PPP

The point-to-point protocol

PPP versus SLIP

- PPP
  - Where is PPP used
  - What is the task of LCP
  - What is the task of NCP
- SLIP
  - Serial Line IP
  - Predecessor of PPP
  - We don't even think of it today

Introduction (1)

- Goal of PPP
  - Convey datagrams over a serial link
  - Both synchronous or asynchronous serial links are supported
  - Both bit or byte oriented transmissions are supported
- Basically, PPP consists of
  - One Link Control Protocol (LCP)
  - Several Network Control Protocols (NCPs)

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.

Introduction (2)

- HDLC is basis for encapsulation
  - Only framing and error detection necessary
  - Only simple unnumbered information frames (UI)
- PPP supports full-duplex links only (!)
- PPP Frame = Datagram + 2-8 bytes extra header
  - Extra header consists of HDLC header and PPP header
- Byte Stuffing: Data dependent overhead!

Overhead

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

Byte Stuffing

If the flag byte (126) occurs in the data field it has to be escaped using the escape byte 125, while byte 126 is transmitted as a two byte sequence (125, 94) and the escape byte itself is transmitted as (125, 93).

LCP

- Link Control Protocol (LCP)
  - Setup, configure, test and terminate PPP connection
  - Supports various environments
- LCP negotiates
  - Encapsulation format options
  - Maximal packet sizes
  - Identification and authentification of peers (!)
  - Determination of proper link functionality

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, authenticate the identity of its peer on the link, determine when a link is functioning properly and when it is defunct, detect a looped-back link and other common misconfiguration errors, and terminate the link.

NCPs

- Network Control Protocols (NCPs)
  - Helper to establish various network protocols
  - IP uses "IPCP"
- Typical tasks
  - Assignment and management of IP addresses
  - Compression and authentication

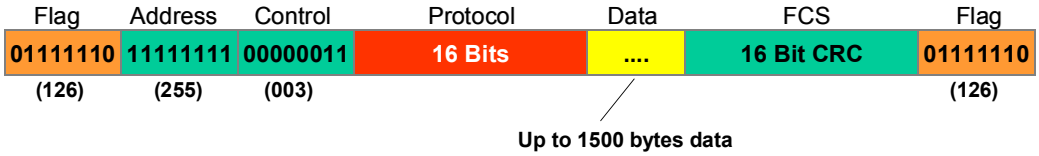
Point-to-Point links tend to exacerbate many problems with the current family of network protocols. For instance, assignment and management of IP addresses, which is a problem even in LAN environments, is especially difficult over circuit-switched point-to-point links (such as dial-up modem servers). These problems are handled by a family of Network Control Protocols (NCPs), which each manage the specific needs required by their respective network-layer protocols.

NCPs have been developed for all important network layer protocols such as IP, which uses the IP Control Proocol (IPCP).

There are also NCPs designed to enable compression and authentication.

Data Link Layer: HDLC

- Address 11111111 means "all stations"
  - PPP does not assign individual station addresses
- Only the control field 00000011 is used
  - Unnumbered Information (UI) command
- Protocol field identifies datagram
  - Already part of PPP, not HDLC (!)



(C) Herbert Haas 2005/03/11 7

Protocol: The True PPP Field

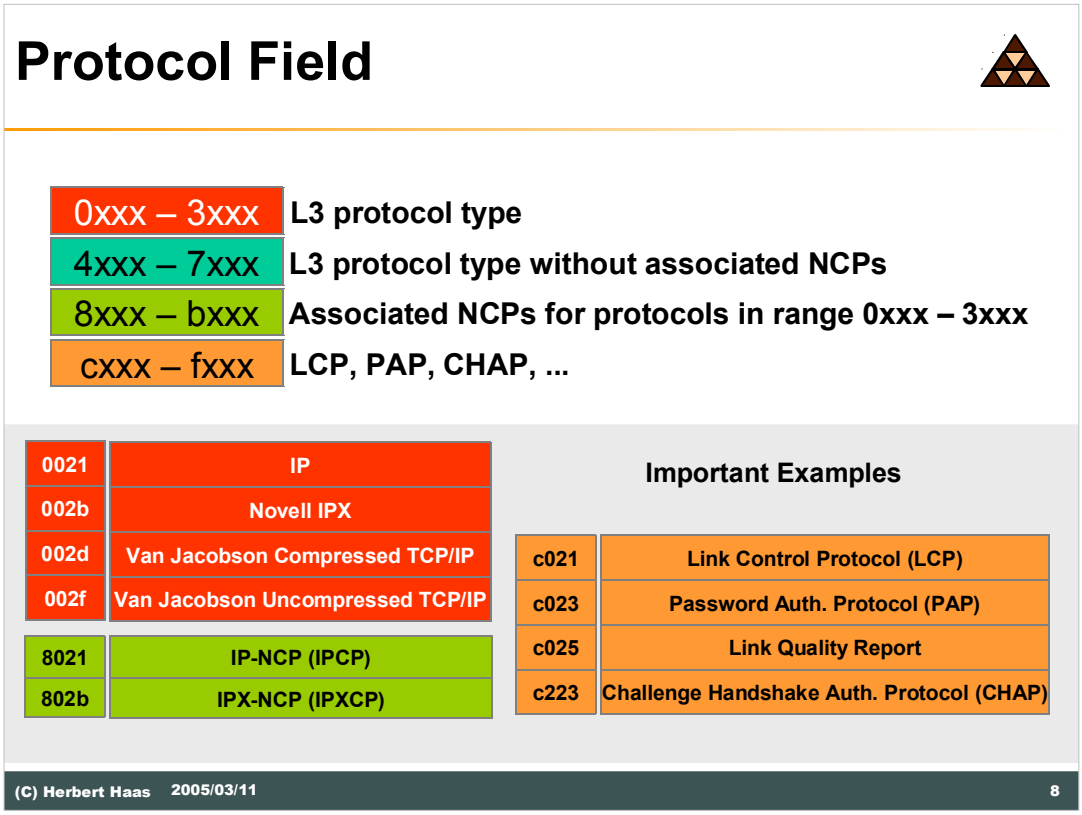
The most important field is the protocol field, which has two octets and its value identifies the datagram encapsulated in the Information field of the packet.

PPP Header Compression

If protocol field compression is enabled, the protocol field is reduced from 2 to 1 byte. Since the first two bytes are always constant, that is the address byte (always 255) and the control byte (always 003), PPP also supports address-and-control-field-compression, which omits these bytes.

Byte Stuffing

If the flag byte (126) occurs in the data field it has to be escaped using the escape byte 125, while byte 126 is transmitted as a two byte sequence (125, 94) and the escape byte itself is transmitted as (125, 93).



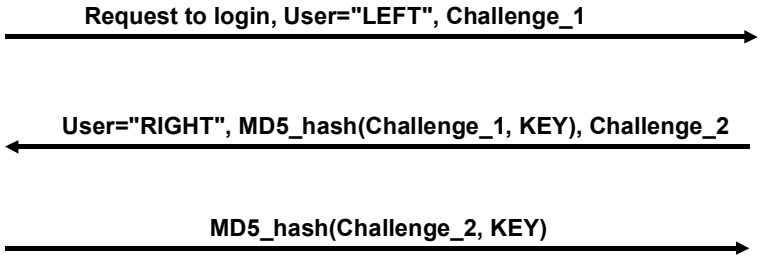
Protocol Field Values

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).

All these numbers are controlled by the IANA (see RFC-1060).

CHAP – The Challenge Handshake Authentication Protocol

- Supports 1-way and 2-way authentication
- Periodically verifies the identity of the remote node using a three-way handshake
- Relies on MD5 hash (regarded as weak today)
  - Offline dictionary attacks possible!
- Still widely used



Microsoft's MSCHAPv2 is even worse

PPP today

- Is still a usual choice when carrying IP packets over high-speed serial lines
- Several flavors for different media
  - PPPOE (over Ethernet)
  - PPPOA (over ATM)
  - PPTP (Tunnel PPP through a IP network)
  - POS – Packet over SONET/SDH
- See RFC 1661, 1662