IPv6 Maintenance Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 24, 2021

X. Geng
M. Chen
F. Yang
Huawei Technologies

February 20, 2021

SRH Extension for Redundancy Protection
draft-geng-6man-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 replication, 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 August 24, 2021.

Copyright Notice

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 replication, 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 redundancy protection, which is a network device that could implement packet replication.

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

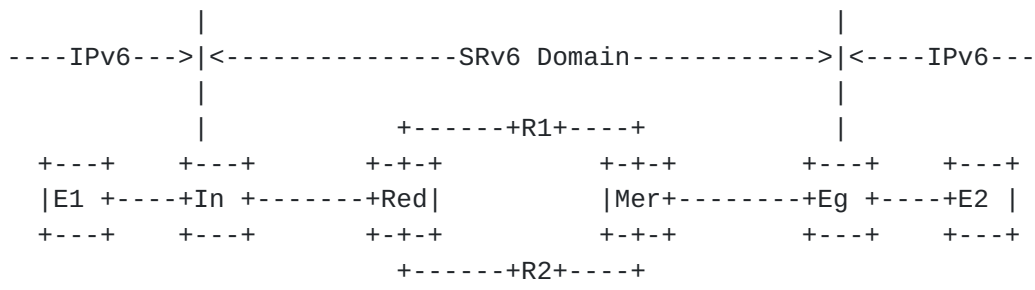
Flow Identification: information in SR data service to indicate one flow.

Sequence Number: information in SR data service to indicate the packet sequence of one flow.

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 over SRv6 Scenario

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+SRH header of packet is popped, and the packet is sent to the destination E2.

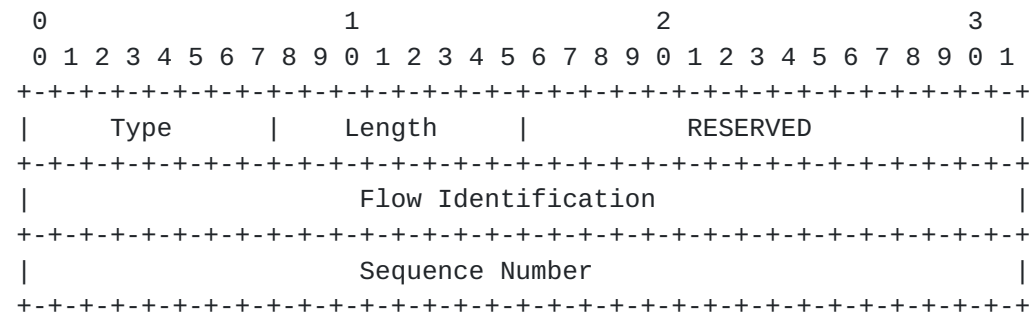
The process of redundancy protection is as follows: 1) The flow is replicated in Red (Redundancy Node); 2) Two replicated flows go through different paths till Mer (Merging Node); When there is any failures happened in one the path, the service continues to deliver through the other path without break; 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 [RFC8754] 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 Extension for Redundancy Protection

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



where:

- Type: 8 bits, indicates the use of redundancy protection, to be assigned by IANA.
- Length: 8 bits.
- Reserved: 16 bits. MUST be 0 on transmission and ignored on receipt.
- Flow Identification: 32 bits, which is used for identifying the redundant protection flow.
- Sequence Number: 32 bits, which is used for indicating sequence number of the redundant protection flow.

5. IANA Considerations

This document requires registration of a specific type of TLV used for redundancy protection in "Segment Routing Header TLVs" registry.

6. Security Considerations

TBD

7. Acknowledgements

Thanks for the valuable comments from James Guichard and Andrew Malis.

8. 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>.

[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>.

[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

Xuesong Geng
Huawei Technologies
Beijing
China

Email: gengxuesong@huawei.com

Mach(Guoyi) Chen
Huawei Technologies
Beijing
China

Email: mach.chen@huawei.com

Fan Yang
Huawei Technologies
Beijing
China

Email: shirley.yangfan@huawei.com