

Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 13, 2012

U. Chunduri
W. Lu
A. Tian
Ericsson Inc.
N. Shen
Cisco Systems, Inc.
March 12, 2012

IS-IS Extended Sequence number TLV
draft-chunduri-isis-extended-sequence-no-tlv-01

Abstract

This document defines Extended Sequence number TLV to protect Intermediate System to Intermediate System (IS-IS) PDUs from replay attacks.

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 13, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as

described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	4
1.2.	Acronyms	4
2.	Replay attacks and Impact on IS-IS networks	4
2.1.	Replay attacks	4
2.2.	Impact of Replays	5
3.	Extended Sequence Number TLV	5
3.1.	Sequence Number Wrap	7
4.	Packet Encoding	7
4.1.	IIHs	7
4.2.	LSPs	7
4.3.	SNPs	8
4.3.1.	CSNPs	8
4.3.2.	PSNPs	8
5.	IANA Considerations	8
6.	Security Considerations	8
7.	Acknowledgements	8
8.	Appendix A	9
8.1.	Appendix A.1	9
8.2.	Appendix A.2	9
9.	Appendix B	10
9.1.	Operational/Implementation consideration	10
10.	References	10
10.1.	Normative References	10
10.2.	Informative References	10
	Authors' Addresses	11

1. Introduction

With the rapid development of new data center infrastructures, due to its flexibility and scalability attributes, ISIS has been adopted widely in various L2 and L3 routing deployment of the data centers for critical business operations. At the meantime the SDN-enabled networks even though put more power to Internet applications and also make network management easier, it does raise the security requirement of network routing infrastructure to another level.

This document defines Extended Sequence number TLV to protect Intermediate System to Intermediate System (IS-IS) PDUs from replay attacks.

A replayed IS-IS PDU can potentially cause many problems in the IS-IS networks ranging from bouncing adjacencies to black hole or even some form of Denial of Service (DoS) attacks as explained in [Section 2](#). This problem is also discussed in security consideration section, in the context of cryptographic authentication work as described in [\[RFC5304\]](#) and in [\[RFC5310\]](#).

Currently, there is no mechanism to protect IS-IS HELLO PDUs (IIHs) and Sequence number PDUs (SNPs) from the replay attacks. However, Link State PDUs (LSPs) have sequence number in the LSP header as defined in [\[RFC1195\]](#), with which it can effectively mitigate the intra-session replay attacks. But, LSPs are still susceptible to inter-session replay attacks.

This document defines a new Extended Sequence Number (ESN) TLV to thwart these threats and can be deployed with authentication mechanism as specified in [\[RFC5304\]](#) and in [\[RFC5310\]](#) for a more secure network.

Replay attacks can be effectively mitigated by deploying a group key management protocol (similar to as defined in [I-D.weis-gdoi-mac-tek], using GDOI [\[I-D.ietf-msec-gdoi-update\]](#)) with a frequent key

change policy. Currently, there is no such mechanism defined for routing protocols and one of the KARP WG goals is to define such mechanism eventually. Even if such a mechanism is in use, usage of this TLV can be helpful to avoid replays before the keys are changed.

Also, it is believed, even when such key management system is deployed, there always will be some manual key based systems that co-exist with KMP (Key Management Protocol) based systems. The ESN TLV defined in this document is more helpful for such deployments.

[1.1.](#) Requirements Language

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 [RFC 2119](#) [[RFC2119](#)].

[1.2.](#) Acronyms

CSNP	-	Complete Sequence Number PDU
ESN	-	Extended Sequence Number
IIH	-	IS-IS Hello PDU
KMP	-	Key Management Protocol (auto key management)
LSP	-	IS-IS Link State PDU
MKM	-	Manual Key management Protocols
PSNP	-	Partial Sequence Number PDU
SNP	-	Sequence Number PDU

[2.](#) Replay attacks and Impact on IS-IS networks

This section explains the replay attacks and the applicability of the same for IS-IS networks. Though this has been described in detail in

KARP IS-IS gap analysis document, it is being restated below for completeness.

[2.1.](#) Replay attacks

Replaying a captured protocol packet to cause damage is a common threat for any protocol. Securing the packet with cryptographic authentication information alone can not mitigate this threat completely.

In intra-session replay attacks, a secured protocol packet of the current session is replayed, can cause damage if there is no other mechanism to confirm this is a replayed packet.

In inter-session replay attacks, captured packet from one of the previous session can be replayed to cause the damage. IS-IS packets are vulnerable to both these attacks as there is no sequence number verification for IIH packets, SNP packets and limited protection for LSPs.

[2.2.](#) Impact of Replays

At the time of adjacency bring up an IS sends IIH packet with empty neighbor list (TLV 6) and with or without the authentication information as per provisioned authentication mechanism. If this packet is replayed later on the broadcast network all ISes in the broadcast network can bounce the adjacency to create a huge churn in the network.

Today Link State PDUs (LSPs) have intra-session replay protection as LSP header contains 32-bit sequence number which is verified for every received packet against the local LSP database. But, if the key is not changed, an adversary can cause an inter-session replay attack by replaying a old LSP with higher sequence number and fewer prefixes or fewer adjacencies. This forces the receiver to accept and remove the routes from the routing table, which eventually causes traffic disruption to those prefixes.

In broadcast networks a replayed Complete Sequence Number packet (CSNP) can force the receiver to request Partial Sequence Number packet (PSNP) in the network and similarly, a replayed PSNP can cause unnecessary LSP flood in the network.

Please refer KARP IS-IS gap analysis document for further details.

3. Extended Sequence Number TLV

The Extended Sequence Number (ESN) TLV is composed of 1 octet for the Type, 1 octet that specifies the number of bytes in the Value field and an 8 or 12 byte Value field.

x CODE - TBD.

x LENGTH - total length of the value field, which is 12 bytes for IIH, SNP PDUs and 8 bytes for LSPs.

x Value - 64-bit Extended Session Sequence Number (ESSN), which is present for all IS-IS PDUs followed 32 bit monotonically increasing per Packet Sequence Number (PSN). PSN is not required for LSPs.

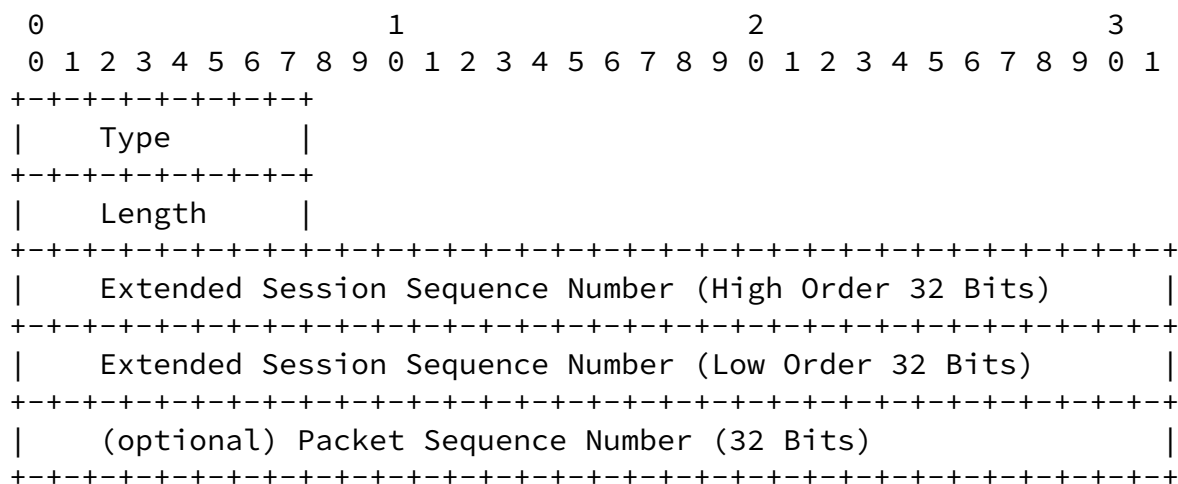


Figure 1: Extended Sequence Number (ESN) TLV

The Extended Sequence Number (ESN) TLV Type is TBD. Please refer to IANA Considerations, in [Section 5](#) for more details. Length indicates the length of the value field; which is 12 bytes for IIH and SNP PDUs and 8 bytes for LSPs.

In order to provide protection against both inter-session and intra-session replay attacks, the IS-IS Extended Session Sequence Number (ESSN) is defined a 64-bits value; the value MUST contain ever increasing number in all IS-IS PDUs including LSPs whenever it is changed due any situation as specified in [Section 3.1](#).

The 32-bit Packet Sequence Number (PSN) MUST be set and increase monotonically for IIH or SNP PDUs sent by IS-IS router. Upon reception, the Packet Sequence number MUST be greater than the last sequence number in the IIH or SNP PDUs accepted from the sending IS-IS router. Otherwise, the IIH or SNP PDU is considered as replayed PDU and dropped.

As LSPs contain 32-bit sequence number field already in the LSP header, Packet Sequence Number in the ESN TLV MUST be omitted by setting the length field to 8 bytes and implementations continue to refer the header sequence number for all encoding and validation purposes.

The ESN TLV defined here is optional. The ESN TLV MAY present in any IS-IS PDU. If present and authentication is in use this TLV MUST be included as part of the authentication data to calculate the digest. A sender MUST only transmit a single ESN TLV in a IS-IS PDU.

[3.1](#). Sequence Number Wrap

If the 32-bit Packet Sequence Number in ESN TLV and for LSPs the 32-bit header sequence number wraps; or session is refreshed; or even for the cold restarts the 64-bit ESSN value MUST be set higher than the previous value. IS-IS implementations MAY use guidelines provided in [Section 8](#) for accomplishing this.

[4.](#) Packet Encoding

The ESN TLV defined in this document is optional and the encoding and decoding of this TLV in each IS-IS PDU is as detailed below.

[4.1.](#) IIHs

The IIH ESN TLV information is maintained per IS-IS interface and per level. For a broadcast interface, it can have two sets of ESN TLV information, if the circuit belongs to both level-1 and level-2. For point-to-point (P2P) interface, only one ESN TLV information is needed. This TLV information can be maintained as part of the adjacency state.

While transmitting, the 64-bit ESSN MUST always be started with a non zero number and MAY use the guidelines as specified in [Section 8](#) to encode this 64-bit value. The 32-bit PSN starts from 1 and increases monotonically for every subsequent packet.

While receiving, the 64-bit ESSN MUST always be either same or higher than the stored value in the adjacency state. Similarly, the 32-bit PSN MUST be higher than the stored value in the adjacency state. If the PDU is accepted then the adjacency state should be updated with the last received IIH PDU's ESN TLV information.

For an adjacency refresh or the 32-bit PSN wrap the associated higher order 64-bit ESSN MUST always be higher than the previous value and the lower order 32-bit packet sequence number starts all over again.

[4.2.](#) LSPs

For LSPs, while originating, the 64-bit ESSN MUST always be started with a non zero number and MAY use the guidelines as specified in [Section 8](#) for encoding this value.

While receiving, the 64-bit Extended Sequence Number MUST always be either same or higher than the stored value in the LSP database. This document does not specify any changes for the existing LSP header 32-bit sequence number validation mechanism.

[4.3.](#) SNPs

[4.3.1.](#) CSNPs

In broadcast networks, only Designated Intermediate System (DIS) CSNP ESN TLV information is maintained per adjacency (per level) similar to IIH ESN TLV information. The procedure for encoding, verification and sequence number wrap scenarios are similar as explained in [Section 4.1](#), except separate DIS ESN TLV information should be used. In case of DIS change all adjacencies in the broadcast network MUST reflect new DIS's CSNP ESN TLV information in the adjacency and should be used for encoding/verification.

In P2P networks, CSNP ESN TLV information is maintained per adjacency similar to IIH ESN TLV information. The procedure for encoding, verification and sequence number wrap scenarios are similar as explained in [Section 4.1](#), except separate CSNP ESN TLV information should be used.

[4.3.2.](#) PSNPs

In both broadcast and P2P networks, PSNP ESN TLV information is maintained per adjacency (per level) similar to IIH ESN TLV information. The procedure for encoding, verification and sequence number wrap scenarios are similar as explained in [Section 4.1](#), except separate PSNP ESN TLV information should be used.

[5.](#) IANA Considerations

This document requests that IANA allocate from the IS-IS TLV Codepoints Registry a new TLV, referred to as the "Extended Sequence Number" TLV, with the following attributes: IIH = y, LSP = y, SNP = y, Purge = y.

[6.](#) Security Considerations

This document describes a mechanism to the replay attack threat as discussed in the Security Considerations section of [\[RFC5304\]](#) and in [\[RFC5310\]](#). This document does not introduce any new security concerns to IS-IS or any other specifications referenced in this document.

[7.](#) Acknowledgements

The authors of this document do not make any claims on the

originality of the ideas described. Authors are thankful for the review and the valuable feedback provided by Acee Lindem and Joel Halpern.

[8. Appendix A](#)

IS-IS routers implementing this specification SHOULD use available mechanisms to preserve the 64-bit Extended Session Sequence Number's strictly increasing property, when ever it is changed for the deployed life of the IS-IS router (including cold restarts).

This Appendix provides only guidelines for achieving the same and implementations can resort to any similar method as far as strictly increasing property of the 64-bit ESSN in ESN TLV is maintained.

[8.1. Appendix A.1](#)

One mechanism for accomplishing this is by encoding 64-bit ESSN as system time represented in 64-bit unsigned integer value. This MAY be similar to the system timestamp encoding for NTP long format as defined in [Appendix A.4 of \[RFC5905\]](#). New current time MAY be used when the IS-IS router loses its sequence number state including in Packet Sequence Number wrap scenarios.

Implementations MUST make sure while encoding the 64-bit ESN value with current system time, it should not default to any previous value or some default router time of the system; especially after cold restarts or any other similar events. In general system time must be preserved across cold restarts in order for this mechanism to be feasible. One example of such implemetation is to use a battery backed real-time clock (RTC).

[8.2. Appendix A.2](#)

One other mechanism for accomplishing this would be similar to the one as specified in [\[I-D.ietf-ospf-security-extension-manual-keying\]](#), to use the 64-bit ESSN as a wrap/boot count stored in non-volatile storage. This value is incremented anytime the IS-IS router loses its sequence number state including in Packet Sequence Number wrap scenarios.

The drawback of this approach per [Section 6](#) of [\[I-D.ietf-ospf-security-extension-manual-keying\]](#), if used is applicable here. The only drawback is, it requires the IS-IS implementation to be able to save its boot count in non-volatile storage. If the non-volatile

storage is ever repaired or upgraded such that the contents are lost, keys MUST be changed to prevent replay attacks.

[9. Appendix B](#)

[9.1. Operational/Implementation consideration](#)

Since the ESN is maintained per interface, per level and per packet type, this scheme can be useful for monitoring the health of the ISIS adjacency. A Packet Sequence Number skip on IIH can be recorded by the neighbors which can be used later to correlate with adjacency state changes over the interface. For instance in a multi-access media, all the neighbors have the skips from the same IIH sender or only one neighbor has the Packet Sequence Number skips can indicate completely different issues on the network.

[10. References](#)

[10.1. Normative References](#)

- [RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", [RFC 1195](#), December 1990.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5905] Mills, D., Martin, J., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", [RFC 5905](#), June 2010.

[10.2. Informative References](#)

- [I-D.ietf-karp-threats-reqs]
Lebovitz, G., Bhatia, M., and R. White, "The Threat Analysis and Requirements for Cryptographic Authentication of Routing Protocols' Transports", [draft-ietf-karp-threats-reqs-03](#) (work in progress), June 2011.
- [I-D.ietf-msec-gdoi-update]
Weis, B., Rowles, S., and T. Hardjono, "The Group Domain

of Interpretation", [draft-ietf-msec-gdoi-update-11](#) (work in progress), August 2011.

[I-D.ietf-ospf-security-extension-manual-keying]
Bhatia, M., Hartman, S., Zhang, D., and A. Lindem,
"Security Extension for OSPFv2 when using Manual Key
Management",
[draft-ietf-ospf-security-extension-manual-keying-00](#) (work
in progress), May 2011.

Chunduri, et al. Expires September 13, 2012 [Page 10]

Internet-Draft IS-IS Extended Sequence number TLV March 2012

[I-D.weis-gdoi-mac-tek]
Weis, B. and S. Rowles, "GDOI Generic Message
Authentication Code Policy", [draft-weis-gdoi-mac-tek-02](#)
(work in progress), March 2011.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic
Authentication", [RFC 5304](#), October 2008.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R.,
and M. Fanto, "IS-IS Generic Cryptographic
Authentication", [RFC 5310](#), February 2009.

[RFC6518] Lebovitz, G. and M. Bhatia, "Keying and Authentication for
Routing Protocols (KARP) Design Guidelines", [RFC 6518](#),
February 2012.

Authors' Addresses

Uma Chunduri
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
USA

Phone: 408 750-5678
Email: uma.chunduri@ericsson.com

Wenhu Lu
Ericsson Inc.
300 Holger Way,

San Jose, California 95134
USA

Email: wenhu.lu@ericsson.com

Albert Tian
Ericsson Inc.
300 Holger Way,
San Jose, California 95134
USA

Phone: 408 750-5210
Email: albert.tian@ericsson.com

Chunduri, et al. Expires September 13, 2012 [Page 11]

Internet-Draft IS-IS Extended Sequence number TLV March 2012

Naiming Shen
Cisco Systems, Inc.
225 West Tasman Drive,
San Jose, California 95134
USA

Email: naiming@cisco.com

