Virtualization of Customer Premises Equipment (vCPE)

Customer Profile

Customer: A Cloud Service Provider

Reach: Global

Industry: Telecommunications

The Challenge

A Cloud Service Provider serving both business and residential customers across multiple global regions is evaluating Virtual Network Function and hypervisor vendors for its SD-WAN and vCPE solution offerings. CSPs are realizing the benefits of vCPE and SD-WAN as complementary technologies and there is an increased momentum for such combined deployments, to benefit from the promises of NFV and SDN paradigms. Policy validation and performance benchmarking of the vCPEs represent a daunting task, particularly considering the multiplicity of service types with varied SLA requirements.

Virtualization of Customer Premises Equipment (vCPE)

There are three broad types of vCPE deployments, each with varying distributions of functionality between the customer premises and the cloud (Service Provider edge). They are described below:

- **Cloud CPE**
  Most of the vCPE functions such as NAT, Firewall, QOS Policies are deployed in the cloud at the Provider Edge, with basic functionality such as forwarding and IP address management (IPAM) supported at customer premises

- **On Premises OTT vCPE**
  More functionality such IPAM, NAT, Firewall and QOS Policies are supported by the vCPE VNFs at the customer premises. Customer control plane and data plane traffic is carried on an OTT connection

- **On-premises vCPE**
  More functionality such IPAM, NAT, Firewall and QOS Policies are supported by the vCPE VNFs at the customer premises. Customer control plane and data plane traffic is carried over a dedicated link owned by the service provider

The customer premises may be easiest to virtualize if modular container-based methods are employed. Multiple vCPEs in an enterprise edge may need careful orchestration. In a residential customer domain, the end customer may be stymied by the vagaries (and possible faults) of "soft" network functions. A virtualized CPE implementation at the customer premises means potentially lower Opex costs for the customer, while representing an easy way for the CSP to manage network edges and roll out new functions.

The vCPE may be comprised of multiple VNFs such as vRouter, vFirewall, vLoadbalancer and vDPI or it may consist of a vRouter implementing more than one functionality offered by the independent VNFs. The vRouter VNF plays the type of central role in vCPE deployments and often implements multiple functionalities of vCPE. The COTS platform implementing vRouter can utilize hypervisors such as KVM for the Linux environment, as well as Virtual Infrastructure Manager for MANO functions. Potential vCPE deployment options must be considered by the CSP early in end-to-end NFV deployments.

Problem Statement

This case study is focused on the performance benchmarking of a vRouter deployed in an OpenStack & KVM environment using an Open vSwitch accelerated via DPDK, thus illustrating how Spirent's NFV test solution was instrumental in identifying the performance bottlenecks in a multi-vendor shared NFV environment.

SD-WAN and vCPE testing can be divided into four high-level test scenarios independent of the vCPE deployment configuration:

- Policy validation of vCPE (functional and large scale)

- VNF lifecycle management for vCPE constituent VNFs

- Benchmarking performance and scale of vCPE

- Validation of policy based routing for SD-WAN

Each vCPE deployment consists of multiple VNFs providing the desired functionality to achieve functionalities such as IPAM, policy control, traffic shaping, admission control, authentication, routing and access to the desired services. For supporting these functionalities and services VNFs in each vCPE deployment rely on standardized protocols such as DHCP, IGMP/MLD snooping, RIP, BFD, LACP and 802.1X. These control plane protocols are supplemented by static configuration capabilities such as firewall rules and traffic shaping policy rules.

Performance Benchmarking of NFV data plane is a critical aspect of helping Service Providers in making the transition to NFV based network. Shared infrastructure and multi-tenant environment introduces complexity in test scenarios making the traditional benchmarking procedures of relying entirely on test traffic metrics insufficient for data plane benchmarking in a NFV environment. The possibility of multi-vendor VNFs, hypervisor, NFVI nodes sharing the same infrastructure resources renders the assumption of treating SUT as a black box invalid. The shared infrastructure resources necessitate not only to look at external user workload for performance benchmarking, but also look at the impact of performance of each of the individual components on each other. Performance isolation of the comprised entities is a luxury that cannot be taken for granted with the current state of virtualization technologies.

DUT Profile and Anticipated Performance

In this particular CSP example, the compute node at the customer edge is an open rack-mounted server with 16 logical CPU cores with hyperthreading enabled, four Ethernet NIC cards, and 64Gbytes of RAM. Note that OVS switch is used for layer 2 switching and DPDK is used as an acceleration technology for packet forwarding. Four logical CPU cores are dedicated to OVS-PMD, while four logical CPU cores are dedicated to implementing VNFs. The virtual switch is expected to implement a 2Gbps aggregate switching capacity. VNFs should implement 1Gbps bidirectional forwarding capacity with a maximum latency of 30 ms, based on a frame size of 256 bytes. When carrying IMIX traffic, the DUT should handle up to 10,000 traffic flows and throughput must be greater than 90% of line rate (1Gbps). Conceptual diagram of the DUT test setup is shown in Figure 1.
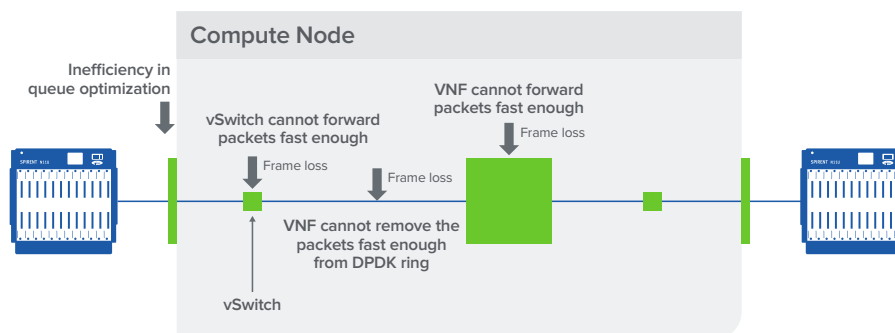

Figure 1: DUT of vRouter Functions on Target Hardware, Testing Hypervisor and VNFs

Spirent NFV Test Solution

Spirent provides a comprehensive set of test methodologies to benchmark NFV data plane that provide insights into NFVi resource utilization in addition to network performance metrics. Together, NFVi resource utilization metrics and test traffic performance metrics enable Service Providers to characterize user workloads and VNF performance metrics. This in turn helps the Service Providers in capacity planning, resource provisioning and identifying performance bottlenecks in an NFV environment.

The illustration below indicates how test topology and results are presented to users.

Virtual Test Topology
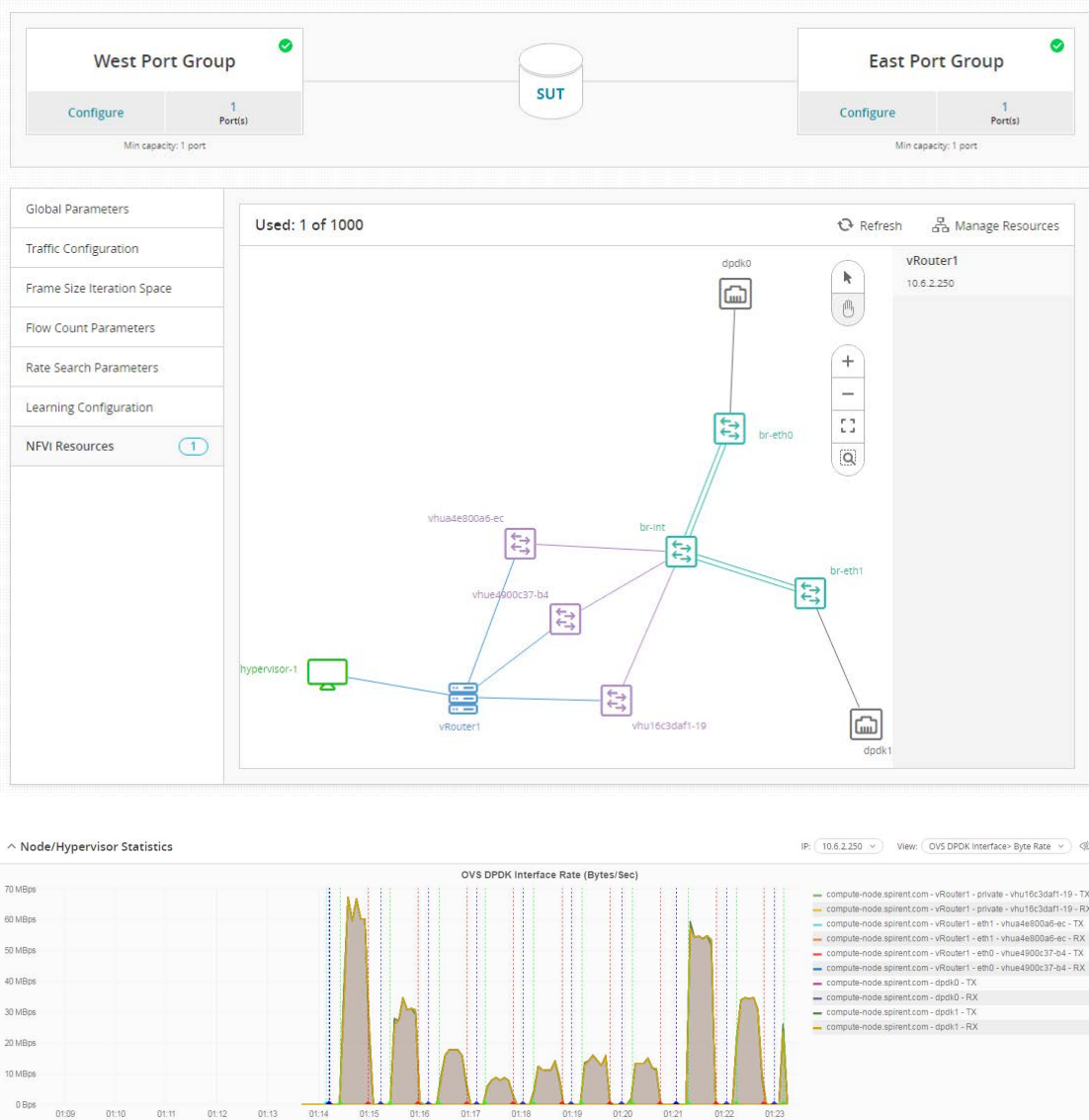
Conclusion: Lessons Learned

Contrary to the claims of some vendors and the wishes of many customers, not all VNF implementations optimize the use of NFVi resources. Nor do hypervisors provide complete performance isolation of VNFs. This is particularly true in multi-vendor shared environment that is typical for vCPE deployments.

In the types of tests performed, benchmarking compared various allocation levels of CPU cores and memory for VNFs and virtual switch. The SUT was exposed to varying user workloads. By providing comparative data on benchmark and workload cases, the user characterized the SUT network performance under varying NFVi resource allocation and workloads. The tests provided the intelligence necessary to make appropriate decisions for resource allocation, vendor selection and capacity planning to support the desired number of subscribers and user workloads at the defined SLA levels.

By using Spirent NFV test solutions, we were able to:

- Characterize VNF performance for specified workloads.

- Analyze different resource allocations (CPU, memory, network bandwidth) for the VNF.

- Identify performance bottlenecks, using an E2E solution based on both test traffic metrics and NFVi resource utilization metrics.

- Provide correlation between the two sets of test metrics.

- Correlated test results and fault isolation across vCPE helped **reduce root cause analysis time by up to 80%**. NOTE: The more complex the system or testbed, the more the root cause analysis time will be reduced, with customers able to realize more benefits as a result.

- Accurate testing and reduced analytics time can deliver higher ROI for NFV tests, and lower Total Cost of Ownership for the service provider.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

Contact Us

For more information, call your Spirent sales representative or visit us on the Web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com