IS-IS Minimum Remaining Lifetime

draft-ginsberg-isis-remaining-lifetime-00.txt

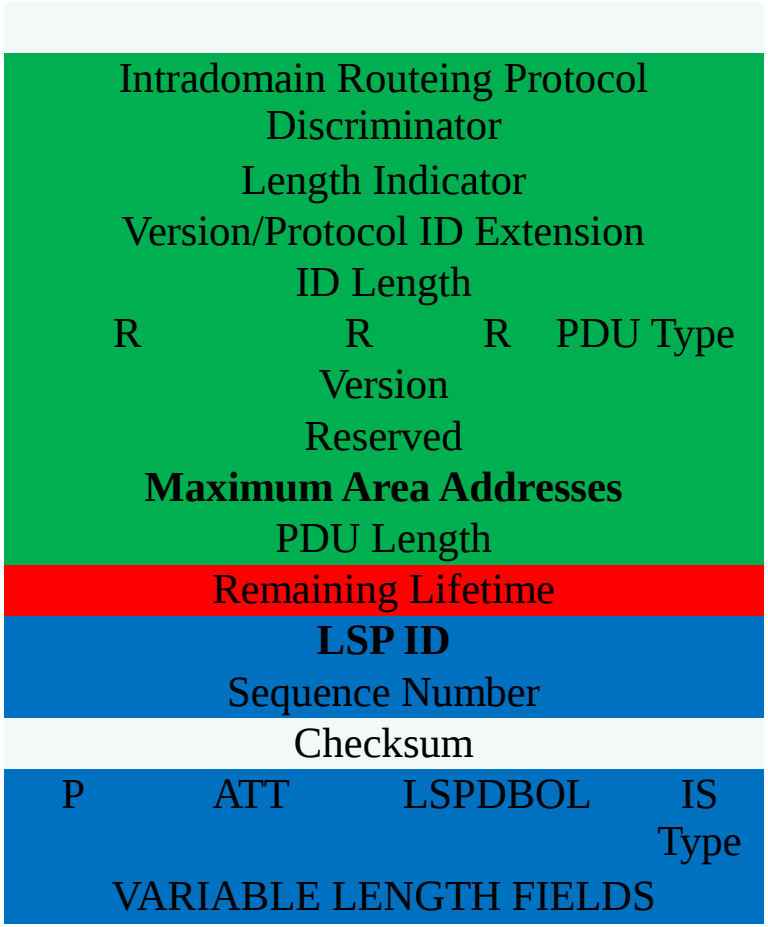
Les Ginsberg (ginsberg@cisco.com)
Stefano Previdi (sprevidi@cisco.com)
Paul Wells (pauwells@cisco.com)
Bruno Decraene(bruno.decraene@orange.com)
Tony Przygienda(antoni.przygienda@ericsson.com)
Hannes Gredler(hannes@gredler.at)

Problem Statement

draft-decraene-isis-lsp-lifetime-problem-statement-00

RemainingLifetime field in LSP header may get corrupted and corruption is undetectable even in the presence of cryptographic authentication. This can cause loss of connectivity and/or flooding storms.

LSP Format and Validation



Protected by cryptographic authentication (RFC 5304/RFC 5310)

Unprotected

Protected by checksum and cryptographic authentication

Consequences of Corruption

RemainingLifetime is greater than lifetime at the originator: Benign

LSP will be updated by originator before it expires – or originator becomes unreachable and LSP will not be used and eventually age out

RemainingLifetime is less than lifetime at the originator (but non-zero): Problem

LSP will age out prematurely and be purged prematurely. Leads to connectivity loss and additional LSP churn

Remaining Lifetime is zero (looks like a purge): handled by use of cryptographic authentication and support for RFC 6233 (restricts TLVs allowed in purges)

Causes of Corruption

Hardware failure by transmitter or receiver

Software failure by transmitter or receiver

Man-in-the-middle-DOS-attack:

Attacker can replay LSPs and change RemainingLifetime without having to know authentication keys

Corruption may be persistent

Keys to Solution

Definition of “newer LSP”:

Greater Sequence #

Same sequence # and RemainingLifetime is 0 (local is non-zero)

LSPs normally refreshed by originator before RemainingLifetime expires

If originator is unreachable LSPs are not used

Purging is an optimization – not required for correct operation of the protocol

Solution

Currently we store the Remaining Lifetime received when updating LSPDB w a “newer LSP”

New Behavior: If the RemainingLifetime of the new LSP is less than MaxAge it is set to MaxAge

Backwards Compatible

No change to Update Process

No change to purging logic

LSPs may be retained longer than before if originator becomes unreachable but this is benign

Deployment Considerations

MaxAge (AKA LSP Lifetime) is configurable

In the presence of inconsistent settings of MaxAge local MaxAge may be less than MaxAge on originator and problem might still occur

Implementations may wish to use a different value (>= MaxAge) as the lifetime inserted into new received LSPs

Logging of potential corrupt RemainingLifetime received in LSPs may be desirable

May be useful to retain and display the RemainingLifetime received when it is overwritten

WG adoption requested