TEAS Working Group   J. He
Internet Draft   I. Busi
Updates (if published): RFC 4872   Huawei
Intended status: Standards Track

Expires: April 20, 2019   October 22, 2018

GMPLS Signaling Extensions for Shared Mesh Protection
draft-he-teas-gmpls-signaling-smp-00.txt

Status of this Memo

Copyright Notice

Abstract

ITU-T Recommendation G.808.3 [G808.3] defines the generic aspects of a shared mesh protection (SMP) mechanism, where the difference between SMP and shared mesh restoration (SMR) is also identified. ITU-T Recommendation G.873.3 [G873.3] defines the protection switching operation and associated protocol for shared mesh protection (SMP) at the optical data unit (ODU) layer. RFC 7412 provides requirements for any mechanism that would be used to implement SMP in an MPLS-TP network.

This document updates RFC 4872 to provide the extensions to the Generalized Multi-Protocol Label Switching (GMPLS) signaling to support the control of the shared mesh protection.

Table of Contents

1. Introduction

RFC 4872 [RFC4872] defines extension of RSVP-TE to support shared mesh restoration (SMR) mechanism. Shared mesh restoration can be seen as a particular case of pre-planned LSP rerouting that reduces the recovery resource requirements by allowing multiple protecting LSPs to share common link and node resources. The recovery resources for the protecting LSPs are pre-reserved during the provisioning phase, and an explicit restoration signaling is required to activate (i.e., commit resource allocation at the data plane) a specific protecting LSP instantiated during the provisioning phase.

ITU-T Recommendation G.808.3 [G808.3] defines the generic aspects of a shared mesh protection (SMP) mechanism. ITU-T Recommendation G.873.3 [G873.3] defines the protection switching operation and associated protocol for shared mesh protection (SMP) at the optical data unit (ODU) layer. RFC 7412 provides requirements for any mechanism that would be used to implement SMP in an MPLS-TP network.

SMP differs from SMR in the activation/protection switching operation. The former activates a protecting LSP via the automatic protection switching (APS) protocol in the data plane when the working LSP fails, while the latter via the control plane signaling. It is therefore necessary to distinguish SMP from SMR during provisioning so that each node involved behaves appropriately in the recovery phase when activation of a protecting LSP is done.

This document updates RFC 4872 to provide the extensions to the Generalized Multi-Protocol Label Switching (GMPLS) signaling to support the control of the shared mesh protection mechanism. Only the generic aspects for signaling SMP are addressed by this document. The technology-specific aspects are expected to be addressed by other drafts.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

In addition, the reader is assumed to be familiar with the terminology used in [RFC4872] and [RFC4426].

3. SMP Definition

ITU-T Recommendation G.808.3 [G808.3] defines the generic aspects of a shared mesh protection (SMP) mechanism. ITU-T Recommendation G.873.3 [G873.3] defines the protection switching operation and associated protocol for shared mesh protection (SMP) at the optical data unit (ODU) layer. RFC 7412 provides requirements for any mechanism that would be used to implement SMP in an MPLS-TP network.

The SMP mechanism is based on pre-computed protection transport entities that are pre-configured into the network elements. Pre-

configuration here means pre-reserving resources for the protecting LSPs without activating a particular protecting LSP (e.g. in circuit networks, the cross-connects in the intermediate nodes of the protecting LSP are not pre-established). Pre-configuring but not activating the protecting LSP allows the common link and node resources in a protecting LSP to be shared by multiple working LSPs that are physically (i.e., link, node, SRLG, etc.) disjoint. Protecting LSPs are activated in response to failures of working LSPs or operator's commands by means of the APS protocol that operates in the data plane. SMP is always revertive.

SMP has a lot of similarity to SMR except that the activation in case of SMR is achieved by control plan signaling during the recovery operation while SMP is done by APS protocol in the data plane. SMP has advantages with regard to the recovery speed compared with SMR.

4. GMPLS Signaling Extension for SMP

Consider the following network topology:

```
A---B---C---D
 \         /
  E---F---G
 /         \
H---I---J---K
```

The working LSPs [A,B,C,D] and [H,I,J,K] could be protected by [A,E,F,G,D] and [H,E,F,G,K], respectively. Per [RFC3209], in order to achieve resource sharing during the signaling of these protecting LSPs, they must have the same Tunnel Endpoint Address (as part of their SESSION object). However, these addresses are not the same in this example. Similar to SMR, a new LSP Protection Type of the secondary LSP is defined as "Shared Mesh Protection" (see PROTECTION object defined in [RFC4872]) to allow resource sharing along nodes E, F, and G. In this case, the protecting LSPs are not merged (which is useful since the paths diverge at G), but the resources along E, F, G can be shared.

When a failure is detected on one of the working LSPs (say working LSP [A,B,C,D]), the switching operation for the egress node (say node A) will be triggered by an Signal Degrade (SD) or Signal Fail (SF) on the working LSP. The egress node A will send a protection

switching request APS message (for example SF) to its adjacent (downstream) intermediate node (say node E) to activate setting up the corresponding protecting LSP. If the protection resource is available, Node E will send a confirmation message to the egress node A and forward the switching request APS message to its adjacent (downstream) node (say node F). When the confirmation message is received by node A and the protection resource is available, the cross-connection on node A is established. At this time the traffic is bridged to and selected from the protecting LSP at node A. The node E will wait for the confirmation message from node F, which triggers node E to set up the cross-connection for the protection transport entity being activated. If the protection resource is not available (due to failure or being used by higher priority connections), the switching will not be successful; the intermediate node may send a message to notify the end node, or keep trying until the resource is available or the switching request is cancelled. If the resource is in use by a lower priority protection entity, the lower priority service will be removed and then the intermediate node will follow the procedure as described for the case when the resource is available.

The following subsections detail how shared mesh protection can be implemented in an interoperable fashion using GMPLS RSVP-TE extensions (see [RFC3473]). This includes:

(1) the ability to identify a "secondary protecting LSP" (hereby

called the "secondary LSP") used to recover another primary working LSP (hereby called the "protected LSP")

(2) the ability to associate the secondary LSP with the protected LSP

(3) the capability to include information about the resources used by the protected LSP while instantiating the secondary LSP.

(4) the capability to instantiate during the provisioning phase several secondary LSPs in an efficient manner.

(5) the capability to support activation of a secondary LSP after failure occurrence via APS protocol in the data plane.

4.1. Identifiers

To simplify association operations, both LSPs (i.e., the protected and the secondary LSPs) belong to the same session. Thus, the SESSION object MUST be the same for both LSPs. The LSP ID,

however, MUST be different to distinguish between the protected LSP carrying working traffic and the secondary LSP.

A new LSP Protection Type "Shared Mesh Protection" is introduced to the LSP Flags of PROTECTION object (see [RFC4872]) to set up the two LSPs. This LSP Protection Type value is applicable to both uni- and bidirectional LSPs.

4.2. Signaling Primary LSPs

The PROTECTION object (see [RFC4872]) is included in the Path message during signaling of the primary working LSPs, with the LSP Protection Type value set to "Shared Mesh Protection".

Primary working LSPs are signaled by setting in the POTECTION object the S bit to 0, the P bit to 0, the N bit to 1 and in the ASSOCIATION object, the Association ID to the associated secondary protecting LSP_ID.

Note: N bit is set to indicate that the protection switching signaling is done via data plane.

4.3. Signaling Secondary LSPs

The PROTECTION object (see [RFC4872]) is included in the Path message during signaling of the secondary protecting LSPs, with the LSP Protection Type value set to "Shared Mesh Protection".

Secondary protecting LSPs are signaled by setting in the PROTECTION object the S bit and the P bit to 1, the N bit to 1 and in the ASSOCIATION object, the Association ID to the associated primary working LSP_ID, which MUST be known before signaling of the secondary LSP. Moreover, the Path message used to instantiate the secondary LSP SHOULD include at least one PRIMARY_PATH_ROUTE object (see [RFC4872]) that further allows for recovery resource sharing at each intermediate node along the secondary path.

With this setting, the resources for the secondary LSP SHOULD be pre-reserved, but not committed at the data plane level, meaning that the internals of the switch need not be established until explicit action is taken to activate this LSP. Activation of a

secondary LSP and protection switching to the activated protecting LSP is done using APS protocol in the data plane.

After protection switching completes the protecting LSP SHOULD be signaled with the S bit set to 0 and O bit set to 1 in the PROTECTION object. At this point, the link and node resources must be allocated for this LSP that becomes a primary LSP (ready to carry normal traffic). The formerly working LSP MAY be signaled with the A bit set in the ADMIN_STATUS object (see [RFC3473]).

5. Updates to PROTECTION Object

GMPLS extension requirements for SMP introduce several updates to the Protection Object (see [RFC4872]).

5.1. New Protection Type

A new LSP protection type "Shared Mesh Protection" is added in the protection object. This LSP Protection Type value is applicable to both uni- and bidirectional LSPs.

LSP (Protection Type) Flags

0x11   Shared Mesh Protection

5.2. Other Updates

N bit and O bit in the Protection object as defined in [RFC4872] are also updated to include applicability to SMP.

Notification (N): 1 bit

When set to 1, this bit indicates that the control plane message exchange is only used for notification during protection switching. When set to 0 (default), it indicates that the control plane message exchanges are used for protection-switching purposes. The N bit is only applicable when the LSP Protection Type Flag is set to either 0x04 (1:N Protection with Extra-Traffic), or 0x08 (1+1 Unidirectional Protection), or 0x10 (1+1 Bidirectional Protection), or 0x11 (Shared Mesh Protection). The N bit MUST be set to 0 in any other case.

Operational (O): 1 bit

When set to 1, this bit indicates that the protecting LSP is carrying the normal traffic after protection switching. The O bit is only applicable when the P bit is set to 1, and the LSP Protection Type Flag is set to either 0x04 (1:N Protection with Extra-Traffic), or 0x08 (1+1 Unidirectional Protection), or 0x10 (1+1 Bidirectional Protection), or 0x11 (Shared Mesh Protection). The O bit MUST be set to 0 in any other case.

6. Security Considerations

No further security considerations than [RFC4872].

7. IANA Considerations

There are no IANA actions required.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[RFC3473] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC4426] Lang, J., Rajagopalan, B., and D. Papadimitriou, "Generalized Multi-Protocol Label Switching (GMPLS) Recovery Functional Specification", RFC 4426, March 2006.

[RFC4872] Lang, J.P., Ed., Rekhter, Y., Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, May 2007.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017.

[G808.3] ITU-T, "Generic protection switching - Shared mesh protection", G.808.3, October 2012.

8.2. Informative References

[G873.3] ITU-T, "Optical transport network - Shared mesh protection", G.873.3, September 2017.

[RFC7412] Weingarten, Y., Aldrin, S., Pan, P., Ryoo, J., Mirsky, G., "Requirements for MPLS Transport Profile (MPLS-TP) Shared Mesh Protection", RFC 7412, December 2014.

Authors' Addresses

Jia He
Huawei Technologies Co.,Ltd.
F3-1B, R&D Center, Huawei Industrial Base, Bantian, Longgang
District, Shenzhen, China

Email: hejia@huawei.com

Italo Busi
Huawei

Email: italo.busi@huawei.com