NFVRG
Internet-Draft
Intended status: Informational
Expires: September 19, 2016

CJ. Bernardos
UC3M
A. Rahman
JC. Zuniga
InterDigital
LM. Contreras
P. Aranda
TID

March 18, 2016

Gap Analysis on Network Virtualization Activities
draft-irtf-nfvrg-gaps-network-virtualization-00

Abstract

The main goal of this document is to serve as a survey of the different efforts that have been taken and are currently taking place at IETF and IRTF in regards to network virtualization, automation and orchestration, putting them into context considering efforts by other SDOs, and identifying current gaps and challenges that can be tackled at IETF or researched at the IRTF.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 19, 2016.

Table of Contents

1. Introduction

The telecommunications sector is experiencing a major revolution that will shape the way networks and services are designed and deployed for the next decade. We are witnessing an explosion in the number of applications and services demanded by users, which are now really capable of accessing them on the move. In order to cope with such a

demand, some network operators are looking at the cloud computing paradigm, which enables a potential reduction of the overall costs by outsourcing communication services from specific hardware in the operator's core to server farms scattered in datacenters. These services have different characteristics if compared with conventional IT services that have to be taken into account in this cloudification process. Also the transport network is affected in that it is evolving to a more sophisticated form of IP architecture with trends like separation of control and data plane traffic, and more fine-grained forwarding of packets (beyond looking at the destination IP address) in the network to fulfill new business and service goals.

Virtualization of functions also provides operators with tools to deploy new services much faster, as compared to the traditional use of monolithic and tightly integrated dedicated machinery. As a natural next step, mobile network operators need to re-think how to evolve their existing network infrastructures and how to deploy new ones to address the challenges posed by the increasing customers' demands, as well as by the huge competition among operators. All these changes are triggering the need for a modification in the way operators and infrastructure providers operate their networks, as they need to significantly reduce the costs incurred in deploying a new service and operating it. Some of the mechanisms that are being considered and already adopted by operators include: sharing of network infrastructure to reduce costs, virtualization of core servers running in data centers as a way of supporting their load-aware elastic dimensioning, and dynamic energy policies to reduce the monthly electricity bill. However, this has proved to be tough to put in practice, and not enough. Indeed, it is not easy to deploy new mechanisms in a running operational network due to the high dependency on proprietary (and sometime obscure) protocols and interfaces, which are complex to manage and often require configuring multiple devices in a decentralized way.

Network Function Virtualization (NFV) and Software Defined Networking (SDN) are changing the way the telecommunications sector will deploy, extend and operate their networks. This document provides a survey of the different efforts that have taken and are currently taking place at IETF and IRTF in regards of network virtualization, looking at how they relate to the ETSI NFV ISG, ETSI MEC ISG and ONF architectural frameworks. Based on this analysis, we also go a step farther, identifying which are the potential work areas where IETF/ IRTF can work on to complement the complex network virtualization map of technologies being standardized today.

2. Terminology

The following terms used in this document are defined by the ETSI NVF ISG, the ONF and the IETF:

Application Plane - The collection of applications and services that program network behavior.

Control Plane (CP) - The collection of functions responsible for controlling one or more network devices. CP instructs network devices with respect to how to process and forward packets. The control plane interacts primarily with the forwarding plane and, to a lesser extent, with the operational plane.

Forwarding Plane (FP) - The collection of resources across all network devices responsible for forwarding traffic.

Management Plane (MP) - The collection of functions responsible for monitoring, configuring, and maintaining one or more network devices or parts of network devices. The management plane is mostly related to the operational plane (it is related less to the forwarding plane).

NFV Infrastructure (NFVI): totality of all hardware and software components which build up the environment in which VNFs are deployed

NFV Management and Orchestration (NFV-MANO): functions collectively provided by NFVO, VNFM, and VIM.

NFV Orchestrator (NFVO): functional block that manages the Network Service (NS) lifecycle and coordinates the management of NS lifecycle, VNF lifecycle (supported by the VNFM) and NFVI resources (supported by the VIM) to ensure an optimized allocation of the necessary resources and connectivity.

OpenFlow protocol (OFP): allowing vendor independent programming of control functions in network nodes.

Operational Plane (OP) - The collection of resources responsible for managing the overall operation of individual network devices.

Service Function Chain (SFC): for a given service, the abstracted view of the required service functions and the order in which they are to be applied. This is somehow equivalent to the Network Function Forwarding Graph (NF-FG) at ETSI.

Service Function Path (SFP): the selection of specific service function instances on specific network nodes to form a service graph through which an SFC is instantiated.

virtual EPC (vEPC): control plane of 3GPPs EPC operated on NFV framework (as defined by [I-D.matsushima-stateless-uplane-vepc]).

Virtualized Infrastructure Manager (VIM): functional block that is responsible for controlling and managing the NFVI compute, storage and network resources, usually within one operator's Infrastructure Domain.

Virtualized Network Function (VNF): implementation of a Network Function that can be deployed on a Network Function Virtualisation Infrastructure (NFVI).

Virtualized Network Function Manager (VNFM): functional block that is responsible for the lifecycle management of VNF.

3. Background

3.1. Network Function Virtualization

The ETSI ISG NFV is a working group which, since 2012, aims to evolve quasi-standard IT virtualization technology to consolidate many network equipment types into industry standard high volume servers, switches, and storage. It enables implementing network functions in software that can run on a range of industry standard server hardware and can be moved to, or loaded in, various locations in the network as required, without the need to install new equipment. To date, ETSI NFV is by far the most accepted NFV reference framework and architectural footprint [etsi_nvf_whitepaper]. The ETSI NFV framework architecture framework is composed of three domains (Figure 1):

- Virtualized Network Function, running over the NFVI.
- NFV Infrastructure (NFVI), including the diversity of physical resources and how these can be virtualized. NFVI supports the execution of the VNFs.
- NFV Management and Orchestration, which covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs. NFV Management and Orchestration focuses on all virtualization specific management tasks necessary in the NFV framework.

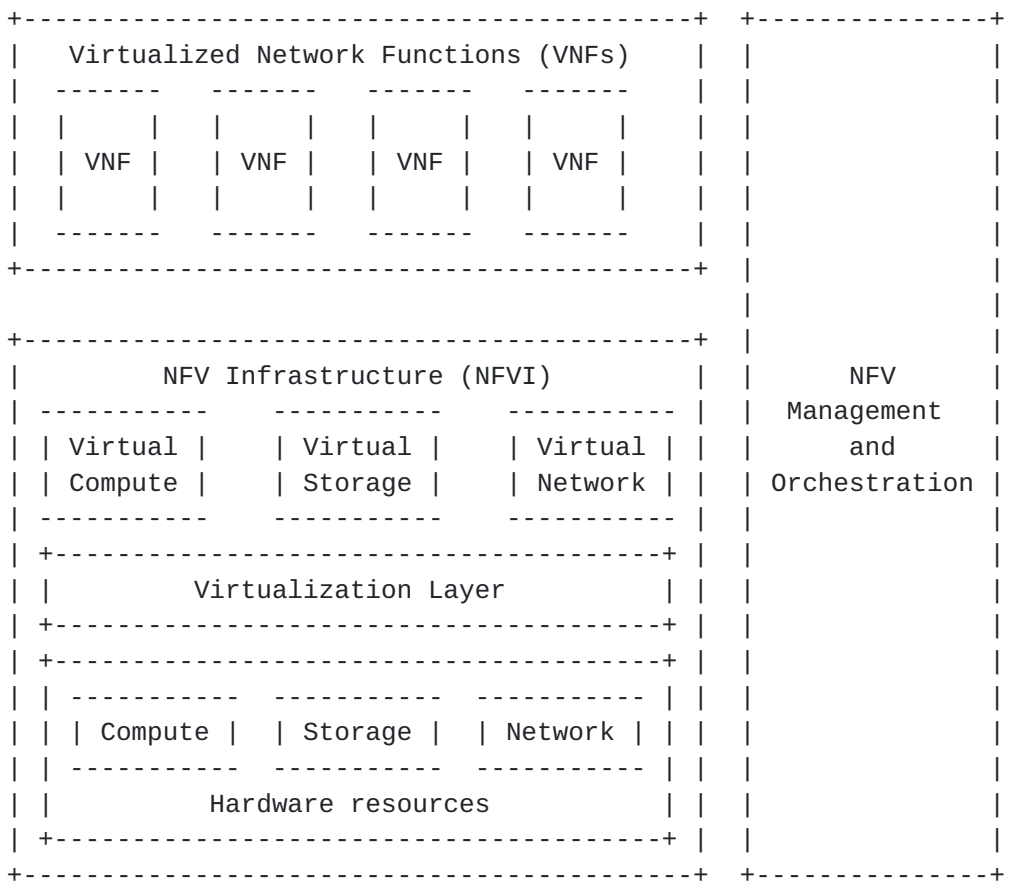

Figure 1: ETSI NFV framework

The NFV architectural framework identifies functional blocks and the main reference points between such blocks. Some of these are already present in current deployments, whilst others might be necessary additions in order to support the virtualization process and consequent operation. The functional blocks are (Figure 2):

- Virtualized Network Function (VNF).
- Element Management (EM).
- NFV Infrastructure, including: Hardware and virtualized resources, and Virtualization Layer.
- Virtualized Infrastructure Manager(s) (VIM).
- NFV Orchestrator.
- VNF Manager(s).
- Service, VNF and Infrastructure Description.

o Operations and Business Support Systems (OSS/BSS).

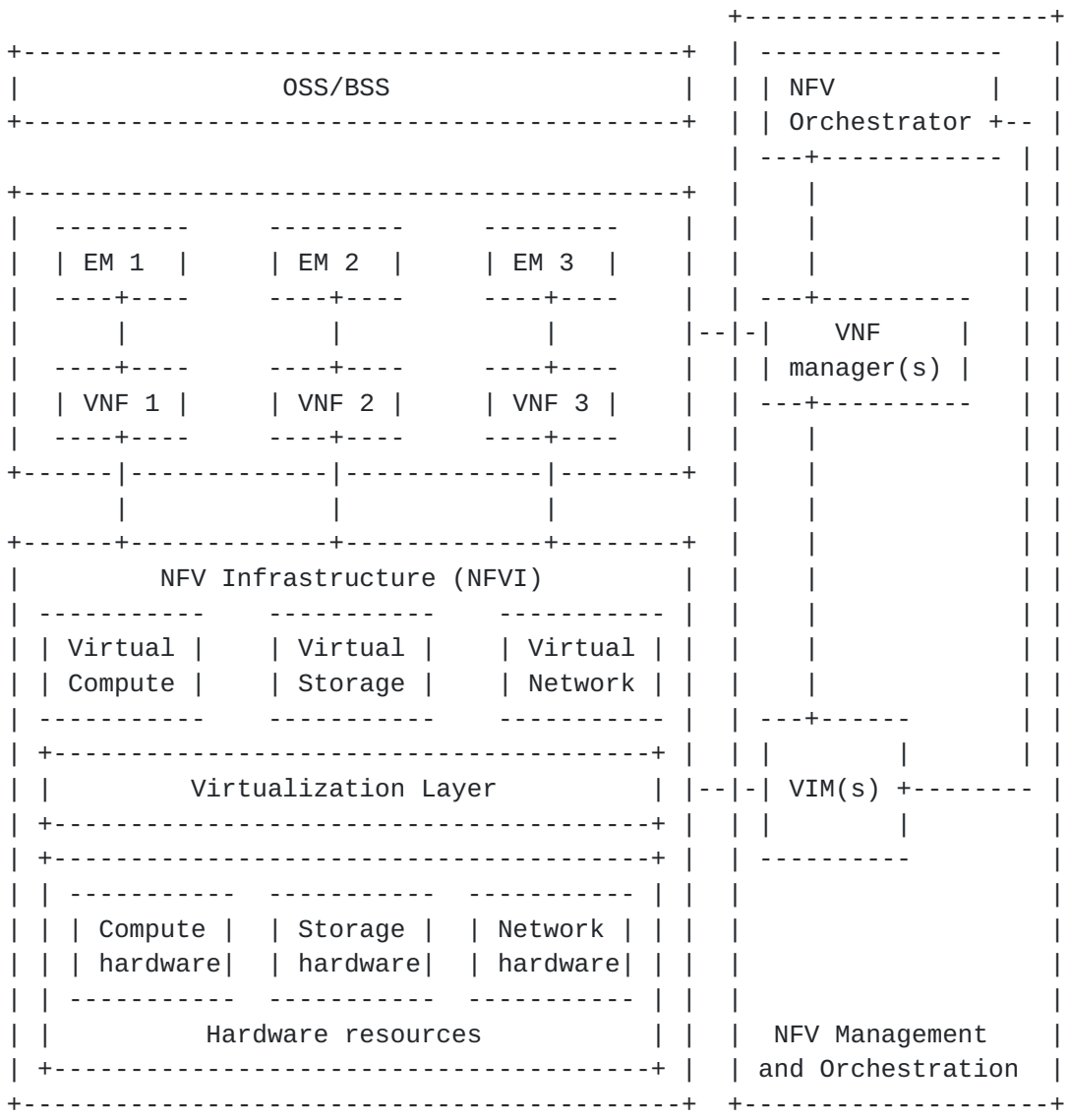

Figure 2: ETSI NFV reference architecture

3.2. Software Defined Networking

The Software Defined Networking (SDN) paradigm pushes the intelligence currently residing in the network elements to a central controller implementing the network functionality through software. In contrast to traditional approaches, in which the network's control plane is distributed throughout all network devices, with SDN the control plane is logically centralized. In this way, the deployment of new characteristics in the network no longer requires of complex and costly changes in equipment or firmware updates, but only a change in the software running in the controller. The main advantage

of this approach is the flexibility it provides operators with to manage their network, i.e., an operator can easily change its policies on how traffic is distributed throughout the network.

The most visible of the SDN protocol stacks is the OpenFlow protocol (OFP), which is maintained and extended by the Open Network Foundation (ONF: https://www.opennetworking.org/). Originally this protocol was developed specifically for IEEE 802.1 switches conforming to the ONF OpenFlow Switch specification. As the benefits of the SDN paradigm have reached a wider audience, its application has been extended to more complex scenarios such as Wireless and Mobile networks. Within this area of work, the ONF is actively developing new OFP extensions addressing three key scenarios: (i) Wireless backhaul, (ii) Cellular Evolved Packet Core (EPC), and (iii) Unified access and management across enterprise wireless and fixed networks.

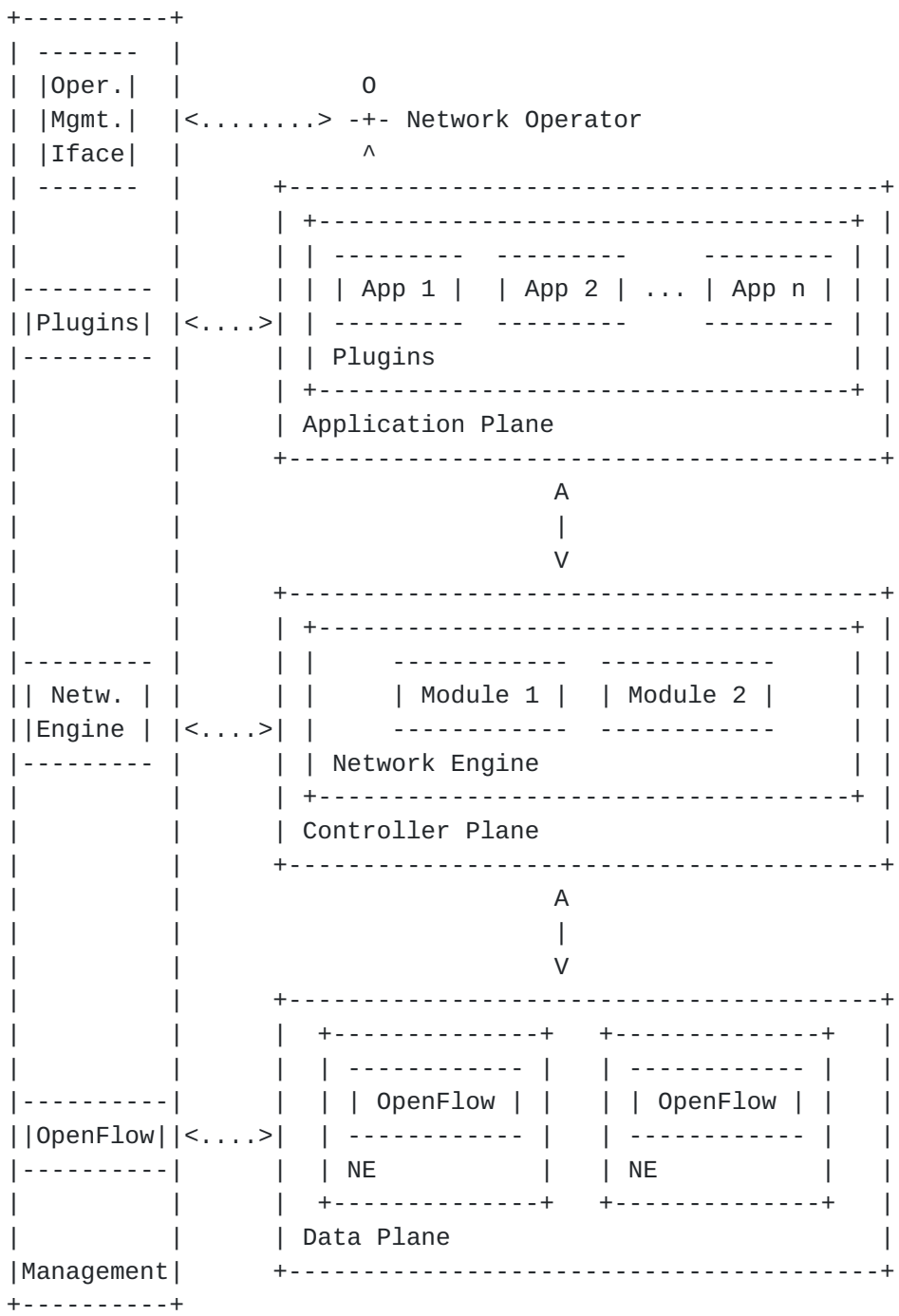

Figure 3: High level SDN ONF architecture

Figure 3 shows the blocks and the functional interfaces of the ONF architecture, which comprises three planes: Data, Controller, and Application. The Data plane comprehends several Network Entities (NE), which expose their capabilities toward the Controller plane via a Southbound API. The Controller plane includes several cooperating modules devoted to the creation and maintenance of an abstracted

resource model of the underneath network. Such model is exposed to the applications via a Northbound API where the Application plane comprises several applications/services, each of which has exclusive control of a set of exposed resources.

The Management plane spans its functionality across all planes performing the initial configuration of the network elements in the Data plane, the assignment of the SDN controller and the resources under its responsibility. In the Controller plane, the Management needs to configure the policies defining the scope of the control given to the SDN applications, to monitor the performance of the system, and to configure the parameters required by the SDN controller modules. In the Application plane, Management configures the parameters of the applications and the service level agreements. In addition to the these interactions, the Management plane exposes several functions to network operators which can easily and quickly configure and tune the network at each layer.

The SDNRG has documented a reference layer model in RFC7426 [RFC7426], which is reproduced in Figure 4. This model structures SDN in planes and layers which are glued together by different abstraction layers. This architecture differentiates between the control and the management planes and provides for differentiated southbound interfaces (SBIs).

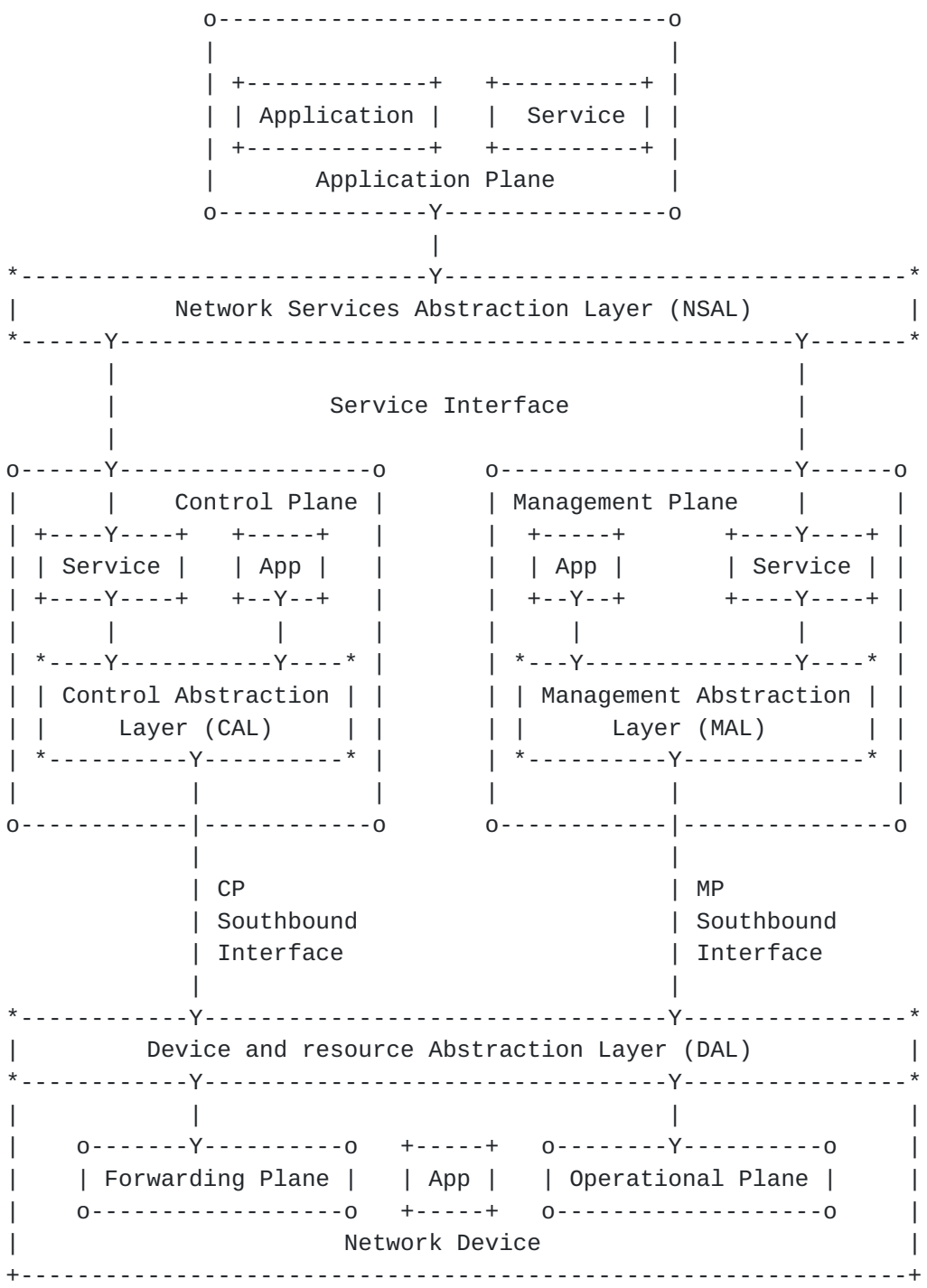

Figure 4: SDN Layer Architecture

3.3. Mobile Edge Computing

Mobile Edge Computing capabilities deployed in the edge of the mobile network can facilitate the efficient and dynamic provision of services to mobile users. The ETSI ISG MEC working group, operative

from end of 2014, intends to specify an open environment for integrating MEC capabilities with service providers networks, including also applications from 3rd parties. These distributed computing capabilities will make available IT infrastructure as in a cloud environment for the deployment of functions in mobile access networks. It can be seen then as a complement to both NFV and SDN.

3.4. IEEE 802.1CF (OmniRAN)

The IEEE 802.1CF Recommended Practice specifies an access network, which connects terminals to their access routers, utilizing technologies based on the family of IEEE 802 Standards (e.g., 802.3 Ethernet, 802.11 Wi-Fi, etc.). The specification defines an access network reference model, including entities and reference points along with behavioral and functional descriptions of communications among those entities.

The goal of this project is to help unifying the support of different interfaces, enabling shared network control and use of software defined network (SDN) principles, thereby lowering the barriers to new network technologies, to new network operators, and to new service providers.

3.5. Distributed Management Task Force

The DMTF is an industry standards organization working to simplify the manageability of network-accessible technologies through open and collaborative efforts by some technology companies. The DMTF is involved in the creation and adoption of interoperable management standards, supporting implementations that enable the management of diverse traditional and emerging technologies including cloud, virtualization, network and infrastructure.

There are several DMTF initiatives that are relevant to the network virtualization area, such as the Open Virtualization Format (OVF), for VNF packaging; the Cloud Infrastructure Management Interface (CIM), for cloud infrastructure management; the Network Management (NETMAN), for VNF management; and, the Virtualization Management (VMAN), for virtualization infrastructure management.

3.6. Open Source initiatives

The Open Source community is especially active in the area of network virtualization. We next summarize some of the active efforts:

- OpenStack. OpenStack is a free and open-source cloud-computing software platform. OpenStack software controls large pools of

compute, storage, and networking resources throughout a datacenter, managed through a dashboard or via the OpenStack API.

- OpenDayLight. OpenDaylight (ODL) is a highly available, modular, extensible, scalable and multi-protocol controller infrastructure built for SDN deployments on modern heterogeneous multi-vendor networks. It provides a model-driven service abstraction platform that allows users to write apps that easily work across a wide variety of hardware and southbound protocols.

- ONOS. The ONOS (Open Network Operating System) project is an open source community hosted by The Linux Foundation. The goal of the project is to create a software-defined networking (SDN) operating system for communications service providers that is designed for scalability, high performance and high availability.

- OpenContrail. OpenContrail is an Apache 2.0-licensed project that is built using standards-based protocols and provides all the necessary components for network virtualization-SDN controller, virtual router, analytics engine, and published northbound APIs. It has an extensive REST API to configure and gather operational and analytics data from the system.

- OPNFV. OPNFV is a carrier-grade, integrated, open source platform to accelerate the introduction of new NFV products and services. By integrating components from upstream projects, the OPNFV community aims at conducting performance and use case-based testing to ensure the platform's suitability for NFV use cases. The scope of OPNFV's initial release is focused on building NFV Infrastructure (NFVI) and Virtualized Infrastructure Management (VIM) by integrating components from upstream projects such as OpenDaylight, OpenStack, Ceph Storage, KVM, Open vSwitch, and Linux. These components, along with application programmable interfaces (APIs) to other NFV elements form the basic infrastructure required for Virtualized Network Functions (VNF) and Management and Network Orchestration (MANO) components. OPNFV's goal is to increase performance and power efficiency; improve reliability, availability, and serviceability; and deliver comprehensive platform instrumentation.

- OSM. Open Source Mano (OSM) is an ETSI-hosted project to develop an Open Source NFV Management and Orchestration (MANO) software stack aligned with ETSI NFV. OSM is based on components from previous projects, such Telefonica's OpenMANO or Canonical's Juju, among others.

- OpenBaton. OpenBaton is a ETSI NFV compliant Network Function Virtualization Orchestrator (NFVO). OpenBaton was part of the

OpenSDNCore project started with the objective of providing a compliant implementation of the ETSI NFV specification.

Among the main areas that are being developed by the former open source activities that related to network virtualization research, we can highlight: policy-based resource management, analytics for visibility and orchestration, service verification with regards to security and resiliency.

4. Network Virtualization at IETF/IRTF

4.1. SDN RG

The SDNRG provides the grounds for an open-minded investigation of Software Defined Networking. They aim at identifying approaches that can be defined and used in the near term as well as the research challenges in the field. As such, they SDNRG will not define standards, but provide inputs to standards defining and standards producing organizations.

It is working on classifying SDN models, including definitions and taxonomies. It is also studying complexity, scalability and applicability of the SDN model. Additionally, the SDNRG is working on network description languages (and associated tools), abstractions and interfaces. They also investigate the verification of correct operation of network or node function.

The SDNRG has produced a reference layer model RFC7426 [RFC7426], which structures SDNs in planes and layers which are glued together by different abstraction layers. This architecture differentiates between the control and the management planes and provides for differentiated southbound interfaces (SBIs).

4.2. SFC WG

Current network services deployed by operators often involve the composition of several individual functions (such as packet filtering, deep packet inspection, load balancing). These services are typically implemented by the ordered combination of a number of service functions that are deployed at different points within a network, not necessary on the direct data path. This requires traffic to be steered through the required service functions, wherever they are deployed.

For a given service, the abstracted view of the required service functions and the order in which they are to be applied is called a Service Function Chain (SFC), which is called Network Function Forwarding Graph (NF-FG) in ETSI. An SFC is instantiated through

selection of specific service function instances on specific network nodes to form a service graph: this is called a Service Function Path (SFP). The service functions may be applied at any layer within the network protocol stack (network layer, transport layer, application layer, etc.).

The SFC working group is working on an architecture for service function chaining that includes the necessary protocols or protocol extensions to convey the Service Function Chain and Service Function Path information to nodes that are involved in the implementation of service functions and Service Function Chains, as well as mechanisms for steering traffic through service functions.

In terms of actual work items, the SFC WG is chartered to deliver: (i) a problem statement document [RFC7498], (ii) an architecture document [RFC7665], (iii) a service-level data plane encapsulation format (the encapsulation should indicate the sequence of service functions that make up the Service Function Chain, specify the Service Function Path, and communicate context information between nodes that implement service functions and Service Function Chains), and (iv) a document describing requirements for conveying information between control or management elements and SFC implementation points.

Potential gap: as stated in the SFC charter, any work on the management and configuration of SFC components related to the support of Service Function Chaining will not be done yet, until better understood and scoped. This part is of special interest for operators and would be required in order to actually put SFC mechanisms into operation.

Potential gap: redundancy and reliability mechanisms are currently not dealt with by any WG in the IETF. While this has been the main goal of the VNFpool BoF efforts, it still remains un-addressed.

4.3. NVO3 WG

The Network Virtualization Overlays (NVO3) WG is developing protocols that enable network virtualization overlays within large Data Center (DC) environments. Specifically NVO3 assumes an underlying physical Layer 3 (IP) fabric on which multiple tenant networks are virtualized on top (i.e. overlays). With overlays, data traffic between tenants is tunneled across the underlying DC's IP network. The use of tunnels provides a number of benefits by decoupling the network as viewed by tenants from the underlying physical network across which they communicate [I-D.ietf-nvo3-arch].

Potential gap: It would be worthwhile to see if some of the specific approaches developed in this WG (e.g. overlays, traffic isolation, VM

migration) can be applied outside the DC, and specifically if they can be applicable to network virtualization (NFV). These approaches would be most relevant to the ETSI Network Function Virtualization Infrastructure (NFVI), and the Virtualized Infrastructure Manager part of the MANO.

4.4. DMM WG

The Distributed Mobility Management (DMM) WG is looking at solutions for IP networks that enable traffic between mobile and correspondent nodes taking an optimal route, preventing some of the issues caused by the use of centralized mobility solutions, which anchor all the traffic at a given node (or a very limited set of nodes). The DMM WG is considering the latest developments in mobile networking research and operational practices (i.e., flattening network architectures, the impact of virtualization, new deployment needs as wireless access technologies evolve in the coming years) and aims at describing how distributed mobility management addresses the new needs in this area better than previously standardized solutions.

Although network virtualization is not the main area of the DMM work, the impact of SDN and NFV mechanisms is clear on the work that is currently being done in the WG. One example is architecture defined for the virtual Evolved Packet Core (vEPC) in [I-D.matsushima-stateless-uplane-vepc]. Here, the authors describe a particular realization of the vEPC concept, which is designed to support NFV. In the defined architecture, the user plane of EPC is decoupled from the control-plane and uses routing information to forward packets of mobile nodes. This proposal does not modify the signaling of the EPC control plane, although the EPC control plane runs on an hypervisor.

Potential gap: in a vEPC/DMM context, how to run the EPC control plane on NFV.

The DMM WG is also looking at ways to supporting the separation of the Control-Plane for mobility- and session management from the actual Data-Plane [I-D.ietf-dmm-fpc-cpdp]. The protocol semantics being defined abstract from the actual details for the configuration of Data-Plane nodes and apply between a Client function, which is used by an application of the mobility Control-Plane, and an Agent function, which is associated with the configuration of Data-Plane nodes according to the policies issued by the mobility Control-Plane.

Potential gap: the actual mappings between these generic protocol semantics and the configuration commands required on the data plane network elements are not in the scope of this document, and are

therefore a potential gap that will need to be addressed (e.g., for OpenFlow switches).

4.5. I2RS WG

The Interface to the Routing System (I2RS) WG is developing a high-level architecture that describes the basic building-blocks to access the routing system through a set of protocol-based control or management interfaces. This architecture, as described in [I-D.ietf-i2rs-architecture], comprises an I2RS Agent as a unified interface that is accessed by I2RS clients using the I2RS protocol. The client is controlled by one or more network applications and accesses one or more agents, as shown in the following figure:

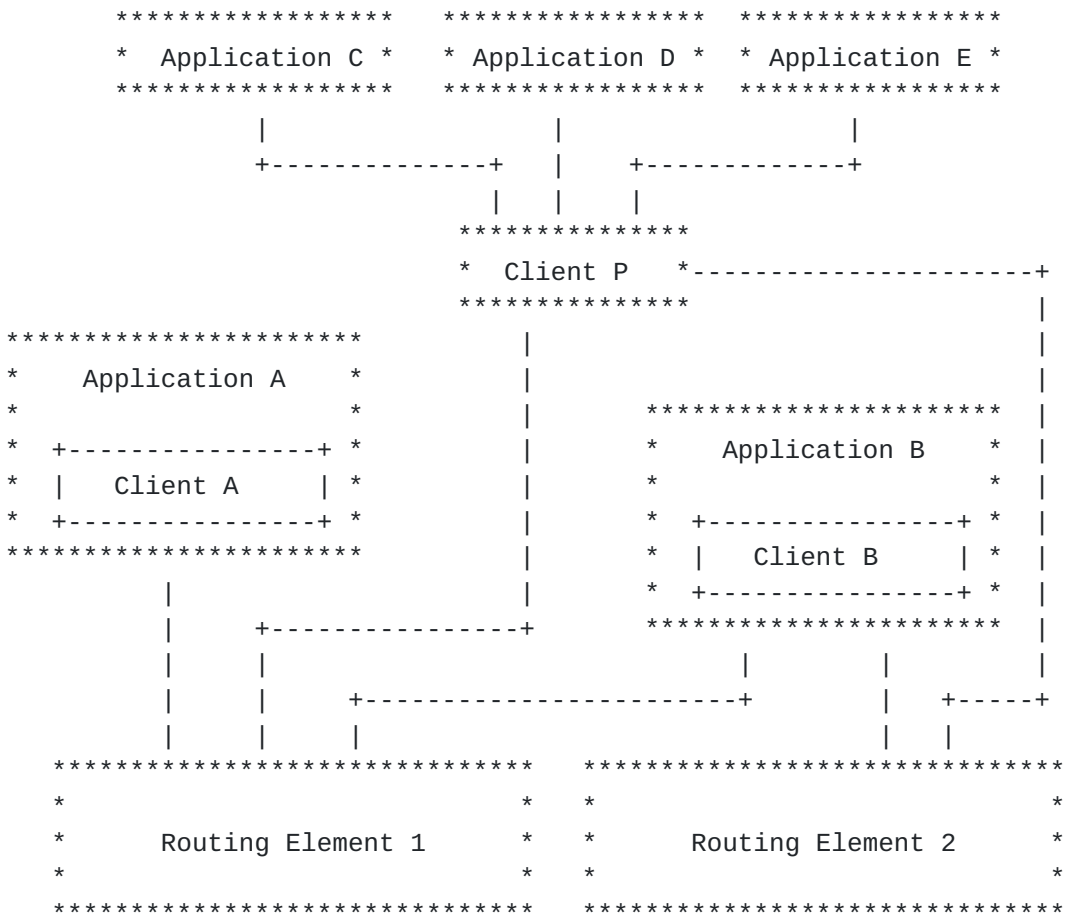

Figure 5: High level I2RS architecture

Routing elements consist of an agent that communicates with the client or clients driven by the applications and accesses the different subsystems in the element as shown in the following figure:

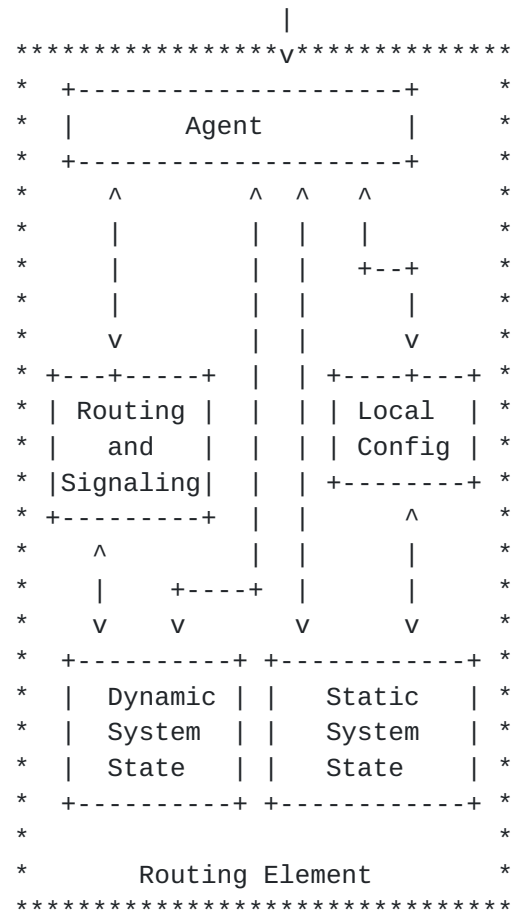

Figure 6: Architecture of a routing element

The I2RS architecture proposes to use model-driven APIs. Services can correspond to different data-models and agents can indicate which model they support.

Potential gap: network virtualization is not the main aim of the I2RS WG. However, they provide an infrastructure that can be part of an SDN deployment.

4.6. BESS WG

BGP is already used as a protocol for provisioning and operating Layer-3 (routed) Virtual Private Networks (L3VPNs). The BGP Enabled Services (BESS) working group is responsible for defining, specifying, and extending network services based on BGP. In particular, the working group will work on the following services:

- BGP-enabled VPN solutions for use in the data center networking. This work includes consideration of VPN scaling issues and mechanisms applicable to such environments.

- Extensions to BGP-enabled VPN solutions for the construction of virtual topologies in support of services such as Service Function Chaining.

Potential gap: The most relevant activity in BESS that would be worthwhile to investigate for relevance to network virtualization (NFV) is the extensions to BGP-enabled VPN solutions to support of Service Function Chaining [I-D.rfernando-bess-service-chaining].

4.7. BM WG

The Benchmarking Methodology Working Group (BMWG) provides recommendations concerning the key performance characteristics of internetworking technologies, or benchmarks for network devices, systems, and services. The scope of BMWG includes benchmarks for the management, control, and forwarding planes, and is.

The main distinguishing characteristic of BMWG from other IETF measurement initiatives like the IPPM WG is that BMWG is limited to characterization of implementations using controlled stimuli in a lab environment. The BMWG does not attempt to produce benchmarks for live, operational networks.

As part of the tasks of the BMWG, it is explicitly tasked to develop benchmarks and methodologies for VNF and related infrastructure benchmarking, Benchmarking Methodologies have reliably characterized many physical devices. This work item extends and enhances the methods to virtual network functions (VNF) and their unique supporting infrastructure. The first deliverable from this activity mentioned in the charter of the WG is a document [I-D.ietf-bmwg-virtual-net] that considers the new benchmarking space to ensure that common issues are recognized from the start, using background materials from industry and SDOs (e.g., IETF, ETSI NFV). This document investigates the additional methodological considerations necessary when benchmarking VNFs instantiated and hosted in general-purpose hardware. The approach is to benchmark physical and virtual network functions in the same way when possible, thereby allowing direct comparison. Also defining benchmarking combinations of physical and virtual devices in a System Under Test.

Benchmarks for platform capacity and performance characteristics of virtual routers, switches, and related components will be also addressed, including comparisons between physical and virtual network functions. In many cases, the traditional benchmarks should be applicable to VNFs, but the lab set-ups, configurations, and measurement methods will likely need to be revised or enhanced.

There are additional documents of the BMWG relevant to the virtualization area, such as: [I-D.ietf-bmwg-sdn-controller-benchmark-term], [I-D.ietf-bmwg-sdn-controller-benchmark-meth], [I-D.kim-bmwg-ha-nfvi] and [I-D.vsperf-bmwg-vswitch-opnfv].

4.8. TEAS WG

Transport network infrastructure provides end-to-end connectivity for networked applications and services. Network virtualization facilitates effective sharing (or 'slicing') of physical infrastructure by representing resources and topologies via abstractions, even in a multi-administration, multi-vendor, multi-technology environment. In this way, it becomes possible to operate, control and manage multiple physical networks elements as single virtualized network. The users of such virtualized network can control the allocated resources in an optimal and flexible way, better adapting to the specific circumstances of higher layer applications.

Abstraction and Control of Transport Networks (ACTN) intends to define methods and capabilities for the deployment and operation of transport network resources [I-D.ceccarelli-teas-actn-framework]. This activity is currently being carried out within the Traffic Engineering Architecture and Signaling (TEAS) WG.

Several use cases are being proposed for both fixed and mobile scenarios [I-D.leeking-teas-actn-problem-statement].

Potential gap: Several use cases in ACTN are relevant to network virtualization (NFV) in mobile environments. Control of multi-tenant mobile backhaul transport networks, mobile virtual network operation, etc, can be influenced by the location of the network functions. A control architecture allowing for inter-operation of NFV and transport network (e.g., for combined optimization) is one relevant area for research.

4.9. I2NSF WG

The I2NSF WG at defining interfaces to the flow based network security functions (NSFs) hosted by service providers at different premises. Network Security Function (NSF) is to ensure integrity, confidentiality and availability of network communications, to detect unwanted activity, and to block it or at least mitigate its effects. NSFs are provided and consumed in increasingly diverse environments. Users of NSFs could consume network security services hosted by one or more providers, which may be their own enterprise, service

providers, or a combination of both. The NSFs may be provided by physical and/or virtualized infrastructure.

Without standard interfaces to express, monitor, and control security policies that govern the behavior of NSFs, it becomes virtually impossible for security service providers to automate their service offerings that utilize different security functions from multiple vendors. Based on this, the main goal of I2NSF is to define an information model, a set of software interfaces and data models for controlling and monitoring aspects of NSFs (both physical and virtual) [I-D.jeong-i2nsf-sdn-security-services].

Since different security vendors may support different features and functions on their devices, I2NSF focuses on flow based NSFs that provide treatment to packets/flow.

The I2NSF WG's target deliverables include: (i) a use cases, problem statement, gap analysis document, (ii) a framework document, presenting an overview of the use of NSFs and the purpose of the models developed by the WG, (iii) a single, unified, Information Model for controlling and monitoring flow-based NSFs, (iv) the corresponding YANG Data Models derived from the Information Model, (v) a vendor-neutral vocabulary to enable the characteristics and behavior of NSFs to be specified without requiring the NSFs themselves to be standardized, and (vi) an examination of existing secure communication mechanisms to identify the appropriate ones for carrying the controlling and monitoring information between the NSFs and their management entities. The WG is also targeted to work closely with I2RS, Netconf and Netmod WGs, as well as to communicate with external SDOs like ETSI NFV.

Potential gap: aspects of NSFs such as device or network provisioning and configuration are out of scope.

Potential gap: the use of SDN tools to interact with security functions is not explictly considered, but seems a potential approach, as for example described for the particular case of IPsec flow protection in [I-D.abad-sdnrg-sdn-ipsec-flow-protection].

4.10. IPPM WG

The IP Performance Metrics (IPPM) WG defines metrics that can be used to measure the quality and performance of Internet services and applications running over transport layer protocols (e.g. TCP, UPD) over IP. It also develops and maintains protocols for the measurement of these metrics. The IPPM WG is a long running WG that started in 1997. The architecture (framework) for IPPM WG metrics and associated protocols are defined in RFC 2330 [RFC2330]. Some

examples of recent output by IPPM WG include "A Reference Path and Measurement Points for Large-Scale Measurement of Broadband Performance" (RFC 7398 [RFC7398]) and "Framework for TCP Throughput Testing" (RFC 6349 [RFC6349]).

The IPPM WG currently does not have a charter item or active drafts related to the topic of network virtualization. On the automation and orchestration side, there is an ongoing effort [I-D.cmzrjp-ippm-twamp-yang] to define a YANG model for the IPPM protocol.

Potential gap: There is a pressing need to define metrics and associated protocols to measure the performance of NFV. Specifically, since NFV is based on the concept of taking centralized functions and evolving it to highly distributed SW functions, there is a commensurate need to fully understand and measure the baseline performance of such systems. A potential topic for the IPPM WG is defining packet delay, throughput, and test framework for the application traffic flowing through the NFVI.

4.11. NFV RG

The NFVRG focuses on research problems associated with virtualization of fixed and mobile network infrastructures, new network architectures based on virtualized network functions, virtualization of the home and enterprise network environments, co-existence with non-virtualized infrastructure and services, and application to growing areas of concern such as Internet of Things (IoT) and next generation content distribution. Another goal of the NFVRG is to bring a research community together that can jointly address such problems, concentrating on problems that relate not just to networking but also to computing and storage constraints in such environments.

Since the NFVRG is a research group, it has a wide scope. In order to keep the focus, the group has identified some near term work items: (i) Policy based Resource Management, (ii) Analytics for Visibility and Orchestration, (iii) Virtual Network Function (VNF) Performance Modelling to facilitate transition to NFV and (iv) Security and Service Verification.

4.12. VNFpool BoF

The VNFPOOL BoF proposed to work on the way to group Virtual Network Function (VNF) into pools to improve resilience, provide better scale-out and scale-in characteristics, implement stateful failover among VNF members of a pool, etc. Additionally, they propose to create VNF sets from VNF pools. For this, the BoF proposed to study

signaling (both between members of a pool and across pools), state sharing mechanisms between members of a VNFPOOL, the exchange of reliability information between VNF sets, their users and the underlying network, and the reliability and security of the control plane needed to transport the exchanged information.

The use cases initially considered by VNFPOOL include Content Deliver Networks (CDNs), the LTE mobile core network and reliable server pooling. The VNFPOOL work has been dropped in the IETF.

Potential gap: VNFPOOL tried to introduce and manage resilience in virtualized networking environments and therefore addresses a desirable feature for any software defined network. VNFPOOL has also been integrated into the NFV architecture [I-D.bernini-nfvrg-vnf-orchestration].

5. Summary of Gaps

Potential Gap-1: as stated in the SFC charter, any work on the management and configuration of SFC components related to the support of Service Function Chaining will not be done yet, until better understood and scoped. This part is of special interest for operators and would be required in order to actually put SFC mechanisms into operation.

Potential Gap-2: redundancy and reliability mechanisms are currently not dealt with by SFC or any other WG in the IETF. While this has been the main goal of the VNFpool BoF efforts, since VNFPOOL work has been dropped for the time being without any WG being chartered, the technical topics it aimed at targetting still remain un-addressed.

Potential Gap-3: it would be worthwhile to see if some of the specific approaches developed in the NVO3 WG (e.g. overlays, traffic isolation, VM migration) can be applied outside the DC, and specifically if they can be applicable to network virtualization (NFV). These approaches would be most relevant to the ETSI Network Function Virtualization Infrastructure (NFVI), and the Virtualized Infrastructure Manager part of the MANO.

Potential Gap-4: the most relevant activity in BESS that would be worthwhile to investigate for relevance to network virtualization (NFV) is the extensions to BGP-enabled VPN solutions to support of Service Function Chaining.

Potential Gap-5: in a vEPC/DMM context, how to run the EPC control plane on NFV.

Potential Gap-6: in DMM, on the work item addressing the separation of the Control-Plane for mobility- and session management from the actual Data-Plane, the actual mappings between these generic protocol semantics and the configuration commands required on the data plane network elements (e.g., OpenFlow switches) are not currently in the scope of the DMM WG.

Potential Gap-7: network virtualization is not the main aim of the I2RS WG. However, they provide an infrastructure that can be part of an SDN deployment.

Potential Gap-8: VNFPOOL tries to introduce and manage resilience in virtualized networking environments and therefore addresses a desirable feature for any software defined network. VNFPOOL has also been integrated into the NFV architecture [I-D.bernini-nfvrg-vnf-orchestration].

Potential Gap-9: within the Traffic Engineering Architecture and Signaling (TEAS) WG, several use cases in ACTN are relevant to network virtualization (NFV) in mobile environments. Control of multi-tenant mobile backhaul transport networks, mobile virtual network operation, etc, can be influenced by the location of the network functions. A control architecture allowing for inter-operation of NFV and transport network (e.g., for combined optimization) is one relevant area for research.

Potential Gap-10: within I2NSF', aspects of NSFs such as device or network provisioning and configuration are out of scope.

Potential Gap-11: the use of SDN tools to interact with security functions is not explictly considered in I2NSF, but seems a potential approach, as for example described for the particular case of IPsec flow protection in [I-D.abad-sdnrg-sdn-ipsec-flow-protection].

Potential Gap-12: there is a pressing need to define metrics and associated protocols to measure the performance of NFV. Specifically, since NFV is based on the concept of taking centralized functions and evolving it to highly distributed SW functions, there is a commensurate need to fully understand and measure the baseline performance of such systems. A potential topic for the IPPM WG is defining packet delay, throughput, and test framework for the application traffic flowing through the NFVI.

6. IANA Considerations

N/A.

7. Security Considerations

TBD.

8. Acknowledgments

The authors want to thank Dirk von Hugo, Rafa Marin, Diego Lopez, Ramki Krishnan, Kostas Pentikousis, Rana Pratap Sircar and Alfred Morton for their very useful reviews and comments to the document.

The work of Pedro Aranda is supported by the European FP7 Project Trilogy2 under grant agreement 317756.

9. Informative References

[I-D.abad-sdnrg-sdn-ipsec-flow-protection]
Abad-Carrascosa, A., Lopez, R., and G. Lopez-Millan, "Software-Defined Networking (SDN)-based IPsec Flow Protection", draft-abad-sdnrg-sdn-ipsec-flow-protection-01 (work in progress), October 2015.

[I-D.bernini-nfvrg-vnf-orchestration]
Bernini, G., Maffione, V., Lopez, D., and P. Aranda, "VNF Pool Orchestration For Automated Resiliency in Service Chains", draft-bernini-nfvrg-vnf-orchestration-01 (work in progress), October 2015.

[I-D.ceccarelli-teas-actn-framework]
Ceccarelli, D. and Y. Lee, "Framework for Abstraction and Control of Traffic Engineered Networks", draft-ceccarelli-teas-actn-framework-01 (work in progress), March 2016.

[I-D.cmzrjp-ippm-twamp-yang]
Civil, R., Morton, A., Zheng, L., Rahman, R., Jethanandani, M., and K. Pentikousis, "Two-Way Active Measurement Protocol (TWAMP) Data Model", draft-cmzrjp-ippm-twamp-yang-02 (work in progress), October 2015.

[I-D.ietf-bmwg-sdn-controller-benchmark-meth]
Vengainathan, B., Basil, A., Tassinari, M., Manral, V., and S. Banks, "Benchmarking Methodology for SDN Controller Performance", draft-ietf-bmwg-sdn-controller-benchmark-meth-00 (work in progress), October 2015.

[I-D.ietf-bmwg-sdn-controller-benchmark-term]
Vengainathan, B., Basil, A., Tassinari, M., Manral, V., and S. Banks, "Terminology for Benchmarking SDN Controller Performance", draft-ietf-bmwg-sdn-controller-benchmark-term-00 (work in progress), October 2015.

[I-D.ietf-bmwg-virtual-net]
Morton, A., "Considerations for Benchmarking Virtual Network Functions and Their Infrastructure", draft-ietf-bmwg-virtual-net-01 (work in progress), September 2015.

[I-D.ietf-dmm-fpc-cpdp]
Liebsch, M., Matsushima, S., Gundavelli, S., and D. Moses, "Protocol for Forwarding Policy Configuration (FPC) in DMM", draft-ietf-dmm-fpc-cpdp-01 (work in progress), July 2015.

[I-D.ietf-i2rs-architecture]
Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", draft-ietf-i2rs-architecture-13 (work in progress), February 2016.

[I-D.ietf-nvo3-arch]
Black, D., Hudson, J., Kreeger, L., Lasserre, M., and T. Narten, "An Architecture for Overlay Networks (NVO3)", draft-ietf-nvo3-arch-04 (work in progress), October 2015.

[I-D.jeong-i2nsf-sdn-security-services]
Jeong, J., Kim, H., Jung-Soo, P., Ahn, T., and s. sehuilee@kt.com, "Software-Defined Networking Based Security Services using Interface to Network Security Functions", draft-jeong-i2nsf-sdn-security-services-04 (work in progress), March 2016.

[I-D.kim-bmwg-ha-nfvi]
Kim, T. and E. Paik, "Considerations for Benchmarking High Availability of NFV Infrastructure", draft-kim-bmwg-ha-nfvi-00 (work in progress), October 2015.

[I-D.leeking-teas-actn-problem-statement]
Lee, Y., King, D., Boucadair, M., Jing, R., and L. Contreras, "Problem Statement for Abstraction and Control of Transport Networks", draft-leeking-teas-actn-problem-statement-00 (work in progress), June 2015.

[I-D.matsushima-stateless-uplane-vepc]
Matsushima, S. and R. Wakikawa, "Stateless user-plane architecture for virtualized EPC (vEPC)", draft-matsushima-stateless-uplane-vepc-05 (work in progress), September 2015.

[I-D.rfernando-bess-service-chaining]
Fernando, R., Rao, D., Fang, L., Napierala, M., So, N., and A. Farrel, "Virtual Topologies for Service Chaining in BGP/IP MPLS VPNs", draft-rfernando-bess-service-chaining-01 (work in progress), April 2015.

[I-D.vsperf-bmwg-vswitch-opnfv]
Tahhan, M., O'Mahony, B., and A. Morton, "Benchmarking Virtual Switches in OPNFV", draft-vsperf-bmwg-vswitch-opnfv-01 (work in progress), October 2015.

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, DOI 10.17487/RFC2330, May 1998, <http://www.rfc-editor.org/info/rfc2330>.

[RFC6349] Constantine, B., Forget, G., Geib, R., and R. Schrage, "Framework for TCP Throughput Testing", RFC 6349, DOI 10.17487/RFC6349, August 2011, <http://www.rfc-editor.org/info/rfc6349>.

[RFC7398] Bagnulo, M., Burbridge, T., Crawford, S., Eardley, P., and A. Morton, "A Reference Path and Measurement Points for Large-Scale Measurement of Broadband Performance", RFC 7398, DOI 10.17487/RFC7398, February 2015, <http://www.rfc-editor.org/info/rfc7398>.

[RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC7426, January 2015, <http://www.rfc-editor.org/info/rfc7426>.

[RFC7498] Quinn, P., Ed. and T. Nadeau, Ed., "Problem Statement for Service Function Chaining", RFC 7498, DOI 10.17487/RFC7498, April 2015, <http://www.rfc-editor.org/info/rfc7498>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <http://www.rfc-editor.org/info/rfc7665>.

[etsi_nvf_whitepaper]
"Network Functions Virtualisation (NFV). White Paper 2", October 2014.

Appendix A. The mobile network use case

A.1. The 3GPP Evolved Packet System

TBD. This will include a high level summary of the 3GPP EPS architecture, detailing both the EPC (core) and the RAN (access) parts. A link with the two related ETSI NFV use cases (Virtualisation of Mobile Core Network and IMS, and Virtualisation of Mobile base station) will be included.

The EPS architecture and some of its standardized interfaces are depicted in Figure 7. The EPS provides IP connectivity to user equipment (UE) (i.e., mobile nodes) and access to operator services, such as global Internet access and voice communications. The EPS comprises the core network -- called Evolved Packet Core (EPC) -- and different radio access networks: the 3GPP Access Network (AN), the Untrusted non-3GPP AN and the Trusted non-3GPP AN. There are different types of 3GPP ANs, with the evolved UMTS Terrestrial Radio Access Network (E-UTRAN) as the most advanced one. QoS is supported through an EPS bearer concept, providing bindings to resource reservation within the network.

The evolved NodeB (eNB), the Long Term Evolution (LTE) base station, is part of the access network that provides radio resource management, header compression, security and connectivity to the core network through the S1 interface. In an LTE network, the control plane signaling traffic and the data traffic ar handled separately. The eNBs transmit the control traffic and data traffic separately via two logically separate interfaces.

The Home Subscriber Server, HSS, is a database that contains user subscriptions and QoS profiles. The Mobility Management Entity, MME, is responsible for mobility management, user authentication, bearer establishment and modification and maintenance of the UE context.

The Serving gateway, S-GW, is the mobility anchor and manages the user plane data tunnels during the inter-eNB handovers. It tunnels all user data packets and buffers downlink IP packets destined for UEs that happen to be in idle mode.

The Packet Data Network (PDN) Gateway, P-GW, is responsible for IP address allocation to the UE and is a tunnel endpoint for user and control plane protocols. It is also responsible for charging, packet

filtering, and policy-based control of flows. It interconnects the mobile network to external IP networks, e.g. the Internet.

In this architecture, data packets are not sent directly on an IP network between the eNB and the gateways. Instead, every packet is tunneled over a tunneling protocol - the GPRS Tunneling Protocol (GTP over UDP/IP. A GTP path is identified in each node with the IP address and a UDP port number on the eNB/gateways. The GTP protocol carries both the data traffic (GTP-U tunnels) and the control traffic (GTP-C tunnels). Alternatively Proxy Mobile IP (PMIPv6) is used on the S5 interface between S-GW and P-GW.

In addition to the above basic functions and entities, there are also additional features being discussed by the 3GPP that are relevant from a network virtualization viewpoint. One example is the Traffic Detection Function (TDF), which can be used by the P-GW, and in general by the whole transport network, to decide how to forward the traffic. In a virtualized infrastructure, this kinf of information can be used to elastic and dynamically adapt the network capabilities to the traffic nature and volume.

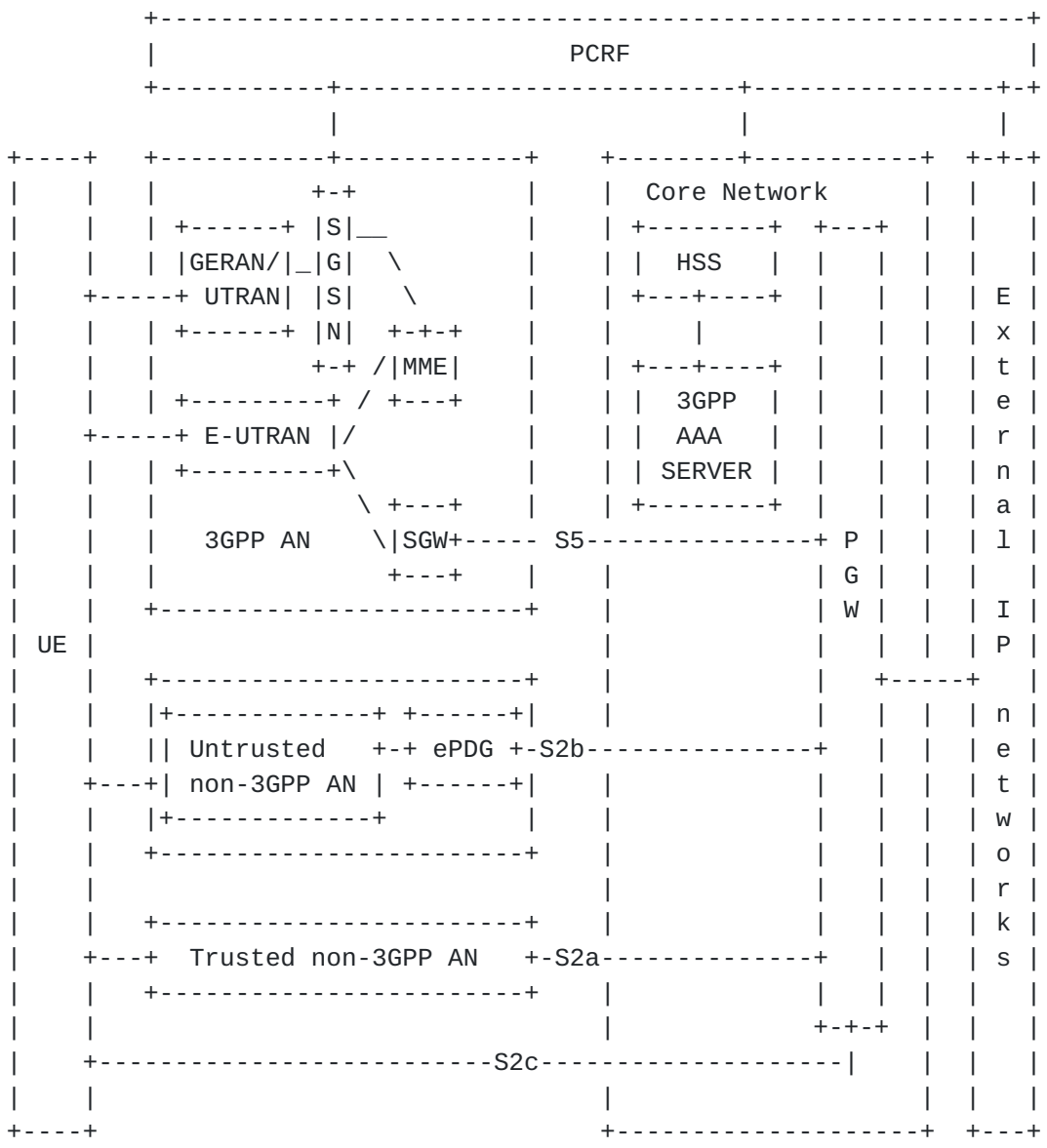

Figure 7: EPS (non-roaming) architecture overview

A.2. Virtualizing the 3GPP EPS

TBD. We describe how a "virtual EPS" (vEPS) would look like and the existing gaps that exist from the point of view of network virtualization.

Authors' Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Akbar Rahman
InterDigital Communications, LLC
1000 Sherbrooke Street West, 10th floor
Montreal, Quebec H3A 3G4
Canada

Email: Akbar.Rahman@InterDigital.com
URI: http://www.InterDigital.com/

Juan Carlos Zuniga
InterDigital Communications, LLC
1000 Sherbrooke Street West, 10th floor
Montreal, Quebec H3A 3G4
Canada

Email: JuanCarlos.Zuniga@InterDigital.com
URI: http://www.InterDigital.com/

Luis M. Contreras
Telefonica I+D
Ronda de la Comunicacion, S/N
Madrid 28050
Spain

Email: luismiguel.conterasmurillo@telefonica.com

Pedro Aranda
Telefonica I+D
Ronda de la Comunicacion, S/N
Madrid 28050
Spain

Email: pedroa.aranda@telefonica.com