WHITE PAPER

Communications Service Providers
Service Assurance

PoC Demonstrates Automated Assurance and DevOps in Service Chains and 5G Network Slices

Intel, Telenor,* Arctos Labs,* Netrounds,* and RIFT.io* automate service validation and assurance with network orchestration and virtual test agents.

Introduction

To compete successfully in the market, communications service providers (CommSPs) must offer hyperscale, dynamic services that can be quickly configured and deployed while continuing to meet agreed-upon levels of service and security. Intel, Telenor,* Arctos Labs,* Netrounds,* and RIFT.io* constructed a proof of concept (PoC) demonstration that embodies management, orchestration, and testing in a virtual environment. The PoC, which uses Open Source MANO* (OSM) and software from the participants, was exhibited at Mobile World Congress 2017.

Challenge

Achieving service agility and ensuring exceptional quality of experience (QoE) for their customers are top goals for CommSPs, but increasing network complexity has introduced some challenges. This complexity is largely due to the expanding adoption of virtualization, software-defined networks (SDN) and network functions virtualization (NFV), and the frequent changes and updates that will be needed in multivendor virtual environments, as well as the fact that resources will be shared in these environments.

The ability to efficiently add and update customers and services is key to customer retention. Today, it is heavy on resources and expensive to test services with truck rolls or manual testing after each change or update. With the increased frequency of service changes and updates to further compound CommSPs' problems, it will become physically impossible.

Despite the complexity they bring, SDN, NFV, and other techniques make it possible to provide more dynamic and programmable services. CommSPs can automate many of the operational processes, including scaling and healing of services based on capacity demand, performance degradation, and faults. NFV also enables orchestration of Virtual Test Agents (vTAs) in conjunction with the network service (NS). The ability to orchestrate and automate service activation and validation makes assurance of network quality possible in complex, virtual environments, while at the same time saving operational costs and conserving resources. CommSPs need the right management, orchestration, and test solutions to ensure that their hyperscale data centers deliver carrier-grade service levels throughout the entire lifecycle. End-to-end service validation and assurance are particularly important during network service (NS) design, initial activation testing, service operation, and with each update or change. This is where DevOps approaches to network management become instrumental in maintaining dynamic network services with high customer QoE.

In a survey of more than 300 companies conducted by Dimensional Research,[1] participants said that human error caused 97% of network outages and that monitoring only predicted half of all network issues. Fifty percent also said that

Table of Contents

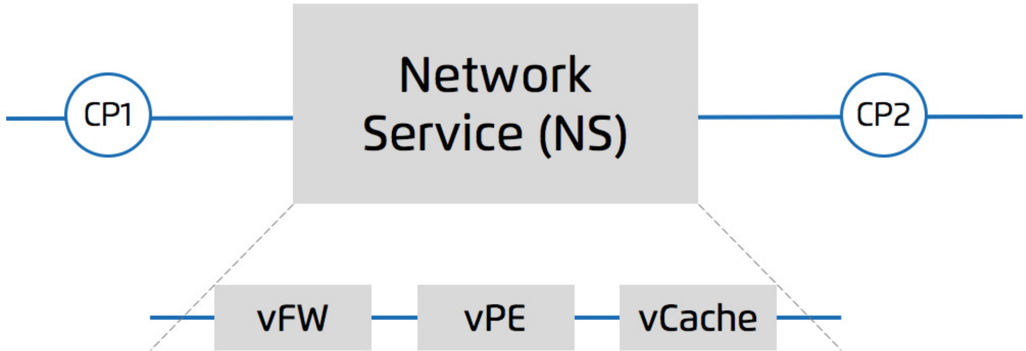

Figure 1. Network service[2]

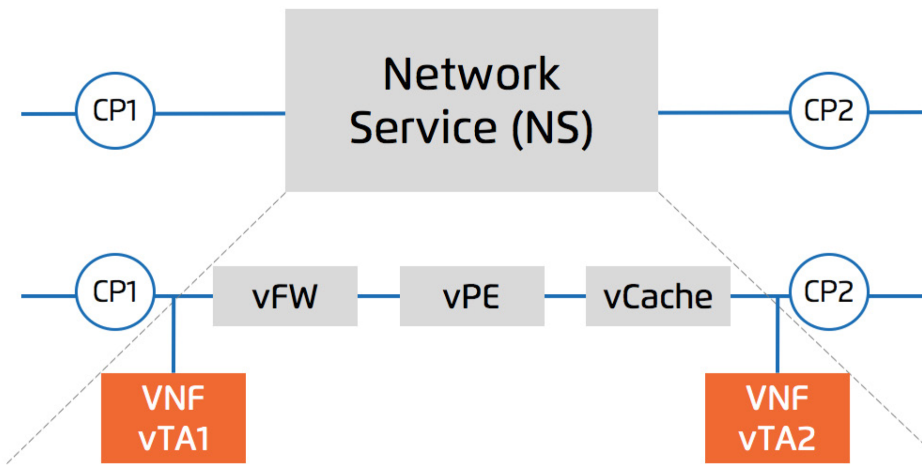

Figure 1a. Location of vTAs for testing a new network service[2]

network complexity is growing and increasing the incidence of network outages.

Active testing is key for DevOps, and it is needed to ensure end-to-end quality both prior to customer launch and after each and every update, no matter how small the change. Passive monitoring methods catch failures in a reactive manner, not in a proactive manner. Initial and ongoing testing with actively generated traffic from the end-user perspective is required to accurately assure QoE 100% of the time.

Dynamic Network Services

Network services are end-to-end products offered to customers; they come with full functional descriptions and specified performance. A simple example NS is shown in Figure 1, in which the network service that might be used to connect a customer to the provider's networks consists of a virtual firewall (vFW), virtual provider edge (vPE), and virtual cache (vCache).

As the purpose of the PoC is to demonstrate how testing of a new NS can be orchestrated and automated in dynamic environments, Figure 1a shows the location of the virtual test agents (vTA) within the network service.

NS components often require specific hardware support. Security applications, for example, may require processor-based encryption support. VNFs that handle significant network throughput will likewise benefit from intelligent network controllers. An automated means of matching requirements to resources is required.

Management and network orchestration (MANO) is the key tool that makes dynamic NS creation possible. MANO is the process of defining, cataloging, and connecting virtual processing and networking blocks, supported by intelligent workload placement. Other tools support automatic scaling of network services based on demand.

The integration of virtual active test and measurement elements with MANO is the special sauce that ensures successful activation and continued performance. The combination of NFV and advanced MANO provides CommSPs with the automation they need to meet customer need in minutes or seconds, rather than in days, weeks, or even months.

DevOps, the collaboration of development and operations functions throughout all stages of the development and fulfillment of a network service, provides significant benefits when applied to modern, complex networks. Creating a service that includes active testing in the network service design allows network operations staff to automate testing processes and ensure services are delivered right the first time to customers, whether it is the initial delivery of the service or after any small or significant update or change to the service.

5G Systems and Network Slices

5G systems are the next generation of wireless networking. Traditional cellular networks are predominantly a one-size-fits-all proposition, making them difficult to scale, adapt to changing demands, or meet the needs of new use cases. The growth in wireless data and services expected by 2020 will require automated networks that adapt to traffic that is expected to grow by a factor of 1,000, involve 100 times the number of devices, and require data rates more than 100 times current averages.[3]

5G systems will not only encompass high rate and high throughput networks, but will feature cross-domain integration and multiple radio access technology (RAT) environments. 5G is more about organization and optimization than new wireless technologies.

Network slices will be an essential part of 5G networks, enabled by SDN, NFV, and RAT advancements. Slices are essentially a connectivity service defined by a number of customizable software-defined functions that dictate coverage area, duration, capacity, speed, latency, robustness, security, and availability. 5G slices provide network services for specific types of users and devices and specify bandwidth, quality of service (QoS) profiles, and computational requirements. Network providers will offer networks as a service for common and specialized connectivity.

PoC Objectives

Intel, Arctos Labs, Netrounds, and RIFT.io, working with the team at Telenor Research, designed a PoC architecture for demonstration at Mobile World Congress 2017. It featured MANO as a key enabler for automated network service lifecycle management and end-to-end service activation, validation, and operations. The solution was exclusively software-based, eliminating the need for purpose-built hardware. All elements can be remotely operated, without the truck rolls and expensive field technicians normally required to assure service quality in operation. Active end-to-end service assurance was used to validate the service from the end-user's perspective.

The demonstration introduces the development and operations (DevOps) approach to network management. Testing of new services is included at design time, and then executed at run time prior to offering the service to subscribers. Full automation is included through API-driven programmable components and orchestration of Netrounds' vTAs.

RIFT.io's RIFT.ware* was used in conjunction with Open Source MANO for NFV orchestration (NFVO), while OpenStack* was used as the virtual infrastructure manager (VIM). VNFs were onboarded using the NFVO, including Netrounds' vTAs and a Cisco* CSR vRouter. RIFT.ware and OSM defined and orchestrated the network service, complete with vTAs.

OSM Release ONE was used for the demo with RIFT.ware's orchestration responsible for three primary functions:

- allocation of compute, network, and storage resources for deployment of VNFs and their interconnections
- automatic configuration of network functions
- creation of networks and traffic forwarding between the network functions in a coordinated way to form the network service

MANO-based configuration can be driven by input from CommSP/OSS high-level service primitives, VNF and element managers (EM), network infrastructure, and VIMs.

A network service was used to demonstrate service validation and run-time performance measurements. The demonstration also took advantage of OpenStack Enhanced Performance Awareness (EPA) contributions from Intel to allocate the required resources for the VNFs.

PoC Architecture

A high-level PoC architecture is shown below. In this PoC, Open Source MANO and RIFT.io are providing the orchestration. Netrounds Control Center interacts with the orchestrators via an application programming interface (API), and it also coordinates the Netrounds Virtual Test Agents (vTAs). VNF2 and VNF3 are undefined to indicate that the architecture is open to a number of VNFs that can be defined by the CommSP.

User Interfaces (UI) from RIFT.io and Netrounds Control Center are used and shown in the demonstration.

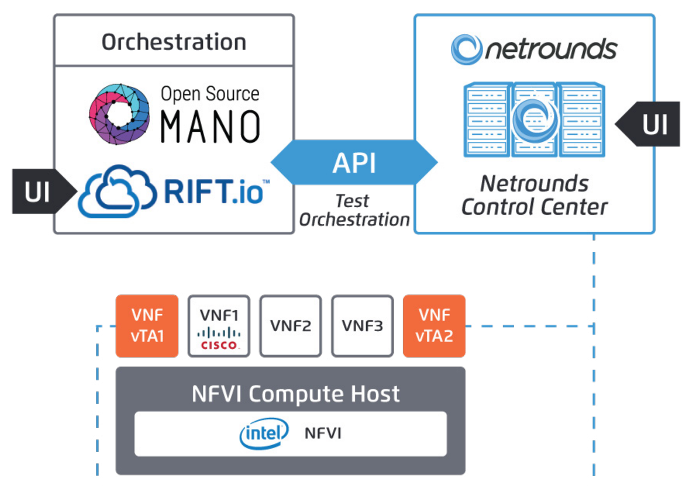

Figure 2. PoC architecture[4]

The PoC NS is shown in Figure 3. CP1 and CP2 are connection points to the network service, which, when expanded, consists of a vRouter (a Cisco Cloud Router–CSR) with Netrounds vTAs situated as NS endpoints in order to test the service end to end.

The three VNFs are shown in Figure 3. Virtual links connect the vTAs to the vRouter VNF. The vTAs send active test traffic through the vRouter service.

Several industry standard tests were run to validate performance:

- **TWAMP** – Two-way active measurement protocol was used to measure loss by reflecting traffic toward the vRouter.

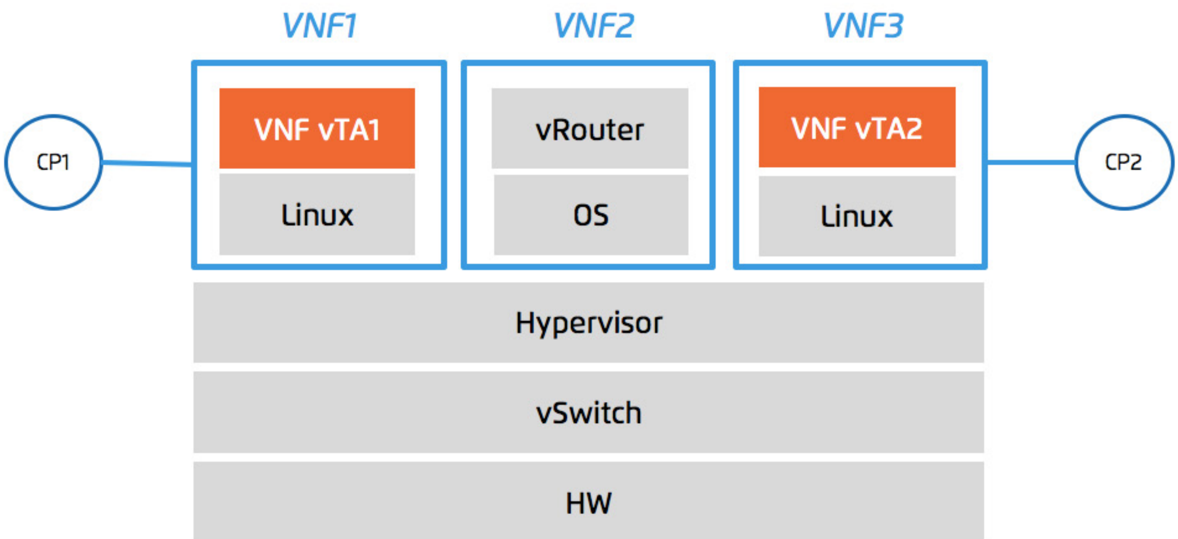

Figure 3. PoC Network Service[2]

- **Path MTU Discovery** – This test verifies the maximum transfer unit size through the service chain.
- **QoS Validation** – For different types of service level agreement (SLA) services corresponding to the network slices (shown below in Figure 4), this test verifies that differentiated services code points (DSCP) in packet headers that indicate the level of service requested for traffic were adhered to.

This initial demonstration illustrates how vTAs thoroughly validate NS functionality. Testing occurs prior to service turn-up, while in production, and after any software and configuration updates or changes. The vTAs also continuously monitor traffic during normal network usage so that network quality issues or SLA threshold violations are reported immediately and proactive problem resolution may occur as soon as possible.

The network service (NS) associated with the simplified demonstration, however, represents only a small part of an entire network and several network slices with differing SLA requirements based on their real-world applications. Figure 4 is a more representative network, spanning several elements in an end-to-end connection from end-user to the requested service with different network slices, according to QoS requirements. It is critical that complete end-to-end service connections be tested. Proper testing and monitoring must likewise be undertaken to assure service QoS requirements are being met. vTAs deployed at each end of the network service or slice accomplish this task for service validation, continuing operation, and SLA compliance.

Three network slices are outlined below. Each network slice has a critical SLA requirement matching its customer and use case:

- A mobile broadband (MBB) slice is required for residential subscribers, and is a best effort Internet service. Throughput is the critical key performance indicator (KPI) for SLA requirement assurance in this instance. A network service for this real-world application may include a vCache and a virtual deep packet inspection (vDPI) VNF.
- The massive Internet of Things (IOT) use case requires low packet loss to meet SLA requirements. A vFW and virtual IOT (vIOT) gateway (GW) may well be included in this use case.
- Real-time industrial application SLA requirements center on low latency. This is of crucial importance since these applications are very sensitive to any network latency or interruptions. This is illustrated in Figure 4 with the user plane of the EPC being separated from the control plane and placed in a regional data center closer to the user to decrease latency.

The vTAs also continuously monitor traffic during normal network usage so that network quality issues or SLA threshold violations are reported immediately and proactive problem resolution may occur as soon as possible.

The next stage of the PoC demonstration is shown in Figure 5. The network testing and monitoring emulates the traffic necessary to assure key SLAs for each of the outlined network slices in Figure 5. Three different network slices were tested using Netrounds vTAs per their differing SLA requirements; these correspond to different KPIs measured for each slice.

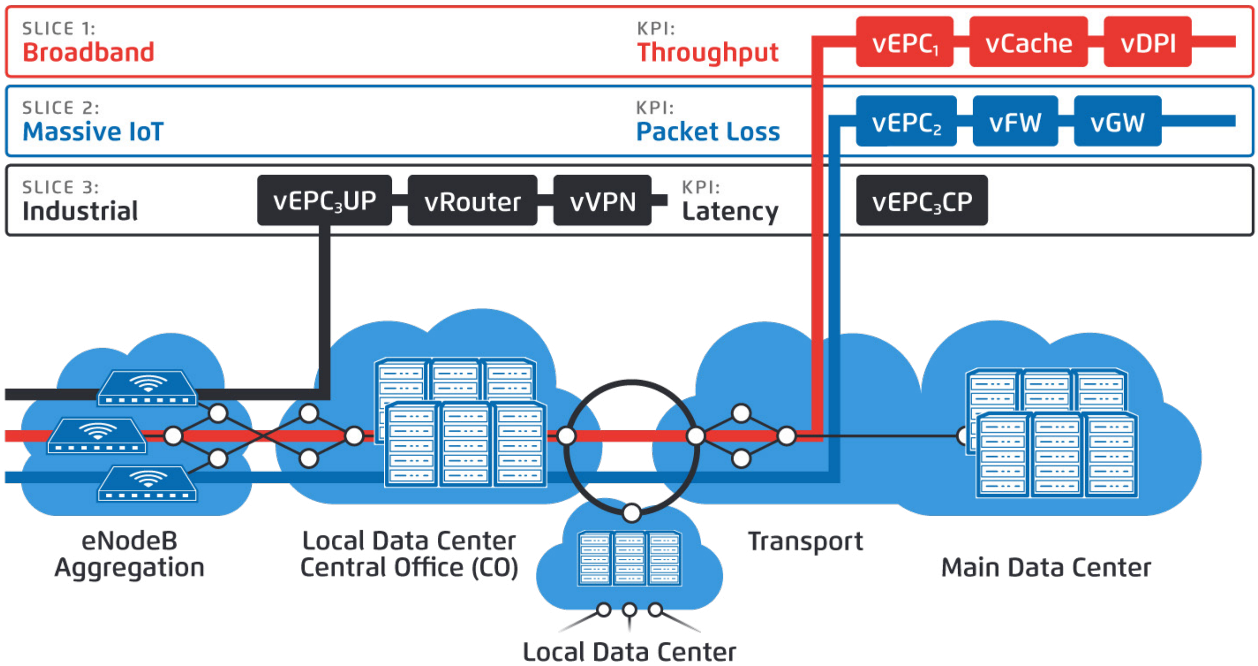

Figure 4. Three network slices with different critical key performance indicators[2]

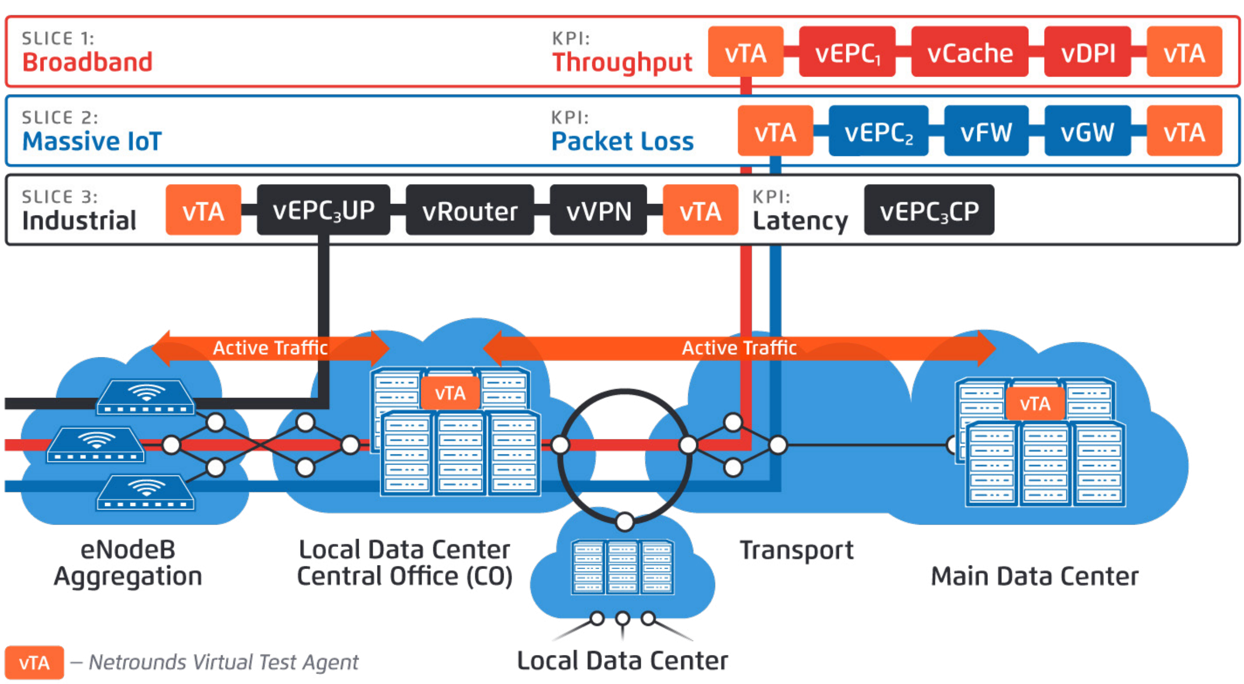

Figure 5. Levels using Virtual Test Agents and actively generated traffic[2]

PoC Demonstration Steps

The PoC demonstration includes design- and run-time activities.

Design-Time Activities

Design-time activities included:

1. Preparation of VNF definitions (VNFDs) for all VNFs. In this case, two vTAs, a vPE, a vRouter, and a vCache VNFD were created. (See Figure 6.)
2. Preparation of the network service descriptor (NSD) for the network pictured in Figure 3. (See Figure 8.)
3. Preparation of Netrounds templates for activation test and ongoing monitoring. (See Figure 7.)

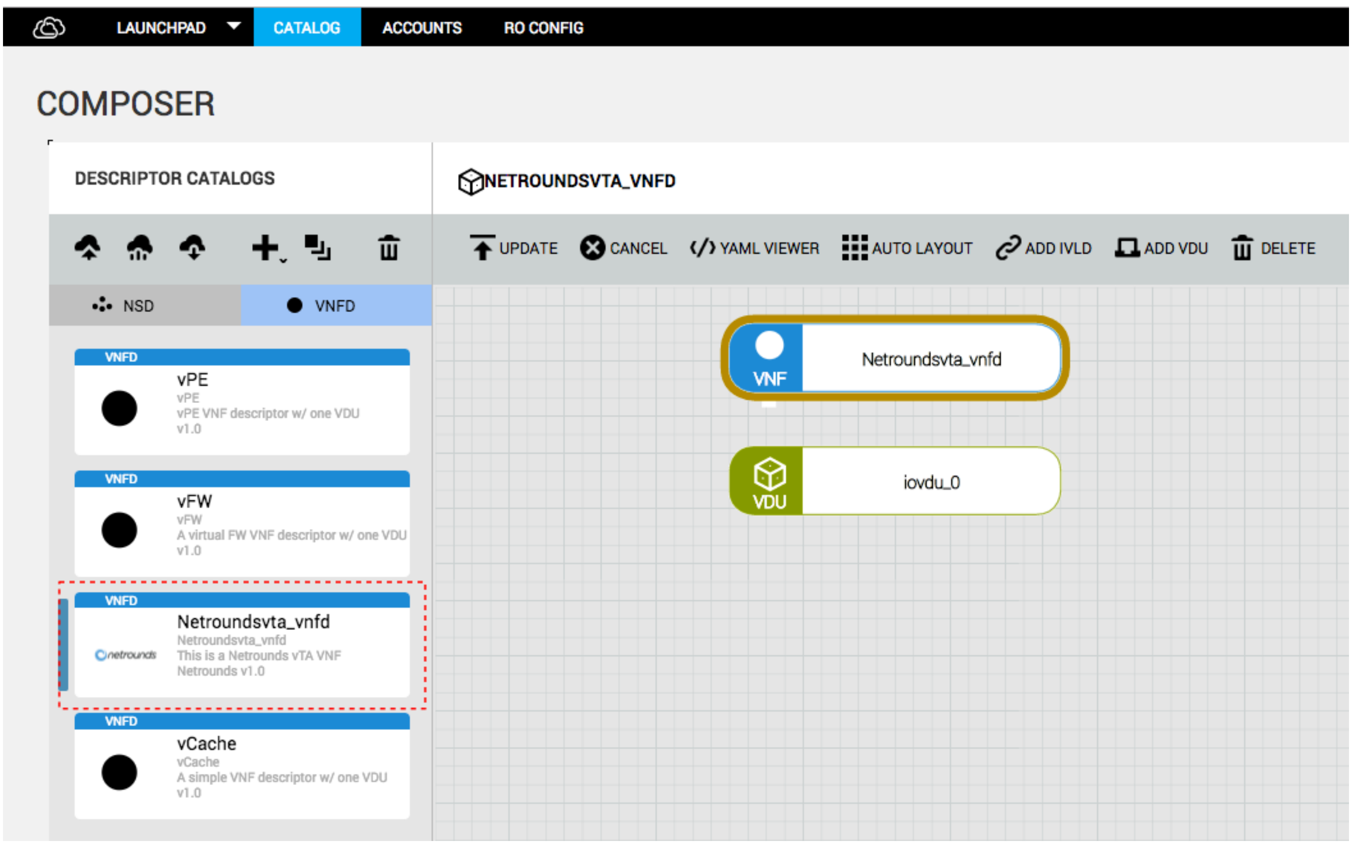

Figure 6. VNFD for the Netrounds Virtual Test Agent (vTA) as shown in the RIFT.io Composer UI

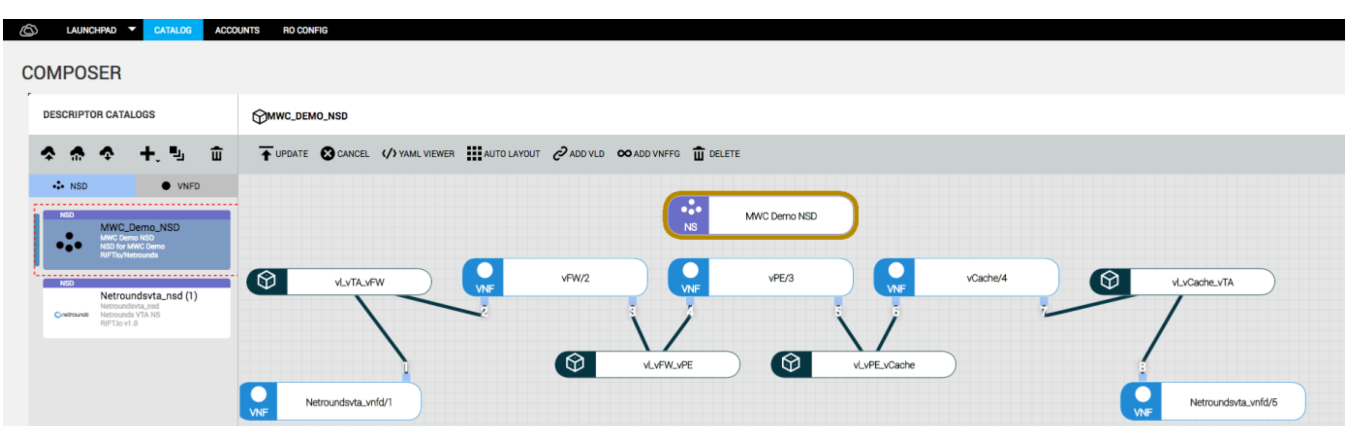

Figure 7. Network Service Descriptor Definition – VNFDs stitched together with virtual links

A fundamental element of DevOps methodology is to design the service for effective testing. The NSD in this PoC not only defines the service chain, but also the lifecycle operations for running active service activation tests and monitoring. Most fundamentally, it also orchestrates the Netrounds vTAs as part of the service chain.

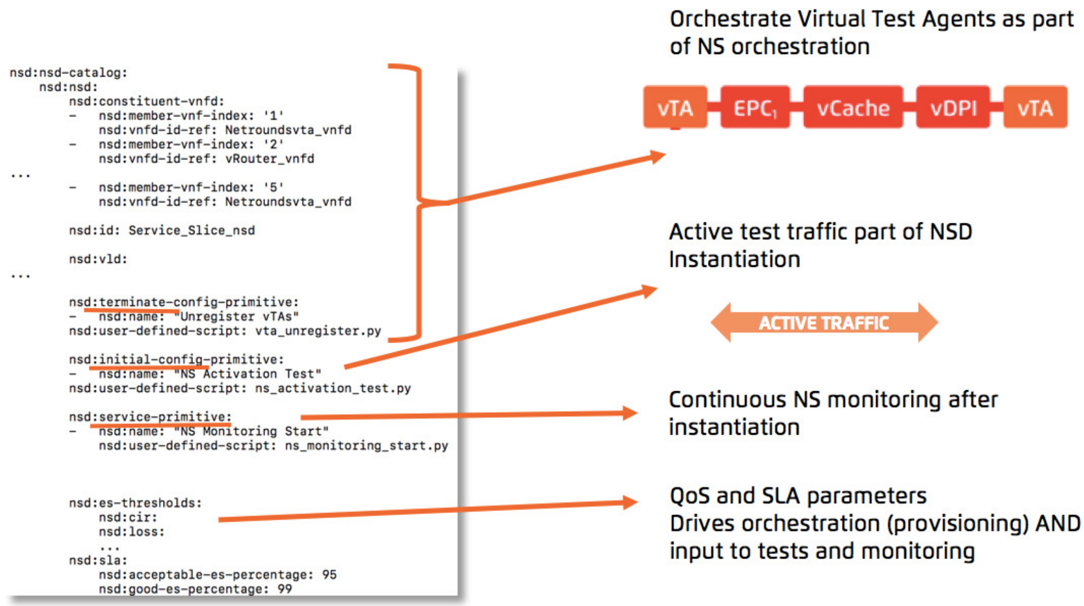

Figure 8. NSD design

Define the Activation Test Template

The creation of the service activation test template is illustrated in Figure 9. This was done in Netrounds' Control Center using a point and click process in the Test Builder.

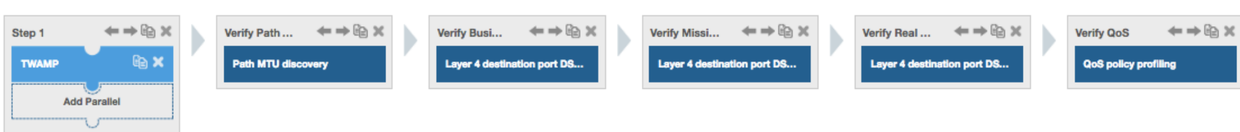

Figure 9. Netrounds Activation Test Template

The five sequential steps included in the service activation test template are:

- Step 1: TWAMP
- Step 2: Path MTU Discovery
- Steps 3-5: DSCP validation for three different classes. The screen shot for the business-critical mapping is shown in Figure 10.
- Step 6: Tests the QoS/shaping of four different QoS classes using TCP/UDP. The test configuration for one "sub-test" is shown in Figure 11.

Figure 10. Test definition for business critical mapping

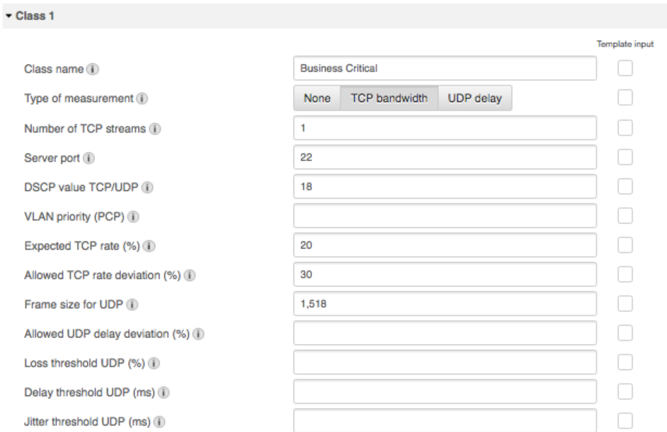

Figure 11. Test definition for business critical sub-test

The resulting test template will be used when OSM instantiates an NS to validate that the service is working per the specification.

Define the Monitoring Template

For each instantiated network service that passes the activation test, OSM will request that Netrounds perform continuous active service monitoring. The template for the monitoring is shown in Figure 12. The vTAs will send traffic through the service chain to validate that the SLA is met in real-time. The monitoring thresholds are different for different classes as seen in the monitoring template.

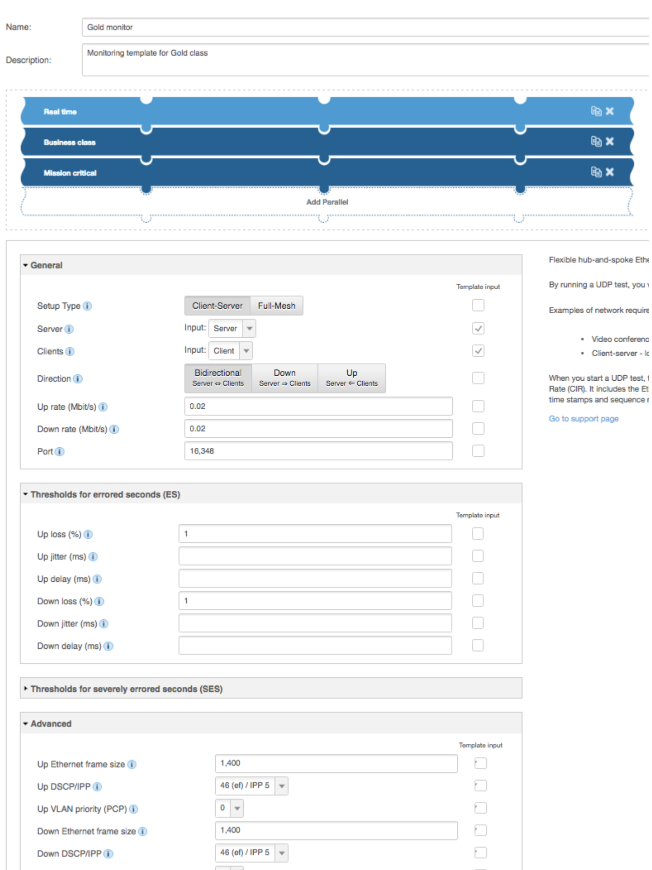

Figure 12. Netrounds monitoring template

Run-Time Activities

At run-time, the OSM orchestrator repeats the following tasks for each service:

1. Instantiate all VNFs in the NSD per the VNFD.
2. Stitch the service elements per the NSD.
3. Run the activation test for the service.
4. If activation test is successful, start ongoing monitoring.

Instantiate the Network Service

Individual network services are instantiated from the NSD. Each network service corresponds to a slice with different QoS parameters. The actual QoS threshold values for the different slices are given as input parameters to the NSD.

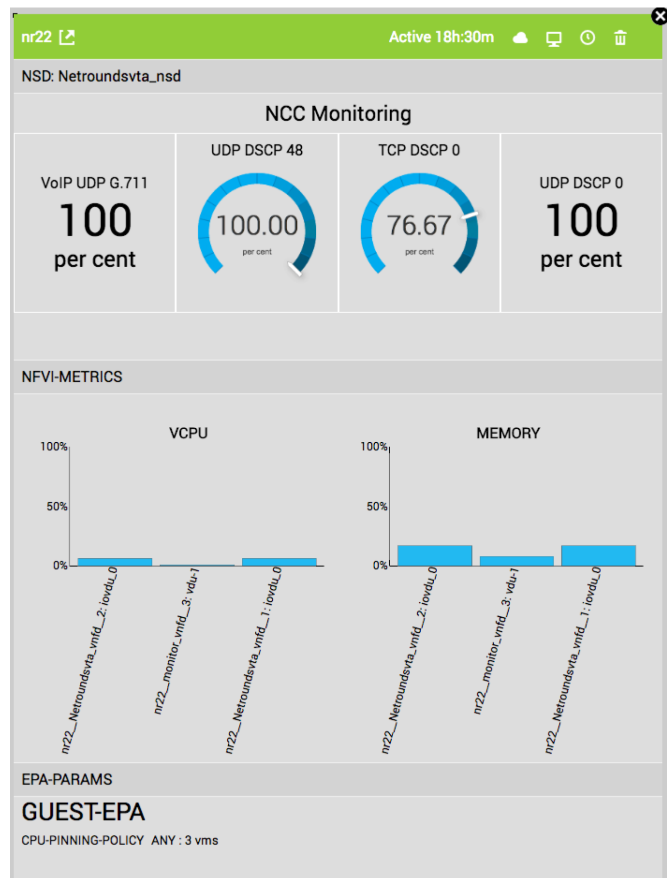

Figure 13. Instantiated network service with active monitoring ongoing

After the service is successfully instantiated, OSM triggers the Netrounds activation test. The activation test generates active traffic through the service chain to validate all aspects of the service before onboarding any customers as defined by the test template.

The ongoing status and results of the activation test are viewed in the Netrounds user interface. Figure 14 shows that the test first failed, and then after fixing the underlying problem, the activation test succeeds.

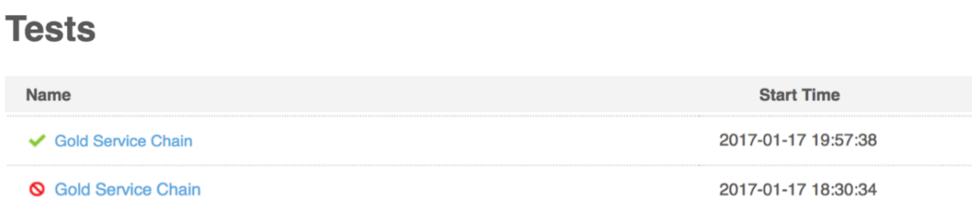

Figure 14. Test results shown in Netrounds Control Center

Following the success of the activation test, OSM will trigger ongoing real-time monitoring for every service instance, as shown in Figure 15.

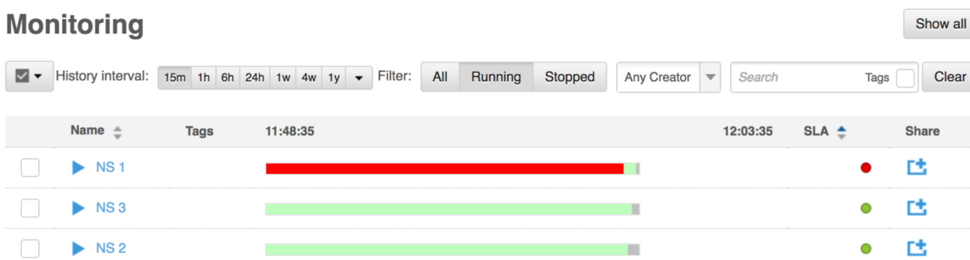

Figure 15. Real-time monitoring shown in Netrounds Control Center

As seen in Figure 16, the NS 1 Network Service violated the SLA at the moment of the screen shot, as well as for the time periods measured prior to that point in time. SLA violation generates notifications that can be picked up by the orchestrator and service assurance systems. Technicians can drill down to the individual KPIs being measured, as shown in Figure 16, and begin remote troubleshooting.

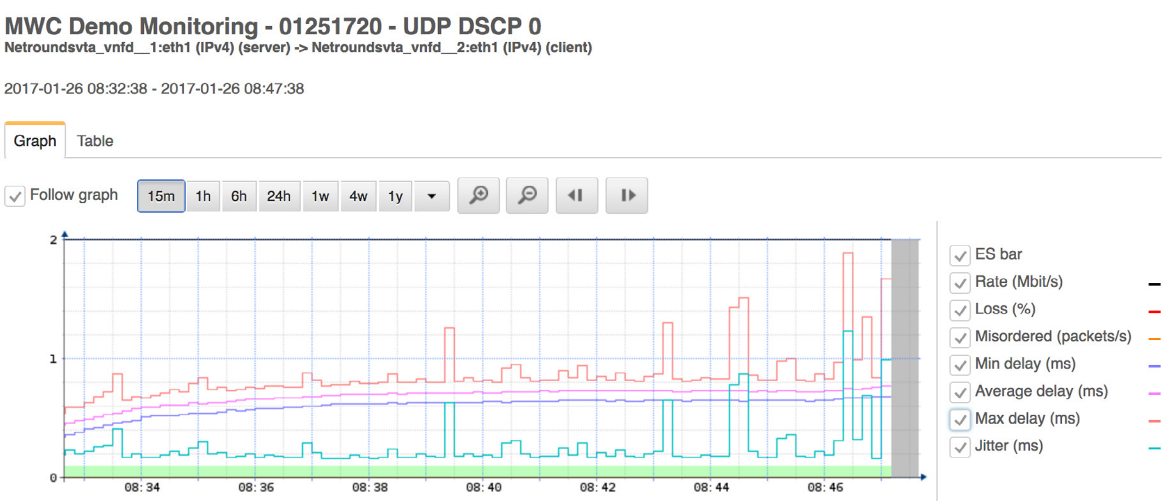

Figure 16. Monitoring test results - KPIs

Technology

Intel

Intel provides the proven performance required for dynamic, fast-moving, and flexible virtual environments. The company has pushed the development of cutting-edge technologies, including OpenStack EPA, that enable CommSPs to deliver the best quality to their customers. Intel® Xeon® CPUs E5-2620 v3s powered the Dell PowerEdge R730xd servers used in the PoC. The servers also include Intel® Ethernet Converged Network Adapter X520-T2 G1P5 (10 GbE), and Intel® Ethernet Converged Network Adapter 2P X520 and four-port 10 GbE 2P Intel® Ethernet Server Adapter I350 rNDC provided the connectivity. Linux* operating system version Ubuntu* 16.04 server, with Intel-backed enhancement, provides access to EPA-related hardware, including CPU pinning, PCI pass-through, data direct I/O, cache allocation technology (CAT), and Intel® QuickAssist Technology.

Telenor Group

Telenor Group is one of the world's major mobile operators with more than 214 million consolidated mobile subscriptions. Telenor Group has mobile operations in 13 markets in the Nordic region, Central and Eastern Europe, and in Asia. Telenor Research, Telenor's own corporate research unit, plays a key role in providing insights and competences that enable Telenor to become a customer-centric software and data-driven company utilizing the latest development within technology.

Netrounds

Netrounds Test Agents actively generate traffic and analyze detailed, real-time measurements across multiple applications, services, and interfaces. Test agent capabilities include multilayer measurement of Internet performance, network performance, IPTV and OTT video, VoIP telephony and SIP, mobile radio, and remote packet inspection.

All Test Agents are controlled and updated remotely through Netrounds' unifying Control Center, which can be hosted by Netrounds or deployed on premises. Test Agents are entirely software based. They can run on bare metal servers or PCs, be embedded in appliances or browsers, or be used as Virtual Test Agents (vTAs)—as utilized in this PoC demonstration. Test Agents cover layer 2 through 7 protocols.

Netrounds' platform addresses the full service lifecycle and is used to test and assure network services end-to-end from the customer perspective. A complete read-write API to Netrounds Control Center allows all active network analytics to be fed into adjacent operating support systems (OSS), such as SQM, FM, and PM solutions. The API allows Netrounds to be easily integrated into OSS automation workflows. Automation of Test Agents makes service testing a part of service instantiation.

In remote troubleshooting, Netrounds can significantly reduce mean time to repair (MTTR) for network issues and remove the need for truck rolls and other costly manual methods used today for problem resolution.

RIFT.io

RIFT.ware is an open source NFV orchestration and automation platform that simplifies development, deployment, and management of virtual network functions and multivendor network services.

RIFT.ware modules instantiate and terminate VNFs at multiple locations, in the thousands within multiple cloud environments. RIFT.ware does this through application programming interfaces that abstract the differences between VNFs, management systems, and NFV infrastructure elements.

RIFT.ware's lifecycle and orchestration (MANO) module is responsible for managing Network Service and VNF lifecycles. It is responsible for Network Service composition and instantiation, VNF catalog management, allocation/deallocation to achieve elasticity, and integration with OSS for configuration management.

Open Source MANO

ETSI OSM[5] is an operator-led ETSI community backed by a standards organization chartered to create a hardened, secure code base. OSM delivers a production-quality open source management and orchestration (MANO) stack that meets the requirements of production NFV networks and is aligned with ETSI NFV information models. OSM enables increased multivendor interoperability versus traditional standardization models and proprietary tools.

OSM Release ONE has been engineered, tested, and documented to allow for rapid installation in operator labs worldwide that seek to create a scalable and interoperable open source MANO environment. It substantially enhances interoperability with other components (VNFs, VIMs, SDN controllers) and creates a plug-in framework to make platform maintenance and extensions significantly easier to provide and support.

Using OSM, individual VNFs are onboarded via VNF descriptors into a VNF catalog. Network services are defined by Network Service Descriptors (NSDs) that specify the connections between VNF descriptors. Through the use of NSDs, MANO will instantiate and connect all the components of an NSD into a complete network service.

Arctos Labs

Arctos Labs engages with operators and vendors to provide consulting to assist their telco cloud transformation journeys. Arctos' primary services include strategy consulting on technology, architecture, and automation for operations support systems, DevOps and model development, as well as network software testing and validation. For this PoC, Arctos Labs acted as a systems integrator, building the environment based on OpenStack and adding the orchestration components.

Benefits

There can be substantial benefits to applying a DevOps approach for network operations and network service design and enabling automation of deployment and maintenance of service chains and 5G slices. It allows service providers to take advantage of the flexibility that NFV offers without losing sight of quality.

Integrating test and monitoring into services at the service design stage allows these functions to be automated, validating that services work before customers are onboarded. Automation increases operational efficiencies and decreases human error—saving OPEX and decreasing expensive downtime. Reducing downtime also protects against costs related to SLA validation and network outages. One report[6] suggests that this can be as high as USD 11,000 per minute per server.

The profitability of the infrastructure can be enhanced through dynamic orchestration of the optimal location to run VNFs and EPA-guided VNF optimization. Automation and testing can provide a more accurate view of data center usage that allows for more intelligent, careful network planning.

The orchestrator can also trigger continuous SLA monitoring of dynamic network services that will notify operations staff of any SLA violations and allow for proactive remote troubleshooting to begin. This monitoring functionality also provides a closed feedback loop to the design.

New services can be designed to make the most of existing infrastructure and to take advantage of new user trends and behaviors such as Pokémon GO,* Spotify,* etc., and to employ network slicing with 5G technologies. This maximizes utilization of existing investments and minimizes unnecessary CAPEX. Optimization can increase capacity headroom, allowing for surges without purchases of excess equipment. And, optimized services increase QoE, reducing subscriber churn.

Conclusion

When network services are designed, an accompanying test should be designed into that service that validates that the service delivers the required QoS. For service assurance, the NSD onboarding process includes the vTAs for end-to-end deployed service testing. The same procedure should be followed for running service instances. A service level SLA monitoring definition should be part of the NSD onboarding and be run continuously after a successful activation test and subsequent customer launch for the service.

While the industry is mostly focused on VNF health from a resource perspective, this PoC illustrates the need for a quality test of the network service as a whole, i.e., does it deliver the intended end-user quality? Are network slice SLA requirements being met? Active tests are needed to answer that question.

OSM can orchestrate Virtual Test Agents that send active traffic as part of the service chain deployment. This leads to a less complex assurance solution and more precise end-user KPIs than traditional passive methods combined with inventory/topology databases. Without active testing and monitoring of end-to-end services and real-time, individual network slices, proactive troubleshooting actions and self-healing is difficult, if not impossible.

Network slices are a combination of different QoS settings at the end-points and within individual VNFs. It is essential that the slice delivers the right QoS for the end-user services. QoS for network slices must be continuously tested and monitored upon activation and when any changes or updates are made so that operators do not fail to meet agreed-upon SLAs and customers do not experience adverse network quality when it matters most. Passive monitoring methods will be unable to determine if slices deliver the needed QoE until customers are onboarded and traffic flows. With the method described in this PoC the orchestrator can assure the QoS of the slice at provisioning time.

Intel, Telenor, Arctos Labs, Netrounds, and RIFT.io have demonstrated how NFV enables full orchestration of active vTAs to build a dynamic, automated, and programmable infrastructure.

Abbreviations

API	Application Programming Interfaces
DevOps	Development and Operations
DSCP	Differentiated Services Code Points
DPI	Deep Packet Inspection
ETSI	European Telecommunications Standards Institute
EM	Element Manager
EPC	Evolved Packet Core
FM	Fault Manager
GW	Gateway
IOT	Internet of Things
IPTV	Internet Protocol Television
MANO	Management and Network Orchestration
MBB	Mobile Broadband
MTU	Maximum Transfer Unit
NFV	Network Functions Virtualization
NFVO	Network Functions Virtualization Orchestration
NS	Network Service
NSD	Network Service Descriptor
OSM	Open Source MANO
OSS	Operating Support System
OTT	Over The Top
PM	Performance Manager
RAT	Radio Access Technology
SLA	Service Level Agreement
SDN	Software Defined Networks
SQM	Service Quality Manager
vFW	Virtual Fire Wall
VIM	Virtual Infrastructure Manager
VNF	Virtual Network Function
VNFD	Virtual Network Function Definition
vPE	Virtual Provider Edge
VoIP	Voice Over IP
vTA	Virtual Test Agent
QoE	Quality of Experience
QoS	Quality of Service
SIP	Session Initiation Protocol
TWAMP	Two-Way Active Measurement Protocol

[1] http://veriflow.net/_files/veriflow-global-survey.pdf.

[2] Figure provided courtesy of Netrounds.

[3] 5G Systems, Ericsson White Paper, January 2015. https://www.ericsson.com/res/docs/whitepapers/wp-5g-systems.pdf.

[4] Figure provided courtesy of Netrounds. The Open Source MANO logo is courtesy of Creative Commons License 2.0. Open Source MANO is an ETSI-hosted initiative.

[5] European Telecommunications Standards Institute https://osm.etsi.org/.

[6] "What's the Real Cost of Network Downtime?" Light Reading column by Charlie Ashton, September 3, 2014. http://www.lightreading.com/data-center/data-center-infrastructure/whats-the-real-cost-of-network-downtime/a/d-id/710595.