Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 6, 2014

L. Deng
China Mobile
H. Song
Huawei
G. Karagian
U. of Twente
E. Haleplidis
U. of Patras
B. Martini
CNIT

June 4, 2014

NFV configuration north bound use cases
draft-deng-nfvcon-nb-use-cases-00

Abstract

This specification lists some classical use cases of NFV configuration, especially those related to the north bound operation with the involvement of network function provider and the network function consumers, for example VNF installation, migration, replication, on-demand resource allocation and etc.. These use cases are only relative to the virtualization characteristics of network functions. These use cases will be used to identify the proper standard space and scope for the NFV configuration.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes the typical use cases for NFV (Network Function Virtualization) configuration and management. Based on the Network Function Configuration Architecture, see VNF configuration architecture [I-D.zhou-opsawg-vnf-config-arch], four key roles can be identified in these use cases, (1), the network function provider, (2) network service provider, (3), the network function consumer, (4), the NFV control plane, (5), the NFV infrastructure, see Figure 1.

Network function providers provide the network function software and related description information that are necessary for the network function consumer to know. Network function providers are responsible for the lifecycle management of the network functions, for example, on-shelf, updates, and delete.

Network function consumers are those who use the network functions deployed inside the network service provider, i.e. NSP's network. The network function consumers can be the home user, the enterprise user or the NSP. Home user and enterprise user can directly manage their network functions such like virtual firewall or virtual residential gateway in the provider's network. But NSPs can also be the user of network functions, for example, carrier grade NAT.

```
  +----------------+   +----------------+   +----------------+
  |Network Function|   |Network Function|   |Network Service |
  |   Provider     |   |Consumer        |   |                |
  +----------------+   +-------+--------+   +----------------+
                --             |                  --
                  --           |                --
                    --         |             ---
                      --       |          ---
                        --     |        --
                          --   |     ---
                            -- |   --
                +--------------------------------+
                |NFV Control and Management Plane|
                +--------------------------------+
                               |
                               |
                               |
           +-------------------+---------------------+
           | NFV Infrastructure                      |
           |+----------+    +---------+   +--------+ |
           || Computing|    | Storage |   | Network| |
           |+----------+    +---------+   +--------+ |
           +-----------------------------------------+
```

Figure 1 Key roles used in use cases
(Note: this architecture will be mapped to the published ETSI NFV architecture)

There are many issues that the NFV control plane may be involved in, and it is assumed that the existing standard protocols have already solved the physical network functions' management and operation problems (despite the fact that they have not), but they have not solved the new problems introduced by the virtualization of network functions, for example, the virtualization network function installation, the dynamic lifecycle management, the dynamic migration, the revocable of a particular network function. In this document, only those use cases relative to the new problems will be introduced.

2. Terminology

Note: The following terms used in this document will be aligned with their definitions from ETSI GS NFV 003[ETSI_GS_NFV_003] . (Note: It will aovid confusion of different terms. But what about the copyright issue? or there is no copyright issue?)

Network Function Provider: a Network Function Provider (NFP) provides virtual network function software.

Network Service Provider (NSP): a company or organization, that provides a network service on a commercial basis to third parties. A network service is a composition of network functions and defined by its functional and behavior specification. The NSP operates the NFV Control Plane.

Network Function Consumer: a Network Function Consumer (NFC) is the consumer of virtual network functions. It can be either an individual user, home user or the enterprise user.

Virtual Network Function: an implementation of an executable software program that constitutes the whole or a part of a network function that can be deployed on a virtualization infrastructure.

Physical Network Function: a physical network function indicates a physical appliance of functional building block within an operator's network infrastructure, which has well-defined external interfaces and a well-defined functional behavior.

NFV Infrastructure: NFV Infrastructure indicates the computing, storage and network resources to implement the virtual network function. High performance acceleration platform is also part of it.

NFV Control and Management Plane: a NFV Control and Management Plane is operated by a NSP and orchestrates the NFV Infrastructure to provide NFV service to NFC.

3. Use Cases

3.1. VNF store: NSP's app store for VNFs

By the decoupling between the software implementation and hardware platform of network devices enabled by virtualization technology, it is envisioned that various functional components of consumer/network devices (e.g. gateway, firewall, IDS, WAN acceleration), which are traditionally provided by the local NSP/ third party device manufactures in the form of dedicated hardware boxes, can be deployed into a virtual machine within the local NSP's data center as a piece of software instance (i.e. virtual network function or VNF).

By setting up an VNF store, an NSP operated application store dedicated for various VNFs, the local NSP would be able to provide a much convenient way for its users (both enterprise and individual consumers) to search for, learn more about, compare between and make purchase for specific NSP VNFs according to its personalized needs, and a more convenient way for the network function providers to provide their software package. Please note that a NSP itself can be the customer of the VNF store. The main motivation for a NSP to become the customer is for its transparent service to its subscribers, for example, traffic optimization, carrier grade NAT and etc.

(Note: the authors will add the list of what should be done in the context of NFVCon.)

3.2. VNF as a Service (VNFaaS): configuration and management

This use case is based on Use case #2: Virtual Network Function as a Service (VNFaaS) described in ETSI GS NFV 001[ETSI_GS_NFV_001] . This use case focuses on the configuration of a virtualized enterprise service, where the VNF is the NSP's application and the enterprise user is the consumer of this service. By making the VNF functionality available to enterprise users as a service is comparable to the cloud computing concept denoted as the Software as a Service (SaaS). According to NIST SP 800-146 [NIST_SP_800-146] SaaS is the possibility for the consumer to use software applications running on a cloud infrastructure. The consumer, however, cannot manage the application only from a configuration perspective and cannot control the underlying infrastructure.

The main motivation of specifying such virtualized enterprise service is that rather than that enterprise users invest their own capital in deployment of networking infrastructure, the NSP may be able to provide advanced networking features as a measured service on an expense basis.

Several examples of VNFaaS are provided in ETSI GS NFV 001[ETSI_GS_NFV_001]. For example, in use case #2: Virtual Network Function as a Service (VNFaaS), the VNFaaS is related to the services that are deployed by enterprise users at the edge of branch offices. Due to the fact that the enterprise users are faced with big required investments, such enterprise users are looking for outsource alternatives, which can be the virtualization of the enterprise CPE (e.g., VFN of an access router) into the NSP's network. In this example the used VNFs are the virtualized CPE and PE (Provider Equiment). In use case #5: Virtualization of Mobile Core and IMS (IP Multimedia Subsystem), the VNFaaS is related to services that are related to the virtualization of the EPC (Evolved Packet Core). The EPC and IMS are standardized by the 3GPP standardization body. In this example the VNFs are the network entities supported by the EPC, such as the MME (Mobility Management Entity), P-GW (Packet Data Network Gateway), S-GW (Serving Gateway), Home Subscriber System (HSS). In this example the VNFaaS is the EPCaaS.

Both that VNFaaS provider and enterprise consumer share the responsibility for the management of the VNFaaS. The NSP is responsible for the lifecycle management of the VNFaaS instances to provide the expected service level (SLA) for the subscribers to the VNFaaS. The VNFaaS lifecycle management is similar to the cloud lifecycle management steps. In particular, the EU FP7 project Mobile Cloud Networking (MCN) [MCN], defined the following lifecycle management steps that can also be applied for the VNFaaS lifecycle management:

- Design: at this stage the service's technical design is carried out.

- Implement: with a service design the service is implemented.

- Deploy and provision: The VNF management is deployed and the necessary service instances are starting to be created. o

- Runtime and Operation: the created VNF and service instances for each tenant are monitored and managed. It is during this step where scaling in and out of VFNs is carried out. Scaling in occurs when a VFN is releasing resources and scaling out occurs when new resources are allocated to a VFN.

- Disposal: the VFNs associated with a service instance are disposed.

The enterprise users expect to manage and configure their customer premises entities.

The NFVcon can focus on providing the interfaces and protocols required by the network function provider, network service provider and the network function consumer to configure and manage the VNFaaS.

Some challenges that need to be solved are:

- o Appropriate authentication and authorization mechanism are required to support the orchestration of VNF instances. For example only authorized VNF instances are permitted to execute on the NFVI. Moreover, mechanisms should be provided such that VNF instances can only access the physical and virtual terminations to which their access is authorized.

- o A virtualized environment needs to guarantee complete isolation among the network function consumers. Special considerations are needed for protecting network function consumer data and configuration files.

- o By providing a VNFaaS as a measured service requires usage measurement metrics and infrastructure appropriate to the type of VNF as well as appropriate Service Level Agreements. VNFaaS usage measurements need the appropriately auditable accounting treatment to be used as basis for service billing arrangements.

- o Resource scaling: scaling up and down network resources used by VNFs

- o Service awareness: service aware resource allocation to network functions

- o State maintenance: Network and network function state management during network function relocation, replication and resource scaling

- o Appropriate mechanism for monitoring/fault detection/diagnosis of all components and their states after virtualization, e.g., VNF instances, hardware, hypervisor

- o Traffic control separation mechanism: Data and management traffic identification/separation for non-virtualized and virtualized networks.

3.3. VNF as a Platform (VNFaaP): configuration and management

This use case is based on Use case #3: Virtual Network Platfom as a Service (VNPaaS) described in ETSI GS NFV 001[ETSI_GS_NFV_001]. This use case focuses on the configuration of a virtualized network platform, where a network service provider makes available a suite of

infrastructure and applications as a platform on which the enterprise users can deploy their own network applications. By using this platform, the enterprise users could develop their own network service that is customized to their business purposes.

Making the VNF platform available to enterprise users as a service is comparable to the cloud computing concept as a Platform as a Service (PaaS), which is defined in NIST SP 800-146 [NIST_SP_800-146] as follows. PaaS is the possibility for the consumer to use software applications running on a cloud infrastructure. The consumer can control the deployed application, but it cannot control the underlying network or the cloud infrastructure (i.e., the NFVI).

In this use case the NSP provides a toolkit of (1) networking and computing infrastructure and (2) potentially some VNFs as a platform, for the creation of a virtual network, denoted as Virtual Network Platform as a Service (VNPaaS). The enterprise consumer uses this toolkit to develop its own virtual network.

The VNPaaS is similar to VNFaaS, but it differs mainly on the scope of control provided to the consumer of the service. The VNPaaS is able to provide a larger scale service, which typically will be the provision of a virtual network rather than a single virtual network function. In particular, the VNFaaS is limited to the configuration of a set of VNF instances made available by the NSP, while the VNPaaS provides the possibility to the enterprise consumer to introduce their own VNF instances as well.

Several types of services can be supported by a VNPaaS, ranging from a simple firewall service for a single enterprise to a whole business communication suite based on an IMS network for a 3rd party.

The NFVcon can focus on providing the interfaces and protocols required by the network function provider, network service provider and the network function consumer to configure and manage the VNPaaS.

In addition to the VNFaaS challenges listed in Section 3.3, some additional challenges need to solved:

- o Access control should be based on an authorized user identity

- o Infrastructure resources need to provide mechanisms to separate workloads from different network service providers.

- o Infrastructure resources and network functions support an interface used to monitor, guarantee and limit the usage of the resources by each network service provider.

3.4. VNF migration: travel with your NSP "devices"

A travelling consumer's experience would be highly improved if he/she found that all their subscribed network devices are also travelling with them automatically/on demand. The portability of VNF-based NSP services is based on VNF migration within the local NSP's data centers or even across different NSPs' domains.

```
+----------------+    2.vRGW is migrated to a +----------------+
| Haibin's vRGW  +---------------------------->  Haibin's vRGW |
+--------+-------+    data center in Shenzhen +--------+-------+
         |                                             |
         |                                             |
Previous |                                             |
         |                                             | Now
         |                                             |
         |                                             |
         |                                             |
     +---+--+    1.Haibin left Nanjing             +---+--+
     |Haibin+------------------------------------->|Haibin|
     +------+      and moved to Shenzhen           +------+

     Nanjing                                       Shenzhen
```

Figure 2. VNF migration

As shown in Figure 2, while Haibin moves from Nanjing to Shenzhen, his virtual residential gateway (including DHCP, firewall and ALG functions and etc) is also migrated from Nanjing to Shenzhen. This kind of migration, when compared with the dedicated hardware box residential gateway, can improve the user's experience as he did not lose any data or configuration.

Usually it has the following features:

o It allows a network function consumer to do migration configuration/subscription for a given VNF;

o It allows the local NSP to detect the movement of a travelling consumer and trigger subsequent VNF migration accordingly;

o It provides robust authentication mechanism for a roaming user to access a migrated VNF;

o It provides clearly stated resource requirement for accommodating a migrated VNF in a visiting datacenter/NSP domain, and provide reliable resource/performance splicing for a migrated

VNF against local abuse from bugs/holes in third party developed software. This may not be visible to the NFC, but the SLA will be met during and after the migration.

3.5. VNF installation: customizing personal VNFs

A NSC may want to customize its VNF instance, to specialize its installation of functional building blocks, with regarding to its own requirements from traffic pattern, service preference, and security/ privacy sensitivity.

Take traffic pattern for example, if there is a VNF for censoring the traffic, if the traffic sent to this VNF are video packets, then the NSC may want to install a video censoring function block, e.g. for pornography. If the traffic sent to the VNF is text packets then the user may want to install a text censoring function block. If the traffic is a combination of video and text, then the NSC may need to install another functional block for classification. NFCs do not need to install unnecessary function blocks on their own VNFs.

There are also considerations from security or privacy aspects. A website's owner has much more concerns on security protection than an individual subscriber, while a habitual on-line shopper cares much more on privacy protection than a webpage visitor. This also brings different components to be installed on the NFC's VNF.

Deployment position considerations can be another advantage of virtualization.

The difference between this VNF installation and the traditional dedicated hardware physical network function appliance is that a NFC can customize his VNF and the position of the VNF, and make the VNF run immediately after his requirements are sent to the NFV control plane.

(Note: the authors will add the list of what should be done in the context of NFVCon.)

3.6. VNF template: common profile for managing multiple VNF instances

For enterprise scenario, it is often the case that an IT personnel is responsible for setting up the network access environments for a potentially quite large number of individual employees. Although there maybe variations among employees' requirements and entitlements according to their roles and ranks in the organizational hierarchy, it is expected that by predefining some general applicable VNF templates to capture the common demand for a group and allowing the consumer to apply them to multiple VNF instances simultaneously with

a simple command/interface, the management cost would be greatly reduced. This kind of VNF includes the virtual firewall.

If there are some exactly same VNFs, the NFV control and management plane (1) can map the same configuration to multiple replicas, without that the NFC needs to know the position of the VNFs, and (2) operates them individually.

This use case has the following features:

- It allows pre-defined template for VNF configuration;

- It allows for template-based VNF group management.

(Note: the authors will add the list of what should be done in the context of NFVCon.)

3.7. Dynamic resource usage

Network function customers may have demand for automatic scale out and scale in for resource usage, and pay for the amount of resource it has used. This is extremely useful when the NFC cannot predict his resource usage or the resource usage is not stable. For example, one enterprise user as a NFC may have much traffic processing load on its VNF(s) during the daytime, but in the night, the NFC does not have any load on its VNF(s). Automatic scale out and scale in can be implemented in different ways, such like automatically generating/ deleting new VNF instances while monitoring the load status.

This use case may require the NFC and the NFV control and management plane to negotiate the policy of it.

3.8. Service Function Chaining

For service function chains, NFC tells the NFV control and management plane about the specific service processing order, to make specific traffic go through that order. The service functions can be inside one VNF, different VNFs in one physical server or different VNFs in different physical servers. The description from the NFC to the NFV control and management plane may include the traffic classification rules, and the service chaining order, and other relative policies. The control and management plane can be agnostic of the service chaining logic, but must be able to pass the right chain description/ policy to the right VNF.

4. Security Considerations

Network function virtualization may make attacks easier, when using standard IT method to normalize the dedicated network function appliances, and make it easily accessed by the consumers. In particular, the following security considerations need to be taken into account:

- Access control should be based on an authorized user identity

- Provide robust authentication mechanism for a roaming user to access a migrated VNF

- Appropriate authentication and authorization mechanism are required to support the orchestration of VNF instances. For example only authorized VNF instances are permitted to execute on the NFVI. Moreover, mechanisms should be provided such that VNF instances can only access the physical and virtual terminations to which their access is authorized.

- A virtualized environment needs to guarantee complete isolation among the network function consumers. Special considerations are needed for protecting network function consumer data and configuration files.

5. Acknowledgement

Thanks to Diego Lopez for his valuable comments to this document. And thanks to the people who joined the succesful side meeting discussion, some of the ideas are from the discussion. The main people are: Diego Lopez, Mehmet Ersue, Melinda Shore, Juergen Schoenwaelder, Jiang Yuanlong, Cathy Zhou, Zhen Cao,Hui Deng, Georgios Karagian, Evangelos Haleplidis, Deng Lingli, Kostas Pentikousis, Michael Scharf.

6. References

6.1. Normative References

[I-D.zhou-opsawg-vnf-config-arch]
Zhou, H., Song, H., and F. Qiao, "Virtual Network Function Configuration Architecture", draft-zhou-opsawg-vnf-config-arch-00 (work in progress), September 2013.

6.2. Informative References

[ETSI_GS_NFV_001]
"Network Functions Virtualisation (NFV); Use Cases", ETSI GS NFV specification Network Functions Virtualisation (NFV) ETSI ISG, ETSI GS NFV 001, v1.1.1, October 2013.

[ETSI_GS_NFV_003]
"Network Function Virtualisation (NFV); Terminology for Main Concepts in NFV", ETSI GS NFV specification Network Function VIrtualisation (NFV) ETSI ISG, ETSI GS NFV 003, v1.1.1, Oct 2013.

[NIST_SP_800-146]
"Draft Cloud Computing Synopsis and recommendations", NIST specifications , May 2011.

Authors' Addresses

Deng Lingli
China Mobile

Email: denglingli@chinamobile.com

Haibin Song
Huawei

Email: haibin.song@huawei.com

Georgios Karagian
U. of Twente

Email: karagian@cs.utwente.nl

Evangelos Haleplidis
U. of Patras

Email: ehalep@gmail.com

Barbara Martini
CNIT

Email: barbara.martini@cnit.it