White Paper - Huawei Observation to NFV

HUAWEI

White Paper - Huawei Observation to NFV

1 NFV Overview 2

1.1 Motivation for Network Function Virtualization 2

1.2 NFV Ecosystem Is Being Built Up 3

2 Major Gaps Hindering Network Function Virtualization 7

2.1 Management and Orchestration 7

2.2 Performance Analysis and Measurement for Cloud OS 7

2.3 Reliability and Availability Requirements Regarding NFV 8

2.4 Security and Software Management 9

3 Huawei's Views on Telecom Virtualization Movement 10

3.1 MANO Integrating Cloud Management into Mobile Network Operation 10

3.2 Service Chaining Deployment in a Mobile Network 11

3.3 NFV Enabling Network Operators' Openness to Infrastructure Stage 12

4 Conclusions 13

List of acronyms and abbreviations

Acronym or Abbreviation	Full Name
COTS	commercial off-the-shelf
ETSI	European telecommunications standards institute
FMSS	flexible mobile service steering
IaaS	Infrastructure as a service
INF WG	architecture of the virtualization infrastructure working group
ISG	industry standard group
MANO	management & orchestration
NFV	Network Function Virtualization
NFVI	Network Function Virtualization infrastructure
NFVO	Network Function Virtualization Orchestrator
SDN	software defined network
SDO	standards developing organization
SEC EG	security expert group
SFC	service function chaining
SLA	Service Level Agreement
SWA WG	software architecture working group
VIM	virtualized infrastructure manager
VNF	virtual network function
VNFM	virtual network function manager

1 NFV Overview

1.1 Motivation for Network Function Virtualization

NFV (Network Function Virtualization) is a network evolution which utilizes COTS hardware and new virtualization technologies to deploy network functions for operators' networks, and it has profound impact on network operation and deployment with the following benefits:

- The network function virtualization technologies can better leverage mature IT cloud computing technologies to transform telecom networks to service-oriented networks. The network function virtualization technologies, with smart data analysis such as smart resource prediction and automatic resource orchestration, can help to reduce network CAPEX and OPEX and improve operation efficiency.
- The network function virtualization technologies along with SDN technologies would enable dynamic, flexible and automatic network and service chaining configuration based on application layer demand.
- The network function virtualization technologies provide operators with more flexibility to further open up their network capabilities and services to users and other services.
- The network function virtualization technologies also help network operators to deploy or support new network services faster and cheaper to realize better service agility.

1.2 NFV Ecosystem Is Being Built Up

1.2.1 ETSI NFV ISG Status

The ETSI NFV Industry Standard Group (ISG) was initially founded by seven global network operators to promote the network function virtualization concept in late 2012. NFV ISG is becoming an industry focal platform to develop NFV architectural framework and requirement, and coordinate with various other standard organizations and open source communities on developing standard and implementing open source for NFV. NFV ISG has successfully attracted extensive attentions from the industry and has been building up a significant ecosystem with various industry players, such as worldwide network operators, telecom equipment vendors, virtualization software and solution suppliers, and hardware and solution suppliers. As of October 18, 2014, the ETSI NFV ISG membership has grown to 230 companies. The ETSI NFV architecture is started by leveraging cloud computing architecture and technologies and creating new network technologies, such as VNF execution environment, and management & orchestration. The ETSI NFV architecture uses COTS hardware with identified hardware acceleration, virtualization environment including container technologies, vCPU, vStorage and vSwitch support, and abstract resource management and operation.

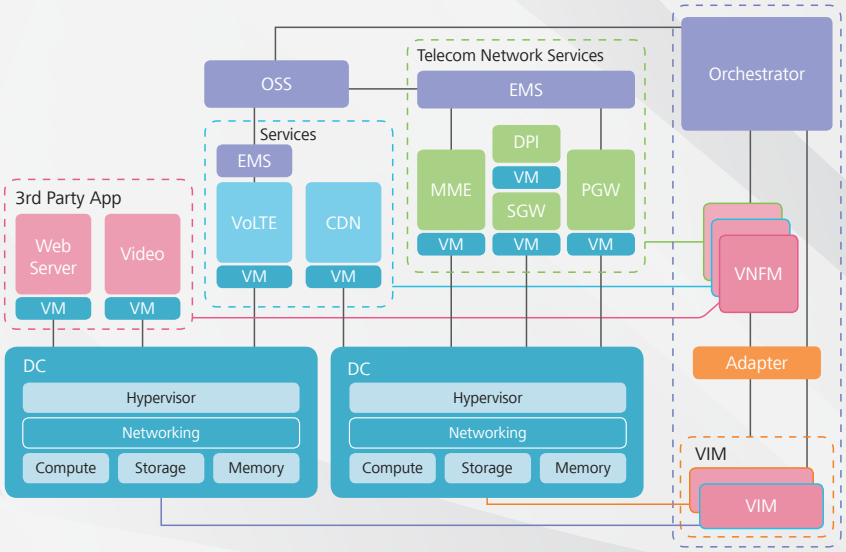

Figure 1: NFV reference architectural framework

Figure 1 illustrates the NFV reference architectural framework. As such, three core parts of the framework are identified:

- NFV management and orchestration, including the Orchestrator, VNFM, and VIM functional blocks. The two main responsibilities of the Orchestrator are orchestration of NFVI resources across multiple VIMs and the lifecycle management of Network Services. The VNFM is responsible for VNF lifecycle management. The VIM is in charge of controlling and managing the NFVI compute, storage, and network resources, usually within one operator's Infrastructure Domain.
- VNF, virtualized network function which can be capable of running over the NFVI.
- NFVI, including hardware servers, the virtual layer which can integrate and virtualize the hardware resources, and the abstract virtual resources.

Huawei has started research in cloud computing technologies and begun to develop related products and solutions since 2008, and has been actively participating in NFV discussions since the foundation of ETSI NFV ISG. As a network equipment vendor, Huawei has been involved in all of NFV working groups and expert groups, and has made significant technical contributions to the NFV Group Specifications. Huawei has provided expertise to VNF software design/standard, virtualization software and hardware design, application offering system, and management/operation.

1.2.2 Other Standard Organizations Are Embracing NFV

ETSI NFV ISG, as an industry standardization project, is expected to build an industry consensus on how to integrate an NFV standardization ecosystem. Ideally, standardization bodies represent players from the industry in terms of VNF software, integration service, NFVI hypervisor, NFVI network solutions, and computing and storage hardware.

ETSI NFV ISG, in a standard manner, works on the NFV platform, work flow, and interface in reasonable details. Participants from operators and vendors are working on identification of requirements for open source projects, as an ICT integration platform of virtualization.

Some NFV-related works which have been started in relevant SDOs are listed in Table 1.

Table 1: Relevant SDOs and their work on NFV

Organization	NFV-related Work
3GPP	Huawei and CMCC initiated a SID in SA5 to study the impacts of NFV on 3GPP network management system.
IETF	IETF is to provide protocol support for NFV. The WGs or topics related to NFV include: NFV RG, NFVCon (BoF), NFVPool (BoF), and SDN-related WGs.
DMTF	DMTF has defined the Open Virtualization Format (OVF) as a virtual machine packaging standard for a single virtual machine or a complex set of virtual machines. OVF and the DMTF Common Information Model (CIM) may be used as one option for capturing some or all of the VNF package and/or VDU Descriptor.
OASIS	OASIS TOSCA TC works to enhance the portability of applications and services. OASIS TOSCA provides an interoperable description for cloud application; it is a technology capable of describing NFV entities like VNF and Network Service in an interoperable template.
BBF	BBF is working on how cloud-based technologies including NFV can be used in the implementation of the Multi Service Broadband Network. Many work items related to NFV are in process in BBF: • WT-328 – Virtual Business Gateway • Stage 1 for introduction of Network Function • Virtualization in Multi-Service Broadband Network (MSBN) • Migrating to NFV in the Context of WT-178

1.2.3 Open Source for NFV

The IT software application industry usually uses open source to achieve certain business objectives, such as to reduce development costs, increase the popularization of specific software products, or quickly achieve interoperability. Endorsement to fund an open source project is motivated to reduce development costs by collecting multiple parties' code, speed up software development, and achieve interoperability among software components from different software vendors for large-scale software architecture (for example, OpenStack).

As an industry forum, the open source projects should be the place to form industry consensus by code to support software architecture for a particular use. To use the OpenStack project as an example, it forms software architecture applicable to public cloud and private cloud uses which allowed core architecture values of openness and componentry supports. Cloud software and solution providers are able to integrate commercial application into cloud computing solutions.

Open Platform for NFV (OPNFV) is another example that supports NFV. As an open source project to accelerate innovation based on virtualization environment, OPNFV supports NFV-related functions such as fault management, performance management, NFVI hardware configuration and virtualized resource management which are required for NFV infrastructure.

2 Major Gaps Hindering Network Function Virtualization

2.1 Management and Orchestration

2.1.1 Interfaces and Interoperability Issues

Significant progress was made in ETSI NFV phase 1 to finalize the NFV MANO framework and fairly sufficient definitions were created for MANO logical entity and interfaces. However, there is still much detail information that needs to be defined to achieve interoperability between different vendors with different functions. For example, the NFV MANO Group Specification specifies concepts of VNF Descriptor and Network Service Descriptor as template of application to allocate infrastructure resource and generate network service but without defining the detail information and data model to construct those descriptors.

2.2 Performance Analysis and Measurement for Cloud OS

Network service availability and design based on COTS hardware is a new challenge to VNF which runs on the hardware and the service that constitute the VNF. The NFV Platform, which integrates features of flexibility and elasticity to deploy VNF, needs to collect and correlate performance and measurements from different layers and components to guarantee end-to-end service performance indications.

DC networking performance in virtualization environment would rely on more network-service-friendly designs which are also measurable to VNF as part of an end-to-end network service.

The performance test on common virtualization environment indicates some new requirements for the NFV platform based on cloud computing technologies:

- The NFV platform might see positive linear increasing correlation between packet forwarding performance requirement and hardware resource. The proportional results indicated by the test curve might imply more optimization of scheduling process of packet forwarding in virtualization platform.
- Hardware might present slightly different performance (for example, average throughput and average CPU load) according to multiple applications of protocol handling or network function processes (for example, encryption and decryption).

A lot of testing results indicate that the use of hardware acceleration helps achieve better packet processing and forwarding performance. For example, packet forwarding efficiency would benefit from hardware acceleration and software switching enhancement of Netmap based on Huawei network I/O card acceleration solution in proper deployment scenarios.

2.3 Reliability and Availability Requirements Regarding NFV

There should be reliability and availability requirements for an NFV environment, for example, the reliability and availability of a single virtualized network function should be the same as that before, and the NFV system that consists of multiple VNFs should be the same or reach the acceptable level as those for a legacy system.

VNFs as part of an end-to-end network service should fulfill even higher reliability and availability requirements through some reliability and availability mechanisms, which include fault prevention, fault detection, fault correlation, resiliency and so on.

- A fault prevention mechanism could be used to avoid error during the planning, designing and deployment, for example through affinity and anti-affinity policies and single point of failure prevention. And it could be also used to avoid the failures during the system operation through failure prediction, overload prevention, and so on.
- A fault detection mechanism could be used to detect a failure and locate the root cause, which includes software/hardware failure detection, cross-layer monitoring, liveness checking (for example, heartbeat), fault correlation and so on.
- A resiliency mechanism could be used for service remediation and recovery after a failure has occurred, for example through VNF redundancy, VNF migration, stateful/stateless VNF protection and so on.

Figure 2: NFV reliability & availability mechanisms

2.4 NFV Security Consideration

Security plays a very important role in NFV environment. As well as identified topics in the Group Specification document *"NFV security problem statement"*, the following security gaps are also identified:

- Security monitoring is an important measure to detect threats and mitigate attacks on networks. However, if it is not implemented correctly, the network security may be weakened, which will make the network more vulnerable to attacks. Compared with the traditional networks, NFV faces a challenge of achieving effective security monitoring and network security.
- Lifecycle management security needs to take the following fact into account: The dynamic management during NS/VNF instantiation, scaling, upgrade, migration, and secured wipe causes the VNF and the bearing entities of VNF to change dynamically. The dynamically changing network and elements require dynamic management of the security policy for the virtualized network and dynamic resource allocation based on the security policy.
- IPSec and TLS mechanisms are widely deployed to protect the links between two communication entities by using certificates as the credentials to prevent attacks such as spoofing, tampering and information disclosure. These mechanisms can also be used to protect the new interfaces introduced by NFV scenarios. However, the traditional manual certificate deployment mechanism cannot meet the automation requirements of NFV, and the automation mechanism defined in 3GPP networks faces challenges in the virtualized environment. In the NFV environment, VNF instances are created dynamically, and multiple instances may be created according to the same VNF software, which is quite different from those in the traditional networks.

3 Huawei's Views on Telecom Virtualization Movement

3.1 MANO Integrating Cloud Management into Mobile Network Operation

3.1.1 Real-Time Virtualization Management Platform

The NFVI virtualization platform, called NFV Infrastructure, requires a unified NFVI resource management and orchestration system. This resource management and orchestration system would not only provide virtual resource management and orchestration, but also provide end-to-end network service management and orchestration. These two aspects of management and orchestration can be implemented in one system or separate systems.

The network service management system should take charge of end-to-end service SLA monitoring and management, with frequent and real-time interaction with the resource management system. The NFVI resource management should supervise virtualized resources and be extended to further manage physical resources. The NFV resource management and orchestration system requires allocating dedicated hardware resources to proper virtual network functions.

3.1.2 Interaction Between Network SDN Controller and NFV MANO

SDN is a desirable complement to NFV to provide better service-oriented traffic steering and service chaining. Because MANO manages and orchestrates the virtual network resources and connections between VNFs for the end-to-end network service, there is a need for MANO and SDN controller, which is the brain of SDN, to work together for efficient traffic routing. One deployment option on the interaction between SDN controller and MANO is illustrated below. In this deployment scenario, the network operator uses the network service orchestration function to configure network service chaining policies, and through the NFV MANO framework, provisions the service chaining policies to the network controller in the NFVI networking layer.

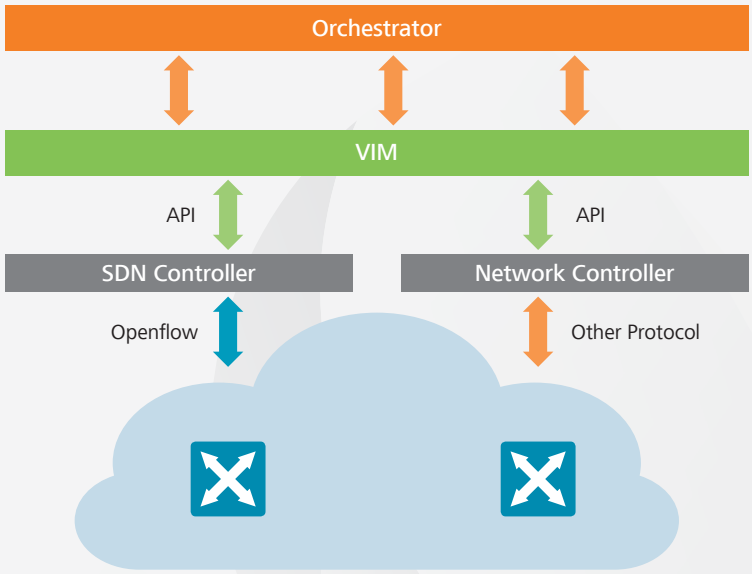

Figure 3: Network Controller as part of the NFVI network management plane

3.2 Service Chaining Deployment in a Mobile Network

As service deployment requirements in mobile networks increase, mobile network operators confront big challenges with traditional service enablers in data center.

- First of all, mobile network Gi-LAN with layered structure results in more complexities to enable, modify and maintain a new service.
- Secondly, the automation configuration to service enablers is more complicated when the number of services in mobile network increases significantly.

In NFV deployment, Gi-LAN service deployed in virtualization brings particular requirements for the service chaining solution.

- A service chain containing both physical functions and virtualized functions would require the service chaining solution to support sequencing of physical service functions and virtualized service functions.
- Flexibility features of Gi-LAN service chaining orchestration and control capabilities, forwarding logic for service configuration, and cross-DC deployment are needed.

Huawei Gi-LAN service chaining solution has considered the technologies developed by NFV, 3GPP SA1 FMSS, ONF open flow protocol, and IETF SFC.

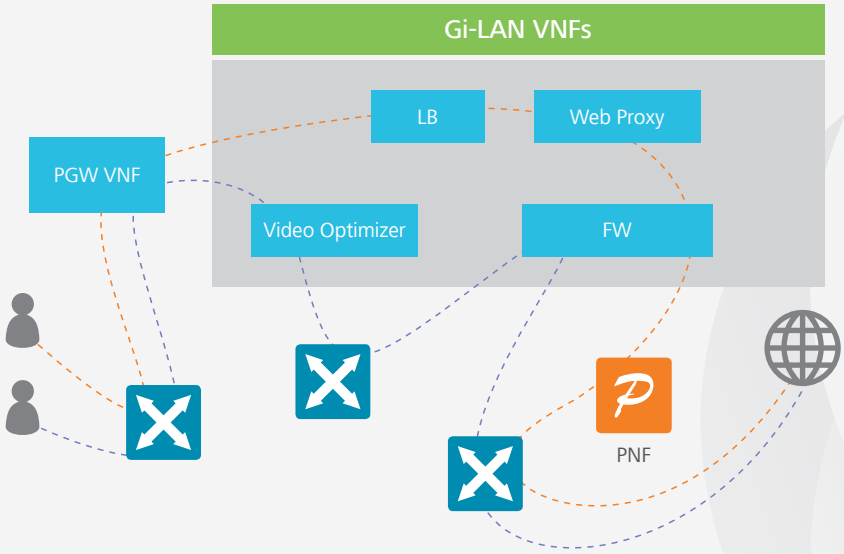

Figure 4: Gi-LAN with service functions

3.3 NFV Enabling Network Operators' Openness to Infrastructure Stage

Operators are enabled by the network capability platform to allow external applications or parties, in a designed approach, to use certain network capabilities according to specific business models. Network capabilities such as multimedia communication, presence, location, and subscriber data can be made available – subject to privacy and integrity measures – as components in the application developers' toolbox, and various QoS mechanisms can be applied to reduce latency and enhance QoE of the IP-based OTT services.

Operators' authentication, payment and billing capabilities can be built into and reused by third-party applications, which simplifies for both application developers and users. With NFV, operators can provide more flexibility in services and capabilities, for example not only provide simple network capabilities but also provide more comprehensive services, such as NFVIaaS, VNFaaS, and VNF platformaaS.

Operators can shift from being a pure connectivity provider to becoming a provider of capabilities and qualities tailored to buyers' needs. Traditional Telco examples include dynamic changes to QoS parameters, bandwidth allocation on demand, or even the establishment of "bandwidth exchange marketplaces" where operators can monetize their excess capacity.

4 Conclusions

NFV is evolution for network transformation with many challenges but more opportunities and benefits to the industry. It should be a joint effort between all the industry players, such as network operators, network solution providers, telecom applications providers, and IT infrastructure solution providers. Huawei, as one of the leading companies, will keep on working with industry partners for the success of NFV. The industry organizations such as ETSI NFV ISG and OPNFV along with SDOs and Open Source communities will be working closely together to enable large-scale network virtualization deployments to become a reality.

Reference:

- ETSI NFV ISG Published Documents: http://www.etsi.org/technologies-clusters/technologies/nfv
- ETSI NFV ISG Draft Documents: http://docbox.etsi.org/ISG/NFV/Open/Latest_Drafts/
- 3GPP specifications: http://www.3gpp.org/specifications/
- IETF SFC WG: https://datatracker.ietf.org/wg/sfc/
- Open Network Foundation (ONF): https://www.opennetworking.org/
- Intel DPDK: http://dpdk.org/
- Netmap: http://info.iet.unipi.it/~luigi/netmap/
- OpenStack, Open Source Cloud Computing Software: http://www.openstack.org/

Copyright © Huawei Technologies Co., Ltd. 2014. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademark Notice

, **HUAWEI**, and are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

Other trademarks, product, service and company names mentioned are the property of their respective owners.

General Disclaimer

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808
Version No.: M3-023985-20141119-C-1.0

www.huawei.com