Hochschule für Technik und Wirtschaft
Fakultät für Ingenieurwissenschaften

Ausarbeitung Protokolle

Autoren:
Deniz Kadiogullatri 3553892
Christoph Drost 3576450

Betreuer:
Jonas Vogt, M.Sc.

19. Februar 2014

Inhaltsverzeichnis

1 Einleitung

Im Folgenden sollen verschiedene Layer 2 Protokolle für kabelgebundene Netze miteinander verglichen werden. Um die Zusammenhänge besser erklären zu können, möchten wir erst auf das ISO/OSI Referenzmodell eingehen.

1.1 Das ISO/OSI Referenzmodell

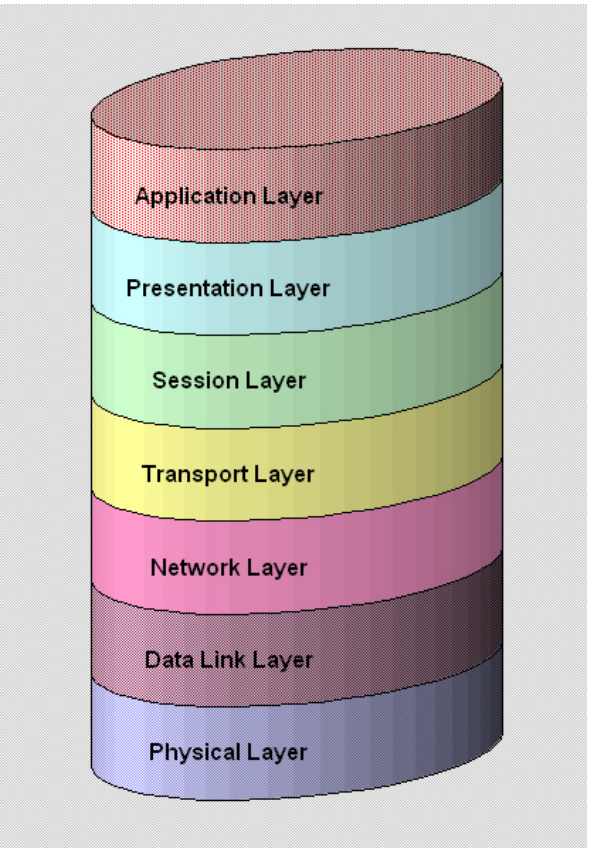

Abbildung 1: Das ISO/OSI Referenzmodell im Überblick [8]

Diese Grafik stellt die Schichten des ISO/OSI Referenzmodell dar. Das ISO/OSI Referenzmodell, (Open Systems Interconnection Model) ist ein allgemeines Kommunikationsmodell, das die Kommunikation unterschiedlichster Geräte beschreibt. Es beschreibt ein komplettes Telekommunikationsnetzwerk. Die einzelnen Funktionen sind in 7 Schichten aufgeteilt.
Das ISO/OSI Referenzmodell standardisiert die Netzwerk Architektur. Dadurch können Hersteller Lösungen anbieten, die auf der ganzen Welt genutzt werden können. Eine proprietäre Lösung hätte zu Insellösungen geführt. Ein weiterer Vorteil ist, dass die einzelnen Schichten, oder Layer, über Schnittstellen miteinander kommunizieren. Das ermöglicht ein Austauschen einzelner Komponenten, ohne die gesamte Architektur ändern zu müssen.
Da das ISO/OSI Referenzmodell nur ein Referenzmodell darstellt, müssen die einzelnen Schichten konkret implementiert werden. Diese Implementierungen sind eigene Protokolle.

1.2 Der Layer 2

Der Layer 2, Data Link Layer, setzt auf dem Physical Layer auf und stellt dem Network Layer seine Dienste zur Verfügung. Der Physical Layer beschreibt, wie der Name schon sagt, die physikalischen Eigenschaften der Verbindung. Hier findet noch keine Logik statt. Als höhere Schicht nutzt der Data Link Layer die Eigenschaften des Physical Layer, bzw. nutzt ihn, um die Informationen auf das Medium zu bringen.
Die Aufgaben des Layer 2 im Überblick:

- Aufteilung in Frames
- Fehlerkontrolle

1.2.1 Aufteilung in Frames

Die Datenblöcke werden im Layer 2 in Frames aufgeteilt. Die Vorteile des Framing sind die schnellere Nutzung eines shared Mediums und dass bei fehlerhaften Daten nur die fehlerhaften Frames neu übertragen werden müssen. Die schnelle Nutzung eines Shared Mediums resultiert daraus, dass ein Sender, der einen großen Datensatz überträgt, nicht dauerhaft das Medium belegt. Sendet der Teilnehmer A ein Gigabyte und der Teilnehmer B nur ein Byte, kann der Teilnehmer B seine Frames zwischen denen von Teilnehmer A unterbringen und seine Übertragung abschließen, bevor Teilnehmer B fertig ist.

1.2.2 Fehlerkontrolle

Der Data Link Layer führt eine Fehlerkontrolle durch. Dazu zählen eine Suche nach Duplikaten und eine Suche nach inkorrekt oder unvollständig gesendeten Paketen. Wenn ein Fehler entdeckt wird, wird eine neue Übertragung der Frames angefordert [19, S. 91]. Die Fehlerkontrolle wird über den „Cyclic Redundancy Check“ CRC durchgeführt. Dieses Verfahren ist eine Methode zur Prüfsummenberechnung, die beim Sender und bei der Senke durchgeführt wird. Sind beide Prüfsummen gleich, kann angenommen werden, dass das Frame korrekt übertragen wurde. Damit die Senke die Prüfsummen vergleichen kann wird die des Senders mitgeschickt.
Die Frames werden mit Sequence Numbers durchnummeriert. Der Empfänger prüft, ob die Frames in der richtigen Reihenfolge ankommen. Bei einer „out-of-sequence transmission“ kann von einem verlorenen Frame ausgegangen werden, das entsprechende Frame wird neu angefordert, bzw. der Layer 3 wird benachrichtigt.

2 Die Layer 2 Protokolle im Überblick

2.1 Ethernet

Ethernet ist ein weit verbreitetes Layer 2 Protokoll. 90% aller lokal installierten Netzwerke sind mit Ethernet realisiert[13]. Ethernet wurde ursprünglich für die Anbindung eines Druckers bei der Firma Xerox Corporation entwickelt. Die damalige Übertragungsgeschwindigkeit von 2,94 Mbit/s wurde auf aktuell 100 Gbit/s gesteigert, weitere Steigerungen sind zu erwarten.

Die Daten werden bei Ethernet über einen eigenen Übertragungskanal transportiert (vgl. **??**). Kollisionen werden durch „CSMA/CD“ entdeckt, bzw. aufgelöst. Die Übertragung läuft gleichberechtigt und verbindungslos. Die Daten werden an alle Teilnehmer weitergeleitet, diese vergleichen die Empfängeradresse mit ihrer eigenen und verwerfen die Frames, die nicht an sie adressiert sind. Diese Aussage kann eingeschränkt werden, da Switche die Daten nur an Ports leiten, an denen die entsprechenden Senken angeschlossen sind.

2.1.1 Gebräuchliche Übertragungsmedien des Ethernet

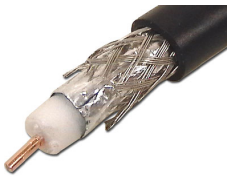

Abbildung 2: Koaxkabel [6]

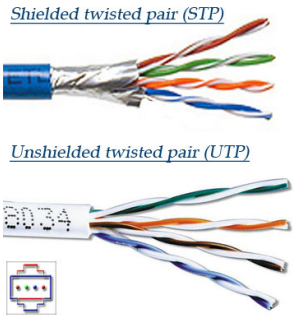

Abbildung 3: Twistet Pair Kabel [11]

Abbildung 4: Lichtwellenleiter [12]

Historisch gesehen muss das Koaxialkabel als Medium des Ethernet genannt werden. Das Koaxialkabel wurde 1990 mit der Einführung von 10BaseT (IEEE 802.3i) durch Unshielded Twisted Pair Kabel ersetzt. Ab 1998 wurden mit der Einführung des Gigabit Ethernet auch Lichtwellenleiter genutzt.

2.1.2 Adressierung

Ethernet nutzt zur Adressierung von Teilnehmern deren MAC-Adresse. MAC-Adressen, Media Access Control Adress, sind Hardwareadressen und werden weltweit eindeutig vergeben. Sie bestehen aus 6 Byte und sind nach folgendem Muster aufgebaut:
Hersteller–Hersteller–Hersteller–xx–xx–xx
Der Herstellerteil, auch Organizationally Unique Identifier (OUI), wird von der IEEE vergeben. Jeder Hersteller hat seinen eigenen Bereich, der durch die ersten 3 Byte bestimmt wird. Die letzten drei Byte werden vom Hersteller selber vergeben. Dabei ist der Hersteller für die eindeutige Vergabe der letzten drei Byte verantwortlich. Einige Hersteller haben mittlerweile mehrere eigene Bereiche.

2.1.3 Zugriff auf das Medium

Historisch gesehen nutzt Ethernet das Übertragungsmedium als Shared Medium. Die einzelnen Teilnehmer wurden am selben Koaxialkabel über T-Stücke angeschlossen. Um Kollisionen zu vermeiden, wurde ein geeignetes Verfahren zur Vermeidung benötigt. Von einer Kollision spricht man, wenn mehrere Teilnehmer gleichzeitig auf das Medium zugreifen, also Signale aussenden. Die Signale überlagern sich gegenseitig und sind nicht mehr nutzbar. Bei Ethernet wird CSMA/CD eingesetzt. Bei diesem Verfahren

wird vor dem Senden geprüft, ob die Leitung frei ist. Erst wenn die Leitung frei ist wird gesendet (Carrier Sense). Wenn zufällig mehrere Teilnehmer gleichzeitig ein Signal aussenden (Multiple Access) kommt es dennoch zu Kollisionen. Der/Die Sender prüfen während dem Senden, ob es zu Kollisionen kommt (Collision Detect) und brechen ihre Übertragung im Fall einer Kollision ab. Nach einem Abbruch wird eine zufällige Zeit gewartet bis erneut gesendet wird. Der Grund, warum es trotz diesem Verfahren zu Kollisionen kommen kann, ist die Signallaufzeit. Die Signale brauchen eine gewisse Zeit um über die Leitungen übertragen zu werden.
In seinen Anfangszeiten übertrug Ethernet im Halbduplex Verfahren. Das bedeutet, dass ein Übertragungskanal zum Senden und zum Empfangen genutzt wird. Dadurch halbiert sich natürlich rechnerisch die Datenrate, bzw. kann durch häufige Kollisionen und den damit verbundenen Wartezeiten noch weiter absinken. Mit der Einführung von Twisted Pair Kabeln und Lichwellenleitern wurde der Vollduplex Betrieb ermöglicht. Dadurch konnte die Übertragungsrate gesteigert werden und Kollisionen wurden vermieden.

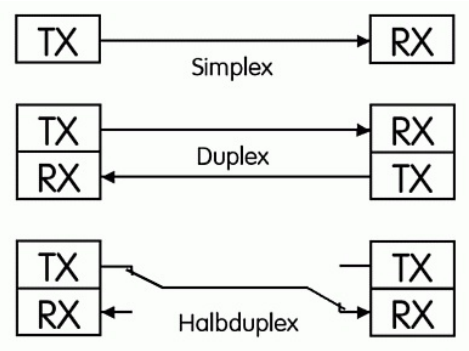

Abbildung 5: Unterschied der Duplex Übertragungen [3]

2.1.4 Frames

Um Daten über Ethernet übertragen zu können, werden sie in Frames aufgeteilt. Der Vorteil daran ist, dass ein Sender bei großen Übertragungen nicht das gesamte Netzwerk belegt und dass bei einer fehlerhaften Übertragung nur einzelne Frames neu versandt werden müssen. Der Ausdruck Frame kann wörtlich genommen werden. Die Nutzdaten werden in einen Rahmen (Frame) eingepackt.
Ein Frame ist folgendermaßen aufgebaut:

- Die Präambel
- Die Hardware Quell- und Zieladresse
- Ein Typ- oder Längenfeld
- Nutzdaten
- Eine Checksumme

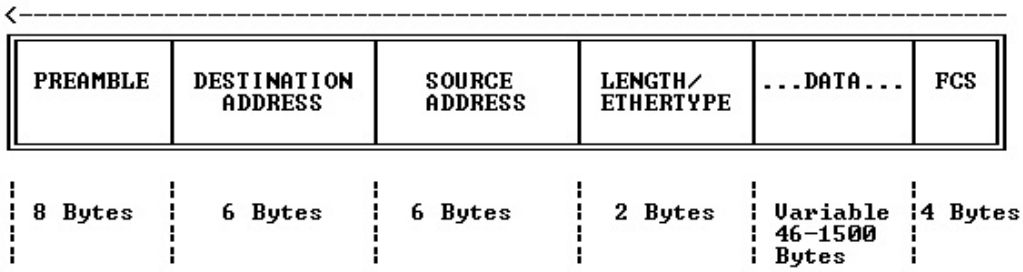

Abbildung 6: Ethernet 802.3 Frame [16]

2.1.4.1 Präambel Die Präambel enthält eine Bitfolge, die dem Empfänger signalisiert, dass ein Rahmen ankommt. Die Präambel besteht aus 8 Byte mit einer alternierenden Folge aus 0 und 1. Die letzten 2 Bits im letzten Byte sind immer 1. Hier besteht ein kleiner Unterschied zwischen DIX und IEEE. Obwohl die Bitfolgen die gleichen sind, ist die Präambel im IEEE Standard formell in die 7 Byte lange Präambel und den 1 Byte langen Start-of-Frame-Delimiter aufgeteilt. Die Präambel dient u.a. zur Synchronisation der Empfängerstationen.

2.1.4.2 Die Hardware Quell- und Zieladresse Die Adressen sind MAC Adressen. Ihr Aufbau ist bereits in **??** beschrieben worden. Ein Ethernet Frame enthält sowohl die Ziel-, als auch die Quelladresse.

2.1.4.3 Typ- oder Längenfeld Um zu verstehen, warum beide Bezeichnungen möglich sind, muss man wieder die Historie betrachten. Die DIC Gruppe nutzte das Feld als Typfeld. Dort wurde definiert, welche Daten des höheren Layers übertragen werden. Im Standard IEEE 802.3 wird das Feld als Längenfeld genutzt.Um welchen Standart, bzw. um welches Feld es sich handelt, kann anhand des Wertes ermittelt werden. Die Typenbezeichnungen beginnen ab 1635 (0x0600). Ein Wert darunter kann nur eine Längenangabe sein. Jumbo- und Super Jumboframes sind abseits von IEEE 802.3 definiert.

2.1.4.4 Nutzdaten Die Nutzdaten sind die Daten, die eigentlich übertragen werden sollen. Das Feld mit den Nutzdaten hat eine Mindestlänge von 46 Byte und eine Maximallänge von 1500 Byte. Die Mindestlänge kommt von der Anforderung des CSMA/CD, wonach ein Frame mindestens 64 Byte haben muss. Zieht man von den 64 Byte die Headerlänge (14 Byte) und die Checksumme (4 Byte) ab kommt man auf 46 Byte. Wird die Mindestlänge der Nutzdaten unterschritten, wird das Feld mit sogenannten Pads aufgefüllt. Sie haben den Wert 00.

2.1.4.5 Checksumme Die letzten 4 Byte eines Ethernet Frames sind die FCS, Frame Checking Sequence, oder Frame Checking Field. Die FCS dient der Sicherstellung, dass der Frame korrekt übertragen wurde. Der Inhalt dieses Feldes wird mithilfe des CRC-Algorithmus errechnet. Sowohl Sender, als auch Empfänger, wenden ihn an. Werden beim Sender und Empfänger unterschiedliche Werte errechnet, kann davon ausgegangen werden, dass auf Layer 1 Bits verfälscht wurden. Neben dem CRC Verfahren werden zur Prüfung auch andere Kriterien zur Prüfung eines Frames angewandt:

- Die Framelänge stimmt nicht mit dem Längenfeld überein (nur bei IEEE 802.3)
- Die Framelänge ist kein ganzzahliges Vielfaches eines Byte

2.1.5 Topologie

Ethernet ist keiner bestimmten Netzwerk Topologie zuzuordnen. Heute gebräuchlich ist eine Sterntopologie, andere Formen sind aber auch möglich.

2.2 LAPD

LAPD, Link Access Procedure on the D-channel ist auch ein Protokoll der Schicht 2. Es wird genutzt, um Layer 3 Informationen zwischen den Teilnehmern des ISDN Netzwerks zu übertragen. Für diese Übertragung wird der D-Kanal genutzt.

2.2.1 Der D-Kanal

Der D-Kanal wird im ISDN zur Signalisierung genutzt. Er stellt 16 kbit/s zur Verfügung. Signalisieren bedeutet, dass der Teilnehmer und die Vermittlungsanlage Informationen austauschen. Das können Informationen sein, ob der Teilnehmer verfügbar ist, oder auch Informationen mit denen ein Gespräch aufgebaut wird. Im Gegensatz zu den B-Kanälen, über die Nutzdaten, wie z.B. Sprache, übertragen werden, kommunizieren über den D-Kanal nur Prozessoren.

2.2.2 Gebräuchliche Medien des LAPD

Der Layer 1 unter LAPD wird durch den S_0 und den U_{K0} Bus beschrieben. Für S_0 werden üblicherweise 4 Draht Kupfer Verkabelungen verwendet, für U_{K0} eine Kupfer Doppelader.

Abbildung 7: Ein typisches IDSN Kabel (S_0) [15]

Abbildung 8: Kupferkabel im Überblick [9]

2.2.3 Adressierung

LAPD nutzt zur Adressierung der Teilnehmer den TEI, Terminal Endpoint Identifier. Der TEI wird entweder durch eine feste Einstellung im Endgerät, oder durch die Vergabe der Vermittlungsstelle vergeben. Er besteht aus 7 Bit. Der TEI ist im normalen Betriebszustand eindeutig, darf aber nicht mit der Rufnummer verwechselt werden.

2.2.4 Der Zugriff auf das Medium

LAPD ist das Signalisierungsprotokoll des ISDN. An einem S_0 Bus teilen sich bis zu 8 Teilnehmer einen D-Kanal. Der Zugriff durch die Teilnehmer ist priorisiert. Zur Regelung, welcher Teilnehmer bevorrechtigt ist, gilt, je mehr logische Einsen den Teilnehmer identifizieren, desto niedriger ist die Priorität. Da der D-Kanal als Shared Medium genutzt wird, muss eine Kollisionsbehandlung stattfinden. Um zu überprüfen, ob eine Kollision stattgefunden hat, gibt es den E-Kanal. Auf diesen wird der D-Kanal durchgeschleift. Der Teilnehmer kann anhand vom E-Kanal überprüfen, ob die Informationen, die er gesendet hat, unverfälscht zurück kommen. Ist das der Fall, kann er davon ausgehen, dass es zu keiner Kollision mit den Signalen anderer Teilnehmer gekommen ist.
Der S_0 Bus arbeitet in einem Vollduplexverfahren (vgl. Abbildung **??**). Die Zuweisung der Ressourcen erfolgt über Zeitschlitze.

2.2.5 Frames

LAPD teilt die Daten der Schicht 3 in Frames auf. Dabei werden folgende unterschiedliche Frametypen benutzt:

- Blockbegrenzung
- Adressfeld
- Steuerfeld
- Daten
- Blockprüfung
- Blockbegrenzung

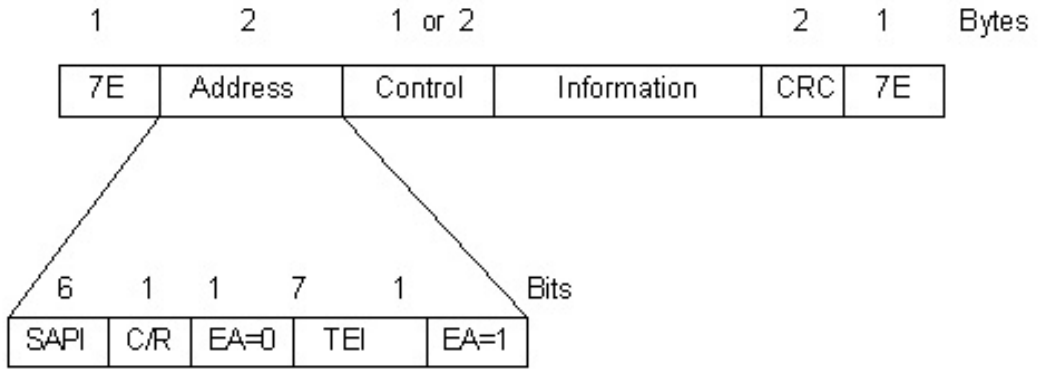

Abbildung 9: LAPD Frame [4]

2.2.5.1 Blockbegrenzung Die Blockbegrenzung ist ein Byte, das aus einer Bitkombination besteht, die im restlichen Block nicht vorkommt. Sie stellt den Anfang und das Ende des Blocks dar und hat die Bitfolge 01111110.

2.2.5.2 Adressfeld Das Adressfeld besteht aus 2 Byte. Es enthält den SAPI und den TEI, die je 1 Byte groß sind. Die Größe 1 Byte ist eigentlich ungenau, da man die Byte, wie in Abbildung **??** zu sehen ist, wieder genauer aufteilen kann. Jedes dieses Byte hat ein EA (Extended Adress), damit wird angegeben, ob dem Byte noch weitere folgen. Der SAPI, Service Access Point Identifier, identifiziert die Dienste der Schicht 2. Er besteht aus 6 Bit, das C/R Bit und das EA Bit vervollständigen das Byte. Das C/R-Feld kennzeichnet, ob das Paket eine Anweisung (Command) für den Empfänger enthält oder ob es eine Antwort (Response) auf eine zuvor erhaltene Anweisung enthält. Aktuell sind 3 Typen des SAPI definiert [14]:

- Die gesicherte Übermittlung von Signalisierungsinformationen (SAPI 0)
- Die Übertragung von paketvermittelteten Daten (SAPI 16)
- Die Festlegung von eindeutigen TEI (SAPI 63)

Der TEI wurde bereits in **??** genauer beschrieben. Im Byte des TEI wird EA = 1 gesetzt, da der TEI das letzte Adress Byte ist.

2.2.5.3 Steuerfeld LAPD kennt 4 Rahmentypen. Sie haben verschiedene Funktionen, die im Steuerfeld gekennzeichnet werden. Die Informationen zu dem Steuerfeld sind aus [14] zitiert:

I-Rahmen Der I-Rahmen, Informationsrahmen, dient der Übermittlung von Schicht 3 Informationen. Der I-Rahmen ist der einzige, der einen Sendefolgezähler enthält.

S-Rahmen Der S-Rahmen, Steurrahmen, dient zum Quittieren von empfangenen Rahmen. Mit ihm werden außerdem Zustandsmeldungen (z.B. empfangsbereit) gesendet und bei groben Protokollfehlern andere Rahmen abgewiesen.

U-Rahmen Der U-Rahmen, umnummerierter Rahmen, dient der Übertragung von Steuerkriterien, für die eine Nummerierung nicht möglich oder nicht nötig ist. Beispielsweise kann man dafür das Kommando für die Initialisierung (SABME) einer Schicht 2 Verbindung, oder die Abweisung von fehlerhaften Rahmen (FRMR) nennen.

UI-Rahmen Der UI-Rahmen, umnummerierter Informationsrahmen, ist eine Spezialität des LAPD Protokolls. Er wird für für spezielle Prozeduren im Zusammenhang mit der P-MP-Konfiguration am Basisanschluss benötigt und überträgt die Informationen des Layer 2 (TEI Management) oder des Layer 3 (kommender Ruf). Er wird genutzt wenn vorher noch keine Layer 2 Verbindung eingerichtet wurde. UI-Rahmen werden nicht quittiert.

2.2.5.4 Daten Welche Daten übertragen werden, wird im Steuerfeld geregelt. Die reine Übertragung von Layer 3 Daten erfolgt nur in I-Blöcken. Die Blöcke werden nummeriert und von der Gegenseite bestätigt. Der Empfang kann durch einen I-Block oder durch einen S-Block bestätigt werden. Wie oft eine Bestätigung zu erfolgen hat, wird durch die Fenstergröße geregelt. Hier sind Werte zwischen eins und sieben möglich. Das Senden von weiteren Frames ist nur möglich, wenn die vorherigen bestätigt wurden. Bei einem Standard ISDN Basisanschluss ist die Fenstergröße eins, bei einem Primärmultiplexanschluss beträgt die Fenstergröße sieben. Das bedeutet, dass bei einem ISDN Basisanschluss nur ein Frame gesendet werden darf, wenn der vorherige bestätigt wurde. Bei einem Primärmultiplexanschluss können sieben Frames gesendet werden, bevor die erste Bestätigung erfolgt sein muss. Erfolgt die Bestätigung von einem Frame, kann ein weiteres gesendet werden.
Ein I-Block darf maximal 260 Byte groß sein. Daraus ergibt sich eine maximal Gesamtgröße von 268 Byte pro LAPD Frame, wenn I-Blöcke genutzt werden.

2.2.5.5 Blockprüfung Die Blockprüfung findet bei sowohl beim Sender, als auch beim Empfänger statt. Die FCS, Frame Checking Sequence, wird vom Sender errechnet und in das entsprechende Feld geschrieben. Der Empfänger errechnet sie auch und vergleicht sie mit der des Senders. Unterscheiden sich die Werte, kann von einem Fehler bei der Übertragung ausgegangen werden. Die Größe der FCS, Frame Checking Sequence, ist auf zwei Byte festgelegt.

2.2.5.6 Blockbegrenzung Siehe **??**.

2.3 PPP

Das Point-to-Point-Protokoll ist ein typisches OSI Layer 2 Protokoll und hat die Aufgabe, Daten der höheren Schichten über eine Punkt-zu-Punkt-Verbindung zu übertragen. Beispiele für Punkt-zu-Punkt-Verbindungen sind ATM-Verbindungen, leitungsvermittelnde Netze, wie Wählverbindungen über das analoge Telefonnetz (über ein Analog-Modem), oder GSM.
Die Aufgaben von PPP sind, neben den klassischen Layer 2 Aufgaben, diese Verbindungen zu initialisieren, aufrecht zu erhalten und wieder zu beenden.
Zur Initialisierung gehört die Authentisierung, das Bestimmen der Paketgröße, die Vergabe von IP Adressen und das Verschlüsseln von Daten. Das Initialisieren dieser Optionen nennt man auch Aushandeln. Zum Aushandeln existiert ein eigenes Protokoll, das sogenannte Link Control Protocol, im Folgenden als LCP bezeichnet. LCP wird innerhalb des PPP Frames als Nutzdaten übertragen. Die Funktionen von LCP im Überblick:

- Aufbau der Verbindung
- Konfiguration der Verbindung
- Testen der Verbindung
- Abbau der Verbindung

LCP wird ausserdem auch dafür benutzt um die Verbindung aufzubauen, zu konfigurieren und testen sowie zum Abbauen der Verbindung.
PPP ist in RFC 1661 definiert und wurde in mehreren anderen RFC, wie in RFC 1662 und 1663, weiter ausgearbeitet.
PPP erlaubt es dem aufsitzenden Protokoll, einem Protokoll des Layer 3, eigene Optionen auszuhandeln. Diese Optionen betreffen lediglich das Protokoll des höheren Layer. Die Funktionalität dieser Aushandlungen ist in den Network Control Protocol, NPC, implementiert.
Beispiele für NCP sind IPCP für IP, AppleTalk Control Protokoll für Appletalk oder IPXCP für IPX. Das IPCP steht für IP Control Protocol.
Wenn Beispielsweise IP über PPP übertragen wird, dient IPCP(Internet Protocol Control Protocol) als NCP. Über dieses Protokoll wird nach dem Verbindungsaufbau dem einwählenden Client eine IP-Adresse, Subnetzmaske und Standartgateway über IPCP-Packete zu gesendet.

2.3.1 LCP

Das Link Control Protocol stellt PPP Methoden zum Steuern der Verbindung zur Verfügung. Diese Methoden werden genutzt, um eine Punkt-zu-Punkt-Verbindung etablieren, konfigurieren, verwalten und beenden zu können. LCP selbst durchläuft vier einzelne Phasen:

1. Aufbau der Verbindung. Dabei wird die Konfiguration ausgehandelt. Dieser Schritt muss vor dem nächsten abgeschlossen sein, abgeschlossen ist er, wenn LCP die ausgehandelten Parameter bestätigt. Die Bestätigung ist erfolgt, wenn ein Bestätigungsframe gesendet und empfangen wurde.

2. (optional) Die Qualität der Verbindung wird ermittelt und es wird ermittelt, ob die Qualität für den Layer 3 ausreichend ist. LCP kann die Verbindung des Layer 3 so lange unterbinden, bis diese Phase abgeschlossen ist.

3. Übergabe an die NCP Protokolle.

4. Beenden der Verbindung. Beim regulären Beenden der Verbindung durch das LCP werden die höheren Protokolle informiert, die dann entsprechend reagieren können. Das Beenden kann sowohl durch den Benutzer, als auch durch physikalische Ereignisse erfolgen.

LCP unterscheidet zwischen drei Frames. Einen um Verbindungen aufzubauen und zu konfigurieren, einen zum Beenden der Verbindung und einen zum Verwalten der Verbindung.
LCP regelt nicht die eigentlichen Layer 2 Optionen, sondern beschreibt, wie diese ausgehandelt werden. Was für Prozesse?
Im Folgenden die einzelnen Typen und ihre Bedeutung:

- Configure-request - Liste der vorgeschlagenen Optionen und Werte
- Configure-ack - Alle Optionen werden angenommen
- Configure-nak - Einige Optionen werden nicht angenommen

- Configure-reject - Einige Optionen können nicht Verhandelt werden
- Terminate-request - Anforderungen zum Trennen der Verbindung
- Terminate-ack - Verbindung wurde getrennt
- Code-reject - Unbekannte Anforderungen erhalten
- Protocol-reject - Unbekanntes Protocol angefordert
- Echo-request - Anforderungen, den Rahmen zurückzusenden
- Echo-reply - Rückgabe des Rahmens
- Discard-request - Rahmen verwerfen (für Testzwecke)

2.3.2 Verbindungsablauf des PPP

Im folgenden durchlaufen wir die verschiedenen Zustände des Verbindungsaufbaus bis hin zum Abbau der Verbindung anhand der unten gezeigten Zeichnung. Als ersten ist die Leitung tot. Das bedeutet es existiert kein Träger auf der physikalischen Ebene und auch keine Verbindung auf der Bitübertragungsschicht. Nachdem eine physikalische Verbindung aufgebaut worden ist wechselt der Zustand zu Aufbauen. Genau in diesem Augenblick beginnt dann die Verhandlung der LCP Optionen. Wenn diese erfolgreich sein sollten können nun die beiden Parteien die mit einander kommunizieren möchten ihre Identität prüfen. Das heisst der Zustand wechselt auf Authentifizieren. Falls dieser Fall nun fehlschlägt wird die Verbindung Beendet, dh. auch der Zustand ändert sich und der Träger wird wieder freigegeben. Somit wären wir wieder im Ausgangszustand. Im Gegengesetzten Fall würde der nächste Zustand Netz heissen und das entsprechende NCP-Protokolle aufgerufen werden um die Vermittlungsschicht zu konfigurieren. Nach dem die Konfiguration erfolgreich abgeschlossen ist wechselt der Zustand nach Öffnen in der die eigentliche Datenübertragung stattfindet. Wenn diese Beendet ist und alle Daten erfolgreich übertragen worden sind kann die Verbindung wie bereits oben geschrieben Beendet werden.

Noch mal nachlesen

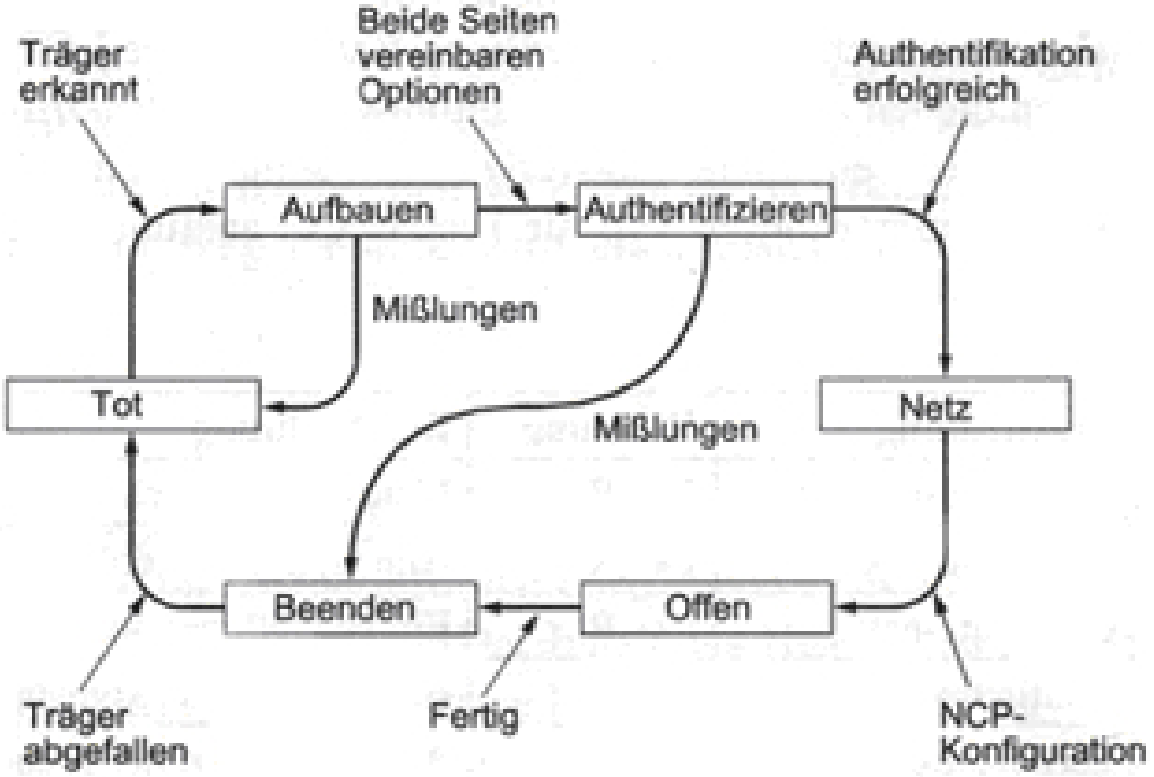

Abbildung 10: Übersicht PPP Verbindungsaufbau [*]

2.3.3 PPP Frame

PPP besitzt eine Rahmenbildungsmethode die Anfang und Ende eines jeden Rahmens kennzeichnet. Diese übernimmt ebenfalls die Aufgabe der Fehlererkennung. Ist das so? Warum dann am Ende FCS?
Der Rahmen besteht aus insgesamt sieben Feldern. Dazu gehören Flag, Adress, Steuerung, Protokoll, Nutzdaten, Prüfsumme und wieder Flag.

flag	address	control	protocol	information	fcs (crc)	flag
1 byte	1 byte	1 byte	2 bytes	up to 1500 bytes	2 bytes	1 byte

Abbildung 11: Darstellung eines PPP Frames [18]

2.3.3.1 Flag Das Flag besteht am Anfang, sowie am Ende aus einem Byte (011111110).

2.3.3.2 Adress Das Adressfeld besteht aus einem Byte mit der festen Bitfolge 11111111. Dies dient dazu, dass alle Stationen den Rah-

men akzeptieren und zum Vermeiden, dass Verbindungsadressen zugewiesen werden müssen. Da dieses Feld in der Standardkonfiguration immer gleich ist, besteht die Möglichkeit, wie auch bei dem Steuerungsfeld, dieses Feld zwischen zwei Parteien entfallen zu lassen. Dadurch können zwei Byte pro Rahmen eingespart werden.

2.3.3.3 Control Das Feld Steuerung, als Standardwert 00000011, zeigt einen unnummerierten Rahmen an. PPP bietet keine zuverlässige Übertragung mit Folgenummern und Bestätigungen. Es ist allerdings möglich eine solche Übertragung zu realisieren. Die genauen Details sind in RFC 1663 definiert, sie werden jedoch in der Praxis nicht häufig eingesetzt.

2.3.3.4 Protocol Das vierte Feld, Protokoll, gibt an welche Art von Paket in den Nutzdaten übertragen wird. Dies können beispielsweise LCP, NCP, IP, IPX und andere Protokolle sein. Normalerweise ist die Größe des Feldes auf zwei Byte festgelegt, es ist jedoch möglich, die Länge über LCP auf ein Byte herunter zu handeln.

2.3.3.5 Information In diesem Feld werden die eigentlichen Nutzdaten übertragen. Die Größe des Nutzdaten Feldes wird üblicherweise von den Parteien ausgehandelt und festgelegt. Findet dieser Prozess über das LCP nicht statt, so ist das Feld standardmäßig auf 1.500 Byte festgelegt. Kann das Feld bei einer Übertragung nicht vollständig gefüllt werden, wird es durch Padding Daten gefüllt.

2.3.3.6 FCS Die Prüfsumme kann auf bis zu 4 Byte ausgehandelt werden, im Normalfall reichen aber 2 Byte aus. Sie dient zum Überprüfen ob der Rahmen richtig gesendet wurde. Die Prüfsumme wird anhand des CRC Algorithmus vom Sender und Empfänger berechnet.

2.3.4 LCP Frame

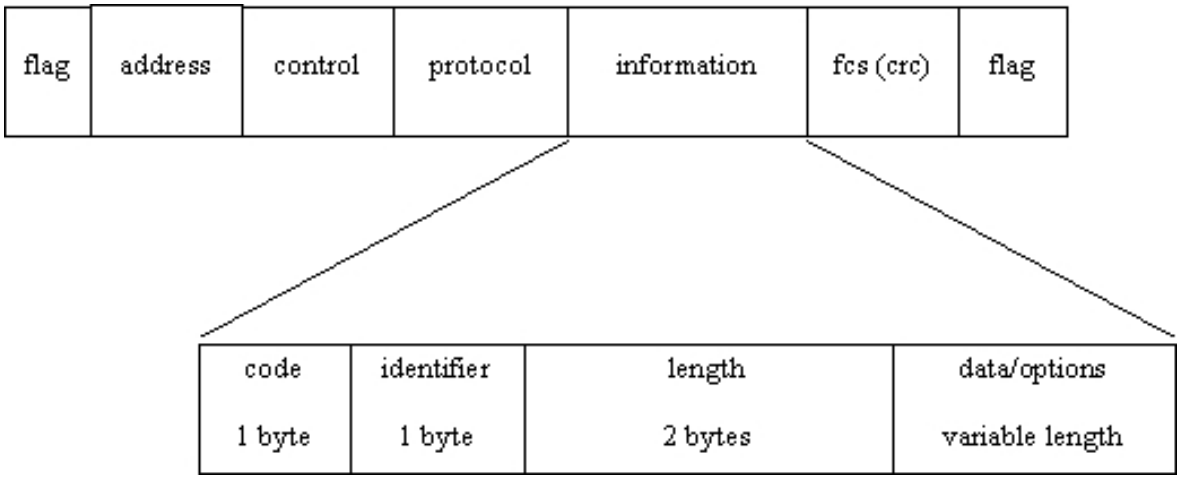

Abbildung 12: Darstellung eines LCP Frames innerhalb eines PPP Frames[18]

Die Grafik zeigt noch einmal den PPP Frame. In diesem Abschnitt möchten wir aber das Information Feld genauer betrachten.
In dem Information Feld wird, zur Verhandlung, wieder ein eigener Rahmen übertragen, der LCP Frame.

2.3.4.1 Code Der Code besteht aus 8 Bits und gibt an welche Aktion ausgeführt werden soll. Die einzelnen Befehle, bzw. Operationen wurden bereits in **??** näher beschrieben.

2.3.4.2 Indentifier Der Indentifier ermöglicht die Unterscheidung, ob ein Rahmen eine Anfrage oder eine Antwort enthält.

2.3.4.3 Length Das Lenght Feld beschreibt die Größe des gesamten Frames. Die gesamte Größe ist die Größe inklusive des Headers. Hier erfährt der Empfänger auch wie viele Daten übertragen wurden.

2.3.4.4 Data/Options Im Data/Options Feld ist der eigentliche Payload enthalten. Die Größe des Feldes ist variabel. Die Daten werden in Form von Optionen gesendet die ebenfalls wieder eine Art Header haben. Der Header besteht aus der Beschreibung der Option, der Länge der Daten und den eigentlichen Daten.

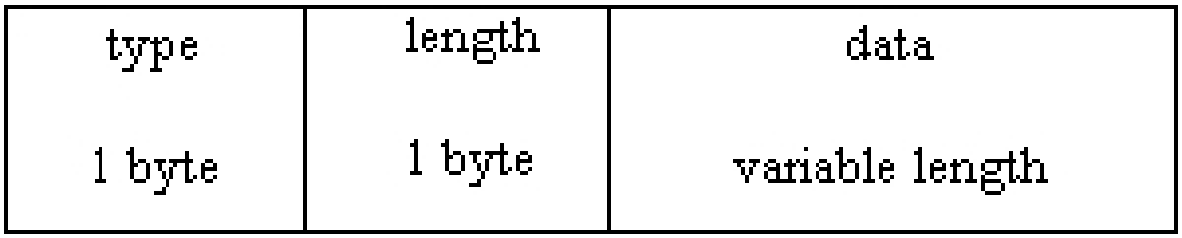

Abbildung 13: Darstellung eines Options Frames innerhalb eines LCP Frames[**ppp-lcp-option-info2.header**]

Für das Type-Feld sind folgende Werte zulässig:

- 1 Maximum-Receive-Unit
- 2 Async-Control-Character-Map
- 3 Authentication-Protocol
- 4 Quality-Protocol
- 5 Magic-Number
- 6 RESERVED
- 7 Protocol-Field-Compression
- 8 Address-and-Control-Field- Compression1

Ein Beispiel für einen LCP Frame wäre ein Frame mit der Option Authentication. Die enthaltenen Daten sind in dem Fall das gewählte Authentication-Protocol.

3 Vergleich der Protokolle

3.1 Frames

Ethernet nutzt, sieht man von verschiedenen Standards ab, immer die gleichen Frames. Sie haben eine variable Länge, die zwischen 64 und 1518 Byte betragen kann.
LAPD nutzt vier verschiedene Frameformate.
PPP nutzt das selbe Rahmenformat wie HDLC, wobei standardmäßig 7-9 Byte für den eigentlichen Rahmen und 1500 Byte für Nutzdaten genutzt werden.

3.2 Adressierung

Die Adressierungsverfahren der 3 Protokolle unterscheiden sich grundsätzlich.
Ethernet sendet die Adresse von Sender und Empfänger mit. Diese Adressen sind im Normalfall fest vergeben und werden in die Hardware eingebrannt.
LAPD nutzt variable Adressen und sendet nur die Adresse des Teilnehmers mit.
PPP nutzt zwar Adressen, diese sind aber nicht relevant.

3.3 Sendequittierung

Bei Ethernet werden gesendete Frames nicht quittiert.
Beim LDAP müssen die empfangen Frames quittiert werden. Wird ein Frame nicht quittiert, kann das nächste nicht verschickt werden. Wie viele Frames vor dem Quittieren gesendet werden können, regelt die Fenstergröße.
PPP hat keine Sendequittierung.

3.4 Prüfsumme

Alle 3 verglichenen Protokolle arbeiten mit dem CRC Algorithmus. Bei Ethernet und LAPD ist die Prüfsumme auf vier, bzw. zwei Byte festgelegt. Bei PPP ist sie variabel und wird von den Teilnehmern ausgehandelt.

3.5 Sendemodus

Die Übertragung des Ethernet ist sowohl im Halb- als auch im Vollduplex-Modus möglich.
LAPD überträgt, bedingt durch den S_0 Bus, im Vollduplex-Modus.
PPP setzt eine Vollduplex Leitung voraus.

3.6 Exklusivität auf dem Medium

Sowohl Ethernet als auch LAPD nutzen ihr Medium als Shared Medium.
Für PPP ist eine exklusive Leitung als Vorraussetzung gegeben.

3.7 Zusammenfassung

Vergleich	Ethernet	LAPD	PPP
Framegröße	26 Byte + Data	7-8 Byte + Data	7-9 Byte + Data
Data Größe	46-1500 Byte	Variabel	Variabel
Präambel	ja	ja	ja
Präambel Größe	8 Byte (bzw. s. **??**)	1 Byte	1 Byte
Präambel Wert	0101...011	01111110	01111110
Präambel Abschluss	Nein	Ja	Ja
Sende-quittierung	nein	ja	nein
Prüfsumme	ja	ja	ja
Prüfsumme Größe	4 Byte fest	2 Byte fest	max. 4 Byte variabel
Frametypen	1	4	1
Kollisions-kontrolle	ja	ja	Nein
Kollisions-kontrolle-Art	CSMA/CD	CSMA/CA	Nein
Exklusivität	Shared	Shared	not Shared
Sendemodus	Halb- und Vollduplex	Vollduplex	Vollduplex

Literatur

[1] URL: http://www.elektronik-kompendium.de/sites/net/0906111.htm (besucht am 2013).

[2] URL: http://www.umfi98.de/ppp.html.

[3] DJ4UF E. Moltrecht. *Unterschied Duplex Halbduplex*. http://www.dj4uf.de/. 2014.

[4] Rhys Haden. *LAPD Rahmen*. rhyshaden.com. 2014.

[5] *ITU-T Recommendation Q.920*. Recommendation. 1994.

[6] itwissen.info. *Koaxial Kabel*. http://www.itwissen.info/definition/lexikon/Koaxialkabel-COAX-coaxial-cable.html.

[7] Franz-Joachim Kauffels. *Lokale Netze : [Übertragungsmedien, Verkabelungssysteme, Zugriffsverfahren; die Wireless-Revolution: Maschennetze; umfangreiches Referenzmaterial auf CD]*. 16. Aufl., IT-Studienausg., 1. Aufl. Heidelberg: mitp, 2008. ISBN: 978-3-8266-5961-4. URL: http://www.gbv.de/dms/ilmenau/toc/568528190.PDF.

[8] W. Leisch. *Das ISO/OSI Modell*. http://www.leisch.org/images/osi.jpg. 2001.

[9] Stefan Müller. *Telefon Hauptkabel (2000 DA), Verzweigungskabel (100 DA) und Installationskabel (6 DA)*. de.wikipedia.org. Jan. 2006.

[10] Kristof Obermann. *Datennetztechnologien für Next Generation Networks : Ethernet, IP, MPLS und andere*. Hrsg. von Martin Horneffer. Wiesbaden, 2013.

[11] pace.edu. *Twistet Pair Kabel*. http://webpage.pace.edu/ms16182p/networking/cables.html. Jan. 2014.

[12] phoenixcontact.com. *Lichtwellenleiter*. https://www.phoenixcontact.com/assets/images_ed/global/web_content/pic_con_a_0042960_int.jpg.

[13] Jörg Rech. *Ethernet : Technologien und Protokolle für die Computervernetzung; [Standard-Ethernet, Fast Ethernet, Gigabit-Ethernet, 10Gigabit-Ethernet, Wireless Ethernet]*. 1. Aufl. Hannover: Heise, 2002. ISBN: 3-88229-186-9.

[14] Gerd Siegmund. *Technik der Netze*. 5., völlig neu bearb. und erw. Aufl. Titel später ersch. im Verl. moderne industrie Buch AG & Co.KG. Teilw. ersichtlich vom Etikett des Verl. moderne industrie Buch mit neuer 2. ISBN. Heidelberg: Hüthig, 2002. ISBN: 3-7785-3954-X; 3-8266-5021-2. URL: http://www.gbv.de/dms/ilmenau/toc/342664387siegm.PDF.

[15] Infra Struktur. *ISDN Kabel*. http://blog.infra-struktur.de/. 2007.

[16] Inc. Tampa Bay Interactive. *Ethernet 802.3 Frame*. http://telecom.tbi.net/novphy2.gif. 2004.

[17] Andrew S. Tanenbaum. *Computernetzwerke*. Pearson Studiumi-netzwerke. Pearson, 2009. ISBN: 978-3-8273-7046-4. URL: http://www.gbv.de/dms/bs/toc/608656437.pdf.

[18] *Überblick eines PPP Headers*. Feb. 2014. URL: http://technet.microsoft.com/en-us/library/cc768082.aspx.

[19] Debbra Wetteroth. *OSI reference model for telecommunications*. McGraw-Hill telecom professional. New York [u.a.]: McGraw-Hill, 2002. ISBN: 0-07-138041-8.

Abbildungsverzeichnis