploy new services. This new role will encompass:

- Providing information on the co-existence of SDN and non-SDN networks
- Providing analytics on most/least used resources and services
- Providing recommendations on optimal paths or resources for new services
- Preventing over-provisioned resources that lead to network or service failures
- Acting as a “source of truth” for Application Layer Traffic Optimization (ALTO) servers

The first of these new tasks provides a capability that does not exist elsewhere. Typically, an SDN controller will have knowledge about the SDN-capable systems and services it controls, but will have little or no knowledge outside of that domain. In addition, as many environments deploy a separate SDN controller for each network domain (optical, core, edge or access), they have no end-to-end visibility[4]. This is provided by next-generation infrastructure management systems.

Section 4:

Conclusions

Networks are changing dramatically and quickly, and these changes demand a new generation of infrastructure management tools, approaches and standards. These new tools must be agile, real time (nearly) and proactive. They must offer the promise to finally “close the loop” among the traditional operational silos.

CA Technologies, with its long history in multi-vendor, multi-technology infrastructure management, understands these challenges, and has the experience and insight to lead the future of the software-defined world. CA Technologies expertise in fault, performance and application management of networked resources and services forms a foundation for new offerings that deliver on the promise of SDN, which is a stunning example of businesses that are being rewritten by software.

Section 5:

About the Authors

Mike Shevenell is a Software Architect in the CA Technologies Infrastructure Management group focusing on SDN and NFV management. Prior to his current assignment, he was part of the development team for CA Spectrum dating back to its first release in 1990. Over the years, he has worked on a number of projects related to network services management, including IP services management applications for MPLS, MPLS L3 VPN, MPLS VPLS, multicast, QoS, enterprise VPNs and BGP. He has participated on the OMG SDN standards group as well as being an invited member of Cisco’s onePK Advisory Group (now Cisco DevNet).

Tim Diep works in Product Management at CA Technologies focusing on CSP Infrastructure Management including SDN-NFV management strategy and solutions. Prior to joining CA, Tim spent more than a decade at Juniper Networks and Motorola, helping to shape the early days of cable HSD broadband, telco CDN, router integrated network functions and mobile video delivery. Tim holds patents in “applying differentiated services” and “granular access control management.”

[1] Rajamani, Rajesh," SDN/NFV Infrastructure and Orchestration Testing," SDN/MPLS Conference 2014, used by permission of Spirent Corporation.

[2] Shevenell, Michael & Normandin, Jason, "Impact of Software Defined Networking on Infrastructure Management," CA Technology Exchange, November 2013. http://www.ca.com/us/lpg/ca-technology-exchange/impact-of-software-defined-networking-on-infrastructure-management.aspx.

[3] Matsumoto, Craig, "NFV Market Size: How's $2B for a Guess," SDN Central, April 1, 2014. https://www.sdncentral.com/news/nfv-market-size-2b-first-guess/2014/04/.

[4] IETF RFC 7149, "Software-Defined Networking: A Perspective from within a Service Provider Environment," March 2014. https://tools.ietf.org/html/rfc7149.

[5] McGlynn, Brian, "Is SNMP Dead?" Davra Networks Blog, http://www.davranetworks.com/news/is-snmp-dead.

[6] Brockners, Frank, "Infrastructure Software: SDN makes network management a first class citizen." Cisco Blogs, http://blogs.cisco.com/getyourbuildon/sdn-makes-network-management-a-first-class-citizen-infrastructure-software/.

[7] Iwata, Atshushi, "Innovation for network businesses by SDN WAN Technologies – O3 Project", SDN/MPLS Conference 2014.

[8] Wilson, Carol, "Standards Lose Steam as Software Dominates," Light Reading 2/15/2014. http://www.lightreading.com/carrier-sdn/nfv-(network-functions-virtualization)/standards-lose-steam-as-software-dominates/d/d-id/707588.