                         Optional Checksums in
            Intermediate System to Intermediate System (ISIS)

Status of this Memo

Copyright Notice

Abstract

   This document describes an optional extension to the Intermediate
   System to Intermediate System (ISIS) protocol, used today by several
   Internet Service Proviers (ISPs) for routing within their clouds.
   ISIS is an interior gateway routing protocol developed originally by
   OSI and used with IP extensions as Interior Gateway Protocol (IGP).
   ISIS originally does not provide Complete Sequence Numbers Protocol
   Data (CSNP) and Partial Sequence Numbers Protocol Data Unit (PSNP)
   checksums, relying on the underlying layers to verify the integrity
   of information provided. Experience with the protocol shows that
   this precondition does not always hold and scenarios can be imagined
   that impact protocol functionality. This document introduces a new
   optional Type, Length and Value (TLV) providing checksums.

1. Introduction

   ISIS [ISO90, Cal90a, Cal90b] CSNPs and PSNPs and IIHs can be
   corrupted in case of faulty implementations of L2 hardware or lack of
   checksuming on a specific network technology. As a particularly ugly
   case, corruption of length and/or TLV length fields may lead to the
   generation of extensive numbers of "empty" LSPs in the receiving
   node. Since we cannot rely on authentication as a checksum
   mechanism, this document proposes an optional TLV to add checksums to
   the elements.

   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 [Bra97].

2. TLV Description

   This optional TLV MAY BE included in all CSNP, PSNP and IIH packets
   and an implementation that implements optional checksums MUST accept
   PDUs if they do NOT contain the optional checksum. Implementations
   that receive an optional checksum TLV and support it MUST discard the
   PDU if the checksum is incorrect. An implementation that does NOT
   implement optional checksums MUST accept a PDU that contains the
   checksum TLV. An implementation that supports optional checksums and
   receives it within any other PDU than CSNP, PSNP or IIH MUST discard
   the PDU. Such an implementation MUST discard the PDU as well if more
   than one optional checksum TLVs are included within it.
   Additionally, any implementation supporting optional checksums MUST
   accept PDUs with an optional checksum with the value 0 and consider
   such a checksum as correct.
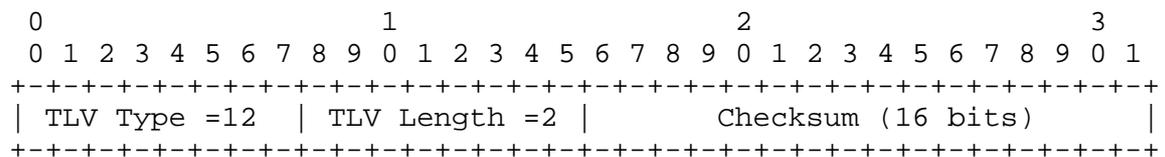
3. Checksum Computation

   The checksum is a fletcher checksum computed according to [ISO98],
   Annex C over the complete PDU. To compute the correct checksum, an
   implementation MUST add the optional checksum TLV to the PDU with the
   initial checksum value of 0 and compute the checksum over such a PDU.

4. Interaction with TLVs using PDU Data to Compute Signatures

   The implementation MUST either omit the optional checksum on an
   interface or send a 0 checksum value if it includes in the PDU
   signatures that provide equivalent or stronger functionality, such as
   HMAC or MD5. Otherwise an implementation that handles such
   signatures but does not handle the optional checksums, may fail to
   compute the MD5 signature on the packet. Such a failure would be
   caused by the fact that MD5 is computed with the checksum value set
   to 0 and only as a final step is the checksum value being filled in.

5. TLV Format

   [Prz01] lists the according value of the TLV type and discusses
   issues surrounding the assignment of new TLV codepoints.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | TLV Type =12  | TLV Length =2 |        Checksum (16 bits)     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

6. Acknowledgments

   Tony Li mentioned the original problem. Mike Shand provided
   comments. Somehow related problems with purging on LSP checksum
   errors have been observed by others before. Nischal Sheth spelled
   out the issues of interaction between MD5 and the optional checksums.

7. Security Considerations

   ISIS security applies to the work presented. No specific security
   issues as to the new element are known.

References

   [Bra97]   Bradner, S., "Key Words for Use in RFCs to Indicate
             Requirement Levels", BCP 14, RFC 2119, March 1997.

   [Cal90a] Callon, R., "OSI ISIS Intradomain Routing Protocol", RFC
             1142, February 1990.

   [Cal90b] Callon, R., "Use of OSI ISIS for Routing in TCP/IP and Dual
             Environments", RFC 1195, December 1990.

   [ISO90]   ISO. Information Technology - Telecommunications and
             Information Exchange between Systems - Intermediate System
             to Intermediate System Routing Exchange Protocol for Use in
             Conjunction with the Protocol for Providing the
             Connectionless-Mode Network Service. ISO, 1990.

   [ISO98]   ISO. Information Technology - Protocol for Providing the
             Connectionless-Mode Network Service: Protocol
             Specification. ISO, 1998.

   [Prz01]   Przygienda, T., "Reserved Type, Length and Value (TLV)
             Codepoints in Intermediate System to Intermediate System",
             RFC 3359, August 2002.

Author's Address

   Tony Przygienda
   Xebeo
   One Cragwood Road
   South Plainfield, NJ 07080

   Phone: (908) 222 4225
   Email: prz@xebeo.com

Full Copyright Statement

Acknowledgement