# PPP

## POINT TO POINT PROTOCOL

### OVERVIEW OF THE PPP PROTOCOL SUITE FOR POINT TO POINT LINKS

Peter R. Egli
INDIGOO.COM

## Contents

## 1. SLIP (Serial Line IP, RFC1055) versus PPP

**SLIP is a predecessor of PPP.**
**SLIP was used as framing protocol over serial lines before the advent of PPP.**
**PPP was devised in order to overcome the deficiencies of SLIP.**

**SLIP framing:**

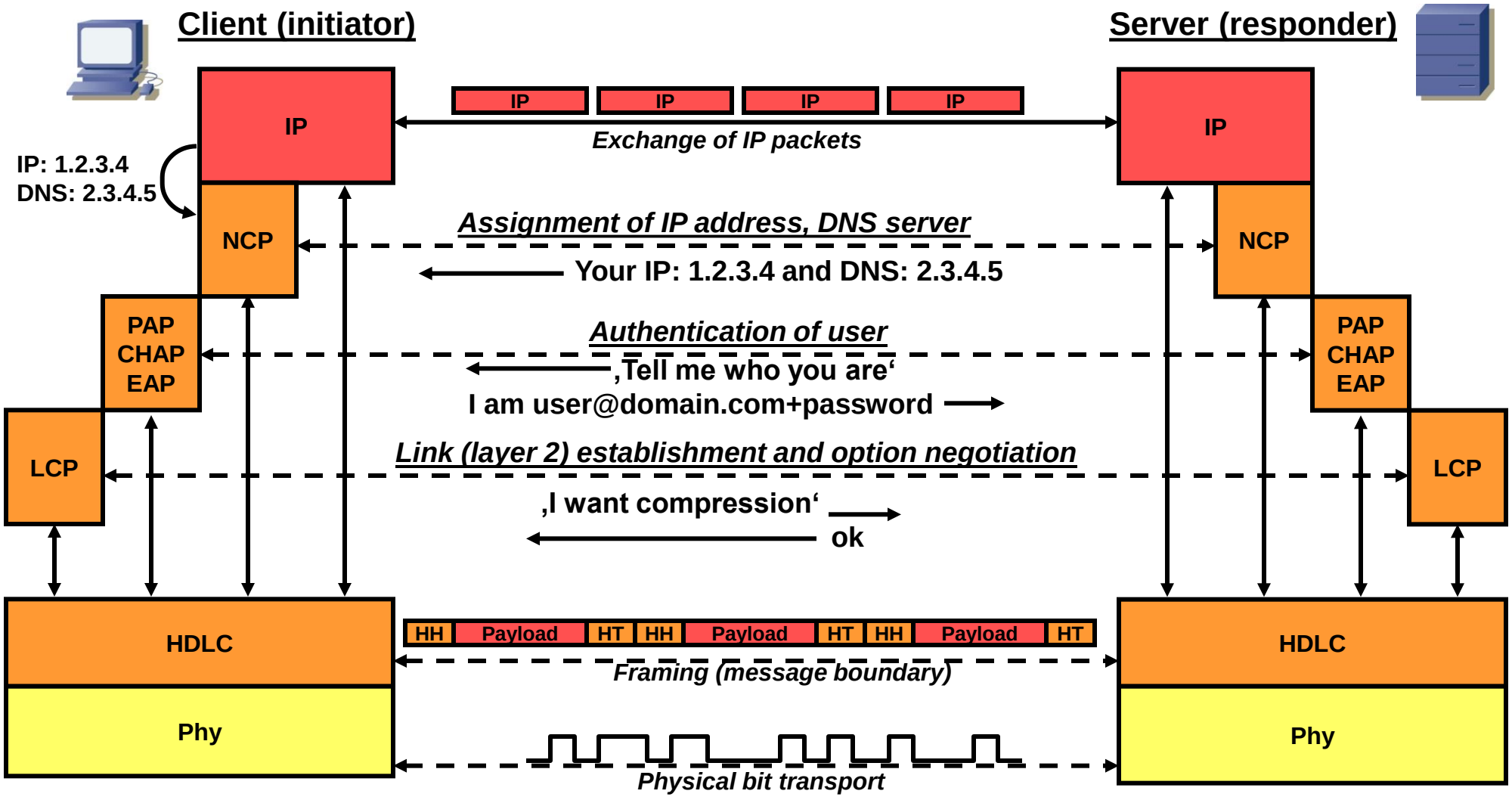
**Frame delimiter = The byte 0xC0 serves as frame delimiter.**
**For transparency, the bytes 0xDB, 0xDC are used as escape sequence for 0xC0 in the payload.**
**→ 0xC0 in payload becomes 0xDB 0xDC in SLIP frame.**
**→ 0xDB in payload becomes 0xDB 0xDD in SLIP frame.**

**SLIP deficiencies:**

**1. SLIP does not have error detection mechanism (left to TCP to detect and recover from errors on the transmission line).**
**2. SLIP only supports IP (no other layer 3 protocols).**
**3. SLIP does not provide dynamic IP address assignment.**
**4. SLIP does not provide authentication.**

## 2. Overview of PPP

**PPP is a protocol suite for serial links which do not provide a framing (raw bit pipes).**



# 3. Layer 2 functions

## Layer 2 functions and corresponding PPP protocol:

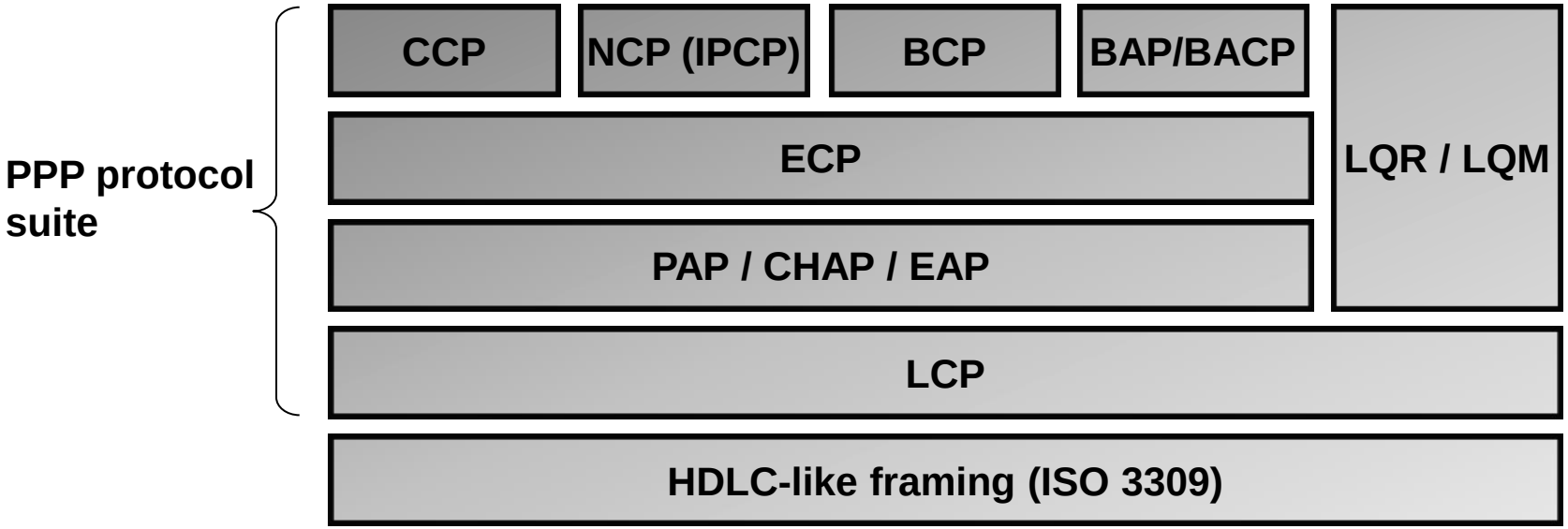
| L2 Function | Description | Provided by PPP Protocol |
|---|---|---|
| Framing | Serial lines provide bit transport, thus a means for finding the start of packets is required. | HDLC (not part of PPP protocol suite but provided by ISO 3309 HDLC). PPP defines HDLC as default framing protocol. |
| Link setup, control | Link characteristics like maximum frame size need to be negotiated between both ends. | LCP |
| Authentication | Client (and optional server) authentication make sure the right communication partners talk to each other. | PAP / CHAP / EAP |
| Encryption | Communication may need confidentiality. | ECP along with encryption algorithms like 3DES or AES |
| Bandwidth allocation for multi-links | To fulfill increased bandwidth demands, bonding of multiple channels may be required (Multilink PPP-MLPPP). | BAP / BACP |
| Bridging / routing mode on both ends | The link ends may be operated in bridged or routed mode. Bridging requires a control protocol. | BCP |
| Setup of network functions | Each network protocol (IP, IPX) requires its own control protocol for functions like IP address assignment. | NCP (IPCP) |
| Data compression on link | Serial links are typically slow (modem lines etc.), so compression increases available bandwidth. | CCP |
| Monitoring the link | The link quality may need to be monitored. | LQR / LQM |

## 4. PPP (RFC1661 et.al.) protocol stack

**PPP is not a single protocol but a protocol suite containing protocols that address various aspects of point-to-point layer 2 communication.**

**PPP is an asymmetric protocol suite. The 2 parties in a PPP session are the initiator (I, usually client) and the responder (R, usually server).**

**PPP's main function are:**
**a. Packet encapsulation and framing on point-to-point links**
**b. Link setup (LCP sub-protocol)**
**c. Authentication**
**d. Network control, basically assigning an IP address and DNS server addresses to clients**



## 5. PPP protocols (1/2)

**LCP Link Control Protocol:**
**LCP negotiates and controls link parameters on both ends (e.g. MRU Max. Receive Unit, header compression, encapsulation).**

**CHAP - CHallenge Authentication Protocol:**
**Description see below.**

**PAP - Password Authentication Protocol:**
**Description see below.**

**EAP - Extensible Authentication Protocol:**
**EAP is a protocol that supports a range of authentication algorithms/protocols.**

**IPCP - IP Control Protocol (is an NCP Network Control Protocol):**
**IPCP establishes IP operation on both ends of point-to-point links (mainly assignment of IP address and DNS server from responder to initiator).**

## 5. PPP protocols (2/2)

**CCP - Compression Control Protocol:**
CCP negotiates and controls compression on both ends of link.

**BCP - Bridging Control Protocol:**
BCP establishes bridging operation on both ends of point-to-point link (similar to IPCP, but instead of routing it initializes bridging).

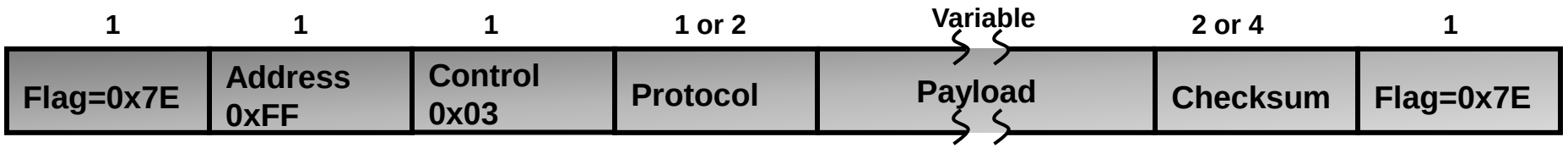
**BAP/BACP - Bandwidth Allocation (Control) Protocol:**
BAP/BACP can be used to add/remove individual links in a multi-link bundle (MultiLink PPP).

**ECP - Encryption Control Protocol:**
ECP allows configuring and enabling encryption on both ends of the link.

**LQM – Link Quality Monitoring:**
LQM is used for monitoring the link quality. LQR is used for link quality reporting.

## 6. PPP framing with HDLC

**The PPP framing is a variant of HDLC (High Level Data Link Control).**
**The framing is character oriented, i.e. the frame always has an integral number of bytes (=octet).**
**When the payload (user data) contains flags, an escape byte 0x7D is inserted (byte stuffing).**




**The field address is fixed = 0xFF which means that all stations are to accept the frame.**

**Control = 0x03 means that the frame is unnumbered (PPP does provide error detection, but no error correction; reliable transmission with PPP is set forth in RFC1663).**

**The protocol field identifies the layer 3 protocol contained in the payload (for protocol values see IANA assigned numbers).**

**The payload is variable length (default 1500 bytes).**

**The checksum is either a 2 byte CRC16 (default) or 4 byte CRC32 (for frames > 4kB).**

# 7. LCP and NCP

## A. LCP (Link Control Protocol):

**LCP is used for establishing the link.**
**LCP allows negotiating link options like:**

- **a. Authentication protocol to be used.**
- **b. Header compression / address field compression.**
- **c. MRU (maximum receive unit).**

**LCP periodically tests the link with symmetric LCP-Echo requests / replies.**
**LCP brings down the link gracefully when it is no longer in use.**

## B. NCP (Network Control Protocol):

**NCP is used for the dynamic assignment of an IP address to the client and the assignment of a primary and secondary DNS server.**

**The host must set a default route to the PPP interface since there is no default gateway IP address (the link is point-to-point, thus typically the link is unnumbered without an IP address on the server side).**

## 8. PPP authentication

**PAP and CHAP are used for Authentication with PPP (is the one I am talking to the one he pretends to be?).**

**PAP RFC1661 Password Authentication Protocol:**

**PAP simply sends a username and password (cleartext) to the remote computer.**
**Thus PAP is considered insecure.**
**PAP is symmetric and does not allow asymmetric settings with an authenticator and a peer (authenticator authenticates peer).**

**CHAP RFC1994 Challenge Handshake Authentication Protocol:**

**With CHAP, an authenticator (usually server) authenticates a peer (usually client).**
**Thus CHAP is asymmetric.**
**CHAP procedure:**

1. **The authenticator computes a random value (=challenge) to foil replay attacks.**
2. **The authenticator sends the challenge to the peer.**
3. **The peer computes a hash (MD5) value on the identifier (username), secret (password) and challenge.**
4. **The peer sends hash value to authenticator.**
5. **The authenticator performs the same calculation and checks if the result is ok.**

# 9. Typical PPP session

## Wireshark trace of a PPP session with CHAP authentication.

```
I:  1    0.000000 Client -> Server PPP LCP PPP LCP Configuration Request
R:  2    0.028594 Server -> Client PPP LCP PPP LCP Configuration Request
I:  3    0.029362 Client -> Server PPP LCP PPP LCP Configuration Ack
R:  4    0.030818 Server -> Client PPP LCP PPP LCP Configuration Reject
I:  5    0.031299 Client -> Server PPP LCP PPP LCP Configuration Request
R:  6    0.063986 Server -> Client PPP LCP PPP LCP Configuration Ack
I:  7    0.064776 Client -> Server PPP LCP PPP LCP Identification
I:  8    0.066026 Client -> Server PPP LCP PPP LCP Identification
R:  9    0.068683 Server -> Client PPP CHAP PPP CHAP Challenge
I: 10    0.069147 Client -> Server PPP CHAP PPP CHAP Response
R: 11    0.718392 Server -> Client PPP CHAP PPP CHAP Success
I: 12    0.720670 Client -> Server PPP CCP PPP CCP Configuration Request
I: 13    0.722227 Client -> Server PPP IPCP PPP IPCP Configuration Request
R: 14    0.885780 Server -> Client PPP IPCP PPP IPCP Configuration Request
I: 15    0.932285 Client -> Server PPP IPCP PPP IPCP Configuration Ack
I: 16    0.933597 Client -> Server PPP IPCP PPP IPCP Configuration Request
R: 17    0.959508 Server -> Client PPP IPCP PPP IPCP Configuration Nak
I: 18    0.960196 Client -> Server PPP IPCP PPP IPCP Configuration Request
R: 19    0.984960 Server -> Client PPP IPCP PPP IPCP Configuration Ack
... PPP data
R: 20    1.156618 Server -> Client PPP LCP PPP LCP Echo Request
I: 21    1.275972 Client -> Server PPP LCP PPP LCP Echo Reply
R: 22   11.156947 Server -> Client PPP LCP PPP LCP Echo Request
R: 25   13.341129 Server -> Client PPP LCP PPP LCP Termination Ack
```

LCP

CHAP

NCP (IPCP)

LCP

**Key:**
**I:** **Initiator**
**R:** **Responder**