Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 4, 2014

Pierre Francois
IMDEA Networks
Clarence Filsfils
Cisco Systems, Inc.
Bruno Decraene
Orange
Rob Shakir
BT
January 31, 2014

Use-cases for Resiliency in Segment Routing
draft-francois-spring-resiliency-use-case-00

Abstract

This document describes the use cases for resiliency in SR networks.

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 http://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 4, 2014.

Table of Contents

1. Introduction

Segment Routing (SR) aims at supporting services with tight SLA guarantees [1]. This document reviews alternative techniques to provide Fast Reroute (FRR) for SR traffic. Note that these techniques can be applied to protect LSPs created with LDP as well as pure IP traffic.

A FRR technique involves the pre-computation and dataplane pre-installation of backup path such as the repair traffic in 50msec upon failure detection. The term "protection" is often used as a synonym for FRR. Such technique supposes the existing of a sub-10msec failure detection technique.

Three key alternatives are described: path protection, local protection without operator management and local protection with operator management.

The purpose of this document is to illustrate the different techniques and explain how an operator could combine them in the same network. Solutions are not defined in this document.

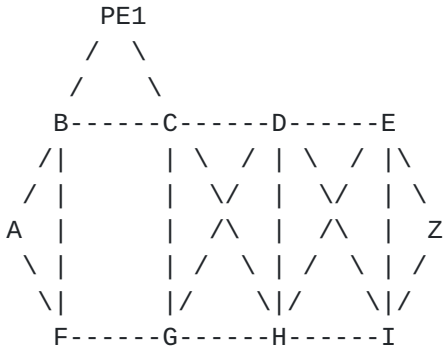

Figure 1: Reference topology

We use Figure 1 as a reference topology throughout the document. We describe the various use-cases in the next sections. All link metrics are equal to 1, with the exception of the links of PE1 which are configured with a metric of 100.

2. Path protection

A first protection strategy consists in excluding any local repair but instead use end-to-end path protection.

For example, a PW from A to Z can be "path protected" in the direction A to Z in the following manner: the operator configures two

SR tunnels T1 and T2 from A to Z. The two tunnels are installed in the forwarding plane of A and hence are ready to encapsulate and forward packets. The two tunnels are installed over disjoint paths using adjacency segments (T1 over segment list {AB, BC, CD, DE, EZ} and T2 over segment list {AF, FG, GH, HI, IZ}). When T1 is up, the packets of the PW are sent on T1. When T1 fails, the packets of the PW are sent on T2. When the tunnel T1 comes back up, the operator either allows for an automated reversion of the traffic onto T1 or selects an operator-driven reversion. The end-to-end liveness of a tunnel is for example checked with BFD.

From an SR viewpoint, we would like to highlight the following requirement: the adjacency segments used to support the tunnels T1 and T2 MUST NOT benefit from local protection. This is achieved by resetting the B-flag in the related AdjSID's as per the IGP extensions defined in [3].

3. Management-free local protection

An alternative protection strategy consists in management-free local protection.

For example, a PW from C to E transported by the single segment NodeSID(E) benefits from management-free local protection by having each node along the path (e.g. C and D) to automatically pre-compute and pre-install backup path for the destination E. Upon local detection of the failure (e.g. link BFD), the traffic is repaired over the backup path in sub-50msec.

The backup path computation should support the following requirements:

- 100% link, node, and SRLG protection in any topology
- Automated computation by the IGP
- Selection of the backup path such as to minimize the chance for transient congestion and/or delay during the protection period, as reflected by the IGP metric configuration in the network.

An SR solution aimed at supporting these requirements is defined in [2].

4. Managed local protection

A final alternative protection strategy consists in managed local protection.

For policy reasons, the operator may want very specific backup paths to be used.

For example, the operator may want the backup path to end at the next-hop (or next-next-hop for node failure) hence excluding IPFRR/ LFA types of backup path. Also, the operator might want to tightly control the backup path to the next-hop: for the destination Z upon the failure of link CD, the backup path CGHD might be desired while the backup paths CGD and CHD are refused.

The protection mechanism must support the explicit configuration of the backup path either under the form of high-level constraints (end at the next-hop, end at the next-next-hop, minimize this metric, avoid this SRLG...) or under the form of an explicit segment list.

5. Co-existence

The operator may want to support several very-different services on the same packet-switching infrastructure.

The SR resiliency architecture allows the co-existence of different FRR techniques.

Let us illustrate this for adjacency segments with the following example.

- Node C is configured with 3 adjacency segments for the connected interface to D: AdjSID(CD1), AdjSID(CD2) and AdjSID(CD3)
- SR Flow F1: from A to E over segment list {NodeSID(C), AdjSID(CD1), NodeSID(E)}
- SR Flow F2: from F to I over segment list {NodeSID(C), AdjSID(CD2), NodeSID(I)}
- SR Flow F3: from G to Z over segment list {NodeSID(C), AdjSID(CD3), NodeSID(Z)}
- Node C is configured with a distinct protection technique for each adjacency segment. AdjSID(CD1) is configured without protection, AdjSID(CD2) is configured to benefit from management-free local protection and AdjSID(CD3) is configured for managed local protection over the path {AdjSID(CH), AdjSID(HD)}

Such a co-existence is partially supported by the SR IGP extensions [ref tbd]

- Multiple adjacency segments can be advertised for the same adjacency
- The non-protected property of AdjSID(CD1) is signalled by a reset B flag.

- The protected property of AdjSID(CD2) and AdjSID(CD3) are signalled by a set B flag.

The SR IGP extension should be extended to discreminate between AdjSID(CD2) and AdjSID(CD3). A single flag could be defined (managed path vs fully automated).

6. References

[1] Filsfils, C., Previdi, S., Bashandy, A., Decraene, B., Litkowski, S., Horneffer, M., Milojevic, I., Shakir, R., Ytti, S., Henderickx, W., Tantsura, J., and E. Crabbe, "Segment Routing Architecture", draft-filsfils-rtgwg-segment-routing-00 (work in progress), June 2013.

[2] Francois, P., Filsfils, C., Bashandy, A., Decraene, B., and S. Litkowski, "Topology Independent Fast Reroute using Segment Routing", November 2013.

[3] Previdi, S., Filsfils, C., and A. Bashandy, "IS-IS Segment Routing Extensions", October 2013.

Authors' Addresses

Pierre Francois
IMDEA Networks
Leganes
ES

Email: pierre.francois@imdea.org

Clarence Filsfils
Cisco Systems, Inc.
Brussels
BE

Email: cfilsfil@cisco.com

Bruno Decraene
Orange
Issy-les-Moulineaux
FR

Email: bruno.decraene@orange.com

Rob Shakir
BT
London
UK

Email: rob.shakir@bt.com