TEAS Working Group
Internet Draft
Intended status: Standards Track

Expires: September 2020

Yi Lin
Huawei Technologies
Bin Yeong Yoon
ETRI

March 9, 2020

RSVP-TE Extensions in Support of Proactive Protection
draft-lin-teas-gmpls-proactive-protection-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes protocol-specific procedures and extensions for Generalized Multi-Protocol Label Switching (GMPLS) Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE) signaling to support Label Switched Path (LSP) Proactive Protection, which create the protecting LSP after a failure is predicted and before it becomes a real failure.

Table of Contents

1. Introduction

[RFC4872] and [RFC4873] describe protocol-specific procedures and extensions for GMPLS RSVP-TE signaling to support end-to-end LSP

recovery (including protection and restoration) and segment LSP recovery, respectively.

Traditional protection solution (e.g., 1+1 or 1:1 protection) could have very fast protection switch after failure happens, but takes twice of resource in the network during the whole lifetime of the LSP. On the other hand, the traditional restoration solution has much higher resource use, but the recovery of the LSP is much slower, due to the additional signaling time to create the restoration LSP.

In order to reduce the recovery resource while keeping the very fast protection switch, an approach is to use the failure prediction technologies and to create 1+1 or 1:1 protection only when a potential failure is predicted. This approach refers to "Proactive Protection" in this document.

This document extends the RSVP-TE protocol to support the control of the Proactive Protection.

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.

3. Overview of Predicted Failure and Related Recovery Methods

3.1. Predicted Failure

In most cases, there will be some indications before a physical failure happens in a network. For example, abnormal fluctuation of noise of a lightpath, BER (Bit Error Rate) (before error correction) rising, temperature rising of a transponder.

Therefore, by monitoring on certain physical parameters and

analyzing the change tendency using, for example, Machine Learning (ML) or other technologies, a node is possible to predict whether failure will happen in an upcoming period of time.

Note that a predicted failure is different from a Signal Degrade in that:

- When Signal Degrade happens to a connection, the connection is still available but the quality of the signal carried by this

connection has declined and is lower than the predetermined threshold. For example, the BER of a connection rises and is out of tolerance.

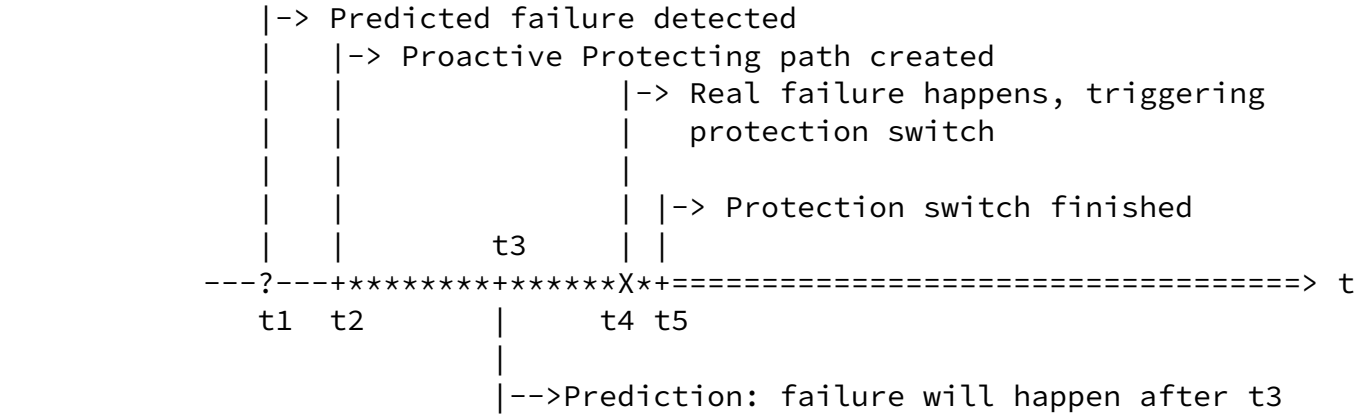
- When a predicted failure of a connection is inferred, no failure nor degradation happens at present, but there is a trend that after a period of time, failure will probably happen, which will cause Signal Fail or Signal Degrade.

The methods to predict failures are outside the scope of this document.

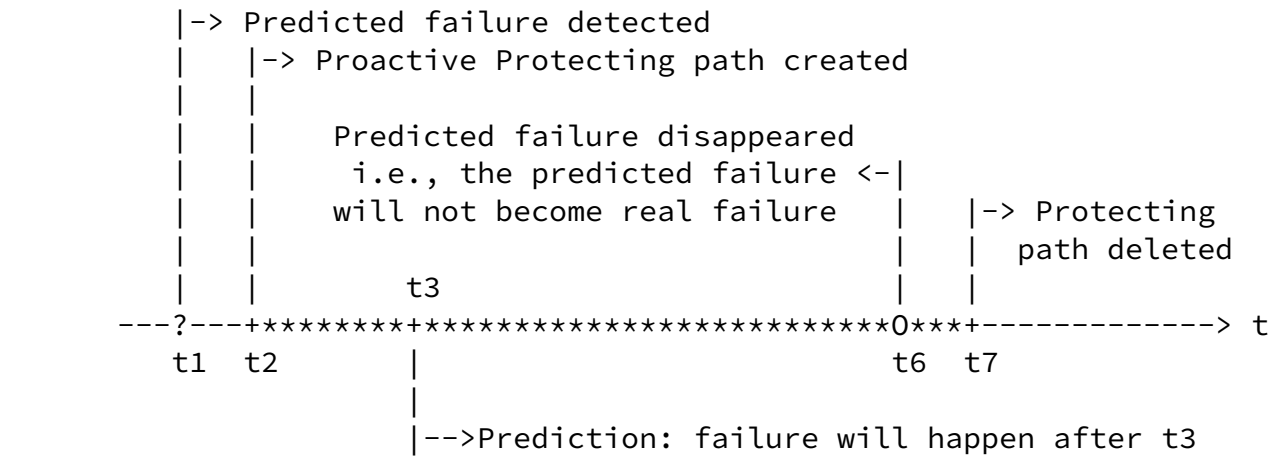
3.2. Proactive Protection

The "Proactive Protection" refers to an LSP protection approach which create the protecting LSP after a failure is predicted and before it becomes a real failure. Both end-to-end protection (defined in [RFC4872] and segment protection (defined in [RFC4873]) are applicable for the Proactive Protection.

The main procedure of Proactive Protection is shown in Figure 1:



Case 1: Predicted failure happens as predicted



Case 2: Predicted failure disappeared and will not happen

?: Predicted failure
X: Real failure happen
O: Predicted failure disappeared
----: No protecting path
****: protecting path created, traffic carried by protected path
====: protecting path created, traffic carried by protecting path

Figure 1: Overview of Proactive Protection

- t1: The protection source node of an LSP is notified that a failure will probably happen after t3, so it starts to create 1+1 or 1:1 protection of the connection. Here the protection source node can be the source node of the LSP (for end-to-end protection case), or a branch node located between the source node and the

predicted failure point of the LSP (for segment protection case).

- t2: The 1+1 or 1:1 protecting path is created between the protection source node and the protection destination node. Here the protection destination node can be the destination node of the LSP (for end-to-end protection case), or a merge node located between the predicted failure point and the destination node of the LSP (for segment protection case).

  Note that at t2, since there is no real failure or signal degradation happened, the protection switch will not be triggered, and the traffic still remains in the protected path.

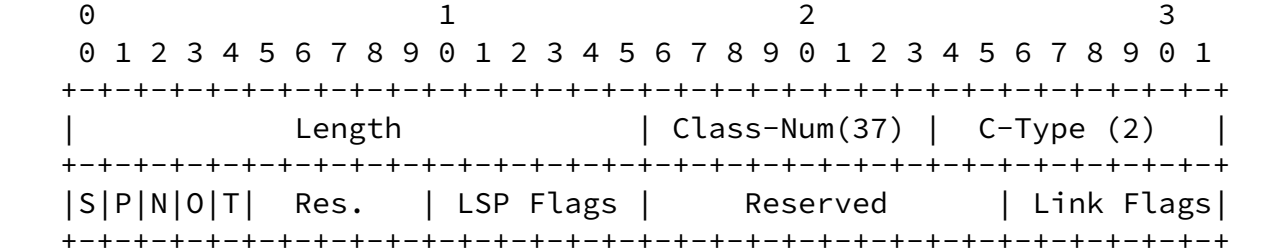
- t4: If real failure happens as predicted, the 1+1 or 1:1 protection switch will be triggered.

- t5: Protection switch finished and the traffic is now switched to the protecting path.

- The intermediate node, which detected the predicted failure, will continue to monitor the change tendency of the related physical parameters to make further prediction before the predicted failure becomes a real failure. If, at t6, the intermediate node finds that the change tendency causing the predicted failure disappeared and the status is stable enough, i.e., the intermediate node confirms that the predicted failure will not become real failure, it MAY send another notification to clear the predicted failure. In this case, the protection source node MAY decide to tear down the protecting path at t7 after t6, in order to save the network resource.

4. Modified PROTECTION Object Format

This document modifies the PROTECTION object (C-Type=2) by adding two new bits T and A in reserved fields, as shown in Figure 2 below:



```
|I|R|A|  Reserved   | Seg.Flags |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: The modified PROTECTION object (C-Type=2)

- T (Triggered End-to-end Proactive Protection): 1 bit, when set (1), it indicates that the end-to-end Proactive Protection are required.

  Note that if T bit is set (1), the LSP Flags SHOULD be one of:
  0x04 1:N Protection with Extra-Traffic
  0x08 1+1 Unidirectional Protection
  0x10 1+1 Bidirectional Protection

- A (proActive Segment Protection): 1 bit, when set (1), it indicates that the Proactive Segment Protection are required.

  Note that If A bit is set (1), the Seg. Flags SHOULD be one of:
  0x04 1:N Protection with Extra-Traffic
  0x08 1+1 Unidirectional Protection
  0x10 1+1 Bidirectional Protection

See [RFC4872] and [RFC4873] for the definition of other fields.

5. Extension to ERROR_SPEC Object

5.1. New Error Code / Sub-code

Two new Error Sub-codes under Error Code "25 - Notify Error" are defined in this document, which are used to notify the event of a predicted failure and the event of disappearance of the previous predicted failure:

Error Code = 25: "Notify Error" (see [RFC3209])

Error Sub-code = TBA1: "Notify Error/LSP Local Predicted Failure"

Error Sub-code = TBA2: "Notify Error/LSP Local Predicted Failure disappeared"

5.2. New TLVs in ERROR_SPEC Object

When predicting a failure, a certain time before which the failure

may happen may also be predicted. This time information is useful for the source node to know how long it should wait for the predicted failure to become a real failure, and to decide when it's safe to tear down the protecting LSP if the predicted failure didn't happen.

A new TLV in IPv4/IPv6 IF_ID ERROR_SPEC Object is defined in this document, which is used to indicate the time before which the predicted failure will probably become real failure. The format of this new TLV is shown in Figure 3 below:

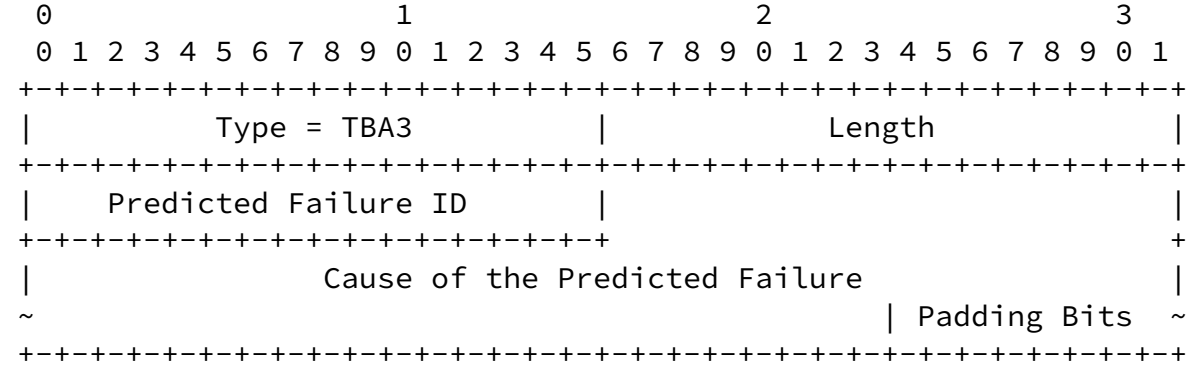


Figure 3: New TLV (type=TBA3) in ERROR_SPEC Object

- Type: TBA3

- Length: variable and MUST be equal or greater than 8, the total length of the whole TLV in Byte, including the Type and Length

fields.

- Predicted Failure ID: an ID to identify the predicted failure, which is unique within the scope of the node predicting the failure.

- Cause of the Predicted Failure: the cause of the predicted failure in text format. It SHOULD be a string of printable ASCII characters, without a NULL terminator. This field is optional. If there is no information for this field, the padding bits (16 bits) will be filled immediately after the "Predicted Failure ID" field.

- Padding Bits: Added after the "Cause of the Predicted Failure" field to make the whole TLV a multiple of four bytes if necessary.

Padding bits MUST be set to 0 and MUST be ignored on receipt.

Another new TLV in IPv4/IPv6 IF_ID ERROR_SPEC Object is defined in this document, which is used to indicate the disappearance of the previous predicted failure. The format of this new TLV is shown in Figure 4 below:

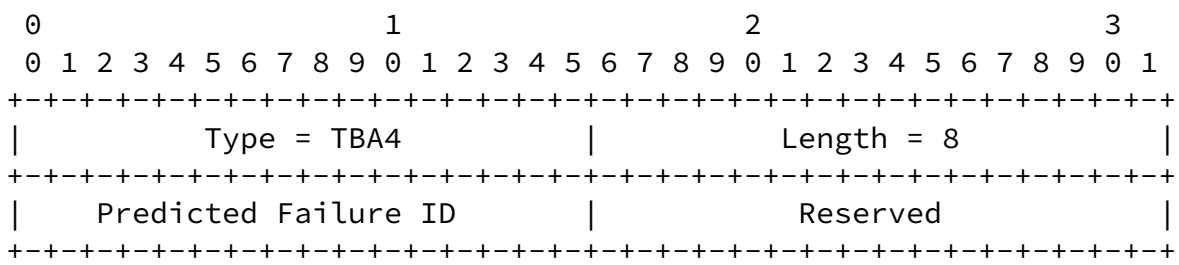


Figure 4: New TLV (type=TBA4) in ERROR_SPEC Object

- Type: TBA4

- Length: 8.

- Predicted Failure ID: the ID of the previous predicted failure which is now disappeared.

- Reserved: MUST be zero.

6. End-to-end Proactive Protection

6.1. Creation of the Protected LSP

To create an LSP with recovery type of "End-to-end Proactive Protection", the source node of the LSP generates a Path message with a PROTECTION object included. The T bit in the PROTECTION

object MUST be set to 1 (End-to-end Proactive Protection), so that all other nodes along the LSP can start the failure prediction function on related links/nodes.

Note that the N bit in the PROTECTION object is used to indicate whether the control plane message exchange is only used for notification or for protection-switching purpose after real failure happens, see [RFC4872]. In other words, the N bit have nothing to do with the notification of a predicted failure before real failure

happens.

To allow the notification of predicted failure event to the source node by the Notify message, the NOTIFY REQUEST object MUST also be included in the Path message (see [RFC3473]), where the "Notify Node Address" SHOULD be the address of the source node of the LSP.

6.2. Notification of Predicted Failure Event

When an intermediate node on an LSP infers that a failure will happen and will affect the LSP, a Notify message will be sent to the source node of the LSP, to inform such predicted failure event. A new error code/sub-code "Notify Error/LSP Local Predicted Failure" is used in the ERROR_SPEC object or IF_ID_ERROR_SPEC object in the Notify message.

The Notify message SHOULD include a TLV (type = TBA3) in the IPv4 or IPv6 IF_ID_ERROR_SPEC object, to indicate the ID and the cause of the predicted failure.

On receiving the Notify message with error code/sub-code "Notify Error/LSP Local Predicted Failure", the source node of the LSP SHOULD trigger the procedure to create the protecting LSP, according to the protection type indicated in the "LSP Flags" field of the PROTECTION object in the Path message for the protected LSP. The procedures of creating the protecting LSP and the protection switching after real failure happens are described in [RFC4872], except that the T bit in the PROTECTION object of this new Path message MUST set to 1.

The source node SHOULD also store the ID of the predicted failure and create the association between this ID and the created protecting LSP locally.

6.3. Tearing Down of the Protecting LSP

After sending Notify message to the source node for notifying the predicted failure, the intermediate node will continue to monitor

the change tendency of the related physical parameters to make further prediction. If it confirms that the change tendency causing the predicted failure disappeared and the predicted failure will not become real failure, it MAY send another Notify message with error

code/sub-code "Notify Error/LSP Local Predicted Failure disappeared", to clear the previous predicted failure.

The Notify message SHOULD include a TLV (type = TBA4) in the IPv4 or IPv6 IF_ID_ERROR_SPEC object, to indicate the ID of the previous predicted failure which is now disappeared. The value of this ID MUST equal to the one in the previous Notify message sent to the source node to notify this predicted failure.

On receiving the Notify message with error code/sub-code "Notify Error/LSP Local Predicted Failure disappeared", the source node of the LSP SHOULD check if it has received the Notify message from the same intermediate node before, with the same ID of the predicted failure:

- If yes, and if the protecting LSP has already been created, the source node MAY trigger the procedure to tear down the protecting LSP. See [RFC4872] about the process of tearing down a protecting LSP. Note that the source node MAY wait for a certain period of time before tearing down the protecting LSP, according to local policy. Implementations SHOULD allow this policy to be configured to provide a default across all LSPs on a node, but SHOULD also allow it to be configured per LSP.

- If no, this Notify message can be simply ignored.

7. Proactive Segment Protection

7.1. Creation of the Protected LSP

To create an LSP with recovery type of "Proactive Segment Protection", the source node of the LSP generates a Path message, where:

- A PROTECTION object is included, where the A bit MUST be set to 1 (Proactive Segment Protection), so that all nodes along the protected LSP can start the failure prediction function on related links/nodes if supported. The "Seg. Flags" are used to indicate the protection type of the Proactive Segment Protection.

- One or more SERO objects MAY included (i.e., explicit Proactive Segment Protection), indicating the branch node and the merge node of each segment recovery LSP. If no SERO object is included, it

indicates that the dynamic Proactive Segment Protection method is used.

- A NOTIFY REQUEST object is included, where the Notify Node Address" SHOULD be the address of the source node of the LSP.

For explicit Proactive Segment Protection, when a branch node receives a Path message with A bit set to 1 in the PROTECTION object, the branch node follows [RFC4873] to process the Path message, except that the Path message for the recovery LSP will not be generated and be sent at this stage. Also, one more NOTIFY REQUEST object SHOULD be added to the Path message of the protected LSP, which carries the address of this branch node.

For dynamic Proactive Segment Protection, when an intermediate node receives a Path message with A bit set to 1 in the PROTECTION object, the node will determine if it has the ability to be a branch node, as described in Section 6.2 of [RFC4873]. If yes, it follows the same procedure as what a branch node does in the case of explicit Proactive Segment Protection, as described above. If not, the node only follows the standard procedure to create the protected LSP.

7.2. Notification of Predicted Failure Event

When an intermediate node between a pair of branch and merge nodes on an LSP infers that a failure will happen and will affect the LSP, a Notify message will be sent to the nearest branch node on the upstream direction of the LSP, to inform such predicted failure event. The error code/sub-code "Notify Error/LSP Local Predicted Failure" is used in the ERROR_SPEC object or IF_ID_ERROR_SPEC object in the Notify message.

Similar to End-to-end Proactive Protection, the Notify message SHOULD include a TLV (type = TBA3) in the IPv4 or IPv6 IF_ID_ERROR_SPEC object, to indicate the ID and the cause of the predicted failure.

On receiving the Notify message with error code/sub-code "Notify Error/LSP Local Predicted Failure", the branch node on the protected LSP SHOULD generate a new Path message, and send this new Path message along the segment recovery LSP between the branch and the merge nodes. The procedures of generating new Path message and creating the segment recovery LSP are the same as what is described in [RFC4873], except that the A bit in the PROTECTION object of this new Path message MUST set to 1.

The branch node SHOULD also store the ID of the predicted failure and create the association between this ID and the created segment recovery LSP locally.

7.3. Tearing Down of the Segment Recovery LSP

After sending Notify message to the branch node for notifying the predicted failure, the intermediate node will continue to monitor the change tendency of the related physical parameters to make further prediction. If it confirms that the change tendency causing the predicted failure disappeared and the predicted failure will not become real failure, it MAY send another Notify message with error code/sub-code "Notify Error/LSP Local Predicted Failure disappeared", to clear the previous predicted failure.

The Notify message SHOULD include a TLV (type = TBA4) in the IPv4 or IPv6 IF_ID_ERROR_SPEC object, to indicate the ID of the previous predicted failure which is now disappeared. The value of this ID MUST equal to the one in the previous Notify message sent to the branch node to notify this predicted failure.

On receiving the Notify message with error code/sub-code "Notify Error/LSP Local Predicted Failure disappeared", the branch node of the LSP SHOULD check if it has received the Notify message from the same intermediate node before, with the same ID of the predicted failure.

- If yes, and if the segment recovery LSP has already been created, the branch node MAY trigger the procedure to tear down the segment recovery LSP. See [RFC4873] about the process of tearing down a segment recovery LSP. Note that the branch node MAY wait for a certain period of time before tearing down the segment recovery LSP, according to local policy. Implementations SHOULD allow this policy to be configured to provide a default across all LSPs on a node, but SHOULD also allow it to be configured per LSP.

- If no, this Notify message can be simply ignored.

7.4. Priority and Resource Pre-emption

It's possible that after recovery LSP is created and before the predicted failure becomes a real failure, another real failure happens on the LSP outside the protected segment. In this case, the source node (or an intermediate node in the upstream direction of the real failure) may start a restoration procedure to recover the LSP. For the same protected LSP, since recovering from a real

failure always has higher priority than protecting against a

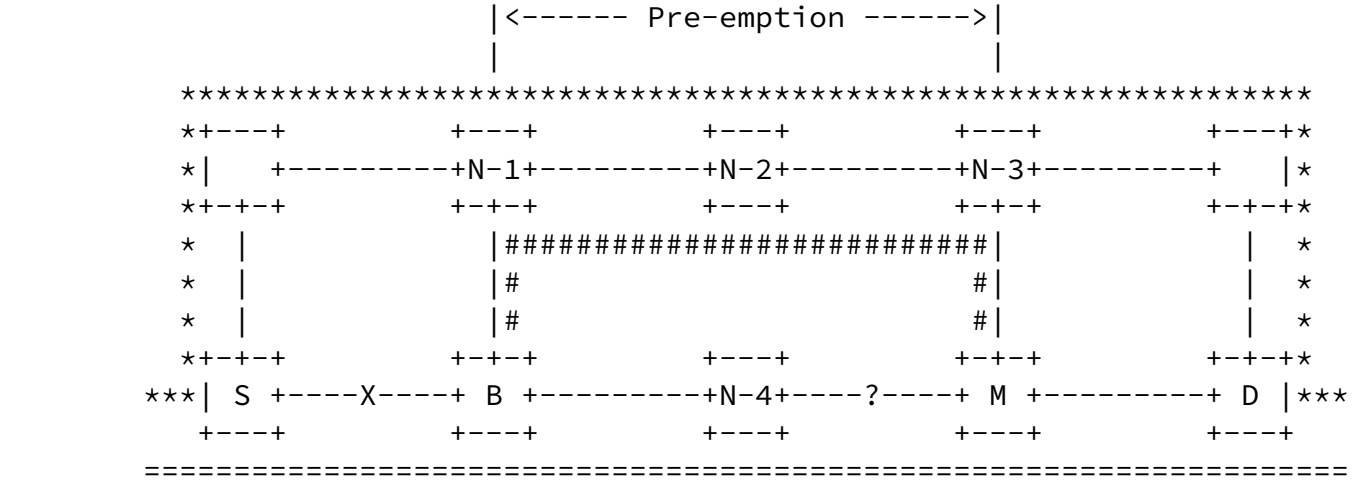
predicted failure which still hasn't happened, the restoration LSP can pre-empt the resource of the segment recovery LSP.

As shown in Figure 5, assume that node B (branch node) was notified of a predicted failure event between N-4 and M (merge node), and has created the segment recovery LSP along B, N-1, N-2, N-3 and M. If another failure between S (source node) and B happens before the predicted failure becomes a real failure, node S will try to create the restoration LSP. Since that resource is limited, the restoration LSP can pre-empt the resource of the segment recovery LSP between N-1 and N-3.

The nodes along the segment recovery LSP has enough information to determine whether pre-emption is allowed. This is because these nodes know that:

- The current segment recovery LSP is used for Proactive Segment Protection through the A bit in the PROTECTION object;

- The segment recovery LSP and the restoration LSP are protecting the same LSP through the association relationship.



S: Source node D: Destination node
B: Branch node M: Merge node
X: Real failure ?: Predicted failure (haven't happened yet)

=====: Protected LSP

#####: Segment Recovery LSP
*****: Restoration LSP

Figure 5: Resource pre-emption by restoration LSP

8. Consideration of Backward Compatibility

TBD.

[Editor's note]: will add some description about interwork with legacy nodes which do not support the function of failure prediction and reporting.

9. Security Considerations

TBD.

10. IANA Considerations

IANA assigns values to RSVP protocol parameters. Within the current document, two new Error code/sub-code values are defined:

Error Code = 25: "Notify Error" (see [RFC3209])

- "Notify Error/LSP Local Predicted Failure" (TBA1)
- "Notify Error/LSP Local Predicted Failure disappeared" (TBA2)

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, 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., Ed., "Generalized Multi-Protocol Label

Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[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, May 2007.

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

11.2. Informative References

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

12. Authors' Addresses

Yi Lin
Huawei Technologies
H1, Huawei Xiliu Beipo Village, Songshan Lake
Dongguan
Guangdong, 523808 China
Email: yi.lin@huawei.com

Bin Yeong Yoon
ETRI
Email: byyun@etri.re.kr