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

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

June 6, 2014

APONF Architecture
draft-zhou-aponf-architecture-00

Abstract

Currently, there are transport applications that have specific demands on a communication network. This document describes the APONF basic architecture, its elements and interfaces. The main APONF architecture entity is the Application-based Policy Decision (ABPD), which supports groups/classes of application models. Each of these models supports application demands that are similar in nature and therefore can be grouped/classified together. Moreover, the ABPD maps the classified application models into network capabilities, e.g., network management and traffic policies.

(http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

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

There are transport applications, see e.g., [ID.montpetit-transport-use-cases], that have specific and real time demands on the communication network. In particular, these demands require the use of specific network management and traffic policies which are currently not directly provided by the communication network to these applications. This introduces difficulties for the applications to use these network capabilities efficiently and may cause user experience degradation, e.g., congestion and delay. It is therefore, required that the communication network manages and/or controls the application traffic according to the requirements imposed by the application.

The application's demands on a communication network may be different, but there are several application demands that may be similar, such as Web Surfing/Browsing applications, IoT applications, virtual network function services, which can be grouped/classified together. The classified application demands on a communication network can be presented and modeled as classified application-based policies. A set of application-based policy models may be needed for auto-mapping of application's demands to existing network management and/or traffic policies.

This will allow applications to use the network capabilities in a more accurate and efficient way.
The main goal of this document is to specify the APONF basic architecture, its elements and interfaces. The main APONF architecture entity is the Application-based Policy Decision (ABPD), which supports classified application models.
The Application-based Policy Decision entity provides an interface to the application to generate the classified application models and to map these models to the network management and traffic policies that can be used by the communication network. The definition of these network management and traffic policies is out of the APONF scope.

2. Terminology

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 virtualisation infrastructure.

TAPS (Transport Services): The main goal of this activity (currently BOF) is to provide the means to applications to specify the services they can receive from the transport protocol, but

NFVcon (Network Functions Virtualization configuration): The main goal of this activity (BOF status) is to support the dynamic configuration of NFV instances.

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.

Abstraction and Control of Transport Networks (ACTN): 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.

3. Overview of the APONF Architecture

This section depicts an overview of the architecture of application-based policy on network functions. Figure 1 shows the basic

architecture of the application-based policy on network functions.
The entities used in the APONF architecture are:

O) Application: A transport application that needs to observe the network or manipulate the network to achieve its service requirements. Several applications may communicate with the Application Based Policy Decision block.

O) Application Based Policy Decision (ABPD): A functional entity Which provides an interface to the application to generate the grouped/classified application models and to map these models to existing network management and traffic policies that can be used by the communication network. It can communicate with multiple applications simultaneously.

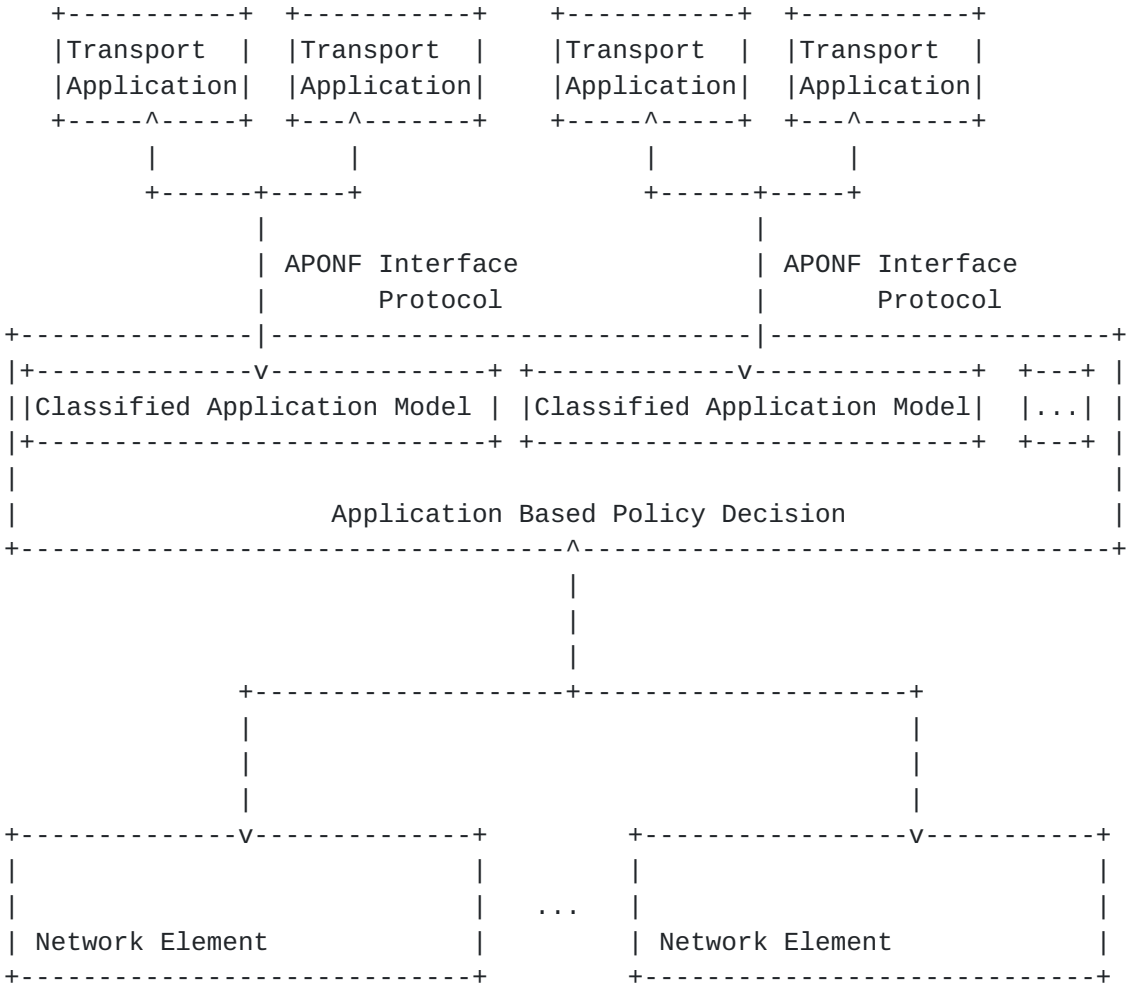

Figure 1: Architecture of application-based policy on network functions

o) Network Element (NE): A NE handles incoming packets based on the policy information communicated with the applications and enforces

the corresponding network management and traffic manipulation.

4. Transport Applications

The Transport Architecture entity represents transport applications. This architecture is expected to be used for several categories of transport applications, e.g., Web Surfing/Browsing, Streaming Video, Real-time Communications, Data storage, etc.

These transport Applications provide a set of application-based policy models which are imposing similar network management and traffic policy requirements on the communication network.
The application's demands on the network may be different, but some application's demands on the communication network may be similar, and can be grouped/classified together. Such similar application's demands can be: Web Surfing/Browsing applications, IoT applications, virtual network function services, etc. The classified application demands on a communication network can be presented and modeled as classified application-based policies and models.

The traditional applications can communicate real time, using an existing interface, e.g., netconf, restconf, or some new protocols proposed by interested parties, with the transport applications and exchange information requested by the Application-Based Policy Decision entity. The definition of this interface is out of the scope of this document.

The Transport Applications entity will use the APONF interface to communicate with the Application Based Policy Decision (ABPD) entity.

5. Application Based Policy Decision

The Application-Based Policy Decision (ABPD) block, is a an entity used between the Transport Application entity and the network elements to provide and maintain the application-based policies. It supports the APONF interface/protocol and is a software repository, which stores the information associated with each NE, and maps the classified application models to existing network management and traffic policies. In particular, by creating application-based policies that mirror application semantics, a better mapping to existing traffic and network management policies can be realized. This provides a simple, self-documenting mechanism for capturing application-based policy requirements and mapping them to existing traffic and network management policies. This will allow applications to use the network capabilities in a more accurate and efficient way.

The definition of these network management and traffic policies is out of the APONF scope. Examples of such existing network management and traffic policies that are considered by APONF are the following:

- o) Manage dynamically network semantics (supported by e.g., SNMP/MIB, COPS-PR/PIB, NetConf/Yang, CLI, Web Services/MIB, nfvcon (Network Function Virtualization configuration) activity).

- o) Orchestrate dynamically virtualized functions (supported by e.g., SCF WG, nfvcon activity, Abstraction and Control of Transport Networks (ACTN) activity).

o) Permit/Block/Redirect the traffic (supported by e.g., I2RS WG, FORCES WG, Application Enabled Collaborative Network (AECON) activity).

o) Log the traffic (supported by e.g., I2RS WG, FORCES WG, AECON activity).

o) Copy the traffic (supported by e.g., I2RS WG, FORCES WG, AECON activity).

o) Set the traffic (supported for/by e.g., NAT, Firewall, I2RS WG, FORCES WG, AECON activity).

o) Mark the traffic (supported for/by e.g., Intserv, Diffserv, PCN, MPLS).

These application-based policy models can meet the application's demands on the communication network and map these demands to network management and traffic policies that can be understood by the communication network.

6. Network Elements

The Network Element (NE) handles incoming packets based on the policy information communicated with the ABPD block and makes corresponding policy enforcement, which is based on existing network management and traffic policies, see Section 5.
A NE may be a physical entity or a virtual entity and is locally managed, whether via CLI, SNMP, or NeTConf. Examples of NEs can include:

- A router that has an extended function module. The extended module handles incoming packets basing on the flow table of the module.
- A server that runs vRouter or vSwitch.
- A CGN that runs NAT, Tunnel En/De-capsulation functions.
- A virtual network function (VNF) entity.

7. The APONF Interface/Protocol

This APONF Interface/Protocol, needs to be specified by the APONF WG and is used to support the communication between the Transport Application entity and the ABPD entity, see Section 5.

8. Security Considerations

Authentication and authorization mechanisms are needed to ensure that the transport applications communicating with the ABPD entity are

indeed authenticated and authorized. Furthermore, the privacy of the end users running the applications that make use of APONF must be protected.

9. IANA Considerations

This document has no actions for IANA.

10. Acknowledgements

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

11. References

11.1 Informative References

[ID.montpetit-transport-use-cases]
Montpetit, M. and I. Zhovnirovsky, "Use Cases and Requirements", Feb 2014.

Authors' Addresses

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

Email: cathy.zhou@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

Georgios Karagiannis
University of Twente

Email: g.karagiannis@utwente.nl