Point to Point Protocol(PPP)

vkota1.@sycamores.indstate.edu

November 2015

1 Introduction

Point-to-point protocol is a Data link protocol that can be used to provide direct communication between any two communicating nodes which are intended to exchange data. Exchange of information can be done in the form of data packets. Point-to-Point protocol can be used to establish connection authentication, Compression and transmission encryption. The point-to-point connections which uses this protocol should be capable of supporting full-duplex communication. Many physical networks like phone line, serial cable, cellular telephone , trunk line, specialized radio links and fiber optics such as SONET uses PPP. PPP can also be used over internet access connections. Since IP data packets cannot be transmitted directly over a modem line without some data link protocol, Internet Service Providers have been using PPP for customer dial-up access to the internet. PPP can be fragmented into Encapsulation, Link Control Protocol(LCP) and Network Control Protocol(NCP).

2 History

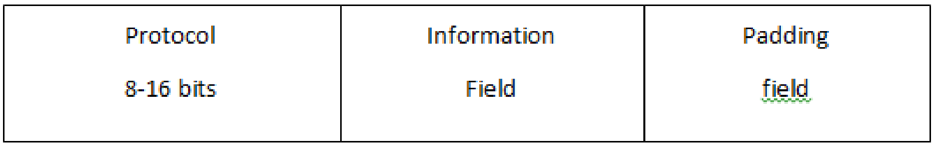
In the late 1980s, Serial Line Protocol (SLIP) is the de facto standard for serial IP implementation. It provides basic layer two framing for IP but it doesn't provide features such as reliability, security and high performance operation over serial links that users need since it frames the end of each datagram.To solve the problem in SLIP, an IETF document related to PPP was introduced,that is, RFC 1134. It was published in 1989. Another RFC is proposed which is RFC 1171 in 1990. It is the first mail PPP standard. This early document has been revised several times and several other documents added that define the protocols that comprises the entire PPP suite. PPP is made based on the High-Level- Data Link Control (HDLC) protocol but not developed from any other scratch. The general operation and framing structure of PPP is adapted from HDLC protocol.

3 Description

Point-to-point protocol is a Data link protocol that can be used to provide direct communication between any two communicating nodes which are intended to exchange data. Exchange of information can be done in the form of data packets. Point-to-Point protocol can be used to establish connection authentication, Compression and transmission encryption. The point-to-point connections which uses this protocol should be capable of supporting full-duplex communication. PPP can be fragmented into three parts: 1. Encapsulation 2. Link Control Protocol (LCP) 3. Network Control Protocol (NCP)

3.1 Encapsulation

PPP provides Encapsulation so that distinctive protocols at the network layer can be supported simultaneously. Frames are used for the transmission of data. Transmission of data is done from the left to right. Frames of PPP are encapsulated in a lower-layer protocol that provides framing and may provide other functions such as a checksum to detect transmission errors. PPP on serial links is usually encapsulated in a framing similar to HDLC.



Protocol 8-16 bits	Information Field	Padding field

Encapsulation Of PPP Packets

3.1.1 Protocol Field

Protocol field is maybe a couple bytes and it distinguishes the information being sent in the data field. All protocol qualities are odd numbers. The minimum critical bit of the lower byte is constantly set to “1” and that of the most critical bit is constantly set to “0”.Frames that disregard these guidelines are dealt with as unrecognized protocols. Few examples of protocol field values are: 0xC021 for Link control protocol 0xC023 for Password Authentication Protocol 0x8021 for Internet Protocol Control Protocol

3.1.2 Information Field

Information field is zero or more bytes long. Information field has a most extreme length (including padding and excluding protocol field) of 1500 bytes. This point of confinement is termed as the Maximum Receive unit (MRU) at the less than desirable end and Maximum Transmit Unit(MTU) at the transmitting end. The default field length is additionally 1500 bytes. Arrangements are conceivable between associates as to the MRU value.

3.1.3 Padding

Padding is a discretionary field. The data field may be padded with as numerous bytes as expected to achieve the MRU. Notwithstanding, both associates ought to have the capacity to perceive the padding bytes from the true data. This stage is discretionary when there is no such demand made.

3.2 Block Diagram

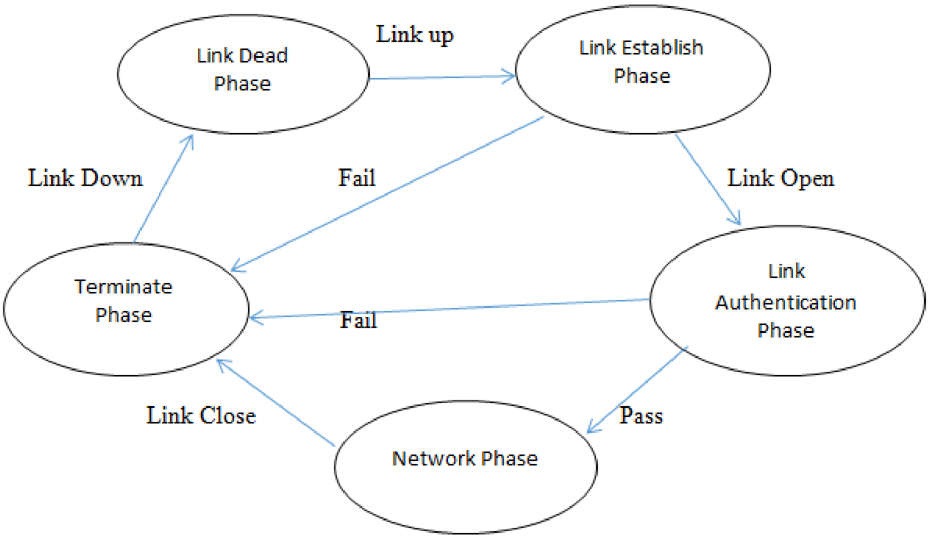
To build up correspondence between two associates, LCP packets should first be sent both approaches to arrange the connection. Any companion may ask for approval after connection arrangement. This stage is discretionary when there is no such demand made. Figure 1.2 demonstrates the stage outline that the connection goes through keeping in mind the end goal to bolster PPP.

The end of the connection foundation stage (or the confirmation stage as the case may be) triggers the following stage - the system stage. In this stage a Network Control Protocol (NCP) is initially chosen and afterward the connection can continue to comply with the principles of sending/accepting NCP bundles. A percentage of the accessible Network Layer Conventions (NLP) are ATCP (AppleTalk Control Protocol), IPCP (Internet Convention Control Protocol), Novell IPX Control Protocol, and so on. These conventions are like the LCP in message design, with changing subtle elements. It is at this layer, that messages can be sent to choose IP addresses. The connection stays open for correspondences until exceptional LCP/NCP bundles are sent to shut down the connection or different occasions trigger a shutdown (time out, human mediation, and so on.).

3.3 PPP Phases

3.3.1 Link Dead Phase

The connection/link begins and stops in this stage. The discovery of a transporter signal at the companion triggers the connection to continue to the following stage. Separating from the modem line ought to take the connection/link back to this stage.



Different Phases Of PPP

3.3.2 Link Establishment Phase

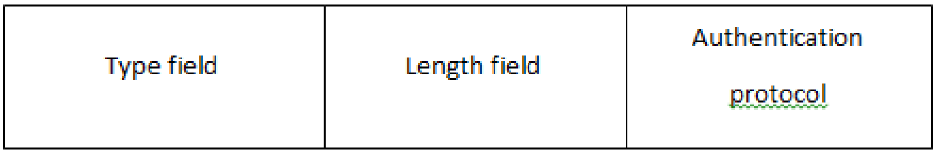
Once the vicinity of the associate/peer is recognized, the connection/link continues to this stage. In this Link Establishment Phase, the LCP sets up a solid association by trading configuration packets. After the connection arrangement has been assented upon, configure-Ack packets are sent and got. Arrangement choices have characterized default values, which can be changed amid this stage. These alternatives are free of the system layer convention being actualized. These choices are arranged between the companions taking into account the equipment and programming capacities at both the finishes. Other than LCP packets got amid this stage ought to be disposed of and logged. At the point when the connection is in the system layer convention (NLP) stage, getting a Configure-Request packets causes the connection to move back to the Link Establishment Phase. End of this Link Establishment phase the LCP open state.

3.3.3 Authentication Phase

Authentication phase is a discretionary stage. Before continuing to the NLP, an associate may demand confirmation or approval by the other associate. As a matter of course, this stage is discretionary. On the off chance that an associate solicitations validation, a solicitation must be issued during the connection/link establishment phase where setup alternatives are arranged. In the event that asked, this stage must be entered when join foundation is finished. It is conceivable that connection quality determination may happen amid this stage. On the off chance that connection quality determination should be performed while in the confirmation stage, suitable need levels ought to be given to the quality determination process. Entering the NLP, requires passing the confirmation stage. Coming up short at approval requires the connection to move to the end stage, strictly when a adequate number of fizzled endeavors. Just confirmation convention, LCP, and connection quality determination packets can be sent and got amid this stage. All other bundles got must be disposed of and logged. There are two sorts of authentication protocols that can be actualized.

Password Authentication Phase The Password Authentication Phase gives a simple execution of companion validation. It is just performed after the connection foundation stage. The companion over and over solicitations an ID/Password pair until verification is recognized. In the event that invalid validation is gotten after rehashed numerous solicitations, the connection is ended. This convention is not the most secure execution since passwords are sent with no encryption over the connections. There is no insurance from rehashed trial assaults to hack the password.

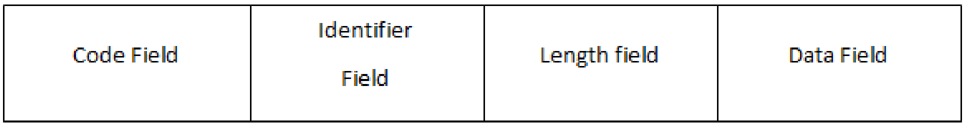
Configuration Option Figure below demonstrates the arrangement for the verification convention design alternative to demand PAP acceptance by the companion. In this arrangement,
Sort = 3
Length = 4
Authentication Protocol = 0xC023 for PAP



Type field	Length field	Authentication protocol

Configuration Format For PAP

Packet Format The non-specific PAP packet is appeared in Figure below. Every PPP frame houses one and only PAP packet in its data field. The field of protocol is set to 0xC023, held for the PAP. The code field is 1-byte wide and is either 1,2 or 3 relying upon whether an Authentication-Request, Authentication-Ack, or Authentication-Nak is being sent or got. Requests and replies are matched by making use of the identifier field(1-byte wide).The length of the PAP packets are held by the length fields(2-bytes wide), which incorporates every one of the fields transmitted (Code, length, identifier, and information fields).The length of data field is zero or more bytes wide and its substance relies on upon the code field substance (Request, Acknowledge or Not-Acknowledge).



Code Field	Identifier Field	Length field	Data Field

Configuration Format For PAP,LCP

Challenge-Handshake Authentication Protocol Not at all like the PAP, where confirmation/authentication is asked for just at the starting time of link establishment, the CHAP requires occasional companion acceptance. This is done at beginning connection/link establishment, and could likewise be asked for after connection/link establishment. The authenticator sends a test sign to the associate who reacts with a worth registered from an unpredictable calculation. This returned worth is thought about at the authenticator's end with its normal worth. In the event that the qualities coordinate, the companion is approved or else the connection/link is ended after a predetermined number of fizzled endeavors .This guarantees more noteworthy security in the usage. In the event that this protocol is executed, the protocol field esteem in the PPP edges has an estimation of 0xC223.

3.3.4 Network Layer Protocol Phase

1.4.4 Network Layer Protocol Phase: Once the Point to Point protocol has effectively gone through the authentication stage, the NLP stages must be configured (like the LCP phases). A few samples of NLPs are Internet Protocol (IP), AppleTalk (AT) and so on. The design of these NLPs is accomplished by actualizing the suitable NCPs. The comparing NCPs are Internet Protocol Control Protocol (IPCP) for IP, AppleTalk Control Convention (ATCP) for AT and so on. Each NCP can be opened and shut autonomously whenever. The RFC guidelines firmly suggest the evasion of settled timeouts while sitting tight for NCPs to design. This is because of the noteworthy dormancy included in puncturing through the join foundation stage (counting quality determination and conceivable validation). Any upheld NLP bundles got when the comparing NCP is shut are disposed of in the wake of logging. Packets which are unsupported by NLP must, in the LCP open state, be come back with a Protocol-Reject packets.

3.3.5 Link Termination Phase

The connection/link can be ended anytime of time. Link termination can happen because of any of the accompanying components-bearer can not be distinguished, confirmation disappointment, unmoving period time-out, human mediation or awful connection/link quality. The connection/link is closed down in the wake of sending and getting Terminate packets. Before closing down, PPP advises the upper NLPs so that fitting activity (end) is taken at all layers. Aa the trading of terminate packets are done, the execution shuts the physical-connect in this manner ending the connection. After sending a Terminate-Request, the requester sits tight for a Terminate-Ack or sits tight for a clock to lapse before real end. In like manner, the recipient of a Terminate-Request packet sits tight for the associate to detach or sits tight for no less than one time-out period in the wake of issuing a End Ack packet before detaching. Any non-LCP parcels got after the connection is ended are logged and tossed. Connection conclusion at the LCP level is adequate for end. It is most certainly not required that there be end at each NCP level. Conflictingly, each NCP conclusion is not adequate explanation behind connection end. The connection/link has now come to the connection/link dead phase once more.

3.4 Option Negotiation For LCP

Keeping in mind the end goal to achieve the open state and enter the NLP phase of the piece outline, an all around characterized limited state robot is depicted by the RFC. This is quickly talked about in this segment. The distinctive properties of this machine are occasions, activities and state moves, as with most limited state machines. Some definitions are given beneath for more clarity. An occasion is any outer event or order - for e.g., accepting packets from the associate, connection transparent close charges, time-out of the restart clock and so on. An even triggers the state machine to change state or stay in its current state. An activity is the result of the occasion. Cases of activities incorporate reinitializing the restart clock, sending bundles to the companion, activating connection/link status banners and so on. Each occasion need not make an activity be performed. A state move is the response of the state machine to an occasion. A state move may keep the machine in its present state. For instance, in the Closed state, getting a connection/link close occasion makes the state machine to stay in the Closed state without performing any activities.

3.5 LCP Packets

Packets of LCP can be classified into configuration packets, termination packets and maintenance packets. One and only LCP packet is packaged into the PPP data field. The protocol field in the PPP casing peruses 0xC021 (for LCP). The bland arrangement of a LCP packet is appeared in the figure. It is like that of the PAP packets.

Type of LCP packet is indicated by the code field. For instance, ConfigureRequest parcel has a code field of 1, Configure-Ack has a code field of 2, and so forth. The identifier as on account of the PAP packet coordinates the requests and replies.

The length of the LCP packet is held by the Length field including the code, identifier, length and information fields. This length is constrained by the MRU arranged.

The code field determines whether the data field is zero or more bytes. For e.g., when sending a Configure-Ack to the associate, the information field holds the design alternatives that can be arranged.

4 Advantages and Disadantages

4.1 Advantages

1. CHAP gives assurance against playback assault by the associate through the utilization of an incrementally changing identifier and a variable test esteem. 2. The utilization of rehashed difficulties is expected to restrain the season of introduction to any single assault. The authenticator is in control of the recurrence and timing of the difficulties. 3. This validation technique relies on a ”secret” known just to the authenticator and that associate. The secret is not sent over the connection. 4. In spite of the fact that the verification is one and only route, by arranging CHAP in both headings the same mystery set may effectively be utilized for shared confirmation. 5. Since CHAP may be utilized to confirm a wide range of frameworks, name fields may be utilized as a file to find the best possible mystery in a vast table of insider facts. This likewise makes it conceivable to bolster more than one name/secret pair per framework, and to change the secret being used whenever amid the session.

4.2 Disadvantages

1. CHAP requires that the secret be accessible in plaintext structure. Irreversibly encoded secret key databases ordinarily accessible can't be utilized. 2. It is not as helpful for expansive establishments, since every conceivable secret is kept up at both finishes of the connection.

Implementation Note To abstain from sending the secret over different connections in the system, it is suggested that the test and reaction qualities be analyzed at a focal server, as opposed to every system access server. Something else, the secret should be sent to such servers in a reversibly encoded structure. Either case requires a trusted relationship, which is outside the extent of this detail.

5 Conclusion

The point to point protocol (PPP) is a standard for imparting over the Web between two gatherings at the physical layer. Having experienced the dominant part of the RFC, I watched that despite the fact that the standard does not drive us to execute every one of the choices it records, it expects the usage to handle all decisions ought to the next associate require them.

This can further expand the multifaceted nature of the software.
The level of PPP programming executed on the WMI can effectively dial the Internet administration supplier (ISP), translate and convey LCP transaction packets to the ISP. The connection association is broken by the ISP after a period out period. Since this was not a noteworthy step towards the PPP objective, it was definitely not shown to the personnel or the faculty.

6 Reference

1. Simpson, W., Editor, "The Point-to-Point protocol(PPP)" , STD 51, RFC 1661, DayDreamer, July 1994.
2. Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, USC/Information Science Institute, October 1994.
3. Rivest, R., and S. Dusse, "The MD5 Message-Digest Algorithm", MIT Laboratory for Computer Science and RSA Data Security, Inc., RFC 1321, April 1992.