Putting the Network Back in VNF

Written by Kyle Greenwell,
PMTS – Verizon

verizon business ready

Key Points

Network virtualization is increasingly playing a key role in the overall Cloud Computing revolution, where the mantra to virtualize everything has led to new approaches to building infrastructure and delivering applications. Critical factors causing network virtualization maturation to lag behind other cloud infrastructure technologies include:

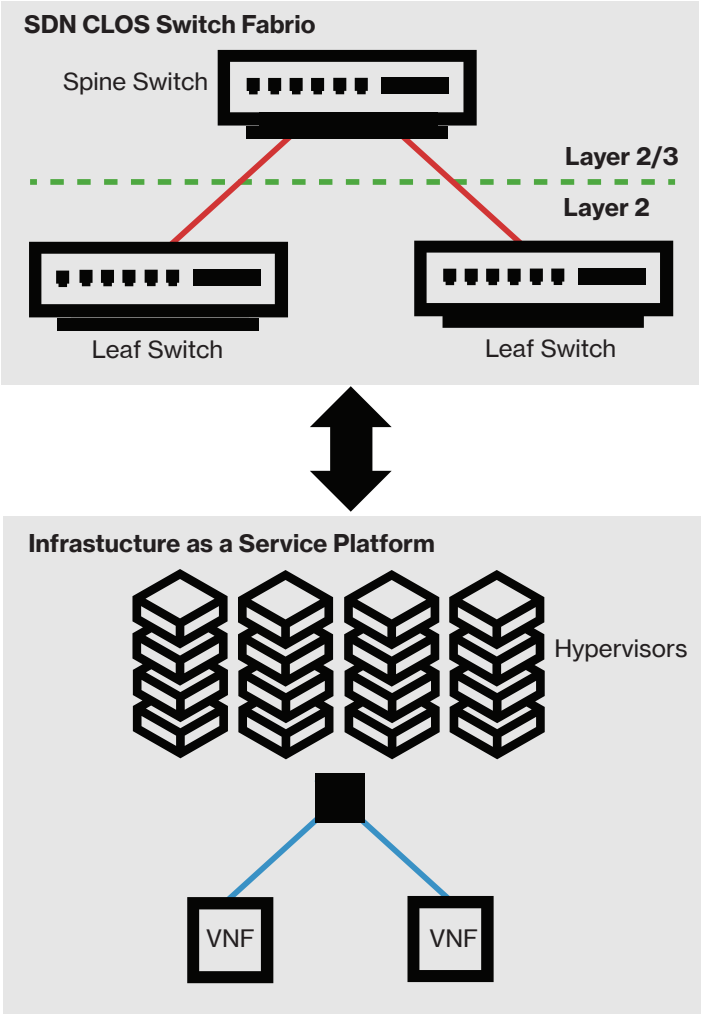
- Few or no standards for virtualized networking applications
- Limited understanding by cloud vendors of WAN networking requirements
- Vendors primarily focused on their own solutions at the expense of interoperability
- Vendor heavy reliance on hardware to optimize performance

Combining virtualization and cloud computing architectures with WAN networking only magnifies the problem by adding the need for additional layers of required interoperability testing across, up, and down the technology stack. In a world where vendors have traditionally taken a standalone appliance approach, the need for testing standards to support interoperability has never been greater.

Next Generation Network Virtualization

OpenStack-based virtualization began as an evolution of the data center to reduce both CapEx and OpEx. It accomplishes this goal by reducing vendor lock-In and enabling rapid deployment and expansion, which increases efficiency and productivity of the entire infrastructure stack. The data center environment, however, primarily focuses on the building of scalable storage and compute resources with tangential support for networking. It was never designed to extend past the data center and incorporate WAN resources and distributed architectures.

Now, virtualization's newest evolution will expand beyond IT infrastructure and the data center, to bring the same benefits to the network. Network virtualization shares the same goals and focus as traditional IT virtualization with some additional requirements that are specific to networking functions. Unlike its data center cousin, network virtualization requires guaranteed high bandwidth delivery services and extreme compute requirements, but generally does not need much storage.



Software Version Tracking

- SDN Controller
- Switch firmware & OS
- Hypervisor firmware & OS
- Infrastructure Virt Software
- VNF

Figure 1: Example Infrastructure as a Service platform, including software version tracking requirements

Since little attention has been paid to cloud WAN networking, very little is new with Virtual Network Functions (VNF). Most vendors do not engineer their VNF from scratch. Instead, they start from their existing purpose-built hardware appliances, separating their code base into a software package that can be virtualized. Routers, firewalls, and load balancers all come in hardware versions. Hardware-based networking products have the advantage of being closely controlled and engineered by the product team to provide consistent function and performance across any network.

Virtualizing hardware-based products removes these purpose built integration benefits by standardizing the underlying infrastructure with Commercial off the Shelf (CotS) servers. The shared cloud environment removes the ability to custom tailor and tweak performance using hardware based on a specific vendor's needs, as the vendor has little or no control over the hardware or cloud architecture. Features like CPU Pinning, Data Claim Development Kit (DPDK), and Single Route Input/Output Virtualizion (SRIOV) are certainly available, along with other methods for optimizing network traffic flows and application runtime efficiency, but a service provider is not going to customize its virtual or cloud infrastructure to match a single vendor's test environment; it does not make business sense to spread technical resources so thin. Currently, no optimization or industry-wide fixed configuration provides predictability in the environment in which these VNFs will be run. Nearly every organization will have some uniqueness in its networks and cloud implementations that will cause the VNF's performance and functionality to vary greatly. Different hardware profiles, Software Defined Networking (SDN) solutions, and configurations will all affect the performance of a VNF. This creates a challenge for network engineers to provide accurate test results for their organization's virtual or cloud infrastructure. As can be expected, vendor tests tend to produce performance results based on an ideal deployment, utilizing every available feature in order to deliver the best results possible. Because the underlying infrastructure hardware and configuration is so important to performance, vendor-provided test results are likely less valuable for an organization's infrastructure and, more importantly, less indicative of actual performance in real life conditions.

VNF Validation

A common misperception has crept into the industry that VNFs are simple to implement, onboard, and provision. The reality is not so simple. Even if an organization's virtual or cloud infrastructure is in place and ready for a VNF, the VNF must be evaluated and validated for implementation within the specific virtual or cloud environment before actually deploying it into production. The risks of failure in production, where real customers are depending on Verizon to deliver reliable and high performance networking functions, are too high. To that end, Verizon has developed comprehensive testing suites that test VNFs and service chains to quantify our customers' experience and network performance in production conditions.

Verizon has been testing and deploying network functions in a large service provider environment for decades. Through the years, an approach to testing for function and performance has led to thousands of successful deployments across the globe. During the past several years, this testing philosophy has been adapted to better align with the unique requirements of VNFs tested within OpenStack cloud environments. This validation process includes a comprehensive combination of onboarding, functional, performance, security, and end-to-end testing. Verizon has developed an in-house test execution and automation platform for this function.

Onboarding testing is required for a virtual product deployment. This testing helps ensure a VNF can be deployed within a virtual environment in a consistent and predictable manner. Verizon onboarding includes

- Uploading the vendor image to the OpenStack image service (Glance)
- Manually instantiating the image
- Validating console availability for initial configuration
- Testing basic network elements, including
    - Attaching and detaching network interfaces
    - Validating Layer 3 connectivity via ping

Verify vendor can provide valid file types for environment (QCOW, RAW, etc.)
Create project with quotas based on vendor provided specifications
Create project users
Create flavor(s) for specified instances
Upload image(s) to Glance via dashboard (9GB or less) or CLI (greater than 9GB)
Create private network(s) and virtual router(s) if necessary
Verify image is available for use in project space
Instantiate image at least once within the system and validate the image is running by accessing the image software
Verify access to the VNF embedded console for base configuration
Verify interface(s) to a network(s) can be correctly added to the launched image for configuration within the VNF
Verify VNF can be terminated through the GUI
Verify valid computer size(s) are available for image(s). If not, verify the required compute size can be supported
Verify multiple interfaces can be added to an instance and verify routing between the interfaces (For applications with multiple Interfaces)
Verify manual/auto partitioning is supported (if necessary)
VNFs that provide options for API access to Openstack should be tested for API access. Verify that the VNF can access the API using the Openstack endpoint(s)
Verify the creation and attachment of a volume to a VNF if required
Check instance and action logs for any errors during instantiation and while running
Verify security groups can be created to block or allow traffic

Figure 2: Onboarding test cases for VNF testing within Verizon's Hosted Network Services platform.

Functional testing depends on the service(s) required. Verizon has developed a test plan for several service types, including virtual routing, firewall, SD-WAN, and WAN Optimization. These test plans seek to validate the specific functions each service type provides. Examples include:

- validating routing protocols for a virtual router
- Validating anti-malware, and web filtering functions within a virtual firewall
- Validating application-aware routing in an SD-WAN solution.

Verify creating a policy to control intra-zone traffic
Verify enabling logging and creating a 5 –tuple firewall policy
Verify providing source and destination NAT/PAT
Verify malformed packet protection
Verify intrusion detection features (if available)
Verify web filtering
Verify anti-malware functions
Verify data loss protection features
Verify automatic signature updates
Verify URL blocking features

Figure 3: Sample of virtual firewall functional test cases

Performance Testing

Performance testing requires some decisions about what types and mixes of data the organization considers important. Verizon tests VNFs, including service chains (combining multiple VNFs to provide multiple services) for baseline performance by gathering data on throughput and sessions. Throughput testing includes testing multiple mixed traffic patterns, as well as an RFC25441 test for throughput testing against multiple frame sizes. Session testing includes both max sessions and new sessions per second. VNFs that handle VoIP traffic are tested for delay and jitter characteristics. Finally, a soak test is performed, by monitoring CPU and memory utilization and VNF logs, while utilizing an average load on the VNF over a period of multiple days. These tests are done with minimal configuration, enabling as few features as possible in order to capture the VNF's maximum performance within the Verizon cloud infrastructure.

Once the baseline performance is captured, targeted performance testing can take place when required. This targeted performance testing may enable additional features within the VNF. Some examples include testing with IPSEC tunnels configured on an SD-WAN solution or testing with specific quality of service (QoS) profiles configured for a virtual router managing VoIP traffic. These results are unique for certain services, VNFs, or configurations, and are necessary for capacity planning.

End-to-end testing runs test cases that validate the entire path of a service. These may include connectivity to other OSS/BSS systems like monitoring, alarming systems, element managers, SNMP servers, and provisioning applications. Tests also include connectivity to required elements outside the virtual or cloud infrastructure.

Finally, the deployment methodology must be tested. Deployment may be manual, may utilize a cloud infrastructure service like HEAT (OpenStack) or CloudFormation (AWS), or may be a full-blown orchestration platform (VNFM).

VNF Testing Challenges

The testing of VNFs has many unique challenges. The separation of software from a vendor's hardware product platform enables faster software release cycles, which the vendors quickly take advantage of. Gone are the days of the predictable two software releases per year. Now vendors are pushing out software much more frequently, even in some cases continuously. Faster release cycles can benefit an organization looking to enable new features and functionality in its networks, or a quicker response to patching bugs or security vulnerabilities. It also means yet more testing cycles are required, and those cycles need to complete that much faster. Exacerbating this problem, the underlying virtual or cloud infrastructure is constantly releasing new software as well. Every time new infrastructure code is released, the VNFs deployed on that infrastructure must be regression tested to ensure interoperability and performance metrics do not change.

An organization's infrastructure environment is also an important consideration when it comes to testing. Many organizations are deploying in hybrid and multi-cloud environments. Special consideration must be taken based on the underlying infrastructure requirements. If products will be deployed in a multi-cloud environment, testing must occur in both environments to help ensure functionality, performance, and interoperability. Some VNFs have special feature requirements generated from their hardware based origins, such as CPU pinning, DPDK, and SRIOV. These features must be tested to ensure the VNF is properly utilizing the features required.

Conclusion

Organizations of all sizes can benefit greatly from network virtualization. Many of the benefits of IT virtualization also apply to network virtualization. It is important, however, to remember that networks are complex pieces of infrastructure that enable the entire IT organization or in the case of telecoms, multiple organizations. Without a well-planned, tested, and deployed network, the entire IT infrastructure and the business it supports suffer. By using a well thought out testing methodology, organizations can successfully test and implement virtual network functions in their infrastructure-as-a-service platform. As organizations evolve in this process, a whole new world of benefits will be realized. Among them are test automation, deployment and lifecycle orchestration, and configuration management automation that, once implemented, can further drive down costs and improve productivity.

Footnote:
1.Request For Comment (RFC) #2544 is the published standard by the Internet Engineering Task Force (IETF) for benchmarking methodology for network interconnected devices.

Acknowledgements:
Glenn Tracy, Senior SDN/NFV Architect - WiPro, contributed to this whitepaper while working with Verizon on a Statement of Work contract.

© 2019 Verizon. All Rights Reserved. The Verizon names and logos and all other names, logos and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

verizon business ready