Computer Networks 92 (2015) 380–395

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Toward dynamic virtualized network services in telecom operator networks

Ivano Cerrato [a], Alex Palesandro [a], Fulvio Risso [a,*], Marc Suñé [b], Vinicio Vercellone [c], Hagen Woesner [b]

[a] Department of Computer and Control Engineering, Politecnico di Torino, Torino, Italy
[b] Berlin Institute for Software Defined Networks GmbH, Berlin, Germany
[c] Telecom Italia lab, Torino, Italy

ARTICLE INFO

Article history:
Received 17 November 2014
Revised 29 May 2015
Accepted 25 September 2015
Available online 9 October 2015

Keywords:
NFV
SDN
Service graph
Forwarding graph
Virtual network functions
Network orchestration

ABSTRACT

NFV and SDN are nowadays seen as a solid opportunity by telecom operators to reduce costs while at the same time providing new and better services. Recently, the Unify project proposed a multi-layered architecture that, leveraging different levels of abstraction, can orchestrate and deploy generic network services on the physical infrastructure of the telecom operator. In this paper, we exploit such an architecture to deliver end-to-end generic services in presence of multiple concurring players (e.g. network operator, end-users), leveraging a new simple data model. Particularly, we propose a description-based approach allowing the deployment agile, implementation-independent and high-level network services over a distributed set of resources. The resulting data model can abstract generic services, including both middlebox-based (e.g., firewalls, NATs, etc.) and traditional LAN-based ones (e.g., a BitTorrent client). Finally, two distinct prototypes, originated by different design principles, are implemented in order to validate our proposal with the aim of demonstrating the adaptability of our approach to different contexts.

1. Introduction

The way network services are delivered has dramatically changed in the last few years thanks to the Network Functions Virtualization (NFV) paradigm, which allows network services to experiment the same degree of flexibility and agility already available in the cloud computing world. In fact, NFV proposes to transform the network functions that today run on dedicated appliances (e.g., firewall, WAN accelerator) into a set of software images that can be consolidated into high-volume standard servers, hence replacing dedicated middleboxes with virtual machines implementing those Virtual Network Functions (VNFs). Thanks to their software-based nature, VNFs could be potentially deployed on any node with computing capabilities located everywhere in the network, ranging from the home gateway installed in the customer premises to the data center servers [1,2].

NFV is mainly seen as a technology targeting network operators, which can exploit the power of the IT virtualization (e.g., cloud and datacenters) to deliver network services with unprecedented agility and efficiency and at the same time achieve a reduction of OPEX and CAPEX. However, also end users (e.g., xDSL customers) can benefit from NFV, as this would enable them to customize the set of services that are active on their Internet connection. But, while NFV currently focuses mostly on middlebox-based applications (e.g., NAT, firewall), end users are probably more oriented to services based on traditional network facilities (e.g., L2 broadcast domains), which receive less consideration in the NFV world.

* Corresponding author. Tel.: +39 011 0907008.
E-mail address: fulvio.risso@polito.it (F. Risso).

http://dx.doi.org/10.1016/j.comnet.2015.09.028
1389-1286/

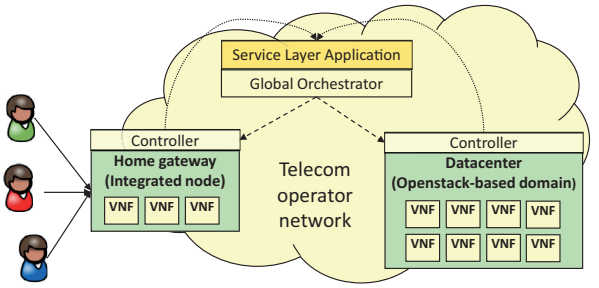

Fig. 1. Deployment of virtual network functions on the telecom operator network.

Motivated by the growing interest, e.g., of telecom operators, in extending the functionalities of Customer Premise Equipments (CPEs) in order to deliver new and improved services to the users [3–6], this paper presents a solution that is oriented to deliver *generic* network services that can be selected by *multiple players*. Particularly, our proposal enables also the *dynamic* instantiation of *per-user* network services on the large infrastructure of the telecom operators, possibly starting from the home gateway to the data center, as depicted in Fig. 1. Our solution enables several players (e.g., telecom operator, end users, etc.) to cooperatively define the network services; moreover, it is general enough to support both traditional middlebox functions as well as traditional host-based network services. For example, a customer can define its own network service by asking for a transparent firewall and a BitTorrent client, while the network operator complements those applications by instantiating a DHCP and a NAT service.[1]

In our solution, the entire network infrastructure is controlled by a service logic that performs the identification of the user that is connecting to the network itself, following the approach proposed in [7]. Upon a successful identification, the proper set of network functions chosen by the user is instantiated in one of the nodes (possibly, even the home gateway) available on the telecom operator network, and the physical infrastructure is configured to deliver the user traffic to the above set of VNFs.

The paper describes the service-oriented layered architecture to achieve those objectives, modeled after the one proposed by the Unify project [8,9], and a possible set of data models that are used to describe and instantiate the requested network services starting from an high-level and user-friendly view of the service. The high-level description is then converted into a set of primitives (e.g., virtual machines, virtual links) that are used to instantiate the service on the physical infrastructure. Moreover, it presents two possible implementations of the nodes of the infrastructure layer on which the service is actually deployed. Particularly, we explored two solutions that are based on different technologies, with different requirements in terms of hardware resources. The first is based on the OpenStack open-source framework and it is more appropriate to be integrated in (existing) cloud environments; the second exploits mostly dedicated software and it is more oriented to the domestic/embedded segment (e.g., resource-constrained CPEs).

The remainder of this paper is structured as follows. Section 2 provides an overview of the related works, while Section 3 introduces an architecture to deploy general network services across the whole network under the control of the telecom operator (as shown in Fig. 1). Section 4 details some formalisms expressing the service to be deployed, which are then exploited to solve the challenges arising from our use case, as discussed in Section 5. Section 6 details the preliminary implementation of the architecture, which is then validated in Section 7, both in terms of functionalities and performance. Finally, Section 8 concludes the paper and provides some plans for the future.

2. Related work

At least three FP7 EU-funded projects focusing on the integration of the NFV and SDN concepts (UNIFY [10], T-NOVA [11] and SECURED [12]) started recently. Particularly, the first one aims at delivering an end-to-end service that can be deployed everywhere in the telecom operator network, starting from the points of presence at the edge of the network to the datacenter, by exploiting SDN and NFV technologies. Similarly, T-NOVA proposes an equivalent approach that puts more emphasis on the target of providing a uniform platform for third-party VNF developers, while SECURED aims at offloading personal security applications into a programmable device at the edge of the network. An SDN-based service-oriented architecture has been proposed also in [13,14], which enables to deliver middlebox-based services to user devices, leveraging Service Function Chaining and SDN concepts.

From the industry side, the IETF Service Function Chaining (SFC) [15] working group aims at defining a model to describe and instantiate network services, which includes an abstract set of VNFs, their connections and ordering relations, provided with a set of QoS constraints. Similarly, the European Telecommunications Standards Institute (ETSI) started the Industry Specification Group for NFV [16], which aims at developing the required standards and sharing their experiences of NFV development and early implementation. Based on the ETSI proposal, the Open Platform for NFV (OPNFV) project [17] aims at accelerating the evolution of NFV by defining an open source reference platform for Virtual Network Functions.

The problem of CPE virtualization, which represents one of the possible use cases of our architecture, is investigated in several papers (e.g., [3–6]); however they have a more limited scope as they do not foresee the possibility to instantiate the service across an highly distributed infrastructure and focus on more technological-oriented aspects.

Finally, the OpenStack [18] community is aware of the possibility to use that framework to deliver NFV services as well, as shown by the new requirements targeting traffic steering and SFC primitives [19,20]; in fact, we rely on some preliminary implementation of those functions [21] in order to build our prototype.

[1] It is worth pointing out that, in this paper, we assume that end users are only enabled to select VNFs *trusted* by the operator. The case in which they can deploy *untrusted* VNFs (e.g., implemented by the end users themselves) would in fact open security issues that are beyond the scope of this work.