MPLS Working Group
Internet Draft
Intended status: Standards Track

H. Zhang
J. He
Huawei

H. Li
China Mobile

March 8, 2010

Expires: September 2010

SD-Triggered Protection Switching in MPLS-TP
draft-zhl-mpls-tp-sd-02.txt

Abstract

In MPLS-TP survivability framework, a fault condition includes both Signal Failure (SF) and Signal Degrade (SD) that can be used to trigger protection switching. This document describes Signal Degrade (SD) detection and the consequent protection switching mechanism.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on April 8, 2010.

Table of Contents

1. Introduction

In packet transport network, protection switching can be triggered by fault conditions and external manual commands. The fault conditions include Signal Failure (SF) and Signal Degrade (SD). SF on a transport entity can be detected by fault management OAM functions; SD on a transport entity can be detected by performance monitoring OAM functions.

The SD condition used for protection switching mostly depends on

packet loss ratio. For some services that are sensitive to time and synchronization, the SD condition may depend on packet loss ratio, packet delay and delay variation.

In MPLS-TP OAM tools, the packet loss measurement (LM) is used to measure the amount of the lost service packets and compute the loss ratio of service packet. The packet Delay Measurement (DM) is used to measure the packet delay and delay variation by sending periodic DM packets during the diagnostic interval. The LM and DM mechanisms are out of scope of this document.

The detection of SD (e.g. packet loss) must be based on service packets. But in some situation, there is no normal traffic on working/protection transport entity, which makes the detection of SD based on service packets impossible and causes switch flapping.

This document describes the mechanism for SD detection and consequent protection switching in 1:1 and 1:n protection architecture.

2. Terminology

The reader is assumed to be familiar with the terminology in MPLS-TP. The relationship between ITU-T and IETF terminologies on MPLS-TP can be found in [Rosetta stone].

MPLS-TP: MPLS Transport Profile

SF: Signal Failure

SF-W: SF for working entity

SF-P: SF for protection entity

SD: Signal Degrade

SD-W: SD for working entity

SD-P: SD for protection entity

APS: Automatic Protection Switching

OAM: Operations, Administration and Maintenance

CC/CV: Continuity Check/Connectivity Verification

LM: Loss Measurement

DM: Delay Measurement

3. SD-Triggered Protection Switching Architecture

The SD-triggered protection switching complies with general protection architecture.

In case of MPLS-TP 1+1 protection architecture, the normal traffic is permanently sent on both working and protection entities by the permanent bridge at the source. Therefore, the detection of SD or the clearing of SD on both working and protection entities can be based on the characteristics of the normal traffic.

In case of MPLS-TP 1:1 and 1:n protection architecture, the selector bridge is usually adopted at the source end. The normal traffic is transported on the working entity together with the OAM of the working entity, while on the protection entity only the OAM of the protection entity is transported alone so that it may not be possible to detect SD. If SD is detected on a working entity, protection switching is occurred, and the traffic is transported on the protection entity together with OAM. On the working entity OAM packets is transported alone, and the detected SD may be cleared even if the working entity is still degraded. This will result in another switch of traffic back to the working entity, and SD may be detected again, etc.

As mentioned above, in case of 1:1 and 1:n protection architecture, the normal traffic will be either on the working transport entity or on the protection transport entity. This makes it impossible to detect SD on the standby entity. Consequently SD will be detected only after a protection switch and flapping may happen.

4. SD-Triggered Protection Solution Analysis

In case of 1:1 and 1:n protection architecture, there are the

following solutions to implement the SD-triggered protection switching without flapping.

- The detection of SD is based on OAM packets; (Section 4.1)

- The broadcast bridge has to be applied to enable SD detection in SD-triggered protection, together with

  - the special APS request priority (Section 4.2), or

  - the extra protection switching coordination (Section 4.3).

  The broadcasting is applied only in case protection switching is active.

4.1. SD-Triggered Protection Based on OAM packets

4.1.1. Detection of SD

In case of 1:1 and 1:n protection architecture, for the transport entity on which there is no normal traffic, the detection of SD can be based on OAM packets, e.g.

- OAM packets for Test

The Test OAM packets can be used to simulate the characteristics of the normal traffic and replace the normal service. With the performance monitoring OAM packets (LM) the SD condition of the transport entity can be detected.

- OAM packets for CC/CV

The CC/CV OAM packets can be used instead of normal service in packet loss measurement. That is, the performance monitoring OAM packets (LM) will count CC/CV packets and the loss measurement is based on CC/CV packets, which will be used as the input of SD condition of the transport entity where there is no normal service.

The above-mentioned SD-triggered protection switching mechanism based on OAM packets (test or CC/CV) is general and flexible without constraint to the bridge type at source end, that may be selector bridge or broadcast bridge.

The performance measurement by Test OAM packets is accurate. But the usage of test packets on the protection entity defeats the objective of the 1:1 and 1:n architectures, which is to have the protection entity bandwidth available for best effort traffic during the time there is no fault or degradation of the working transport entity. The test packets consume now this bandwidth. For the case of the 1:1 protection, this makes the bandwidth usage of this 1:1 architecture similar to the bandwidth usage of the 1+1 architecture.

OAM packets for CC/CV are sent in fixed transmission period (3.3ms, 10ms, 1s, etc.) which doesn't exactly reflect the condition of real services. It is applicable only in places without strict requirement for SD measurement. The detection of SD by CC/CV is not recommended when the packet loss is caused by congestion.

4.1.2. APS Protocol

In APS request types, similar to the definition of SF-W (SF for working entity) and SF-P (SF for protection entity), a definition of

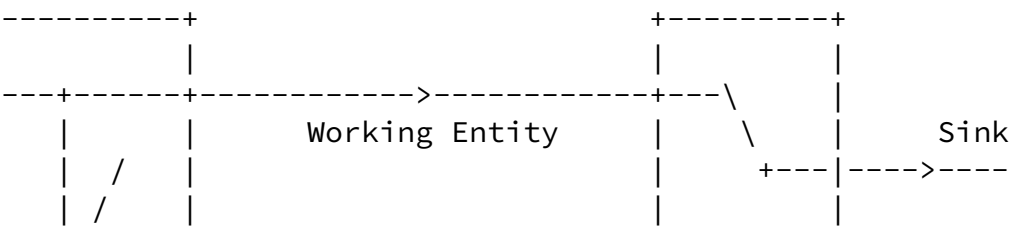
SD-W (SD for working entity) and SD-P (SD for protection entity) is required to prevent flapping.

The priority of SD-P and SD-W shall be fixed as SD-P > SD-W similar to SF-P > SF-W. In this case a protection switching based on SD detection on the working entity shall not be initiated if there exists also an SD condition on the protection transport entity.

4.2. Broadcast Bridge with Special APS Request Priority

SD-triggered protection based on normal traffic can be implemented by adopting broadcast bridge at source end with the special APS request priority.

4.2.1. Protection Switching



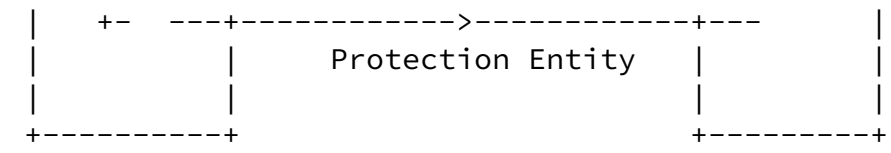


Figure 1 Normal Condition in 1:1 Protection Architecture

In the normal state, the normal traffic is sent only on the working transport entity and only the SD condition of the working transport entity can be evaluated (see Figure 1).

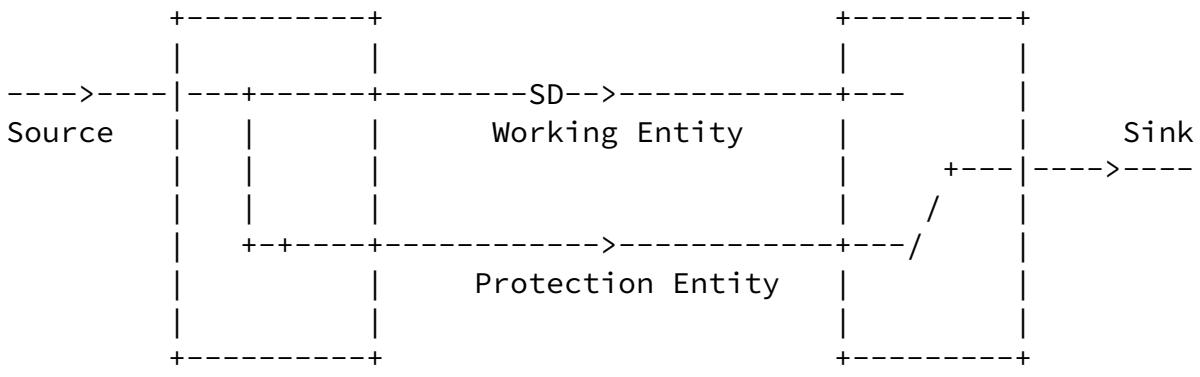


Figure 2 SD on Working Entity in 1:1 Protection Architecture

When SD is detected on the working transport entity, the sink end sends SD-W indication to the source end and the selector at the sink end switches to the protection transport entity. The broadcast bridge at the source end will then send the normal traffic on both working and protection transport entities and the performance of both working

and protection transport entities can be monitored for SD (see Figure 2).

If SD is detected on the protection transport entity as well, i.e. SD-W and SD-P exist simultaneously, normal traffic will still be selected at the sink from the protection transport entity to avoid flapping between protection and working states.

4.2.2. APS Protocol

In this case the priority of SD-W and SD-P in the APS protocol is fixed as SD-W > SD-P to avoid flapping between protection entity and working entity.

4.3. Broadcast Bridge with Extra Protection Switching Coordination

SD-triggered protection based on normal traffic can be implemented by adopting broadcast bridge at source end with the extra protection switching coordination.

The SD-W based protection switch action described in section 4.2.1 assumes that the probability of SD condition occurring on both working entity and protection entity at the same time is very small. When this assumption is not considered to be reasonable, the operation of the selector may be modified as described hereafter.

4.3.1. Protection Switching

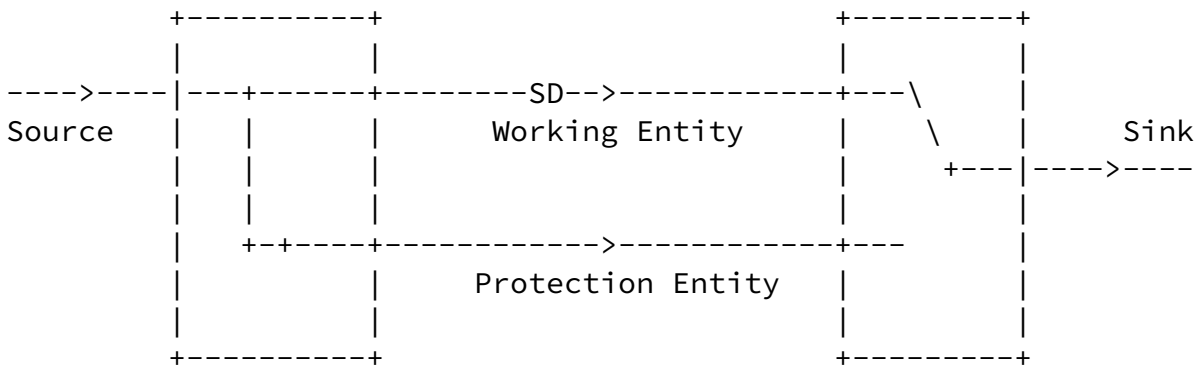


Figure 3 SD on Working Entity in 1:1 Protection Architecture

When the sink end detects an SD condition, it does not switch to the protection entity immediately. Instead, the broadcast bridge at the source end will first send the normal traffic on both working and protection transport entity after receiving SD-W indication sent by the sink end (see Figure 3). Then sink end is able to detect the SD condition of working and protection transport entity.

If SD is detected on the protection transport entity as well, the normal traffic remains broadcasted to both working and protection transport entities and is selected from the working transport entity; if no SD is detected on the protection transport entity the normal traffic is selected from the protection entity.

4.3.2. APS Protocol

The SD priority is the same as described in 4.1.2: SD-P > SD-W.

4.4. Analysis

In section 4.1, 4.2 and 4.3, the different mechanisms for detecting SD are described. The mechanism described in 4.2 is preferred because of its simplicity, accuracy and flexibility.

5. Security Considerations

To be added in a future version of the document.

6. IANA Considerations

IANA is requested to allocate two further APS request codes as follows:

xx Signal Degradation for Working entity (SD-W);

yy Signal Degradation for Protection entity (SD-P).

7. Acknowledgments

The authors would like to thank Huub van Helvoort for his input to and review of the current document.

8. References

8.1. Normative References

[RFC5654] Niven-Jenkins,B., Brungard,D., and Betts,M., "Requirements

of an MPLS Transport Profile", RFC5654, September 2009

[ITU-T Recommendation G.808.1 Amd1] ''Generic protection switching - Linear trail and subnetwork protection'', ITU-T G.808.1 Amendment 1, January 2009

8.2. Informative References

[MPLS-TP Framework] Bocci,M., and Bryant,S., "A Framework for MPLS in Transport Networks", draft-ietf-mpls-tp-framework-10 (Work in progress), February 2010

[MPLS-TP Survive Frmk] Sprecher,N., and Farrel,a., ''Multiprotocol Label Switching Transport Profile Survivability Framework", draft-ietf-mpls-tp-survive-fwk-03(work in progress), November 2009

[MPLS-TP OAM Requirements] Vigoureux,M., Ward,D., and Betts,M., ''Requirements for OAM in MPLS Transport Networks'', draft-ietf-mpls-tp-oam-requirements-06(work in progress), March 2010

Author's Addresses

Haiyan Zhang
Huawei Technologies Co., Ltd.

Phone: +86-755-28972333
Email: zhanghaiyan@huawei.com

Jia He
Huawei Technologies Co., Ltd.

Phone: +86-755-28972333
Email: hejia@huawei.com

Han Li
China Mobile Communications Corporation

Email: lihan@chinamobile.com