NFVRG/SDNRG groups
Internet-Draft
Intended status: Informational
Expires: January 7, 2016

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

July 6, 2015

Gap Analysis on Network Virtualization Activities
draft-bernardos-nfvrg-gaps-network-virtualization-01

Abstract

Network Function Virtualization (NFV) and Software Defined Networking (SDN) are changing the way the telecommunications sector will deploy, extend and operate their networks. These new technologies aim at reducing the overall costs by outsourcing communication services from specific hardware in the operators' core to server farms scattered in datacenters (i.e. compute and storage virtualization). In addition, the connecting networks are fundamentally affected in they way they route, process and control traffic(i.e. network virtualization).

Virtualization is becoming a trend which is being adopted in many scenarios for different purposes. This document overviews existing efforts around virtualization at the IETF/IRTF, focusing on those related to NFV and SDN. These efforts are mapped to the most relevant architectures being defined outside IETF, namely at the ETSI NFV ISG, the ETSI MEC ISG and the ONF.

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, putting them into context considering efforts by other SDOs, and identifying current gaps that can be tackled at IETF or researched at the IRTF.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft will expire on January 7, 2016.

Copyright Notice

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 now following a cloud computing paradigm, enabling the 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, and the ONF and the IETF:

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).

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).

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. The ETSI NFV framework architecture framework is composed of three domains (Figure 1):

o Virtualized Network Function, running over the NFVI.

o NFV Infrastructure (NFVI), including the diversity of physical resources and how these can be virtualized. NFVI supports the execution of the VNFs.

o 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.

```
   +-------------------------------------------+  +---------------+
   |   Virtualized Network Functions (VNFs)    |  |               |
   |  -------   -------   -------   -------    |  |               |
   |  |     |   |     |   |     |   |     |    |  |               |
   |  | VNF |   | VNF |   | VNF |   | VNF |    |  |               |
   |  |     |   |     |   |     |   |     |    |  |               |
   |  -------   -------   -------   -------    |  |               |
   +-------------------------------------------+  |               |
                                                  |               |
   +-------------------------------------------+  |               |
   |         NFV Infrastructure (NFVI)         |  |      NFV      |
   | -----------    -----------    ----------- |  |  Management   |
   | | Virtual |    | Virtual |    | Virtual | |  |      and      |
   | | Compute |    | Storage |    | Network | |  | Orchestration |
   | -----------    -----------    ----------- |  |               |
   | +---------------------------------------+ |  |               |
   | |         Virtualization Layer          | |  |               |
   | +---------------------------------------+ |  |               |
   | +---------------------------------------+ |  |               |
   | | -----------  -----------  ----------- | |  |               |
   | | | Compute |  | Storage |  | Network | | |  |               |
   | | -----------  -----------  ----------- | |  |               |
   | |          Hardware resources           | |  |               |
   | +---------------------------------------+ |  |               |
   +-------------------------------------------+  +---------------+
```

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).

```
                                                  +--------------------+
   +-------------------------------------------+  | ----------------   |
   |                 OSS/BSS                   |  | | NFV          |   |
   +-------------------------------------------+  | | Orchestrator +-- |
                                                  | ---+------------ | |
   +-------------------------------------------+  |    |             | |
   |  ---------     ---------     ---------    |  |    |             | |
   |  | EM 1  |     | EM 2  |     | EM 3  |    |  |    |             | |
   |  ----+----     ----+----     ----+----    |  | ---+----------   | |
   |      |             |             |        |--|-|    VNF     |   | |
   |  ----+----     ----+----     ----+----    |  | | manager(s) |   | |
   |  | VNF 1 |     | VNF 2 |     | VNF 3 |    |  | ---+----------   | |
   |  ----+----     ----+----     ----+----    |  |    |             | |
   +------|-------------|-------------|--------+  |    |             | |
          |             |             |           |    |             | |
   +------+-------------+-------------+--------+  |    |             | |
   |         NFV Infrastructure (NFVI)         |  |    |             | |
   | -----------    -----------    ----------- |  |    |             | |
   | | Virtual |    | Virtual |    | Virtual | |  |    |             | |
   | | Compute |    | Storage |    | Network | |  |    |             | |
   | -----------    -----------    ----------- |  | ---+------       | |
   | +-------------------------------------+ |  | |        |       | |
   | |         Virtualization Layer          | |--|-| VIM(s) +-------- |
   | +-------------------------------------+ |  | |        |         |
   | +-------------------------------------+ |  | ----------         |
   | | -----------  -----------  ----------- | |  |                    |
   | | | Compute |  | Storage |  | Network | | |  |                    |
   | | | hardware|  | hardware|  | hardware| | |  |                    |
   | | -----------  -----------  ----------- | |  |                    |
   | |           Hardware resources          | |  |  NFV Management    |
   | +-------------------------------------+ |  | and Orchestration  |
   +-------------------------------------------+  +--------------------+
```

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). 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.

```
+----------+
| -------  |
| |Oper.|  |            O
| |Mgmt.|  |<........> -+- Network Operator
| |Iface|  |            ^
| -------  |      +----------------------------------------+
|          |      | +------------------------------------+ |
|          |      | | ---------  ---------     --------- | |
|--------- |      | | | App 1 |  | App 2 | ... | App n | | |
||Plugins| |<....>| | ---------  ---------     --------- | |
|--------- |      | | Plugins                            | |
|          |      | +------------------------------------+ |
|          |      | Application Plane                      |
|          |      +----------------------------------------+
|          |                         A
|          |                         |
|          |                         V
|          |      +----------------------------------------+
|          |      | +------------------------------------+ |
|--------- |      | |     ------------  ------------     | |
|| Netw. | |      | |     | Module 1 |  | Module 2 |     | |
||Engine | |<....>| |     ------------  ------------     | |
|--------- |      | | Network Engine                     | |
|          |      | +------------------------------------+ |
|          |      | Controller Plane                       |
|          |      +----------------------------------------+
|          |                         A
|          |                         |
|          |                         V
|          |      +----------------------------------------+
|          |      |  +--------------+   +--------------+   |
|          |      |  | ------------ |   | ------------ |   |
|----------|      |  | | OpenFlow | |   | | OpenFlow | |   |
||OpenFlow||<....>|  | ------------ |   | ------------ |   |
|----------|      |  | NE           |   | NE           |   |
|          |      |  +--------------+   +--------------+   |
|          |      | Data Plane                             |
|Management|      +----------------------------------------+
+----------+
```

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.

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 computing capabilities will make available IT infrastructure for the deployment of functions in mobile access networks. It can be seen then as a complement to both NFV and SDN.

4. Network Virtualization at IETF/IRTF

4.1. 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 [I-D.ietf-sfc-architecture], (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.

4.2. 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 mobile 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.

4.3. 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).

4.4. 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:

```
          ******************   *****************  *****************
          *  Application C *   * Application D *  * Application E *
          ******************   *****************  *****************
                   |                  |                  |
                   +--------------+   |    +-------------+
                                  |   |    |
                                ***************
                                *  Client P   *----------------------+
                                ***************                      |
   ***********************          |                                |
   *    Application A    *          |                                |
   *                     *          |       ***********************  |
   *  +----------------+ *          |       *    Application B    *  |
   *  |   Client A     | *          |       *                     *  |
   *  +----------------+ *          |       *  +----------------+ *  |
   ***********************          |       *  |   Client B     | *  |
             |                      |       *  +----------------+ *  |
             |     +----------------+       ***********************  |
             |     |                              |        |         |
             |     |     +------------------------+        |   +-----+
             |     |     |                                 |   |
      *******************************   *******************************
      *                             *   *                             *
      *      Routing Element 1      *   *      Routing Element 2      *
      *                             *   *                             *
      *******************************   *******************************
```

Figure 4: 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:

```
                      |
     *****************v**************
     *  +---------------------+     *
     *  |       Agent         |     *
     *  +---------------------+     *
     *     ^        ^  ^   ^        *
     *     |        |  |   |        *
     *     |        |  |   +--+     *
     *     |        |  |      |     *
     *     v        |  |      v     *
     * +---+-----+  |  | +----+---+ *
     * | Routing |  |  | | Local  | *
     * |   and   |  |  | | Config | *
     * |Signaling|  |  | +--------+ *
     * +---------+  |  |      ^     *
     *    ^         |  |      |     *
     *    |    +----+  |      |     *
     *    v    v       v      v     *
     *  +----------+ +------------+ *
     *  |  Dynamic | |   Static   | *
     *  |  System  | |   System   | *
     *  |  State   | |   State    | *
     *  +----------+ +------------+ *
     *                              *
     *       Routing Element        *
     ********************************
```

Figure 5: 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.

4.5. 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:

- o 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.

o 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 mobile network virtualization (NFV) is the extensions to BGP-enabled VPN solutions to support of Service Function Chaining [I-D.rfernando-bess-service-chaining].

4.6. VNFpool BoF

The VNFPOOL BoF is working 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 proposes 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 VNFPOOL BoF started work on the charter, use case study, and requirements and initial architecture. The use cases include Content Deliver Networks (CDNs), the LTE mobile core network and reliable server pooling. Currently, there is no activity on the mailing list setup for this activity.

Potential gap: 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].

4.7. 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 mobile network virtualization (NFV). 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.

4.8. 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.

4.9. 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).

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

Potential Gap-9: 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-10: several use cases in ACTN are relevant to mobile network virtualization (NFV). 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.

6. IANA Considerations

N/A.

7. Security Considerations

TBD.

8. Acknowledgments

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

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[I-D.bernini-nfvrg-vnf-orchestration]
Bernini, G., Maffione, V., Lopez, D., and P. Aranda, "VNF Orchestration For Automated Resiliency in Service Chains", draft-bernini-nfvrg-vnf-orchestration-00 (work in progress), July 2015.

[I-D.ceccarelli-teas-actn-framework]
Ceccarelli, D. and Y. Lee, "Framework for Abstraction and Control of Transport Networks", draft-ceccarelli-teas-actn-framework-00 (work in progress), June 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-00 (work in progress), May 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-09 (work in progress), March 2015.

[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-03 (work in progress), March 2015.

[I-D.ietf-sfc-architecture]
Halpern, J. and C. Pignataro, "Service Function Chaining (SFC) Architecture", draft-ietf-sfc-architecture-09 (work in progress), June 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-04 (work in progress), March 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.

[RFC7426] Haleplidis, E., Pentikousis, K., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, January 2015.

[RFC7498] Quinn, P. and T. Nadeau, "Problem Statement for Service Function Chaining", RFC 7498, April 2015.

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.

```
            +---------------------------------------------------------+
            |                           PCRF                          |
            +-----------+--------------------------+----------------+-+
                        |                          |                |
   +----+   +-----------+------------+    +--------+-----------+  +-+-+
   |    |   |          +-+           |    |  Core Network      |  |   |
   |    |   | +------+ |S|__         |    | +--------+  +---+  |  |   |
   |    |   | |GERAN/|_|G|  \        |    | |  HSS   |  |   |  |  |   |
   |    +-----+ UTRAN| |S|   \       |    | +---+----+  |   |  |  | E |
   |    |   | +------+ |N|  +-+-+    |    |     |       |   |  |  | x |
   |    |   |          +-+ /|MME|    |    | +---+----+  |   |  |  | t |
   |    |   | +---------+ / +---+    |    | |  3GPP  |  |   |  |  | e |
   |    +-----+ E-UTRAN |/           |    | |  AAA   |  |   |  |  | r |
   |    |   | +---------+\           |    | | SERVER |  |   |  |  | n |
   |    |   |             \ +---+    |    | +--------+  |   |  |  | a |
   |    |   |   3GPP AN    \|SGW+----- S5---------------+ P |  |  | l |
   |    |   |               +---+    |    |             | G |  |  |   |
   |    |   +------------------------+    |             | W |  |  | I |
   | UE |                                 |             |   |  |  | P |
   |    |   +------------------------+    |             |   +-----+   |
   |    |   |+-------------+ +------+|    |             |   |  |  | n |
   |    |   || Untrusted   +-+ ePDG +-S2b---------------+   |  |  | e |
   |    +---+| non-3GPP AN | +------+|    |             |   |  |  | t |
   |    |   |+-------------+         |    |             |   |  |  | w |
   |    |   +------------------------+    |             |   |  |  | o |
   |    |                                 |             |   |  |  | r |
   |    |   +------------------------+    |             |   |  |  | k |
   |    +---+  Trusted non-3GPP AN   +-S2a--------------+   |  |  | s |
   |    |   +------------------------+    |             |   |  |   |
   |    |                                 |             +-+-+  |  |   |
   |    +--------------------------S2c--------------------|    |  |   |
   |    |                                 |                    |  |   |
   +----+                                 +--------------------+  +---+
```

Figure 6: 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