RTGWG Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 13, 2022

F. Yang
M. Chen
T. Zhou
Huawei Technologies

July 12, 2021

Associated Channel over IPv6
draft-yang-rtgwg-ipv6-associated-channel-01

Abstract

This document introduces a control channel based on IPv6, called Associated CHannel over IPv6 (ACH6), that may carry different types of control and management messages. By using the associated channel, messages can be transmitted between network nodes to provide functions like path identification, OAM, automatic protection switchover signaling, resource reservation, etc., targeting to provide high quality SLA guarantees to IPv6 services.

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 January 13, 2022.

Table of Contents

1. Introduction

IPv6 is becoming widely accepted to provide connectivity in many new emerging scenarios, including Cloud Network convergence, Cloud-Cloud interconnection, 5G vertical industries, and Internet of Things etc. However, due to the best effort forwarding genes, native IP (for both IPv4 and IPv6) cannot provide the forwarding capabilities such as explicit path, control and management based on the forwarding path, to meet the requirements of services accordingly.

Generic Associated Channel (G-ACh) [RFC5586] introduces an associated control channel to MPLS to provide a set of maintenance functions, including OAM, performance monitoring, automatic protection switching and support of management to MPLS Sections, MPLS Label Switched Paths (LSPs), and MPLS pseudowires (PWs).

Triggered by MPLS G-ACh, to enhance the control and management capabilities to IPv6, this document introduces an associated channel to a specific IPv6 path, called Associated Channel over IPv6 (ACH6). Associated channel over IPv6 intends to create a control channel associated with the IPv6 data forwarding path for control and management purposes. By using the associated channel, messages can be transmitted between the network nodes to provide functions like path identification, OAM, automatic protection switchover signaling, resource reservation, etc., targeting to provide high quality SLA guarantees to services. To identify an IPv6 forwarding path, associated channel ID is also introduced.

This document defines an ACH6 architecture, a TLV-based format of ACH6, and discusses how ACH6 format can be encapsulated in IPv6 packet. It also discusses the applicability of ACH6 in IPv6 network.

2. Terminology

This document uses the terminology defined in [RFC8200] , and it also introduces the following new terms:

OAM: Operations, Administration, and Maintenance

SLA: Service Level Agreement

G-ACh: Generic Associated Channel

ACH6: Associated CHannel over IPv6

3. Architecture of Associated Channel over IPv6

3.1. ACH6 Network Reference Model

Figure 1 gives a network reference model of associated channel over IPv6. The key components in ACH6 network reference model include ACH6 Ingress Node, ACH6 Mid-Point Node, and ACH6 Egress Node. These nodes must be IPv6-capable node.

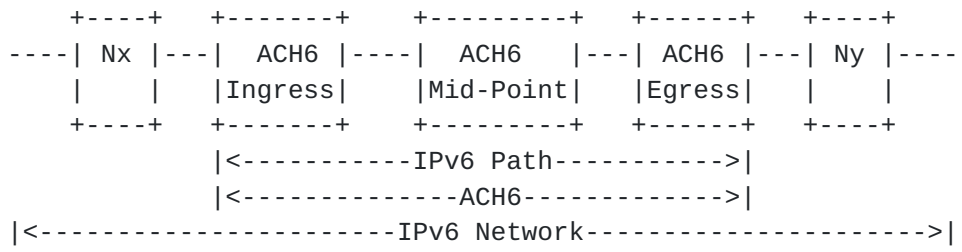

Figure 1 ACH6 Network Reference Model

In the network reference model,

Nx/Ny: IPv6 node, can be either a host or a router.

ACH6 Ingress Node: is the node indicates the entering of control and management channel over an IPv6 path, where control and management messages are generated and encapsulated.

ACH6 Mid-Point Node: is the node that has the capability to process control and management messages over an IPv6 path. For a strict explicit IPv6 path, all the IPv6 hop(s) forwarded from IPv6 source address to IPv6 destination address are mid-point node(s).

ACH6 Egress Node: is the node indicates the exiting of control and management channel over an IPv6 path, where control and management messages are recovered and delivered to control or management plane for further process.

IPv6 Path: a specific path from the source node to the destination node in IPv6 forwarding plane. An IPv6 path can be explicitly or implicitly represented by forwarding hops from IPv6 source node to IPv6 destination node.

ACH6: Associated Channel over IPv6

3.2. ACH6 Processing

Regarding to an IPv6 path, an ACH6 control channel is established to this specific IPv6 path for a required purpose. ACH6 ingress node acts as the IPv6 source node, and ACH6 egress node is the IPv6 destination node. ACH6 ingress node encapsulates control or management messages into IPv6 packets, identifies the specific channel type which carried messages belong to, and sends the IPv6 ACH6 packets to the destination of IPv6 path. The control and management messages can either piggyback with data packets, or generated and transmitted separately.

When ACH6 Mid-Point Node receives ACH6 IPv6 packets, it firstly recognizes ACH6 associated channel to interpret the control protocol, and then processes the messages. The processing of messages can include for example READ or/and WRITE, depending on the specification of protocols used in the associated channel. ACH6 Mid-Point Node needs to transmit the IPv6 packets carried with the original or modified ACH6 messages to the destination of IPv6 packet.

ACH6 Egress Node receives ACH6 IPv6 packets and recognizes itself as the destination. Based on the specific type of control protocol, the message is delivered to control or management planes for further process.

4. Format of Associated Channel over IPv6

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 pieces of information, including the identification of the associated channel and the carried message.

4.1. Identification of ACH6

The identification of associated channel, called Associated Channel ID, indicates the path where the packets of the associated channel are transmitted on. This identification also indicates the same path of the service forwarding path with which the associated channel is associated. When the Associated Channel ID is carried in the associated channel, ACH6 edge nodes and intermediated nodes should interpret it to identify the same IPv6 path.

The associated channel ID can be defined either globally unique or site local, or even link local. The Associated Channel ID can be self-generated, or designated from management plane, or advertised and allocated via control protocol.

4.2. Carried Message of ACH6

At least one control or management protocol messages are transmitted via associated channel over IPv6. When multiple protocols are running over an IPv6 path, messages of different protocols can be sent either in separate ACH6 TLVs in one ACH6 packet or in separate ACH6 packets with only one type of ACH6 TLV.

4.3. ACH6 TLV Format

An Associated CHannel over IPv6 (ACH6) TLV is designed to carry the identification and carried message of an associated channel. ACH6 TLV has the following format:

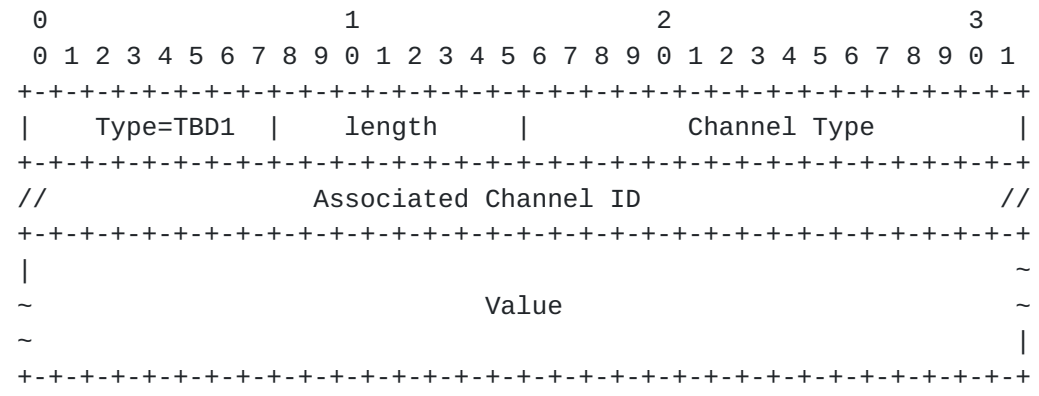

Figure 2 ACH6 TLV Format

Type: 8 bits, indicates it is an associated channel ACH6 TLV, and request a value assigned by IANA. The uniform type of TLV generalizes the applicability of ACH6 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 of Value field. It indicates the specific type of messages carried in associated channel. Note that a new ACH6 TLV Channel Type Registry would be requested to IANA. In 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 portion of Value field. It specifies the messages indicated by Channel Type and carried in associated channel.

Note that the Value field of ACH6 TLV MAY contain sub-TLVs to provide additional context information to ACH6 TLV.

4.4. Encapsulation of ACH6 TLV in IPv6

In the context of IPv6, ACH6 TLV can be encapsulated in different types of IPv6 extension headers, or as an independent IPv6 payload. Note that, no matter which way ACH6 TLV is applied, there is no semantic change to IPv6 extension headers.

4.4.1. Encapsulated in IPv6 Destination Options Header

ACH6 TLV can be encapsulated in IPv6 Destination Options Header as the TLV-encoded options. Figure 2 gives an example of an ACH6 TLV encapsulated in IPv6 Destination Options Header.

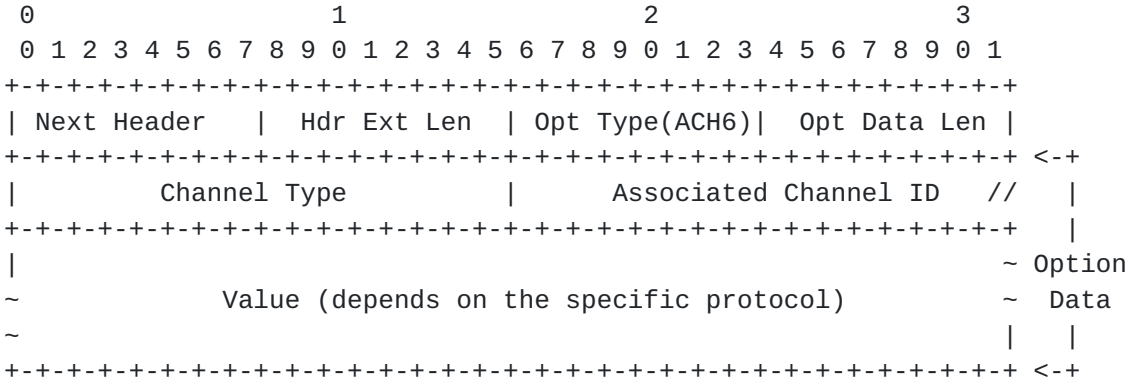

Figure 3 ACH6 TLV in IPv6 Destination Options Header

According to the note 1 and note 3 described in section 4.1 of[RFC8200], ACH6 TLV encapsulated in IPv6 Destination Options Header can provide two semantics of an 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.

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

ACH6 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 ACH6 TLV in IPv6 Hop-by-Hop Options Header shares the same encapsulation shown in Figure 3.

When it is encapsulated in IPv6 Hop-by-Hop Options Header, it provides an associated channel at every node along the forwarding path. ACH6 ingress node inserts the IPv6 HbH Option Header with ACH6 Option Type, every mid-point node examines, processes and transmits the IPv6 packet to next forwarding hop. ACH6 egress node receives the IPv6 packet as the destination node, ACH6 messages are processed and delivered to control or management plane for further usage. Processing is limited, can be READ and/or REWRITE.

Routers that are not configured to support Hop-by-Hop Options SHOULD ignore this option and SHOULD forward the packet.

Routers that support Hop-by-Hop Options, but that are not configured to support this option SHOULD ignore the option and SHOULD forward the packet.

4.4.3. Encapsulated in IPv6 Segment Routing Header

ACH6 TLV can be encapsulated in IPv6 Segment Routing Header, as SRH optional TLV. Figure 3 gives an example of an ACH6 TLV encapsulated in IPv6 Segment Routing Header.

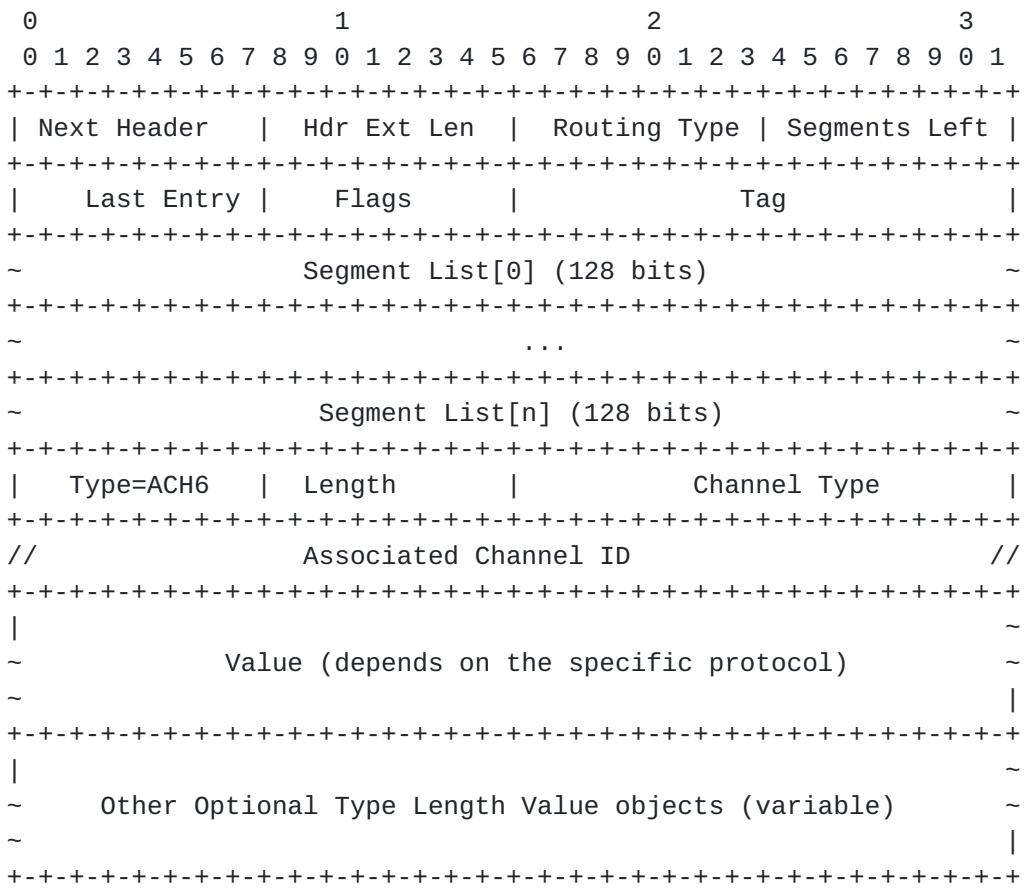

Figure 4 ACH6 TLV in IPv6 Segment Routing Header

When ACH6 TLV is encapsulated in IPv6 Segment Routing Header, it provides an associated channel at every SRv6 endpoints along the path.

4.4.4. Encapsulated in Payload

ACH6 TLV can also be encapsulated in the payload of an IPv6 packet. The term 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 it is associated. For example, synthetic packet can encapsulate the same segment list as the one used in IPv6 SRH of service data. If ACH6 TLV format is encapsulated in payload, TLV Type and Length can be omitted, a new codepoint of IP Protocol Numbers should be assigned.

4.5. Considerations

When ACH6 TLV is deployed in either IPv6 extension headers or payload in IPv6 networks, there are serveral considerations needs to be taken into account:

C1: MTU Increase

Given that ACH6 messages increases the packet size of IPv6 packet, it may face the risk of exceeding the PMTU. This problem can be solved by taking two things into considerations. Firstly, the mechanism of each protocol should clearly specify the maximum size limit of carried messages in one IPv6 packet. Secondly, operators or hosts who makes use of ACH6 to carry control and management messages should carefully design and ensure the addition of messages would not exceed the agreed PMTU.

C2: Processing of IPv6 Extension Header

Though IPv6 Extension Headers especially IPv6 Hop-by-Hop Option Header is not widely used in the Internet, there are some limited environments like Data Centers and Interconnections between Data Centers are experimentally using IPv6 Option Headers. It is worth to keep the possibility of carrying ACH6 messages as Option in IPv6 Extension Headers.

5. Applicability

5.1. Path Identification

In a native IPv6 network, packets are 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.

5.2. OAM

OAM includes 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 ACH6 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 ACH6 TLV to provide a set of OAM functions. By using ACH6 TLV to carry OAM messages in an 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 degradation that happens on the intermediate node could be discovered and further indicated in associated channel to monitor the path status.

5.3. 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. ACH6 TLV can be used to transmit the protection state control messages on an IPv6 forwarding path to provide the function of bidirectional protection switchover.

6. 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 ACH6 TLV.
- This document request IANA to create a new registry of IPv6 ACH6 Channel Types to identify the usage of associated channel.

7. Security Considerations

TBD

8. Acknowledgements

TBD

9. References

9.1. 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>.

9.2. 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.

[RFC5586] Bocci, M., Ed., Vigoureux, M., Ed., and S. Bryant, Ed., "MPLS Generic Associated Channel", RFC 5586, DOI 10.17487/RFC5586, June 2009, <https://www.rfc-editor.org/info/rfc5586>.

[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>.

[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>.

[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>.

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