MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 22, 2014

J. Ryoo
ETRI
H. van Helvoort
Huawei Technologies
A. D'Alessandro
Telecom Italia
August 21, 2013

Priority Modification for the PSC Linear Protection
draft-rhd-mpls-tp-psc-priority-01.txt

Abstract

This document contains the modifications to the priorities of inputs in [RFC6378], "MPLS Transport Profile (MPLS-TP) Linear Protection" in an effort to satisfy the ITU-T's protection switching requirements and correcting the problems that have been identified.

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 February 22, 2014.

Table of Contents

1. Introduction

This document contains the modifications to the priorities of inputs in [RFC6378], "MPLS Transport Profile (MPLS-TP) Linear Protection" in an effort to satisfy the ITU-T's protection switching requirements and correcting the problems that have been identified.

In this document, the priorities of FS and SF-P are swapped and the priority of Clear SF is raised. In addition to the prioririty modification, this document introduces the use of a Freeze command in an Appendix. The reasons for these changes are explained in the following sub-sections from technical and network operational aspects.

1.1. Motivations for swapping priorities of FS and SF-P

Defining the priority of FS higher than that of SF-P can result in a situation where the protected traffic is taken out-of-service. Setting the priority of any input that is supposed to be signaled to the other end to be higher than that of SF-P can result in unpredictable protection switching state, when the protection path

has failed and consequently the PSC communication stopped. An example of the out-of-service scenarios is shown in Appendix A

According to Section 2.4 of [RFC5654] it MUST be possible to operate an MPLS-TP network without using a control plane. This means that external switch commands, e.g. FS, can be transferred to the far end only by using the PSC communication channel and should not rely on the presence of a control plane.

As the priority of SF-P has been higher than FS in optical transport networks and Ethernet transport networks, for network operators it is important that the MPLS-TP protection switching preserves the network operation behaviour to which network operators have become accustomed. Typically, the FS command is issued before network maintenance jobs, replacing optical cables or other network components. When an operator pulls out a cable on the protection path by mistake, the traffic should be protected and the operator expects this behaviour based on his/her experience on the traditional transport network operations.

1.2. Motivation for raising the priority of Clear SF

The priority level of Clear SF defined in [RFC6378] can cause traffic disruption when a node that has experienced local signal fails on both working and protection paths is recovering from these failures.

An exmaple of sequence diagram showing the problem with the priority level of Clear SF defined in [RFC6378] is shown in Appendix B.

1.3. Motivation for introducing Freeze command

With the priority swapping between FS and SF-P, the traffic is always moved back to the working path when SF-P occurs in Protecting Administrative State. In the case that network operators need an option to control their networks so that the traffic can remain on the protection path even when the PSC communication channel is broken, the Freeze command, which is a local command and not signaled to the other end, can be used. The use of the Freeze command is described in Appendix C.

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. Acronyms

This draft uses the following acronyms:

FS Forced Switch
MPLS-TP Transport Profile for MPLS
SF Signal Fail
SFc Clear Signal Fail

4. Updates to the PSC RFC

This section describes the changes required to modify the priorities of FS, SF-P and Clear SF in the PSC protocol defined in [RFC6378]

4.1. Updates to Section 4.3.2. Priority of Inputs

The list of local requests in order of priority should be modified as follows:

3 Clear Signal Fail/Degrade (OAM / control-plane / server indication)

4 Signal Fail on protection (OAM / control-plane / server indication)

5 Forced Switch (operator command)

6 Signal Fail on working (OAM / control-plane / server indication)

7 Signal Degrade on working (OAM / control-plane / server indication)

4.2. Updates to Section 4.3.3.2. Unavailable State

Remove the following bullet items and their text:

- A local Forced Switch SHALL be ignored by the PSC Control logic when in Unavailable state as a result of a (local or remote) Lockout of protection. If in Unavailable state due to an SF on protection, then the FS SHALL cause the LER to go into local Protecting administrative state and begin transmitting an FS(1,1) message. It should be noted that due to the unavailability of the protection path (i.e., due to the SF condition) that this FS may not be received by the far-end until the SF condition is cleared.

- A remote Forced Switch message SHALL be ignored by the PSC Control logic when in Unavailable state as a result of a (local or remote) Lockout of protection. If in Unavailable state due to a local or remote SF on protection, then the FS SHALL cause the LER to go

into remote Protecting administrative state; if in Unavailable state due to local SF, begin transmitting an SF(0,1) message.

4.3. Updates to Section 4.3.3.3. Protecting Administrative State

Remove the following text in the first paragraph:

> The difference between a local FS and local MS affects what local indicators may be received -- the Local Request logic will block any local SF when under the influence of a local FS, whereas the SF would override a local MS.

Replace the following bullet item text:

- A local Signal Fail indication on the protection path SHALL cause the LER to go into local Unavailable state and begin transmission of an SF(0,0) message, if the current state is due to a (local or remote) Manual Switch operator command. If the LER is in (local or remote) Protecting administrative state due to an FS situation, then the SF on protection SHALL be ignored.

With:

- A local Signal Fail indication on the protection path SHALL cause the LER to go into local Unavailable state and begin transmission of an SF(0,0) message.

Replace the following bullet item text:

- A remote Signal Fail message indicating a failure on the protection path SHALL cause the LER to go into remote Unavailable state and begin transmitting an NR(0,0) message, if the Protecting administrative state is due to a Manual Switch command. It should be noted that this automatically cancels the current Manual Switch command and data traffic is reverted to the working path.

With:

- A remote Signal Fail message indicating a failure on the protection path SHALL cause the LER to go into remote Unavailable state and begin transmitting an NR(0,0) message. It should be noted that this automatically cancels the current Forced Switch or Manual Switch command and data traffic is reverted to the working path.

4.4. Updates to Appendix A. PSC State Machine Tables

Modify the state machine as follows (only modified cells are shown):

Part 1: Local input state machine

	OC	LO	SF-P	FS	SF-W	SFc	MS	WTRExp
N								
UA:LO:L								
UA:P:L				i				
UA:LO:R								
UA:P:R				i				
PF:W:L								
PF:W:R								
PA:F:L			UA:P:L					
PA:M:L								
PA:F:R			UA:P:L					
PA:M:R								
WTR								
DNR								

Part 2: Remote messages state machine

	LO	SF-P	FS	SF-W	MS	WTR	DNR	NR
N								
UA:LO:L								
UA:P:L			i					
UA:LO:R								
UA:P:R			i					
PF:W:L								
PF:W:R								
PA:F:L		UA:P:R						
PA:M:L								
PA:F:R		UA:P:R						
PA:M:R								
WTR								
DNR								

Remove the following item in the footnotes for the table:

[19] Transition to PA:F:R and send SF (0,1).

5. Security considerations

No specific security issue is raised in addition to those ones already documented in [RFC6378]

6. IANA considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

7. Acknowledgements

8. Normative References

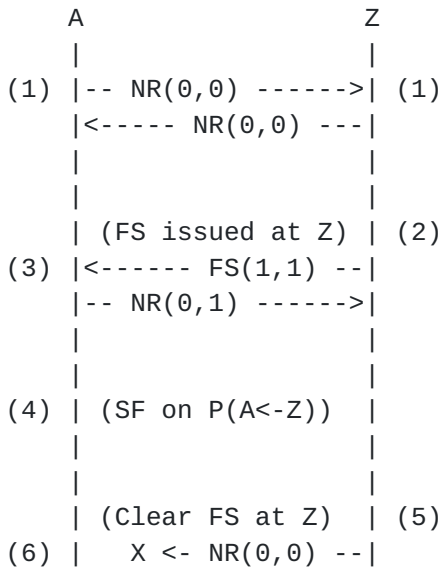
[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[RFC6378] Weingarten, Y., Bryant, S., Osborne, E., Sprecher, N., and A. Fulignoli, "MPLS Transport Profile (MPLS-TP) Linear Protection", RFC 6378, October 2011.

Appendix A. An exmaple of out-of-service scenarios

The sequence diagram shown is an example of the out-of-service scenerios based on the priority level defined in [RFC6378]. The first PSC message which differs from the previous PSC message is shown.



```
                |                 |
                |                 |
```

(1) Each end is in Normal state, and transmits NR (0,0) messages.

(2) When a Forced Switch command is issued at node Z, node Z goes into local Protecting Administrative state (PA:F:L) and begins transmission of an FS (1,1) messages.

(3) A remote Forced Switch message causes node A to go into remote Protecting Administrative state (PA:F:R), and node A begins transmitting NR (0,1) messages.

(4) When node A detects a unidirectional Signal Fail on the protection path, node A keeps sending NR (0,1) message because SF-P is ignored under the state PA:F:R.

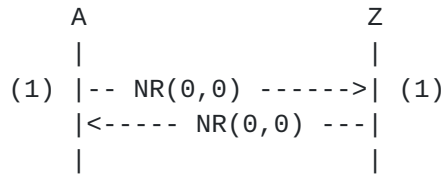
(5) When a Clear command is issued at node Z, node Z goes into Normal state and begins transmission of NR (0,0) messages.

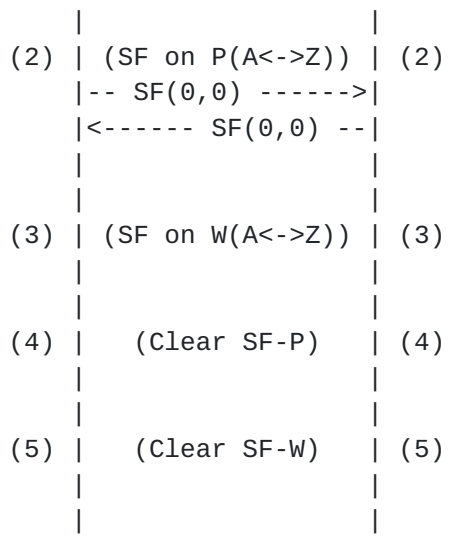
(6) But node A cannot receive PSC message because of local unidirectional Signal Fail indication on the protection path. Because no valid PSC message is received, over a period of several continual messages intervals, the last valid received message remains applicable and the node A continue to transmit an NR (0,1) message in the state of PA:F:R.

Now, there exists a mismatch between the bridge/selector positions of node A (transmitting an NR (0,1)) and node Z (transmitting an NR (0,0)). It results in out-of-service even when there is neither signal fail on working path nor FS.

Appendix B. An exmaple of sequence diagram showing the problem with the priority level of Clear SF

An exmaple of sequence diagram showing the problem with the priority level of Clear SF defined in [RFC6378] is given below. The following sequence diagram is depicted for the case of bidirectional signal fails. However, other cases with unidirectional signal fails can result in the same problem. The first PSC message which differs from the previous PSC message is shown.





(1) Each end is in Normal state, and transmits NR (0,0) messages.

(2) When signal fail on protection (SF-P) occurs, each node enters into [UA:P:L] state and transmits SF (0,0) messages. Traffic remains on working path.

(3) When signal fail on working (SF-W) occurs, each node remains in [UA:P:L] state as SF-W has a lower priority than SF-P. Traffic is still on the working path. Traffic cannot be delivered as both working and protection paths are experiencing signal fails.

(4) When the signal fail on protection is cleared, local "Clear SF-P" request cannot be presented to the PSC control logic, which takes the highest priority local request and runs PSC state machine, as the priority of "Clear SF-P" is lower than that of SF-W. Consequently, there is no change in state, and the selector and/or bridge keep pointing at the working path, which has signal fail condition.

Now, traffic cannot be delivered while the protection path is recovered and available. It should be noted that the same problem will occur in the case that the sequence of SF-P and SF-W events is changed.

If we further continue with this sequence to see what will happen after SF-W is cleared,

(5) When the signal fail on working is cleared, local "Clear SF-W" request can be passed to the PSC control logic (state machine) as there is no higher priority local request, but this will be ignored in the PSC control logic according to the state transition definition in [RFC6378]. There will be no change in state or protocol message transmitted.

As the signal fail on working is now cleared and the selector and/or bridge are still pointing at the working path, traffic delivery is resumed. However, each node is in [UA:P:L] state and transmitting SF(0,0) message, while there exists no outstanding request for protection switching. Moreover, any future legitimate protection switching requests, such as SF-W, will be rejected as each node thinks the protection path is unavailable.

Appendix C. Freeze Command

The "Freeze" command applies only to the near end (local node) of the protection group and is not signaled to the far end. This command freezes the state of the protection group. Until the Freeze is cleared, additional near end commands are rejected and condition changes and received PSC information are ignored.

"Clear Freeze" command clears the local freeze. When the Freeze command is cleared, the state of the protection group is recomputed based on the persistent condition of the local triggers.

Because the freeze is local, if the freeze is issued at one end only, a failure of protocol can occur as the other end is open to accept any operator command or a fault condition.

Authors' Addresses

Jeong-dong Ryoo
ETRI
218 Gajeongno
Yuseong-gu, Daejeon 305-700
South Korea

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

Huub van Helvoort
Huawei Technologies
Karspeldreef 4,
Amsterdam 1101 CJ
the Netherlands

Phone: +31 20 4300936
Email: huub.van.helvoort@huawei.com

Alessandro D'Alessandro
Telecom Italia
via Reiss Romoli, 274
Torino 10141
Italy

Phone: +39 011 2285887
Email: alessandro.dalessandro@telecomitalia.it