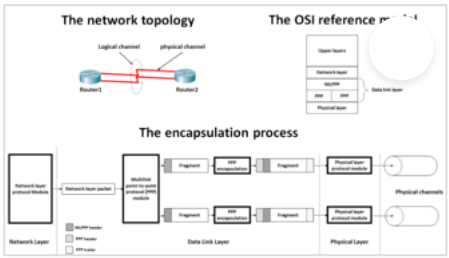
Point-to-Point Protocol

In computer networking, **Point-to-Point Protocol** (**PPP**) is a data link layer (layer 2) communication protocol between two routers directly without any host or any other networking in between.[1] It can provide loop detection, authentication, transmission encryption,[2] and data compression.



Point-to-Point Protocol

PPP is used over many types of physical networks, including serial cable, phone line, trunk line, cellular telephone, specialized radio links, ISDN, and fiber optic links such as SONET. Since IP packets cannot be transmitted over a modem line on their own without some data link protocol that can identify where the transmitted frame starts and where it ends, Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet.

PPP is used on former dial-up networking lines.[3] Two derivatives of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used most commonly by ISPs to establish a digital subscriber line (DSL) Internet service LP connection with customers.

Description

PPP is very commonly used as a data-link-layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older Serial Line Internet Protocol (SLIP) and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB) in the X.25 protocol suite). The only requirement for PPP is that the circuit provided be duplex. PPP was made to work with numerous network-layer protocols, including Internet Protocol (IP), TRILL, Novell's Internetwork Packet Exchange (IPX), NBF, DECnet and AppleTalk. Like SLIP, this is a full Internet connection over telephone lines via modem. It is more reliable than SLIP because it double checks to ensure Internet packets arrive intact.[4] It resends any damaged packets.

PPP was designed somewhat after the original HDLC specifications. The people who had designed PPP included many additional features that had been seen only in proprietary data-link protocols up to that time. PPP is specified in RFC 1661.

RFC 2516 describes Point-to-Point Protocol over Ethernet (PPPoE) as a method for transmitting PPP over Ethernet that is sometimes used with DSL. RFC 2364 describes Point-to-Point Protocol over ATM (PPPoA) as a method for transmitting PPP over ATM Adaptation Layer 5 (AAL5), which is also a common alternative to PPPoE used with DSL.

PPP, PPPoE and PPPoA are widely used in WAN lines.

PPP is a layered protocol that has three components:[4]

1. An encapsulation component that is used to transmit datagrams over the specified physical layer.

2. A Link Control Protocol (LCP) to establish, configure, and test the link as well as negotiate settings, options and the use of features.
3. One or more Network Control Protocols (NCP) used to negotiate optional configuration parameters and facilities for the network layer. There is one NCP for each higher-layer protocol supported by PPP.

Automatic self configuration

LCP initiates and terminates connections gracefully, allowing hosts to negotiate connection options. It is an integral part of PPP, and is defined in the same standard specification. LCP provides automatic configuration of the interfaces at each end (such as setting datagram size, escaped characters, and magic numbers) and for selecting optional authentication. The LCP protocol runs on top of PPP (with PPP protocol number 0xC021) and therefore a basic PPP connection has to be established before LCP is able to configure it.

RFC 1994 describes Challenge-Handshake Authentication Protocol (CHAP), which is preferred for establishing dial-up connections with ISPs. Although deprecated, Password Authentication Protocol (PAP) is still sometimes used.

Another option for authentication over PPP is Extensible Authentication Protocol (EAP) described in RFC 2284.

After the link has been established, additional network (layer 3) configuration may take place. Most commonly, the Internet Protocol Control Protocol (IPCP) is used, although Internetwork Packet Exchange Control Protocol (IPXCP) and AppleTalk Control Protocol (ATCP) were once popular.[5][6] Internet Protocol Version 6 Control Protocol (IPv6CP) will see extended use in the future, when IPv6 replaces IPv4 as the dominant layer-3 protocol.

Multiple network layer protocols

PPP permits multiple network layer protocols to operate on the same communication link. For every network layer protocol used, a separate **Network Control Protocol** (**NCP**) is provided in order to encapsulate and negotiate options for the multiple network layer protocols. It negotiates network-layer information, e.g. network address or compression options, after the connection has been established.

PPP architecture

LCP	CHAP	PAP	EAP	IPCP	IP
PPP encapsulation					
HDLC-like Framing				PPPoE	PPPoA
POS					
RS-232	SONET/SDH		Ethernet		ATM

For example, IP uses IPCP, and Internetwork Packet Exchange (IPX) uses the Novell IPX Control Protocol (**IPX/SPX**). NCPs include fields containing standardized codes to indicate the network layer protocol type that the PPP connection encapsulates.

The following NCPs may be used with PPP:

- IPCP for IP, protocol code number 0x8021, RFC 1332
- the OSI Network Layer Control Protocol (OSINLCP) for the various OSI network layer protocols, protocol code number 0x8023, RFC 1377
- the AppleTalk Control Protocol (ATCP) for AppleTalk, protocol code number 0x8029, RFC 1378
- the Internetwork Packet Exchange Control Protocol (IPXCP) for the Internet Packet Exchange, protocol code number 0x802B, RFC 1552

- the DECnet Phase IV Control Protocol (DNCP) for DNA Phase IV Routing protocol (DECnet Phase IV), protocol code number 0x8027, RFC 1762
- the NetBIOS Frames Control Protocol (NBFCP) for the NetBIOS Frames protocol (or NetBEUI as it was called before that), protocol code number 0x803F, RFC 2097
- the IPv6 Control Protocol (IPV6CP) for IPv6, protocol code number 0x8057, RFC 5072

Looped link detection

PPP detects looped links using a feature involving magic numbers. When the node sends PPP LCP messages, these messages may include a magic number. If a line is looped, the node receives an LCP message with its own magic number, instead of getting a message with the peer's magic number.

Configuration options

The previous section introduced the use of LCP options to meet specific WAN connection requirements. PPP may include the following LCP options:

- **Authentication** - Peer routers exchange authentication messages. Two authentication choices are Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Authentication is explained in the next section.
- **Compression** - Increases the effective throughput on PPP connections by reducing the amount of data in the frame that must travel across the link, using a agreed-on algorithm such as BSD compress or Deflate. The protocol decompresses the frame at its destination. See RFC 1962 (https://datatracker.ietf.org/doc/html/rfc1962) for more details.
- **Error detection** - Identifies fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link. The Magic Number field helps in detecting links that are in a looped-back condition. Until the Magic-Number Configuration Option has been successfully negotiated, the Magic-Number must be transmitted as zero. Magic numbers are generated randomly at each end of the connection.
- **Multilink** - Provides load balancing several interfaces used by PPP through Multilink PPP (see below).

PPP frame

Structure

PPP frames are variants of HDLC frames:

Name	Number of bytes	Description
Flag	1	0x7E, the beginning of a PPP frame
Address	1	0xFF, standard broadcast address
Control	1	0x03, unnumbered data
Protocol	2	PPP ID of embedded data
Information	variable (0 or more)	datagram
Padding	variable (0 or more)	optional padding
Frame Check Sequence	2	frame checksum
Flag	1	0x7E, omitted for successive PPP packets

If both peers agree to Address field and Control field compression during LCP, then those fields are omitted. Likewise if both peers agree to Protocol field compression, then the 0x00 byte can be omitted.

The Protocol field indicates the type of payload packet: 0xC021 for LCP, 0x80xy for various NCPs, 0x0021 for IP, 0x0029 AppleTalk, 0x002B for IPX, 0x003D for Multilink, 0x003F for NetBIOS, 0x00FD for MPPC and MPPE, etc.[7] PPP is limited, and cannot contain general Layer 3 data, unlike EtherType.

The Information field contains the PPP payload; it has a variable length with a negotiated maximum called the Maximum Transmission Unit. By default, the maximum is 1500 octets. It might be padded on transmission; if the information for a particular protocol can be padded, that protocol must allow information to be distinguished from padding.

Encapsulation

PPP frames 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, described by IETF RFC 1662.

Name	Number of bytes	Description
Flag	1	indicates frame's begin or end
Address	1	broadcast address
Control	1	control byte
Protocol	1 or 2 or 3	l in information field
Information	variable (0 or more)	datagram
Padding	variable (0 or more)	optional padding
FCS	2 (or 4)	error check

The Flag field is present when PPP with HDLC-like framing is used.

The Address and Control fields always have the value hex FF (for "all stations") and hex 03 (for "unnumbered information"), and can be omitted whenever PPP LCP Address-and-Control-Field-Compression (ACFC) is negotiated.

The frame check sequence (FCS) field is used for determining whether an individual frame has an error. It contains a checksum computed over the frame to provide basic protection against errors in transmission. This is a CRC code similar to the one used for other layer two protocol error protection schemes such as the one used in Ethernet. According to RFC 1662, it can be either 16 bits (2 bytes) or 32 bits (4 bytes) in size (default is 16 bits - Polynomial $x^{16} + x^{12} + x^5 + 1$).

The FCS is calculated over the Address, Control, Protocol, Information and Padding fields after the message has been encapsulated.

Line activation and phases

Link Dead
: This phase occurs when the link fails, or one side has been told to disconnect (e.g. a user has finished his or her dialup connection.)

Link Establishment Phase
: This phase is where Link Control Protocol negotiation is attempted. If successful, control goes either to the authentication phase or the Network-Layer Protocol phase, depending on whether authentication is desired.

Authentication Phase
: This phase is optional. It allows the sides to authenticate each other before a connection is established. If successful, control goes to the network-layer protocol phase.

Network-Layer Protocol Phase
: This phase is where each desired protocols' Network Control Protocols are invoked. For example, IPCP is used in establishing IP service over the line. Data transport for all protocols which are successfully started with their network control protocols also occurs in this phase. Closing down of network protocols also occur in this phase.

Link Termination Phase
: This phase closes down this connection. This can happen if there is an authentication failure, if there are so many checksum errors that the two parties decide to tear down the link automatically, if the link suddenly fails, or if the user decides to hang up a connection.

Over several links

Multilink PPP

Multilink PPP (also referred to as **MLPPP**, **MP**, **MPPP**, **MLP**, or Multilink) provides a method for spreading traffic across multiple distinct PPP connections. It is defined in RFC 1990. It can be used, for example, to connect a home computer to an Internet Service Provider using two traditional 56k modems, or to connect a company through two leased lines.

On a single PPP line frames cannot arrive out of order, but this is possible when the frames are divided among multiple PPP connections. Therefore, Multilink PPP must number the fragments so they can be put in the right order again when they arrive.

Multilink PPP is an example of a link aggregation technology. Cisco IOS Release 11.1 and later supports Multilink PPP.

Multiclass PPP

With PPP, one cannot establish several simultaneous distinct PPP connections over a single link.

That's not possible with Multilink PPP either. Multilink PPP uses contiguous numbers for all the fragments of a packet, and as a consequence it is not possible to suspend the sending of a sequence of fragments of one packet in order to send another packet. This prevents from running Multilink PPP multiple times on the same links.

Multiclass PPP is a kind of Multilink PPP where each "class" of traffic uses a separate sequence number space and reassembly buffer. Multiclass PPP is defined in RFC 2686

Tunnels

Derived protocols

PPTP (Point-to-Point Tunneling Protocol) is a form of PPP between two hosts via GRE using encryption (MPPE) and compression (MPPC).

Simplified OSI protocol stack for an example SSH+PPP tunnel

Application	FTP	SMTP	HTTP	…	DNS …
Transport	TCP				UDP
Network	IP				
Data Link	**PPP**				
Application	**SSH**				
Transport	TCP				
Network	IP				
Data Link	Ethernet				ATM
Physical	Cables, Hubs, and so on				

As a layer 2 protocol between both ends of a tunnel

Many protocols can be used to tunnel data over IP networks. Some of them, like SSL, SSH, or L2TP create virtual network interfaces and give the impression of direct physical connections between the tunnel endpoints. On a Linux host for example, these interfaces would be called **tuno** or **pppo**.

As there are only two endpoints on a tunnel, the tunnel is a point-to-point connection and PPP is a natural choice as a data link layer protocol between the virtual network interfaces. PPP can assign IP addresses to these virtual interfaces, and these IP addresses can be used, for example, to route between the networks on both sides of the tunnel.

IPsec in tunneling mode does not create virtual physical interfaces at the end of the tunnel, since the tunnel is handled directly by the TCP/IP stack. L2TP can be used to provide these interfaces, this technique is called L2TP/IPsec. In this case too, PPP provides IP addresses to the extremities of the tunnel.

IETF standards

PPP is defined in RFC 1661 (The Point-to-Point Protocol, July 1994). RFC 1547 (Requirements for an Internet Standard Point-to-Point Protocol, December 1993) provides historical information about the need for PPP and its development. A series of related RFCs have been written to define how a variety of network control protocols, including TCP/IP, DECnet, AppleTalk, IPX, work with PPP; they can be found on the Datatracker IETF website.[8]

See also

- Diameter
- Extensible Authentication Protocol
- Hayes command set
- Link Access Procedure for Modems (LAPM)
- Multiprotocol Encapsulation (MPE) for MPEG transport stream
- Point-to-Point Protocol daemon (PPPD)
- PPPoX
- RADIUS
- Unidirectional Lightweight Encapsulation (ULE) for MPEG transport stream

References

1. RFC 1661 (https://datatracker.ietf.org/doc/html/rfc1661)
2. RFC 1968 (https://datatracker.ietf.org/doc/html/rfc1968)
3. "41. Point-to-Point Protocol -- Dialup Networking", *Linux: Rute User's Tutorial and Exposition* (https://www.physics.udel.edu/~bnikolic/teaching/phys660/RUTE/rute/node44.html), retrieved 2024-08-20
4. Stevens 1994, pp. 26–27, sec 2.6: "PPP: Point-to-Point Protocol"
5. Simpson, William A. (December 1993). The PPP Internetworking Packet Exchange Control Protocol (IPXCP) (https://datatracker.ietf.org/doc/rfc1552/) (Report). Internet Engineering Task Force.
6. Parker, J. Bradford (November 1992). The PPP AppleTalk Control Protocol (ATCP) (https://datatracker.ietf.org/doc/rfc1378/) (Report). Internet Engineering Task Force.
7. "Point-to-Point (PPP) Protocol Field Assignments" (https://www.iana.org/assignments/ppp-numbers/ppp-numbers.xhtml). IANA. Retrieved 3 September 2015.
8. "IETF Datatracker" (https://datatracker.ietf.org/). Retrieved August 26, 2023.

- William Richard Stevens (2016) [1994]. *TCP/IP Illustrated* [*TCP/IP详解*]. Vol. 卷一：协议 (Volume 1: The Protocols) (1st ed.). Pearson Education Asia Ltd., 人民邮电出版社 (China Posts & Telecommunications Press). ISBN 978-7-115-40132-8.