Network Working Group
Internet Draft
Updates: RFC4204
Category: Standards Track

Dan Li
Huawei
D. Ceccarelli
Ericsson

Expires: November 2010

May 28, 2010

Behavior Negotiation in Link Management Protocol

draft-li-ccamp-lmp-behavior-negotiation-01.txt

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 November 27, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Abstract

The Link Management Protocol (LMP) is used to coordinate the properties, use, and faults of data links in Generalized Multiprotocol Label Switching (GMPLS) networks. Various proposals have been advanced to provide extensions to the base LMP specification. This document provides a generic procedure for LMP implementations that do not recognize or do not support any one of these extensions.

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].

Table of Contents

1. Introduction.....2
2. LMP Behavior Negotiation Procedure.....3
3. Security Considerations.....6
4. IANA Considerations.....6
5. Contributors.....6
6. Acknowledgments.....7
7. References.....7
7.1. Normative References.....7
7.2. Informative References.....7
8. Authors' Address.....8

1. Introduction

The Link Management Protocol (LMP) [RFC4204] is being successfully deployed in Generalized Multiprotocol Label Switching (GMPLS) networks in the field. New LMP behaviors and protocol extensions are being introduced in a number of IETF documents.

In the network, if one GMPLS Label Switching Router (LSR) supports a new behavior or protocol extension, but its peer LSR does not, it is necessary to have a protocol mechanism for resolving issues that may arise. It is also beneficial to have a protocol mechanism to discover the capabilities of peer LSRs. There is no such procedure defined in the base LMP specification [RFC4204], so this document

defines how to handle LMP extensions both at legacy LSRs and at upgraded LSRs that communicate with legacy LSRs.

In [RFC4204], the basic behaviors have been defined around the use of the standard LMP message, which includes Config, Hello, Verify, Test, LinkSummary, ChannelStatus. Per [RCF4204], these behaviors MUST be supported when the LMP is implemented, and the message types from 1 to 20 are used for these behaviors.

In [RFC4207], the SONET/SDH technology-specific information for LMP is defined. The TRACE behavior is added to LMP, and the message types from 21 to 31 were defined for the TRACE function. The TRACE function has been extended for the support of OTNs (Optical Transport Networks) in [LMP TEST].

In [RFC4209], extensions to LMP are defined to allow it to be used between a peer node and an adjacent optical line system (OLS). The LMP object class type and sub-object class name have been extended to support DWDM behavior.

In [RFC5818], the data channel consistency check behavior is defined, the message types from 32 to 34 are used for this behavior.

This document describes the behavior negotiation procedure to make sure both LSRs of each link understand the LMP messages being exchanged between peers.

2. LMP Behavior Negotiation Procedure

The Config message is used in the control channel negotiation phase of LMP [RC4204]. The LMP behavior negotiation procedure is defined in this document as an addition at this phase.

The Config message is defined in Section 12.3.1 of [RFC4204] and carries the <CONFIG> object (class name 6) as defined in Section 13.6 of [RFC4204]. Multiple <CONFIG> objects (each with a different Class Type) MAY be present on a Config message in which case all of the objects MUST be processed.

Two class types have been defined:

- C-Type = 1, HelloConfig, defined in [RFC4204]

- C-Type = 2, LMP_WDM_CONFIG, defined in [RFC4209]

This document defines a third C-Type with value 3 (TBD by IANA) to report and negotiate new and future LMP extensions and behaviors.

- C-Type = 3, ENHANCED_BEHAVIOR_CONFIG

Two different types of flag are defined in this object: Architecture Flags and Capability Flags. The first set of flags indicates the network architecture supported by the node (e.g. OTN, SDH/SONET, DWDM), while the second one all the optional capabilities supported by the protocol implementation (e.g. Link Verification, Fault Management). The existing RFCs define the following capabilities:

- Control Channel Management (Mandatory)

- Link Property Correlation (Mandatory)

- Link Verification (Optional)

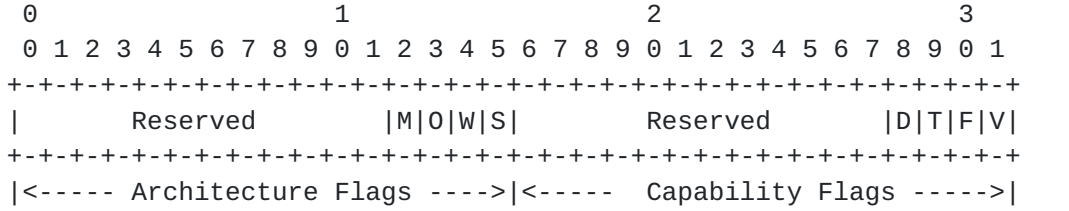
- Fault Management (Optional)

- Trace Monitoring (Optional)

- Data Channel Status Confirmation (Optional)

Due to the fact that Control Channel Management and Link Property Correlation are mandatory capabilities, no capability flag is defined for their configuration. When an architecture flag is set, automatically these two capabilities are implicitly supported. With respect to the other ones, a flag for each of them is defined.

The format of the new type of CONFIG Class is defined as follows:



Architecture Flags:

S: 1 bit

This bit indicates support for the SONET/SDH.

W: 1 bit

This bit indicates support for WDM.

O: 1 bit

This bit indicates support for OTN.

M: 1 bit

This bit indicates support for MPLS-TP

Capability Flags:

V: 1 bit

This bit indicates support for the Link Verification capability defined in [RFC4204].

F: 1 bit

This bit indicates support for the Fault Management capability defined in [RFC4204].

T: 1 bit

This bit indicates support for the Trace Monitoring defined in [RFC4204], [RFC4207] and [LMP TEST].

D: 1 bit

This bit indicates support for the Data Channel Status Confirmation messages defined in [RFC5818].

Further bits may be defined in future documents.

The Reserved field MUST be sent as zero and MUST NOT be ignored on receipt. This allows the detection of supported/unsupported LMP behaviors.

Upon receiving a bit set related to a non supported behavior, a ConfigNack message MUST be sent with a <CONFIG> object representing the supported LMP behaviors.

An LSR that receives a Config message containing a <CONFIG> object with a C-Type that it does not recognize MUST respond with a ConfigNack message as described in [RFC4204]. Thus, legacy LMP nodes that do not support the ENHANCED_BEHAVIOR_CONFIG C-Type defined in this document will respond with a ConfigNack message.

3. Security Considerations

[RFC4204] describes how LMP messages between peers can be secured, and these measures are equally applicable to messages carrying the new <CONFIG> object defined in this document.

The operation of the procedures described in this document does not of itself constitute a security risk since they do not cause any change in network state. It would be possible, if the messages were intercepted or spoofed to cause bogus alerts in the management plane, or to cause LMP peers to consider that they could or could not operate protocol extensions, and so the use of the LMP security measures are RECOMMENDED.

4. IANA Considerations

IANA maintains the "Link Management Protocol (LMP)" registry which has a subregistry called "LMP Object Class name space and Class type (C-Type)".

IANA is requested to make an assignment from this registry as follows:

6	CONFIG	[RFC4204]

CONFIG Object Class type name space:

C-Type	Description	Reference
3	ENHANCED_BEHAVIOR_CONFIG	[This.I-D]

5. Contributors

Diego Caviglia
Ericsson
Via A. Negrone 1/A 16153
Genoa Italy
Phone: +39 010 600 3736
Email: diego.caviglia@ericsson.com

6. Acknowledgments

Thanks to Adrian Farrel and Lou Berger for their useful comments.

7. References

7.1. Normative References

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

[RFC4204] J. Lang, Ed., "Link Management Protocol (LMP)", RFC 4204, October 2005.

[RFC4207] J. Lang, Ed., "Synchronous Optical Network (SONET)/ Synchronous Digital Hierarchy (SDH) Encoding for Link Management Protocol (LMP) Test Messages", RFC 4207, October 2005.

[RFC4209] A. Fredette, Ed., "Link Management Protocol (LMP) for Dense Wavelength Division Multiplexing (DWDM) Optical Line Systems", RFC 4209, October 2005.

[RFC5818] D. Li, Ed., "Data Channel Status Confirmation Extensions for the Link Management Protocol", RFC 5818, April 2010.

7.2. Informative References

[LMP TEST] D. Ceccarelli, Ed., "Link Management Protocol (LMP) Test Messages Extensions for Evolutive Optical Transport Networks (OTN)" draft-ceccarelli-ccamp-gmpls-g709-lmp-test-02.txt, May, 2010.

8. Authors' Address

Dan Li
Huawei Technologies
F3-5-B R&D Center, Huawei Industrial Base,
Shenzhen 518129 China
Phone: +86 755-289-70230
Email: danli@huawei.com

Daniele Ceccarelli
Ericsson
Via A. Negrone 1/A
Genova - Sestri Ponente
Italy
Email: daniele.ceccarelli@ericsson.com