SDN and NFV: The Game-changing Impact 2017-2023

February 2018

2201 World Trade Center, Brigade Gateway Campus, Malleswaram, Bengaluru India – 560055

Phone:+1 973 973 541 9600, +91 80 6793 5731 Email: marketing@insight-corp.com

www.insight-corp.com

The contents of this study represent our analysis of the information generally available to the public or released by responsible individuals in the companies mentioned. It does not contain information provided in confidence by our clients. Since much of the information in the study is based on a variety of sources that we deem to be reliable, including subjective estimates and analyst opinion, Techgradient and Insight Research does not guarantee the accuracy of the contents and assumes no liability for inaccurate source materials.

Table of Contents

Tables and Figures

1. EXECUTIVE SUMMARY

Insight Research conducted an in-depth market research forecast of SDN and NFV technologies. The exercise involved extensive primary research and exhaustive secondary research to build a comprehensive market forecast model.

This chapter highlights the salient findings of the market research report on Software-Defined Networks (SDN) and Network Functions Virtualization (NFV) technologies. The chapter also enumerates the prominent drivers for SDN and NFV technologies.

The Open Networking Forum (ONF) defines SDN as follows:

> *"Software-Defined Networking is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services."*

NFV can be defined in the following manner:

> *"The migration from physical networking hardware to virtualized network functions is termed as Network Functions Virtualization."*

SDN and NFV mark the building of irreversible momentum towards software-enablement of telecommunications networks. While they sound similar, SDN and NFV are not interchangeable terms. SDN focuses on simplifying network design, deployment, management and troubleshooting functions; whereas NFV concerns itself with unshackling network equipment and devices from the clutches of proprietary technologies and migrate the network functions to general purpose hardware.

There are obvious elements of complementariness between SDN and NFV:

- NFV can facilitate scaling up of SDN setups
- SDN can simplify the instantiation, management and monitoring of NFV elements

1.1 SALIENT QUANTITATIVE OBSERVATIONS

The following table presents the global market for SDN and NFV.

Table 1-1: Global market for SDN and NFV 2017-2023 ($ million)

	2017	2018	2019	2020	2021	2022	2023	CAGR
SDN	2,343	4,914	8,731	13,243	18,499	24,750	31,964	54.6%
NFV	4,824	5,688	6,735	8,017	9,585	11,464	13,699	19.0%
Total	**7,167**	**10,602**	**15,466**	**21,260**	**28,084**	**36,214**	**45,663**	**36.2%**

Source: Insight Research

Insight Research forecasts an attractive compounded annual growth rate (CAGR) more than thirty six percent for the combined SDN and NFV market. The market sizing for SDN involved independent assessment of key use-cases, while the market sizing for NFV technologies was derived from the market size for individual VNFs.

This report analyses the SDN technology market as a cumulative market of distinctive use-cases. Insight Research considers the following principal SDN use-cases:

- Central Office Rearchitected as Datacenter (CORD)
- Service Delivery/Fulfilment
- Network-as-a-Service (NaaS)/ Bandwidth on Demand (BoD)
- Mobile Network Virtualization/Network Slicing
- Software-Defined Wide Area Network (SD-WAN)
- Service Function Chaining

Similarly, the NFV market is organized as a cumulative market of multiple Virtual Network Functions (VNF). Insight Research considers fifteen major VNFs organized along six VNF categories.

The following figure summarizes the VNF categories and individual VNF types included in those categories

Figure 1-1: VNF categories and types

VNF Category	VNF Type
Switching and Routing	Virtual Load Balancer (vLB), Virtual Application Delivery Controller (vADC), Virtual WAN Optimizer (vWOC)
	vRouter, Virtual Carrier-Grade Network Address Translation (vCGNAT)
	vSwitch
Core WAN Functions	Virtual IP Multimedia Subsystem (vIMS), Virtual Call Session Control (vCSC), Virtual Policy and Charging Rules Function (vPCRF)
	Virtual Baseband Unit (vBBU), Virtual Radio Access Network (vRAN), extensible Radio Access Network (xRAN)
	Virtual Evolved Packet Core (vEPC), Virtual Voice over Long Term Evolution (vVoLTE)
Interfaces and Gateways	Virtual Advanced Media Software (vAMS), Virtual Session Border Controller (vSBC), Virtual Web Real-Time Communication (vWebRTC) Gateway (GW)
	Virtual Customer Premise Equipment (vCPE), Virtual Service Gateway (vSG)
	Virtual Wireless Access Gateway (vWAG)
Standard Device	Virtual Domain Name Server (vDNS)
	vFirewall
	Virtual Internet Protocol Security (IPSec), Virtual VPN (vVPN) Controller
IP Applications	Virtual Intelligent Messaging (vIM)
	Virtual Voice over Internet Protocol (vVoIP)
Testing	vProbe, Virtual Test Agent (vTA)

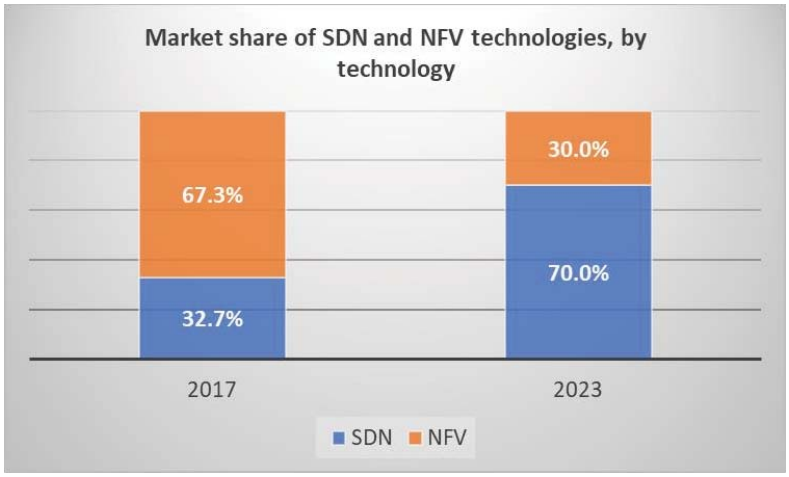
Source: Insight Research

For a given VNF type, this report forecasts the cumulative market size of individual terms, excluding any overlapping references. While these are distinctive terms, they practically deliver the same function and can be used interchangeably.

There is a distinct dichotomy between the paths charted by each of these technologies individually.

The following figure presents the market share of SDN and NFV technologies, by technology.

Figure 1-2: Market share of SDN and NFV technologies, by technology



Source: Insight Research

NFV is clearly the early leader. NFV owes its leadership to its varied user-base. It enjoys substantial traction from the Enterprise as well as from the Service Provider user segments. The Enterprise user-base will be instrumental in providing NFV with the early advantage. Enterprise-level implementation is performed at lower scales as compared to Service Provider-level integration. The implementation barrier is therefore substantially lower for Enterprises, whose decision-making is much faster than in case of Service Providers, wherein the higher stakes involved can slow down decision making.

SDN technologies will receive an overwhelmingly large chunk of their patronage from the Service Provider user-segment. SDN and NFV aim at eventually substituting conventional network elements and their networks. The market for such elements and networks is overwhelmingly skewed in favor of Service Providers. Service Providers will eventually dominate as they get increasingly attuned to benefits of these technologies. A turning point of sorts will be the fifth generation (5G) cellular network roll-outs.

SDN will therefore be a slow-starter, but the eventual market leader.

1.2 Drivers for SDN and NFV

Any casual dipstick of contemporary discussion surrounding SDN and NFV will list a plethora of benefits that these technologies bring to the table. While there is some merit in the optimism exhibited by stakeholders, the outlook needs to be tempered with realism.

It is worthwhile taking a pragmatic look at the drivers that play a key role in the march towards SDN and NFV.

1.2.1 Service agility

Applications are being increasingly hosted on virtualized servers resulting in flexibility in resource management. The increasing use of mobile platforms and Bring Your Own Device (BYOD) in enterprises shows that end users are consuming application services belonging to different domains and presented in different forms, on the same device. Real time communications and high availability requires that applications and services be rolled out with high agility. This in turn means that networks need to support the agility demanded by these modern applications.

Telcos can leverage the capabilities provided by SDN and enable dynamic network services for their customers and help them migrate to modern IT applications infrastructure. Insight Research, during the course of the study, came across claims of reduction in implementation times to the extent of 70 percent.

As network control is decoupled from forwarding, more general-purpose hardware can be used to provide reliable and flexible network services. By adopting NFV, telcos can provision network services on-demand for their customers. Instead of a truck roll out for specialized network hardware, additional NFV instances can be created on the same generic CPE on the premises of the customer. If concerns related to resilience and availability are addressed satisfactorily, it is easy to visualize the time savings that telcos and their customers can accrue.

1.2.2 Centralized control

Server virtualization was clearly a software-based approach of solving the problem of running applications on dedicated hardware. In addition to the flexibility, the software control over application lifecycle provided administrators with powerful tools for managing, securing and troubleshooting applications.

In traditional IT organizations, it was common to have different teams to manage the server infrastructure and the network infrastructure. With the move towards an agile and dynamic IT application environment, this silo-based approach between compute and networks was a hindrance. Centralized control of the compute and network infrastructure that provides more integrated management can break these barriers.

Modern-day telco networks continue to grow in complexity. Telcos provide network services to a variety of customers from small businesses to large enterprises. The smaller

customers may use “managed services” that require the telcos to operate the network on behalf of the customer. And the large enterprises may want some operate some parts of their network on their own. From a telco perspective, these diverse requirements are best addressed using centralized control. Access control techniques can then be applied to provide different ways to operate the network.

The premise for centralization is not foolproof. Companies like Pluribus believe thoughtless centralization of the control plane can induce complexity in networks. Pluribus is convinced that it is heralding the new wave of SDNs by decentralizing the control plane.

1.2.3 Enhanced reliability

SDNs have borrowed heavily from server virtualization constructs to improve their reliability. This may sound counterintuitive. Server virtualization allowed applications to be shrink-wrapped and be hosted on any hardware server. If the underlying hardware had a fault, the entire application can be smoothly migrated to another hardware without the application realizing it. This reliability improvement provided by server virtualization required a corresponding support from the underlying network as well.

Taking cue from the portability provided by server virtualization, SDNs can also insulate the larger networks from localized faults. As telcos deploy and operate large telecom networks, the reliability of the network is of utmost importance. Using the abstraction provided by SDN, telcos can expand and enhance their network services independent of the network hardware. This independence also provides resilience against failures as both software and the hardware can be upgraded or changed independent of one another.

1.2.4 Software-driven approach

The traditional IT environment consisted mainly of physical networking hardware. It was common to have networking equipment from multiple vendors for various reasons. However, hardware from different vendors posed a challenge for interoperability and added complexity to the network design. Devices from different vendors may not support the same capabilities. This mismatch can be solved by applying software updates, but newer versions of networking software require initial soaking period, thereby slowing down the ability to roll out fresh networking capabilities. Applications that are tightly coupled with physical networks may also be impacted due to upgrade related outages.

In environments like datacenter and public clouds, the network needs to scale very rapidly with the demand for more computing and storage resources for applications. Designing a growing network with only physical devices is no longer a viable solution. Along with server and storage virtualization, the need for network virtualization is paramount.

Virtualization can be achieved by a software-driven approach so that applications are truly decoupled from the underlying network hardware. The reduced dependency with network hardware also minimizes the challenges associated with multi-vendor networks. A more software-based approach would provide network administrators with better tools and simplify the management by hiding the vendor-specific complexity. For example, with a software-based approach, applications can be moved within the data center such that parts of the network can be upgraded without impacting the applications. Software-driven approach also facilitates dynamic alteration in security parameters.

1.2.5 Cost savings

Instead of using specialized network hardware, businesses can now use general purpose compute to host VNFs. General-purpose hardware straightaway reduces the capital expenditure and eliminates the dependency on network hardware vendor. The VNFs can be provisioned on demand and can even be scaled up or down based on the load on the network. Telcos can therefore offer more software subscription-based services and thereby lower the operating expenses for their customers. The pay-as-you-go approach of consuming enterprise applications can now be adopted for network services as well.

The benefits of cost savings are not restricted to NFV implementations. SDN fundamentally postulates a determined move towards generalized COTS hardware. Individual vendors will offer products with SDN functionality. In ideal scenarios, the differences between products offered by varied vendors will continue to diminish. SDN will be the torchbearer towards standardization in the long run.

1.2.6 Vendor neutral hardware

The approach of using physical networking hardware has several challenges. Vendor lock-in is the gravest of these challenges. Multi-vendor installations can lead to interoperability challenges. By using x86 based servers to run VNFs it is possible to be immune from vendor-specific hardware challenges. Telcos can also offer the x86 based platforms as Customer Premises Equipment (CPE) devices and allow them to run multi-vendor VNF on them.

The move towards vendor neutral hardware has grave implications for established players such as Broadcom, who dominate the switch fabric market. The limitations of this approach should also be understood. General-purpose hardware can never substitute Application-Specific Integrated Circuits (ASIC) in core switching functions for the foreseeable future.

1.2.7 Optimal utilization of resources

Optimal resource utilization is the most significant driver for the adoption of NFV. The virtual network functions are quite simply software entities that can be created and destroyed on demand. Users need not wait for new hardware to arrive and be physically connected for use. For example, if a network is being subjected to a Distributed Denial-of-Service (DDoS) attack, NFV can facilitate seamless deployment of more firewall and IPS instances to thwart the attack. Once the threat is neutralized, the instances can be destroyed, ensuring that the x86 hardware resources are used optimally.

1.2.8 Flexibility in network design

With only basic network connectivity implemented using physical cables, the logical network becomes more significant. Network virtualization supports seamless isolation independent of underlying physical connectivity. By applying SDN methodologies it is possible to create more flexible and adaptive network design to support complex application requirements.

1.2.9 Benign effect on capital and operating expenditure

x86 based servers require much lesser capital investment. There is considerable protection against hardware faults when compared to dedicated networking hardware. NFV instances are treated like software entities and can be deployed using subscription-based licensing. This is beneficial from an operating expense perspective.

The optimism towards cost savings needs to be tempered in the short run. Service Providers and Enterprises will need to equip themselves to manage operations in a software-driven environment. The reskilling of resources will lead to a short-term dent in the cost savings accrued from SDN and NFV technologies.

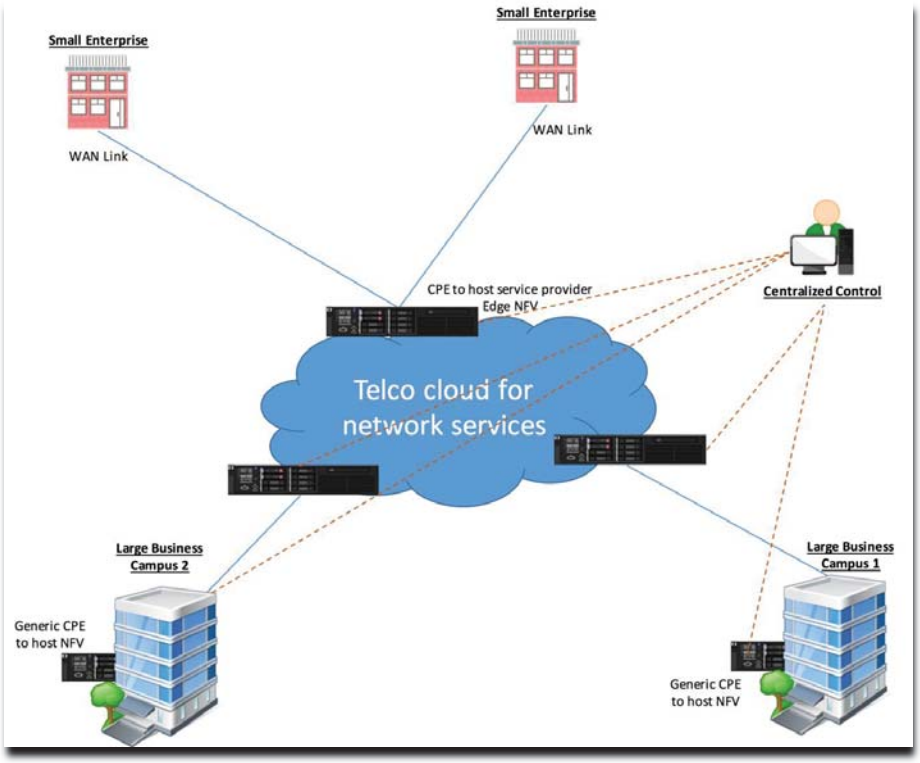
1.2.10 Ownership of feature-rich services

NFV based approach allows telecom service providers to offer a broad range of networking services and features as VNFs. Centralized control allows end users to provision and consume the services that they desire. Therefore, consumers can mix and match VNFs from different network vendors and design a network service chain suits their need. The ability to choose the network service along with the full control to operate it can be provided to end users using this architecture.

1.2.11 Takeaways for telcos from SDN and NFV

The following figure shows how telco network services can be provided to small enterprises and large businesses using SDN and NFV technologies.

Figure 1-3: Telco cloud and networking services.



Source: Insight Research

Small enterprises can leverage the *virtualized* network functions such as Firewall, Intrusion Prevention that are hosted *inside* the telco cloud. This eliminates the need for an on-premise complex network CPE thereby reducing capex for the small enterprises without compromising on the functionality. The Software-as-a-Service (SaaS) model of pay-as-you-go can be applied to these network services hosted in the telco cloud.

Large businesses require more sophisticated network capabilities on their premises. The same general-purpose hardware, that hosts VNFs for the telcos, can be reused as a simple CPE that can host VNFs such as Firewall, WAN Optimizers inside the branches of large businesses. These VNFs use WAN links to connect to their peer network services running inside telco cloud.

The above is a very simplistic explanation. Its very simplicity has prompted telcos such as AT&T to launch FlexWare, it's virtual CPE offering on an aggressive scale, as its debut into the VNF space.

In essence, SDN and VNF technologies enable telcos to adopt a graded approach towards customer engagement. Telcos can debut with less complex VNFs like vCPE and then move towards more intricate SDN and NFV constructs.