Network Working Group
Internet-Draft
Intended status: Experimental
Expires: September 10, 2020

X. Geng
M. Chen
Huawei
March 09, 2020

SRH Extension for Redundancy Protection
draft-geng-spring-redundancy-protection-srh-00

Abstract

Redundancy protection is a method of service protection by sending copies of the same packets of one flow over multiple paths, which includes packet replicaiton, elimination and ordering. This document defines SRv6 header(SRH) extensions to support redundancy protection.

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 .

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 September 10, 2020.

Table of Contents

1. Introduction

Redundancy protection is a method of providing 1+1 protection by sending copies of the same packets of one flow over multiple paths, which includes packet replicaiton, elimination and ordering. This document defines SRv6 header(SRH) extensions to support redundancy protection.

2. Terminology and Conventions

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 [RFC2119].

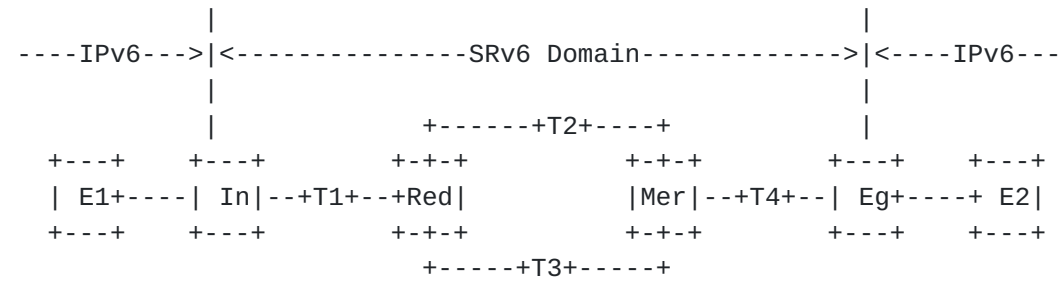
Redundancy Node: the start point of redudancy protection, which is a network device that could implement packet replication.

Merging Node: the end point of redudancy protection, which is a network node that could implement packet elimination and ordering(optionally).

Editor's Note: Similar mechanism is defined as "Service Protection" in the [RFC8655]. In this document, we define a new term "Redundancy Protection" to distinguish with other service protection method. Some of the terms are the similar as [RFC8655].

3. Redundancy Protection Requirement Analysis

The figure shows how to provide redundancy protection over SRv6.



As the figure shows, an IPv6 flow is sent out from the end station E1. The packet of the flow is encapsulated in an outer IPv6+SRH header in the Ingress(In) and transported through an SRv6 domain. In the Egress(Eg), the outer IPv6 header+SR of the packet is popped, and the packet is sent to the destination E2.

The process of redundancy protection is as follows: 1) The flow is replicated in Rep(Redundancy Node); 2) Tow replicated flows go through different paths till Mer (Merging Node); When there is any failures happened in one the path, the service continues to deliver through the other path without break; 3) The first received packet of the flow is transmitted from Mer (Merging Node) to Eg(Egress), and the redundant packets are eliminated. 4) Sometimes, the packet will arrive out of order because of redundancy protection, the function of reordering may be necessary in the Merging Node.

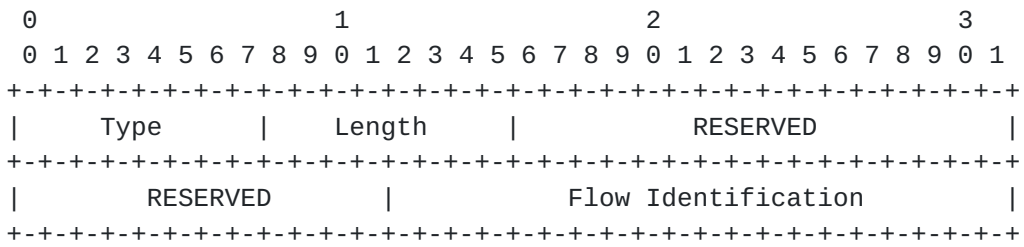
This document defines Flow Identification and Sequence Number in Segment Routing Header(SRH) as an extension of the current draft[I-D.ietf-6man-segment-routing-header] to support redundancy protection.

Flow Identification is used to distinguish flows and Sequence Number is used to distinguish packets in the same flow when doing packet merging and ordering.

4. SRH Extensions for Redundancy Protection

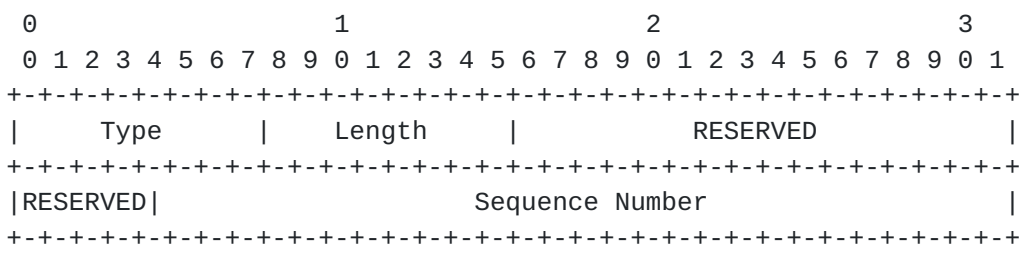
Flow Identification and Sequence Number could be defined in SRH optional TLV.

4.1. Option 1: seperated TLVs for flow identification and sequence number



where:

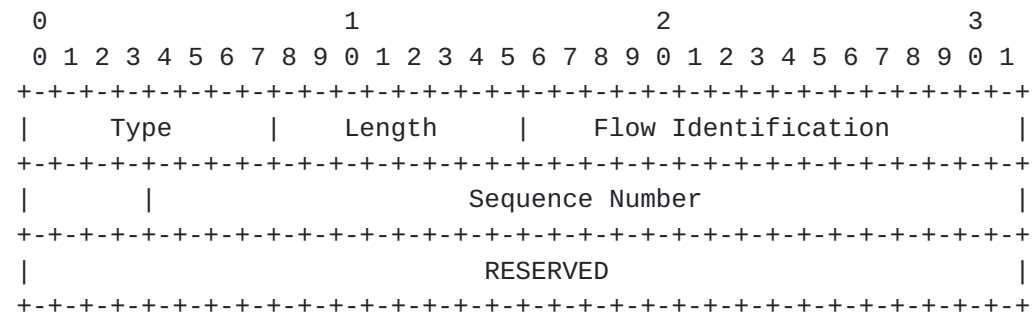
- Type: 8bits, to be assigned by IONA.
- Length: 8 octets.
- RESERVED: 28 bits, MUST be 0 on transmission and ignored on receipt.
- Flow Identification: 20 bits, which is used for identifying redundant protection flow.



where:

- Type: 8 bits, to be assigned by IONA.
- Length: 8.
- RESERVED: 20 bits. MUST be 0 on transmission and ignored on receipt.
- Sequence Number: 28 bits, which is used for indicating sequence number of the redundant protection flow.

4.2. Option 2 unified TLV for flow identification and sequence number



where:

- Type: 8bits, to be assigned by IANA.
- Length: 8 octets.
- Flow Identification: 20 bits, which is used for identifying the redundant protection flow.
- Sequence Number: 28 bits, which is used for indicating sequence number of the redundant protection flow.
- Reserved: 32 bits. MUST be 0 on transmission and ignored on receipt.

5. IANA Considerations

TBD

6. Security Considerations

TBD

7. Acknowledgements

Thank you for valuable comments from James Guichard and Andrew Mail

8. Normative References

[I-D.ietf-6man-segment-routing-header]
Filsfils, C., Dukes, D., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header-26 (work in progress), October 2019.

[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>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

Authors' Addresses

Xuesong Geng
Huawei

Email: gengxuesong@huawei.com

Mach(Guoyi) Chen
Huawei

Email: mach.chen@huawei.com