MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2011

C. Pignataro
R. Asati
Cisco Systems

March 11, 2011

# The Generalized TTL Security Mechanism (GTSM) for Label Distribution Protocol (LDP)
## draft-asati-pignataro-mpls-ldp-gtsm-01

Abstract

The Generalized TTL Security Mechanism (GTSM) describes a generalized use of a packets Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to verify that the packet was sourced by a node on a connected link, thereby protecting the router's IP control-plane from CPU utilization based attacks. This technique improves security and is used by many protocols. This document defines the GTSM use for Label Distribution Protocol (LDP).

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on September 12, 2011.

Table of Contents

## 1. Introduction

LDP [RFC5036] specifies two Discovery mechanisms, a Basic one and an Extended one, both using UDP transport. The Basic Discovery mechanism is used to discover LSR neighbors that are directly connected at the link level, whereas the Extended Discovery mechanism is used to locate LSR neighbors that are not directly connected at the link level. Once discovered (or located), the LSR neighbors can establish the LDP peering session, using the TCP transport connection.

The Generalized TTL Security Mechanism (GTSM) [RFC5082] is a mechanism based on IPv4 Time To Live (TTL) or (IPv6) Hop Limit value verification so as to provide a simple and reasonably robust defense from infrastructure attacks using forged protocol packets from outside the network. GTSM can be applied to any protocol peering session that is established between routers that are adjacent. Therefore, GTSM can fully benefit LDP protocol peering session established using Basic Discovery.

This document specifies LDP enhancements to accommodate GTSM. In particular, this document specifies the enhancements in the following areas:

1. Common Hello Parameter TLV of LDP Link Hello message

2. Sending and Receiving procedures for LDP Link Hello message

3. Sending and Receiving procedures for LDP Initilization message

While GTSM specifies that it SHOULD NOT be enabled by default in order to remain backward-compatible with the unmodified protocol, this document specifies having GTSM for LDP be enabled by default but not be enforced unless both peers can detect each others' support for GTSM procedures as described in this document.

### 1.1. Specification of Requirements

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].

### 1.2. Scope

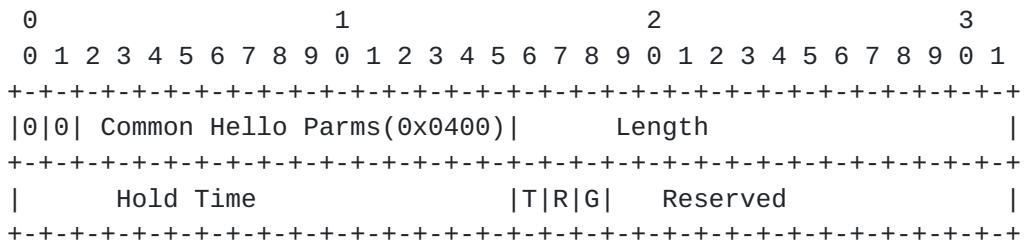
This document defines procedures for LDP using IPv4 routing, but not for LDP using IPv6 routing, since the latter has GTSM built into the protocol definition [I-D.ietf-mpls-ldp-ipv6].

Additionally, this document applies to LDP peering sessions set up using Basic Discovery only. LDP peering sessions set up using Extended Discovery are outside the scope of this document (see Section 5.5 of [RFC5082]).

## 2. GTSM Procedures for LDP

### 2.1. GTSM Flag in Common Hello Parameter TLV

A new flag in Common Hello Parameter TLV, named G flag (for GTSM), is defined by this document. An LSR indicates that it is capable of applying GTSM procedures, as defined in this document, to the subsequent LDP peering session, by setting the GTSM flag to 1. The Common Hello Parameters TLV, defined in Section 3.5.2 of [RFC5036], is updated as shown in Figure 1.




G, GTSM
A value of 1 specifies that this LSR wishes to support GTSM procedures, where a value of 0 specifies that this LSR does not wish to support GTSM.

Figure 1: GTSM Flag in Common Hello Parameter TLV

The G flag is meaingful only if T and R flags are set to 0 (which must be the case for Basic Discovery), otherwise, the value of G flag should be ignored on receipt.

Any LSR not supporting GTSM for LDP, as defined in this document, would continue to ignore the G flag, independent of T and R flags' value, as per Section 3.5.2 of [RFC5036].

### 2.2. GTSM Sending and Receiving Procedures for LDP Link Hello

Firstly, LSRs using LDP Basic Discovery [RFC5036] send LDP Hello messages to link-level multicast address (224.0.0.2 or "all routers"). Such messages are never forwarded beyond one hop and assumed to have their IP TTL or Hop Count = 1.

An LSR may indicate that it is capable of applying GTSM procedures to

the subsequent TCP/LDP peering session by setting the G flag (for GTSM) to 1 in Common Hello Parameter TLV in the LDP Link Hello message [RFC5036].

An LSR, upon receiving an LDP Link Hello message, would recognize the presence of G flag (in Common Hello Parameter TLV) only if it supports GTSM for LDP, as specified in this document. If an LSR recognizes the presence of G flag with the value =1 in the received LDP Link Hello message, then it must enforce GTSM for LDP in the subsequent TCP/LDP peering session with the neighbor that sent the Hello message, as specified in Section 2.3 of this document.

If an LSR does not recognize the presence of G flag (in Common Hello Parameter TLV of Link Hello message), or recognizes the presence of G flag with the value = 0, then the LSR must not enforce GTSM for LDP in the subsequent TCP/LDP peering session with the neighbor that sent the Hello message. This ensures backward compatibility as well as automatic GTSM de-activation.

If an LSR that has sent the LDP Link Hello with G flag = 1, then the LSR must set IP TTL or Hop Count = 255 in the forthcoming Transport Connection(s) with that neighbor (LSR2, say). Please see Section 2.3 for more details about the TCP transport connection specifics.

### 2.3. GTSM Sending and Receiving Procedures for LDP Initialization

If an LSR that has sent and received LDP Link Hello with G flag = 1 from the directly-connected neighbor (LSR2, say), then the LSR must enforce GTSM procedures, as defined in Section 3 of [RFC5082], in the forthcoming Transport Connection with that neighbor (LSR2, say). This means that the LSR must check for the incoming unicast packets' TTL or Hop Count to be 255 for the particular LDP/TCP peering session and decide the further processing as per the [RFC5082].

If an LSR that has sent LDP Link Hello with G flag = 1, but received LDP Link Hello with G flag = 0 from the directly-connected neighbor (LSR3, say), then the LSR must not enforce GTSM procedures, as defined in Section 3 of [RFC5082], in the forthcoming Transport Connection with that neighbor (LSR2, say).

## 3. IANA Considerations

IANA is requested to assign the G, GTSM bit in the Common Hello Parameters TLV (see Figure 1 in Section 2.1), as per allocation policy defined at [I-D.asati-pignataro-mpls-ldp-iana].

## 4. Security Considerations

This document increases the security for LDP, making it more resilient to off-link attacks.

## 5. Acknowledgments

The authors of this document do not make any claims on the originality of the ideas described. The concept of GTSM for LDP has been proposed a number of times, and is documented in both the Experimental and Standards Track specifications of GTSM. Among other people, we would like to acknowledge Enke Chen and Albert Tian for their document "TTL-Based Security Option for the LDP Hello Message".

## 6. References

### 6.1. Normative References

[I-D.asati-pignataro-mpls-ldp-iana]
Pignataro, C. and R. Asati, "Label Distribution Protocol (LDP) Internet Assigned Numbers Authority (IANA) Considerations Update", draft-asati-pignataro-mpls-ldp-iana-01 (work in progress), March 2011.

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

[RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP Specification", RFC 5036, October 2007.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007.

### 6.2. Informative References

[I-D.ietf-mpls-ldp-ipv6]
Manral, V., Papneja, R., and R. Asati, "Updates to LDP for IPv6", draft-ietf-mpls-ldp-ipv6-00 (work in progress), November 2010.

Authors' Addresses

Carlos Pignataro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: cpignata@cisco.com

Rajiv Asati
Cisco Systems
7025-6 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: rajiva@cisco.com