Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 10, 2015

U. Chunduri
W. Lu
A. Tian
Ericsson Inc.
N. Shen
Cisco Systems, Inc.
January 6, 2015

IS-IS Extended Sequence number TLV
draft-ietf-isis-extended-sequence-no-tlv-04

Abstract

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

Table of Contents

1. Introduction 2
1.1. Requirements Language 3
1.2. Acronyms 3
2. Replay attacks and Impact on IS-IS networks 4
2.1. IIHs 4
2.2. LSPs 4
2.3. SNPs 4
3. Extended Sequence Number TLV 4
3.1. Sequence Number Wrap 5
4. Mechanism and Packet Encoding 6
4.1. IIHs 6
4.2. SNPs 6
5. Backward Compatibility and Deployment 6
5.1. IIH and SNPs 7
6. IANA Considerations 7
7. Security Considerations 7
8. Contributors 7
9. Acknowledgements 7
10. Appendix A 8
10.1. Appendix A.1 8
10.2. Appendix A.2 8
11. Appendix B 9
11.1. Operational/Implementation consideration 9
12. References 9
12.1. Normative References 9
12.2. Informative References 9
Authors' Addresses 10

1. Introduction

With the rapid development of new data center infrastructures, due to its flexibility and scalability attributes, IS-IS has been adopted widely in various L2/L3 routing and switching deployment of the data centers and 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.

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 [ISO10589], with which it can effectively mitigate the intra-session replay attacks. But, LSPs are still susceptible to inter-session replay attacks.

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

The new ESN TLV defined here 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 (being developed as defined in [I-D.yeung-g-ikev2] and [I-D.hartman-karp-mrkmp]) with a frequent key change policy. Currently, there is no such mechanism defined for IS-IS. Even if such a mechanism is defined, 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

PDU - Protocol Data Unit

PSNP - Partial Sequence Number PDU

SNP - Sequence Number PDU

2. Replay attacks and Impact on IS-IS networks

Replaying a captured protocol packet to cause damage is a common threat for any protocol. Securing the packet with cryptographic authentication information alone cannot mitigate this threat completely. This section explains the replay attacks and the applicability of the same for each IS-IS PDU.

2.1. IIHs

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.

2.2. LSPs

Normal operation of the IS-IS update Process as specified in [ISO10589] provides timely recovery from all LSP replay attacks. Therefore the use of the extensions defined in this document are prohibited in LSPs. Further discussion of the vulnerability of LSPs to replay attacks can be found in [I-D.ietf-karp-isis-analysis].

2.3. SNPs

A replayed CSNP can result in the sending of unnecessary PSNPs on a given link. A replayed CSNP or PSNP can result in unnecessary LSP flooding on the link.

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 a 12 byte Value field. This TLV is defined only for IIH and SNP PDUs.

x CODE - TBD.

x LENGTH - total length of the value field, which is 12 bytes.

x Value - 64-bit Extended Session Sequence Number (ESSN), which is followed by a 32 bit monotonically increasing per Packet Sequence Number (PSN).

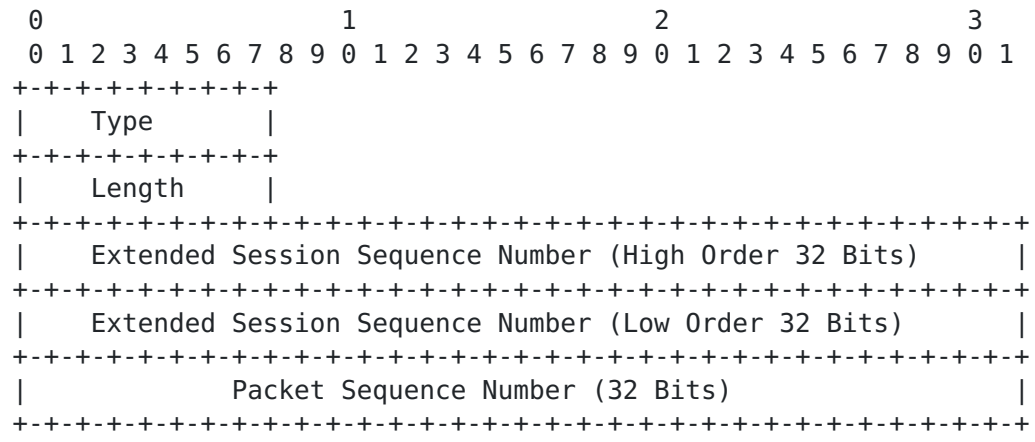

Figure 1: Extended Sequence Number (ESN) TLV

The ESN TLV defined here is optional. Though this is an optional TLV, this can be mandatory on a link when 'verify' mode is enabled as specified in Section 5.1. The ESN TLV MAY be present only in any IIH and SNP PDUs. A PDU with multiple ESN TLVs is invalid and MUST be discarded on receipt.

The 64 bit ESSN MUST be non-zero and MUST contain ever increasing number whenever it is changed due any situation as specified in Section 3.1. For each PDU which contains the ESN TLV the 96 bit unsigned integer value consisting of the 64 bit ESSN and 32 bit Packet Sequence Number (PSN) - where ESSN is the higher order 64 bits - MUST be greater than the most recently received value in a PDU of the same type originated by the same IS.

3.1. Sequence Number Wrap

If the 32-bit Packet Sequence Number in ESN TLV wraps or for the cold restart of the router, the 64-bit ESSN value MUST be set higher than the previous value. IS-IS implementations MAY use guidelines provided in Section 10 for accomplishing this.

4. Mechanism and Packet Encoding

The encoding of ESN TLV in each applicable IS-IS PDU is detailed below. Please refer to Section 5 for appropriate operations on how to inter-op with legacy node(s) that do not support the extensions defined in this document. If the received PDU with ESN TLV is accepted then the stored value for the corresponding originator and PDU type MUST be updated with the latest value received. Please note that level information is included in the PDU type.

4.1. IIHs

ESN TLV information is maintained for each type of IIH PDU being sent on a given circuit. The procedures for encoding, verification and sequence number wrap scenarios are explained in Section 3.

4.2. SNPs

A separate CSNP/PSNP ESN TLV information is maintained per PDU type, per originator and per link. The procedures for encoding, verification and sequence number wrap scenarios are explained in Section 3.

5. Backward Compatibility and Deployment

The implementation and deployment of the ESN TLV can be done to support backward compatibility and gradual deployment in the network without requiring a flag day. This feature can also be deployed for the links in a certain area of the network where the maximum security mechanism is needed, or it can be deployed for the entire network.

The implementation SHOULD allow the configuration of ESN TLV feature on each IS-IS link level. The implementation SHOULD also allow operators to control the configuration of 'send' and/or 'verify' the feature of IS-IS PDUs for the links and for the node. In this document, the 'send' operation is to include the ESN TLV in its own IS-IS PDUs; and the 'verify' operation is to process the ESN TLV in the receiving IS-IS PDUs from neighbors.

In the face of an adversary doing an active attack, it is possible to have inconsistent data view in the network, if there is a considerable delay in enabling ESN TLV 'verify' operation from first node to the last node in the network. This can happen primarily because, replay PDUs can potentially be accepted by the nodes where 'verify' operation is still not provisioned at the time of the attack. To minimize such a window it is recommended that provisioning of 'verify' SHOULD be done in a timely fashion by the network operators.

5.1. IIH and SNPs

On the link level, ESN TLV involves the IIH PDUs and SNPs (both CSNP and PSNP). The "send" and "verify" modes described above can be set independently on each link and in the case of a broadcast network independently for each level.

To introduce ESN support without disrupting operations, ISs on a given interface are first configured to operate in 'send' mode. Once all routers operating on an interface are operating in 'send' mode 'verify' mode can be enabled on each IS. Once 'verify' mode is set for an interface all the IIH and SNP PDUs being sent on that interface MUST contain the ESN TLV. Any such PDU received without an ESN TLV MUST be discarded when 'verify' mode is enabled

6. 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:

Type	Description	IIH	LSP	SNP	Purge
TBD	ESN TLV	Y	N	Y	N

Figure 2: IS-IS Codepoints Registry Entry

7. 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.

8. Contributors

Authors would like to thank Les Ginsberg for his significant contribution in detailed reviews and suggestions.

9. Acknowledgements

As some sort of sequence number mechanism to thwart protocol replays is a old mechanism, authors of this document do not make any claims on the originality of the overall protection idea described. Authors are thankful for the review and the valuable feedback provided by Acee Lindem and Joel Halpern.

10. Appendix A

IS-IS nodes implementing this specification SHOULD use available mechanisms to preserve the 64-bit Extended Session Sequence Number's strictly increasing property, whenever it is changed for the deployed life of the IS-IS node (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.

10.1. 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 node 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 node 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 implementation is to use a battery backed real-time clock (RTC).

10.2. 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 node 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.

11. Appendix B

11.1. Operational/Implementation consideration

Since the ESN is maintained per interface, per level and per PDU type, this scheme can be useful for monitoring the health of the IS-IS 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. Effective usage of the TLV defined in this document for operational issues MAY also need more system information before making concrete conclusions and defining all that information is beyond the scope of this document.

12. References

12.1. Normative References

[ISO10589] International Organization for Standardization, "Intermediate system to intermediate system intra-domain-routing routine 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.

[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.

12.2. Informative References

[I-D.hartman-karp-mrkmp] Hartman, S., Zhang, D., and G. Lebovitz, "Multicast Router Key Management Protocol (MaRK)", draft-hartman-karp-mrkmp-05 (work in progress), September 2012.

[I-D.ietf-karp-isis-analysis] Chunduri, U., Tian, A., and W. Lu, "KARP IS-IS security analysis", draft-ietf-karp-isis-analysis-03 (work in progress), September 2014.

[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-11 (work in progress), November 2014.

[I-D.weis-gdoi-mac-tek]
Weis, B. and S. Rowles, "GDOI Generic Message Authentication Code Policy", draft-weis-gdoi-mac-tek-03 (work in progress), September 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

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

Email: naiming@cisco.com