Network Working Group
Request for Comments: 3429
Category: Informational

H. Ohta
NTT

November 2002

Assignment of the 'OAM Alert Label' for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM) Functions

Status of this Memo

Copyright Notice

Abstract

This document describes the assignment of one of the reserved label values defined in RFC 3032 (MPLS label stack encoding) to the 'Operation and Maintenance (OAM) Alert Label' that is used by user-plane Multiprotocol Label Switching Architecture (MPLS) OAM functions for identification of MPLS OAM packets.

1. Introduction

This document describes the assignment of one of the reserved label values defined in RFC 3032 (MPLS label stack encoding [2]) to the 'OAM Alert Label' that is used by user-plane MPLS OAM functions for identification of MPLS OAM packets as described in the ITU-T Recommendation Y.1711 [1] (on MPLS OAM functions).

2. OAM functions

MPLS OAM (Operation and Maintenance) functions provide necessary tools for network operators to operate and maintain the networks. MPLS OAM functionality is required at the MPLS layer, and more specifically at each MPLS level, independent of OAM functionality provided by the lower layers (SONET/SDH, etc.). The objectives of the OAM functions include the following:

- Defect and failure detection: Defect/failures affecting the transport of user information are detected by continuous or periodic checking. As a result, maintenance event information or appropriate alarms will be produced.

- Reporting the defect/failure information: Defect information is given to other management entities (e.g., Operation Support System) in order to provide the appropriate indications to the maintenance staff for maintaining the Quality of Service (QoS) level offered to customers.

- Defect/failure localization: Determination by internal or external test systems of a failed entity is performed if defect information is insufficient.

- Performance monitoring: Performance (packet losses, transfer delay, bit errors, etc.) of the user information transport is measured in order to estimate the transport integrity.

3. OAM Packet Identification

The user-plane MPLS OAM mechanisms as described in the ITU-T Recommendation Y.1711 [1] uses a special label called 'OAM Alert Label' to differentiate OAM packets from the normal user packets. One of the reserved label values defined in RFC 3032 (MPLS label stack encoding [2]) is assigned to 'OAM Alert Label'. A value of 14 is used for this purpose.

4. MPLS OAM work in ITU-T SG13

ITU-T Study Group 13, Question 3/13 is progressing work on user-plane MPLS OAM and has produced the following documents:

(1) Recommendation Y.1710 (Requirements for OAM functionality for MPLS networks) [3]

(2) Corrigendum 1 to Recommendation Y.1710 [4]

(3) Recommendation Y.1711 (OAM mechanisms for MPLS networks) [1]

(4) Draft Recommendation Y.1720 (Protection switching for MPLS networks) [6] relies on OAM mechanisms in Y.1711, under last call as of Nov. 2002.

5. Considerations on penultimate hop popping (PHP)

In response to concerns raised during IETF meetings and in related discussions, this section provides an explanation on how MPLS OAM functions defined in ITU-T Recommendation Y.1711 [1] are applied to MPLS networks where PHP is in effect.

5.1 Scope of ITU-T Recommendation Y.1711

The scope of ITU-T Recommendation Y.1711 includes application to both non-PHP and PHP cases as quoted below [1].

"1 Scope
This Recommendation provides mechanisms for user-plane OAM (Operation and Maintenance) functionality in MPLS networks according to the requirements and principles given in Recommendation Y.1710. OAM functions specified in this Recommendation can be applied to both non-PHP and PHP cases unless otherwise stated. The current version of this recommendation is designed primarily to support point-to-point and multipoint-to-point explicit routed LSPs (ER-LSPs)."

5.2 Applicability of MPLS OAM to PHP

There are two cases where PHP is used:

Case 1: The ultimate node is an MPLS LSR, and implements both MPLS control-plane and data-plane, but is not able to perform 2 lookups at line rate. So it asks the penultimate node to pop the top label (rather than swapping it), using the MPLS reserved label 3 (implicit null label) as per defined in RFC 3032 [2].

Case 2: The ultimate node has no MPLS label look up and processing capability and does not recognize labeled packets. This node asks for PHP, using the MPLS reserved label 3 (implicit null label) as defined in RFC 3032 [2].

Currently, MPLS OAM functions defined in ITU-T Recommendation Y.1711 [1] can only be applied to Case 1. The next subsection describes the node behavior in Case 1. Application for Case 2 needs further study. Also, application to carrier supporting carrier scenarios is for future study.

5.3 Node behavior when OAM functions are activated

Where the ultimate LSR is an MPLS LSR and PHP is in effect, the penultimate LSR pops the top label and forwards the OAM packet (with the OAM label and the OAM payload intact) to the ultimate LSR [5].

- If the ultimate LSR supports MPLS OAM, it understands that a received packet with an OAM label on top is an OAM packet, since the original top label has been removed by the penultimate LSR. It also knows the ingress LSR that originated the MPLS OAM packet from the TTSI (Trail Termination Source Identifier) value of the

received MPLS OAM packet. TTSI is a unique identifier for ingress LSR that is contained in MPLS OAM packets (see ITU-T Recommendation Y.1711 [1]).

- If the ultimate LSR does not support MPLS OAM, the OAM packet is discarded as per section 3.18 of RFC 3031 [5].

6. IANA Considerations

The IANA has reserved the use of the MPLS label value of 14 as the 'OAM Alert Label'. See section 3 for additional information.

7. Security Considerations

This document does not raise any security issues that are not already present in either the MPLS architecture or in the architecture of the network layer protocol contained within the encapsulation.

OAM functions could enhance the security of MPLS networks. For example, Connectivity Verification (CV) function defined in ITU-T Recommendation Y.1711 [1] can detect mis-connections, and therefore can prevent customers' traffic being exposed to other customers.

8. Acknowledgements

The author wishes to thank Shahram Davari with PMC-Sierra, Neil Harrison with British Telecom, Monique Morrow, Thomas D. Nadeau, Hari Rakotoranto and Chip Sharp with Cisco Systems, Khalid Ahmad and David Allan with Nortel Networks, and Mina Azad with Azad-Mohtaj Consulting for their valuable contributions and discussions.

9. Normative References

[1] ITU-T Recommendation Y.1711, "OAM mechanism for MPLS networks", November 2002.

[2] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinaccia, D., Li, T. and A. Conta, "MPLS label stack encoding", RFC 3032, January 2001.

[3] ITU-T recommendation Y.1710, "Requirements for OAM functionality for MPLS networks" July 2001.

[4] ITU-T Corrigendum 1 to Recommendation Y.1710, November 2002.

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

10. Informative Reference

[6] ITU-T Draft Recommendation Y.1720, "Protection switching for MPLS networks", under last call as of November 2002.

11. Author's Address

Hiroshi OHTA
NTT
3-9-11 Midori-Cho, Musashino-Shi
Tokyo 180-8585 Japan

Phone: +81 422 59 3617
Fax: +81 422 59 3787
EMail: ohta.hiroshi@lab.ntt.co.jp

12. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.