NFV World Showcase 2013
Provisioning, Portability and Elasticity
EDITOR’S NOTE

Since EANTC has been founded in 1991, we have tested innovative technologies that changed the telecommunications industry. The virtualization of network functions clearly marks an important evolutionary step. Technology leadership and market shares are stirred up, now that network functions are being removed from specialized hardware and are following trends in the data center towards virtualization.

To accelerate this development, leading service providers and vendors have formed an Network Functions Virtualization Industry Specification Group (NFV ISG) under the umbrella of the European Telecommunications Standards Institute (ETSI).

As an ETSI member, EANTC has contributed to the development of an NFV Proof of Concept (PoC) framework. It standardizes the high-level requirements and documentation guidelines for public NFV proof of concept demonstrations.

EANTC’s goal is to help vendors and service providers to independently validate the functionality, performance, interoperability, and manageability of NFV solutions. We have tested all NFV use cases in non-virtualized environments before and have already developed test methodology for fixed and mobile application-layer NFV scenarios.

We invited vendors to first public EANTC PoC demonstration to be showcased live at Layer123’s SDN & OpenFlow World Congress, October 15–18.

Three vendors – Huawei, Metaswitch and Procera – already picked up our gauntlet and provided virtualized network functions for our test. An EANTC team has independently evaluated the vendor solutions; we proudly disclose the results of our tests in this white paper. Given that this was the very first evaluation opportunity, we are happy to share it with the vendors. We created a test plan that captured all aspects that we wanted to verify and shared it with the vendors. We also wanted to verify and shared it with the vendors. We then created a tailor-made test plan for each of the vendors’ solutions based on the actual NFV use case they were bringing to the table. We emulated subscriber traffic and used it as a way to verify that the Virtualized Functions were actually working.

Participants and Devices

In these early days of Network Function Virtualisation (NFV), we tested individual vendors’ solutions leaning on the vendors to integrate their use cases with the underlying and overlying components. The document is therefore split into two parts. Initially we provide an overview of the individual vendor solution. In the second part we provide a status report on the Foundation Function Virtualisation. In this part we highlight the achievements and challenges at this point in time and offer feedback to the ETSI NFV ISG.

Huawei VNF Forwarding Graphs and Carrier Grade NAT

Huawei brought two scenarios built up on the same NFV architecture – CG-NAT and Service Chains. Both solutions, which are still in the early development phase, are intended for residential services.

The CG-NAT service intends to provide a solution for the increasing shortage of IPv4 addresses and transition to IPv6, by implementing nearly any NAT and IPv4-via-IPv6 technique. The Service Chains make it possible to chain DPI, Parental Controls or other similar functions for flexible services. NFV gives the possibility to flexibly provision such services to the customers, optimize resource use and scale the performance.

Metaswitch Perimeta Session Border Controller

Metaswitch selected to showcase their Perimeta Session Border Controller (SBC) Virtual Network Function as a Service use case. Metaswitch positions the solution as a carrier-class software SBC, able to deliver required security and performance without proprietary hardware. It uses the concepts behind NFV to provide independent distribution and scaling of its signaling (SSC) and media (MSC) components. Those same concepts are also leveraged to provide support for migration and elasticity, both key NFV goals.

Procera Deep Packet Inspection

Procera presents a virtualized implementation of their PacketLogic Intelligent Policy Enforcement solution based on Deep Packet Inspection (DPI) technology. Procera explained that the Virtualized PacketLogic solutions enable network operators to deploy Internet Intelligence pervasively through their infrastructure. The solution demonstrated the policy enforcement capabilities of the PacketLogic solution including application identification, traffic management, and intelligent charging in an NFV environment.

• Instantiation and Provisioning – We first focused on the foundation operations that are required to instantiate a Virtual Network Function. We looked at the ability of starting service instances remotely. We also checked if the VNF has an interface to abstract configuration and functionality from the hardware.

• Portability – Once service instances were available, we moved to the next stage verifying the loading, execution and moving of VNFs. Last but not least we verified that the VNF can provide the capability to optimize its location.

• Elasticity – Since one of the promises of NFV is the ability to scale up and down resources, we simulated conditions that cause functions to require more resources and checked that the emulated subscribers did not experience any degraded service on account of this.

We created a test plan that captured all aspects that we wanted to verify and shared it with the vendors. We then created a tailor-made test plan for each of the vendors’ solutions based on the actual NFV use case they were bringing to the table. We emulated subscriber traffic and used it as a way to verify that the Virtualized Functions were actually working.
SHOWCASE RESULTS

Executing the tests required traffic generation and measurement. We thank Ixia for providing the tools that enabled us to test the solutions in as much as possible as real-world deployment will be.

![Logical Test Topology](image)

The validation testing of each VNF varied, since each was delivering very different functionality. In each of the use cases we used Ixia testers to send emulated and stateful subscriber traffic to verify that the VNFs were functioning as designed.

Instantiation and Provisioning

We were impressed to see that all Virtual Network Functions (VNFs) already could be installed remotely on Common Off-the-Shelf (COTS) servers using command line interface (CLI) or web interfaces. In most cases, the virtual images were prepared in advance and only had to be copied into the hypervisor. We saw that configuration was quick (within 10 minutes) and could be automated in the near future. Each virtual machine was assigned memory and CPU resources. The array of servers that were brought into the test were all X86-based. This meant that in terms of hardware virtualisation, any of the hypervisors available could work (we saw Linux KVM/OpenStack and VMware used by all vendors). A bigger challenge was the abstraction of the network interfaces. At the time the tests were performed, direct interaction between the server’s network interfaces was required by the guest OS. In two of our tests, the vendor indicated that the virtual switch was creating a performance bottle neck. One vendor bypassed the virtual switch while another asked us to decrease the amount of traffic we were generating.

We also asked the participating vendors to bring an orchestrator to the tests. One vendor brought a home-grown tool to act as an orchestrator while others used existing orchestrator-like tools such as VMWare’s vCloud Director/vShield or OpenStack. The latter solutions are tightly coupled with the hypervisors. Hypervisor-agnostic virtualisation of network equipment still needs to be standardized.

The area of Manageability and Orchestration (MANO) now has its own working group within the ISG, and is a key focus for many in the NFV space. It is very clear from both the NFV ISG and the developing ecosystem of NFV elements that provision of the management and orchestration functionality is absolutely not the remit of the VNFs themselves.

Portability

All vendors demonstrated an ability to migrate VNFs to a different physical host with minimal or no service inter-rupption. In most cases, migration required that a secondary instance was already prepared and executed on the target location, so the migration only involved redirection of traffic. The secondary VNF instances automatically synchronized their state with the primary instance, which made them well-suited for High-Availability configurations. We could test such scenarios by triggering on-demand failure as well as through forceful termination of a process. Through use of virtual IPs, such High Availability clusters could be made fully transparent for the network infrastructure.

Physical migration still required network configuration adjustments within guest virtual machines in some cases, something that an operator is likely to remain completely in the domain of the host machine and hypervisor.

Elasticity

Most vendors have already implemented a possibility to automatically load-balance the traffic across multiple VNFs of the same type, as well as automatic integration of the newly spawned instances into the resource pools. Thus, the implementations already cover the most difficult part of the elasticity requirements.

Of the implementations tested, some had the ability to automatically spawn additional VNF instances in an overload situation. There are obvious overlaps with the management and orchestration layer here. In fact, the expectation within the NFV ecosystem is that additional capacity will be delivered through the spawning of additional VNF instances, and that the decision to do so lies firmly with the MANO layer, based on KPI metrics from the VNFs, not an individual VNF. The key requirement on the VNF itself is the ability to report relevant metrics and to allow creation and deletion of instances.

Advances in the MANO implementations and standards will lead to advances in the functionality the complete NFV systems can deliver.

Whether VNF creation was the result of spawning by the NFV process itself or driven by management, the VMs were pre-allocated with fixed resources, and so ultimately the maximum number of additional VMs which could be created would be limited by the resources available on the host system. There will obviously always be these fundamental limitations, since virtualisation does not create additional resources, merely making it possible to make more efficient use of the resources which are available.

CONCLUSION

We were able to verify that the solutions under test were truly virtualised and performed as intended with emulated subscriber traffic. The vendors are clearly looking to address operational challenges — the functions we tested benefit from the data center environment by spreading the load across multiple servers. Migration of virtual network functions is a reality as well already. NFV is in essence a telecommunication network. We can expect more complex operations than exist in data centers. The orchestrator will play a central role in the success of NFV in carrier networks.

As expected from any technology in its early days, there are aspects that require further standardization: A standard interface between the hypervisor, virtual switch and VNF will enable a market for orchestration functions. Interaction between hypervisors, networking interfaces, guest operating systems and the virtual functions themselves are likely to keep standard bodies occupied in years to come. State-synchronization between virtual functions is a challenge and could also benefit from further standardization. EANTC will continue to contribute our experience to the ETSI NFV ISG.