Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 28, 2020

Z. Li
S. Peng
Huawei Technologies
D. Voyer
Bell Canada
C. Xie
China Telecom
P. Liu
China Mobile
C. Liu
China Unicom
K. Ebisawa
Toyota Motor Corporation
Y. Ueno
NTT Communications Corporation
S. Previdi
Individual
J. Guichard
Futurewei Technologies Ltd.
September 25, 2019

# Problem statement and use cases of Application-aware IPv6 Networking (APN6)

**draft-li-apn6-problem-statement-usecases-00**

Abstract

Operators are facing the challenges of providing better network services for users. As the ever-developing 5G and industrial verticals evolve, more and more services that have diverse network requirements such as ultra-low latency and high reliability are emerging and accessing the network, differentiated service treatments are desired by users. However, operators are still not aware of applications, which cause that only coarse-grained services can be provided to users. As a result, operators are only evolving to be large but dumb pipes without corresponding revenue increase. As the network technologies evolve including deployments of IPv6 and SRv6, the programmability provided by IPv6 and SRv6 encapsulations can be augmented by conveying the application related information into the network. Adding application knowledge to the network layer, allow applications to specify finer granularity requirements, which eventually bridges network and applications.

This document analyzes the existing problems of the current operators in the application awareness, and outlines various use cases that could benefit from the Application-aware IPv6 Networking (APN6).

## 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].

## Status of This Memo



## Copyright Notice



## Table of Contents

## 1. Introduction

Operators are facing the challenges of providing better network services for users. As the ever-developing 5G and industrial verticals evolve, more and more services that have diverse network requirements such as ultra-low latency and high reliability are emerging and accessing the network, differentiated service treatments are desired by users. However, operators are still not aware of applications, which cause that only coarse-grained services can be provided to users. As a result, operators are only evolving to be large but dumb pipes without corresponding revenue increase. As the network technologies evolve including deployments of IPv6 and SRv6, the programmability provided by IPv6 and SRv6 encapsulations can be augmented by conveying the application related information into the network. Adding application knowledge to the network layer, allow applications to specify finer granularity requirements, which eventually bridges network and applications.

This document analyzes the existing problems of the current operators in the application awareness, and outlines various use cases that could benefit from the Application-aware IPv6 Networking (APN6).

## 2. Terminology

ACL: Access Control List

APN6: Application-aware IPv6 Networking

DPI: Deep Packet Inspection

PBR: Policy Based Routing

QoE: Quality of Experience

## 3. Problem Statement

This section summarizes the challenges faced by the operators to satisfy the various requirements of applications and provide fine-granular traffic operations.

### 3.1. Large but dumb pipe

Currently, the network is still not aware of applications, that is, the network and applications are actually decoupled.  It is difficult for network operators to provide fine-granular traffic operations for performance-demanding applications.  In order to satisfy the SLA requirements operators continue to increase the network bandwidth but only carrying very light traffic load (around 30%-40% of its capacity).  This situation greatly increases the CAPEX and OPEX but only brings very little revenue from the carried services, which makes operators' network infrastructure large but dumb pipes.

### 3.2. Network on its own

As the network evolves, VPN/TE/FRR play important roles in satisfying the service isolation, SLA guarantee, and high reliability, etc. Those network technologies have been evolving themselves, which make the network features continuously upgrading.  However, such continuous upgrading doesn't bring corresponding revenue increase. Marginal Utility has been reduced, which has become the bottleneck of operators to increase their revenue.

### 3.3. Decoupling of network and applications

MPLS played a very important role in helping the network enter the generation of All-IP successfully.  However, MPLS actually doesn't allow a close interworking with the application layer since MPLS encapsulation is, typically, not used by the packet source.

As new services continuously evolve, more encapsulations are required, and this isolation and decoupling has further become the blockage towards the seamless convergence of the network and applications.

### 3.4. Challenges of traditional differentiated service provisioning

A number of IETF activities have been reviewed which are primarily intended to evolve the IP architecture to support new service definitions which allow preferential or differentiated treatment to be accorded to certain types of traffic.  The challenge when using

traditional ways to guarantee SLA is that the packets are not able to carry enough information for indicating applications and expressing their service/SLA requirements.  The network devices mainly rely on the 5-tuple of the packets or DPI.  However, there are some challenges of those traditional methods in differentiated service provisioning.

1.  Five tuples used for ACL/PBR

Five tuples are widely used for ACL/PBR.  However, they cannot provide enough information for the fine-grained service process, and can only be seen as indirect application information which needs to be translated in order to indicate a specific application.  It will further impact on the forwarding performance.

2.  Deep Packet Inspection (DPI)

If more information is needed, it has to be done through the use of DPI in order to deeply inspect the packets.  However, this will introduce more CAPEX and OPEX in the network and also it imposes security challenges.

3.  Orchestration and SDN-based solution

In the era of SDN, typically, a SDN controller is used to manage and operate the network infrastructure and orchestrator elements allow to introduce application requirements so that the network is programmed accordingly.  The SDN controller can be aware of the service requirements of the applications on the network through the interface with the orchestrator, and the service requirement is used by the controller for traffic management over the network.  However, this method raises the following problems:

1) The whole loop is long and time-consuming which is not suitable for the fast service provisioning for critical applications;

2) Too many interfaces are involved in the loop, as shown in Figure 1, which introduce challenges of standardization and inter-operability.

```
                     +--------------+
               /-----| Orchestrator | -------------------\
              /      +--------------+     Resource        \
APP Req.     /                     \        Management      \
       +---------+            +---------+       &        +---------+
       |SDN Ctrl1|            |SDN Ctrl2|    Service     |SDN Ctrl3|
       +---------+            +---------+  Provisioning  +---------+
APP Req. /     \             /           \             /           \
      +-/-+  +--\--+  +-----------+  +-----------+  +-----------+  +-----------+
      |APP|  | DCN |  |Network D1|..|Network D3|  |Network D4|..|Network D6|
      +---+  +-----+  +-----------+  +-----------+  +-----------+  +-----------+
```

Figure 1. Many interfaces involved in the long service-provisioning loop

### 3.5. Challenges of supporting new 5G and edge computing

As the continuous development of 5G, IoT, and edge computing, more and more new type of services are (and will be) accessing network. Vast volume of network traffic with diverse requirements such as low latency and high reliability rapidly increases. If we continue to use traditional methods, it will cause much higher CAPEX and OPEX to satisfy the ever-developing applications' diverse requirements.

## 4. Application-aware IPv6 Networking (APN6)

To resolve the above-mentioned issues, one possible way is to convey the application characteristic information (including application identification and network performance requirements) into the network, and make the network aware of application characteristic information more quickly in order to perform the fine-granularity network resource adjustment and SLA performance guarantee, hence to better serve demanding applications.

The IPv6 encapsulation including its extension headers (EH) [RFC8200] are well suited for a good programmability and can be utilized to encapsulate application information as well as other necessary information. EH provides very good foundations for the application-aware fine-granularity service provisioning. We name this technology as APN6.

The advantages of using IPv6 to support APN6 include,

1. Simplicity: Conveying application information with IPv6 encapsulation can just be based on IP reachability.

2. Seamless convergence: Much easier to achieve seamless convergence between applications and network since both are based on IPv6.

3. Great extensibility: IPv6 encapsulation including its extension headers can be used to carry very rich information relevant to applications.

4. Good compatibility: On-demand network upgrade and service provisioning. If the application information is not recognized by the node, the packet will be forwarded based on pure IPv6, which ensure backward compatibility.

5. Little dependency: Information conveying and service provisioning are only based on the forwarding plane of devices, which is different from the Orchestration and SDN-based solution which involves multiple elements and diverse interfaces.

6. Quick response: Flow-driven and direct response from devices since it is based on the forwarding plane.

APN6 has the following key elements,

1. Application information is conveyed by the IPv6 encapsulation: The conveyed application characteristic information (application-aware information) includes application identification and/or its network performance requirements. This element is not enforced but actually provides an open option for applications to decide whether to input this application-aware information.

2. Application information and network service provisioning matching: provide fine-granularity network service provisioning (traffic operations) and SLA guarantee based on the application-aware information carried in IPv6 packets. This element provides the network capabilities to applications. According to the application-aware information, appropriate network services are selected and provisioned to the demanding applications and satisfy their performance requirements.

3. Network measurement based on IPv6: measure the network performance and update the matching between the applications and corresponding network services in order for better fine-granularity SLA compliance. The network measurement methods include in-band and out-of-band, passive, active, per-packet, per-flow, per node, end-to-end, etc. These methods can also be integrated.

```
             Applications         |          Network

   Element 1: Conveying  -------------------->
                                 /|\
             Application Info     |     Network capabilities
                                  |       (SLA guarantee)
                                  |             /|\
                         Element 2: Matching     |
                                                 |
                                     Element 3: Network Measurement
```

Figure 2. Illustration of the key elements of APN6

## 5. Use cases of APN6

This session provides the use cases that can benefit from the application awareness. The corresponding requirements for APN6 are also outlined.

### 5.1. App-aware SLA Guarantee

Among various applications being carried and running in the network, some revenue-producing applications such as online gaming, video streaming, and enterprise video conferencing have much more demanding performance requirements such as low network latency and high bandwidth. In order to achieve better Quality of Experience (QoE) of the end users and engage customers, the network needs to be able to provide fine-granularity and even application-level SLA guarantee. Differentiated service provisioning is desired.

One of the key objective of APN6 is for operators to provide fine-granularity SLA guarantee instead of coarse-grain traffic operations. This will enable operators to provide differentiated services for different applications of their customers and make increase revenue accordingly.

Requirements for APN6:

For achieving App-aware SLA Guarantee, APN6 needs to perform the three key elements as described in Section 4. Application-level fine-granularity traffic operation that may include finer QoS scheduling is the key to guarantee the SLA of each specific demanding application.

### 5.2. App-aware network slicing

More and more applications/services with diverse requirements are being carried over and sharing operators' network infrastructure, the same to the enterprise case. However, it is still desired to have customized network transport that is able to support some application's specific requirements, considering also the service and resource isolation, which drives the concept of network slicing.

Network slicing provides ways to partition the network infrastructure in either control plane or data plane into multiple network slices that are running in parallel. These network slices can serve diverse services and fulfill their various requirements at the same time. For example, the mission critical application that requires ultra-low latency and high reliability can be provisioned over a separated network slice.

Requirements for APN6:

For achieving App-aware network slicing, APN6 needs to perform the three key elements as described in Section 4 in the context of network slicing. To be more specific, for the element 2, it needs to match to a specific network slice according to the application information carried in the IPv6 packets. The network measurement in element 3 also needs to happen within each network slice.

### 5.3. App-aware deterministic networking

[RFC8578] documents use cases for diverse industry applications that require deterministic flows over multi-hop paths. Deterministic flows provide guaranteed bandwidth, bounded latency, and other properties relevant to the transport of time-sensitive data, and can coexist on an IP network with best-effort traffic. It also provides for highly reliable flows through provision for redundant paths.

Requirements for APN6:

For achieving App-aware deterministic networking, APN6 needs to perform the three key elements as described in Section 4 in the context of deterministic networking. To be more specific, for the element 2, it needs to match to a specific deterministic path according to the application information carried in the IPv6 packets. The network measurement in element 3 also needs to be performed on each app-aware deterministic path.

### 5.4. App-aware service function chaining

The end-to-end service delivery often needs to go through various service functions, including traditional network service functions such as firewalls, DPI as well as new application-specific functions, both physical and virtual. The definition and instantiation of an ordered set of service functions and subsequent steering of the traffic through them is called Service Function Chaining (SFC) [RFC7665]. SFC is applicable to both fixed and mobile networks as well as data center networks.

Generally, in order to manipulate a specific application traffic along the SFC, a DPI needs to be deployed as the first service function of the chain to detect the application, which will impose high CAPEX and consume long processing time. For the encrypted traffic, it even becomes impossible to inspect the application.

Requirements for APN6:

For achieving App-aware service function chaining, APN6 needs to perform the three key elements as described in Section 4 in the context of service function chaining. To be more specific, for element 1 class information can be conveyed. For element 2, it needs to match to a specific service function chain and subsequent steering according to the application information carried in the IPv6 packets. The network measurement in element 3 also needs to happen within each app-aware service function chain.

### 5.5. App-aware network measurement

Network measurement can be used for locating silent failure and predicting QoE satisfaction, which enables real-time SLA awareness/ proactive OAM. Operations, Administration, and Maintenance (OAM) refers to a toolset for fault detection and isolation, and network performance measurement. In-situ Operations, Administration, and Maintenance (IOAM) records operational and telemetry information in the packet while the packet traverses a path between two points in the network.

Requirements for APN6:

For achieving App-aware network measurement, APN6 needs to perform the two key elements as described in Section 4 in the context of network measurement. The network measurement in element 3 does not need to be considered here.

## 6. IANA Considerations

This document does not include an IANA request.

## 7. Security Considerations

Since the application information is conveyed into the network, it does involve some security and privacy issues.

First of all, APN6 only provides the capability to the applications to provide their profiles and requirements to the network, but it leaves the applications to decide whether to input this information. If the applications decide not to provide any information, they will be treated in the same way as today's network and cannot get the benefits from APN6.

Once the application information has been carried in the IPv6 packets and conveyed into the network, the IPv6 extension headers, AH and ESP, can be used to guarantee the authenticity of the added application information.

Any scheme involving an information exchange between layers (application and network layers in this case) will obviously require an accurate valuation of security mechanism in order to prevent any leak of critical information.  Some additional considerations may be required for multi-domain use cases.  For example, how to agree upon which application information/ID to use and guarantee authenticity for packets traveling through multiple domains (network operators).

## 8. Acknowledgements

The authors would like to acknowledge Robert Raszuk for his valuable review and comments.

## 9. Contributors

Liang Geng
China Mobile
China

Email: gengliang@chinamobile.com

Chang Cao
China Unicom
China

Email: caoc15@chinaunicom.cn

Cong Li
China Telecom
China

Email: licong.bri@chinatelecom.cn

# 10. References

## 10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

## 10.2. Informative References

[I-D.ietf-6man-segment-routing-header] Filsfils, C., Dukes, D., Previdi, S., Leddy, J., Matsushima, S., and d. daniel.voyer@bell.ca, "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header-23 (work in progress), September 2019.

[I-D.ietf-spring-srv6-network-programming] Filsfils, C., Camarillo, P., Leddy, J., daniel.voyer@bell.ca, d., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-02 (work in progress), September 2019.

Authors' Addresses

Zhenbin Li
Huawei Technologies
China

Email: lizhenbin@huawei.com

Shuping Peng
Huawei Technologies
China

Email: pengshuping@huawei.com

Daniel Voyer
Bell Canada
Canada

Email: daniel.voyer@bell.ca

Chongfeng Xie
China Telecom
China

Email: xiechf.bri@chinatelecom.cn

Peng Liu
China Mobile
China

Email: liupengyjy@chinamobile.com

Chang Liu
China Unicom
China

Email: liuc131@chinaunicom.cn

Kentaro Ebisawa
Toyota Motor Corporation
Japan

Email: ebisawa@toyota-tokyo.tech

Yukito Ueno
NTT Communications Corporation
Japan

Email: yukito.ueno@ntt.com

Stefano Previdi
Individual
Italy

Email: stefano@previdi.net

James N Guichard
Futurewei Technologies Ltd.
USA

Email: jguichar@futurewei.com