Internet Engineering Task Force (IETF)
Request for Comments: 8918
Updates: 5305, 6232
Category: Standards Track
ISSN: 2070-1721

L. Ginsberg
P. Wells
Cisco Systems
T. Li
Arista Networks
T. Przygienda
S. Hegde
Juniper Networks, Inc.

September 2020

Invalid TLV Handling in IS-IS

Abstract

The key to the extensibility of the Intermediate System to Intermediate System (IS-IS) protocol has been the handling of unsupported and/or invalid Type-Length-Value (TLV) tuples. Although there are explicit statements in existing specifications, deployment experience has shown that there are inconsistencies in the behavior when a TLV that is disallowed in a particular Protocol Data Unit (PDU) is received.

This document discusses such cases and makes the correct behavior explicit in order to ensure that interoperability is maximized.

This document updates RFCs 5305 and 6232.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8918.

Table of Contents

1. Introduction

The Intermediate System to Intermediate System (IS-IS) protocol [ISO10589] utilizes Type-Length-Value (TLV) encoding for all content in the body of Protocol Data Units (PDUs). New extensions to the protocol are supported by defining new TLVs. In order to allow protocol extensions to be deployed in a backwards compatible way, an implementation is required to ignore TLVs that it does not understand. This behavior is also applied to sub-TLVs [RFC5305], which are contained within TLVs.

Also essential to the correct operation of the protocol is having the validation of PDUs be independent from the validation of the TLVs contained in the PDU. PDUs that are valid must be accepted [ISO10589] even if an individual TLV contained within that PDU is not understood or is invalid in some way (e.g., incorrect syntax, data value out of range, etc.).

The set of TLVs (and sub-TLVs) that are allowed in each PDU type is documented in the "TLV Codepoints Registry" established by [RFC3563] and updated by [RFC6233] and [RFC7356].

This document is intended to clarify some aspects of existing specifications and, thereby, reduce the occurrence of non-conformant behavior seen in real-world deployments. Although behaviors specified in existing protocol specifications are not changed, the clarifications contained in this document serve as updates to [RFC5305] (see Section 3.3) and [RFC6232] (see Section 3.4).

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all

capitals, as shown here.

2. TLV Codepoints Registry

[RFC3563] established the IANA-managed "IS-IS TLV Codepoints Registry" for recording assigned TLV codepoints [TLV_CODEPOINTS]. The initial contents of this registry were based on [RFC3359].

The registry includes a set of columns indicating in which PDU types a given TLV is allowed:

IIH — TLV is allowed in Intermediate System to Intermediate System Hello (IIH) PDUs (Point-to-point and LAN)

LSP — TLV is allowed in Link State PDUs (LSPs)

SNP — TLV is allowed in Sequence Number PDUs (SNPs) (Partial Sequence Number PDUs (PSNPs) and Complete Sequence Number PDUs (CSNPs))

Purge — TLV is allowed in LSP Purges [RFC6233]

If "Y" is entered in a column, it means the TLV is allowed in the corresponding PDU type.

If "N" is entered in a column, it means the TLV is not allowed in the corresponding PDU type.

3. TLV Acceptance in PDUs

This section describes the correct behavior when a PDU that contains a TLV that is specified as disallowed in the "TLV Codepoints Registry" is received.

3.1. Handling of Disallowed TLVs in Received PDUs Other Than LSP Purges

[ISO10589] defines the behavior required when a PDU is received containing a TLV that is "not recognised". It states (see Sections 9.5 - 9.13):

> Any codes in a received PDU that are not recognised shall be ignored.

This is the model to be followed when a TLV that is disallowed is received. Therefore, TLVs in a PDU (other than LSP purges) that are disallowed MUST be ignored and MUST NOT cause the PDU itself to be rejected by the receiving IS.

3.2. Special Handling of Disallowed TLVs in Received LSP Purges

When purging LSPs, [ISO10589] recommends (but does not require) the body of the LSP (i.e., all TLVs) be removed before generating the purge. LSP purges that have TLVs in the body are accepted, though any TLVs that are present are ignored.

When cryptographic authentication [RFC5304] was introduced, this

looseness when processing received purges had to be addressed in order to prevent attackers from being able to initiate a purge without having access to the authentication key. Therefore, [RFC5304] imposed strict requirements on what TLVs were allowed in a purge (authentication only) and specified that:

> ISes MUST NOT accept purges that contain TLVs other than the authentication TLV.

This behavior was extended by [RFC6232], which introduced the Purge Originator Identification (POI) TLV, and [RFC6233], which added the "Purge" column to the "TLV Codepoints Registry" to identify all the TLVs that are allowed in purges.

The behavior specified in [RFC5304] is not backwards compatible with the behavior defined by [ISO10589]; therefore, it can only be safely enabled when all nodes support cryptographic authentication. Similarly, the extensions defined by [RFC6232] are not compatible with the behavior defined in [RFC5304]; therefore, they can only be safely enabled when all nodes support the extensions.

When new protocol behaviors are specified that are not backwards compatible, it is RECOMMENDED that implementations provide controls for their enablement. This serves to prevent interoperability issues and allow for non-disruptive introduction of the new functionality into an existing network.

3.3. Applicability to Sub-TLVs

[RFC5305] introduced sub-TLVs, which are TLV tuples advertised within the body of a parent TLV. Registries associated with sub-TLVs are associated with the "TLV Codepoints Registry" and specify in which TLVs a given sub-TLV is allowed. Section 2 of [RFC5305] is updated by the following sentence:

> As with TLVs, it is required that sub-TLVs that are disallowed MUST be ignored on receipt.

The existing sentence in Section 2 of [RFC5305]:

> Unknown sub-TLVs are to be ignored and skipped upon receipt.

is replaced by:

> Unknown sub-TLVs MUST be ignored and skipped upon receipt.

3.4. Correction to POI "TLV Codepoints Registry" Entry

An error was introduced by [RFC6232] when specifying in which PDUs the POI TLV is allowed. Section 3 of [RFC6232] states:

> The POI TLV SHOULD be found in all purges and MUST NOT be found in LSPs with a non-zero Remaining Lifetime.

However, the IANA section of the same document states:

> The additional values for this TLV should be IIH:n, LSP:y, SNP:n, and Purge:y.

The correct setting for "LSP" is "n". This document updates [RFC6232] by correcting that error.

This document also updates the previously quoted text from Section 3 of [RFC6232] to be:

> The POI TLV SHOULD be sent in all purges and MUST NOT be sent in LSPs with a non-zero Remaining Lifetime.

4. TLV Validation and LSP Acceptance

The correct format of a TLV and its associated sub-TLVs, if applicable, is defined in the document(s) that introduces each codepoint. The definition MUST include what action to take when the format/content of the TLV does not conform to the specification (e.g., "MUST be ignored on receipt"). When making use of the information encoded in a given TLV (or sub-TLV), receiving nodes MUST verify that the TLV conforms to the standard definition. This includes cases where the length of a TLV/sub-TLV is incorrect and/or cases where the value field does not conform to the defined restrictions.

However, the unit of flooding for the IS-IS Update process is an LSP. The presence of a TLV (or sub-TLV) with content that does not conform to the relevant specification MUST NOT cause the LSP itself to be rejected. Failure to follow this requirement will result in inconsistent LSP Databases on different nodes in the network that will compromise the correct operation of the protocol.

LSP Acceptance rules are specified in [ISO10589]. Acceptance rules for LSP purges are extended by [RFC5304] and [RFC5310] and are further extended by [RFC6233].

[ISO10589] also specifies the behavior when an LSP is not accepted. This behavior is _not_ altered by extensions to the LSP Acceptance rules, i.e., regardless of the reason for the rejection of an LSP, the Update process on the receiving router takes the same action.

5. IANA Considerations

IANA has added this document as a reference for the "TLV Codepoints Registry".

IANA has also modified the entry for the Purge Originator Identification TLV in the "TLV Codepoints Registry" to be IIH:n, LSP:n, SNP:n, and Purge:y.

The reference field of the Purge Originator Identification TLV has been updated to point to this document.

6. Security Considerations

As this document makes no changes to the protocol, there are no new

security issues introduced.

The clarifications discussed in this document are intended to make it less likely that implementations will incorrectly process received LSPs, thereby also making it less likely that a bad actor could exploit a faulty implementation.

Security concerns for IS-IS are discussed in [ISO10589], [RFC5304], and [RFC5310].

7. References

7.1. Normative References

[ISO10589] International Organization for Standardization, "Information technology -- Telecommunications and information exchange between systems -- Intermediate System to Intermediate System intra-domain routeing 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, November 2002.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3563] Zinin, A., "Cooperative Agreement Between the ISOC/IETF and ISO/IEC Joint Technical Committee 1/Sub Committee 6 (JTC1/SC6) on IS-IS Routing Protocol Development", RFC 3563, DOI 10.17487/RFC3563, July 2003, <https://www.rfc-editor.org/info/rfc3563>.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008, <https://www.rfc-editor.org/info/rfc5304>.

[RFC5305] Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, DOI 10.17487/RFC5305, October 2008, <https://www.rfc-editor.org/info/rfc5305>.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, DOI 10.17487/RFC5310, February 2009, <https://www.rfc-editor.org/info/rfc5310>.

[RFC6232] Wei, F., Qin, Y., Li, Z., Li, T., and J. Dong, "Purge Originator Identification TLV for IS-IS", RFC 6232, DOI 10.17487/RFC6232, May 2011, <https://www.rfc-editor.org/info/rfc6232>.

[RFC6233] Li, T. and L. Ginsberg, "IS-IS Registry Extension for Purges", RFC 6233, DOI 10.17487/RFC6233, May 2011, <https://www.rfc-editor.org/info/rfc6233>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[TLV_CODEPOINTS] IANA, "IS-IS TLV Codepoints", <https://www.iana.org/assignments/isis-tlv-codepoints/>.

7.2. Informative References

[RFC3359] Przygienda, T., "Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System", RFC 3359, DOI 10.17487/RFC3359, August 2002, <https://www.rfc-editor.org/info/rfc3359>.

[RFC7356] Ginsberg, L., Previdi, S., and Y. Yang, "IS-IS Flooding Scope Link State PDUs (LSPs)", RFC 7356, DOI 10.17487/RFC7356, September 2014, <https://www.rfc-editor.org/info/rfc7356>.

Acknowledgements

The authors would like to thank Alvaro Retana.

Authors' Addresses

Les Ginsberg
Cisco Systems

Email: ginsberg@cisco.com

Paul Wells
Cisco Systems

Email: pauwells@cisco.com

Tony Li
Arista Networks
5453 Great America Parkway
Santa Clara, CA 95054
United States of America

Email: tony.li@tony.li

Tony Przygienda
Juniper Networks, Inc.
1194 N. Matilda Ave
Sunnyvale, CA 94089
United States of America

Email: prz@juniper.net

Shraddha Hegde
Juniper Networks, Inc.
Embassy Business Park
Bangalore 560093
KA
India

Email: shraddha@juniper.net