Network Working Group S. Peng
Internet-Draft Z. Li
Intended status: Informational Huawei Technologies
Expires: June 19, 2021 December 16, 2020

APN Scope and Gap Analysis
draft-peng-apn-scope-gap-analysis-00

Abstract

The APN work in IETF is focused on developing a framework and set of mechanisms to derive, convey and use an identifier to allow for implementing fine-grain user-, application-, and service-level requirements at the network layer. This document describes the scope of the APN work and the solution gap analysis.

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

Application-aware Networking (APN) is introduced in [I-D.li-apn-framework] and [I-D.li-apn-problem-statement-usecases]. APN conveys an identifier along with data packets into network [I-D.li-6man-app-aware-ipv6-network] and make the network aware of fine-grain user-, application-, and service-level requirements.

Such identifier is acquired, constructed in a structured value, and then encapsulated in the packets. Such structured value is treated as an opaque object in the network, to which the network operator applies policies in various nodes/service functions along the path and provide corresponding services. The identifier may represent the application traffic of a particular user but does not identify the actual user nor the actual application for network operators.

The example use-case presented in this draft further expands on the rationale for such identifier and how it can be derived and used in that specific context.

This document describes the scope of the APN work and the solution gap analysis.

2. Terminologies

APN: Application-aware Networking

CPE: Customer Premises Equipment

DPI: Deep Packet Inspection

OS: Operating System

3. APN Framework and Scope

The APN framework is introduced in [I-D.li-apn-framework], as shown in the Figure 1.

```
+-----+                                                    +-----+
|App x|-\                                                /-|App x|
+-----+ |  +-----+   +-----------------------+   +-----+ | +-----+
         \-|App- |   |   Application-aware   |   |App- |-/
           |aware|---|        Network        |---|aware|
         /-|Edge |   |  Service Provisioning |   |Edge |-\
+-----+ |  +-----+   +-----------------------+   +-----+ | +-----+
|App y|-/     |                                     |    \-|App y|
+-----+       |<--- Network Operator Controlled --->|      +-----+
                            Limited Domain
```

Figure 1. APN Framework and Scope

With APN, the identifier is added to the data packets (e.g. in the IPv6 extensions headers [I-D.li-6man-app-aware-ipv6-network]) and delivered to the network, wherein, according to this identifier, corresponding network services are provisioned.

The identifier can be added either directly by the application (e.g. App x in the Figure 1) or at the network edge devices (i.e. App-aware Edge in the Figure 1), named as host-side solution and network-side solution, respectively.

With the host-side solution, after the identifier is obtained by application, it will be added to the data packets during its encapsulation process going through the protocol stack in the OS. The host-side solution may require an update of the underlying operating system in order to allow the application element to pass the identifier to the socket service when building the packet header.

With the network-side solution, the identifier is added according to the configured policy at the network edge device. For the APN work to be conducted in IETF, we will focus on the network-side solution.

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.

4. Example Use Case and Existing Issues

To be more specific and more concrete, here we use SD-WAN as an example use case to further expand on the rationale for such identifier and how it can be derived and used in that specific context.

In the case of SD-WAN, an enterprise usually buys WAN services from an SD-WAN provider for its employees to access the applications in the Cloud, and then the SD-WAN provider may buy WAN lines from a network operator. The enterprise may know what applications will use the SD-WAN services but it will only provide the 5 tuples of those applications to the SD-WAN provider. So the SD-WAN provider does not know what applications it is actually serving. And then, the SD-WAN provider would usually buy WAN services from Network Operator. It will only provide 5 tuples to the Network Operator and the service performance requirements for steering their customer's traffic. In this way, the Network Operator does not know anything else about the traffic except the 5 tuples and requirements. Nowadays, SD-WAN is usually using 5-tuple to steer the traffic into corresponding WAN lines across the Network Operator's network [SD-WAN].

However, there are two main issues in the current SD-WAN deployments.

1) It is complicated and hard to resolve the 5 tuples. Even worse, with the traffic being all encrypted, it becomes impossible to obtain any transport layer information. Moreover, in the IPv6 data plane, with the extension headers being added before the upper layer, in some implementations it becomes very difficult and even impossible to obtain transport layer information because that information is so deep in the packet. So there is no 5 tuples anymore, and maybe only 2 tuples are available.

2) Currently there is still no way to apply various policies in different nodes along the network path onto a traffic flow altogether, that is, 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. Maybe we could stack those various policies in a list of TLVs at the

headend. However, it is going to introduce great complexities and impose big challenges on the hardware processing and forwarding.

5. Basic Solution and Benefits

With APN, at the edge node, i.e. CPE, of the SD-WAN (see Figure 2), the 5-tuple, plus information related to user or application requirements is constructed into a structured value. Please note, here the structured value is just a bit string and does not indicate actual application or user identification. This information is only meaningful for the network operators to apply various policies in different nodes/service functions, which can be enforced from the Controllers.

```
                          +------------------+
              +---------|SD-WAN Controller|---------+
              |         +--------|--------+         |
              |                  |                  |
              |          +-------|-------+          |
              |          |SDN  Controller|          |
              |          +-------|-------+          |
+-----+       |                  |                  |      +-----+
|App x|-\     |                  |                  |    /-|App x|
+-----+ |  +--|--+   +-----------|-----------+   +--|--+ | +-----+
         \-|     |   |   Application-aware   |   |     |-/
           |CPE 1|---|        Network        |---|CPE 2|
         /-|     |   |  Service Provisioning |   |     |-\
+-----+ |  +-----+   +-----------------------+   +-----+ | +-----+
|App y|-/     |                                     |    \-|App y|
+-----+       |<--- Network Operator Controlled --->|      +-----+
                          Limited Domain
```

Figure 2. SD-WAN using the APN Framework

With such identifier in the network, we can easily solve the two issues above-mentioned. We will not need to resolve the 5-tuple and perform the deep inspection any more. This structured value is encapsulated in the IP layer and can be easily read by the routers and service functions. If the data plane is SRv6, for example, such identifier can be encapsulated in an SRH TLV where it represents the policy corresponding to the application requirements.

Since this identifier is taken as an object to the network, the network operators will simply place the policies in the nodes/service functions where this indicated traffic will go through, and the corresponding node/service function will just apply policies for this

object. This can be easily done by utilizing this structured value, which is not possible with any current existing mechanism.

Such structured value will also bring other benefits, for example,

- o Improve the forwarding performance since it will only use 1 field in the IP layer instead of resolving 5 tuples, which will also improve the scalability.

- o Very flexible policy enforcement in various nodes and service functions along the network path.

Furthermore, with such structured value, more new services could be enabled, for example,

- o Even more fine-granularity performance measurement could be achieved and the granularity to be monitored and visualized can be controllable, which is able to relieve the processing pressure on the controller when it is facing the massive monitoring data.

- o The policy execution on the service function can be only based on this value and not based on 5-tuple, which can eliminate the need of deep packet inspection.

- o The underlay performance guarantee could be achieved for SD-WAN overlay services, such as explicit traffic engineering path satisfying SLA and selective visualized accurate performance measurement.

6. Solution Gap Analysis

There are already some solutions specified in IETF, which use identifier to perform traffic steering and service provisioning. However, none of them is the same as APN and able to achieve the same effects.

6.1. IPv6/MPLS Flow Label

[RFC6437] specifies the IPv6 flow label which enables the IPv6 flow classification. However, the IPv6 flow label is mainly used for Equal Cost Multipath Routing (ECMP) and Link Aggregation [RFC6438].

Similarly, [RFC6391] describes a method of adding an additional Label Stack Entry (LSE) at the bottom of the stack in order to facilitate the load balancing of the flows within a pseudowire (PW) over the available ECMPs. A similar design for general MPLS use has also been proposed in [RFC6790] using the concept of Entropy Label.

6.2. SFC ServiceID

Subscriber Identifier and Performance Policy Identifier are specified in [I-D.ietf-sfc-serviceid-header]. These identifiers are carried only in the Network Service Header (NSH) [RFC8300] Context Header, as shown in Figure 3, while the APN identifier can be carried in various data plane encapsulations.

```
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Metadata Class       |      Type     |U|    Length   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   ~                      Subscriber Identifier                    ~
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Metadata Class       |      Type     |U|    Length   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   ~                     Performance Policy Identifier             ~
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3. Subscriber Identifier and Performance Policy Identifier

In this draft [I-D.ietf-sfc-serviceid-header], the Subscriber Identifier carries an opaque local identifier that is assigned to a subscriber by a network operator, and the Performance Policy Identifier represents an opaque value pointing to specific performance policy to be enforced. In this way, in order to apply various policies in different nodes along the network path onto a traffic flow altogether, e.g., 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, those various policies would have to be stacked in a list of TLVs at the headend, introducing great complexities and big challenges on the hardware processing and forwarding.

The APN identifier, which is a structured value, is treated as an opaque object in the network, to which the network operator applies policies in various nodes/service functions along the path and provide corresponding services. The identifier may represent the

application traffic of a particular user but does not identify the actual user nor the actual application for network operators.

6.3. IOAM Flow ID

A 32-bit Flow ID is specified in [I-D.ietf-ippm-ioam-direct-export], which is used to correlate the exported data of the same flow from multiple nodes and from multiple packets, while the APN identifier can serve more various purposes.

6.4. Binding SID

The Binding SID (BSID) [RFC8402] is bound to an SR Policy, instantiation of which may involve a list of SIDs. Any packets received with an active segment equal to BSID are steered onto the bound SR Policy. A BSID may be either a local or a global SID. While the APN identifier is not bound to SRv6 only, and it can be carried in various data plane encapsulations.

6.5. FlowSpec Label

The flow specification (FlowSpec) [RFC5575] is actually an n-tuple consisting of several matching criteria that can be applied to IP traffic, which include elements such as source and destination address prefixes, IP protocol, and transport protocol port numbers. In BGP VPN/MPLS networks, BGP FlowSpec can be extended to identify and change (push/swap/pop) the label(s) for traffic that matches a particular FlowSpec rule in [I-D.ietf-idr-flowspec-mpls-match] and [I-D.ietf-idr-bgp-flowspec-label]. In [I-D.liang-idr-bgp-flowspec-route], BGP is used to distribute the FlowSpec rule bound with label(s). While the APN identifier is not bound to MPLS only, and it can be carried in various data plane encapsulations.

6.6. Summary

As driven by ever-emerging new 5G services, fine-granularity service provisioning becomes urgent. The existing solutions are either specific to a particular scenario or data plane. While APN aims to define a generalized identifier used for fine-granularity service provisioning, and can be carried in various data plane encapsulations.

7. IANA Considerations

There are no IANA considerations in this document.

8. Acknowledgements

The authors would like to acknowledge Martin Vigoureux, Alvaro Retana, Barry Leiba, Stefano Previdi, Adrian Farrel, and Daniel King for their valuable review and comments.

9. Informative References

[I-D.ietf-idr-bgp-flowspec-label]
liangqiandeng, l., Hares, S., You, J., Raszuk, R., and d. danma@cisco.com, "Carrying Label Information for BGP FlowSpec", draft-ietf-idr-bgp-flowspec-label-01 (work in progress), December 2016.

[I-D.ietf-idr-flowspec-mpls-match]
Yong, L., Hares, S., liangqiandeng, l., and J. You, "BGP Flow Specification Filter for MPLS Label", draft-ietf-idr-flowspec-mpls-match-01 (work in progress), December 2016.

[I-D.ietf-ippm-ioam-direct-export]
Song, H., Gafni, B., Zhou, T., Li, Z., Brockners, F., Bhandari, S., Sivakolundu, R., and T. Mizrahi, "In-situ OAM Direct Exporting", draft-ietf-ippm-ioam-direct-export-02 (work in progress), November 2020.

[I-D.ietf-sfc-serviceid-header]
Sarikaya, B., Hugo, D., and M. Boucadair, "Service Function Chaining: Subscriber and Performance Policy Identification Variable-Length Network Service Header (NSH) Context Headers", draft-ietf-sfc-serviceid-header-14 (work in progress), December 2020.

[I-D.li-6man-app-aware-ipv6-network]
Li, Z., Peng, S., Li, C., Xie, C., Voyer, D., Li, X., Liu, P., Liu, C., and K. Ebisawa, "Application-aware IPv6 Networking (APN6) Encapsulation", draft-li-6man-app-aware-ipv6-network-02 (work in progress), July 2020.

[I-D.li-apn-framework]
Li, Z., Peng, S., Voyer, D., Li, C., Geng, L., Cao, C., Ebisawa, K., Previdi, S., and J. Guichard, "Application-aware Networking (APN) Framework", draft-li-apn-framework-01 (work in progress), September 2020.

[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. 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.liang-idr-bgp-flowspec-route]
Liang, Q. and J. You, "BGP FlowSpec based Multi-dimensional Route Distribution", draft-liang-idr-bgp-flowspec-route-00 (work in progress), October 2014.

[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>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <https://www.rfc-editor.org/info/rfc5575>.

[RFC6391] Bryant, S., Ed., Filsfils, C., Drafz, U., Kompella, V., Regan, J., and S. Amante, "Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network", RFC 6391, DOI 10.17487/RFC6391, November 2011, <https://www.rfc-editor.org/info/rfc6391>.

[RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, DOI 10.17487/RFC6437, November 2011, <https://www.rfc-editor.org/info/rfc6437>.

[RFC6438] Carpenter, B. and S. Amante, "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels", RFC 6438, DOI 10.17487/RFC6438, November 2011, <https://www.rfc-editor.org/info/rfc6438>.

[RFC6790] Kompella, K., Drake, J., Amante, S., Henderickx, W., and L. Yong, "The Use of Entropy Labels in MPLS Forwarding", RFC 6790, DOI 10.17487/RFC6790, November 2012, <https://www.rfc-editor.org/info/rfc6790>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[SD-WAN] MEF 70.1 Draft (R1), available at https://www.mef.net/wp-content/uploads/2020/08/MEF-70-1-Draft-R1.pdf/, "SD-WAN Service Attributes and Service Framework", August 2020.

Authors' Addresses

Shuping Peng
Huawei Technologies
Beijing
China

Email: pengshuping@huawei.com

Zhenbin Li
Huawei Technologies
Beijing
China

Email: lizhenbin@huawei.com