RTGWG Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 26, 2021

F. Yang
M. Chen
T. Zhou
Huawei Technologies
February 22, 2021

Associated Channel over IPv6
draft-yang-rtgwg-ipv6-associated-channel-00

Abstract

In this document, an associated channel is introduced to provide a control channel based on IPv6, carrying types of control and management messages. By using the associated channel, messages can be transmitted between the network nodes to provide functions like path identification, OAM, protection switchover signaling, etc., targeting to provide high quality SLA guarantee to service.

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

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 August 26, 2021.

Copyright Notice

Table of Contents

1. Introduction

IPv6 is becoming widely accepted to provide the connectivity in many new emerging scenarios, including Cloud Network convergence, Cloud-Cloud interconnection, 5G vertical industries, Internet of Things, as well as the legacy networks migrating towards SR over IPv6. However, IP packet is locally lookup, and forwarded hop by hop without aware of the forwarding path. Path segment over SRv6 [I-D.ietf-spring-srv6-path-segment] provides a good solution to identify an SR path over IPv6, but can only be applicable in source routing paradigm.

To identify an IPv6 forwarding path, further to better control and manage the path, this document introduces an associated channel based on IPv6, intenting to create a control channel for the control and management usages. By using the associated channel, messages can be transmitted between the network nodes to provide functions like path identification, OAM, protection switchover signaling, etc., targeting to provide high quality SLA guarantee to service.

This document also defines a TLV format for the associated channel and how it can be encapsulated in IPv6 packet, and the potential applicability in IPv6 networks. Applications of associated channel in IPv6 shall be specified in different documents and thus are out of scope of this document.

2. Terminology

OAM: Operations, Administration, and Maintenance

SLA: Service Level Agreement

ACH: Associated CHannel

3. Associated Channel

An associated channel provides a control channel that carries at least one or more types of control and management messages. The type of message is not limited to any specific usage. The associated channel is specified by two parts of information, including the identification of associated channel and the carried message.

3.1. Identification of Associated Channel

The identification of associated channel indicates the path where the packets of associated channel are transmitted on. This identification also indicates the same path of the service forwarding path which the associated channel is associated to.

3.2. ACH TLV to Carry Message

An Associated CHannel (ACH) TLV is designed to carry the message of an associated channel. ACH TLV has the following format:

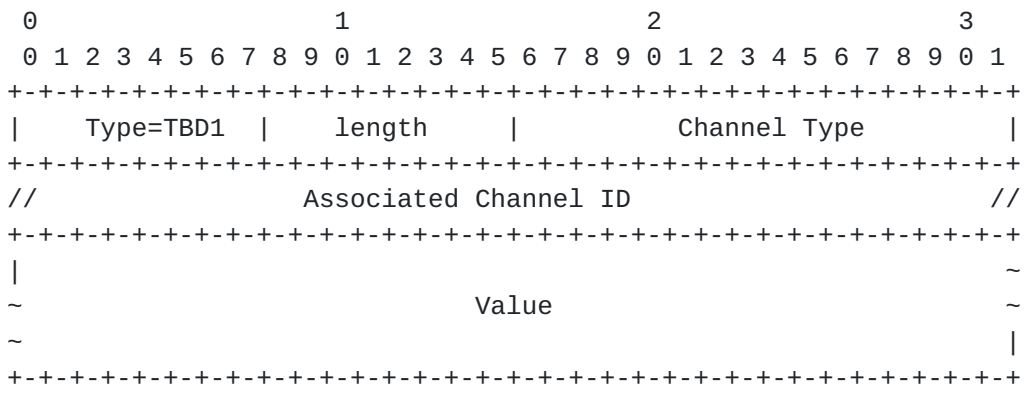

Figure 1 ACH TLV Format

Type: 8 bits, indicates it is an associated channel (ACH) TLV, and request a value assigned by IANA. The uniform type of TLV generalizes the applicability of ACH TLV to support various types of messages.

Length: 8 bits, defines the length of Value field in bytes.

Channel Type: is a 16-bit-length fixed portion as a part of Value field. It indicates the specific type of messages carried in associated channel. Note that a new ACH TLV Channel Type Registry would be requested to IANA. In the later documents which specify application protocols of associated channel, MUST also specify the applicable Channel Type field value assigned by IANA.

Associated Channel ID: indicates the identification of associated channel. The length is TBD.

Value: is a variable part of Value field. It specifies the messages indicated by Channel Type and carried in associated channel. Note that the Value field of ACH TLV MAY contain sub-TLVs to provide additional context information to ACH TLV.

3.3. Encapsulation of ACH TLV in IPv6

In the context of IPv6, ACH TLV can be encapsulated in different types of IPv6 extension header or even IPv6 payload. Note that, no matter which way ACH TLV is applied, there is no semantic change to IPv6 extension headers. Moreover, ACH TLV can be carried either with user data in an in-situ way, or in a independent synthetic packet.

3.3.1. Encapsulated in IPv6 Destination Options Header

ACH TLV can be encapsulated in IPv6 Destination Options Header as the TLV-encoded options. Figure 2 gives an example of an ACH TLV encapsulated in IPv6 Destination Options Header.

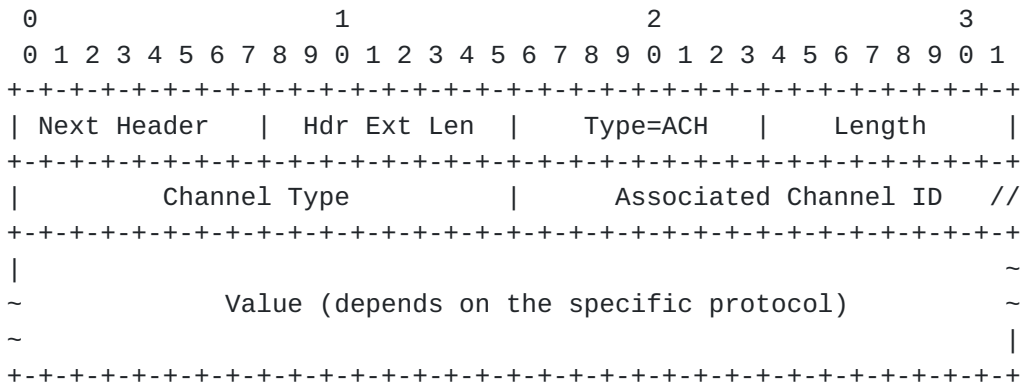

Figure 2 ACH TLV in IPv6 Destination Options Header

According to the note 1 and note 3 described in section 4.1 of[RFC8200], ACH TLV encapsulated in IPv6 Destination Options Header can provide two semantics of associated channel. When only IPv6 Destination Options Header exists or IPv6 Destination Options Header exists after the Routing Header, an end to end associated channel is provided to transmit the messages between two endpoints. When both IPv6 Destination Options Header and Routing Header exist, and IPv6 Destination Options Header exists before the Routing Header, an associated channel is provided at network nodes of the first destination that appears in the IPv6 Destination Address field plus subsequent destinations listed in the Routing header.

3.3.2. Encapsulated in IPv6 Hop-by-Hop Options Header

ACH TLV can be encapsulated in IPv6 Hop-by-Hop Options Header as the TLV-encoded options. Same option type numbering space is used for both Hop-by-Hop Options header and Destination Options header. Similarly, the ACH TLV in IPv6 Hop-by-Hop Options Header shares the same encapsulation shown in Figure 2.

When it is encapsulated in IPv6 Hop-by-Hop Options Header, it provides an associated channel at every node along the forwarding path.

3.3.3. Encapsulated in IPv6 Segment Routing Header

ACH TLV can be encapsulated in IPv6 Segment Routing Header, as SRH optional TLV. Figure 3 gives an example of an ACH TLV encapsulated in IPv6 Segment Routing Header.

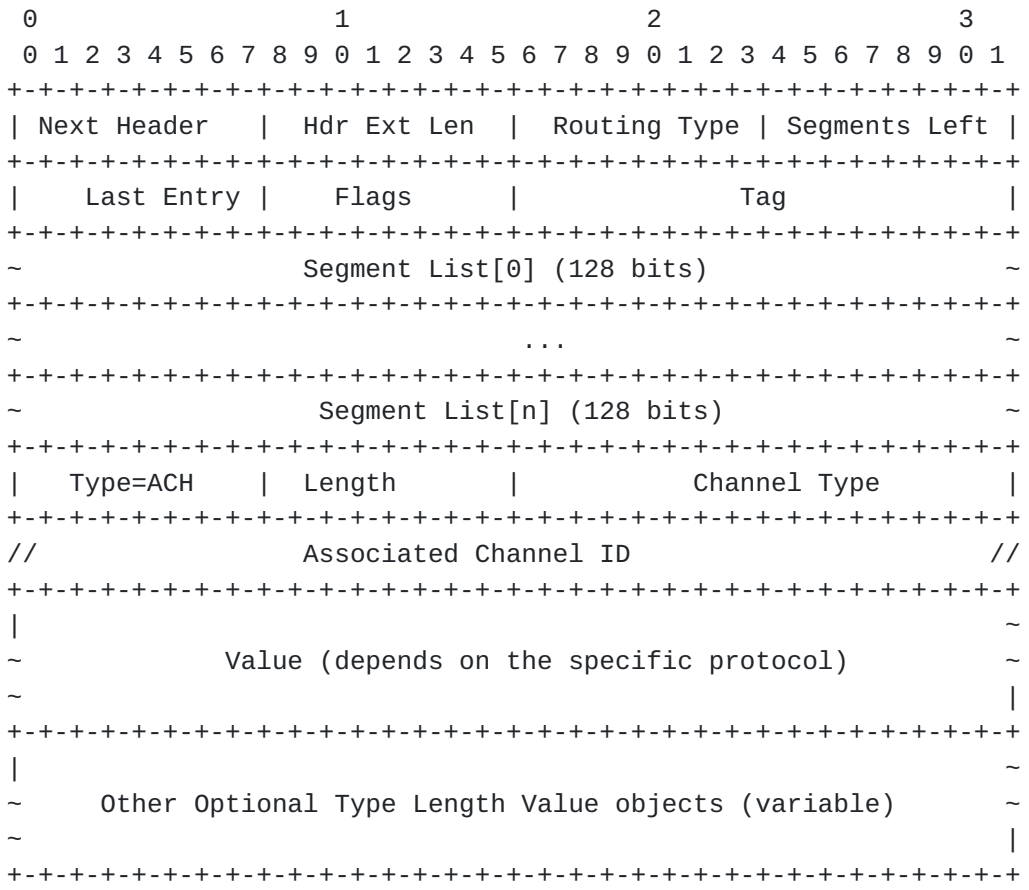

Figure 3 ACH TLV in IPv6 Segment Routing Header

When ACH TLV is encapsulated in IPv6 Segment Routing Header, it provides an associated channel at every SRv6 endpoints along the path.

3.3.4. Encapsulated in Payload

ACH TLV can also be encapsulated in the payload of an IPv6 packet. The term of payload here means the octets after the IPv6 header and extension headers. A synthetic packet is created with the payload of messages. and transmitted in an associated channel. The synthetic packet can use the same routing information with service data whose associated channel is associated to. For example, synthetic packet can encapsulate the same segment list as the one used in IPv6 SRH of service data.

3.4. Processing of ACH TLV

Take the ACH TLV encapsulated in Segment Routing Header as an example. At headend, ACH TLV is encapsulated with control and management messages in Segment Routing Header. When midpoint or tail-end receives an SRv6 packet with ACH TLV, it recognizes the ACH TLV, check the Channel Type field to interpret the protocol, and continue with processing of messages. The processing of message is not limited, for example READ or/and WRITE. It should depend on the specification of protocols used in the associated channel.

4. Applicability

4.1. Path Identification

In a native IPv6 network, packets is transmitted hop by hop, there is no way to identify an IPv6 forwarding path. The path needs to be identified when OAM or protection switchover is applied to the path.

4.2. OAM

OAM includes the a group of functions such as connectivity verification, fault indication and detection, and performance measurement of loss and delay etc. For example, BFD defines a generic control packet format that can be encapsulated in different data planes to provide low-overhead and short-duration failure detection function. The format can also be encapsulated in ACH TLV as the option TLV of Destination Options Header, to provide the same connectivity verification and fault detect functions without introducing upper layer protocols. Another example is to encapsulate PDU formats of Ethernet OAM [ITU-T G.8013] in Value field of ACH TLV to provide a set of OAM functions. By using ACH TLV to carry OAM messages in associated channel, different OAM functions can be easily integrated. The OAM functions can be performed in either end-to-end or hop-by-hop mode. For example, signal degrade happens on the intermediate node could be discovered and further indicated in associated channel to monitor the path status.

4.3. Assist to Protection Switchover

Linear protection [RFC6378] provides a very flexible protection mechanism in a mesh network because it can operate between any pair of endpoints. ACH TLV can be used to transmit the protection state control messages on an IPv6 forwarding path to provide the function of bidirectional protection switchover.

5. IANA Considerations

- This document requests IANA to assign a codepoint of Destination Options and Hop-by-Hop Options.
- This document requests IANA to assign a codepoint of Segment Routing Header TLVs to indicate ACH TLV.
- This document request IANA to create a new IANA-managed registry of ACH Channel Type to identify the usage of associated channel.

6. Security Considerations

TBD

7. Acknowledgements

TBD

8. References

8.1. 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>.

8.2. Informative References

[I-D.ietf-spring-srv6-path-segment] Li, C., Cheng, W., Chen, M., Dhody, D., and R. Gandhi, "Path Segment for SRv6 (Segment Routing in IPv6)", draft-ietf-spring-srv6-path-segment-00 (work in progress), November 2020.

[RFC6378] Weingarten, Y., Ed., Bryant, S., Osborne, E., Sprecher, N., and A. Fulignoli, Ed., "MPLS Transport Profile (MPLS-TP) Linear Protection", RFC 6378, DOI 10.17487/RFC6378, October 2011, <https://www.rfc-editor.org/info/rfc6378>.

[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>.

Authors' Addresses

Fan Yang
Huawei Technologies
Beijing
China

Email: shirley.yangfan@huawei.com

Mach(Guoyi) Chen
Huawei Technologies
Beijing
China

Email: mach.chen@huawei.com

Tianran Zhou
Huawei Technologies
Beijing
China

Email: zhoutianran@huawei.com