Abstract

This document specifies the fast redundancy protection mechanism, aimed at providing protection of the links and domain boundary nodes for network that use segment routing.

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 March 1, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

This document extends the use of Anycast-SID FRR to provide links and domain boundary nodes that use segment routing.

2. Conventions used in this document

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.

3. Motivation

The procedures specified in this document, in combination with [I-D.ietf-spring-segment-routing] provide the fast redundancy protection.

The procedures specified in this document aims at providing protection of the links and domain boundary nodes for network that use segment routing

4. Anycast-SID FRR Solution

4.1. Domain boundary nodes protection

The solution consists of three parts.

- Configure the same anycast prefix and associated prefix-sid for each domain boundary node that forms redundant protection, then the anycast prefix and associated prefix-sid with Anycast-Group flag should be advertised to the neighbor node.

- Create the anycast-group forwarding entry (i.e. FRR entry) after the direct neighbor node of the domain boundary nodes receive the prefix-sid with Anycast-Group flag advertisement. The anycast-

---

group forwarding entry includes the forwarding information which points to each of the domain boundary node, then the forwarding entry pointing to the main domain boundary (one of the direct connected boundary nodes from the PLR) is set to the active state, and others are set to the backup state. Only the direct neighbor of the domain boundary nodes need to set up the anycast-group forwarding entry.

- if the neighbor node detects the main domain boundary node failure, the neighbor node immediately activates the backup entry. Note that the backup entry contains the node-sid of the slave boundary node, and the packet will be forwarded based on the node-sid, not the anycast prefix-sid again.

The figure above describes a network example with two groups of the domain boundary nodes. The GW11 and GW12 are in the same anycast group. They are all configured with the same anycast prefix and the same prefix-sid 100, in addition, GW11 has node-sid 110 and GW12 has node-sid 120. All these prefix-sid should be advertised to the Neighbors (e.g., node A3 and A5), and the anycast-group forwarding entry will be set up by the direct Neighbor node A3 and A5. For example, the anycast-group forwarding entry created by A3 contains a master item which points to anycast-sid 100 and a slave item which points to node-sid 120.

When A3 detects GW11 failure, it immediately diverting traffic from GW11 to A4 (e.g. the best next-hop to node-sid 120) according to the anycast-group forwarding entry.
It is an implementation choice for data-plane whether the slave item only points to node-sid 120 for cascade table lookup, or integrates the forwarding information of node-sid 120 (such as a single next-hop, a TI-LFA FRR index for cascade table lookup, or an ECMP index for cascade table lookup).

Note that the anycast-group FRR described in this document could co-exist with other FRR solutions, such as LFA/RLFA/TI-LFA. The anycast-group FRR solution needn’t complex alternate path computation, it just reuses the forwarding information which points to the slave boundary node.

4.2. Links and nodes protection in Inter-Area scenario

TBD.

5. Security Considerations

TBD.

6. Acknowledgements

TBD.

7. Normative references

[I-D.ietf-isis-segment-routing-extensions]

[I-D.ietf-ospf-ospfv3-segment-routing-extensions]

[I-D.ietf-ospf-segment-routing-extensions]
[I-D.ietf-spring-segment-routing]


Authors' Addresses

Ran Chen
ZTE Corporation
No.50 Software Avenue, Yuhuatai District
Nanjing, Jiangsu Province  210012
China

Phone: +86 025 88014636
Email: chen.ran@zte.com.cn

Shaofu Peng
ZTE Corporation
No.68 Zijinghua Road, Yuhuatai District
Nanjing, Jiangsu Province  210012
China

Email: peng.shaofu@zte.com.cn

Jie Han
ZTE Corporation
No.68 Zijinghua Road, Yuhuatai District
Nanjing, Jiangsu Province  210012
China