Internet Engineering Task Force (IETF)
Request for Comments: 6361
Category: Standards Track
ISSN: 2070-1721
J. Carlson
WorkingCode
D. Eastlake 3rd
Huawei
August 2011

PPP Transparent Interconnection of Lots of Links (TRILL) Protocol Control Protocol

Abstract

The Point-to-Point Protocol (PPP) defines a Link Control Protocol (LCP) and a method for negotiating the use of multiprotocol traffic over point-to-point links. This document describes PPP support for the Transparent Interconnection of Lots of Links (TRILL) Protocol, allowing direct communication between Routing Bridges (RBridges) via PPP links.

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 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6361.

Copyright Notice

Copyright (c) 2011 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

The TRILL Protocol [RFC6325] defines a set of mechanisms used to communicate between RBridges. These devices can bridge together large 802 networks using link-state protocols in place of the traditional spanning tree mechanisms [RFC5556].

Over Ethernet, TRILL uses two separate Ethertypes to distinguish between encapsulation headers, which carry user data, and link-state messages, which compute network topology using a protocol based on [IS-IS] [RFC6326]. These two protocols must be distinguished from one another, and segregated from all other traffic.

In a network where PPP [RFC1661] is used to interconnect routers (often over telecommunications links), it may be advantageous to be able to bridge between Ethernet segments over those PPP links, and thus integrate remote networks with an existing TRILL cloud. The existing Bridging Control Protocol (BCP) [RFC3518] allows direct bridging of Ethernet frames over PPP. However, this mechanism is inefficient and inadequate for TRILL, which can be optimized for use over PPP links.

To interconnect these devices over PPP links, three protocol numbers are needed, and are reserved as follows:

Value (in hex)	Protocol Name
005d	TRILL Network Protocol (TNP)
405d	TRILL Link State Protocol (TLSP)
805d	TRILL Network Control Protocol (TNCP)

The usage of these three protocols is described in detail in the following section.

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 [RFC2119].

2. PPP TRILL Negotiation

The TRILL Network Control Protocol (TNCP) is responsible for negotiating the use of the TRILL Network Protocol (TNP) and TRILL Link State Protocol (TLSP) on a PPP link. TNCP uses the same option negotiation mechanism and state machine as described for LCP (Section 4 of [RFC1661]).

TNCP packets MUST NOT be exchanged until PPP has reached the Network-Layer Protocol phase. Any TNCP packets received when not in that phase MUST be silently ignored.

The encapsulated network layer data, carried in TNP packets, and topology information, carried in TLSP packets, MUST NOT be sent unless TNCP is in the Opened state. If a TNP or TLSP packet is received when TNCP is not in the Opened state and LCP is in the Opened state, an implementation MUST silently discard the unexpected TNP or TLSP packet.

2.1. TNCP Packet Format

Exactly one TNCP packet is carried in the PPP Information field, with the PPP Protocol field set to hex 805d (TNCP). A summary of the TNCP packet format is shown below. The fields are transmitted from left to right.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
+-+-+-+-+
```

Code

Only LCP Code values 1 through 7 (Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject, Terminate-Request, Terminate-Ack, and Code-Reject) are used. All other codes SHOULD result in a TNCP Code-Reject reply.

Identifier and Length

These are as documented for LCP.

Data

This field contains data formatted as described in Section 5 of [RFC1661]. Codes 1-4 use Type-Length-Data sequences, Codes 5 and 6 use uninterpreted data, and Code 7 uses a Rejected-Packet, all as described in [RFC1661].

Because no Configuration Options have been defined for TNCP, negotiating the use of the TRILL Protocol with IS-IS for the link state protocol is the default when no options are specified. A future document may specify the use of Configuration Options to enable different TRILL operating modes, such as the use of a different link state protocol.

2.2. TNP Packet Format

When TNCP is in the Opened state, TNP packets are sent by setting the PPP Protocol field to hex 005d (TNP) and placing TRILL-encapsulated data representing exactly one encapsulated packet in the PPP Information field.

A summary of this format is provided below:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| V | R |M|Op-Length| Hop Count | Egress (RB2) Nickname         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Ingress (RB1) Nickname        | Inner Destination MAC ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

This is identical to the TRILL Ethernet format (Section 4.1 of [RFC6325], "Ethernet Data Encapsulation"), except that the Outer MAC (Media Access Control) header and Ethertype are replaced by the PPP headers and Protocol Field, and the Ethernet Frame Check Sequence (FCS) is not present. Both user data and End-Station Address Distribution Information (ESADI) packets are encoded in this format.

The PPP FCS follows the encapsulated data on links where the PPP FCS is in use.

Unlike the TRILL Ethernet encapsulation, PPP nodes do not have MAC addresses, so no outer MAC is present. (High-Level Data Link Control (HDLC) addresses MAY be present in some situations; such usage is outside the scope of this document.)

2.3. TLSP Packet Format

When TNCP is in the Opened state, TLSP packets are sent by setting the PPP Protocol field to hex 405d (TLSP) and placing exactly one IS-IS Payload (Section 4.2.3 of [RFC6325], "TRILL IS-IS Frames") in the PPP Information field.

Note that point-to-point IS-IS links have only an arbitrary circuit ID, and do not use MAC addresses for identification.

3. TRILL PPP Behavior

1. On a PPP link, TRILL always uses point-to-point (P2P) Hellos. There is no need for TRILL-Hello frames, nor is per-port configuration necessary. P2P Hello messages, per "Point-to-Point IS to IS hello PDU" (Section 9.7 of [IS-IS]), do not use Neighbor IDs in the same manner as on Ethernet. However, per Section 4.2.4.1 of [RFC6325], the three-way IS-IS handshake using extended circuit IDs is required on point-to-point links, such as PPP.

2. RBridges are never appointed forwarders on PPP links. If an implementation includes BCP [RFC3518], then it MUST ensure that only one of BCP or TNCP is negotiated on a link, and not both. If the peer is an RBridge, then there is no need to pass unencapsulated frames, as the link can have no TRILL-ignorant peer to be concerned about. If the peer is not an RBridge, then TNCP negotiation fails and TRILL is not used on the link.

3. An implementation that has only PPP links might have no Organizationally Unique Identifier (OUI) that can form an IS-IS System ID. Resolving that issue is outside the scope of this document; however, it is strongly RECOMMENDED that all TRILL implementations have at least one zero-configuration mechanism to obtain a valid System ID. Refer to ISO/IEC 10589 [IS-IS] regarding System ID uniqueness requirements.

4. TRILL MTU-probe and TRILL MTU-ack messages (Section 4.3.2 of [RFC6325]) are not needed on a PPP link. Implementations MUST NOT send MTU-probe messages and SHOULD NOT reply to these messages. The MTU computed by LCP SHOULD be used instead. Negotiating an LCP MTU of at least 1524, to allow for an inner Ethernet payload of 1500 octets, is RECOMMENDED.

4. Security Considerations

Existing PPP and IS-IS security mechanisms may play important roles in a network of RBridges interconnected by PPP links. At the TRILL IS-IS layer, the IS-IS authentication mechanism [RFC5304] [RFC5310] prevents fabrication of link-state control messages.

Not all implementations need to include specific security mechanisms at the PPP layer, for example if they are designed to be deployed only in cases where the networking environment is trusted or where other layers provide adequate security. A complete enumeration of possible deployment scenarios and associated threats and options is not possible and is outside the scope of this document. For applications involving sensitive data, end-to-end security should always be considered in addition to link security to provide security in depth.

However, in case a PPP layer authentication mechanism is needed to protect the establishment of a link and identify a link with a known peer, implementation of the PPP Challenge Handshake Authentication Protocol (CHAP) [RFC1994] is RECOMMENDED. Should greater flexibility than that provided by CHAP be required, the Extensible Authentication Protocol (EAP) [RFC3748] is a good alternative.

If TRILL-over-PPP packets also require confidentiality, the PPP Encryption Control Protocol (ECP) link encryption mechanisms [RFC1968] can protect the confidentiality and integrity of all packets on the PPP link.

And when PPP is run over tunneling mechanisms, such as the Layer Two Tunneling Protocol (L2TP) [RFC3931], tunnel security protocols may be available.

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

5. IANA Considerations

IANA has assigned three PPP Protocol field values, 005d, 405d, and 805d, as described in Section 1 of this document.

IANA has created a new "PPP TNCP Configuration Option Types" registry in the PPP-Numbers registry, using the same format as the existing "PPP LCP Configuration Option Types" registry.

All TNCP Configuration Option Types except 0 are "Unassigned" and available for future use, based on "IETF Review", as described in BCP 26 [RFC5226]. Option 0 is allocated for use with Vendor-Specific Options, as described in [RFC2153].

6. References

6.1. 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.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC6325] Perlman, R., Eastlake 3rd, D., Dutt, D., Gai, S., and A. Ghanwani, "Routing Bridges (RBridges): Base Protocol Specification", RFC 6325, July 2011.

6.2. Informative References

[IS-IS] International Organization for Standardization, "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.

[RFC1968] Meyer, G., "The PPP Encryption Control Protocol (ECP)", RFC 1968, June 1996.

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[RFC2153] Simpson, W., "PPP Vendor Extensions", RFC 2153, May 1997.

[RFC3518] Higashiyama, M., Baker, F., and T. Liao, "Point-to-Point Protocol (PPP) Bridging Control Protocol (BCP)", RFC 3518, April 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed., "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, March 2005.

[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.

[RFC5556] Touch, J. and R. Perlman, "Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement", RFC 5556, May 2009.

[RFC6326] Eastlake, D., Banerjee, A., Dutt, D., Perlman, R., and A. Ghanwani, "Transparent Interconnection of Lots of Links (TRILL) Use of IS-IS", RFC 6326, July 2011.

7. Acknowledgements

The authors thank Jari Arkko, Stewart Bryant, Ralph Droms, Linda Dunbar, Adrian Farrel, Stephen Farrell, Radia Perlman, Mike Shand, and William A. Simpson for their comments and help.

Authors' Addresses

James Carlson
WorkingCode
25 Essex Street
North Andover, MA 01845 USA

Phone: +1-781-301-2471
EMail: carlsonj@workingcode.com

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

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