

INTERNET-DRAFT
Intended Status: Informational
Expires: April 16, 2015

R. Huang
H.Song
Huawei
October 13, 2014

Problem Statement and Use Cases for Application Intelligent
Policy Interface (AIPI)
draft-huang-appsawg-aipi-ps-uc-00

Abstract

This document discusses the problem statement and use cases of an interface named Application Intelligent Policy Interface (AIPI) that translates the real application requirements (e.g., network should ensure how many users of the OTT provider watch high definition video simultaneously.) into network level requirements, e.g., configurations or service deployments requirements and network QoS requirements, are useful and necessary for modern networks.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Copyright and License Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1	Introduction	3
2	Terminology	3
3.	Problem Statement	4
3.1	Gap Between Application Requirements and Network	4
3.2	Difficulty for Network adaptation	4
3.3	Difficulty for Network Policies Maintenance	5
4.	Use Cases for Application Intelligent Policy Interface	5
4.1	OTT Service Deployment	5
4.2	Enterprise Service Isolation and Interconnection	6
4.3	Automatic Adaptation	6
5	Existing Work	6
6	IANA Considerations	7
7	Security Considerations	7
8	Acknowledgments	7
9	References	7
9.1	Normative References	7
9.2	Informative References	8
	Authors' Addresses	8

1 Introduction

With the rapid development of network technologies, the network is more and more open. Many new technologies, e.g., SDN and NFV, etc., are emerging to help OTT application providers to get control of the network more flexibly than before. So far, these technologies are all network oriented, which based on network elements, ports, links, protocols or virtualization of the above. For those OTT application developers with little knowledge of network or small enterprise, they may not be able to fully utilize the network resources or correctly set network services to meet their requirements from the services and applications they provide.

This document further argues that an interface that translates the real application requirements (e.g., network should ensure how many users of the OTT provider watch high definition video simultaneously.) into network level requirements, e.g., configurations or service deployments requirements and network QoS requirements, are useful and necessary for modern networks. How the interface looks like is an issue outside the scope of the present document. The remainder of this document develops this idea into detail: Section 2 provides terminology; Section 3 discusses the problem statements; Section 4 provides some use cases in which the interface could be used, and Section 5 analyses the current related IETF work.

2 Terminology

AIPI: Application Intelligent Policy Interface, which is used for translating the application requirements to network level requirements.

Software-Defined Networking (SDN): A framework that supports the separation of Control and Forwarding Planes via standardized interfaces.

Network Functions Virtualization (NFV): A network architecture concept that proposes using IT virtualization related technologies to virtualize entire classes of network node functions into building blocks that may be connected, or chained, together to create communication services.

Network Policy: network level policies that can be directly used to configure the network elements

Application Intelligent Policy: Application oriented policies that reflect the QoS of the application service, but cannot be directly configured to network elements

3. Problem Statement

3.1 Gap Between Application Requirements and Network

Traditional network and applications effectively treat each other as black boxes. Network is effectively isolated from the end-systems, which then have little control over how the network handles packets. Likewise, the network has limited visibility on the application logic.

With the increasingly demanding of network opening, technologies like SDN and NFV becomes the future trends of network development. A key objective of this open network is to facilitate and exploit the virtualization of network functions so that they can be provided on a programmable basis for applications and service innovators. It seems to be a good way for OTT or enterprise applications to have some insight into network infrastructure. However, applications may focus more on service logic, service implementation, performance and experience, in stead of network information. Deep network capabilities exposed by the programmable network will be impossible for non-network-owning players to replicate.

Moreover, many different sets of network interfaces for applications are emerging. They provide network functions like path computation, loop avoidance, routing, security and many other tasks through abstracting and normalizing the quirks and eccentricities of different data plane devices. However, these interfaces are all network oriented. OTT applications may not adequately use these interfaces to fulfill their own requirement as they have no idea how their service running in the network really works. For example, OTT applications may not know which one is the most suitable path to choose. Also, there is no common consensus about how those parameters of network (e.g., bandwidth, delay, jitter, etc.) affect the QoE of OTT applications.

3.2 Difficulty for Network adaptation

Most of current interfaces really provides a way for OTT applications to easily apply for network resources or network functions or certain QoS (delay, loss, jitter). Due to the gap between OTT applications requirements and network, OTT applications may abuse these interface for their goods. For example, OTT applications may request more bandwidth than that they really need, or they may apply for some functions that they never use.

There are also some cases that requests from the OTT applications can't be accepted for network because of extravagant demands, while there do exist some other ways to fulfill the real requirements of

OTT applications. Obviously, current interfaces between OTT applications and network couldn't do network adaptations since network has no idea what OTT applications really want.

3.3 Difficulty for Network Policies Maintenance

Plenty varieties of requirements for service performance and access control breed plenty of complicated network configuration or QoS rules and ACL policies deployments. Usually these configurations and policies are maintained by network administrators who may not understand what the corresponding real service requirements are. With the change of network configuration and policies due to the updates of service requirements, e.g., new service deployment or old service expired, the maintenance of the network becomes more and more difficult especially along with the transfer of network administrators.

4. Use Cases for Application Intelligent Policy Interface

If network has an interface enabling OTT applications to input their own application service requirements and has the ability to translate the application service requirements to network requirement, problems will be solved. AIPI (application intelligent policy interface) is dedicated to cope with such problems. In this document, we mainly discuss several use cases that AIPI which is application friend could be applied.

4.1 OTT Service Deployment

OTT service providers can benefit from using such an application oriented interface so that they don't have to care about the underlay network details of no matter physical or virtual devices and functions. Instead, they just need to focus on what they are good at, which are their applications and services for end users.

Suppose an OTT video provider wants to activate the service which ensure 1000 end user to watch its high definition live video content simultaneously. Traditional way is to request some specific bandwidth resources or CDN services or VPN from ISPs. These kind of requests are usually exaggerated which may result in wasting of resources. When using AIPI, the OTT provider only needs to provide inputs from its perspective. For example, the OTT provider indicate that the video is 720p, and it's a live http streaming, and he wants his end users could watch fluently and the QoE should be excellent. Then ISP will analyse the requirements from the OTT provider, and translate them into network QoS, e.g., bandwidth >5120kpbs, RTT<120ms, jitter<50ms and loss<1%.

When OTT providers have same service deployments in different networks, they can also benefit by using AIPI. Same request can be transmitted by AIPI to different ISP networks instead of figuring out what network resources they need in each different network.

4.2 Enterprise Service Isolation and Interconnection

Enterprise networks are growing in complexity and size with globalization, outsourcing, and wireless expanding the reach of the network beyond its traditional design parameters. IT departments are tasked with ensuring the applications and services run well across both private and public networks. Add to that ongoing application and data center projects such as virtualization and cloud computing all the components that make up that network becomes even more of a challenge. Especially with the frequent personnel transfer of functions, locations or departments, IT departments are facing a huge workload.

AIPI is a way to make IT departments work more efficiently and effectively. Using AIPI, the administrators of IT departments just need to maintain the requirements from their enterprise and leave the automatic configurations and deployments to network service providers, which hence largely reduces the OPEX of IT departments.

4.3 Automatic Adaptation

AIPI is also helpful for network providers to achieve automatic adaptation for OTT service providers. With AIPI, network providers who know network the best will learn the real requirements from OTT service providers, and they certainly have the ability to figure out how to satisfy these requirements with minimum resources and maximum efficiency.

The advantage is also reflected when network problems affecting OTT service SLAs happen. For example, when a node on the specific OTT service path is experiencing congestions, network provider could just choose another path which satisfies the requirements for this OTT service without any communication with this OTT provider.

5 Existing Work

There are some existing efforts in IETF that may be related to this work. In this section, we give a detailed analysis towards them.

Application Enabled Collaborative Networking (AECON): AECON [AECON] is trying to work out ways to enable communication of flow characteristics between applications in end users and the network by

active information exchange. And the information communicated through AECON is network oriented.

Shared Unified Policy Automation (SUPA): The main goal of SUPA [SUPA] is to provide a way for network management applications and for network services to specify share application based policies to the network infrastructure using a simplified view of the network. SUPA is also a network oriented interface and does not really concern OTT applications.

Interface to the Routing System (I2RS): I2RS [I2RS] facilitates real-time or event driven interaction with the routing system through a collection of protocol-based control or management interfaces which allow information, policy and operational parameters to be injected into or retrieved from the routing system of network. It is network oriented as it collects and injects network information.

Application-Layer Traffic Optimization (ALTO): ALTO [ALTO] is considered as a solution to expose abstract topologies and costs to applications in P2P domain, datacenter networks and content distribution networks (CDN). It is also network oriented rather than application oriented.

AIPI tries to specify an application oriented interface which conveys the real application requirements to network and facilitates the translation from real application requirements to network requirements. AIPI is about the communication between Application deployment servers and network. AIPI could further use SUPA to configure or adjust network.

6 IANA Considerations

This draft includes no request to IANA.

7 Security Considerations

TBD.

8 Acknowledgments

The authors would like to thank Hanyu Wei for giving valuable comments and suggestions.

9 References

9.1 Normative References

[SUPA] IETF SUPA (Shared Unified Policy Automation) BoF Charter,

<https://github.com/liushucheng/SUPA/wiki/SUPA-Charter>

[AECON] IETF AECON (Application Enabled Collaborative Networking)
barBoF,
<http://trac.tools.ietf.org/bof/trac/wiki/BofIETF90#>

[I2RS] IETF I2RS (Interface to the Routing System) WG Charter,
<http://datatracker.ietf.org/wg/i2rs/charter/>

[ALTO] IETF ALOT (Application-Layer Traffic Optimization),
<http://datatracker.ietf.org/wg/alto/charter/>

9.2 Informative References

[NFV] http://en.wikipedia.org/wiki/Network_Functions_Virtualization

[SDN] <http://tools.ietf.org/html/draft-haleplidis-sdnrg-layer-terminology-06>

Authors' Addresses

Rachel Huang
Huawei
101 Software Avenue, Yuhua District
Nanjing 210012
China

EMail: rachel.huang@huawei.com

Haibin Song
Huawei
101 Software Avenue, Yuhua District
Nanjing 210012
China

EMail: songhaibin@huawei.com