CCAMP Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 5, 2012

WJ. He, Ed.
F. Zhang
ZTE

July 4, 2011

RSVP-TE Extensions to Notification for Shared Mesh Protection
draft-he-ccamp-notification-shared-mesh-protection-00

Abstract

The shared mesh protection(SMP) mechanism enables multiple protection paths within a shared mesh protection domain to share protection resources, which allows only one of the n working paths to be protected at the same time. This document extends RSVP-TE to notify the state of shared resources in MPLS Transport Profile (MPLS-TP) mesh topology.

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 January 5, 2012.

Table of Contents

1. Introduction

In mesh protection, network resources may be shared to provide protection for working paths that do not share the same endpoints. This form of protection can make very efficient use of network resources, but requires careful synchronization to ensure that only one set of traffic is switched to the protection resources at any time.

[RFC4872] defines the shared mesh restoration schemes based on control plane extensions, but does not cover the shared mesh protection scenarios.

In order to coordinate the use of protection resources, this document specifies the notification schemes to notify the endpoint of the protecting LSP the state of the shared resource.

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. Shared Mesh Protection

Consider the following topology:

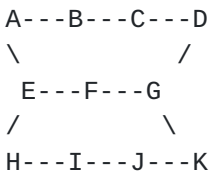

Figure 1 : A Shared Mesh Protection Topology

The working LSPs W1[via nodes A,B,C,D] and W2[via nodes H,I,J,K] could be protected by P1[via nodes A,E,F,G,D] and P2[via nodes H,E,F,G,K]respectively. For both cases, 1:1 protection may be used.

Thus, it is possible for the network resources on the segment EFG to be shared by the two protection paths. In this way, shared mesh protection can substantially reduce the amount of network resources that have to be reserved.

If there are no failures affecting either of the two working paths, the network segment EFG may carry no traffic. In the event of only one failure, the segment EFG carries traffic from the working path that experiences the failure.

3.1. Shared Mesh Protection Planning

Shared mesh protection will typically be subject to careful network planning. Operator plans the shared mesh protection group (SMPG) which includes the protected paths and protecting paths. Different SPMGs do not share protection resources and are protected independently.

In Figure 1, the working LSP W1,W2 and protecting LSPs P1,P2 consist of a shared mesh protection group, in which the protecting LSPs P1 and P2 share the segment FEG although they belong to different sessions. In order to achieve this, the "Resource Sharing" Association type that defined in [RFC4873] and [I-D.ietf-ccamp-assoc-ext] can be used here. When operators plan shared mesh protection group, they will assign a group ID and a virtual address for the shared mesh protection group. The protecting LSP will be signaled with the "Resource Sharing" type ASSOCIATION object, the Association ID is set to the group ID, and the Association source is set to the group virtual address.

3.2. Signaling Protection LSPs

When the protecting LSPs are signaled, the PROTECTION object, Notify Request object and "Recovery" type ASSOCIATION object are included in the Path message. Furthermore, the "Resource Sharing" type ASSOCIATION object SHOULD be inserted, the Association ID set to the associated protection group ID and the Association source set to the protection group virtual address.

Any node processing a Path message for which the node does not have a matching state, and which contains an ASSOCIATION object with a "Resource Sharing" type, examines existing LSPs for matching Association Type, Association Source, and Association ID values. If any match is found, then [RFC3209] style resource sharing SHOULD be provided between the new and old LSPs.

3.3. Processing

This section illustrates the realization of the shared mesh protection for the topology shown in Figure 1.

3.3.1. Basic Operation

If a failure occurs on the W2, the shared mesh protection will operate as follows:

a. Node H detects the signal failure, switches the traffic to P2, and sends Path message to node E with O bit of protection object setting to 1.
b. Upon receipt of the Path message with the O bit of protection object from 0 to 1, node E compares the protection switching priority of P2 and P1, then send notify message with the new error code/sub-code "notify error/resource occupied by the high priority" or "notify error/resource occupied by the low priority" to P1's ingress node.

When the fault of the working LSP disappears, the shared mesh protection will operate as follows:

a. The ingress node H will switch traffic to the working LSP, and refresh the Path message with the O bit of protection object setting to 0.
b. Upon receiving the Path message with the O bit of protection object from 1 to 0, sharing start endpoint(node E) will send notify message with new error code/sub-code "notify error/ resource available" to the other protecting LSP's ingress node.

3.3.2. Rerouting

If the ingress of the protecting LSP receives notify message with "notify error/resource occupied by the high priority", the node should reroute the protecting LSP. Because that the traffic of higher priority LSP may also be lost during the preemption, the node may also reroute for a more optimized path according to the local policy, when the node receives notify message with "notify error/ resource occupied by the low priority". If the protecting LSP reroutes, the new LSP will exclude the shared segment which was occupied by the other LSP.

3.3.3. Preemption

During the sharing resource was occupied by one of the protecting LSPs, the other working LSP may also experiences some fault. In this case, these resource MUST be preempted by the high priority LSP.

In Figure 1, if a failure occurs on the W1 while the W2 is still in failure state, the shared mesh protection will operate as follows:

- The node A will not switch the traffic, if it has received the notification that the resource has been occupied by the high priority.
- The node A has not received the notification that the resource has been occupied by the high priority LSP. The operation is as follows:
  1. Node A switches the traffic to P1, and sends Path message to node E with O bit of protection object setting to 1.
  2. Once Node E (sharing start endpoint)receives the Path message with the O bit of protection object from 0 to 1, it compares the protection switching priority of P2 and P1. The node will send notify message with the new error code/sub-code "notify error/resource occupied by the high priority" to P2's ingress node.
  3. Upon receipt of the notify message that the resource has been occupied by the high priority, node H will switch the traffic from P2 to W2, and sends Path message to node E with O bit of protection object setting to 0.

4. IANA Considerations

TBD

5. Security Considerations

TBD

6. Acknowledgement

TBD

7. Informative References

[I-D.ietf-ccamp-assoc-ext]
Berger, L., Faucheur, F., and A. Narayanan, "RSVP Association Object Extensions", draft-ietf-ccamp-assoc-ext-00 (work in progress), May 2011.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC4872] Lang, J., Rekhter, Y., and D. Papadimitriou, "RSVP-TE

Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, May 2007.

[RFC4873] Berger, L., Bryskin, I., Papadimitriou, D., and A. Farrel, "GMPLS Segment Recovery", RFC 4873, May 2007.

Authors' Addresses

Wenjuan He (editor)
ZTE

Email: he.wenjuan1@zte.com.cn

Fei Zhang
ZTE

Email: zhang.fei3@zte.com.cn