Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 26, 2021

Z. Li
S. Peng
Huawei Technologies
D. Voyer
Bell Canada
C. Li
China Telecom
P. Liu
China Mobile
C. Cao
China Unicom
G. Mishra
Verizon Inc.
K. Ebisawa
Toyota Motor Corporation
S. Previdi
Huawei Technologies
J. Guichard
Futurewei Technologies Ltd.

May 25, 2021

Application-aware Networking (APN) Framework
draft-li-apn-framework-03

Abstract

A multitude of applications are carried over the network, which have varying needs for network bandwidth, latency, jitter, and packet loss, etc. Some new emerging applications have very demanding performance requirements. However, in current networks, the network and applications are decoupled, that is, the network is not aware of the applications' requirements in a fine granularity. Therefore, it is difficult to provide truly fine-granularity traffic operations for the applications and guarantee their SLA requirements.

This document proposes a new framework, named Application-aware Networking (APN), where application-aware information (i.e. APN attribute) including APN identification (ID) and/or APN parameters (e.g. network performance requirements) is encapsulated at network edge devices and carried in packets traversing an APN domain in order to facilitate service provisioning, perform fine-granularity traffic steering and network resource adjustment.

Status of This Memo

This Internet-Draft will expire on November 26, 2021.

Copyright Notice

Table of Contents

1. Introduction

A multitude of applications are carried over the network, which have varying needs for network bandwidth, latency, jitter, and packet loss, etc. Some applications such as online gaming and live video streaming have very demanding network requirements and therefore require special treatment in the network. However, in current networks, the network and applications are decoupled, that is, the network is not aware of the applications' requirements in a fine granularity. Therefore, it is difficult to provide truly fine-granularity traffic operations for the applications and guarantee their SLA requirements accordingly. [I-D.li-apn-problem-statement-usecases] describes the challenges of traditional differentiated service provisioning methods, such as five tuples used for ACL/PBR causing coarse granularity as well as orchestration and SDN-based solution causing long control loops.

This document proposes a new framework, named Application-aware Networking (APN), where application-aware information (APN attribute) including application-aware identification (APN ID) and application-aware parameters (APN Parameters), is encapsulated at network edge devices and carried along with the encapsulation of the tunnel that is used by the packet to traverse the APN domain. The APN attribute will facilitate service provisioning and provide fine-granularity services in the APN domain.

The APN attribute is acquired based on the existing information in the packet header such as 5-tuple and QinQ (S-VLAN and C-VLAN) at the edge devices of the APN domain, added to the data packets along with the tunnel encapsulation, delivered within the network, and removed when the packets leave the domain together with the tunnel encapsulation.

APN aims to apply various policies in different nodes along a network path onto a traffic flow altogether, for example, at the headend to steer into corresponding path, at the midpoint to collect corresponding performance measurement data, and at the service function to execute particular policies.

APN works within a limited trusted domain. Typically, an APN domain is defined as a Network Operator controlled limited domain (see Figure 1), in which MPLS, VXLAN, SR/SRv6 and other tunnel technologies are adopted to provide network services.

2. Specification of Requirements

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].

This document is not a protocol specification and the key words in this document are used for clarity and emphasis of requirements language.

3. Terminology

ACL: Access Control List

APN: Application-aware Networking

APN6: Application-aware Networking for IPv6/SRv6

LB: Load Balancing

MPLS: Multiprotocol Label Switching

PBR: Policy Based Routing

QoE: Quality of Experience

SDN: Software Defined Networking

SLA: Service Level Agreement

SR: Segment Routing

SR-MPLS: Segment Routing over MPLS dataplane

SRv6: Segment Routing over IPv6 dataplane

4. APN Framework and Key Components

The APN framework is shown in Figure 1. The key components include App-aware Edge Device (APN-Edge), App-aware-process Head-End (APN-Head), App-aware-process Mid-Point (APN-Midpoint), and App-aware-process End-Point (APN-Endpoint).

Packets carry application characteristic information (i.e. APN attribute) which includes the following information:

- o Application-aware identification (APN ID): identifies the set of attributes, indicating that all packets belonging to the same flow will be given the same treatment by the network. ;

- o Application-aware parameters (APN parameters): The typical application-aware parameters are the network performance requirement parameters including bandwidth, delay, delay variation, packet loss ratio, etc.

```
Client                                                             Server
+-----+                                                            +-----+
|App x|-\                                                       /->|App x|
+-----+ |   +-----+ +-----+   +---------+   +--------+ +-----+  |  +-----+
         \->|APN  | |APN  |-A-|APN      |-A-|APN     | |APN  |->/
User side   |-    |-|-    |-B-|-        |-B-|-       |-|-    |
         /->|Edge | |Head |-C-|Midpoint |-C-|Endpoint| |Edge |->\
+-----+ |   +-----+ +-----+   +---------+   +--------+ +-----+  |   +-----+
|App y|-/      |------------------APN Domain--------------|      \->|App y|
+-----+                                                             +-----+
```

Figure 1: Framework and Key Components

The key components are introduced as follows.

- o App-aware Edge Device (APN-Edge): this network device receives packets from applications and obtains the APN attribute based on the configuration on this device according to the existing information in the packet header, such as 5-tuple, VLAN or double VLAN tagging (C-VLAN and S-VLAN). The APN-Edge device adds the APN attribute in the tunnel encapsulation. The packets carrying the APN attribute will be sent to the APN-Head, and the APN attribute will be used to apply various policies in different nodes along the network path onto the traffic flow, e.g., at the headend to steer into corresponding path satisfying SLAs, at the midpoint to collect corresponding performance measurement data, at the service function to execute particular policies. When the packets leave the APN domain, the APN attribute will be removed together with the tunnel encapsulation.

- o App-aware-process Head-End (APN-Head): This network device receives packets from the APN-Edge, obtains the APN attribute, and initiates the corresponding process. Generally, in order to satisfy different SLA requirements, a set of paths, tunnels or SR policies, are set up between the APN-Head and the APN-Endpoint.

These multiple parallel paths have different SLA guarantees. The APN-Head maintains the matching relationship between the APN attribute and the paths between the APN-Head and the APN-Endpoint. The APN-Head determines the path between the APN-Head and the APN-Endpoint according to the APN attribute carried in the packets and the matching relationship with it, which satisfies the service requirements of the applications. The APN-Head forwards the packets along the path. The APN attribute conveyed by the packet received from the APN-Edge can also be copied or be mapped to the outgoing packet header.

o App-aware-process Mid-Point (APN-Midpoint): the APN-Midpoint provides the path service and enforces various policies according to the APN attribute carried in the packets. The APN-Midpoint may also adjust the resource locally to guarantee the service requirements depending on a specific policy and the APN attribute conveyed by the packet. Policy definitions and mechanisms are out of the scope of this document.

o App-aware-process End-Point (APN-Endpoint): the process of the specific service path will end at the APN-Endpoint. If the outer tunnel header for the path between the APN-Head and the APN-Endpoint exists, it will be removed by the APN-Endpoint. If the APN attribute is copied or mapped to the outer tunnel header by the APN-Head, it will also be removed along with the outer tunnel header.

Note that in the actual implementation, the APN-Edge can co-exist with the APN-Head or APN-Endpoint, that is, one network device can implement the functionalities of both APN-Edge and the APN-Head/APN-Endpoint.

5. APN Requirements

This section specifies the requirements for supporting the APN framework, including the requirements for conveying and handling the APN attribute.

5.1. APN Attribute Conveying Requirements

The APN attribute consists of APN ID and APN parameters.

APN ID includes the following identifiers (IDs),

o Application Group ID: identifies an application group of the traffic.

o User Group ID: identifies the user group of the traffic.

APN ID can be acquired through different ways. In the APN work it MUST be acquired according to the existing available information in the packet header without inspection into the payload.

The different combinations of the IDs can be used to provide different granularity of the service provisioning and SLA guarantee for the traffic.

The APN parameters are the network performance requirement parameters. The network service requirement can include the following parameters:

- Bandwidth: the bandwidth requirement

- Latency: the latency requirement

- Packet loss ratio: the packet loss ratio requirement

- Jitter: the jitter requirement

The different combinations of the parameters are for further expressing the more detailed service requirements, conveyed together with the APN ID, which can be used to match to appropriate tunnels/SR Policies and queues that can satisfy these service requirements.

APN attribute MUST be encapsulated within tunnels in the network layer. The tunnels include but not limit to MPLS, VxLAN, SR-MPLS, and SRv6. It can be extended according to requirements in the future.

[REQ 1a]. APN ID SHOULD include Application Group ID to indicate the application group that the packet belongs to.

[REQ 1b]. APN ID SHOULD include User Group ID to indicate the user group that the packet belongs to.

[REQ 1c]. APN ID MUST include either Application Group ID or User Group ID.

[REQ 1d]. APN ID MUST be acquired from the existing available information of the packet header without interference into the payload.

[REQ 1e]. APN parameters is OPTIONAL.

[REQ 1f]. APN attribute MUST be carried by the outer tunnel encapsulation.

[REQ 1g]. All the nodes along the path SHOULD be able to process the APN attribute if needed.

[REQ 1h]. The APN attribute is generated by the APN-Edge though local policy.

[REQ 1i]. The APN attribute SHOULD be kept intact when directly copied at the APN-Head and carried in the tunnel encapsulation.

[REQ 1j]. The APN attribute MUST be removed along with the tunnel encapsulation by the APN-Edge when the packets leave the APN domain.

5.1.1. Protocol Extensions Requirements

The APN attribute is conveyed with the tunnel encapsulation. There are two typical types of tunnels:

- MPLS-based tunnel: LDP tunnel, RSVP-TE tunnel, SR-MPLS tunnel or policy, etc.

- IPv6-based tunnel: IPv6-based VxLAN tunnel, IPv6-based UDP tunnel, IPv6-based GRE tunnel, SRv6 tunnel or policy, etc.

In order to support encapsulation of APN attribute, the MPLS data plane and IPv6 data plane need to be extended.

In order to support acquiring the APN attribute according to the existing available information in the packet header, YANG models should be defined to configure the mapping between the application/user group ID and the existing information in the packet header and configure the corresponding APN attribute for the application/user group. It can also be implemented with protocol extensions such as BGP and PCEP which can advertise the information from the central controller to the APN-Edge.

In addition, in the APN domain, the above-mentioned mapping and applying APN parameters may also be advertised from the APN-Edge/APN-Head to other devices or from the network devices to the central controller in the APN domain. IGP extensions or BGP-LS extensions should be introduced to achieve the purposes.

[REQ 1-1a] MPLS encapsulation SHOULD be extended to be able to carry the APN attribute for MPLS-based tunnels.

[REQ 1-1b] IPv6 encapsulation SHOULD be extended to be able to carry the APN attribute for IPv6-based tunnels.

[REQ 1-1c] YANG models SHOULD be defined to implement the mapping between the application/user group ID and the existing available information in the packet header and configure the corresponding APN parameters.

[REQ 1-1d] BGP extensions SHOULD be defined to advertise the mapping between the application/user group ID and the existing available information in the packet header and the corresponding APN parameters from the central controller to the APN-Edge in the APN domain.

[REQ 1-1e] PCEP extensions SHOULD be defined to advertise the mapping between the application/user group ID and the existing available information in the packet header and the corresponding APN parameters from the central controller to the APN-Edge in the APN domain.

[REQ 1-1f] IGP extensions SHOULD be defined to advertise the mapping between the application/user group ID and the existing available information in the packet header and the corresponding APN parameters from the APN-Edge to the network devices in the APN domain.

[REQ 1-1g] BGP-LS extensions SHOULD be defined to advertise the mapping between the application/user group ID and the existing available information in the packet header and the corresponding APN parameters from the network devices to the central controller in the APN domain.

5.2. APN attribute Handling Requirements

The APN Head and APN-Midpoint perform matching operation against the APN attribute, that is, to match IDs and/or service requirements to the corresponding network resources such as tunnels/SR policies and queues.

5.2.1. App-aware SLA Guarantee

In order to achieve better Quality of Experience (QoE) of end users and engage customers, the network needs to be able to provide fine-granularity SLA guarantee [I-D.li-apn-problem-statement-usecases].

[REQ 2-1a]. With the APN attribute, the APN-Head SHOULD be able to steer the traffic to the tunnel/SR policy that satisfies the matching operation.

[REQ 2-1b]. With the APN attribute, the APN-Head SHOULD be able to trigger the setup of the tunnel/SR policy that satisfies the matching operation.

[REQ 2-1c]. With the APN attribute, the APN-Head and APN-Midpoint SHOULD be able to steer the traffic to the queue that satisfies the matching operation.

[REQ 2-1d]. With the APN attribute, the APN-Head and APN-Midpoint SHOULD be able to trigger the configuration of the queue that satisfies the matching operation.

[REQ 2-1e]. If the tunnels are used to satisfy the performance requirements, the APN-Head SHOULD be able to copy or map the APN attribute conveyed by the packet received from the APN-Edge to the outer tunnel header.

[REQ 2-1f]. If the tunnels are used to satisfy the performance requirements and the APN attribute are conveyed along with the outer tunnel, the APN-Endpoint MUST remove the APN attribute along with the outer tunnel.

5.2.2. App-aware 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. The resources on each node need to be associated to corresponding slices.

[REQ 2-2a]. With the APN attribute, the APN-Head SHOULD be able to steer the traffic to the slice that satisfies the matching operation.

[REQ 2-2b]. With the APN attribute, the APN-Midpoint SHOULD be able to associate the traffic to the resources in the slice that satisfies the matching operation.

5.2.3. App-aware deterministic networking

Along the path each node needs to provide guaranteed bandwidth, bounded latency, and other properties relevant to the transport of time-sensitive data for the Detnet flows that coexist with the best-effort traffic.

[REQ 2-3a]. With the APN attribute, the APN-Head SHOULD be able to steer the traffic to the appropriate path that satisfies the matching operation.

[REQ 2-3b]. With the APN attribute, the APN-Head SHOULD be able to trigger the setup of the appropriate path that satisfies the matching operation for the Detnet flows.

[REQ 2-3c]. With the APN attribute, the APN-Midpoint SHOULD be able to associate the traffic to the resources along the path that satisfies the performance guarantee.

[REQ 2-3d]. With the APN attribute, the APN-Midpoint SHOULD be able to reserve the resources for the Detnet flows along the path that satisfies the performance guarantee.

5.2.4. 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, LB as well as new application-specific functions, both physical and virtual. SFC is applicable to both fixed and mobile networks as well as data center networks.

[REQ 2-4a]. With the APN attribute, the App-aware-process devices SHOULD be able to steer the traffic to the appropriate service function.

[REQ 2-4b]. The App-aware-process devices including VAS SHOULD be able to process the APN attribute carried in the packets.

5.2.5. App-aware network measurement

Network measurement can be used for verifying whether the network performance requirements have been satisfied, as well as locating silent failure and predicting QoE satisfaction, which enables real-time SLA awareness/proactive OAM and potential resource adjustments.

[REQ 2-5a]. The App-aware-process devices SHOULD be able to perform IOAM based on the APN attribute.

[REQ 2-5b]. The network measurement results can be reported based on the APN attribute and verify whether the performance requirements are satisfied.

6. IANA Considerations

This document does not include an IANA request.

7. Security Considerations

In the APN work, in order to reduce the privacy and security issues, the following specifications are defined:

[S1]. The APN attribute MUST be conveyed along with the tunnel information in the APN domain. The APN attribute is encapsulated and removed at the APN-Edge.

[S2]. The APN ID (including the Application Group ID and the User Group ID) MUST be acquired from the existing available information in the packet header without interference into the payload.

According to the above specifications, the APN attribute is only produced and used locally within the APN domain without the involvement of the host/application side.

In order to prevent the malicious attack through the APN attribute, the following policies can be configured at the network devices of the APN domain:

[P1]. If the APN attribute is conveyed without the tunnel information, the packet MUST be dropped.

[P2]. If the APN attribute is not known to the APN domain, it should trigger the alarm information. The packet can be forwarded without being processed or dropped depending on the local policy.

[P3]. If the network service requirements exceed the specification for the specific Application Group ID and/or User Group ID, it should trigger the alarm information. The packet should be discarded to prevent abusing of the resources.

[P4]. There should be rate-limiting policy at the APN-Edge to prevent the traffic belonging to a specific Application Group ID and/or User Group ID from exceeding the preset limit.

8. Acknowledgements

The authors would like to acknowledge Robert Raszuk (Bloomberg LP), and Yukito Ueno (NTT Communications Corporation) for their valuable reviews and comments.

9. Contributors

Daniel Bernier
Bell Canada

Email: daniel.bernier@bell.ca

Chongfeng Xie
China Telecom

Email: xiechf@chinatelecom.cn

Feng Yang
China Mobile

Email: yangfeng@chinamobile.com

Zhuangzhuang Qin
China Unicom

Email: qinzhuangzhuang@chinaunicom.cn

Chang Liu
China Unicom

Email: liuc131@chinaunicom.cn

Gyan Mishra
Verizon

Email: hayabusagsm@gmail.com

Luis M. Contreras
Telefonica

Email: contreras.ietf@gmail.com

Luc-Fabrice Ndifor Ngwa
MTN

Email: Luc-Fabrice.Ndifor@mtn.com

10. References

10.1. Normative References

[I-D.li-apn-problem-statement-usecases]
Li, Z., Peng, S., Voyer, D., Xie, C., Liu, P., Qin, Z., Ebisawa, K., Previdi, S., and J. N. Guichard, "Problem Statement and Use Cases of Application-aware Networking (APN)", draft-li-apn-problem-statement-usecases-01 (work in progress), September 2020.

[I-D.peng-apn-security-privacy-consideration]
Peng, S., Li, Z., Voyer, D., Li, C., Liu, P., and C. Cao, "APN Security and Privacy Considerations", draft-peng-apn-security-privacy-consideration-00 (work in progress), September 2020.

[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

[RFC3272] Awduche, D., Chiu, A., Elwalid, A., Widjaja, I., and X. Xiao, "Overview and Principles of Internet Traffic Engineering", RFC 3272, DOI 10.17487/RFC3272, May 2002, <https://www.rfc-editor.org/info/rfc3272>.

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

Cong Li
China Telecom
China

Email: licong@chinatelecom.cn

Peng Liu
China Mobile
China

Email: liupengyjy@chinamobile.com

Chang Cao
China Unicom
China

Email: caoc15@chinaunicom.cn

Gyan Mishra
Verizon Inc.
USA

Email: gyan.s.mishra@verizon.com

Kentaro Ebisawa
Toyota Motor Corporation
Japan

Email: ebisawa@toyota-tokyo.tech

Stefano Previdi
Huawei Technologies
Italy

Email: stefano@previdi.net

James N Guichard
Futurewei Technologies Ltd.
USA

Email: jguichar@futurewei.com