TEAS Working Group
Internet-Draft
Updates: 4872, 4873 (if approved)
Intended status: Standards Track
Expires: October 21, 2022

J. He
I. Busi
Huawei Technologies
J. Ryoo
B. Yoon
ETRI
P. Park
KT

April 19, 2022

GMPLS Signaling Extensions for Shared Mesh Protection
draft-ietf-teas-gmpls-signaling-smp-12

Abstract

ITU-T Recommendation G.808.3 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 defines the protection switching operation and associated protocol for SMP at the Optical Data Unit (ODU) layer. RFC 7412 provides requirements for any mechanism that would be used to implement SMP in a Multi-Protocol Label Switching - Transport Profile (MPLS-TP) network.

This document updates RFC 4872 and RFC 4873 to provide the extensions to the Generalized Multi-Protocol Label Switching (GMPLS) signaling to support the control of the SMP.

Copyright Notice

Table of Contents

1. Introduction

RFC 4872 [RFC4872] defines extension of Resource Reservation Protocol - Traffic Engineering (RSVP-TE) to support Shared Mesh Restoration (SMR) mechanisms. SMR can be seen as a particular case of pre-planned Label Switched Path (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 explicit restoration signaling is required to activate (i.e., commit resource allocation at the data plane) a specific protecting LSP that was instantiated during the provisioning phase. RFC 4873 [RFC4873] details the encoding of the last 32-bit Reserved field of the PROTECTION object defined in [RFC4872]

ITU-T Recommendation G.808.3 [G808.3] defines the generic aspects of a shared mesh protection (SMP) mechanism, which are not specific to a particular network technology in terms of architecture types, preemption principle, and path monitoring methods, etc. ITU-T Recommendation G.873.3 [G873.3] defines the protection switching operation and associated protocol for SMP at the Optical Data Unit (ODU) layer. RFC 7412 [RFC7412] provides requirements for any mechanism that would be used to implement SMP in a Multi-Protocol Label Switching - Transport Profile (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 does it via 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. SMP has advantages with regard to the recovery speed compared with SMR.

This document updates [RFC4872] and [RFC4873] to provide the extensions to the Generalized Multi-Protocol Label Switching (GMPLS) signaling to support the control of the SMP mechanism. Specifically, it;

o defines a new LSP protection type, "Shared Mesh Protection," for the LSP Flags field [RFC4872] of the PROTECTION object (see Section 6.1),

o updates the definitions of the Notification (N) and Operational (O) fields [RFC4872] of the PROTECTION object to take the new SMP type into account (see Section 6.2), and

o updates the definition of the 16-bit Reserved field [RFC4873] of the PROTECTION object to allocate 8 bits to signal the SMP preemption priority (see Section 6.3).

Only the generic aspects for signaling SMP are addressed by this document. The technology-specific aspects are expected to be addressed by other documents.

RFC 8776 [RFC8776] defines a collection of common YANG data types for Traffic Engineering (TE) configuration and state capabilities. It defines several identities for LSP protection types. As this document introduces a new LSP Protection Type, [RFC8776] is expected to be updated to support the SMP specified in this document. [I-D.ietf-teas-yang-te] defines a YANG data model for the provisioning and management of TE tunnels, LSPs, and interfaces. It includes some protection and restoration data nodes relevant to this document. Management aspects of the SMP are outside the scope of this document, and they are expected to be addressed by other documents.

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], RFC 4426 [RFC4426], and RFC 6372 [RFC6372].

3. SMP Definition

[G808.3] defines the generic aspects of an SMP mechanism. [G873.3] defines the protection switching operation and associated protocol for SMP at the ODU layer. [RFC7412] provides requirements for any mechanism that would be used to implement SMP in a MPLS-TP network.

The SMP mechanism is based on pre-computed protecting LSPs 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 protecting LSPs allows link and node resources to be shared by the protecting LSPs of multiple working LSPs (that are themselves disjoint and thus unlikely to fail simultaneously). 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. The APS protocol messages are exchanged along the protecting LSP. SMP is always revertive.

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

4. Operation of SMP with GMPLS Signaling Extension

Consider the following network topology:

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

Figure 1: An example of SMP topology

The working LSPs [A,B,C,D] and [H,I,J,K] could be protected by the protecting LSPs [A,E,F,G,D] and [H,E,F,G,K], respectively. Per RFC 3209 [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, this document defines a new LSP Protection Type of the secondary LSP as "Shared Mesh Protection" (see Section 6.1) to allow resource sharing along nodes E, F, and G. Examples of shared resources include the capacity of a link and the cross-connects in a node. 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, such as Signal Fail (SF) and Signal Degrade (SD), occurs on one of the working LSPs (say working LSP [A,B,C,D]), the end node (say node A) that detects the failure initiates the protection switching operation. End node A will send a protection switching request APS message (for example, SF) to its adjacent (downstream) intermediate node (say node E) to activate the corresponding protecting LSP and will wait for a confirmation message from node E.

If the protection resource is available, node E will send the confirmation APS message to the end node A and forward the switching request APS message to its adjacent (downstream) node (say node F). When the confirmation APS message is received by node A, the cross-connection on node A is established. At this time traffic is bridged to and selected from the protecting LSP at node A. After forwarding the switching request APS message, node E will wait for a confirmation APS message from node F, which triggers node E to set up the cross-connection for the protecting LSP 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 (node E) MUST send a message to notify the end node (node A) (see Section 5.5). If the resource is in use by a lower priority protecting LSP, the lower priority service will be removed and then the intermediate node will follow the procedure as described for the case when the protection resource is available for the higher priority protecting LSP.

If node E fails to allocate the protection resource, it MUST send a message to notify node A (see Section 5.5). Then, node A will stop bridging and selecting traffic to/from the protecting LSP and proceed with the procedure of removing the protection allocation according to the APS protocol.

5. GMPLS Signaling Extension for SMP

The following subsections detail how LSPs using SMP can be signaled in an interoperable fashion using GMPLS RSVP-TE extensions (see RFC 3473 [RFC3473]). This signaling enables:

(1) the ability to identify a "secondary protecting LSP" (LSP [A,E,F,G,D] or LSP [H,E,F,G,K] from Figure 1, hereby called the "secondary LSP") used to recover another "primary working LSP" (LSP [A,B,C,D] or LSP [H,I,J,K] from Figure 1, 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 efficiently, and

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

5.1. 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 and the secondary LSP.

A new LSP Protection Type "Shared Mesh Protection" is defined (see Section 6.1) for the LSP Flags of PROTECTION object (see [RFC4872]) to set up the two LSPs. This LSP Protection Type value is applicable only to bidirectional LSPs as required in [G808.3].

5.2. 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 PROTECTION object the S bit to 0, the P bit to 0, and 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.

5.3. 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, the P bit, and 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 MUST 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 MUST 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 MUST 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 traffic). The formerly working LSP MAY be signaled with the A bit set in the ADMIN_STATUS object (see [RFC3473]).

Support for extra traffic in SMP is for further study. Therefore, mechanisms to set up LSPs for extra traffic are outside the scope of this document.

5.4. SMP Preemption Priority

The SMP preemption priority of a protecting LSP that the APS protocol uses to resolve the competition for shared resources among multiple protecting LSPs, is indicated in Preemption Priority field of the PROTECTION object in the Path message of the protecting LSP.

The Setup and Holding priorities in the SESSION_ATTRIBUTE object can be used by GMPLS to control LSP preemption, but, they are not used by the APS to resolve the competition among multiple protecting LSPs. This avoids the need to define a complex policy for defining Setup and Holding priorities when used for both GMPLS control plane LSP preemption and SMP shared resource competition resolution.

When an intermediate node on the protecting LSP receives the Path message, the priority value in the Preemption Priority field MUST be stored for that protecting LSP. When resource competition among multiple protecting LSPs occurs, the APS protocol will use their priority values to resolve the competition. A lower value has a higher priority.

In SMP, a preempted LSP MUST NOT be terminated even after its resources have been deallocated. Once the working LSP and the protecting LSP are configured or pre-configured, the end node MUST keep refreshing both working and protecting LSPs regardless of failure or preempted situation.

5.5. Notifying Availability of Shared Resources

When a lower priority protecting LSP is preempted, the intermediate node that performed preemption MUST send a Notify message with error code "Notify Error" (25) (see [RFC4872]) and error sub-code "Shared resources unavailable" (TBA1) to the end nodes of that protecting LSP. Upon receipt of this Notify message, the end node MUST stop sending and selecting traffic to/from its protecting LSP and try switching the traffic to another protecting LSP, if available.

When a protecting LSP occupies the shared resources and they become unavailable, the same Notify message MUST be generated by the intermediate node to all the end nodes of the protecting LSPs that have lower SMP preemption priorities than the one that has occupied the shared resources. In case the shared resources become unavailable due to a failure in the shared resources, the same Notify message MUST be generated by the intermediate node to all the end nodes of the protecting LSPs that have been configured to use the shared resources. These end nodes, in case of a failure of the working LSP, MUST avoid trying to switch traffic to these protecting LSPs that have been configured to use the shared resources and try switching the traffic to other protecting LSPs, if available.

When the shared resources become available, a Notify message with error code "Notify Error" (25) and error sub-code "Shared resources available" (TBA2) MUST be generated by the intermediate node. The recipients of this Notify message are the end nodes of the lower priority protecting LSPs that have been preempted and/or all the end nodes of the protecting LSPs that have lower SMP preemption priorities than the one that does not need the shared resources anymore. Upon receipt of this Notify message, the end node is allowed to reinitiate the protection switching operation as described in Section 4, if it still needs the protection resource.

5.6. SMP APS Configuration

SMP relies on APS protocol messages being exchanged between the nodes along the path to activate an SMP protecting LSP.

In order to allow the exchange of APS protocol messages, an APS channel has to be configured between adjacent nodes along the path of the SMP protecting LSP. This is done by other means than GMPLS signaling, before any SMP protecting LSP has been set up. Therefore, there are likely additional requirements for APS configuration which are outside the scope of this document.

Depending on the APS protocol message format, the APS protocol may use different identifiers than GMPLS signaling to identify the SMP protecting LSP.

Since APS protocol is for further study in [G808.3], it can be assumed that APS message format and identifiers are technology-specific and/or vendor-specific. Therefore, additional requirements for APS configuration are outside the scope of this document.

6. Updates to PROTECTION Object

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

6.1. 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 only bidirectional LSPs.

LSP (Protection Type) Flags:

0x20: Shared Mesh Protection

The rules defined in Section 14.2 of [RFC4872] ensure that all the nodes along an SMP LSP are SMP aware. Therefore, there are no backward compatibility issues.

6.2. Updates on Notification and Operational Bits

The definitions of the N and O bits in Section 14.1 of [RFC4872] are replaced as follows:

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 0x04 (1:N Protection with Extra-Traffic), 0x08 (1+1 Unidirectional Protection), 0x10 (1+1 Bidirectional Protection), or 0x20 (Shared Mesh Protection). The N bit MUST be set to 0 in any other case. If 0x20 (SMP), the N bit MUST be set to 1.

Operational (O): 1 bit

When set to 1, this bit indicates that the protecting LSP is carrying 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 0x04 (1:N Protection with Extra-Traffic), 0x08 (1+1 Unidirectional Protection), 0x10 (1+1 Bidirectional Protection), or 0x20 (Shared Mesh Protection). The O bit MUST be set to 0 in any other case.

6.3. Preemption Priority

[RFC4872] reserved a 32-bit field in the PROTECTION object header. Subsequently, [RFC4873] allocated several fields from that field, and left the remainder of the bits reserved. This specification further allocates the preemption priority field from those formerly-reserved bits. The 32-bit field in the PROTECTION object defined in [RFC4873] are updated as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|I|R|   Reserved    | Seg.Flags |   Reserved    | Preempt Prio  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Preemption Priority (Preempt Prio): 8 bit

This field indicates the SMP preemption priority of a protecting LSP, when the LSP Protection Type field indicates "Shared Mesh Protection". The SMP preemption priority value is configured at the end nodes of the protecting LSP by a network operator. A lower value has a higher priority. The decision of how many priority levels to be operated in an SMP network is a network operator's choice.

See [RFC4873] for the definition of other fields.

7. IANA Considerations

IANA maintains a registry called "Resource Reservation Protocol (RSVP) Parameters" with a subregistry called "Error Codes and Globally-Defined Error Value Sub-Codes". Within this subregistry there is a definition of the "Notify Error" error code (25). The definition lists a number of error value sub-codes that may be used with this error code. IANA is requested to allocate further error value sub-codes for use with this error code as described in this document.

Value	Description	Reference
TBA1	Shared resources unavailable	(this document)
TBA2	Shared resources available	(this document)

8. Security Considerations

Since this document makes use of the exchange of RSVP messages including a Notify message, the security threats discussed in [RFC4872] also apply to this document.

Additionally, it may be possible to cause disruption to traffic on one protecting LSP by targeting a link used by the primary LSP of another, higher priority LSP somewhere completely different in the network. For example, in Figure 1, assume that the preemption priority of LSP [A,E,F,G,D] is higher than that of LSP [H,E,F,G,K] and the protecting LSP [H,E,F,G,K] is being used to transport traffic. If link B-C is attacked, traffic on LSP [H,E,F,G,K] can be disrupted. For this reason, it is important not only to use security mechanisms as discussed in [RFC4872] but also to acknowledge that detailed knowledge of a network's topology, including routes and priorities of LSPs, can help an attacker better target or improve the efficacy of an attack.

9. Acknowledgements

The authors would like to thank Adrian Farrel, Vishnu Pavan Beeram, Tom Petch, Ines Robles, John Scudder, Dale Worley, Dan Romascanu, Eric Vyncke, Roman Danyliw, Paul Wouters, Lars Eggert, Francesca Palombini, and Robert Wilton for their valuable comments and suggestions on this document.

10. Contributor

The following person contributed significantly to the content of this document and should be considered as a co-author.

Yuji Tochio
Fujitsu
Email: tochio@fujitsu.com

11. References

11.1. Normative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC3473] Berger, L., Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, DOI 10.17487/RFC3473, January 2003, <https://www.rfc-editor.org/info/rfc3473>.

[RFC4426] Lang, J., Ed., Rajagopalan, B., Ed., and D. Papadimitriou, Ed., "Generalized Multi-Protocol Label Switching (GMPLS) Recovery Functional Specification", RFC 4426, DOI 10.17487/RFC4426, March 2006, <https://www.rfc-editor.org/info/rfc4426>.

[RFC4872] Lang, J., 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, DOI 10.17487/RFC4872, May 2007, <https://www.rfc-editor.org/info/rfc4872>.

[RFC4873] Berger, L., Bryskin, I., Papadimitriou, D., and A. Farrel, "GMPLS Segment Recovery", RFC 4873, DOI 10.17487/RFC4873, May 2007, <https://www.rfc-editor.org/info/rfc4873>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

11.2. Informative References

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

[I-D.ietf-teas-yang-te] Saad, T., Gandhi, R., Liu, X., Beeram, V. P., Bryskin, I., and O. G. D. Dios, "A YANG Data Model for Traffic Engineering Tunnels, Label Switched Paths and Interfaces", draft-ietf-teas-yang-te-29 (work in progress), February 2022.

[RFC6372] Sprecher, N., Ed. and A. Farrel, Ed., "MPLS Transport Profile (MPLS-TP) Survivability Framework", RFC 6372, DOI 10.17487/RFC6372, September 2011, <https://www.rfc-editor.org/info/rfc6372>.

[RFC7412] Weingarten, Y., Aldrin, S., Pan, P., Ryoo, J., and G. Mirsky, "Requirements for MPLS Transport Profile (MPLS-TP) Shared Mesh Protection", RFC 7412, DOI 10.17487/RFC7412, December 2014, <https://www.rfc-editor.org/info/rfc7412>.

[RFC8776] Saad, T., Gandhi, R., Liu, X., Beeram, V., and I. Bryskin, "Common YANG Data Types for Traffic Engineering", RFC 8776, DOI 10.17487/RFC8776, June 2020, <https://www.rfc-editor.org/info/rfc8776>.

Authors' Addresses

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

Email: hejia@huawei.com

Italo Busi
Huawei Technologies

Email: italo.busi@huawei.com

Jeong-dong Ryoo
ETRI
218 Gajeongno
Yuseong-gu, Daejeon 34129
South Korea

Phone: +82-42-860-5384
Email: ryoo@etri.re.kr

Bin Yeong Yoon
ETRI

Email: byyun@etri.re.kr

Peter Park
KT

Email: peter.park@kt.com