

The Point-to-Point Protocol (PPP)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP is comprised of three main components:

1. A method for encapsulating multi-protocol datagrams.
2. A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
3. A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

This document defines the PPP organization and methodology, and the PPP encapsulation, together with an extensible option negotiation mechanism which is able to negotiate a rich assortment of configuration parameters and provides additional management functions. The PPP Link Control Protocol (LCP) is described in terms of this mechanism.

Table of Contents

1.	Introduction	1
1.1	Specification of Requirements	2
1.2	Terminology	3
2.	PPP Encapsulation	4
3.	PPP Link Operation	6
3.1	Overview	6
3.2	Phase Diagram	6
3.3	Link Dead (physical-layer not ready)	7
3.4	Link Establishment Phase	7
3.5	Authentication Phase	8
3.6	Network-Layer Protocol Phase	8
3.7	Link Termination Phase	9
4.	The Option Negotiation Automaton	11
4.1	State Transition Table	12
4.2	States	14
4.3	Events	16
4.4	Actions	21
4.5	Loop Avoidance	23
4.6	Counters and Timers	24
5.	LCP Packet Formats	26

5.3	Configure-Nak	30
5.4	Configure-Reject	31
5.5	Terminate-Request and Terminate-Ack	33
5.6	Code-Reject	34
5.7	Protocol-Reject	35
5.8	Echo-Request and Echo-Reply	36
5.9	Discard-Request	37
6.	LCP Configuration Options	39
6.1	Maximum-Receive-Unit (MRU)	41
6.2	Authentication-Protocol	42
6.3	Quality-Protocol	43
6.4	Magic-Number	45
6.5	Protocol-Field-Compression (PFC)	48
6.6	Address-and-Control-Field-Compression (ACFC)	
	SECURITY CONSIDERATIONS	51
	REFERENCES	51
	ACKNOWLEDGEMENTS	51
	CHAIR'S ADDRESS	52
	EDITOR'S ADDRESS	52

1. Introduction

The Point-to-Point Protocol is designed for simple links which transport packets between two peers. These links provide full-duplex simultaneous bi-directional operation, and are assumed to deliver packets in order. It is intended that PPP provide a common solution for easy connection of a wide variety of hosts, bridges and routers [1].

Encapsulation

The PPP encapsulation provides for multiplexing of different network-layer protocols simultaneously over the same link. The PPP encapsulation has been carefully designed to retain compatibility with most commonly used supporting hardware.

Only 8 additional octets are necessary to form the encapsulation when used within the default HDLC-like framing. In environments where bandwidth is at a premium, the encapsulation and framing may be shortened to 2 or 4 octets.

To support high speed implementations, the default encapsulation uses only simple fields, only one of which needs to be examined for demultiplexing. The default header and information fields fall on 32-bit boundaries, and the trailer may be padded to an arbitrary boundary.

Link Control Protocol

In order to be sufficiently versatile to be portable to a wide variety of environments, PPP provides a Link Control Protocol (LCP). The LCP is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link. Other optional facilities provided are authentication of the identity of its peer on the link, and determination when a link is functioning properly and when it is failing.

Network Control Protocols

Point-to-Point links tend to exacerbate many problems with the current family of network protocols. For instance, assignment and management of IP addresses, which is a problem even in LAN

respective network-layer protocols. These NCPs are defined in companion documents.

Configuration

It is intended that PPP links be easy to configure. By design, the standard defaults handle all common configurations. The implementor can specify improvements to the default configuration, which are automatically communicated to the peer without operator intervention. Finally, the operator may explicitly configure options for the link which enable the link to operate in environments where it would otherwise be impossible.

This self-configuration is implemented through an extensible option negotiation mechanism, wherein each end of the link describes to the other its capabilities and requirements. Although the option negotiation mechanism described in this document is specified in terms of the Link Control Protocol (LCP), the same facilities are designed to be used by other control protocols, especially the family of NCPs.

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

- MUST** This word, or the adjective "required", means that the definition is an absolute requirement of the specification.
- MUST NOT** This phrase means that the definition is an absolute prohibition of the specification.
- SHOULD** This word, or the adjective "recommended", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighed before choosing a different course.
- MAY** This word, or the adjective "optional", means that this item is one of an allowed set of alternatives. An implementation which does not include this option **MUST** be prepared to interoperate with another implementation which does include the option.

1.2. Terminology

This document frequently uses the following terms:

- datagram** The unit of transmission in the network layer (such as IP). A datagram may be encapsulated in one or more packets passed to the data link layer.
- frame** The unit of transmission at the data link layer. A frame may include a header and/or a trailer, along with some number of units of data.
- packet** The basic unit of encapsulation, which is passed across the interface between the network layer and the data link layer. A packet is usually mapped to a frame: the

single frame.

peer The other end of the point-to-point link.

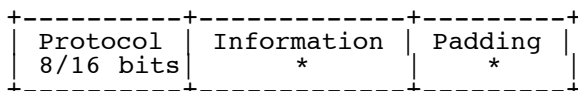
silently discard

The implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.

2. PPP Encapsulation

The PPP encapsulation is used to disambiguate multiprotocol datagrams. This encapsulation requires framing to indicate the beginning and end of the encapsulation. Methods of providing framing are specified in companion documents.

A summary of the PPP encapsulation is shown below. The fields are transmitted from left to right.



Protocol Field

The Protocol field is one or two octets, and its value identifies the datagram encapsulated in the Information field of the packet. The field is transmitted and received most significant octet first.

The structure of this field is consistent with the ISO 3309 extension mechanism for address fields. All Protocols MUST be odd; the least significant bit of the least significant octet MUST equal "1". Also, all Protocols MUST be assigned such that the least significant bit of the most significant octet equals "0". Frames received which don't comply with these rules MUST be treated as having an unrecognized Protocol.

Protocol field values in the "0****" to "3****" range identify the network-layer protocol of specific packets, and values in the "8****" to "b****" range identify packets belonging to the associated Network Control Protocols (NCPs), if any.

Protocol field values in the "4****" to "7****" range are used for protocols with low volume traffic which have no associated NCP. Protocol field values in the "c****" to "f****" range identify packets as link-layer Control Protocols (such as LCP).

Up-to-date values of the Protocol field are specified in the most recent "Assigned Numbers" RFC [2]. This specification reserves the following values:

Value (in hex)	Protocol Name
0001	Padding Protocol
0003 to 001f	reserved (transparency inefficient)
007d	reserved (Control Escape)
00cf	reserved (PPP NLPID)
00ff	reserved (compression inefficient)
8001 to 801f	unused
807d	unused
80cf	unused
80ff	unused
c021	Link Control Protocol
c023	Password Authentication Protocol
c025	Link Quality Report
c223	Challenge Handshake Authentication Protocol

Developers of new protocols MUST obtain a number from the Internet Assigned Numbers Authority (IANA), at IANA@isi.edu.

Information Field

The Information field is zero or more octets. The Information field contains the datagram for the protocol specified in the Protocol field.

The maximum length for the Information field, including Padding, but not including the Protocol field, is termed the Maximum Receive Unit (MRU), which defaults to 1500 octets. By negotiation, consenting PPP implementations may use other values for the MRU.

Padding

On transmission, the Information field MAY be padded with an arbitrary number of octets up to the MRU. It is the responsibility of each protocol to distinguish padding octets from real information.

3. PPP Link Operation

3.1. Overview

In order to establish communications over a point-to-point link, each end of the PPP link MUST first send LCP packets to configure and test the data link. After the link has been established, the peer MAY be authenticated.

Then, PPP MUST send NCP packets to choose and configure one or more network-layer protocols. Once each of the chosen network-layer protocols has been configured, datagrams from each network-layer

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.