

MPLS Working Group
Internet Draft
Intended status: Standard
Expires: January 2012

Pranjal Kumar Dutta
Alcatel-Lucent

Giles Heron
Cisco Systems

Thomas Nadeau
CA Technologies

July 3, 2011

Targeted LDP Hello Reduction
draft-pdutta-mpls-tldp-hello-reduce-02.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 January 3, 2011.

Abstract

Targeted LDP Hellos are used for establishing adjacencies with non-directly connected peers. After an LDP session is established to a targeted peer, the session Keepalives are sufficient to notify the intent of an LSR to maintain its adjacency with the peer. This document proposes a mechanism to turn off Targeted LDP Hellos after LDP session is established to a peer.

Table of Contents

1. Introduction.....	2
2. Conventions used in this document.....	3
3. Terminology.....	3
4. Targeted LDP Hello Reduction Procedure.....	3
5. Security Considerations.....	5
6. IANA Considerations.....	5
7. Conclusion.....	5
8. References.....	5
8.1. Normative References.....	5
8.2. Informative References.....	5
9. Acknowledgments.....	6

[1. Introduction](#)

LDP Hello messages are exchanged as part of the LDP discovery mechanism [[RFC5036](#)]. There are two types of LDP discovery mechanism described in [[RFC5036](#)] - Basic Discovery and Extended Discovery.

To engage in LDP Basic Discovery on an interface, an LSR periodically sends LDP Link Hellos out the interface to the well-known LDP discovery port for the "all routers on this subnet" group multicast address. Receipt of an LDP Link Hello on an interface, identifies a hello adjacency with a potential LDP peer reachable at the link level on the interface. Thus an LSR may establish hello adjacency with multiple peers discovered over a single interface and must continue to transmit hellos at regular intervals even after hello adjacency is established to a peer.

Extended discovery is used to support LDP sessions between non-directly connected LSRs. An LDP Targeted Hello is sent to a specific address rather than to the "all routers" group multicast address for the ongoing interface. Receipt of a LDP Targeted Hello identifies a hello adjacency with a potential LDP peer at network level.

In Extended discovery there can be only one Targeted Hello Adjacency between two peers. Note that throughout this document "peer" means the LDP LSR designated by a unique LDP Identifier. Once the LDP session is operational between two targeted LDP peers, periodic session Keepalives are used to maintain the LDP session. After the session is operational the periodic Targeted Hellos between the LSRs become redundant, as session Keepalives in turn serves the intent of each LSR to maintain its adjacency to its peer.

When an LSR maintains a large number of LDP sessions (in thousands) to targeted peers, it is an additional burden to send and receive Targeted Hellos for all peers at periodic intervals. In MPLS deployments at access or mobility backhaul, there can be very large volume of LDP sessions with targeted LDP adjacencies to each base station. Moreover additional mechanisms such as centralized BFD [[BFD](#)] may be used to track liveness of ldp sessions.

Another problem with targeted hello adjacency arises is Denial Of Service (DoS)_attacks. It is possible that existing hello adjacencies can get lost due to DoS attack on LDP Hello receiver by spurious hello packets. Unlike TCP sessions it is not always possible to provide per peer protection for UDP based hellos. Implementations can use methods to protect existing adjacencies while throttling spurious adjacencies but such methods may not be available in low cost MPLS devices in access. So it is important to avoid dependency on targeted LDP hellos on session maintenance as far as possible.

This document proposes an optional mechanism to turn off Targeted LDP Hellos after a LDP session is established to a targeted peer, without changes in the procedures defined in [[RFC5036](#)].

2. Conventions used in this document

INFO (REMOVE): INCLUDE THIS SECTION OR PORTIONS THEREOF IF DESIRED

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

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. Terminology

This document uses the terminology defined in [[RFC3031](#)] and [[RFC5036](#)].

4. Targeted LDP Hello Reduction Procedure

The Targeted LDP Hello Reduction procedure uses the existing Common Hello Parameters TLV defined in [[RFC5036](#)]. Figure 1. shows the encoding of the TLV from [[RFC5036](#)] for reference.

Note that it is not mandatory to advertise infinite hold time after session is established but can be any value that is significantly larger than configured hello hold time. It is RECOMMENDED to advertise Inifinite holdtime after session setup to derive maximum advantage from the procedure described above.

5. Security Considerations

- Control plane aspects
 - LDP security (authentication) methods as described in [[RFC5036](#)] is applicable here.
- Data plane aspects
 - This specification does not have any impact on the MPLS forwarding plane setup by LDP.

6. IANA Considerations

This document does not require any IANA consideration.

7. Conclusion

The method proposed in the document reduces significant burden on an LDP LSR that maintains Targeted LDP sessions to a large number (in thousands) of peers. Further, if BFD [[BFD](#)][BFD-MHOP] is used for tracking connectivity to peers it is desirable to turn off Targeted LDP hellos after the LDP session is setup.

8. References

8.1. Normative References

- [RFC5036] Andersson, L., et al. "LDP Specification", [RFC5036](#), October 2007.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

8.2. Informative References

- [RFC3031] Rosen, E., et al. "Multiprotocol Label Switching Architecture", [RFC 3031](#), January 2001.
- [BFD] Katz, D., et al. "Bidirectional Forwarding Detection", [draft-ietf-bfd-base-011.txt](#), January 2010.

[BFD-MHOP] Katz, D., et al. "BFD for Multihop Paths",
[draft-ietf-bfd-multihop-09.txt](#), January 2010.

9. Acknowledgments

The authors would like acknowledge the comments and suggestions from Wim Henderickx, Vach Kompella, Florin Balus, Mustapha Aissaoui, Mathew Bocci and Paul Kwok.

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Pranjal Kumar Dutta
701 E Middlefield Road,
Mountain View, CA 94043.
USA.
Email: pranjal.dutta@alcatel-lucent.com

Giles Heron
Cisco Systems
Email: giheron@cisco.com

Thomas D. Nadeau
CA Technologies
273 Corporate Drive, Portsmouth, NH, USA

Email: thomas.nadeau@ca.com

Copyright Notice

Copyright (c) 2011 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.