Network Working Group                                        B. Decraene
Internet-Draft                                                C. Schmitz
Intended status: Informational                                    Orange
Expires: July 15, 2016                                  January 12, 2016

# IS-IS LSP lifetime corruption - Problem Statement
draft-decraene-isis-lsp-lifetime-problem-statement-01

## Abstract

The IS-IS protocol exchanges Link State Packet (LSP) to exchange routing information. The lifetime of this LSP is located in the LSP header and is neither protected from corruption by the Fletcher checksum nor by cryptographic authentication. So the LSP lifetime may be altered, either accidentally or maliciously any time.

The lifetime field of the LSP is an important field for the correct operation of IS-IS. Corruption of this LSP lifetime may cause flooding storm with severe impact in the network.

This draft documents the problem statement and calls for a solution.

## Status of This Memo



## Copyright Notice

Table of Contents



## 1. Introduction

A LSP is a Link State PDU, originated by a router and then flooded in the routing domain. A LSP may advertise topological, reachability or general routing information. A LSP is valid for the duration of its lifetime which is set by the originator and decreased during flooding and as time passes. Lifetime is encoded in the LSP header and is not protected by the LSP header Fletcher checksum nor by the cryptographic signature because both are computed by the originator while the lifetime is modified during flooding.

## 2. Lifetime is not protected from corruption

The IS-IS protocol is defined in [ISO10589-Second-Edition]. IS-IS exchanges Link State PDU (LSP) to advertise routing information. Each LSP its lifetime advertised in the PDU header. This lifetime is neither protected by the Fletcher checksum in the LSP header nor by the cryptographic checksum (TLV 10) defined in [RFC5304]. Hence the LSP lifetime may be corrupted but still used.

The lifetime field of the LSP header is an important field for the correct operation of IS-IS. Corruption of the LSP lifetime may cause LSP churn with severe impact in the network.

## 3. Consequences of a corrupted LSP Lifetime

The lifetime field of the LSP is an important field for the correct operation of IS-IS. This section evaluates the impact of LSP lifetime corruption on one LSP.

### 3.1. Lifetime corrupted to zero

In this case, a non-purge LSP gets its LSP lifetime corrupted to zero between its origination and a router "R" receiving the LSP.

If cryptographic authentication, as defined in [RFC5304], is not enabled in the network, this corrupted LSP is processed as if its lifetime has expired. This will replace any non-expired version of the same LSP in the LSPDB and will cause the purge to be flooded network-wide. This creates a topological change in the network, requiring new routes computation and installation. This purge LSP is then flooded in the whole network, including to routers having a non corrupted version of the LSP. Finally, the originator of the LSP receive the purge LSP and advertise a new LSP with an increased sequence number. If the corruption is systematic, the processes cycles forever.

If cryptographic authentication is enabled in the network, [RFC5304] and [RFC6233] restrict the TLV code that are allowed in a purge. They specify that LSP with zero lifetime but having TLV not allowed in purge, must be ignored. As only a few TLV are acceptable in purge, this provides an effective protection as the LSP with the corrupted LSP lifetime will be ignored. Note that this additional check has been added because the lifetime, hence LSP purge, is not authenticated.

### 3.2. Lifetime corrupted to a non zero value

In this case, a non-purge LSP gets its LSP lifetime corrupted to value strictly greater than zero between its origination and a receiving IS-IS router.

This corrupted LSP is accepted as a regular LSP. The problem is that the originator is not aware of this change and if the lifetime has been reduced as a result of this corruption, the originator will likely not refresh the LSP before it expire. When the LSP expire, a LSP purge will be originated and flooded in the network. This creates a topological change in the network, requiring new routes computation and installation. At some point, the originator of the LSP receive the purge LSP and advertise a new LSP with an increased sequence number. If the corruption is systematic, the processes cycles forever.

Cryptographic authentication does not provide any additional protection.

If the lifetime is corrupted to a small to very small value, the effect is virtually equivalent to a purge. Hence, the restriction, introduced by [RFC5304], to restrict the list of TLV allowed in a purge LSP is not really effective. Hence, [RFC5304] does not succeed in "prevent[ing] a hostile system from receiving an LSP, setting the Remaining Lifetime field to [a small value], and flooding it, thereby initiating a purge without knowing the authentication password".

### 3.3. Summary

Cryptographic authentication addresses one case, where the LSP lifetime is corrupted to zero. All others cases triggers a flooding storm.

If the corruption is systematic on a given link, all LSPs flooded through that link are affected, creating flooding storm for multiple LSPs with severe impact in the network.

## 4. Protocol extension

Given the importance of the IGP for the network and the services carried in those IP/MPLS networks, and given the possibly large impact of LSP lifetime corruption, this documents calls for a protocol extension protecting or mitigating from the corruption of LSP lifetime.

Preferably, the protocol extension could be deployed incrementally with incremental benefit.

## 5. IANA Considerations

This document has no IANA action.

## 6. Security Considerations

This document describes a lack of integrity protection of the LSP LifeTime field. This LifeTime may be altered as a result of packet corruption (e.g. over transmission links, in routers' linecard or switch fabric) or may be voluntarily modified by an external party having access to one of theses resources used between IS-IS neighbours. Such modification are not detected by IS-IS checksum defined in [ISO10589-Second-Edition] nor the cryptographic authentication defined in [RFC5304]. This field is important for the protocol as it contains the life time of the routing information.

Modification of the lifetime of a single LSP transient impact the network by transiently removing a node from the routing topology and impacting the traffic crossing this node. This may also impact traffic not crossing the link as micro-loops may happen which would saturate some links.

Systematic modification of the lifetime of all LSPs crossing a single link would have a huge impact on the network. One part of the network would likely become virtually inoperative as having no (stable) available routes across the network. The whole flooding domain (L1 area or L2) would also be severely affected, especially since IGP instabilities creates instabilities to routing and signalling protocols relying on the IGP such as BGP, LDP, RSVP-TE, PCE...

As such, this may be considered as a security vulnerability.

## 7. Acknowledgement

The authors wish to thank Hannes Gredler, Les Ginsberg, Paul Wells and Stefano Previdi for discussions related to this topic.

## 8. References

### 8.1. Normative References

[ISO10589-Second-Edition]
International Organization for Standardization, "Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)", ISO/IEC 10589:2002, Second Edition, Nov 2002.

### 8.2. Informative References

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008, <http://www.rfc-editor.org/info/rfc5304>.

[RFC6233] Li, T. and L. Ginsberg, "IS-IS Registry Extension for Purges", RFC 6233, DOI 10.17487/RFC6233, May 2011, <http://www.rfc-editor.org/info/rfc6233>.

Authors' Addresses

Bruno Decraene
Orange

Email: bruno.decraene@orange.com

Christof Schmitz
Orange

Email: christof.schmitz@orange.com