A Brief Overview of Network Functions Virtualisation

Kazuaki Obana, Takeshi Kinoshita, and Katsuhiro Shimano

Abstract

Many network functions such as firewalls and intrusion detection systems have been implemented on specifically designed hardware. Today we are seeing a technological trend in which these functions are being implemented as software running on general purpose servers. The European Telecommunications Standards Institute has established an Industry Specification Group (ISG) to discuss and define the requirements for Network Functions Virtualisation (NFV). This article introduces the concept of NFV and summarizes the activities of the NFV ISG.

Keywords: NFV, network functions virtualisation, virtualisation

1. Introduction

The performance of central processor units (CPUs) and memories, basic components of a general purpose server, has been steadily improving in accordance with Moore's law*1. One core of today's multi-core CPUs can handle a million packets per second. Therefore, sufficient performance may well be achieved even if network functions are implemented as software in a general purpose server. Virtualisation*2 presents an advantage in doing so because it enables execution of cloud computing capabilities such as flexible, on-demand deployment of network resources. Network Functions Virtualisation (NFV) is thus coming closer to practical use, and many network carriers have begun testing it for that purpose (**Fig. 1**). The NFV Industry Specification Group (ISG) was established by the European Telecommunications Standards Institute (ETSI) to address issues concerning the realization of the technology.

In existing network appliances, network functions are implemented with specifically designed, proprietary hardware. The performance of these appliances has been improved through the development of hardware that meets specific requirements while retaining carrier-grade reliability. To introduce a new service, newly designed appliances with the required functionalities must be installed at the carrier's buildings, which increases costs for the carrier. Operation and maintenance of the appliances is also an issue because different processes are involved for each kind of appliance, and managing them in an integrated way from a remote site is usually difficult.

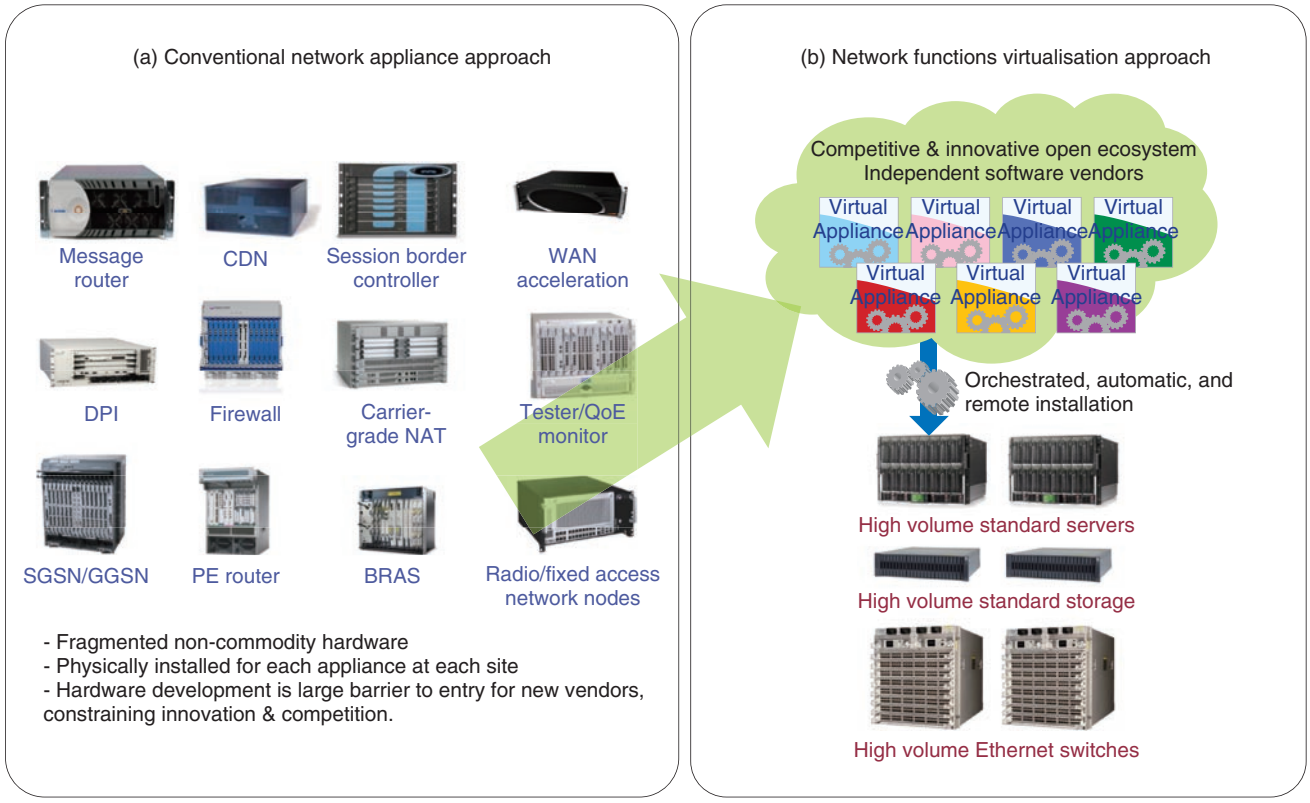
In contrast, the objective with NFV is to implement network functions on general purpose servers. The virtualisation allows the functions to be updated on demand, making it easier to achieve integrated remote maintenance. NFV thus reduces the OPEX (operational expenditure), while also reducing the CAPEX (capital expenditure) through the use of widely used servers, which are usually available at a lower cost.

2. Applications and use cases

The functions being discussed by the NFV ISG vary through the data plane and the control plane for both fixed-line and mobile networks. They include all the currently used network functions such as carrier-grade network address translation (NAT) and

*1 A computing term that originated around 1970; the simplified version states that processor speeds, or overall processing power for computers, will double every two years.

*2 The British spelling used by ETSI is retained throughout the article.



BRAS: broadband remote access server
CDN: content delivery network
DPI: deep packet inspection
GGSN: gateway GPRS (general packet radio service) support node
NAT: network address translation
PE: provider edge
QoE: quality of experience
SGSN: serving GPRS support node
WAN: wide area network

Fig. 1. NFV approach.

broadband remote access server (BRAS) functions implemented in a carrier's central offices; evolved packet core, IP (Internet protocol) multimedia subsystem (IMS), and eNode B functions implemented in mobile networks; functions of home gateways and set-top boxes located at a customer's premises; IPsec tunneling, deep packet inspection, and other traffic analysis or protocol handling functions; load balancer (LB), content delivery network (CDN), and other network control functions; and firewall, intrusion detection system, and other security functions.

Of these, nine use cases were selected as high level cases by the NFV ISG and were described in a recently published document [1]:

(1) Network Functions Virtualisation Infrastructure as a Service,
(2) Virtual Network Functions as a Service,
(3) Virtual Network Platform as a Service,
(4) VNF (Virtual Network Functions) Forwarding Graphs,
(5) Virtualisation of Mobile Core Network and IMS,
(6) Virtualisation of Mobile Base Station,
(7) Virtualisation of the Home Environment,
(8) Virtualisation of CDNs,
(9) Fixed Access Network Functions Virtualisation.

3. History of the NFV ISG

A number of carriers across the world recognized the need to establish a common forum for discussing NFV to lead the technological movement, and thus collaborated in preparing a whitepaper [2] intended to promote international efforts towards realizing NFV. They include AT&T, BT, CenturyLink, China Mobile, Colt, Deutsche Telekom, KDDI, NTT, Orange, Telecom Italia, Telefonica, Telstra, and

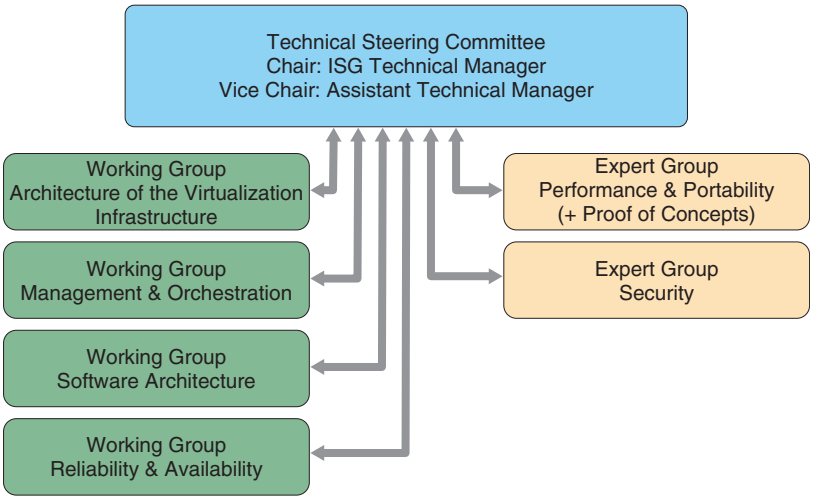


Fig. 2. WG/EG structure.

Verizon. In October 2012, at the SDN (software-defined networking) and Openflow World Congress held in Darmstadt, Germany, they announced the publication of the whitepaper as well as the establishment of the NFV ISG under the auspices of ETSI. (The second version of the whitepaper [3] was published at the conference in 2013.) Since the NFV ISG was officially formed in November 2012, its members have increased to more than 140 companies and organizations consisting of vendors of communications equipment, information equipment, and software. Some 200 to 300 people attend the periodic meetings, where they have active discussions. The NFV ISG does not specify technological details concerning implementation of NFV but presents its architecture and requirements so that they can be used as a basis for the technological specifications developed by other standards organizations. Many of the key persons are also members of other standards organizations, and they facilitate collaboration between organizations. Now that the NFV ISG has released official documents, it is highly expected that standardization processes underway at other organizations will advance further.

Inside the NFV ISG, each Working Group (WG) and Expert Group (EG) discusses issues concerning a specific theme (**Fig. 2** and **Table 1**). Representatives from WGs and EGs constitute a Technical Steering Committee (TSC), which coordinates and guides the activities of different groups. A Network Operator Council (NOC) was created to guide the organization as it was established. It also discusses strategic aspects of the activities (**Fig. 3**).

Plenary meetings are held every quarter, and all NFV ISG members are eligible to take part. Additionally, rapporteurs, who are responsible for completing documentation, can convene ad hoc meetings to discuss items in detail and improve the content of documents. Because only a limited number of members can attend these meetings, draft documents edited at the meetings are made accessible to all NFV ISG members before the next plenary meeting. The draft documents are subject to comments from members and are made ready for approval via an online meeting or at a plenary meeting.

At plenary meetings, WGs and EGs hold separate face-to-face sessions. In other cases, online sessions are often held. They include joint meetings, in which members from more than one WG gather to collect opinions from relevant WGs. People from different countries and regions throughout the world take part in these meetings, so it is often difficult to determine a suitable meeting date and time. The fact that many members belong to more than one WG or EG makes this even harder. The representatives of WGs and EGs thus make diligent efforts to coordinate meeting schedules.

The first plenary meeting was held in January 2013 at the Sophia Antipolis technology park in France, where the headquarters of ETSI is located. All of the plenary meetings up to and including the most recent one, the fourth, have been held in either Europe or the United States. It is likely that a future meeting will move to another region. If other standards organi-

Table 1. Areas focused on by Working and Expert Groups.

WG/EG	Description
Architecture of Virtualisation Infrastructure WG	Developing a reference architecture for the NFV virtualisation infrastructure. Working domains include: Compute, Hypervisor, Network Infrastructure, Interfaces & Abstractions, Test Access, Scalability, Portability, and Replicability.
Management & Orchestration WG	Defining a management and orchestration framework for virtual network functions and the infrastructure these functions run on. Scope includes requirements for orchestration and management, identifying gaps in current standards and best practices, and providing recommendations to fill in the gaps. Topics include: abstraction models and APIs, provisioning & configuration, operational management, interworking with existing OSS/BSS.
Software Architecture WG	Developing a classification system for network functions and defining the phases of network evolution towards a fully managed and orchestrated platform, including the impact on interfaces, legacy external functions, and management systems.
Reliability & Availability WG	Focusing on aspects related to robustness and resiliency in a virtualised network environment. The scope includes use case analysis and definition of the architecture framework, models, and requirements for network resiliency and service sustainability.
Performance & Portability EG (Proof of Concepts)	Assessing performance limitations of selected key virtualized network functions representative of different kinds of workloads. It will seek to identify best practices to optimize the performance of different workloads and investigate how to achieve predictable performance and isolation while assuring portability.
Security EG	Working to ensure that NFV designs in security from the start and that security accreditation bodies address NFV. Scope includes both information security and performance isolation. The group is working to engage accreditation institutions and those with global security expertise and will identify the security deltas introduced by NFV and assign activities to the relevant working groups.

API: application programming interface
BSS: business support system
OSS: operations support system

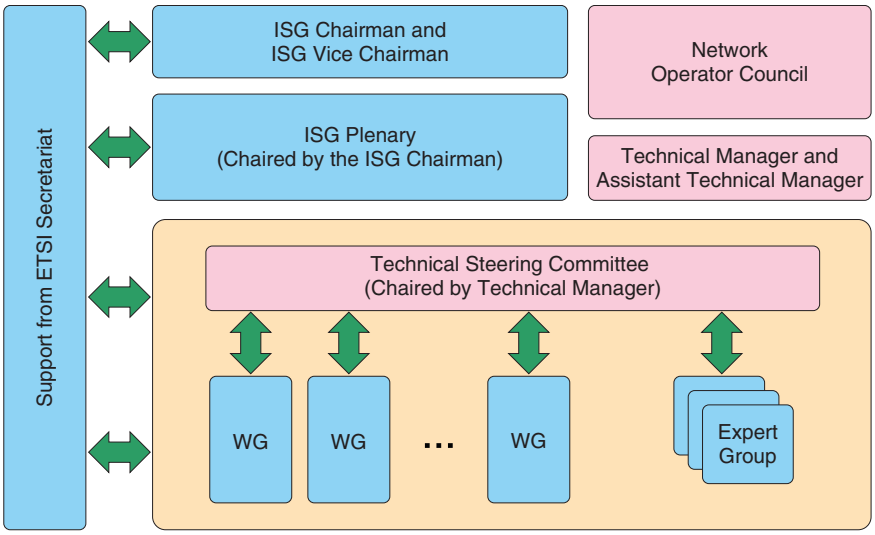


Fig. 3. ETSI NFV ISG organization and structure.

zations such as ONF (Open Network Forum) or IETF (Internet Engineering Task Force) are planning to have meetings around the same period as meetings planned by the NFV ISG, the schedule may be adjusted so that participants can attend all of the meetings, although the schedule is not always subject to change for this reason.

4. Procedures and current status

The documentation process in the NFV ISG is consensus based, meaning that all attendees need to

agree to the revisions for them to be included in a document. Otherwise, discussions will not go further until any objections are dropped. In these cases, the pending issues are described in the Editor's notes. The members who are most concerned with the issues are required to continue discussions at other opportunities and to later submit contributions intended to gather agreement. No voting has taken place in this process as of yet to determine which of various opposing proposals to adopt.

At the first plenary meeting, the NFV ISG agreed to form four WGs and two EGs. After each group initiated technical discussions, the members strongly recognized the need to have documents that would be used for reference in the discussions of each group. At the second plenary meeting, they decided to create reference documents, each of which describes one of the following four Work Items (WIs): NFV Use Cases [1], NFV Architectural Framework [4], Terminology for Main Concepts in NFV [5], and NFV Virtualisation Requirements [6]. The WGs and EGs continued their own discussions as long as the discussions did not relate to the WIs. For related technical issues, they halted discussions until the completion of the reference documents.

Documents of the NFV ISG are created as a Group Specification (GS) and then published upon being approved. These documents are made open and available to the public after the official publication.

The published documents are also sent to other standards organizations. It is highly expected that the discussions at these other organizations will go into further depth after the WGs and EGs release their respective GSs. So far, the four abovementioned WIs, as well as the WI titled Proof of Concepts (PoC), have already been documented as GSs, which are available on the ETSI NFV website.

5. Outlook

The publication of the five GSs will help promote the technical discussions held by each of the WGs and EGs, and more GSs will be published as they progress. We expect that the relevant standards organizations will deepen their discussions based on the GSs that the NFV ISG release. We also expect that the member companies and organizations of the NFV ISG will actively make PoC proposals because the PoC framework is formalized in the published GS. These activities are expected to strengthen the development of technology toward realizing commercial NFV services.

References

[1] ETSI GS NFV 001, Use Cases.
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf
[2] ETSI NFV ISG White Paper #1.
http://portal.etsi.org/NFV/NFV_White_Paper.pdf
[3] ETSI NFV ISG White Paper #2.
http://portal.etsi.org/NFV/NFV_White_Paper2.pdf
[4] ETSI GS NFV 002, Architectural Framework.
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf
[5] ETSI GS NFV 003, Terminology for Main Concepts in NFV.
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/003/01.01.01_60/gs_NFV003v010101p.pdf
[6] ETSI GS NFV 004, Virtualisation Requirements.
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/004/01.01.01_60/gs_NFV004v010101p.pdf
[7] ETSI GS NFV-PER 002, Proof of Concepts; Framework.
http://www.etsi.org/deliver/etsi_gs/NFV-PER/001_099/002/01.01.01_60/gs_NFV-PER002v010101p.pdf

Kazuaki Obana
Senior Research Engineer, Media Innovation Laboratory, NTT Network Innovation Laboratories.

He received the B.E. and M.E degrees in electrical engineering from Waseda University, Tokyo, in 1995 and 1997, respectively. After joining NTT Optical Network Systems Laboratories in 1997, he engaged in R&D of priority queuing by time and place information, a reverse proxy with a shaping function, and a fast transmitting system with multi-lanes. From 2008 to 2012, he worked on R&D of customer premises equipment in Promotion Project 1, NTT Cyber Solutions Laboratories. Since moving to NTT Network Innovation Laboratories in 2012, he has been engaged in R&D of programmable nodes.

Takeshi Kinoshita
Researcher, Media Innovation Laboratory, NTT Network Innovation Laboratories.

He received the B.E. and M.E. degrees in nuclear engineering from Kyoto University in 1994 and 1996, respectively. After joining NTT Optical Network Systems Laboratories in 1996, he studied optical fiber communications systems in access networks and their management. He then moved to the R&D center of NTT WEST, where he was responsible for developing and introducing commercial services, including broadband internet access, IP v4/v6 VPN, and wide area Ethernet. He also worked on reducing energy consumption of datacenter components such as servers, communications equipment, and air-conditioning systems. His current research involves virtualisation of network functions and its implementation.

Katsuhiro Shimano
Senior Engineer, Supervisor, NTT Network Innovation Laboratories.

He received the B.S. degree in physics from Waseda University, Tokyo, in 1991 and the M.S. degree in physics from the University of Tokyo in 1993. Since joining NTT in 1993, he has studied optical networks and network management and related areas such as optical network management systems, GMPLS, and traffic engineering. He also spent time at the headquarters working on NGN network architecture from the first phase of construction. Recently, he has been leading the research on SDN and network virtualisation at NTT Network Innovation Laboratories.