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

G. Karagiannis
University of Twente
W. Liu
T. Tsou
Huawei Technologies
Q. Sun
China Telecom
D. Lopez
Telefonica
June 6, 2014

Problem Statement for Application Policy on Network Functions (APONF)
draft-karagiannis-aponf-problem-statement-00

Abstract

As more and more modern network applications grow in scale and complexity, their demands and requirements on the supporting communication network will increase. In particular, these demands require the use of specific network management and traffic policies which currently are not provided directly by the communication network to these applications. Application demands that are similar in nature can be grouped together in grouped/classified application models. This draft specifies the need for application policy on network functions (APONF) APONF protocol(s), mechanisms and models required by transport applications to easily, accurately, and efficiently select and use the available communication network capabilities, i.e., network management and/or traffic policies.

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 December 5, 2014.

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. In particular, these demands require the use of specific network management and traffic policies which currently are not provided directly by the communication network to these applications.

Furthermore, and 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.

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.

Currently, there are transport applications that have specific demands on a communication network. For example, some specialized applications, like virtual network function services, may need to *dynamically manage* the network infrastructure, and other specialized applications, like streaming applications and Internet of Things (IoT) applications, may require from the network to treat their traffic according to their demands. If possible, an application may require from the communication network to apply the following different network management and/or traffic capabilities, such as:

- o) dynamically (re)configure a network entity
- o) accelerate the service deployment
- o) getting better network services from transport network
- o) providing better user experience

The application's demands on a communication network are different, but there are several application demands that may be similar, such as different Web Surfing/Browsing applications, IoT applications, virtual network function services, which can be grouped/classified together. The grouped/classified application demands on a communication network can be presented and modeled as grouped/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. These application-based policy models could 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.

The main goal of APONF is to specify the application-based policy protocol(s), mechanisms and models required by transport applications to easily, accurately, and efficiently select and use the available communication network capabilities, i.e., network management and/or traffic policies.

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 and privacy considerations. The IANA considerations are given in Section 8. Section 9 gives the acknowledgements and Section 10 lists the used references.

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 virtualization 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. Use Cases

This section briefly describes the use cases that are associated with different types of grouped/classified application-based policy models. The detailed description of these use cases is provided in other Internet draft(s).

3.1. Interactive Application Policy

This type of policy provides a bidirectional transport layer channel. The bidirectional channel needs to support data-loss protection and link detection. Both, the bandwidth and delay parameters of the bidirectional channel need to be configured to guarantee that application operates satisfactorily. Examples of applications that are using this policy are web surfing and voice call conference applications.

3.2. Streaming Application Policy

Streaming applications usually need large bandwidth and an unidirectional transport layer channel. In this type of applications the high bandwidth and the guaranteed delivery parameters of the unidirectional channel need to be configured on demand. Examples of applications that are using this policy are IPTV and VoD applications.

3.3. Media Sharing Application Policy

Media sharing application policies include capabilities such as media resource lookup and routing applied to reduce the use of the network bandwidth.

3.4. P2P Application Policy

P2P (Peer to Peer) applications are using P2P concepts such as P2P Content distribution and P2P content searching techniques. The P2P application policies include capabilities like mass sessions creation and media resource location.

3.5. Data Storage Application Policy

Applications, such as cloud computing applications need to be able to store and retrieve large amounts of data quickly and on demand. The Data Storage application policies include dynamic reconfiguration of data storage and dynamic increase/decrease of network bandwidth.

3.6. IOT Application Policy

Internet of Things (IoT) applications are using various types of communicating Internet enabled entities, e.g. sensors, robots, computers, that can be located in several geographical areas and which are able to monitor, generate and disseminate information during short periods of time. IoT application policies include short-duration session creation and route decision capabilities.

3.7. Virtualized Enterprise Application policy

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.

4. Requirements/Objectives

Before describing the APONF requirements/objectives a brief description on the network entities proposed in [APONF-architecture] is given below:

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. 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.

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.

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.

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

o) specify the APONF groups/classes of application policies and models

o) provide mechanisms that can accurately map and store the APONF groups/classes of application policies and models into existing network management and traffic policies.

o) specify the protocol and the required mechanisms that are able to support the communication between the transport applications and the ABPD entity that maintains the groups/classes of application policies and models.

o) provide the means to use existing network management and/or traffic conditioning protocols and mechanisms to enforce the application policies (via the associated network management and traffic policies) into network entities. Such protocols and mechanism are supported for/by e.g., SNMP/MIB, COPS-PR/PIB, NetConf/Yang, Web Services/MIB, nfvcon activity, SCF WG, ACT activity, I2RS WG, FORCES WG, AECON BOF activity, NAT, Firewall, Intserv, Diffsrerv, PCN, MPLS.

o) provide authentication and authorization mechanisms to support the communication between the Transport Application and the ABPD entity.

o) provide privacy support for the end users running the applications that make use of the APONF protocol and mechanisms.

5. Relationships between APONF and other IETF Working Groups

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

APONF is different than existing WGs and other IETF activities, due to the fact that APONF is the only activity that specifies the application-based policy protocol(s), mechanisms and models required by transport applications to easily, accurately, and efficiently

select and use the available communication network capabilities,
i.e., network management and/or traffic policies.
APONF may use existing network management and/or traffic conditioning
protocols and mechanisms to enforce the application policies into

network entities, see Section 6. Such protocols and mechanism are supported for/by e.g., SNMP/MIB, COPS-PR/PIB, NetConf/Yang, Web Services/MIB, nfvconf activity, SCF WG, ACT activity, I2RS WG, FORCES WG, AECON BOF activity, NAT, Firewall, Intserv, Diffsrerv, PCN, MPLS. The TAPS (Transport Services) activity may apply the Transport Application entity, see Section 4, in order to interact and use the grouped/classified application policies and models maintained by the ABPD entity.

6. Existing Protocols and Methods

The APONF protocol and mechanisms will have an impact on layers 4 and above.

The definition of the used 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).

7. 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.

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, Qiong Sun, Chongfeng Xie, Benoit Claise, Ian Farrer, Marc Blancet, Zhen Cao, Hosnieh Rafiee, Mehmet Ersue, Simon Perreault, Fernando Gont, Jose Saldana.

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

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

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

[APONF-architecture] C. Zhou, T. Tsou, Q. Sun, D. Lopez, G. Karagiannis, "APONF Architecture", IETF Internet draft, draft-zhou-aponf-architecture-00, June 2014

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