Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 22, 2013

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

January 18, 2013

IS-IS Extended Sequence number TLV
draft-chunduri-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.

Status of this Memo

Copyright Notice

Table of Contents

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 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.

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 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

This section explains the replay attacks and the applicability of the same for 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 can not mitigate this threat completely. This has been described in detail in "Replay Attacks" section of KARP IS-IS gap analysis document [I-D.chunduri-karp-is-is-gap-analysis].

2.1. Impact of Replays

At the time of adjacency bring up an IS sends IIH packet with empty neighbor list (TLV 6) and with or with out 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 PDU 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. The more common pre-conditions for inter-session replay attacks with LSPs and the current in-built recovery mechanism, have been discussed in details in Section 2.3.1.1 of KARP IS-IS gap analysis document [I-D.chunduri-karp-is-is-gap-analysis]. This document does not propose any solution to completely mitigate the replay threat for LSPs as network can still recover reliably after processing a disruptive reply.

In broadcast networks a replayed Complete Sequence Number PDU (CSNP) can force the receiver to request Partial Sequence Number PDU (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 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 and applicable for IIH and SNP PDUs.

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).

```
 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
+-+-+-+-+-+-+-+-+
|    Type       |
+-+-+-+-+-+-+-+-+
|    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Extended Session Sequence Number (High Order 32 Bits)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Extended Session Sequence Number (Low Order 32 Bits)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Packet Sequence Number (32 Bits)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Extended Sequence Number (ESN) TLV

The Extended Sequence Number (ESN) TLV Type is TBD. Please refer to IANA Considerations, in Section 6 for more details. Length indicates the length of the value field; which is 12 bytes for IIH and SNP PDUs.

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 IIH and SNP PDUs 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 node. 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 node. Otherwise, the IIH or SNP PDU is considered as replayed PDU and dropped.

The ESN TLV defined here is optional. The ESN TLV MAY present only in any IIH and SNP PDUs. 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 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 9 for accomplishing this.

4. Mechanism and 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. Also refer, when to ignore processing of the ESN TLV as described in Section 5 for appropriate operation in the face of legacy node(s) in the network with out having this capability.

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 9 to encode this 64-bit value. The 32-bit PSN starts from 1 and increases monotonically for every subsequent PDU.

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. SNPs

4.2.1. 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.

4.2.2. 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. 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 it's 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). When the router software is upgraded to include this feature, the network operators can configure the IS-IS to 'send' the ESN TLV in it's IIH PDUs and SNPs for those IS-IS interfaces on the IS-IS area or level. When all the routers attached to the link or links have been upgraded with this feature, network operators can start to configure 'verify' on the IS-IS interfaces for all the routers sharing the same link(s). This way deployment can be done in

per link basis in the network. The operators may decide to only apply ESN TLV feature on some of the links in the network, or only on their multi-access media links.

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. 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, Joel Halpern and Les Ginsberg.

9. 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, when ever 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.

9.1. 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).

9.2. 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.

10. Appendix B

10.1. 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.

11. References

11.1. 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.

11.2. Informative References

[I-D.chunduri-karp-is-is-gap-analysis]
Chunduri, U., Tian, A., and W. Lu, "KARP IS-IS security gap analysis", draft-chunduri-karp-is-is-gap-analysis-03 (work in progress), October 2012.

[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-threats-reqs]
Lebovitz, G., Bhatia, M., and B. Weis, "Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements", draft-ietf-karp-threats-reqs-07 (work in progress), December 2012.

[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-02 (work in progress), April 2012.

[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