

Network Working Group
Internet Draft
Expires in six months

Joel M. Halpern
Newbridge Networks Inc.
September 1994

PPP LCP Option for Data Encapsulation Selection
draft-ietf-pppext-dataencap-03.txt

Status of this Memo

This document is a submission to the Point-to-Point Protocol Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the `ietf-ppp@merit.edu` mailing list.

Distribution of this memo is unlimited.

This document is an Internet Draft. 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. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a ``working draft'' or ``work in progress.''

To learn the current status of any Internet-Draft, please check the ```1id-abstracts.txt`'' listing contained in the Internet-Drafts Shadow Directories on `ds.internic.net` (US East Coast), `nic.nordu.net` (Europe), `ftp.isi.edu` (US West Coast), or `munari.oz.au` (Pacific Rim).

Abstract

The Point-to-Point Protocol (PPP) [[1](#)] provides a standard method for transporting multi-protocol datagrams over point-to-point links.

This document defines a method for negotiating the encapsulation to be used for the transfer of data by PPP. It applies only to links for which there exists a "nominal" data encapsulation other than PPP.

DRAFT

Data Encapsulation Selection

September 1994

1. Introduction

PPP is defined in the base specification [1] as a set of encapsulations (syntax) and state machines (semantics). The use of this combination results in the robust negotiation of options and transmission of data over Point-to-Point links. PPP defines an extensible Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.

In recent years, several wide-area technologies with multi-point non-broadcast characteristics have developed. For each of these, data encapsulation syntax and operational semantics have been developed within the IETF ([2], [3], [4], [5]). The syntax used in each case was developed to meet a broad range of requirements. This syntax is herein referred to as the "nominal" encapsulation.

As work with these technologies has advanced, the desire for parameter negotiation and additional capabilities has become clear. Different techniques have been used in different cases. For X.25, for example, the solution was to use PPP over separate circuits from other encapsulations.

In the Frame-Relay case, that was considered insufficient. In particular, there was a desire to make use of the powerful PPP state machine and negotiation mechanism over Frame Relay circuits operating with previously defined syntax. Also, there was a desire to make the full power of the PPP machinery available to Frame Relay users.

The first step in doing this was to define how to carry PPP negotiation frames over Frame Relay. As the document on this [6] was discussed, it became clear that there was a further issue. The same encapsulation used to carry PPP negotiation frames is also used to carry PPP data frames. The question then arises as to the form of inter-operation. It is clearly desirable, when practical, that stations use uniform encapsulation.

The first step towards resolving this was taken in the PPP specifications for individual link technologies. As specified, for example in [6], when a PPP protocol NCP is negotiated, the data transfer takes place using the PPP data encapsulation for that NCP. This gives strong operation of the PPP NCP and data transfer mechanisms. For any protocol whose related NCP has not been negotiated, data can be exchanged using the "nominal" encapsulation.

This document defines an LCP option which, when negotiated, allows data to be transferred in the link "nominal" encapsulation even after the protocol NCP has been negotiated.

2. Nominal-Data-Encapsulation

Description

The LCP Nominal-Data-Encapsulation Configuration Option negotiates the use of the link nominal data encapsulation for NCP configured data, rather than the usual PPP encapsulation. If LCP reaches the Opened state without this option, the PPP protocol encapsulation is used for any protocol whose NCP is in the Opened state.

As with all LCP options, use of this option is at the discretion of the implementation and operator. A node cannot force another node to use an option, and correct operation of the link is expected to continue without the option, although the performance might be less than optimal.

Alternatively, such a node could open the LCP, but refuse to perform any NCP negotiations, so as to prevent the usage of any data encapsulations other than the nominal. Or, further, such a node could, after opening the LCP, close it again to indicate a desire NOT to communicate under the circumstances.

| These behaviors allow one to support the range of goals, including full operation of PPP over Frame Relay (as given in [6]), and support for minimal parameter negotiation in addition to [RFC 1490](#) support.

A summary of the Nominal-Data-Encapsulation Configuration Option format is shown below. The fields are transmitted from left to right.

```

      0                               1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |
+---+---+---+---+---+---+---+---+

```

Type

14

Length

2

Joel M. Halpern

expires in six months

[Page 2]

DRAFT

Data Encapsulation Selection

September 1994

3. Incompatibilities

The PPP LCP Protocol-Reject MUST not be generated, since the nominal protocols will not be recognized by PPP.

The PPP LCP Protocol-Field-Compression option MUST NOT be used, since ambiguities might result.

This option is incompatible with NCP options which affect the data transfer syntax. Generally, any NCP option which would change the way the data is sent for that NCP cannot be used if the Nominal-Data-Encapsulation option has been negotiated.

Some examples of facilities which MUST NOT be used:

- the Bridging CP option for Bridge LAN ID.
- the Compression CP, and any compression protocols defined for use by PPP.
- the IP CP option for header compression.
- the IPX CP option for header compression.

Other NCP options SHOULD be carefully examined before implementation of this option, and proper operation is not guaranteed.

4. Loss of State

There is a potential problem of undetected loss of shared state, as a result of the interaction between a PPP NCP and the use of nominal data encapsulation. When nominal encapsulation is used, either because the NCP has not been negotiated, or because the Nominal-Data-Encapsulation was negotiated, there is the possibility for invisible loss of shared state.

If the two sides have agreed to use the LCP Nominal-Data-Encapsulation option, then they will be exchanging data using an encapsulation which is not recognized by PPP. If the "remote" unit is then transparently reset or replaced, it could choose to send data without initiating any LCP (or NCP) negotiation. Since it would use the same data format, communication would appear to be taking place properly, when in fact the shared state does not exist.

This problem affects LCP shared state even in the absence of the LCP Nominal-Data-Encapsulation Configuration Option, since the nominal

encapsulation is used for any protocols for which no NCP has been negotiated. Thus, shared LCP state can be lost, even when no NCPs have been negotiated. The use of the Nominal-Data-Encapsulation option causes the problem to apply to shared NCP state as well. This includes such attributes as:

- address assignment for IP, IPX, AppleTalk, etc.
- routing protocol negotiation.
- broadcast suppression.

Virtually every NCP negotiation of naming or which affects choice of traffic over the link is subject to the problem of undetected loss of shared state.

Security Considerations

As outlined in the section on Loss of State, the use of the LCP Nominal-Data-Encapsulation option leaves the systems open to certain undetected restart or replacement scenarios.

In particular, the strength of the identity associated with any initial authentication protocol is weakened, since there is the possibility of replacement of the remote system transparently. Said replacement includes redirection of the underlying communications technology.

References

- [1] Simpson, W., Editor, "The Point-to-Point Protocol (PPP), [RFC 1548](#), 1993 December.
- [2] Piscitello, D.; Lawrence, J. Transmission of IP datagrams over the SMDS Service, [RFC 1209](#), 1991 March
- [3] Bradley, T.; Brown, C.; Malis, A. Multiprotocol Interconnect over Frame Relay, [RFC 1490](#), 1993 July.
- [4] Malis, A.; Robinson, D.; Ullmann, R. Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, [RFC 1356](#), 1992 August
- [5] Heinanen, J. Multiprotocol Encapsulation over ATM Adaptation Layer 5, [RFC 1483](#), 1993 July
- [6] Simpson, W. A. PPP in Frame Relay, Internet Draft

Acknowledgments

Joel M. Halpern expires in six months [Page 5]

DRAFT Data Encapsulation Selection September 1994

Chair's Address

The working group can be contacted via the current chair:

Fred Baker
Advanced Computer Communications
315 Bollay Drive
Santa Barbara, California 93117

EMail: fbaker@acc.com

Author's Address

Questions about this memo can also be directed to:

Joel M. Halpern
Newbridge Networks Inc.
593 Herndon Parkway
Herndon, VA 22070-5241

+1 703 708-5954

EMail: jhalpern@newbridge.com

<u>1.</u>	Introduction	<u>1</u>
<u>2.</u>	Nominal-Data-Encapsulation	<u>2</u>
<u>3.</u>	Incompatibilities	<u>3</u>
<u>4.</u>	Loss of State	<u>3</u>
	SECURITY CONSIDERATIONS	<u>5</u>
	REFERENCES	<u>5</u>
	ACKNOWLEDGEMENTS	<u>5</u>
	CHAIR'S ADDRESS	<u>6</u>
	AUTHOR'S ADDRESS	<u>6</u>