Designation of PLRs in RSVP-TE Fast Reroute
draft-dong-ccamp-rsvp-te-plr-designation-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 1, 2010.

Copyright Notice

Copyright (c) 2009 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 (http://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.

Abstract

Dong, et al. Expires September 1, 2010 [Page 1]
This document defines RSVP-TE extensions which enable the ingress node to designate particular LSRs along the path as Points of Local Repair (PLRs) of the protected LSP, and further indicate the protection type of each PLR. These mechanisms could enhance the control over the establishment of backup LSPs, and also could save the resources needed for establishing and maintaining unnecessary backup LSPs.

Table of Contents

1. Introduction..................................................2
2. Conventions used in this document............................3
3. Problem Statement............................................3
4. RSVP-TE Extensions...........................................3
   4.1. Extensions to IPv4 Prefix Subobject....................3
   4.2. Extensions to IPv6 Prefix Subobject....................4
   4.3. Backward Compatibility................................5
5. Selection of PLRs............................................5
6. Operations...................................................5
   6.1. Operation of Head End...................................5
   6.2. Operation of Other LSRs................................5
7. Security Considerations......................................6
8. IANA Considerations..........................................6
9. References...................................................6
   9.1. Normative References..................................6
   9.2. Informative References................................6
Authors’ Addresses..............................................7

1. Introduction

Currently the fast reroute mechanisms of RSVP-TE enable the ingress node of protected LSP to indicate whether local protection is desired and whether node protection is desired for this LSP. However, such indication is relevant to the whole LSP, the ingress node cannot indicate which LSRs on the path are desired to be PLRs, and the protection type of each PLR.

This document defines RSVP-TE extensions to enable an ingress node to designate particular nodes along the path as Points of Local Repair (PLRs) of the protected LSP, and further indicate the protection type of the PLRs.

These mechanisms could enhance the control of the ingress node of the protected LSP on the establishment of backup LSPs. It is useful when only a subset of the LSRs on the path are required to operate as PLRs, and only some of them are required to provide node protection. Since
in such cases not all of the LSRs need to perform as PLRs, these mechanisms could save the resources of establishing and maintaining unnecessary backup LSPs.

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. Problem Statement

RFC 4090 has defined mechanisms to establish local protection for a particular LSP. The fast reroute mechanisms of RFC 4090 enable the ingress node of the protected LSP to indicate whether local protection is desired and what protection type is needed for this LSP. However, such indication is at the granularity of LSP level, the ingress node cannot explicitly indicate which subset of LSRs along the path are desired to be PLRs, and the protection type of each PLR.

In some scenarios the ingress node may need to specify particular LSRs as PLRs, and the protection type of each particular PLR. This can be helpful in many aspects. Firstly, this enables the ingress node to setup the backup LSPs in a more controllable way. Secondly, this could avoid making LSRs which do not have enough resources to provide local protections work as PLRs. Thirdly, this could save bandwidth reserved for unnecessary backup LSPs.

The subsequent sections define extensions to RSVP-TE to meet the requirements in such scenarios, and describe operations needed for these extensions.

4. RSVP-TE Extensions

The Explicit Route Object (ERO) is extended to carry information of PLR designation and type of local protection. The low order bits of the Reserved field in IPv4 prefix and IPv6 prefix subobjects are used as flags to indicate whether the LSR represented by the subobject should operate as a PLR and the desired type of local protection.

4.1. Extensions to IPv4 Prefix Subobject

Two new flags are defined in this subobject. The structure of extended IPv4 prefix subobject is as below:
P: Local Protection flag. The P bit represents whether this subobject is designated as a PLR. It will be set to 0 if the node is designated to be a PLR for the protected LSP, and set to 1 otherwise. If the "Local Protection Desired" flag in the SESSION_ATTRIBUTE Object is not set, no local protection will be used for the whole LSP, and the value of the P bit is insignificant.

N: Node Protection flag. The N bit represents whether node protection is required for this subobject. It will be set to 1 if node protection is desired, and set to zero if the protection type is indicated by the Node Protection flag in the SESSION_ATTRIBUTE Object. Note the N bit makes sense only when the "Local Protection Desired" flag in the SESSION_ATTRIBUTE Object is set and the above P bit is set to 0.

4.2. Extensions to IPv6 Prefix Subobject

Two new flags are defined in this subobject. The structure of extended IPv6 prefix subobject is as below:

P: Local Protection flag. The P bit represents whether this subobject is designated as a PLR. It will be set to 0 if the node is designated to be a PLR for the protected LSP, and set to 1 otherwise. If the...
"Local Protection Desired" flag in the SESSION_ATTRIBUTE Object is not set, no local protection will be used for the whole LSP, and the value of the P bit is insignificant.

N: Node Protection flag. The N bit represents whether node protection is required for this subobject. It will be set to 1 if node protection is desired, and set to zero if the protection type is indicated by the Node Protection Flag in the SESSION_ATTRIBUTE Object. Note the N bit makes sense only when the "Local Protection Desired" flag in the SESSION_ATTRIBUTE Object is set and the P bit is set to 0.

4.3. Backward Compatibility

The P bit and N bit are designed to be backward compatible with current protection mechanisms. LSRs which do not support this extension will treat these bits as reserved bit and ignore the value of them. When both the 2 bits are set to 0 by head end LSR, the protection behavior of all other LSRs on the path (no matter support this extension or not) is the same as current mechanisms.

5. Selection of PLRs

The selection of PLRs and the protection type are determined by the tunnel ingress node. Normally it can be based on local policy of the ingress node and information about the network. For example, the ingress node may decide to choose a subset of LSRs on the path as PLRs and specify particular protection type to protect critical nodes and/or links, or it may exclude some nodes from being PLRs to reduce burden on these nodes and save bandwidth.

6. Operations

6.1. Operation of Head End

If the head-end LSR needs to control the protection of the LSP, it SHOULD set the P bit and N bit in corresponding ERO subobjects of the PATH message properly based on the result of PLR selection.

6.2. Operation of Other LSRs

If a PATH message is received, the LSR SHOULD check the "Local Protection Desired" and "Node protection desired" flags in the SESSION Attribute Object along with the P bit and N bit in corresponding ERO subobjects, then perform protection based on the flags.
If some LSR on the path needs to add subobjects to the ERO, it MAY set the P bit and N bit of the subobjects according to local policy.

7. Security Considerations

This document does not introduce new security issues.

8. IANA Considerations

There is no IANA action required by this draft.

9. References

9.1. Normative References


9.2. Informative References
Authors’ Addresses

Jie Dong
Huawei Technologies Co.,Ltd
KuiKe Building, No.9 Xinxi Rd.,
Hai-Dian District
Beijing, 100085
P.R. China
EMail: dongjie_dj@huawei.com

Mach(Guoyi) Chen
Huawei Technologies Co.,Ltd
KuiKe Building, No.9 Xinxi Rd.,
Hai-Dian District
Beijing, 100085
P.R. China
EMail: mach@huawei.com

Chun Liu
Huawei Technologies Co.,Ltd
Huawei Building, No.156 Beiqing Rd.
Hai-Dian District
Beijing, 100095
P.R. China
EMail: liuchuner1981@huawei.com