Eine Einführung in PPP – wie es funktioniert, Pros und Cons

Martin Hellwig, Michael Schulze, Michael Stahn
Kommunikationsnetze 1
Technische Universität Darmstadt

***Abstract*—Diese Arbeit behandelt das Thema Point-to-Point Protocol (PPP). Dieses Protokoll wurde als Ersatz für frühere Einwahlprotokolle entwickelt. Heutzutage findet es seine Hauptanwendung beim Einwählen via DSL. Neben der technischen Umsetzung und Spezifikation wird in dieser Arbeit auch ein möglicher Verbindugsaufbau via PPP gezeigt.**

***Index Terms*—PPP, PPPoE, PPPoA, Point-to-Point.**

I. Einleitung

DAS Point-to-Point Protocol wurde ursprünglich im Jahr 1994 von W. Simpson entwickelt. Im OSI-Modell ist es zusammen mit anderen Protokollen in der Sicherungsschicht (engl. Data Link layer) dafür zuständig eine direkte Verbindung zwischen zwei Clients über ein leitungsvermittelndes Netz herzustellen. Für diesen Zweck werden auch Möglichkeiten der Authentifizierung spezifiziert [4]. Ebenfalls besteht die Möglichkeit die Daten zu verschlüsseln oder zu komprimieren. Die Protokolle der OSI-Netzwerkschicht können dann die bestehende PPP-Verbindung zur Übermittlung von Daten nutzen. Eine PPP-Verbindung (beispielsweise zwischen Internet Service Providern, Routern, Hosts oder Netzwerkbrücken) ist eine Full-Duplex Verbindung und versucht die zu übermittelnden Pakete in der richtigen Reihenfolge zu übertragen.
Die Notwendigkeit dieses Protokolls war zu dieser Zeit sehr hoch, da ältere Standards, wie beispielsweise SLIP, nicht mehr zeitgemäß waren. Ebenfalls wurde der Telefonstandard "Link Access Protocol, Balanced", welcher in der X.25-Protokollfamilie benutzt wurde, durch PPP ersetzt. Speziell für die Internetverbindung für Heimanwender wurde für den alten ISDN-Standard ein Ersatz erschaffen. Eine Eigenschaft des Point-to-Point Protokolls ist es, für andere Protokolle der Netzwerkschicht leicht zu bedienen und zu nutzen zu sein. Mit den beiden Unterprotokollen PPPoE (Point-to-Point over Ethernet)[6] und PPPoA (Point-to-Point over ATM)[5] kann man sich nun mithilfe eines Routers direkt mit dem Provider verbinden, was höhere Datenraten zulässt. Dabei bleibt aber weiterhin der Vorteil (welcher zum Beispiel bei ISDN vorhanden ist), dass man zeitgebundene Tarife für die Endkunden anbieten und abrechnen kann. Bei heutigen DSL-Anschlüssen besitzt man zwar eine dauerhafte physikalische Verbindung zum Provider, doch erst mit dem Aufbau der PPP-Verbindung ist man auch virtuell mit dem Provider verbunden und kann somit das Internet nutzen. Nicht nur für heimische Internet-Anschlüsse wird PPP genutzt, sondern in allen Netzwerkverbindungen, in welchen man sich erst einwählen muss. Dazu gehört auch das Mobilfunktnetz oder auch die Einwahl über eine ISDN-Verbindung.
In folgendem Bild (siehe Bild 1) wird gezeigt für welchen Zweck das PPP-Protokoll bei DSL-Zugängen genutzt wird. Dabei stellt der heimische Router eine dauerhafte virtuelle Verbindung zu der Gegenstelle des Providers her, welche (aktuell in Deutschland so geregelt) im Normalfall alle 24 Stunden neu aufgebaut wird, da dann die Verbindung seitens des Anbieters automatisch getrennt wird.

Neben DSL-Anschlüssen gibt es in Deutschland die

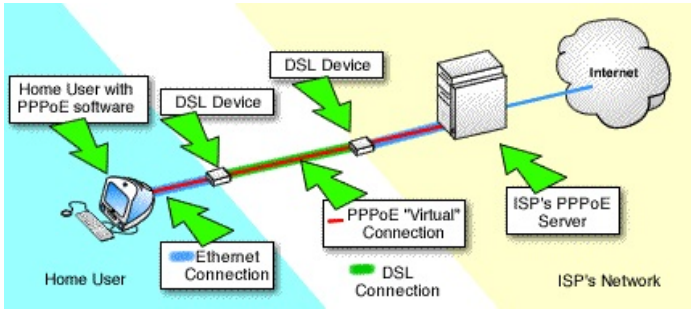

Fig. 1. Darstellung einer PPP-Verbindung zwischen Heimanwender und ISP (Entnommen aus [8])

Alternative des Kabelanschlusses. Bei Kabelanschlüssen wird nicht das PPP-Protokoll zum Aufbau einer Verbindung genutzt, sondern das DOCSIS-Protokoll zusammen mit einer DHCP-ähnlichen [7] Funktionsweise.
Auch die weit verbreitete aber mittlerweile als unsicher geltende VPN-Lösung Point-to-Point Tunneling

Protocol (PPTP) basiert auf PPP. Sie nutzt nachdem ein sicherer Tunnel erstellt wurde PPP zur Verbindung mit einem entfernten Netwerk. Dabei stellt PPP auch Sicherheitsfunktionen wie z. B. die Authentifizierung bereit.

Sektion 2 behandelt die Funktionsweise von PPP zusammen mit dem Aufbau des PPP-Headers. Sektion 3 beschreibt einen Verbindungsaufbau am Beispiel einer PPPoE-Verbindung. In Sektion 4 werden Vor- und Nachteile zwischen PPP und dem älteren SLIP aufgezeigt. Zuletzt ziehen wir in Sektion 5 ein Fazit zu den hier vorgestellten Fakten zu PPP.

II. Aufbau von PPP

Das Point-to-Point-Protokoll befindet sich im OSI-Modell auf der Sicherungsschicht (Schicht 2, wie in Abbildung 2 zu sehen) und beinhaltet Pakete der überliegenden Schichten.
PPP besteht aus folgenden drei Kernfunktionen:

1) Rahmenbildung inklusive Fehlererkennung
2) Verbindungssteuerung
3) Aushandeln von Optionen

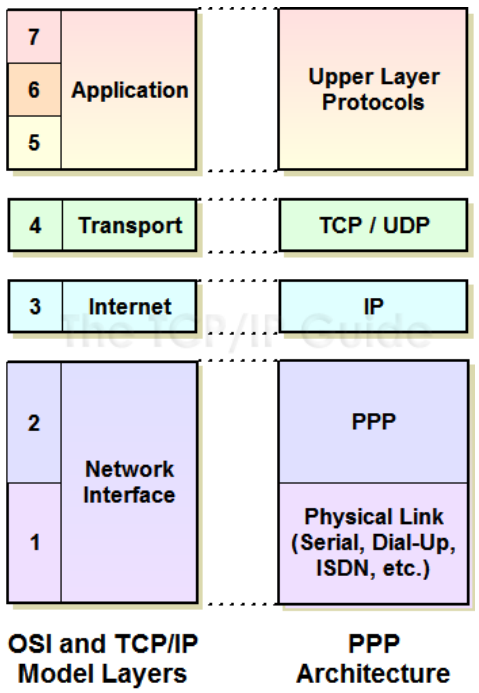

Fig. 2. Eingliederung im OSI/TCP-Modell (Entnommen von [15])

A. Rahmenbildung

Die Rahmenbildungsmethode von PPP kennzeichnet eundeutig das Ende und den Anfang des nächsten Rahmens und kann Übertragungsfehler erkennen. Es ist ähnlich dem *High-Level Data Link Control* (HDLC) Protokoll aufgebaut, ist statt diesem aber nicht bit- sondern byteorientiert. Dies bedeutet, dass immer eine gerade Anzahl von Bytes verwendet wird. Obwohl PPP auch zuverlässige Übertragungen bieten kann wird meist ein unnummerierter, also unbestätigter Datentransfer genutzt.

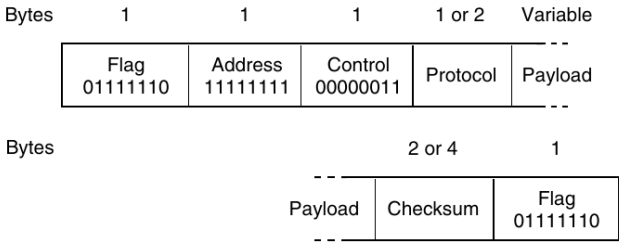

Fig. 3. PPP-Rahmen im unnummerierten Modus (Entnommen aus [16])

Im Folgenden wird der detaillierte Aufbau eines PPP-Rahmens erläutert (siehe Abbildung 3).
Das 1. Byte stellt dabei das sogenannte *Flagbyte* dar, welches den Anfang und das Ende des Rahmens kennzeichnet und immer aus den Bits `01111110` (hexadezimal `0x7E`) besteht. Sollte im Payload die selbe Bitfolge vorkommen, wird diese vor dem Versand "escaped", also markiert und umgewandelt (auch Bytestopfen genannt). Hierfür wird diesem Byte ein weiteres Escapebyte vorangestellt (`0x7D`) und anschließend das Eigentliche mit `0x20` XOR-verknüpft. Somit wird aus dem Flagbyte im Payload `0x7D 0x5E`. Mithilfe des Escaping kann einfach nach Anfang und Ende des Rahmens gesucht werden. Beim Auslesen wird nach dem Flagbyte `0x7D` gesucht, selbiges bei Fund gelöscht und das nachfolgende wieder mit `0x20` XOR-verknüpft. Zwischen zwei Rahmen wird nur ein Flagbyte benötigt um beide abzugrenzen.
Das 2. Byte ist das *Addressbyte*, das immer auf `11111111` gesetzt ist um an allen Stationen durchgelassen zu werden. Ähnlich einem IP-Broadcast muss somit keine spezifische Adresse zugewiesen werden.
Nach dem *Addressbyte* folgt das *Controlbyte*, welches immer mit `00000011` gesetzt ist, um anzugeben, dass der Rahmen unnummeriert ist. Bei schlechten Verbindungen mit Verlusten, wie z. B. drahtlose Netzwerke sollte die Rahmennummerierung aktiviert werden. Da *Addressbyte* und *Controlbyte* meist konstant sind, können Teilnehmer aushandeln die beiden Bytes nicht zu nutzen, letztlich also den Overhead der Rahmen zu vermindern.
Das folgende Feld bezeichnet das Protokoll des sich im Payload befindenden Paket. Bitfolgen die mit

einer 1 beginnen (ab `0x8000`), werden für PPP-Verbindungsprotokolle verwendet (z. B. LCP, NCP). Bitfolgen beginnend mit einer 0 bezeichnen Protokolle der Vermittlungsschicht (Schicht 3): IPv4/IPv6, aber auch z. B. IPX oder Appletalk. Das Feld ist standardmäßig 2 Byte groß, kann aber per LCP auch auf 1 Byte heruntergesetzt werden.
Der Payload beinhaltet die eigentlichen Daten, also Pakete anderer Protokolle. Seine Länge beträgt standardmäßig 1500 Byte, kann aber auch per LCP auf eine andere Größe vereinbart werden. Sind die zu übertragenen Daten kleiner als die definierte Payload-Größe, so kann mittels Padding aufgefüllt werden. Nach dem Payload folgt eine Checksumme (CRC), die über die Felder Address, Control, Protokoll und den Payload berechnet wird. Das Feld der Checksumme ist standardmäßig 2 Byte groß, kann aber auch auf 4 Byte verhandelt werden (CRC32). Durch diese Checksumme können Übertragungsfehler effektiv entdeckt werden.

B. Unterprotokolle zur Verbindungssteuerung und Aushandeln von Optionen

a) Link Control Protocol: Das *Link Control Protocol* (LCP) dient zum Aufbau, Konfiguration und Prüfung von PPP-Verbindungen. Zur Konfiguration dienen diverse Optionen, die in LCP-Paketen im Payload von PPP-Rahmen übertragen werden. Der initiierende Rechner schlägt Optionen vor, die vom Kommunikationspartner entweder angenommen oder komplett bzw. teilweise abgelehnt werden können. Mögliche Optionen sind u. a. die *Maximum Receive Unit* (MRU), das Authentifizierungsprotokoll oder das Qualitätsprotokoll. Ersteres legt die maximale zu übermittelnde Paketgröße fest. Mögliche Authentifizierungsprotokolle sind z. B. das *Password Authentication Protocol* (PAP) oder das *Challenge Handshake Authentification Protocol* (CHAP). Über ein optionales Qualitätsprotokoll können Daten zur Verbindungsqualität ausgetauscht werden. Daneben gibt es noch eine Vielzahl weiterer Optionen, die sich z. B. um Komprimierung, Nummerierung oder Identifikation kümmern (LCP Erweiterungen).

b) Network Control Protocol: Das *Network Control Protocol* (NCP) enthält verschiedene Protokolle zur Aushandlung von Ende-zu-Ende Verbindungsoptionen der Teilnehmer. Am weitesten verbreitet ist dabei das *Internet Protocol Control Protocol* (IPCP) für IPv4. Hierüber können Optionen wie IP-Adresse, Gateway, DNS-Server und Kompression ausgehandelt werden. Damit ist IPCP über Wählverbindungen in seiner Funktion ähnlich dem *Dynamic Host Control Protocol* (DHCP) in Ethernet-Netzwerken. Neben IPCP gibt es weitere NPCs für andere Protokolle der Vermittlungsschicht beispielsweise IPV6CP für IPv6, IPXCP für IPX oder ATCP für Appletalk.

III. Kommunikationsabläufe

Das PPP eignet sich für die Übertragung über eine Vielzahl an Physical Layer Protokollen. Hierzu zählen unter anderem Synchronous Optical Network (SONET), GPRS-/UMTS oder auch in Verbindung mit Ethernet über die weit verbeitete PPPoE-Variante für die Übertragung über Direct Subscriber Line (DSL) Anschlüsse[1]. An dieser Stelle wird exemplarisch der Kommunikationsablauf anhand von PPPoE aufgezeigt.

A. PPP over Ethernet

Das PPPoE Protokoll ist in RFC 2516 spezifiziert und wurde ursprünglich von den Firmen UUNET Technologies, Redback Networks und RouterWare entwickelt [6]. PPPoE ermöglicht die Übertragung von PPP-Paketen auf Basis von Ethernet, wodurch die Authentifizierungsfunktionen von PPP mit den simultanen Zugriffsmöglichkeiten des Ethernet kombiniert werden. Die Notwendigkeit für PPPoE resultierte aus dem Anfang dieses Jahrtausends einhergehenden Einzugs der DSL-Technologie und der notwendigen Umstrukturierung der benötigten Software und Hardware. Ziel war es, ein Protokoll zu entwickeln, welches die bis dahin vorherrschende Einwahlverfahren möglichst kostengünstig ersetzt. Mit PPPoE war es einerseits möglich die bis dahin bestehenden Software-Stacks für PPP mit minimalen Anpassungen weiter zu verwenden und ließ sich andererseits mit einfacher und damit günstiger Hardware umsetzen[10]. Eines der Haupteinsatzgebiete von PPPoE sind somit Breitbandzugänge über DSL-Anschlüsse, Wireless-Zugängen oder Kabelmodems und wird auch von vielen Internet Service Providern (ISP) zu diesem Zweck eingesetzt [9, p.88].
Der strukturelle Aufbau eines typischen PPPoE-Pakets ist in Abbildung 4 zu sehen. Hierbei ist die Verschachtelung der Protokolle der einzelnen Layer zu erkennen: Die unterste Ebene bildet Ethernet, gefolgt von PPPoE zur PPP bis zum Internet Protokoll. Der Aufbau von Ethernet und IP-Paketen wird als bekannt vorausgesetzt und hier nicht näher erläutert. Die Bedeutung der PPPoE-Header ist in Tabelle 5 dargestellt. Der Ablauf einer PPPoE-Verbindung teilt sich in die drei Phasen Discovery, Session und Terminate ein. Diese werden in Abbildung 6 in den folgenden Abschnitten näher erläutert (vgl. [6]).

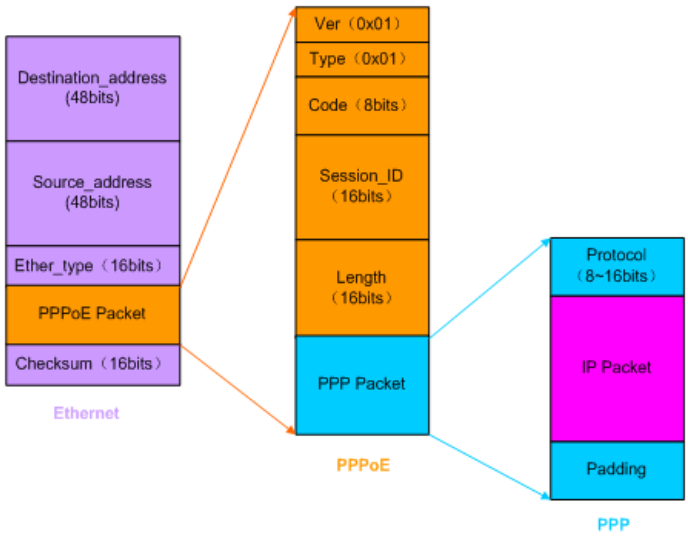

Fig. 4. Aufbau eines PPPoE-Pakets (Entnommen von [11])

Ver	Verwendete Version des PPPoE. Der Wert ist immer 1.
Type	Verwendeter Typ des PPPoE. Der Wert ist immer 1.
Code	Typ des PPPoEPakets: 0x00 = Sitzungsdaten; 0x09 = PADI; 0x07 = PADO oder PADT; 0x19 = PADR; 0x65 indicates PADS
Session_ID	Eindeutiger identifier einer PPPSitzung
Length	Länge des PPPoEPayloads
Protocol	Protokolltyp des nächsten Layers

Fig. 5. Bedeutung der PPPoE-Header

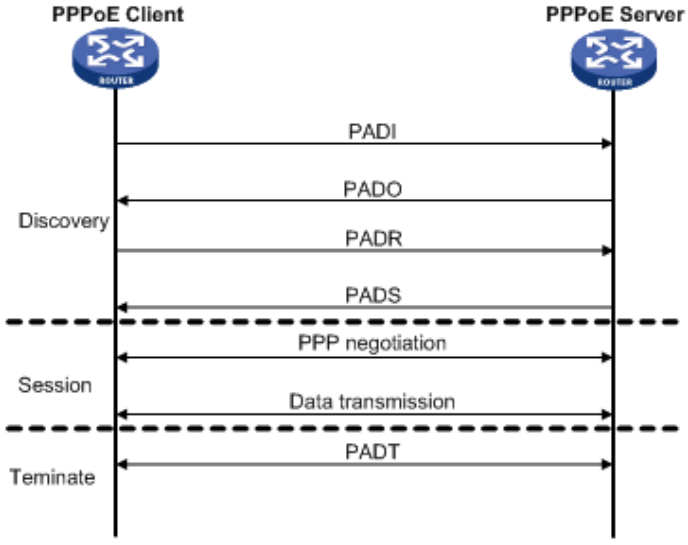

Fig. 6. Ablauf einer PPPoE-Session (Entnommen aus [11])

1) Discovery: Das Ziel dieser Phase ist das Auffinden der MAC-Adresse des Servers (auch Concentrator genannt) sowie das Ableiten einer PPPoE Session-ID durch den Client (auch Host genannt). Abhängig von der Topologie können sich mehrere Server im Netzwerk befinden, welche in dieser Phase durch den Client entdeckt werden. Die Discovery-Phase selbst ist zustandslos, d.h. auf Seiten aller Kommunikationen werden keine Verbindungsinformationen gespeichert.
Das erste gesendete PPPoE Active Discovery Initiation (PADI) Paket stellt ein Broadcast an alle im Netzwerk vorhanden Server dar. Dieses enthält den Namen des vom Client angefragten Service, auf welches Server mit einem PPPoE Active Discovery Offer (PADO) Paket antworten. Das Antwortpaket hat als Zieladresse die des Clients und enthält neben dem Namen des Servers optional weitere vom Server angebotene Service-Namen. Es folgt ein PPPoE Active Discovery Request (PADR) Paket mit welchem der Client den von ihm nun gewählten Server und Service unter allen gefundenen direkt adressiert. Nach Erhalt des PADR beginnt der Server mit dem Aufbau einer PPP Session und bestätigt dies mit einem PPPoE Active Discovery Session-confirmation (PADS) Paket. Diese enthält auch eine Session-ID, welche die folgende Session eindeutig Identifiziert.

2) Session: In der Sitzungsphase erfolgt die weitere Konfiguration der Verbindung, die Authentifikation des Clients sowie der eigentliche Datenaustausch. Dieser ist im Gegensatz zur Discovery und Terminate Phase PPP-spezifisch und in Abbildung 7 und 8 genauer dargestellt. Hierbei wird zunächst ein Verbindungsaufbau über das Link Control Protocol (LCP) durchgeführt. Daraufhin erfolgt eine optionale Authentifikation entweder über das Password Authentication Protocol (PAP) oder dem Challenge-Handshake Authentication Protocol (CHAP). Bei einem DSL-Anschluss entspricht dies dem Nachweis der Kenntnis der vom ISP mitgeteilten Anschlussdaten. Es erfolgt die Zuweisung einer Netzwerkadresse über das Network Control Protocol (NCP) und im Anschluss der Austausch der eigentlichen Nutzdaten. Die Verbindung kann nun jederzeit terminiert werden, z.B. aufgrund von Inaktivität oder einem Session-Timeout.

3) Terminate: Die PPPoE Verbindung kann jederzeit von beiden Kommunikationspartnern beendet werden. Hierfür sendet der Client oder der Server ein PPPoE Active Discovery Terminate (PADT) Paket. Nach Erhalt dieses Pakets ist kein weiterer Datenaustausch über die Session erlaubt.

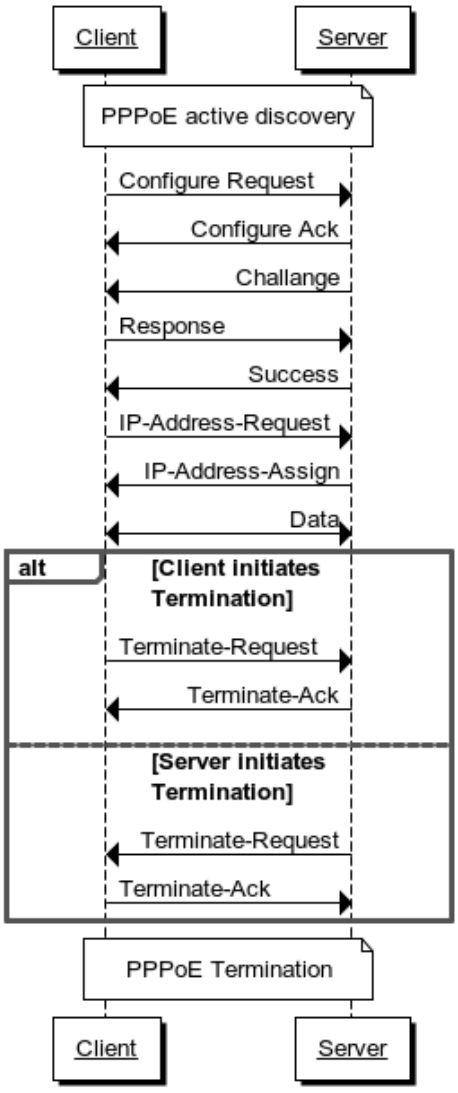

Fig. 7. PPP-Spezifischer Teil eines PPPoE-Verbindungsaufbaus (Entnommen aus [12])

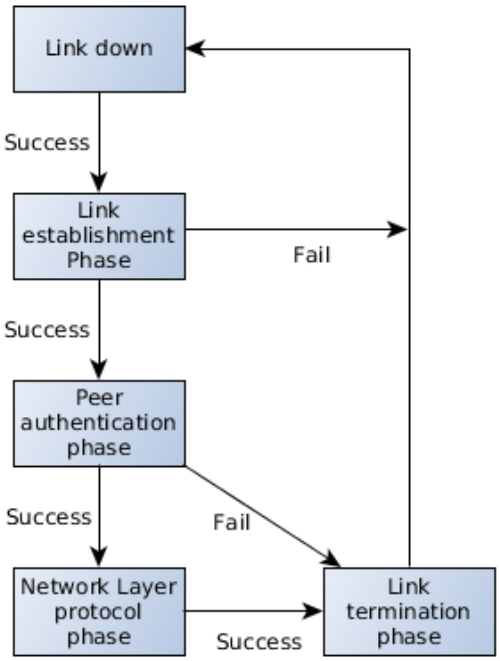

Fig. 8. Phasen der PPP-Session (Entnommen aus [13])

IV. Vor- und Nachteile

Das PPP entstand ursprünglich aus dem Serial Line Internet Protocol (SLIP). Eine Betrachtung der Unterschiede bzw. Neuerungen in PPP lässt somit eine Bewertung der Vor- und Nachteile zu (vgl. [14]). Die Vorteile von PPP lassen sich zunächst wie folgt zusammenfassen:

- **Mehrere Netzwerkprotokolle über einen Übertragungskanal:** Das ältere SLIP-Protokoll unterstützt immer nur ein einziges Netzwerkprotokoll.
- **Fehlerkorrekturverfahren:** Frames mit falschen Checksummen werden von PPP erneut vom Kommunikationspartner angefordert. Das ältere SLIP unterstützt kein Fehlerkorrekturverfahren, sondern delegiert die Fehlerbehandlung an andere Protokolle weiter. Dies bedeutet i.d.R. zusätzliche Arbeitsschritte welche die Fehlerkorrektur und somit auch die Übertragung verlangsamen können.
- **Software-Flußkontrolle:** Bei Aushandlung der Steuerzeichen über LCP kann PPP auch auf Datenübertragungseinrichtungen verwendet werden, die mit Software-Flußkontrolle (XON/XOFF) arbeiten – z.B. zwischen Modem und Computer. SLIP unterstützt dies nicht.
- **Vereinfachung der Authentifizierung:** Bei identischem Authentisierungsverfahren beider Kommunikationspartner entfällt im allgemeinen die manuelle bzw. skriptgestützte Identifizierung beim Kommunikationspartner, was in vielen Fällen auch die Verwendung von Skripts überflüssig macht. SLIP unterstützt dies nicht.
- **Automatisches Aushandeln einer IP-Adresse:** PPP – genauer IPCP – unterstützt von sich aus das automatische Aushandeln einer dynamisch zugewiesenen IP-Adresse im gegensatz zu SLIP.
- **Aushalndung der Kompression:** Die Kommunikationspartner handeln mittels IPCP aus, ob Van-Jacobson-Header-Compression verwendet werden soll. Im Fall von SLIP muss der Kommunikationspartner wissen, ob das Verfahren unterstützt wird oder nicht und die Software entsprechend konfigurieren.

Neben den Vorteilen existieren allerdings auch die folgenden Nachteile:

- **Verzögerung der Konfiguration:** Eine Aushandlung der Einstellungen durch das LCP und das darauffolgende Aushandeln der Einstellungen durch die verschiedenen NCPs kann einige Sekunden in Anspruch nehmen. Bei SLIP kommt es zu keiner Verzögerung.
- **Daten overhead:** PPP-Frames zur Übertragung von Netzwerkprotokolldaten enthalten zusätzlich zu den Daten standardmäßig 9 Bytes Steuer- und Kontrollinformation. Selbst unter Verwendung von Address-and-Control-Field-Compression und Protocol-Field-Compression womit Zusatzinformation somit auf 4 Bytes reduziert werden, sind das immer noch 3 Bytes mehr als bei der Verwendung von SLIP, das mit einem Byte an Zusatzinformation auskommt.
- **Zusätzliche Systemressourcen:** Der komplizierte Aufbau von PPP bedingt wesentlich mehr Systemressourcen (Rechenzeit, Speicher) als SLIP, das mit einer sehr einfachen Frame-Struktur das Auslangen findet. Bei schnellen PPP-Verbindungen und unzureichend ausgestatteten Computern kann dies zu Einbußen bei der Arbeitsgeschwindigkeit führen.
- **Größere zu übertragende Datenmenge:** Bei vielen mit LCP zu übertragenden Steuerzeichen, die vor der Übertragung umkodiert werden müssen, erhöht sich die zu übertragende Datenmenge, vorausgesetzt die zu übertragenden Datagramme enthalten viele solcher Steuerzeichen. Der Grund hierfür ist das jedes Steuerzeichen, das ursprünglich mit einem Byte dargestellt werden konnte, nach dem Umkodieren zwei Byte beansprucht.

V. Fazit

Wie in der Einführung erwähnt, war das Point-to-Point Protocol notwendig, da die damals aktuellen Standards nicht alle mittlerweile benötigten Anforderungen erfüllen konnten. Durch die einfache Handhabung der aufgebauten verbindung für Netzwerkschichtprotokolle, ist vermutlich auch die große Verbreitung des Protokolls zu erklären. Bei fast allen Möglichkeiten eine Internetverbindung aufzubauen (sei es über DSL oder im Mobilfunknetz) wird PPP als Einwählprotokoll genutzt. Zwar wird im Kabelnetz mittlerweile ein anderes Protokoll verwendet, doch durch die einfache Umsetzung des Point-to-Point Protokolls wird es wahrscheinlich noch einige Jahre der Standard beim Verbinden mit dem ISP sein.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999. Andrew S. Tanenbaum: Computer Networks, 5.th edition, Prentice Hall, 2011 James F. Kurose / Keith W. Ross, Computernetzwerke, Pearson, 2012

[2] A Method for Transmitting PPP Over Ethernet (PPPoE) (IETF RFC2516), L. Mamakos, K. Lidl, J. Evarts, 1999.

[3] Point-to-Point Tunneling Protocol (IETF RFC 2637), K. Hamzeh, The Internet Society, Juli, 1999.

[4] Point-to-Point Protocol (IETF RFC 1661), W. Simpson, The Internet Society, Juli, 1994.

[5] Point-to-Point Protocol over AAL5 (IETF RFC 2364), G. Gross, The Internet Society, Juli, 1998.

[6] Point-to-Point Protocol over Ethernet (IETF RFC 2516), L. Mamakos, The Internet Society, Februar, 1999.

[7] The DOCSIS (Data-Over-Cable Service Interface Specifications) Device Class DHCP (Dynamic Host Configuration Protocol) Relay Agent Information Sub-option (IETF RFC 3256), D. Jones , The Internet Society, April, 2002.

[8] Veranschaulichung einer PPP-Verbindung, Vicomsoft, http://www.vicomsoft.com/learning-center/pppoe/

[9] Cisco IOS in a Nutshell James Boney, O'Reilly Media 2005

[10] Implementation and Applications of DSL Technology, Philip Golden Hervé Dedieu, Krista S. Jacobsen, 1998

[11] Aufbau eines PPPoE-Pakets, H3C http://www.h3c.com/portal/Products___Solutions/Technology/WAN/Technology_White_Paper/200911/654415_57_0.htm

[12] PPP-Verbindungsaufbau, Startnetworks http://www.startnetworks.info/2011/05/pppoetheory.html

[13] PPP-Zustände, Oracle http://docs.oracle.com/cd/E19096-01/sol.ppp301/805-4018/6j3qil163/index.html

[14] PPP, Eine Alternative zu SLIP?, Uni Wien http://comment.univie.ac.at/95-3/19/

[15] Eingliederung von PPP im OSI–Modell, Abrufdatum: 29.05.2014, http://www.tcpipguide.com/free/

[16] Computernetzwerke, Andrew S. Tanenbaum, Pearson Verlag, 5. Auflage, 2012.