Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 21, 2015

G. Karagiannis
University of Twente
W. Liu
T. Tsou
Huawei Technologies
Q. Sun
China Telecom
D. Lopez
Telefonica

July 21, 2014

Problem Statement for Application Policy on Network Functions (APONF)
draft-karagiannis-aponf-problem-statement-03

Abstract

As more and more modern network management applications grow in scale and complexity, their demands and requirements on the supporting communication network will increase.
In particular, today network operators are challenged to create an abstract view of their network infrastructure and help service developers on using and programming this abstraction rather than manipulating individual devices. In this context, network management applications can be used to provide the required configuration and application programming interfaces to such service developers. The main goal of APONF is to (1) communicate the up to date abstract view of the network between the network management application systems and network management and controlling systems and (2) map the abstract view of the network into specific network management policies, i.e., device level configuration models.

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 January 21, 2015.

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].

Table of Contents

1. Introduction

Today, as the Internet grows, more and more new services keep on arising, and network traffic is rapidly increased, which may result in slow performance of network devices (e.g., BRAS) and poor end-user experience. This also implies that demands and requirements of such new services on the supporting communication network will increase.

Furthermore, and especially for cloud applications, the cloud tenants and developers usually need to use the communication network capabilities, such as dynamic network management easily, accurately and efficiently. In this way, the deployment of new applications and services may be accelerated and the user experience can be improved.

Moreover, the Development Operations (DevOps), see e.g., [DevOps], is

another network development trend which orchestrates the complex interdependent processes associated with software development and IT operations in order to accelerate the production and roll out of software products and services.

Currently, the separation of development and operation of network technologies leads to slow deployment of network functions/devices and poor user experiences. The communication network needs to provide graceful adjustment capabilities in order to accommodate the diverse needs of applications and the rapid network evolution.

In addition, today network operators are challenged to create an abstract view of their network infrastructure and help application developers on using and programming this abstraction rather than manipulating individual devices. An abstract view of a network infrastructure can be realized using a network service graph. A network service graph provides an abstraction view of a network infrastructure, which also includes network service attributes. The network service attributes are network management application dependent which may include the network service dependencies and network configuration and topology used by a network management application, the used flow steering policy, the IPv6 transition policy, the Distributed Data Center application policy. Network management applications are Operational Support System (OSS) like applications that help a communication service provider to monitor, control, analyze and manage a communication network.

In this context, network management applications can be used to provide the required configuration and application programming interfaces to such service developers. Subsequently, a network management application can use the application based demands and possibly update its associated network service attributes. Examples of network management applications that can modify the network service attributes are for example, Distributed Data Center Application and IPv6 transitions.

For each network service instance a network service graph needs to be generated and maintained.

The up to date network service graph needs to (1) be communicated between the network management application systems and the network management and controlling systems, (2) map the attributes of the network service graph into specific network management policies, i.e., device level configuration models.

Currently, there are no IETF standard mechanisms or modeling languages that can directly be applied to model the network service graphs. IETF has however, created the IETF SFC WG [SFC] to document a new approach to service deliver and operation, where one of its goals is to realize the service function chain that defines an ordered set of service functions that must be applied to packets and/or layer-2 frames selected as a result of classification. Furthermore, the ACTN (Abstraction and Control of Transport Networks) activity can partially provide a solution to this challenge, by

providing means to model the network abstraction.
Moreover, NFVcon (Network Functions Virtualization configuration) is planning to work on the definition of network service graphs.

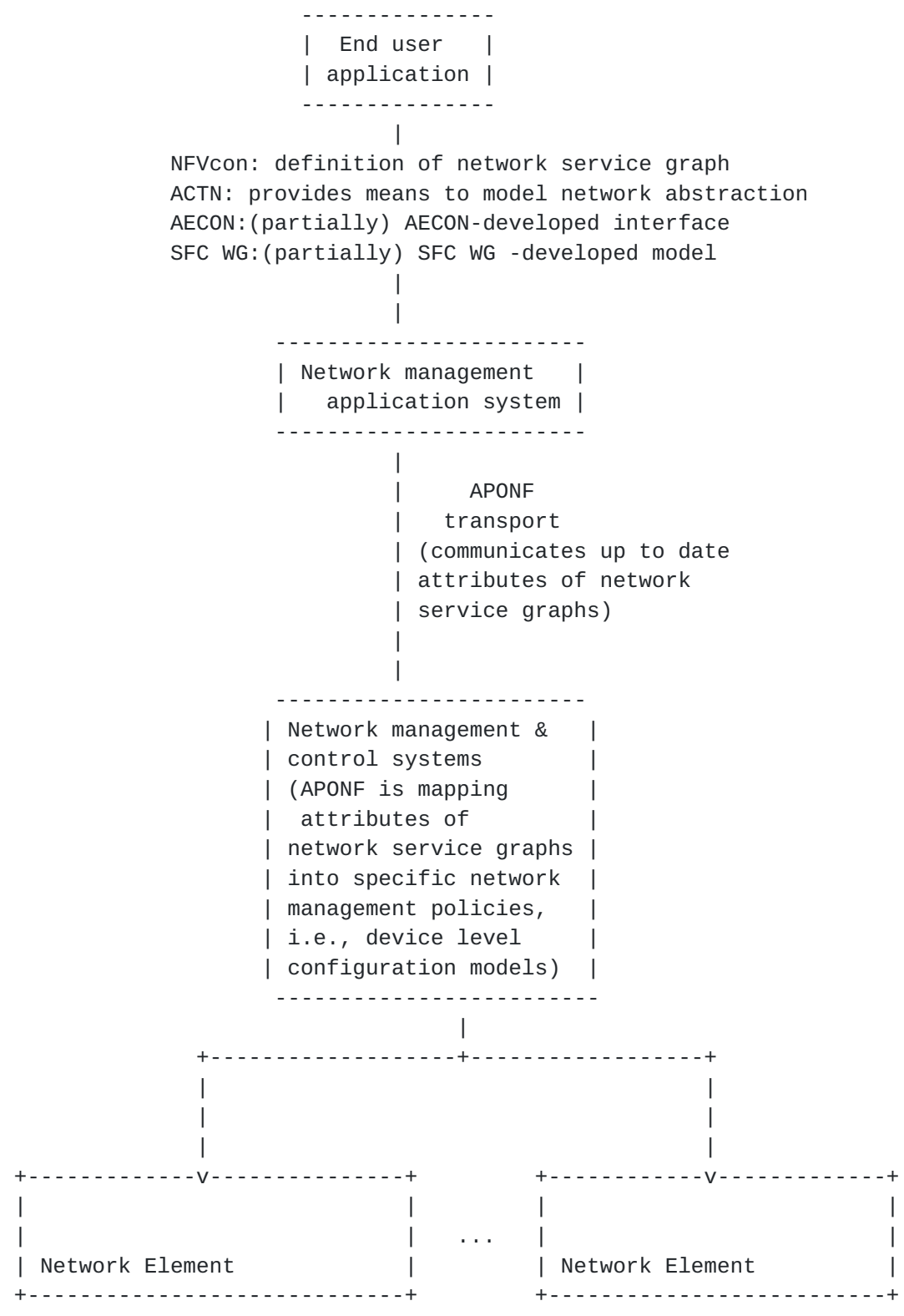

Figure 1: APONF goal and scope

Furthermore, there are currently no IETF solutions that can be used to provide the necessary configuration interfaces to service developers to program the abstract view of a network infrastructure.

The AECON (Application Enabled Collaborative Network) activity can partially provide a solution to this challenge, by providing the required flow descriptions. Moreover, the NFVcon activity is planning to work on the definition of this configuration interface.

Moreover, there are no IETF solutions that can directly be used to (1)enable the streaming transfer of bulk-variable/data of network service graphs between network management application systems and network management and controlling systems, (2) map the attributes of the network service graphs into specific device level configuration models.
The APONF activity can provide a solution to this challenge. In particular, APONF will investigate and select one of the protocols that have been specified by the IETF.
For example, a possible protocol that can be enhanced and used is the Network Configuration Protocol (NETCONF) [RFC6241].

The main goal of APONF, see Figure 1, is to:

- o) enable the streaming transfer of bulk-variable/data of the up to date network service graphs between network management application systems and network management and controlling systems, by using and extending an existing IETF signaling protocol.
- o) map the attributes of the network service graph into specific network management policies, i.e., device level configuration models.

This document is organized as follows. Section 2 presents the terminology. Section 3 provides a brief overview of the use cases associated with APONF. The requirements/objectives are provided in Section 4. Section 5 presents the relationships between APONF and other IETF Working Groups and other IETF activities. The existing IETF protocols and methods that can be used by the APONF solutions are given in Section 6. Section 7 provides the security considerations. The IANA considerations are given in Section 8. Section 9 gives the acknowledgements and Section 10 lists the used references.

2. Terminology

Device level configuration model: supports the description of the network management policies and it describes the configuration details at the device level.

Network service dependencies: dependencies between different service functions/nodes.

Network Management Application: Operational Support System (OSS) like applications that help a communication service provider to monitor, control, analyze and manage a communication network.

Network management application systems: Systems or platforms that run the network management application.

Network configuration model: provides a declarative configuration of the network

Network topology model: describes the topology of a multi-layer network.

Network service: a Network management application. Each network service can be represented by a classified application based policy model, since it can model the group of demands coming from a bundle of end user applications that impose similar requirements on the communication network.

Network service graph: provides an abstraction view of a network infrastructure, which also includes network service attributes. The network service attributes are network management application dependent which may include the service dependencies and network configuration and topology used by a network management application, the used flow steering policy, the IPv6 transition policy, the Distributed Data Center application policy. These attributes can be extended based on the requirements imposed by the network management application. For each network service instance, i.e., network management application instance, an unique network service graph needs to be generated and maintained.

Network element: a physical entity or a virtual entity that can be locally managed and operated.

Service Function Chain (SFC): A service Function chain defines an ordered set of service functions that must be applied to packets and/or layer-2 frames selected as a result of classification. The implied order may not be a linear progression as nodes may copy to more than one branch. The term service chain is often used as shorthand for service function chain.

Service Function Path (SFP): The instantiation of a service function chain in the network. Packets follow a service function path from a classifier through the required instances of service functions in the network.

VNF (Virtualized Network Function): An implementation of an executable software program that constitutes the whole or a part of an NF and can be deployed on a virtualization infrastructure.

3. Use Cases

This section briefly describes the use cases that are associated with different types of network management applications. The detailed description of these use cases is provided in other Internet draft(s).

3.1 Distributed Data Center

A large-scale IDC (Inter Data Center) operator provides server hosting, bandwidth, and value-added services to enterprises and ISPs, and has more than 10 data centers and more than 1Tbs bandwidth in a capital city. In current IDC network, traffic is routed by

configuring policy routes and adjusting routes prioritization to choose an outgoing link. This type of static provisioning comes with high costs and poor operability. Furthermore, the link bandwidth resources in the data centers are not efficiently utilized.

Services usually do not have consistent bandwidth requirements at all times of a day, e.g. video ISP usually require more bandwidth at non-working hours but require less bandwidth at working hours. Some customers have relative high QoS requirement for their services, e.g. IM (Instant Messaging). Static bandwidth and QoS provisioning for all the customers and services is not reasonable and not a cost-effective solution.
APONF can be used to optimize the traffic paths dynamically and have the ability to load balance between data centers and links, and direct customer traffic via network management policies (e.g., models, software programs routines) based on customer grade and QoS requirements. A detailed description of this use case is provided in [ID.draft-cheng-aponf-ddc-use-cases].

3.2 IPv6 transition

The IPv6 transition has been an ongoing process throughout the world due to the exhaustion of the IPv4 address space. However, this transition leads to costly end-to-end network upgrades and poses new challenges of managing a large number of devices with a variety of transitioning protocols. While IPv6 transition tools exist, there are still new challenges to be solved. Operators may need various types of IPv6 transition technologies depending on performance requirements, deployment scenarios, etc.

To address these difficulties, APONF can be used as the software defined unifying approach that can provide a unified way to deploy IPv6 in a cost-effective, flexible manner. A detailed description of this use case is provided in [ID.draft-sun-aponf-openv6-use-cases].

3.3. Virtualized Enterprise Applications

Virtualized Enterprise applications make the Virtualized Network Function (VNF) functionality available to enterprise users as a service, comparable to the cloud computing concept denoted as the Software as a Service (SaaS), see [NIST SP 800-146].
Virtualized Enterprise application policies include dynamic orchestration of virtualized network functions, dynamic increase/decrease of network bandwidth, pay as you go billing and charging.
GiLAN is another important application of network function virtualization. In mobile core networks, it is preferable that QoS provisioning and network function requirements are different for subscribers with different profiles. In such scenarios, specialized network management applications such as BSS/OSS can send application based demands to a policy decision point, which further map these application based demands to GiLAN specific VNF policies, and realize the required QoS and with appropriate network functions, for example, for dynamic path reconfiguration.

APONF can be used to support the dynamic network reconfiguration demands imposed by such virtualized enterprise applications. A detailed description of this use case is provided in [ID.draft-huang-aponf-use-cases].

3.4. Source Address Validation and Traceback (SAVI)

It has been long known that the IPv4/IPv6 transition makes the Tracking and validation of source IP address thorny. Whenever an IPvX packet is translated into an IPvY packet, there are three Troublesome issues: 1. how to track the origin of the IPvY packet which is actually in the IPvX world? 2. how to validate the IPvX packet at the edge of the IPvY world to prevent possible spoofing? 3. how to protect the IPvY address from being spoofed in the IPvY world? SAVI[RFC7039] has given the source address validation solutions for both IPv4 and IPv6.
In order to address the above issues, APONF can be used to block or permit the traffic based on the validation of the source address.
A detailed description of this use case is provided in [ID.draft-bi-aponf-sdsavi].

3.5 Using the abstract view of network by service developers

This use case description argues that service developers can profit by using the abstract view of the network during the programming and development process instead of manipulating individual devices.
In this way one can write software that programs an arbitrary network.
APONF can be used to interface the programmed arbitrary network into network management policies, i.e., device configuration models. A detailed description of this use case is provided in [ID.draft-liu-aponf-using-abstract-view-use-case].

4. Requirements/Objectives

The requirements/objectives that need to be supported by the APONF methods, models and protocol solutions are the following ones:

- o) monitor and verify the freshness of the network service graph.
- o) extend an existing IETF protocol to securely and efficiently distribute the network service graphs between network management applications systems (e.g., OSS) and the network management and/or controlling systems.
- o) use application based demands generated by network management applications systems to map the network service graph instance into specific network management policies, i.e., into device level configuration models. Such application based demands are:
  - a) encapsulating, de-encapsulating packets associated with a flow into a tunnel (for example, VPN service, IPv6 transition service demands on the network)

b) blocking, or dropping packets associated with a flow in (the edge of) the network element when the network security service is aware of the attack (for example, SAVI service, Anti-DoS service demands on the network).

c) configure and dynamically reconfigure data centers to steer and reroute traffic associated with a specific flow

d) configure and dynamically reconfigure data centers to change priorities of different types of traffic associated with a specific flow

e) logging the traffic associated with a flow for network security service,

f) optimization of the traffic based on the IETF ALTO [ALTO]

g) other actions defined by the administrator

o) specify the Authentication Authorization and Accounting (AAA) method

5. Relationships between APONF and other IETF Working Groups and IETF activities

The following relationships between APONF and other IETF WGs and IETF activities have been identified:

IETF SFC WG: the main goal is to document a new approach to service delivery and operation, where one of its goals is to realize an abstract view of a network by using a service graph denoted as the Service Function Path (SFP). This will enable the development of suitable models for network configuration and network topology.

APONF can use as much as possible these models in order to derive the network service graphs associated with each network service.

AECON (Application Enabled Collaborative Network): The main goal of the AECON activity (currently BOF) is to allow applications to explicitly signal their flow characteristics to the network.

The AECON activity can partially provide a solution for the specification of the necessary configuration interfaces to service developers to program the abstract view of a network infrastructure, by providing the required flow descriptions.

ACTN (Abstraction and Control of Transport Networks): The main goal of this activity is to enable discussion of the architecture, use-cases, and requirements that provide abstraction and virtual control of transport networks to various applications. The aim of ACTN is to facilitate virtual network operation: the creation of a virtualized environment allowing operators to view and control multiple multi-subnet, multi-technology networks as a single virtualized network.

ACTN activity can partially provide a solution to the definition of the network service graph, by providing means to model the network abstraction. Moreover, APONF can use all means that will be provided by ACTN on virtual network operation.

NFVcon (Network Functions Virtualization configuration): The main goal of this activity is to support the dynamic configuration of NFV instances.
The NFVcon activity is planning to focus on the definition of the network service graphs. Moreover, NFVcon might also focus on the specification of the necessary configuration interfaces to service developers to program the abstract view of a network infrastructure.

APONF can use the network service graph definitions and the specification of the configuration interfaces provided by the Netcon activity.

Use Cases for Autonomic Networking (UCAN): The main goal of UCAN (BOF status) is to collect and analyze use cases for Autonomic Networking. The main objective of Autonomic Networking (AN) is the support of self-management, including self-configuration, self-optimization, self-healing and self-protection.
The goal is to find commonalities between various use cases, to be able to determine generic requirements for Autonomic Networking functions and to conclude whether there is scope for a common, generic Autonomic Networking Infrastructure for all autonomic functions.

APONF can be seen as a possible UCAN use case that can use the Autonomic Networking capabilities provided by UCAN.

APONF is different than existing WGs and other IETF activities, due to the fact that APONF is the only activity that:

- o) enables the streaming transfer of bulk-variable/data of the up to date network service graphs between network management application systems and the network management and controlling systems
- o) map the attributes of the network service graph instances into specific network management policies, i.e., device level configuration models.

6. Existing Protocols and Methods

The APONF protocol and mechanisms will have an impact on layers 4 and above. Note however, that APONF will also have an impact on layer 3, related to issues such as IP tunneling.
A gap analysis is being performed in order to identify and select the IETF protocol that, after extension, can enable the streaming transfer of bulk-variable/data of the up to date network service graphs between network management application systems and the network management and controlling systems.
For example, a possible protocol that can be enhanced and used is the Network Configuration Protocol (NETCONF) [RFC6241].

The following activities are out of the APONF scope:

o) the generation of the abstract view of the network infrastructure using an network service graph

o) the necessary configuration interfaces to service developers to program the abstract view of a network infrastructure.

o) definition of the used network service graphs

o) the specification of the network management policies and their associated device configuration models

7. Security Considerations

Security is a key aspect of any protocol that allows state installation and extracting of detailed configuration states. More investigation remains to fully define the security requirements, such as authorization and authentication levels.

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgements

The authors of this draft would like to thank the following persons for the provided valuable feedback: Spencer Dawkins, Jun Bi, Xing Li, Chongfeng Xie, Benoit Claise, Ian Farrer, Marc Blancet, Zhen Cao, Hosnieh Rafiee, Mehmet Ersue, Simon Perreault, Fernando Gont, Jose Saldana, Jean Francois Tremblay, Tom Taylor.

10. References

10.1. Normative References

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

10.2. Informative References

[ALTO] R. Alimi, R. Penno, Y. Yang, "ALTO Protocol", IETF Internet draft (work in progress), March 2014

[DevOps] DevOps website, http://devops.com/

[ID.draft-sun-aponf-openv6-use-cases] C. Xie, Q. Sun, JF. Tremblay, "Use case of IPv6 transition in APONF", IETF Internet draft Work in progress), draft-sun-aponf-openv6-use-cases-00, July 2014

[ID.draft-cheng-aponf-ddc-use-cases] Y. Cheng, C. Zhou, G. Karagiannis, JF. Tremblay, "Use Cases for Distributed Data Center

Applicatinos in APONF", IETF Internet draft (Work in progress), draft-cheng-aponf-ddc-use-cases-00, July 4, 2014

[ID.draft-huang-aponf-use-cases] C. Huang, Jiafeng Zhu, Peng He, Shucheng (Will) Liu, G. Karagiannis, "Use Cases on Application-centric Network Management and Service Provision" IETF Internet draft (Work in progress), draft-huang-aponf-use-cases-01, Juy 2014

[ID.draft-liu-aponf-using-abstract-view-use-case] W. Liu, T. Tsou, G. Karagiannis, J. Saldana, "APONF Use Case: Using Abstract View of Network by Application Developers", IETF Internet draft (Work in progress), draft-liu-aponf-using-abstract-view-use-case-00, July 4, 2014

[ID.draft-bi-aponf-sdsavi] J. Bi, G. Yao, "Software Defined SAVI", IETF Internet draft (Work in progress), draft-bi-aponf-sdsavi-00, July 4, 2014

[NIST SP 800-146] Badger et al.: "Draft Cloud Computing Synopsis and recommendations", NIST specifications, May 2011.

[RFC6241] R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC7039] J. Wu, J. Bi, M. Bagnulo, F. Baker, C. Vogt, "Source Address Validation Improvement (SAVI) Framework", IETF RFC 7039, October 2013.

[SFC] IETF SFC (Service Function Chaining) WG charter, http://datatracker.ietf.org/wg/sfc/charter/

Authors' Addresses

Georgios Karagiannis
University of Twente

Email: g.karagiannis@utwente.nl

Will(Shucheng) Liu
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com

Tina Tsou

Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: Tina.Tsou.Zouting@huawei.com

Qiong Sun
China Telecom
No.118 Xizhimennei street, Xicheng District
Beijing 100035
P.R. China

Email: sunqiong@ctbri.com.cn

Diego Lopez
Telefonica

Email: diego@tid.es