An Instrumentation and Analytics Framework for Optimal and Robust NFV Deployment

Paul Veitch, Michael J. McGrath, and Victor Bayon

Paul Veitch is with BT.

Michael J. McGrath and Victor Bayon are with Intel Labs Europe.

ABSTRACT

This article details a novel approach to the fine-tuning of carrier-grade virtualized network function deployments for both performance optimization and diagnostic purposes, using embedded instrumentation with an analytics framework. The work presented in this article is the output of a co-lab established between BT and Intel Labs Europe to investigate network-function-virtualization-related problems faced by traditional telecom operators. Results from comprehensive testing of virtual CDN and WAN acceleration use cases are presented. These results led to the development of a number of insights that will help network operators optimize the deployment of NFV on standard high volume servers. Significantly, it was found that the default configuration for some use cases resulted in suboptimal resource allocation and consumption. Consequently, opportunities exist for carriers to fine-tune their NFV deployments from both the technical and economic perspectives using approaches such as embedded instrumentation.

INTRODUCTION

The topic of network functions virtualization (NFV) is receiving significant attention within the telecommunications industry as a means to deliver innovative and scalable network capabilities at lower cost and with greater flexibility. Additionally, the scale of global investment in data center technology makes it increasingly attractive to deploy network functions as software that runs on standard high volume (SHV) servers [1, 2].

Network operators planning a gradual migration from legacy standalone hardware appliances to an architecture based on virtual network functions (VNFs) face a variety of technical and operational challenges. A major area of consideration is testing and diagnostics, whereby VNFs must be validated — prior to operational deployment — in terms of functionality, performance, robustness, and manageability. Traditional black box testing using externalized test points can result in a very restricted test methodology producing inadequate or, in the worst case scenario, skewed test results. It is important to recognize that a variety of factors should be considered in any testing regime. This includes both the resource consumption of the VNFs and their footprints on the host server/hypervisor.

The BT-Intel co-lab was established to combine expertise from both organizations to address NFV in a holistic fashion. This form of collaborative approach is critical to the successful rollout of VNFs into carrier networks due to the unique blend of IT and network skills required for deploying, provisioning, optimizing, and managing them. This article details research work from two use cases that focused on the fine-tuning of NFV deployments for both performance optimization and diagnostic purposes, using an embedded instrumentation and analytics framework in a carrier-grade environment. Results from comprehensive end-to-end testing are presented together with key insights that will help network operators optimize the deployment of VNFs on SHV servers.

PROBLEM STATEMENT AND RELATED WORK

The NFV architectural framework dictates that network functions reside as software-based virtual appliances running on an x86 server with a *hypervisor* providing access to the server's compute, storage, and network resources. The architecture is designed in such a manner that each VNF should be unaware of other guest VNFs running on the same server, due to the isolation and partitioning of resources conducted by the hypervisor within the virtualization layer. A high-level representation of the key components making up the overall NFV framework has been defined by the European Telecommunications Standards Institute (ETSI) Industry Specification Group [3].

The traditional approach to testing and validation of telecommunications equipment normally involves point testing of devices known as systems under test (or SUT). Additionally, devices such as network emulators can introduce

0163-6804/15/$25.00 © 2015 IEEE

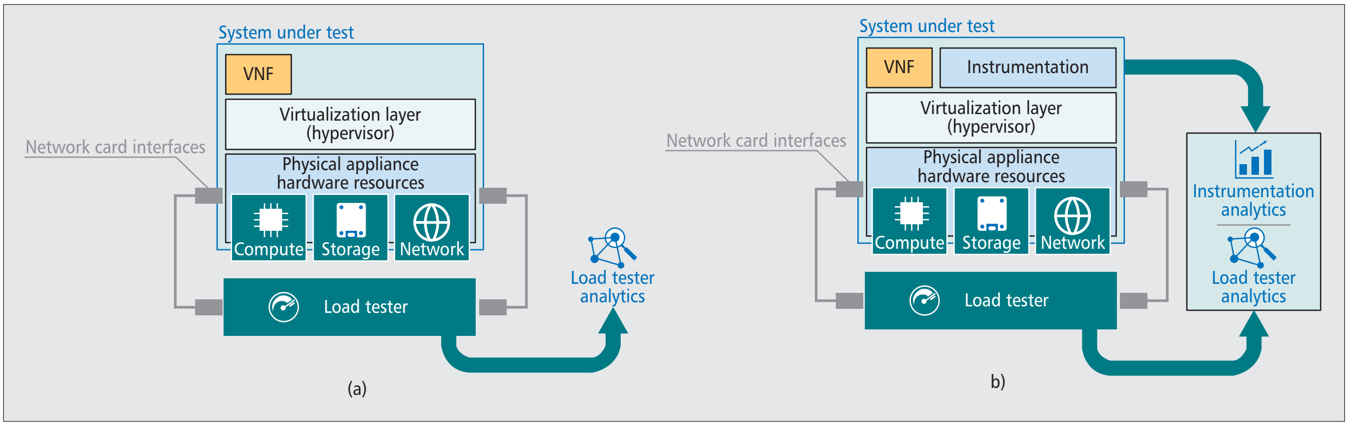


Figure 1. NFV Testing Framework: a) no instrumentation; b) embedded instrumentation.

"real-world" impairments such as latency into the test configuration. The SUTs include network functions such as routers, wide area network (WAN) accelerators, optimizers, firewalls, and load balancers. For characterization of key performance indicators such as network throughput, packets per second (PPS), and latency, a suitable load testing device must be connected to the external interfaces of the network device.

A major challenge faced by network operators planning to evolve their network estate based on the principles of NFV is the accurate characterization of VNFs in a test environment such that an optimal and robust deployment is possible in a fully operational network domain. It is therefore vital to understand any performance bottlenecks and limitations that could exist for devices running in a virtualized configuration. Since an extra layer of virtualization is introduced between the network function and the underlying hardware resources, it is critical to characterize the behavior and performance of devices in such an environment.

As the concepts of test and diagnostics within the context of NFV are relatively new, much of the published literature relevant to network operators has been channeled through standards bodies such as ETSI. A key contribution containing insights into the value and necessity of NFV test and diagnostics is the "Performance and Portability Best Practices" report [4].

The instrumentation and integrated analytics framework described in this article offers network operators an approach based on the use of instrumentation to enable performance management of VNFs in a consolidated manner. The key contribution of this article is to demonstrate the value of embedded instrumentation and integrated analytics techniques to help network operators optimize and "harden" their NFV configurations prior to an operational deployment based on a system-wide view of the VNF and its interactions with both virtual and physical resources.

Benefits and Trade-offs of Embedded Instrumentation

As shown in Fig. 1a, a traditional test methodology can be used with VNFs by connecting load generation test equipment to the network interfaces of the host x86 server. The performance characterization will be limited by the fact that the test points are 100 percent "externalized" and hence do not generate measurements from within the virtualized environment; the result is a relatively simple — but restricted — test configuration. Figure 1b illustrates an alternative approach based on embedded instrumentation that can be used within the virtualized environment to generate a more fine-grained view of performance-related test metrics. The instrumentation toolset collects and presents data for real-time processing, analysis, and visualization affording greater informational depth and detail.

Although embedded instrumentation adds additional complexity to the overall test setup, this can be offset against the following benefits for network operators:

- A richer set of metrics can be captured and analyzed due to in situ measurement within virtual machines (VMs)/VNFs resident on the NFV infrastructure (NFVI).
- Instrumentation can be deployed in a flexible fashion prior to actual NFV deployment as part of a "pre-optimization" exercise, leading to enhanced fine-tuning and customization of implementations.
- Data obtained from embedded instrumentation in a test environment can be used to determine the most useful metrics to be monitored under standard operational conditions.
- An enhanced diagnostics capability is afforded above and beyond the use of traditional externalized test points.

It should be stressed that embedded instrumentation can act as a complementary test and diagnostics resource to traditional methods, rather than as a wholesale replacement of such techniques. This fact, along with a more detailed explanation of the instrumentation and its application to real-world use cases are described in the following sections.

Instrumentation and Analysis Overview

Deploying VNFs in a performant manner on virtualized infrastructures creates significant challenges to ensure that the workload is allocated

A particular challenge for the instrumentation of virtualized network workloads is the ability to collect high rate event data without impacting the workload performance. The overhead associated with the data collection process is commonly referred to as the observer effect.

the necessary compute resources. In addition, it is necessary to ensure that the workload consumes these resources in an efficient and effective manner in order to meet the key performance indicators (KPIs) required by a network operator. Standard tools used by many operators, including hardware-based traffic load generators, can test the performance level of a VNF; however, they do not provide the necessary insights into how the VNF workload is interacting at a resource and process level within its host VM. Instrumentation of the VM environment to provide data on key system-level metrics helps to address the information gap between the *external* perspective of the test equipment and the *internal* view from within the VNF and its host VM.

Although many tools (mostly user space) already exist to assist in the gathering and monitoring of kernel counters within Linux-based systems, they provide little customization and, more importantly, offer only fragmented data sets, making a full stack view of the system and integration with analysis systems difficult [5]. This places a significant overhead on the user to process and assemble the data in a manner that can easily be exported, summarized, analyzed, interpreted, and cross-correlated with the testing equipment. The potential number of metrics that can be generated by the instrumentation easily reaches hundreds of metrics per second and millions of data points per hour.

One key feature of instrumentation is support for customization and configuration "per VNF" and the corresponding test environment. This is significant given the diversity of potential VNF workloads (multimedia, security, etc.). Typically, the configuration depends on the characteristics of the specific VNF workload (e.g., network bound, local storage bound, CPU bound). The total number of metrics available depends on:

- The number of layers instrumented and the "per layer" configuration (network layer, storage layer, performance model layer, etc.)
- The per layer granularity of the instrumentation such as aggregated per resource (e.g., overall aggregated CPU utilization)
- The sampling rate

The instrumentation framework used in the co-lab comprises two main sets of components.

Unified multi-layer/multi-host/multi service instrumentation: Focused on collecting data from the available and instrumented layers, including across hosts and service compositions. This data can be accessed and manipulated under a single unified namespace. A web-based interface uses an application program interface (API) to access and query the experimental data in the common namespace and execute analysis jobs.

Exploration, analysis, and visualization of instrumentation data. This capability allows a large number of metrics to be viewed and interacted with simultaneously. Users can employ statistical analysis capabilities to filter and identify relationships between variables across the stack in single and multiple experiment configurations.

Unified Single-Namespace Instrumentation Components and VNF Performance Modeling

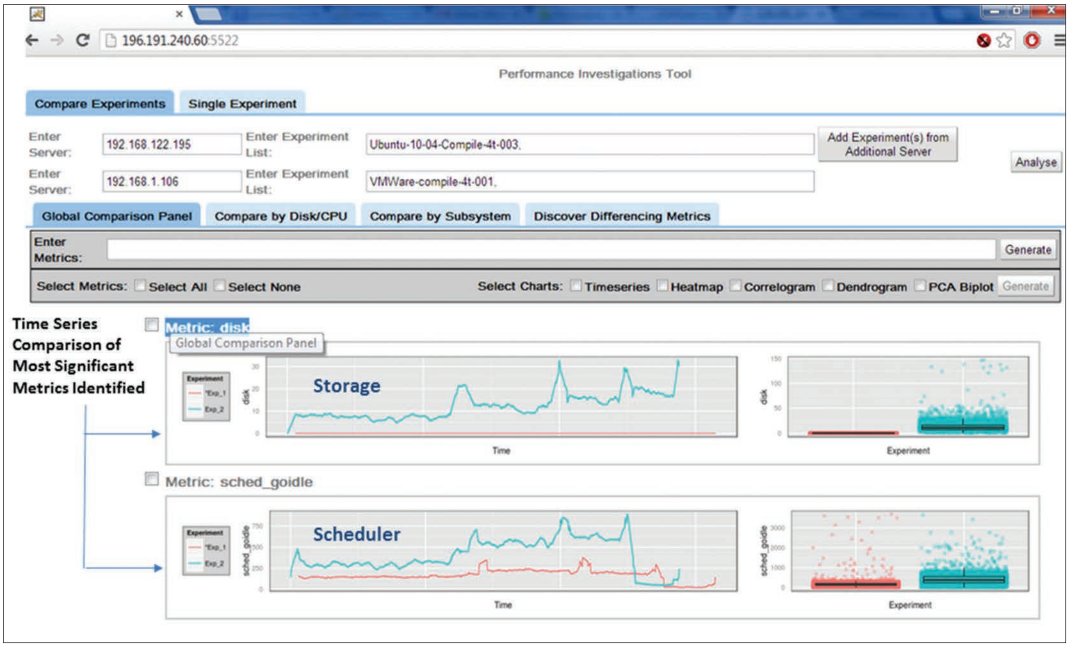
A particular challenge for the instrumentation of virtualized network workloads is the ability to collect high-rate event data without impacting the workload performance. The overhead associated with the data collection process is commonly referred to as the *observer effect* [5]. The instrumentation used in the use cases presented in this article was implemented as a low overhead agent that can be embedded inside a VNF host VM. Each agent implements a series of modules, each of which typically instruments one or more layers or subsystems, such as the I/O network and CPU subsystems. The main function of the various modules developed was to read the local kernel (e.g., */proc* filesystem), service, application counters, and so on, and to transform the data collected into usable formats by parsing and normalization. The agent then collects, synchronizes, and integrates the data from the different subsystems into a single unified namespace and exports the data to other components/services such as analysis and visualization.

Each VNF requires a different set of instrumentation modules depending on the workload type. Therefore, the architecture of the instrumentation is highly extensible supporting integration of new metrics as well as the implementation of customized derived metrics that can form part of the local metric namespace. Derived metrics are based on the fusion of raw metrics using defined mathematical transformations into a single metric that is typically indicative of operational performance in a manner that cannot be measured directly. It is envisaged that as the use of embedded instrumentation in VNF deployments becomes more widespread, new categories of derived metrics will emerge on a per VNF type, offering unique opportunities for innovation.

Exploration, Analysis, and Visualization Components

The exploration, analysis, and visualization components of the instrumentation framework play an important role in helping to filter and identify the metrics of interest from the hundreds of potential metrics across different VNFs. Figure 2 illustrates the main components of the user interface (UI). Different VNF experimental runs can be selected by the user and compared across multiple test runs using different methods such as clustering, principal component analysis, and information gain, as well as summary statistics across all metrics and experiments. This form of approach allows the user to filter and find the most relevant metrics across the experiments encompassing different criteria such as which metrics changed the most, correlated differently, achieved higher values of utilization, and/or saturated across configurations.

Once the experimental runs and comparison



Enter Server: 192.168.122.195
Enter Experiment List: Ubuntu-10-04-Compile-4t-003,

Enter Server: 192.168.1.106
Enter Experiment List: VMWare-compile-4t-001,

Figure 2. Web-based user interface of the instrumentation framework.

The initial focus for both use cases was an exploratory phase to assess the stability of the instrumentation framework and to establish that it had no measureable impact on the performance of the VNF. Comparison of instrumented and uninstrumented versions of the VNF case studies confirmed no notable impact on performance.

operators are selected, the framework computes the user choice and returns the result of the analysis. In the case of Fig. 2 the analysis provides a series of ranked graphs that shows a "per metric" time series and a box plot comparison of the same metric across different configurations. For this particular case, the comparisons consist of two separate experiments. The box plot allows the user to quickly evaluate the magnitude of the variation and the data distribution, while the time series graphs allow the user to see how the metric evolves on a temporal basis.

The following section provides further examples of how the tool was used in real-world test cases, including performance optimization and anomaly detection/fault finding scenarios.

Case Studies

The two case studies presented in this section are representative of real-world NFV deployments that communication service providers (CSPs) are actively progressing. Figure 3a shows the first of these, involving a content delivery network (CDN) cache as the SUT, while Fig. 3b shows the second scenario involving a WAN accelerator as the SUT. Both the CDN and WAN acceleration devices are proprietary off-the-shelf virtual instances of the network functions, and were installed and configured on Intel XEON®-based servers running a commercial type 1 hypervisor.

In the first scenario involving a virtualized CDN cache, the load tester was set up to generate multiple on-demand client requests for video content, served directly from the cache itself and returned to those clients. Although other components existed in the overall setup (including an origin server to distribute "source content" to the CDN cache, cache management software, switches, etc.), only the key components are illustrated for simplicity. The physical connectivity between the load tester and the server hosting the CDN application was 10 Gigabit Ethernet.

In the second scenario, based on a virtualized WAN acceleration device, the load tester was set up to generate multiple on-demand client requests for file content, served from designated servers on the load tester at the far end of the network link. An impairment device, which introduced a configurable and uniform network delay, was used for "WAN emulation" purposes representative of a multiprotocol label switched (MPLS) core network, and two bookended acceleration devices were deployed on either side of the impairment device. The device at the "client end" was a hardware-based appliance, while the device at the "server end" was a virtualized appliance, and was the actual SUT; together, these components form the end-to-end network service. WAN acceleration devices work in tandem to reduce protocol chattiness as well as to detect patterns of repetition in the data packets being transferred across the WAN [6]. Smaller-sized tokens are sent in place of the repetitive data packets, significantly reducing the number of packets that are sent over the WAN or viewed another way, accelerating the end-to-end data transfer. Both diagrams in Fig. 3 indicate the presence of embedded instrumentation within the VNF, as outlined in the previous section.

Results and Insights

The initial focus for both use cases was an exploratory phase to assess the stability of the instrumentation framework and to establish that it had no measureable impact on the performance of the VNF. Comparison of instrumented and uninstrumented versions of the VNF case studies confirmed no notable impact on performance, as indicated by test data presented in Table 1, collected as part of an initial baselining evaluation exercise.

	Throughput without instrumentation	Throughput with instrumentation
CDN 10G load-progressive download	10 Gb/s	10Gb/s
CDN 10G load-adaptive bit rate	10 Gb/s	9.85 Gb/s
WAN accelerator-500M load	500 Mb/s	500 Mb/s
WAN accelerator-1Gb/s load	1 Gb/s	1 Gb/s

Table 1. Baseline throughput data measurements using instrumented and uninstrumented test configurations.

Case Study 1: Virtual CDN

The virtual CDN testing included video-on-demand (VoD) content served using HTTP-based progressive download, as well as adaptive bit rate (ABR) VoD and live streaming, with a specific focus on network throughput as the KPI of principal interest.

Based on vendor recommendations, the number of virtual CPU (vCPU) cores allocated for the test of the CDN cache was initially set at 12, and this comfortably achieved the target throughput of 10 Gb/s. This was easily verifiable using the built-in load testing analysis tools. Additionally, the instrumentation indicated that the actual vCPU usage was relatively low, as indicated by significant periods of CPU idle time in both scatter plots and heat maps. This led to the consideration that similar performance could be achieved with lower numbers of vCPUs in an effort to minimize CPU idle time; hence, the tests were re-run with 4- and 6-vCPU configurations for the virtual CDN application.

Figure 4a shows the load tester view of achieved network throughput for 4, 6, and 12 vCPUs, which in all cases peaks at 10 Gb/s. Figure 4b shows the difference in the scatter plots and heat maps applicable to the 4- and 12-vCPU scenarios. It was clear from the box-and-whiskers-scatter-plots and heat maps that there is much higher idle time (where the vCPU is not doing anything useful, white/lighter areas visible on the heat maps) in the 12-vCPU case compared to 4 vCPUs. Viewed from another perspective, this is the same as saying that the 4-vCPU setup makes more efficient use of the available vCPU resources as the vCPU workloads are much higher.

This insight would not have been possible without access to the CPU idle time data gleaned from the embedded instrumentation. This leads to the compelling prospect that fewer CPUs may achieve the target performance, which could result in an economic benefit for the network provider. For example, the same server could host multiple CDN applications in a multi-tenant setup, or other virtualized applications could make use of the unallocated CPU cores.

However, a further stage of analysis may lead to the determination of the optimal setup. The graphs presented in Fig. 5 show the bytes (worked on per) millisecond ratio (BMSR) performance metric plotted for the same tests. This is a derived metric based on the sum of total network reads and writes (network throughput in bytes) vs. total CPU utilization in milliseconds. A larger value for this metric (i.e., increased throughput and less CPU required to "push" bytes around) indicates better performance which is indicative of efficient network utilization. The data shows that the 6-vCPU case had the highest

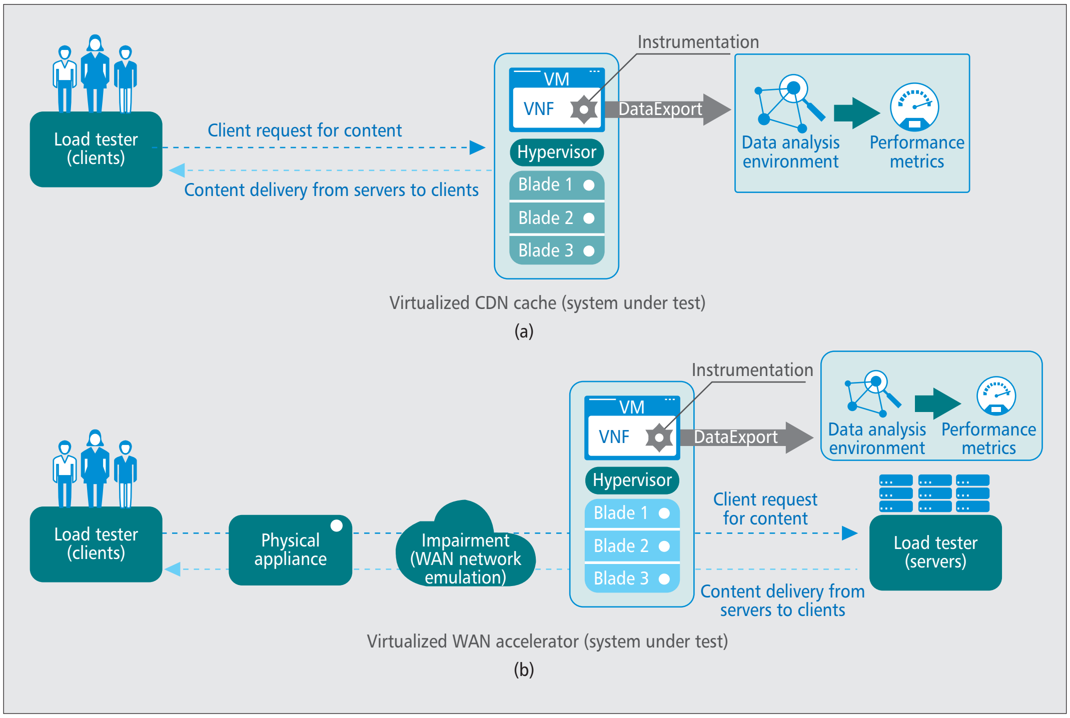

Instrumentation
VM
VNF
DataExport
Data analysis environment
Performance metrics
Load tester (clients)
Client request for content
Content delivery from servers to clients
Hypervisor
Blade 1
Blade 2
Blade 3
Virtualized CDN cache (system under test)
(a)
Instrumentation
VM
VNF
DataExport
Data analysis environment
Performance metrics
Hypervisor
Blade 1
Blade 2
Blade 3
Load tester (clients)
Physical appliance
Impairment (WAN network emulation)
Client request for content
Content delivery from servers to clients
Load tester (servers)
Virtualized WAN accelerator (system under test)
(b)

Figure 3. NFV scenarios: a) virtual CDN; b) virtual WAN acceleration.

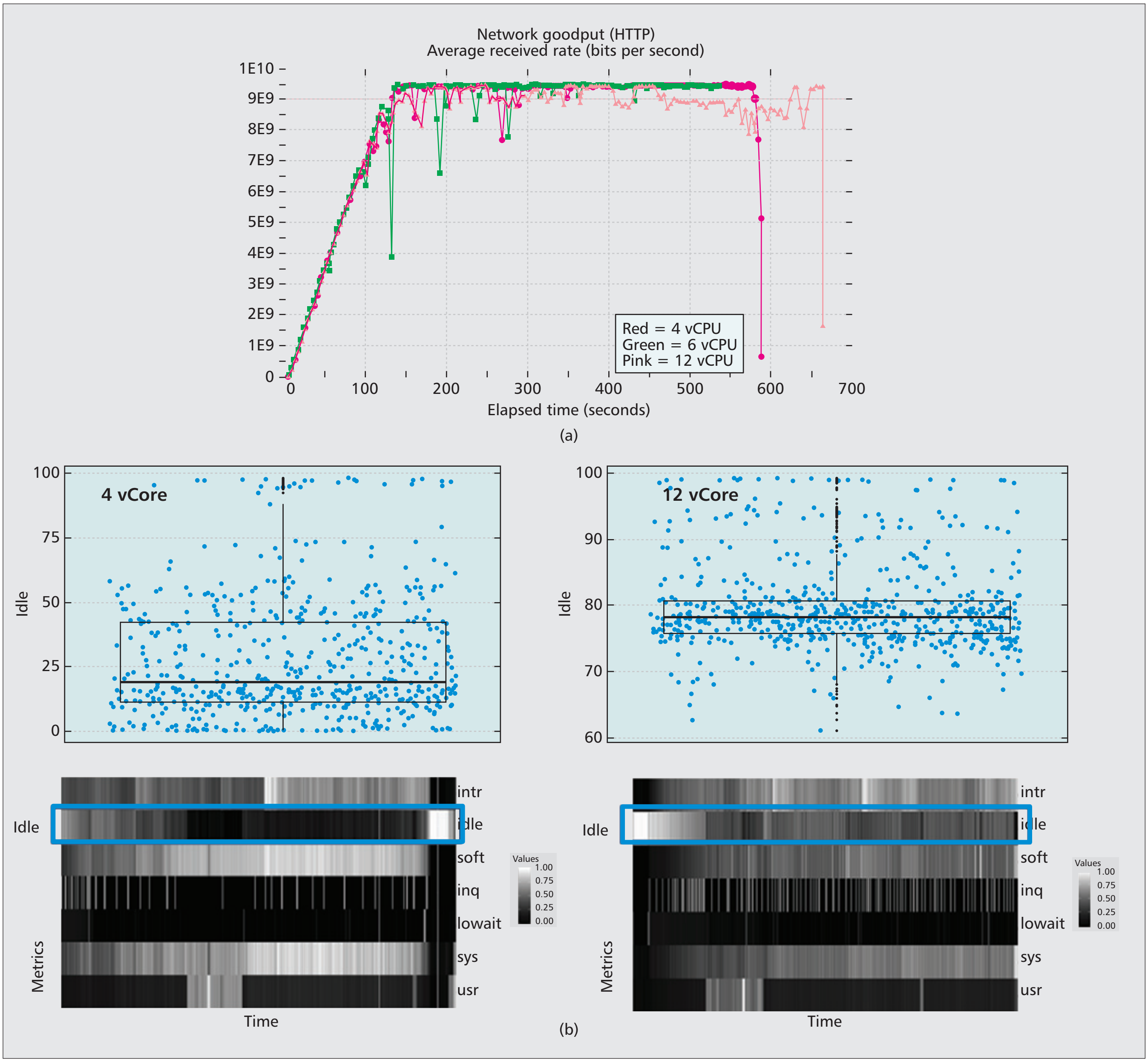


Figure 4. a) External view — 4, 6, and 12 vCPUs; b) internal view — box-and-whisker with scatter plots and corresponding heatmaps for visualization of CPU idle, 4 and 12 vCPUs.

value for this particular metric, suggesting that the “optimal” setup for this virtual CDN cache is 6 vCPU cores, which is still 50 percent lower than the original vCPU allocation and hence makes a significant saving in allocated resources. It also results in a setup that lends itself to higher vCPU utilization levels than 12 vCPUs while retaining headroom capacity. A 4-vCPU configuration — while effective from a utilization perspective — provides minimal headroom capacity and therefore may not be suitable from an operational perspective. The analytics functionality of the instrumentation framework supports the creation of derived or synthetic metrics such as BMSR, which can be implemented specifically for a VNF by the network operator.

The results for this particular scenario indicate an ability to “fine-tune” server resources that are better matched to “expected” traffic metrics such as bandwidth throughput. Any subsequent changes in traffic patterns that dictate scaling up or scaling down of resources to satisfy the demand should be accommodated more easily by leveraging the built-in elasticity of an NFV architecture compared to fixed hardware.

Case Study 2: Virtual WAN Acceleration

The virtual WAN accelerator was originally tested in the absence of any embedded instrumentation to assess performance metrics under a range of test scenarios and traffic types. This included a baseline characterization of HTTP and HTTPS (i.e., encrypted with secure socket layer, SSL) traffic flows from end user “clients” accessing remote “servers” as previously illustrated in Fig. 3b.

As the deployment of VNFs into carrier networks gathers momentum, the use of embedded instrumentation to complement existing external testing approaches and internal VNF metric capabilities is likely to grow in importance and utility. There are, however, many interesting problems that have yet to be explored in any significant depth.

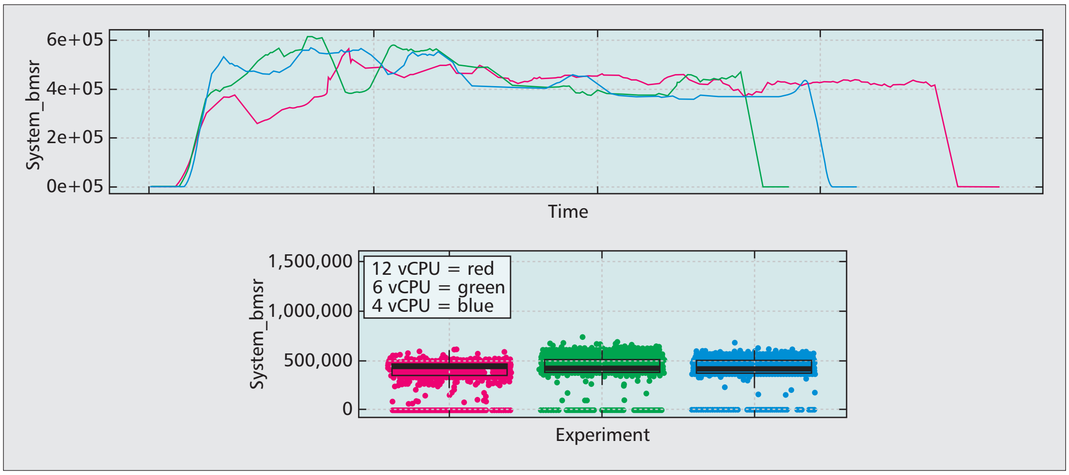


Figure 5. BMSR metric plotted for 4, 6, and 12 vCPUs.

When the instrumentation was installed, many of the tests were revisited with the initial objective of achieving performance-related "fine-tuning" of allocated server resources, similar in objective to the virtual CDN case study outlined earlier. Although not part of the original test plan, additional test validation insights were obtained from a fault diagnostic perspective. A scenario arose whereby the WAN accelerator stopped accelerating HTTPS traffic and reverted to a mode where it simply passes packets through uninspected. This is indicated on the traffic graph shown in Fig. 6, where the throughput drops from around 800 Mb/s (where traffic is being accelerated) to approximately 250 Mb/s (where traffic has stopped being accelerated), which is the default setting of the WAN emulation device.

Without instrumentation installed, thereby adhering to traditional end-to-end external test points, the traffic graph output from the load tester would act as the key evidence of the problem. Analysis of the heat map output from the instrumentation, however, indicated an I/O disk spike event just prior to the point at which optimization stops, and can actually be correlated with a traffic dip occurring prior to the major drop in traffic shown in the traffic graph of Fig. 6. This observation, garnered from the instrumentation data, resulted in the vendor focusing their attention on the virtual WAN acceleration behavior prior to the traffic drop. The eventual explanation for the behavior was attributed to the detection of a packet that could not be decrypted by the WAN accelerator and hence, as part of security best practice, reverted to a safer mode of operation where no optimization/acceleration is performed (thus passing packets through transparently). On the basis of prior experience, it was suggested by the vendor that such behavior would most likely be due to the particulars of the load tester's SSL settings, which in some cases can generate "bad packets." Review of the load tester setup identified a configuration option that deactivated specific SSL settings, which resulted in the test being successfully run with no cessation of the optimization/acceleration capability.

The slightly unexpected but no less compelling insight gleaned during this case study was that embedded instrumentation can provide an extra layer of granularity for fault diagnostic purposes during test and validation of a specific VNF. The utilization of heat maps allows us to plot different types of metrics (normalized) and to quickly observe the behavior of tens, hundreds, or even thousands of metrics simultaneously over a period of time. This feature is particularly useful for anomaly detection/fault finding scenarios, as illustrated by this example.

Conclusions and Further Work

NFV will undoubtedly present network operators with a number of significant implementation challenges, many of which are already being addressed through collaborative activities across the industry. This article has addressed the specific problem of test and diagnostics, whereby VNFs must be validated — prior to operational deployment — in terms of functionality, performance, robustness, and manageability. In some ways, thorough VNF validation is more demanding than standalone physical hardware, since there are many more possible permutations of hardware build and hypervisor, not to mention the deployment of a range of VNFs from different vendors co-resident on the same server (i.e,. the multi-tenant or noisy neighbor problem).

By devising distinct case studies using very different VNFs with unique characteristics subject to testing, the benefits of embedded instrumentation have been highlighted. The main conclusions that can be drawn from the BT/Intel tests with integrated instrumentation software are as follows:

- The integration of the instrumentation did not negatively affect the "baseline" performance of the VNFs.
- The use of analytics to capture certain performance parameters complemented the load testing capability by enabling additional layers of insight and visualization.
- The increased granularity of the performance characteristics view afforded by embedded instrumentation enabled fine-tuning of allocated server resources (vCPU cores) in a manner that provided a better match with expected traffic loads, hence

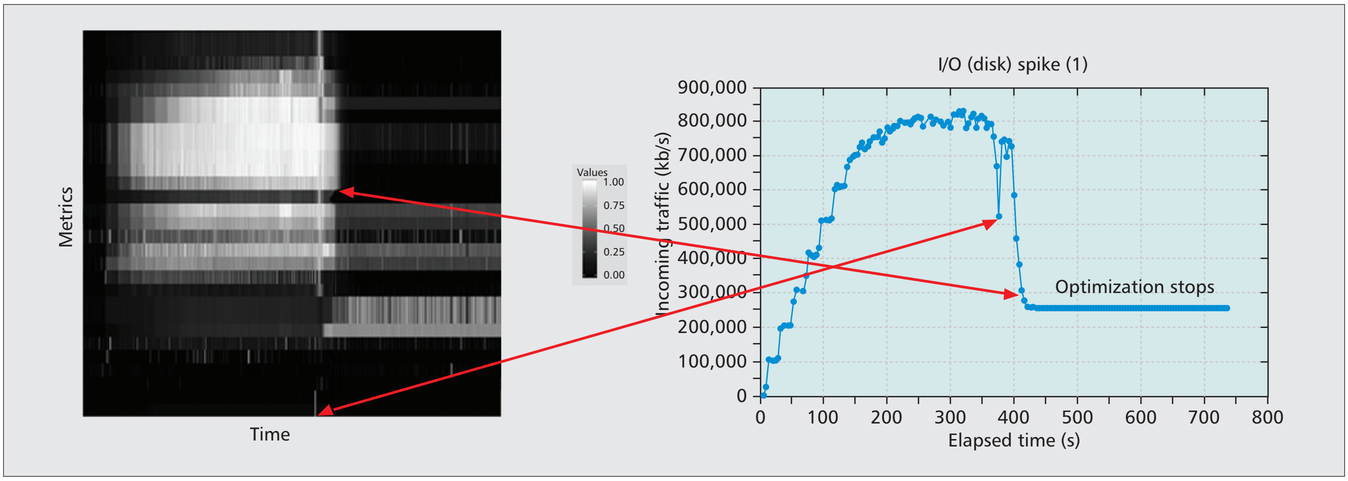


Figure 6. Virtual WAN acceleration fault diagnostics.

optimizing the set-up. This approach has significant techno-economic advantages over traditional methods, and lends itself to fully maximizing the promise of resource elasticity offered by NFV.

- The granular view of the performance characteristics afforded by the embedded instrumentation led to the diagnosis of a nonoptimal configuration of the end-to-end setup of the WAN acceleration use case. Without the instrumentation data, this issue might otherwise have been left unresolved; at best, it would have taken significantly longer to identify the root cause.

As the deployment of VNFs into carrier networks gathers momentum, the use of embedded instrumentation to complement existing external testing approaches and internal VNF metric capabilities is likely to grow in importance and utility. There are, however, many interesting problems that have yet to be explored in any significant depth. Some of these areas of interest include, but are not limited to:

- Further investigation of use cases involving multiple instances of the same VNF, as well as a range of different VNFs on the same physical server. The latter scenario represents concerns regarding noisy neighbor effects; that is, can we be certain the presence of one VNF is not detrimentally affecting the performance of another VNF?
- Investigation of more complex network services comprising multiple VNFs deployed in both a single data center or across multiple geographically dispersed data centers.
- Using results from instrumentation to devise planning rules for VNFs co-resident on servers, exposing platform-specific features to improve VNF workload placement decisions, hypervisor type, and range of VNFs planned for support on a particular server.
- Identifying how VNFs scale and perform reliably in commodity cloud environments rather than on bespoke hardware nodes that are optimized for that specific function.

It is likely that the rate at which NFV deployments occur across industry in the coming years will be influenced to some degree on how comprehensively these technical challenges are addressed.

Acknowledgments

BT and Intel acknowledge support from William Tai of Riverbed Technology for his assistance with case study 2.

References

[1] R. Jain and S. Paul, "Network Virtualization and Software Defined Networking for Cloud Computing: A Survey," *IEEE Commun. Mag.*, vol. 51, 2013, pp. 24–31.

[2] ETSI, "Network Functions Virtualisation (NFV) — Network Operator Perspectives on Industry Progress," White Paper #3, Oct. 2014.

[3] ETSI ISG, "Network Functions Virtualisation (NFV): Architectural Framework," 2013.

[4] ETSI ISG, "Group Specification-NFV Performance and Portability Best Practises," NFV-PER 001 v1.1.1, 2014.

[5] B. Gregg, *Systems Performance: Enterprise and the Cloud.*, 1st ed., Prentice Hall, 2014.

[6] S. Plamondon, "How WAN Optimization Works," *Riverbed Connections*, Aug. 2013, http://www.riverbed-news.com/2013/08/how-wan-optimization-works/.

Biographies

Paul Veitch (paul.veitch@bt.com) holds M.Eng. and Ph.D. degrees from the University of Strathclyde, Glasgow, United Kingdom. He joined BT at Martlesham Heath, Ipswich, United Kingdom, in 1996, and worked on various aspects of broadband transmission, multi-service platforms, and 3G mobile infrastructure design before joining Verizon Business (UUNET) in 2000. He returned to BT in 2003, and was infrastructure design authority for IP VPN and BT Consumer networks before joining a small team of network innovation specialists in 2012 to lead on NFV proof-of-concept validation and business development.

Michael J. McGrath (michael.j.mcgrath@intel.com) is a senior researcher at Intel Labs Europe. He holds a Ph.D. from Dublin City University. He has been with Intel for 15 years, holding a variety of operational and research roles. He is currently a researcher in the FP7 T-Nova project, which is focused on the concept of network functions as a service (NFaaS). He is also a researcher at the BT Intel Co-Lab based at Adastral Park, United Kingdom, which is focused on research relating to the deployment of VNFs in carrier grade network env(ironments. Michael has co-authored more than 25 peer reviewed publications.

Victor Bayon (victor.bayon-molino@intel.com) is a senior researcher at Intel Labs Europe and a member of the BT Intel Co-Lab based at Adastral Park. His main area of interest is the development of instrumentation, performance analysis, and performance management tools, and their application to different domains such as NVF in carrier grade environments. He holds a Ph.D. from Nottingham University, United Kingdom.