Prodapt CONSULTING powering global telecom

WHITE PAPER

SDN & NFV

Introduction

Two of the biggest hypes which are currently causing a storm in the telecom industry are SDN and NFV. SDN is an acronym for Software Defined Networking and NFV stands for Network Functions Virtualisation. Both of these topics have their background in IT, already proved their value in datacentres and now promise to be the holy grail for the telecom industry allowing service providers & operators to overcome their current challenges, such as the intense competition with Over The Top (OTT) providers. Just like any other innovation promises for that matter…

Two of the biggest hypes which are currently causing a storm in the telecom industry are SDN and NFV.

This white paper will take a closer look at these new developments, how applicable they are for the telecom sector, whether to believe the hype and how to position SDN and NFV in a service provider and operator's strategy realistically. The paper will first give some background on cloud computing and networking to better position SDN and NFV in its context, then it will explain SDN and NFV, look at their benefits and maturity in terms of standardisation and vendor solution development & availability. By zooming in on a couple of present-day challenges faced by a telecom operator it shows whether implementing SDN and NFV will (help) overcome these challenges. Based on this assessment the white paper then discusses relevance and position of SDN and NFV on a service provider's roadmap and in its business strategy. The final part this white paper introduces a few ways how Prodapt Consulting can help service providers and operators to achieve this.

Cloud Concepts

Developments such as cloud computing and cloud networking led to SDN & NFV

Before this white paper will zoom in on SDN & NFV this chapter will give some insight in developments that led to SDN & NFV such as cloud computing and cloud networking.

Cloud Computing

Application Service Providers, Grid Computing, Virtualisation and Service Oriented Architectures are examples of developments that led to new ways of people using computers, gather information and integrate IT systems. Cloud computing can be seen as a result of this.

NIST defines Cloud Computing as follows. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Important aspects of cloud computing to remember are:

- Abstracted pool/grid of resources: The amount and configuration of the resources that provide the cloud computing service (e.g. storage, computing power, etc…) are abstracted for the user.
- Elasticity: The pool of resources is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible.
- Service Orientation: The capabilities offered by the pool of resources are exposed externally by means of a service interface (API, web services, etc.).
- Virtualisation: Actual resources, capabilities, etc. (e.g. hardware platform, storage device, etc.) are recreated by software in a virtual version.

Traditionally cloud computing services have been offered in three types of service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Cloud Networking

Cloud computing has focused on offering computing and storage resources in a service oriented model. Until recently networks weren’t part of this approach. However networks are just as well a pool of resources that can be abstracted and organised as a service that can adapt itself to support variations in resources (bandwidth) demand. Especially when the networks are the underlying infrastructure that give access to cloud computing services. So with the development of more advanced networking technologies it is a natural progression that, similar to computing and storage, networking resources will be offered in a service oriented model. Additionally network functions and services including connectivity, security, management and control, can be virtualised and pushed inside the cloud. This is called Network as a Service (NaaS) or cloud networking.

SDN

Software Defined Networking (SDN) is one of the technologies that give form to some of these cloud networking aspects. This chapter will explain SDN and some of its benefits and weaknesses. It will inform on SDN standardisation and vendor solutions.

SDN is an approach to networking in which network control is decoupled from the data forwarding function

SDN Overview

SDN is an approach to networking in which network control is decoupled from the data forwarding function, see *Fout! Verwijzingsbron niet gevonden.*. This network control is centralised in the SDN controller. The controller approaches the underlying network elements as an abstracted pool of resources, contains an end-to-end view of that network and makes this directly programmable. Characteristics of the network like for example the connectivity, the flow of traffic through it and the inspection and modification of traffic in the network become programmable. This programmability is exposed as services to SDN applications over the northbound interface. The SDN controller translates the instructions received from the SDN applications into individual configurations for the underlying network elements over the southbound interface via the standardised OpenFlow protocol.

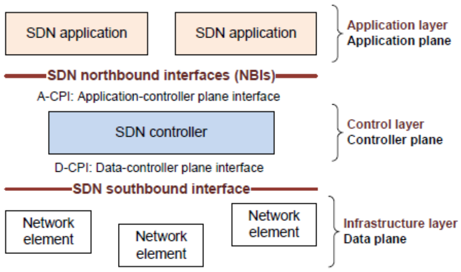


Figure 1. High Leve SDN Architecture - Source: ONF

So SDN mainly covers the cloud computing aspects “abstracted pool/grid of resources” and “elasticity”. More recently more attention is paid to “service orientation” of north bound interfaces as well.

Listed below are some example SDN use cases:

- Data centres: Business applications that run on Virtual Machines (VM) in the datacentre have to be scalable. When these scalability needs increase and new VMs must be spun up due to hardware cluster limits, these new VMs may need to be set up in different physical LANs. Existing VMs may also need to be moved to different LANs. The SDN controller automatically manages these workload changes towards the physical network elements, so the business applications can seamlessly continue their work.

- DDoS Mitigation Tools: DDoS mitigation solutions can use traffic statistics provided by OpenFlow switches to detect traffic anomalies, engage the traffic redirection capabilities of an SDN controller to divert suspicious traffic to a DDoS detection appliance, and finally install DDoS-specific flow entries into ingress switches to block the offending traffic.

SDN Benefits

SDN comes advertised with the following benefits:

- Centralized control of multi-vendor environments: SDN control software can control any OpenFlow-enabled network device from any vendor, including switches, routers, and virtual switches.
- Reduced complexity through automation: OpenFlow-based SDN offers a flexible network automation and management framework, which makes it possible to develop tools that automate many management tasks.
- Higher rate of innovation: SDN adoption accelerates business innovation by allowing IT network operators to literally program—and reprogram—the network in real time to meet specific business needs and user requirements as they arise.
- Increased network reliability and security: SDN makes it possible for IT to define high-level configuration and policy statements, which are then translated down to the infrastructure via OpenFlow.

While all of these SDN benefits may be true to a certain extent, many of them are also used as arguments to opt for other (competing) concepts & technologies. Chapter **Fout! Verwijzingsbron niet gevonden.** will focus on the telecommunications industry and assess which of these benefits have any real value.

SDN Weaknesses

The current state of SDN also comes with a couple of weaknesses:

- Immature: SDN is a very young technology that has only merely left the academic and research world. It has no proven track record yet outside of the IT datacentre.
- Centralised architecture: While the centralized SDN controller is one of the most important strengths of SDN it also introduces some risks. If the controller or OpenFlow links fails the network isn't configurable anymore and will not adapt to changing circumstances, whereas traditional networks with the distributed control plane as part of the network will continue to function. In worst case scenario, with SDN, the whole network may come to a halt caused by severe failure or deliberate sabotage.
- Security: Due to its immaturity and centralised architecture, SDN introduces many new potential security risks. E.g. how secure is the OpenFlow protocol; how secure is the SDN controller against unauthorized use; while SDN offers possibilities to mitigate traditional DDoS attacks, the SDN stack can be the subject of a DDoS attack itself.
- Internal view: SDN originated purely as an approach to optimize privately owned networks. Exposing the (abstracted) SDN capabilities externally is only subject of recent developments. How to do interworking between

multiple SDN domains or control multiple network domains with one umbrella SDN controller are topics that have hardly been covered yet.

- Management challenges: a) When network configurations can change in seconds, it is imperative that management systems stay in sync. b) A management view on the changes made programmatically is also required. c) Impact to existing services of requested programmatic changes. What governs the multiple application requests for network resources to be provisioned or changed programmatically? How does the network know if the requested changes are a good idea? d) Reachability of the network infrastructure, does OpenFlow require a separate network like ITU-T TMN defined the Data Communication Network (DCN) for management traffic?

SDN is developed and standardised, in an open, collaborative way by the Open Networking Foundation (ONF).

> NFV allows network operators to deploy network functions as virtualized software instances instead of dedicated hardware appliances.

SDN Standardisation

SDN is developed and standardised, in an open, collaborative way by the Open Networking Foundation (ONF). The following topics are examples on which ONF is working on extending existing and defining new SDN standards:

- Architecture and Framework
- Configuration and Management
- Extensibility
- Forwarding Abstraction
- Northbound Interfaces
- Optical Transport
- Wireless & Mobile

The most mature standard is the OpenFlow protocol. Recently (June 2014) also a first version of the SDN architecture has been published.

SDN Vendors

The past 2 to 3 years has seen the announcement of many SDN products [SDNPr]. These can roughly be divided into four categories:

- Open Source software: There is a big open source SDN community. The best known initiative is Open Daylight, which is a suite of components, such as SDN switches, SDN controller, NFV applications, etc. see section **Fout! Verwijzingsbron niet gevonden.**. A comprehensive list of open source tools can be found at [SDNOSS].
- Start-ups: Many new companies came into existence offering innovative SDN capabilities.
- Traditional telecom vendors, such as Alcatel Lucent, Ciena, Cisco, Huawei, Juniper, etc. presented their SDN capable equipment to market later then the small start-ups. In many cases the SDN product line offered by these vendors is the result of the acquisition of one or more of these SDN start-ups.
- Traditional IT vendors, such as HP, IBM, Oracle, Google and even Facebook (Wedge switch & FBOSS control software) are also working on SDN offerings. Due to their IT background their offerings focus more on the SDN controller and application side rather than the SDN capable network equipment.

A nice overview of the main vendors can be find here [SDNStrat].

NFV

Network Functions Virtualisation (NFV) is another technology that applies cloud networking concepts in the telecommunications space. This chapter will

> One of the biggest NFV challenges is the management and orchestration (MANO).

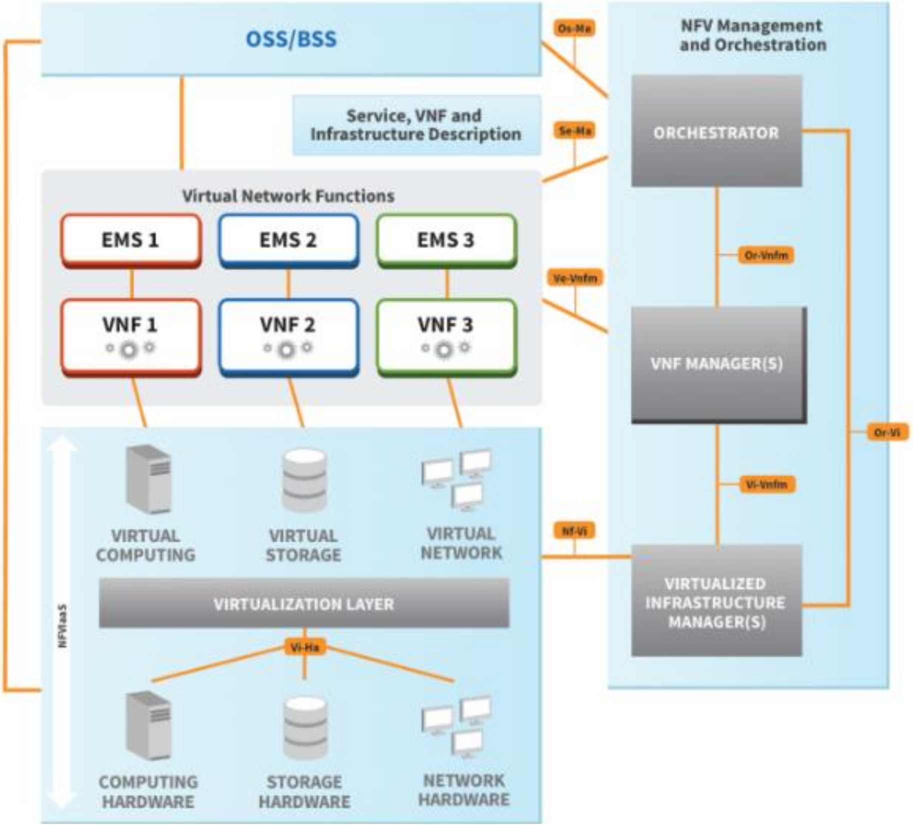


Figure 2. High Level NFV Architecture - Source: Cyan

introduce NFV, its benefits and weaknesses. It will take a short look at NFV standardisation and vendor solutions.

NFV Overview

Where SDN is a clearly defined concept, Network Functions Virtualisation rather is an umbrella term. NFV allows network operators to deploy network functions as virtualized software instances instead of dedicated hardware appliances. These software-based network functions can run on industry-standard high-volume servers and storage platforms, located in datacentres and in end-user locations. NFV enables creation of logically isolated network partitions over shared physical network infrastructures so that multiple heterogeneous virtual networks can simultaneously coexist over the shared infrastructures; it allows the aggregation of multiple resources and makes the aggregated resources appear as a single resource.

The high level NFV architecture is shown in **Fout! Verwijzingsbron niet gevonden.**. The middle horizontal layer is the layer where the Virtualised Network Functions (VNF) run. They run on NFV Infrastructure (NFVI), which can be virtual and/or physical storage, computing or networking infrastructure. The vertical to the right contains NFV management and orchestration functionality. The VNFs are exposed (in a service oriented way) to e.g. OSS and BSS for them to consume.

One of the biggest NFV challenges is the management and orchestration (MANO). It has to take care of the lifecycle of virtual functions running on top of the NFVI. It manages

when many CPEs are virtualised in the operator (or Enterprise central office) cloud, economies of scale can be gained.

In many cases a combination [of NFV] with an SDN solution can be considered to also abstract the actual connectivity to the customer location.

The NFVI resources, including computing, networking, storage, and virtual machines (VMs) and its creation, size, allocation to and connectivity between VNFs, etc.

An example NFV case is the virtualisation of (Enterprise) CPE (Customer Premises Equipment). In this scenario physical appliances located at the customer's location are replaced by VNFs in the operator NFV infrastructure that contain the same functionality, such as QoS enabled routing, firewall, intrusion detection, etc. A big advantage of this architecture is that when many CPEs are virtualised in the operator (or Enterprise central office) cloud, economies of scale can be gained. Note that in many cases a combination with an SDN solution can be considered to also abstract the actual connectivity to the customer location. An example is shown in **Fout! Verwijzingsbron niet gevonden.**.

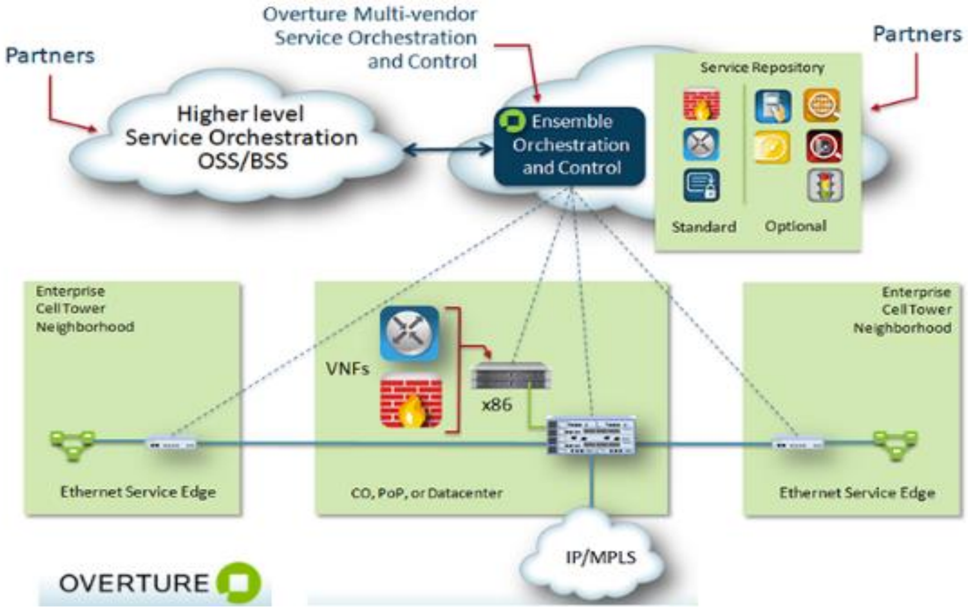

Overture Multi-vendor Service Orchestration and Control
Partners
Higher level Service Orchestration OSS/BSS
Ensemble Orchestration and Control
Partners
Service Repository
Standard
Optional
Enterprise Cell Tower Neighborhood
VNFs
x86
Enterprise Cell Tower Neighborhood
Ethernet Service Edge
CO, PoP, or Datacenter
Ethernet Service Edge
IP/MPLS
OVERTURE

Image 3. Virtualised CPE - Source: Overture

NFV allows network operators to share resources across different customer bases and rapidly scale service up/down

NFV Benefits

A few of NFV benefits as claimed by ETSI:

- Reduced equipment costs and reduced power consumption through consolidating equipment and exploiting the economies of scale of the IT industry.
- Increased speed of Time to Market by minimising the typical network operator cycle of innovation.
- Availability of network appliance multi-version and multi-tenancy, which allows use of a single platform for different applications, users and tenants. This allows network operators to share resources across services and across different customer bases.
- Targeted service introduction based on geography or customer sets is possible. Services can be rapidly scaled up/down as required.

The first two items are typical marketing catchphrases, which are used as arguments for virtually any innovation. Since NFV is a very new concept there aren't many real world implementations yet that can confirm these. The latter two however really are beneficial characteristics only offered by NFV.

NFV Weaknesses

This section will list a few weaknesses of NFV in its current state. Where SDN is developed in an open forum and is benefitting from the same sharing mentality as many other open source projects, NFV is developed more in a traditional telecommunications approach. As section **Fout! Verwijzingsbron niet gevonden.** will further elaborate NFV is specified by ETSI. As with most telecommunication standardisation efforts, NFV specification by ETSI is done in all length and detail and lagging behind on the real world NFV developments. So the following NFV weaknesses can be identified:

- NFV standardisation is still under development
- The NFV standards that are being defined are reference architecture, interface and framework documents. Because of this all products on the market are vendor specific NFV interpretations. While based on existing cloud and virtualisation components (e.g. OpenStack, VM Ware, etc.) integration will still be a big challenge.

Other weaknesses of current NFV state and implementations are:

- Vendors and operators are using NFV to copy and rebuild traditional network equipment and functionality into software. While NFV offers the opportunity to also rethink network architectures and services and potentially come up with whole new networking concepts, even converging control and management/OSS/BSS functionality that can benefit from the powerful IT resources it makes use of.
- When implementing an NFV solution it is still unclear what the overall impact will be on performance and reliability. Will the many VNFs running on a pool of standard server infrastructure perform as well as their optimised hardware counterparts? Will communication between the different VNFs be as quick as a dedicated purpose-dimensioned networks? Will availability and uptime be as high?

NFV is still this young a technology and vendors are still developing their VNF offerings.

NFV Standardisation

The NFV standards being developed by ETSI (European Telecommunications Standards Institute) are called guidelines. Following guidelines have been published:

- NFV Performance & Portability Best Practises
- Use Cases
- Architectural Framework
- Terminology for Main Concepts in NFV
- Virtualisation Requirements
- Proofs of Concepts; Framework

Currently work is ongoing to detail the different areas identified in the architectural framework, for example:

- Compute Domain
- Hypervisor Domain
- Infrastructure Network Domain
- Interfaces and Abstractions
- Management and Orchestration

The TM Forum is also involved in NFV related standardisation. TM Forum claims that virtual services require new virtual operations practices. Hence their ZOOM (Zero-time Orchestration, Operations and Management) initiative aims to support ETSI to detail the MANO area of the NFV architecture and, among others, identifies where TM Forum specifications can help standardise the information presented and interfaces of the MANO reference points.

What is the best concept to apply, SDN or NFV? The answer is , if done properly, a combination of the two.

Next to the standardisation efforts by ETSI and TM Forum, they both work on proof of concepts in the form of ETSI open demonstrations of NFV concepts in Proof of Concepts and TM Forum Catalyst projects. Some examples:

- Demonstration E2E orchestration of virtualized LTE core-network functions and SDN-based dynamic service chaining of VNFs
- VNF Router Performance with DDoS Functionality
- Multi-Cloud SDN-NFV Service Orchestration

NFV Vendors

NFV product availability is a different story than SDN. Next to the OpenDaylight initiative (see section 5.1) there aren't many other open source projects. CloudNFV is one of the few examples but hasn't come up with much more than slideware.

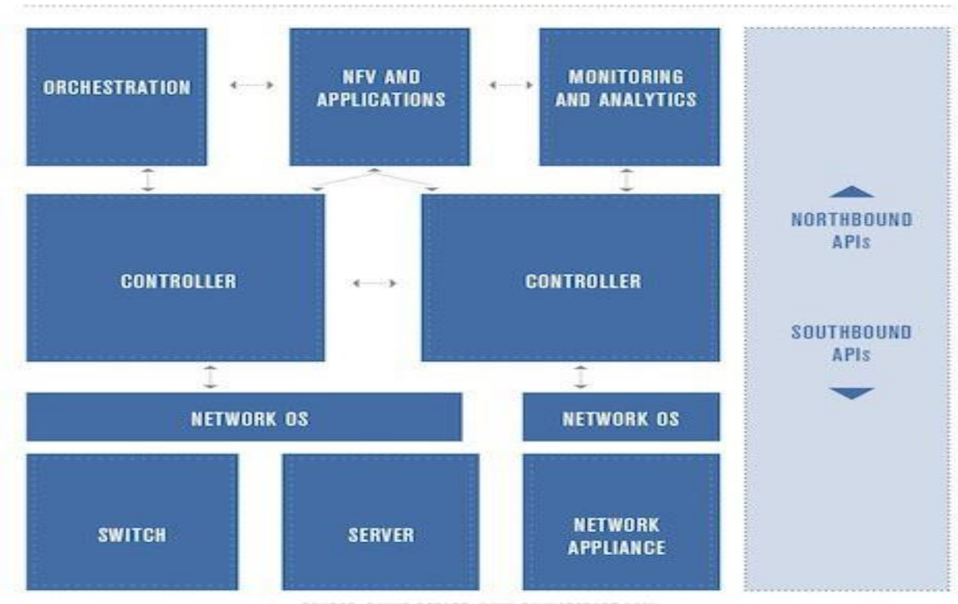
Many (traditional) vendors claim to offer NFV (MANO) platforms, some examples:

- Alcatel – Lucent CloudBand
- Cyan Planet Orchestrate
- HP NFV Director
- Huawei NetMatrix

There are some vendors, e.g. Brocade, Calsoft & Centec, offering virtualised switches, Firewalls, CPE solutions etc. But in general the availability of individual VNFs (Virtual Network Functions) that can be deployed in an NFV environment is limited. Whether this is because standard network functionality that is offered as software (e.g. an HSS, PCRF, etc.) can also be deployed in an NFV environment just as easy as on a dedicated piece of hardware may be the case. But a more likely reason is that NFV is still this young a technology and vendors are still developing their VNF offerings.

Putting it all together

Before this white paper assesses applicability of SDN & NFV for the telecommunications sector this chapter first explains how both SDN & NFV can be used together. A strategy that is also applied in the OpenDaylight project, introduced at the end of this chapter.



SOURCE: RAYNO REPORT (WWW.RAYNOREPORT.COM)

Figure 4. Combining SDN & NFV - Source: raynoreport.com

At this early stage of SDN and NFV adoption, the industry acknowledges the benefits of establishing an open, reference framework for programmability and control through an open source SDN and NFV solution.

Combination of SDN and NFV

Motivation behind both SDN and NFV is very similar. Optimizing network functionality by making use of IT advances and offering this functionality in a service oriented way. This raises the following question. What is the best concept to apply, SDN or NFV? The answer is, if done properly, a combination of the two.

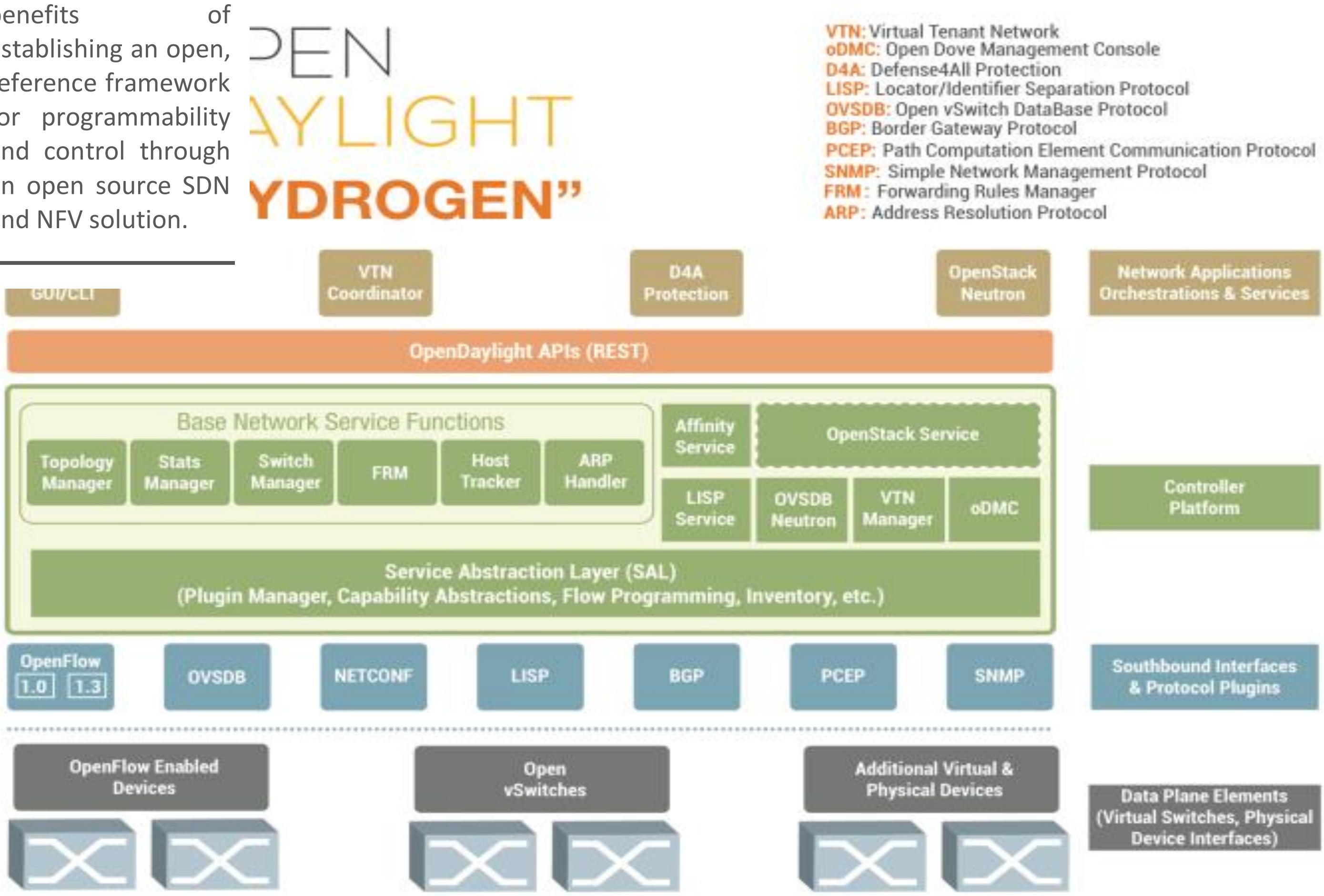

OPEN
DAYLIGHT
"HYDROGEN"
VTN: Virtual Tenant Network
oDMC: Open Dove Management Console
D4A: Defense4All Protection
LISP: Locator/Identifier Separation Protocol
OVSDB: Open vSwitch DataBase Protocol
BGP: Border Gateway Protocol
PCEP: Path Computation Element Communication Protocol
SNMP: Simple Network Management Protocol
FRM: Forwarding Rules Manager
ARP: Address Resolution Protocol
GUI/CLI
VTN Coordinator
D4A Protection
OpenStack Neutron
Network Applications Orchestrations & Services
OpenDaylight APIs (REST)
Base Network Service Functions
Topology Manager
Stats Manager
Switch Manager
FRM
Host Tracker
ARP Handler
Affinity Service
OpenStack Service
LISP Service
OVSDB Neutron
VTN Manager
oDMC
Controller Platform
Service Abstraction Layer (SAL)
(Plugin Manager, Capability Abstractions, Flow Programming, Inventory, etc.)
OpenFlow
1.0
1.3
OVSDB
NETCONF
LISP
BGP
PCEP
SNMP
Southbound Interfaces & Protocol Plugins
OpenFlow Enabled Devices
Open vSwitches
Additional Virtual & Physical Devices
Data Plane Elements (Virtual Switches, Physical Device Interfaces)

Figure 5. Open Daylight architecture - Source: Open Daylight

An SDN Controller is used to program the physical and virtual network infrastructure (sometimes called network OS) to create subnets and routing rules that can be used *for* both interconnecting Virtualized Network Functions (VNFs) when deploying an NFV-based service (e.g. connecting (Gx) virtualised PCRF & PCEF) and *by* VNFs to translate the virtualised network functionality offered into actual network configurations. I.e. SDN control plane elements may be deployed as VNFs in an NFV infrastructure. This is schematically illustrated in **Fout! Verwijzingsbron niet gevonden.**.

This is the theory. In practice it will be a much bigger challenge to implement a combined SDN and NFV solution as vendors offer a myriad of options that rather offer overlapping than complementing functionality introducing additional headaches such as lack of interoperability, limited management tools or fragmentation. An initiative that intents to prevent this from happening is Open Daylight.

Open Daylight

The Open Daylight project justifies its project with following motivation. At this early stage of SDN and NFV adoption, the industry acknowledges the benefits of establishing an open, reference framework for programmability and control through an open source SDN and NFV solution. Such a framework maintains the flexibility and choice to allow organizations to deploy SDN and NFV as they please, yet still mitigates many of the risks of adopting early stage technologies and integrating with existing infrastructure investments.

OpenDaylight software is a combination of components including a controller, interfaces, protocol plug-ins and applications, see **Fout! Verwijzingsbron niet gevonden.**. The Northbound and Southbound interfaces are clearly defined and documented APIs.

Opportunities for the telecom sector

So far this white paper has introduced SDN, NFV and how to use them together. Obviously the organisations behind both concepts promise mountains of gold when implementing SDN and NFV, not only in the IT datacentre but also in the fixed and wireless networks of telecom operators and service providers. An example of this promise (by Open Daylight) is shown in **Fout! Verwijzingsbron niet gevonden.**

This chapter wi
challenges of tele
them with the SD
are advertised. Th
these claimed ber
the operator chal
scenario is given h
indeed benefit fro

The most important challenges for telecom operators are: security, cost, meeting service levels (optimisation, improvements, simplification) and innovation.

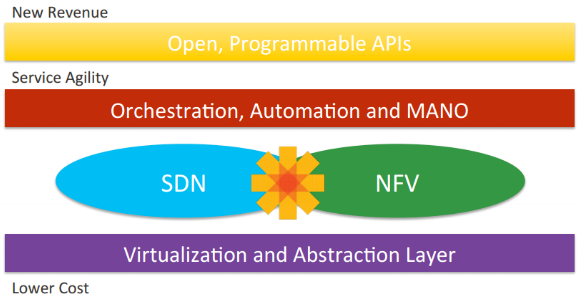

New Revenue
Open, Programmable APIs
Service Agility
Orchestration, Automation and MANO
SDN
NFV
Virtualization and Abstraction Layer
Lower Cost

Image 6: SDN & NFV promises - Source: Open Daylight

Telecom operator challenges

Telecom operators all have to deal with similar challenges. Some of them have been the same for many years, some of them are fairly new, such as securing networks and services. The following challenges are of high concern for telecom operators:

1. Security, how to prevent and deal with security vulnerabilities and other related threats.
2. Meeting (network) service levels, networks are showing signs of stress across many fronts.
3. Cost pressures for both equipment and operations.
4. Doing better (and simpler) at day to day operations.
5. Time to market to implement new services and new technology is too long.

This list of challenges is confirmed by a study done by Gigaom Research [SDNOper]. It's remarkable to see that improving current operations is higher on the list than quickly introducing new services. Apparently operators are struggling even more with getting their own stuff together than with full on competing with Over The Top service providers and other internet start-ups. Or they are simply focusing on becoming a very efficient and profitable dumb pipe operator and don't need all these fancy new technologies to be agile in offering new services.

Can operators beneft from SDN and NFV?

When looking at the benefits discussed in section **Fout! Verwijzingsbron niet gevonden.**, **Fout! Verwijzingsbron niet gevonden.** and **Fout! Verwijzingsbron niet gevonden.** one could conclude that SDN & NFV can solve some of the challenges operators are faced with, most importantly: security, cost, meeting service levels (optimisation, improvements, simplification) and innovation. This section will take a closer look at these challenges and assess whether SDN & NFV are really the solution to them.

Before you can benefit from the agility that SDN & NFV offers you need to have an SDN/NFV architecture. The huge investment and migration required is what keeps operators from doing this.

Security

SDN offers capabilities to mitigate security threats, such as DDoS attacks. Efficient traffic steering and path management allows for detection and isolation of threats. NFV allows security improving functionality (firewalls, intrusion and malware detection, etc.) to run centrally taking advantage of more available computing power and eliminating the need to have this functionality deployed on every network node.

Judging from the above, security seems like a very valid reason to deploy SDN & NFV. However two major concerns need to be taken into account. While SDN & NFV may offer increased security for known types of threats, as already raised in section **Fout! Verwijzingsbron niet gevonden.**, at the same time new technologies like these introduce new, still unknown, security risks themselves. Secondly, the above drawn approach to apply SDN & NFV to increase security will only be fully effective if it is done with the whole operator (network) infrastructure in scope, hence migrating an operator's complete installed base to SDN and NFV.

Cost

Operators are constantly on a quest to lower OpEx and CapEx. Like many other innovations both SDN and NFV claim to reduce cost. Indeed, with SDN the need for expensive networking equipment is reduced a lot. Additionally many network optimising tasks can be done automatically, saving on manpower. NFV also achieves reduction in cost, since VNFs can run on standard hardware instead of their appliance counterparts that require expensive dedicated hardware

But, this all assumes an operator can switch to this cost saving SDN & NFV architecture overnight and dump their expensive old infrastructure. Also let's not forget the CapEx that is required for the new environment. And taking into account the trend that the bulk of equipment cost is already in software (e.g. service platforms, OSS & BSS) rather than hardware, the case to switch to SDN & NFV, purely based on cost reduction isn't such a strong one.

Meeting service levels

An important selling point of both SDN and NFV is the way both concepts optimise resource usage, not only to save on equipment, see previous section, but also to quickly adapt to changing circumstances and requirements to keep the offered QoS in line with agreed service levels. SDN allows for advanced bandwidth management, adding networking resources if required, end-to-end rerouting traffic over the path that best meets requirements, etc. The elastic characteristics of NFV infrastructure allows to quickly add computing power if required. For example with a virtual EPC (Evolved Packet Core) network in case of events that cause a spike in mobile data usage the virtual PCRF & PGW will simply get more resources allocated to handle this increase in data session (requests).

Similar as with security though, this benefit will only solve the operator’s challenge when SDN & NFV is in place. Migrating to a SDN & NFV solution however may be much more expensive than optimising current infrastructure. It should also be taken into account that both SDN & NFV are still nascent technologies and there is no track record yet that proves claimed benefits are met in a real-world (5 nines) operator environment.

Innovation

Another argument that is used a lot to push SDN & NFV is that an SDN/NFV based architecture is more agile than traditional architectures. It allows for defining and introducing new types of services significantly quicker and offers new ways to monetize them. Some examples:

- Bandwidth on Demand: provide services only with the bandwidth they need, when they need it by dynamically establishing or resizing connectivity from the fixed or wireless access network through the core as necessary, so customers pay only for what they consume.
- Application specific networks: SDN and NFV allow an operator to logically separate its network into “slices”. Each slice can then be tailored, in terms of characteristics (security, bandwidth, QoS, etc.) and offered to a targeted industry sector or individual customer. Some examples are dedicated slices for Machine-to-Machine / Smart City use, CDN (Content Delivery Network) providers or content providers themselves (e.g. Netflix, see **Fout! Verwijzingsbron niet gevonden.**) or an alternative to the IP VPNs offered to enterprises.
- Network features as a service: Examples are managed router, managed CPE, managed security, and network performance assurance, etc.

While these are all interesting opportunities for new revenue streams, it seems that operators are rather reluctant. Obviously the first reason is the same as with the other topics just discussed. Before you can benefit from the agility that SDN & NFV offers you need to have an SDN/NFV architecture. The huge investment and migration required is what keeps operators from doing this. This reluctance is driven both by the economic crisis just behind us that has limited funds and previous investments already done (IMS, 4G, EPC, Fiber, OSS/BSS, etc.). Another

Summarising, SDN & NFV do offer the means for operators to overcome some of its challenges. However before these benefits can be harvested, a complete SDN/NFV architecture has to be implemented.

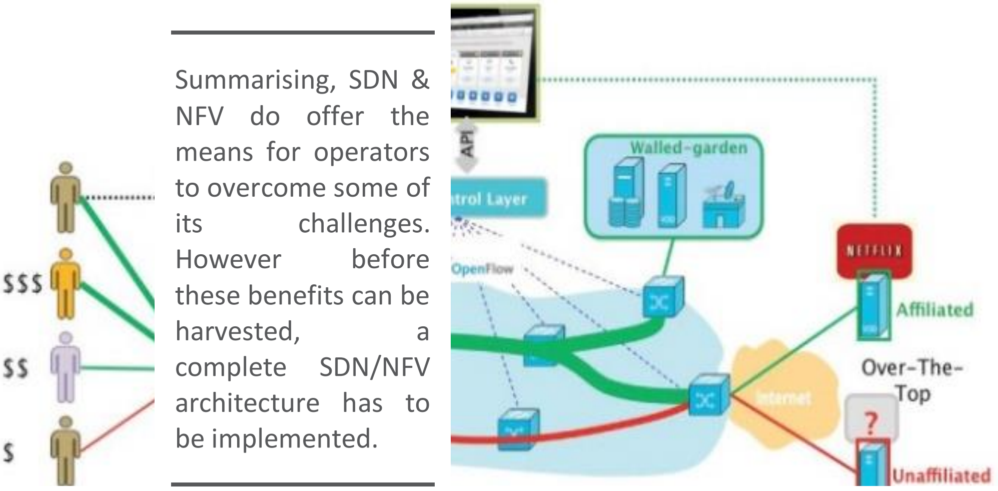


Image 7. Guarante lix traffic - Source: ONF

reason why operators aren't offering these new services right away is that they come with quite some uncertainties. While the technology allows for monetizing these services, based on e.g. usage, location or many other parameters it's questionable whether customers are willing to pay extra over free or cheap alternatives offered by OTT providers. Secondly regulation authorities are also looking at these new technologies and services and working on legislation. Net neutrality is a topic that potentially can prohibit an operator to offer Netflix QoS enhanced connectivity and similar propositions.

So the answer to the question "Can operators benefit from SDN & NFV" is "eventually yes". Only when SDN & NFV have matured more and a positive business case, that includes migration costs etc., has been defined then introducing SDN/NFV can be very rewarding for operators.

Summarising, SDN & NFV do offer the means for operators to overcome some of its challenges. However before these benefits can be harvested a complete SDN/NFV architecture has to be implemented. This is the biggest hurdle, for multiple reasons:

- Justification of the investment: Like with many other new technologies that offer enterprise wide capabilities (e.g. enterprise service bus, All-IP networks, etc.), who's going to pay for it? If it's up to the first use case/service that will make use of it, it will most likely never happen due to the high amount of CapEx undermining the business case.
- Migration: For SDN/NFV to really meet its promise it should be used as foundation architecture for most if not all services offered by the operator. This immediately causes a huge headache, as current installed base needs to be migrated to the new SDN/NFV architecture. A huge migration project like this is a potential disaster waiting to happen. In case the current infrastructure and/or operations is sourced to an MSP (Managed Service Provider) the migration to an SDN/NFV architecture may even be more complex.
- Position in the overall system landscape: SDN & NFV are new, they offer functionality that is partly network control, partly network management, partly process management and partly new functionality harder to categorise. How does it fit in the existing architecture? How to integrate or does it partly overlap with existing service platforms, management systems, OSS, BSS, etc.?

So the answer to the question "Can operators benefit from SDN & NFV" is "eventually yes". Only when SDN & NFV have matured more and a positive business case, that includes migration costs etc., has been defined introducing SDN/NFV can be very rewarding for operators.

Example fruitful SDN & NFV scenario

The example scenario introduced in section **Fout! Verwijzingsbron niet gevonden.**, CPE virtualisation, seems like one of the most valid scenarios for an operator to introduce an SDN/NFV solution and start offering (the CPE) services based upon it, because:

- Cloud CPEs offer many benefits over the hardware counterparts located on customer locations
- The scenario is relatively isolated. It does not require the whole operator's infrastructure to migrate to SDN/NFV. And as such can act as a proof of concept for SDN/NFV before deploying it more widely.
- It allows for a phased deployment of NFV and SDN. One can start with NFV and the virtualised CPEs. Later SDN can be added to also optimise the access network, configured by the Cloud CPE, over which the customers are serviced.

Most likely this is only just the beginning of a networking paradigm shift, as programmability of the network opens up more possibilities than we can currently even think of.

As an ACG Research study shows [CPECl] business services implemented in hardware CPE, such as IP-VPN and security services, are high cost, require long installation intervals, and are difficult to modify and upgrade. This slow and rigid process creates customer dissatisfaction and impairs the operator's ability to innovate and upsell services.

Cloud CPEs reduce field equipment installation and support costs. More importantly, operators can rapidly deploy new cloud-based services that are free of traditional physical CPE installation and maintenance limitations. Functions such as IPv6 NAT1, DPI based functions, and firewall capabilities are moved to the provider edge router and to virtualized data centres. A self-care portal allows the customer to configure these services in real time. Cloud CPE automation and orchestration capabilities eliminate many manual processes. Consequently, services become faster to develop, deploy, and contribute revenue. Added to that a centralised approach running on standard hardware exploits the better scale economies of the data centres.

This scenario is very comparable to another business market scenario, IP Centrex, where VoIP PBX functionality has been moved into the operator cloud. As shown above Cloud CPE will have similar benefits as IP Centrex has already proven. Potentially convergence between Cloud CPE and IP Centrex will allow for new compelling services.

Both SDN and NFV are developments that are here to stay, and the fact that they're still at the beginning of their existence gives telecom operators some more time to wait for them to mature and prove themselves more.

Conclusion

The goal of this white paper was to take a closer look at the new developments SDN and NFV, see whether all the hype is justified and determine how useful they are for telecom operators.

All the praise for SDN and NFV is very understandable. They both offer many new opportunities in terms of cost reduction, resource optimisation and service innovation. Most likely this is only just the beginning of a networking paradigm shift, as programmability of the network opens up more possibilities than we can currently even think of.

At the same time this wide range of possibilities and interpretations is its biggest threat. Vendors all have their own SDN or NFV solutions, real or still only on paper. And with the embryonic state of standardisation how to compare competing solutions and integrate them with current environments is a big unknown.

Many of the telecom operator's challenges, such as mitigate security threats, lower operational cost, optimise resource usage to meet service levels and innovate with new service offerings all seem to be solvable with SDN and NFV. However for an average telecom operator there are some big hurdles to be taken before these benefits can be reaped. The fact that SDN and NFV are very new means there is hardly any track record of SDN and NFV implementations outside the datacentre. Secondly most of these benefits will only be achieved when the operator first migrates a greater part if not its complete infrastructure over to a SDN/NFV architecture.

So, does this mean telecom operators should simply ignore all the SDN and NFV hype? Certainly not. Both SDN and NFV are developments that are here to stay, and the fact that they're still at the beginning of their existence gives telecom operators some more time to wait for them to mature and prove themselves more. An operator shall first position SDN and NFV in their technology roadmap, determine where it fits in the target architecture and when future business needs can be supported by SDN and/or NFV capabilities. Having a concrete scenario that can benefit from SDN/NFV all on its own seems like the best approach to introduce SDN/NFV as it allows the operator to gain experience with it and lessens the need for a full swing migration towards an SDN/NFV based architecture. Unfortunately there aren't many of these scenarios. One case that seems like a good candidate is the virtualisation of CPEs.

Prodapt Consulting

When your organisation wants to know more about SDN and/or NFV Prodapt Consulting can provide you with the required insight and help you build the strategy around SDN and NFV. Prodapt Consulting can facilitate RFP, RFI, RFQ projects when selecting SDN/NFV solutions and support your organisation with the implementation of the solution. Furthermore Prodapt Consulting can assist you in interoperability testing, end-to-end quality management and integration with OSS/BSS. These are all areas that Prodapt Consulting has experience in and can help you with.

References

[SDNPr]: https://www.sdncentral.com/sdn-nfv-products/
[SDNOSS]: http://www.sdncentral.com/comprehensive-list-of-open-source-sdn-projects/
[SDNStrat]: http://searchsdn.techtarget.com/feature/Major-SDN-vendor-strategies-at-a-glance.
[SDNOper]: Mark Leary, Gigaom, SDN, NFV, and open source: the operator's view, March 19, 2014.
[CPECl]: ACG Research, Business Case for NFV/SDN Programmable Networks, 2014.

Contact Details

Europe

Prodapt Consulting B.V.
De Bruyn Kopsstraat 14
2288 ED Rijswijk Z-H
The Netherlands

Phone	:	+31 70 414 0722

Adriaan van Donk

Phone	:	+31 6 5335 4335
E-mail	:	adriaan.van.donk@prodaptconsulting.com

Ben van Leliveld

Phone	:	+31 6 5335 4337
E-mail	:	ben.van.leliveld@prodaptconsulting.com

Paul Termijn

Phone	:	+31 6 3010 9117
E-mail	:	paul.termijn@prodaptconsulting.com

www.prodaptconsulting.com