Network Working Group
Internet Draft
Intended status: Standard Track

J.He
Huawei Technologies

H.Li
China Mobile

E. Bellagamba
Ericsson

Expires: May 2011

November 18, 2010

Indication of Client Failure in MPLS-TP
draft-he-mpls-tp-csf-03.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a Multi-Protocol Label Switching Transport Profile (MPLS-TP) Operations, Administration and Maintenance (OAM) tool to propagate a client failure indication across an MPLS-TP network in case the propagation of failure status in the client layer is not supported as required in [RFC5860].

Table of Contents

1. Introduction.....2
2. Conventions used in this document.....3
2.1. Terminology.....3
3. Mechanisms of CSF.....4
3.1. General.....4
3.2. Transmission of CSF.....5
3.3. Reception of CSF.....6
3.4. Configuration of CSF.....6
4. Frame format of CSF.....6
5. Consequent actions.....8
6. Security Considerations.....8
7. IANA Considerations.....8
8. Acknowledgments.....8
9. References.....8
9.1. Normative References.....8
9.2. Informative References.....9
10. Authors' Addresses.....9

1. Introduction

In transport network OAM functionalities are important and fundamental to ease operational complexity, enhance network availability and meet service performance objectives by efficient and automatic detection, handling, diagnosis and appropriate reporting of defects and performance monitoring.

As defined in [RFC 5860] MPLS-TP OAM MUST provide a function to

enable the propagation, from edge to edge of an MPLS-TP network, of information pertaining to a client (i.e., external to the MPLS-TP network) defect or fault condition detected at an End Point of a PW or LSP, if the client layer OAM functionality does not provide an alarm notification/propagation functionality (e.g. not needed in the

original application of the client signal, or the signal was originally at the bottom of the layer stack and it was not expected to be transported over a server layer), while such an indication is needed by the downstream.

This document defines such a MPLS-TP OAM tool as Client Signal Fail indication (CSF) to propagate client failures and their clearance across a MPLS-TP domain.

According to [RFC 5921], MPLS-TP supports two native service adaptation mechanisms via:

1) a PW, to emulate certain services, for example, Ethernet, Frame Relay, or PPP / High-Level Data Link Control (HDLC).

2) an LSP, to provide adaptation for any native service traffic type supported by [RFC3031] and [RFC3032]. Examples of such traffic types include IP packets and MPLS-labeled packets (PW over LSP, or IP over LSP).

As to the first adaptation mechanism via a PW, the mechanism of CSF function to support propagation of client failure indication follows [static-pw-status]. The PW status relevant to CSF function is AC fault as defined in [RFC 4447] and [RFC 4446].

As to the second adaptation mechanism via LSP, the mechanism is detailed in this draft and is used in case the client of MPLS-TP can not provide itself with such failure notification/propagation.

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 [RFC 2119].

2.1. 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].

ACH: Associated Channel Header

AIS: Alarm Indication Signal

CSF: Client Signal Fail indication

FDI: Forward Defect Indication

G-ACh: Generic Associated Channel

GAL: G-ACh Label

LSR: Label Switching Router

MEP: Maintenance Entity Group End Point

MIP: Maintenance Entity Group Intermediate Point

OAM: Operations, Administration, and Maintenance

MPLS-TP: MPLS Transport Profile

RDI: Remote Defect Indication

3. Mechanisms of CSF

3.1. General

Client Signal Fail indication (CSF) provides a function to enable a MEP to propagate a client failure indication to its peer MEP across a MPLS-TP network in case the client service itself does not support propagation of its failure status.

Packets with CSF information can be issued by a MEP, upon receiving failure information from its client service. Detection rules for client failure events are client-specific and are therefore outside the scope of this document.

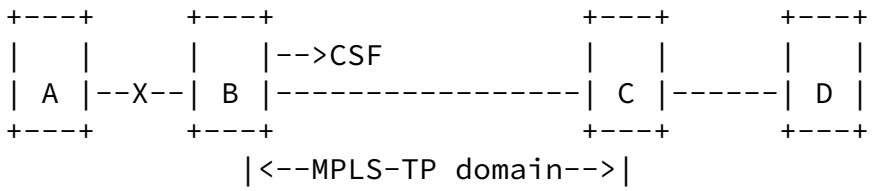

Figure 1 Use case of CSF

Figure 1 depicts a typical connection scenario between two client network elements (Node A and Node D) interconnected through MPLS-TP transport network. Client Node A connects to MPLS-TP Node B and Client Node D connects to MPLS-TP Node C. Node B and C support MPLS-TP MEP function.

If a failure is detected between Node A and Node B and is taken as a native client failure condition, the MEP function in Node B will initiate CSF signal and it will be sent to Node C through MPLS-TP network. CSF signal will be extracted at Node C as an indication of client signal failure. Further, this may be mapped back into native client failure indication and regenerated towards client Node D.

Node B learns the failure between A and B either by direct detection of signal fail (e.g. loss of signal) or by some fault indications between A and B (e.g. RDI, AIS/FDI).

If the connection between Node A and B recovers, Node B may stop sending CSF signals to Node C (implicit failure clearance mechanism) or explicitly send failure clearance indication (e.g. by flags in CSF PDU format) to Node C to help expedite clearance of native client failure conditions.

Accordingly, Node C will clear client failure condition when a valid client data frame is received and no CSF is received (implicit failure clearance mechanism) or upon receiving explicit failure clearance indication.

3.2. Transmission of CSF

Upon learning signal failure condition of its client-layer the MEP can immediately start transmitting periodic packets with CSF information. A MEP continues to transmit periodic packets with CSF

information until the client-layer signal failure condition is cleared.

The clearance of CSF condition can be communicated to the peer MEP via:

- Stopping transmission of CSF signal but forwarding client data frames, or
- Forwarding CSF PDU with clearance indication.

Transmission of packets with CSF information can be enabled or disabled on a MEP.

Detection and clearance rules for CSF events are client and application specific and outside the scope of this draft.

The period of CSF generation is client and application specific and outside the scope of this draft.

3.3. Reception of CSF

Upon receiving a packet with CSF information a MEP either declares or clears a client-layer signal fail condition according to the received CSF information and propagates this as a signal fail indication to its client-layer.

3.4. Configuration of CSF

Specific configuration information required by a MEP to support CSF transmission is the following:

CSF transmission period - this is application dependent.

PHB - identifies the per-hop behavior of packet with CSF information.

A MIP is transparent to packets with CSF information and therefore does not require any information to support CSF functionality.

4. Frame format of CSF

Figure 2 depicts the frame format of CSF. CSF PDUs are encapsulated using the ACH, according to [RFC 5586]. GAL is used as an alert based exception mechanism to differentiate CSF packets (with ACH as G-ACh packets) from user-plane packets as defined in [RFC 5586].

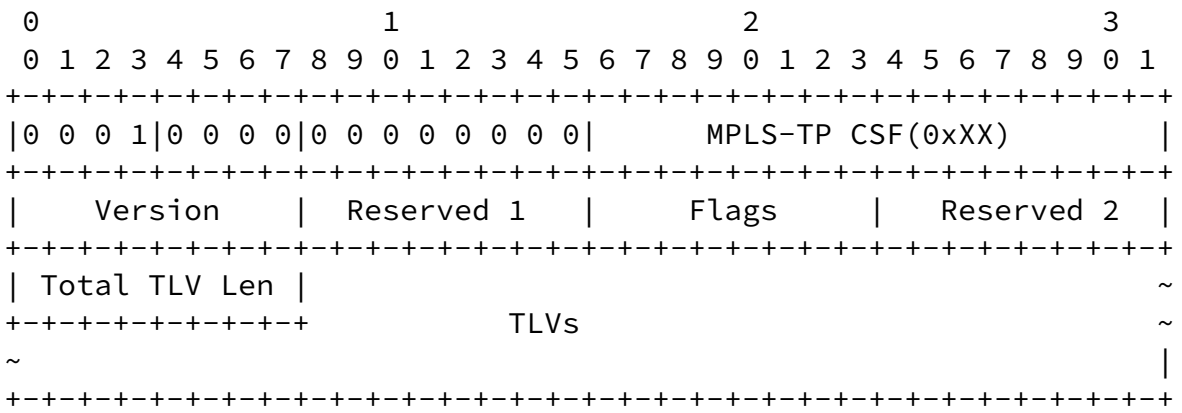

Figure 2 Frame format of CSF

The first four bytes represent the Generic ACH ([RFC 5586]):

- first nibble: set to 0001b to indicate a control channel associated with a PW, a LSP or a Section;

- ACH Version(bits 4 to 7): set to 0, as specified in [RFC 5586]

- ACH Reserved (bits 8 to 15): set to 0 and ignored on reception, as specified in [RFC 5586];

- ACH Channel Type (Bits 16 to 31): value 0xXX identifies the payload as CSF PDU. To be assigned by IANA.

- CSF Version (Bits 32 to 39): Set to 0;

- CSF Reserved 1 (Bits 40 to 47): This field MUST be set to zero on transmission and ignored on receipt;

- CSF Reserved 2 (Bits 56 to 63): This field MUST be set to zero on transmission and ignored on receipt;

- Total TLV Length: Total of all included TLVs. No TLVs are

defined currently. The value is 0.

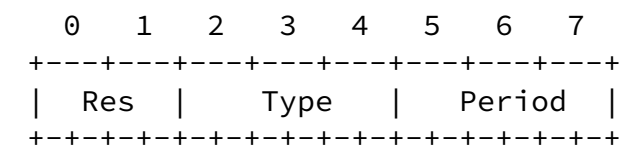

Figure 3 Format of Flags in CSF PDU

Figure 3 depicts the format of Flags in CSF PDU.

- Flag Reserved (Bits 48 to 49): Set to 0;

- Type (Bits 50 to 52): Set to the following values to indicate CSF types

Value	Type
111	Client Signal Fail - Loss of Signal (CSF-LOS)
001	Client Signal Fail - Forward Defect Indication (CSF-FDI)
010	Client Signal Fail - Reverse Defect Indication (CSF-RDI)
000	Clearance of Client Signal Fail - (CSF-Clear)

- Period (Bits 53 to 55): CSF transmission period and can be configured.

5. Consequent actions

The primary intention of CSF is to transport a client signal fail condition at the input of the MPLS-TP network to the output port of the MPLS-TP network for clients that do not have alarm notification/propagation mechanism defined.

Further, CSF allows creating a condition at the output port of the MPLS-TP network such that the customer input port is able to detect and alarm that there is no data arriving i.e. the connection is interrupted. In this case, customers may choose another transport network or another port to continue communication.

6. Security Considerations

Malicious insertion of spurious CSF signals (e.g. DoS) is not quite likely in a transport network since transport networks are usually self-managed by operators and providers.

7. IANA Considerations

This document requests that IANA allocates a new Associated Channel Type for CSF function to be used in MPLS-TP OAM.

8. Acknowledgments

The authors would like to thank Haiyan Zhang, Adrian Farrel, Loa Andersson, Matthew Bocci and Andy Malis for their guidance to this work.

9. References

9.1. Normative References

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

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[RFC4446] Martini, L., "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", RFC4446, April 2006

[RFC4447] Martini, L., et al., "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC4447, April 2006.

[RFC5586] Vigoureux, M., Bocci, M., Swallow, G., Ward, D., and R. Aggarwal, "MPLS Generic Associated Channel", RFC5586, June 2009

[ITU-T Recommendation G.7041] "Generic framing procedure (GFP)", ITU-T G.7041, October 2008

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

[RFC 5860] Vigoureux, M., Ward, D., and M. Betts, "Requirements for OAM in MPLS Transport Networks", RFC5860, May 2010

[RFC 5921] Bocci, M., Bryant, S., and D. Frost, "A Framework for MPLS in Transport Networks", RFC 5921, July 2010

[static-pw-status] Martini, L., Swallow, G., Heron, G., and M. Bocci, "Pseudowire Status for Static Pseudowires", draft-ietf-pwe3-static-pw-status-01 (work in progress), October 2010

9.2. Informative References

[MPLS-TP OAM Frmk] Busi,I., and D. Allan, "MPLS-TP OAM Framework and Overview", draft-ietf-mpls-tp-oam-framework-09(work in progress), October 2010

[Rosetta stone] Van Helvoort, H., Andersson, L., Sprecher, N., "A Thesaurus for the Terminology used in Multiprotocol Label Switching Transport Profile (MPLS-TP) drafts/RFCs and ITU-T's Transport Network Recommendations", draft-ietf-mpls-tp-rosetta-stone-02 (work in progress), May 2010

10. Authors' Addresses

Jia He
Huawei Technologies Co., Ltd.

Email: hejia@huawei.com

Han Li
China Mobile Communications Corporation

Email: lihan@chinamobile.com

Elisa Bellagamba
Ericsson

Email: elisa.bellagamba@ericsson.com

Intellectual Property

the IETF Standards Process to the IETF Trust pursuant to the provisions of RFC 5378. No language to the contrary, or terms, conditions or rights that differ from or are inconsistent with the rights and licenses granted under RFC 5378, shall have any effect and shall be null and void, whether published or posted by such Contributor, or included with or in such Contribution.

Disclaimer of Validity

Copyright Notice