Internet Economics III

Burkhard STILLER
Oliver BRAUN
Frank EYERMANN
Arnd HEURSCH
Peter RACZ
(Hrsg.)

Institut für Informationstechnische Systeme, IIS

Bericht Nr. 2004-01
Februar 2004

Universität der Bundeswehr München

Fakultät für

INFORMATIK

Werner-Heisenberg-Weg 39 • D-85577 Neubiberg

B. Stiller, O. Braun, F. Eyermann, A. Heursch, P. Racz (edts.): Internet Economics III
Technical Report No. 2004-01, Februar 2004
Information Systems Laboratory IIS, Departement of Computer Science
University of the Federal Armed Forces Munich
Werner-Heisenberg-Weg 39, D-85577 Neubiberg, Germany
URL: http://www.informatik.unibw-muenchen.de/

Introduction

The Information System Laboratory (Institut für Informationstechnische Systeme, IIS) of the Department of Computer Science, University of the Federal Armed Forces Munich, Germany offered its students again a new update of the seminar entitled "Internet Economics" during the fall term 2003 (HT03).

Internet Economics as a term has found its path into the emerging field of technology, mainly driven by the Internet, and the use of such technology in a highly commercialized environment, essentially characterized by economic means. This environment as a whole covers the network itself — mainly described by technology and network operational views — and addresses its public use for applications and for customers. Additionally, this interaction between the network and the customer determines the boundary at which the exchange of payload (user data) must be specified in standards, however, where commercial relations in terms of Service Level Agreements and the specification of tariffs and prices has to take place. Therefore, these challenging interfaces and their use in practical systems has been the key driver for this term's seminar.

Content

This third edition of the seminar entitled "Internet Economics III" discusses in the first chapter the basis of all networking, the operating system required at hosts or end-systems. In particular, the view is directed toward Linux, which is investigated with respect to its networking features and its position in the current market.

The second chapter addresses a key basis for any charging tasks to be performed, either transport or content: the metering technology. The Internet view, as defined in the Real Time Flow Measurement group, and the Internet Protocol Data Record approach are discussed and their effects on service metering are outlined.

The following chapter discusses possible technologies for electronic payment systems. A presentation of key approaches, their advantages, and drawbacks is utilized to discuss the European perspective in their practical application in real life.

In addition, the fourth chapter combines the charging approach with a highly decentralized networking paradigm, a peer-to-peer system. Based on a small risk analysis the basics for peer-to-peer systems, pricing, and trust are outlined. A solution proposal in terms of a referral system and incentives concludes this chapter.

The fifth chapter returns the view on the network, but not the one used today. IPv6 as the successor of IPv4 will come at one day, however, the question is, will it be an enabler or an obstacle for e-commerce? This chapter runs through the IPv6 protocol and the Internet Service Provider model. Based on those statements important aspects of e-commerce applications, required from a networking protocol, are outlined.

Finally, the last chapter addresses a clear application perspective on content distribution networks. The key characteristics and advantages of such networks are summarized and applied mechanisms for an operational system are discussed.

Seminar Operation

All interested students worked on an initially offered set of papers and book chapters, relating to the topic titles as presented in the Table of Content below. They prepared a written chapter as a focussed summary and an evaluation of the key topics. Each of these chapters is included in this technical report and allows for an overview on important areas of concern, business models in operation, and problems encountered. In addition, every student prepared a slide presentation of approximately 45 minutes to present his findings and summaries to a varying audience of students attending the seminar and other interested students or research assistants. Following a general question and answer part, a student-lead discussion debated lively open issues and critical statements with the audience.

Local IIS support for talks, reports, and their preparation by students is granted to Peter Racz, Arnd Heursch, Frank Eyermann, Oliver Braun, and Burkhard Stiller. A larger number of pre-presentation discussions have provided valuable insights in the emerging and moving field of Internet Economics and their currently visible effects, both for students and supervisors. Many thanks to all people contributing to the success of this event!

Neubiberg, February 2004

Inhaltsverzeichnis

Kapitel 1

Networking with Linux - Technology and Market

Volker Förster

This work describes the development of Linux based on an economical and technical point of view. In recent years Linux became more and more popular. Especially in the server section where Linux has become one of the major operating systems besides Windows. In the home section on the other hand, the total share of the market stayed almost constant over the past few years at around 5 %.
Different studies came to different results regarding the question, whether the total cost of ownership is higher for Windows or for Linux. One important reason to select Linux as favorite operating system is the big variety of technologies and options implemented in the Linux Kernel.
Linux offers many different queuing and routing algorithms, for example CBQ, PRIO, SFQ, Policy Routing etc. In addition to this, today's Linux Kernels provides implementations of future-oriented technologies such as IPv6, VPN and IPSec, which can often be found in other operating systems only as additional, sometimes commercial software. Furthermore Linux is able to serve as WAN Router, so that it can replace costly hardware router in that environment.
The list of features is extended by other services, for example: combining a cluster of server to one virtual server, the ressource reservation protocol (RSVP) and many more.
The numerous features regarding network management and service seem to justify the growth of Linux in the server section. On the other hand this variety of features and complexity could be the reason for Linux having only small success in the home section yet, since administration of all these features requires some competence and time to get along.

Inhaltsangabe

1.1 Einleitung

In der heutigen Zeit wird das Wort Linux immer präsenter. Sei es in der Werbung, sei es im Finanzsektor oder in den täglichen Nachrichten. Immer häufiger hört man von den vielen Erfolgsmeldungen oder Vorzügen von Linux. Es gibt sogar Meldungen, die Linux als ernstzunehmende Konkurrenz von Microsoft Windows sehen, und Linux eine große Verbreitung zusprechen.
Allerdings ist der Kontext, in dem das Wort Linux fällt, meist immer auf den Business Sektor begrenzt, und die wenigsten Privatanwender, die sich in Elektronikmärkten einen Personal Computer zulegen, finden dort Linux als Betriebssystem vor. Hauptsächlich im Serverbereich taucht das Open Source Betriebssystem auf, was die Frage aufwirft, ob sich Linux wirklich nur in diesem Bereich bis dato durchsetzen konnte.
Im Rahmen dieser Seminararbeit soll daher untersucht werden, wie die Entwicklung und Verbreitung von Linux in den letzten Jahren vorangeschritten ist, vor allem in welchen Bereichen der Wirtschaft. Komplexität und Einsatzkosten werden hier genauso von Belang sein, wie Bedienbarkeit, Wartbarkeit und Wartungsaufwand. Neben der wirtschaftlichen Sicht sollen Gründe für diese Verbreitung auch aus technischer Sicht aufgedeckt werden. Networking wird hier zentraler Gegenstand der Untersuchungen sein, da dies in den Haupteinsatzbereichen von Linux am häufigsten von Nöten ist, wie sich im Verlauf der Arbeit zeigen wird. Der Einblick wird hierbei über allgemeine Dienste wie http, ftp, mail usw. hinausgehen und eher besondere Eigenschaften vorstellen, die im normalen Umgang mit Linux eher unberücksichtigt bleiben. Dazu zählen verschiedene Queuing Algorithmen, IPv6, VPN u.ä..
Die vorgestellten Implementierungen entstammen dabei aus dem neuen Kernel 2.6.0, der in der Beta-Version zum Einsatz kommt, sowie dem Kernel der aktuellen Suse Linux Distribution 9.0, der bereits einige Features des Kernels 2.6.0 mit sich bringt, und bei einigen Anwendungen stabiler läuft.

1.1.1 Gliederung des Dokuments

Die Gliederung des Dokuments passt sich der bereits in der Einleitung beschriebenen Fragestellung an. So wird nach einer kurzen Einführung zu Hintergründen von Linux die zugrunde liegende Literatur angegeben werden. Im Anschluss daran soll die erste große Frage, die Gegenstand dieser Seminararbeit ist, behandelt werden: Die Entwicklung und Verbreitung von Linux in den vergangenen Jahren.
Wie bereits in der Einleitung angedeutet, werden hier der Home und Business Sektor getrennt behandelt, da sich die Entwicklungen in diesen Bereichen stark voneinander unterscheiden. Im Anschluss daran soll der Installations- und Wartungsaufwand von Linux beleuchtet, und daraufhin mit dem von Microsoft Windows verglichen werden. Dies wird als wichtiger Grund für die Umstellung auf Linux angegeben. Den Abschluss der wirtschaftlichen Fragestellung bildet ein Vergleich der zugrunde liegenden Konzepte, Open Source und Lizenzvergabe, welcher auch gleichzeitig den Übergang zum technischen Teil der Seminararbeit darstellt.
In diesem Abschnitt sollen zuerst allgemeine Dienste wie z.B. http, ftp usw. kurz vorgestellt, und ein Einblick in die Netzwerk-relevanten Komponenten gegeben werden, um

dann davon ausgehend, im nächsten Punkt auf spezielle Netzwerkkonzepte einzugehen. Hierzu werden als erstes spezielle Queuing Algorithmen vorgestellt, welche auch unter dem Oberbegriff QoS Support in Linux zusammengefasst werden können. Dabei sollen auch Beispiele für den Einsatz unter Linux angegeben werden.
Als nächster Punkt sollen Routing-Algorithmen in Linux vorgestellt, und sowohl auf iptables wie auch auf Routingtabellen eingegangen werden. Den Schwerpunkt der technischen Fragestellung bilden VPN und IPv6, die unmittelbar den Routingstrategien folgen. Der Schwerpunkt liegt in diesen Kapiteln, da sowohl die Sicherheit in Netzwerken wie auch IPv6, dessen Einführung ja ohne Frage in nicht allzu ferner Zukunft begonnen wird, bereits jetzt ausführlich diskutierte Themenbereiche sind, deren konkreter Einsatz allerdings bis dato in den wenigsten Fällen durchgeführt wurde. Den Abschluss dieses Abschnittes bildet eine kurze Erläuterung zur WAN Unterstützung von Linux und eine Vorstellung Dienste höherer Schichten.
Im letzten Abschnitt wird der Inhalt zusammengefasst und versucht, einen Ausblick über die Entwicklung von Linux aufgrund der in der Arbeit gesammelten Information zu geben.

1.1.2 Geschichte und Entwicklung von Linux

Linux ist im Vergleich zu Microsoft Windows ein recht junges Betriebssystem (vorausgesetzt man sieht die Kombination von MSDOS und Windows als Urahn des heutigen Windows an). Es ist ein frei verfügbares Betriebssystem, das aus Minix entsprang. Der Grund war hauptsächlich der Mangel an Fähigkeiten, den Minix (bewusst) mit sich brachte. Anders als Minix besitzt es daher keinen Mikrokern, sondern einen monolithischen Ansatz. Linux wurde 1991 von Linus Torvalds, einem finnischen Studenten entwickelt und ist kompatibel zum POSIX-1003.1 Standard. 1992 verbreitete Linus die erste Version über FTP im Internet, was die Anzahl der Tester enorm erhöhte. Dies war auch der Ursprung für den Zustand, dass Linux unter offenen und verteilte Bedingungen entwickelt werden konnte. Einer der Hauptvorteile daran ist, dass Linux meist von Studenten auf begrenzten Ressourcen weiterentwickelt wurde und wird, und damit sehr effizient mit Ressourcen umgeht. Im Laufe des Jahres 1993 wurde der Linux Kernel an die GNU Umgebung der Free Software Foundation angepasst. Dies ermöglichte die Nutzung einer großen Sammlung von damals bereits existierender Software. 1994 wurde die Netzwerkfähigkeit in Linux integriert, was einen weiteren, enormen Anstieg der Userzahl mit sich brachte. Als weiterer wichtiger Schritt folgte im Jahre 1995 die endgültige Freigabe der Linux Quellen durch Linus Torvalds, indem er Linux unter die GPL stellte. Im gleichen Jahr wird eine grafische Benutzerschnittstelle für Linux durch das XFree86-Projekt erstellt. Im darauf folgenden Jahr folgte die Portierung auf andere Plattformen und 1996 schließlich die Fähigkeit von Linux, Prozesse auf mehrere Prozessoren zu verteilen, und diese zu verwalten. Ebenso wurde es durch die 1996 erschienene Version 2.0 möglich, Linux auch auf 64 bit Architekturen zu portieren. Im folgenden Jahr begann die Portierung von Software namhafter Hersteller auf Linux, wie z.B. der Webbrowser von Netscape.
Im Jahre 1998 erfolgt nun ein wichtiger Schritt. Das Desktop Projekt KDE wird begonnen. KDE ist neben GNOME heutzutage eine von zwei GUIs, die für Linux erstellt wurden. Ein weiterer wichtiger Punkt in diesem Jahre, waren Ankündigungen von IBM und Compaq, Linux jetzt als Betriebssystem für ihre Server einsetzen wollen. Im Jahre 1999 wurde

schließlich, wie schon oben erwähnt, mit der Entwicklung der GNOME Umgebung begonnen. Die Jahre 2000 bis heute sind von vielen Weiterentwicklungen geprägt. Als wichtiger Punkt ist noch die Veröffentlichung des Quellcodes von StarOffice zu nennen, was als Grundstein für das heute in Linux vorhandene OpenOffice diente.
Anhand dieser Entwicklung soll es dem Leser nun möglich sein, die im Abschnitt Market dargelegte Entwicklung von Linux auch nachvollziehen zu können. Man wird Parallelen zwischen den technischen Fortschritten und Erweiterungen und dem Absatz von Linux entdecken.

1.1.3 Zugrunde liegende Literatur

Ein Grossteil der Literatur der ersten Hälfte der Seminararbeit besteht aus Onlineberichten über Studien, die zur Bestimmung des Marktanteils von Betriebssystemen durchgeführt worden sind. Die Quellen mögen zwar veraltet erscheinen, es sei jedoch darauf hingewiesen, dass aktuelle Zahlen meist nur gegen Bezahlung zur Verfügung standen, und deshalb oft nur die Entwicklung bis in das Jahr 2000 beschrieben werden kann. Die zweite Hälfte der Seminararbeit beruht stark auf der Dokumentation des Linux Kernels 2.6.0-test8, sowie Online-Beschreibungen zu den augeführten Funktionen. Implementierungsaspekte und Hintergründe lieferte *Linux Kernel-programmierung* [Kernel] besonders im Bezug auf die Implementierung des ISO/OSI Schichtenmodells in Linux.
Allgemeine Informationen über Betriebssysteme, hier besonders Windows und Linux, finden sich auch in *Moderne Betriebssysteme* [Tanen] welches neben dem Sammeln von Hintergrundinformationen, einen Einblick in die Arbeitsweise und die zugrundeliegende Betriebssystemtheorie ermöglicht.

1.2 Market

Nachdem nun ein kurzer Einblick in die zeitliche Entwicklung gegeben wurde, soll untersucht werden, wie sich Linux in bestimmten Bereichen der Wirtschaft durchsetzen konnte. Die schon oben angesprochene, immer häufigere Präsenz von Linux im täglichen Leben lässt erahnen, dass sich die Bedeutung von Linux und damit auch sein Marktanteil in den letzten Jahren deutlich verändert hat.
Zunächst soll eine Betrachtung des Marktanteils erfolgen, aufgeteilt nach Home und Business Section. Dies ist notwendig, da in diesen Bereichen sehr unterschiedliche Anforderungen an ein Betriebssystem gestellt werden. Diese unterschiedlichen Anforderungen führen schließlich auch zu einer unterschiedlichen Bewertung des Systems und damit auch zu einer unterschiedlichen Einsatzhäufigkeit. Man kann zwar eine starke Konvergenz der Betriebssysteme feststellen [Tanen], dennoch wird sich im Laufe der Untersuchung zeigen, dass Nutzer Linux als Server- und PC-Betriebssystem unterschiedlich bewerten.

1.2.1 Entwicklung des Absatzes

Die Entwicklung des Absatzes lässt sich gut anhand verschiedener Studien nachvollziehen, die den Absatz von Linux in den Jahren 1996 - 2002 beschreiben. Dennoch sei angemerkt, dass Linux aufgrund seiner Open Source Charakteristik auch im Internet frei verfügbar ist, und deshalb diese Prognosen keine 100%igen Aussagen geben können [Linmag]. Zu hoch könnte der Anteil der Nutzer sein, die Linux aus den Internetquellen beziehen und einsetzen.
Dies erklärt auch die im Folgenden auftretenden Widersprüche bzw. Unstimmigkeiten in den Ergebnissen. Ein weiterer wichtiger Faktor ist der Auftraggeber der Studie, da sich hier unterschiedliche Ziele hinter den in Auftrag gegebenen Studien verbergen.
Ein besonderen Bereich bilden die Embedded Systems, die ja ebenfalls eigene Anforderungen an ein Betriebssystem mit sich bringen. Der Grund, warum dies hier nicht näher behandelt wird, ist die Tatsache, dass das Einsatzgebiet von Embedded Systems viel zu groß ist, als dass ein Universalbetriebssystem all diese Anforderungen abdecken könnte. Weiterhin existieren in diesem Bereich hauptsächlich proprietäre Systeme, bei denen die Hersteller nicht möchten, Entwicklungen die sie bezüglich der Software getätigt haben im Zuge von Open Source der Öffentlichkeit zur Verfügung zu stellen. Dadurch wäre es Mitbewerbern möglich, die eingesetzte Software wiederzuverwenden, und damit die Entwicklungskosten zu sparen, was keinesfalls im Interesse der Hersteller ist. Linux kommt zwar auch in diesem Bereich zum Einsatz, jedoch werden hier keine großen Veränderungen oder Durchbrüche erwartet [enet].

1.2.1.1 Desktop Section

Der Marktanteil der Home Section zeigt ein anderes Bild, als es im Server-/Businessbereich der Fall ist, wie sich noch zeigen wird. Allerdings ist auch hier die zukünftige Entwicklung ungewiss, da sich auch hier Zahlen finden lassen, die gegen ein weiteres Wachstum sprechen.
Drei Studien aus dem Jahre 2001 und 2002 beschreiben den Marktanteil von Linux im Desktop Bereich:

- IDC-Studie (2001): Die IDC Studie gibt einen Marktanteil von Linux für den Privatbereich in Höhe von 4% an. Das dies keine hohe Zahl ist zeigt der Vergleich mit dem MAC-OS, dem in dieser Studie ein Marktanteil von 5-6% zugesprochen wurde. Außerdem wurde in dieser Studie explizit vorhergesagt, dass ein Durchbruch von Linux im Heim-Bereich ausbleiben wird. Hier zeigt sich das erste Mal, wie unterschiedlich die Studien ausfallen können, wenn man die Suse Emnid Studie zum Vergleich heranzieht [ProLin].

- SUSE-Emnid Studie (2001): Die SUSE-Emnid Studie geht nicht direkt auf den Marktanteil von Linux ein. Sie versucht vielmehr die zukünftige Entwicklung zu prognostizieren. So würden nach dieser Studie 10 % der Anwender bei einem neuen System auf Linux umsteigen, 23 % würden diesen Schritt zumindest erwägen

[ProLin]. Außerdem gibt diese Studie an, dass 46 % aller Linux Nutzer Stabilität als wichtigstes Kriterium ihres Betriebssystems angeben, während es unter den Windows Nutzern nur 13 % sind, die ihr Betriebssystem als besonders stabil charakterisieren. Auch hier werden, ähnlich wie in der Metagroup Studie, fehlende Anwendungsprogramme als Grund für den nur spärlichen Wechsel zu Linux genannt [about].

Das die damaligen Zahlen auch heute nicht an Gültigkeit verloren haben, zeigt eine aktuelle Metagroup Studie des Jahres 2002:

- Meta Group Studie (2002): Die Meta Group beziffert den Marktanteil von Linux als Desktop Betriebssystem auf 7 %. In dieser Studie werden auch Gründe für den bis dato recht geringen Einsatz von Linux im Desktop Bereich gegeben. Wichtige Punkte sind dabei fehlende Anwendungen, Dominanz der Microsoft Produkte, schlechter Bedienkomfort und enormer Support-Aufwand. Weiterhin besitzen Microsoft Produkte, so Metagroup, eine hohe Funktionalität und sind aufgrund ihrer „ guten Integration in Serveranwendungen nicht leicht zu ersetzen“. Genauso wird gesagt, dass eine „Linux-Welle im Desktop Bereich nicht erwartet wird“ [metagroup].

Man sieht auch bereits, dass sich Linux im Home Bereich, trotz leichter Unterschiede zwischen den einzelnen Studien bislang noch nicht durchsetzen konnte. Man kann zwar einen leichten Anstieg erkennen, aber von einem Durchbruch kann nicht die Rede sein.
Im Bezug auf die kommende Entwicklung gibt es bereits heute Prognosen, die Linux einen Marktanteil von 20 % in 5 Jahren vorhersagen [NForge], ob diese Prognosen jedoch Recht behalten, oder ob sie nur auf momentanen Entwicklungen wie dem Einsatz von Linux im Bundestag oder bei der Stadt München beruhen [symlink] ist schwer zu sagen. Bereits im Jahre 2000 wurde vereinzelt ein Durchbruch auf dem Desktop prophezeit [ProLin] , welcher jedoch ausblieb. Da es jedoch auch anders lautende Stimmen bezüglich Linux als Desktop Betriebssystem gibt [enet], kann hier, anders als im Server Bereich, keine Prognose abgegeben werden.

1.2.1.2 Server Section

Im Server-/Businessbereich zeigt die Betrachtung des gleichen Zeitraumes jedoch etwas anderes, als dies im Desktop Bereich der Fall ist. Der Marktanteil von Linux ist in den Jahren 1996 - 2000 erheblich gestiegen und stellt hier nicht mehr wie im Desktop-Bereich nur einen kleinen Bereich dar. Dabei fällt auf, dass auch hier der Einsatzbereich entscheidend ist für die Durchdringung des Linux Betriebssystems.
Abbildung 1.1 zeigt die Entwicklung verschiedener Webserver. Die Zahlen stammen aus dem Jahre 2000 von Netcraft. Diese zeigt vor allem den starken Marktanteilsgewinn von Apache, welcher hauptsächlich auf Linux und Solaris läuft, während die Microsoft Server einen eine leichten Rückgang hinnehmen mussten [Linmag].
Löst man sich von der Betrachtung einzelner Webserver, und betrachtet die Entwicklung von Linux als Betriebssystem an sich, erkennt man ebenfalls das große Wachstum, dass Linux in den Jahren 1998-1999 mit sich brachte. Abbildung 1.2. gibt Zahlen einer IDC

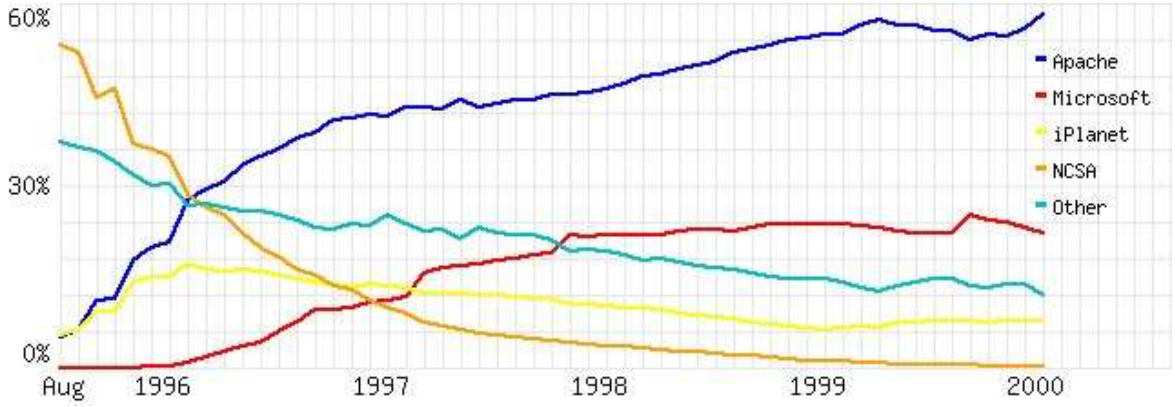

Abbildung 1.1: Entwicklung von Server Software 1996 - 2000 [Linmag]

Studie aus dem Jahre 2000 wieder, die dieses Wachstum bestätigt.
Es wird deutlich, dass Unix der Hauptverlierer aufgrund des Wachstums von Linux ist. Das dieses ebenfalls heute noch aktuell ist, zeigen die Zahlen der Metagroup Studie aus dem Jahre 2002. In dieser wird der Anteil von Linux an neuen Server-Betriebssysteminstallationen auf 15-20 % beziffert.

Marktanteile

Betriebssystem	**1998**	**1999**
Windows NT	38	38
Linux	16	25
Netware	23	19
UNIX	19	15
Andere	4	3

Marktanteile weltweit

Tabelle 1.1.: Linux Marktanteilentwicklung 1998/1999 [Inform]

Weiterhin wird bestätigt, dass „die Unix-Betriebssysteme immer stärker aus der allgemeinen Serverlandschaft in den Bereich der Datenbanksysteme zurückgedrängt“ werden [metagroup].
Die Frage, die sich aufgrund des starken Zuwachs von Linux im Serverbereich aufdrängt, ist die nach den Einsatzbereichen von Linux. Innerhalb des Serverbereiches lassen sich geschäftskritische und nicht geschäftskritische Einsatzbereiche unterscheiden und die hier eingesetzten Betriebssysteme spiegeln dies hauptsächlich im Vertrauen, dass der Nutzer ihnen entgegenbringt, wider. Da Linux allgemein noch ein recht junges Betriebssystem ist, wurde es hauptsächlich in nicht geschäftskritischen Bereichen bis dato eingesetzt, jedoch zeigt sich aktuell auch hier ein Wandel. Abbildung 1.2 gibt die Einsatzgebiete von Linux im Serverbereich wieder.
Der Wandel lässt sich durch die Bewährung von Linux im nicht geschäftskritischen Bereich erklären. Die Unternehmen, die Linux bereits im Einsatz haben, halten es für ausgereift genug, nun auch im geschäftskritischen Bereich, wie etwa Datenbankanwendungen, Dienste zu leisten [enet].
Bei der Betrachtung dieser Zahlen kann man die Frage stellen, ob sich aufgrund dieser Entwicklung nicht auch die zukünftige Entwicklung von Linux vorhersagen lassen wird.

Eine genaue Antwort auf diese Frage kann aber nicht gegeben werden. Auf der einen Seite wird zum Beispiel in [metagroup] gesagt, dass Linux vermutlich bis 2006/07 „seinen Anteil auf Intel-Servern auf 45 % aller neu ausgelieferten Server steigern“ kann. Allerdings werden auch in dieser Studie Bedingungen für dieses Wachstum angegeben.

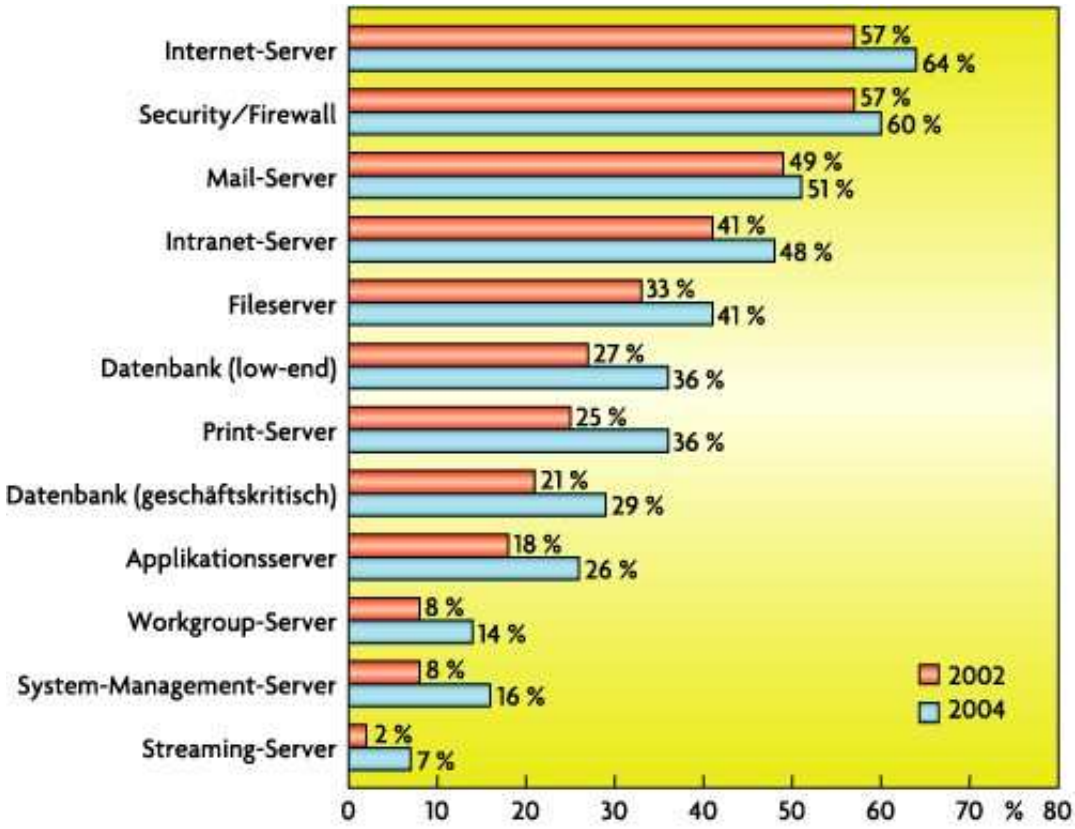

Abbildung 1.2: Wofür wird Linux in ihrem Unternehmen eingesetzt? [enet]

Als wichtigste Punkte werden der Reifegrad von Linux, sprich die technologische Weiterentwicklung, und die Total Cost of Ownership (TCO) genannt, die im nächsten Abschnitt noch näher beleuchtet werden sollen. Besonders die Support Kosten, die bei Linux im Vergleich zu anderen, gereiften Betriebssystemen noch sehr hoch sind, müssten fallen, damit ein weiterer Erfolg garantiert werden kann [metagroup].
Auch andere Faktoren, wie die Konkurrenz können Auswirkungen auf die zukünftige Entwicklung haben. Aus den oben angegebenen Zahlen ergab sich noch keine Änderung der Dominanz der Microsoft Betriebssysteme. Nimmt man nun aktuelle Zahlen über den Absatz von Windows Server 2003 hinzu, so findet man neben der durch die Neueinführung bedingten hohen Verkaufszahlen, auch Ergebnisse, die im Widerspruch zu dem rasanten Marktanteilsgewinn von Linux stehen. Abbildung 1.3 zeigt die Entwicklung des Einsatzes von Windows Server 2003. Diese Graphik alleine, zeigt noch keine der angesprochenen Probleme, nimmt man aber die Zahlen aus Tabelle 1.2 hinzu, so fallen die 5 % ehemaliger Linux Rechner auf.

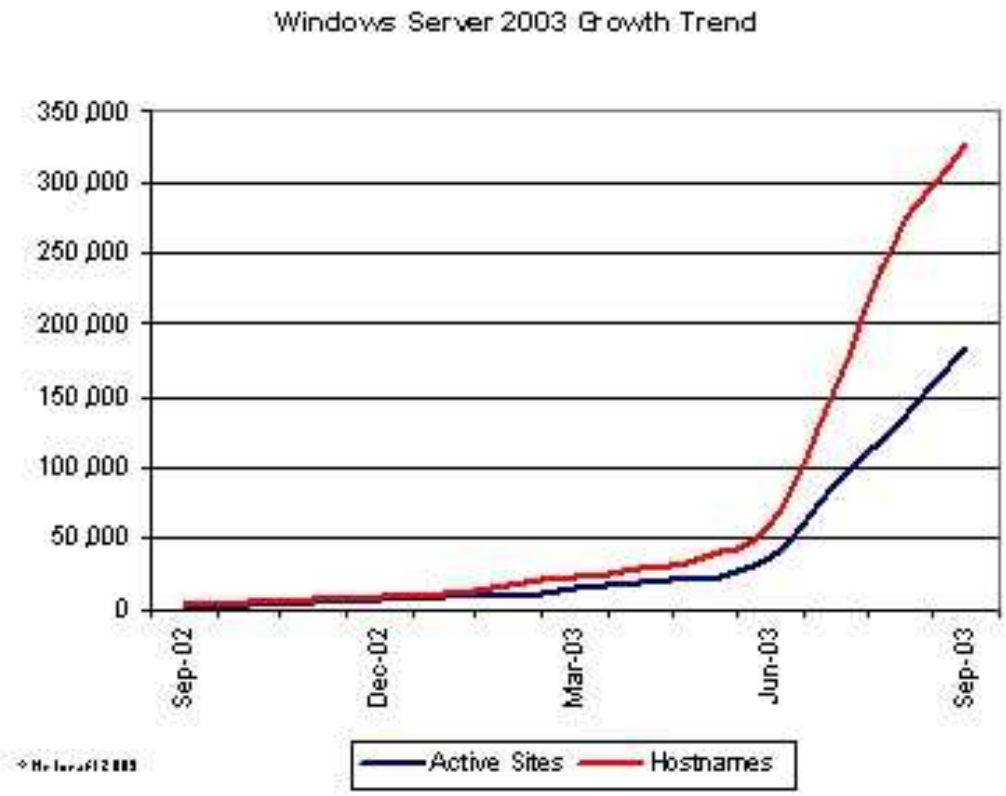

Abbildung 1.3: Entwicklung des Absatzes von Windows Server 2003 [netcra]

Herkunft	
Neue Seiten	42 %
Upgrades	49 %
Linux	5 %
FreeBSD	1 %

Tabelle 1.2.: Herkunft der Windows Server 2003 Rechner [netcra]

Und diese 5 % waren nicht nur ein einmaliges Ereignis bedingt durch die Einführung von Windows Server 2003, sondern hielten bis September 2003 an. Es findet also eine kontinuierlich Abwanderung statt [netcra].
Diese Beispiele machen deutlich, dass die Zahlen der Studien zwar eine positive Entwicklung von Linux in der Vergangenheit dokumentieren, dass sich anhand dieser Entwicklung aber nur vage Informationen über die Zukunft gewinnen lassen. Zu viele Faktoren spielen für eine genaue Prognose eine Rolle.
Nachdem nun die Entwicklung im Server Bereich dargelegt wurde, soll nun auch nach den Gründen für den Marktanteilsgewinn von Linux gesucht werden. Dazu wird der Installations- und Wartungsaufwand, und damit auch die TCO (Total Cost of Ownership) für den Desktop und Server Bereich bestimmt.

1.2.2 Total Cost of Ownership

Bevor der Installations- und Wartungsaufwand jedoch im Detail besprochen werden kann, soll erst der Begriff TCO (Total Cost of Ownership) aufgeschlüsselt werden.
Die Kosten für ein Betriebssystem werden nicht nur durch die Anschaffungskosten bestimmt. Im Gegenteil sie machen nur 20 % der Gesamtkosten aus. Abbildung 1.4 zeigt die Aufteilung der Gesamtkosten eines Betriebssystems. Die restlichen Bereiche, auch

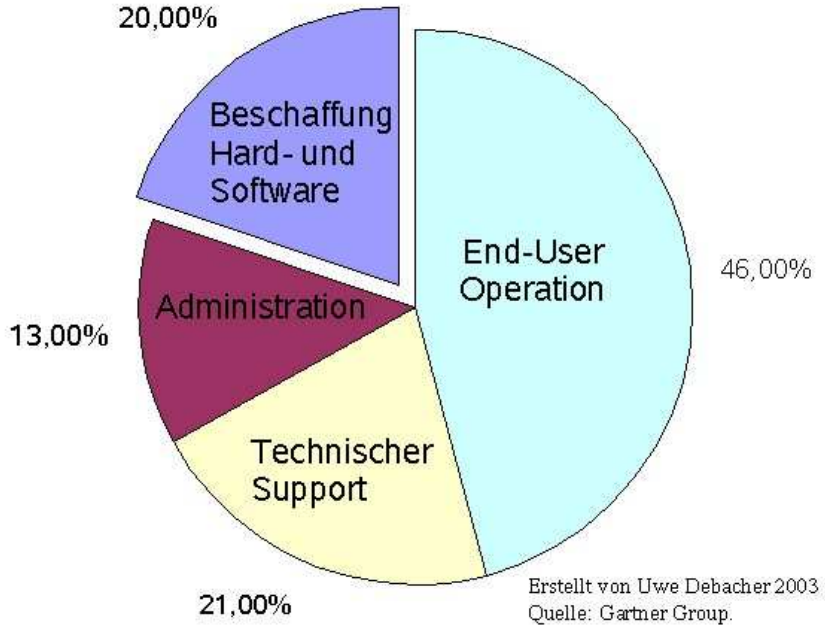

Abbildung 1.4: Unterteilung von TCO [linHH]

unter dem allgemeinen Begriff Support und Wartung zusammenzufassen, machen einen wesentlich grösseren Teil dieser Kosten aus. Besonders die Betreuung und Schulung von Benutzern stellen hierbei einen großen Teil der Kosten. Dies erklärt auch später folgende Ergebnisse, dass Windows, trotz Lizenzgebühren, bei der Anschaffung kostengünstiger als das lizenzfreie Linux sein kann. Wie schon öft erwähnt hat der Einsatzbereich eines Betriebssystems große Auswirkungen. Auch bei der Bestimmung von TCO ist dies der Fall. Die Ergebnisse unterscheiden sich innerhalb des Serverbereiches so stark, dass die Frage welches Betriebssystem nun günstiger ist, nicht allgemein beantwortet werden kann. Weiterhin ergeben sich immer Probleme bei der Betrachtung von Studien. So, muss man neben dem Auftraggeber auch zugrunde liegende Daten, Unternehmensgröße, Randfaktoren, Rabatte, usw. berücksichtigen [linWo]. Aufgrund dieser Faktoren, liefern viele der durchgeführten Studien, unterschiedliche, und teilweise sogar widersprüchliche Ergebnisse. Im Folgenden sollen zwei Studien exemplarisch für den Server-Bereich dargestellt werden. Es bleibt dem Leser überlassen, sich im Internet nach weiteren Studien umzusehen. Die folgenden Studien zeigen beispielhaft, wie sehr sich die TCO eines Betriebssystems unterscheiden können. Deshalb wird im Folgenden zwischen Webservern und File-/Printservern unterschieden.
Wie schon in Abbildung 1.2 gezeigt, hat Linux seinen Haupteinsatzbereich unter den Webservern. Betrachtet man nun die TCO, so wird dies auch deutlich. Abbildung 1.5

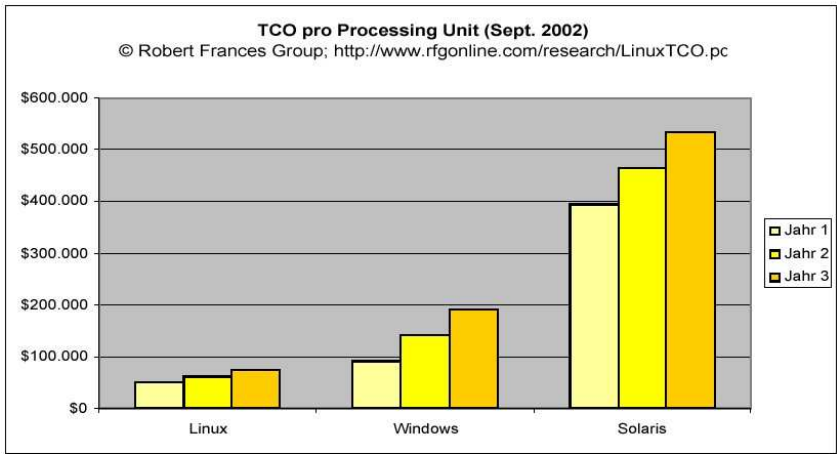

Abbildung 1.5: TCO bei Webservern[linWo]

zeigt die Kosten für Linux im Einsatzbereich eines Webservers. Die Studie wurde von IBM im Jahre 2002 in Auftrag gegeben wurde. Die darin vorgestellte Kostenersparnis wird auch in einer von Microsoft in Auftrag gegebenen IDC Studie aus dem Jahre 2002 bestätigt [IDC].
Im Enterprise Bereich, besonders im Bezug auf File-, Netzwerk- und Printserver gibt es jedoch Studien, die Windows als günstigeres Betriebssystem sehen. So die IDC Studie aus dem Jahre 2002, die von Microsoft in Auftrag gegeben wurde. Ihre Ergebnisse werden in Abbildung 1.6 dargestellt.

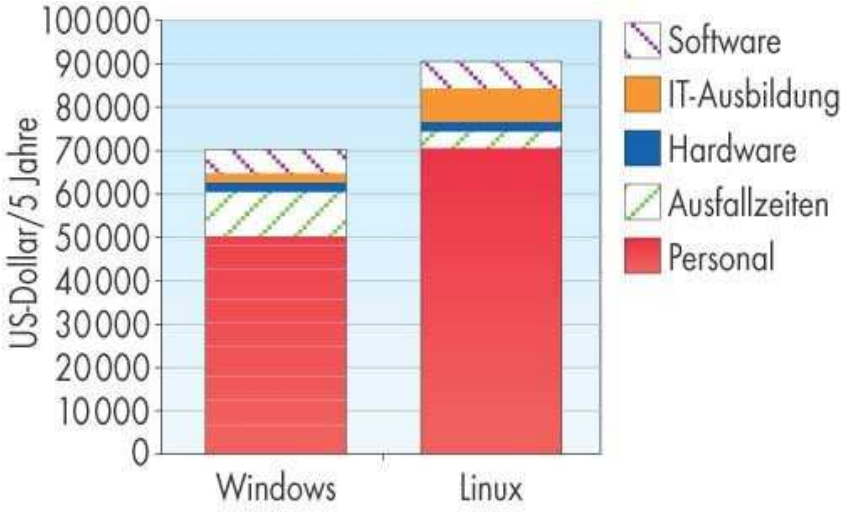

Abbildung 1.6: TCO Windows und Linux als File-,Netzwerk-, und Printserver[IDC]

Es fallen vor allem die deutlich erhöhten Personalkosten auf, die in fast allen Studien auf Seiten von Linux auftauchen, und in der hohen Komplexität begründet sind. Auf der anderen Seite kann Linux geringere Ausfallzeiten für sich verbuchen, da bei Linux meist „on the fly“ geupdated werden kann. Es gibt jedoch bereits Studien, die das Gegenteil dieser

Studie belegen, wie z.B. die Soreon Studien des Jahres 2003 [linWo] und selbst in der IDC Studie wird gesagt, dass „durch die Entwicklung besserer Software für das Netzwerkmanagement unter Linux – wie etwa HP OpenView und IBM Tivoli – der Kostennachteil gegenüber Windows 2000 schwinden werde“ [IDC]. Man sieht also, dass sich Linux auch hier in nicht allzu ferner Zukunft durchsetzen könnte.
Eine eventuelle Ersparnis beim Einsatz von Linux kann, wie gesehen, nur schwer durch Studien beschrieben werden. Dass jedoch durchaus Einsparpotential vorhanden ist, zeigt das Beispiel von Merrill Lynch: Durch den Einsatz von virtuellen Linux Servern, anstelle der Microsoft Exchange Server sollen dort 600000 Dollar Hardwarekosten und sogar fünf mal so viel an Personalkosten für den Support gespart werden [InfoW2].
Im Desktop Bereich ist diese Situation noch eine andere, da hier die TCO noch durch andere Faktoren bestimmt werden. Es kommt hier viel mehr als im Server Bereich zu tragen, dass Linux ein sehr junges Betriebssystem ist, dessen Akzeptanz noch sehr gering ist. Selbst innerhalb einer Studie gibt es unterschiedliche Aussagen, die weder für das eine noch das andere Betriebssystem sprechen. Eine aktuelle Studie der Gartner Group aus dem Jahre 2003 gibt die TCO eines Linux Desktops für Büroarbeiten - basierend auf einer Hardware Laufzeit von 3 Jahren - mit US$ 5305 an, bzw. US$ 4402 wenn der Nutzer keinen root Zugang erhält. Windows XP liegt mit US$ 5148 genau dazwischen. Betrachtet man neben den regulären Büroarbeiten komplizierte Arbeiten, wie das konzeptionelle Auswerten von Daten etc., so verschieben sich die Zahlen nur leicht nach oben, an der eigentlichen Aussage ändert sich jedoch nichts [newsfact]. Allerdings wird in dieser Studie gesagt, dass ein Wechsel von Windows zu Linux im Desktop Bereich nur sinnvoll ist, wenn wenige Programme zum Einsatz kommen. Bei einer grösseren Vielfalt von eingesetzten Programmen, führe an Windows kein Weg vorbei [newsfact2]. Weiterhin wird hervorgehoben, dass hauptsächlich für Win95 Nutzer ein Wechsel lukrativ sein könne, da dieses System von Microsoft nicht mehr unterstützt wird, während es bei Windows 2000 und Windows XP keine großen Einsparungen gegenüber Linux geben dürfte, da diese neuen Windows Versionen, stabiler, moderner und kostengünstiger seien [newsfact2].
Es kann also auch im Desktop Bereich keine genaue Aussage gemacht werden. Aufgrund der vielen Einflussmöglichkeiten auf die TCO, kann eine Firma vor einem Betriebssystem Wechsel die entstehenden Kosten nur durch eine Analyse in ihrem Betriebsumfeld ermitteln und mit der bestehenden Lösung vergleichen.

1.2.3 Open-Source- vs. Lizenz-Betriebssysteme

Nachdem nun im letzten Abschnitt versucht wurde, die Kosten von Linux mit denen von Windows zu vergleichen, soll das zugrunde liegende Konzept und die vorhandenen Strukturen hinter den Betriebssystemen beleuchtet werden. Damit soll es dem Leser ermöglicht werden, die unterschiedlichen Arbeitsweisen, Funktionsumfänge und technischen Möglichkeiten besser zu verstehen.
Der Ursprung von Open Source Software liegt in der Entwicklung von Unix begründet. AT&T entwickelte 1969 das Betriebssystem Unix, durfte aber mit diesem Betriebssystem als Telefongesellschaft keinen Gewinn machen. Daher wurde Unix gegen eine geringe Gebühr als Lizenz weitergegeben und nicht von AT&T supported. Aus diesem Grund gingen viele Universitäten dazu über, das BS weiter zu entwickeln [Open]. Im Laufe der Jahre folgten dann noch weitere Versuche, ein kostenloses Betriebssystem zu erschaffen. Vor

allem ging es vielen Entwicklern darum, ein freies Entwicklungsumfeld zu besitzen, und unabhängig in der Entwicklung zu sein. Dies brachte den Vorteil der rasanten Weiterentwicklung von Open Source Betriebssystemen, durch die vielen Entwickler. Dem gegenüber steht die Closed Source Vermarktung durch Lizenzen, in deren Vordergrund eine Gewinnmaximierung steht, da das Prinzip dem wirtschaftlichen Sektor entspringt. Hier werden die Features von einer Firma fest vorgegeben, dafür sind die Produktupdateszyklen weitaus größer und sie bleiben in einem notwendigen Rahmen.
Durch seinen großen Erfolg versucht Linux zurzeit den Übergang vom Entwicklungssystem einiger „Hacker“ zum Big Business System zu erreichen, jedoch zeigen die derzeitigen Rechtsstreitigkeiten über Urheberrechtsverletzungen, dass hier auch Probleme lauern können [heise].

1.3 Linux Networking Konzepte

In Abschnitt 1.2 wurde der Durchbruch von Linux vor allem im Bereich der Web-Server aufgezeigt. Da in diesen Bereichen die Netzwerkfunktionalität eines Betriebssystems entscheidend ist, soll in diesem Abschnitt detailliert auf einige Funktionen eingegangen werden. Dabei sollen besonders ausgefallene Funktionen und zukünftige Technologien im Vordergrund stehen, und nicht vertiefend auf Basisdienste, die in fast jedem Betriebssystem vorhanden sind, eingegangen werden.

1.3.1 Protokolle

Bevor einige Details der Networking Funktionen von Linux beschrieben werden, werden noch kurz die Funktionsweise und die dabei verwendeten Protokolle in Linux betrachtet. Die Abbildung 1.7 zeigt den allgemeinen Paketfluss in Linux. Ankommende Pakete wer-

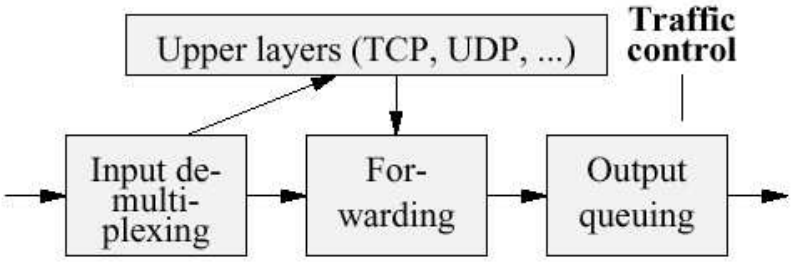

Abbildung 1.7: Verarbeitung von Netzwerkdaten[DffLin]

den entweder weitergeleitet, oder an das entsprechende Protokoll übergeben. Forwarding übernimmt die Wahl des richtigen Interfaces, Kapselung, etc.[DffLin]. Deshalb übergeben höher liegende Protokolle wie TCP/UDP Pakete an diesen Teil der Netzwerk Implementierung. Im Anschluss daran gelangen Pakete zur Queue des entsprechenden Interfaces. Hier werden die im nächsten Abschnitt vorgestellten Queuing Algorithmen zum Einsatz kommen.

Nach dieser allgemeinen Beschreibung, sollen die Schichten auf dem Weg eines Paketes beginnend von der Anwendungsschicht über TCP/IP bis hin zur Bitübertragungsschicht genauer betrachtet werden. Abbildung 1.8 zeigt das Schichtenmodell der Linux Architek-

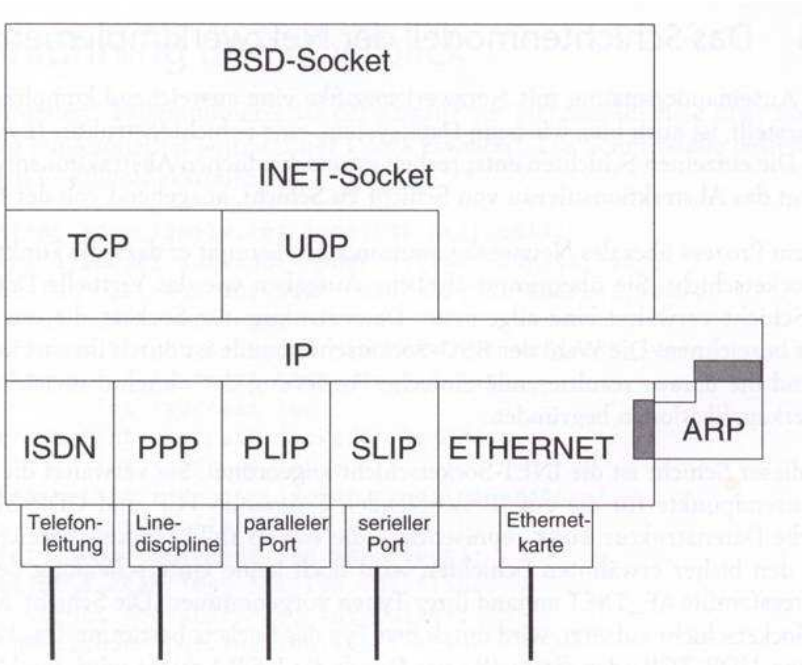

Abbildung 1.8: Layerstruktur in Linux[Kernel]

tur. Während TCP, UDP, IP und Ethernet hinreichend bekannte Protokolle sind, soll hier auf die Linux spezifischen Schichten der BSD- und Inet-Sockets eingegangen werden.
Die BSD-Sockets übernehmen in erster Linie eine Verwaltungsfunktion, ähnlich dem virtuellen Dateisystem. Ihre Hauptaufgabe ist die Verwaltung der allgemeinen Datenstruktur für Sockets. Die darunter liegende Schicht der INET-Sockets hat indessen eine umfassendere Aufgabe. Sie verwaltet die Kommunikationsendpunkte von TCP und UDP und ist damit beim Versenden für die Wahl des richtigen Protokolls zuständig; je nach Typ des Sockets wird TCP, UDP oder auch direkt IP angesprochen. Linux bietet neben den genannten auch noch weitere Sockettypen für ATM, IPv6, AX.25 und andere [Kernel].

1.3.2 Queuing

Nachdem jetzt die Schichten etwas näher betrachtet worden sind, soll jetzt wieder die allgemeine Abbildung 1.7 aufgegriffen und speziell die Ouput Queue betrachtet werden.
In Linux finden sich unter „QoS and/or fair queuing“ verschiedene Queuing Algorithmen. Wird diese Option im Kernel nicht aktiviert, so steht in Linux nur ein einfacher FIFO Queuing Mechanismus zur Verfügung. Durch Aktivierung der Option wird es jedoch möglich, verschiedenen Verbindungen gewisse Garantien zu geben, was vor allem in Soft Real Time Anwendungen benötigt wird. Durch die Aktivierung von QoS Support stehen auch Differentiated Services und das Ressource Reservation Protokoll zur Verfügung, dass im Abschnitt 1.3.8 vorgestellt wird. Die zur Verfügung stehenden Algorithmen sind folgende:

- HTB (Hierarchical Token Buckets): HTB, arbeitet ähnlich wie CBQ, nur mit schärferen Restriktionen. Das bedeutet, werden die Ziele von HTB erfüllt, werden auch die von CBQ erfüllt. HTB teilt eine vorhandene physikalische Bandbreite auf, und stellt so mehrere virtuelle Kanäle bereit. Die Kanäle können wiederum weiter unterteilt werden, so dass eine Baumstruktur entsteht, in der die Blätter die eigentlichen Verbindungen darstellen. Jeder Kanal erhält eine zugesicherte Bandbreite und eine Maximalbandbreite. Dies ist notwendig, da nicht genutzte Bandbreiten zwischen den einzelnen Verbindungen ausgeliehen werden können. Die tatsächlich Bandbreite ergibt sich als Minimum aus Maximalbandbreite und zugesicherter Bandbreite plus ausgeliehener (borrowed) Bandbreite. Zusätzlich bekommen die Kanäle eine Priorität zugewiesen, die vor allem der Zuweisung der Bandbreite dient. Die genaue Funktionsweise des Ausleihens von Bandbreite soll hier nicht näher behandelt werden, da die Erklärung der Funktionsweise recht komplex und sehr umfangreich ist. Sie ist aber unter [HTBTH] nachzulesen.

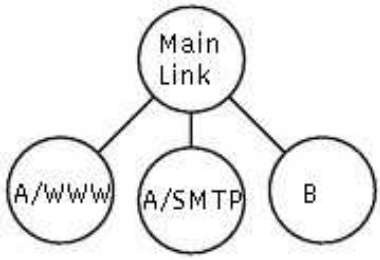

Abbildung 1.9: Beispiel HTB Queuing[HTB]

Zu der Verwendung sollen hier nur die weiteren Ziele des Algorithmus angegeben werden: Verändert ein Kanal seine Bandbreite, soll dies keinen anderen Kanal beeinflussen, außer dieser leiht vom gleichen übergeordneten Knoten aus. Weiterhin sollen hoch-priorosierte Kanäle eine geringere Verzögerung als niedrig-priorisierte Kanäle haben, vorausgesetzt sie liegen auf dem gleichen Level (Tiefe des Baumes). Es werden dadurch Modellierungen wie in Abbildung 1.9 möglich. Hier sind zwei Kunden A und B, von denen jeder einen gewissen Teil der Gesamtbandbreite erhält. Die Bandbreite von Kunden A wird noch einmal unterteilt in eine bestimmte Bandbreite für HTML und eine für alles andere [HTB]. Die Einrichtung von HTB erfolgt über das Kommandozeilentool tc, dass sich im iproute2+tc package befindet, welches auch zur Einrichtung von Policy routing, NAT, advanced tunnels, RSVP, etc. benötigt wird.

- TEQL (True Link Equalizer): Dieser Scheduling Algorithmus ermöglicht es, mehrere physikalische Netzwerk Interfaces zu einem virtuellen zu verbinden um damit die Bandbreiten der Devices in einer zu vereinigen. Die Einrichtung ist sehr einfach, sie geschieht ebenfalls über das Kommandozeilentool tc. Es gibt keine Beschränkungen bezüglich der Bandbreite der Netzwerkkarten die kombiniert werden, allerdings wird bei einer sehr großen Differenz der virtuelle Link aufgrund von häufigem Packet-Reordering unbrauchbar.

- CBQ (Class Based Queuing) Teilt eine physikalische Verbindung ebenfalls in mehrere virtuelle Verbindungen auf. Das Beispiel, was bei HTB bereits vorgestellt wurde, kann also auch hier angewendet werden. Allerdings arbeitet CBQ etwas anders. CBQ versucht vielmehr für die virtuellen Verbindungen die Sendegeschwindigkeit so herunter zu regeln, dass die geforderte Bandbreite erreicht wird. Dies wird durch Berechnen der Zeitspanne erreicht, die zwischen zwei Paketen liegen muss. Allerdings treten bei CBQ hier Probleme auf, da das Errechnen der Belegung eines Links und dessen Bandbreite von vielen Faktoren abhängt. CBQ benutzt zwei Verfahren dazu: Zuerst wird der Anteil der Bandbreite, die zugewiesen werden soll, von der theoretisch möglichen berechnet. Zusätzlich wird noch die Belegung der Netzwerkkarte gemessen, anhand der Zeit, die zwischen zwei Anfragen nach Daten von der Bitübertragungsschicht vergeht. Dadurch soll eine Nährung gefunden werden. Da HTB bessere Ergebnisse liefert und die gleichen Aufgaben übernehmen kann, wird hier darauf verzichtet, die komplexe Konfiguration und genaue Vorgehensweise vorzustellen. Weitere Angaben für Interessierte finden sich unter [Diffserv].

- PRIO: Priority Queuing ist ein fast selbst erklärender Algorithmus. Ankommende Pakete erhalten durch einen Classifier eine bestimmte Priorität. Dies kann z.B. aufgrund des TOS (Type of Service) Wertes in den Paketen geschehen. Jede Priorität oder Klasse erhält nun eine eigene Queue, in der die Pakete nach FIFO gescheduled werden. Pakete aus Klassen niedrigerer Priorität können erst gesendet werden, wenn alle Queues höherer Priorität leer sind. Wird in Linux diese Queuing discipline einer Netzwerkkarte zugeordnet, so werden automatisch drei Klassen erstellt [Opal].

- SFQ (Stochastic Fairness Queuing): Wie der Name schon sagt, gehört SFQ zu den Fair Queuing Algorithmen. Das bedeutet, dass jeder Datenstrom einen gerechten Zugang zum Netzwerk erhält. Dies verhindert, dass Datenströme mit hohen Bursts mehr Kapazität belegen, als ihnen zusteht. Die allgemeine Funktionsweise eines solchen Algorithmus ist in der folgenden Abbildung angegeben. Man sieht wie die Datenströme auf einzelne Queues aufgeteilt werden. Normalerweise wird in einem Fair Queuing Algorithmus jeder Datenfluss einer Queue zugewiesen wie es in der Abbildung der Fall ist [Diffserv].
  Der Zusatz Stochastic bei SFQ kommt daher, dass SFQ nicht jedem Datenstrom eine Queue zuweist, sondern mittels einer Hash Funktion die Datenströme einer festen Anzahl von Queues zuteilt. Die Queues werden dann genau wie bei einem reinen Fair Queuing durch Round Robin abgearbeitet. In der Abbildung macht dies der Scheduler. Um Konflikte zu vermeiden, z.B. dass zwei sehr frequentierte Datenströme einer Queue zugeordnet werden, wechselt SFQ den Hash Algorithmus sehr häufig, damit diese Kollisionen nur kurze Zeit auftreten können [Diffserv]. SFQ sollte beim Einsatz mit anderen Algorithmen kombiniert werden, um einen guten Durchsatz zu erreichen.

- RED (Random Early Detection): RED steht im Gegensatz zu FIFO, PRIO, SFQ und HTB. All diese Algorithmen benutzen eine FIFO Queue. Der Nachteil dabei ist, dass Pakete am Ende der Queue fallen gelassen werden müssen, wenn die Queue

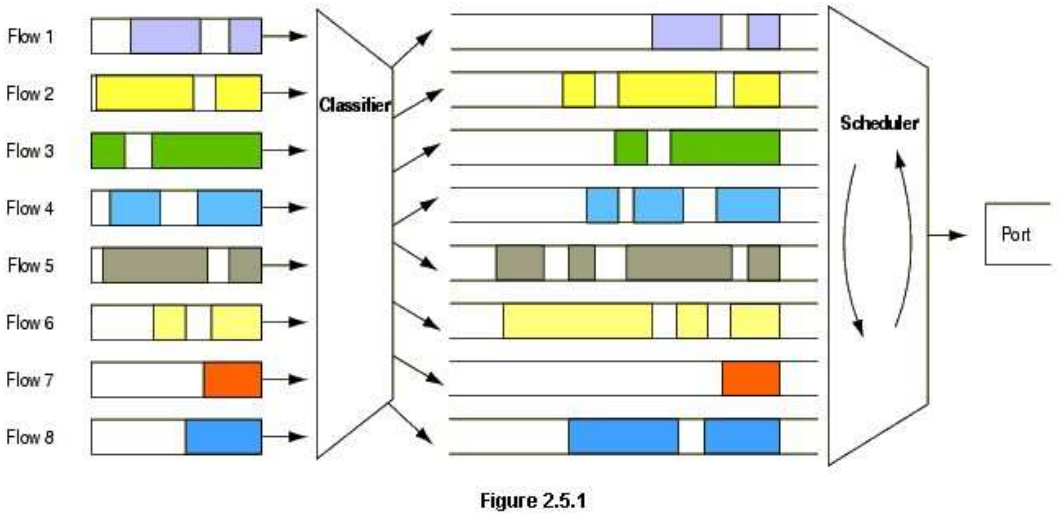

Abbildung 1.10: Funktionsprinzip Fair Queuing[Opal]

voll ist. Eine Benachrichtigung der Sender zur Leistungsanpassung (wie etwa bei TCP) geschieht also erst, wenn eine Congestion bereits eingetreten ist. Um dies zu umgehen, versucht RED die Sender bereits bei nicht voller Queue so zu drosseln, dass Congestions weitestgehend vermieden werden. Dazu werden Pakete bereits bei nicht voller Queue mit einer gewissen Wahrscheinlichkeit verworfen. Dazu wird folgende Berechnung eingesetzt:

$avg = (1 - W) * avg + W *$ `current_queue_len` [Kern]

Diese Formel berechnet ein so genanntes Exponential Weighted Moving Average (EWMA). Es dient dazu die durchschnittliche Länge der Queue über die Zeit zu glätten. W gibt dazu das Gewicht an, wie schnell aktuelle Werte den Durchschnitt beeinflussen. Um größere Bursts zu ermöglichen, muss man W herabsetzen, damit ein Anstieg in diesem Fall langsamer erfolgt. Jetzt wird der aktuelle Wert verglichen:

$avg >$ `th_max` -> Paket wird verworfen
$avg <$ `th_min` -> Paket wird angenommen
`th_min` $< avg <$ `th_max` -> Wahrscheinlichkeit wird ermittelt:
$Pb = max_P *$ `(avg - th_min)/(th_max-th_min)`

Pb ist die Wahrscheinlichkeit, mit der das Paket verworfen wird. max_P ist die maximale Wahrscheinlichkeit, die Pb annehmen kann. Sie wird vom Nutzer bestimmt und sollte die Größenordnung von 0.01 oder 0.02 haben [Kern]. Pb wird aber auch durch die aktuelle Länge der Queue bestimmt. Ein Packetdrop wird wahrscheinlicher, je länger die Queue ist. Dies ermöglicht eine recht frühe Kontrolle des Paketaufkommens. Abbildung 1.11 zeigt jetzt, welchen Einfluss das eben vorgestellte Verfahren hat:

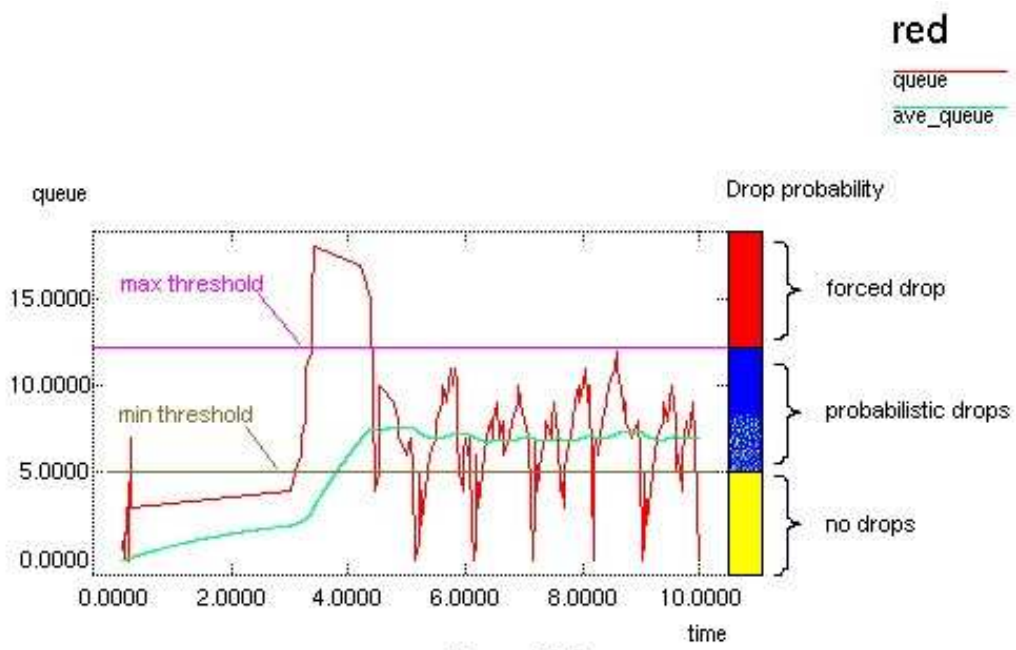

Abbildung 1.11: RED Funktionsweise[Opal]

Die grüne Linie zeigt die durchschnittliche Queue Länge, die wie o.a. berechnet wird. Die rote Linie zeigt die eigentliche Queue Länge. Man sieht das ab 3 Sekunden die Queue Länge über das maximum threshold steigt, sich der Durchschnitt aber nur langsam anpasst und noch keine Pakete verworfen werden. Dadurch ist es RED möglich, auf Bursts angemessen zu reagieren. Erreich die grüne Linie den Bereich zwischen minimum und maximum threshold, so werden die Pakete mit einer gewissen Wahrscheinlichkeit verworfen, was der blaue Balken deutlich macht. Die Durchschnittliche Queue Länge bleibt jetzt relativ konstant. Zum Abschluss sei noch gesagt, dass der Einsatz von RED in Netzwerk Gateways die Performance des Netzwerkes erheblich verbessern kann. Informationen hierzu, sowie des recht komplexen Einsatzes von RED, finden sich in [Opal].

1.3.3 Routing

Queuing ist aber nicht das Einzige, was Einfluss auf einen Datenstrom hat. Routing, also das Weiterleiten der Pakete vom Ursprungs- zum Zielrechner und umgekehrt, hat einen noch viel größeren Einfluss auf Durchsatz, Delay, Jitter etc.. Die Entscheidung, wie das Paket weiterzuleiten ist, trifft ein Algorithmus, der natürlich von Fall zu Fall unterschiedlich arbeiten kann.
In Linux wird Routing durch mehrere Komponenten bestimmt. Das eigentliche Routing wird durch Routing Tabellen angegeben. Ein Eintrag in einer Routing Tabelle hat die folgende Form:

DESTINATION GATEWAY NETMASK INTERFACE [TYPE][OPTIONS]
Pakete werden beim Eintreffen mit den Regeln verglichen. Die passende Regel wird dann ausgewählt und das Paket an die in der Regel angegebene Netzwerkkarte weitergeleitet. Zusätzlich haben die iptables einen Einfluss auf die Paketweiterleitung. Iptables sind Filter und bilden eine Art Firewall, die auch den Status einer Verbindung berücksichtigen kann.
Soll Linux als Software-Router eingesetzt werden, muss IP_Forwarding im Kernel aktiviert werden. IP_Forwarding dient zum Weiterleiten von Paketen zwischen mehreren Netzwerkkarten. Wird zusätzlich noch Advanced Router aktiviert, so können in Linux mehrere Algorithmen ausgewählt werden. Die vorhandenen Algorithmen arbeiten wie folgt:

- Policy Routing: Normalerweise werden beim Routing nur die Zieladressen der Pakete betrachtet. Je nach Zieladresse wird das passende Ausgangsinterface ausgewählt. Wird Policy Routing aktiviert, so ist es dem Router möglich, auch die Quelladresse des Paketes beim Routing auszuwerten.

- Netfilter MARK as routing key: Diese Option ermöglicht verschiedene Routen für Pakete mit verschiedenen MARK Werten anzugeben. Die Mark Value wird im Gegensatz zu den anderen hier vorgestellten Routing Algorithmen in den iptables ausgelesen. Entsprechende Verfahrensweisen werden bei einer Regel mittels
  –mark value[\mask]
  angegeben.

- Equal Cost Multipath: Soll ein Paket weitergeleitet werden, so gibt wird dies normalerweise an Hand einer einzige Regel getan, die für das Paket zutrifft. Equal Cost Multipath erlaubt es, mehrere Regeln für ein Paket anzugeben. Der Router geht in diesem Fall davon aus, dass alle zutreffenden Regeln denselben Wert (Cost) haben und wählt dementsprechend eine zufällig aus. Dies erlaubt unter anderem bei mehreren vorhandenen Wegen, die von gleicher Güte sind, die Pakete auf alle Wege aufzuteilen, um die Auslastung der Wege gering zu halten.

- Use TOS value as routing key: Use TOS value arbeitet ähnlich wie Netfilter MARK. Allerdings werden hier das Type of Service Feld eines Paketes ausgelesen. Dieses Feld gibt an, welcher Behandlung das Paket bedarf, wie z.B. hoher Durchsatz, geringe Verzögerung, etc.. Dementsprechend werden verschiedene Regeln für Pakete mit verschiedenen TOS values angegeben, um die Anforderungen auf die verschiedenen Wege abzubilden.

Weitere Funktionalität geht, wie schon angesprochen, von den iptables aus. Durch diese wird es möglich, neben den reinen Filter-Einstellungen, eine adress translation durchzuführen. Die folgende Abbildung zeigt, wie dies genutzt wird.
Die DHCP Clients stellen ihre Internetverbindung über den DHCP Server her. Damit die lokalen Adressen des 192.168.0.0\24 (Das Windows XP Standard DHCP Subnetz) Subnetzes nicht nach außen sichtbar werden (sie wären nicht topologisch korrekt), werden

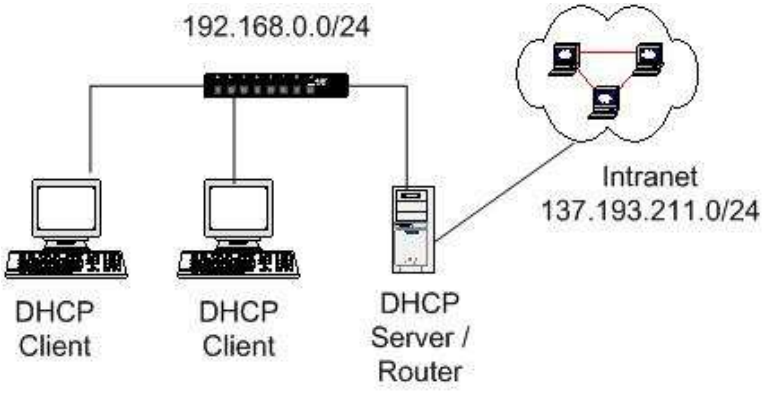

Abbildung 1.12: Network Address Translation

ausgehende Pakete vom DHCP Server verändert. Die 192.168.0.X Adressen werden durch die IP Adresse des DHCP Servers ersetzt. Antworten auf diese Pakete gelangen so zurück zum DHCP Server. Dieser weiß, welche Verbindungen von den DHCP Clients bestehen, und kann so nun abermals die Adresse der Pakete verändern. Die Zieladresse wird von 137.193.211.X auf 192.168.0.Y geändert. Damit erhält der Rechner die Antwort, von dem die ausgehenden Pakete auch stammen.
Die Routing-Regeln in Linux werden normalerweise mittels dem Befehl route eingegeben. Davon soll jedoch in neuen Kernel Abstand genommen und stattdessen die iproute2 tools verwendet werden [Diffserv]. Besonders bei der Verwendung von Tunneln ist dieses Vorgehen fehlerfreier, da in iproute2 Tunnel integraler Bestandteil des tools sind. Eine HOWTO zur Benutzung des iproute2 tools und die Einrichtung von Routing Regeln findet sich unter [Diffserv]. Die Nutzung der iptables ist in der manual page der iptables gut beschrieben.
Zusätzlich zu den Routing Algorithmen gibt es noch weitere Routing spezifische Funktionen im Linux Kernel. IP Multicast Routing ermöglich die Weiterleitung von Paketen, die mehrere Ziel Adressen haben [Kern]. Dadurch können Multicast Pakete über die Grenzen eines Subnetzes hinweg empfangen werden. RP_Filter nutzt die Eigenschaft des Policy Routings, auch die Herkunftsadresse eines Paketes auszuwerten. Mit Hilfe des RP_Filters werden die Herkunftsadressen mit dem Routing Tabellen Eintrag verglichen. Damit können Pakete, die von einer fremden Adresse im Kontext einer Verbindung abgeschickt wurden, um diese zum Beispiel zu manipulieren, abgefangen werden. Dies soll bereits beim Routing eine erhöhte Sicherheit bieten.

1.3.4 VPN

Sicherheitsfragen spielen aber heute eine immer größere Rolle, als dass einfache Mechanismen beim Routing ausreichen würden, Sicherheit in Netzwerken zu garantieren. Ein Sicherheitsfeature, dass heute in vielen Netzwerken an Bedeutung gewinnt, ist Virtual Private Networks, kurz VPN. VPN wurde ursprünglich zur Sicherung des Remote Access von mobilen Clients entwickelt. Es wurde versucht, anstelle von teuren, angemieteten Kanälen, oder Modemstrecken, das Internet dazu zu benutzen, Rechnern in beliebigen Regionen der Welt, Zugang zu lokalen Firmen-Netzwerken zu gewähren. Allerdings ist

dies nicht das einzige Einsatzgebiet von VPNs. Sie können ebenfalls genutzt werden, um Lokale Netzwerke über das Internet sicher zu verbinden. Die Arbeitsweise von VPNs wird in Graphik 1.13 veranschaulicht:

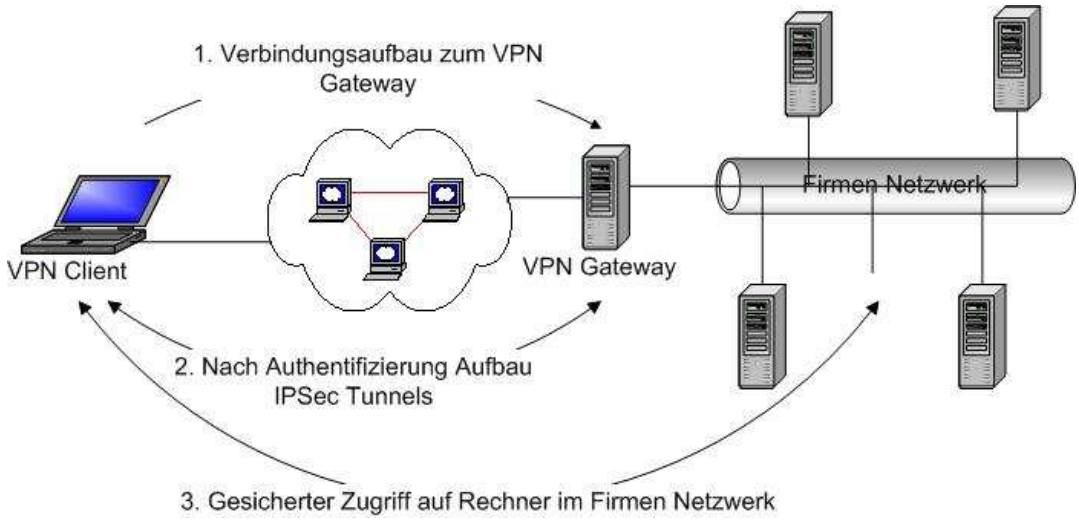

Abbildung 1.13: Ablauf VPN Aufbau

In der Graphik wurde IPSec als Tunneling Protokoll genannt. IPSec ist nicht das einzige Protokoll, dass für VPNs zur Verfügung steht, jedoch wurde es im Rahmen einer Studienarbeit als das beste und sicherste herausgestellt.
Linux bietet Unterstützung für VPNs durch die Software FreeS/WAN, die zwar nicht im Kernel vorhanden ist, aber mittlerweile mit den meisten Distributionen ausgeliefert wird. FreeS/WAN wurde für den 2.6.0er Kernel geändert, da sich in diesem Kernel eine IPSec Implementierung im Kernel befindet, die im folgenden Kapitel beschrieben wird.

1.3.5 IPSec

IPSec ist nicht als VPN Protokoll entwickelt worden, sondern als eine komplette Sicherheitsarchitektur ursprünglich für IPv6. Mittlerweile ist es aber auch für IPv4 verfügbar. Wie der Name schon vermuten lässt, ist es eine Erweiterung des IP Protokolls und arbeitet damit auf Schicht 3 des ISO/OSI Referenzmodells. Damit ist es auf den Transport von Protokollen höherer Schichten beschränkt. Spezifiziert wird es im RFC 2401 [2401].
IPSec benutzt zwei verschiedene Protokolle zur Verschlüsselung, Authentifizierung und Aufrechterhaltung der Vertraulichkeit der Daten, AH und ESP. AH (Authentication Header) übernimmt die Aufgaben der Authentifizierung und der Datenintegrität während ESP (Encapsulation Security Payload) die Verschlüsselung der Daten übernimmt. IPSec kann in zwei verschiedenen Modi arbeiten: Tunnel Mode und Transport Mode. Abbildung 1.14 zeigt die verschiedenen Arbeitsweisen.
Im Transport Mode werden nur die Nutzdaten des eigentlichen IP Paketes von IPSec behandelt. Es wird der AH zwischen IP Header und Header der höheren Protokolle eingefügt. Im Tunnel Mode wird das ursprüngliche Paket komplett in ein neues IPSec Paket gekapselt. Dem Paket wird ein neuer IP Header und ein AH vorangestellt, das eigentliche

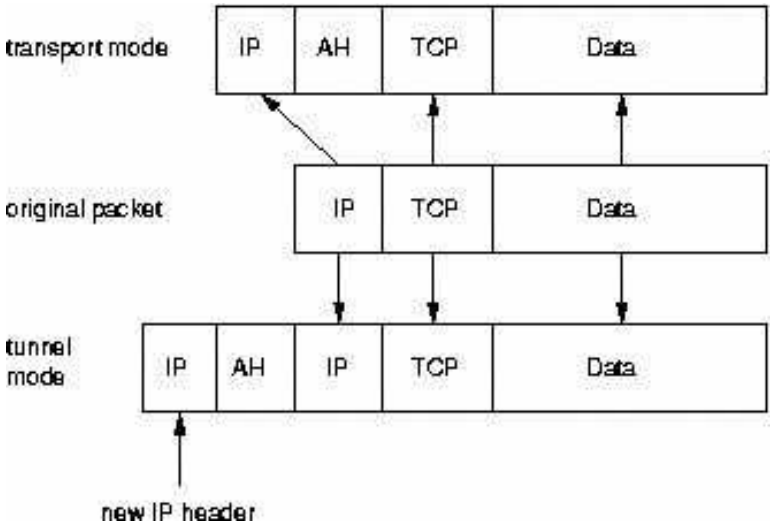

Abbildung 1.14: Aufbau IPSec Header [IPSecHowto]

IP Paket wird zum Nutzdatenteil des neuen Paketes. Genaue Informationen zu den eingesetzten Verschlüsselungs- und Authentifizierungsverfahren finden sich unter [2401].
In Linux wurde IPSec bis zum Kernel 2.4 durch FreeS\WAN realisiert und war nicht im Kernel vorhanden. Der Grund warum FreeS\WAN nicht in den Kernel waren neben politischen Gründen die schlechte Integrierbarkeit des Codes [lartc]. In aktuellen Kerneln wie dem 2.4.21-99 oder 2.6.0 findet sich eine native IPSec Implementierung im Kernel. FreeS\WAN wurde angepasst, um dieses native IPSec zu verwalten. Neben FreeS\WAN stehen auch die ipsec-tools zur Konfiguration zur Verfügung. Die eigentliche Konfiguration erfolgt über die Angabe von Security Associations, die aus Quelle, Ziel und Anweisung bestehen. Beispiel:
add 10.0.0.11 10.0.0.216 ah 15700 -A hmac-md5 „1234567890123456“;
Hiermit wird gesagt, dass Daten von Adresse 10.0.0.11 zu Adresse 10.0.0.216, die einen AH benötigen mit HMAC-MD5 und Secret „1234567890123456“ unterschrieben werden können. Dieses Beispiel und weitere Informationen zur Einrichtung finden sich unter [lartc].

1.3.6 IPv6

Ein weiteres wichtiges Feature, dass bereits in den aktuellen Kerneln, wenn auch zurzeit nur experimentell, zur Verfügung steht ist IPv6. Zunächst soll eine allgemeine Einführung über IPV6 gegeben werden, bevor zu dem Linux spezifischen Teil übergegangen wird.
Zurzeit wird im Internet hauptsächlich IPv4 als Protokoll der Vermittlungsschicht eingesetzt. Die meisten User, die einen mit dem Internet oder einem Rechnernetz verbundenen Rechner haben, sind in irgendeiner Form mit der IP Adresse konfrontiert worden. Das IPv4 Protokoll übernimmt in heutigen Rechnernetzen die Aufgabe der Adressierung und Weiterleitung der von einem Computer gesendeten Pakete. Anhand der IP Adresse wissen Router, Bridges, etc., die sich auf dem Weg zwischen Ursprungs und Ziel Rechner befinden, wohin sie dieses Paket weiterleiten sollen. Aufgrund der explosionsartigen Vergrösserung des Internets jedoch, wurde besonders dieser Adressraum, der von IPv4 zur

Verfügung gestellt wird zu klein, oder wird dies zumindest in absehbarer Zeit werden. Dies liegt darin begründet, dass die IPv4 Adressen aus 32 bit bestehen und viele von diesen aus organisatorischen Gründen gar nicht verwendet werden können. Betrachtet man nun die heutige Entwicklung von Handys, PDAs, Notebooks usw., so wird deutlich, dass in Zukunft noch viel mehr Geräte eine IP Adresse benötigen werden, um an der weltweiten Kommunikation via Internet, teilnehmen zu können.
Aufgrund dieser Tatsache begann 1990 die IETF, eine neue Version von IP zu erarbeiten. Dabei sollte nicht nur das Adressraum Problem, sondern auch andere existierende Probleme von IPv4 behoben werden. Die Hauptziele bei der Erarbeitung waren die folgenden:

1. Starke Vergrösserung des Adressraumes
2. Routing Tabellen verkleinern
3. Protokoll vereinfachen zur schnelleren Paketverarbeitung
4. Erhöhte Sicherheit
5. Mehr Beachtung von Type of Service
6. Roaming ohne Adresswechsel ermöglichen
7. Protokoll soll sich mit der Zeit weiterentwickeln können
8. Koexistenz mit IPv4 über Jahre hinweg

[tanen2] Das Ergebnis dieser Arbeit ist IPv6. Es bringt im Vergleich zu IPv4 viele Vorteile mit sich. So ermöglicht es die vollständige Autokonfiguration von Clients, ohne dass ein zentraler Server wie bei DHCP in IPv4 betrieben werden muss, es unterstützt Mobilität durch Zuweisung von mehreren Adressen an eine Netzwerkkarte und Integration von IPSec, nur um einige zu nennen [Suse]. Der Unterschied und die Änderungen zwischen den IP Versionen werden am besten durch die Betrachtung Pakete sichtbar.

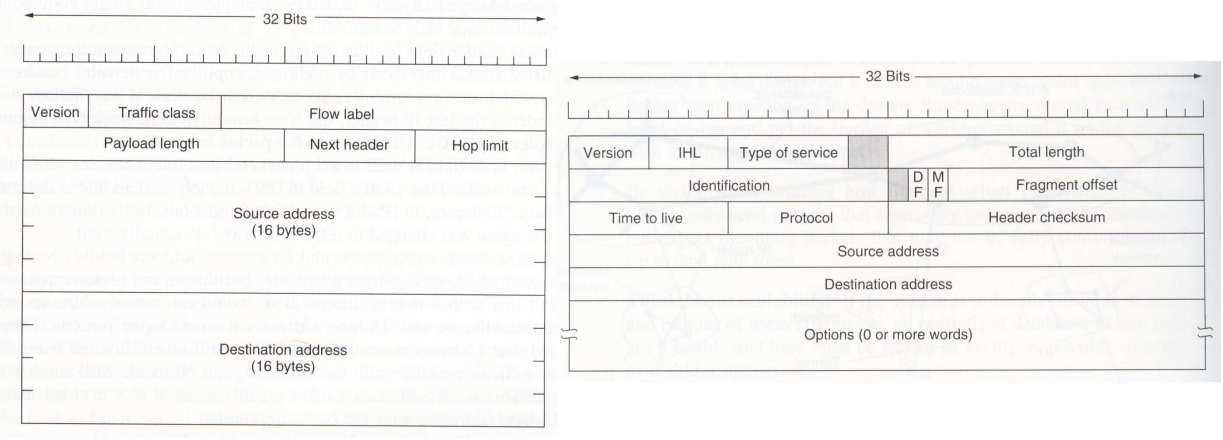

Abbildung 1.15: IPv6 (links) und IPv4 (rechts) Header [tanen2]

Abbildung 1.15 zeigt rechts ein Paket von IPv4 und links ein minimales Paket von IPv6. Zuerst fällt das Flow Label Feld auf, dass es Sender und Empfänger erlaubt, eine virtuelle Verbindung mit bestimmten Bedingungen und Anforderungen zu erstellen [tanen2]. Die wohl wichtigste Änderung ist das Next header field. Dieses Feld stellt die Vereinfachung des Headers dar. Es gibt an ob optionale Header vorhanden sind. Diese optionalen Header können in [tanen2] eingesehen werden. Ist kein oder kein weiterer optionaler Header vorhanden gibt dieses Feld das verwendete Transportprotokoll an. Durch diese optionalen Header ist es möglich, das Paket im Bedarfsfall so klein wie möglich zu machen, da ungenutzte Optionen erst gar nicht mit eingebracht werden. Die letzte auffällige Neuerung ist das Hop Limit Feld. Es entspricht im Wesentlichen dem Time to live Feld aus IPv4. In IPv4 wurde die Lebenszeit in Sekunden angegeben, jedoch hat kein Router diese Zeitangabe wirklich verwendet. Vielmehr wurde auch hier, bei jedem Durchgang durch einen Router 1 von der Time to live subtrahiert. Um dies nun auch im Namen des Feldes deutlich zu machen, wurde das Feld umbenannt in Hop Limit [tanen2]. Es bleibt noch anzumerken, dass das Checksum Feld des IPv4 Headers verschwunden ist. Dies soll ebenfalls effizienter sein und die Checksum ist in heutigen Netzen nicht mehr notwendig.
Nachdem nun die wesentlichen Änderungen des Paketkopfes dargestellt wurden, soll noch kurz die neue Adressierungsart präsentiert werden. Bei IPv6 muss zwischen verschiedenen Arten der Adressierung unterschieden werden. Es gibt in IPv6 unicast, multicast und anycast Adressen. Da unicast und multicast bereits aus IPv4 bekannt sind, wird hier nur die Funktionsweise von Anycast genauer vorgestellt.
Anycast Adressen verweisen ähnlich wie multicast Adressen auf eine Gruppe von Schnittstellen. Allerdings werden bei einem anycast Pakete nicht an alle angegebenen Schnittstellen ausgeliefert, sondern nur an die Schnittstelle, die nach dem verwendeten Routingprotokoll dem Absender am nächsten ist [Suse]. Dadurch kann zum Beispiel der Ausfall eines Servers durch Auswahl des zweitnächsten abgefangen werden [Suse].
Die Adressierung in IPv6 geschieht nicht wie in IPv4 über die XXX.XXX.XXX.XXX Schreibweise. In IPv6 wird eine Adresse durch acht Blöcke a 16bit in Hexadezimalschreibweise angegeben, wobei die einzelnen Blöcke durch Doppelpunkt voneinander getrennt werden. Eine Beispiel IPv6 Adresse würde demnach wie folgt aussehen:

8000:0000:0000:0000:0123:4567:89AB:CDEF [tanen2]

Da in diesen Adressen häufig mehrere Nullen vorkommen werden, wurden Vereinfachungen für die Adressen eingeführt. Innerhalb eines Blockes können führende Nullen weggelassen werden, d.h. aus 0123 würde 123. Eine weitere Vereinfachung, auch „collapsing“ genannte [Suse], erlaubt es, Blöcke von vier Nullen wegzulassen. O.a. Adresse ist also äquivalent zu:

8000:123:4567:89AB:CDEF [tanen2]

Es können jedoch auch IPv4 Adressen in dieser neuen Schreibweise eingegeben werden, und zwar wird dazu der bisherigen Punkt Schreibweise einfach ein Paar von Doppelpunkten vorangestellt.

Die IPv6 Adresse setzt sich aus mehreren Teilen zusammen. Der erste Block bildet ein Präfix, und bestimmt den Typ der Adresse. Die Bedeutung der verschiedenen Präfixe kann z.B. unter [HOWTO] nachgesehen werden. Der Mittelteil beschreibt ein Netzwerk oder ist ohne Bedeutung. Der Schlussteil bestimmt schließlich einen Host.
Unicast Adressen nutzen nun diese Aufteilung des Paketes. Der erste Teil, die Public Topology, wird für das Routing benötigt. Der zweite Teil, die Site Topology, enthält Routinginformationen über das Subnetz und der dritte Teil, die Interface IP, beschreibt die Zielschnittstelle. Für den dritten Teil wird die MAC Adresse als Bestandteil verwendet, da diese einmalig auf der Welt ist und damit die Konfiguration der Rechner vereinfacht. Es werden 64 Bit EUI-64 Token gebildet, die aus 48 bit der MAC Adresse und 24 bit Zusatzinformationen bestehen, dadurch können auch Geräte ohne eigene MAC Adresse einen EUI-64 Token erhalten [Suse].

1.3.7 WAN

Linux's Fähigkeiten beschränken sich jedoch nicht nur auf den Local Area Network Bereich. Auch Wide Area Network Funktionalität findet sich im Kernel wieder. Wide Area Networks decken, anders als Local Area Networks, eine große Fläche ab. Sie stellen das Bindeglied zwischen verschiedenen Local Area Networks dar. Der wichtigste Bestandteil eines WANs sind Router, die die korrekte Weiterleitung der Pakete übernehmen. Dabei sind nicht wie in einem LAN alle Rechner miteinander verbunden. In einem WAN besitzt eine Router mehrere transmission lines zu anderen Routern wie in der folgenden Abbildung zu sehen.

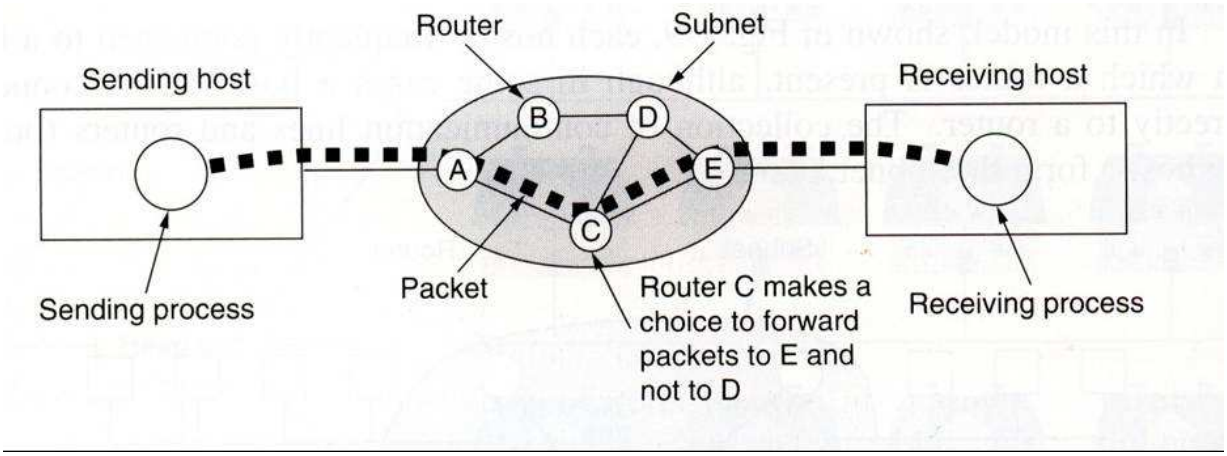

Abbildung 1.16: WAN [tanen2]

In der Abbildung gibt es mehrere Wege vom Sender zum Empfänger, allerdings sind nicht alle Router miteinander verbunden. So ist z.B. die Route ACE oder ABDE möglich, nicht aber ABCE. WANs sind wie LANs auch packet switched Networks, das bedeutet, Pakete werden einzeln betrachtet und gerouted. Erst im Zielrechner werden sie wieder in die richtige Reihenfolge gebracht. So können zusammengehörige Pakete theoretisch verschiedene Routen durch das Netz nehmen, in der Praxis sind die Routen jedoch meist fest vorgegeben. Die Algorithmen, die die Paketweiterleitung übernehmen wurden bereits im

Abschnitt 1.3.3 vorgestellt. Hier soll nur noch auf zusätzliche Funktionalität von Linux eingegangen werden, die den Einsatz von Linux in einem WAN möglich macht.
Normalerweise werden als Router in einem WAN spezielle Rechner eingesetzt, auf denen ein Unix oder proprietäres BS läuft. Als Alternative kann ein Linux Rechner mit WAN Interface Cards eingesetzt werden, wofür nicht einmal die Hälfte der Kosten eines WAN Routers benötigt werden [Kern]. Linux unterstützt traditionelle WAN Protokolle wie X.25 oder Frame Relay bereits und somit ist zum Betrieb von Linux als WAN Router nur noch das WAN Router Utility Package für die Hardware Unterstützung der WAN Interface Cards nötig, das im Kernel angeboten wird. Zur Konfiguration wird in Linux ein WAN Tool Package eingesetzt, das zusätzlich installiert werden muss.

1.3.8 Besondere Dienste

Im letzten technischen Kapitel sollen nun noch kurz einige besondere Dienste im Netzwerkbereich vorgestellt werden. Diese Dienste sind anders als die bisher besprochenen keine geläufigen Dienste, und sollen zum Abschluss zeigen, dass Linux mit noch weit mehr Features aufwarten kann, als bisher angesprochen.

- Virtual Server: VS erlaubt es, einen virtuellen Server als Cluster mehrerer Server einzurichten. Mindestens einer der Rechner muss über die Virtual Server Konfiguration verfügen, um die ankommenden Pakete abzufangen und an die übrigen Server aufzuteilen. Um eine Aufteilung der Pakete an die einzelnen Server zu ermöglichen, muss ein Scheduling Algorithmus diese Aufgabe übernehmen. Die VS Implementierung, bietet dabei das Scheduling via NAT, Tunneling oder direct Routing an. Als Algorithmen stehen neben bekannten wie Round Robin, auch VS spezifische wie least-connections (Server mit wenigsten Verbindungen bekommt Auftrag) oder destination hashing (Hash Table basierend auf der Ziel Adresse). Diese sind alle in [Kern] dokumentiert.

- RSVP (Resource Reservation Protocol): RSVP wurde in RFC 2205 spezifiziert. Es ist ein Transportprotokoll (Schicht 4) und ermöglicht einem Host bestimmte QoS für einen Datenstrom anzufordern. Diese Anforderungen werden von Routern auf dem Weg weitergeleitet um eine Art Verbindung aufzubauen und diese aufrecht zu erhalten [RSVP]. Die Anforderungen an die Verbindung werden als minimale und maximale Datenrate angegeben. In Linux ist es möglich die Scheduler aufgrund eines RSVP classifiers zu veranlassen, die zu der Verbindung gehörigen Pakete getrennt zu behandeln [Kern].

- SCTP: Das Stream Control Transmission Protocol ist in RFC 2960 beschrieben. Es ist ein zuverlässiges Transportprotokoll das oberhalb eines verbindungslosen, paketorientierten Netzwerkes arbeitet. Es bietet eine fehlerfreie, nicht duplizierte Datenübertragung an und ist in der Lage sich verschiedenen MTU (maximum transfer units) Größen anzupassen. Zusätzlich kann es Nachrichten sequenziell innerhalb mehrerer Datenströme ausliefern und mehrere Nachrichten in einem SCTP Paket übertragen [SCTP].

1.4 Zusammenfassung

Fasst man nun die wirtschaftlichen und technischen Aspekte zusammen, so ist klar, warum sich Linux besonders im Web-Serverbereich durchsetzen konnte. Nicht nur dass Linux hier einen Kostenvorteil mit sich bringt, Linux bietet als Serverbetriebssystem innerhalb eines Netzwerkes zahlreiche Optionen, die eine detaillierte Individualisierung des Systems zulassen. Allerdings wurde auch aufgezeigt, dass ein lizenzfreies Betriebssystem, nicht unbedingt auch das günstigere sein muss. Aufgrund der hohen Komplexität des Systems (Kernel mit mehr als 800 Optionen [Suseonline]) ist auch der Personalaufwand zur Pflege und zum Einsatz des Betriebssystems entscheidend höher. Hinzu kommt, dass Applikationen noch nicht in der Bandbreite für Linux zur Verfügung stehen, wie das für Windows der Fall ist. Natürlich stellt sich abschließend die Frage nach der Zukunft. Allerdings wurde innerhalb der Seminararbeit schon oft erwähnt, dass es unmöglich ist, konkrete Angaben zu machen, besonders im Desktop Bereich. Ein wichtiger Faktor wird der Umgang mit der Komplexität von Linux sein. Distributoren bieten heute vorkonfigurierte Kernels an, die ohne großes Zutun auf vielen Rechner laufen, allerdings ist in diesem Fall der Vorteil der individuellen Gestaltung des Betriebssystems durch die Vorkonfiguration etwas erschwert. Allerdings bieten sich hier, anders als bei Windows, mehrere Distributoren an, was einen Markt und damit auch die Preise niedrig halten sollte.
Die im zweiten Teil vorgestellten Technologien wie IPv6, IPSec, etc. werden Linux in Zukunft sicherlich von Vorteil sein. Bereits heute diese Technologien zur Verfügung zu haben, könnte den Marktanteil von Linux positiv beeinflussen. Allerdings zeigt dieses Beispiel auch, dass die rasche Weiterentwicklung von Linux auch ein regelmässiges Update des Betriebssystems verlangt. Während neue Windows Versionen nur alle 2-3 Jahre auf den Markt kommen, so muss man, um auch immer in den vollen Genuss des Fortschritts zu kommen, jedes Vierteljahr eine neue Release der Distributoren kaufen, oder sich einen neuen Kernel aus dem Internet herunterladen und konfigurieren. In Windows entfällt all dies, da hier die Entscheidung bereits durch Microsoft getroffen wird. Ob sich deshalb Linux auch im Desktop Bereich durchsetzen wird, ist offen. Die Entwicklung der vergangenen Jahre deutet nicht darauf hin, aber bedingt durch die Schnellebigkeit der Informatik Branche, muss dieser Trend nicht zwangsläufig für die Zukunft gelten.
Um die Entwicklung von Linux zu begründen und eine vage Prognose zu ermöglichen, wurden in der Seminararbeit verschiedenste Funktionalität beschrieben.
Es wurde aufgezeigt, dass Linux neben einem einfachen FIFO Queing auch andere Algorithmen beherrscht. Die Funktionsweisen von HTB, TEQL,CBQ, PRIO, SFQ und RED wurden dargestellt und deren Auswirkungen auf den Datentransfer beschrieben. Auch auf die Konfiguration der verschiedenen Algorithmen wurde eingegangen.
Weiterhin wurde Linux Routing Fähigkeit betrachtet und die verschiedenen Routing Algorithmen präsentiert, die Linux mit sich bringt: Policy Routing, Netfilter Mark, Equal Cost Multipath, TOS Value. In diesem Zusammenhang wurden auch Routing relevante Aspekte wie adress translation und IP Multicast Routing näher beschrieben.
Den wohl wichtigsten Zusammenhang zum wirtschaftlichen Teil stellen, wie schon oben angegeben, die Punkte VPN, IPSec und IPv6 dar. Neben einer kurzen Einführung zu diesen Themen wurden die Implementierungen der aktuellen Kernel vorgestellt, und auch auf deren Einrichtung eingegangen.

Abschließend wurde die WAN Unterstützung von Linux und besondere Dienste, die in den Kerneln als Option zur Verfügung stehen vorgestellt. Als Beispiel zu den besonderen Diensten dienten Virtual Server, RSVP und SCTP.

Literaturverzeichnis

[Kernel] Michael Beck, Harald Böhme, Mirko Dziadzka, Ulrich Kunitz, Robert Magnus, Claus Schröter, Dirk Verworner - *Linux Kernel-programmierung* 6. Auflage, Addison-Wesley 2001

[Tanen] Andrew S. Tanenbaum - *Moderne Betriebssystem* 2. überarbeitete Auflage, Pearson Studium, 2002

[tanen2] Andrew S. Tanenbaum - *Computer Networks* Fourth Edition, Pearson Education International, 2003

[Suse] *Administrationshandbuch Suse Linux 9.0* 6. Auflage, Suse Linux AG

[HOWTO] Peter Bieringer
Linux IPv6 HOWTO
http://mirrors.bieringer.de/Linux+IPv6-HOWTO-de/

[Kern] Linux Kernel 2.4.21-99/2.6.0 Dokumentation

[heise] *SCO vs. Linux: McBride warnt die Open Soruce Gemeinde*
http://www.heise.de/newsticker/data/jk-09.09.03-001/

[Diffserv] Bert Hubert
Linux Advanced Routing & Traffic Control HOWTO
http://lartc.org/howto/

[DffLin] Almsberger, Salim, Kuznetsov
Differentiated Services on Linux
ftp://icaftp.epfl.ch/pub/linux/diffserv/misc/dsid-01.ps.gz

[SCTP] Stewart
RFC 2960 Stream Control Transmission Protokoll
http://www.ietf.org/rfc/rfc2960.txt

[RSVP] Braden
RFC 2205 RSVP
ftp://ftp.isi.edu/in-notes/rfc2205.txt

[2401] S. Kent
Security Architecture for the Internet Protocol
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2401.html

[IPSecHowto] *IPsecHOWTO*
http://www.ipsec-howto.org/x143.html

[HTBTH] Martin Devera
Hierarchical token bucket theory
http://luxik.cdi.cz/ devik/qos/htb/manual/theory.html

[HTB] Martin Devera
HTB Linux queuing discipline manual - user guide
http://luxik.cdi.cz/ devik/qos/htb/manual/userg.htm

[Suseonline] *Kernel Kompilieren*
http://portal.suse.de/sdb/de/1999/07/kernel_safe_compile.html

[Opal] Leonardo Balliache
Differentiated Service on Linux HOWTO
http://www.opalsoft.net/qos/DS.htm

[Linmag] *Business Update*
http://linux-magazin.de/Artikel/ausgabe/200/04/BusinessUpdate.html

[InfoW] *Linux auf Desktop noch erfolglos.* 2003
http://www.infoweek.ch/news/n_single.cfm?ID=6612

[InfoW2] *Linux spart Millionen bei Merrill Lynch*
http://www.infoweek.ch/news/n_single.cfm?ID=7098

[ProLin] Benjamin Klöpfer, Peter Ganten
Ist GNU/Linux auf dem Desktop tot?
http://www.pl-forum.de/berichte/lt2001/vortrag_ganten.html

[chip] *Linux ist als Betriebssystem kein Außenseiter mehr.* 2003
`http://www.chip.de/news/c_news_10209795.html`

[lartc] *IPSEC:secure IP over the Internet*
http://lartc.org/howto/lartc.ipsec.html

[enet] Joachim Kroll
Linux im Unternehmenseinsatz - Vom Hype zur realen Anwendung
http://www.elektroniknet.de/topics/embeddedsystems/fachthemen/
2002/0015/index_a.htm

[NForge] *Global IT firm predicts Linux will have 20 % desktop market share by 2008*
http://www.newsforge.com/article.pl?sid=03/08/13/1424212

[symlink] *Siemens sieht 20 % Marktanteil für Linux*
http://www.symlink.ch/articles/03/08/17/1210216.shtml

[metagroup] *Linux - Betriebssystemlandschaft im Wandel*
http://www.metagroup.de/studien/2002/linux/ergebnisse/linux-summary.pdf

[about] *EMNID-STUDIE: Linux im Kommen*
http://www.aboutit.de/view.php?ziel=/autor/s/suse,artikel,2001.html

[Inform] *Betriebssyteme*
http://www.informationweek.de/index.php?/channels/channel17/000610a.htm

[netcra] *Windows 2003 Server doubles active sites since July*
`http://news.netcraft.com/archives/2003/09/10/windows_server_2003_doubles_active_sites_since_july_5_were_previously_running_linux.html`

[linHH] *Thintelligent*
http://www.linux-hamburg.de/thintelligent/

[linWo] Dr. Rainer Lischka
IT-Kostenoptimierung durch Open Source-Lösungen
http://www.lizenzfrei.at/downloads/kostenoptimierung.pdf

[IDC] *Studie Windows 2000 Versus Linux in Enterprise Computing*
http://www.kefk.net/Linux/Business/TCO/IDC/index.asp

[newsfact] James Maguire
Windows vs. Linux: TCO Feud Rages On
http://www.newsfactor.com/perl/story/22012.html

[newsfact2] James Maguire
Linux Desktop Rarely Cost-Effective
http://www.newsfactor.com/perl/story/22288.html

[Open] *Open Source: Geschichte und Grundlagen*
http://ig.cs.tu-berlin.de/w2000/ir1/referate/k-1a/

Kapitel 2

Towards Service Usage Metering

Ronny Schäfer

Diese Arbeit soll eine Übersicht über den Bereich des nutzungssensitiven Messens und Verwaltens von Kommunikationsdiensten geben. Es werden Ergebnisse der Internet Protocol Detail Record *(IPDR) Organisation, sowie der* Internet Engineering Task Force *(IETF) und speziell ihrer* Real-Time Flow Measurement Group *(RTFM) vorgestellt, welche in realen Netzen Anwendung finden. Es werden Messarchitekturen für IP-Netze vorgestellt, sowie Datenformate zum Austausch von Nutzungsinformationen besprochen. NeTraMet als implementierte Anwendung wird vorgestellt.*
In einem zweiten Teil werden mögliche Antworten auf Fragen eher ökonomischer Art gegeben. Es geht um die Veränderungen der Internet Gesellschaft - und Nutzung, die das Service-Metering mit sich bringen. Eingegangen wird dabei besonders auf das Geschäft der Internet Service Provider *ISP's und auf Dienstleister, die dem Bereich des* Content Business *zuzuordnen sind.*

Inhaltsangabe

2.1 Einleitung

Moderne Kommunikationsnetze, wie das Internet werden in der Zukunft immer größer, komplexer und heterogener. Die Datenraten und die Anzahl der Benutzer nehmen genauso drastisch zu, wie die Menge der angebotenen Dienste. Beispielhaft seinen hier nur Videoconferencing oder Voice over IP genannt.
Damit geht gleichzeitig auch eine Veränderung im Netzverkehr einher. Darauf müssen die Serviceanbieter im Internet reagieren, wollen sie mit der Entwicklung der Dienst-Angebote Schritthalten. Unter Anderem ist das Problem größerer Internet-Service-Anbieter, geeignete Steuermechanismen zur Ressourcenkontrolle zu finden, bisher ohne Lösung. Eine Vielzahl neuer Tarife erfordert auch neue Abrechungsmethoden. Ausschließliche Messungen von Online-Zeit und bzw. oder Datenvolumen sind nicht mehr zeitgemäß. Bisher benutzte Mechanismen sind dazu allerdings ungeeignet, zu statisch, keinem einheitlichen Standard unterworfen und mit den neuen Diensten teilweise überfordert

2.2 Technische Aspekte

In der Einleitung wurden die Trends und damit einherlaufende Probleme moderne Kommunikationsnetzwerke kurz geschildert. Um diese Probleme in den Griff zu bekommen, wurden diverse Anstrengungen verschiedenster, weiter unten näher vorgestellter, Organisationen unternommen. Die Ziele, der Kommunikationsunternehmen lassen sich auf folgende Punkte vereinigen:

- Entwicklung Kunden- und Dienstspezifischer Abrechnungsverfahren (Billing)
- Einheitliche Standards für Nutzungsdaten
- Quality of Service (QoS)
- Unterstützung von Fehlersuche
- Sicherheit
  - Frühzeitige Erkennung von Denail of Service
  - Intrusion Detection
- Erkenntnisse für Planung und Dimensionierung zukünftiger bzw. Ausbau bestehender Netze

Im Folgenden wird nun vorgestellt, welche Gremien und Abteilungen heutzutage massgebend für die Entwicklung und Standardisierung auf dem Gebiet des nutzungssensitiven Messens und Verwaltens von Kommunikationsdiensten verantwortlich sind. Ihre Ergebnisse sind ebenfalls Gegenstand dieses Kapitel.

2.2.1 Internet Protokol Detail Record Organisation(IPDR)

Die IPDR ist ein Industriegremium, welches sich mit der Definition und Spezifikation eines Datenaustauschformates für abrechnungsrelevante Daten sowie eines Übertragungsprotokols beschäftigt.
Das grosse Problem in der Vergangenheit war, dass für die Abrechnung von Kommukationsdiensten keine Standards vorgegeben waren. Die Kommunikation der an der Abrechnung beteiligten Komponenten des Systems musste sich aufgrund des Fehlens einheitlicher Schnittstellen auf proprietäre Lösungen bzw. auf Gateways zwischen den abrechnenden Stellen stützen. Eine schnelle und problemfreie Zusammenstellung von Rechnungsdaten konnte nicht immer gewärleistet werden. Aus diesem Grund kam es zur Gründung der IPDR, der sich alle Arten von an Abrechnung, Messung und Telekommunikation beteiligten Unternehmen anschlossen.

2.2.1.1 Ziele der IPDR

Ziel war es, endlich einheitliche Standards zu schaffen und im Speziellen:

- Definition der wesentlichen Kriterien des Datenaustausches zwischen Netzelementen und *Operation Support Systemen*
- Definition der massgeblichen Parameter für IP-Transaktionen
- Bereitstellen von Erweiterungsmöglichkeiten sowohl für Telekommunikationsdienste als auch Netze

Vorrangiges Ziel und auch Thema dieser Arbeit ist also die Spezifikation einer Messarchitektur sowie des IP-detail-record (IPDR)Datenformats. Dies ist vergleichbar mit dem, aus der Telefonie bekannten *Call-Detail-Record* (CDR), wird hier allerdings für die IP-Datenübertragung definiert.

2.2.1.2 IPDR High-Level Model

Um dem oben genannten Ziel der einheitlichen Schnittstellen der Netzelemente Rechnung zu tragen, legt die aktuelle Spezifikation der IPDR [1], die gleichzeitig die Grundlage dieses Abschnitts darstellt, folgendes IPDR-Schichtenmodell fest.(Abb.2.1)

Das Schichtenmodell basiert auf der *Telecom Operations Map*(TOM) des TM Forums [1] und ist dem *Network Data Management-Prozess* der untersten Netzwerkschicht zuzuordnen. Das *IPDR High-Level Modell* ist in 3 Schichten unterteilt.

[1] 1988 gegründetes Wirtschaftsforum, welches sich mit Fragen des Betriebs und des Managements von Telekommunikationsdiensten und -infrastrukturen beschäftigt. In der TOM befinden sich die wesenlichen Ergebnisse der Arbeit bezüglich der Automation der Geschäftsprozesse von Unternehmen des Telekommunikationsbereichs.

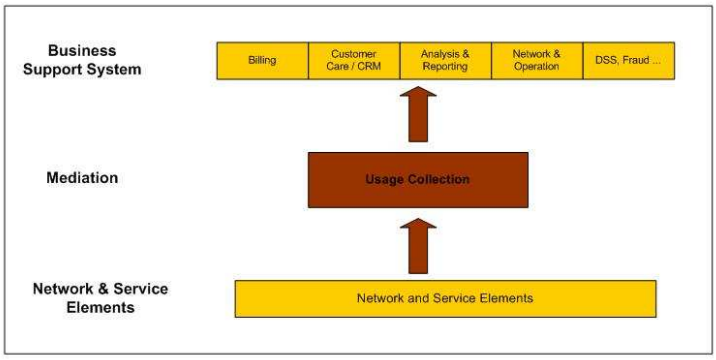

Abbildung 2.1: IPDR High-Level-Model

- **Network and Service Element layer** beinhaltet alle Netzwerkelemente wie WebServer, Router, E-Mail-, Datei- und Druckserver, Gateways, die notwendig sind, um dem Benutzer die entsprechende Dienstleistung anbieten zu können.
- **Mediation systems** sind zwischen der Netzwerk-Infrastruktur und den *Business Support Systems* (BSS) aufgehangen. Sie implementieren ein Interface zum BSS über welches die Dienst- und Netzwerknutzungsdaten zur Verfügung gestellt werden, sowie eine Schnittstelle zu den *service elements* des Netzwerks, über die Steuerdaten des BSS weitergeleitet werden. Ihre Hauptaufgabe besteht darin, alle, vom BSS benötigten Nutzungsdaten zu sammeln und diese in normalerweise engen zeitlichen Rahmen weiterzumelden. Dies beinhaltet auch eine Filterung der Gesamtdatenmenge auf das gewünschte Ziel.
- Das **Business Support System** umfasst alle Systeme, die technische oder kommerzielle Funktionen in Telekommunikationsunternehmen implementieren, wie z.B. Rechnungsstellung, Marketing und Netzwerkkonfiguration.

2.2.1.3 IPDR Reference Model

Nach der Gliederung der Netzdienste in 3 Schichten wird mit einer Betrachtung der Architektur des von der IPDR vorgeschlagenen Systems fortgefahren. Das *IPDR Reference Model* (Abb. 2.2) zeigt die Komponenten und Schnittstellen des *Mediation layers* sowie der Endsysteme.

Das Modell sieht insgesamt 6 verschiedene Elemente vor und nummeriert die Schnittstellen von A bis E durch, wobei D die oben angesprochene einheitliche Schnittstelle nach außen ist. Die einzelnen Elemente werden nun kurz vorgestellt.

- **Service Consumer (SC)** stellt den Endnutzer, der die Dienste des *Service Element* in Anpruch nimmt, dar.
- Das **Service Element(SE)** steht stellvertretend für Hardware des oben angesprochenen *Network and Service Element Layer*.

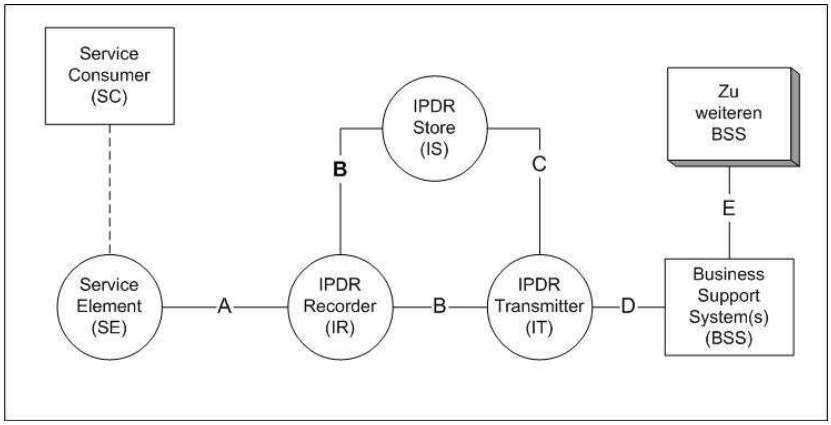

Abbildung 2.2: IPDR Reference Model

- Der **IPDR Recorder (IR)** hört die Protokolle und Datenübertragungen des *Service Element* ab und transformiert die so gewonnenen Informationen in IPDRs. Ein Recorder kann mehere SE abhören

- Der **IPDR Store (IS)** wandelt die einzelnen IPDRs, welche vom IR gesendet werden in *IPDR Documents* um und speichert diese unter Umständen für eine angegebene Zeit.

- Der **IPDR Transmitter (IT)** erledigt folgende 3 Aufgaben: Umwandlung von direkt vom IR kommenden IPDRs in *IPRD Documents*. Gruppierung zusammengehöriger IPDR-Dokumente, z.B. Meldungen über Datenfluss einer bestimmten Anwendung. Übertragung der *IPDR-Documents* zu einem oder meheren BSS.

- Das **Business Support System (BSS)** umfasst alle Systeme, die technische oder kommerzielle Funktionen in Telekommunikationsunternehmen implementieren.

Die Schnittstellen werden von der IPDR nicht spezifiziert. Lediglich D wird eingehend behandelt. Dennoch sei hier eine kurze Übersicht der übertragenen Daten angeführt:

- A: Auslieferung von Nutzungsinformationen vom SE zum IR

- B: Übertragen von IPDRs von IR zu IS oder IT

- C: Übertragen von IPDR Documents vom IS zum IT

- D: Übertragen von IPDR Documents vom IT zum BSS

- E: Übertragen von IPDR Documents von BSS zu BSS

2.2.1.4 Das IPDR-Document

Das *IPDR Document* stellt das vereinheitlichte, von der IPDR Organisation standardisierte Datenformat zur Übertragung von Nutzungsdaten dar.
Ein *IPDR Document* (Abb. 2.3) wird im XML-Format gespeichert und übertragen. Damit ist eine Auswertung mit beliebigen XML-Parsern möglich.

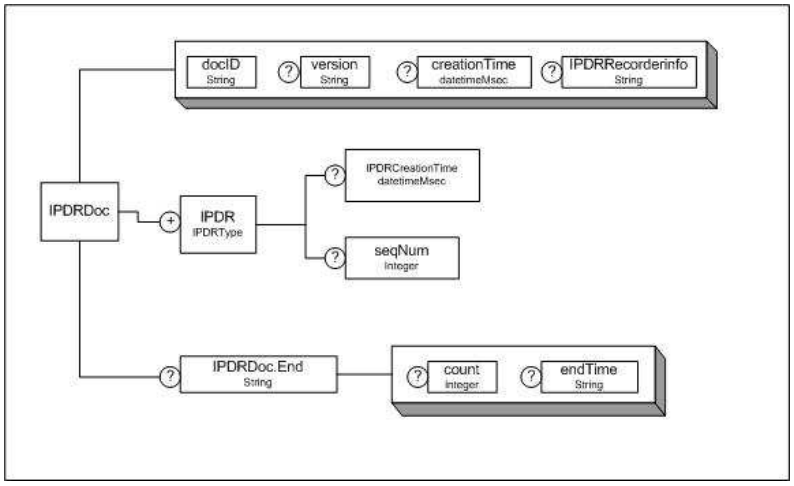

Abbildung 2.3: IPDR-Document

Grundsätzlich sieht das Datenformat eine Unterscheidung in einen dienstunabhängigen und einen dienstspezifischen Teil eines IPDR-Dokuments vor. Das sog. *IPDR Master Schema* (Abb. 2.4) legt die Struktur des dienstunabhängigen Teils fest und wird in [1] definiert. Die dienstspezifischen Teile werden in getrennten Dokumenten charakterisiert. Das *IPDR Master Dokument* besteht unter Anderem aus einem Header, der allgemeine Daten, wie z.B. Versionsnummer und Erstellungsdatum, enthält.

```
<element name = "IPDR" type = "ipdr:IPDRType">
    <annotation>
        <documentation>
            An IPDR describes an event between a service
            consumer and a service element. Details of the event
            are contained within this record. All IPDR elements
            have a time indicating when the event occurred.
        </documentation>
    </annotation>
</element>
<element name = "IPDRCreationTime" type = "ipdr:dateTimeMsec"/>
<element name = "seqNum" type = "integer"/>
<complexType name = "IPDRType"
    final = "restriction">
    <annotation>
        <documentation>
            This is the base type for the IPDR element. The
            service-specific schema can extend this by deriving
            from it.
        </documentation>
    </annotation>
    <sequence>
        <element ref = "IPDRCreationTime" minOccurs = "0"/>
        <element ref = "seqNum" minOccurs = "0"/>
    </sequence>
</complexType>
```

Abbildung 2.4: IPDR-Master Schema

Ein *IPDR Master-Document* kann mehrere IPDR's (Abb.2.5) beinhalten, welche die eigentlichen Daten über eine spezifische Dienstnutzung enthalten.

```
<element name = "IPDRDoc">
        <annotation>
            <documentation>
                The IPDRDoc element is the top level container of a set
                of IPDRs. The document will also define the entity
                which recorded these IPDRs via the IPDRRec element.
            </documentation>
        </annotation>
        <complexType>
            <sequence>
                <element ref = "ipdr:IPDR" maxOccurs = unbounded"/>
                <element ref = "ipdr:IPDRDoc.End" minOccurs = "0"/>
            </sequence>
            <attribute name = "docId" use = "required" type ="string"/>
            <attribute name = "version" type = "string"/>
            <attribute name = "creationTime" type = "ipdr:dateTimeMsec"/>
            <attribute name = "IPDRRecorderInfo" type = "string"/>
        </complexType>
</element>
```

Abbildung 2.5: IPDR-Schema

Internet Protocol Detail Records beinhalten die *IPDR-CreationTime*, die die Aufnahmezeit des Datensatzes repräsentiert, sowie die *Sequence Number (seqNum)*, einen optionalen Integer-Wert um die Datensätze zu ordnen. Der erste IPDR-record hat die *seqNum* 0.

Da es bisweilen unmöglich scheint für alle Dienste allgemeingültige Abrechnungsattribute zu standardisieren, stellt die IPDR hier 2 Möglichkeiten zur Verfügung. Zum einen bietet sie eine Grammatik an, wie dienstspezifische Abrechnungsattribute spezifiziert werden können Zum Anderen werden für unterschiedliche, bekannte und allgemein oft genutzte Dienste, wie z.B. VoIP, dienstspezifische Abrechnungsattribute von der IPDR festgelegt. Für genauere Erläuterungen sei hier auf [1] verwiesen.
Das Datenformat ist derart ausgelegt, dass Erweiterungen ohne Weiteres möglich sind.

2.2.1.5 Vergleich zu CDR

Call Detail Records (CDR) sind Datenstrukturen, welche Informationen über einen Anruf(Nebenstelle oder Position, Dauer, Uhrzeit, angewählte Rufnummer)enthalten, die von einer TK-[2] , einer ACD-Anlage[3] oder einem Vermittlungssystem im Telefonnetz aufgenommen werden. Diese Daten sind die Basis für Call Center-Managementsoftware und die Rechnungsstellung der Telefongesellschaften (Billing)[11]. CDRs werden auch bei Verbindungen über mehere Netze hinweg an der Schnittstelle dieser untereinander erzeugt.

2.2.1.6 Bewertung

Die Ziele, der IPDR, die Spezifizierung eines einheitlichen Datenmodells und Kommunikationsprotokols für Abrechnungsdaten, wurden zweifelsohne erreicht. Da die IPDR aus der

[2] Telekommunikationsanlage, branchenüblicher Ausdruck für Nebenstellenanlage im deutschsprachigen Raum

[3] Atomatic Call Distrubutor

Kooperation zahlreicher namenhafter Firmen hervorgegangen ist, sollte der praktischen Umsetzung dieses Standards in der Beziehung nichts im Wege stehen. Die Kooperation IPDR-konformer Geräte wird damit für die Zukunft vereinfacht. Jedoch aufgrund der hohen Komplexität des Systems sind bisher noch keine derartigen Systeme in Anwendung und es bleibt abzuwarten, ob Kosten und Nutzen in einem vernünftigen Verhältnis stehen.

2.2.2 Real-Time Traffic Flow Measurement group (RTFM)

Die *RTFM group* ist eine Arbeitsgruppe der *Internet Engineering Task Force (IETF).* Das Aufgabenfeld der mittlerweile wieder aufgelösten *Real Time Traffic Flow Measurement Group* (RTMF) umfasste die Spezifikation einer Architektur sowie von Protokollen für die Nutzungserfassung im Internet. Ziele waren hier eine Basis für Netzplanung und Abrechnung von Diensten zu schaffen.

2.2.2.1 Internet Engineering Task Force (IETF)

Die *IETF* ist eine internationale Organisation, die für die Weiterentwicklung und Spezifikation neuer Technologien für das Internet ins Leben gerufen wurde.
Hierbei werden für einzelne Aufgaben und Themen sog. *Working Groups* gebildet. Ziel der Arbeit solcher *Working Groups* ist die Spezifikation und Verabschiedung von Internet Standards. Um das zu erreichen, werden im Laufe der Arbeit diverse Diskussionsvorschläge, sog. *Internet Drafts* veröffentlicht. Hat eine *Working Group* ihre Arbeit beendet, so wird sie wieder aufgelöst und die Ergebnisse werden in Form von durchnummerierten *Request for Comment* (RFC) dokumentiert, die später zu Internet Standards aufwachsen.

2.2.2.2 Traffic Flows

Der Zentrale Punkt für die Nutzungserfassung im Internet ist die Definition von *Flows. Flows* repräsentieren einen bestimmten zusammengehörigen Teil des Netzverkehrs, vergleichbar mit Kommunikationsverbindungen.
Netzwerkströme *(Network Traffic Flows)* bestehen also aus Datenpaketen, zwischen zwei logischen Endpunkten. Diese Endpunkte werden durch folgende 3 Attribute charakterisiert:

- link layer: Ethernet Adresse
- network layer: IP Adresse
- transport layer: Protokoll Typ (Port Nummer)

2.2.2.3 Rule-Sets

Flows werden von so genannten *Rule-Sets* definiert, deren Grundlage IP-Adressen, Mac-Adressen, Ports oder Header von Protokollpaketen bestimmter Anwendungen sein können. Mit anderen Worten: Rule-Sets sagen aus, was in welchem Zeitabschnitt gemessen werden soll. Rule-Sets sind Pattern-Matching Programme für die *Pattern Matching Engine(PME)*[4].
Die Sprache zur Definition von Rule Sets wird als *Simple Rule Set Language*(SRL)[9] [10] bezeichnet. SRL spezifiziert *Traffic Flows* und die entsprechenden Reaktionen der Metering Architektur darauf. SRL ist eine imperative Programmiersprache.

```
# broadcast.srl: Look for Broadcast packets
#
if SourcePeerType == dummy # PC meter time-filler packets
    ignore;
if DestAdjacentAddress == FF-FF-FF-FF-FF-FF {
        save SourcePeerType;
        save SourcePeerAddress/32;
        save DestPeerAddress/32;
        save SourceTransType;
        save SourceTransAddress/16;
        save DestTransAddress/16;
        count;
}
set 9;
```

Abbildung 2.6: SRL - Programm

Das hier (Abb. 2.6) vorliegende Programm überwacht alle Pakete mit der MAC-Adresse FF-FF-FF-FF-FF-FF und speichert alle Adress-Attribute.

Ähnlich der IPDR-Organisation, wo die Definition von allgemeinen Abrechnungsattributen sehr schwierig ist, stellt die Ermittlung der Rule-Sets eine sehr komplexe und schwierige Aufgabe dar. Es konnte bisher kein allgemein anwendbares Verfahren gefunden werden. Statt dessen werden proprietäre Lösungen für Standarddienste implementiert. Die Definition spezifischer Regeln für einzelne Anwendungen wird dem jeweiligen Administrator überlassen.

2.2.2.4 Die RTFM-Architektur

Nachdem nun geklärt ist, was RTFM-basierte Systeme aufzeichnen sollen und wie dies spezifiziert wird, bleibt die Frage zu klären, wie welche Hardware zu diesem Zwecke eingesetzt wird. In [5] wird eine Architektur für die Nutzungserfassung entworfen.

[4] spezifiziert in RFC 2064

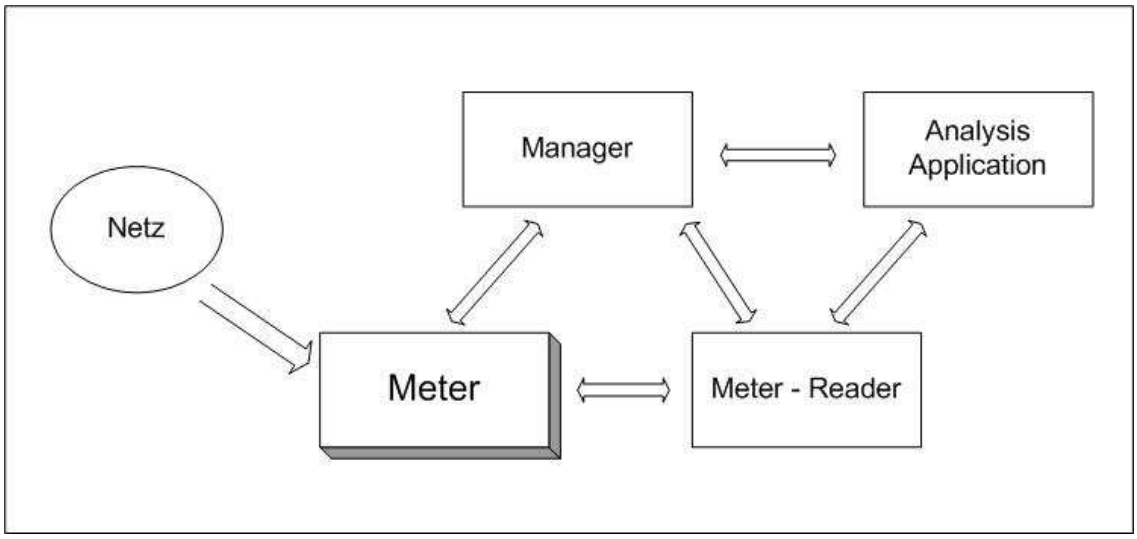

Abbildung 2.7: RTFM Architektur

Die gezeigte Architektur (Abb. 2.7) beschreibt die Elemente, welche zur Messung und Aufbereitung von Nutzungsdaten notwendig sind. Sie werden im einzelnen kurz vorgestellt:

- Der **Meter** ist das Aufzeichnungselement mit Verbindung zum normalen IP-Netz. Er zeichnet auf, analysiert und filtert die gewonnenen Daten auf Basis der oben besprochenen Rule-Sets. Er ordnet also Netzverkehr bestimmten Flows zu. Der Meter ist weiterhin in der Lage, die gewonnenen Daten zwischenzuspeichern.
  Beim Einsatz mehrerer Meter gibt es zwei grundlegende Szenarios:

  1. *redundantes Metering*: Es werden zwei oder mehrere Meter identisch konfiguriert
  2. *verteiltes disjunktes Metering*: Mehrere Meter werden so konfiguriert, dass ein ankommendes Datenpaket von genau einem Meter zu einem Traffic Flow zugeordnet wird.

- **Meter Reader** dienen der weiteren Verarbeitung der Flow Daten. Ein Meter Reader ist in der Lage, die Flows mehrerer Meter auszuwerten. Die Daten eines Meter können auch durch mehere Meta-Reader ausgewertet werden. Ergebnis dieser Auswertung sind *Usage Data*.

- Die Auswertung der *Usage Data* erfolgt durch eine sogenannte **Analysis Application**, welche zwar in RFC 2722[5] erwähnt wird, jedoch nicht Teil der Standardisierung ist.

- Der **Manager** steuert und konfiguriert Meter und Meter-Reader. Der Manager konfiguriert die Meter, indem er die Konfigurationsdateien, also die Rule-Sets auf die jeweiligen Meter schreibt. Der Manager bestimmt desweiteren, wie die gewonnenen Daten zwischen den Elemten ausgetauscht werden. Er regelt, welche Reader Daten von welchen Metern in welchen Intervallen auslesen und auswerten dürfen.

- In [5] bzw. [6] wird des weiteren noch eine **Management Information Base** (MIB) definiert, welche Konfigurationsdaten für das gesamte System bereithält und mit Hilfe derer der Manager via *Simple Network Management Protocol (SNMP)* die Komponenten konfigurieren kann. Die MIB besteht aus 4 Teilen. Die *control section* beinhaltet Tabellen über die Rule-Sets, Interfaces, Meter-Reader und Manager. Der zweite Teil umfasst die Struktur und Tabellen für die Flow-Daten. Teil 3 hat eine Tabelle, in der alle Rule-Sets gespeichert sind, die von den Metern benutzt werden können. Teil 4 beinhaltet die *conformance statements*, welche in RFC 2520 definiert werden

RTFM ist in der momentanen Ausführung ein rein passives System. Das heißt, es misst nur Datenverkehr von anderen Netzelementen. Im Rahmen von *QoS* gibt es Überlegungen, aktive Elemente mit einzubeziehen. Das heisst, es werden Kontrollpakete vom System selbst losgeschickt um z.B. Aussagen über Verzögerungen machen zu können.

2.2.3 Beispielanwendungen für Metering Systeme

2.2.3.1 NeTraMet

NeTraMet (Network Traffic Meter) ist eine Open-Source Software, erstellt von den Entwicklern des RTFM Frameworks als Beispielanwendung. Sie hat es durchaus zur Marktreife gebracht und wird heutzutage häufig zu Messzwecken eingesetzt.

Das als NeTraMet bezeichnete System besteht eigentlich aus mehreren Teilkomponenten.

- **NeTraMet** stellt eine Implementierung des Meter-Moduls des RTFM Reference Model dar. Er zeichnet auf, analysiert und filtert die gewonnenen Daten. Es gibt 2 Arten, die Meter einzusetzen. *Redundantes Metering* kennzeichnet den Einsatz zweier identisch konfigurierter un den selben Traffic überwachender Meter. Im Gegensatz dazu steht *verteiltes disjunktes Metering* für eine Strategie, in der genau ein Meter ein Datenpaket einem Traffic Flow zuordnet.

- **NeMaC (NeTraMet Manager / Collector)** implementiert RTFM Reader und Manager.

- **nifty** ist der entsprechende *Traffic Flow Analyser*, der aus den gewonnenen Daten Grafiken produtziert.

Die Komponenten kommunizieren mittels SNMP[5].

[5] Simple Network Management Protocol

2.2.3.2 NetFlow

Ein weiteres Meter-Programm stellt **NetFlow** von *Cisco-Systems* dar. Es bietet aber bei weitem nicht die Konfigurationsmöglichkeiten, die NeTraMet zur Verfügung stellt. Es werden alle IP-Flows in der feinsten Granularität gemessen und nur wenige Aggregationsschemata zur Verfügung gestellt. NetFlow generiert sogenannte *Traffic Reports* für jeden Flow. Dieser beeinhaltet

- flowID
- Quell- und Ziel IP, Port und Protokoll
- Paket- und Byte-Zähler für jeden Flow
- Zeit des ersten und letzten Pakets

Aufgrund der feinen Granularität und der damit einhergehenden großen und umfassenden Datenmenge ist mit NetFlow eine sehr flexible Auswertung möglich. Auf der anderen Seite können diese grossen Datenmengen sehr schnell Server und ganze Netzwerke überfluten.

2.2.3.3 Linux NetFilter

NetFilter ist ein Paket-Klassifizierer basierend auf dem Linux Kern. Anwendung findet er hauptsächlich in Firewall-Umgebungen. Er ist trotzdem auch zum Zählen beziehungsweise Überwachen von Netz-Traffic im Kontext dieser Arbeit in er Lage. Weitere Anwendungsgebiete sind Accounting und *Network Address Translation (NAT)*. Prinzip ist, das Pakete auf einem bestimmten Weg durch den Kernel an verschiedenen Punkten erfasst und klassifitiert werden können. Die Administrartion erfolgt über die Kommandozeile.

2.2.4 Vergleich der Metering-Systeme

In [2] werden die Metering-Systeme folgendermaßen charakterisiert.

	NeTraMet	NetFlow	NetFilter
FlowDefinition	bidirektional (optinal unidirektional)	unidirektional	variabel
Flow-Granularität	variabel	festes Set von Attributen, einige feste Aggregationsschemata	variabel
Diffserv Codepoint	ja	ja	ja
RSVP Flowspee	Erweiterungskonzept in [3]	nein	nein
IPv6 Adressen	ja	nein	ja
Multicast Attribute	geplant	geplant für Cisco IOS 12.0 (7) T	nein
Sampling	ja	nein	nein
QoS Messungen	ja	nein	nein
Unterstützte Betriebssysteme	DOS, Linux, BSD Solarism IRIX	Cisco IOS	Linux
Kosten	frei erhältlich	ca. 5000,- pro Lizenz	frei erhältlich

NeTraMet bietet die höchste Flexibilität der vorgestellten Meter. Die Definition von Verkehrsklassen kann über die Klassifikationsregel frei gewählt werden. Da die Klassifizierung im User Space stattfindet, kann NeTraMet auf verschiedenen Betriebssystemen eingesetzt werden. Cisco NetFlow ist ein vergleichsweise statisches Meter. Die Attribute, mit der die Klassen unterschieden werden, sind fest vorgegeben. Ausserdem ist das Meter ausschließlich zusammen mit Cisco IOS verfügbar. Dafür kann bei der Klassifikation eine höhere Leistungsfähigkeit erzielt werden. Bezüglich zusätzlicher Funktionalität schneidet NetFlow im Vergleich zu NeTraMet eher schlecht ab. Eine Erklärung dafür ist mit Sicherheit die freie Verfügbarkeit des NeTraMet-Quellcodes, die eine Weiterentwicklung des Tools durch interessierte Entwickler ermöglicht.Dies trifft auch auf den Linux-Klassifizierer Netfilter zu. Da Netfilter jedoch - anders als NeTraMet und NetFlow - primär für Anwendungen wie Firewalling konzipiert wurde, sind hier bisher nur wenige Erweiterungen für Accounting und Messzwecke verfügbar.

2.2.4.1 Bewertung und Zukunft des Systems

Die RTFM hat mit den RFCs 2720 bis 2724 ein funktionierendes System zur Messung von Nutzungsdaten spezifiziert. Dies wurde bereits in einigen realen Anwendungen (z.B. *NeTraMet*) bewiesen.
Das Ursprüngliche Ziel der Überwachung von Traffic Flows war bei der Netzplanung und Bewertung zu suchen. Es wird für die Zukunft angedacht, die Möglichkeiten des RTFM auf die Anwendungsebene auszudehnen um somit Informationen z.B. über Antwortzeiten von Anwendungsprogrammen zu erhalten. Die RFC 2724 stellt die Basis für Überlegungen der Erweiterung des RTFM - Flow- Definition für die Dienstgütemessung dar.
Zur Kommunikation zwischen RTFM- und IPDR-basierten Systemen sei nur folgendes

erwähnt: Es gibt bisher keine standadisierten Schnittstellen zwischeneinander. Systemübergreifende Anwendungen müssen sich daher auf proprietäre Lösungen im Einzelfall stützen.

2.3 Auswirkungen des Service Metering

Wie bereits anfangs erwähnt ist das Internet grossen Veränderungen unterworfen. Anfangs war es nur ein Kommunikationsmedium für das Militär, dann diente es zum Informationsaustausch von Forschungseinrichtungen und Universitäten und mittlerweile ist es zu einem Massenmedium geworden mit einem kaum mehr überschaubaren Angebot an Dienstleistungen. Aus diesem Grund wurden die oben besprochenen Anstrengungen unternommen. Das Ergebnis waren Strategien, Prinzipien, Standards und auch Implementierungen für das Service Metering.

Dies eröffnet natürlich neue Möglichkeiten für viele Dienstleister im Internet. Im Folgenden werden die Auswirkungen auf das Internet und Unternehmen, deren Geschäftbereiche sich über das Internet erstrecken, von mehreren Standpunkten aus behandelt.

2.3.1 Tarifizierung im Internet

Die *Internet Service Provider* sehen sich immer mehr einem Konkurrenzkampf untereinander ausgesetzt. Dieser kann kaum noch durch erweiterte Dienstangebote gewonnen werden. In der Vergangenheit wiesen Leistungskataloge noch Punkte wie Nachrichtenservice, kostenlose E-Mail Adressen oder WebSpace aus, um somit Kunden zu locken bzw. an sich zu binden. Diese Strategie kann heutzutage kaum noch zu messbarem Erfolg führen, da der Kunde im Internet eben diese Dienste bei unzähligen Anbietern kostenlos in Anspruch nehmen kann. Service Metering eröffnet den ISPs neue Wege, um Kunden zu werben und sich von den Konkurrenten abzuheben. Die Zauberformel heißt hier *günstige nutzerspezifische Tarifmodelle.*

Einen Überblick über die Ebenen des Accounting-Management und wo die oben vorgestellten Metering Systeme einzuordnen wird hier (Abb. 2.8) gezeigt. Es ist ersichtlich, das Metering Verfahren die Grundlage moderne Tarifizierung sind.

2.3.1.1 Pauschaltarife

Bisher waren Pauschaltarife die gängige Abrechnungsvariante im Internet. Dem Nutzer wurde ein fester Betrag für die Dienstnutzung und -bereitstellung in Rechnung gestellt. Dieser war unabhängig vom realen Dienstnutzungsvolumen (Verbindungsdauer, Datenmenge). Die Rechnungen waren also keineswegs kundenspezifisch. In den letzten Jahren wurden zwar immer mehr Tarife zur Verfügung gestellt, doch das grundlegende Prinzip blieb erhalten. Flat-Rates stellen in diesem Zusammenhang einen stark in der Nutzergunst ansteigenden Tarif dar.

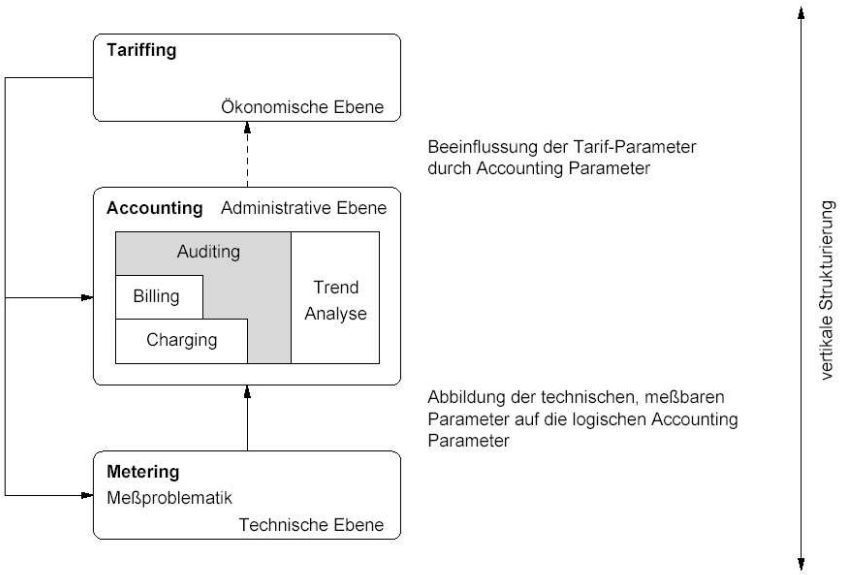

Abbildung 2.8: Ebenen des Accounting Managements, [14]

Folgendes Problem ergibt sich daraus: *Ungerechtigkeit der Bezahlung*
Durch Pauschaltarife bezahlen Nutzer auch Online-zeit, die sie nicht in Anspruch genommen haben. Also bezahlen sie die Internet-Nutzung anderer Kunden mit.

2.3.1.2 Nutzungsorientierte Tarife

An diesem Punkt setzten nutzungsorientierte Tarife an. Die Abrechnung erfolgt hier aufgrund des in Anspruch genommenen Dienstnutzungsvolumens, beispielsweise aufgeschlüsselt nach Übertragungsvolumen oder Zeit. Sie ist also für jeden Kunden individuell. Die Preiserstellung erfolgt dann Aufgrund der Anzahl der Abrechnungseinheiten abhängig von z.B. Dienstgüte und Tageszeit. Technische Grundlage solcher Tarife ist die Nutzungserfassung, auf Basis oben erläuterter Erkenntnisse.
Nutzungsorientierte Tarife werden von den Kunden immer mehr gefordert. Eine mögliche Einteilung ist im Folgenden vorgenommen. Sie erhebt allerdings keinen Anspruch auf Vollständigkeit und gibt nur einige Beispiele wieder.

- *Zeitbasierte Tarife*
  Hier wird nach 'online-Zeit' abgerechnet. Dies ist der momentan vorherschende nutzungsorientierte Tarif. Er erfordert jedoch keine Metering Systeme sondern lediglich eine Zeitmessung.

- *Volumenorientierte Tarife*
  basieren auf der ureigentlichen Metering-Anwendung, dem Zählen von Datenpaketen. Die Abrechnung erfolgt hier aufgrund des verursachten Netztraffics, z.B. könnten 100 MB Download-Volumen 5 Euro kosten. Das Problem bei volumenbasierten Tarifen ist die fehlende Nutzertransparenz. Der Nutzer ist nicht, oder nur schwerlich in der Lage, selbst zu beurteilen, wie viel Traffic er verursacht. Es ist nicht so

intuitiv verständlich wie z.B. die Zeit. Aus diesem Grund ergeben sich Probleme bei der Kostenkontrolle durch den Nutzer.

- *Inhaltsorientierte Tarife*
  Bei dieser Abrechnungsvariane werden verschiedene Inhalte unterschiedlich abgerechnet. Beispielsweise könnte man Real-Time Börsen Daten mit einem Live-Internet-Programm anbieten und die dadurch erzeugten Datenpakete mit einem bestimmten Preis pro MB versehen, der sich vom normalen Tarif für z.B. Browsen abhebt. Technisch wird dies durch das Aufbohren der Metering-Kriterien auf die Anwendungsebene erreicht. Es werden also die Protokollköpfe bestimmter Anwendungen gezählt.

- *Prioitäts-basiertes Preisschema*(Priority Based Pricing) verwendet mehere Dienstklassen mit unterschiedlichen, jeweils festen Preisen. Meist werden die unterschiedlichen Dienstklassen auch Unterschiede bezüglich Qualität und Umfang der Leistungen aufweisen.
  Diese Art der Tarifizierung stützt sich allerdings auf *Quality of Service*, was momentan im Internet generell nicht angeboten werden kann.

2.3.1.3 Bewertung und Zukunft

Man kann das Szenario noch erweitern und dynamische Tarifizierungsmodelle einsetzen. Heutiger Standard sind statische Tarifmodelle, wo der der Abrechnung zu Grunde liegende Tarif einmal vor der Nutzung und dann für eine vorher bestimmte längere Zeit festgelegt wird. Im Gegensatz dazu werden die Tarife unter Nutzung dynamischer Tarifmodelle erst unmittelbar vor oder bereits während der Nutzung festgelegt. Man könnte so z.B. günstigere Tarife anbieten, wenn das Netz momentan nicht sehr stark ausgelastet ist. Ein Solches Tarifmodell ist z.B. das *smart market model* als Implementuerung von *second price auction*. Sie werden heutzutage aufgrund ihrer hohen Komplexität und Resourcenanforderungen allerdings nicht eingesetzt, sondern nur in Versuchsanlagen getestet.
Nutzungsorientierten Tarifen gehört sicherlich die Zukunft. Das Problem der ungerechten Abrechnung von Verbindungen kann damit in den Griff bekommen werden. Jeder bezahlt nur das, was er wirklich verbraucht hat und was er haben wollte. Dies ist allerdings auch kein Allheilmittel. Mögliche Probleme ergeben sich in der geringen Nutzertransparenz. Weitere Probleme können sich in der größeren Komplexität neuer Abrechnungsverfahren ergeben. Es bleibt abzuwarten, ob das Kosten-Nutzen-Verhältnis in einer vernünftigen Relation steht.

2.3.2 Einflüsse des Metering auf die Netzplanung

Metering kann Netzbetreiber in die Lage versetzen, genauere Analysen ihrer Hardware durchzuführen. Bezüglich Ausbau und Konzeption neuer Netze ist man in der Lage, Antworten auf folgende Fragen zu erlangen.

- Welche Nutzlast ist zu erwarten?

- Welche Arten von Diensten stehen im Vordergrund?

So ist der ISP besser in der Lage, mit seinem Angebot auf den Kunden einzugehen. Metering eröffnet ihm aber auch Möglichkeiten, das Nutzerverhalten einzuschätzen und somit so zu beeinflussen, dass bespielsweise Veränderungen an der Netzinfrastruktur nicht nötig sind.

2.3.3 Usage Metering und Content Business

Content Business bezeichnet Unternehmensformen im Internet, die über reine Übertragungsleistungen hinaus gehen. Sie bieten beispielsweise komplette Anwendungen an, wie Video on Demand, interaktive Spiele oder Informationen über Wirtschaft und Finanzen. In den nächsten Jahren wird es das klassische Internet-Geschäft, dass sich auf die Abrechnung von Online-Zeit oder reinen übertragenen Daten stützt, nicht mehr geben. Statt dessen treten Content-Anwendungen immer mehr in den Vordergrund. Dies behauptet [4]. Content Billing darf nicht mit eCommerce verwechselt werden. Der Unterschied ist, dass eCommerce das Internet lediglich zur Zahlungsabwicklung nutzt und bei eContent die gesamte Applikation auf Basis des Internet läuft.

2.3.3.1 Wie können Ergebnisse der IPDR und RTFM Content Business unterstützen?

Mittels Usage Metering ist man in der Lage, das abzurechnen, was der Kunde wirklich will, also den Inhalt bzw. die tatsächlich erbrachte Leistung und nicht nur das übertragene Datenvolumen. Dies zielt auf die weiter oben bereits besprochene Erweiterung der Metering-Kriterien auf Anwendungsebene ab. Hier kommen nun auch die Errungenschaften der IPDR ins Spiel. Durch die Standardisierung des Datenaustauschs zwischen Netzwerkelementen und Supportsystemen, speziell der Definition der Internet Protocol Detail Records (IPDR) leistet sie einen entscheidenden Beitrag bei der Integration von Management- und Billing-Systemen. Eine schnelle und fehlerfreie Rechungsstellung würde unterstützt. Dies macht das Angebot des Content-Anbieters attraktiver für den Kunden.

2.3.3.2 Beispiele für Content-Angebote

> "Die IPDR erlaubt den Betreibern von IP-Netzen der nächsten Generation, leistungsfähiger und kosteneffektiver zu arbeiten und mit neuen und innovativen Serviceleistungen zusätzliche Geschäftsmöglichkeiten zu erschließen. Schließlich sind die Perspektiven von Content Billing fast unbegrenzt. Beispiel: Callasong.de, ein von CyberSolutions gehosteter Web-Auftritt zur Bereitstellung und Abrechnung von Musik-Contents. Der Kunde kann in einem Online-Shop MP3-Musikdateien bestellen und direkt auf seinen PC herunterladen. Musikbands stellen ihre Songs als MP3-Dateien auf den Callasong.de-Server und erhalten anteilig Geld, wenn sie von Usern bezogen werden. Die MP3-Dateien der Bands lassen sich individuell innerhalb einer vorgegebenen Spanne

bepreisen und entsprechend abrechnen. Auch interaktiver Fernunterricht lässt sich verwirklichen: dazu gehören Online-Prüfungen oder sprachunterstützte Frage- und Antwortstunden. Content Billing wird auch im Mobilfunk immer wichtiger. Ein Beispiel ist der Pannenservice, bei dem ein Mechaniker das liegengebliebene Fahrzeug per Handy-Kamera untersucht und dem Halter per Text, Sprache oder Grafik hilft. Auch die Medizin bietet viele Einsatzmöglichkeiten. Dazu gehört die Ferndiagnose bei Bergunfällen oder die Einbindung von Spezialisten, die nicht am Unfallort sind. Hersteller wie Ericsson entwickeln hierfür bereits UMTS-basierte Handies mit besonders großem Display und multimedialen Fähigkeiten.“ [13]

2.3.4 Veränderungen der Internet-Nutzung

2.3.4.1 Mobiles Internet

Das Geschäft der Mobilfunkanbieter beschränkt sich keinesfalls mehr auf Telefonie - Anwendungen. Multimedia hat auch hier Einzug gehalten. Mit der Festsetzung von GPRS als einen paketvermittelten Standard zur Datenübertragung wurden plötzlich Internetdienste sinnvoll und einigermaßen kostengünstig nutzbar. Mit der Entwicklung hin zu den sogenannten 3G - Netzen, also UMTS wird das Telefon mehr und mehr zum mobilen Internet-Endgerät. Diese Entwicklung ist ohne Mediation und Usage Metering nicht möglich. Usage Metering stellt die Grundlage für Transparente Tarifizierung von Inhalten und neuen Diensten dar. Dies gilt besonders auf dem mobilen Sektor, wo die Bandbreite ein noch stärker limitierender Faktor ist als im Festnetz. Es kann nun sehr genau abgerechnet werden, nicht nur nach Volumen, sondern auch nach Art der Anwendung. Man kommt dem Kunden also sehr entgegen. Beispielsweise kann somit das nicht sonderlich netzlastintensive Browsen im Internet zu günstigen Konditionen angeboten werden.

2.3.4.2 Vor- und Nachteile für den Nutzer

In gleichem Masse, in dem Metering Verfahren Vorteile für Dienstleister im Internet wie ISP bringen, kommen dem Nutzer diese Vorteile auch zu Gute. Doch Usage Metering muss nicht nur positive Aspekte haben.

ISPs versuchen durch verschiedene, an das Nutzungsverhalten angepasste Tarife, neue Kunden zu gewinnen. Der Wettbewerb dürfte das Internet für den Endnutzer somit günstiger machen. Er kann sich den für ihn besten Tarif aussuchen.

ISPs und andere Internet-Firmen versuchen mittels Metering, Informationen über das Kundenverhalten zu gewinnen. Diese Informationen können dem Kunden z.B. über die Rechnung aber auch zugänglich gemacht werden. Dadurch kann sich der Nutzer selbst besser analysieren um beispielsweise seine Effektivität zu erhöhen. Kostensenkungen für den Endnutzer können damit also einhergehen.

Internet Dienstleister versuchen aufgrund von z.B. Browsing-Informationen, dem Kunden dynamisch generierte, auf seine Surf-Gewohnheiten angepasste Seiten zu offerieren. Man möchte somit den Kundenwünschen besser entsprechen um leichter Dienstleistungen welcher Art auch immer verkaufen zu können. Dem Kunden bringt es den Vorteil, dass er schnell auf ihn bezogene 'Elemente' angeboten bekommt. Er kann somit seine online-Kosten senken.
Dem gegenüber kann diese Verfahrensweise aber auch dazu führen, dass Internet-Nutzer ständig auf neue, offensichtlich für ihn zugeschnittene Produkte, aufmerksam gemacht werden. Dynamisch erzeugte Webseiten könnten einen Kunden aufgrund seines Nutzungsprofils erst einmal durch mehrere Seiten von Angeboten schicken, die laut Profilanalyse seinen Interessen entsprechen, bevor er zu seinem eigentlichen Ziel gelangt. Dies ist vergleichbar mit gängigen Vorgehensweisen in Supermärkten, wo dem Kunden auf seinem Weg von Eingang zur Kasse möglichst viele Produkte gezeigt werden sollen. Das Browsen wäre somit ineffizienter und teilweise lästig.

2.4 Zusammenfassung

In diesem Dokument haben wir sowohl technische als auch ökonomische Aspekte des Usage Metering in IP-Netzen behandelt. Es wurden hierbei die zwei grundlegenden Forschungs- und Entwicklungsrichtungen beleuchtet. Dies war zum einen die IPDR, welche ein einheitliches Datenformat für die Übertragung von Nutznugsdaten sowie eine Messarchitektur für nutzungssensitives Messen von Kommunikationsverbindungen entwickelt. Zum zweiten war dies die RTFM. Auch sie entwickelte eine Messarchitektur. Jedoch kein einheitliches Datenformat. Grundlegender Unterschied der beiden Ansätze ist die Definition von Traffic-Flows. Dies ist die Grundlage der Nutzungserfassung in RTFM-Systemen. IPDR kennt derartige Kriterien für Kommunikationsverbindungen nicht. NeTraMet stellt eine bereits eingesetzte Implementierung des RTFM-Konzeptes dar. Im Gegensatz dazu existiert aufgrund der Komplexität kein bereits kommerziell eingesetztes, auf IPDR basiertes, System. Auch Schnittstellen zwischen den beiden Metering-Ansätzen existieren nicht und müssten im Bedarfsfall für spezielle Anwendungen extra implementiert werden.
Ungeachtet dessen haben Metering Systeme in der Internet-Welt bereits Einzug gehalten. Sie bilden die Basis zahlreicher Veränderung des Internet. Beispielsweise werden ISP in die Lage versetzt, dem Kunden nutzungsorientierte Tarifmodelle anbieten zu können. Desweiteren können Metering-Systeme genauere Erkenntnisse im Hinblick auf Netzplanung liefern. Ein weiterer wichtiger Anwendungsfall ist die Unterstützung von eContent-Anwendungen. Besonders Internet-Dienste in Mobilfunknetzen wie UMTS erfordern Metering-Syteme zur Resourcenkontrolle und Abrechnung, da Bandbreite hier noch stärker limitierend wirkt.
Jedoch haben Metering-Verfahren auch Nachteile. Die grosse Frage ist hier, ob der Mehraufwand für diese Messsysteme, sowohl finanziell als auch was den zusätzlichen Netztraffic angeht, in einem vernünftigen Verhältnis zum Nutzen steht. Es bleibt also abzuwarten, ob sich derartige Systeme grossflächig durchsetzen werden.

Literaturverzeichnis

[1] IPDR, “Netrwork Data Management - Usage (NDM-U) for IP based Services“, Version 3.1.1, http://www.ipdr.org, October 2002;

[2] Georg Carle, Sebastian Zander, Tanjy Zseby, “Policy basiertes Metering für IP-Netze“;

[3] Massimiliano Canosa, Martino De Marco, Alessandro Maiocchi “Traffic accounting mechanism for Internet Integrated Services“, CEFRIEL, Politecnico di Milano, 1998;

[4] “Netpressure.com - Bandwidth Demand in the Content Economy“, Phillips group;

[5] N. Brownlee, C. Mills, G. Ruth,“Traffic Flow Measurement Architektur - RFC 2722“, http://www.ietf.org, October 1999;

[6] N. Brownlee,“Traffic Flow Measurement MIB - RFC 2720“, http://www.ietf.org, October 1999;

[7] N. Brownlee, “RTFM: Applicability Statement - RFC 2721“,http://www.ietf.org, October 1999;

[8] N. Brownlee, “Traffic Flow Measurement: Experiences with NeTraMet - RFC 2123“, http://www.ietf.org, March 1997;

[9] N. Brownlee, “SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups - RFC 2723“, http://www.ietf.org, March 1997;

[10] Nevil Brownlee, “SRL Compiler and Language Users Guide, “Version 4.2, August 1998

[11] “calljob - Personaldienstleistungen für Call-Center Branche“;http://www.calljob.de

[12] “IETF/IRTF“; http://www.ietf.org/, http://www.irtf.org/

[13] Jörg Stimmer, Johannes´Koethe, “Jetzt kommt es auf den Inhalt an - Content Billing: Herausforderung und Lösung“, telepublico-Verlag, 2003;

[14] Tim Furche, David Schmitz,“Accounting Management“, 20.07.2000

Kapitel 3

Electronic Payment Systems

Enrico Bonatesta

This thesis presents up-to-date payment systems by first dealing with the beginning of the Internet (military development and usage, later on scientific and today's commercial usage) in order to better understand the current problems.
Next, we will differentiate and explain advantages and disadvantages of payment systems in order to be able to explain today's standards. No distinct products are presented though, instead we elaborate on the functions and general solution proposals.
After this we present solution proposals which are not spread well in Europe yet and possible future solutions. The following chapers deal with the most significant point of this thesis: the comparison of the different systems in relation to overhead, customer's satisfaction and both advantages and disadvantages from customers' and dealers' viewpoint.
Finally, this problem is taken account of from the European Union's position. Reasons for an increased interest from the EU are considered as well as the main problems the EU has to deal with in future. The results are concluded and evaluated in the end.

Inhaltsangabe

3.1 Einleitung

„Laut aktuellen Umfragen brechen 50 Prozent aller Onlineshop-Kunden beim Bezahlvorgang den Einkauf im Internet ab. Sprich die Hälfte der potentiellen eCommerce-Kunden springt aufgrund der Bezahlverfahren noch kurz vor Kaufabschluss ab“ [VG01]
Diese Aussage spiegelt sehr deutlich das Problem wieder, dass derzeit eine ganze Reihe von Payment-Verfahren angeboten werden, deren Leistungsfähigkeit sowohl für Anbieter als auch für Kunden sehr schwer einzuschätzen ist. [MK0102] Deswegen werden nun nachfolgend momentan eingesetzte sowie auch in Zukunft eventuell verwendete Lösungen bezüglich des Overheads, der Akzeptanz beim Kunden und bezuglich Sicherheits- und Kostenaspekten analysiert.

3.1.1 Geschichte

Um die entstandene Problematik jedoch besser verstehen zu können, muss man als aller erstes die Geschichte des Internets betrachten, da diese essentiell für den heutigen Standard ist.

3.1.1.1 Militärische Nutzung

Ein wichtiger Meilenstein zur Entwicklung des Internets war 1957 der Sputnik-Schock zu Zeiten des „Kalten Krieges“. Die Westmächte standen einem Ostblock gegenüber, der in der Lage war, einen Nuklearschlag durch Interkontinentalraketen auf Amerika zu verüben und der vor allem den Amerikanern durch den Satelliten zeigte, dass diese im Vergleich zu den russischen Entwicklern ein Defizit hatten. Vor allem die US-Air-Force sorgte sich darum, dass die Kommandostruktur bei einem Atombombenabwurf auf die USA nicht aufrecht erhalten werden könnte. Dieser Problematik war man sich auch im Pentagon bewusst, weswegen das US-Verteidigungsministerium die Advanced Research Projects Agency (ARPA, später dann DARPA) gründete, welche den Auftrag zur Entwicklung neuartiger Technologien hatte. Und so wurde verzweifelt nach einem Netz gesucht, welches eben solch einen Nuklearangriff überstehen sollte. Somit war schon die erste Vorgabe gegeben: Das Netz musste dezentral aufgebaut werden. 1966 hat das zur ARPA gehörige Information Processing Techniques Office (IPTO) geplant, alle Computerzentren der ARPA miteinander zu koppeln. Ziel war dabei zusätzlich, dass auch verschiedene Rechner miteinander kommunizieren können. Als Basis der Planung verwendete man Paul Barans „Distributed Networks“ und 1969 verbindete des „ARPANET“(der Vorläufer des heutigen Internets) vier Rechner an vier Universitäten in den USA. Dabei waren alle verwendeten Rechner von unterschiedlichen Herstellern und benutzten unterschiedliche Betriebssysteme. Somit war es erstmals gelungen, Rechner unterschiedlichster Art miteinander zu verbinden. Dieses Computernetz kann man aber nicht mit dem heutigen Internet gleichsetzen,da es sich nur um ein Compuernetz und nicht um ein netz von Computernetzen handelte. Ferner kam es erst 1972 zur Erfindung der elektronischen Post (sog. eMails) durch Ray Tomlinson. Erst zu diesem Zeitpunkt wurde dann das Netzwerk auch genutzt, weil das Versenden elektronischer Post eine Vielzahl von Vorteilen zur herkömmlichen

Post hatte (schneller, billiger, bequemer,...). Durch diesen Aufschwung wurden auch immer mehr Anhänger und Forscher gefunden, die sich für das Netzwerk interessierten. Ein weiteres Ereignis, welches die Beliebheit noch mehr steigerte, war die Präsentation auf der International Conference on Computer Communications. Dabei wurde durch 40 miteinander verbundenen Rechnern ununterbrochen drei Tage lang die Vorteile und Möglichkeiten dieses ARPANETs gezeigt. Zur Erweiterung des ARPANETs trug die ARPA selbst entscheidend bei, da diese ihr Wissen an Universitäten, der NASA, dem Wetterdienst, der National Science Foundation und der Air Force weitergab. So entstanden nun weitere Netze, wie z. B. das ALOHANET auf Hawaii, welches 1972 an das ARPANET angeschlossen wurde. Um nun selbst die verschiedensten Computernetzwerke zu verbinden, musste ein einheitliches Protokoll entwickelt werden, und 1974 wurde das TCP/IP als geeignetes Protokoll entwickelt, welches allerdings erst 1983 zum Standard des ARPANETs wurde. Ein weiterer Meilenstein in der Geschichte war die Entwicklung von sogenannten USENETs 1976, also Newsgroup-Foren für die unterschiedlichsten Interessen. 1983 hatte sich das ARPANET in das militärisch genutzte MILNET und das nun vollständig zivil genutzte ARPANET gespalten.

3.1.1.2 Wissenschaftliche Nutzung

1985 entwickelte sich dann ein weiteres Netz neben dem ARPANET: das National Science Foundation Network, kurz NSFNET. Dieses Netz wurde nun in den Folgejahren immer beliebter, wohingegen immer weniger Forscher das ARPANET nutzten, welches 1990 dann für überflüssig gehalten und aufgelöst wurde. Seine Funktionen übernahm nun das NSFNET. Diesem Netz schlossen sich nun nach und nach weitere Netzwerke aus anderen Ländern an. 1991 zog sich das Department of Defensive (DoD) dann vollständig aus der Förderung des Internets zurück, und im selben Jahr wurde das Hyperlink- System entwickelt. Doch erst 1993 gelang dem Internet der wahre Durchbruch, obwohl auch vorher schon die Wachstumsrate enorm war. Grund hierfür war die Entwicklung eines Browsers (Netscape Navigator). So konnten nun interessante Seiten und ähnlichen Themenbereiche aufgrund des Hyperlinksystems verlinkt werden, wobei die Navigation nun auch keine sehr guten Computerkenntnisse mehr nötig waren.

3.1.1.3 Kommerzielle Nutzung

1993 war auch das Jahr, in dem die Universitäten ebenfalls die Finanzierung des Internet einstellten, welche sie seit dem Rückzug des DoD stellvertretend übernommen haben. Das Wachstum des World Wide Webs nimmt auch heute noch stetig zu, vergleiche hierzu die Grafik 3.1, und so gibt es im heutzutage (Dezember 2003) mittlerweile 45.980.112 verschiedene Websites.

3.1.2 Entstandene Probleme und Entwicklung

Aufgrund der Entwicklung bzw. auch der Änderung des Internets haben sich zahlreiche Probleme ergeben. So gab und gibt es heute keine Zugangskontrolle, was sich allerdings

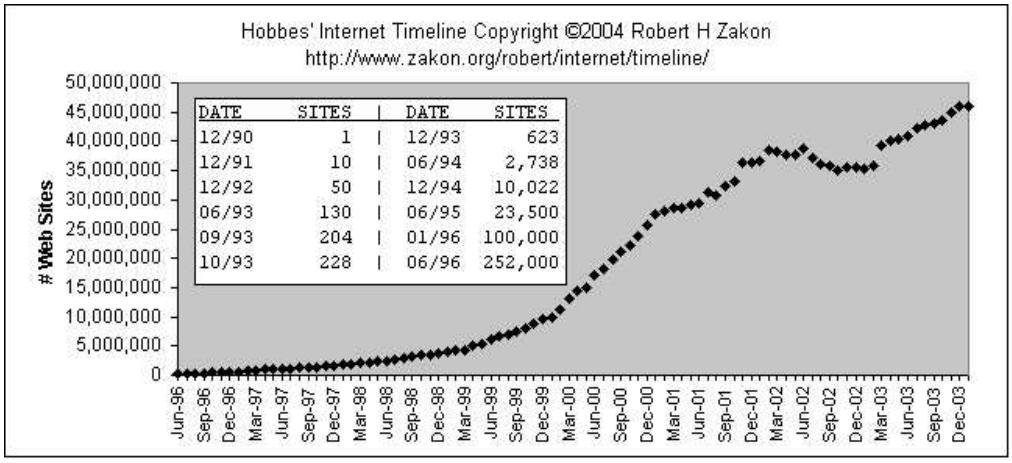

Abbildung 3.1: Das Wachstum des World Wide Web
[RZ03]

in dem Internet der Zukunft ändern wird. Ferner wird sich in diesem Internet auch eine Unterscheidung von Paketen aufgrund der Dienstedifferenzierung realisieren lassen, welche bislang absolut gleich behandelt wurden. Ein weiteres Problem entstand 1993, als die Universitäten (dem Militär folgend) die Finanzierung des Internets aufgaben und es nur noch kommerziell genutzt wurde. Da die finanzielle Deckung mittels Werbung langfristig keine Lösung sein wird, werden in Zukunft vermehrt Gebühren für Inhalte verlangt, wobei dieses „Paid Content“ jedoch kein Teil dieser Ausarbeitung ist. Das Hauptproblem liegt aber daran, dass bei der damaligen Entscheidung und Entwicklung wichtig war, das es dezentral aufgebaut ist. Diese Dezentralisierung hat aber zur Folge, das man die Entwicklungen heutzutage nur noch schwer steuern kann und somit eine Vereinheitlichung praktisch fast nicht möglich ist.

3.1.3 Was sind Payment Systeme?

Um diese Frage klären zu können, muss man sich erst vergegenwärtigen, wo man diese Systeme eigentlich einordnen muss. Wie schon erwähnt ist ePayment ein Teil des eCommerce, also des elektronischen Handels. Dabei wird analog zum konventionellen Handel auch zuerst die Ware von einem Händler angeboten, welche dann durch den Kunden ausgewählt und bestellt wird. Danach gibt es zwei Möglichkeiten: Bei der ersten wird sofort im Anschluss an das Bestellen bezahlt und erst danach wird die Ware geliefert. Die Alternative ist, das vor dem Bezahlen zuerst die Ware geliefert wird. Bei beiden Verfahren wird der Bezahlvorgang als eCommerce bezeichnet. Dieses kann man auch in Abbildung 3.2 deutlich erkennen.

3.1.3.1 Anforderungen

„Ein gutes Zahlungssystem muß verschiedene Anforderungen erfüllen. So muß es resistent gegenüber Manipulationsversuchen sein. Geleichzeitig dürfen die Kosten pro Transaktion, um diese Sicherheit zu erreichen, nur sehr gering sein. Manchmal wünscht der Käufer,

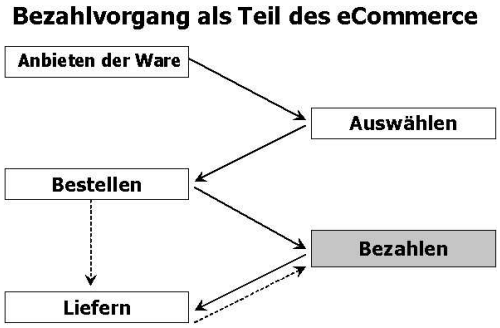

Abbildung 3.2: Wo muss man Payment Systeme eingliedern [HM03]

seine Einkäufe anonym zu tätigen, wie es etwa mit Bargeld möglich ist. Diese Anforderung läßt sich wiederum nur schwer mit dem Wunsch nach einer besonders sicheren Bezahlungsmöglichkeit verbinden. Auch sollten Transaktion in beliebiger Höhe, von 0,1 Eurocent bis zu Tausenden von Euros ökonomisch durchführbar sein. Weiter müssen Zahlungssysteme,um akzeptiert zu werden, von allen Beteiligten einfach zu bedienen sein.Der technischen Realisierung der genannten Forderungen stehen jedoch politische und rechtliche Hürden im Weg.“[SFE97] Um aber die nachfolgenden Anforderungen von Payment Systems genau zu analysieren, ist es notwendig, die eigentlichen Funktionen von Geld zu erläutern. „Der Volkswirtschaftslehre nach lässt sich Geld begreifen als ein Medium, welches drei postulierte Funktionen erfüllt:

- erstens die des allgemein akzeptierten Zahlungsmittels
- zweitens soll Geld die Wertaufbewahrung erlauben
- und drittens soll das Geld als gemeinsamer Nenner die Recheneinheit stellen

Jedoch wurde Geld im Verlauf der Mednschheitsgeschichte zu weit mehr als einem Medium, dass diese drei Funktionen - vielleicht in unterschiedlich akzentuierter Qualität und Güte- erfüllt.“ [KlSp98] Was sollten aber nun speziell E-Payment-Verfahren anbieten?

Als erstes sollten die **Einstiegs- und Betriebskosten niedrig** sein. Denn ob sich ein Verfahren tatsächlich rechnet und somit auch durchsetzt , hängt stark von den Kosten bei der Inbetriebnahme ab, wie z. B. ein Kartenlesegerät für eine Guthabenkarte oder der Software für eine „elektronische Geldbörse“.

Zweitens sollten auch die **Transaktionskosten niedrig** sein. Dabei hängt dies allerdings stark davon ab, ob sich genügend Kunden an dem System beteiligen. Das jedoch hängt wiederum von all den hier aufgeführten Anforderungen bzw. der Umsetzung dieser Anforderungen ab.

Dritten sollten idealerweise Systeme ausgewählt werden, die eine **einfache Nutzung** garantieren. Sollte hierbei zusätzliche Software von Nöten sein, so sollte sie zumindest einfach ohne größeren Aufwand zu installieren und ein technischer Support seitens des Anbieters gewährleistet sein. Systeme, für die man besondere Fachkenntnisse oder spezielle komplexe Software benötigt, schrecken den Kunden ebenso ab, wie Systeme, bei denen man

personenbezogene Daten bei jedem Zahlvorgang eingeben muss. Auch spielt hierbei die Geschwindigkeit für viel Konsumenten eine Rolle. Dauert der Zahlungsvorgang zu lange, existiert zumindest die Gefahr, das der potentielle Käufer sich durch ein paar Mausklicks einen anderen, ebenbürtigen Händler aussucht.

Der vierte Punkt begründet sich in der Globalität. Für Unternehmen, die weltweit erreichbar sein wollen, gehört auch, dass sie alle gängigen Währungen akzeptieren. Da man bei einem solchen Unternehmen von einer internationallen Käufercliental ausgehen kann, sollten sich gerade deswegen „Universallösungen“ bei Paymentsystemen dadurch auszeichen, dass sie einen **Wechselkurs - Umrechner** anbieten.

Last but not least sollte auch eine **größtmögliche Verbreitung** des Systems gegeben sein. Denn je höher die Akzeptanz eines elektronischen Zahlungssystems ist, umso attraktiver wird es für eine noch größere Anzahl von Anwendern, und somit zum sogenannten Selbstläufer. Man vergleiche hierzu den Aufstieg der Ec-Karte. (vgl [HM03])

3.1.3.2 Vorteile

Die Vorteile für Paymentsysteme im Vergleich zu klassischen Bezahlsystemen (wie z. B. Nachnahme) begründen sich in der nicht mehr ausreichend entsprechenden Deckung der Bedürfnisse von Markt und Mensch. So wurde vergleichsweise in der Vergangenheit der Scheck als ein neues Bezahlverfahren für größere Geldsummen anstelle des Bargelds eingeführt. Ziel war und ist immer ein größerer Anwendungskomfort und eine höhere Leistungsfähigkeit. So auch bei Paymentsystemen. Derzeit werden im elektronischen Handel zwar immer noch klassische Bezahlsysteme genutzt, aber man (Hersteller und Anbieter von elektr. Zahlungssystemen sowie Unternehmer) ist bestrebt, so genannte E-Payment-Lösungen zu etablieren und einzusetzen. Aus mehreren guten Gründen, da sowohl Anbieter als auch Käufer von einer elektronischen Abwicklung der Zahlungsvorgänge profitieren können:

1. **Höhere Effizienz**

   Durch eine vollständig, durchgängig elektronisch abgewickelte Transaktion kann es zu einer viel höheren Effizienz der Geschäftsabläufe führen. Die Anzahl der Mitarbeiter kann dadurch evtl. verringert werden (Vorteil für den Anbieter) und somit auch viele Fehlerquellen ausgemerzt werden (Vorteil für Käufer und Anbieter). Dadurch wird das Produkt evtl. auch billiger und ist wahrscheinlich deutlich schneller beim Käufer. Dies ist sowohl für den Verkäufer gut, da sein Ruf positiv beeinflußt wird, sowie für den Käufer, der sehr zufrieden sein kann.

2. **Niedrige Transaktionskosten**

   Auch die Transaktionskosten einer elektronischen Zahlung sind meist deutlich niedriger als bei Verwendung traditioneller Verfahren. Dies begründet sich vor allem in administrativen Kosten. Offensichtlich ist dies ein Vorteil für beide Parteien.

3. **Weniger Zahlungsausfälle**

   Eine Gefahr bei traditionellen Verfahren, wie z. B. per Rechnung, ist der Zahlungsausfall durch die schlechte Zahlungsmoral der Kunden und den damit verbundenen Nebenkosten die durch Mahnbescheide und dem zeitlich ausfallenden Kapital entstehen. Dies könnte man durch Vorkasse oder aber durch Bonitätsprüfungen um ein Vielfaches senken, vielleicht sogar ganz vermeiden. Ferner wird durch die nahezu zeitgleiche Abwicklung von Lieferung und Bezahlung weniger Kapital gebunden. Dies wiederum würde deutlich dem Verkäufer zugute kommen, indirekt aber auch dem Käufer.

4. **Höhere Umsätze** Durch den anfangs schon erwähnten Anstieg im Bereich des eShopping erhöht sich der Umsatz in diesem Markt kontinuierlich. Einfache Paymentsysteme erleichtern dies und fördern es sogar. Werden dabei auch noch unterschiedliche Zahlungssysteme angeboten, bei denen der Kunde auswählen kann, welches ihm am angenehmsten und/ oder sichersten scheint, so kann man zusätzlich Kunden gewinnen bzw. an sich binden. Diese Instrumentalisierung von Bezahlkomfort und Bezahlsicherheit sollte man nicht außer Acht lassen. (vgl. hierzu [HM03])

3.1.3.3 Nachteile

Es gibt leider auch einige Nachteile bei ePayment-Systemen. So sind die meisten Systeme nur für eine gewisse Geld-Spanne geeignet, entweder für Kleinstbeträge oder sehr große Beträge. Es kann aber auch sein, dass die Anonymität eventuell verloren geht und ein Missbrauch der Transaktionsdaten stattfindet. Ein weiterer Nachteil kann in der Beschaffung zusätzlicher benötigter Zusatzsoftware liegen.[03] Gleiches gilt auch für eventuell benötigte Mittelsmänner, die ebenfalls einen Risikofaktor darstellen können. Auch eine höhere Anzahl an Angestellten, die Benutzer informieren und aufklären, kann ein Nachteil sein. [IS00] Der Kreditkartenmissbrauch und Sicherheitsaspekte sind aber wahrscheinlich die größten Nachteile des heutigen eCommerce [TJM99]

3.1.4 Blick in die Zukunft

Aufgrund der beschriebenen Schwierigkeiten und angetrieben von der Aussicht, in einigen Jahren mit Millionen von potentiellen Käufern direkt kommunizieren zu können, entwickelten und entwickeln einige Firmen Systeme, mit denen Bezahlen im Internet auf eine sichere Art und Weise möglich ist. Dabei werden auch Allianzen gegründet, mit dem Ziel einheitliche Standards zu etablieren. Dies ist auch dringend nötig, da eine Umfrage der Universität Karlsruhe aufgezeigt hat, dass sich 70 % der Befragten eine Standardisierung von Internetzahlungsverfahren wünschen, um so dass eShopping attraktiver zu machen [UK0102]. In diesem Falle ist vor allem die EU gefordert, siehe hierzu auch Kapitel 3.5 auf Seite 80. Hierbei muss man sich jedoch immer vor Augen halten, das der Zahlungsverkehr im Internet ein zentrales, derzeit noch nicht vollständig gelöstes Problem ist.

3.2 Analyse verschiedener Payment Systeme

Da es mittlerweile einige Lösungen in diesem Bereich gibt, ist es vorerst wichtig, dass die Unterteilung zuerst einmal dargestellt wird. Dadurch kann man die Lösungen besser verstehen und auch gleich den einzelnen Klassen zuordnen.

3.2.1 Logische Unterteilung der Payment Systeme

Es gibt heutzutage eine Vielzahl an Klassifizierungen von Paymentsystemen. Die häufigsten werden nun nachfolgend dargestellt.

3.2.1.1 Unterteilung zwischen Buchgeld und Tokenbasierten Verfahren

„Das wohl häufigste Kriterium unterscheidet sie danach, ob es sich um ein Buchgeld oder ein token basiertes Verfahren handelt. Bei dem Buchgeld basierenden Zahlungsverfahren besteht zum Kreditkartenkonto des Kunden ein direkter oder indirekter Bezugspunkt. Es handelt sich hier um einen sog. traditionellen Zahlungsweg. Das Tokenverfahren ist sog. elektronisches Geld, das nur im Internet seine Gültigkeit hat. Mit seiner Übertragung wird die Ware bezahlt und das Eigentum an den Token geht auf den Verkäufer über.“ [X01]

3.2.1.2 Unterteilung nach der Höhe der Transaktion

Eine weitere mögliche Unterteilung der Payment Systeme ist die Klassifizierung nach der Höhe der Transaktionen. Da jedoch hier noch keine definitive allgemeine Einigkeit über die Grenzwerte zwischen den unterschiedlichen Ausprägungen der Klassifizierung und den Klassen selbst herrscht, wird nachfolgend das Schema dargestellt, welches in dieser Arbeit verwendet wird, wobei es jedoch auch andere Unterteilungen gibt.

- Macropayments (>1000 Euro)
- Medium oder Small Payments (5,0 - 1000 Euro)
- Micropayments (0,1 - 5,0 Euro)
- Nanopayments (<0,1 Euro)

Diese Aufteilung ist sehr stark an den zugrundeliegenden Geschäftsbeziehungen und den dafür eingesetzten Zahlungsverfahren orientiert. Es gibt aber auch Quellen, in denen nur zwischen Micro- und Macropayment unterschieden wird, da bei diesen beiden spezielle Anforderungen bezüglich der Sicherheit und der Höhe der verursachten Transaktionskosten für einen Bezahlvorgang gestellt werden. (vgl. dazu [YB03], [UK02][TSMS98])

3.2.1.3 Unterteilung nach dem Zeitpunkt

Eine andere mögliche Kategorisierung setzt das Augenmerk auf den Zeitpunkt, an dem das Kundenkonto durch dem Zahlungsbetrag belastet wird. So gibt es Verfahren die das Kundenkonto schon vor einer Transaktion belasten. Solche Verfahren werden „Pre-Paid“ genannt, und hierbei unterscheidet man in Hardware-basierten sowie Software-basierten Lösungen. Für erstere ist z. B. die Geldkarte zu nennen, wohingegen bei zweiterer PaySafeCard ein mögliches Beispiel ist. Eine weitere Kategorie sind die sogenannten Pay-Now-Verfahren, bei der der Kunde sofort nach einer Transaktion bzw. dem Erhalt der Ware zahlen muss, wie z. B. bei Nachnahme. Die dritte und letzte Kategorie sind Pay-Later Verfahren, bei der das Kundenkonto erst später belastet wird. Beispiele für diese Variante sind Kreditkarten, Rechnungen und Billingsysteme. [UK02]

3.2.1.4 Unterteilung aufgrund der beteiligten Akteure

Auch diese Klassifizierung wird in einigen Quellen verwendet. Dabei ist entscheidend, welche Personen/Unternehmen daran beteiligt sind. So sind neben dem Kunden und Händler eine Vielzahl weiterer möglicher Drittpersonen denkbar, wie zum Beispiel die Herausgeber von Werteinheiten (Banken, Telefongesellschaften und große Handelsketten). Aber auch die Entwickler und Betreiber von Zahlungssystemen können dabei eine Rolle spielen, da sie zum Beispiel die Händlereinnahmen an die Banken weiterleiten. Ein weiterer Akteur könnte auch eine Zertifizierungsstelle sein sowie bei kartenbasierten Payment-Systemen der Kartenherausgeber und die damit verbundenen Aufladestellen. (vgl. [MM99], [YB03])

Wie schon erwähnt, gibt es noch einige andere Unterteilungen, wie die eben aufgeführte Unterscheidung in eine reine oder hardwareunterstützte Softwarelösung, wie es bei kartenbasierten Zahlungssystemen realisiert wird. Eine weitere Möglichkeit wäre die Unterteilung in On- und Offline Zahlungssystemen. Diese Kategorisierungen werden aber in dieser Ausarbeitung nicht näher erläutert.

3.2.2 Vorstellen aktueller Verfahren

Die Entwicklung bei den Paymentsystemen ist äußerst dynamisch. So gab es z.B. 1998 folgende Paymentsysteme

1. CyberCash
2. Cybercoin
3. eCash
4. First Virtual
5. Millicent

6. Mondex
7. NetBill
8. Netcash
9. Netcheque
10. SET
11. und herkömmliche Verfahren wie Nachnahme, Kreditkarte, etc

Nur drei Jahre später im Jahr 2001, gab es von den vorgestellten Verfahren nur noch 5, 6, 10 und 11.[MB01] Dafür kam eine Großzahl anderer Systeme auf dem Markt. Aus diesem Grund werden nun nachfolgend keine einzelnen Systeme vorgestellt sondern nur die Grundprinzipien erörtert.

3.2.2.1 Abbuchung mittels Kreditkarte

„International bezahlt man mit Kreditkarte“[HM03]. Dieses Zitat sagt eigentlich schon ziemlich alles. Bei dieser Variante des ePayment gibt ein Käufer seine Kreditkartennummer an und erhält nach dem Pay-later Prinzip seine Ware. Schwachpunkt dieser Lösung ist eigentlich nur die Übermittlung der Nummer sowie deren „Aufbewahrung“. Doch in den letzten Jahren gab es schon einige Verbesserungen, wie z. B. die verschlüsselte Übermittlung durch SSL. Nachteilig ist bei einer Kreditkartentransaktion allerdings, das diese nur für den Medium-/Macropayment-Sektor sinnvoll ist.[HM03]

3.2.2.2 Abbuchung mittels Lastsschriftverfahren

Das Lastsschriftverfahren wird ähnlich wie beim traditionellen Einkauf auch im elektronischen Handel eingesetzt. Es erlaubt dem Händler, sofort nach Eingang der Erlaubnis und vor dem Versenden der Ware das Geld direkt vom Konto des Kunden abzubuchen. Da aber im traditionellen Handel hierfür eine Unterschrift benötigt wird, gab es eine kleine Modifikation, da dies im eCommerce nicht ohne weiteres möglich ist. Bislang hat ein Großteil der Transaktionen ohne Unterschrift stattgefunden, was dazu führte, dass bei Differenzen der Kunde dies abstreiten konnte. Dies führte auf Händlerseite zu Zahlungsausfällen. Deswegen wurde das System nun weiterentwickelt, so das es nun möglich ist, eine eindeutige elektronische Signatur abzugeben. Diese ist (nach dem Signaturgesetz) heutzutage einer normalen Unterschrift gleichgesetzt. Das Verfahren ist allerdings nur in Deutschland möglich und ist eigentlich nur im Medium-/ Macropayment-Sektor sinnvoll. [HM03]

3.2.2.3 Abbuchung mittels Rechnung

Dieses Verfahren wird nicht nur im konventionellen Handel genutzt, sondern auch Vielfach beim eCommerce. Hierbei kann ein Kunde im Internet einkaufen, die Rechnung wird ihm dann mit der Ware zugesendet bzw. per eMail mitgeteilt. Danach kann der Kunde in einem gewissen Zeitraum die Überweisung tätigen. Dieses Verfahren ist ein klassischen Pay-later System und kann im Medium-/ Macro-Sektor sowie eingeschränkt auch im Micro-Sektor verwendet werden. [UK02]

3.2.2.4 Abbuchung mittels Geldkarte

Guthabenkarten, auch Smart cards genannt, werden vor dem eigentlichen Kaufvorgang mit einem gewissen Geldbetrag aufgeladen, entweder bei Banken oder Kartenbietern, wobei dem Kundenkonto dieser Betrag abgebucht wird. Diesen Betrag können dann die Kunden bei Transaktionen aufbrauchen und die Geldkarte gegebenenfalls wieder aufladen. Da hierfür bei Kaufvorgängen jedoch ein Kartenleseautomat benötigt wird, und da es auch umständlich ist, die Karten immer wieder neu aufzuladen, haben sich Geldkarten allerdings noch nicht durchgesetzt. Dieses Prepaidverfahren ist aber für Micro- als auch für Medium- sowie Macrosystem- Verfahren geeignet.[HM03]

3.2.2.5 Abbuchung mittels sog. Scratchcards

Diese Rubbelkarten sind ebenfalls ein Prepaid-Verfahren und ähneln dem Prinzip von Rubbelkarten, die bei Handys ohne Vertrag genutzt werden. Diese Karten kann man im stationären Handel, wie zum Beispiel an Kiosken oder an Tankstellen erwerben. Ein Beispiel für solch einen Anbieter ist die Paysafecard, mit der man ohne Angabe von persönlichen Daten im Internet einkaufen kann. Bei der Paysafecard gibt es zwei unterschiedliche Versionen, wobei die rote Karte für Jugendliche unter 18 Jahren Erotikseiten sperrt. Die Blaue hingegen ist für Volljährige vorgesehen und hat keine Einschränkungen. Es funktioniert folgendermaßen: Nachdem ein Kunde ein Produkt in einem Onlineshop ein Produkt ausgewählt hat, gibt er einen x-stelligen PIN-code ein (bei der Paysafecard ist dieser Code 16 stellig), denn er vorher auf seiner Karte freigerubbelt hat. Eventuell gibt er dazu noch ein Passwort ein. Der Scratchcard-Server überprüft dann das Guthaben dieser bestimmten Karte und belastet danach die entsprechende PIN mit dem Kaufpreis. Bei diesen Transaktionen können je nach System auch mehrere solcher Karten (bis zu 10 Stück) kombiniert werden. [UK02]

3.2.2.6 Abbuchung mittels elektronischer Schecks

Dieses klassische Bezahlverfahren im konventionellen Handel wurde ebenfalls im elektronischen Handel nachgeahmt und ist im Medium-/Macropaymentsektor in den USA verfügbar. „Dem Konzept des elektronischen Schecks liegt die Idee zugrunde, ein elektronisches Dokument aus Bits und Bytes, das dieselben Informationen wie das konventionelle Scheckformular enthält, zu verwenden und dieses mit einer digitalen Signatur für

den sicheren Einsatz im Internet zu versehen.[...] Ein elektronischer Scheck enthält dabei alle Informationen, die auch ein konventioneller Scheck aufweist: den Namen des Ausstellers, seiner Bank und den des Empfängers, die Accountnummer, den Zahlungsbetrag und die Währungseinheit sowie eine digitale Unterschrift, welche die Echtheit des Schecks bestätigt."[IB97] Dabei werden in Onlineshops digitale Formulare bereitgestellt, die der Kunde ausfüllen muss. Die Information wird dann an den Händler gesendet, wobei dieser dann die Beträge (nach Überprüfung der Echtheit durch bestimmte Geldinstitute) einlösen kann. „NetCheque" ist ein konkreter Ansatz zur Umsetzung dieser elektronischen Schecks. [IB97]

3.2.2.7 Abbuchung mittels digitalem Bargeld

[MM99] Die Abbuchung mittels digitalem Bargeld ist ebenfalls eine mögliche Variante beim Bezahlvorgang im eCommerce, wobei es grundsätzlich nur im Micropayment-Sektor verwendet wird. Um das Prinzip dieser elektronischen Geldbörsen leichter zu verstehen, wird es am Beispiel CyberCoin (von der Firma CyberCash) veranschaulicht, wobei dieses Produkt mittlerweile schon lange nicht mehr aktuell ist. Es zeigt aber sehr deutlich das Prinzip digitaler Münzen. Dabei muss ein Kunde zuerst den Betrag angeben, der von seinem Bankkonto auf das CyberCoin-Schattenkonto geladen werden soll. Dann werden die Daten vom Gateway geprüft und an die zuständige Bank weitergeleitet. Daraufhin erhält der Kunde die sogenannten CyberCoins, welche er dann in einer elektronischen Geldbörse aufbewahren kann. Gleichzeitig wird sein Bankkonto mit dem jeweiligen Betrag belastet. Will der Kunde nun eine Bestellung oder Transaktion durchführen, so überträgt der Händler das Gut, wobei es erst am Ende der Transaktion freigeschalten wird. Danach führt der Kunde die Zahlungsanweisung durch und das Cashregister des Händlers fügt gewisse Daten hinzu. Daraufhin werden die modifizierten Cybercoins an das Gateway weitergeleitet und die Daten überprüft. Schließlich werden die Cybercoins dann vom Schattenkonto des Kunden auf das Schattenkonto des Händlers übertragen. Abschließend wird dann das Gut freigeschaltet.[TU02]

Wie schon erwähnt, besteht bei manchen Zahlungen der Bedarf nach Anonymität. Dagegen steht aber die mögliche Rückverfolgung bei solchen digitalem Bargeld. Deswegen sind heutige elektronische Münzen teilweise mit einem Zusatzverfahren ausgestattet, was man auch als Blinding bezeichnet. Diese blinden Signaturen, wurden von David Chaum entwickelt, um Seriennummern von elektronischen Objekten (z.B. digitale Münzen des eCash-Systems) während des Signaturprozesses auszublenden. Somit kann nachträglich keine Zuordnung zwischen Seriennummer und Benutzern stattfinden. [LC2]

3.2.2.8 Abbuchung mit Hilfe von Treuhändern

Vor allem in Auktionshäusern wie eBay wird häufig die sog. Treuhänderschaft angeboten, was somit dazu führt, dass man letztendlich auch diese Art von Zahlungsverkehr zum ePayment hinzuzählen muss. Hierbei soll durch denn sog. Treuhänder (meist in Form eines Rechtsanwalts oder Notars) gewährleistet werden, dass der Kunde seine Ware erhält und nicht umsonst bezahlt, und ebenso soll für den Händler gewährleistet werden, dass er

sein Geld sicher erhält. Die Funktionsweise ist ganz einfach: der Kunde bezahlt nach der Bestellung der Ware den Preis in ein Konto ein, dass vom Treuhänder gestellt wird. Dieser gibt dann, nach Eintreffen des Geldes, dem Händler eine positive Bestätigung, woraufhin dieser die Ware versendet. nachdem der Kunde die Ware erhalten hat, gibt dieser dem Treuhänder ebenfalls eine Rückmeldung, woraufhin dieser veranlässt, dass der Betrag auf das Konto des Händlers überwiesen wird.(vgl. [LC2],[X01])

3.2.3 Vorstellen zukünftiger, noch nicht marktrelevanter Verfahren

3.2.3.1 Elektronische Münzen als Lotteriescheine

Das Hauptziel dieses Micropaymentsystems ist die Minimierung der Transaktionenkosten. Es funktioniert folgendermaßen: Ein Kunde erwirbt Lotteriescheine, die einen bestimmten Nennwert haben, z. B. 1 Eurocent, und die eine gewisse Gewinnwahrscheinlichkeit, z. B. 1/1000 haben. Dabei verpflichtet er sich, dass er den Preis eines Scheines bezahlt, z. B. 10 Euro, sollte dieser gewinnen. Gewinnt kein Schein, so muss er nichts bezahlen. Mit diesen Scheinen kann er nun, je nach Höhe des jeweiligen Nennwerts, im Internet gewisse Dienstleistungen erwerben. Ein Beispiel hierfür: Ein Kunde nutzt gewisse Dienstleistungen und benötigt hierfür 215 Lotteriescheine, also einen Nennwert von 2,15 Euro. Gewinnt dabei keines seiner Lose, so muss er (0x10 Euro=) 0 Euro bezahlen. Gewinnt aber eines seiner Lose, so muss er (1x10 Euro=)10 Euro bezahlen.

Mit Hilfe der Wahrscheinlichkeitsrechnung kann man auch beweisen, dass bei solch einer Verteilung, und dem Kauf von Lotterielosen in Höhe von 100 Euro Nennwert es kaum zu Überbezahlung bzw. Unterbezahlung kommt. So liegt die Wahrscheinlichkeit, mehr als 200 Euro zu bezahlen, unter 0,4 % und die Wahrscheinlichkeit weniger als 50 Euro zu bezahlen unter 3 %. Wie man erkennen kann, kann man die Anzahl der Transaktionen durch diese Methode im Vergleich zu konventionellen Zahlungsmethoden deutlich verringern. So sind nun nicht mehr 1000 x 1 Eurocent zu bewältigen, sondern nur noch 1 x 1000 Eurocent. [RL01]

3.2.3.2 eGold

Das eGold System ging 1996 durch die amerikanische Delaware Corporation Gold & Silver Reserve Inc. (G&SR) online. Dieses elektronische System ist vor allem in Amerika beheimatet, hält aber mittlerweile auch in Deutschland Einzug. Es beinhaltet die Eröffnung und Führung eines persönlichen Kontos mit allen Funktionen (Waren und Dienstleistungen online erwerben, Überweisungen an andere eGold-Konten tätigen, Rechnungen bezahlen, Umtausch in Bargeld), wie dies ein normales Bankkonto ebenfalls bietet. Der einzige Unterschied besteht darin, dass das Konto nicht mit gewöhnlichen Devisen geführt wird, sondern auf der Basis des US-Dollars in Gold, Silber, Platin oder Palladium, je nach angegebener persönlicher Wahl. Das handelsüblichste Metall ist bei diesem Paymentsystem das Gold, wobei auch der entsprechende aktuelle Kurs Einfluß hat. Es kann aber auch direkt

mit dem US-Dollar gehandelt werden.Dabei ist die Eröffnung eines Kontos grundsätzlich kostenlos. Die Minimaleinlage über den normalen Bankentransfer beträgt jedoch 1.000,00 US-Dollar. Dieses Guthaben wird dann in dem entsprechend gewählten Metallwert geführt. Es gibt aber auch noch eine Alternativlösung für Kunden, die diesen hohen Betrag nicht aufbringen wollen oder können. Es basiert darauf, dass das Konto auch ohne Mindesteinlage geführt werden kann. Danach kann man sich von anderen eGold-Benutzern einen gewissen Betrag darauf überweisen lassen, sei es als Bezahlung einer Dienstleistung oder ein Austausch von Devisen durch eine Überweisung auf das Bankkonto des jeweiligen Geschäftspartner. Hintergrund dieser Möglichkeit ist die Problematik, dass alle eGold-Transaktionen Partner benötigen, die beide(!) ein eGold-Konto besitzen. Um auf das eGold-Konto Geld einzahlen zu können, muss man entweder diesen Betrag überweisen oder man bezahlt per Kreditkarte. Seit neuestem ist aber auch die Bezahlung mittels Moneybooker möglich, welches speziell für kleinere Beträge erschaffen wurde. Die Funktionsweise ist relativ einfach: Als allerstes geht man dabei auf sein eGold-Konto, welches verschlüsselt und mit einem Passwort geschützt ist. Nach der Auswahl „Spend“ gibt man nur die eGold-Nummer des Empfängers an, trägt den Betrag ohne Kommas und Punkten ein, wählt die gewünschte Währung und erwähnt evtl. noch den Verwendungszweck. Nach einer nochmaligen Überprüfung aller Daten und der Bestätigung mittels „confirm“ erhält man eine Seite „e-metal payment order-confirmation“, welche eine Referenznummer (batchnumber) beinhaltet. Diese Referenznummer ist die Überweisungsnummer, unter der die Transaktion getätigt wurde und die man dann später auch auf den Kontoauszügen sehen wird. Damit ist dieser Vorgang abgeschlossen und das Geld ist auf einem anderen eGold-Konto transferiert. Ein Vorteil dieser Lösung ist, dass eine Überweisung vom e-Gold Konto auf ein anderes im Vergleich zu einer herkömmlichen Banküberweisung unmittelbar erfolgt. Sie wird zeitgleich verbucht. Es gibt also keine Verzögerung. (vgl. hierzu [MB01], [HJ03])

3.2.3.3 mPayment

Bei mobilen Bezahlsystemen benutzt man andere etablierte Geräte bzw. Konzepte für den Bezahlvorgang. Bestes Beispiel hierfür ist das Handy. Es gibt aber auch hier zahlreiche unterschiedliche nationale Lösungen, wie es die Abbildung 3.3 deutlich macht. Um das Prinzip sichtbar zu machen, werden nun am Beispiel von „Vodafone m-pay“ die Grundlagen besprochen. Bei dieser Payment-Solution ist keine Anmeldung, Vorab-Registrierung oder Freischaltung nötig. Ferner sind auch keine speziellen Zugangscodes bzw. Zusoftwares erforderlich. Ebensowenig ist eine Kreditkarte gefordert. Die Funktionsweise ist eigentlich sehr leicht, nur gibt es zwei Varianten, die nun nachfolgend betrachtet werden müssen:

1. **Bestellung über das Handy**

   Hier wählt ein Kunde über ein WAP-fähiges Handy ein Angebot aus und kriegt darauf eine Bestätigungsaufforderungen, welche per Knopfdruck möglich ist. Die Abbuchung erfolgt dann per Handyrechnung oder vom Prepaid-Guthaben. Vodafone übernimmt also das Inkasso-Verfahren und die Authorisierung mittels der SIM-Karten jedes einzelnen Handys.

2. **Bestellung mittels PC**

   Hier wählt ein Kunde ebenfalls die Ware aus, gibt dann seine Handynummer in dem Portal an, worauf er eine SMS mit dem Bezahlcode erhält. Diesen gibt er dann im Online-Shop an, bestätigt diesen dann, und erhält dann die Ware. Auch hier verläuft die Abbuchung analog.

Dieses Pay-Later-Verfahren ist sowohl im Micropayment-Sektor als auch begrenzt im Medium-/Macropayment-Sektor sinnvoll verwendbar.(vgl. hierzu [HM03], [MZ02],[MK0102], [MK02])

Banko.max (Austria)	Oskar (Check Republic)
BankPass Mobile (Italy)	Paiement CB sur mobile (France)
Bibit (Holland, international)	Paybox (Germany, Sweden, Spain, Austria, UK)
Cellonet (Sweden, Netherlands)	PayDirect (USA)
Cingular DirectBill (USA)	Payitmobile (Germany)
EMPS (Sweden, Finland)	Payline (France)
EMT (Estonia)	PayPal (USA)
Fundamo (South Africa)	Phonepaid (UK)
Genion M-payment (Germany)	Promonetic (France)
GiSMo (Sweden, UK, Germany)	Sonera Mobile Pay (Finland, Sweden)
iCash (Sweden)	Sonofon mBanking (Denmark)
Metax (Denmark)	StreetCash (Germany)
Mint (Sweden)	Swisscom Sicab (Switzerland)
MobilMat (Italy)	Telenor Mobil (Norway)
mobilpay (Austria)	Telepay EU (Finland, Germany, Italy, France)
MobiPay (Spain)	Telia Payit (Sweden)
mPay (Denmark)	VisaMóvil (Spain)
NTT DoCoMo i-mode (Japan)	Vodafone m-pay bill(UK)
Omnitel Onphone (Italy)	Waaap Pag (Brasil)

Abbildung 3.3: mobile Payment-Systeme
[MK02]

3.2.3.4 Bezahlung per eMail

Dieses weltweite Internetbezahlsystem wurde von PayPal entwickelt und ist bislang grötenteils in den USA vertreten (ähnliche Verfahren sind Bidpay (Western Union), Billpoint (ebay), Anypay (Europa),egg (in England) und VISA direkt). Es ist kostenlos, sekundenschnell und währungsunabhängig, wobei bei Pay-Pal ein „echtes“ US-Dollar-Konto geführt wird, also kein virtuelles Geld. Alternativ gibt es mittlerweile auch Britische Pfund- oder Euro-Konten. Momentan nutzen es 20 Mio Kunden und es funktioniert folgendermaßen:[MB03] „Nach der Anmeldung mit der Angabe der persönlichen Daten und der Email-Adresse, wird eine eigene Kreditkarte benötigt. Über diese Kreditkarte wird eine Testbuchung in Höhe von $1,95 vorgenommen. Auf dem Kreditkartenauszug erscheint dann bei der nächsten Abrechnung ein 4-stelliger Code. Diese Code-Nummer wird dann auf der PayPal-Seite angegeben und wird dann in den Status Verified versetzt. Danach ist man ein sog. Verified Personal User und kann Zahlungen leisten bzw. Geld anfordern.“[LC1] Für die eigentliche Transaktion ist kein Bankkonto mehr nötig. Der Kunde überweist einen gewissen Betrag an seine persönliche eMail-Adresse. Die Transaktionen werden dann innerhalb PayPal unter Ausschluss von Banken geführt, wobei Einzahlungen auf das PayPal-Konto nur über Kreditkarte und Auszahlungen nur auf ein Bankkonto

möglich ist. Kontoführungsgebühren werden nur bei Ein-/Auszahlungen berechnet, Überweisungen sind kostenlos. Sollte das PayPal-Kundenkonto negative Salden aufweisen, so wird der Betrag automatisch von der Kreditkarte abgebucht. Wenn das PayPal-Konto gedeckt ist, wird das Transaktionsvolumen vom PayPal-Konto abgezogen. Somit sind keine Vorauszahlungen nötig, es ist also nicht nur ein Prepaid-Verfahren, sondern kann auch als Pay-Later-System verwendet werden(Nachteil: höhere Kontoführungsgebühren). Will man Geld überweisen, so sendet der Kunde eine eMail mit dem Betrag, welcher unmittelbar auf das PayPal-Konto des Empfängers gutgeschrieben wird. Nachteilig bei dem ganzen Verfahren ist, das der Empfänger ebenfalls PayPal-Kunde sein (oder werden) muss. Ebenfalls zu erwähnen sind eine notwendige Kreditkarte und die hohen Kosten bei einer „Geldabhebung“. Außerdem läuft derzeit ein Verfahren in den USA gegen dieses System, wobei die nötige Banklizenz Hauptstreitpunkt ist. [MB03]

3.3 Vergleich derzeitig angewandter Produkte

3.3.1 Bezüglich Vertrauenswürdigkeit bei den Endbenutzer

Das vertrauenswürdigste Bezahlverfahren ist die Bezahlung per Rechnung. Der Kunde bezahlt grundsätzlich nur für Produkte, die er auf alle Fälle erworben hat und das erst, nachdem er sie bekommen hat.[UK02] Dies hat auch eine Studie der Universität Karlsruhe gezeigt, welche in der Abbildung 3.4 dargestellt ist.

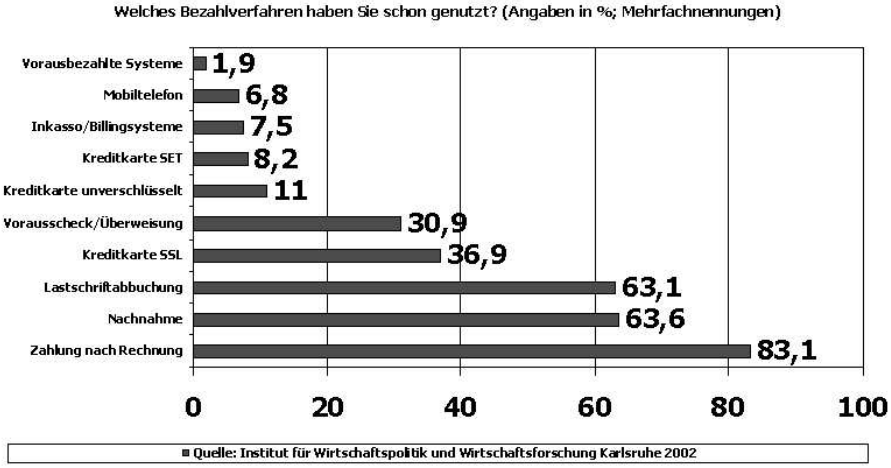

Abbildung 3.4: Akzeptanz aktueller Paymentsysteme [HM03]

In dieser Studie wird aber auch deutlich, dass vor allem traditionelle Verfahren wie die Nachnahme und die Lastschriftabbuchung immer noch am Beliebtesten sind, und von den Käufern am Häufigsten genutzt werden. Außerdem ist auch ersichtbar, dass die Kreditkarte durch die Verschlüsselungstechnik SSL zunehmend an Bedeutung gewinnt. Geldkarten, Scratchcards, elektronische Schecks und digitales Bargeld hingegen haben kaum Relevanz bei den Endbenutzern, teils aus Gründen der Unbekanntheit bzw. nicht flächendeckenden

Verbreitung, teils aus Gründen des Misstrauens. Letzteres trifft besonders bei digitalem Bargeld zu.

3.3.2 Bezüglich Sicherheit, Overhead und Kosten

3.3.2.1 Aus Anbietersicht

Die sichersten Systeme aus Verkäufersicht sind alle Systeme, die dem Händler eine vollständige Zahlungsgarantie einräumen. Das ist allerdings nur bei den im voraus bezahlten Verfahren möglich, sowie bei einer Hinzuziehung eines Treuhänders. Somit sind alle Prepaid- Verfahren für Verkäufer am sichersten. Bezahlung auf Rechnungen hingegen wird bei vielen Online-Shops nur äußerst ungern verwendet, da sie für den Händler mit gewissen Risiken/Nachteilen wie Vorleistung, Eingangskontrolle und Mahnwesen verbunden ist. Wenn es verwendet wird, dann meist nur um auf die Wünsche der Kunden einzugehen. [UK02] Die Kosten der Zahlungssysteme variieren dabei sehr stark. So sind die Installationsgebühren, die monatlichen Grundgebühren und die Transaktionskosten von System zu System deutlich unterschiedlich (selbst innerhalb eines Paymentsystemverfahrens), wobei nur die Transaktionskosten zumindest einigermaßen ähnlich hoch sind.[DU03] So ist das Scratchcard-Verfahren Paysafecard sehr teuer für den Anbieter, da er eine einmalige Summe in Höhe von 1000 Euro für die Anbindung zahlen muss, sowie monatlich 500 Euro für die Grundgebühr. Die Transaktionskosten sind bei diesem Verfahren volumenabhängig.[UK02] Im Vergleich hierzu ist selbst die Rechnung trotz möglichen Zahlungsausfällen doch die wahrscheinlich günstigere Variante. Der Treuhänder kann im Vergleich zu einer einfachen Rechnung deutlich billiger sein, wenn häufig damit zu rechnen ist, dass nicht bezahlt wird. Hat man allerdings zahlungskräftige Endverbraucher, die stets ihre Rechnungen bezahlen, so kann die Rechnung die kostengünstigere Variante sein. Grundsätzlich kann man sagen, dass es keine Musterlösung von Verfahren im Bezug auf die Kosten gibt. Es ist vielmehr von dem Einsatzgebiet abhängig und dies sollte im Vorfeld eingehend erläutert werden. Ferner ist der direkte Vergleich dieser Verfahren sehr schwierig, da keine dieser Lösungen in einer Reinform auftritt, sondern meistens mit zahlreichen anderen Paymentsystemen kombiniert als Softwarepaket käuflich zu erwerben ist. Der größte Verwaltungsoverhead entsteht bei Einsatz von Treuhändern, Rechnungen und digitalem Bargeld.

3.3.2.2 Aus Käufersicht

Die sichersten Systeme aus Sicht der Käufer sind Bestellungen per Nachnahme oder Rechnung, also nach Erhalt der Ware. Diese wird aber dadurch oft sehr teuer, gerade wenn es sich um sehr billige Artikel handelt, im Bereich 50 Euro und weniger. Aber entgegen der Annahme, dass das Zahlen im Internet zu unsicher ist, erfüllen vor allem die Zahlungssysteme im Micropayment-Sector ein ausreichend bis hohes Maß an Sicherheit. Zusätzlich haben die Nutzer in der Regel eine Stornierungsmöglichkeit bei Schadensfällen [DU03] Auch aus Käufersicht gilt, dass es keine Musterlösung für die Kosten bzw. die Sicherheit gibt. So muss man abwägen, wie hoch die Transaktion sein wird, und wieviel man bereit ist

für die Sicherheit zu bezahlen. Sicherheit und Kosten stehen also indirekt proportional in Verbindung. Allerdings ist erwähnenswert, dass durch die nötige Anschaffung eines Geldkartenleseautomaten (zu heutigen Preisen)für Geldkrten diesein ihrem Fortschritt stark gebremst werden.

3.4 Vergleich derzeit noch nicht angewandter/marktreifer Lösungen

3.4.1 Bezüglich Vertrauenswürdigkeit bei den Endbenutzer

Vor allem das Lotterieverfahren wird hier die größten Probleme haben. Erstens ist eine sehr hohe Anzahl der Benutzer nötig, um eine gerechte Verteilung zu gewährleisten und zweitens wird es sehr schwierig sein, die Bevölkerung davon zu überzeugen, das dieses System eine Zuvielbezahlung im Allgemeinen ausschließt. Grund hierfür ist, dass ein Großteil der Nutzer nicht den höchsten Bildungsstand hat und von Wahrscheinlichkeitsrechnungen noch nie etwas oder nur sehr wenig davon gehört hat. Im Vergleich dazu haben mPayment-Systeme denn Vorteil, dass sie auf Lösungen aufbauen, die das Vertrauen der Kunden schon gewonnen haben. Gleiches versucht auch eGold, da es auch hier schon Vertrauen (auf Gold) im Vorfeld gibt. So verliert Gold im Gegensatz zu Sorten und Devisen nie an Wert. Allerdings ist das Verfahren äußerst Suspekt für Kunden, die noch nie damit zu tun hatten. Somit ist für eGold ebenso wie für die Bezahlung mittels eMail noch viel Aufklärungsarbeit notwendig, um wirklich den Durchbruch zu schaffen.

3.4.2 Bezüglich Sicherheit, Overhead und Kosten

3.4.2.1 Aus Anbietersicht

Grundsätzlich ist das Lotterie-System für Anbieter sicher, solange gewährleistet ist, dass alle bezahlen. Die mPayment-Lösungen, bei denen der Telefonbetreiber das Inkasso vornimmt, sind aus Händlersicht die sichersten Verfahren. Die Sicherheit bei der Bezahlung per eMail und/ oder mittels eGold hängt immer vom jeweiligen Anbieter ab, ob dieser vertrauenswürdig ist oder nicht. Bezüglich der Kosten kann man allgemein noch nicht sehr viel sagen, da es sich ja um noch nicht marktreife Verfahren handelt, bei denen unterschiedliche Systeme des gleichen Verfahrens auch deutlich unterschiedliche Preise verlangen. So geht z. B. bei mPayment-Lösungen die Spanne weit auseinander, da einige Anbieter den Dienst kostenlos zur Verfügung stellen, andere wiederum berechnen Grundgebühren hierfür. Ferner gibt es sogar in den gleichen Systemen der gleichen Verfahren Unterschiede. So kostet ein reiner PayPal-Account dem Händler nichts, wohingegen der gleiche Shop mit der Zusatzfunktion „Kreditkartenakzeptanz“ ein Disagio von 2,7% bzw. 3,4% berechnet wird, plus zusätzlich 0,35 Euro Transaktionskosten. [LC1]

3.4.2.2 Aus Käufersicht

Die Sicherheit für Kunden bei all diesen Varianten ist bislang nur bei mPayment gegeben. So kann das Lotterieverfahren zwar stochastisch grundsätzlich richtig sein, es funktioniert allerdings nur bei einer sehr hohen Anzahl an Teilnehmern. Zusätzlich kann es durch „schwarze Schafe“ sehr leicht gefälscht werden, indem man einfach die Gewinnwahrscheinlichkeit erhöht. Auch das Verfahren mittels eMail ist noch nicht fälschungssicher und hat zudem auch die Probleme, dass hier auch noch Kreditkarten verwendet werden, mit all ihren Risikofaktoren. Ferner ist auch das eGold-System prinzipiell nicht sicher, da es auch hier durch Gauner möglich ist, nie den Gegenwert in Gold wirklich bereitzustellen. Die Kosten sind für den Käufer bei allen ziehmlich niedrig, wobei allerdings manchmal Anwendungen dabei sind, die extrem teuer sind. So gibt es bei PayPal zwar keine Kontoführungsgebühren bei einer Überweisung, jedoch werden diese bei Ein- und Auszahlungen berechnet. Hier fallen sehr hohe Kosten an. Gleiches gilt bei einer Einzahlung in das eGold-Konto, da hier jedesmal Kreditkartengebühren fällig sind [HJ03]. Und auch bei dem Lotterieverfahren kann es sehr schnell teuer werden, wenn man Pech hat und häufig „gewinnt“. Wie bei den Verkäufern gilt auch bei den Anwendern, dass die Spanne bei mPayment-Lösungen weit auseinander geht.

3.5 Was geschieht auf EU-Ebene?

3.5.1 Gründe für die europäische Relevanz

Es gibt zahlreiche Gründe, wieso sich die EU an Paymentsystemen interessiert. Als allererstes möchte man eine solide Ausgangsbasis aufbauen. „Ziel der EU ist es, einen immer engeren Zusammenschluss der europäischen Staaten und Völker zu schaffen, um die den wirtschaftlichen und sozialen Fortschritt zu sichern“[EU00]. Wie man in Abbildung 3.5 sehen kann, sind heutzutage jedoch eine sehr große Anzahl unterschiedlichster Paymentsysteme im Einsatz. Bei vielen Entwicklungen waren regionale Aspekte, wie z.b. dem Kaufverhalten in den einzelnen EU- Ländern oder die Handy-Dichte des einzelnen Landes, entscheidend bzw. beeinflussend. So sind heutzutage manche Lösungen in gewissen Ländern sehr wichtig, wohingegen sie in anderen Ländern kaum genutzt werden.[BK01]
Ein weiterer Punkt hat symbolischen Charakter. So möchte man nach der Währungsunion 2002 nun auch bei den elektrischen Zahlungssystemen eine europaweite Vereinheitlichung erreichen.
Der dritte Punkt ist auch eine Vereinheitlichung der Rechtsgrundlagen. So heißt es in der Richtlinie 2000/31 des europäischen Parlaments wortwörtlich: „Die Weiterentwicklung der Dienste der Informationsgesellschaft in der Gemeinschaft wird durch eine Reihe von Hemmnissen für das reibungslose Funktionieren des Binnenmarktes behindert, die die Ausübung der Niederlassungsfreiheit und des freien Dienstleistungsverkehrs weniger attraktiv machen. Die Hemmnisse bestehen in Unterschieden der innerstaatlichen Rechtsvorschriften sowie in der Rechtsunsicherheit hinsichtlich der auf Dienste der Informationsgesellschaft jeweils anzuwendenden nationalen Regelungen. Solange die innerstaatlichen Rechtsvorschriften in den betreffenden Bereichen nicht koordiniert und angepaßt sind,

Electronic Internet-Payment Methods in the European Union / June 2001				
	Type		Brand/solutions	
Access products	Credit transfers		electronic giro [SF], *fun [DE]	Solo e-payment [SF]
	Electronic checks			
	Debit card payments		Bezahlen.at [AU, *DE], BACS [UK] [CyberCash] [DE], CyberCOMM [F], Dankort PBS [DK], I-Pay [NL]	Leonia [SF], Maestro pilot [AU], Switch [UK], Virtual Cash [ES], Visa debit [UK]
Credit card payments			SET, 3D-SET [AU,BE, DE, I, DK, F, IRE, NL, ES] SET facil [ES], SET light [AU, I]	Banxsafe [BE], Clikpay [IRE], CyberCOMM [F], I-Pay[NL], Telepay light [I]
Virtual e-wallet/accounts			[Barclaycoin] [UK], [CyberCash] [DE], Earthport [UK], [Klebox/K-wallet] [F, SE], Mover card [I]	Nochex [UK], [*Odysseo] [F], PayHound [UK], Safedoor [UK], Smart Creds [UK]
Prepaid products	Single purpose		WebCard [AU]	
	E-money 2000/46/EC	Smart card based	Avant [SF], *Danmont [DK], *Cash [SE], Chipknip/[Chipper] [NL], GeldKarte [DE], Euro 6000 [ES], MiniPay/PayOnWeb [I], *Mondex [F], [Mondex] [UK],	Monedero 4B [ES], *Moneo [F], Quick [AU], *PayCard [DE], Porta Moedas Multibanco [P], Proton [BE], [SmartAxis] [UK], VisaCash [ES, *UK]
		Software wallet	[Clickpay] [DK], CopyLock (p) [UK] [eCash] [AU, DE, SF]	Magex (p) [UK], [MoneyPenny] [SF]
	Prepaid dedicated accounts		*Cartafacile[I], *Commerzbank virtual card [DE], Cybertarjeta [ES], *Kalibra [I], *WebC@rd [DK], *MicroMoney [DE], MoneraOnline [I]	Nexgo Kleingeldbörse [DE], OmniPay card [I], Paysafecard [AU, DE], [Roots] [UK], Virtual cash plus [ES], Smart Creds [UK] SplashPlastic [UK]
Money surrogates			[Beenz][F, UK], bonus.net [DE], IncentivCash[UK], I-Points[UK], Maximiles[F]	MyPoints [UK] Payback [DE], webmiles [DE], Zakis [ES]
(Micro)Billing			0900 Interconnect [NL], [BT Array] [UK], Chargeitdigital [UK] Firstgate click&buy [DE], Infin Micropayments [DE], Kiosque [F]	Net900 [DE], NET 900 Kontopass [DE], Post/Torget[SE], Qpass [ES], switchpoint [NL], X-Press-Pay [DE]
Mobile Payment Systems			banko.max [AU], Banxsafe [BE], EasyBuy [I], EMPS (p) [SF, I, SE], *Genion M-Payment [DE], GiSMo [SE,UK], *iCash SE], *Mint [SE], *Mobilbank (p) [DE], [Mobilix] [DK], Movilpago [ES], Omnipay Onphone [I], Orange Mobile Payment [DK]	Pagomobile [I], Paiement CB sur mobile [F], Paybox [AU, DE, SE, ES], *Payitmobil [DE], Payline 300 [F], Phonepaid [UK] Sonera Mobile Pay (p) [SF], * Sonofon [DK], Streetcash [DE], Telia Pavit (p) [SE], Visamóvil [ES]

Legend: [ ] contains country code, [scheme] = scheme discontinued; * announcement.

Abbildung 3.5: ePayment-Systeme in der EU
[BK01]

können diese Hemmnisse gemäß der Rechtsprechung des Gerichtshofes der Europäischen Gemeinschaften gerechtfertigt sein. Rechtsunsicherheit besteht im Hinblick darauf, in welchem Ausmaß die Mitgliedstaaten über Dienste aus einem anderen Mitgliedstaat Kontrolle ausüben dürfen.“[EU00]

3.5.2 Hauptprobleme, die geregelt werden müssen

Eines der Hauptprobleme in der EU ist die Frage „Wer darf elektronisches Geld emitieren?“, aber auch die Bestrafung bei Missbrauch von elektronischem Geld, sowie die Bekämpfung von Betrug sind Brennpunkte, die geregelt werden müssen. Auch die Anerkennung einer elektronischen Rechnung, die Regelung des Patentrechtes und die der Wettbewerbspolitik sind dringend nötig. Ferner war auch die Regelung des Gerichtsstandes notwendig, wobei die EU mit der Richtlinie über den elektronischen Geschäftsverkehr eine erste Harmonisierung vorgenommen hat. Es gilt nun das „Herkunftslandprinzip“, wobei hier wiederum zahlreiche Ausnahmen zutreffen, in denen wiederum die Vorschriften der einzelnen Staaten beachtet werden müssen. Aber auch europaweit geltende Regelungen wie zum Beispiel das Verbraucherschutzgesetz mit ihrer Regelung über „Konsumentengeschäfte“ führen zu solchen Ausnahmen.(vgl. hierzu [BB03],[EU00], [PT98])

3.5.3 Fazit

Wie man deutlich erkennen kann, sind die heutzutage verbreiteten und genutzten Paymentsysteme eigentlich keine Neuerfindungen sondern nur Weiterentwicklungen und Abbildungen von herkömmlichen Zahlungsweisen. Dabei ist auch offensichtlich, das momentane Software-Lösungen von Paymentsystemen für Onlineshops nicht nur eine, sondern eine Vielzahl von Paymentmöglichkeiten anbieten. Hier versucht man offenbar, die Individualität der einzelnen Nutzer (mit seinen jeweiligen Ängsten und Vorlieben) zu berücksichtigen. Das erfolgsversprechendste neu entwickelte Payment-System ist wohl das mPayment, da hier schon auf Vertrauen der einzelnen Telefongesellschaften aufgebaut wird. Zusätzlich kann man auch sagen, dass der mCommerce wahrscheinlich die unterschiedlichsten Geschäftsmodelle hervorbringen wird, wobei sich einige durchsetzen können und andere wiederum nicht. Es ist allerdings fraglich, ob sich ein einheitliches Zahlungssystem weltweit (oder zumindest europaweit) jemals durchsetzen werden kann. Aber die Zukunft wird es zeigen...

Literaturverzeichnis

[KlSp98] Fritz Klein, Klaus Spremann, „Telegeld“, Verlag Neue Züricher Zeitung, Zürich, 1998, ISBN 3-85823-736-1

[SFE97] Rolf Schuster, Johannes Färber, Markus Eberl, „Digital Cash- Zahlungssysteme im Internet“, Springer-Verlag, Berlin, 1997, ISBN 3-540-61981-X

[TV00] Tobias Vetter, „Die Geschichte des Internets“, 25. August 2000 , http://www.phil-fak.uni-duesseldorf.de/mmedia/web/index6.html

[RZ03] Robert H. Zakon, „Hobbes' Internet Timeline v7.0“, 2003, http://www.zakon.org/robert/internet/timeline/

[UK02] “Zahlungssysteme im Internet – eine Übersicht“, 2002, http://www.iww.uni-karlsruhe.de/IZV5/Zahlungssysteme.pdf

[UK0102] “Ausgewälte Ergebnisse der Online-Umfrage IZV5“, 2002, http://www.iww.uni-karlsruhe.de/IZV5/IZV5Ergebnisse.pdf

[JH01] Joachim Henkel, „Anforderungen an Zahlungsverfahren im E-commerce“, April 2001, http://www.inno-tec.bwl.uni-muenchen.de/forschung/henkel/Anf_E-Paym_JH.pdf

[HM03] Mike Hieronimus/ Fadi Mohsen, “e-f@cts Informationen zum E-Business“, April 2003, http://www.bmwi.de/Redaktion/Inhalte/Downloads/br-doku1363-zahlungsverkehr-im-internet.pdf,property=pdf.pdf

[RS00] Raimund Specht, „E-Commerce- Homebanking und der HBCI-Standard“, 14. Februar 2000, http://www.spemaus.de/studium/ecommerce/ausarbeitung.xhtml

[TSMS98] Thomas Schöpf/ Martin Stumpf, „Zahlungssysteme im Internet“, 11.02.98, http://www11.informatik.tu-muenchen.de/lehre/seminare/seminarWS9798/schoepf/

[IS00] „eCommerce-Disadvantages Of Tradition Business Applications“, 2000, http://www.isos.com.my/ecommerce/disadvantages.htm

[TJM99] „e-commerce disadvantages“, 1999, http://hamp.hampshire.edu/~tjm99/disadvantages.html

[03] "E-Commerce" ,2003, http://www.3-dreams.com/projects/luciddomains/e-commerce.html

[MK02] Malte Krüger,"Grenzüberschreitendes Bezahlen im gemeinsamen Markt des mobilen Europas", 20. Juni 2002, http://www.telematik-institut.org/trierer_symposien/digitales_geld/vortrage/m-payments_trier_krueger.pdf

[CK02] Carsten Kröhl, „Mobile Payment Systeme am Beispiel der paybox.net AG", 03. Juni 2002, http://www.hausarbeiten.de/rd/faecher/vorschau/5380.html

[PT98] Dr.Peter Troberg, „Elektronische Zahlungssysteme: Was geschieht auf EG-Ebene ?", Juni 1998, http://www.itas.fzk.de/deu/tadn/tadn298/trob298a.htm

[JM97] Dr.Jochen Musch, „Die Geschichte des Netzes: ein historischer Abriß", 1997, http://www.psychologie.uni-bonn.de/sozial/staff/musch/history.htm#11

[YB03] Yingcheng Bi, „Informationssysteme im elektronischen Handel",Juni 2003, http://www.ipd.uka.de/~oosem/ ISEC03/ausarbeitung/YingchengBi.pdf

[VG01] Volker Gieritz, „Neue Architektur für Internet-Payment", 12.Januar 2001, http://www.ebanker.de/texte/94.asp

[PL03] Paul Lang, „Tenfold-Ten ways to accept payment in your Web store",2003 http://www.sellitontheweb.com/ezine/tentips007.shtml

[MZ02] Manuel Zieger, „Die elektronische Zahlung - Angebot, Nutzung und Wertschöpfung", 2002, http://www.hausarbeiten.de/rd/faecher/hausarbeit/bwi/22851.html

[PK16] Petra Kursawe, „Bevorzugte Zahlmethoden im Web", 16.März 2001, http://www.ebanker.de/texte/174.asp

[PK17] Petra Kursawe, „Kinderkrankheiten beim Mobile Payment", 17.Mai 2001, http://www.ebanker.de/texte/244.asp

[PK29] Petra Kursawe, „Krieg der Payment-Systeme", 29.Mai 2001, http://www.ebanker.de/texte/257.asp

[X01] "Jur-Report 02/2001", Februar 2001, http://www.it-sicherheitsmanagement.de/jurrepeort/022001.htm

[DU03] Dannenberg/Ulrich, "Paid Content: Kleines Geld - große Geschäfte", Mai 2003, http://www.competence-site.de/ecommerceshop.nsf/53E650FCD47A7670C1256D2D004C7B6D/$File/paid%20content_kleines%20geld_große%20geschäfte_052003.pdf

[NP03] Nicola Popoff, "Zahlungsdrehscheibe für Hutchinson 3G Austria Kunden", 07. Juli 2003, http://www.de.atosorigin.com/news/2003/AOAustria-Hutchison3.php

[PL02] P.Luther, „Analyse und Einsatzmöglichkeiten mobiler TK-Endgeräte als technische Zahlungsbasis im Rahmen des M-Commerce“, Juli 2002 http://www.diplomica.com/db/diplomarbeiten6554.html

[BB03] Birgit Baumgartner, „E-Business: Rechtliche Rahmenbedingungen in der EU und in der Schweiz“, September 2003, http://www.osec.ch/osec/eics/e-business/broschuere_de.pdf

[FL01S] Frank Legler, „Grundlagen elektronischer Bezahlsysteme“, 2001, http://www.informatik.hu-berlin.de/Institut/struktur/algorithmenII/Lehre/WS2001-2002/Bezahlsysteme/04GrundlBezahl/GrundlBezahl.pdf

[FL01] Frank Legler, „Grundlagen elektronischer Bezahlsysteme“, 2001, http://www.informatik.hu-berlin.de/~legler/studium/seminare/ebs/eBS.pdf

[RL01] Remus Lazar, „Micro-Payment Ssysteme“, 2001, http://www.informatik.uni-stuttgart.de/ipvr/vs/lehre/ss01/Seminare/Hauptseminar/material/A_Micropayments.pdf

[MM99] Dr. Michael Möhring, „Elektronisches Geld und Internet-Zahlungssysteme“, Februar 1999, http://www.uni-koblenz.de/~moeh/publik/egiz.html

[MK0102] Markus Klietmann, „Mobile Payment- Verfahren im Vergleich“, 03.01.2002, http://www.ecin.de/zahlungssysteme/mobilepayment/print.html

[BK01] Knud Böhle/Malte Krüger, „Payment Culture Matters“, August 2001, http://epso.jrc.es/Docs/Backgrnd-4.pdf

[EU00] “RICHTLINIE 2000/31/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES“, 08. Juni 2000, http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_de.pdf

[MB01] Matthias Brüstle, „Virtuelles Geld-elektronisches Geld, ePayment im Vergleich“, 2001, http://www.franken.de/de/veranstaltungen/kongress/2001/epayment.pdf

[MB03] M. Birkelbach, “Benutzergerechte Bezahl- u. Einkaufssysteme“, 15. Mai 2003, http://www.emr-sb.de/news/20031505Birkelbach.pdf

[LC1] Leinert Consult, „PayPal – Bezahlung per Email“, http://www.leinert.com/paypal/

[LC2] Leinert Consult, „Payment Glossar, Payment ABC bzw. Paymenlexikon“, http://www.leinert.com/paymentbegriffe/index.htm

[TU02] TU Dresden, "Computer Integrated Business (CIB)", 2002, http://www.tu-dresden.de/wwwiisih/ftp/cib/ws02/Skript-030623.pdf

[IB97] "Elektronisches Geld:Potentiale, Kritik und Sicherheitsprobleme",1997, http://www.wiwi.uni-frankfurt.de/~guth/Lehre/Diplomarbeiten/download/D4.pdf

[HJ03] "Wie eröffne ich ein eGold-Konto", 2003, http://www.heimjob24.com/egold.htm

Kapitel 4

Bepreisung von Peer-to-Peer-Systemen

Stephan Lukas

Peer-to-Peer-Netzwerke haben sich als eine sehr vielversprechende Möglichkeit ergeben, um Dateien zu tauschen oder Ressourcen zu teilen. Dies erfolgte bisher alles ohne kommerziellen Hintergrund und erforderte auf Seiten der Anwender ein großes Maß an Zusammenarbeit um diese Netzwerke effektiv zu betreiben bzw. überhaupt aufrecht zu erhalten.

Diese Ausarbeitung beschäftigt sich mit den Problemen heutiger Peer-to-Peer-Systeme, die sich größtenteils in einer mangelnden konstruktiven Beteiligung der Mehrheit der Nutzer solcher Systeme wiederspiegeln. Bei näherer Betrachtung dieser unkooperativen Verhaltensmuster, sind diese meist darauf zurückzuführen, dass kein direkter Nutzen aus Kooperation und auf der anderen Seite keine effektive Bestrafung von Unkooperation existiert bzw. praktiziert wird. Da unter mangelnder Beteiligung der Mehrzahl der Nutzer die Gesamtperformance des Systems leidet, betrachtet diese Ausarbeitung mögliche Lösungsansätze um Peer-to-Peer-Dienste zu bepreisen bzw. Motivationen für eine sinnvolle Zusammenarbeit zu schaffen.

Inhaltsangabe

4.1 Einführung

Peer-to-Peer-Netzwerke haben in den letzten Jahren stark an Bedeutung gewonnen. Mit dem Aufkommen der mp3-Technologie und dem daraus entstehenden Hype jegliche Arten von Musikdateien in Unmengen über das Internet zu tauschen, profitierten Peer-to-Peer-Systeme von dem großen Zulauf begeisterter Musikliebhaber. In der Anonymität eines solchen Netzes wurde es möglich, diese sich am Rande der Legalität befindenden Tauschaktivitäten mit einem ruhigen Gewissen zu vollziehen. Gegenmaßnahmen der Musikindustrie, die starke Verluste bei ihren Einnahmen hinnehmen musste, wie geringe Lizenzgebühren für jeden Download zu verlangen, schlugen beispielsweise bei Napster fehl. Es wurden immer wieder neue Möglichkeiten gefunden diese Lizenzgebühren zu umgehen. Als Konsequenz daraus wurde Napster vorübergehend stillgelegt. Trotz allem, und nicht zuletzt auch wegen neu entwickelten Videoformaten, erfreuen sich Peer-to-Peer-Netze wachsender Beliebtheit und können immer größer werdende Benutzerzahlen vorweisen. Allerdings geht dadurch der grundlegende Tauschcharakter der Peer-to-Peer-Systeme verloren. Nicht wegen der großen Anzahl der Nutzer, dies ist durchaus positiv für solche Netze, sondern durch immer häufiger zu beobachtenden Verhaltensmuster vieler User. Es wird von der Mehrzahl nicht getauscht, sondern einfach nur genutzt, d.h. Dateien werden zwar heruntergeladen, aber im Gegenzug keine Leistung an das Netz erbracht.

Im Gegensatz zur herkömmlichen Client-Server-Interaktion des Internets, können und müssen die User in einem Peer-to-Peer-System sowohl die eine als auch die andere Aufgabe übernehmen, um das Netzwerk am Leben zu halten. Dabei ist ein oft zu beobachtendes passives Client-Verhaltensmuster, wobei nur Leistungen erhalten werden, völlig destruktiv innerhalb eines Peer-to-Peer-Netzes.

4.1.1 Risikogruppe: Anwender

Eine große Zahl an Dateien freigebenden und kooperativen Usern ist der Grundpfeiler eines jeden gut funktionierenden P2P-Systems. Allerdings können die Anwender auch der größte Störfaktor bzw. die schlimmste Leistungsbremse sein.

Ein Großteil der heute existierenden Forschungsarbeiten auf dem Gebiet der P2P-Systeme beschäftigt sich allein mit der Entwicklung und Verbesserung von Protokollen, außer acht lassend, dass in der Anonymität eines P2P-Netzes sich in der Mehrzahl rationale Anwender befinden. Aufgrund dieser einseitigen Forschung existieren kaum Kontrollstrukturen, die es ermöglichen, die verschiedensten Verhaltensweisen der riesigen Zahl an Anwendern differenziert zu beurteilen, noch gibt es angemessene Sanktionsmechanismen um die Mehrheit der Benutzer zur konstruktiven Zusammenarbeit zu motivieren.

Rationale Anwender folgen, sofern sie die Möglichkeit dazu haben, nicht blindlings vorgegebenen Protokollen. Sie werden immer bemüht sein, ihren eigenen Nutzen zu maximieren. So hat man in den jetzigen Peer-to-Peer Netzen keinen direkten Nutzen davon, Dateien freizugeben, noch ist es sonderlich Vorteilhaft die Anfragen anderer Anwender weiterzuleiten. Durch die Abwesenheit entsprechender Sanktionen oder Motivationsmaßnamen innerhalb der P2P-Netze wird dieses Verhalten stark begünstigt.

Die vorliegende Ausarbeitung hat zum Ziel, bekannte Theorien und Mechanismen zur Erschaffung geeigneter Kontroll- und Motivationsmaßnamen vorzustellen, bzw. deren Grundlagen näher zu beleuchten. Bevor dies geschehen kann, sollte ein genauerer Blick auf die Anwender selbst geworfen werden. Dabei ist besonders zu betrachten, welche Arten von Anwendern in P2P-Systemen zu finden sind, welche Verhaltensweisen man antreffen kann und welche Folgen sich daraus ergeben.

4.1.2 Anwender und deren Verhalten

Innerhalb eines Peer-to-Peer-Netzwerkes kann man zwischen drei grundlegenden Arten von Anwendern unterscheiden [1, S. 6]:

Altruistische/selbstlose Anwender folgen, wenn immer möglich, dem vorgegebenen Protokoll und nehmen dafür auch Nachteile für sich selbst in Kauf. Ein Computerabsturz wäre beispielsweise einer der wenigen Gründe, warum ein selbstloser Anwender einem Protokoll nicht folgt. Diese Art von Anwender ist eher selten anzutreffen und bildet die löbliche Ausnahme in P2P-Netzwerken.

Rationale Anwender sind die wohl am häufigsten anzutreffende Gruppe in P2P-Systemen. Sie verfolgen eine Strategie, abhängig von den zugrunde liegenden Regeln des jeweiligen Peer-to-Peer-Netzes, um ihren eigenen Nutzen zu maximieren. Diese Strategie kann zur Folge haben, dass die allgemeine Performance des gesamten Netzes leidet. Zu dieser Gruppe zählen auch die so genannten Free-Rider. Dieser Begriff fällt meist im Zusammenhang mit Nutzern, die nur vom P2P-Netz profitieren, ohne selbst jegliche Leistungen an das Netz zu erbringen.

Irrationale/böswillige Anwender sind eher selten anzutreffen. Sie verfolgen keine Strategien bei ihren Interaktionen im Netzwerk. Ihre Handlungen sind völlig willkürlich, also weder vorhersehbar, noch nachvollziehbar, da sie selbst Verluste oder Schäden für sich selbst in Kauf nehmen.

Es wäre wünschenswert, wenn man die letzten beiden Anwendergruppen, besser kontrollieren könnte, um in der Lage zu sein vorausschauender Netzwerkprotokolle zu entwickeln. Allerdings ist es auch einleuchtend, dass die dritte Gruppe schwer fassbar ist. Es ist unmöglich, jemanden zu beeinflussen, dessen Interessen und Verhaltensmuster nicht vorhersehbar sind. Verwalter eines Peer-to-Peer-Systems haben hier nur die Möglichkeit, falls ein solches Verhalten erkannt wurde, denjenigen Nutzer aus dem Netz auszuschließen.

Solche harten Sanktionen sind nicht unbedingt der beste Weg um mit der zweiten Gruppe von Anwendern, den rational handelnden, umzugehen. Schließlich sollte zumindest teilweise für jeden diese Art des Verhaltens nachvollziehbar sein. Desweiteren ist diese Gruppe durchaus in ihren Interaktionen beeinflussbar und kann so, unter den richtigen Voraussetzungen, nützlich für den Gesamtbetrieb des Netzes gemacht werden. Wie diese sinnvolle Motivation aussehen kann, wird später ausführlich erläutert.

4.1.2.1 Unkooperatives Verhalten

Es gibt verschiedene Arten unkooperativen Verhaltens seitens der Anwender, die in Peer-to-Peer-System auftreten können und schädlich für den Netzbetrieb sind. Dessen sollte man sich bewusst sein, bevor man Gegenmaßnahmen dazu betrachtet.

Abbildung 4.1: Unkooperatives Verhalten [2, S. 15]

Wie man aus der Abbildung 2.1 entnehmen kann, ist unkooperatives Verhalten in verschiedene Gruppen unterteilbar:

1. **Entschuldbare Nichtkooperation** als begründetes Fehlverhalten, beispielsweise in Folge eines Systemabsturzes
2. **Fehlverhalten** als unbegründedete Nichtkooperation
   (a) **Böswilliges Fehlverhalten** muss für den jeweiligen Anwender selbst nicht unbedingt rentabel sein. Er nimmt hier Nachteile für sich selbst in Kauf mit dem Ziel, dem Peer-to-Peer-System zu schaden oder aus anderen nicht nachvollziehbaren Gründen. Die Gruppe der irrationalen Anwender verhalten sich in der Regel so.
   (b) **Rentables Fehlverhalten** hiervon verspricht sich der User grundsätzlich einen Vorteil für sich selbst. Dieser Verhalten trifft auf die Gruppe der Rationalen Anwender zu.
      i. **Eigennütziges Verhalten** z.B. Das Nichterbringen eines Services.
      ii. **Freigiebiges Verhalten** z.B. Vergeben von ungerechtfertigt hohen Bewertungen mit dem Hintergedanken, selbst besser bewertet zu werden (Bewertungen werden im weiteren Verlauf besprochen)

4.1.3 Probleme unkooperativen Verhaltens

Ein unkooperatives Verhalten, wie es oben geschildert wurde, hat negative Auswirkungen auf die Gesamtperformance eines Peer-to-Peer-Systems.

- Zum einen kann es zur Überlastung einiger einzelner Peers kommen, so genannten Hotspots. Sind die Systemressourcen ungleichmäßig verteilt, indem z.B. nur auf einzelnen Rechnern ein umfangreiches Angebot an Dateien freigegeben ist, werden diese Rechner verständlicherweise überdurchschnittlich oft angesprochen. Das führt unter ungünstigen Umständen sehr schnell zur Aus- und Überlastung dieser Rechner.

- Zum anderen basieren viele Protokolle, z.B. zur Weiterleitung von Anfragen, auf die Zusammenarbeit aller Anwender. Je mehr sich hier daran beteiligen, um so schneller wird der Vorgang und um so größer ist die Aussicht auf Erfolg. Das bedeutet natürlich auch im Umkehrschluss, dass bei einem geringen Maß an Kooperation das P2P-Netz weit hinter seinen Möglichkeiten zurückbleibt und dadurch sozusagen ausgebremst wird.

Um die Auswirkungen unkooperativen Verhaltens besser Beurteilen zu können und als Folge daraus, Gegenmaßnahmen zu entwickeln, ist es nötig weitere Grundlagen zu betrachten. Dazu gehören der Aufbau und die Funktionsweise heutiger Peer-to-Peer-Systeme, sowie die nötigen Voraussetzungen, um Anwender zur Kooperation zu Motivieren.

4.2 Grundlagen für Pricing-Mechanismen

Pricing-Mechanismen sollen die Aufgabe haben innerhalb von Peer-to-Peer-Netzen Anreize zur Kooperation zu schaffen. Die Ansätze um diese Anreize zu entwickeln können völlig unterschiedlich sein. Grundsätzlich werden intrinsische und extrinsische Motivationen geschaffen um die Zusammenarbeit zu steigern.

Um diese Pricing-Mechanismen entwickeln zu können, bzw. um sie nachzuvollziehen, ist es unabdingbar vorweg grundlegende Begriffe zu klären. Hierzu gehören der Aufbau und die Funktionsweise von Peer-to-Peer-System, eine genauere Betrachtung des Begriffs Pricing und eine Einführung der Schlagwörter Vertrauen und Reputation. Dieses sind die Grundlagen für die weiteren Betrachtungen.

4.2.1 Begriffsbestimmung Peer-to-Peer-Systeme

4.2.1.1 P2P-Arten

Peer-to-Peer-Netze existieren heute mit vielfältigen Einsatzformen. Die drei wichtigsten, bzw. wohl bekanntesten sind:

Dateiaustausch zum ursprünglich nicht kommerziellen Tauschen jeglicher Art von Dateien innerhalb einer Gruppe Gleichgesinnter.
Bsp.: Napster, Gnutella, Freenet

Verteilte Rechenleistung kann für Großprojekte genutzt werden, deren Rechenaufwand sehr umfangreich ist. Dieses wird dann in kleinere Teilaufgaben unterteilt, die auf verschiedenen Computern berechnet werden.
Bsp.: Seti@home,Genome@home

Verteilte Informationsspeicherung Bsp.: zur Speicherung von Reputationspunkten auf verschiedenen Rechnern

4.2.1.2 Aufbau

Zusätzlich zur Funktion unterscheiden sich P2P-Netze in ihrem möglichen Aufbau, d.h. allerdings nicht, dass P2P-Systeme, die die gleichen Funktionen erfüllen auch den selben Aufbau haben müssen. Folgende Peer-to-Peer-Netze werden unterschieden [5]:

1. **Zentralisiertes P2P-Netz** in diesen Systemen, befindet sich eine spezieller Rechner mit einer zentralen Index-Datenbank. In dieser Datenbank ist verzeichnet, welcher Rechner im gesamten Netz welchen Dienst anbietet.
   Ein Service suchender Peer stellt seine Anfragen an den zentralen Rechner und erhält als Antwort alle Peers die den gesuchten Service anbieten, mit welchen er daraufhin eine direkte Verbindung herstellen kann.
   Bsp.: Napster

2. **Dezentralisiertes unstrukturiertes P2P-Netz** oder auch reines Peer-to-Peer-Netz genannt, ist das heutzutage wohl am meisten genutzte Peer-to-Peer-System. Allerdings ist es auch das mit den größten Problemen, gerade wegen dieser Unstrukturiertheit. Der Großteil der Aussagen dieser Ausarbeitung bezieht sich auf diese Netze.
   Sie kennzeichnet eine verteilte Architektur, in denen es nicht so etwas wie eine zentrale Datenbank gibt. Jeder Peer kann sowohl als Servicebietender (Agent) und Servicesuchender bzw. -empfänger (Principal) agieren. Auf der Suche nach einem entsprechenden Service wird die Anfrage von Peer zu Peer weitergeleitet. Damit sind sie besonders unanfällig für Fehler, wie Ausfälle einzelner Computer, im Gegenzug sind sie eben auch sehr auf Zusammenarbeit angewiesen.
   Bsp.: Gnutella, Freenet, Kazaa

3. **Dezentralisiertes strukturiertes P2P-Netz** ist eine Mischform aus den vorangegangenen Beiden. Besonders leistungsfähige Rechner können hier die Funktion eines Superknotens übernehmen, d.h. sie nehmen erstellen eine Index-Datenbank für einen Teil des Netzes und vereinfachen somit den Zugriff auf diese Inhalte.
   Bsp.: FastTrack, CAN, CHORD

4.2.1.3 Funktionsweise

Die reinen Peer-to-Peer-Netze sind, wie bereits erwähnt, am häufigsten in der Praxis anzutreffen. Zu ihrer Funktion ist Kooperation zwischen den einzelnen Anwendern unabdingbar, das geht allein schon aus dem Suchvorgang hervor. Aber es gibt noch weitere

Hauptfunktionen, einschließlich der Suche, die einem reinen Peer-to-System zugeordnet werden können [3, S. 2]:

Bootstrapping ist unabdingbar, dass Peers am Netzwerk teilnehmen können. Kazaa nutzt dafür beispielsweise GWebCache-Server auf den ein Modul zur Adressfindung läuft.

Suchprozess wird gestartet, indem der initialisierende Servicesuchende eine Anfrage an alle ihm bekannten Peers schickt. Diese können die Anfrage entweder beantworten oder senden sie wiederum an die ihnen bekannten Peers weiter. So verbreitet sich eine Anfrage bei entsprechender Beteiligung schnell im Netzwerk und hatte gute Aussichten auf Erfolg. Diese Anfragen sind meist zusätzlich mit einer TTL, hops oder etwas ähnlichem versehen, nach dessem Ablauf sie verworfen werden.

Download Nachdem der anfragende Peer alle eingehenden Antworten gesammelt hat, kann er sich einen Serviceanbietenden Peer auswählen und mit ihm eine Verbindung über http oder tcp herstellen. Der Download erfolgt über diese Verbindung.

4.2.2 Begriffsbestimmung Pricing

Das Zauberwort in Peer-to-Peer-Netzen ist und bleibt Kooperation. Sie ist unbedingt notwendig um die fehlende Infrastruktur zu kompensieren. Doch wie kann man Kooperation in einem System voller autonomer Anwender erzeugen? Wie bringt man sie dazu effektiv zusammenzuarbeiten? Wie veranlasst man unbeteiligte Anwender dazu, Anfragen zu beantworten oder zumindest weiterzuleiten, um den Netzbetrieb aufrecht zu erhalten, oder besser noch eigene Ressourcen dem System zur Verfügung zu stellen?

Erzwingen kann man dies sicher nicht. Dafür fehlen meist die Autoritären Instanzen, um dies durchzusetzen. Weiterhin mangelt es an Mechanismen, die feststellen, welche Peers in welchem Maße zum Netzbetrieb beitragen, um entsprechende Schlussfolgerungen für etwaige Sanktionen zu treffen.

Ein naheliegender Lösungsansatz wäre hier z.B. der marktwirtschaftliche: Ein Anfragensteller muss für positive Antworten, wie Weiterleitungen und Serviceangebote, zahlen und eben diese weiterleitenden Anwender bzw. Serviceanbieter werden für ihre Leistungen bezahlt (siehe auch den Abschnitt *Pricing in Referral Systems*). Jede Verhaltensweise die dem üblichen Free-Riding entgegenläuft, muss belohnt werden, um diese Ansätze zu unterbinden. Es muss mit Pricing-Mechanismen hierfür die geeignete Motivation geschaffen werden am Betrieb des P2P-Netzes mitzuwirken. Auf die verschiedensten Bedingungen angepasste Motivationsmodelle werden im Abschnitt *Anreizmodelle* erläutert.

Der Begriff des Pricings sollte hierbei nicht allein auf einfaches Bezahlen minimiert werden. Vielmehr ist er Aufzufassen als eine Art der Belohnung besonders aktiver Anwender und indirekter Bestrafung der Free-Rider, da hier eine Belohnung ausbleibt. Diese Belohnung muss als Grundlage dienen, um am Netzbetrieb teilzunehmen oder besonderen Service zu erhalten, damit jeder Anwender bestrebt ist, positive Leistungen an das Netz zu erbringen.

4.2.3 Begriffsbestimmung Vertrauen und Reputation

[4]Ein Punkt, der mit der Einführung des Pricings aufkommt, ist der des Vertrauens. Wie kann man sich sicher sein, dass ein Agent nach der Aushändigung seiner Belohnung auch tatsächlich den gewünschten Service ausführt? Woher weiß man, dass der angebotene Service wirklich gut ist? Wer garantiert, dass eine Anfrage wirklich weitergeleitet wird? Diese und mehr Fragen zeigen auf, dass ein gewisses Maß an Vertrauen innerhalb eines P2P-Systems existieren muss. Diese Vertrauensbasis will aber erst einmal geschaffen werden.

Möglich ist dies durch die Einführung von Bewertungen, so genannten Reputationen. Dies ist beispielsweise wie bei *ebay* realisierbar, geschieht aber in der Regel sehr viel differenzierter. Eine Reputation spiegelt die Zufriedenheit vorhergehender Servicenehmer mit dem jeweiligen Peer wieder und beinhaltet die Bewertung des Leistungen des einzelnen Anwenders ans Netz (Freigabe, Rechenleistung, Zuverlässigkeit...).

Diese Reputationen können je nach Peer-to-Peer-System völlig unterschiedliche Aspekte aufnehmen, solange sie ihren Zweck, der Unterscheidung und Bewertung einzelner Peers, erfüllen. Gewöhnlich wird die Reputation als Vektor oder Skalar gespeichert und in Reputationspunkten gemessen. Dies ermöglicht es Servicesuchenden sich bei der Wahl ihrer Servicequellen an objektiven Bewertungen zu orientieren. Nach der Ausführung des Services kann der Principal den Agenten bewerten. Weiterhin ist es für Serviceanbieter erstrebenswert positive Reputationen zu erhalten, da damit oft, zusätzlich zu erhöhten Serviceaufträgen, eine besserer Service für sie verbunden wird. Anwender mit guten Reputationspunkten erhalten in der Regel besseren oder zusätzlichen Service. Der Abschnitt *Servicedifferenzierung* beschäftigt sich näher mit der Umsetzung von Reputationssystemen.

4.3 Lösungsansätze

Die folgenden Abschnitte stellen Systeme bzw. Modelle vor die sich jeweils mit den Bereichen Pricing, Motivation und Reputation näher beschäftigen.

4.3.1 Pricing in Referral Systems

Das hier vorzustellende System [1] zeigt mögliche Realisierungen eines statischen und eines dynamischen Pricingmechanismus in Form von einfachen Zahlungsverkehr am Beispiel eines Referral Systems.

4.3.1.1 Referral System

Zuvor sollte allerdings der Begriff des Referral Systems geklärt werden. Dieses System ist eine Unterart der reinen Peer-to-Peer-Systeme. Jeder Peer wird repräsentiert durch einen

Softwareagenten der die Effizienz seiner Nachbarn durch Interaktionen erlernt und damit den Suchvorgang optimiert. Jeder Agent enthält eine begrenzte Liste seiner Nachbarn, die er verändern kann. Diese Liste enthält nicht nur Verweise zu den Nachbarn selbst, sondern auch eine eigene Bewertung für jeden einzelnen. Außerdem besitzt jeder Peer eine Reputation für sich selbst, an der andere erkennen können, was dieser Peer an Service bietet. Der wesentlicher Unterschied zu reinen Peer-to-Peer-Netzen besteht darin, dass Antworten nicht direkt weitergeleitet werden. Ein Peer kann auf eine Anfrage, die er selbst nicht beantworten kann, mit einer Liste seiner Nachbarn antworten. Der Anfragende kann dann mit Hilfe dieser Verweise neue Anfragen starten.

4.3.1.2 Statisches Pricing

Nun gibt es zwei Möglichkeiten Zahlungsmechanismen in diesen Systemen einzuführen. Der erste arbeitet mit statischen, der zweite mit dynamischen Preisen.

Wie kann man nun einen solchen statischen Pricingmechanismus gestalten? Das funktioniert relativ primitiv. Man legt vorweg feste Preise für bestimmte Serviceleistungen, wie Verweise oder Antworten, fest. Dabei sollten natürlich Antworten mehr wert sein als Verweise. Der Zahlungsprozess läuft folgendermaßen ab:

1. Der Suchende schickt seine Anfrage an die ihm bekannten Nachbarn.
2. Angefragte die keine Antwort haben, schicken dem Anfragenden eine Nachricht, dass sie Verweise zu weiteren Nachbarn haben.
3. Möchte der Anfragende diese Verweise haben, bezahlt er den festgelegten Preis und erhält im Gegenzug die Verweisliste, die er weiter verfolgen kann.
4. Hat ein Angefragter eine Antwort, benachrichtigt er darüber den Anfragenden.
5. Der Anfragende sammelt alle Nachrichten über Antworten und sucht sich eine Quelle anhand der in den Verweisen enthaltenen Bewertungen aus, bezahlt und erhält die Antwort.

Das Problem bei einem statischen Pricingmechanismus ist vielleicht weniger Realisierung eines zugehörigen Protokolls als die Festlegung gerechtfertigter Preise. Es dürfte ziemlich schwierig sein, dauerhaft gültige Preise für einen Service zu finden, dessen Qualität sich durchaus über die Zeit ändern kann. Weiterhin kann der selbe Service bei verschiedenen Quellen unterschiedlich gut sein, wenn man beispielsweise die Zuverlässigkeit des Agenten oder andere Bewertungskriterien mit einbezieht. Diese Schwierigkeiten bei der Findung eines Preises kann ein statischer Mechanismus nicht lösen.

4.3.1.3 Dynamisches Pricing

Die Probleme des statischen Pricingmechanismus bei der Festlegung eines Preises, existieren bei einem dynamischen Verfahren nicht. Hier werde Preise für einen Service durch

die Bewertungen des jeweiligen Agenten bestimmt und können sich mit der Zeit ändern, d.h. dynamisch anpassen.

- Wie einführend erwähnt hat jeder Peer sein eigenes Profil und je ein Modell seiner bekannten Nachbarn.
  - In seinem eigenen Profil ist festgehalten, was er für seine eigenen Serviceleistungen, Verweise und Antworten, verlangt.
  - In den Modellen zu seinen Nachbarn ist festgehalten, was ihm die Serviceleistungen des jeweiligen Nachbarn wert sind.
- Diese Werte werden regelmäßig angepasst.
  - Jeweils nach einem bestimmten Zeitintervall werden die Kosten im Profil mit Hilfe eines Faktors x, $0 < x < 1$, gesenkt.
    Wird ein Service verkauft, erhöht sich dessen Wert im Profil um den Faktor y, $1 < y < 2$.
  - Die Werte in den Modellen werden nach dem erhält eines Services verändert. War der Servicenehmer zufrieden bzw. unzufrieden mit der Leistung, erhöht bzw. senkt er die Werte für den Service seines Nachbarn in seinem Modell um z.
  - Die Auswahl eines Services erfolgt nach der Höhe der Belohnung für den Servicenehmer. Die Belohnung ist die Differenz aus dem Betrag was dem Servicenehmer der Service wert ist und dem Betrag, was der Serviceleistende verlangt.

Mit Hilfe dieses Systems ist es möglich Preise dynamisch zu gestalten, wobei preisbestimmend die Nachfrage nach einem Service ist. Dies ist sicherlich eine sinnvolle Möglichkeit der Preisfestlegung. Allerdings sind diese Überlegungen im Moment noch in einer proprietären Phase. Diese Mechanismen wurden vorerst nur in einer Studie getestet, wobei speziellere Eigenschaften von Peer-to-Peer-Netzen noch nicht berücksichtigt wurden. Die Entwicklung befindet sich in einer groben Vorphase, weshalb die Funktion nur in Simulationen getestet werden konnte.

4.3.1.4 Simulationsergebnisse und Zusammenfassung

Da diese Studien zu Pricingmechanismen sich noch in der Entwicklungsphase befinden, waren Testläufe nur innerhalb einer Simulation möglich. Folgende Ausgangsbedingungen hatte die Simulation:

1. Alle Preise für Serviceleistungen sind zu Beginn der Simulation gleich.
2. Jeder Peer erhält ein Startguthaben mit dem er Service kaufen kann und welches sich durch Serviceverkauf erhöht.
3. Es nehmen bis zu 500 Peers an der Simulation teil.

4. Einige Peers verhalten sich wie Free-Rider.

Die Simulation üblicher Interaktionen in einem Peer-to-Peer-System bewirkte folgende wünschenswerte Effekte:

1. Das Guthaben der einzelnen Free-Rider tangierte nach einer bestimmten Zeit immer gegen null. Um weiter an der Peer-to-Peer-Umgebung teilnehmen zu können, müssen sie sich beispielsweise ein weiteres Guthaben erkaufen. Somit ist definitiv sichergestellt, dass unkooperative Nutzer nach einer gewissen Zeit für den Service den sie empfangen selbst zahlen müssen. Im Gegensatz dazu konnten normal interagierende Peers für den Zeitraum der Simulation gut von ihrem Startguthaben leben, d.h. sie brauchten kein neues Guthaben erwerben.

2. Weiterhin wurde auch die Preisentwicklung bei besonders hochwertigem Service untersucht. Es ergab sich, dass der Preis besonders guter Serviceleistungen wie gewünscht anstieg. Je besser der Service war, um so höher stieg der Preis. Auf diese Art könnten Effekte wie die Überlastung einiger besonders guter Peers vermieden werden. Über diese Preisentwicklung regulierten sich die so genannten Hotspots selbst.

Die Simulation ergab, dass der dynamische Pricingansatz geeignet ist, typische Probleme eines Peer-to-Peer-Netzwerkes wie Free-Rider und Hotspots selbstständig zu regulieren. Allerdings ist, wie bereits angesprochen, dieser Ansatz noch in der Entwicklungsphase. Viele spezielle Eigenschaften heutiger Peer-to-Peer-Netzwerke sind noch nicht berücksichtigt. Jedoch ist dieser Pricingmechanismus zukünftig recht vielversprechend um diese Probleme zu lösen oder gar Ansätze für die kommerzielle Nutzung solcher Netzwerke bereitstellt.

4.3.2 Anreizmodelle

Kooperation ist unabdingbar zur Kompensation fehlender Infrastruktur innerhalb reiner Peer-to-Peer-Systeme. Allerdings können autonome Peers selbst entscheiden, ob sie kooperieren oder nicht. Es müssen Anreize geschaffen werden die möglichst alle Peers zur Zusammenarbeit motivieren. Bisher nutzte man den Begriff der Belohnung um eine geeignete Motivation zu schaffen. Das kann aber durchaus zu eng gefasst sein. Mitgliedschaft in einer Gruppe kann schon unter Umständen genügend Motivation sein, unbedingt zu kooperieren, ohne direkt eine Belohnung zu erhalten. Aus diesem Grund wird der Begriff der Belohnung durch die Anreizmodelle [2] erweitert.

Definition Ein Anreizmodell ist ein Modell, welches zur Kooperation motivieren soll. Es umfasst eine Menge von abstrakten Mechanismen, die anreizbasierte Pricingschemata verwenden können. [2, S. 3]

Anreizmodelle schaffen eine Art Katalog von Anreizschemata die variabel in den verschiedensten Anwendungsumgebungen eingesetzt werden können. Hierfür definieren sie die unterschiedlichsten wünschenswerten Aspekte innerhalb einer Peer-to-Peer-Anwendung und welches Anreizschema diese erfüllen kann. Dieses Schema kann daraufhin genutzt werden um weitere Pricingmechanismen zu definieren.

Diese in dieser Theorie entwickelten Anreizmodelle werden im folgenden vorgestellt. Eine Gegenüberstellung der Vor- und Nachteile aller Modelle befindet sich in der Übersicht am Ende des Kapitels.

4.3.2.1 Vertrauensbasierte Anreizmodelle

Prinzipiell unterscheidet die Theorie der Anreizmodelle zwischen vertrauensbasierten und handelsbasierten Anreizmodellen. Die Grundidee der vertrauensbasierten Anreizmodelle ist, dass der Agent den gewünschten Service allein schon dann ausführt, wenn er dem Auftraggeber traut. Er bekommt dafür keine direkte Belohnung. Der Agent sieht den Nutzen hierbei darin, dass er entweder das selbe Ziel wie der Auftraggeber verfolgt oder er glaubt, dass durch diese Serviceleistung die Kooperation für ihn mit anderen steigt.

4.3.2.1.1 Kollektiv-Modell

Anreiz: Gegenseitiges Vertrauen und unbedingte Kooperation aufgrund gemeinsamer Mitgliedschaft in einer Gruppe mit selben Interessen und Zielen.

Eigenschaften: Der Agent erhält keine Belohnung für einen Service, da er Mitglied in der Gruppe ist. Dafür würde er im Gegenzug ebenfalls Serviceleistungen ohne weitere Bezahlung erhalten.
Diese Kollektive können vergänglich sein. Weiterhin können einzelne Peers gleichzeitig verschiedenen Kollektiven angehörigen. Diese Kollektive können Interaktionen mit anderen Peers oder Gruppen durchführen. Dabei kommen andere Anreizmodelle zum tragen.

Beispiel: Familie, Geräte einer Person innerhalb eines Netzes

Existierende Annäherungen beispielsweise im militärischen und privaten Bereich

4.3.2.1.2 Gemeinschaftsmodell

Anreiz Der Agent führt Interaktionen mit den Mitgliedern einer Gemeinschaft aus, in der Hoffnung eine gute Reputation zu bekommen. Gute Reputationen sind notwendig um ebenfalls wieder einen Service zu erhalten.

Eigenschaften Grundsätzlich wird der Agent vom Auftraggeber nach der Serviceleistung bewertet. Der umgedrehte Fall kann auftreten, wenn beispielsweise der Auftraggeber ungerechtfertigte Bewertungen verteilt. Zusätzlich können andere den Agenten bewerten, wenn sie ihn z.B. beim schnüffeln erwischen.

Beispiel: Früher tauschten benachbarte Dörfer Waren als Geschenke aus

Existierende Annäherungen RPG, CORE, Watchdog, Confident

4.3.2.2 Handelsbasierte Anreizmodelle

Im Gegensatz zu den vertrauensbasierten Anreizmodellen beruhen diese auf eine explizite Belohnung des Agenten. Meist ist diese Belohnung eine Art Serviceleistung im Gegenzug. Man unterscheidet weiterhin zwischen den sofortigen und verschobenen Gegenleistungen.

4.3.2.2.1 Sofortige Gegenhandlung Hierbei erfolgt die Belohnung direkt während oder nach der Serviceleistung des Agenten.

4.3.2.2.1.1 Tauschhandelmodell

Anreiz Der Agent wird mit einer direkten Austausch einer Serviceleistung belohnt, d.h. Agent und Auftraggeber führen gleichzeitig einen Service aus.

Eigenschaften Diese Art von Handel kann recht schwerfällig werden, da stets zwei komplette Aktionen vollführt werden müssen, bevor eine neue gestartet werden kann. Dadurch kann das Ganze auch sehr komplex werden. Hinzu kommt, dass der Servicesuchende auch immer einen Service bieten muss, der den jeweiligen Agenten interessiert.

Beispiel: Tauschhandel mit wertvollen Waren.

Existierende Annäherungen keine

4.3.2.2.2 Verschobenen Gegenhandlung Bei dieser Art handelsbasierter Anreizmodelle bekommt der ausführende Agent eine Gegenhandlung zugesagt, d.h. Serviceleistung und Belohnung sind zeitlich versetzt.

4.3.2.2.2.1 Schuldscheinmodell - Ausstellung und Übergabe

Anreiz Der Agent bekommt vom Auftraggeber einen Schuldschein über eine Gegenleistung überreicht.

Eigenschaften Möchte ein Auftraggeber einen Service, tauscht er diesen gegen einen von ihm ausgestellten Schuldschein. Der Schuldschein berechtigt den Agenten beim Aussteller einen Service einzulösen. Hat ein Auftraggeber bereits einen anderen Schuldschein gesammelt, kann er auch diesen im Gegenzug zu einem Service übergeben. Der jeweilige Agent muss sich dann mit seinen Serviceforderungen an den Aussteller des Schuldscheines wenden. Da Serviceleistungen sehr unterschiedliche Werte haben können, ist es möglich Schuldscheine auch nur über Teilaktionen auszustellen.

Beispiel reales Schuldscheinsystem

Existierende Annäherungen keine

4.3.2.2.2.2 Bankmodell

Anreiz Jede Identität hat ein Konto bei einer neutralen Instanz, einer Bank. Eine Belohnung findet über Schecks statt.

Eigenschaften Diese Schecks sind eine Art Schuldschein bei denen die Bank der Schuldner ist. Überreicht der Agent der Bank den Scheck, wird ihm dieser gutgeschrieben und dem Auftraggeber abgezogen. Auf diese Weise können die Belohnungen dem Service besser angepasst werden.

Beispiel Bankbetrieb

Existierende Annäherungen APE, Sprite, TermiNodes

4.3.2.2.2.3 Banknotenmodell

Anreiz Der Agent erhält als Belohnung Banknoten, die durch eine zentrale Instanz ausgegeben werden.

Eigenschaften Diese Banknoten sind ebenfalls eine Art Schuldschein die vorweg von einer Bank ausgestellt werden. Damit sind Schuldscheine, sofern die Bank vertrauenswürdig ist, definitiv gedeckt.

Beispiel Geldscheine

Existierende Annäherungen keine

Die Abbildung 2.2 stellt die hier vorgestellten Anreizmodelle gegenüber und vergleicht sie hinsichtlich mehrerer Aspekte, die es möglich machen sie den verschiedensten Ansprüchen zuzuordnen.

Damit ist es gelungen eine Art Katalog für Anreizmodelle zu schaffen, aus dem, je nach Anwendungsumgebung, ein passendes Modell gewählt werden kann.

4.3.3 Servicedifferenzierung

In den vorangegangenen Kapiteln wurden Ansätze vorgestellt, wie Pricingmechanismen mittels einfachen Zahlungsverkehrs realisiert werden könnten. Ebenfalls wurden verschiedene Möglichkeiten erläutert, wie Anreize zur Kooperation geschaffen werden. Dieser letzte Abschnitt stellt ein System vor, welches Anhand der Reputationspunkte eines Peers, den ihm zustehenden Service bestimmt. [3]

Eigenschaft \ Modell		Kollektiv	Gemeinschaft	Tauschhandel	Schuldschein: Ausstellung	Schuldschein: Übergabe	Bank	Banknoten
Rollen		asymmetrisch		symmetrisch	asymmetrisch			
Belohnung	Art	keine	Reputation	Handlung	Schuldschein		Scheck	Banknote
	Granularität		beliebig	Aktion	Teilaktion		beliebig	Banknote
	Festsetzung		Auftraggeber	Auftr./Agent	Markt/Agent			Markt
	Speicherung		Auftr./Andere	Agent/Andere	Agent/Scheckinhaber			
Bewältigt	eigennützig	+	-	+	+			
	freigiebig			+	+	o	+	
	entschuldbare Nichtkooperation		o	-	-	o		
Trust	Trusted	Auftraggeber		niemand	Auftraggeber	Auftraggeber/ Schuldner	Auftraggeber/ Bank	Auftraggeber/ Zentr. Auth.
	Anonymität	-		+	-	o/-	o	+
Skalierbarkeit		--	-	+	o		+	++
Existierende Annäherungen		verschiedene (Militär, Privat)	RPG, CORE, Watchdog, Confident	keine	keine		APE, Sprite, TermiNodes	keine

Abbildung 4.2: Übersicht Anreizmodelle [2, s. 16]

Reputation dienen der Unterscheidung zwischen einzelnen Peers anhand deren Leistungen ans Netz und werden anhand von Reputationspunkten verglichen. Die Grundidee bei der Servicedifferenzierung besteht darin, je besser die Leistungen an das Peer-to-Peer-Netzwerk sind, um so einen besseren Service erhält auch dieser Peer bei seinen Interaktionen mit anderen.

Hierfür wird der Begriff des Servicelevels (LoS = Level of Service) eingeführt. Man unterscheidet hier zwischen drei verschiedenen:

Basic LoS Die Reputationspunkte liegen unterhalb eines bestimmten Wertes a

Enhanced LoS Die Reputationspunkte liegen zwischen dem Wert a und dem Werte b

Premium LoS Die Reputationspunkte liegen oberhalb des Wertes b

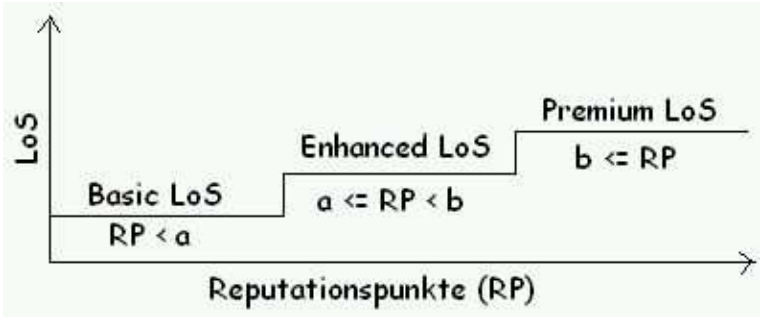

Abbildung 4.3: Servicelevel [3, S. 2]

Die Werte für a und b sind innerhalb des Peer-to-Peer-Systems bekannt, damit jeder Peer in der Lage ist Reputationspunkte dem entsprechenden Servicelevel zuzuordnen.

4.3.3.1 Parameter für die Serviceunterscheidung

Im Bereich des Internets sind Parameter der Servicedifferenzierung, wie Delay, Bandbreite oder Jitter längst bekannt. Im folgenden werden Parameter vorgestellt, die zur Serviceunterscheidung innerhalb von P2P-Netzen genutzt werden können. Sie beziehen sich dabei auf die drei Hauptfunktionsbereiche eines Peer-to-Peer-Systems.

Booten
- Art und Leistungsfähigkeit direkt verbundener Peers (Kooperation, Netzwerkdistanz, Rechenleistung, Speicher, Bandbreite)

Suchprozess
- Anzahl der Hops bis eine Anfrage verworfen wird
- Premium Inhalt entspricht besonders begehrten Inhalt
- Schwer zu findender Inhalt
- Speicherung von Anfragen, bzw. die Resultate der Anfragen
- Inhaltspeicherung von häufigen Anfragen durch Superknoten
- Shortcuts zwischen Peers mit ähnlichen Interessen
- Belastungsausgleich zwischen Peers mit ähnlichen Interessen, durch Speicherung der Inhalte kürzlicher Anfragen.

Download
- Transferrate
- Scheduling Policy

Wie diese Parameter nun genutzt werden wird im Folgenden erklärt. Grundsätzlich gilt hier, was man selbst anbietet, bekommt man auch geboten.

4.3.3.2 Das Servicediffernzierungsprotokoll (SDP)

Das Servicedifferenzierungsprotokoll soll genutzt werden, um eine Serviceunterscheidung in Peer-to-Peer-Systemen zu erreichen. Es erweitert die Grundfunktionalität von P2P-Netzen um die Servicedifferenzierung. Es ist dabei flexibel hinsichtlich der Struktur von Reputionspunkten. Diese Struktur muss nur allen Peers bekannt sein, ebenso die Zuordnung der Reputationspunkte zu den Serviceleveln. Dies kann als Teil der Software realisiert sein, oder wird beim Bootvorgang übergeben.

Die Funktion wird beispielhaft am Suchprozess und Download erläutert. Ein durch die Servicedifferenzierung erweiterter Suchprozess sieht folgendermaßen aus:

Phase 1: Der anfragende Peer sendet mit seiner Anfrage seine Reputationspunkte. Diese erweiterte Query wird als Query_SDP bezeichnet. Somit soll jeder Angefragte Zugriff auf die Reputationspunkte haben.

Phase 2: Der erweiterte Suchprozess SearchProzess_SDP wird gestartet. Jeder angefragte Peer entnimmt die Reputationspunkte aus der Query_SDP und ordnet sie dem entsprechenden Servicelevel zu. Wenn die Hops der Anfrage noch nicht überschritten sind, wird die Anfrage je nach zugeordnetem Servicelevel bearbeitet werden:

Basic LoS: Die Anfrage wird normal nach den Vorgaben des darunter liegenden Protokolls bearbeitet.

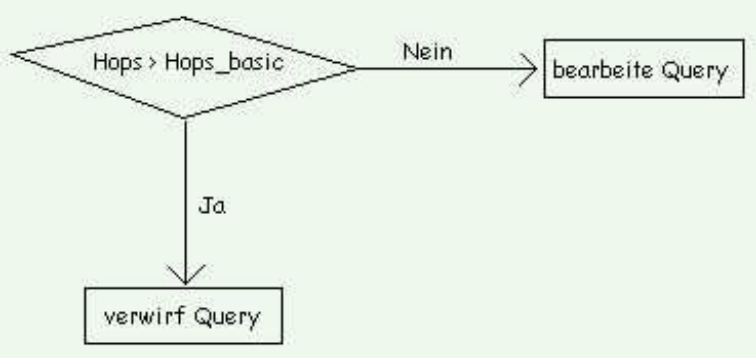

Abbildung 4.4: Basic LoS [3, S. 6]

Enhanced LoS Zuerst wird geschaut ob Resultate zu den Anfrage bereits in den gespeicherten Anfragen vorliegen. Falls nicht, wird die Anfrage ebenfalls normal nach den Vorgaben des darunter liegenden Protokolls bearbeitet.

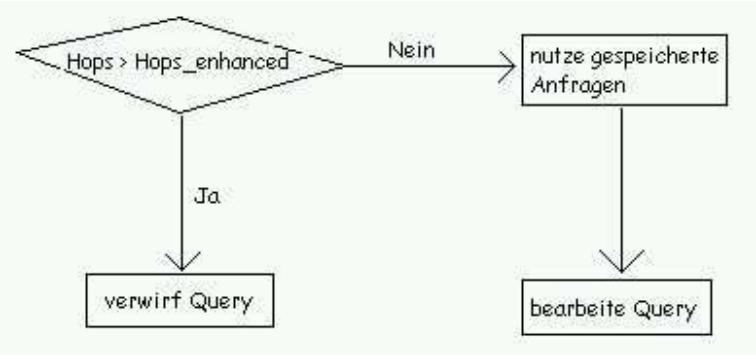

Abbildung 4.5: Enhanced LoS [3, S. 6]

Premium LoS Hier wird zu der Anfrage sowohl in den gespeicherten Anfragen, im gespeicherten Inhalt, im Premium Inhalt und im schwer zu findenden Inhalt nachgeschaut, bevor die Anfrage bei keinen Sucherfolgen normal weiter bearbeitet wird.

Die Zuordnung der Dienste zu den Serviceleveln soll nur als Beispiel dienen und ist willkürlich gewählt. Die Suchmethoden können natürlich auch völlig anders den entsprechden Serviceleveln zugeordnet werden.

Phase 3: Falls keine Antwort auf die Anfrage gefunden wurde, wird diese nach der Spezifikation des Netzwerkprotokolls weitergeleitet. Wurde eine Antwort auf die Anfrage gefunden, wird eine QueryHit_SDP (inklusive der Reputationspunkte des Finders) an den Anfragenden gesendet.

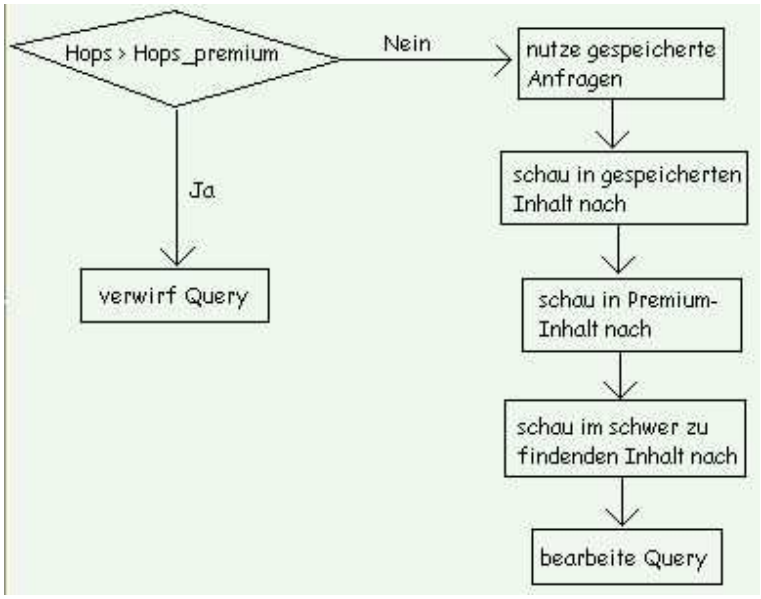

Abbildung 4.6: Premium LoS [3, S. 6]

Auf einen erfolgreichen Suchprozess folgt der Download:

Phase 1: Der Anfragende Peer extrahiert aus den QueryHit_SDPs die Reputationspunkte und sucht sich anhand dieser Punkte einen Agenten aus. Zu diesem stellt er über http oder tcp eine Verbindung her und übermittelt erneut seine Reputationspunkte.

Phase 2: Der Agent ordnet anhand der Reputationspunkte dem Anfragenden einem Servicelevel zu. Dementsprechend wird eine Transferrate und Schedulingpolice gewählt und der Download kann beginnen.

4.3.3.3 Reputationspunkte

Die Reputationspunkte als Grundlage des Servicedifferenzierungsprotokolls sind im Zusammenhang mit ihrer Speicherung zugleich auch sein größtes Problem. Um Servicedifferenzierung nutzen zu können, sind vertrauenswürdige Reputationspunkte notwendig. Diese müssen ebenfalls für alle Peers verfügbar sein, damit sie damit arbeiten können. Das Servicedifferenzierungsprotokoll geht davon aus, dass die Reputationspunkte mit der Anfrage mitgesendet werden. Damit ist eine zentrale Speicherung der Reputationspunkte ungünstig. Bei einer einzigen Suche muss unter Umständen der Zugriff auf die Reputationspunkte sehr oft erfolgen. Damit wird diese Version sehr langsam und es kann zu einem Overhead im Netz führen. Auf der anderen Seite steht die dezentrale Speicherung, mit mehreren Möglichkeiten. Allerdings hat jede der existierenden Möglichkeiten zur dezentralen Speicherung mindestens eine der folgenden drei Eigenschaften, die sie unbrauchbar für das Servicedifferenzierungsprotokoll machen.

Reputationspunkte on-demand Um vertrauenswürdige Reputationspunkte zu erhalten ist es möglich sie on-demand zu berechnen. Dies führt zu einem ähnlichen Problem wie bei der zentralen Speicherung. Aufgrund der Häufigen Verwendung der

Reputationspunkte kann es bei deren Berechnung zu einer untragbaren Verzögerung kommen. Damit ist die Erzeugung on-demand ungeeignet für die Servicedifferenzierung

Subjektivität Um die Reputationspunkteberechnung verteilt zu halten, basieren alle Verfahren auf einer subjektiven Bewertung, was für die Servicedifferenzierung nicht angebracht ist. Um diese Subjektivität zu vermeiden wäre eine Berechnung on-demand nötig, was aber nach dem vorangegangenen Punkt auch auszuschließen ist.

Wertebereich Da die Reputationspunkte in der Regel nicht fest sind sondern meist steigend, müsste ständig die Abbildung der Reputationspunkte auf die Servicelevel angepasst werden.

Allerdings existieren auch Systeme auf die die Sevicedifferenzierung anwendbar ist. Hier ist vor allem ein partielles verteiltes System zu nennen.

- Es benutzt einen vertrauenswürdigen Reputationsberechnenden Agenten (RCA = Reputation Computing Agent), der objektive skalare Reputationen erzeugt.
- Peers sammeln Credits für ihre Arbeit und lassen diese in regelmäßigen Abständen vom RCA in eine äquivalente verschlüsselte Reputation umwandeln, die sie lokal speichern.
- Zum Lesen kann diese verschlüsselte Reputation entschlüsselt werden.
- Diese Reputationen können je nach Teilnahme am Netz fallen oder steigen.

4.3.3.4 Zusammenfassung

Allgemein sind im Servicedifferenzierungsprotokoll keine Sicherheitsaspekte garantierbar bzw. vorgesehen, selbst wenn das darunterliegende Protokoll Sicherheit bietet. Weiterhin gibt es keine Anonymität, da für die Reputationspunkte keine eindeutige Identifizierung vorsehen. Auch kann durch böswillige Nutzer das Servicelevel einfach ignoriert werden und der verdiente Service wird nicht angeboten. Oder es kooperieren mehrere böswillige Nutzer und bieten sich besseren Service als das jeweilige Servicelevel vorsieht.

In einem solchen Peer-to-Peer-System muss mangelnde Beteiligung nicht unbedingt nur aus böswilliger Natur sein. Vielmehr kann es einfach daran liegen das die nötige Softwareerweiterung um die Servicedifferenzierung fehlt. Ohne diese zusätzliche Software können Peers an Interaktionen nicht teilnehmen.

Auch dieses Protokoll befindet sich noch in der Entwicklung. Es bietet viele richtige und gute Ansätze um Fehlverhalten in Peer-to-Peer-Systemen zu unterbinden, hat aber ebenfalls noch viele ungeklärte Probleme zu bewältigen.

4.4 Zusammenfassung

Die hier vorgestellten Anreizmodelle können und werden, im Gegensatz zum SDP und den Zahlungsmechanismen, schon jetzt in den verschiedensten Peer-to-Peer-Systemen genutzt. Aber auch sie klären nicht alle Einzelheiten der zu entwickelnden Protokolle ab. Sie liefern den Grundstein, bzw. die Grundidee wie Kooperation in den doch recht unterschiedlichen Systemen mehr oder weniger extrinsisch motiviert werden kann. Dabei bieten sie Vorlagen die alle denkbaren Ansprüche und Wünsche an ein Peer-to-Peer-Netz abdecken. Wie diese Grundideen durch Protokolle realisiert werden, ist nicht geklärt, bzw. vorgegeben. Sie beschäftigen sich auch nicht mit der Frage, wie Preise oder anderweitige Vergütungen für Serviceleistungen festgelegt werden sollen.

Mit der Festlegung der Höhe der Vergütung haben sich die anderen beiden Modelle beschäftigt. Basierend auf dem Gemeinschaftsmodell der Anreizmodelle werden hier die Belohnungen für Serviceleistungen über Reputationen festgelegt. Der durchaus wünschenswerte und realistische Ansatz dabei ist, dass nicht jeder Service gleichwertig ist und damit nicht gleichartig belohnt werden sollte. Über Reputationen wird versucht den jeweiligen Agenten und seine Serviceleistungen einzuschätzen und anhand dessen eine gerechtfertigte Belohnung zu bestimmen. Die Art der Belohnung war in diesen zwei Anwendungen auf der einen Seite Geld und auf der anderen Seite ein höherwertiger Service.

Nun könnte man behaupten, dass, sobald Geld ins Spiel kommt, der eigentliche Grundgedanke von Peer-to-Peer-Netzen, der reine Tauschhandel unter Gleichgesinnten, verloren geht. Dem kann man teilweise zustimmen, wenn man nur die Nutzer betrachtet, die ihr negatives Verhalten trotz Anreizmechanismen nicht ändern. Diese könnten zwar weiterhin an Netzwerkbetrieb teilnehmen, d.h. nach ihren üblichen Verhaltensmustern nur Dateien von anderen Peers herunterladen, müssten dafür aber früher oder später regelmäßig Geld bezahlen. Dafür ist aber nun wiederum ein Peer-to-Peer-System nicht unbedingt notwendig. Dieser reine Kauf von Daten oder Service ist genauso gut oder wahrscheinlich sogar besser über Client-Server-Interaktionen realisierbar. Aus dem selben Grund möchte ich bestreiten, dass es sinnvoll wäre ein Peer-to-Peer-System kommerziell zu nutzen. Möchte man Serviceleistungen oder Dateien kaufen oder verkaufen, ist dies sicher mit einem sehr viel geringeren organisatorischen und entwicklungstechnischem Aufwand verbunden, wenn man dafür die bekannte und bereits erwähnte Client-Server-Struktur nutzt. Denn wie das Beispiel der Abschaltung Napsters zeigte, wird es wohl immer möglich sein, etwaige Zahlungsmechanismen zu umgehen.

Auf der anderen Seite, kann, egal ob mit Geld oder anderweitiger Belohnung, sicherlich durchaus das eigentliche Grundproblem des unkooperativen Verhaltens effektiv angegangen werden ohne das die Gefahr besteht, die Vorzüge eines Peer-to-Peer-Systems zu verlieren und sich immer mehr der Grundfunktionalität einer Client-Server-Architektur anzunähern. Auch mit dem Konzept des dynamischen Pricings kann man, gerade dann wenn die nötige Kooperation der einzelnen Peers vorliegt, ein Netzwerk betreiben, in das der kooperative Nutzer keine Kosten investieren muss. Dafür könnte man beispielsweise jedem neuen User ein Startguthaben fiktiv bereitstellen mit dem er agieren kann. Wie die Testläufe in der Simulation zu dem Konzept ergaben, verloren nur die so genannten Free-Rider im Laufe der Zeit ihr Guthaben und konnten nicht mehr am Netzwerkbetrieb

teilnehmen ohne ihr Guthaben in irgend einer Weise neu zu erhöhen. Somit ist es für jeden rationalen Anwender erstrebenswert kooperativ zu Handeln. Ähnlich funktioniert dies beim SDP, insofern es erstrebenswert ist ein höheres Servicelevel zu erlangen.

4.4.1 Fazit

Die Forschung zu Pricingmechanismen in Peer-to-Peer-Netzen ist noch im Anfang begriffen. Es existieren viele nützliche Ansätze um Probleme durch die fehlende doch so wichtige Kooperation zu bekämpfen. Vorgestellt wurden hier verschiedene Zahlungsmechanismen und Anreizmodelle. Die dazu entwickelten Protokolle befinden sich größtenteils noch in der Testphase. Die damit verbundenen Ideen sind aber durchaus in der Lage, die Kooperation rationaler Anwender entscheidend zu erhöhen ohne dabei kommerzielle Aspekte in eine Peer-to-Peer-System einzubringen. Wie bereits angesprochen, denke ich, dass Peer-to-Peer-Systeme ihren eigentlichen Tauschhandelsbasierten Charakter verlieren, wenn sie kommerziell genutzt werden. Ist eine kommerzielle Nutzung vorgesehen, dürfte ein Client-Server-basierter Verkauf von Serviceleistungen wesentlich effektiver, besser erprobt und einfacher umzusetzen sein.

Mit den präsentierten Mechanismen wurde der Weg bereitet, dem existierenden Dilemma des Free-Ridings in heutigen Peer-to-Peer-Systemen entgegenzuwirken. Dabei wird versucht der Grundcharakter von solchen Netzen aufrechtzuerhalten. Es bleibt oberflächlich betrachtet, insofern die Anwender tatsächlich kooperieren, ein reines Tauschgeschäft zwischen allen ähnlich gesinnten Nutzern. Bei reger Beteiligung an Interaktionen innerhalb des Systems sollte kein Anwender für Leistungen Geld bezahlen, bzw. jeder Anwender mit einem bestimmten Startguthaben ohne weitere Einzahlungen agieren können. Hierbei bleibt die Frage der Legalität solcher Tauschgeschäfte allerdings offen, nicht zuletzt, weil sich deren Kontrolle mehr als schwierig gestaltet.

Literaturverzeichnis

[1] B. Yu, M. Singh: Mechanism Design of Agent-Based Peer-to-Peer Systems; Second International Workshop on Agents and Peer-to-Peer Computing (AP2PC 2003), Melbourne, Australia, July 14, 2003. http://p2p.ingce.unibo.it/NotRevisedPapers/16_yu.pdf

[2] P. Obreiter, J. Nimis: A Taxonomy of Incentive Patterns - The Design Space of Incentives for Cooperation; Second Inetrnational Workshop on Agents and Peer-to-Peer Computing (AP2PC 2003), Melbourne, Australia, July 14, 2003. http://www.ipd.uka.de/ obreiter/publications/2003TR9.pdf

[3] M. Gupta, M. Ammar: Service Differentiation in Peer-to-Peer Networks Utilizing Reputations; Fifth International Workshop on Networked Group Communications (NGC'03), Munich, Germany, September 16-19, 2003. http://www.cc.gatech.edu/grads/g/Minaxi.Gupta/pubs/priority.pdf

[4] M. Koch, K. Möslein, M. Wagner: Vertrauen und Reputation in Online Anwendungen und virtuellen Gemeinschaften, December 22, 2003. http://www11.informatik.tu-muenchen.de/publications/pdf/Koch2000b.pdf

[5] R. Steinmetz: Peer-to-Peer Charakteristische Eigenschaften, October 14, 2003. http://www.kom.e-technik.tu-darmstadt.de/ws-p2p/slides/Steinmetz_P2P-specification-TUD-030924-V.3.pdf

Kapitel 5

Der Einfluß von IPv6 auf E-Commerce

Holger Moos

Die vorliegende Arbeit beschreibt den Einfluß, den das neue Internetprotokoll IPv6 momentan auf den Bereich des E-Commerce hat und in Zukunft haben könnte. Nachdem die Motivation für die Entwicklung von und die Umstellung auf IPv6 dargestellt wird, folgt zunächst eine sehr kurze Begriffsklärung der Begriffe „IPv6“ und „E-Commerce“. Die Darstellung der Motivation geschieht vor allem im Hinblick auf den E-Commerce Sektor. Neben dem folgenden allgemeinen Überblick über IPv6 mit den Vor- und Nachteilen seiner Einführung in die Infrastrukturen des Internets und anderer Computernetze erfolgt die sehr konkrete Beschreibung des Elements der IP Security (IPSec) und die Beschreibung der Migration von IPv6 mit entsprechenden Mechanismen. In diesem Zusammenhang wird auch auf die mögliche Koexistenz von IPv6 mit IPv4 eingegangen. Des Weiteren wird ein kurzer Überblick über den aktuellen Fortschritt der Einführung von IPv6 in die Infrastruktur vor allem des Internets und der Kompatibilität von Hardware mit IPv6 gegeben. Nach dieser Hinführung zum eigentlichen Thema wird schließlich konkret auf den Bereich des E-Commerce eingegangen. Hierbei werden die Sicherheitsanforderungen diesen Bereichs genannt und die mögliche Erfüllung dieser Anforderungen durch die in IPv6 enthaltene IPSec beschrieben. Des Weiteren wird auf die Kompatibilität von Betriebssystemen und Software mit IPv6 eingegangen, um den Einfluß des neuen Internetprotokolls im E-Commerce auf Applikationsebene zu beschreiben. Im dritten Abschnitt, dem Abschnitt zu E-Commerce, wird schließlich die im Sinne größerer Sicherheit mögliche Zusammenarbeit mit Firewalls beschrieben und mit bisherigen Lösungen verglichen, was im besonderen für den Bereich des Business-to-Business (B2B) relevant ist. Im letzten Abschnitt wird nach dem Fazit dieser Arbeit schließlich ein Ausblick in die mögliche Zukunft von IPv6 gegeben, wobei es in erster Linie um den Fortgang der allgemeinen Einführung von IPv6 im Internet und anderen Computernetzen und den zukünftigen Einfluß im Bereich des E-Commerce geht.

Inhaltsangabe

5.1 Einleitung

Nachdem bereits auf der ersten Seite meiner Ausarbeitung eine Zusammenfassung und somit auch ein Überblick über die vorliegende Arbeit gegeben wurde, folgt nun an dieser Stelle ausschließlich die Motivation und eine kurze Begriffsklärung.

5.1.1 Motivation

Die Entwicklung von IPv6 läßt sich in erster Linie auf den sehr knappen IP-Adreßraum zurückführen. Dieser läßt sich wiederum auf die allgemeine Steigerung der Anzahl an Internetnutzern, aber auch vor allem auf die Entwicklung, daß jeder PDA, jedes Handy, jedes Auto oder auch die unterschiedlichsten Haushaltsgeräte eine IP benötigen bzw. benötigen werden, zurückführen, wobei die verschiedensten Geräte und Dienste zunehmend auf eine permanente IP-Verbindung angewiesen sein werden.

So gibt es unterschiedliche Prognosen, wie lange die momentan noch verfügbaren Adressen ausreichen werden. In einem SPIEGEL Online-Artikel[16] war in diesem Jahr z.B. zu lesen, daß das „numerische Adreßbuch“ bereits im Jahre 2005 voll sein werde. Aber auch die EU-Kommission[15] und die Gartner Group[7] gehen davon aus, daß dies in den Jahren 2005/2006 der Fall sein wird, wobei man in eher positiven Prognosen von einer Zeitspanne zwischen 2006 bis 2011 ausgeht.

Neben der Berücksichtigung des Adreßraum-Problems wurden während der Entwicklung bereits sehr früh zusätzliche Mechanismen, wie z.B. die Unterstützung von Sicherheitsaspekten auf IP-Ebene, hinzugefügt und Änderungen gegenüber dem sich bereits bewährten und in Computernetzen sich weitgehend durchgesetzten IPv4 vorgenommen.

Eine solch fundamentale Änderung der Infrastruktur von Computernetzen durch die Einführung eines neuen Internetprotokolls nimmt natürlich auch Einfluß auf die unterschiedlichsten Anwendungsbereiche dieser Netze, so auch auf den Bereich des E-Commerce. Hierbei ist zu erwähnen, daß sich Änderungen von Infrastruktur und allgemein an Hard- und Software, wenn auch gewollt, nicht unbedingt nur positiv auswirken können. So sind solche Änderungen auch stets mit Risiken, wie z.B. dem Vorliegen von instabilen Systemen und Sicherheitslücken im System, verbunden. Gerade im Bereich des E-Commerce können sich diese Risiken in besonders großem Maße negativ auswirken, und es kann besonders hier ein enormer finanzieller Schaden entstehen.

Die Beleuchtung gerade des E-Commerce ist aber auch aufgrund der Tatsache interessant, daß eine sehr stark zunehmende Nutzung diesen Bereiches des Internets vorliegt. Die Gesellschaft für Konsumforschung (GfK) geht in ihrer Studie[6] vom 14. Oktober 2003 davon aus, daß bei der Zahl der Einkäufe deutscher Privathaushalte die in diesem Jahr im Internet getätigten Bestellungen um 27 Prozent gegenüber dem Vorjahr zulegen werden.

5.1.2 Begriffsklärung

IPv6 IPv6 stellt die neue Generation des Internetprotokolls dar und wurde zu Beginn seiner Entwicklung im Jahre 1993, als die zahlreichen Vorschläge für ein neues Internetprotokoll, die es Anfang der 90er Jahre gab, zusammengefaßt wurden, als IPng – „Internet Protocol Next Generation“ bezeichnet. Die Standardisierung des Protokollkerns unter dem Namen IPv6 erfolgte schließlich im Jahre 1997 durch die IETF.[11]

E-Commerce Eine allgemein gültige Definition dieses Begriffs gibt es nicht. An dieser Stelle hätte man auch die Begriffe E-Business, Internet Commerce, u.a. nutzen können. In der vorliegenden Arbeit wird der Begriff E-Commerce jedoch verwendet, um zum einen das Anbieten und Verkaufen von Waren und Dienstleistungen über das Internet, aber um zum anderen auch Geschäftsprozesse von Firmen zu beschreiben, die mit Hilfe des Internets oder des jeweiligen Intranets umgesetzt werden. Somit sind also sowohl die Bereiche Business-to-Consumer (B2C) und Consumer-to-Consumer (C2C) als auch Business-to-Business (B2B)im folgenden von Interesse.

5.2 IPv6

In diesem Abschnitt geht es nun um eine genauere Betrachtung von IPv6, im besonderen natürlich der Veränderungen zu IPv4, der Migration und der damit zusammenhängenden Vor- und Nachteile von IPv6. Speziell IPSec wird in diesem Abschnitt ebenfalls näher beleuchtet. Gleichzeitig stellt sich auch die Frage, in wie weit die Implementierung von IPv6 in Hardware und die Einführung durch Internet Service Provider fortgeschritten ist.

5.2.1 Übersicht/Vergleich zu IPv4

Die für die vorliegende Arbeit wichtigsten Punkte in dieser Übersicht sind die beiden folgenden:

Erweiterter Adreßraum Der erweiterte Adreßraum war, wie im vorherigen Abschnitt bereits beschrieben, im Grunde genommen auch der wichtigste Punkt für die Entwicklung eines neuen Internetprotokolls. So werden bei IPv6 Adressen von 128 Bit Länge anstatt 32 Bit Länge, wie bei IPv4, verwendet.

IPSec Als zweiter Punkt, der bereits sehr früh eine große Rolle spielte, läßt sich die Übernahme von IPSec als integralen Bestandteil des neuen Internetprotokolls, und eben nicht mehr nur als optionale Erweiterung, nennen. Somit wurde der bereits oft geforderten Einzug von Sicherheitsaspekten auf IP-Ebene, welche zu Beginn des Internets als in erster Linie wissenschaftliches und akademisches Computernetzwerk nicht notwendig und nicht gefordert waren, realisiert. Dieser Aspekt ist natürlich besonders für den Bereich des E-Commerce von großer Bedeutung, wo man die Implementierung von Sicherheitsaspekten als entscheidendes Kriterium für die Nutzung von

Computernetzen, im Besonderen des Internets, für das eigene Business bezeichnen kann. Bisher wurden Sicherheitsmechanismen jedoch nur für spezielle Anwendungen entwickelt und beschränkten sich somit auch nur auf bestimmte Anwendungen und Funktionen, wobei sich hier besonders für E-Commerce-Anwendungen z.B. SSL nennen läßt. Im Gegensatz dazu stellt IPSec einen Ansatz dar, den gesamten Datenverkehr, auch von nicht speziell gesicherten Anwendungen, abzusichern. Die konkrete Gestalt von IPSec bzw. die einzelnen Mechanismen, die in ihr implementiert sind, wird bzw. werden im folgenden Abschnitt noch genauer beleuchtet.

Weitere Punkte zur Charakterisierung von IPv6 bzw. als Abgrenzung zu IPv4, die in dieser Arbeit nicht weiter erläutert werden, sind hier lediglich kurz aufgelistet:

- Integrierte Autokonfigurationsmechanismen
- Vereinfachtes Headerformat
- Basis Header + variable Extension Headers (Modularisierung des Headers)
- Type of Service (ToS)
- Echter Multicast
- Möglichkeit eines Anycasts
- „Quality of Service“-Unterstützung

Zur „Quality of Service“-Unterstützung, die durch ein 20-bit langes, so genanntes „Flow-Label“-Feld im IPv6-Header gewährleistet werden soll, läßt sich noch sagen, daß diese zur Zeit des Verfassens der RFC 2460[2] zur Spezifikation von IPv6 mit einem experimentellen Status versehen wurde, da die Anforderungen an eine solche Unterstützung noch nicht genau definiert waren. Die grundlegenden Überlegungen zu diesem „Flow-Label“-Feld lassen sich im Anhang A der genannten RFC nachlesen.

5.2.2 Vorteile

Neben der enormen Größe des bei IPv6 vorliegenden Adreßraums und der Übernahme von IPSec als integralen Bestandteil lassen sich ohne nähere Erläuterung die folgenden Vorteile nennen:

- Verkleinerung der Routingtabellen
- Effizienteres Routing
- Unterstützung verschiedener Dienste wie z.B. Echtzeitübertragung
- Vorhandensein eines verbesserten MobileIP's
- Nutzung von echtem Multicast anstatt des bandbreitenverschwendenden Broadcasts

5.2.3 Nachteile

Unmittelbare Nachteile lassen sich im Moment nicht erkennen, da man erst am „Beginn“ der Einführung des neuen Internetprotokolls steht. Solche unmittelbaren Nachteile können sich erst durch veränderte Rahmenbedingungen ergeben, genauso wie man erst zur heutigen Zeit die Nachteile von IPv4 erkennen kann, welche am Anfang dieser Protokollversion eben nicht wirklich als solche vorhanden waren bzw. als Nachteile gesehen wurden. Jedoch lassen sich mittelbare Nachteile erwähnen, die nicht im Protokoll selbst liegen, sondern in seiner Einführung und der somit notwendigen komplexen Umstrukturierung des Internets und anderer Computernetzwerke.

Ohne dem entsprechenden noch folgenden Abschnitt über die Migration und die mögliche Koexistenz von IPv6 mit IPv4 vorzugreifen, seien an dieser Stelle die folgenden Punkte, vor allem für Firmen bei der Transition ihrer Intranets zu IPv6 und allgemein für ISP's, als nachteilig zu nennen:

- Kosten für die Aktualisierung bzw. das Ersetzen von Hard- und Software
- Kosten und Zeitaufwand für Weiterbildung, vor allem der Administratoren
- Allgemein erhöhte Personalbindung
- Zunächst ein unter Umständen instabileres System, als dies mit der alten Protokollversion der Fall war
- Das Vorliegen von Sicherheitslücken durch fehlerhafte Konfiguration oder allgemein schlechte Administration des Gesamtsystems

Bei diesen Punkten können besonders die beiden letzten gerade im Bereich des E-Commerce einen enormen finanziellen Schaden anrichten, was dazu führt, daß die Unternehmen sehr vorsichtig bei der Einführung von IPv6 sind und diese somit nur sehr schleppend fortschreitet.

5.2.4 IPSec

Die durch IPSec gegebene Sicherheit umfaßt in erster Linie Authentizität, Integrität und Verschlüsselung der zu versendenden Datenpakete, was mit Hilfe der beiden im Folgenden beschriebenen Extension Headers, dem Authentication Header und dem Encapsulating Security Payload Header, in Verbindung mit den unterschiedlichen Modi der Übertragung geschieht. Neben der Tatsache, daß IPSec bereits fest in IPv6 integriert ist, besteht die Möglichkeit, es als Erweiterung von IPv4 einzusetzen.[11]
Die Architektur von IPSec selbst ist im RFC 2401[14] beschrieben, wobei die Beschreibung einer vollständigen Spezifikation von IPSec gemäß RFC 2411[3] in einer Reihe von Dokumenten aufgeteilt ist.

Authentication Header (AH) Dieser Extension Header wird im RFC 2402[12] beschrieben und realisiert die Authentisierung und den Integritätsschutz von IP-Datagrammen, wodurch die Identität des Absenders eines Datenpakets nachvollziehbar und die Unverfälschtheit der übertragenen Daten garantiert wird. Dieser Header ist wie in der folgenden Abbildung gezeigt aufgebaut, wobei das „Authentication Data"-Feld die verschlüsselte Prüfsumme des jeweiligen Datenpakets enthält und das „Sequence Number"-Feld dazu dient, wiedergegebene, bereits übertragene Pakete zu erkennen.

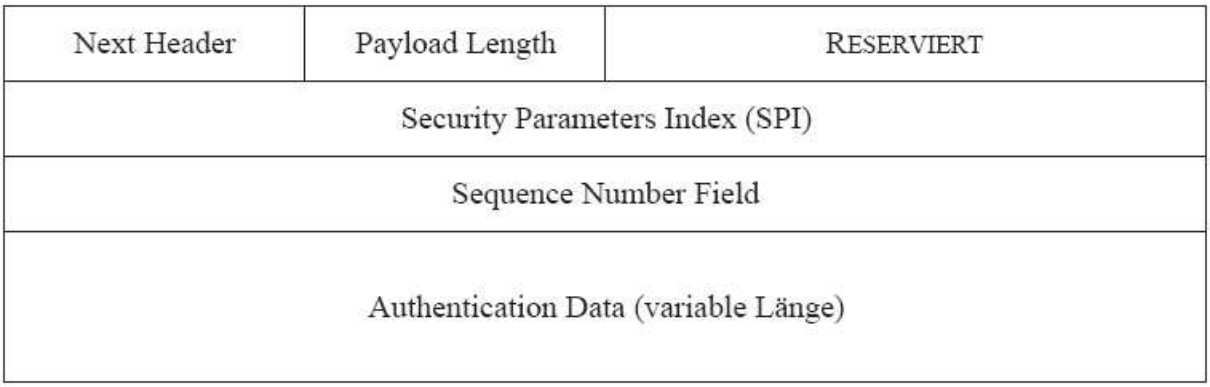

Abbildung 5.1: Der Authentication Header

Eine genaue Beschreibung aller Felder kann im genannten RFC nachgelesen werden. Das Verfahren zur Berechnung der Prüfsumme im „Authentication Data"-Feld, welches als Standard definiert wurde und durch alle Implementierungen unterstützt werden muß, ist „Keyed MD5". Optional können aber auch weitere Verfahren implementiert werden, wodurch bei Beginn einer Kommunikation noch die Einigung auf ein bestimmtes Verfahren erfolgen muß. Findet hierbei keine Einigung statt, wird das Standardverfahren verwendet, so daß die gewünschte Sicherheit auf jeden Fall gewährleistet ist.

Encapsulating Security Payload (ESP) Der Extension Header des ESP's ist im RFC 2406[13] beschrieben. Er ermöglicht eine Verschlüsselung der zu übertragenen Daten und bietet so Vertraulichkeit der Daten, je nach Verfahren aber auch Integrität der Daten und Authentisierung der Datenquelle. Das Format des Headers entspricht der folgenden Abbildung.

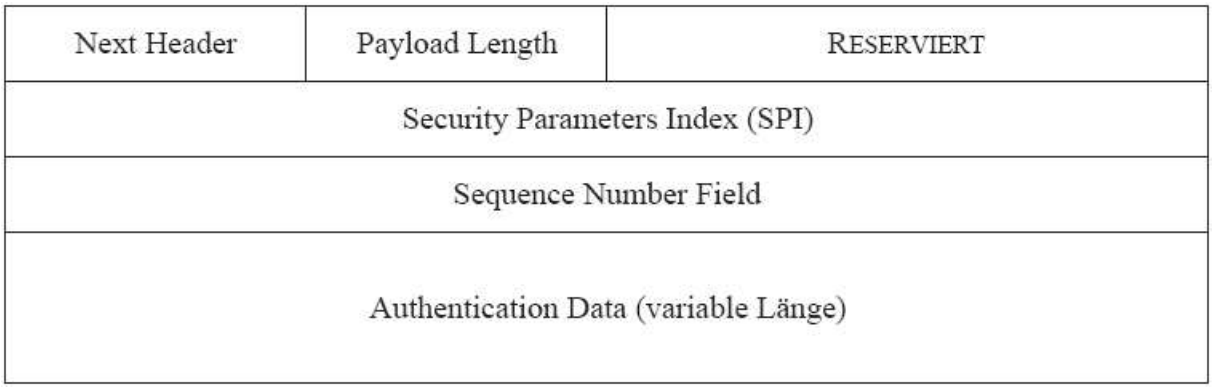

Abbildung 5.2: Der Encapsulating Security Payload Header

Während im „Authentication Data"-Feld wie beim AH die Prüfsumme steht, ist die „Sequence Number" ebenfalls wie beim AH für die Realisierung der Anti-Replay-Funktionalität zuständig. Eine genaue Beschreibung aller Felder kann im genannten RFC nachgelesen werden.
Gesteuert wird die Verwaltung des Datenverkehrs unter Verwendung von IPSec von zwei Datenbanken. Dies ist zum einen die Security Policy Database (SPD) und zum anderen die Security Association Database (SAD), wobei in der SAD die zu verwendenden Authentisierungs- und Verschlüsselungsparameter für einzelne Verbindungen festgelegt werden können. Auch beim ESP gibt es grundlegende Verschlüsselungsalgorithmen, die von einer konformen Implementierung unterstützt werden müssen, so daß sich Kommunikationspartner wenigstens auf einen dieser Standards einigen können, um eine sichere Verbindung aufzubauen, sofern sie diese Standards für die entsprechende Verbindung bereit sind zu akzeptieren.

Modi Für den Einsatz von IPSec, im besonderen bei der Verschlüsselung der einzelnen Datenpakete mit Hilfe des ESP's, stehen die beiden folgenden Modi zur Verfügung[11]:

Transport-Modus In diesem Modus wird lediglich das Payload des entsprechenden Datenpakets verschlüsselt, und der Basis-Header bleibt unverändert. Somit dient dieser Modus in erster Linie der Host-zu-Host-Kommunikation.

Tunnel-Modus Der wohl meistverwendete Modus, da er sowohl zwischen einzelnen Gateways als auch zwischen Gateways und Hosts gemischt betrieben wird, ist der Tunnel-Modus. Er kann z.B. auch für LAN-zu-LAN-Verbindungen eingesetzt werden, um die Sicherheitsmechanismen von Firewalls zu ergänzen und somit ein Virtual Private Network (VPN) aufzubauen. Weitere Informationen befinden sich im entsprechenden Abschnitt dieser Arbeit.
Bei diesem Modus wird das gesamte ursprüngliche Datagramm als Payload verwendet, dem schließlich ein neuer Header vorgesetzt wird, wodurch der ursprüngliche Header verschlüsselt werden kann. Hierdurch können zusätzlich Informationen wie z.B. die Zieladressen geschützt und somit auch die Vertraulichkeit des Datenflußes gewährleistet werden.

Für den Aufbau einer gesicherten Verbindung ist es natürlich erforderlich, daß ein Kommunikationspartner authentisiert werden kann. Hierzu besteht jedoch die Notwendigkeit

einer verläßlichen globalen Infrastruktur, in der alle Kommunikationspartner mit ihren Public-Keys registriert sind. Eine solche globale Infrastruktur ist jedoch zurzeit nicht gegeben. Da diese aber auch als Anforderung für die Absicherung von z.B. E-Mail und HTTP gilt, ist dies kein spezifisches Problem von IPSec, sondern eher ein allgemeines Problem und muß daher durch übergreifende Arbeitsgruppen gelöst werden. Des weiteren ist auch ein dazugehöriges, verläßliches Verfahren für die Vereinbarung und Verteilung von Schlüsseln notwendig, welches ebenfalls im Standard nicht festgelegt wurde.[4]
Der konkrete Nutzen, den IPSec für E-Commerce bzw. Anwendungen im E-Commerce besitzt, wird im Abschnitt zur Sicherheit im E-Commerce nach der Beschreibung der einzelnen Sicherheitsanforderungen geschildert.

5.2.5 Migration/Koexistenz mit IPv4

Eine schlagartige Migration zu IPv6 ist weder im Internet, noch in den umfangreichen Computernetzen größerer Firmen möglich. Beim Internet ist dies im besonderen Maße der Fall, da hier einfach eine enorm große Anzahl an Systemen angeschlossen sind und die Struktur an sich sehr komplex ist. Genauso kann auch bei Intranets von Frimen die Komplexität eine Rolle spielen, vor allem aber auch die Kosten, die bei einer Umstellung z.B. durch den notwendigen Austausch von einzelnen Komponenten anfallen. Diese Aspekte spielen bei kleineren Unternehmen eine eher geringere Rolle. Jedoch liegt der Schwerpunkt dieser Arbeit schließlich auf dem Internet als „Marktplatz“ des E-Commerce und auf größeren Unternehmen, die ihre Computernetze miteinander verbinden und intensiv für ihre Geschäftsprozesse nutzen.

Da also die erwähnte schlagartige Migration aus den genannten Gründen nicht möglich ist bzw. nicht durchgeführt wird, spielen Begriffe wie „sanfte Migration“ und „zeitweilige Koexistenz“ in diesem Zusammenhang eine große Rolle. So wird der Begriff der „sanften Migration“ verwendet, um zu verdeutlichen, daß die Migration in mehreren Stufen ablaufen kann. Hierbei kann eine Stufe unter anderem aus dem Aktualisieren der Software einer bestimmten Art von Komponenten, wie z.B. Router, Gateways usw., oder dem kompletten Austausch dieser Komponenten bestehen. Aufgrund dieser stufenförmigen Migration ist es jedoch notwendig, daß die Koexistenz mit IPv4 in einem konkreten Computernetz und im Internet allgemein über Jahre hinweg möglich ist, ohne daß die bisherige Stabilität eingeschränkt wird. In diesem Zusammenhang ist es natürlich von großem Interesse, in welcher Art und Weise eine konkrete Migration nun ablaufen soll bzw. muß, um die Koexistenz zu gewährleisten.

An dieser Stelle läßt sich sagen, daß eine möglichst zügige Einführung von IPv6 in Computernetzen, vor allem des Internets, zu einem entscheidenden Teil mit dem Vorhandensein von einheitlichen und wohldurchdachten Transitionsmechanismen steht und fällt.
Somit wurden während dem Standardisierungsprozeß von IPv6 gleichzeitig auch solche Mechanismen durch die eigens dafür zusammengestellte Arbeitsgruppe NGTRANS der IETF entwickelt und im RFC 2893[5] beschrieben.

Die drei grundlegenden Mechanismen, die hierbei entwickelt wurden, sind die folgenden[1]:

Tunneling Dieser Mechanismus entspricht grundsätzlich dem Tunnel-Mechanismus, der bereits in IPv4-Netzen z.B. für MobileIP eingesetzt wird und auch beim Tunnel-Modus von IPSec zum Einsatz kommt. Hierbei wird ein existierendes IPv6-Datagramm in ein neues Paket gekapselt, welches einen IPv4-Header besitzt und somit über den bestehenden IPv4-Backbone verschickt werden kann. Sobald das erstellte Paket am Ziel, bei dem es sich wiederum um ein IPv6-Netz handelt, angekommen ist, wird das ursprüngliche IPv6-Paket entkapselt und kann seinen Weg in diesem IPv6-Netz fortsetzen. Sinnvoll ist dieser Mechanismus z.B. für „IPv6-Inseln“, die über das Internet miteinander verbunden werden sollen. Somit wird es auch für Forschungsnetze, wie z.B. das „6bone“, genutzt, da so bereits sehr früh Implementationen von IPv6 getestet werden können, wobei man die existierende IPv4-Infrastruktur ohne Veränderungen verwenden kann.
Durch diesen Mechanismus gehen allerdings Eigenschaften des neuen Internetprotokolls, wie z.B. der Type of Service, verloren, wodurch diese einzelnen Eigenschaften unter anderem in dem angesprochenen Forschungsnetz wiederum nicht getestet werden können.
Zur Kapselung und Entkapselung der IPv6-Pakete in bzw. aus IPv4-Paketen sind jedoch zusätzlich Dual Stack Routers notwendig, bei denen der folgende Mechanismus verwendet wird.

Dual Stack Dieser Mechanismus besteht daraus, daß in Routern und Hosts zwei Protokollstacks, jeweils einer für IPv4 und einer für IPv6, gleichzeitig implementiert sind, um neben den nun möglichen IPv6-Verbindungen auch weiterhin die Kommunikation mit dem IPv4-Backbone zu gewährleisten. Dies ist besonders am Anfang und speziell für die Hosts und Routers, die sich an Schnittstellen zwischen zwei Strukturen mit den beiden unterschiedlichen IP-Versionen befinden, bis zur vollständigen Migration von IPv6 notwendig.

Protocol Translation Durch die Protocol Translation wird die Struktur eines gesendeten Pakets umgewandelt, so daß sie der entsprechend anderen Version des Internetprotokolls entspricht. Dies ist für die Kommunikation von Hosts, die ausschließlich IPv6-Pakete erzeugen können, aber mit einem IPv4-Host kommunizieren wollen, von entscheidender Bedeutung. Bei diesem Mechanismus ist allerdings eine zusätzliche Infrastruktur notwendig, um die Adressen bzw. DNS-Anfragen in die jeweilig andere Protokollversion umzuwandeln.

Insgesamt gesehen, verschafft erst die Kombination dieser Mechanismen einem Administrator eines komplexen Computernetzwerks die Flexibilität und Interoperabilität, um die Einführung von IPv6 in das bestehende Netzwerk erfolgreich und möglichst effizient vorzunehmen.

5.2.6 Kompatible Hardware

Die Implementierung von IPv6 in aktueller Hardware ist bereits soweit fortgeschritten, daß jeder namhafte Hersteller von Routern und weiteren Komponenten wie z.B. Netzwerkkarten bereits eine vollständige Unterstützung der neuen IP-Version in seinen aktuellen Komponenten bietet. Hier lassen sich z.B. die Hersteller Cisco, Fujitsu oder Hitachi

nennen.[10] Während die Unterstützung zuerst nur auf Software-Basis vorhanden war, wobei sich hier natürlich ein großer Performance-Verlust ergab, befindet sich bereits heute die Implementierung bei allen namhaften Herstellern in der Hardware. Teilweise ist auch die Aktualisierung von älteren Routern durch Software-Updates möglich, was jedoch ebenfalls zu dem bereits erwähnten Performance-Verlust führt. Des Weiteren wird IPv6 auch von unterschiedlichen Mobiltelefon-Herstellern wie z.B. der Firma Nokia unterstützt, auch wenn sich dies momentan noch eher auf den asiatischen Markt bezieht.

5.2.7 Einführung durch Internet Service Provider (ISP)

In Asien ist man auch mit der allgemeinen Einführung von IPv6 bei den verschiedenen ISP's deutlich weiter als in Europa. Hier werden schon sehr viele kommerzielle Dienste unter Verwendung von IPv6 angeboten. Dies ist zum einen darauf zurückzuführen, daß die Einführung besonders in den Ländern Japan und Nordkorea von deren Regierungen unterstützt und es sogar zur Auflage gemacht wird, daß die dortigen ISP's bis 2005 die Fähigkeit besitzen müssen, IPv6-Dienste anzubieten.

Zum anderen läßt sich an dieser Stelle erwähnen, daß eine ungleiche Aufteilung des IP-Adreßraums von IPv4 auf der Welt vorliegt. So stehen einem Land wie China weniger IPv4-Adressen zur Verfügung als etwa dem MIT oder der Firma Genuity, einem Anbieter für IP-basierte Netzwerkdienste, in den Vereinigten Staaten.

Als im Grunde genommen erster ISP, der bereits im April 2000[17] IPv6 in kommerziellen Internet-Diensten unterstützte, ist NTT/Verio zu nennen, der mit seinem „NTT/Verio Global Backbone“ bereits in deutlichen Ansätzen, wiederum in erster Linie in Asien, eine Infrastruktur für kommerzielle Angebote geschaffen hat. In diesem Zusammenhang läßt sich noch erwähnen, daß NTT bereits angekündigt hat, Ende diesen Jahres als erster ISP auch in Nordamerika kommerzielle Dienste unter Nutzung von IPv6 verfügbar zu machen. Der Grund für diesen recht späten Ansatz ist die Tatsache, daß der Regierung, den Universitäten und Organisationen der USA 74 Prozent aller IPv4-Adressen zur Verfügung stehen.[7]

In Europa findet zumindest eine relativ ausgiebige Nutzung von Forschungs- bzw. Testnetzen wie dem 6bone statt. Aber auch wenige kommerzielle IPv6-Dienste werden in Europa unter anderem ebenfalls durch NTT bereits angeboten, wobei z.B. die Unterstützung der EU durch eine Vielzahl von Projekten weiter zunimmt. Hierbei spielt sicher auch die Ankündigung, die Infrastruktur ihres Computernetzes, d.h. ihrer einzelnen Behörden und Ämter auf IPv6 umzustellen, eine Rolle. Allgemein nimmt die Zahl der Ankündigungen von bevorstehenden Umstellungen stetig zu. Hier lassen sich z.B. auch der Ankündigung für die Computernetze der Bundeswehr der Bundesrepublik Deutschland oder der Streitkräfte der Vereinigten Staaten von Amerika nennen.

5.2.7.1 Folgerung

Insgesamt gesehen, steht auf der Hardware-Seite einer zügigen Einführung von IPv6 nichts mehr im Wege, während die einzelnen ISP's sicherlich auf dem Weg der Umstellung sind, wenn auch eine weitreichende Einführung hier noch nicht erkennbar ist.

5.3 E-Commerce

Eine sehr kurze Begriffsklärung zu E-Commerce wurde bereits in der Einleitung gegeben. Um den folgenden Abschnitt besser einordnen zu können, werden hier die wichtigsten Aspekte bzw. Ausprägungen des E-Commerce genannt, die für die vorliegende Arbeit relevant sind.

So geht es zum einen um die C2C- und B2C-Bereiche, bei denen zwischen den teilnehmenden Parteien in erster Linie über das Internet z.B. Waren oder Dienstleistungen angeboten und nach dem Aushandeln und Abschließen von Kaufverträgen schließlich ver- bzw. gekauft werden. Vor allem geht es hier auch darum die komplette Abwicklung eines Einkaufs über das Internet bzw. das E-Commerce-Portal eines Unternehmens abzuwickeln, wozu eben auch die Bezahlung der Waren bzw. Dienstleistungen zählt. Hierbei werden Daten wie z.B. allgemeine Bankverbindungen mit Kontonummern oder Kreditkartendaten übermittelt. Zu diesem Bereich lassen sich die vielen Internet-Shops und Internet-Auktionshäuser zählen.

Zum anderen geht es um den Bereich des B2B, bei dem es unter Nutzung des Internets z.B. um allgemeine Auftragsabwicklungen, von der Anfrage für Waren oder Dienstleistungen über konkrete Bestellungen bis hin zum endgültigen Vertragsabschluß bzw. Kauf der Waren oder Dienstleistungen, zwischen größeren Firmen und deren Zulieferern bzw. allgemein zwischen einzelnen Firmen geht. Des weiteren erfolgen in diesem Bereich auch z.B. die verteilte Bearbeitung von Projekten und allgemein die Übertragung von unterschiedlichsten Unternehmensdaten über das Internet. Für die vorliegende Arbeit ist auch die Kommunikation bzw. der Datenaustausch von z.B. Strategien, Projekten und Mitarbeiterdaten zwischen einzelnen Zweigstellen einer Firma über das Internet relevant, wodurch dies für die folgenden Abschnitte ebenfalls dem Bereich des B2B zugeordnet wird.

Insgesamt geht es also vor allem um Transaktionen und um vertrauliche Daten, die u.a. über das Internet abgewickelt bzw. übertragen werden.

5.3.1 Sicherheit

Besonders Sicherheitsaspekte besitzen im Bereich des E-Commerce eine hohe Relevanz, gerade wenn es darum geht Computernetze in diesem Bereich zu erweitern oder zu verändern.

Durch die wenn auch langsame Einführung von IPv6 mit der integrierten IPSec stellt sich nun die Frage, wie die Sicherheitsanforderungen des E-Commerce konkret aussehen und in

wie weit diese eben nach der Umstellung auf IPv6 auf IP-Ebene realisiert werden können. Zunächst also zu den einzelnen essentiellen Anforderungen, die hier vorliegen[17]:

Vertraulichkeit Die Vertraulichkeit beschreibt die Anforderung, daß nur diejenigen Personen an einer Kommunikation teilnehmen dürfen, die hierzu bestimmt waren, d.h. eine konkrete Transaktion durchführen wollten. So darf ein Dritter nichts mit evtl. abgefangenen Daten anfangen können. In diesem Zusammenhang lassen sich Daten wie Passworte, Kontodaten, Kreditkartennummern, aber auch allgemein private Daten oder Dokumente über Entwicklungen, Strategien und Geschäftsprozesse einer Firma nennen.

Authentizität Die Authentizität gibt die Sicherheit, daß bei einer Kommunikation jeder Teilnehmer die Gewißheit haben kann, daß sein Kommunikationspartner auch derjenige ist, der er vorgibt zu sein, und mit dem er ursprünglich kommunizieren bzw. Transaktionen abwickeln wollte. Somit darf also keine Möglichkeit bestehen, die Identität des Senders zu verändern bzw. zu fälschen.

Integrität Durch die Forderung der Integrität soll gewährleistet sein, daß allgemein die übertragenen Daten z.B. bei Transaktionen nicht modifiziert und somit gefälscht werden können, ohne daß dies durch den Empfänger der Daten sichtbar wird. Hierbei geht es nicht unbedingt darum, die Möglichkeit zu schaffen, die ursprünglichen Daten wieder zu rekonstruieren, sondern vor allem die Modifikation zu erkennen, damit die Daten als ungültig deklariert und verworfen werden können.

Verbindlichkeit Als letzte Sicherheitsanforderung des E-Commerce läßt sich die Verbindlichkeit nennen. So darf keiner der Kommunikationspartner die Teilnahme an der erfolgten Kommunikation und somit an einer möglicherweise vorgenommenen Transaktion abstreiten können. In diesem Zusammenhang muß also sowohl die Identität der Kommunikationspartner eindeutig bestimmbar als auch die entsprechende Transaktion belegbar sein.

5.3.1.1 Erfüllung der Anforderungen

Grundsätzlich scheinen die aufgeführten Sicherheitsanforderungen durch zwei grundlegende Aspekte der IT-Sicherheit gewährleistet werden zu können. Hierbei handelt es sich zum einen um eine verläßliche Authentisierung der Teilnehmer einer Kommunikationsverbindung und zum anderen um die Verwendung von sicheren Verschlüsselungsalgorithmen.

Kommen wir nun dazu, welche dieser Anforderungen durch IPSec erfüllt werden können, ohne eine Garantie für die Erfüllung zu geben, da IPSec noch nicht in dem Maße eingesetzt wird, daß sich bereits Möglichkeiten des Umgehens der unterschiedlichen Sicherheitsmechanismen gezeigt haben konnten.

Während die Anforderungen der Authentizität und der Verbindlichkeit, d.h. der Nicht-Abstreitbarkeit gesendeter Daten, durch den Authentication Header umgesetzt werden, kann die Vertraulichkeit der Daten und des Datenflußes durch den Encapsulating Security Payload Header gewährleistet werden, sofern man sich zu Beginn der Kommunikation auf

einen konkreten Algorithmus einigen konnte bzw. einen der Standardalgorithmen für die konkrete Verbindung akzeptiert.
Bei der Umsetzung von Verbindlichkeit gibt es allerdings die Voraussetzung, daß alle Datenpakete einer Kommunikation den jeweiligen Empfänger auch erreicht haben. Des Weiteren ist hier von Interesse, wer unabhängig genug ist, eine entsprechend vorgenommene Transaktion wirklich zu belegen.
Um den Schutz der Integrität der gesendeten Daten zu realisieren, können sowohl der eine als auch der andere Extension Header genutzt werden, da bei beiden verschlüsselte Prüfsummen gebildet werden bzw. gebildet werden können. Jedoch bezieht sich dieser Schutz lediglich auf die Erkennung einer Integritätsverletzung und nicht auf die Wiederherstellung der möglicherweise verletzten Integrität gesendeter IP-Datagramme.

5.3.1.2 Vorteile durch IPv6

Als Vorteil von IPv6 mit IPSec, der sich nun in Beziehung zur Sicherheit im E-Commerce ergibt, läßt sich zum einen die Tatsache nennen, daß nun eine sichere Punkt-zu-Punkt-Verbindung auf IP-Ebene möglich ist.
Somit ergibt sich zum anderen auch ein im Endeffekt geringerer administrativer Aufwand, was eigentlich auch der entscheidendere Vorteil ist, da eine sichere Kommunikation auch bisher durch andere Mechanismen bereits möglich war und ist. Dieser geringere Administrationsaufwand läßt sich wiederum auf die Tatsache zurückführen, daß lediglich zu Beginn der Einführung ein enormer Aufwand auf IP-Ebene entsteht, um IPSec für unterschiedliche Verbindungen korrekt zu konfigurieren, wobei eben auch wie bereits genannt, eine verläßliche globale Struktur zur Schlüsselvergabe und Schlüsselverwaltung notwendig ist, während danach der bisherige Administrationsaufwand für Sicherheitsmechanismen auf anderen Ebenen, wie z.B. der Applikationsebene, entfällt bzw. sich stark verringert. Des Weiteren müssen die Endbenutzer auch nicht auf diese Sicherheitsmechanismen geschult werden.
Natürlich kann man die bestehenden Sicherheitsmechanismen auch weiterhin beibehalten, um eine erhöhte Gesamtsicherheit zu erhalten, wobei die Beibehaltung sowieso so lange nötig ist, wie eine komplette Umstellung auf IPv6 nicht erfolgt ist.

5.3.1.3 Nachteile durch IPv6

Neben den beschriebenen Vorteilen können sich aber auch Nachteile im Bezug zu Sicherheitsaspekten ergeben, die jedoch nicht unmittelbar auf die neue Protokollversion zurückzuführen sind, sondern unter Umständen fehlerhafte Implementierungen oder schlechte Administration durch fehlendes Know-How als Ursache haben.

5.3.1.4 Folgerung

Außer den Kosten und dem Zeitaufwand der Einführung von IPv6 ist für E-Commerce Unternehmen also nun auch der Typ ihres Business entscheidend, da sicherlich die Neigung eher dazu vorliegt, sich mit der Migration von IPv6 zu beschäftigen, Testnetze zu

nutzen und Projekte zu verfolgen bzw. aktiv zu unterstützen, wenn ein erhöhtes Maß an Sicherheit für dieses Business notwendig und damit auch der Administrationsaufwand in diesem Bereich enorm ist.
Hingegen sehen kleinere Unternehmen des E-Commerce einen sicherlich eher geringen Nutzen, da ihnen bisherige Sicherheitsmechanismen wie z.B. SSL völlig ausreichen und sie somit den zu erwartenden Aufwand als nicht gerechtfertigt erachten. Dies ist für solche Unternehmen zumindest so lange der Fall, wie eine komplette Umstellung von Computernetzen auf IPv6 nicht unmittelbar in Sicht ist.

5.3.2 Betriebssysteme und Applikationen

Im folgenden soll ein kurzer Überblick geschaffen werden, in wie weit die Einführung von IPv6 auf Applikationsebene bereits fortgeschritten ist, da auf Hardware-Ebene, wie bereits betrachtet, einer zügigen Umstellung auf IPv6 nichts im Wege steht.

5.3.2.1 Betriebssysteme

Um die Applikationsebene zu beleuchten, ist zunächst der Blick auf die bereits vorgenommene Implementierungen von IPv6 in einzelnen Betriebssystemen wichtig, wobei man sagen kann, daß IPv6 bereits für alle gängigen Betriebssysteme implementiert ist.
Zu diesen Betriebssystemen gehören die unterschiedlichen Distributionen von BSD, wie z.B. NetBSD, FreeBSD oder OpenBSD, bei dem eine vollständige IPv6-Kompatibilität bereits seit Version 2.7. vorliegt. Dies ist weitestgehend dem so genannten KAME-Projekt zu verdanken. Entsprechend dem KAME-Projekt bei BSD ist das USAGI-Projekt im Zusammenhang mit den unterschiedlichen Linux-Distributionen zu nennen, die ebenfalls alle in ihren aktuellen Kernel-Versionen IPv6 unterstützen. Für genauere Informationen zu den entsprechenden Kernel-Versionen wird auf Kapitel 1, „Networking with Linux – Technology and Market“ verwiesen.
Des Weiteren gehören zu diesen Betriebssystemen Microsoft Windows XP ab Service Pack 1 und Windows 2003, bei denen die Implementierungen in Produktionsqualität vorliegen, während für Windows 2000 eine Aktualisierung zur Unterstützung von IPv6 lediglich zu Testzwecken vorgenommen werden sollte.
Bei Apple's Mac OS liegt die standardmäßige Unterstützung seit der Version 10.2 „Jaguar“ vor.
Zu der begonnenen Liste von Betriebssystemen läßt sich auch Solaris von SUN Microsystems hinzufügen, dessen Version 7 bereits den Prototypen einer IPv6-Implementierung besaß, und die in den Versionen 8 und 9 nun Produktionsqualität besitzt.
Außer den bereits genannten sind am Rande noch die Betriebssysteme IBM AIX, HP-UX und OpenVMS von HP/Compaq/DEC zu erwähnen.[8]

5.3.2.2 Grundlegende Applikationen

Nach diesem Blick auf die unterschiedlichen Betriebssysteme sollen nun grundlegende Arten von Client- und Serverapplikationen betrachtet werden, ohne auf konkrete Programme

einzugehen, da hier nur ein allgemeiner Überblick notwendig ist, um den aktuellen Stand von IPv6-Implementierungen zu verdeutlichen. Zu diesen Arten von Applikationen werden an dieser Stelle Programme, wie z.B. Ping oder Traceroute, Telnet-, SSH-, FTP- und E-Mail-Clients und Server und die unterschiedlichen Webbrowser, die den meisten Betriebssystemen beiliegen bzw. in den einzelnen Betriebssystem-Distributionen enthalten sind, gezählt.

Genau wie im Bereich der Betriebssysteme läßt sich auch hier die durchgängige Unterstützung des neuen Internetprotokolls verzeichnen.[9] Dies ist aber nicht nur für diese grundlegenden Applikationen der Fall, sondern auch für Voice-over-IP-, Streaming-Software und vor allem für Web-Server, wie z.B. von Apache ab der Version 2.0 und den Microsoft IIS 6.0 (jeweils in Produktionsqualität).

5.3.2.3 Spezielle Applikationen

Aufgrund der Tatsache, daß keine konkreten Hinweise auf spezielle E-Commerce-Applikationen, wie z.B. für Portale im Internet, bezüglich Transaktionsunterstützung oder Bezahlmöglichkeiten, im Rahmen dieser Arbeit gefunden werden konnten, muß jedoch davon ausgegangen werden, daß gerade in diesem Bereich noch ein sehr großer Nachholbedarf besteht.

5.3.2.4 Folgerung

Zusammenfassend ergeben sich aber dennoch weder auf Betriebssystemebene noch im Bereich der grundlegenden Netzwerk-Applikationen Hinderungsgründe für eine zügige Transition zu IPv6, wobei man sich hier auf die Möglichkeit der technische Realisierung beschränkt und die anfallenden Investitionskosten außer acht läßt.

Es scheint nur offensichtlich so zu sein, daß die Software-Hersteller spezieller Applikationen auf eine umfangreiche Infrastruktur, d.h. in erster Linie auf die ISP's, die sich wenn überhaupt erst am Beginn einer Umstellung befinden, warten, während diese aufgrund der enormen Kosten und des enormen Zeitaufwands erst noch auf eine deutlich erhöhte Nachfrage durch die Internet-Nutzer, im besonderen auch durch größere Firmen, warten. Gleichzeitig fragt man sich natürlich als Entscheidungsträger einer Firma im Bereich des E-Commerce, in wie weit eine etwaige IPv6-Infrastruktur durch bestehende Software-Produkte genutzt wird. Dieses Szenario kann durchaus als einer der Gründe für die zögerliche Verbreitung von kommerziellen IPv6-Diensten gesehen werden.

5.3.3 Zusammenarbeit von IPSec mit Firewalls

In diesem Abschnitt soll verdeutlicht werden, in wie weit eine Zusammenarbeit von dem in IPv6 enthaltenen IPSec mit Firewalls sowohl möglich als auch sinnvoll ist, um die durch eine Firewall gewährleisteten Sicherheitsaspekte zu erweitern, ohne an dieser Stelle die Funktionalität einer Firewall zu erläutern und wobei eine Ersetzung weder gewollt noch möglich ist.

So wird bei dieser Erweiterung der Sicherheitsaspekte sowohl der Authentication Header als auch der Encapsulating Security Payload Header und zwar unter Verwendung des Tunnel-Modus genutzt. Aufgrund dieser Erweiterung können die folgenden Probleme, die bei der ausschließlichen Verwendung einer Firewall durch fehlende Sicherheitsmechanismen bei dem Versenden von IP-Datagrammen auftreten, gelöst werden[4]:

Abhören von Daten Dieses Problem bezieht sich zum einen auf Daten, mit deren Hilfe weitere Angriffe geführt werden können, wie z.B. Informationen über Accounts, Paßworte oder Kontodaten, zum anderen aber auch auf geheimzuhaltende Firmendaten, wie z.B. über Strategien oder Geschäftsprozesse.

IP-Spoofing Bei einem solchen Angriff werden Tools eingesetzt, um IP-Pakete mit gefälschten Absender-Adressen zu generieren, um sich somit Privilegien zu erschleichen, sofern die Absender-Adressen der Authentisierung oder Zugriffskontrolle dienen.

TCP-Hijacking Ziel eines solchen Angriffs ist es, eine von einem berechtigten Benutzer aufgebaute Verbindung zu einem Zeitpunkt nach dessen Authentisierung zu übernehmen, was bei einer verschlüsselten Datenübertragung nicht möglich ist.

5.3.3.1 Virtual Private Networks

Im Grunde genommen entsteht bei dieser Zusammenarbeit somit ein Virtual Private Network (VPN). Durch ein solches VPN kann also eine sichere Vernetzung von Firmen und Zweigstellen, was besonders im Bereich des Business-to-Business große Relevanz besitzt, und auch die sichere Anbindung von entfernten Endbenutzern, wie Heimarbeitern oder Vertretern, was zumindest für alle größeren Firmen ebenfalls von Bedeutung ist, vorgenommen werden. Bei solchen VPN's wurde bisher ein ähnliches Verfahren, also unter Verwendung einer Firewall mit dem zusätzlichen Verschlüsseln der Daten und dem Tunneln der IP-Pakete, genutzt.

Nun stellt sich aber die Frage, warum die Zusammenarbeit von IPSec mit Firewalls einer bereits bestehenden Lösung vorzuziehen ist. Als Antwort auf diese Frage lassen sich mehrere Gründe nennen. Zum einen kann die spezielle Implementierung von IPSec in Firewalls und Routern eine erhöhte Sicherheit bei der Übertragung von Daten ermöglichen, ohne daß ein Performance-Verlust auftritt oder eine spezielle Konfiguration der einzelnen Clients erforderlich ist. Zum anderen sind die bisherigen Implementierungen des entsprechenden Verfahrens nicht immer interoperabel, was im Grunde genommen das größte Problem darstellt, während man sich bei IPSec immer noch auf einen der Standards bei den Verschlüsselungsalgorithmen einigen kann. Des Weiteren gibt es in einigen Ländern, wie unter anderem den USA, Exportbeschränkungen für kryptographische Anwendungen, wodurch sich für Firmen mit Zweigstellen oder anzubindenden Mitarbeitern in anderen Ländern Probleme ergeben konnten, was mit einer einheitlichen IPv6 Infrastruktur nicht mehr der Fall wäre.

5.4 Schlußbemerkungen

Zum Schluß dieser Arbeit läßt sich erkennen, daß der Einzug von IPv6 in Computernetzen bereits begonnen hat bzw. die Möglichkeit besteht, eine IPv6-Infrastruktur ohne technische Probleme aufzubauen und somit zu realisieren. Außerdem nimmt die Einführung von IPv6 zwangsläufig Einfluß auf die verschiedensten Bereiche, so auch auf den Bereich des E-Commerce.

Es stellt sich aber nun die Frage, was die Gründe für eine im allgemeinen doch eher langsame Umstellung auf das neue Internetprotokoll sind, da schließlich die Implementierung in Hardware, in Betriebssystemen und grundlegenden Netzwerkapplikationen in ausreichendem Maße vorhanden ist. Hier stehen verständlicherweise die Kosten und der Aufwand an erster Stelle, gefolgt von der Tatsache, daß nur eine sehr geringe Anzahl an Applikationen, die speziell auf den Bereich des E-Commerce zugeschnitten sind und die Vorteile von IPv6 konkret nutzen, vorhanden ist.
Um die anfallenden Kosten und den Aufwand für ISP's und E-Commerce-Anbieter nochmals genauer zu benennen, lassen sich hier Weiterbildung der Mitarbeiter, in erster Linie der Systemadministratoren, Planung einer umfassenden Migrationsstrategie für das eigene Intranet und dessen Anbindung ans Internet, Anschaffung neuer Hard- und Software und ein wenigstens zu Beginn sehr viel höherer Administrationsaufwand erwähnen.
Die so entstehenden Investitionskosten und der mit der Umstellung verbundene Aufwand läßt sich im Hinblick auf den gegenwärtigen konkrete Nutzen, der aufgrund einer fehlenden globalen Infrastruktur noch nicht so deutlich sichtbar wird, sehr schwer rechtfertigen, besonders wenn im allgemeinen ein enormer Konkurenzkampf zwischen z.B. einzelnen E-Commerce-Anbietern herrscht, bei dem Kostenminimierung schließlich einer der wichtigsten Punkte ist.

5.4.1 Fazit

Der Einfluß von IPv6 auf den Bereich des E-Commerce liegt nicht nur aufgrund allgemeiner Aspekte, die mit der Umstellung der Infrastruktur von Rechnernetzen auf eine neue IP-Version existieren, vor, sondern vor allem auch aufgrund der Tatsache, daß mit IPv6 zum ersten Mal Sicherheitsmechanismen auf der IP-Ebene realisiert werden und eben auf Sicherheitsmechanismen im Bereich des E-Commerce sicherlich das Hauptaugenmerk liegt.
Dennoch muß man an dieser Stelle erwähnen, daß die bisher bereits entwickelten Sicherheitsunterstützungen durch die sie enthaltenen unterschiedlichen Anwendungen an und für sich nicht schlechter sind als die in IPv6 in Form der IPSec implementierte Sicherheitsunterstützung. Auch wenn IPSec sehr viele Vorteile mit sich bringt, scheint die Einführung von IPv6 nur oder vor allem aus diesem Grund, d.h. den beschriebenen Sicherheitsaspekten, in anbetracht der damit verbundenen Kosten und des Aufwands nicht gerechtfertigt.

Der entscheidende Grund für die notwendige Einführung von IPv6, zumindest im Internet, ist somit sicherlich der aus heutiger Sicht sehr begrenzte IPv4-Adreßraum und die sich daraus ergebende Tatsache, daß der Ausbau und Unterhalt von IPv4 immer teurer und

aufwendiger wird. Dies wird vor allem deutlich, wenn man betrachtet, in welchen Regionen der Erde die Einführung von IPv6 momentan am schnellsten von statten geht. Das sind nämlich genau diejenigen Regionen, in denen ein vergleichsweise enormer Mangel an verfügbaren IP-Adressen besteht.

Um wieder auf den Einfluß, den IPv6 im Bereich des E-Commerce besitzt, zurückzukommen, läßt sich sagen, daß dieser Einfluß bzw. Nutzen höchstens im Bereich des B2B bzw. in firmeninternen Computernetzen konkret vorhanden ist, wenn z.B. VPN's mit IPv6-Netzen gebildet werden, während dies in allen anderen Bereichen nicht der Fall ist. Dies läßt sich einfach auf die Tatsache zurückführen, daß die Sicherheit nicht für alle Teilnehmer an Transaktionen auf IP-Ebene gewährleistet werden kann, da weder zum jetzigen Zeitpunkt noch in naher Zukunft eben noch nicht alle Teilnehmer auf IPv6 umgestiegen sind bzw. sein werden.
Somit müssen bis zur vollständigen Migration weiterhin die bewährten Sicherheitsmechanismen parallel genutzt werden, wodurch sich also zunächst im Bereich der Sicherheit kein wesentlicher Vorteil ergibt.

Insgesamt läßt sich die Umstellung auf IPv6 jedoch als Zukunftsinvestition und Plattform für zukünftige Dienste, die mit IPv4 nicht mehr realisiert werden können, sehen.

5.4.2 Zukunftsaussichten

Der begrenzte IPv4-Adreßraum und die damit verbundene Tatsache, daß es immer schwieriger werden wird, neue IPv4-Adressen zu erhalten, macht die Migration im Internet letztlich unumgänglich. Ein schnelleres Fortschreiten der Schaffung grundlegender globaler Infrastruktur wird vermutlich in absehbarer Zukunft erkennbar werden und damit wird auch eine schnellere Umsetzung bei Software-Produkten und im Bereich kommerzieller Dienste einhergehen.

Wenn die Einführung schließlich erst in größerem Umfang stattgefunden hat, findet auch die enthaltene IPSec stärker Verwendung und nimmt damit im Zusammenhang mit ihren bestehenden Vorteilen zwangsläufig einen größeren Einfluß vor allem auf den E-Commerce Sektor, wobei meiner Meinung nach bis 2010 eine weitgehende Verbreitung von IPv6 erfolgt sein wird.

Literaturverzeichnis

[1] Alcatel: „The Move to IPv6 – Technical Paper“, www.cid.alcatel.com/doctypes/techpaper/pdfa4/IPv6_A4_tp.pdf, 26. Oktober 2003

[2] S. Deering, R. Hinden: „Internet Protocol, Version 6 (IPv6) Specification“, www.ietf.org/rfc/rfc2460.txt, Dezember 1998

[3] N. Doraswamy, R. Glenn: „IP Security Document Roadmap“ von R. Thayer (RFC 2411), www.ietf.org/rfc/rfc2411.txt, November 1998

[4] Uwe Ellermann: „IPv6 und Firewalls“, www.cert.dfn.de/team/ue/fw/ipv6fw/, 30. Oktober 2003

[5] R. Gilligan, E. Nordmark: „Transition Mechanisms for IPv6 Hosts and Routers“ (RFC2893), www.ietf.org/rfc/rfc2893.txt, August 2000

[6] Martin Günther(V.i.S.d.P.): „e-Commerce legt weiter zu“ (GfK Web*Scope-Studie), www.gfk.de, 14. Oktober 2003

[7] Silvia Hagen: „IPv6 – Zurück zur Einfachheit“, www.oreilly.de/artikel/ipv6_1.html, 30. Oktober 2003

[8] JOIN-Projekt-Team: „IPv6 in Betriebsystemen“, www.join.uni-muenster.de/Implementationen/Betriebsysteme.php, 2. November 2003

[9] JOIN-Projekt-Team: „IPv6 in verschiedener Software“, www.join.uni-muenster.de/Implementationen/Software.php, 2. November 2003

[10] JOIN-Projekt-Team: „IPv6-Support in Routern und bei verschiedenen Herstellern“, www.join.uni-muenster.de/Implementationen/Router.php, 2. November 2003

[11] Thomas Kastner: „Einführung in IPv6 und IPSec“, www.viatec.at/install/papers/IPv6_und_IPsec.pdf, Dezember 2001

[12] S. Kent, R. Atkinson: „IP Authentication Header“ (RFC 2402), www.ietf.org/rfc/rfc2402.txt, November 1998

[13] S. Kent, R. Atkinson: „IP Encapsulating Security Payload (ESP)“ (RFC 2406), www.ietf.org/rfc/rfc2406.txt, November 1998

[14] S. Kent, R. Atkinson: „Security Architecture for the Internet Protocol“ (RFC 2401), www.ietf.org/rfc/rfc2401.txt, November 1998

[15] Kommission der Europäischen Gemeinschaften: „eEurope 2002 Auswirkungen und Prioritäten“, www.euresearch.ch/media/eEurope_Impact_Priorities_Comm_de_2002.pdf, 13. März 2001

[16] SPIEGEL Online: „Bald ist das Verzeichnis voll“, www.spiegel.de/netzwelt/technologie/0,1518,271560,00.html, 27. Oktober 2003

[17] H. Joseph Wen, J. Michael Tarn: „The Impact of the Next-Generation Internet Protocol on E-commerce Security“, www.isaca.org.au/articles/IP-ECommerce-Security.pdf, 10. Oktober 2003

Kapitel 6

Content Distribution Networks

Thomas Götzinger

Betrachtet man das Einsatzgebiet und die Verbreitung heutiger Rechnernetze vor allem des Internets, so stellt man fest, dass die Anzahl der Nutzer sowie das Einsatzspektrum sich gegenüber der Anfangszeit der Rechnernetze extrem gewandelt hat. Gerade im Bereich des Internets ist ein enormer Anstieg der Zahl an Benutzern, sowie an bereitgestelltem Inhalt zu verzeichnen. Dieser Anstieg, der eine erhöhtes Verkehrsaufkommen im Netz zur Folge hat, muss durch neue Technologien und Verfahren ausgeglichen werden, um die Leistungsfähigkeit der bestehenden Netze zu erhalten.
Eines dieser neuen Verfahren ist Content Distribution Networks (CDN). CDN versucht die Leistung eines Rechnernetzes durch Verteilung des Inhaltes auf mehrere geographisch unterschiedlich platzierten Sites zu erhöhen. Der original Server der den Inhalt bereitgestellt hat, verteilt seinen Inhalt auf mehrere sogenannte Surrogate Server, die somit im Auftrag des originalen Server den Inhalt an die anfragenden Clients verteilen können.
Jeder Client kann nun bei einer Anfrage durch bestimmte Verfahren (Client Redirection Mechanisms) zu seiner „nächsten" Site umgeleitet werden, um somit z.B. seine Antwortzeit zu reduzieren.
Bereits diese kurze Darstellung bietet Anlass für einige Fragen, die sich im Zusammenhang mit der Implementierung eines Content Distribution Networks stellen: Wie kann der anfragende Client umgeleitet werden, oder welche Verfahren erlauben eine Bestimmung der „nächsten" Site, bzw. was bedeutet überhaupt die nächste Site? Die Seminararbeit beantwortet nicht nur die eben skizzierten Fragen, sondern untersucht darüber hinaus welche Probleme durch den Einsatz von CDN's in heutigen Rechnernetzen gelöst werden können, wie CDN umgesetzt werden kann und welche zukünftige Entwicklungen im Zusammenhang mit CDN in Planung sind.

Inhaltsangabe

6.1 Einführung

6.1.1 Heutige Rechnernetze

Über die letzten Jahrzehnte hin hat das Einsatzgebiet der Rechnernetze einen großen Wandel erfahren. Blickt man in die 70'er Jahre zurück war der Bekanntheitsgrad von Rechnernetzen auf einen kleinen Teil der Bevölkerung beschränkt. Zu dieser Gruppe, die sich schon damals mit Netzwerken beschäftigte, gehörten vor allem Professoren und Wissenschaftliche Mitarbeiter von Technischen Instituten an Universitäten sowie Experten in der Wirtschaft an. Die Netze waren geographisch verstreut und das einzelne Rechnernetz war meist auch nur lokal auf die jeweilige Universität oder Firma beschränkt.
Die heutige Akzeptanz und Verbreitung der Rechnernetze steht zu der oben geschilderten Situation im völligen Kontrast. Rechnernetze haben in den Industrieländer ihren Weg bis in den kleinsten Haushalt gefunden. Neue Rechnernetze wurden errichtet und die Älteren (z.B. das Internet) haben sich zu riesigen, komplexen Netzen ausgedehnt.
Die explosive Ausdehnung der Größe, Anzahl, Komplexität und Nutzung von Rechnernetzen hat jedoch auch Konsequenzen auf die Leistung, z.B. der web-basierten Anwendungen. Nicht zu unrecht wird die Abkürzung WWW oft als „World Wide Wait" [5] interpretiert. In Abbildung 6.1 sind mögliche Gründe dieses *Slow Access Time Problems* dargestellt.

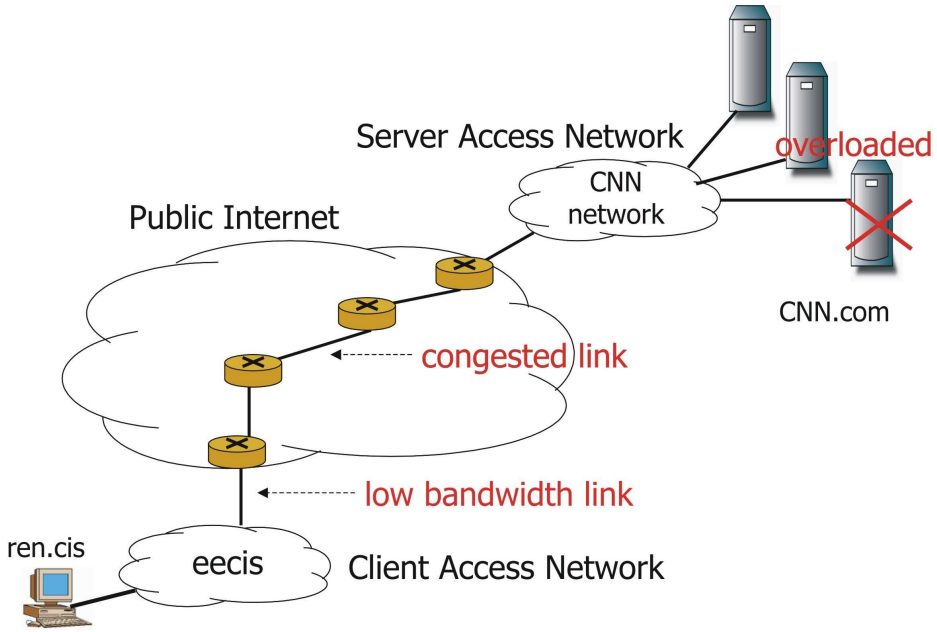

Abbildung 6.1: World Wide Wait, Quelle: [5]

In der Abbildung sind anhand eines Clients der in Verbindung mit einem Server *cnn.com* steht die Stellen im Netz beschrieben, die die Leistung negativ beeinflussen können. Neben eines überlasteten Servers kann sowohl ein verstopfter Pfad, als auch eine Verbindung mit geringer Bandbreite zu einem schlechten Antwortzeitverhalten führen.
Eine Lösung der oben dargestellten Problematik beruht in der Verteilung der Last einer Site auf mehrere im Netz beliebig verteilten Sites, durch kopieren des ganzen oder Teilen

des Inhaltes einer originalen Site auf Ausweichsites. Die einzelnen Sites können aus einem einzelnen oder mehreren Servern bestehen. Bei jeder Anfrage eines Clients an den originalen Server, wird der Client an den für ihn besten Server weitergeleitet. Diese Menge an Sites, die zur Erhöhung der Leistung der web-basierten Anwendungen dienen, bilden zusammen ein Content Distribution Network (CDN), welches Gegenstand dieser Seminararbeit ist.
Bevor eine detaillierte Betrachtung der Komponenten und Mechanismen eines Content Distribution Networks erfolgt, soll sich erst mit der Frage beschäftigt werden, warum Anwendungen aufgrund von Stau im Netz an Leistung einbüßen können. Dabei soll auch klar die Problematik herausgestellt werden, zu der CDN eine Lösung bietet. Weiterhin werden Techniken vorgestellt, die abseits von CDN versuchen die Leistung von web-basierten Anwendungen sicherzustellen. Die Techniken sollen hier jedoch nicht bis ins Detail untersucht werden, sondern es werden eher Probleme aufgezeigt, die bei ihrer Implementierung entstehen können sowie in welchen Situationen sie versagen.

6.1.2 Leistungsmerkmale in web-basierten Anwendungen

Abbildung 6.1 aus Abschnitt 6.1.1 zeigt durch ein einfaches Modell die Infrastruktur eines Netzes in der ein Client eine verteilte Applikation nutzt. Hier hat der Nutzer eine spezielle Anwendung (z.B. Web-Browser). Durch ein Client Access Network ist er mit dem Backbone Network verbunden. Das andere Ende der Verbindung bildet ein Server, der durch das Server Access Network mit dem Backbone verbunden ist. Auf dem Server befindet sich die Anwendung, auf die der Client zugreifen möchte.
Die meisten Situationen aus der alltäglichen Arbeit mit dem Internet können auf dieses einfache Modell abgebildet werden. Meist erfolgt die Kommunikation zwischen einem Nutzer und dem Server durch eine Anfrage-Antwort Beziehung. Die Antwortzeit aus Sicht des Nutzers ist die Zeit zwischen dem Generieren einer Anfrage und dem Erhalt der Antwort. Sie eignet sich sehr gut zur Feststellung der Leistungsfähigkeit einer web-basierten Anwendung. Wobei eine Anwendung dann am Leistungsfähigsten gegenüber einem Nutzer ist, wenn die Anforderung der Leistung einer Anwendung und die Anwendung selbst nicht durch den Verkehr anderer Benutzer beeinflusst wird. Diese Situation bezeichnet man als das *best-case Scenario*[1], welches als untere Schranke für die Antwortzeit dient. In der Praxis liegt die Antwortzeit über dieser Schranke. Der Grund dafür sind andere Anwendungen und Nutzer, die untereinander in Konkurrenz um die bestehende Bandbreite und Rechenkapazität stehen. Daher muss zur Erhaltung der Leistungsfähigkeit im Netz die Leistungseinbußen, die durch den eben beschriebenen Verkehr auftreten in akzeptablen Rahmen gehalten werden. Die zwei folgenden Abschnitte zeigen nun zwei verschiedene klassische Ansätze auf, die abseits von CDN versuchen die gerade beschriebenen Einbußen in gewissen Grenzen zu halten.

6.1.2.1 Capacity Planning

Durch die Kapazitätsplanung wird die Leistungsfähigkeit des Netzes dadurch sichergestellt, dass eventuell vorhandene Flaschenhälse durch neuere, leistungsfähigere Hardware schon im Vorfeld beseitigt werden. Im Zentrum dieser Lösung steht die Annahme, dass

falls eine Anwendung nicht akzeptabel arbeitet, muss mindestens ein Flaschenhals im System vorhanden sein.
Als Basis zur Durchführung der Kapazitätsplanung steht die Schätzung der Systemlast. Falls für jede Verbindung innerhalb des Netzes die Last hinreichend genau vorausgesagt werden kann, ist die Installation eines neuen Links mit ausreichender Kapazität möglich. Ähnliches gilt dies für die Last eines Servers oder einer Serverfarm. Gibt es zu jeder Anwendung eine Schätzung über den Verbrauch an Ressourcen des Servers, so kann eine Maschine installiert werden, die die Last adequat bewältigen kann. Die Kapazitätsplanung stellt die geforderte Leistung jedoch nur sicher, solange der Anstieg an Bandbreite bzw. Serverlast mit Sicherheit vorausgesagt werden kann. Ist diese Voraussetzung erfüllt und wird gemäß diesen Voraussagen genügend Bandbreite und Rechenkapazität bereitgestellt, können fast alle Anwendungen eine Leistung nahe dem best-case Scenario erbringen.
Die Effizienz der Kapazitätsplanung hängt sehr stark von der Genauigkeit der Abschätzung der Systemlast ab. Diese starke Abhängigkeit führt dazu, dass in Systemen mit großen, nicht vorhersagbaren Lastschwankungen ein hohes Leistungsniveau durch Kapazitätsplanung nicht mit Sicherheit gewährleistet werden kann oder um die Leistungsfähigkeit doch zu garantieren das System stark überdimensioniert werden muss. Eine weiterer nicht unerheblicher Einfluss auf die Effektivität dieses Ansatzes ist die Varianz der Systemlast. Meist basieren die Voraussagen auf der Durchschnittslast. Jedoch kann die Last abhängig von Tageszeit oder Wochentag sehr starken Schwankungen unterliegen. Beispielsweise hat ein Liveticker zur 1. Fussballbundesliga ihre Spitzenzeiten während den Spielzeiten am Wochenende, außerhalb dieser Zeiten ist die Last sehr gering. In Abbildung 6.2 wird dies verdeutlicht indem die Lasten zweier verschiedener Server aufgetragen sind.
Die Lasten beider Server haben ungefähr den gleichen Durchschnittswert. Würde man

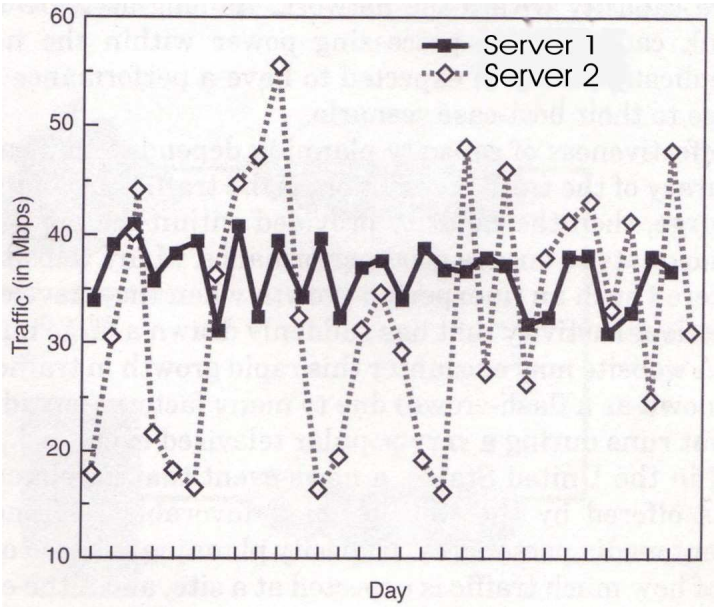

Abbildung 6.2: Unterschiedliche Lastschwankungen zweier Server

die Rechenleistung des Servers abhängig von der mittleren Ankunftsrate der Anfragen machen, so hätten beide die gleiche Leistung. Dies würde aber dazu führen, dass Server 2 viel häufiger als Server 1 seine Last nicht bewältigen könnte. Eine Lösung dieses Problems

wäre die Varianz der Last bei der Planung mit einzubeziehen. Ein Beispiel wäre eine 90% Hürde, d.h. man wähle die Verbindung bzw. den Knoten so, dass 90% der geschätzten Last unter der gewählten Leistungsfähigkeit liegt. Somit muss nur in wirklichen Spitzenzeiten mit Leistungseinbußen gerechnet werden. Im Beispiel der obigen Abbildung würde Server 2 somit eine höhere Rechenleistung zustehen als Server 1.
Kapazitätsplanung ist somit eine Technik die nur dann effizient arbeitet, falls die Umgebung in der sie eingesetzt wird wenigen Lastschwankungen unterliegt. Sie kann sehr ineffizient sein, falls die Wahrscheinlichkeit für die Richtigkeit der Prognose sehr klein ist. Durch den Preisverfall für Hochgeschwindigkeitsroutern wird die Kapazitätsplanung für den Internet-Core, trotz einer Ineffizienz aufgrund der Überdimensionierung der Links, vorwiegend zur Erhaltung der Leistungsfähigkeit eingesetzt. Jedoch sind Probleme der Kapazitätsplanung im Zusammenhang mit der Infrastruktur des Internets nicht komplett zu vermeiden. Denn das schnellste Internet-Core nützt zur Erhaltung der Leistungsfähigkeit wenig, wenn der Knoten zum Access Network verstopft ist. Somit lässt sich hier abschließend bemerken, dass alle Maßnahmen der Kapazitätsplanung, beruhen diese auch auf richtigen Prognosen, sich kaum positiv auf das Antwortzeitverhalten auswirken, falls die Verbindung an anderer Stelle sehr stark belegt ist.

6.1.2.2 Quality of Service

Quality of Service(QoS) basiert auf der Annahme, dass es zu wenig Ressourcen im Netz gibt. Auch wenn heute die Anzahl an installierten Ressourcen die benötigte Menge um ein Vielfaches übersteigt, auf lange Sicht werden diese durch das Aufkommen von neuen Applikationen, neuen Nutzern oder durch ein Ansteigen der benötigten Bandbreite der derzeitigen Nutzern komplett in Anspruch genommen. Diese Ressourcenknappheit führt jedoch dazu, dass es nicht mehr möglich ist jedem im Netz aktiven *Datenfluss*[1] genügend Ressourcen zur Verfügung zu stellen. Quality of Service versucht nun die Leistung einiger im Bezug auf Verzögerung und Bandbreite sehr empfindlichen Datenflüssen auf Kosten der Leistung anderer zu erhalten. Es gibt zwei auch in der Praxis anerkannte Lösungsansätze.
Der erste Ansatz, als *Reservation Approach* bezeichnet, versucht die Leistungsfähigkeit des Netzes dadurch zu erhalten, indem die Anwendungen das Netz informieren wieviel Ressourcen sie benötigen um eine ausreichende Qualität sicherzustellen. Die Information des Netzwerks wird durch ein Signalisierungsprotokoll durchgeführt. Der Signalisierungsprozess sendet Informationen mit dem Ressourcenbedarf an alle die Knoten, die an der Übertragung beteiligt sind. Nur wenn alle benachrichtigten Knoten ein positives Signal über die Reservierung der Ressourcen zurücksenden, kann die Übertragung beginnen. Der einerseits positiven Seite der Leistungsgarantien der einzelnen Datenflüsse steht jedoch ein großes Problem bei der Implementierung des Reservation Approach gegenüber. Die Signalisierungsprozesse sind sehr komplex und ineffizient, vor allem wenn alle Fehlersituationen wie Nachrichtenverlust oder Routenänderung mit berücksichtigt werden. Ein weiteres Problem entsteht bei verbindungslosen Netzarchitekturen wie IP, da es hier sehr schwierig ist an jedem Knoten die Pakete zu ihren zugehörigen Datenflüsse in Beziehung zu setzen.

[1] Datenfluss engl. Traffic flow

Die zweite Umsetzung von QoS ist der *Class Differentiation Approach*, der im Gegensatz zum Reservation Approach kein Signalisierungsprozess benötigt. Hier werden alle Datenflüsse in Klassen eingeteilt. Die Klassenzugehörigkeit wird mit in das Paket kodiert. Weiterhin wird zu jeder Klasse eine bestimmte Ressourcenmenge assoziiert. Jeder Switch kann dann anhand der Klasse des eintreffenden Paketes entscheiden wieviel Ressourcen das Paket erhält. Eine einfache Implementierung dieses Ansatzes sind Rechnernetze die zwei oder mehr Prioritätsklassen anbieten. Besteht Stau in einer Netzverbindung so wird die Leistung der höherprioritären Klasse weniger beeinträchtigt als die der niederen Klasse. Im Vergleich zum Reservation Approach ist diese Lösung einfacher, jedoch können durch die Bildung von Klassen keine harten Garantien für die Leistung der einzelnen Datenflüsse gegeben werden. Auch die Datenflüsse der höchstprioritären Klasse können, falls zu viele der hochprioritärer Klassen gleichzeitig aktiv sind einem Stau innerhalb des Netzes ausgesetzt sein.
Das Hauptproblem beider Ansätze das einer Verbreitung der QoS Architektur in IP-Netze gegenübersteht ist, dass eine Änderung der bestehenden Infrastruktur dieser Rechnernetze notwendig wäre. Jeder Router müsste die Reservierung oder Servicedifferenzierung unterstützen, um effektiv arbeiten zu können. Gerade im Hinblick auf die Anzahl der Router, die in der Infrastruktur des Internets installiert sind, wären die damit verbundenen Kosten enorm. Weiterhin stellt sich im Internet die Frage welche Flows bevorzugt werden sollen. Da gerade die Antwortzeit für einen Content Provider[2] eine Rolle im Hinblick auf Download- bzw. Zugriffszahl seines angebotenen Inhalts spielt, ist jeder der Provider daran interessiert eine möglichst gute Verbindung innerhalb des Internets zu erhalten. Bei der Betrachtung der Vielzahl von Domains, die zusammen das Internet bilden und welche jeweils einer eigenen Administration unterliegen, entsteht ein weiteres Problem für den QoS Ansatz. Die Präferenz einiger Datenflüsse gegenüber anderer muss über die Grenze der Domains hinweg gewährleistet werden, was zu Absprachen zwischen diesen führen müsste.

6.2 CDN - Overview

Der Blickpunkt der oben erläuterten Techniken liegt bei der Kapazitätsplanung auf den Prognosen, bei Quality of Service in der Sicherung der Dienstgüte bei enstandenen Flaschenhälsen. Ist jedoch ein Teilpfad zwischen Client und Server blockiert, wird dieser Pfad bei beiden Techniken beibehalten. Die in Abbildung 6.1 dargestellten drei Hauptprobleme während einer Client-Server Verbindung können durch die beiden Techniken nicht alle gelöst werden, denn keine der beiden Ansätze löst das Problem des belasteten Teilpfades. Obwohl QoS sich diesem Problem bemächtigt, kann dieser Ansatz wie oben erwähnt in bestimmten Situationen versagen. Eine weitverbreitete Lösung um den Weg zwischen Client und Server innerhalb des Internets zu entlasten ist mit Hilfe eines sogenannten *Proxy*. Dieser Ansatz soll im folgenden Abschnitt erläutert werden.

[2]Content Provider: Jede selbständige Organisation, oder Firma die Inhalte für die Benutzer des Netzwerks bereitstellt [5].

6.2.1 Proxy

Ein Proxy-Server „ist eine Netzwerkeinheit, die HTTP-Anfragen im Auftrag eines Client erfüllt“[2]. Jeder Proxy hat einen eigenen Speicher, in dem er Kopien der zuletzt angefragten Objekte verwaltet. Der Ablauf einer HTTP-Anfrage unter Verwendung eines Proxies sieht dann wie folgt aus:

1. Der Browser beim Client baut eine TCP-Verbindung zum Web-Cache auf und sendet eine HTTP-Anfrage für das Objekt an den Proxy.

2. Der Proxy prüft, ob sich eine Kopie des angeforderten Objektes in seinem Speicher befindet. Falls ja, wird das Objekt durch eine HTTP-Antwortnachricht an den Client gesendet. Dieser Fall wird auch als *Cache-Hit* bezeichnet

3. Befindet sich keine Kopie des angeforderten Objektes im Speicher des Proxies (*Cache-Miss*), so sendet dieser eine HTTP-Anfrage über eine TCP-Verbindung an den eigentlichen Content Server[3].

4. Nach erhalten dieser Nachricht sendet der Content Server das Objekt als HTTP-Antwort an den Proxy zurück.

5. Wenn der Proxy das Objekt erhält, speichert dieser zuerst eine Kopie in seinem Speicherbereich und sendet anschließend im Rahmen einer HTTP-Antwort eine Kopie des Objektes an den Client.

In Abbildung 6.3 wird der oben beschriebene Ablauf schematisch dargestellt.

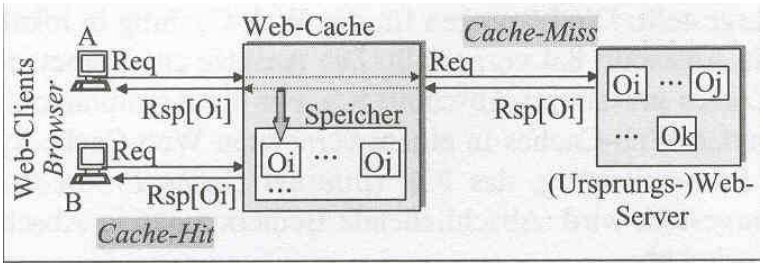

Abbildung 6.3: Aufgabe eines Proxies, O_i, O_j, O_k:Daten-Objekte; Req: HTTP-Request; Resp: HTTP-Response, Quelle: [3]

Bei der Betrachtung der eben referenzierten Abbildung stellen sich folgende Fragen: Welchen Vorteil bietet solch eine Struktur und an welcher Stelle sollte ein Proxy installiert werden um den Gewinn an Leistung zu maximieren.
Der Vorteil der Installation eines Proxy Servers ist eng verknüpft mit Punkt 2 der obigen Aufzählung. Falls sich ein Objekt bereits im Cache befindet, kann dieses vom Proxy Server geliefert werden. Befindet sich der Proxy näher beim Client als der Content Server, so wird das Antwortzeitverhalten beim Client verbessert. Weiterhin wirkt dieser Ansatz

[3]Content Server: Server einer Organisation, Firma, usw. die Daten für die Nutzer des Netzes bereitstellt

einer Bandbreitenverschwendung entgegen, da die Pakete nicht den kompletten Weg zwischen Client und Server bewältigen müssen. Durch die genannte Vorteile bzw. Ziele der Installation eines Proxies werden auch die Bereiche in denen dieser installiert werden sollte, bereits ziemlich eingegrenzt. In den folgenden zwei Abschnitten werden 2 verschiedene Lösungsmöglichkeiten [4] vorgestellt, die sich mit der Frage nach dem Standort eines Proxy Servers beschäftigen.

6.2.1.1 Reverse Proxy

Ein Proxy Server wird als *Reverse Proxy Server* bezeichnet, falls er im Umfeld eines Content Servers installiert ist und diesem als Web-Cache dient. Die Aufgabe des Reverse Proxies ist den anfragenden Clients, die sich außerhalb einer Domain, z.B. UniBw-Muenchen.de befinden, Inhalt eines Servers in dieser Domain, z.B. von www.UniBw-Muenchen.de zu liefern. Abbildung 6.4 veranschaulicht das Konzept.

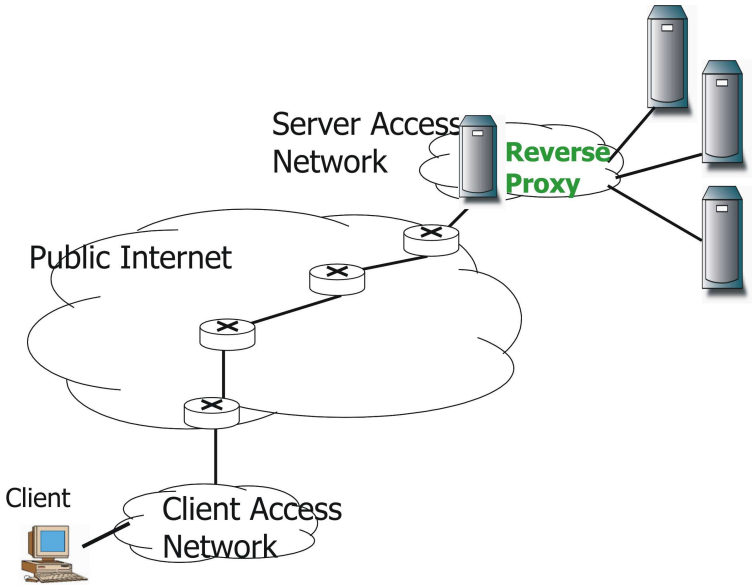

Abbildung 6.4: Reverse Proxy

Es gibt zwei mögliche Installationsorte für den Reverse Proxy. Der erste liegt serverseitig des Access Point zwischen Server Access Network und Backbone Network, der zweite auf Seiten des Backbone-Networks der eben skizzierten Stelle.
Durch eine serverseitige Lösung können Inhalte zwischen dem Proxy und den dahinterliegenden Content Servern durch eine eventuell vorhandene breitbandige Verbindung schnell ausgetauscht werden und somit auch Objekte die sich nicht im Speicher befinden schnell angefordert werden. Zum anderen werden bei beiden Umsetzungen die Content Server durch die gestiegene Gesamtrechenleistung entlastet. Ein weiterer Vorteil ergibt sich hinsichtlich der Konsistenz der zwischengespeicherten Daten. Da ein Reverse Proxy im Administrationsbereich des Content Providers bzw. in der näheren Umgebung dessen liegt, können Updates der bereitgestellten Daten direkt an den Proxy weitergegeben werden, um somit eine Verbreitung veralteter Daten zu verhindern. Beide Umsetzungen haben durch den Standort nahe des Servers weitere Vorteile. Der Proxy speichert nur die Daten

der dahinter liegenden Content Servern eines Content Providers zwischen, so dass der Proxy genau auf diese Typen von Daten optimiert werden kann. Zuletzt sollte hier noch erwähnt werden, dass der Reverse Proxy wegen der Lage unmittelbar vor den Content Servern für alle Gruppen von Clients im Rechnernetz Anfragen behandeln kann. In diesem Zusammenhang spricht man auch von der *Web-Cache-Reichweite*, die bei diesem Ansatz natürlich sehr hoch ist.
Durch die Installation in der Nähe des Ursprungsservers ergeben sich bei beiden Installationsorten jedoch auch erhebliche Nachteile. In Abbildung 6.4 ist gut zu erkennen, dass die Anfrage fast den kompletten Weg durch das Netz nehmen muss. Somit kann der Vorteil einer verkürzten Antwortzeit - wie in Abschnitt 6.2.1 skizziert - hier kaum gelten gemacht werden. Weiterhin kann der Proxy zum sogenannten *Single Point of Failure* werden. Alle Anfragen werden durch seine Rolle als Stellvertreter für die dahinter liegenden Server erst an ihn gerichtet. Daher kann die Verfügbarkeit bei Ausfall des Proxies enorm beeinträchtigt werden. Das Problem der sogennanten „letzten Mile“, d.h. der geringen Bandbreite auf dem Link zwischen Server Access Network und Backbone Network wirkt sich bei der serverseitigen Installierung negativ auf das Antwortzeitverhalten aus. Dieser Einfluss kann durch die Installation des Reverse Proxy auf Seiten des Backbone-Networks verhindert werden, da hier genau dieser Teilpfad der Verbindung bei einem Cache-Hit vermieden wird.

6.2.1.2 Forward Proxy

Der 2. Ansatz zur Verwendung eines Proxies wird als *Forward Proxy Server* bezeichnet. Ein Forward Proxy wird in der Nähe des Access Points installiert, der die Schnittstelle zwischen Client Access Network und dem Internet bildet. Die Aufgabe des Forward Proxies ist es für Clients innerhalb einer Domain, z.B. UniBw-muenchen.de, Inhalte von allen Content Servern die außerhalb der Domain angesiedelt sind zu liefern. In Abbildung 6.5 wird der eben erläuterte Ansatz veranschaulicht.
Man stellt schnell fest, dass sich die Vorteile eines Forward Proxies aus den Nachteilen eines Reverse Proxy ergeben. Ein entscheidender Vorteil eines Forward Proxy, der auch direkt aus der obigen Abbildung entnommen werden kann, liegt in der Nähe zu den Clients. Ist der vom Client angefragte Inhalt im Cache des Proxies enthalten so muss die Anfrage bzw. die Antwort nicht den komplette Weg durch das Internet nehmen, sondern nur den kurzen Pfad zwischen Client und Proxy. Falls sogar eine breitbandige Verbindung innerhalb des Client Access Network besteht, ist die Antwortzeit ein Bruchteil der Zeit, die benötigt werden würde, wäre die Anfrage an den originalen Server gerichtet worden. Zuletzt spart die verringerte Nutzung des Netzes zudem auch Übertragungskosten ein.
Betrachtet man die Vorteile des in Abschnitt 6.2.1.1 vorgestellten Reverse Proxy kann man auch die Nachteile dieses Ansatzes erkennen. Der erste Nachteil ergibt sich hinsichtlich der Konsistenz der zwischengespeicherten Daten. Da die Content Server nicht wissen, wo überall im Internet verstreut Proxy Server stehen, die ihre Daten zwischenspeichern, können diese nicht gezielt aktualisiert werden. Dadurch können veraltete Daten durch den Forward Proxy weiterhin geliefert werden. Ein weiterer Nachteil ist, dass ein Forward Proxy alle Typen von Daten zwischenspeichern muss. Da die Clients, für die der Proxy Anfragen bearbeitet, die Möglichkeit besitzen von allen Providern Daten anfragen zu können, kann hier keine Spezialisierung des Forward Proxy erfolgen. Gravierender wiegt

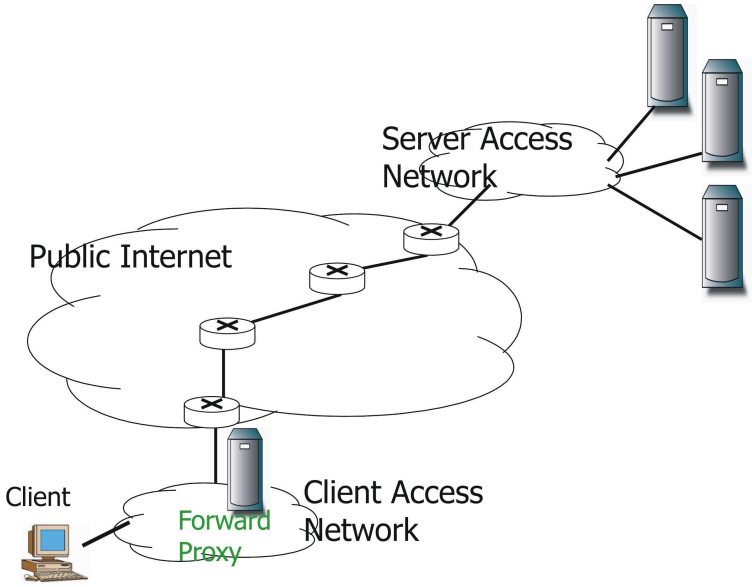

Abbildung 6.5: Forward Proxy

in diesem Kontext jedoch nicht die fehlende Spezialisierung sondern der Fall, dass ein Forward Proxy einen bestimmten Datentyp nicht unterstützt und somit nicht speichern kann. Somit würde jede Anfrage an Daten dieses Typs vom originalen Content Server bezogen werden müssen, was gerade im Falle von umfangreichen Daten (z.B. Multimedia-Streams) ein erheblicher Nachteil darstellt. Zuletzt sollte hier erwähnt werden, dass die bereits in Abschnitt 6.2.1.1 erwähnte Web-Cache-Reichweite hier sehr klein ist, da ein Forward Proxy nur für eine bestimmte Gruppe von Clients (z.B. Clients einer Domain) zuständig ist.

6.2.1.3 Fazit

Ist der Proxy nun die Lösung für die in Abbildung 6.1 vorgestellten Probleme? Konfrontiert man die Techniken eines Forward bzw. Reverse Proxies mit der dargestellten Problematik, ist folgendes Fazit zu ziehen.
Durch die Installation eines Reverse Proxies erhält man serverseitig eine erhöhte Rechenleistung, was zur Lösung des Problems eines überlasteten Servers bzw. einer überlasteten Serverfarm führen kann. Jedoch müssen alle Anfragen den kompletten Weg durch das Netz nehmen. Dadurch können verstopfte Pfade innerhalb des Netzes zu einem enormen Problem führen.
Die durchschnittliche Antwortzeit der Anfragen der Clients, für die der Forward Proxy die Stellvertreterrolle einnimmt, kann nur dann wesentlich verringern werden, falls die Cache-Hit Rate sehr hoch ist. Die Hit Rate hängt jedoch von mehreren Faktoren ab, auf die der Proxy nicht unbedingt Einfluss hat. Speichert der Proxy beispielsweise meistens dynamischen Inhalt[4] zwischen, so wird dieser Inhalt sehr schnell ungültig und er muss erneut vom originalen Server bezogen werden. Ist durch diese Einflüsse die Hit Rate sehr gering, werden die meisten Anfragen an den originalen Server weitergeleitet. Da der Proxy

[4]Inhalt der stetiger Änderung unterliegt, z.B. der Liveticker zu einem Tennisspiel

keinen Einfluss auf den Verkehr anderer Nutzer des Netzwerks nimmt, kann das Problem des verstopften Pfades auch hier negativen Einfluss nehmen.
So lässt sich abschließend bemerken, dass sowohl Forward als auch Reverse Proxy keine Garantien für bessere Antwortzeiten sind.

6.2.2 Warum Content Distribution Networks?

Im folgenden soll nun das Problem des „World Wide Wait“ aus Abschnitt 6.1.1 dargestellt werden, um somit die Problemsituation aufzuzeigen zu der ein Content Distribution Network eine Möglichkeit zur Lösung darstellt.
Ein Client kann eine Verbindung zu einer Webseite herstellen, indem er die URL des zur Webseite zugehörigen Server angibt. Falls die Anzahl der Anfragen die Kapazität des Servers bzw. der Netzwerkverbindung übersteigt, resultiert daraus ein schlechtes Antwortzeitverhalten. Die klassischen Lösungen wie in Abschnitt 6.1.2 erläutert, können nur unter bestimmten Umständen eine befriedigende Lösung bieten. Eine weitere Lösung ist das Installieren von Forward bzw Reverse Proxies, um bei weit entfernten Clients die Verschwendung der Bandbreite zu verhindern sowie die Antwortzeit zu verringern. Jedoch auch diese Lösung führt wie in Abschnitt 6.2.1 erläutert nicht immer zum gewünschten Verhalten. Die Anfrage an einen anderen Server umzuleiten, der den angefragten Inhalte liefern könnte, dessen Verbindung zum Client jedoch über einen anderen weniger genutzten Weg führt, würde zu einem besseren Antwortzeitverhalten resultieren.

6.2.3 Was ist ein Content Distribution Network?

Allgemein wird im derzeitigen Internet die Information durch einen Server bereitgestellt, der sich an einer bestimmten Position im Netz befindet. Dem gegenüber steht die große Menge an Nutzern, die beliebig geographisch verteilt in das Netz eintreten. Durch die steigende Popularität von Multimedia Anwendungen wie Videokonferenzen wurden Faktoren wie z.B. *Effizienz der Verfügbarkeit*[5] bei der Bereitstellung von Information wichtiger.
Die Lösung zur Erhaltung der Leistungsfähigkeit des Internet durch Content Distribution Networks basiert auf den im Abschnitt 6.2.1 vorgestellten Ansatz des Proxy. Um den Grundsatz der Verfahrensweise am einfachsten zu erläutern, betrachten wir eine Client-to-Server Verbindung. Solange der komplette Weg zwischen Client und Server genügend freie Bandbreite aufweist, kann die Antwortzeit im gewünschten Rahmen liegen. Ist jedoch ein Abschnitt des Pfades durch eine hohe Anzahl an Datenflüsse überlastet, so wäre es sinnvoll für den Client – sofern die Möglichkeit besteht – sich an einen anderen Server mit besserer Antwortzeit zu wenden, der den gleichen Content[6] bereitstellt. Die Mechanismen eines Content Distribution Networks erlaubt diese Umleitung der Clients.
In Abbildung 6.6 werden die Komponenten eines CDNs am obigen Beispiel erläutert.

[5] Effizienz der Verfügbarkeit bedeutet in diesem Kontext, dass die Qualität von web-basierten Multimedia-Anwendungen stark davon abhängig ist, wie verfügbar die Daten sind. Sollte z.B. das Bild eines Films aufgrund der schlechten Verfügbarkeit der Daten nicht kontinuierlich präsentiert werden können, so ist die Anwendung weniger effizient.

[6] Content: Jede digital verfügbare Kombination aus Text, Bildern, Applets, Frames, MP3, Video, Virtual Reality Objekte, usw. [5]

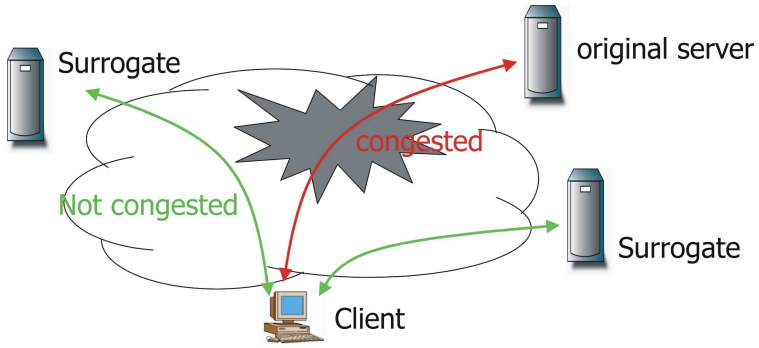

Abbildung 6.6: Content Distribution Network -einfache Darstellung

Ein Client will über ein Backbone Netzwerk einen Server erreichen. Der Weg zwischen Client und originalen Server ist verstopft – dies wird durch die dunkle Wolke verdeutlicht. Bietet sich dem Client jedoch die Möglichkeit mit einem anderen Server, einem sogenannten *Surrogate Server*[7] in Verbindung zu treten, der eine bessere Verbindung aufweist und den kompletten Inhalt seinerseits bereitstellen kann, so sollte der Client die Anfrage an diesen stellen. Dieser spezielle Fall lässt sich natürlich auf die Anforderungen der heutigen Rechnernetzen (im speziellen auf das Internet) verallgemeinern, indem man mehrere Clients und Surrogate Server wie in Abbildung 6.7 gegenüberstellt.

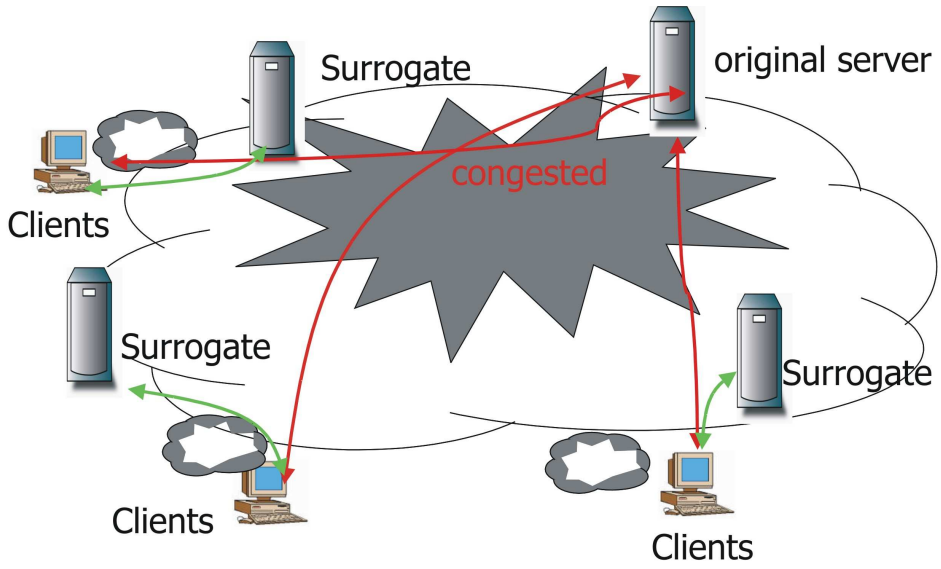

Abbildung 6.7: Content Distribution Network - komplexere Darstellung

Diese Abbildung stellt die typische Anordnung eines CDNs dar. Ein CDN besteht aus einer Menge von *Surrogate Sites*, deren Anordnung auf eine bestmöglich Zufriedenheit der Clients im Hinblick auf Antwortzeit abzielt. Die Anordnung der Surrogates sollte daher am „Rande“ des Internets erfolgen, wobei der Rand die Access Points der Internet Service Provider darstellt. Jeder Surrogate ist dadurch im näheren Umfeld einer Clientgruppe stationiert. Hier wird der Surrogate auch als *Edge Server* bezeichnet. Jeder Client wird

[7]Surrogate Server: Server des Content Distributor – Anbieter eines CDNs – auf welchem der replizierte Content gespeichert ist[5].

mit seiner Anfrage zu einem der Surrogate Sites weitergeleitet, somit kann auch bei einem verstopften Pfad zwischen Client und originaler Site eine hohe Übertragungsqualität gewährleistet werden. Die einzelnen Surrogate Sites können wiederrum aus einem oder mehreren Servern bestehen. Dieser Zuwachs an Rechenleistung der Surrogate Server zu den originalen Server bietet die Möglichkeit mehr Clients zu bedienen bzw. die gleiche Menge an Clients schneller zu bedienen.
Ein Content Distribution Network wie oben erläutert, besteht aus verschiedene Komponenten[9]:

1. Bereitstellung von Daten (Distribution Infrastructure)
2. Bearbeitung der Anfragen (Request routing)
3. Lieferung des Inhalts (Content Delivery)
4. Abrechnungssysteme (Accounting Infrastructure)

Distribution Infrastructure als Komponente hat die Aufgabe den Inhalt vom originalen Server auf die Surrogates zu verteilen. Eine detaillierte Betrachtung von Content Distribution erfolgt in Abschnitt 6.3.3. *Request routing* ist der Bestandteil der die Verbindung zwischen Client und einem Surrogate Server aufbaut. *Content Delivery* liefert Daten von den Surrogates an die Clients. Zuletzt ist das *Accounting-System* der Teil, der es einem „[..] CDN-Provider ermöglicht, den Datenverkehr zu protokollieren, zu messen und den Content-Providern bzw. auch den Internet-Benutzern in Rechnung zu stellen [..]“ [3]. Im folgenden liegt das Hauptaugenmerk vor allem auf dem Request Routing, da diese Komponente, wie in den Abschnitten 6.3.1 sowie 6.3.2 noch erläutert einen enormen Einfluss auf die Leistungsfähigkeit des CDNs hat.

6.2.4 Problemlösung durch Content Distribution Networks

Bevor eine Betrachtung der Mechanismen und Verfahren die ein CDN beinhaltet erfolgt, soll vorab geprüft werden, ob auch alle Probleme die in Abschnitt 6.1.1 sowie in Abbildung 6.1 erläutert wurden, durch ein CDN gelöst werden können.
Die Architektur eines CDNs auf Basis der geographischen Verteilung der Surrogate Server und der kopierten Originaldaten, die auf den Surrogates abgelegt werden, löst das Problem der konzentrierten Last, welches durch die Anfragen an den originalen Server entstehen kann. Weiterhin werden die Links nahe dem originalen Server entlastet, da die Mehrzahl der Anfragen an die Server des CDNs abgegeben werden. Durch die geographisch Verteilung der Surrogate Server ergibt sich eine Verringerung der Antwortzeiten der Anfragen. Nehmen wir an ein Client aus Europa will eine Webseite, die auf einem Server in den USA liegt aufrufen, so wird die Anfrage nach Amerika geleitet. Selbst im best-case Szenario entsteht hier durch die Laufzeit des Pakets eine gewisse Verzögerungszeit. Falls ein CDN diese Webseite bedient, so könnte ein Surrogate der in Europa stationiert wurde die Antwortzeit durch verkleinern der zurückzulegenden Strecke innerhalb des Internets deutlich verringern.
Zum Abschluss diese Abschnitts sollte noch ein Blick auf das Problem des verstopften Links innerhalb des Backbone-Network geworfen werden. Sollte ein Pfad zwischen dem

Client und dem original Server verstopft sein, so könnte die Suche nach einem Surrogate, der kein verstopften Link zwischen ihm und dem Client aufweist, die Antwortzeit reduzieren.

6.3 Verfahren und Mechanismen

Im Abschnitt 6.2.3 wurden die Komponenten eines Content Distribution Networks vorgestellt jedoch blieben einige Fragen offen. Nehmen wir eine Infrastruktur gemäß Abbildung 6.8 an.

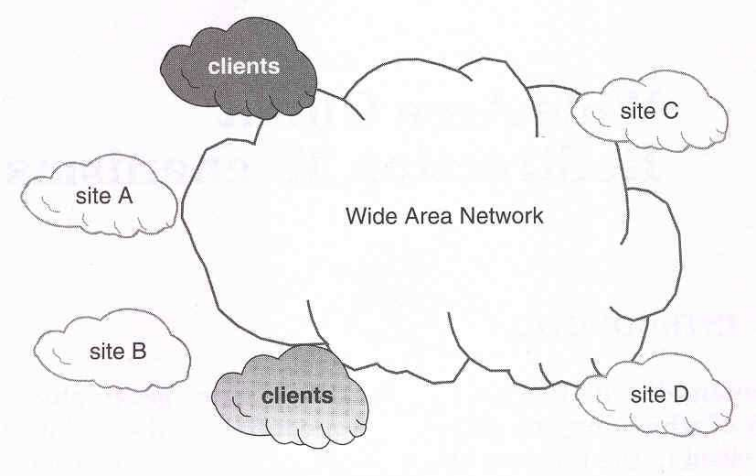

Abbildung 6.8: Situation im WAN, Quelle: [1]

Hier wird ein CDN mit vielen Sites, die verteilt innerhalb eines Wide Area Networks liegen dargestellt. Weiterhin existieren einige Clientgruppen, die jeweils Inhalte abfragen möchten, die durch das Content Distributed Network bereitgestellt werden. Die Clients können geographisch verteilt und unabhängig voneinander an beliebigen Stellen in das Netz eintreten. Jeder Client muss nun zu der Site geleitet werden, die für ihn die beste Leistung bereitstellen kann. Daraus ergeben sich 2 Fragestellungen:

1. Welche ist die *beste* Site für den aktuellen Client?

2. Welche Mechanismen können gewährleisten, dass der Client genau auf diese Site zugreift?

Bevor im Abschnitt 6.3.2 Frage 1 beantwortet wird, soll im folgenden nun die 2. Frage geklärt werden. Techniken zur Lösung dieser Frage existieren für jede Art von CDN bzw. für jede Art von Rechnernetz in dem sie eingesetzt werden, jedoch beziehen sich die Lösungen die in Abschnitt 6.3.1 erläutert werden vor allem auf die web-basierten CDNs.

6.3.1 Client Redirection Mechanisms

Die Aufgabe eines Client Redirection Mechanismus ist, verschiedene Clients, die einen vom CDN bereitgestellten Inhalt anfordern und geographisch verteilt in das Netz eintreten, zu ihrer besten Site leiten zu können. Betrachtet man den Ablauf einer Client-to-Server Verbindung stellt man fest, dass ein möglicher Ansatzpunkt für die Umleitung der einzelnen Clients direkt zu Beginn der Verbindungsaufnahme bei der Umsetzung des URL in eine IP-Adresse ist.

6.3.1.1 DNS based request routing

Zum Verständnis der DNS basierten Umleitungstechnik wird im weiteren ein kurzer Einblick in die Arbeitsweise eines *Domain Name System* (DNS) gewährt werden.
Der Prozess der Übersetzung einer URL in eine IP-Adresse wird durch eine Menge an *Domain Name Servern* sichergestellt. Jede Domain hat dabei ihren eigenen Name Server, der als authentifizierte Einheit die Adressabbildung für seine Domain übernimmt. Die Name Server sind in einer Hierarchie ähnlich der eines Baumes aufgebaut. Zwischen den Servern gibt es Vater-Kind Beziehungen, wobei jeder Vater alle seine Kinder kennt. Die Umkehrung gilt jedoch im allgemeinen nicht, da bei der rekursiven Implementierung (Erläuterungen zu Implementierungsarten folgen weiter unten im Abschnitt) eines DNS-Servers die Kinder jeweils nur die Wurzel des Baumes kennen.
Will eine Client nun, um eine Anfrage an einen Server zu stellen, dessen URL zu einer IP-Adresse auflösen lassen, so wird er eine DNS-Anfrage an seinen lokalen – im Bezug auf die Domain in der sich der Client befindet – Name Server stellen. Falls dieser die gewünschte Information nicht besitzt, gibt es zwei Möglichkeiten [8].
Der Name-Server entscheidet bei der iterativen Implementierung nun zwischen zwei Alternativen. Kennt der Name-Server den Namen des zuständigen DNS-Servers für die Domain in der, der gesuchte Server liegt, sendet er diesen an den Client zurück. Ist ihm der zuständige DNS-Server unbekannt leitet er die Anfrage zu seinem Vater weiter. Falls die eingegebene URL existiert, erhält der Client Name-Server auch bei Wahl der zweiten Alternative nach einer bestimmten Anzahl von Schritten den Namen des zuständigen DNS-Servers. Der Client Name-Server richtet nun die Anfrage an diesen DNS-Server, der als Ergebnis die IP-Adresse liefert. Im rekursiven Fall hat der Name-Server folgende Optionen: (1) Er sendet die Anfrage an einer seiner Kind-Server weiter, (2) leitet die Anfrage an seinen Vater weiter oder, (3)falls er die zugehörige IP-Adresse kennt, löst er die URL in die gesuchte IP-Adresse auf und sendet das Ergebnis zurück. Erreicht eine Antwort ein Domain Name Server, speichert er das Ergebnis für spätere Anfragen.
Die DNS basierte Umleitungstechnik greift nun aktiv in den oben dargestellten Prozess der URL-Auflösung ein. Wie auch schon zu Beginn dieses Abschnitts geschildert, benötigt man Kontrolle über den für die original Site zuständigen Domain Name-Server um die Clients umleiten zu können. Kontrolle soll hier bedeuten, dass alle URL-Anfragen zu einer originalen Site, z.B. www.cnn.com durch den DNS Server von cnn.com zu dem DNS Server des CDNs weitergeleitet werden. Der DNS Server des CDNs übernimmt nun durch die Rückgabe der IP eines der Surrogates die Umleitung. Der DNS Server könnte hier auch die Einheit bilden, die die Entscheidung über die beste Site zu dem anfragenden Client trifft (siehe 6.3.2).

Die Probleme die sich hinsichtlich dieses Verfahrens ergeben, lassen sich mit Hilfe der Abbildung 6.9 erläutern.

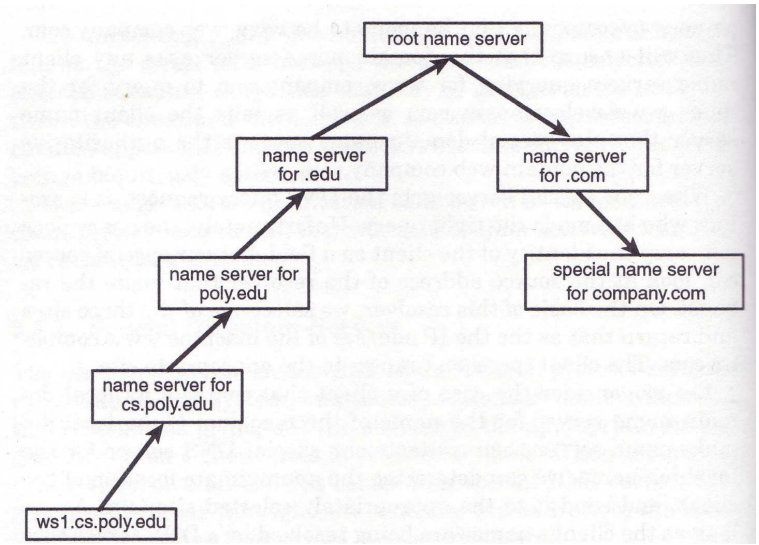

Abbildung 6.9: Weiterleitung einer DNS-Anfrage; Quelle [1]

Hier will eine Client-Maschine ws1.cs.poly.edu auf einen Server www.company.com zugreifen. Die DNS-Anfrage wird über die dargestellten DNS-Server bis zum DNS-Server von company.com weitergeleitet. Nehmen wir an, dass dieser DNS-Server alle Anfragen an den speziellen DNS-Server des Content Distribution Network weiterleitet. Dieser behandelt die Anfrage und liefert die beste Site zu dem anfragenden Client. Die IP-Adresse wird nun auf dem „Rückweg“ von allen Caches der DNS-Server gespeichert, um wie bereits oben erläutert, zukünftige DNS-Anfragen direkt bearbeiten zu können. Somit würde hier im Beispiel jeder zukünftige Zugriff der Clients, die sich sich hierarchisch innerhalb des Netzes des „Wurzelknotens“ befinden, immer auf die Site mit der oben ermittelten IP erfolgen. Damit könnte eine Umleitung zur besten Site nicht mehr gewährleistet sein. Eine Lösung des Problems erfolgt durch beschreiben des Time-To-Live Feldes[8]. Hat das Time-To-Live Feld einen sehr kleinen Wert, wird die Auflösung sehr rasch ungültig und der Eintrag wird verworfen. Jedoch sollte man hier nicht vernachlässigen, dass ein TTL nahe 0 die Antwortzeit dadurch erhöht, dass jede DNS-Anfrage den kompletten Weg zwischen Client und zuständigen DNS-Server des CDNs nehmen muss.

6.3.1.2 URL rewriting

Eine weitere Technik um Clients zu einer Site zu leiten ist das URL rewriting. Um diese Technik zu verstehen, sollte man hier einen Blick auf den Ablauf von der Eingabe einer URL bis zur Anzeige der Internetseite werfen. Zuerst wird die URL mit Hilfe eines normalen DNS-Servers in eine IP-Adresse aufgelöst. Durch die IP-Adresse und einer TCP-Verbindung kann der Client eine HTTP-Anfrage an den Web-Server, der die gewünschte

[8]Time-To-Live (TTL): Jeder Datensatz der Domain Name Server enthält neben URL und zugehöriger IP-Adresse ein TTL-Feld, das angibt, nach welcher Zeit der Eintrag ungültig wird

Webpage bedient, richten. Als HTTP-Antwort liefert der Webserver die gewünschte Seite, z.B. www.cnn.com/index.html. Die TCP-Verbindung wird damit beendet. Sind eingebettet Objekte, z.B. Bilder, Webbanner, usw. in der Seite vorhanden, ist deren Speicherort als URL im Quelltext der Index-Seite angegeben. Daher muss für jedes Objekt die eben beschriebenen Schritte erneut durchgeführt werden.
Bei URL-rewriting werden nun diese URLs zu den eingebetteten Objekte dynamisch durch einen Prozess auf dem originalen Server erzeugt. Die Verweise zeigen nun nicht wie oben auf den originalen Herkunftsort der Objekte, sondern zu einem der Surrogate Server des CDNs. Da die eingebetteten Objekte meist ein viel größeres Datenvolumen ausmachen als die Index-Seite, reduziert diese Technik die Last des originalen Servers und den Verkehr in servernähe enorm. Problem dieses Ansatzes ist jedoch, dass hier der Prozess der auf dem original Server abläuft, welcher nicht dem CDN zugehörig ist, die Entscheidung für einen der Surrogates treffen muss. Abhilfe hierzu könnte eine Kombination aus URL rewriting und DNS based request routing dienen, indem man die Verweise der eingebetteten Objekte durch den DNS-Server des CDN auflösen lässt. Dies funktioniert dadurch, dass man statt der URL eines bestimmten Surrogates den DNS-Server des CDNs als Pseudo-URL angibt. Der Begriff „Pseudo-URL“ wird hier verwendet, da die URL nicht nur die Aufgabe der Angabe Servers hat, sondern auch als Hinweis für den DNS-Server dient, dass ein Surrogate für den anfragenden Client gesucht wird.

6.3.1.3 Vergleich

Vergleicht man beide Techniken miteinander, liegt einer der Unterschiede in der Frage, wie transparent der Ursprungserver des Content Providers gegenüber einem anfragenden Client ist.
Betrachtet man die DNS basierte Technik, so stellt man fest, dass der Originalserver für den Client völlig unsichtbar ist. Die URL des originalen Server wird in eine IP-Adresse einer Surrogate Site aufgelöst. Anhand dieser IP baut der Client die Verbindung zu der zugehörigen Surrogate Site auf, deren Server ihm dann den angefragten Inhalt bereitstellen. Der Client steht somit zu keinem Zeitpunkt in Verbindung mit dem Ursprungserver. Im Fall des URL-Rewriting stellt sich die Situation hingegen etwas anders. Um die angeforderte Webseite zu laden, stellt der Client mindestens eine Verbindung zum originalen Server her. Somit ist der Ursprungserver hier nicht unsichtbar gegenüber dem Client.
Ein weiterer Unterschied liegt in der Frage der benötigten Komponenten zur Umsetzung der Techniken. Im Falle des URL-Rewriting kann der oben erläuterte Prozess des dynamischen Erzeugens von Webseiten auf dem originalen Server des Content Providers laufen. Die in den Webseiten verwiesenen Surrogates sind Teil eines jeden CDN. Hingegen benötigt die DNS-basierte Technik einen speziellen DNS Server, der die DNS-Anfrage bearbeitet.
Zum Abschluss sollte daraufhin gewiesen werden, dass man im Allgemeinen keine der beiden Techniken präferenzieren kann. Denn bei der Frage, welche Technik eingesetzt werden soll, ist vor allem der Faktor „Zweck und Umfeld des CDNs“ mit der Ausschlaggebende. Zweck und Umfeld zielt hier auf die Ziele (Beispiel: Wie hoch kann der originale Server überhaupt belastet werden?) des Content-Providers bei der Auslagerung des Inhalts ab. Jedoch können auch die Techniken, wie in Kapitel 6.3.1.2 erläutert, kombiniert werden.

6.3.2 Client - Site Beziehung

Ein CDN besteht per Definition aus mehreren Sites, falls ein Client nun eine Anfrage stellt, muss die für ihn „beste“ Site ermittelt werden. In diesem Abschnitt werden Techniken betrachtet, die benutzt werden können um diese Entscheidung zu treffen. Weiterhin wird geklärt, welche Bedingungen an die beste Site für einen Client gebunden sind.
Vorweg sollte hier allerdings erwähnt werden, dass diese Frage nicht eindeutig beantwortet werden kann, da die Wahl einer besten Site von dem Zweck des betrachteten Content Distribution Networks abhängt. Ist das CDN eingerichtet worden um die Antwortzeit zu minimieren, so wird man die Site wählen, deren Verbindung zum Client hin im Vergleich zu den anderen CDN-Sites die kleinste Verzögerung aufweist und deren Server bzw. Serverfarm nicht überlastet ist. Ist hingegen die Skalierbarkeit[9] das Hauptziel des CDNs, ist der Faktor der Verbindung zwischen Client und Site eher zu vernachlässigen. Hier wäre die Site die beste, welche die größten Rechenzeitreserven aufweist.
Trotz dieser eben erläuterten Abhängigkeit zwischen Zweck des CDNs und Kriterien zur Suche der besten Site, können die 4 folgenden Faktoren aufgelistet werden, die je nach Art des CDN mehr oder weniger bei der Auswahl einer Site berücksichtigt werden [3]:

1. Vorhandensein des gewünschten Web-Content
   Ist der gewünschte Content auf dem Surrogate gespeichert?
2. Entfernung zwischen Client und Surrogate-Server
   Anhand einer bestimmten Entfernungsmetrik[10] wird der Abstand zwischen Client und den einzelnen Surrogates bestimmt.
3. Aktuelle Last der Surrogates
4. Verfügbare Übertragungsbandbreite

Die untersuchten Mechanismen können in die Gruppe der aktiven und passiven Schemata eingeteilt werden. Obwohl sich beide Gruppen komplett verschiedener Techniken zum Auffinden der besten Site für den anfragenden Client bedienen, besitzen die Mechanismen beider Gruppen zur Entscheidungsfindung einen sogenannten *Decision Maker*, wobei sich jedoch die Lage dieser Komponente auch innerhalb einer Gruppe je nach Art und Zweck des zugrundeliegenden Content Distribution Networks unterscheiden kann.

6.3.2.1 Aktive Schemata

Die Techniken, die zu dieser Gruppe einzuordnen sind, zeichnen sich dadurch aus, dass für den Prozess der Bestimmung der besten Site aktiv Anfragen an den Client durchgeführt werden. Ein Client stellt eine Anfrage an das CDN. Der Decision Maker erhält diese

[9] Skalierbarkeit: hier möglichst viele Anfragen bearbeiten zu können. Wird dann erreicht wenn die Anzahl an Abweisungen unter Berücksichtigung der Gesamtrechenleistung aller Server minimal wird.

[10] Entfernungsmetrik: Basis mit der in Verbindung mit einem Messverfahren die Clients mit den Surrogates in ein Verhältnis gesetzt werden können, z.B. geographische Entfernung, Verzögerungszeit des Netzwerks zwischen Client und Surrogate,...

Anfrage und sendet zur Ermittlung der besten Site für den Client extra Pakete zu jeder CDN-Site. Jede Site hat einen *Performance Monitoring Server* der dieses Paket empfängt und eine Antwort zurücksendet. Der Decision Maker sammelt alle empfangenen Daten und sucht nun anhand dieser Ergebnisse die beste Site, die er dem Client danach mitteilt. Der Inhalt dieser extra Pakete sowie die Antwort der Performance Monitoring Server ist nicht explizit vorgegeben und ist unmittelbar mit dem Zweck des CDNs verbunden, indem Decision Maker und Performance monitoring Server installiert sind.
Ist die Skalierbarkeit Hauptziel des CDNs so sollte der Client zu der am wenigsten belasteten Site verwiesen werden. In diesem Fall würde jeder Performance Monitoring Server der CDN-Sites die aktuelle Last an den Decision Maker zurückgeben. Wurde das CDN installiert um die Antwortzeit zu minimieren muss die Site ermittelt werden, die am nahsten beim Client liegt und wenig Last aufweist. In diesem Fall würde der monitoring Server den Abstand zum Client – in welcher Form (zeitlich, geographisch) auch immer – an den Decision Maker zurückgeben.
In Web-basierten CDNs ermitteln die CDN-Sites aktiv die Distanz zwischen Ihnen und dem Client. Ein beliebtes Verfahren zur Messung der Distanz, welches auch im Standart der IP-Netzwerke unterstützt wird, ist die Nutzung des ICMP-Echo, das auch „ping“ genannt wird.
ICMP, das als Kontrollprotokoll durch alle Geräte unterstützt wird die das IP Protokoll implementieren, erlaubt einer Maschine ein ICMP-Echo-Request zu einer anderen IP-Maschine zu senden. Diese zweite Maschine sendet nach erhalten der Echoanfrage direkt eine Echoantwort. Durch die Messung der Zeit zwischen Senden der Anfrage und Zeitpunkt des Erhaltens der Antwort kann Maschine 1 die Verzögerung im Netzwerk feststellen.
Der Ablauf könnte dann wie in Abbildung 6.10 dargestellt ablaufen:

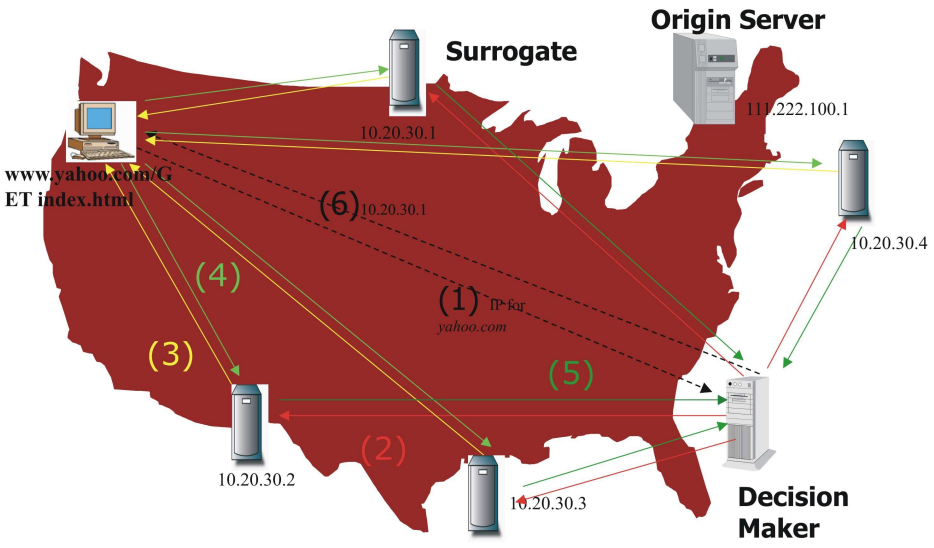

Abbildung 6.10: Verwendung des ICMP-Echo im aktiven Schema

Erreicht eine Anfrage (1) den Decision Maker sendet dieser eine Nachricht an alle Sites des CDN (2). Der Performance Monitoring Server jeder CDN-Site sendet daraufhin ein ping (3) an den anfragenden Client und erhält mit der Echoantwort (4) die Verzögerungszeit. Die Antwort zum Decision Maker (5) kann neben der ermittelten Zeit ebenso die Last der

Server bzw. Serverfarm der Site mit beinhalten. Somit kann der Decision Maker die Site wählen (6), die die geringste Verzögerungszeit aufweist, der wenigsten Last ausgesetzt ist oder er kann eine Auswahl durch Gewichtung beider Faktoren treffen.
Vorteil dieser Lösung ist, dass bei jeder Anfrage die derzeitig optimale Site unter der aktuellen Netzlast bestimmt wird. Dieser Vorteil hat jedoch auch erhebliche Nachteile zur Folge. Ist die Menge der betroffenen CDN-Sites sehr groß entsteht durch den Ping Mechanismus ein erheblicher Verkehr im Netz. Weiterhin dauert das Senden der Nachrichten an die CDN-Sites, anpingen des Client und sammeln der Antworten eine gewisse Zeit. Dieser Overhead ist insbesondere dann gravierend, wenn der angefragte Inhalt einen sehr geringen Umfang hat.

6.3.2.2 Passive Schemata

Die Gruppe der passiven Schemata basiert auf der Verwendung von Routing Tabellen, die eine ankommende Anfrage auf die beste Site abbilden können. Der Aufbau solch einer Tabelle könnte wie folgt gestaltet werden: Die erste Spalte repräsentiert die Client-Gruppen, die zweite Spalte die zu den Client-Gruppen beste Site. Die Routing Tabelle ist ein Teil des Decision Makers, der auf eine Anfrage die Tabelle benutzt um eine Site zu wählen. Die Tabelle kann auch aus mehr als 2 Spalten bestehen, falls weitere Bedingungen wie die Existenz bestimmter Ressourcen (z.B. welche Medientypen der Server speichert) beim Server wichtig sind.
Der Aufbau der Routing Tabelle erfolgt durch eine Routing Information Matrix, die ihrerseits anhand einer Entfernungsmetrik die Distanz zwischen jedem Client und der CDN-Sites bereitstellt. Die Entfernungsmetrik kann auf der Umlaufzeit basieren, wobei jedoch auch die Last der CDN-Sites als Maßstab denkbar ist oder eine Kombination aus beiden Faktoren. Die Matrix kann statisch oder dynamisch erzeugt werden. Eine statische Lösung basiert auf einer statischen Routing Tabelle, so dass die Abbildung von Client zur besten Site über die Tabelle nicht immer der aktuellen Last im Netz bzw. der Server gerecht werden kann. Die dynamische Routing Information Matrix wird durch die Messung der Leistung beim Zugriff der Clients verwaltet. Die Leistungsdiagnose kann auf passivem Überwachen des Verkehrs jedes Clients basieren, oder sie kann durch ein aktives Senden von Proben jeder Site an alle Clients bzw. von jedem Client an alle Sites durchgeführt werden. Die Ergebnisse senden die Sites darauf zum Decision Maker, der diese zur Routing Information Matrix zusammenfügt und basierend darauf die Routing Tabelle bildet.
Man sollte hier bemerken, dass es sich jedoch beim aktiven Senden von Proben um eine Kombination aus aktiven und passivem Schemata handelt. Der aktive Teil besteht aus den Phasen der Aktualisierung der Routing Information Matrix bzw. der Routing Tabelle, der passive Teil aus den Phasen in der die Tabelle zur Abbildung von Client auf Site benutzt wird. Somit ist das Verfahren der Dynamischen Routing Tabelle in Kombination mit dem Senden von Proben, falls die Aktualisierungsrate der Routing Tabelle höher als die Ankunftsrate von Anfragen ist, eher in die Gruppe der aktiven Schemata einzuordnen.
Alternativ zu dieser zentralen Lösung mit einem Decision Maker ist ebenfalls ein verteilter Ansatz zum Bilden der Routing Information Matrix bzw. der Routing Tabelle möglich. Hier führen die einzelnen Sites wie in der zentralen Lösung ihr Performance Monitoring durch, jedoch werden die gesammelten Informationen nicht an den Decision Maker gesendet, sondern an alle anderen Sites des CDNs. Dadurch kann jede Site ihre eigene Routing

Tabelle bilden. Die verteilte Lösung ermöglicht es somit, dass jede Site die Funktion als Decision Maker ausführen könnte.
Im Vergleich zu den aktiven Schemata, die bei jeder Anfrage die derzeitig beste Site für den Client suchen, stellt die Verwendung von Routing Tabellen nur eine Heuristik dar. Durch die Verwendung einer Routing Tabelle, die auf „älteren“ Daten beruht ist nicht gewährleistet, dass der Client an die zur Zeit optimale Site weitergeleitet wird. Dieser Nachteil nimmt man jedoch in kauf, um den in Abschnitt 6.3.2.1 beschriebenen Overhead der aktiven Schemata auszugleichen und dadurch den Entscheidungsfindungprozess für eine Site zu beschleunigen. Dies wird vor allem dann zum Vorteil, falls der angefragte Inhalt sehr geringen Umfang hat.
Das Hauptproblem der passiven Schemata ist, dass sie nur wirksam arbeiten können wenn über jeden anfragenden Client bereits Daten in der Routing Information Matrix gesammelt wurden und damit die Routing Tabelle zur Abbildung auf eine Site verwendet werden kann. Ist der Client dem Decision Maker noch unbekannt, so sind keine Informationen über ihn verfügbar. In solche einem Fall könnte eine Kombination mit einem aktiven Schema doch zum Auffinden der besten Site für den Client führen.

6.3.3 Distribution Infrastructure

Der Blickpunkt des Kapitels 6.3.1 war geprägt von der Beziehung zwischen den Clients und einem Content Distribution Network. Dabei wurde untersucht wie die Anfrage eines Clients durch ein CDN bedient wird. Im weiteren soll nun das Hauptaugenmerk auf die Verbindung zwischen dem originalen Server eines Content Providers und den Surrogates eines CDNs geworfen werden. Zwei Fragen stehen hier im Vordergrund:

1. Wie können die Daten verteilt werden?
2. Wie kann die Konsistenz der verteilten Daten gesichert werden?

Die beiden folgenden Abschnitte werden nun Techniken untersucht, die zur Lösung vor allem der Frage 1 dient. Dabei wird auch geprüft, welche Vor- und Nachteile diese beim Einsatz in einem CDN haben. Frage 2 ist zu umfangreich und wird hier nur kurz angesprochen, da die Erläuterungen zu existenten Lösungen den Rahmen der Seminararbeit nicht gerecht werden können.

6.3.3.1 Data Sharing Schemes

Die Hauptaufgabe des Content Distribution in einem CDN besteht in der Verteilung des Contents von einem Originalserver auf alle oder einem Teil der Surrogates des CDNs. Dabei wird der Content eines Content-Providers vollständig oder nur teilweise auf die Surrogates eines CDNs ausgelagert. Dadurch kann man folgende 2 Lösungen unterscheiden [3]:

1. Vollständige Content-Auslagerung (Full-Site Delivery)
2. Teilweise Content-Auslagerung (Partial-Site Delivery)

Bei *Full-Site Delivery* wird der komplette Inhalt einer Site auf das CDN ausgelagert. Der originale Server ist mit Ausnahme des CDNs für jeden Teilnehmer des Netzes versteckt. Diese Lösung könnte zum Beispiel in Kombination mit dem in Abschnitt 6.3.1.1 vorgestellten Client Redirection Mechanismus verwendet werden. CDN Firmen die Full-Site Delivery betreiben sind: Adero, NetCaching und United Networks' IntelliDNS [7].
Bietet ein CDN Betreiber *Partial-Site Delivery* an, so werden nur Teile des Inhaltes eines Content Providers ausgelagert. Hier werden meist größere Dateien, wie umfangreiche Bilder, Videoanimationen, die z.B im Kontext einer Webseite stehen, durch das CDN gespeichert. Hier ist der originale Server nicht versteckt, jedoch bietet er nur einen geringeren Umfang seiner Daten nach außen hin an. Dies ist vor allem mit der in Abschnitt 6.3.1.2 vorgestellten Technik sinnvoll. CDN Betreiber die Partial-Site Delivery anbieten sind: Akamai, Digital Island, Mirrorimage, Solidspeed and Speedra [7].
Nach der Betrachtung der Strategien zur Auslagerung des Contents eines Content Providers, werden im Folgenden 2 Ansätze dargestellt, die erläutern wie der Inhalt - ein Teil oder der kompletter Inhalt einer Site - auf den Surrogates gespeichert wird.
Der erste Ansatz basiert darauf, dass alle Sites den auszulagernden Inhalt komplett speichern, d.h. jede CDN-Site hat eine komplette Kopie der Daten. Operationen auf den gechachten Daten haben jedoch unterschiedliche Auswirkungen. Bei *Leseoperationen*, die keine Änderungen an den Daten vornehmen, resultiert der Einsatz dieser Technik innerhalb eines CDNs in einer Leistungssteigerung. Operationen die Daten verändern sind hier jedoch etwas genauer zu untersuchen, denn nach einer *Schreiboperation* unterscheiden sich die einzelnen Kopien auf den Surrogates. Daher muss nach einer Schreiboperation (1) eine Synchronisation zwischen den Surrogates durchgeführt werden um somit (2) die Konsistenz der verteilten Daten wiederherzustellen. Somit sollte man vollständige Kopien der Daten dann auf die Surrogates verteilen, wenn die Leseoperationen den Hauptteil der Operationen auf den Daten ausmacht. Zuletzt sollte bemerkt werden, dass hier Kosten für den großen Speicher nicht zu vernachlässigen sind.
Der zweite Ansatz zur Verteilung der Daten auf die Surrogates wir als *Caching* bezeichnet. Hier existiert nur ein Original der Daten, das auf dem originalen Server des Content Providers gespeichert ist. Jeder Surrogate kann Teile der Daten lokal in seinem Speicherbereich cachen. Werden nun Anfragen an einen Surrogate des CDNs gestellt, versucht der Surrogate diese aus seinem lokalen Speicherbereich zu bearbeiten. Falls ein Teil der Daten, die zur Anfragebearbeitung nötig sind, nicht im Speicher des Surrogates vorliegen, gibt es zwei Möglichkeiten:

1. Der Surrogate stellt eine Anfrage nach den fehlenden Daten an die originalen Site (*Pull*).
2. Die Anfrage des Clients wird zur originalen Site weitergeleitet, die daraufhin die benötigten Daten zum Surrogate leitet (*Push*).

Der Leistungsgewinn durch diesen Ansatz basiert auf dem Prinzip, das sich ein Programm „lokal" verhält. Dieses Prinzip zielt darauf ab, dass jedes Programm die Seiten

seines Adressraums nicht gleichmäßig nutzt, sondern manche Speicherbereiche sehr oft, andere hingegen sehr selten aufgerufen werden. Überträgt man dies auf die verteilten Applikationen, lassen sich drei verschiedene Arten der Lokalität unterscheiden [1]. *Temporäre Lokalität* ist der Effekt, dass zu einer gewissen Zeit ein bestimmter Teil der Daten mehrmals aufgerufen wird. *Relationale Lokalität* zeigt auf, dass eine Anwendung in Zukunft meist auf Daten operiert, die zu den aktuellen Daten in Beziehung stehen. Die dritte Art der Lokalität bezeichnet man als *geographische Lokalität*. Diese Art steht für den Zusammenhang zwischen Ort des Anfrage und den Teil der angefragten Daten. Als Beispiel hierzu, nehmen wir an eine große deutsche Zeitung stellt ihren Inhalt online zur Verfügung. So wird der regionale Teil von Bayern im Norden Deutschlands nicht so häufig angefragt wie dies in Bayern der Fall ist. Diese Lokalitäten führen zu erheblichen Vorteilen des Cachings.
Wie bei dem obigen Ansatz können auch hier die Schreiboperationen zur Inkonsistenz der Daten führen. Daher muss zusätzlicher Aufwand zur Konsistenzerhaltung betrieben werden. Auch hier sind die Vorteile umso größer je mehr Leseoperationen auf dem Speicher ausgeführt werden.

6.4 Fazit - Ausblick

Unter dem Blickpunkt eines wie bereits in der Einleitung dargestellten wachsenden Internets, in dem die Web-Inhalte immer professioneller werden und dessen Nutzer immer häufiger auch zeitkritische Inhalte (Video on demand, Web-TV, usw.) anfragen, stellen CDNs Modelle dar um die Leistungsfähigkeit des Netzes zu erhalten. So kann man abschließend folgende Aspekte von CDNs hervorheben:

1. Verkürzung der Wartezeit auf den anfgefragten Inhalt.

2. Steigerung der Verfügbarkeit

Durch die Auswahl eines geeigneten Surrogates kann die Wartezeit für jeden anfragenden Client verringert werden. Gerade bei umfangreichen Inhalt, bei dem der Overhead zur Auswahl eines Surrogates und die Verbindungsherstellung zu diesem kaum ins Gewicht fällt, kann die Verbindung zu einem näheren als dem originalen Server zu einer beträchtlichen Zeitersparnis führen. Auch die Nutzungskosten für das Internet können somit verringert werden.
Die Verfügbarkeit einer Ressource im Internet steigt durch den Einsatz eines CDNs. Zum einen werden „populäre“ Seiten entlastet und die Antwortzeit sinkt, zum anderen kann sogar bei Ausfall des orginalen Servers unter Umständen (DNS basierte Weiterleitungstechnik in Verbindung mit kompletter Auslagerung des Inhalts einer Site) die Verfügbarkeit des vom Content-Provider angebotenen Inhalts gesichert werden.
In einem kurzen Ausblick soll hier noch auf die Zukunft von CDNs eingegangen werden. Der Blickpunkt richtet sich dabei auf die Themen:

1. Content Distribution Internetworking (CDI)

2. Internet Infrastruktur der Zukunft

Auf dem Gebiet der Content Distribution Networks sind noch einige Probleme zu lösen. Insbesondere stellt sich die Frage nach der Vernetzung verschiedener CDNs. Dadurch könnte die Reichweite und Fehlertoleranz erhöht sowie die Skalierbarkeit auch bei einer höheren Anfragerate gesichert werden. Aktivitäten dazu sind durch die Bildung der IETF-Arbeitsgruppe CDI angelaufen.
Content Distribution Networks als Infrastruktur der Zukunft zu beschreiben, bedeutet nicht, dass die Übertragungskapazität erhöht wird, sondern eher um ein neues Modell, den angefragten Inhalt schnell und zuverlässig zum Client zu liefern. Das Einsatzspektrum für CDNs ist sehr groß, jedoch eignet sich vor allem die Verteilung von multimedialem Inhalt auf CDNs. Denn meist unterliegen diese Inhalte einem zeitkritischen Faktor, der eher eingehalten werden kann indem dieser durch ein CDN bedient wird, als durch Bedienung eines originalen Content-Servers. Somit kann man erwarten, dass gerade im Bereich Streaming Media (Video on Demand, Web-TV, usw.) CDN einen Einsatzschwerpunkt finden werden.

Literaturverzeichnis

[1] Dinesh C. Verma, T.J. Watson Research Center IBM,
Content Distribution Networks - An Engineering Approach, John Wiley & Sons, Inc., New York 2002

[2] James F. Kurose, Keith W. Ross,
Computernetze, Ein Top-Down-Ansatz mit Schwerpunkt Internet, Addison-Wesley - Pearson Studium 2002

[3] Anatol Badach, Sebastian Rieger, Matthias Schmauch,
Web-Technologien, Architekturen, Konzepte, Trends, Carl Hanser Verlag München, Wien 2003

[4] Robert Tolksdorf,
Caching im Web, FU Berlin, Februar 2003,
`www.inf.fu-berlin.de/inst/ag-nbi/lehre/0203/V_NBI/16_Caching.pdf`

[5] Girish Borkar,
„Content Distribution Networks“, Department of Computer and Information Sciences, University of Delaware, Dec 2002,
`www.cis.udel.edu/~amer/856/cdn.02f.ppt`

[6] COMP 9333 Advanced Network Mini-Conference Report,
Load Distribution in Content Distribution Networks (CDN), Mai 2003,
`www.cse.unsw.edu.au/~cs9333/miniconfrep03/topic11.pdf`

[7] Balachander Krishnamurthy, Craig Willls, Yin Zhang,
On the Use and Performance of Content Distribution Networks,
`www.icir.org/vern/imw-2001/imw2001-papers/10.pdf`

[8] A. Shaikh, R. Tewari, M. Agrawal
On the Effectiveness of DNS-based Server Selection,
`www.research.ibm.com/people/a/aashaikh/research/-papers/infocom01.pdf`

[9] Janardhan R. Iyengar,
Overlay Networks, with A focus On Content Distribution Networks, April 2002,
`www.cis.udel.edu/~iyengar/courses/Overlays.ppt`