NETWORK FUNCTIONS **VIRTUALIZATION**

Value Creation with Innovative Network Interface Devices (NIDs)

ADVA™ Optical Networking

Growing Business While Adopting Network Function Virtualization

A fast and cost-effective delivery of VPN services to large enterprises with multiple branch offices poses formidable challenges to network operators. The need to support a multitude of equipment configurations, hardware vendors, and appliances leads to an inflexible box-stacking model at the customer premise. Extensive site surveys, site visits and truck rolls substantially increase the solution cost and time, and requires highly skilled operator staff on-site for installation, configuration and trouble-shooting. In a resource-constrained environment, a transformation from a box moving model to an enterprise IT model offers the prospects to do more with less and is one of the main drivers behind Network Functions Virtualization (NFV).

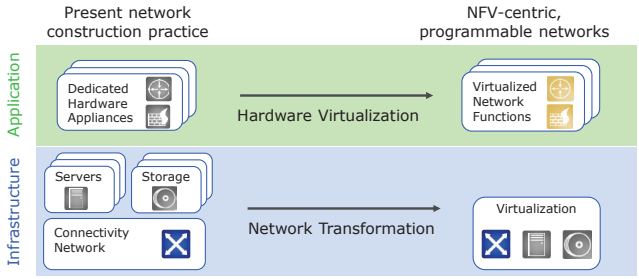
Hardware virtualization has become a recurrent theme in many industries. The same way typewriters became dispensable with the advent of word processing software and personal computers, virtualization strives to replace dedicated hardware appliances with software and general purpose hardware in the networking world. The emergence of matching hardware – reasonably priced printers – was the catalyst for the revolution in document creation and printing. Likewise, tailored hardware is also required in the networking world to fully leverage the virtualization benefits.

Software innovation inspires imagination of service providers and enterprises who envision a significantly simplified ICT infrastructure. Today, a huge variety of hardware built for specific purposes, such as routers, firewalls, load balancers or intrusion detection systems, create a significant effort in integration, operation and maintenance of a communication infrastructure. Emerging NFV technology promises significant simplification as present hardware appliances become replaced by software running on standard servers, frequently creating additional requirements on the underlying physical hardware as outlined with the example above.

NFV and SDN – Two Complementary Technologies

ICT infrastructure consists of many network functions for very different purposes, for example, analyzing network traffic, transcoding data, securing the network or processing user data. As such, functions might not be required concurrently, cost savings can be achieved by pooling and sharing compute and storage resources among network functions. Such gain in operational efficiency is not possible when using dedicated hardware appliances.

The connectivity network has to be able to chain those software appliances in the same way as hardware had been connected physically. The connectivity network needs to respond to newly instantiated appliances by aligning the network topology in an automated way. Manual provisioning is not an option. Software-Defined Networking (SDN) is an emerging technology for programmable flow control using open network control protocols such as OpenFlow and NETCONF/YANG, and effectively complements emerging NFV technology.



Creating Value from Virtualization by Seamless Network Transformation

Operational simplification and resource sharing will result in significant cost savings. Expectations range from 25% to 40% depending on feature set of software appliance, ability to share resources, level of automation and labor cost, among others. Virtualized Network Functions (VNFs) can be placed either within the network/cloud or at the edge.

Edge virtualization replaces customer premise equipment by software appliances running on a customer-premises located server. As VNFs run at the same location as the previously applied hardware, the impact on the network and operational processes is minimized. Cost advantages result from co-hosting several VNFs on a common server and from integrating this server with the Network Interface Device (NID).

Network-hosted virtualization enables sharing centrally pooled resources with many customers. As data leaves the enterprise's security perimeter and is processed at fewer sites deep in the network, traffic volume will grow and data will need to be secured in transit. At the same time, the network topology becomes simpler as edge sites will need to connect to a low number of cloud data center sites. Resilient, secured point-to-point connections will become the preferred connectivity service.

Network and Service Innovation by Network Functions Virtualization

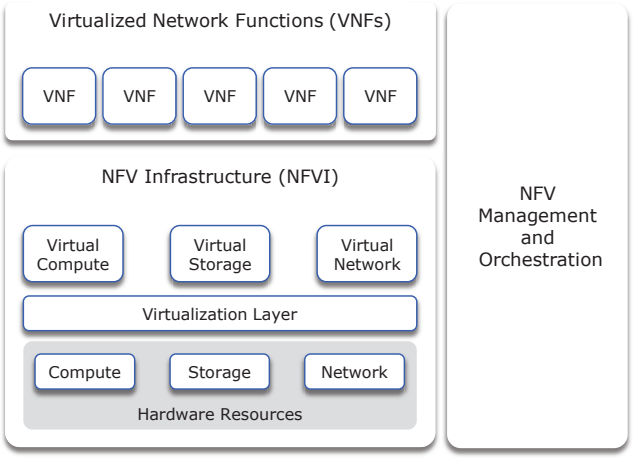
- Replacement of dedicated hardware appliances with software functions
- Rapid service creation without moving hardware and people
- Flexible allocation of VNFs in centralized or distributed fashion
- Open interfaces enabling a functional separation, thus replacing monolithic network designs
- Programmable data plane for automated resource allocation and service chaining

Innovative Network Interface Devices as NFV Foundation

The evolution to a software-centric network requires a network transformation whose pace is more determined by operational and organizational changes rather than technological developments. An approach allowing a seamless, stepwise introduction of NFV is essential to benefit from efficiency gains in the short term, while implementing the transformation steps necessary for the longer term. Open interfaces and open software are key as they prevent vendor lock-in and cause least disruption when moving from the present to a future mode of operation.

NFV Architecture Framework

The NFV architecture has been defined by the ETSI NFV ISG and comprises three principal elements: the NFV Infrastructure (NFVI), VNFs and the NFV Management and Orchestration (MANO) functions. The NFVI consists of physical networking, compute and storage resources that can be geographically distributed and exposed as a common virtualized infrastructure. VNFs are software implementations of network functions, such as routers, firewalls and intrusion detection systems. The MANO functions provide the necessary tools for operating the virtualized infrastructure, managing the life cycle of the VNFs and orchestrating virtual infrastructure and network functions to compose value-added end-to-end network services.



The NFV architecture provides a high-level framework and defines reference points to facilitate interoperability between different constituent components. Proof-of-concepts of practical use cases are utilized to design, develop and test more detailed interoperability requirements, information models and interface definitions following a DevOps approach.

Open Software and Interfaces are Key

Open interfaces and clearly defined reference points are key to accelerate the market adoption of NFV. This approach allows multiple parties to independently develop the building blocks of the NFV architecture and enables service providers and their customers to pick the solutions and implementations best suited to their application and organizational needs. At the same time, the use of established standards, protocols and interface technologies, e.g. from IETF, is highly desirable to shorten time to market and place the NFV framework on a broad basis. For the software implementation, an open framework based on open-source software is the most flexible approach and avoids a lock-in with any particular vendor. Components such as OpenStack and OpenDaylight form a solid foundation for an NFV platform and will be complemented by missing components in reference implementation projects such as OPNFV.

Optimized Demarcation Technology for NFV-Centric Networks

For enterprise connectivity, the ETSI NFV ISG has identified two use cases of particular interest to service providers and their enterprise customers:

- Virtualization of Enterprise Customer Premise Equipment (vCPE)
- Virtualization of Provider Edge functions (vPE)

In both cases, network appliances operating on layer 3 and above are converted into software functions that are hosted on general purpose servers. To guarantee a predictable and stable performance of network services wherever the constituting network functions are located, proven NIDs are essential.

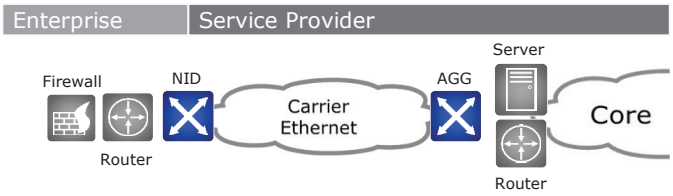
They provide hardware-assisted demarcation, rich Operations, Administration and Maintenance (OAM), timing and security functions and seamlessly integrate into NFV-centric networks. By leveraging open interface standards, they allow customers to pursue a best-of-breed approach without vendor lock-in neither on the hardware nor on the software side. Optional integrated server and storage capabilities allow the placement of VNFs on an as-needed-basis, paired with the capability to service chain these functions inside or across locations. Remote access, management and supervision functions extend to the integrated server and storage functions as well, providing a robust and secure execution environment for demanding VNFs.

Enterprise CPE Virtualization

For cost, speed and flexibility reasons, service providers and enterprises strive towards software-controlled, service-centric networks based on virtualized network-, storage- and server-resources. Starting with a hardware-centric network makes this an ambitious target. The good news is that there are various options for a phased approach realizing cost savings and simplification even at an early stage of technology introduction. Different initial steps are explained below, the benefits and requirements are outlined with a focus on the connectivity network and NID terminating it. The examples are based on the vCPE use case.

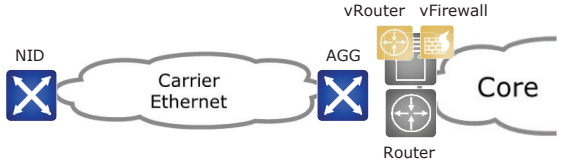
Reference Architecture and Status Quo

Enterprises frequently use layer 2 or layer 3 VPN services provided by a communication service provider to connect their sites or branch offices. The provider operates the network and also manages the customers' edge (CE) router on their premises. The enterprise secures its IT network with firewalls, intrusion detection systems and improves utilization of the VPN by WAN optimization solutions. Typically a NID is deployed to terminate the Ethernet connection and to monitor the L2 link through a Carrier Ethernet network.



Network-Hosted Virtualization

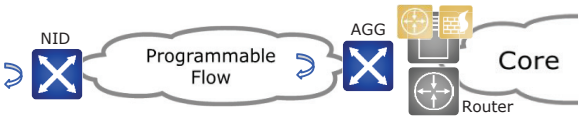
NIDs have been deployed for service demarcation in Carrier Ethernet services for many years and provide a full set of capabilities for turn-up test, in service monitoring, upstream policy management and fault resolution. Centralizing the CE router functions removes considerable complexity from the customer premises, reducing the need for site visits to install, configure, fix and patch the router. However, the service provider still needs visibility of the end point of their service responsibility and will use demarcation technology featuring advanced L3 OAM functionality.



As network functions move from customer premises into the cloud, a need for securing data transported over a public network arises. NIDs with advanced L2 encryption capability will efficiently protect the traffic but will also secure the connectivity network from malicious attacks.

Network-Hosted Virtualization and Programmability

Once CPE routers are virtualized and run on a central server, inter-subnet traffic for the local site needs to be routed through this central server. This creates some inefficiency in bandwidth utilization in the metro network. The NID provides an ideal service provider owned and managed point of policy control, where this traffic can be locally connected without needing to be backhauled to the cloud. SDN and programmability can be a very effective tool to populate the forwarding tables in L2 equipment from a central instance, which has knowledge of IP reachability in the network.



Customer-Premise Hosted NFV

Some service providers and enterprises might prefer to continue with existing operational processes when introducing NFV. They may prefer to operate VNFs at the location of the previously applied dedicated hardware function. As the location of the function is not changed, there is minimum impact to operational processes and the connecting network.

Replacing a router with a virtual router appliance and combining with several chained applications concurrently makes a very compelling business case. NIDs with integrated server and storage resources provide the most cost-efficient solution.

All of the above outlined NFV use cases have cost advantages over present network design and construction practice. Different customers and industries have quite different feature, bandwidth, growth and security requirements. Service providers will use a combination of those use cases as this allows optimizing for specific customer segments.

Open interfaces and open-source software provide a smooth path for introducing programmability, NFV portability as well as simple integration into management and orchestration systems. In addition, openness will break-up previous monolithic network designs.

Towards NFV-Centric Networks

- Starting the journey with proven demarcation technology
- NFV enablement with NIDs featuring L3 OAM and security features
- Integrated compute and storage resources extend NFV functionality
- Openness creating unprecedented speed of innovation
- Hardware assistance for security, synchronization and OAM, among others

Business and Application Scenarios

In the lifespan of a long-term business service solution, the range of hardware types, functions and variants naturally increases. Migrating network appliances into virtual machines minimizes such diversity and associated complexity. Customers migrating onto a vCPE model for their L2/L3 VPN service will see immediate changes in the structure of their solution. A complex and often cumbersome arrangement of routers, firewalls and other devices located in the network closet, is replaced with a single device that works with SDN and NFV technology to consolidate multiple appliances.

Communication, Cloud and Content Service Providers are NFV Innovators

Operators embracing NFV, SDN and open interfaces, can offer extremely fast time to install and turn up new services, achieving a competitive edge through service agility. Complimenting NFV with SDN and programmable hardware can optimize data forwarding and underlying connectivity, providing high performance and assured communications between virtual appliances.

The ability to deploy services as software downloads to the CPE enables service providers to roll out new services across a customer's entire organization without the need to dispatch engineers and install new equipment. Service providers can offer "try before you buy" promotions and short term leases for special events. The model can be extended to allow field sales executives to take an order at the customer site and have it turned up automatically via orchestration.

NFV and SDN together can help service providers to transition from legacy solutions to new VNF-based business service models with simplified connectivity networks and virtual appliances hosted at the customer premises or in the service provider's network.

Cloud service providers offering network storage and compute facilities in their datacenters can explore new business models where they supply end customers with CPE-based VNF hosts and improve the end-user quality of service and quality of experience by mobilizing the location of virtual functions on-demand and installing VNFs in an elastic fashion to the customer premise.

System Integrators as NFV Incubators

System integrators with experience of integrating hardware and software solutions in the carrier network and data center space are ideally positioned to create new offerings, such as NFV platform-as-a-service and managed services.

System integrators can benefit from the emergence of pre-customized solutions that are adaptable to specific customer needs with greater speed by virtue of the programmability and scalability associated with the deployment of functions as software entities on NFV-based infrastructure and platforms.

They can use the open-source software approach of NFV to create integrated solutions that can be offered to multiple customers with synergistic requirements. NFV however also brings flexibility to tune the solution for specific customers with more agility than vendor specific solutions would allow. Single-vendor solutions inevitably involve compromise while open architectures allow the best solutions to be selected and combined.

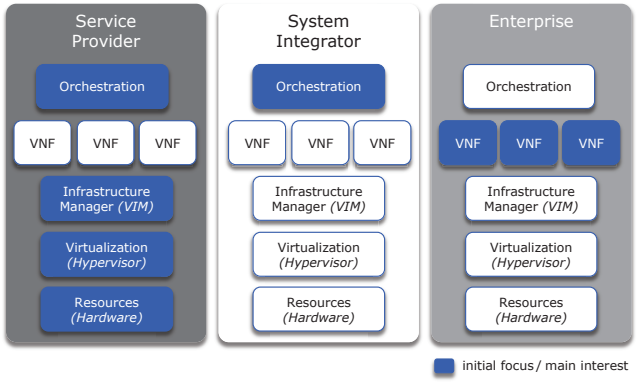
Enterprises Benefit from NFV

An immediate benefit to enterprises is the simplification of IT infrastructure through the adoption of a flexible and programmable L2/L3 forwarding device complimented by virtualization of appliances, such as routers, deep packet inspection, firewall, WAN optimization, intrusion prevention systems and network performance monitoring, with models supporting VNFs hosted locally or in a private cloud.

Many enterprises are considering NFV within their own and often distributed network infrastructure to unburden network operations and focus on immediate business activities.

Enterprises can rapidly test and turn up new services using NFV and create architectural blueprints in software containers that adoption in branch offices.

As NFV matures, appliances relevant to specific industrial verticals will emerge in VNFs targeted, for example, at mobility of the end-user and telemetry collection in the Internet of Things.



A Variety of Cost Saving and Business Growth Opportunities

- Highly flexible software-driven and open solutions replace monolithic network designs
- Significant cost savings with network integration, installation and operation
- Fast service introduction without onsite visits
- Seamless growth from Ethernet services to high-value software appliances
- Attractive use cases for service providers, enterprises and system integrators

For More Information

ADVA Optical Networking SE
Campus Martinsried
Fraunhoferstrasse 9a
82152 Martinsried/Munich
Germany

ADVA Optical Networking North America, Inc.
5755 Peachtree Industrial Blvd.
Norcross, Georgia 30092
USA

ADVA Optical Networking Singapore Pte. Ltd.
25 International Business Park
#05–106 German Centre
Singapore 609916

info@advaoptical.com
www.advaoptical.com

About ADVA Optical Networking

At ADVA Optical Networking we're creating new opportunities for tomorrow's networks, a new vision for a connected world. Our intelligent telecommunications hardware, software and services have been deployed by several hundred service providers and thousands of enterprises. Over the past twenty years, our innovative connectivity solutions have helped to drive our customers' networks forward, helped to drive their businesses to new levels of success. We forge close working relationships with all our customers. As your trusted partner we ensure that we're always ready to exceed your networking expectations. For more information on our products and our team, please visit us at: www.advaoptical.com.

Optical+Ethernet Innovation • Speed for Customers • Trusted Partner

ADVA™ Optical Networking

Version 03/2015