Succeeding in the Market Transition to NFV and SDN with Orchestrated Service Assurance

Many CSPs are productizing or launching commercial-grade network-as-a-service (NaaS) products that include on-demand Ethernet and vCPE. Some examples of commercial deployment of NaaS services are AT&T Network on Demand and Colt DCNet-as-a-service. These solutions provide an array of benefits to the business service customer, including fast service activation, as well as self-service purchase through customers' portals. Best of all, network services can all be virtualized either on the customer premise or in the CSP's point of presence (PoP). This translates to reduced OPEX and CAPEX and an opportunity to further monetize the network with value-added services such as application visibility and control as well as security services.

Although the telecommunication industry's transition to network functions virtualization (NFV) and software defined networking (SDN) is well underway, it will still be at least 4-5 years before mass adoption takes place. CSPs have service-level agreements (SLAs) with their existing business service customers that they need to honor. While these customers are usually happy to adopt enhanced services, they aren't interested in an evolution of their existing network technology that doesn't bring innovative solutions to their problems. Introducing NFV and SDN technology components in one's network can therefore only be done in a risk-controlled manner.

NAAS REQUIRES SERVICE PERFORMANCE ORCHESTRATION

In previous network service evolutions – such as the transition to ATM/FR or IP-VPN – service assurance often came as an afterthought. However, when it comes to network virtualization, service assurance is mandatory at service launch. It holds the keys to automate service activation and fulfillment while meeting customer SLAs. Delaying the adoption of a carrier grade service assurance solution will impact service quality. To illustrate this impact, consider the following:

- **How can a CSP offer network connectivity with specific SLAs through their self-service portal without understanding the current end-to-end network performance?** Doing so would be similar to an airline selling tickets online without knowing when flights have sold out.

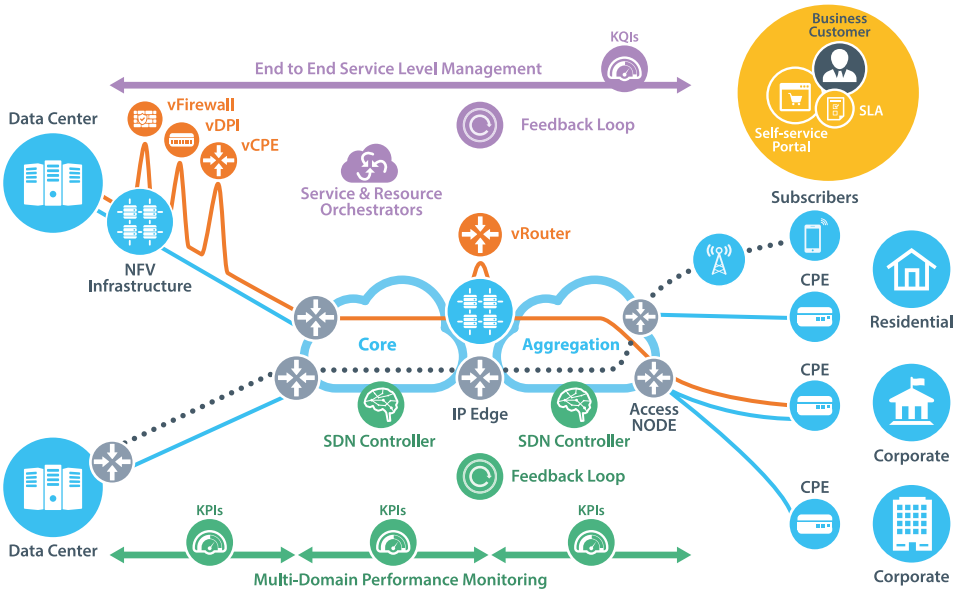
- **How can an SDN controller automatically reconfigure physical or virtual functions without understanding the impact on a subscriber's QoE or an enterprise customer's SLAs?** This would be like designing a building in a way that cuts costs and completes the project as quickly as possible, but neglecting to consider safety and building codes in the process, arguably the most important aspect to consider.

- **How can a VNF Manager(s) understand if virtual functions from different vendors have reached their limit without a solution that monitors their health and capacity in a vendor-agnostic manner?** This would be like the police trying to enforce highway speed limits using their own sight-based judgement.

Another widespread industry trend driving investment into NFV/SDN technologies is collaboration. CSPs are becoming more collaborative which will lead to wider cooperative competition, or co-opetition. Most Mobile Network Operators (MNOs) understand that their profit margin can be augmented by sharing some connectivity costs with their competition, which drives an increase in backhaul and RAN sharing deals. Business service providers need to connect their customer's employees in various offices, at home or on the go in every region where their customer operates. A U.S.-based business service provider will therefore need to contract last-mile connectivity with French and Chinese CSPs if it wants to establish VPN connectivity between Miami, Bordeaux and Beijing.

All of this drives the need for service APIs and an elastic OSS that can negotiate and fulfill connectivity orders on demand. The MEF address this need within their LSO concept and associated reference architecture.

Service Level Management and Performance Monitoring Role within NFV/SDN Based Networks



ORCHESTRATED SERVICE ASSURANCE BRIDGES THE CURRENT GAPS

As many CSPs have come to realize, service assurance is the missing link to productizing commercial-grade NaaS services that can deliver on their SLAs. They are also realizing that service assurance solves problems brought on by the complex nature of NaaS technologies. When offered as a commercial application visibility product, service assurance can increase the monetization potential of the CSP's business services.

During this disruptive industry transition, service assurance has a greater role to play. Companies that are equipped with a carrier-grade, multi-tenant, elastic and open performance assurance platform will maintain customer satisfaction and ultimately secure their successful transition to NFV-based services, reaping the associated rewards.

Performance management tools designed for the enterprise market lack some basic capabilities due to the unique requirements of CSPs. CSPs demand technology that can scale in real time, which requires partnering with companies that focus on designing and continuously enhancing solutions that mirror their requirements.

The adoption of NFV/SDN will push these requirements even further. Therefore, CSPs should understand the critical success factors when selecting their service assurance solution:

- A solution that can model CSPs' and MNOs' services with end-to-end SLA monitoring and vendor-agnostic performance monitoring capabilities
- A solution that has demonstrated its ability to follow CSPs' and MNOs' growth, and has proven itself in the market, supporting leading Tier 1 providers
- A solution offering RESTful APIs that allow users to exchange information with orchestrators, controllers and other complementary functions such as self-service portals
- A fully-automated solution that operates within in a real-time framework driven by self-service portals
- A solution that can easily adapt to new technologies and vendors
- A solution aligned with industry standards such as TM Forum and MEF lifecycle service orchestration (LSO).

Many of these success factors were demonstrated in the recent multi-vendor proof of concept (PoC) with InfoVista Oracle and Juniper as part of a TM Forum Catalyst. The PoC exemplifies how CSPs can achieve NaaS delivery that introduces NFV and SDN components into a network that is fully automated and assured. The result is greater business agility and a simplified end-user experience.

As CSPs and MNOs embark on their NFV/SDN initiatives, service assurance must be part of their strategy. Without it, the benefits of NFV/SDN cannot be realized and any success will be short-lived. Service performance intelligence that dynamically provides an assessment of network performance in real-time and full service-level visibility will ensure CSPs successfully bring these innovative services to life.

For further information, please download our whitepaper from *http://pages.infovista.com/WP-Assuring-Network-Service-Performance-Quality.html?utm_source=website&utm_medium=sidebar*