Network Working Group
Internet draft
Mitchell Erblich
November 2004
Category: Informational
Document: <draft-erblich-ospf-nbr-rexmit-robust-enhance-00.txt>

Robust Enhancement to the Neighbor's Retransmission List when one or more LSA Checksum and length are in Error

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of section 3 of RFC 3667. By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with RFC 3668.

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 April 30, 2005.

Abstract

The ability to process LSAs within a Update packet requires that the length field be correct to generate the next offset within the packet. During the rare times that a checksum error and length LSA fields are incorrect, the beginning of later LSAs header's can't be determined. This draft specifies a transparent

method to allow all valid LSAs to be processed even when these corrupted LSAs exist on the neighbor's retransmission list.

Table of Contents

1. Introduction 2
2. Neighbor retransmission list robust enhancement 2
3. Alternative neighbor retransmission robust enhancement 2
4. References 3
5. Security Considerations 3
6. Author's Address 3

1. Introduction

RFC [2328] for OSPFv2 specifies that on page 142 all the LSAs that exist within the Update packet be processed. In the event that LSAs within this packet are not acknowledged, the non acknowledged LSAs will be retransmitted. These non acknowledged LSAs are repeatedly retrieved for retransmission from the neighbor's retransmission list.

In the past, networks have been moderated by router's bandwidth, memory, and other limitations and have summarized their links. This has kept link-state databases from expanding to excessive levels. However, this has come with a resultant loss of metric information. With current and near future technology, LSDBs can expand to current levels.

What was once rare checksum and length errors within moderately sized LSDBs can become common place when a router is dealing with millions of LSAs.

To allow the OSPF specifications to scale when dealing with the once rare event of a checksum and length LSA error existing on the neighbor retransmission list, rare error events need to be handled.

2. Neighbor retransmission list robust enhancement

With the assumption that a a corrupted LSA with a bad checksum and length is on the neighbor retransmission list. If later non corrupted LSAs are ordered after this corrupted LSA, they can never be processed.

A transparent change to the receiver requires that the

LSA transmitter alter the order of LSAs that are appearing on the Update packet.

The method chosen was to rotate the order by one position on each neighbor retransmission as if the LSAs were in a circular buffer. This allows all the non corrupted LSAs to be processed by the receiver over time.

3. Alternative neighbor retransmission robust enhancement

With the assumption that retransmission of LSAs may infrequently occur due to checksum / length failures and that the problem occurred before the LSAs was copied to the neighbor retransmission LSA list.

An alternative method is for the sender to periodically run a checksum scan on the retransmission LSA list and remove corrupted LSAs from the retransmission list.

The suggested period is 30 seconds to prevent normal retransmissions from having additional checksum overhead.

4. References

[2328] Moy, J., "OSPF Version 2", RFC 2328, April 1998.

5. Security Considerations

This memo does not create any new security issues for the OSPF protocol.

6. Authors Address

Mitchell Erblich
erblichs@earthlink.net

"Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights."

"This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE

INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED
WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."