TRILL Working Group
INTERNET-DRAFT
Intended status: Proposed Standard

Lucy Yong
Donald Eastlake
Sam Aldrin
Huawei Technologies
Jon Hudson
Brocade

Expires: July 12, 2014

January 13, 2014

Transport of TRILL Using Pseudowires
<draft-ietf-trill-o-pw-05.txt>

Abstract

This document specifies how to interconnect a pair of TRILL (Transparent Interconnection of Lots of Links) switch ports using pseudowires under existing TRILL and PWE3 (Pseudowire Emulation End-to-End) standards.

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Distribution of this document is unlimited. Comments should be sent to the authors.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html. The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Table of Contents

1. Introduction.....3
1.1 Conventions used in this document.....3

2. PWE3 Interconnection of TRILL Switches.....4
2.1 PWE3 Type Independent Details.....4
2.2 PPP PWE3 Transport of TRILL.....5

3. IANA Considerations.....7
4. Security Considerations.....7

Appendix A: Use of Other Pseudowire Types.....8
Appendix Z: Change History.....10

Acknowledgements.....12
Normative References.....12
Informative References.....13

Authors' Addresses.....14

1. Introduction

The TRILL (Transparent Interconnection of Lots of Links) protocol [RFC6325] provides optimal pair-wise data frame routing without configuration in multi-hop networks with arbitrary topology. TRILL supports multipathing of both unicast and multicast traffic. Devices that implement TRILL are called TRILL Switches or RBridges (Routing Bridges).

Links between TRILL Switches can be based on arbitrary link protocols, for example PPP [RFC6361], as well as Ethernet [RFC6325]. A set of connected TRILL Switches together form a TRILL campus which is bounded by end stations and layer 3 routers.

This document specifies how to interconnect a pair of TRILL Switch ports using a pseudowire under existing TRILL and PWE3 (Pseudowire Emulation End-to-End) standards.

1.1 Conventions used in this document

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 [RFC2119].

Acronyms used in this document include the following:

IS-IS - Intermediate System to Intermediate System [IS-IS]

MPLS - Multi-Protocol Label Switching

PPP - Point-to-Point Protocol [RFC1661]

PW - Pseudowire [RFC3985]

PWE3 - PW Emulation End-to-End

RBridge - Routing Bridge, an alternative name for a TRILL Switch

TRILL - Transparent Interconnection of Lots of Links [RFC6325]

TRILL Switch - A device implementing the TRILL protocol

2. PWE3 Interconnection of TRILL Switches

When a pseudowire is used to interconnect a pair of TRILL Switch ports, a PPP [RFC4618] pseudowire is used as described below. The pseudowire between such ports can be signaled [RFC4447] or manually configured. In this context, the TRILL Switch ports at the ends of the pseudowire are acting as native service processing elements (NSP [RFC3985]) and, assuming the pseudowires are over MPLS or IP [RFC4023] networks, as label switched or IP routers at the TRILL Switch ports.

Pseudowires provide transparent transport and the two TRILL Switch ports appear directly interconnected with a transparent link. With such an interconnection the TRILL adjacency over the link is automatically discovered and established through TRILL IS-IS control messages [RFC6327bis].

A pseudowire is carried over a packet switched network tunnel [RFC3985], for example, an MPLS or MPLS-TP label switched path tunnel in MPLS networks. Either a signaling protocol or manual configuration can be used to configure a label switched path tunnel between two TRILL Switch ports. This application needs no additions to the existing pseudowire standards.

2.1 PWE3 Type Independent Details

The sending pseudowire TRILL Switch port SHOULD map the inner priority of the TRILL Data packets being sent to the Traffic Class field of the pseudowire label [RFC5462] so as to minimize the probability that higher priority TRILL Data packets will be discarded due to excessive TRILL Data packets of lower priority. TRILL IS-IS PDUs critical to establishing and maintaining adjacency (Hello and MTU PDUs) SHOULD be sent with the Traffic Class that would be used for a priority 7 (maximum priority) TRILL Data packet while other TRILL IS-IS PDUs SHOULD be sent with the Traffic Class that would be used for a priority 6 TRILL Data packet. This minimizes the probability of other traffic interfering with these important control PDUs and causing false loss of adjacency or other control problems.

If a pseudowire supports fragmentation and re-assembly (a feature that have received little or no deployment), then there is no reason to do TRILL MTU testing on it and the pseudowire will not be a constraint on the TRILL campus wide MTU size (Sz) (see Section 4.3.1 [RFC6325]). If the pseudowire does not support fragmentation (the more common case), then the available TRILL IS-IS packet payload size over the pseudowire (taking into account MPLS encapsulation with a control word) or some lower value, MUST be used in helping to

determine MTU size (Sz) (see Section 5 [ClearCorrect]).

An intervening MPLS label switched router or similar packet switched network device has no awareness of TRILL. Such devices will not change the TRILL Header hop count.

2.2 PPP PWE3 Transport of TRILL

For a PPP pseudowire (PW type = 0x0007), the two TRILL Switch ports being connected are configured to form a pseudowire with PPP encapsulation [RFC4618]. After the pseudowire is established and TRILL use is negotiated within PPP, the two TRILL Switch ports appear directly connected with a PPP link [RFC1661] [RFC6361].

If pseudowire interconnection of two TRILL Switch ports is signaled [RFC4447], the initiating TRILL Switch port MUST attempt the connection set-up with pseudowire type PPP (0x0007).

Behavior for TRILL with a PPP pseudowire continues to follow that of TRILL over PPP as specified in Section 3 of [RFC6361].

The following figures show what a TRILL Data and TRILL IS-IS packet look like over such a pseudowire in the MPLS case assuming no TRILL Header extensions:

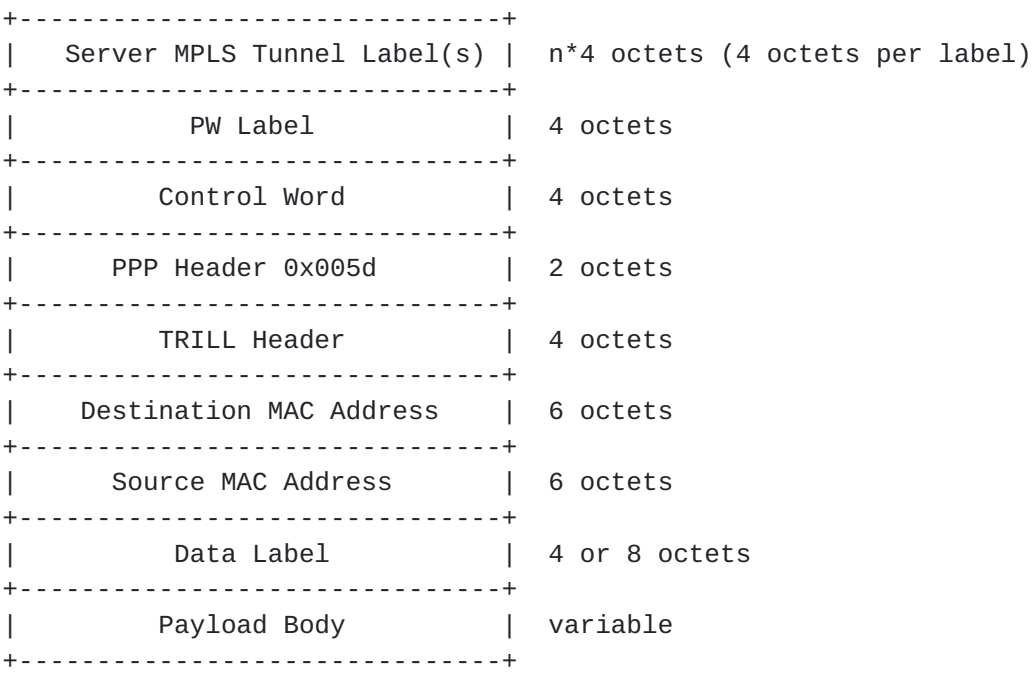


Figure 1. TRILL Data Packet in Pseudowire

"Data Label" is the VLAN Label or Fine Grained Label [FGL] of the payload.

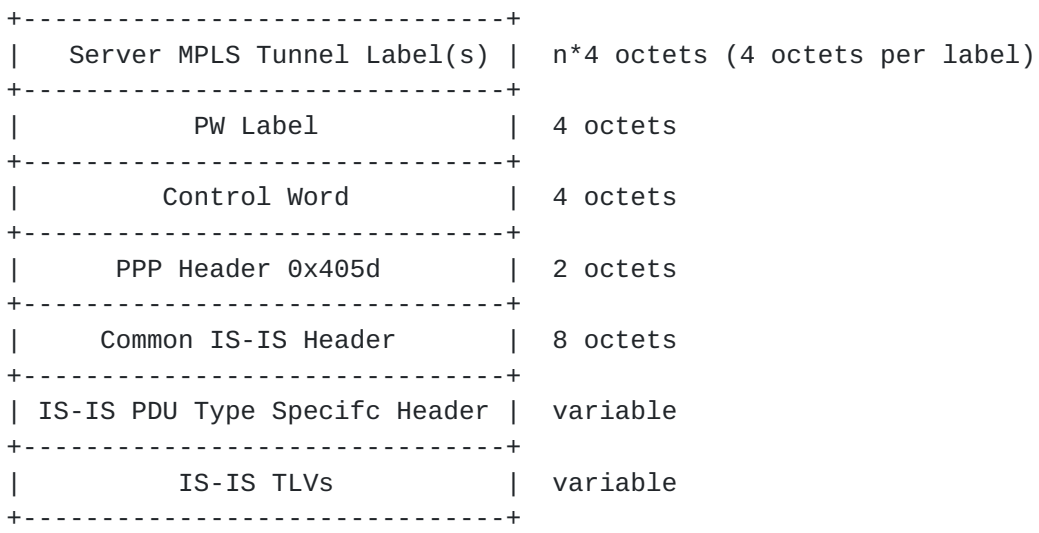


Figure 2. TRILL IS-IS Packet in Pseudowire

The PPP Header fields (0x005d and 0x405d respectively) for TRILL Data and IS-IS packets shown above are specified in [RFC6361].

3. IANA Considerations

No IANA actions are required by this document. RFC Editor: Please remove this section before publication.

4. Security Considerations

TRILL level secuirty mechanisms, such as the ability to use authentication with TRILL IS-IS PDUs [RFC6325], are not affected by link technology, such as the use of pseudowire links as specified in this document.

Link security may be useful in improving TRILL campus security. TRILL is transported over pseudowires as TRILL over PPP over pseudowires, pseudowires are over MPLS or IP, and MPLS and IP are over some lower level link technology. Thus link security below the TRILL level for a pseudowire link could be provided by PPP security, pseudowire security, MPLS or IP security, or security of the link technolgy supporting MPLS or IP.

PPP TRILL security considerations are discussed in [RFC6361]. For security considerations introduced by carrying PPP TRILL links over pseudowires, see [RFC3985], which discusses the risks introduced by sending protocols that previously assumed a point-to-point link on a pseudo wire built on a packet switched network (PSN). However, the PPP layer in TRILL transport by pseudowire is somewhat vestigial and intended primarily as a convenient way to use existing PPP code points to identify TRILL data packets and TRILL IS-IS packets. Furthermore, existing PPP security standards are arguably questionable in terms of current security criteria. For these reasons, it is NOT RECOMMENDED to use PPP security in the transport of TRILL by pseudowires as sepecified in this document.

It is RECOMMENDED that link security be provided at the layers supporting pseudowires transporting TRILL, that is, at the MPLS or IP layer or the link layer transporting MPLS or IP.

For applications involving sensitive data, end-to-end security should always be considered, in addition to link security, to provide security in depth. In this context, such end-to-end security should be between the end stations involved so as to protect the entire path to, through, and from the TRILL campus.

For general TRILL protocol security considerations, see [RFC6325].

Appendix A: Use of Other Pseudowire Types

This informational Appendix briefly discusses use of pseudowire types other than PPP for the transport of TRILL.

The use of Ethernet pseudowires [RFC4448] was examined by the authors and would be possible without change to such pseudowires; however, this would require an additional 12 or 16 bytes per packet within the payload being transmitted over the pseudowire as shown in the following figures for a TRILL Data and TRILL IS-IS packet over such an Ethernet pseudowire in the MPLS case assuming no TRILL Header extensions (compare with Figures 1 and 2):

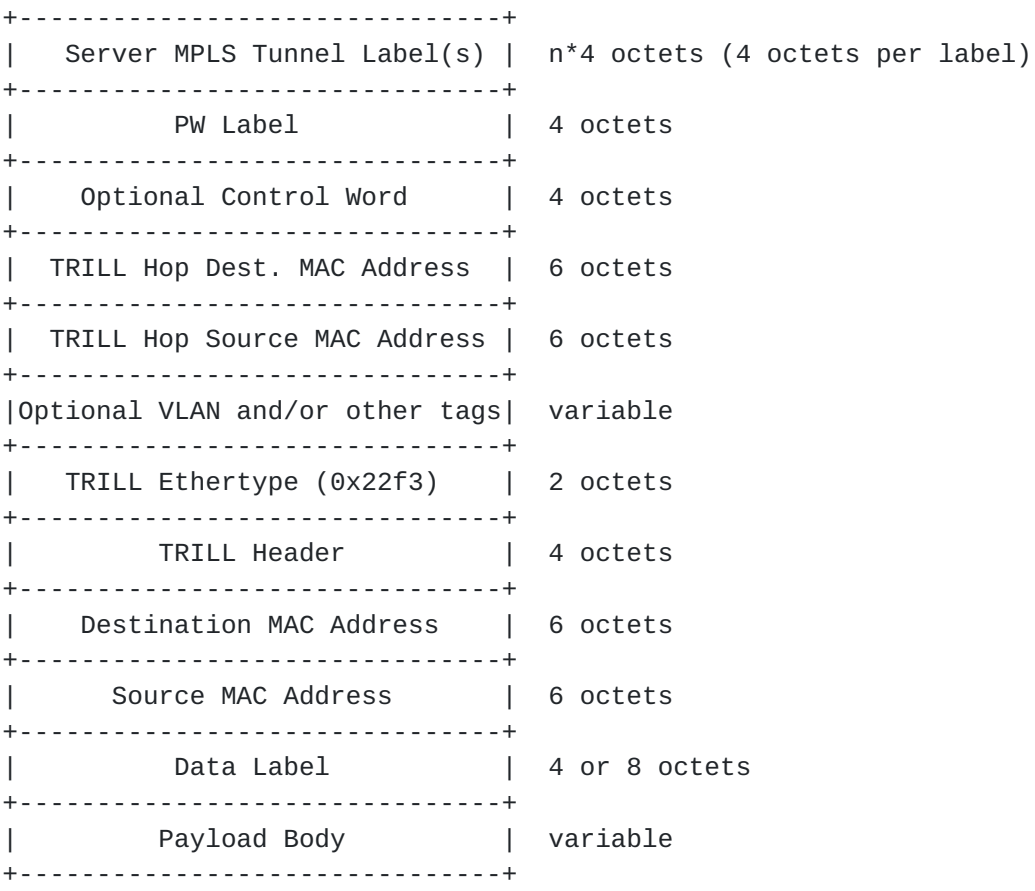


Figure 3. TRILL Data Packet in Ethernet Pseudowire

"Data Label" is the VLAN Label or Fine Grained Label [FGL] of the payload.

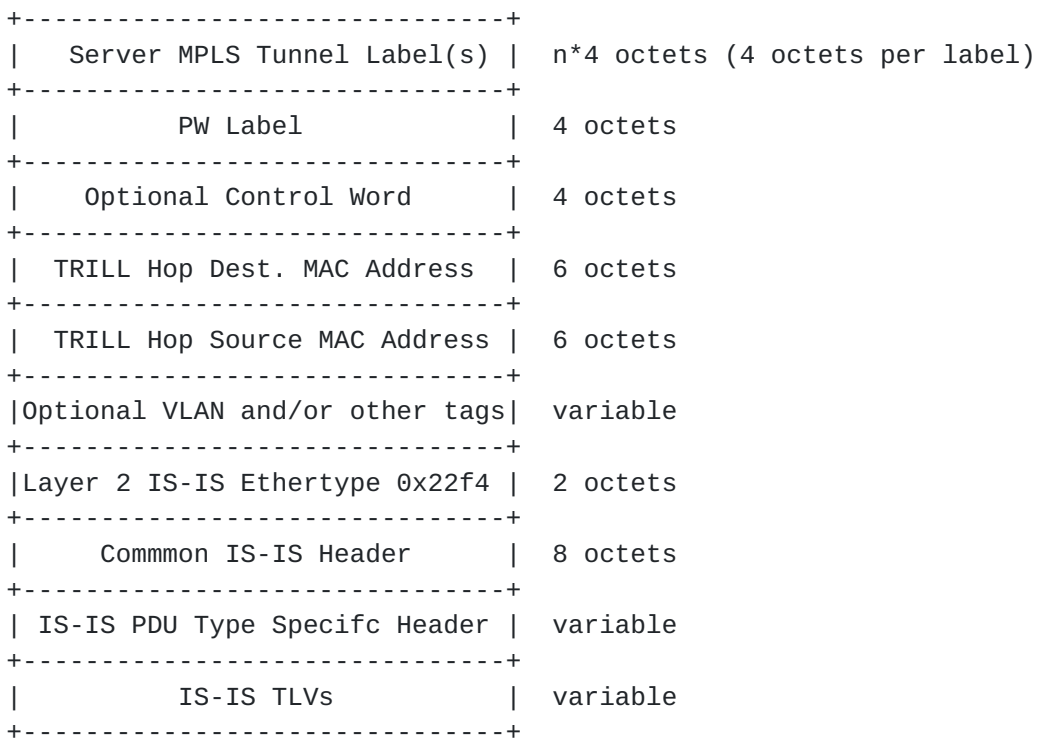


Figure 4. TRILL IS-IS Packet in Ethernet Pseudowire

It would also be possible to specify a new pseudowire type for TRILL traffic but the authors feel that any efficiency gain over PPP pseudowires would be too small to be worth the complexity of adding such a specification. Furthermore using PPP pseudowire encoding means that any traffic dissector that understands TRILL PPP encoding [RFC6361] and understands PPP pseudowires [RFC4618] will automatically be able to recursively decode TRILL transported by pseudowire.

Appendix Z: Change History

RFC Editor Note: Please remove this appendix prior to publication.

From -00 to -01

Add information on Traffic Classes that should be used for TRILL IS-IS PDUs.

Other changes to resolve WG Last Call comments:

- Change title from "TRILL Over Psuedowires".
- Change "Class of Service" to "Traffic Class".
- Expand informational paragraph about the consideration of using other pseudowire types for the transport of TRILL and make that paragraph into Appendix A.
- Add this Change History Appendix Z.

From -01 to -02

Add packet diagrams.

Minor editing changes.

From -02 to -03

Editorial and minor Security Considerations changes based on the Shepherd review by Erik Nordmark. See http://www.ietf.org/mail-archive/web/trill/current/msg06029.html and ensuing conversation.

From -03 to -04

Security Considerations changes based on SECDIR review.

Minor Editorial change to the first sentence of Section 1 based on GENART review.

Add final sentence to first paragraph of Section 2.1 to resolve COMMENT by Barry Leiba.

From -04 to -05

Assorted changes resulting from IESG review:

- Replace "autoconfigured" with "signaled".

Clarify that it is the inner TRILL Data packet priority that is used to determine pseudowire Traffic Class and that the priority is mapped to the Traffic Class.

Clarify that if Ethernet pseudowires were used no change would be required in the Ethernet pseudowire standard.

Expand "Sz" to "MTU size (Sz)".

Note that pseudowire fragmentation has little if any deployment.

Minor editorial improvements.

Acknowledgements

Thanks for the valuable comments from the following who are listed in alphabetic order:

Stewart Bryant, Stephen Farrell, Brain Haberman, Christer Holmberg, Joel Jaeggli, Barry Leiba, Erik Nordmark, Yaron Sheffer, and Yaakov (J) Stein

The document was prepared in raw nroff. All macros used were defined within the source file.

Normative References

[RFC1661] - Simpson, W., Ed., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC2119] - Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4447] - Martini, L., Ed., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

[RFC4618] - Martini, L., "Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks", BCP 116, RFC 4618, September 2006.

[RFC5462] - Andersson, L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, February 2009.

[RFC6325] - Perlman, R., Eastlake 3rd, D., Dutt, D., Gai, S., and A. Ghanwani, "Routing Bridges (RBridges): Base Protocol Specification", RFC6325, July 2011.

[RFC6361] - Carlson, J., and D. Eastlake, "PPP Transparent Interconnection of Lots of Links (TRILL) Protocol Control Protocol", RFC6361, August 2011.

[ClearCorrect] - Eastlake, D., M. Zhang, A. Ghanwani, V. Manral, and A. Banerjee, "TRILL: Clarifications, Corrections, and Updates", draft-ietf-trill-clear-correct, in RFC Editor's queue.

[FGL] - D. Eastlake, M. Zhang, P. Agarwal, R. Perlman, D. Dutt, "TRILL (Transparent Interconnection of Lots of Links): Fine-Grained Labeling", draft-ietf-trill-fine-labeling, in RFC

Editor's queue.

Informative References

[IS-IS] - International Organization for Standardization, "Intermediate system to Intermediate system intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)", ISO/IEC10589:2002, Second Edition, Nov 2002

[RFC3985] - Bryant, S., Ed., and P. Pate, Ed., "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.

[RFC4023] - Worster, T., Rekhter, Y., and E. Rosen, Ed., "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)", RFC 4023, March 2005.

[RFC4448] - Martini, L., Ed., Rosen, E., El-Aawar, N., and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks", RFC 4448, April 2006.

[RFC6327bis] - Eastlake 3rd, D., Perlman, R., Ghanwani, A., Howard, Y., and V. Manral, "TRILL: Adjacency", draft-ietf-trill-rfc6327bis, work in progress.

Authors' Addresses

Lucy Yong
Huawei Technologies
5340 Legacy Drive
Plano, TX 75025 USA

Phone: +1-469-227-5837
Email: lucy.yong@huawei.com

Donald E. Eastlake, 3rd
Huawei Technologies
155 Beaver Street
Milford, MA 01757 USA

Phone: +1-508-333-2270
Email: d3e3e3@gmail.com

Sam Aldrin
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95050 USA

Phone: +1-408-330-4517
Email: sam.aldrin@huawei.com

Jon Hudson
Brocade
130 Holger Way
San Jose, CA 95134 USA

Phone: +1-408-333-4062
jon.hudson@gmail.com

Copyright and IPR Provisions

Copyright (c) 2014 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. The definitive version of an IETF Document is that published by, or under the auspices of, the IETF. Versions of IETF Documents that are published by third parties, including those that are translated into other languages, should not be considered to be definitive versions of IETF Documents. The definitive version of these Legal Provisions is that published by, or under the auspices of, the IETF. Versions of these Legal Provisions that are published by third parties, including those that are translated into other languages, should not be considered to be definitive versions of these Legal Provisions. For the avoidance of doubt, each Contributor to the IETF Standards Process licenses each Contribution that he or she makes as part of the IETF Standards Process to the IETF Trust pursuant to the provisions of RFC 5378. No language to the contrary, or terms, conditions or rights that differ from or are inconsistent with the rights and licenses granted under RFC 5378, shall have any effect and shall be null and void, whether published or posted by such Contributor, or included with or in such Contribution.