PPP TRILL Protocol Control Protocol
<draft-ietf-pppext-trill-protocol-00.txt>

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 PPP Extensions <pppext@ietf.org> or TRILL working group <rbridge@postel.org> mailing list.

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/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on April 12, 2010.

Abstract

The Point-to-Point Protocol (PPP) [1] defines a Link Control Protocol (LCP) and a method for negotiating the use of multi-protocol traffic over point-to-point links. This document describes support for Transparent Interconnection of Lots of Links (TRILL) Protocol, allowing direct communication between Routing Bridges (R Bridges) via PPP links.
1. Introduction

The TRILL Protocol [2] 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.

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 ISO IS-IS. These two protocols must be distinguished from one another, and segregated from all other traffic.

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

<table>
<thead>
<tr>
<th>Value (in hex)</th>
<th>Protocol Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD-00XX</td>
<td>TRILL Network Protocol (TNP)</td>
</tr>
<tr>
<td>TBD-40XX</td>
<td>TRILL Link State Protocol (TLSP)</td>
</tr>
<tr>
<td>TBD-80XX</td>
<td>TRILL Network Control Protocol (TNCP)</td>
</tr>
</tbody>
</table>

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 BCP 14 [3].

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 as LCP.

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 Opened state. If a TNP or TLSP packet is received when TNCP is not in Opened state and LCP is Opened, an implementation SHOULD respond using LCP Protocol-Reject.
2.1. TNCP Packet Format

Exactly one TNCP packet is carried in the PPP Information field, with the PPP Protocol field set to hex TBD-80XX (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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     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 in the same format as for the corresponding LCP Code numbers.

Because no configuration options have been defined for TNCP, negotiating the use of 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 Opened state, TNP packets may be sent by setting the PPP Protocol field to hex TBD-00XX (TNP) and placing the TRILL-encapsulated data in the PPP Information field.

A summary of this format is provided below:
This is identical to the Ethernet format except that the Outer MAC header and Ethertype are replaced by the PPP headers and Protocol Field. Both user data and ESADI packets are encoded in this format.

2.3. TLSP Packet Format

When TNCP is in Opened state, TLSP packets may be sent by setting the PPP Protocol field to hex TBD-40XX (TLSP) and placing the IS-IS Payload in the PPP Information field.

3. TRILL PPP Behavior

1. On a PPP link, TRILL always uses P2P Hellos. There is no need for TRILL-Hello frames, nor is per-port configuration necessary.

2. RBridges are never appointed forwarders on PPP links. If an implementation includes Bridging Control Protocol (BCP) [4], then it must ensure that only 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 nor to any TRILL-ignorant peer to be concerned about. If the peer is not an RBridge, then TRILL is not possible.

3. An implementation that has only PPP links might have no OUI that can form an IS-IS System ID. Resolving that issue is an implementation-dependent matter, but it is expected that, if at all possible, some means of minimizing the need for administrative configuration should be considered in order to accomplish the RBridge goal of zero configuration.

4. MTU-probe and MTU-ack messages are not needed on a PPP link. Implementations MUST NOT send MTU-probe 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

Both PPP authentication and IS-IS authentication mechanisms may play important roles in a network of RBridges interconnected by PPP links. The PPP authentication mechanism protects the establishment of a link, and identify a link with an known peer. The IS-IS mechanisms prevent fabrication of link-state control messages.

Implementors are encouraged to use these existing security mechanisms where appropriate.

5. IANA Considerations

IANA has assigned three similarly-numbered PPP Protocol field values, TBD-00XX, TBD-40XX, and TBD-80XX, as described in Section 1 of this document.

6. References


7. Acknowledgments

The author thanks Radia Perlman and Donald Eastlake for their comments and help.

8.  

8.1. PPP Working Group Chair

James Carlson
WorkingCode
25 Essex Street
8.2. Author

James Carlson
WorkingCode
Email: <carlsonj@workingcode.com>

9. Standard Notices


Copyright (c) 2009 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 in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

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.