How Can I Maintain Control of My Highly Dynamic and Complex SDN/NFV Network?
CA Virtual Network Assurance bridges existing infrastructure management capabilities to meet the needs of software-defined networking (SDN) and network functions virtualization (NFV) network velocity, reducing management complexity while improving network visibility.
Executive Summary

Challenge

The digital consumer in the application economy demands service delivery at lightning speeds—when, where and how they want it. Meeting this demand means that every business must become a digital business in order to be successful. This success will require a network transformation based on software-defined networking (SDN) and network functions virtualization (NFV) technologies, but today’s traditional networks and processes will not be able to cope with this next-generation network speed and complexity. For any network to stay relevant and competitive, the inclusion of SDN/ NFV in its strategic plan is paramount.

Opportunity

Redefining SDN/NFV assurance for tomorrow’s networks requires not just a technology change but an operational change as well. SDN/NFV demands fault and performance to respond quickly and dissect the most intricate service problems in a meaningful, actionable way. CA Virtual Network Assurance enables organizations to transition to SDN/NFV networks with their current infrastructure management investments and operational best practices and applies them to the new networks. In a single platform, the solution provides advanced collection, normalization and detection methods to extend network visibility and remove management complexity of the highly dynamic and complex SDN/NFV network stack.

Benefits

CA Virtual Network Assurance offers next-generation network performance and fault management capabilities needed to support a digital business transformation based on SDN/NFV network technologies. The solution offers the assurance for advanced and innovative service delivery and new product/market identification, strengthening DevOps practices by assuring test network performance and reliability, and reduces network capital expenditures (CapEx) and operating expenditures (OpEx) by maximizing infrastructure spend and avoiding over-provisioning of network resources.
Section 1:
The Challenge: Network Transformation Will Be Disruptive

The networking world is at the beginning of a transformation. A transformation that is not driven by a technical breakthrough but rather by a practical business necessity—the necessity for every business to become a digital business in the application economy. A digital business means speed in delivering products or services; it means meeting the consumer demand for customization and a-la-carte preferences; it means using applications and mobility to reinvent sales, marketing and operations. These goals can be accomplished via new network architectures based on SDN/NFV. For any network to stay relevant and competitive, the inclusion of SDN/NFV in its strategic plan is paramount.

Yet to begin implementing SDN/NFV, the business must plan for not just a technology change but a bigger operational change. And a big part of any operation is assurance of fault and performance. The need to revamp fault and performance assurance in SDN/NFV networks is glaringly obvious because of its speed and virtualization. The old way of doing fault and performance management relied on a slowly changing network and a simple service construction. SDN/NFV demands fault and performance to respond quickly and dissect the most intricate service problems in a meaningful, actionable way. The adoption of virtualization in networking brings revolutionary benefits in scale and agility, but it also brings a whole new level of complexity. Virtualization breaks traditional networking into dynamic components and layers that have to work in unison and that can change at any given time. Virtualization layers add greater performance vulnerabilities to the most basic network functions. For these reasons, each SDN/NFV architecture must be assured with enhanced fault and performance assurance to be deemed deployable.

Requirements

There are six principle requirements in SDN/NFV assurance:

1. Rebuild the multi-layer network stack.
2. Pinpoint known data-plane weaknesses.
3. Utilize the service chain framework.
4. Manage the old and new networks.
5. Keep pace with change velocity.
6. Participate in auto-healing.

Rebuild the multi-layer network stack: The simplest way to understand SDN/NFV is to think of it as a network with many software layers introduced through various forms of virtualization (Figure 1). The first job of any fault and performance assurance solution is to rebuild the network stack. Through reliable stack knowledge, one can begin to isolate fault and analyze performance.
Pinpoint known data-plane weaknesses. In the early days, the great benefits of SDN/NFV came with a cost. The cost was the vulnerabilities introduced into the data-plane. The truth is virtualization software and x86 hardware were not developed to host network functions and move small packets in high volume. Today’s SDN/NFV assurance solutions must provide necessary analytics to help customers stay on top of these known performance symptoms.

Utilize the service chain framework. Since the early days of assurance, the goal has always been to deliver fault and performance in a way that correlates to the business services being delivered to end-users. Now, SDN/NFV architectures have made it easier to accomplish this through the service chain framework which provides the necessary metadata to reconstruct the service chain in management systems. By utilizing this service chain metadata in representing fault and performance, customers can quickly relate network analytics to service impact.

Manage the old and new networks. SDN/NFV is a disruptive endeavor and most networks will start the conversion in pockets. Therefore, the old network and the new SDN/NFV pockets will coexist for a long time. Assurance solutions must be able to handle these hybrid networks from the standpoint of a single pane of glass as well as correlating fault and performance as the packets, flows and services traverse between the old and new networks.

Keep pace with change velocity. The use of automation software to provision the SDN/NFV network enables unprecedented service velocity. Monitoring this velocity requires more than just a faster collection engine. It requires added intelligence to data collection to track when activities spike. Transient data collection enables assurance solutions to keep pace with an always changing network landscape while optimizing data collection cycles.

Participate in auto-healing. The operational nature of SDN/NFV dictates that resolution through human intervention is not sustainable given its velocity of change. Assurance solutions should expect to support a growing need to interface with automation systems for timely resolution of performance issues.

“CA has delivered a technology that enables SDN management. Virtual Network Assurance is a good example of how incumbent vendors can address these new management requirements and help communications service providers succeed with SDN and NFV.”

- Shamus McGillicuddy, Senior Analyst, Enterprise Management Associates (EMA)
Section 2:
The Opportunity: Extend Visibility and Reduce Management Complexity of SDN/NFV Networks

CA Virtual Network Assurance was designed to meet the requirements described above. Figure 2 illustrates the framework of the solution. The framework starts with existing fault and performance systems, such as CA Spectrum® and CA Performance Management, to monitor the old network as well as the underlay in the SDN and NFV networks. CA Virtual Network Assurance is then added to monitor the overlay stack. In this decoupled packaging, you can re-use not only existing infrastructure management investments, but also apply operational best practices to SDN/NFV. Examples of operational best practices are UI, reporting, tenant management, device management, etc. With inventory and performance data from the old and new networks managed in the same solution, you now have not only a single pane, but you also can correlate intersecting network relationships.

CA Virtual Network Assurance, combined with existing fault or performance monitoring systems, can assure a variety of use cases. The main one being NFV based on the ETSI reference model. Specifically, CA Virtual Network Assurance 1.0 can support a variety of service chaining use cases, including vCPE, vGiLAN and vPE. The level of support possible is dictated by the types of VNFs an environment has. The second set of use cases is network virtualization in the data centers. These use cases are found in many enterprise data centers where, through network virtualization, the network becomes self-serviced. The third set of uses cases is an environment that is adopting OpenStack as their next generation cloud orchestrator. CA Virtual Network Assurance can monitor the resource inventories and performance of OpenStack as well as the health of the services provided by OpenStack.
Multi-Layer Stack and Service Chain View

At the core of CA Virtual Network Assurance is the modeling of SDN/NFV as a multi-layer stack. By applying this model to the collection, normalization, presentation and analysis of data, the solution is able to adapt to the component level dynamic nature inherent in these types of networks. This tracking is accomplished through a component level relationship mapping scheme that can maintain an updated network stack, while the tiniest component expands, contracts, relocates, transforms, etc. For example, CA Virtual Network Assurance outputs a uniform data model that represents the multi-layer stack. The data model also contains relationship IDs for each layer that ties them together. If a virtual machine (VM) changes, a new relationship ID for the VM layer will be created and sent upstream to the CA Virtual Network Assurance subscribers. This is a scalable way to track granular changes in dynamic SDN/NFV networks.

The adoption of service chain provisioning is a valuable turning point for the network management industry. Since the early days of SNMP, the goal was to present data in a format that resembles the delivered services to the end-users. While there have been numerous attempts to reach this goal, the end result was either too expensive or too difficult due to the integration complexities. What was missing was a glue that is now available in the form of service chains. CA Virtual Network Assurance supports service chaining and represents collection data, inventories and performance in a service chain view (Figure 3). The key is that, while there are plenty of service chain views in the industry showing the logical (VNF) connections, Virtual Network Assurance visualizes the logical VNF connections as well as the building blocks that support the chain for improved operational knowledge and troubleshooting. Based on this representation, our future vision is to provide performance and analytics at the block level, aggregated, flow analytics and associated application performance on top of the service chain.
Getting Started with SDN/NFV Assurance

Whenever there is a revolutionary technology like SDN and NFV, it is often difficult for the OSS team to decide how to get started. You can jump in head first with sophisticated topologies, correlation schemes, automating alarms and resolutions. This type of endeavor can be a very costly and time consuming implementation. Rather, CA recommends the following practical steps:

**Setup the assurance solution to recognize inventory and hierarchy.** When you are dealing with a complex architecture, it is essential that the assurance solution can model it in a way that’s easily understood by the operational team. A solid hierarchical model can also help you validate the integrity of the provisioning system.

**Track the inventory fluctuation.** This is unique to assuring SDN/NFV. Operations never had to track inventory fluctuation in the legacy hardware-defined network. In SDN/NFV, inventories come and go and move at any given point in time and in volume.

**Monitor resource usage** Now that you have insight into inventory fluctuation, your need an understanding of how these devices are utilizing resources in your environment. Resources should cover compute, storage and networking.

**Focus on known vulnerable areas.** It is well understood in the industry that many challenges in SDN/NFV will manifest themselves in the performance of the virtual switch (vSwitch) or virtual router (vRouter) depending on your architecture. Therefore, a proper out of the box dashboard should be available to focus on this SDN/NFV component. CA recommends monitoring network I/O performance such as throughput, drops and errors, in addition to various report options on CPU utilization of the vSwitch.
“By developing Virtual Network Assurance, CA has taken an important step forward in accomplishing the efficiency and agility goals so central to SDN and NFV, at the same time supporting practical integration of the new solutions into existing network and IT management applications.”

– Paul Parker-Johnson, Senior Analyst, ACG Research

ETSI Conformity

CA Virtual Network Assurance conforms to the ETSI model as an extension of the MANO components (Figure 4). The solution participates in NFVO, VNFM and VIM in order to collect the necessary data for service assurance. The data from MANO is not always the same based on system architecture. This is a reconstruction of the puzzle that CA Virtual Network Assurance needs to do to produce a uniform data model to the upstream client subscribers. In some cases, additional communication to the NFV Infrastructure (NFVI), VNF and enterprise management system (EMS) is necessary to get a comprehensive picture. CA Virtual Network Assurance can be described as a unification gateway that is necessary in an ETSI distributed management architecture. Without such a unification entity, disparate management client systems would be deployed resulting in correlation becoming much more challenging.

Figure 4.
CA Virtual Network Assurance and ETSI Reference Model
Section 3:
Benefits

By leveraging CA Virtual Network Assurance, your organization can realize the following benefits that support a successful digital business transformation:

- **Re-invent service delivery.** More than just guaranteeing Service Delivery but accelerating services to market quickly while having the ability to automatically tailor those services in real time to adjust for utilization or bandwidth constraints for an optimal user experience.

- **Reduce network CapEx/Opex.** While SDN/NFV technology will help businesses reduce spending on physical network infrastructure over the long term, CA Virtual Network Assurance will help our customers maximize infrastructure spend and avoid over-provisioning of network resources and bandwidth as a means of insurance for service outages.

- **Complete your DevOps vision.** The network is not thought of much when customers approach “DevOps”. Now CA can help them complete their DevOps visions by assuring the health of dev, test and live networks for improved development as well as production deployments.

- **Monetize your service offerings.** Businesses expect SDN/NFV to help them find new revenue streams and new markets from innovative service offerings. CA can ensure next-generation network reliability to support new service identification and offerings.

Section 4:
Conclusion

There are two important factors that will determine the success level of the SDN/NFV movement. The first is OSS transformation. What early adopters are realizing is that SDN/NFV technology is much more than an infrastructure upgrade; it requires changing the entire operational processes and personnel. CA, as a company, has been in the OSS business since the early 1990’s. Our products, like CA Spectrum and CA eHealth, efficiently manage much of the infrastructure in the industry today. More important than these solutions is the experience with OSS operational fit. CA understands how OSS teams efficiently operate with dashboards, run reports, management lifecycles, multi-tenant views, etc. As organizations move to SDN/NFV, migrating these operational fit features will be essential.

The second is software. At the core of SDN/NFV is software and it demands quality software vendors to manage it. And CA, from the beginning, is about software. CA develops software to enable our customers to develop quality applications via stable and reliable infrastructure. Furthermore, as SDN/NFV matures, issues such as self-service vulnerability and VNF certification testing will ultimately surface. CA has the knowledge and solutions in assurance, DevOps and security to help our customers solve these future SDN/NFV challenges.
Section 5

About The Author

Tim Diep is director of product management at CA Technologies, Enterprise Management Business Unit. A veteran of the Cable and Networking industry, he joined CA in 2014 to lead the concept development of SDN/NFV Assurance. Before CA, he was with Juniper Networks, where he developed early stage products for cable broadband, router services, and streaming video delivery. Tim holds patents in “applying differentiated services” and “granular access control management.” Email him at timothy.diep@ca.com

To learn more about CA Virtual Network Assurance, visit ca.com/vna.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.