How to Build Automated NFV Infrastructure
Executive summary

It’s been nearly five years since Network Functions Virtualization (NFV) was first conceived by a group of leading network operators, but the promise of running more flexible, better performing and highly cost-efficient communication networks is not yet within their reach. In fact, there is growing scepticism about the business case for NFV. Part of the reason for this sense of disillusionment is that current NFV solutions make trade-offs between service agility, performance and cost savings. Few, if any, solutions can provide all of these benefits, which together forge the fundamental promise of NFV.

In this phase of NFV development, it’s time to get back to basics and rethink how the underlying NFV infrastructure (NFVi) is implemented. The key to achieving the flexibility, performance and cost savings that operators require is to ensure that the NFVi is inherently designed to enable automation.

But how do operators get there? This paper explores the steps network operators can take to construct NFVi that will achieve the performance, flexibility and cost efficiency they need to make the NFV business case work.
Introduction

The drivers for network function virtualization (NFV) all come down to flexibility, performance and cost savings. When a group of the world’s largest network operators launched the NFV initiative back in 2012, the original goals were to reduce equipment costs and power consumption, improve operational efficiency, accelerate time-to-market for new services, open the market to new suppliers, configure the network in real-time, enable multiple functions on the same hardware, enable the re-use of infrastructure, and optimize resource usage through consolidation. While it is unrealistic to expect the telecommunications industry to tick every item on such an all-embracing wish list within five years, confidence in NFV and commercial deployment progress show signs of wavering.

A recent Heavy Reading survey of 40 leading communication service providers (CSPs) indicated that confidence in NFV deployments has dipped over the last year. In November 2016, just 5% of CSPs surveyed said they were extremely confident in the timelines for deploying high-priority network functions, which is down from 22% in November 2015. The survey also found slow progress in putting high-priority network functions into production, as the percentage of CSPs with more than 25% of this type of network function in production decreased from 17% to 13% over the year.

The growing sense of disillusionment about NFV suggests that the transition to virtualized networks will be more complex and will take longer than previously hoped. One of the most high-profile hurdles for NFV has been the thorny issue of management and orchestration (MANO). The industry has rallied around orchestration efforts to find workable solutions. With solutions now in sight for lifecycle orchestration, which will enable service agility through automated service creation and management, a significant hindrance is likely to be removed from the path to NFV.

But while service agility will be supported at the orchestration layer, CSPs are still striving for overall flexibility, performance and cost efficiencies. These capabilities are essential not only for the success of NFV-based services but also for the long-term success of CSPs’ business.

In this phase of NFV development, it’s time to get back to basics and rethink how the underlying NFV infrastructure (NFVi) is implemented and consider whether it is fit for purpose to achieve the flexibility, performance and cost efficiency that CSPs require. The following makes the case for automation as the critical requirement for NFVi and explores the steps CSPs can take to build automated NFVi in order to realize the promise of NFV.
5 Steps to Building Automated NFVi

The NFVi compromises all of the hardware and software components that create the environment in which virtual network functions (VNFs) are deployed, according to the European Telecommunication Standards Institute (ETSI). It consists of a physical layer of standard, off-the-shelf servers and network interface cards (NICs), on top of which runs the virtual layer comprising a hypervisor, virtual infrastructure managers (VIMs), virtual machines (VMs), and virtual network functions (VNFs). The NFVi’s role is to provide a technology platform and the physical resources to support the execution and dynamic configuration of the VNFs, which are implemented across multiple distributed servers. The decisions about NFVi hardware and software implementations are among the most important choices CSPs will make in their network virtualization strategies, because they will determine the level of performance, reliability and cost of CSP services.

In addition to its functional role as the critical technology platform in virtualized environments, the NFVi is also envisioned by ETSI as the foundation for fostering an open, innovative NFV ecosystem, enabling multi-vendor interoperability where VNFs from any supplier can run on any NFVi. It’s clear that the NFVi is a pivotal point in the NFV architecture for enabling the flexibility, performance and cost-efficiency that NFV promises. But how?

In short, the answer is automation. Having the ability to automate workflows and processes on a common hardware platform enables faster service delivery and real-time resource optimization. Ultimately, the goal for NFV is to enable flexibility in the deployment and migration of VNFs while at the same time achieving high performance throughput with minimal server capacity resources. To achieve this, the underlying NFVi needs to be designed from the ground up to support automation.

Industry efforts to build automated NFVi are already underway, but today’s solutions tolerate too many trade-offs between flexibility, performance and cost-efficiency. The following sections explore the steps network operators can take on the path to fully automating their NFVi without sacrificing service quality or breaking the NFV business case.

This is the challenge that need to be addressed now to enable automation and support service agility
Step 1. Get Data Delivery to Work

Not long after the publication of the first NFV white paper by 13 of the world’s largest network operators in late 2012, the Intel Open Network Platform (ONP) emerged as an important conceptual framework for making the transition from traditional physical appliance-based networks to software-based virtualized networks. The ONP server reference architecture provides hardware and software components that are optimized for NFV and SDN deployments. It has a common hardware platform that is based on standard Intel x86 servers and standard NICs, as well as a hypervisor and virtual switch that abstract the hardware from the software. And true to the ethos of ETSI’s NFV efforts, the ONP framework is built on open standards and open source software, including the OpenStack cloud operating system, OpenDaylight SDN controller and Open vSwitch (OVS) virtual switch.

With the inclusion of OVS and hypervisor, the ONP framework represents the first step in building an automated NFVi. OVS is a virtualized software implementation of a traditional network switch. It provides the connectivity in virtualized environments and can be deployed across multiple servers. As VNFs are distributed on different servers, the hypervisor and OVS switch traffic among them wherever they are implemented. This ability to instantiate and move VNFs anywhere in the network enables the flexibility and agility in NFV service chain creation.

ONP is a good starting point for automated NFVi, but it does have drawbacks in performance and cost efficiency. Generally, vSwitch performance is a common source of frustration for network operators, and it has been a bottleneck in NFV implementations. While vSwitch performance may not reach exactly the same levels of hardware appliances, it does need to be better than what it is today. OVS throughput performance falls below industry expectations. In addition, efforts to improve OVS performance typically result in very high server Central Processing Unit (CPU) core consumption, which makes it expensive to run. The more cores that OVS consumes, the less there will be available for other data processing workloads including hosted virtual functions. Operators will end up paying for additional capacity just to have the same performance and functionality as they do today, which defeats the cost-efficiency aims of NFV.
Step 2. Get Data Delivery to Work with Performance

To overcome the performance shortcomings of OVS, the industry looked to an alternative approach with Single Root Input/Output Virtualization (SR-IOV). It’s a familiar network interface in enterprise networking, but it is relatively new to telecom networks. SR-IOV does improve throughput performance, but it sacrifices flexibility and adds complexity.

SR-IOV bypasses the vSwitch and hypervisor and directly interfaces between VNFs and NICs that support SR-IOV. In other words, physical NICs are linked directly to specific virtual functions on the same server, thereby improving throughput performance. But by tying the NIC hardware to the VNF software in this way, SR-IOV effectively removes the abstraction layer that separated the hardware from software in the NFVi, which makes moving VNFs very difficult. The effect can be described as taking the virtualization out of NFV. Also, since there is no standard way to implement the SR-IOV mechanism, vendor-specific versions can add further complexity when it comes to integrating with other elements of the NFVi as well as legacy telco systems.

VNF mobility is important not only because it enables flexibility and service agility, but also because it is essential to the NFV business case. With the ability to easily move VNFs among servers within the data center or to different data center locations as NFV-based services mature, operators can consolidate virtual functions onto fewer servers and optimize server resource utilization. In data centers, the biggest costs are power and cooling. If operators can minimize the number of servers needed for NFV by optimizing where the VNFs run, then they can reduce data center operating costs.

The upshot is that SR-IOV resolves the performance issue, but it undermines VNF mobility and flexibility. Nonetheless, it is an important step on the path to NFVi automation.

Step 3. Get Data Delivery to Work with Performance, Flexibility and Acceptable Cost

The next step to enabling automation on a common hardware platform is OVS Acceleration, which improves the throughput performance of the virtual switch without the need for hypervisor bypass solutions (e.g., SR-IOV), thereby ensuring VNF mobility as well as cost efficiency for network
operators. The technique is similar to Intel’s ONP in that it uses OVS and relies on the data plane development kit (DPDK) as the interface to VNFs. The unique piece in the OVS Acceleration solution is a Field Programmable Gate Array (FPGA)-based NIC that is designed specifically for the requirements of NFV. The solution offloads some of the functionality of OVS onto the NFV NIC so that the virtual switch uses fewer CPU cores and clocks higher overall throughput.

An NFV NIC operates like any standard NIC, providing input and output for traffic coming in and out of standard servers. The way it boosts performance is by creating Contiguous Packet Batches that allow thousands of Ethernet frames and IP packets to be transferred at once. An NFV NIC with OVS Acceleration reduces the number of actions that the OVS has to perform and increases overall throughput. Most of the OVS functionality remains running in software, but having a smaller workload means that the OVS will use fewer CPU cores.

By not tying the NIC to specific VNFs (as the SR-IOV mechanism does), OVS Acceleration ensures that network operators have the VNF mobility they need for agile service chain creation while also increasing throughput performance. Also, by offloading some of the OVS workload onto the NFV NIC, OVS Acceleration reduces the number of CPU cores that OVS consumes. These freed-up resources enable operators to increase the density of VNFs per server to run more revenue-generating service functions per server as well as use less server capacity overall, which will lower network operating costs.

A recent case study illustrates the potential cost savings. In a data center with 10,000 servers, it was found that OVS Acceleration with DPDK on an NFV NIC would use eight times fewer CPU cores per server than OVS with DPDK on a standard Intel NIC. OVS Acceleration can provide full 40 Gbps throughput using just one CPU core. This corresponds to a saving of seven CPU cores per server, which translates into 3,890 fewer 18-core CPU chips and 1,945 fewer dual-socket servers. The resulting total capex and opex savings for network operators related to this reduction corresponds to $8 million over four years. In terms of performance, OVS can be accelerated by up to seven times compared to standard NIC solutions that support OVS and DPDK.
Step 4. Extend Performance Improvements to Other Data Processing

OVS Acceleration resolves a major performance problem facing operators today while also meeting operator requirements for flexibility and cost-efficiency. But the traffic demands on communications networks are unrelenting, and CSPs need to be equipped to cope with the cost of increasing data loads in the long term as well as shorter term performance improvements. As operating costs typically increase in line with data traffic load, CSPs need new ways of lowering the cost-per-bit. This market reality leads to the next step in NFVi automation, which is extending the performance improvements gained through OVS Acceleration to other common data processing functions.

With an FPGA-based NFV NIC, the same common hardware platform used for OVS Acceleration can be used to accelerate heavy data processing tasks, such as encryption and compression. FPGA-based hardware can be programmed and upgraded remotely, which creates a versatile platform that can serve other functions in an NFV environment. The flexibility of FPGA technology also allows third-party IP to be dropped in to the NIC platform to perform a variety of functions. This hardware acceleration approach is essential for building automated NFVi especially where software-based solutions are too costly and resource-intensive.

Data compression and encryption are particularly heavy data processing functions that consume a disproportionate amount of CPU cores. But CSPs are having to process increasing amounts of both traffic types. Encrypted traffic is on the rise worldwide. Network policy control vendor Sandvine estimates that 70% of Internet traffic is encrypted across Europe, Latin America and North America.

In the case of data compression, higher data traffic loads and demands for faster data service delivery are pressuring CSPs to store more data in the data center and closer to where customers are located. To mitigate storage costs, CSPs are compressing the data. But processing compressed data in a virtualized environment is resource intensive and consumes too many CPU cores, which ultimately increases data center operating costs.

CSPs can overcome the high cost of processing compressed and encrypted traffic through hardware acceleration on an NFV NIC. For example, hardware acceleration on an NFV NIC uses 40 times less CPU cores compared to software acceleration on server CPUs. In a data center with 10,000 servers, assuming 10% of servers need hardware acceleration, the total capex and opex saving corresponds to $4 million over four years.

Step 4: Hardware acceleration enables continuous cost improvement
Step 5. Provide insight for continuous optimization

Once the NFVi is running more cost-efficiently through hardware-accelerated data processing, the next step for the full benefits of automation is to implement effective network monitoring to enable continuous optimization as well as security solutions. In traditional physical networks, CSPs could monitor traffic by adding a passive Test Access Point (TAP) to the connection that needed to be monitored between two network nodes. Based on a mechanical relay or optical splitter, the TAP ensures that a copy of all traffic is sent to network appliances dedicated to network monitoring or security. Alternatively, routers and switches provide a Switch Port Analyser (SPAN) port, which makes a copy of the traffic activity of one or more switch ports so that it can be analyzed.

But in virtualized networks, these techniques are difficult to replicate. Virtual TAPs are challenged by VNF mobility whereby virtual functions can be moved around and instantiated on different virtual machines. In addition, virtual TAPs or SPAN ports require the duplication of all traffic in the virtual switch so that it can be analyzed by another virtual function. As virtual switching today is performed in software, this effectively means that double the amount of server CPU cores are required when a virtual switch needs to provide TAP or SPAN port functionality.

A more cost-efficient way to monitor virtualized networks is to take advantage of the fact that the OVS Acceleration solution implemented on the NFV NIC already sees all the traffic in the virtual switch and can replicate this traffic efficiently without using any server CPU cores. This allows a copy of all traffic to be delivered to another location, whether that is another virtual appliance or function on the same server or on another server.

By offloading the traffic monitoring functionality onto a common hardware platform, CSPs will not only reduce operating costs through minimized CPU core use but they will also have constant insight into how the network is performing that will enable further optimization of the NFVi as well as the services and applications they are delivering to customers.
Conclusion

Despite the current sense of disillusionment, the telecommunications industry has made great strides in the development of NFV. Specifically, industry efforts to overcome the complexities of MANO will help to enable service agility in management and service creation functions. As this major hurdle is cleared, the time is right to move the spotlight onto the NFVi and reconsider whether it can match the level of service agility that will be enabled by the MANO layer.

CSPs need more flexibility, better performance and cost savings from their NFV deployments, and the way to achieve these goals is by enabling automation in the NFVi. By adding smarter functionality to the common hardware platform, CSPs can significantly improve the performance of the NFVi while also ensuring flexibility and cost efficiency even as data traffic continues to increase and workloads surge. CSPs will be prepared to cope with future traffic demands that require intensive data processing. Building an automated NFVi is the surest way for CSPs to realize the promise of NFV.
Napatech is the world leader in smarter data delivery solutions for network management and security applications. As data volume and complexity grow, organizations must monitor, compile and analyze all the information flowing through their networks.

Our products use patented technology to capture and process data at high speed and high volume with guaranteed performance, enabling real-time visibility. We deliver data faster, more efficiently and on demand for the most advanced enterprise, cloud and government networks.

Now and in the future, we enable our customers’ applications to be smarter than the networks they need to manage and protect.

Produced by the mobile industry for the mobile industry, Mobile World Live is the leading multimedia resource that keeps mobile professionals on top of the news and issues shaping the market. It offers daily breaking news from around the globe. Exclusive video interviews with business leaders and event reports provide comprehensive insight into the latest developments and key issues. All enhanced by incisive analysis from our team of expert commentators. Our responsive website design ensures the best reading experience on any device so readers can keep up-to-date wherever they are.

We also publish five regular eNewsletters to keep the mobile industry up-to-speed: The Mobile World Live Daily, plus weekly newsletters on Mobile Apps, Asia, Mobile Devices and Mobile Money.

What’s more, Mobile World Live produces webinars, the Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and exclusive home to all GSMA event keynote presentations.

Find out more www.mobileworldlive.com

Disclaimer: The views and opinions expressed in this whitepaper are those of the authors and do not necessarily reflect the official policy or position of the GSMA or its subsidiaries.