Network Function Virtualization: Spirent TestCenter Virtual and Spirent Avalanche Virtual

Network Functions Virtualization: Intel, Spirent, and the Role of Virtual Validation

Executive Summary

The explosion of global network traffic. The establishment of over-the-top (OTT) content providers. The onward march of cloud computing. The promise of the Internet of Things. A timeframe that is measured in hours and days rather than months and years. These are the challenges facing network operators, who must find ways of developing sustainable cost-to-revenue ratios – all while changing traffic types put traditional business models under severe strain.

In this environment, innovations such as software-defined networks (SDNs) and network functions virtualization (NFV) are gaining momentum. Offering unprecedented flexibility and control, both have advantages that make them attractive at an operational level as well as a business level.

This paper describes the essential role that virtual testing and validation plays in the development of a NFV infrastructure. It looks at how virtual test tools from Spirent, built on open, scalable, and high-performing Intel® Architecture, help reduce operational expenditure and facilitate daily management of the network.

NFV: The Operational Perspective

The advantages of NFV in terms of reduced capital and operating expenditures, greater responsiveness to customer demand and the timely delivery of innovative services have dominated the conversation to date. It provides a level of flexibility that enables network operators to optimize deployment of network functions and services to suit business requirements, and adapt available capacity for operational needs.

Not surprisingly, the market is developing fast. A number of operators have already completed proof-of-concept trials and successfully tested various components including virtual broadband remote access servers (BRAS), content delivery networks (CDNs), evolved packet cores (EPC), firewalls, and set-top boxes (STB). In addition, new virtualization protocols and technologies such as Virtual Extensible LAN (VXLAN) and Ethernet virtual private network (E-VPN) are emerging. We have already seen new OpenFlow and cloud-management system vendors entering the space, with many more to be expected.

However, less well discussed, and just as significant are the advantages that NFV brings at the operational level, notably service fulfillment and service assurance.

The traditional network structure has often formed the backdrop to the classic dichotomy between business analysts demanding change, and operational experts charged with its implementation. However, by implementing network functions in software that runs on virtualized standard hardware, NFV eliminates much of the heavy lifting associated with developing and implementing new network services.

The immediate advantage of using TestCenter Virtual or Avalanche Virtual is that they are easier and more convenient than time-consuming and painstaking manual methods. They also have the necessary flexibility and scalability demanded by an NFV environment.

Its combination of virtualized services, standardized hardware, and a single-architecture environment enables new devices and connectivity to be commissioned, installed, and validated remotely. This takes much of the heavy lifting out of the process for developing and adding new services or functionality by eliminating the lengthy cycle of procurement, development, and testing of new equipment. Application software maintenance releases can generally be downloaded to a remote server, which also helps eliminate many of the challenges associated with in-the-field firmware upgrades over multiple combinations of hardware, firmware, and software.

Just as new service development and implementation becomes less time-consuming and resource-intensive, the use of existing hardware becomes much more flexible and efficient. It can be repurposed so that new functions can be moved to, or instantiated in, various network locations without installing new kit.

The effect on operations can be relatively minor – minimizing the number of spares that must be held, for example. Or it can be substantial, such as increasing the ability to consolidate with cloud computing or other data center support arrangements. Above all, available infrastructure can be optimized on a time-of-day basis, and servers loaded to levels based on their available capacity. Not only does this create significant advantages in terms of business continuity, redundancy management, and quality of service, it helps to close that gap between business goals and operational capability.

The Role of Virtual Validation and Testing

For these new capabilities to achieve these goals, however, effective and robust remote validation is required. Testing and validating the reliability and performance of network functions and services prior to deployment in the field, and isolating any faults in the network rapidly and remotely is essential to maintaining the stability of the virtual machine (VM) environment.

Virtual test systems such as Spirent TestCenter Virtual or Avalanche Virtual can test each element on a server remotely, both passively and actively. Where the highest levels of data-plane performance are required, or where timing needs to be accurate within a matter of microseconds, then physical test appliances are still recommended. However, in all other scenarios, these kinds of virtual testing solutions provide the flexibility to test network functions on multiple servers in various locations as well as individual network functions within a single service chain.

The immediate advantage of using TestCenter Virtual or Avalanche Virtual is that they are easier and more convenient than time-consuming and painstaking manual methods. They also have the necessary flexibility and scalability demanded by an NFV environment.

Internally powered by multi-core Intel® Xeon® processors, Spirent's solutions run different software threads on different cores. By deploying on Intel® Architecture with support for virtualization, Spirent's virtual testing solutions can be scaled in multiple dimensions simultaneously. As an example, achieving multi-protocol scale on a border gateway protocol (BGP) and a label distribution protocol (LDP) could be achieved by running BGP on one core and LDP on another.

Ease and convenience aside, remote and scalable testing also allows links between sites to be routinely checked by service assurance systems without disrupting normal operations. The multi-tasking computing hardware can run tests on newly commissioned network elements while continuing to provide seamless functionality for existing components.

Furthermore, back-up links can be continually tested when they are not in use (e.g. overnight) to ensure that resilience measures are reliable and robust.

Solutions like TestCenter Virtual or Avalanche Virtual also enable a degree of proactive monitoring and auto-diagnosis, which in turn offers more preventative fault analysis – with clear long-term advantage.

The Spirent Avalanche solution provides multi-10 Gbps capacity, security and performance testing for virtual firewalls, load balancers, WAN accelerators, DPI boxes, intrusion detection systems (IDS), intrusion preventions systems (IPS), and other virtual Web application infrastructures.

The Spirent TestCenter chassis provides functional and performance testing of virtual BRAS, provider edge, customer edge, and STB devices, as well as routing, access and MPLS protocols.

Enabling Testing with Intel® Architecture

Solutions like Spirent's are a critical element in the NFV ecosystem, and are important drivers for wider adoption. However, their performance is in turn enhanced by the exceptional performance developments in micro-processing architecture for telecommunications and network environments for data-plane workloads.

Intel processors perform packet and signal processing in addition to handling application and control-plane processing, reducing the need for specialized silicon. Traditional network infrastructure device workloads have required the use of silicon components such as network processing units (NPU), digital signal processors (DSP), field-programmable gate arrays (FPGA), application-specific integrated circuits (ASIC), and application-specific standard products (ASSP); and many of these can now be addressed by software applications running on Intel processors.

At the hardware level the Intel® Communications Chipset 89xx Series has been optimized to handle communications workloads using the Intel® QuickAssist Technology interface. This is complemented by the Intel® 82599 10 Gigabit Ethernet Controller and Intel® Ethernet Switch FM6000, enabling speeds of up to 720 Gigabits per second (Gbps).

The advanced hardware features can be exposed to software through the Intel® Data Plane Development Kit (Intel® DPDK), a set of drivers and libraries that can provide a tenfold improvement in packet-processing performance, enabling throughput of more than 100 million packets per second (Mpps) on a single Intel Xeon processor, and 250 Mpps on a dual-socket configuration.

For Spirent, using Intel DPDK drivers in the user space has generated a significant improvement in data-plane performance of the Avalanche Virtual appliances. Spirent deploys the Intel DPDK libraries as its packet-processing interface. By bypassing the Linux kernel for packet processing, Spirent's applications have experienced an additional twofold increase in data-plane performance.

By virtualizing network functions on Intel Architecture, network operators gain the ability to deploy the principles of NFV within their networks with shared infrastructure. Network operators have fewer hardware units to configure, maintain, and support in the field. Intel processors also feature advanced power management functions at the chip level that can power down unused cores within the processor to further enhance the power savings derived from optimized hardware deployments.

This is underpinned by key security features, since Intel® Virtualization Technology (Intel® VT) provides secure, separate partitioning of processing capacity to prevent interference between network services.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) can also be used to accelerate encryption of control plane protocols and to create VPN capabilities on the underlying infrastructure.

Open Ecosystem

Intel is also working with hypervisor partners to ensure the availability of a low-latency, deterministic virtualization environment (such as Wind River's Open Virtualization Profile) to other run multiple workloads on a single multi-core Intel processor, to suit demanding requirements such as Mobile Wireless LTE base-stations.

Together, these developments enable network operators to realize the benefits of virtualization with next generation network infrastructure based on technologies developed by Intel.

Crucially, Intel also works with operating system vendors to ensure that software applications are fully compatible with Intel Architecture and able to take full advantage of its capabilities to support operational workloads. A number of operating systems are already optimized for Intel Architecture. Because Intel processors are software-backwards compatible, transferring to Intel Architecture enables network operators to make investments in software with confidence that those investments will be protected.

It is also critical to opening up the ecosystem. Because Intel Architecture is compatible with a diverse array of software and hardware providers and commercial off-the-shelf (COTS) solutions, a network running on Intel Architecture is not locked into specific vendors. The choice remains in the hands of the operator.

Conclusion

The performance of multi-core Intel processors has created new opportunities to consolidate multiple networking workloads onto a single architecture while still ensuring quality of service and quality of experience through advanced testing. With Intel looking to fulfill Moore's Law for at least the next four years, high-performance network virtualization is a very real proposition for network operators. With it comes the ability to reduce network complexity with no sacrifices in performance.

By taking an architectural approach, network operators can reduce both hardware and software engineering effort, while benefiting from the ever-increasing performance-per-watt of Intel processor-based platforms. This is in addition to the wider benefits that NFV offers: the improved cost-to-revenue equation, the enhanced flexibility and greater customer-focused service delivery.

For more information about network and IT virtualization, visit http://www.intel.com/go/virtualization.