Workgroup: Network Working Group
Internet-Draft:
draft-li-6man-apn-ipv6-encap-00
Published: 4 March 2024
Intended Status: Standards Track
Expires: 5 September 2024
Authors: Z. Li
Huawei Technologies
S. Peng
Huawei Technologies
C. Xie
China Telecom
S. Zhang
China Unicom

Application-aware IPv6 Networking (APN6) Encapsulation

Abstract

Application-aware IPv6 Networking (APN6) makes use of IPv6 encapsulation to convey the APN Attribute along with data packets and make the network aware of data flow requirements at different granularity levels. The APN attribute can be encapsulated in the APN header. This document defines the APN header and its encapsulation in the IPv6 data plane.

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 https://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 5 September 2024.

document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Application-aware Networking (APN) conveys an attribute with data packets in the network and makes the network aware of fine-grained requirements at appropriate level.

Such an attribute is acquired, constructed in a structured value, and then encapsulated in the packets. Such 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 provides corresponding services.

This structured attribute can be encapsulated in various data planes adopted within a Network Operator's controlled and limited domain, e.g. MPLS, VXLAN, SR/SRv6 and other tunnel technologies.

This document defines the application-aware networking (APN) header and its encapsulation in the IPv6 data plane.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminologies

APN: Application-aware Networking

APN6: Application-aware IPv6 Networking, i.e., the data plane of APN is IPv6

APN Attribute: Application-aware information. It is added at the edge devices of an APN domain along with any tunnel encapsulation.

APN ID: Application-aware Networking ID

APN Para: Application-aware Networking Parameters

SRH: Segment Routing Header RFC 8754 [RFC8754]

4. Problem statement and Requirements

In a network operator controlled domain, the ingress edge devices usually have access to rich information, such as VLAN/QinQ, VPN ID, and access interface, which is used to classify the packets into fine granular virtual groups of flows at the edge.

However, after the packets enter the network operators domain, all such information is not immediately visible at transit nodes. It may be hidden inside encapsulation, masked by encryption, mapped to other protocol fields, or stripped from the packets completely.

Furthermore, many mapping schemes, where they are used, lose some level of granularity from the information available at the network edge. For example, when the information is mapped into small fields like DSCP (6 bits) or MPLS EXP (3 bits) the result is that only relatively coarse grained QoS treatment can be provided. MPLS EXP bits are sometimes insufficient to carry what an operator needs, even the DSCP is really too small.

On the other hand, the identification of single application or user is not needed in the network either. Besides the commitment of privacy protection, the traffic running in the network is aggregated and the network does not have such capability nor the necessity of processing such extremely fine granularity.

Therefore, the capability of offering appropriate level of granularity is desired by operators in order to provide fine-grained services.

5. Usage scenarios

The packet treatments needed may vary at different parts of the path within the domain, and enough information is needed to determine these treatments such as steering, triggering, and identifying in an efficient way, that is, to efficiently realize a composite network service provisioning along the path. For example, at the headend to steer into corresponding path at the midpoint to collect corresponding performance measurement data at the service function to execute particular policies flexibly.

Furthermore, when the packet traversing through multiple technology domains of a single operator, where each domain is controlled independently without a hierarchical controller being deployed and each has its own SLA mechanism, in this case, it is difficult to achieve end-to-end consistency in service provisioning (e.g. visualization) due to lack of information to indicate the granularity of traffic flow across multiple domains. The ACL configuration at the following domains edge devices are very complex and dynamic.

This information can be carried directly in the packet or achieved through a mapping from an opaque tag. Existing protocols such as SFC/NSH, SR/SRv6, MPLS, VXLAN, and IPv6, can be taken as implementation basis, but in each case the protocol may need extensions. This draft focuses on the extensions in the IPv6 data plane.

6. APN Header

A common header, i.e. APN Header, is defined and can be used in different data planes. The common header carries the APN attribute that is composed of APN ID and APN parameters.

This document defines three types of APN ID:

- Type 1 APN ID: it is 32 bits.

- Type 2 APN ID: it is 64 bits.

- Type 3 APN ID: it is 128 bits.

According to the types of APN ID, three types of APN headers are defined and follow the same format as follows.

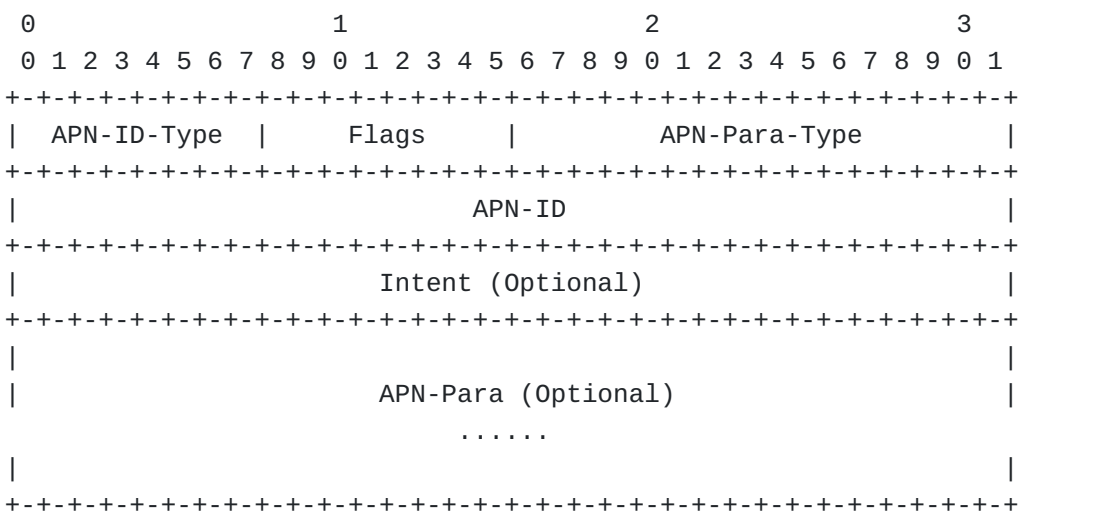

Figure 1. APN Header Format

APN-ID-Type: An 8-bit identifier, indicates the type of APN ID.

Flags: An 8-bit field. The possible flags will be defined in the future versions of this document.

APN-Para-Type: A 16-bit map that specifies which APN parameters are specified for the APN ID. The APN-Para-Type value is a bitmap. The packing order of the APN parameters follows the bit order as specified in the APN-Para-Type bitmap field. The following bits are defined in this document, with details on each bit described in Section 8.

Bit 0 (Most significant bit) When set, indicates the presence of the bandwidth requirement.

Bit 1 When set, indicates the presence of the delay requirement.

Bit 2 When set, indicates the presence of the jitter requirement.

Bit 3 When set, indicates the presence of the packet loss rate requirement.

APN-ID: A 32-bit identifier.

Intent: A 32-bit identifier, represents a set of service requirements to the network.

APN-Para: A variable field including APN parameters. The presence of the APN parameters is indicated by the APN-Para-Type.

7. APN ID

The APN ID is suggested to be divided into three parts:

APP-Group-ID: Application Group ID

USER-Group-ID: User Group ID

Reserved: The reserved field.

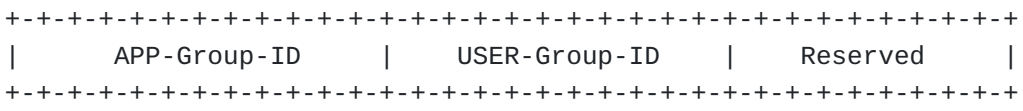

Figure 2. Structure of APN-ID

The lengths of the APP-Group-ID and the USER-Group-ID are variable. Their lengths must be configured and consistent within a specific APN domain.

The APN ID can be configured by using a template [I-D.peng-apn-yang].

8. APN Parameters

In the APN Header, the APN-Para-Type is a bit field to indicate the presence of corresponding APN parameters. When the bit is set, the corresponding APN parameter MUST exist in the APN Header. The length of each APN parameter is 32 bits. Thus it is easy to skip over unknown requirements.

Typical APN parameters are the parameters related with the network performance requirements as follows:

1. Bandwidth Requirement

This Bandwidth Requirement parameter indicates the minimum acceptable bandwidth for the APN traffic. The format of this parameter is shown in the following diagram:

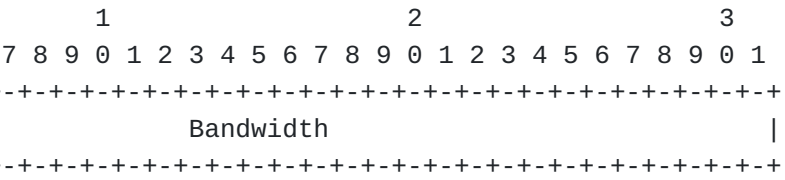

Figure 3. Bandwidth Requirement Parameter

where:

Bandwidth: This 32-bit unsigned integer field carries the bandwidth requirement in Mbps along the path.

2. Delay Requirement

This Delay Requirement parameter indicates the maximum acceptable delay. The format of this parameter is shown in the following diagram:

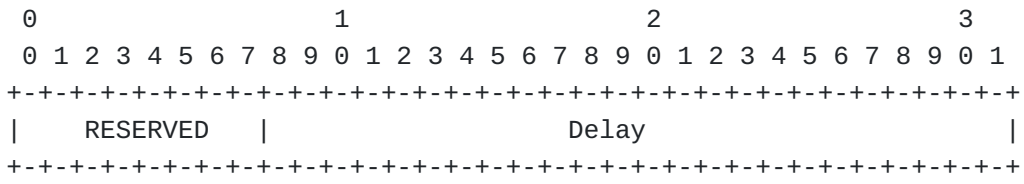

Figure 4. Delay Requirement Parameter

where:

RESERVED: This field is reserved for future use. It MUST be set to 0 when sent and MUST be ignored when received.

Delay: This 24-bit field carries the delay requirements in microseconds, encoded as an unsigned integer value. When set to the maximum value 16,777,215 (16.777215 sec), then the delay is not constrained. This value is the highest delay that can be tolerated.

3. Delay Variation Requirement

This Delay Variation Requirement parameter indicates the maximum acceptable delay variation. The format of this parameter is shown in the following diagram:

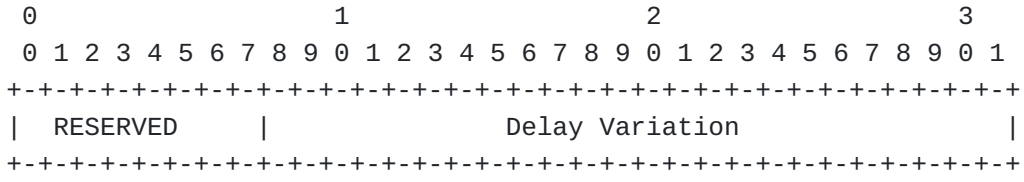

Figure 5. Delay Variation Parameter

where:

RESERVED: This field is reserved for future use. It MUST be set to 0 when sent and MUST be ignored when received.

Delay Variation: This 24-bit field carries the delay variation requirements in microseconds, encoded as an unsigned integer value.

4. Packet Loss Rate Requirement

This Packet Loss Rate Requirement parameter indicates the maximum acceptable packet loss rate. The format of this parameter is shown in the following diagram:

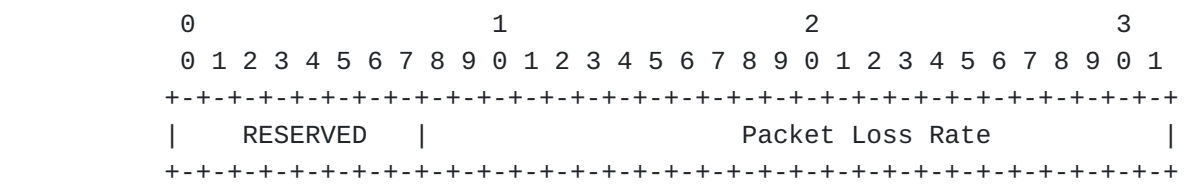

Figure 6. Packet Loss Rate Sub-TLV

where:

RESERVED: This field is reserved for future use. It MUST be set to 0 when sent and MUST be ignored when received.

Packet Loss Rate: This 24-bit field carries packet loss rate requirement in packets per second as an unsigned integer. This value is the highest packet-loss rate that can be tolerated.

9. The APN Option

To support Application-aware IPv6 networking, one IPv6 Header option RFC 8200 [RFC8200], the APN option, is defined.

The APN option has the following format:

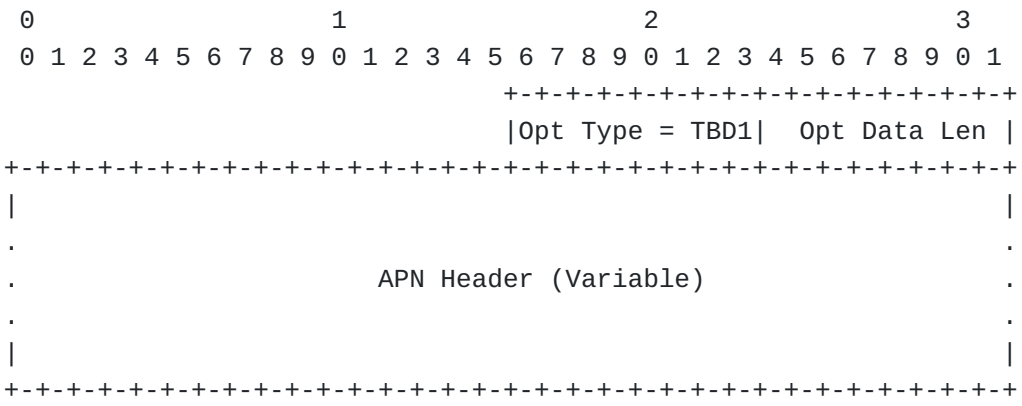

Figure 7. The APN Option

where:

o Opt Type: Type value is TBD1 (suggested value 0x13), an 8-bit unsigned integer. Identifier of the type of this APN Option.

o Opt Data Len: An 8-bit unsigned integer. Length of the Option Data field of this option, that is, length of the APN header.

o APN Header: Option-Type-specific data. It carries the APN header. Variable-length field as specified in Section 6.

10. Locations for the APN Option

The APN IPv6 Header option can be placed in two locations in an IPv6 packet header RFC 8200 [RFC8200] depend upon the scenario and implementation requirements. These are defined in the subsections below.

10.1. IPv6 Hop-by-Hop Options Header (HBH)

The APN option can be carried in the IPv6 Hop-by-Hop Options Header. By using the HBH Options Header, the information carried can be read by every node along the path.

10.2. IPv6 Destination Options Header (DOH)

The APN option can be carried in the IPv6 Destination Options Header. By using the DOH Options Header, the information carried can be read by the destination node but would not normally be seen by other nodes along the path.

11. APN TLV for the SRH

[RFC8754] defines the segment routing header (SRH) and the SRH TLV. The SRH TLV provides meta-data for segment processing. The APN header can be placed in the SRH as the value of one type of SRH TLV following the Segment List. By using the SRH, the information carried can be read by the specified segment destinations along the SRv6 path.

The APN TLV is OPTIONAL and has the following format:

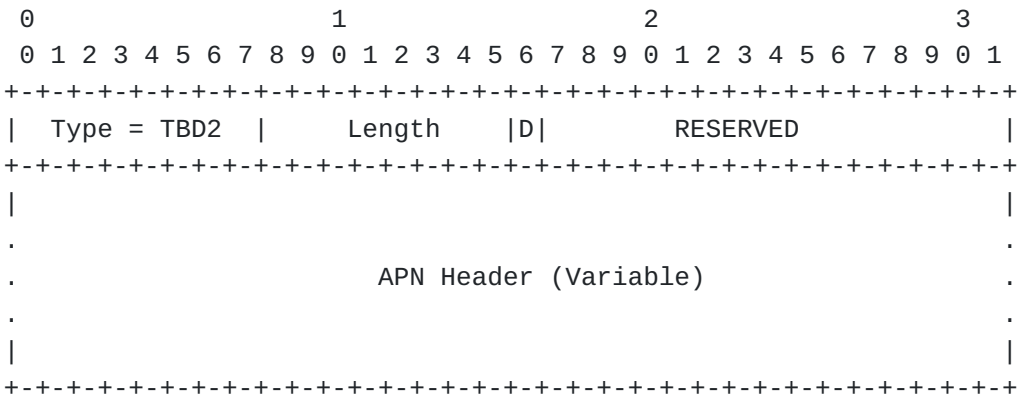

Figure 8. The APN SRH TLV

where:

o Type: TBD2 (suggested value 0x13).

o Length: The length of the variable length data in bytes.

o D: 1 bit. When it is set, it indicates the Destination Address verification is disabled due to use of a reduced segment list.

o RESERVED: 15 bits. MUST be 0 on transmission and ignored on receipt.

o APN Header: It carries the APN header as specified in Section 6. A variable-length field.

12. Implementation Status

Huawei:

Huawei hardware platforms supports APN with current status as follows:

o Huawei ATN with VRPV8 shipping code.

o Huawei CX600 with VRPV8 shipping code.

o Huawei NE40E with VRPV8 shipping code.

o Huawei ME60 with VRPV8 shipping code.

o Huawei NE5000E with VRPV8 shipping code.

o Huawei NE9000 with VRPV8 shipping code.

o Huawei NE8000 with VRPV8 shipping code.

Tshinghua University:

o Linux

BUPT (Beijing University of Posts and Telecommunications):

o P4

13. IANA Considerations

These IANA Considerations conform to [RFC8126].

IANA is requested to create the following new registries on a new "Application-Aware Networking (APN)" webpage.

13.1. APN ID Types

IANA is requested to create the following registry on the Application-Aware Networking (APN) Attribute webpage:

Name: APN ID Types

Registration Procedure: IETF Review

Reference: [this document]

Value	Description	Reference
0	reserved	
1	Type 1 APN ID	[this document]
2	Type 2 APN ID	[this document]
3	Type 3 APN ID	[this document]
4-254	unassigned	
255	reserved	

13.2. APN Parameter Types

IANA is requested to create the following registry on the Application-Aware Networking (APN) Attribute webpage:

Name: APN Parameter Types

Registration Procedure: IETF Review

Reference: [this document]

Bit	Description	Reference
0	Bandwidth requirement	[this document]
1	Delay requirement	[this document]
2	Jitter requirement	[this document]
3	Packet loss requirement	[this document]
4-15	unassigned	

13.3. IPv6 Header Option

IANA is requested to assign an IPv6 Header Option as follows:

Hex Value	Binary Value act	chg	rest	Description	Reference
0x13	00	0	10011	Application-aware Networking	[this document]

13.4. SRH TLV Type

IANA is requested to assign an SRH TLV Type from the range of type values for TLVs that do not change en route (2-127) as follows:

Value	Description	Reference
0x13	Application-aware Networking	[this document]

14. Security Considerations

In the APN work, in order to reduce the privacy and security issues, the APN attribute MUST be conveyed along with the tunnel information in the APN domain. The APN attribute is encapsulated and removed at the edge of the APN domain. The APN 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. If the APN attribute is conveyed without the tunnel information, the packet MUST be dropped. If the APN attributes are 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. If the network service requirements exceed the specification for the specific APN ID, it should trigger the alarm information. The packet should be discarded to prevent abusing of the resources. There should be rate-limiting policy at the edge of the APN domain to prevent the traffic belonging to a specific APN ID from exceeding the preset limit.

15. References

15.1. 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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

15.2. Informative References

[I-D.peng-apn-yang] Peng, S. and Z. Li, "A YANG Model for Application-aware Networking (APN)", Work in Progress, Internet-Draft, draft-peng-apn-yang-03, 9 May 2023, <https://datatracker.ietf.org/doc/html/draft-peng-apn-yang-03>.

Authors' Addresses

Zhenbin Li
Huawei Technologies
Beijing
100095
China

Email: lizhenbin@huawei.com

Shuping Peng
Huawei Technologies
Beijing
100095
China

Email: pengshuping@huawei.com

Chongfeng Xie
China Telecom
China

Email: xiechf@chinatelecom.cn

Shuai Zhang
China Unicom
China

Email: zhangs366@chinaunicom.cn