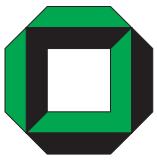

Universität Karlsruhe
Fakultät für Informatik
Institut für Telematik
76128 Karlsruhe

Netzwerk-Management und Hochleistungs-Kommunikation

Teil XIX

Seminar WS 1998/99

Herausgeber:
Elmar Dorner
Meng Gan
Hartmut Ritter
Dr. Jochen Schiller

Universität Karlsruhe
Institut für Telematik

Interner Bericht 04/99
ISSN 1432–7864

Zusammenfassung

Der vorliegende Interne Bericht enthält die Beiträge zum Seminar „Netzwerk-Management und Hochleistungs-Kommunikation“, das im Wintersemester 1998/99 zum neunzehnten Mal stattgefunden hat.

Die Themenauswahl kann grob in folgende vier Blöcke gegliedert werden:

1. Ein Block ist der Nutzung und Weiterentwicklung des Internet gewidmet. Hier geht es unter anderem um die Nutzung des Internet zur Sprachübertragung (Stichwort *voice over IP*), neuartige Ansätze zur Dienstgüteunterstützung (Stichwort *Differentiated Services*) und die Tarifierung benutzter Dienste im Internet.

2. Ein zweiter Block beschäftigt sich mit Problemen der Mobilkommunikation. Die Spanne reicht hier von *Routing in Satellitennetzen* über *Mobile IP* und *Drahtloses ATM* bis hin zu neuartigen Diensten in GSM (Stichworte *HSCSD und GPRS*).

3. Der dritte Block umfaßt den Themenbereich fortgeschrittener LAN-Technologien. Hier geht es um Zugangstechnologien wie *xDSL* und *V.90* ebenso wie um *Gigabit Ethernet* und *Industrielle Busse*.

4. Die Beiträge des vierten Blocks schließlich abstrahieren von den Details der zugrundeliegenden Techniken und beschäftigen sich mit Themen wie der Verwaltung von Netzwerken (Stichwort *management by delegation*), den Konsequenzen der Liberalisierung des deutschen Telekommunikationsmarkts (*Deregulierung*) und der Bedeutung virtueller privater Netze (Stichwort *VPN*).

Abstract

This Technical Report includes student papers produced within small lessons called seminar of “Network Management and High Speed Communications”. For the nineteenth time this seminar has attracted a large number of diligent students, proving the broad interest in topics of network management and high speed communications.

The topics of this report may be divided into four blocks:

1. One block is devoted to advanced Internet technologies. It deals with topics like *voice over IP*), service differentiation in the next generation internet(*Differentiated Services*) and tariffing in the internet.

2. The second block discusses problems or mobile communication systems. This concerns things like *routing in satellite networks* as well as *mobile IP* and *wireless ATM* and the description of new services in the GSM mobile phone system named *HSCSD und GPRS*.

3. The third block deals with advanced LAN-technologies. The articles describe the actual development in the area of *V.90*-standardisation and *xDSL-modems*, upcoming *gigabit ethernet* and bus technologies in a factory environment.

4. The fourth block finally discusses from a more general perspective themes like the management of networked systems (*management by delegation*), the consequences of the opened german telecommunications market and the idea behind *virtual private networks*.

Inhaltsverzeichnis

Vorwort

Das Seminar „Netzwerk-Management und Hochleistungs-Kommunikation“ am Institut für Telematik erfreut sich weiterhin großer Beliebtheit. Die Telematik als Verbindung von Telekommunikation und Informatik entfaltet immer mehr von ihrer Dynamik. Dies zeigt sich an der breiten öffentlichen Diskussion über die zukünftige Bedeutung des Internet, das ja schon lange dem akademischen Bereich entwachsen ist, ebenso wie an der wachsenden Bedeutung der Mobilkommunikation, ob über Satellit oder terrestrisch. Unabhängig vom zugrundeliegenden Netzwerk wird die Betrachtung von Dienstgütefaktoren - und die Abrechnung der Nutzung eines Dienstes - angesichts knapper Ressourcen in Zukunft große Wichtigkeit bei der Ausrichtung der künftigen Netze auf die Bedürfnisse der Anwender besitzen. In diesem Umfeld existiert eine derartige Vielzahl von innovativen Forschungsergebnissen und Produktideen, daß die Behandlung in anderen Lehrveranstaltungen so detailliert nicht möglich ist.

Jetzt liegt auch der nunmehr neunzehnte Seminarband als Interner Bericht vor. Durch die engagierte Mitarbeit der beteiligten Studenten konnte so zumindest ein Ausschnitt aus dem komplexen und umfassenden Themengebiet klar und übersichtlich präsentiert werden. Für den Fleiß und das Engagement der Seminaristen sei daher an dieser Stelle recht herzlich gedankt.

Die weiterhin gute Resonanz bei den Studenten bestätigt uns darin, auch im kommenden Sommersemester 1999 ein derartiges Seminar – natürlich mit geändertem aktuellem Inhalt – durchzuführen, so daß bald ein weiterer Interner Bericht mit neuen Forschungsergebnissen aus innovativen Seminarbeiträgen erscheinen wird. Doch vorerst sollen im vorliegenden Band folgende Themengebiete vorgestellt werden:

Gigabit Ethernet - Stand und Standards

Ethernet stellt heute die Standardtechnik zur Gebäudeverkabelung dar und wird weltweit mit Datenraten von 10 und 100 Mbit/s eingesetzt. Aufgrund der stets wachsenden Bandbreitenanforderungen wurde schon bald der Bedarf nach noch größeren Bandbreiten offensichtlich. Gigabit-Ethernet mit einer Übertragungsrate von 1000 Mbit/s stellt somit eine logische Fortentwicklung dar. Der Beitrag „Gigabit-Ethernet - Stand und Standards“ stellt die aktuellen Standardisierungen zum Thema vor und legt die vielfältigen Probleme mit der hohen Bitrate dar.

Breitband-Internet-Zugänge: xDSL, Kabelmodem und V.90

Mit der zunehmenden privaten Nutzung des Internet für die vielfältigsten Zwecke wird der Bedarf nach preiswerten Internet-Zugängen für Privathaushalte immer dringender. Dabei haben mittelfristig nur die Techniken Einsatzchancen, die bestehende Infrastruktur nutzen. Die vorgestellten Techniken xDSL und V.90 nutzen das vorhandene Kupferkabel der Telefonleitung für hochratige Datenübertragung, während das Kabelmodem das ebenfalls weit verbreitete Breitband-TV-Kabelnetz für zusätzliche hochratige Datenübertragung nutzbar zu machen versucht.

Industrielle Busse: CAN, Profi-Bus und Co.

Während in der Vernetzung von Arbeitsplatzrechnern mittlerweile Ethernet den Standard darstellt, werden im industriellen Umfeld, beispielsweise in Produktionsanlagen, andere Bustypen eingesetzt. Der Beitrag „Industrielle Busse: CAN, Profi-Bus und Co.Gigabit-Ethernet“ stellt die veränderten Anforderungen in diesem Umfeld vor und beschreibt die Standardlösungen in diesem Bereich.

Voice-over-IP - Telefonieren im Internet

Integrierte Sprach-/Datendienste gelten als Inbegriff einer leistungsfähigen und kostengünstigen Kommunikationsinfrastruktur. In dem Beitrag „Voice-over-IP - Telefonieren im Internet“ wird zuerst die Geschichte von Voice over IP vorgestellt. Eine Vielzahl von Ansätzen wie H.323 und intelligente Audio-Kompressions-Methoden werden als Schwerpunkte dieses Beitrags behandelt. Zusätzlich wird ein Überblick über vorhandene Hard- und Software in diesem Bereich gegeben.

Differentiated Services - Neue Ansätze zur Dienstgüte im Internet

Der einheitliche Best-Effort Dienst des Internet reicht nicht aus, um den Anforderungen der stark unterschiedlichen Anwendungen von Multimedia-Diensten bis hin zu Datenbanksystemen gerecht zu werden. Während mit RSVP und der sogenannten Integrated Services-Architektur bereits schon einmal der Versuch unternommen wurde, Dienstgüteunterstützung im Internet zu ermöglichen, versucht die Differentiated Services-Architektur, die Differenzierung der Dienstgüte mit einfacheren und damit erfolgversprechenderen Mitteln zu erreichen. Der Beitrag stellt die Ergebnisse der derzeit noch lange nicht abgeschlossen Diskussion in diesem Bereich dar.

Tarifierungsmodell im Internet

Mit der angesprochenen Differenzierung von Dienstgüte im Internet ergibt sich fast zwangsläufig die Frage nach den Möglichkeiten, die Nutzung unterschiedlicher Dienste mit dem Benutzer auf der Basis eines transparente Tarifierungsmodells abzurechnen. Der diesbezügliche Beitrag veranschaulicht die Notwendigkeit einer Tarifierung ebenso wie die damit verbundenen Probleme, die ihre Ursache in der Struktur des Internet ebenso wie in dem Fehlen von direkt anwendbaren theoretischen Marktmodellen haben.

Virtuelle private Netze - weltweite LANs

Kaum ein größeres Unternehmen besitzt heutzutage nur einen Standort. Um nun aber trotz verteilter Standorte den Eindruck einer „lokalen“ Vernetzung mit den entsprechenden Dienstgarantien und Sicherheitsmechanismen bieten zu könnnen, wurden sogenannte Virtuelle Private Netze (VPN) entwickelt. Der Beitrag „Virtuelle private Netze - weltweite LANs“ schildert die Möglichkeiten, VPNs zu errichten und geht insbesondere auf Protokoll- und Sicherheitsmechanismen ein.

Management by Delegation

Aufgrund der gestiegenen Anforderungen moderner Netze an das Management ist die klassische zentrale Struktur wie sie das Netzwerkmanagementprotkoll SNMP vorsieht, nicht mehr ausreichend. In dem Beitrag „Management by Delegation“ wird das Konzept des Management by Delegation als mögliche Lösung dieser Probleme in seiner allgemeinen Struktur beschrieben. Die beiden Implementierungen nach IETF bzw. OSI werden schließlich genauer betrachtet und miteinander verglichen.

Wegewahl im Weltall - Routing in Satellitennetzen

Mit zunehmender Bedeutung der weltweiten Rechnerkommunikation wächst auch der Wunsch zur Benutzermobilität. Beim traditionellen Funktelefon stößt man bereits an die Grenzen der Netzkapazitäten. Eine neue Möglichkeit zur drahtlosen Kommunikation, nicht nur für Sprache, bietet hier der Einsatz von Satellitensystemen. Ein enormer Vorteil beim Einsatz der Satellitentechnik liegt dabei in dem großen lückenlos versorgten Gebiet.

Sichere Mobilkommunikation im Internet - Trend in Mobile IP

Mit der Einfürhung von Mobile IP, einer Erweiterung zum bestehenden Internet-Protokoll, wurde es möglich, nicht-stationäre Geräte an das Internet anzubinden. Bamit entstehen offenere Netzstrukturen, die nicht mehr unbedingt im Einflußbereich eines einzelnen Betreibers liegen. Besonderes Augenmerk sollte dabei auf die die Tatsache gelegt werden, daß es nun zu mehreren neuen Kommunikationsbeziehungen innerhalb der Diensterbringung kommt. Neben den beiden Endsystemen sind jetzt weitere Komponenten direkt mit der Weiterleitung der Pakete betraut. Sicherheitsbetrachtungen spielen unter diesen Gesichtspunkten eine besonders wichtige Rolle.

Drahtloses ATM - Handover und Routing

Mit der Erweiterung von ATM in den drahtlosen Bereich ergeben sich eine Vielzahl von neuen Aufgabenfeldern. Zentraler Punkt, um eine nahtlose Kommunikation mit sich bewegenden Endsystemen zu ermöglichen, ist das Handover. Es stellt sicher, daß bestehende Verbindungen für das Endsystem transparent von einem Funkversorgungsgebiet zum nächsten weitergereicht werden. Dies ist jedoch nur so lange effizient möglich, wie es im Festnetzbereich geeignete Wegewahlverfahren gibt, die eine Anpassung an die neuen Verhältnisse ermöglichen.

Evolution von GSM - Datentransfer mit HSCSD und GPRS

Das weltweit erfolgreichste Mobilfunksystem ist ohne Zweifel GSM mit über 100 Millionen Benutzern in über 135 Ländern. Jedoch bietet das vorrangig für die Telefonie ausgelegte System lediglich eine Bandbreite von 9.6 kbit/s für die Datenübertragung an. Der Beitrag „Evolution von GSM - Datentransfer mit HSCSD und GPRS“ stellt zwei Erweiterungen von GSM vor, die Datenraten von über 115 kbit/s anbieten - unumgängliche Schritte, soll das Internet auch in die Mobilkommunikation Einzug halten.

Deregulierung - neue Telefongesellschaften, neue Märkte

Gemäß den Richtlinien der EU wurde der deutsche Telekommunikationsmarkt zum 1.1.1998 privaten Anbietern vollständig geöffnet. Über den Markt wacht nun mehr die Regulierungsbehörde für Telekommunikation und Post. Der Beitrag „Deregulierung - neue Telefongesellschaften, neue Märkte“ untersucht die gesetzlichen und regulativen Grundlagen des liberalisierten Telekommunikationsmarktes und die Position der großen Anbieter auf diesem Markt.

Gigabit Ethernet – Stand und Standards

Artur Hecker

Kurzfassung

Ethernet - die am meisten verbreitete Netzwerktechnologie - geht in die nächste Entwicklungsphase. Der Umstieg in die höhere Zehnerpotenz gestaltete sich z.T. schwieriger als am Anfang angenommen. Mehrere unerwartet aufgetretene Probleme warfen den Entwicklungsprozeß immer wieder zurück. Im Sommer 1998 konnte endlich der erste Standard präsentiert werden. Die Spezifikationen und Beschreibungen der herausgebrachten Standards sind das eigentliche Thema dieser Ausarbeitung; daneben wird auf Probleme, Lösungen und Ideen näher eingegangen, die das Gigabit Ethernet Komitee während seiner Entwicklungsarbeit bewältigen bzw. erarbeiten mußte. Ein kleiner Ausblick in die nächste Zukunft des Gigabit Ethernet schließt die Ausarbeitung.

1 Einführung

Die vor ca. 25 Jahren erschienene erste Ethernet-Lösung (10Base5) benutzte schon alle typischen Eigenschaften, die auch heute angewendet werden, um „Ethernet“ von anderen Technologien zu unterscheiden. Die (logische) Bustopologie, das CSMA/CD-Zugriffsverfahren, die Manchester-Kodierung und die 10MBit/s - Übertragungsrate verfolgten die Weiterentwicklung des Ethernet über 10Base2-Ethernet (1984) und 10BaseT-Ethernet mit seiner Sterntopologie (1990) bis zum Jahre 1995, als die ersten sogenannten *Fast Ethernet* Lösungen spezifiziert und von der IEEE 802.3u Gruppe (100BaseT) als neuer 100MBit/s Standard verabschiedet wurden. Doch bevor das passierte, mußten viele Probleme aus dem Weg geräumt werden. Dabei gingen verschiedene Firmen unterschiedliche Wege, aus denen man zwei grundsätzliche Bestreben ablesen konnte: Während die ersteren versuchten, einen neuen Standard auf bestehender Verkabelung zu erarbeiten, versuchten die anderen, die typischen Ethernet-Merkmale beizubehalten, um eine gewisse Abwärtskomatibilität zur damals am meisten verbreiteten Netzwerktechnik zu erreichen. Diese Kompatibilität forderte Opfer, wie z.B. eine stark reduzierte maximale Segmentlänge. Nichtsdestotrotz bietet der heutige Markt ausschließlich Lösungen von diesem Typ, so daß man schlußfolgern kann, daß die Möglichkeit, bestehende Netzwerkkomponenten parallel zu den neuen betreiben zu können für den Kunden am wichtigsten erscheint. So benutzt die heute am meisten verbreitete 100MBit/s Technologie (100BaseTx) dieselben Merkmale, wie ihr Urahn; vereinfacht gesagt sind lediglich die Kodierung und die Übertragungsrate anders; physikalisch bildet 100BaseTx ebenfalls einen Stern und ahmt damit immerhin eher den 10BaseT-Standard nach. Natürlich spielten der bekannte Name und v.a. der geringere Preis eine nicht zu unterschätzende Rolle.

Deshalb erscheint nicht verwunderlich, daß der nächste Schritt in der Geschichte des Ethernet in dieselbe Richtung geht: Man versuchte, einen 1000MBit/s-Standard zu erarbeiten, bei dem die Parallelverwendung der 100- und sogar 10-MBit/s Komponenten möglich ist. Den dabei aufgetretenen Problemen und ihren Lösungen widmet sich diese Ausführung.

2 Namen und Standards

Gigabit Ethernet (GE) ist der Schritt der Ethernettechnologie in die nächste Zehnerpotenz und das nächste Jahrhundert. Die 120 Mitglieder umfassende *Gigabit Ethernet Alliance (GEA, http://www.gigabit-ethernet.org)* wurde im Mai 1996 gegründet und hat sich die Marktakzeptanz und die Kompatibilität auf die Fahnen geschrieben. Wegen erheblichen Unterschieden bei den Kabelarten wurden zwei Arbeitsgruppen gegründet, die jeweils den 1000MBit/s-Betrieb auf einem der geplanten Medien sicherstellen sollten. Dazu wurden die 802.3z-Taskforce und die 802.3ab Taskforce beim IEEE ins Leben gerufen. Die erste sollte den Betrieb auf allen Glasfaser- und Twinaxkabeln standardisieren, die zweite den Betrieb auf UTP/STP-Kabeln. Je nach verwendetem Medium kann man die Kosten reduzieren; allerdings geht die Verbilligung mit der Verkürzung der Segmentlänge und damit i.d.R. auch der maximalen Übertragungsstrecke einher. Die 802.3z-Gruppe hat ihre Arbeit beendet und die Standards für die Lichtwellenleiter und Twinaxkabel im Mai-Juli 1998 fertiggestellt. Die Arbeit der 802.3ab-Gruppe ist noch nicht abgeschlossen, der Standard für TP-Kabel wird für Mitte-Ende 1999 erwartet.

Die veröffentlichten Standards sind 1000Base-LX, -SX und -CX, deren genaue Zuordnung der Tabelle entnommen werden kann:

Kabel für Gigabit Ethernet (abgeschlossene Spezifikation)

Typ, Kern	Wellenlänge	Segmentlänge	Kabeltyp	
CX, ---	---	2-25 m	Twinax	
SX, 62.5 µm	830 nm	2-275 m	Multimode	teurer
SX, 50.0 µm	830 nm	2-550 m	Multimode	
LX, 62.5 µm	1270 nm	2-550 m	Multimode	
LX, 50.0 µm	1270 nm	2-550 m	Multimode	
LX, 10.0 µm	1270 nm	2-5000 m	Monomode	

Abbildung 1: Gigabit Ethernet: Standards und Medien.

Grundsätzlich ist jeder Lichtwellenleiter aus einem Kern (*Core*), einem Glasmantel (*Cladding*) und einem Kunststoffmantel (*Buffer Cladding*) aufgebaut. Die Unterschiede der Lichtwellenleiter liegen dabei in der Beschaffenheit des Kerns: zwei Kennzahlen sind von besonderer Bedeutung: der Durchmesser und die Brechungseigenschaft über dem Querschnitt des Kerns. Aus diesen Unterschieden, auf die später noch genauer eingegangen werden soll, ergaben sich zwei verschiedene Lichtwellenleiterstandards. Außerdem hat das Komitee noch einen Kupferkabelstandard verabschiedet.

2.1 1000BaseSX (S wie standard)

Dieser Standard beschreibt den GE-Betrieb auf billigeren Multimode-Glasfaserkabeln und einzelnen Gradientenindexmultimodekabeln bei „niedriger“ Wellenlänge. Bei einer Wellenlänge von 830nm sind Segmentlängen von 2 bis zu 550m möglich. Im Gesamtkonzept soll dieser Standard die horizontale Gebäudeverkabelung ermöglichen.

2.2 1000BaseLX (L wie luxury)

Diese Spezifikation beschreibt alle „besseren“ Glasfaserkabel (Gradientenmultimodekabel und v.a. Monomodekabel) bei einer höheren Wellenlänge. Unerwartet tauchte ein bestimmtes Problem mit den Gradientenmultimodekabeln (Differential Mode Delay), das auf die z.T. unzureichende Qualität der heute verfügbaren Kabel dieser Art zurückgeführt werden kann. Die Lösung dieses Problems verzögerte die Verabschiendung des Gesamtstandards und führte zur Überarbeitung vieler Punkte. Mit dem nun entwickelten Zwischenkabel (*Offset Mode Conditioning Patch Cable*) beträgt die maximale Segmentlänge von 2 bis 550m bei einer Wellenlänge von 1270nm. Bei den Monomode-Kabeln ist dieses Zwischenstück nicht notwendig und eine Segmentlänge von bis zu 5000m erreichbar. Mit diesem Werk wird die Backboneverkabelung des GE definiert.

2.3 1000BaseCX (C wie cheap oder copper)

Schon während der Entwicklung der allgemeinen Standards konnte man absehen, daß die Einführung einer Twisted-Pair-Spezifikation länger dauern wird. Da man die junge Gigabit Technologie nicht auf Glasfaser als einziges Medium beschränken wollte und außerdem die kostspieligen Fiberoptic-Tranceiver bei Möglichkeit sparen wollte, die zur Vernetzung mit Glasfaser unbedingt notwendig sind, führte man eine Spezifikation auf Twinax-Kabeln ein. Da dieser Standard auf lediglich 25m Segmentlänge beschränkt ist, empfiehlt die GEA die Verwendung von CX bei der Komponentenvernetzung. Dadurch lassen sich pro Port bis zu 600,- DM oder pro Verbindung bis zu 1200,- DM sparen. Bei den dabei verwendeten Twinax-Kabeln handelt es sich um geschirmtes Zweiadernkabel. Bei der bestehenden Spezifikation braucht man somit zwei Leitungen für eine bidirektionale Verbindung. Die Kabelindustrie hat jedoch schon ein sogenanntes Quad-Kabel speziell für diesen Zweck angekündigt.

3 Schichten (ISO/OSI)

Als Netzwerktechnologie ist die Gigabit Ethernet Spezifikation in den untersten zwei ISO/OSI-Schichten angesiedelt. Diese Schichten sind in mehrere Unterschichten aufgeteilt, die jeweils eine bestimmte Aufgabe übernehmen (siehe auch [Rech98])

3.1 Sicherungsschicht (*Data Link Layer*)

Für Gigabit Ethernet mußten beim Zugriffsverfahren aufs eigentlich Netz kaum Änderungen vorgenommen werden, weil jede GE-Komponente imstande sein sollte, mit anderen Ethernet-Geräten zusammenzuarbeiten. So hat sich an der Spezifikation der LLC-Unterschicht keine Änderung ergeben. Die von ihr (Übertragung der Bits) übergebenen Daten werden von der MAC-Unterschicht ebenfalls auf die typische Ethernetweise verpackt: die MAC-Unterschicht hängt zusätzliche Informationen wie Hardware-Adresse, Startadresse und eine Prüfsumme an die Daten an, indem sie die LLC-Daten in Rahmen (*Frames*) einteilt. Beim Empfang passiert dabei genau das Umgekehrte: die angehängten Daten werden von der MAC-Schicht entfernt und an die zuständige LLC-Schicht in der ursrünglichen Form übergeben. Wenn die Datenmenge dabei die vorgeschriebenen 46 Byte unterschreitet, bringt die MAC-Unterschicht diese mit einem sogenannten *Padding*-Verfahren auf die Mindestlänge. Die Maximallänge für Daten beträgt 1500 Byte. Damit kommt man auf die Gesamtrahmengröße, die im Bereich von 64 bis 1518 Byte liegen darf (siehe Abb. 3).

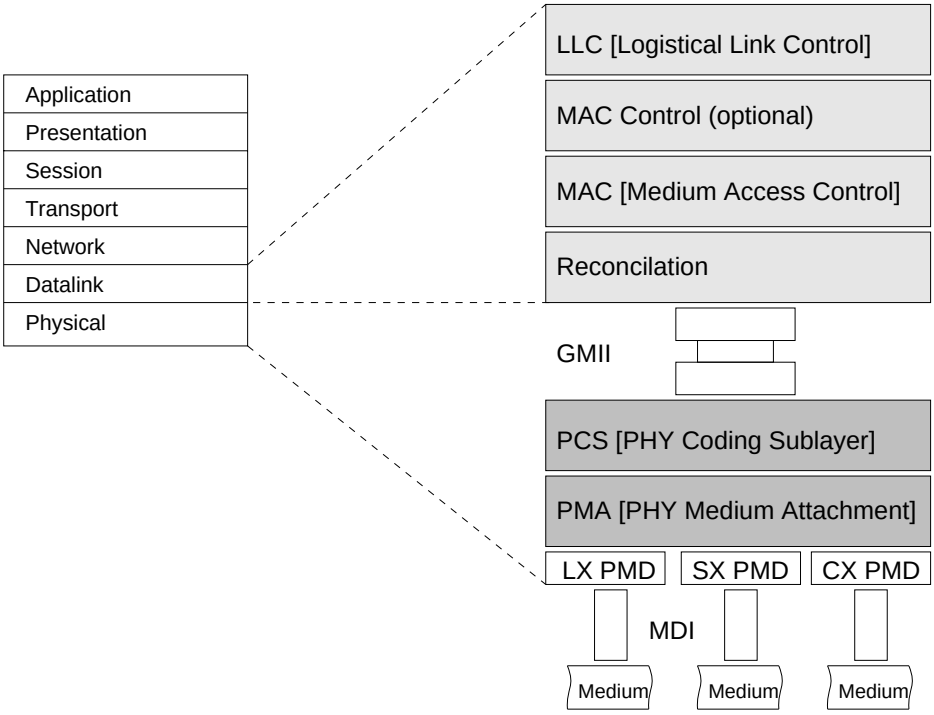

Abbildung 2: Gigabit Ethernet im ISO/OSI-Model

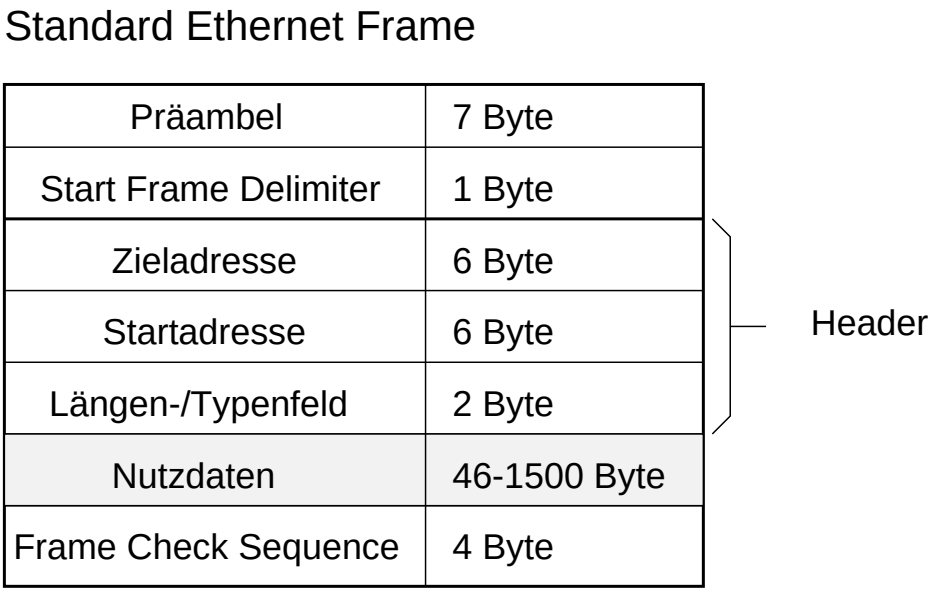

Abbildung 3: Aufbau eines Ethernet Frame

3.1.1 Halbduplexbetrieb

Um die verpackten Daten aufs Medium zu bringen, verwendet der MAC-Sublayer ebenfalls eine bewährte Ethernet-Technik, das bekannte CSMA/CD-Verfahren (*Carrier Sense Multiple Access/Collision Detection*). Dieses bestimmt, wann, wie und wielange eine Station aufs Medium zugreifen darf. Möchte eine Station ein Paket versenden, so überprüft diese, ob das Medium frei ist (*Carrier Sense*). Ist das Medium frei, sendet die Station ihre Daten. Eine Kollision entsteht genau dann, wenn mehrere Stationen ihre Daten quasi gleichzeitig aufs Netz schicken (*Multiple Access*). In diesem Fall springt die Kollisionserkennung der Stationen ein, die bei jedem Senden aktiv wird, und alle Pakete werden verworfen (*Collision Detecti-*

on). Die Stationen warten dann eine zufällige Zeit ab und versuchen, ihre Daten erneut zu senden. Dieses Verfahren ist das Erkennungsmerkmal für Ethernet-Technologien schlechthin und mußte deswegen beibehalten werden. Damit stand das GE-Komitee vor seinem ersten großen Problem: je höher die Übertragungsgeschwindigkeit, desto kürzer ist bei festbleibender Paketgröße die maximal zulässige Strecke zwischen zwei Stationen. Die Ursache dafür ist das Prinzip der Kollisionserkennung. Dieses Problem hätte ohne Änderungen dazu geführt, daß die maximale Segmentlänge auf 20 m reduziert werden müßte. Dies wollen wir uns daher genauer anschauen.

Jeder Sender stellt die Überwachung der Kollisionen nach einer festgesetzten Zeit von 576 Bitzeiten (d.h. Zeit, die der Sender zum Übertragen von 576 Bits braucht) ein. Diese Zahl ergibt sich aus der minimalen Paketlänge (also dem min. MAC-Rahmen) von 512 Bit (64 Byte) und einer folgenden Sperrzeit für die Kollisionserkennung von 64 Bit, die physikalisch bedingt ist. Angenommen, der Abstand zwischen zwei Stationen im Netz ist nun so groß, daß eine Station ein komplettes Paket so schnell abschicken kann, daß nicht alle weiteren Stationen zumindest den Anfang des Pakets mitbekommen. Dadurch hätte eine solcher Stationen die Möglichkeit, selbst ein Paket abzuschicken, da das Medium laut "Carrier Sense" - Mechanismus frei ist. Wir hätten damit zwei Pakete auf dem Medium, sprich eine Kollision. Jedoch könnte der ursprüngliche Sender bei einer genügenden Entfernung seine Kollisionserkennung bereits beendet haben; damit könnte diese (sogenannte *Late Collision*) nicht erkannt werden, und ein Paket ginge unbemerkt verloren.

Die Ausbreitungsgeschwindigkeit v_c des Lichts in der Glasfaser beträgt ca. $200000 km/s$. Bei 1000 MBit/s dauert eine Bitzeit $0,001 \mu s$. Bei 576 Bitzeiten hat man:

$t = 576 \cdot 0,001 \mu s = 0,576 \mu s$

Maximale Strecke damit:

$S = t \cdot v_c = 0,576 \mu s \cdot 200000 km/s = 11,5 m$

Wenn man noch die Verzögerungen in den Geräten beachtet, läßt sich durch diese Rechnung die obenerwähnte maximale zulässige Entfernung zwischen zwei Stationen grob nachvollziehen.

Eine moderne Netzwerktechnologie mit einer maximalen Netzausdehnung von 20 m ist natürlich nicht denkbar. Die Lösung, die man fand, fiel ziemlich einfach aus: Man erhöhte die Mindestpaketlänge und damit auch die "Slot Time", d.h. die Zeit für die eindeutige Belegung des Mediums, auf 512 Byte. Kleinere Rahmen werden mit sogenannten *Extension Symbols* (Erweiterungssymbolen), die nicht mit Daten verwechselt werden können, auf die Mindestlänge aufgefüllt (siehe Abb. 4).

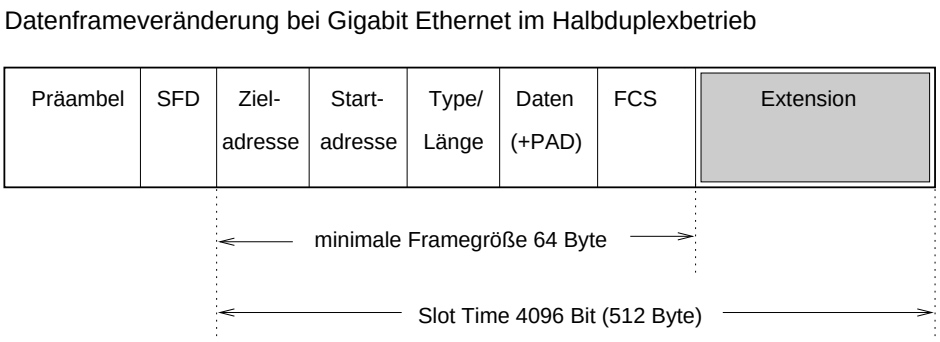

Abbildung 4: MAC-Rahmen in der GE-Spezifikation

Dieselbe Rechnung mit den veränderten Werten ergibt für die Kollisionsüberwachung:

$512 \cdot 8Bit + 64Bit = 4096 + 64Bit = 4160Bit$
$t = 4160 \cdot 0,001\mu s = 4,16\mu s$
$S = 4,16\mu s \cdot 200000km/s = 832m$

Durch die gerätespezifischen Hardwareverzögerungen erhöht sich die Zeit t zusätzlich, was eine weitere Erhöhung der maximalen Segmentlänge bewirkt.

3.1.2 Vollduplexbetrieb

Diese Veränderungen spielen jedoch nur im Halbduplexbetrieb eine Rolle, da im Vollduplexbetrieb definitionsgemäß keine Kollisionen auftreten können. Da jede Station gleichzeitig senden und empfangen kann, ist eine Verlängerung der MAC-Rahmen nicht notwendig. Heute unterstützen fast alle Ethernet-Produkte den Vollduplexmodus. Durch ein *Flow-Control-Verfahren* wird beim GE dafür gesorgt, daß es zu keinem Datenstau kommt: kann ein Teilnehmer keine Daten mehr verarbeiten, teilt er das anderen Stationen mit. Daraufhin reduzieren diese die Datenmenge; die letztere kann jederzeit wieder erhöht werden, wenn der Empfänger nicht mehr unter Last steht.

Die vorgenommenen Änderungen bewahren die vollständige Kompatibilität zu den älteren Ethernet-Netzwerken und versetzen die GE-Komponenten damit in die Lage, sich dynamisch an die verwendete Datenrate anzupassen. Doch die Lösung ist nicht perfekt: Zahlreiche Experimente und *worst case*-Schätzungen zeigen, daß die Datenrate bei sehr vielen extrem kleinen Frames auf 12% des theoretischen Maximums sinken kann. Um die Leistung auch für kleine Rahmen zu verbessern, sieht der GE-Standard eine Möglichkeit zur Gruppierung vor - *Packet Bursting*. Dabei werden viele kleinere Rahmen zu einem großen Paket zusammengefaßt, so daß ein langer Rahmen mit mehr als 512 Byte (also mehr als GE-*Slot Time*) entsteht und fast keine Erweiterungssymbole mehr notwendig sind. Es gibt jedoch eine klar definierte Obergrenze für die maximale Sendezeit, sonst könnte eine Station das Medium für immer belegen: *Burst Limit* = 65536 Bitzeiten (8192 Byte). Ist diese Zeit abgelaufen, darf die Station nur noch das angefangene Paket zu Ende senden. Außerdem wird das erste Paket immer auf die gefordete Mindestlänge von 512 Byte mit Erweiterungssymbolen gebracht (wenn nötig). Alle weiteren Pakete mit ihren Mindestlängen von 64 Bytes werden an das erste Paket so angehängt, daß ein definierter *Interframe Gap* von 12 Bytezeiten dazwischen bleibt, der ebenfalls mit Erweiterungssymbolen aufgefüllt wird (siehe Abb. 5).

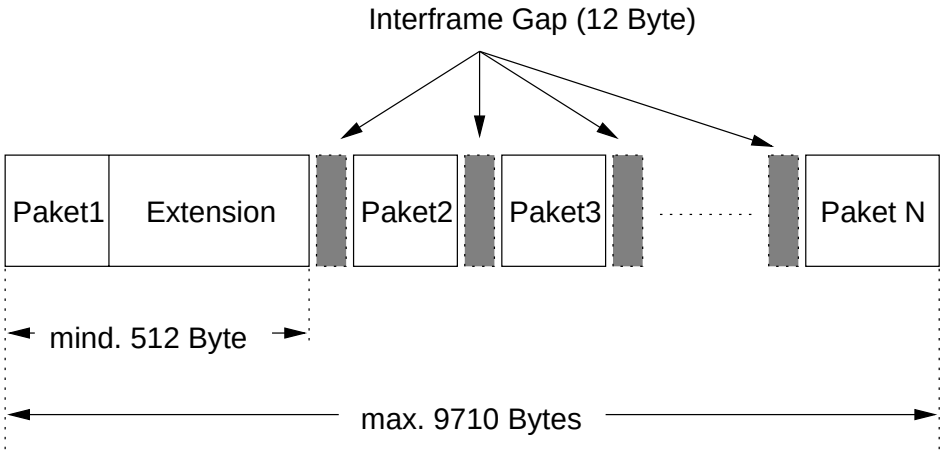

Abbildung 5: Packet Bursting

Eine kleine Rechnung zeigt, wievielen Maximalpaketen dies entspricht:

Gesamtzeit = Burst Limit + MaxLengthPacket = 8192 + 1518 = 9710 Byte

Die Ungleichung

$$\text{anzahl}_{\text{InterframeGap}} \cdot 12 + n \cdot \text{paketLaenge}_{max} < \text{gesamtZeit}$$

liefert für n das gewünschte Ergebnis. Einsetzen (s. Skizze):

$$\begin{array}{lll} \Leftrightarrow & (n-1) \cdot 12 + n \cdot 1518 & < \quad 9710 \\ \Leftrightarrow & 1530 \cdot n & < \quad 9722 \\ \Leftrightarrow & n & < \quad 6,354 \\ \Rightarrow & n = 6, & \end{array}$$

d.h. eine Station darf insgesamt eine Burst-Länge senden, die etwas mehr als sechs Maximalpaketen entspricht.

Fazit: Der Trick mit der Erweiterung löst auf elegante Weise das Entfernungsproblem, ohne den klassischen Ethernetrahmenaufbau zu zerstören. Die zusätzliche Bandbreitenverschwendung, die durch die Auffüllung mit den Erweiterungssymbolen entsteht, läßt sich durch das "Packet Bursting" auf ein Minimum reduzieren und z.T. sogar in eine Leistungsverbesserung umwandeln.

3.2 Bitübertragungsschicht (*Physical Layer*)

Damit sind wir mit den klassischen Unterschichten der 2. Schicht fertig. Beim Gigabit Ethernet wurde jedoch noch eine erweiterte Schnittstelle zwischen die Sicherungsschicht und die Bitübertragungsschicht eingefügt (s. Abb. 2). Ähnlich wie schon die MII-Schicht bei Fast Ethernet, erfüllt die GMII-Schicht *Gigabit Medium Independend Interface* die Aufgaben, die mit der Unterstützung mehrerer Datenraten anfallen. So ermöglicht diese Schicht die Erkennung der momentan verwendeten Datenrate und sorgt allgemein für den Austausch von Informationen über die Verbindungseigenschaften zwischen der PHY- und der MAC-Schicht. Dazu werden beim Verbinden die Übertragungsrate (10/100/1000 MBps) und der Modus (Halb-/ Vollduplex) in einem *Autonegotiation* genannten Verfahren ausgemacht. Das Protokoll für Autonegotiation wurde im Vergleich zum Fast Ethernet geändert: die Informationen werden über spezielle Codegruppen statt über sogenannte Link Pulse ausgetauscht.

Die unterste Schicht im ISO/OSI-Model ist in drei Unterschichten aufgeteilt: *Physical Coding Sublayer (PCS), Physical Medium Attachment (PMA) und Physical Medium Dependent.*

3.2.1 PCS

Ethernet-Technologien verwenden je nach Datenrate verschiedene Kodierungen (s. Abb. 6)
Die Kodierungsunterschicht des GE muß deswegen alle drei Kodierungsarten beherrschen. Die Kodierung spielt eine entscheidende Rolle, denn erst die Wahl einer optimalen Kodierung ermöglicht sichere, dateneffiziente Übertragungen. Der PCS sorgt in einem *Encapsulation Process* außerdem dafür, daß die Daten für die GMII-Schicht unabhängig von der Datenrate immer gleich aussehen, indem alle Änderungen von diesem vorgenommen und wieder rückgängig gemacht werden: z.B. sind die Bitfolgen des *Start of Packet Delimiter* (SOD) bei Fast, Gigabit und „Classic" Ethernet verschieden; GE wandelt außerdem schon das erste Symbol der Präambel zum SOD und setzt ein *End of Packet Delimiter* hinter die *Frame Check Sequence*.

Bei Gigabit Ethernet werden die Daten mit einem von IBM patentierten 8B/10B Verfahren kodiert. Dieses Verfahren ist ähnlich dem von Fast Ethernet und bedeutet zunächst nur, daß acht Bit Binärdaten in zehn Bit lange Codegruppen für die Übertragung umgewandelt werden.

Ethernet	Kodierung
10Base	Manchester (Biphase-L)
100BaseTX	5B/6B NRZ
1000Base	8B/10B NRZ

Abbildung 6: Ethernet-Kodierungen

Das Verfahren ist selbsttaktend, bietet eine Fehlererkennung und sorgt für Gleichspannungsfreiheit. Die Umwandlung von 8 Bit-Blöcken in 10 Bit-Codegruppen erfolgt dabei anhand einer Tabelle, die jedem möglichen Datenoktett (00..FF) jeweils zwei Codegruppen zuweist - eine bestimmte Bitfolge und ihre Negation. Diese sind so gewählt, daß immer die geforderte Mindest- und Maximalanzahl der Pegelwechsel eingehalten wird. Im Laufe der Übertragung werden stets die *Disparität* einer Codegruppe (also die Differenz zwischen der Anzahl der Einsen und der Nullen) und eine *laufende Disparität* (RD) gebildet:
$RD := \sum_i \text{Disparity}_i$

Die Codegruppen sind so gewählt, daß ihre Disparitäten nur die Werte +2, 0 oder -2 annehmen. Dabei stehen in der ersten Spalte der Tabelle nur die Codegruppen mit positiven Disparitäten (oder gleich Null). Ausgehend von einem Startzustand mit laufender Disparität $RD = -1$, wird die einem Oktett entsprechende 10 Bit-Codegruppe gesendet. Ist $RD = +1$, so wird ihre Negation gesendet. (Für Codegruppen mit Disparity = 0 gilt, daß die Disparität ihrer Negation auch 0 ist; wichtig ist dieser Schritt deswegen nur für die Codegruppen mit | Disparity | = 2). Auf diese Weise erreicht man, daß die Anzahl der Nullen und Einsen bei zwei Codegruppen - einer beliebigen und der nach ihr gesendeten - immer gleich ist (*Gleichspannungsfreiheit*)

Die maximal auftretende Baudrate beträgt bei dieser Kodierung 1250 MBaud. Ein Teil der redundanten Symbole, die durch die Umwandlung von acht Bit in zehn Bit entstehen, wird verwendet, um spezielle Signale und Zustände zu kennzeichnen: *Idle Signal, Start of Packet*, etc. Alle nichtdefinierten Kombinationen dürfen nicht auftreten und werden als Fehler (*Violation*) erkannt. So läßt sich aus der Anzahl der Fehlersymbole die Qualität einer Verbindung bestimmen.

3.2.2 PMA

Diese Unterschicht wandelt die vom PCS übergebenen Codegruppen in serielle Daten für den PMD um und umgekehrt. Darüber hinaus ist diese Unterschicht für die Rückgewinnung des Taktes aus dem jeweiligen Kodierungsverfahren zuständig.

3.2.3 PMD

Die unterste Schicht der GE Spezifikation ist, wie der Name schon verdeutlicht, vom Übertragungsmedium abhängig und teilt sich daher in drei Teilbereiche auf, die jeweils den medienabhängigen Standards entsprechen: *SX-PMD* für die Glasfaserübertragung mit kurzer Wellenlänge, *LX-PMD* für lange Wellenlänge und *CX-PMD* für die Übertragung über geschirmte Twinax-Kupferkabel.

4 Probleme und Ideen

4.1 Das Problem mit dem Licht

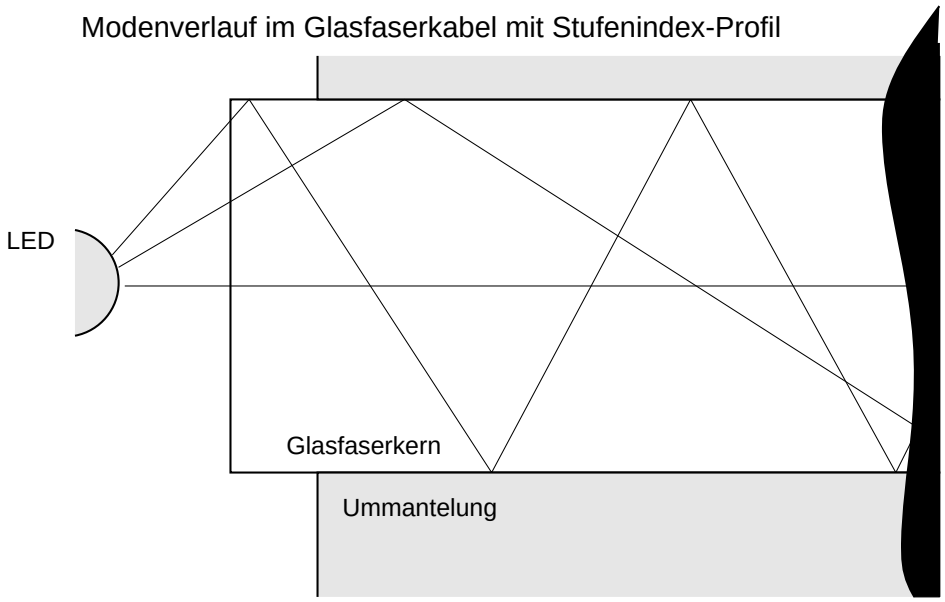

Abbildung 7: Entstehung der verschiedenen Moden

Gigabit Ethernet sieht alle Typen von Glasfaserkabeln zur Übertragung vor. Als Lichtquellen kommen dabei Laser-LEDs mit 830 nm und 1300 nm Wellenlänge zum Einsatz. Die Wahl dieser Spezifikation hat mehrere Gründe.

Eine normale LED strahlt gleichförmig in alle Richtungen (s. Abb. 7). Auf diese Weise entstehen im normalen Glasfaserkabel (*Stufenindex-Profil*) mehrere Strahlenverläufe (*Moden*), die bei einem herkömmlichen Glasfaserkabel unterschiedlich lange Wege mit gleicher Geschwindigkeit zurücklegen. Dies hat zur Folge, daß die Konturen eines Impulses verbreitert werden. Dieser Effekt, als *Dispersion* bekannt, wird noch zusätzlich durch die Tatsache verstärkt, daß eine Lichtquelle nie ganz rein ist; das ausgestrahlte Licht setzt sich also aus mehreren Wellenlängen zusammen - davon hängt jedoch die Ausbreitungsgeschwindigkeit ab.

Die Dispersion steigt mit der Länge der Leitung, da die Impulse kontinuierlich verzerrt werden. Spätestens, wenn die einzelnen Impulse ineinanderragen, kann keine Unterscheidung auf der Empfängerseite vorgenommen werden.

Die einfachste Lösung zur Vermeidung der Dispersion liegt in der extremen Verschmälerung des Kerns einer Glasfaserleitung (Abb. 8).

So gibt es praktisch nur einen Strahlenverlauf, alle Wege sind durch den kleinen Durchmesser fast gleich lang. Die Kabel, die so aufgebaut sind, heißen deswegen *Monomode*-Kabel (das komplette Licht wird durch das Kabelzentrum, auf Mode 0, übertragen), sind jedoch die teuersten: Die Herstellung eines mehrere Kilometer langen Kabels mit einem Kabeldurchmesser, der in der Größenordnung der Lichtwellenlänge liegt ($9\mu m$), ist nicht unproblematisch. Diese Kabel werden hauptsächlich im Bereich der WAN-Verkabelung verwendet, weil die Entfernungen dort nicht anders zu überbrücken sind.

Eine weitere Reduktionsmöglichkeit für Dispersionseffekte liegt in der Verwendung einer *Laser-LED* (LD). Diese LED strahlt von vornherein den Hauptteil des Lichts gebündelt an der Spitze ab. Die Reichweite läßt sich normalerweise erhöhen.

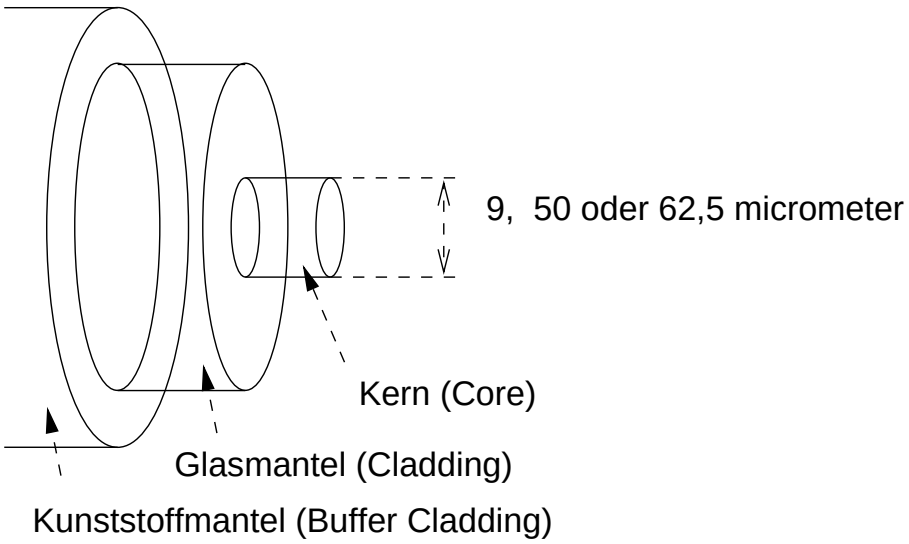

Abbildung 8: Aufbau eines Glasfaserkabels

Da die Monomode-Kabel zu teuer für normalen LAN-Einsatz sind und die Kombination LD - Multimode-Kabel noch immer nicht die gewünschten Reichweiten liefert, dachte man sich eine dritte Möglichkeit aus. Die Ausbreitungsgeschwindigkeit des Lichts ist vom Medium abhängig. Wenn das Licht die Medien wechselt, erfährt es eine Richtungsänderung, die als *Brechung* bekannt ist. Je niedriger die Ausbreitungsgeschwindigkeit im neuen Medium, desto höher ist die Brechung. Um nicht mit absoluten Geschwindigkeiten rechnen zu müssen, vergab man allen Stoffen sogenannte *Brechungsindices*, wobei gilt: Je niedriger der Brechungsindex, desto höher die Geschwindigkeit in diesem Medium.

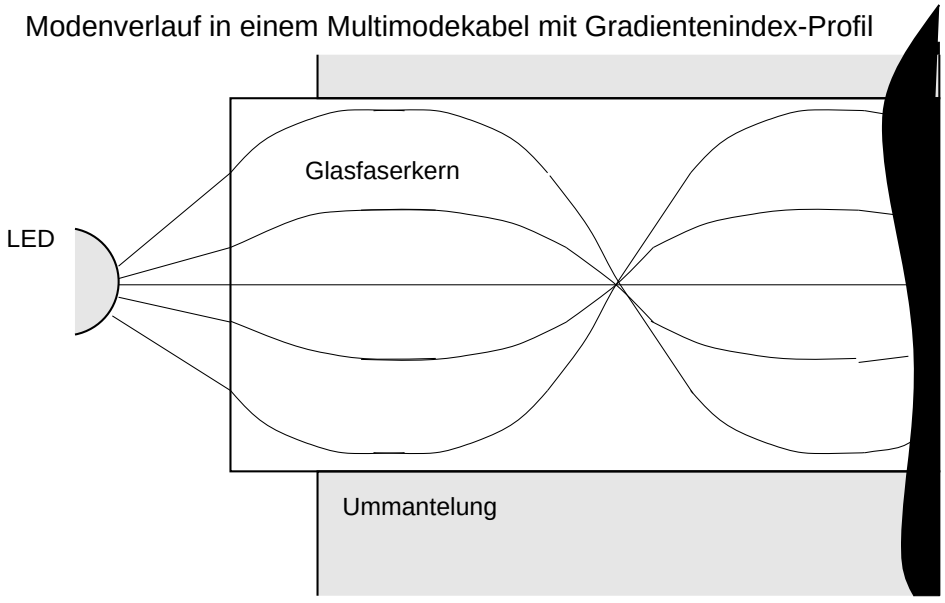

Abbildung 9: Strahlenverlauf in einer Glasfaser mit Gradientenprofil

Die Gradientenlichtwellenleiter machen von den verschiedenen Medien Gebrauch. Bei diesen Kabeln ist der Kern so beschaffen, daß der Brechungsindex zu den Rändern hin abfällt. Auf diese Weise tritt der in Abb. 9 dargestellte Effekt auf. Die Längen der Randwege sind zwar größer, jedoch breitet sich das Licht am Rand mit höherer Geschwindigkeit aus. Folge: kleinere Dispersion.

Doch gerade solche, sogenannte *Gradientenindexmultimodekabel*, haben sich in der Praxis als problematisch im Zusammenhang mit LDs erwiesen. Die Entwickler mußten feststellen, daß viele auf dem Markt verfügbare Kabel nicht das erwartete Profil aufweisen (Abb. 10). Die Funktion zwischen dem Abstand vom Kabelzentrum und dem Brechungsindex fällt nicht, wie erwartet, monoton. Speist man in ein solches Kabel Licht mit einer LD ein, so wird der überwiegende Teil des Lichts auf Mode 0 übertragen. Da dieses Kabel jedoch nicht als Monomode-Kabel konzipiert ist, und die anderen Moden durch diese Änderung inhomogen verlaufen (die Geschwindigkeit und Richtung ergänzen sich nicht wie erwünscht gegenseitig), entsteht im Kabel eine gewisse Instabilität in der Datensignalform. Dieses Problem wird als *Differential Mode Delay* bezeichnet und führte während der Entwicklung zu drastischen Übertragungsproblemen bei höheren Entfernungen.

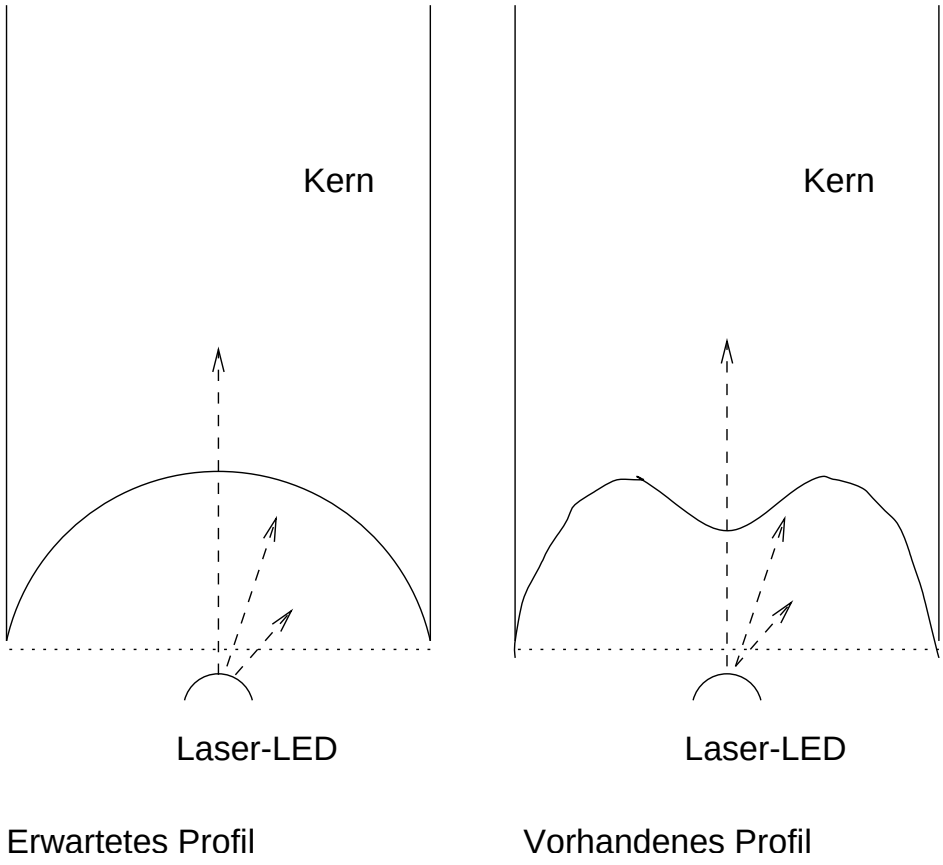

Abbildung 10: Viele Kabel weisen ein verzerrtes Profil auf

Das Gigabit Ethernet Komitee hat zur Unterdrückung des Effekts zwei verschiedene Lösungswege gefunden. Beim SX-Standard wurden die Transeiver in ihren Eingangs- und Ausgangswerten angepaßt. Für den LX-Bereich entwickelte man ein sogenanntes Offset-Mode-Conditioning-Patch-Kabel (Abb. 11). In ausführlichen Tests konnte das GE Komitee beweisen, daß die Verwendung dieses speziellen Kabels die Datenübertragung über die vorgeschriebenen Strecken garantiert.

4.2 Spezielle Problematik der UTP-Kabel

Bis jetzt noch nicht vollständig, aber schon heiß erwartet, sind die Ergebnisse der Arbeit der IEEE 802.3ab Task Force. Doch die Bereitstellung von 1000 MBit/s auf einem ungeschirmten mehradrigen Kupferkabel (“Unschielded Twisted Pair“ oder UTP-Kabel) etwa der Kategorie 5 bringt Probleme mit sich, die schier unlösbar scheinen. So ist das Kabel grundsätzlich für

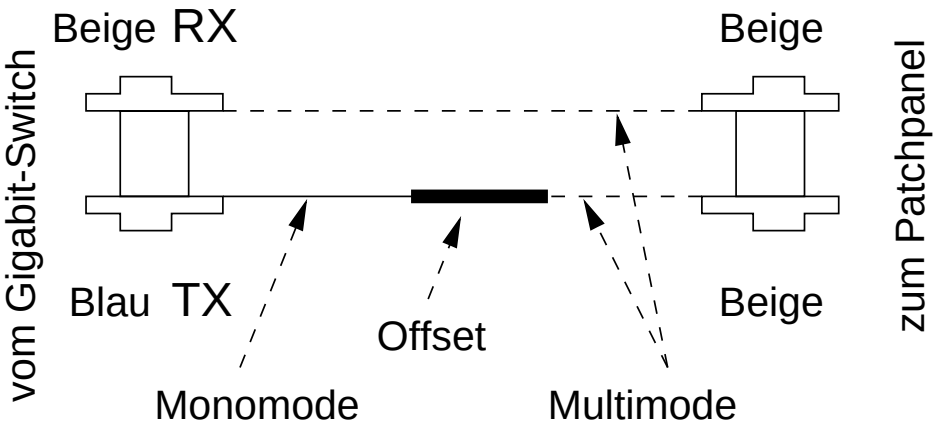

Abbildung 11: "Offset Mode Conditioning Patch"- Kabel

die Datenübertragung von maximal 100 MBit/s ausgelegt; dabei bereitete schon der Spezifikationsentwurf für Fast Ethernet einige Kopfschmerzen. Diese Obergrenze liegt auf der einen Seite in den physkalischen Eigenschaften des Kabels (Übersprechen, Dämpfung), zum anderen in den strengen EMV-Normen (elektro-magnetische Verträglichkeit).

Der erste Schritt auf dem Weg zur Lösung bestand darin, anstatt der sonst verwendeten Bitrate (1250 MBit/s) eine niedrigere zu verwenden (1000 MBit/s). Der zweite Schritt war, von Anfang an alle vier Adernpaare eines UTP-Kabels zu verwenden (die meisten Ethernet-Lösungen verwenden nur zwei Paare). Durch diese zwei Schritte reduzierte man die Datenrate auf 250 MBit/s pro Adernpaar.

Für Vollduplexbetrieb müssen die Daten leider in beide Richtungen übertragen werden können, selbst wenn die Leitungen schon für die Übertragung in eine Richtung belegt sind. Was sich zunächst widersprüchlich anhört, wird durch ein vom ISDN bekanntes Verfahren namens *Echo Cancellation* elegant gelöst: Am Empfänger jeder Station wird das eigene (bekannte) gesendete Signal und alle entstandene Echos vom insgesamt anstehenden Eingangssignal abgezogen; dadurch bleibt aus dem Gemisch der beiden Richtungen nur das Signal der Gegenseite übrig.

Die Hauptreduktion besteht jedoch in der Verwendung eines PAM5-Verfahrens, das die Daten über fünf Ebenen verteilt (-2, -1, 0, +1,+2) und auf diese Weise die Übertragungsfrequenz ums Fünffache reduziert. Die zusätzlich verwendete *Trellis*-Kodierung verteilt die acht Datenbits und ein Parity-Bit zudem so auf die einzelnen Adernpaare innerhalb der fünf Signalebenen, daß sich die elektrischen Eigenschaften des Signals verbessern und am Ende eine geringere Bit-Fehlerrate herauskommt; dabei bleibt sogar genug Redundanz zur Fehlerbeseitigung. Ein *Scrambling* (Verwürfeln) sorgt für gleichmäßige Verteilung der Signalzustände, was die EMV-Eigenschaften deutlich verbessert.

5 Zukunftsmusik

Der 802.3ab-Standard steht inzwischen als *Draft* (Entwurf) zur Verfügung, und es bleibt abzuwarten, wie sich der Entwurf noch im Detail entwickelt. Für Backbone-Bereich kommt in den meisten Fällen sowieso die Glasfaser zum Einsatz. Für den flächendeckenden Einzug von Gigabit Ethernet ist 802.3ab jedoch notwendig, das Thema bleibt also hochaktuell.

Interessant sind sicherlich auch die Bestrebungen, eine bestimmte Datengüte zu garantieren (*Quality of Service*) (QoS). Die Spezifikationen, geschweige denn Implemtierungen, stehen jedoch noch nicht fest (im Gegenteil zu ATM), gehen aber andere Wege als der QoS-Vorreiter ATM (s. [Jürg98]): Die Etablierung der Dienstgüte etwa geschieht bei ATM so, daß der Sender

für die Bereitstellung einer bestimmten Bandbreite zuständig ist - die QoS-Parameter werden über eine Vollduplex-Verbindung ausgehandelt und stehen danach garantiert zur Verfügung. Bei GE wird der Empfänger die benötigte Bandbreite anfordern müssen, die danach „mit hoher Wahrscheinlichkeit“ zur Verfügung gestellt wird.

Die Gigabit Ethernet QoS-Bereiche, für welche die Spezifikation existiert, haben mit älteren Geräten zu kämpfen, die diese Techniken, z.B. die Prioritätssteuerung (802.1P), nicht unterstützen. Im (QoS-)Bereich der Verkehrs- und Flußsteuerung ist ATM ebenfalls nicht nur vielseitiger sondern v.a. auch fortschrittlicher.

GE ist aber einfacher zu handhaben, leicht zu installieren und billiger als ATM. Wenn es zudem auch noch eine gewisse Dienstgüte bietet, gewinnt es an zusätzlicher Lukrativität.

6 Fazit

Bis jetzt wird GE hauptsächlich als High-End-Anbindung von Servern und Switches angeboten und ist immernoch recht teuer. Außerdem wird kaum eine Firma neu verkabeln wollen, nachdem die meisten gerade ihre TP-Verkabelung installiert haben. Mit der Einführung des 802.3ab darf man jedoch eine starke Verbreitung des Standards und die ersten deutlichen Preisstürze erwarten. Insgesamt ist GE sicherlich eine interessante und in bestimmten Einsatzgebieten sinnvolle Alternative zu ATM.

Literatur

[Jürg98] Bernd Reder Jürgen Brockhage. Starkes Rückgrat. *Gateway*, Oktober 1998.

[Rech98] Jörg Rech. Volldampf voraus ... Die Technik von Gigabit Ethernet. *c't - Magazin fü Computertechnik* (13), 1998, S. 212–223.

Breitband-Internet-Zugänge: V.90, xDSL, Kabelmodem

Norbert Schmidt

Kurzfassung

Das Internet ist seit der Einführung ein für Firmen immer größer werdender Wirtschaftsfaktor und für den Privatmann ein immer interessanteres Medium geworden. Mit wachsender Komplexität der Internetinhalte und damit immer größer werdenden Datenpaketen, die im Internet verschickt werden, gibt es einen Bedarf an sehr schnellen Zugangstechniken. Das Modem, das die Telefonleitung zur Übertragung nutzt, ist mit einer Geschwindigkeit von 56 KBit/s an der Obergrenze für diese Technik angelangt. Ebenso das Telefonkabel für die Übertragung nutzend, schafft man mit Hilfe der xDSL-Technik Übertragungsraten von bis zu 52 MBit/s. Eine Alternative dazu bietet das Kabelmodem, das das Kabelfernsehnetz benutzt. Hiermit erreicht man eine Rate von bis zu 40 MBit/s. Diese Techniken und deren praktische Einsatzmöglichkeiten werden in diesem Beitrag vorgestellt.

1 Einleitung

Das 1969 für militärische Zwecke in den USA entwickelte ARPANET wurde nach Beendigung des Kalten Krieges für die Allgemeinheit geöffnet. Durch Vereinigung mit anderen großen Netzen wie BITNET, USENET, UUCP und vielen anderen entstand das heute unter dem Namen Internet bekannte weltweite Datennetz. Das Internet, grob definiert als Netzwerk von Computern, die das TCP/IP-Protokoll benutzen, präsentiert sich heute also als Verbindung vieler, von verschiedenen Organisationen betreuter Teilnetze. Mit zunehmendem Wachstum wurde das Internet für Firmen ein immer größer werdender Wirtschaftsfaktor und durch ein explosionsartiges Ansteigen von Informationen und Dienstleistungen ein für den Privatmann immer interessanter werdendes Medium. Heutzutage kann es sich nahezu kein Unternehmen mehr leisten, im Internet nicht vertreten zu sein. Es gibt zur Zeit im Internet rund 9,5 Mio. Rechner und 39 Mio. Nutzer. Mit steigendem Bedarf kam die Frage auf: Wie kann ich dem Großteil der Bevölkerung einen Internetzugang zur Verfügung stellen? Den Anfang dafür machte das Modem. Mit einer maximalen Schrittgeschwindigkeit von 1200 Baud und der Übertragungsgeschwindigkeit von 2400 Bit/Sekunde begann der Höhenflug des Modems mit dem V.26bis Standard. Als Übertragungsmedium wurde das ohnehin weitverbreitete Telefonkabel genutzt. Die Technologie entwickelte sich bis heute zum V.90 Standard, der eine Übertragungsgeschwindigkeit von bis zu 56.000 Bit/Sekunde bietet. Nach allgemein anerkannter Meinung bilden eben diese 56.000 Bit/Sekunde für die Analogmodem-Technik die absolute Spitze der Fahnenstange. Mit wachsender Komplexität der Internetinhalte wird jedoch der Ruf nach schnelleren Techniken laut. Ebenso die Telefonleitung nutzend, allerdings nicht wie das Modem lediglich auf das Sprachband beschränkt, präsentiert sich die Familie der xDSL-Techniken (ADSL, SDSL, HDSL, VDSL). VDSL als schnellste dieser Familie schafft es auf bis zu 52.000.000 Bit/Sekunde. Weitere Techniken versuchen andere Netze als das Telefonnetz als Datenträger zu benutzen. Das Kabelmodem nutzt das Fernsehnetz, das fast ebenso verbreitet ist wie das Telefonnetz, und erzielt damit momentan Übertragungsraten von bis zu 40.000.000 Bit/Sekunde.

2 Das V.90-Modem

2.1 Einführung von X2 und K56flex

Lange Zeit ging man davon aus, daß mit 33.600 Bit/Sekunde (V.34) die Nutzung des Sprachbandes des Telefonnetzes ausgeschöpft waren. Um so überraschter war man, als die Firma Rockwell im August 1996 ankündigte, man könne mit einer neuen Technologie die Übertragungsgeschwindigkeit von Modems auf maximal 56.000 Bit/Sekunde anheben. Kurz darauf eröffnete der Konkurrent US Robotics, ebenso an einer solchen Technik zu arbeiten. Der Knackpunkt war, daß die beiden Firmen zwar sehr ähnliche jedoch leider keine vollständig kompatiblen Verfahren entwickelten. Wie leider so oft in der Branche scheiterten die Bemühungen um eine Standardisierung. So kamen zwei verschiedene 56-k-Verfahren auf den Markt. Die Variante von der Firma US Robotics wurde X2 getauft, während die Firma Rockwell ihre Version k56flex nannte. Die Technologie beider Varianten ist sehr ähnlich. Bei beiden Verfahren gibt es zwei Arten von Endgeräten. Auf der einen Seite, üblicherweise beim Internet-Provider, steht ein Modem-Rack, das als Host bzw. Server fungiert. Der Host muß direkt an einer digitalen Leitung angeschlossen sein, hierzulande üblicherweise eine Bündelung von ISDN-B-Kanälen. Auf der Gegenseite steht der Client, das Endkunden-Modem. Es muß über eine analoge Leitung an einer Digitalen Vermittlungsstelle angeschlossen sein. Die möglichen 56.000 Bit/Sekunde Übertragungsgeschwindigkeit sind nur in Richtung vom Host zum Client (Downstream) möglich und setzen optimale Leitungsqualität voraus. In der Gegenrichtung kommt grundsätzlich ein herkömmliches Verfahren zum Einsatz, gewöhnlich V.34 mit bis zu 33.600 Bit/Sekunde. Erfüllt die Verbindung die Anforderung des Verfahrens nicht, wird in beiden Richtungen V.34 verwendet. [Koss98b] [Lubi97]

2.2 56k-Technologie Ein Widerspruch zu Shannon?

In der ersten Hälfte dieses Jahrhunderts hat sich der Wissenschaftler Shannon mit der theoretischen Kapazität von Datenübertragungskanälen befaßt. Nach Shannon gibt es einen eindeutigen Zusammenhang zwischen der verfügbaren Bandbreite, dem Verhältnis von Signal- und Rauschpegel und der maximal möglichen Anzahl übertragener Bit pro Sekunde. Nach der Formel von Shannon können bei einer praktisch nutzbaren Bandbreite von rund 3kHz und einem Signal- Rauschpegelverhältnis von in der Praxis 30 bis 35 dB über einen analogen Telefonkanal 30.000 bis 35.000 Bit/Sekunde übertragen werden. So erklärt sich, warum man glaubte mit V.34 (33.600 Bit/s) ans Limit gestoßen zu sein. Ist eine Downstream-Übertragungsrate von 56 kBit/s nun ein Widerspruch zu Shannon? Nein, Shannons Limit gilt selbstverständlich nach wie vor. Geändert haben sich die Voraussetzungen. Statt eines auf beiden Seiten analogen Übertragungskanals ist nun eine Seite digital. Die dort gesendeten Daten gelangen verlustfrei bis in die Vermittlungsstelle des Kommunikationspartners. Der Digital/Analog-Wandler in der Vermittlungsstelle wird so zum vorgelagerten Line-Interface des Host-Modems. Anders als bei der Analog/Digital-Wandlung tritt hierbei kein Quantisierungsrauschen auf, es wird exakt der gewünschte Analogwert reproduziert. Dahinter folgen nur wenige Kilometer Kupferkabel bis zum Modem des Teilnehmers, auf denen zwar analog übertragen wird, jedoch nicht mittels der Modulation der Phase und Amplitude eines Trägersignals. Statt dessen werden Spannungswerte gesendet. Hier finden sich keine Verstärker, Wandler, Konzentratoren oder Switches mehr, nur noch zwei Kupferadern. Für diese gilt das Shannonsche Limit auch, doch sind sowohl Rauschabstand als auch Bandbreite wesentlich höher als für eine leitungsvermittelte Verbindung. In der anderen Richtung ist es schwieriger. Während die Digitalseite durch geeignete Kodierung dafür sorgt, daß die Analogseite die gesendeten Bits dekodieren kann, besteht dieser Weg nicht in der anderen Richtung. Um exakt vorhersagen zu können, welchem gesendeten Analogwert der A/D-Wandler welchen digitalen Wert zuordnen wird und in welchem Zeitraster sie gesendet werden müssen, wäre eine ungleich aufwendigere Probingphase

notwendig, die derzeit noch nicht beherrscht wird und möglicherweise generell zu lange dauern würde, um für Kurzverbindungen noch rentabel zu sein. [Lubi97] [Till97]

2.3 Ein einheitlicher Standard muß her: V.90

Die Einführung von zwei verschiedenen Techniken für den 56k-Markt hatte fatale Folgen. Obwohl die Internetgemeinde die neue Technik begrüßte, wollten viele abwarten, welcher Technik die Internet-Anbieter den Vorzug geben. Die Anbieter warteten ihrerseits ab, was sich am Markt durchsetzen würde. Ein typisches Henne-Ei-Problem. Sowohl bei Rockwell als auch US Robotics blieben die Verkaufszahlen weit hinter den Erwartungen zurück, und die Hersteller sahen ihre erhofften Umsätze schwinden. Doch trotz mehrerer Verhandlungen konnte man sich erst im Februar 1998 auf ein einheitliches Verfahren einigen: V.90. Das geschah in Abstimmung mit dem weltweit akzeptierten Standardisierungsgremium ITU (International Telecommunication Union), das am 17.09.1998 V.90 endgültig verabschiedete. [Koss98b] [Lubi97]

2.4 56k-Technik in der Praxis

V.90 bekam großen Zuspruch seitens der Hersteller und wurde von allen Seiten umgehend implementiert. Damit waren drei unterschiedliche Techniken am Markt, was die Kunden noch mehr verwirrte. Doch es zeichnet sich ab, daß V.90 auch auf Anwenderseite bald den Durchbruch schaffen wird. Durchschnittliche Connect-Raten in Deutschland liegen bei etwa 46.000 Bit/Sekunde. Voraussetzung ist dafür jedoch, daß die Technik auf beiden Seiten korrekt funktioniert. Die Probleme für schlecht funktionierende Technik liegen dabei zumeist auf Seiten der Provider, also der Hosts. Schlechte Software auf Terminal-Servern ist ein Problem mit dem die Anbieter zu kämpfen haben. Außerdem müssen die Software-Updates im laufenden Betrieb eingespielt werden, was in der Umstellungsphase für weitere Probleme sorgen kann. Fast alle Provider haben inzwischen neben dem K56flex oder X2 auch schon einen V.90 Zugang, der sich wohl in Zukunft mehr und mehr durchsetzen und auch technisch verbessern wird. Eigentlich jedes heute gekaufte Modem beherrscht zwar sowohl V.90 als auch eines der anderen beiden Verfahren. Man sollte allerdings darauf achten, daß man auf jeden Fall ein Modem mit Flash-ROM bekommt, damit man Firmware jederzeit auf eine neuere Version bringen kann. Die V.90 Technologie ist wegen ihres jungen Alters eben noch nicht endgültig ausgereift. [Koss98b] [Lubi97]

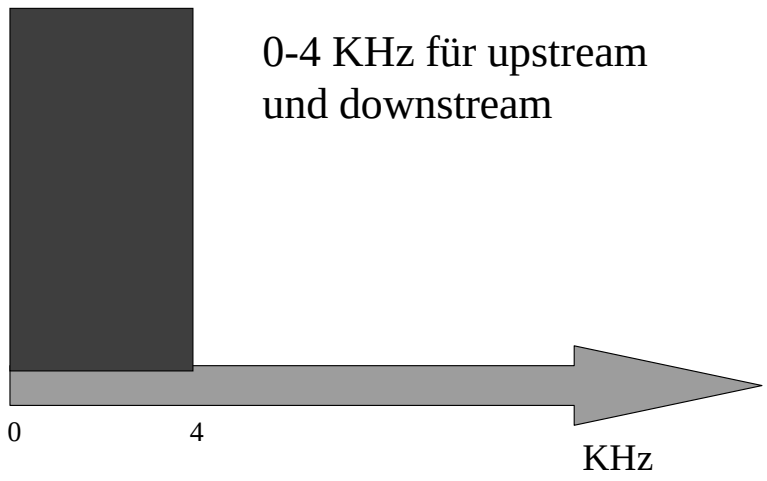

Abbildung 1: Benutzte Frequenzen bei V.90

3 xDSL

Während das Modem auf dem Kupferdraht der Telefonleitung nur ca. 3kHz Bandbreite benutzt, liefert das Medium, die entsprechende Technik vorausgesetzt, durchaus eine viel größere Bandbreite. Da nach Shannon die Bandbreite direkt mit der theoretisch möglichen Übertragungsrate zusammenhängt, kann man durch Erhöhen der Bandbreite unmittelbar den Datendurchsatz steigern. Das macht sich die xDSL-Technik (Digital Subscriber Line) zunutze. Hier wird eine Bandbreite von bis zu 1 MHz benutzt, bei der professionellen Variante VDSL sogar bis zu 30 MHz. Damit nutzt die xDSL-Übertragungstechnik die Kapazitäten der vorhandenen zweiadrigen Anschlußleitungen aus Kupfer wesentlich effektiver als bisherige Techniken. Obwohl in der Literatur gelegentlich von xDSL-Modem gesprochen wird, ist die Assoziation mit einem Modem falsch, denn die Daten bleiben auf der kompletten Übertragungsstrecke digital. Im Unterschied zu einem Modem ist es keine Technik, mit der zwei Nutzer Ende-zu-Ende über einen Telefonkanal Megabit-schnell kommunizieren. Die xDSL-Technik entspricht eher einem Netzwerkkonzept, bei dem einzelne, sternförmig verteilte Stationen an einem zentralen Server angeschlossen sind. Wählverbindungen zwischen zwei Anwendern sind bei der Datenübertragung nicht möglich. Der technische Ansatz der xDSL-Familie läßt sich am ehesten mit ISDN vergleichen. In beiden Fällen wird die Anschlußleitung breitbandiger als bisher genutzt. Und wie ISDN so verwendet auch xDSL an den Enden der Kupferadern spezielle digitale Übertragungstechnik. Beim Nutzer steht im Fall von ISDN der Network Terminator (NT), im Fall von ADSL der ADSL-Adapter. In beiden Fällen steht zum Anschluß von Endgeräten eine definierte Schnittstelle zur Verfügung. Angefangen hat alles in den 80er Jahren mit der rund 160 kBit/s schnellen digitalen Anschlußleitung DSL (Digital Subscriber Line). Anfang der 90er kamen die nächsten Entwicklungsstufen HDSL und SDSL mit bis zu 2 Mbit/s. Als Nachfolger davon wurde ADSL entwickelt, das bis zu 9 Mbit/s schafft. Ende der 90er entstand dann das bis zu 52 Mbit schnelle VDSL. [Till97] [Sand98] [Schm98] [Koss98a]

3.1 HDSL

Der Auslöser für die Entwicklung von HDSL war der erhöhte Bedarf der Netzbetreiber an kostengünstigen 2-Mbit-Systemen für den Einsatz im Ortsbereich. Bis dahin waren sogenannte T1- und E1-Systeme im Einsatz (1,544 Mbit/s, 2,048 Mbit/s). In den frühen 60er Jahren entwickelt, belegen beide Übertragungsarten jeweils zwei der ineinander verdrillten Adernpaare im Ortsnetz. Bedingt durch die Übertragungsverfahren liegt die maximale Länge wegen der hohen Dämpfung der Adernpaare z.B. bei der E1-Leitung bei etwa 1 km. Zur Überbrückung größerer Entfernungen müssen daher zwangsläufig teure Zwischenverstärker zur Regeneration der Signale eingesetzt werden. Die HDSL-Technologie (High Data Rate Digital Subscriber Linie) wurde in erster Linie als kostengünstige Alternative zu den T1/E1-Leitungen konzipiert. Bedingt durch ein anderes Leitungsprotokoll und eine leistungsstarke Echokompensation kann ein HDSL- System gegenüber T1/E1 die drei- bis vierfache Leitungslänge ohne Regenerator überbrücken. Dieser Vorteil senkt sowohl die Investitions- wie auch die Betriebskosten. Ein weiterer Vorteil von HDSL ist die relativ geringe Störung der benachbarten Adern. Üblicherweise werden die einzelnen Adernpaare in größeren Kabeln sehr eng mit hunderten von anderen Adernpaaren verlegt. Während bei T1/E1-Leitungen die benachbarten Adernpaare wegen der Einstrahlungen kaum für andere Anwendungen wie z.B. die Telefonie nutzbar sind, ist dies bei HDSL nicht der Fall. HDSL benötigt mit bis zu 240 kHz deutlich mehr Bandbreite als ISDN, aber genau wie dort kann der analoge Telefondienst nicht mehr im Basisband auf der gleichen Leitung übertragen werden. Eine gemeinsame Nutzung des Adernpaares scheidet also aus. Unter Berücksichtigung der schon erwähnten Störungen erfordert der HDSL-Einsatz im Massengeschäft einen umfassenden und teuren Ausbau des Kabelnetzes. Daher gingen HDSL-

Strecken nur in geringen Stückzahlen in Betrieb, eine Nutzung für private Anwendungen kam kaum in Betracht. [Till97] [Sand98] [Sier98]

3.2 SDSL

Für die SDSL-Technologie (Single Line Digital Subscriber Line) gilt im Grunde das gleiche wie für HDSL. Im Unterschied zu HDSL benötigt der Betreiber für die Übertragung allerdings nur noch ein Adernpaar. Außerdem nutzt SDSL in der Regel Frequenzen oberhalb der von analogen Telefondiensten, so daß der Telefondienst parallel laufen kann. Der Preis für diesen resourcenschonenden Vorteil ist eine gegenüber HDSL um 20% geringere Reichweite von etwa 3 km. Damit ist gleichzeitig ein großer Teil der Anschlußleitungen nicht zu überbrücken, was letztlich ebenfalls den Einsatz im Massengeschäft verhindert. [Till97] [Schm98]

3.3 ADSL

ADSL (Asymmetric Digital Subscriber Line) ist der Nachfolger von HDSL. Das Ziel war eine noch größere Bandbreite, keine Regeneratoren einzusetzen und POTS (Plain Old Telephone Service) auf dem gleichen Adernpaar zuzulassen. Während mittels HDSL/SDSL breitbandige Duplexverbindungen hergestellt werden können, ist ADSL vor allem für asymmetrische Multimediadienste wie z.B. Video-on-Demand geeignet. Upstream schafft man lediglich bis zu 768 kBit/s, während man downstream bis zu 8,2 Mbit/s geliefert bekommt. Gleichzeitig ist sogar die ohne Regenerator überbrückbare Leitungslänge gegenüber HDSL vergrößert. ADSL schafft bei 2 Mbit/s 4 bis 6 km und bei maximaler Datenrate immer noch 2 bis 3 km. Der ADSL-Standard erlaubt eine sehr flexible Aufteilung der genannten Brutto-Bitraten auf verschiedene Kanäle und damit eine Zuordnung der gesamten Kapazität zu verschiedenen Anwendungen. In Upstream-Richtung sind die Grundstufen 16, 64, 160, 384, 576 und 768 kBit/s vorgesehen. In Downstream-Richtung 2.048, 4.096 oder 6.144 Mbit/s. Zusätzlich lassen sich weitere schmalbandige Duplexkanäle einrichten. Das ADSL- System enthält einen speziellen Steuerkanal mit 16 bzw. 64 kbit/s Kapazität, der für die Signalisierung zwischen den Netzknoten und dem Nutzer vorgesehen ist. Auch darin spiegelt sich eine Verwandschaft zu ISDN wieder, das für diesen Zweck den D-Kanal verwendet. Der ADSL-Standard integriert außerdem die analoge Telefonie und den digitalen Nachfolger ISDN. Die analogen Dienste wie Sprache, Fax oder auch Daten werden nach wie vor im Basisband auf der Kupferleitung übertragen. ADSL belegt erst den Frequenzbereich ab ca. 20 kHz und überläßt POTS damit seinen angestammten Platz im Frequenzspektrum. Die Trennung von ADSL und POTS erledigen sogenannte POTS-Splitter. Solche Baugruppen, die eine Hoch- und Tiefpaßfilterung vornehmen, sind Bestandteil jeder ADSL-Übertragungseinheit. Der digitale Dienst ISDN wird dagegen komplett in einen der möglichen 160-kBit- ADSL-Kanäle verlegt und damit innerhalb des ADSL-Systems übertragen. Der Verbleib von ISDN im Basisband hätte eine zu große Verschiebung des ADSL-Spektrums zur Folge, und die damit verbundenen höheren Dämpfungen hätte die Reichweite weiter reduziert. Hierzulande wird die aktuelle Entwicklung von ADSL hauptsächlich von der Telekom vorangetrieben. Unter dem Namen T-DSL startete Ende letzten Jahres mit einem Pilotprojekt in Münster die sukzessive ADSL-Aufrüstung der Telekom. Weitere Pilotprojekte der Telekom wie z.B. in Köln und Bonn sind Mitte Juni an den Start gegangen. Bis zum Jahr 2003 will die Telekom in mehreren Etappen ca. 70 Ortsnetze mit ADSL-Technik ausrüsten und damit bis zu 80% der Geschäfts- und 50% der Privatkunden erreichen. [Till97] [Sand98] [Schm98] [Sier98] [Koss98a]

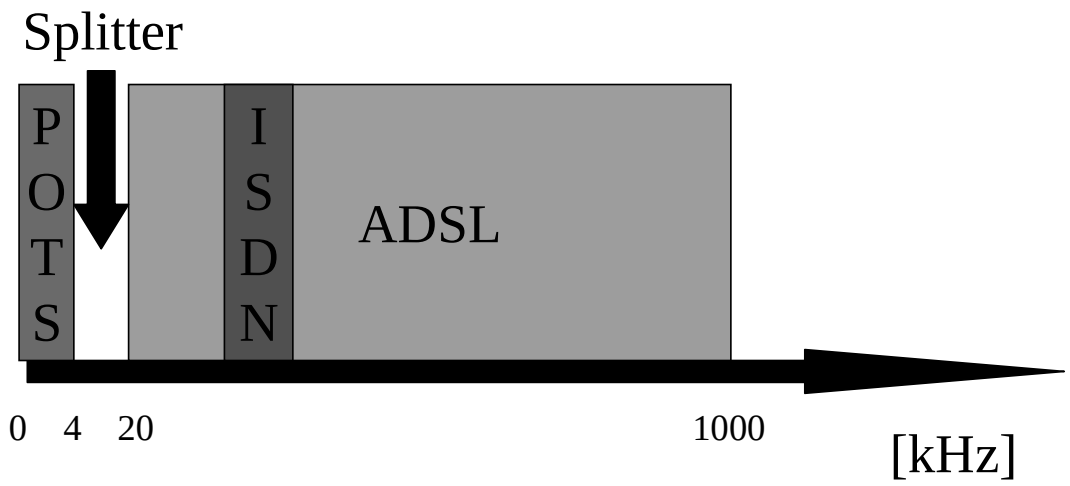

Abbildung 2: Benutzte Frequenzen bei ADSL

3.4 VDSL

Bei 6 bis 8 Mbit/s ist eine Kupferader aber noch lange nicht voll ausgereizt. Wenn der Betreiber die ohne Regeneratoren überbrückbare Reichweite reduziert, so lassen sich sogar noch höhere Datenraten erzielen. Die meisten Telefonnetze sind heutzutage Hybridnetze bei denen die Glasfaser und das Kupfer eine wirtschaftlich sinnvolle Koexistenz führen. Die Glasfaser wird zunehmend auch im Ortsbereich eingesetzt, häufig bis zu den Verteilern am Straßenrand. In einem solchen Hybridnetz beträgt die Länge des kupferbasierten Leitungsendes bis zum Nutzer nur wenige hundert Meter bis zu zwei Kilometern. Für diesen Bereich wurde VDSL mit einer maximalen Übertragungsrate von bis zu 52 Mbit/s entwickelt. Im Gegensatz zu ADSL verbleibt ISDN im Basiskanal. [Till97] [Schm98]

3.5 UDSL

UDSL (Universal Digital Subscriber Line) ist eine mit ADSL verwandte Technologie, die sich derzeit in der Standardisierung befindet. UDSL wird auch als splitterloses ADSL bezeichnet. Es soll ohne Splitter auskommen und dadurch preisgünstiger und einfacher zu installieren sein als ADSL. Damit könnten UDSL-Geräte in die Fußstapfen der aktuellen Sprachband-Modems treten. Bekannte Modemhersteller wie Rockwell oder Motorola unterstützen UDSL bereits jetzt einhellig. Durch den Wegfall des Splitters kann eine gleichzeitige Datenübertragung die Sprachqualität jedoch hörbar beeinträchtigen, so daß manche Hersteller dennoch Splitter empfehlen. UDSL soll nur 1,5 Mbit/s in Empfangsrichtung und 128 kBit/s in Senderichtung bieten und eine Reichweite bis zu 4,5 Kilometern erzielen. An der UDSL-Spezifikation beteiligen sich viele Unternehmen im Rahmen der Universal ADSL Working Group (UAWG). Der Gruppe gehören neben Microsoft, Intel und Compaq eine Reihe namhafter Netzbetreiber und Hersteller an. Mit einem Abschluß der Arbeiten rechnet man nicht vor 1999. [Schm98]

4 Kabelmodem

Als Alternative zu den bisher vorgestellten Techniken benutzt das Kabelmodem ein anderes Medium zur Datenübertragung, nämlich das Kupferkoaxialnetz der Telekom. Es wurde ursprünglich als Verteilnetz für Fernseh- und Rundfunkprogramme konzipiert. Moderne Hybrid-Netze (HFC, Hybrid-Fibre-Coax) bestehen nur im teilnehmernahen Bereich fast ausschließlich aus Koaxialkabeln, der sogenannte Zuführungsnetzabschnitt ist in Glasfasertechnik ausgelegt.

Mit Kabelmodems schafft man momentan eine Übertragungsrate von bis zu 40 Mbit/s. Kabelmodems lassen sich von verschiedenen Computern über Ethernet-Netzwerkkarten anschließen. Im Vergleich mit analogen Modems funktionieren Kabelmodems teilweise wie Router und sind mit Tuner, Netzwerkmanagement- und Diagnosesoftware ausgestattet. Manche Modems integrieren sogar Verschlüsselungs- und Authentisierungsverfahren. Sie sind ferner Frequenzagil, das heißt, sie suchen in einem zugewiesenen Frequenzbereich den saubersten Kanal heraus und stellen sich darauf selbständig ein. Wichtige Bestandteile der HFC-Netze sind die Kabelkopfempfangsstelle (Headend), die Glasfaserknoten (Fibre-Nodes) und die Netzwerk-Interface-Anschlüsse (Network Interface Units). Die Kabelkopfempfangsstelle empfängt analoge und digitale Programme von Satelliten, bereitet sie auf, wandelt sie und leitet sie an die Verteilzentren weiter. Sie ist die geeignete Position um Server für On-Demand-Dienste anzuschließen, die Multimedia-Daten wie MPEG-1-Videos liefern, oder Proxies, die den Zugriff aufs Internet ermöglichen. Die Kabelkopfempfangsstelle ist somit der zentrale und entscheidende Knotenpunkt für die Datenübertragung im Kabelnetz. Mit Ausnahme einiger weniger Kabelinseln in München, im Ruhrgebiet (o.tel.o) oder bei einigen Studentenwohnheimen waren die Kabelkopfempfangsstellen bislang im Besitz der Telekom und damit privaten Betreibern verschlossen. Die Telekom behinderte bisher nach Kräften die Nutzung der Kabelnetze. Man ist viel mehr daran interessiert, seine ADSL-Variante (unter dem Namen T-DSL) an den Mann zu bringen. Allerdings gibt es einen Lichtstreif am Horizont. Die EU-Kommission hat die Blockadepolitik der Telekom beendet. Sie fordert eine komplette Ausgliederung des Breitbandkabelgeschäfts und die Öffnung für private Anbieter. Zum 1. Januar 1999 wurde der Breitbandkabelbereich mit der Telekom-Tochter DeTeKabelservice in eine neue Gesellschaft integriert. Über 50% dieser Gesellschaft muß die Telekom anderen Unternehmen zum Kauf anbieten, die damit in den Besitz dieser bislang immer noch monopolistisch regierten Netzinfrastruktur kommen. Damit verfügen die neuen Kabelnetzbetreiber dann auch über die für die Errichtung interaktiver Dienste entscheidenden Netzabschnitte: die Kabelkopfempfangsstellen, die Verteilzentren und die wichtige sogenannte letzte Meile.

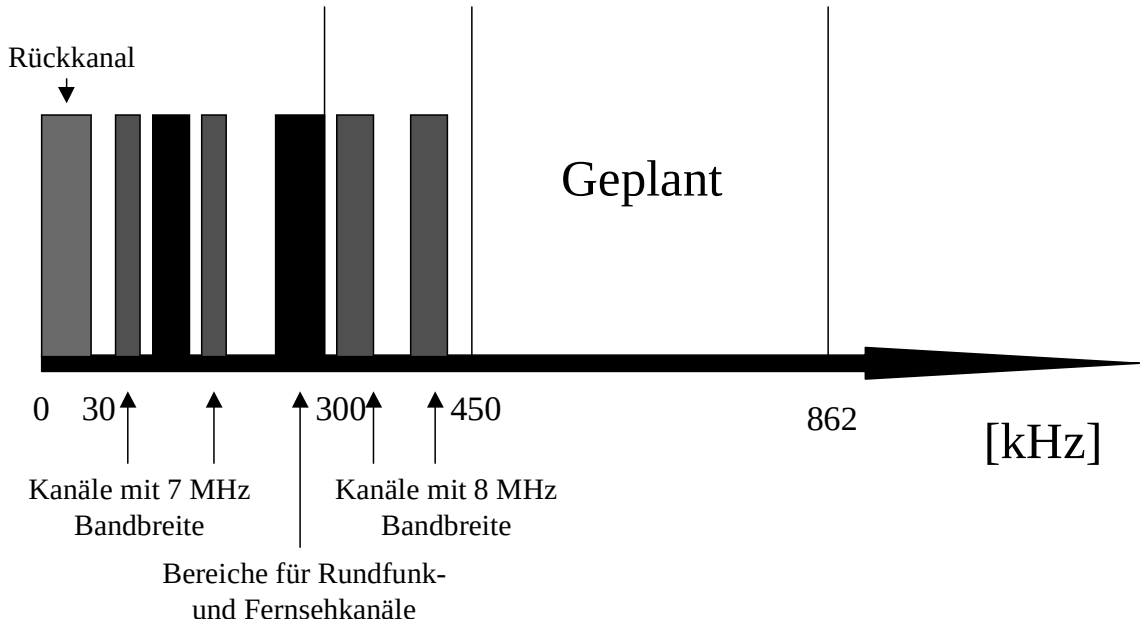

Abbildung 3: Benutzte Frequenzen beim Kabelmodem

Interessant für die neuen Betreiber sind vor allem Netzabschnitte, die sich schnell und kostengünstig auf die Bedürfnisse der interaktiven Dienste umrüsten lassen. Die Innovationskosten spielen für den Einstieg in das Geschäft eine entscheidende Rolle. Um Internet-Zugang und auch Kabeltelefonie realisieren zu können, müssen geeignete Rückkanäle vorhanden sein.

Um ausreichend Bandbreite zu schaffen, soll das Frequenzband von bisher 450 MHz auf 862 MHz erweitert werden. Für die Rückrichtung steht nämlich meistens nur das Frequenzband zwischen 5 und 30 MHz zur Verfügung. Um die Übertragungskapazität für Rückkanäle zu erhöhen, könnten die noch von TV-Programmen belegten Frequenzbereiche freigemacht werden, die TV-Programme könnte man in höhere Frequenzbereiche verlegen, das muß allerdings mit den Landesmedienanstalten verhandelt werden. Nach Schätzungen können zehn Prozent der deutschen Kabelnetze Signale bereits bidirektional übertragen und stehen praktisch umgehend zur Verfügung. Bei 15% des Netzes läßt sich der Rückkanal mit kleinsten technischen Änderungen binnen weniger Tage aktivieren, 60 bis 65% lassen sich binnen Wochenfrist mit geringem Aufwand aufrüsten. Richtig kritisch wird es lediglich bei 10 bis 15%. Hier handelt es sich um 20 bis 25 Jahre alte Netzbereiche, bei denen ein Komplettaustausch bzw. Neubau nötig ist. [Schu98] [Sier98] [Erns98] [Koss98a]

5 Gesamtvergleich der Internet-Zugangstechniken

Die für kleine Firmen und den Privatmann interessanten Internet-Zugangstechniken sind V.90, ADSL und Kabelmodem. V.90 wird wegen der zu kleinen und nicht mehr steigerungsfähigen Datenrate wohl langsam aussterben. Der Wettkampf um den Internet-Zugangsmarkt wird vorerst zwischen ADSL und Kabelmodem ausgefochten. Auf dem US Markt, der dem deutschen immer etwas voraus ist, hat das Kabelmodem zur Zeit 16% Marktanteil, ADSL dagegen nur 6 %. Das Marktforschungsinstitut Allied Business Intelligence sagt allerdings fÜr das Jahr 2004 einen ADSL-Anteil von 37% voraus gegenÜber Kabelmodems mit 16%. In der Studie wird ISDN bis dahin ein Einbruch auf 17% vorausgesagt.[t0199]

Technik	Max. Rate downstream	Max. Rate upstream	Preis	Rate in der Praxis
V.90	56.6 KBit/s	33.6 KBit/s	Modem Kaufpreis ca. 150,- DM. Monatliche Grundgebühr 10 - 25 DM, je nach Anbieter	ca. 47 KBit/s
ADSL	2 MBit/s	2 MBit/s	In Pilotprojekten: Modem Kaufpreis ca. 550,- DM. Monatliche Grundgebühr 48,- DM.	1,5 MBit downstream, 128 KBit upstream
Kabelmodem	40 MBit	je nach Anbieter	Kaufpreis Modem 400,- oder Miete 17,90 DM/Monat. Grundgebühr 85 DM/Monat	550 KBit/s

Tabelle 1: Vergleich ausgewählter Zugangstechniken

Literatur

[Erns98] Nico Ernst. Schnelle Welle. *c't* Band 16, 1998.

[Koss98a] Akel Kossel. Megabit-weise Internet. *c't* Band 16, 1998.

[Koss98b] Axel Kossel. Verbindung mit Tücken. *c't* Band 20, 1998.

[Lubi97] Holger Lubitz. Modem Modernisierung. *c't* Band 1, 1997.

[Sand98] Henning Sandke. Streckenerweiterung. *c't* Band 16, 1998.

[Schm98] Michael Schmoll. Schnelles Kupfer. *c't* Band 16, 1998.

[Schu98] Christiane Schulzki-Haddouti. Internet-Renner. *c't* Band 16, 1998.

[Sier98] Peter Siering. Nachgemessen. *c't* Band 16, 1998.

[t0199] Marktforscher prognostizieren Siegeszug der ADSL-Modems in USA. *Computerwoche* Band 2, 1999.

[Till97] Wolfgang Tillmann. Internet-Schnellbahn für jedermann. *c't* Band 11, 1997.

Industrielle Busse und ihre Unterschiede

Roland Heinemann

Kurzfassung

Feldbusse dienen dazu, Fertigungs-, E/A-Geräte und Sensoren über einen oder mehrere Computer zu steuern. Dabei werden die Meß- und Stellgrößen über den Feldbus zwischen Computer und Computer oder Fertigungsgerät übertragen. Die Topologie der Feldbusse sind einfache Stränge, deren Verknüpfung oder deren Anordnung zu einem Baum. Natürlich kann ein Feldbus auch mit allen anderen möglichen Netztopologien, wie Ring und Stern, gemischt werden. Der hier näher erläuterte Profibus, zeichnet sich durch die im folgenden näher beschriebenen Vorteile, wie beispeilsweise geringe Kosten, einfache Wartung, großen Leistungsumfang durch Modularisierung und dynamische An-/Abkopplung der Teilnehmer, besonders aus.

1 Bestandteile

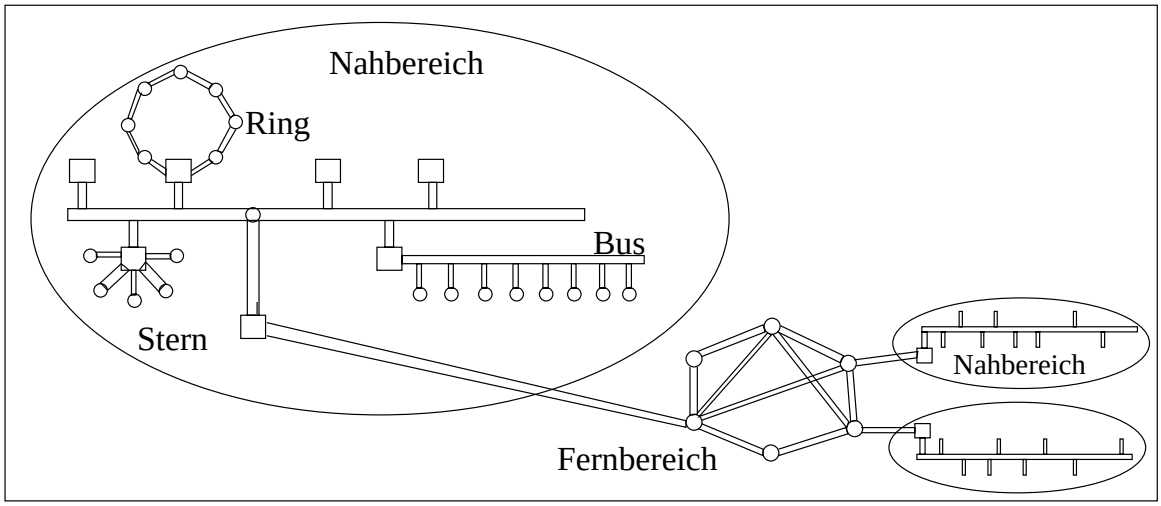

Abbildung 1: Netztopologien.

Feldbusse werden meist als serielle und sehr selten als parallele Busse konzipiert. Wobei auch bei seriellen sehr wohl ein oder mehrere Datenkanäle und notwendige Steuerkanäle nebeneinander geführt werden können. Dabei können den Kanälen physikalische Leitungen, Koaxial- bzw. Twisted Pair oder andere Kabel, eine Frequenz auf einem Lichtleiter oder sogar einem Radiokanal entsprechen. Das Grundprinzip des Busses ist, daß alle Teilnehmer an dieselbe Leitung gekoppelt sind. Dadurch werden Broad- bzw. Multicasting (Rundruf) an alle oder ausgewählte Teilnehmer ohne zeitlichen Verlust möglich. Bei der Ringtopologie entsteht der

zeitliche Verlust durch das Lesen und anschließende Weiterreichen der Nachricht an den Nachfolger. Beim Stern schlägt ikn erster Linie der hohe Verdrahtungsaufwand zu Buche.
Die Teilnehmer werden über sog. Transceiver an den Bus gekoppelt. Dieser realisiert beim Profibus einen Überspannungsschutz und erledigt das Schreiben auf und das Lesen vom Bus. Hier sind die in Abschnitt 3.3 beschriebenen Verfahren entweder als Software- oder als Hardwarelösung anzusiedeln. Dies führt zu einer Unabhängigkeit der Anwendungsschicht vom Verfahren des Buszugriffs. Außerdem bedeutet dies einen Zeitgewinn.
Zusätzlich benötigt wird ein Abschlußwiderstand, um Verfälschung der Daten durch Reflexion des Datensignals am Leitungsende zu vermeiden.

2 Anforderungen

- Zum einen sind die Nachrichten klassifizierbar in Abhängigkeit der Datenmenge und -häufigkeit.

Nachrichtenart	Grafiken	Daten	NC-Programme	Synchron.-Signale	Soll/Ist-Werte	Alarm-Meldungen
zulässige Wartezeit	1-100 s	1-100 s	1-100 s	1-100 ms	20-100 ms	0.1-80 ms
Nachrichten-länge	>10 kbit	1-10 kbit	>10 kbit	8-64 bit	<10 kbit	8-64 bit
Auftritts-häufigkeit	selten	sehr selten	sehr selten	sehr häufig	häufig	selten
Klassifizierung	zeitunkritische Nachrichten			zeitkritische Nachrichten		

Tabelle 1: Klassifizierung von Daten

- Zum anderen ist der Umgang mit sicherheitsrelevanten Daten mit Sorgfalt zu durchdenken, damit kein unberechtigter Zugriff auf diese stattfinden kann.
- Je nach Anwendung kann auch die Echtzeitfähigkeit des Feldbusses für das System von Wichtigkeit sein.
- Die Erweiterbarkeit um weitere Teilnehmer mit Neuinitialisierung des Systems oder sogar dynamisch während das System läuft kann von enormer Wichtigkeit sein.
- Ein für den Betrieb wichtiger Aspekt können der Kostenfaktor beim Aufbau und dem Betrieb sein. Daher ist es wichtig den Verwaltungsaufwand für die Businstanzen möglichst gering zu halten. Billige Komponenten erhält man durch Konkurrenz unter den Anbietern und die Verwendung von Standardkomponenten.
- Über den Bus soll manchmal auch Hilfsenergie zugeführt werden können.
- Oder er soll im sogenannten Ex-Bereich, das ist der Explosionsgefährdeter Bereich, eingesetzt werden.
- Unter anderem sollen die Daten natürlich möglichst sicher übertragen werden.

Diese Anforderungen führen zu unterschiedlichen Protokollen.
Wie man leicht in Abbildung 4 sieht kann man je nach der Anforderung zu anderen Ausführungen kommen. Für Interessierte gibt es zu all diesen unterschiedlichen Bussen ausführliche Literatur. Deshalb hier nur Grundlegendes zu den Feldbussen und im Speziellen zum Profibus.

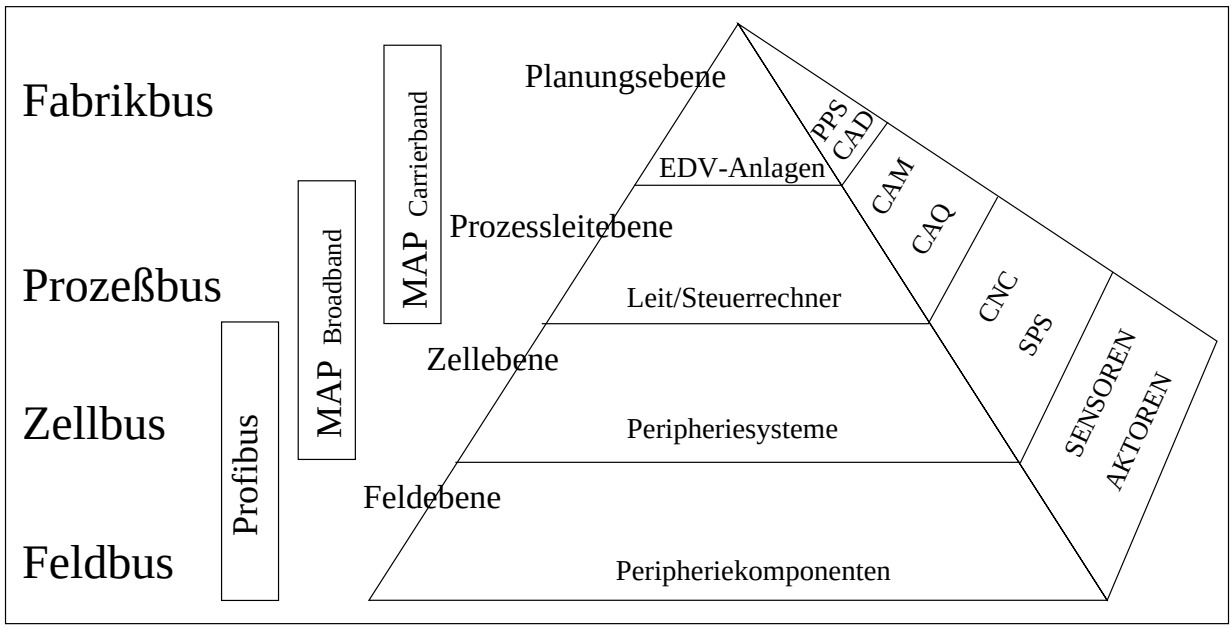

Abbildung 2: Dabei kann man bekannte Busse gewissen Hierarchieebenen zuordnen.

3 Protokoll

3.1 Definition

"Ein Protokoll ist ein Satz von Regeln über Format und Inhalt von auszutauschenden Nachrichten zwischen kommunizierenden Prozessen" [KFBL+92]

3.2

Protokolle werden meist in Anlehnung an das ISO/OSI Schichtenmodell spezifiziert. Bei Feldbussen werden meist nur die Schichten 1, 2 und 7 benutzt. Dadurch ergeben sich allgemeine Anforderungen an ein Protokoll.
Es sollte eine gute Integration verschiedenster Geräte ermöglichen. Des weiteren sollte eine Fehlerdiagnose möglich sein und ein fehlerfreier Datentransfer durch das Protokoll unterstützt werden. Fehlermeldungen an die höhere Schicht sollten dann erfolgen, wenn er nicht auf dieser Schicht behoben werden kann. Um einige Fehler im vorhinein schon vermeiden zu können, sollte das Protokoll eine logische Vollständigkeit aufweisen. Dadurch werden Sackgassen, die das System zur Laufzeit zum Stehen bringen können, vermieden. Man sagt dazu auch „ es soll verklemmungsfrei sein ". Zu alledem sollte es bis auf die physikalische Schicht unabhängig von Leitungslänge, Übertragungsgeschwindigkeit und -medium sein. Weitere sehr nützliche Punkte sind die Unterstützung verschiedener Betriebsmodi der Busteilnehmerund das An-/Abkoppeln einer variablen Anzahl von Busteilnehmern, auch dynamisch während des Betriebs.

3.3 Physikalische Ebene

Unter anderem werden im Protokoll folgende Aspekte der untersten, physikalischen Schicht geregelt.

3.3.1 Datenübertragung

Im **Zeitmultiplexverfahren** dürfen die Teilnehmer nur zeitlich nacheinander das Medium für ihre Übertragung nutzen. Was als einfach zu implementierendes Verfahren kostengünstige Feldbusse liefert.
Beim **Frequenzmultiplexverfahren** wird der Gesamtfrequenzbereich des Mediums in einzelne Frequenzbänder unterteilt. Auf den so entstehenden physikalischen Kanälen können Informationen parallel übertragen werden. Der wesentliche Nachteil hiervon ist, daß die Übertragung nur unidirektional stattfinden kann. Daher benötigt jeder Teilnehmer für die Übertragung seiner Daten zwei Kanäle, einen Sende- und einen Empfangskanal.

3.3.2 Busarbitrierung

Beim Profibus wird die Anforderung des Busses durch die Teilnehmer durch die Kombination folgender Verfahren geregelt.
Als dezentrales Busverteilungsverfahren. Dafür werden die Teilnehmer in **aktive Master**, die den Bus anfordern können, und **passive Slaves**, die nur auf eine sie betreffende Anfrage antworten dürfen, eingeteilt. Wobei in einem Busteilnehmer beide Instanzen realisiert sein können. Aber ein Sensor zum Beispiel benötigt nur die Eigenschaft des Slave, da er ja nur seine Meßwerte anbieten muß.

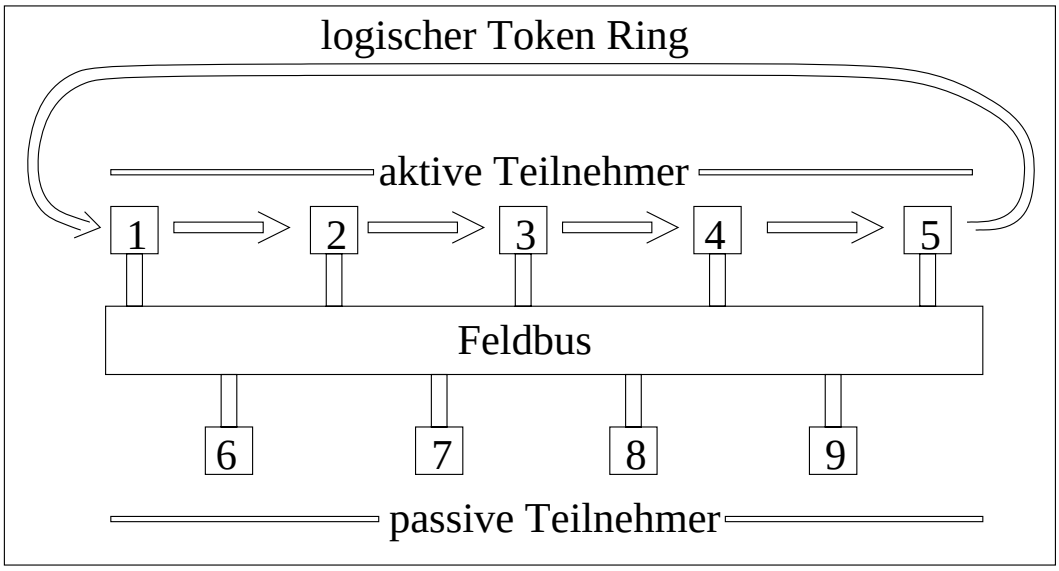

Abbildung 3: Zugriff beim Profibus

Unter den Mastern wird ein logischer **LAN**, d.h. jeder kennt die Adresse seines Nachfolgers und seines Vorgängers im Netz, zur Busvergabe mithilfe eines Token eingerichtet. Hierbei wird das Token nach einer vorgegebenen Zeit weitergereicht. Hat ein Teilnehmer während seiner Zeitscheibe nichts zu tun, so stellt er die Anfrage, ob es neue Busteilnehmer gibt. Diese legen sodann ihre Adresse auf den Bus. Jetzt kontrolliert der Anfragende, ob die Adresse zwischen seiner und der seines Nachfolgers liegt und macht ihn je nach dem zu seinem neuen Nachfolger. Damit ist eine **dynamische Ankopplung** neuer Busteilnehmer und **Reinstanziierung des LAN** auch während des laufenden Betriebs möglich. Das Abkoppeln wird so wie der Verlust des Token gehandhabt. Jeder Master berechnet die Tokenumlaufzeit und vergleicht sie mit dem Sollwert. Kommt das mehrfache dieser Zeit kein Token vorbei und ist auf dem Bus nichts zu hören, so wird der LAN reinstanziiert. Dadurch sind eine Mindestantwortzeit und faire Buszuteilung gewährt.

Bei anderen Protokollen werden vorgenannte Verfahren mitunter allein oder mit folgenden gemischt verwendet.
Die **zentrale Busvergabe** hat den Vorteil, daß die Logik dafür nur einmal implementiert werden muß. Aber natürlich führt dies durch den höheren Verwaltungsaufwand zu längeren Antwortzeiten und zu einem erhöhten Aufkommen an Steuerdaten. Meist werden die Anforderungen des Busses über eine/mehrere Steuerleitungen an die Zentrale übertragen.
Beim **CSMA** Verfahren(Carrier Sense Multiple Access, Mehfachzugriff mit Signalabtastung) hört ein Teilnehmer, der eine Nachricht auf dem Bus senden will, diesen ab. Falls er den Bus ruhig vorfindet, sendet er. Andernfalls stellt er seine Übertragung zurück, um die laufende Übertragung nicht zu stören. Um die Entscheidung für einen weiteren Sendeversuch zu fällen, gibt es verschiedene Möglichkeiten. Entweder zufällig, hier wird mit irgendwelchen Größen des Teilnehmers eine Wartezeit berechnet, oder prioritätsabhängig. Gleichzeitiges Senden mehrere Teilnehmer ist möglich, wenn diese nahezu gleichzeitig den Bus abhören, ihn frei finden und mit dem Senden beginnen. Um die dadurch verursachte Fehlübertragung zu erkennen, muß jede Nachricht vom Empfänger quittiert werden. Solange muß die Nachricht beim Sender zwischengespeichert bleiben. Zu einem Problem führen verlorene oder zerstörte Quittungen, denn der Sender wird seine Nachricht wiederholt senden. Bleibt die Quittung aus oder geht sie immer verloren, so kann der Sender durch seine obige Eigenart durch diesen einen Job völlig blockiert werden. Dies kann nur in höheren Schichten gelöst werden.
Das **CSMA/CD** Verfahren (Carrier Sense Multiple Access with Colition Detection, Mehrfachzugriff mit Signalabtastung und Kollisionserkennung) vermeidet das Problem der Blockade des Senders durch fehlende Quittungen und Kollision zweier Sender. Dafür ist es notwendig, daß der Sender den Bus auch dann noch abhört, wenn er bereits sendet. Wenn er dabei seine Nachricht nicht mehr richtig erhält, nimmt er eine Kollision an und beendet das Aussenden. Nach einer zufällig gewählten Zeit versucht er es noch einmal. Dadurch wird eine erneute Kollision zwischen den Sendern unwahrscheinlicher, aber eben nicht unmöglich. Bei beiden gibt es den Extremfall, daß durch zu große Kollisionszahl ein Großteil der Zeit Schweigen auf dem Bus herrscht, obwohl alle etwas Dringendes zu sagen hätten. Man kann versuchen, dies durch Optimieren der Funktion für den Buszugriff etwas zu mildern.
Oder der Anforderer legt seine **Priorität**, als Adresse kodiert, auf den/die Steuerkanäle und liest dann die daraufliegende. Hierbei löscht in Abhängigkeit von der Realisierung eine 0 eine 1. Daher wäre die Adresse aus lauter 0 die höchste Priorität. Der Nachteil liegt auf der Hand. Ein Teilnehmer mit niedriger Priorität hat nur sehr selten eine Chance, selbst wenn er mal eine sehr wichtige Meldung zu machen hätte.

3.3.3 Synchronisierung

Zur Synchronisierung verwendet der Profibus das **Polling**, Anfrage, mit Rückantwort, "bin bereit". Aber es gibt auch die Möglichkeit, z.B. für einen Sensor, daß er die nachgefragten Daten mit der Antwort auf das Polling gleich mitschickt (immediate answer), ohne daß ein Kanal auf- und später wieder abgebaut werden muß (asynchron).
Beim Integrieren erhält der neue Teilnehmer auch gleichzeitig den Buszugriff übertragen, auch **Handshake** genannt. Andere Busse verwenden mitunter **Try and Error**, bis sie die Bestätigung für die Nachricht erhalten.
Oder über eine weitere Steuerleitung werden alle Teilnehmer über einen **gemeinsamen Takt** global synchronisiert. Eine andere Möglichkeit ist, jedem Byte ein **Startbit** voran und ein **Endebit** nachzustellen. Dies vergrößert die Nachricht natürlich stark.

3.3.4 Fehlerbehandlung

1. Die Übertragungsfehler werden beim Profibus durch

<table>
<tr><td colspan="6">SERIELLE BUSSE</td></tr>
<tr><td colspan="4">Zeitmultiplex</td><td colspan="2">Frequenzmultiplex</td></tr>
<tr><td rowspan="3">Synchrone Übertragung mit zentraler Kontrolle</td><td colspan="3" rowspan="3">Asynchrone Übertragung</td><td>Ein Teilnehmer pro Kanal</td><td>Meherere Teilnehmer pro Kanal</td></tr>
<tr><td colspan="2">Kontrollierter Buszugriff</td><td colspan="2">Zufälliger Buszugriff</td></tr>
<tr><td>Zentrale Buszuteilung</td><td>Dezentrale Buszuteilung</td><td>Carrier-Abtastung (CSMA)</td><td>Carrierabtastung mit Kollisionserkennung (CSMA/CD)</td></tr>
</table>

Abbildung 4: Einteilung der seriellen Busse nach Übertragungs- und Zugriffverfahren

- Prüfsummen(*CRC(Cyclic Redundancy Check), UART Zeichensatz*),
- einer Rückmeldung bei Erfolg und Wiederholung bei Mißerfolg behandelt.

2. Andere Busse verwenden die Zeitüberwachung. Bei dieser wird die Zeit bis zur Antwort gemessen. Ist diese zu lang so erfolgt ein neuer Versuch.

3.3.5 Datencodierung

Beim Profibus werden die zu übertragenden Daten uncodiert in Pakete gepackt. Diese bestehen aus 11 Bits. Diese Codierung wird als UART-Zeichensatz bezeichnet. Dadurch bleiben

1 Startbit, das immer logisch “ 0” ist,
1 Stoppbit, das immer logisch “1” ist,
1 Paritätsbit und
8 Informationsbits

die Datenpakete klein und man hat dennoch eine sehr gute Datensicherheit realisiert. Denn hiermit wird eine Hamindistanz von vier erzeugt. D.h. ein ein Bit-Fehler kann erkannt und behoben werden. Und ein Fehler von zwei Bit immerhin noch erkannt werden.

3.4 Anwendungsschicht

Die Anwendungschicht kennt die Dienstgruppen

- Variable-Access(Zugriff auf Simple-Variables,Records,Arrays, Variable-Lists)

  - Read
  - Write
  - Read-Write
  - Phys-Read
  - Phys-Write
  - Information-Report
  - Information-Report-With-Type
  - Define-Variable-List
  - Delete-Variable-List

- Domain-Access (Befehle für Down-, Upload logisch zusammenhängender Speicherbereiche)
  - Initiat-Download
  - Download-Segment
  - Terminate-Download-Sequence
  - Request-Domain-Download
  - Initiate-Upload-Sequence
  - Terminate-Upload-Sequence
  - Request-Domain-Upload

- Programm-Invocation(Domains, um Programmen zusammenzustellen, zu starten, zu stoppen, zu löschen)
  - Create-Program-Invocation
  - Delete-Program-Invocation
  - Start
  - Resume
  - Reset
  - Kill

- Event-Management(Dienste zur Übertragung von Events vonGerät zu Gerät)
  - Event-Notification
  - EventNotification-With-Type
  - Acknowledge-Event-Notification
  - Alter-Event-Condition-Monitoring

und die Verwaltungsdienstgruppen

- VFD-Support(VirtualFieldDevice)
  Abstraktes Modell um Daten und Verhalten eines Automatisierungssystems aus der Sicht des entfernten Profibus-Anwenders zu beschreiben.

- OV-Management
  Stellt Dienste zum Lesen und Schreiben von Source-Objektverzeichnissen der VFDs der Kommunikationspartner zur Verfügung.

- Context-Managemnet
  Dient zur Verbindungsinitialisierung , zur Freigabe und Abbruch einer belegten Verbindung und zur Abweisungvon unzulässigen Dienste.

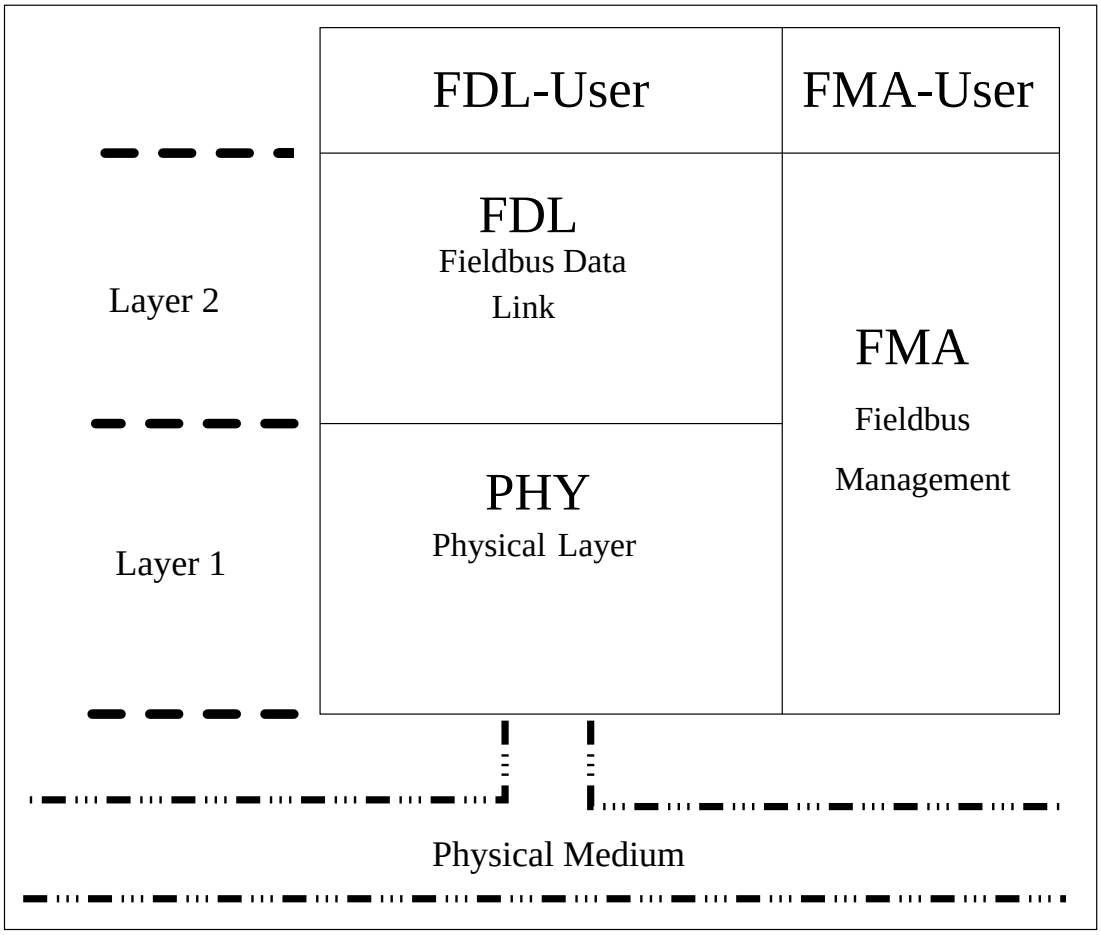

Abbildung 5: Schichten beim Profibus

3.5 Datensicherungsschicht, FDL, FMA

Im Sprachgebrauch des Profibusses wird die Schicht 2 (Abbildung 5) als **FDL(Fieldbus Data Link)** bezeichnet. Sie beinhaltet eine Zustandsmaschine, steuert den Buszugriff und kontrolliert die Tokenumlaufzeit. Für den FDL-User stellt sie zur Datenübertragung folgende Dienste mit ihren zugehörigen Übertragungsprotokollen zur Verfügung.

- SDN Send Data with No acknowledge
- SDA Send Data with acknowledge
- SRD Send and Request Data
- CSRD Cyclic Send and Request Data

3.6 FMA-User

Oder auch FMA7 (Abbildung 5) besitzt neben der Schnittstelle zum Anwender weitere zu benachbarten Schichten.

- Die Schnittstelle zum FMA-User
  Hier stehen Dienste zur De-/Aktivierung und Zurücksetzung des FMA-User.

- Die Schnittstelle zum FMA 1/2
  Die hier residierenden Dienste werden benutzt, um lokale Variablen zu lesen oder zu schreiben

3.7 FMA 1/2

FMA 1/2 (Fieldbus Management der Schichten 1 und 2) stellt die Funktionen zur Verwaltung der Schichten 1 und 2 dem FMA-User zur Verfügung. Über diese greift der FMA7 auf diese Schichten zu. Die Dienste werden in lokale Dienste, welche die eingene Staion beeinflussen, und entfernte Dienste, welche andere am Netz hängende Teilnehmer betreffen, unterschieden. Unter anderen gibt es die RESET, SET VALUE, READ VALUE,EVENT, (R)SAP(Service Access Point, Dienstzugangspunkt),(R)SAP DEACTIVATE als lokale und IDENT, LSAP,LIFELIST als entfernte Dienste.

4 Vorteile serieller Busse

1. Übersichtlichkeit der Verkabelung. Große Kabelbäume und Netze von Kabeln zwischen den Teilnehmern werden größtenteils vermieden.
2. Verwendung von wenigen und billigen Kabeln.
3. Vermeidung von Steckerbatterien.
4. Wesentlich höhere ökonomische Auslastung der Datenwege.
5. Einfacher Anschluß der Teilnehmer über handelsübliche Komponenten bei den meisten Bussen.

5 Kennzeichen des Profibus

Wie schon erwähnt ist beim Profibus das dynamische An- und Abkoppeln der Busteilnehmer auch während des Betriebs mit sehr geringem Aufwand möglich.
Das offene Protokoll führt natürlich zu einem breitgefächerten Herstellerspektrum für die einzelnen Komponenten, da jedem die Spezifikation des Busses zugänglich ist. Dadurch werden die Anschaffungskosten für die Geräte durch die resultierende Vielfalt kompatibler Geräte auf dem Markt niedriger.
Auch die Verkabelung trägt dazu bei. Denn es werden Dank des Protokolls nur einfache Twisted Pair Kabel benötigt. Falls durch die Anwendung noch weitere Leitungen benötigt werden, z.B. für höhere Datensicherheit oder zusätzliche Steuerleitungen, so sollen sie über Sub-9-D Stecker angeschlossen werden. Die Leitungen werden in sogenannten Linien organisiert. Jede darf max. 1.2 km lang sein und es können max. 32 Teilnehmer angeschlossen werden. Die Reichweite kann man noch erhöhen, indem man je 2 Linien über einen Repeater zusammenschliesst. Dadurch wird die Teilnehmeranzahl bei beiden Linien je um eins geringer. Um die Übertragungssicherheit trotz der langen Verbindungswege zu gewährleisten, werden die Spannungsvorzeichen und **nicht** die Spannungspegel als 0 oder 1 interpretiert. Dadurch sind auch noch sehr stark gestörte Signale lesbar. Allerdings dürfen, aufgrund der Echtzeitbedingung, laut Spezifikation zwischen zwei Kommunikationspartnern maximal 3 Repeater zwischengeschaltet sein. Zwischen diesen Randbedingungen ist alles erlaubt, z.B. auch eine Linie an die 32 Linien über den dazugehörigen Repeater angeschlossen sind, um die Teilnehmerzahl zu erhöhen. Um die Echtzeitbedingung möglichst gut zu erfüllen, verzichtet der

Profibus auch auf eine Codierung der Nachrichten.
Außerdem gibt es die Möglichkeit den Slave so zu modifizieren, daß dieser sofort die Antwort ohne weitere Verarbeitungsschritte auf den Bus legt (Immediate Response). Der Profibus bietet sehr viele verschiedene Dienste an, die man je nach Anforderung in modularer Weise zusammenbauen kann. Daher kann man den Implementierungsaufwand für jede Komponente auf das Notwendigste reduzieren. Auf diese Weise kann man bei Sensoren, die meist nur einen Meßwert liefern müssen, einen passiven Thin Slave mit diesen wenigen Eigenschaften implementieren.
Die notwendigen Dienste aus der Vielfalt werden den Produzenten durch Profile bekanntgegeben. Dadurch sind diese in der Lage, die Implementation so billig und schnell wie möglich zu machen. Dabei ist die fertige Lösung so optimal an die Anforderung angepasst, daß die Administration über eine ausgezeichnete Station im Netz keinen EDV-Fachmann benötigt.
Durch diese durchdachte Struktur deckt der Profibus ein sehr großes Anwendungsspektrum bei minimalen Kosten ab.

6 Daten zu verschiedenen BusProtokollen

Feldbusse				
Feldbus	**Länge in m (mit Repeater)**	**Übertragungs-kapazität**	**Medien-zugriff**	**Teilnehmer**
Profibus (DIN 19245)	1200 (4800)	500kbit/s	Token Master/Slave	32 aktive 127 passive
FIP (AFNOR C64-602)	2000	1Mbit/s	zentrale Station	256
SINEC (SIEMENS)	1200 (5000)	500kbit/s	Token Master/Slave	32 aktive 90 passive
BITBUS (Intel)	300 (1200)	2,4MBIT/s(synch.) 375kbit/s(asynch.)	Master/Slave	250
TIWAY (Texas Instr.)	7600	115kbit/s	zentraler Master	254
VAN (ISO DIS 11519-2)	wenige	500kbit/s	Master/Slave	wenige
CAN (ISO DIS 11519-1)	wenige	125kbit/s	CSMA/CD	wenige
EIB (SIEMENS)	13000	9,5kbit/s	CSMA/CA256	

Tabelle 2: Vergleich markanter Daten verschiedener Feldbusse

Wie man der Tabelle entnehmen kann, kommen die verschiedenen Kombinationen der einzelnen Verfahren auf der physikalischen Ebene in existierenden Realisierungen zum tragen. Natürlich beinhaltet diese Auflistung nicht alle existierenden Busvarianten, da einige Hersteller ihre eigenen Produkte entwickelt haben und diese verwenden. Daher liegt keine genaue Spezifikation für diese vor.
Der Profibus liegt bei der Übertragungskapazität und der Anzahl der Teilnehmer im oberen Mittelfeld, bei den maximal überbrückbaren Entfernungen im Mittelfeld. Aber wie man sehen kann, behauptet sich der Profibus mit seinen Werten unter den Feldbussen, die als offene Standards jedem zugänglich sind, wie CAN und VAN, an der Spitze.
Was macht den Profibus dennoch so äußerst attraktiv:
Hier muß man folgende Punkte ins Gedächtnis rufen:

- Der Kostenvorteil durch
  - das offene Protokoll, sprich keine Lizenzgebühren.
  - die Konkurrenz unter den Produktanbietern.
  - eine große Produktpalette
  - die Verbindung mit Koaxialkabel
  - die Ankopplung durch standard Transciever.
- Die Möglichkeit die Implementation der einzelnen Funktionen modular den Erfordernissen angepaßt vorzunehmen(Thin Implementaion).
- Die dynamische An-/Abkopplung der einzelnen Teilnehmer während des Betriebs.
- Der Schutz der untersten Schicht vor ungewünschtem Zugriff durch nicht autorisierte Personen.
- Störsicherheit durch Codierung der Bits als Spannungsvorzeichen
- Einfache Wartung
- modulare Erweiterbarkeit durch verschiedene Anbieter
- gesicherte Antwortzeiten

7 Zusammenfassung

Trotz großer Konkurrenz bietet der Profibus zu optimalen Kosten die größte Flexibilität und Funktionalität unter den Feldbussen.

Durch seine sehr gute Konzeption werden getätigte Investitionen auf lange Sicht hin geschützt. Dieses Preis/Leistungs-Verhältnis macht sich schon von Anfang an in der Unternehmensbilanz positiv bemerkbar. Eine Beschreibung des Konzepts wie auch der Planung und Realisierung des Profibusses findet sich in [KFBL+92]. Das Buch [WRPF+87] behandelt ausführlich die Grundkonzeption der Datensicherheit und Übertragungsverfahren bei den parallelen und seriellen Bussen auf der physikalischen Ebene ausführlich.

Literatur

[KFBL+92] Marianne Katz, Axel Funke, Gerhard Biwer, Yue Li, Thomas Sebastiany, Bernhard Rieger und Klaus Bender. *PROFIBUS Der Feldbus für die Automation*. Klaus BenderMcGraw-Hill, Carl Hanser Verlag München Wien. 2. Auflage, 1992.

[WRPF+87] Bernd Wiemann, Walter Ries, Manfred Platz, Georg Färber und Franz Demmelmeier. *Bussysteme Parallele und serielle Bussysteme, lokale Netze*. Professor DR.-Ing. Georg Färber, R. Oldenbourg Verlag München Wien. 2. Auflage, 1987.

Voice-over-IP - Telefonieren im Internet

Norbert Ottahal

Kurzfassung

Voice-over-IP ist eine zukunftsweisende Technik, die viele Möglichkeiten in der Telefonie auftut. Firmen entwickeln bereits in grossen Mengen Geräte und Programme für den kommerziellen Einsatz. Auch existieren bereits Standards wie zum Beispiel der von der ITU verabschiedete Kommunikationsstandard H.323. Eine Vielzahl von Ansätzen und intelligente Audio-Kompressions-Methoden sparen Bandbreite ein und versuchen den Problemen bezüglich des Echtzeittransportes bei IP gerecht zu werden.

1 Einleitung

Voice-over-IP (VoIP) wird bis zum Jahr 2000 ein Marktvolumen von über 2 Mrd. US-Dollar und bis 2005 einen Marktanteil im Telefoniebereich von über 15 Prozent prognostiziert. Die Möglichkeiten dieser Technik scheinen nahezu unbegrenzt zu sein. Eine Preiseinsparung von bis zu über 80 Prozent beim Telefonieren, Multiconferencing, Bildtelefonie sowie Datenübertragung und Faxen während des Gesprächs machen Voice-over-IP attraktiv, vor allem für Firmen mit einem eigenen Intranet. Daten können nun zusammen mit Sprach- und Bilddaten gleichzeitig über das selbe Netz geschickt werden. Damit eröffnen sich Möglichkeiten wie zum Beispiel bildgestützte Teamarbeit ohne räumliche Einschränkungen. Es können so zwei Mitarbeiter aus verschiedenen Filialen einer Firma quasi eine Standleitung zwischen ihnen aufbauen und so Hand in Hand an einem Projekt arbeiten. Die zusätzliche Verwaltung eines Telefonnetzes entfällt, Firmen können von der Vernetzung ihrer Filialen profitieren, Internetprovider können in den nun offenen Telefonmarkt als Service Provider (Nextgen Telcos) einsteigen und ihre Netze so besser auslasten und auch der private Endkunde gewinnt an den aus dem harten Konkurrenzkampf entsteigenden günstigeren Preisen. [Wess98] [uCis98]

2 Probleme von Voice-over-IP

Natürlich hat diese Technik auch ihre Probleme. Zum einen ergeben sich Qualitätsverluste bei der Komprimierung der Sprachdaten. Dennoch kann man je nach Bandbreite und Entfernung die Qualität von normalen Telefonen erreichen. Die grössten Schwierigkeiten geben sich aber beim Transport der Sprache. Hier erschweren auf der einen Seite die benötigte hohe Bandbreite und auf der anderen Seite die nicht vorhandene Echtzeit-Fähigkeit von IP erheblich. Da IP-Pakete unterschiedlich geroutet werden, kommen die einzelnen Pakete meist mit völlig unterschiedlichen Verzögerungen und Reihenfolgen beim Empfänger an.

Die Kommunikation durch ein firmeneigenes Netz ist dabei noch nicht einmal der am schwersten zu bewältigende Part, sondern der Datenfluss durch das Internet. Hier sind grosse Timelags Hürden für eine flüssige Kommunikation, bereits Verzögerungen von etwa einer Sekunde machen ein Gespräch unattraktiv. Das Internet ist grossen jährlichen Wachstumsraten ausgesetzt, die Datenverkehrsdichte wird immer grösser, dementsprechend werden auch die Datenstaus immer grösser. [uCis98] [KBSS+98] [Rohr98a]

3 Die Geschichte des Voice-over-IP

Den ersten Schritt tat seinerzeit 1995 die israelische Firma Vocaltec mit der ersten Version des Windows-Programmes Internet Phone. Diese erste Version arbeitete noch mit ziemlich ärmlicher Qualität der Sprache und reinem Halbduplex-Betrieb (es konnte immer nur einer gleichzeitig sprechen, genau wie beim CB-Funk). Desweiteren mussten beide Gegenstellen mit der gleichen Software arbeiten. Es waren lediglich PC-to-PC-Verbindungen möglich. Mit den ersten Gateway-Produkten 1996, die einen Zugang zum normalen Telefonnetz gestatteten, begann der Siegeszug der Internettelefonie. Namhafte Firmen wie Ericsson, Alcatel und Siemens erkannten schnell die nahezu unbegrenzten Möglichkeiten dieser neuen Technologie und mit dem Erscheinen des ersten Gateway-Produktes, das Übergänge ins normale Telefonnetz erlaubte, begann der Siegeszug der Internet-Telefonie. Schon seit zwei Jahren investieren namhafte Telefonieanbieter in Voice-over-IP-Versuchsprojekte. Die Firma Qwest zum Beispiel benutzt ein eigenes Netz, durch das die Telefonkunden per VoIP geroutet werden. Dadurch stehen der Firma immer 100 Prozent Bandbreite zur Verfügung und die Verzögerungen sind gut kalkulierbar. [Rohr98b]

4 Die Technik

4.1 Übertragungsstandards

4.1.1 Der H.323-Standard

Die ITU (International Telecommunication Union) hat im Frühjahr 1996 die zwei Kommunikationsstandards H.323 und H.324 verabschiedet, um die Probleme der Interoperabilität der Soft- und Hardware und der Bandbreitensicherung in den Griff zu bekommen. H.323 ist eine Art Hyperstandard, der die Übertragung von Daten, Sprache und Videosequenzen in Echtzeit durch Netze ohne Echtzeitgarantie beschreibt. Er setzt sich aus mehreren Unterstandards zusammen, die jeden Übertragungsmodus definieren. H.323 nutzt parallele UDP-Datenströme für die Client-to-Client-Kommunikation. Dazu benötigt es folgende Komponenten:

1. Gatekeeper: Überwachungseinheit, die die Adresse umrechnet (z.B. ISDN-E.164-Telefonnummer nach IP-Adresse und umgekehrt). Desweiteren verwaltet er die Netzressourcen, indem er Verbindungen, die die Netzkapazität übersteigen, ablehnt. So kann man eine maximale Bandbreite für Multimedia-Anwendungen festlegen und diese garantieren.

2. Gateways: Diese gewährleisten die Anbindung von Geräten ausserhalb der TCP/IP-Welt wie zum Beispiel ISDN-gestützte Bildtelefonie (H.320), PSTN-telefongestützte Bildtelefonie und POTS (Plain Old Telephone System, normale Analogtelefone). Die Gateways passen die unterschiedlichen Transportformate (H.221 und H.225) wie die Ablaufsteuerungsprotokolle (H.245 und H.242), die Audio/Video-Codecs und die Kontrollprotokolle (H.245 und Q.931) an.

3. Proxies: Die H.323-Proxy unterscheidet sich im Wesentlich nicht von seinem Namensvetter, er überwacht den Datenaustausch auf H.323-Basis, der sowohl vom als auch zum lokalen Netz führt. Er entscheidet, welche Benutzer welche Dienste nutzen dürfen und befindet sich meist auf der Firewall des jeweiligen Netzes.

4. Multipoint Control Units: Die MCUs sind Funktionseinheiten für die Unterstützung von Multimedia-Anwendungen, an denen mehr als zwei Personen beteiligt sind (z.B.

Konferenzgesprächen). Sie verwalten Ressources, kümmern sich um Auf- und Abbau der Verbindungen sowie Vermischung der Audio- und Videodaten.

5. Terminals: Die Endgeräte können in Hardware oder Software realisiert werden, benötigt wird lediglich die Audio-Komponente. Daten- und Videoübertragung ist optional. Unterstützen müssen die Geräte die Protokolle für Signalisierung (H.245), Gesprächsaufbau und -abbau (Q.931), Kommunikation mit dem Gatekeeper (RAS) und Streaming (RTP/RTCP).

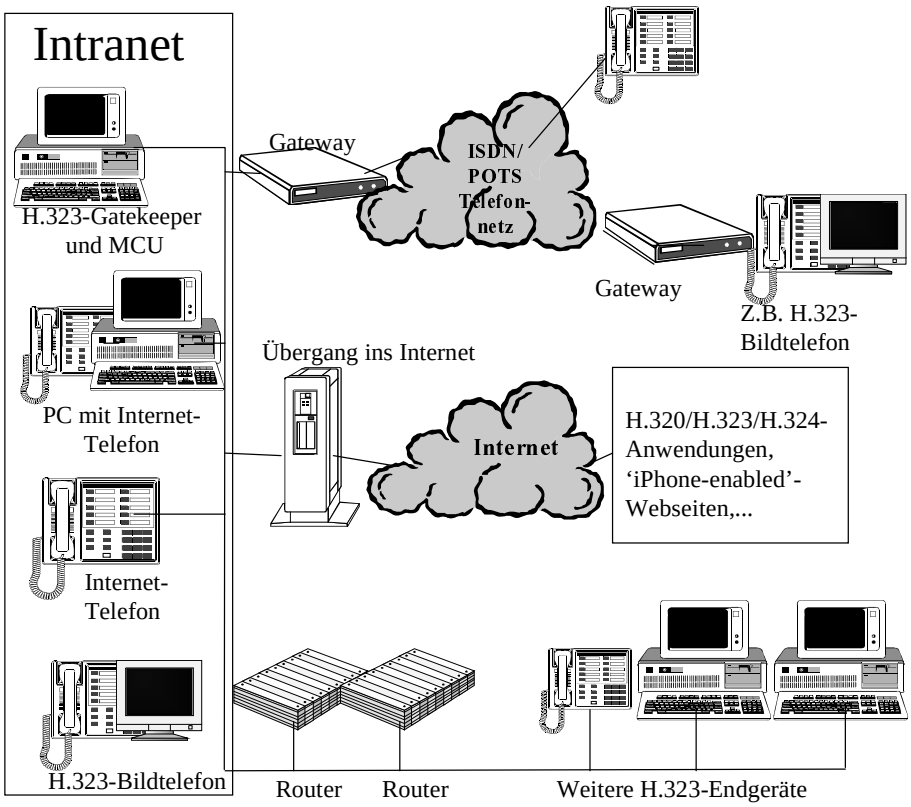

Abbildung 1: H.323-Verbindungen - was ist möglich?

Um die Echtzeit-Probleme von IP in den Griff zu bekommen, hat man zwei neue Protokolle eingeführt. Das Realtime-Transport-Protocol (RTP) versieht die einzelnen UDP-Pakete mit einem Header, der unter anderem einen Zeitstempel (Timestamp) und eine Sequenznummer (Sequence Number) enthält. Somit kann man einen kontinuierlichen Datenstrom gewährleisten. Dabei koordiniert das Realtime-Transport-Control-Protocol (RTCP) Sender- und Empfänger-Protokolle, überwacht die Qualität der RTP-Verbindungen und passt gegebenenfalls die Übertragungsparameter an. Allerdings ist RTP nicht in der Lage, Bandbreite zu sichern.

Als eine gute Ergänzung würde sich das Reservation-Protocol (RSVP) eignen, wurde aber noch nicht aufgenommen. Es reserviert für zwei getrennte, unabhängige Wege die nötige Bandbreite (für Full-Duplex-Betrieb), indem es als reines Signalisierungsprotokoll die Router nach der verfügbaren Bandbreite frägt. RSVP kann so während der Datentransfers die Übertragungsparameter angleichen, wenn ein Router nicht mehr für die nötige Bandbreite garantieren kann. Auf diese Weise kann man eine gewisse Maximalverzögerung garantieren. RSVP selbst hat keine Quality-of-Service-Unterstützung. Es ist vor allem vorteilhaft, zwei getrennte Datenwege für die zwei Kommunikationspartner zu wählen, da der Datenstrom oft völlig unterschiedlich gross sein kann (zum Beispiel Video-on-Demand oder ähnliches). Der Nachteil ist lediglich,

dass Router, Switches und sonstige Netzgeräte upgedatet werden müssen, um dieses Protokoll zu unterstützen.

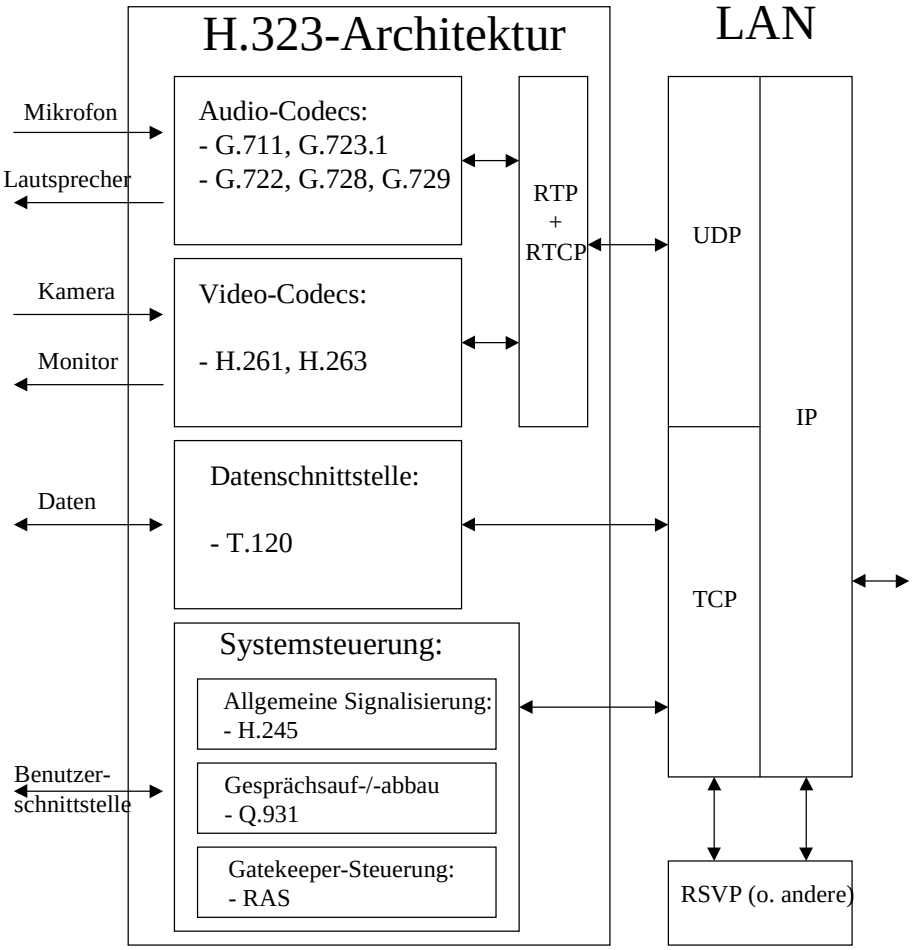

Abbildung 2: Die Architektur von H.323

Beim Aufbau einer H.323-Verbindung wird zunächst über den Port 1720 eine Verbindung hergestellt. Nun wird per Q.931-Protokoll ein Port (>1024) zur Kommunikation ausgehandelt. Über diesen erfolgt dann eine H.245-Verbindung, die zur Festlegung der Verbindungsparameter wie Codecs und ähnlichem dient. Anschliessend erfolgt ein Datenaustausch über einen logischen Kanal per RTP. Für jede Richtung wird ein logischer Kanal benötigt, das RTP-Protokoll selbst benötigt zwei UDP-Verbindungen, eine für den Datenstrom und eine für die Kontrollinformationen. Durch diese Vielzahl von Ports und Pakete ist natürlich ein einfaches Firewall schwer zu realisieren. Generell besteht die Möglichkeit, alle Ports grösser 1024 freizuschalten, da die Portnummern zur Datenübertragung in der nächsthöheren Schicht übertragen werden. [uCis98] [Rohr98b] [KBSS+98] [ITU98]

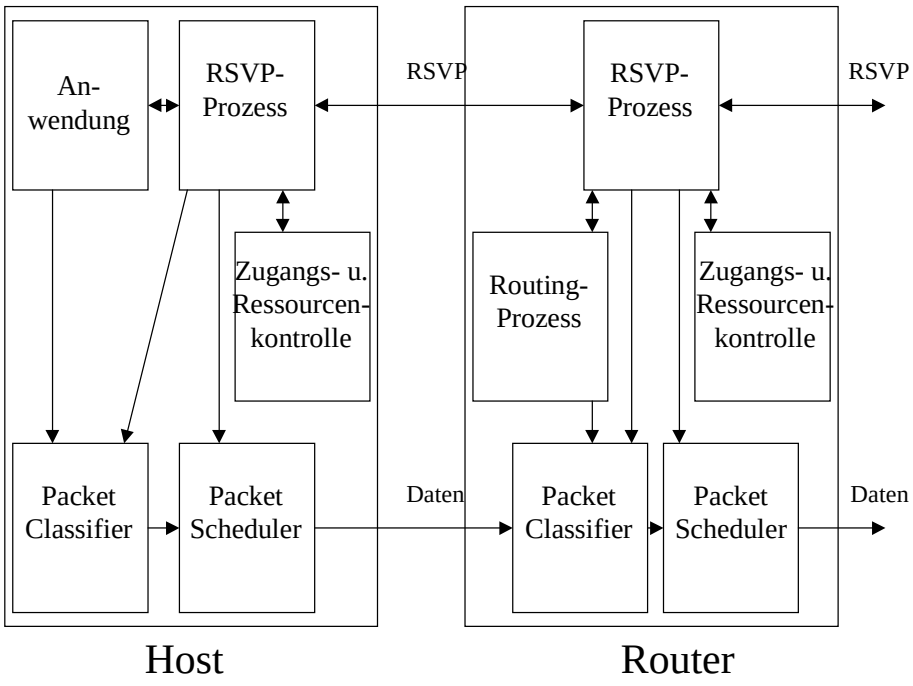

Abbildung 3: RSVP-Datenübertragung

H.32X auf einen Blick			
	LAN/WAN	ISDN	POTS
zugeord. Standard	H.323	H.320	H.324
Sprachübertragung	G.711 (G.722) (G.723.1) (G.728) (G.729)	G.711 (G.722) G.728	 G.723.1 (G.729)
Videodaten	H.261 H.263	H.261 (H.263)	H.261 (H.263)
Multiplexing	H.225.0	H.221	H.223
Kontrolldatenübertrag.	H.245	H.230, H.242	H.245
Multipoint-Verbindungen	H.323	H.231, H.243	nicht multipointfähig
Datenkonferenzen	T.120	T.120	T.120

Standard-Übersicht	
Standard	Aufgaben
G.711	8 khz-abgetastetes PCM-Sprachsignal; 64, 56 und 48 kbps Datenrate (ISDN-Sprachqualität)
G.722	ADPCM-Audio-Codec; 7 khz, 64, 56 und 48 kbps Datenrate
G.723.1	Sprach-Codecs für 5,3 und 6,3 kbps (Audiokompression 10:1)
G.728	LD-CELP-Sprach-Codec für 16 kbps
G.729, G.729a	ACELP-Sprach-Codecs für 8 kbps
H.261	Videodatenübertragung über n*64-kbps-Verbindungen, 176x144 Pixel (Quarter-CIF), optional bis zu 352x288 Pixel (CIF), variable Bildfrequenz
H.263	Videodatenübertragung für niedrige Bandbreite, 128x96 Pixel (Sub-QCIF) und 176x144 Pixel (Quarter-CIF), optional bis 1408x1152 Pixel (16CIF), abwärtskompatibel zu H.261
H.221, H.223, H.225.0	Protokolle, die das Multiplexen und Demultiplexen der verschiedenen logischen Audio-, Video- und sonstiger Datenströme in/aus einem gemeinsamen Datenstrom beschreiben
H.230, H.242	Protokolle zur Steuerung und Synchronisierung von Datenübertragungen in audiovisuellen Systemen
H.231, H.243, H.245	Protokolle für die Ende-zu-Ende-Übertragung von Kontrolldaten zwischen zwei und mehr Multimedia-Geräten, etwa der Aushandlung der Verbindungsparameter und Gerätemöglichkeiten
H.320	allgemeiner Standard zur Beschreibung von Bild-Telefonie über ISDN-Verbindungen
T.120	Standard für Data-Sharing-Anwendungen (z.B. gemeinsame Datenbankzugriffe, Whiteboard-Applikationen); sowohl für Point-to-Point- als auch für Multipoint-Anwendungen

4.1.2 SIP (Session Initiation Protocol)

SIP ist ein weiterer Ansatz zur Standardisierung. Eine einfachere Signalisierung und eine Verzögerung, die bis um Faktor 4 kleiner ist als H.323, machen SIP vor allem im Mobile-IP-Bereich attraktiv. Im Gegensatz zu ITU wird hier das Internet-Protokoll verwendet und ist zu H.323 interoperabel. Die Paketverluste werden auf Anwendungsebene ausgeglichen, Signalisierungen finden über UDP statt. SIP definiert nicht wie H.323 eine Menge von Unterstandards sondern lediglich einen Rahmen (Framework). SIP adressiert über URLs, besitzt eine HTTP-Syntax und eine sogenannte Session Description für ein einheitliches Netzwerk. Call Center sind leicht über SIP implementierbar. [Hass98b]

4.1.3 Gegenüberstellung H.323 - SIP

H.323 vs. SIP	
H.323	SIP
flexibel aber komplex; aufwendiges Signalisierungsverfahren (H.225/H.245)	einfache Signalisierung; besser für Thin Clients wie Mobiltelefone
Session-up Latency 6,5 bis 8 RTT H.323-Signalisierung basiert auf TCP, bei Paketverlust lange Delays	Session-Up Latency 1,5 RTT SIP verwendet UDP für die Signalisierung, Fehler werden auf der Anwendungsebene behandelt
H.323 compliant bezieht sich auf einen Teil eines umfangreichen Standard-Sets	textbasiert, einfach erweiterbar, auf dem Internet-Protokoll HTTP aufgebaut, H.323 interoperabel
breite Industrieunterstützung	nicht fertig entwickelt

Trotz der vielen Vorzüge von SIP gegenüber H.323 wird ein Umstieg kaum denkbar sein, alleine schon wegen der hohen getätigten Investitionen in die H.323-Technologie. Ausserdem ist SIP noch nicht fertig entwickelt. Es bleibt fraglich, ob SIP jemals wirklich trotz der unkomplizierten Signalisierung zu H.323 interoperabel bleiben wird. SIP wäre leicht nachrüstbar, weil alles ausschliesslich auf HTTP und UDP basiert, so dass eine spätere Integration in H.323 durchaus denkbar wäre. H.323 ist der am meisten verbreitete Standard und durchaus leistungsfähig, so dass wohl die Industrie nicht an einen Umstieg denken wird.

4.2 Sprachcodierung

Die Sprache kann auf zwei verschiedenen Arten codiert werden. Auf der einen Seite gibt es die waveform coders wie zum Beispiel das PCM-Verfahren (Pulse Code Modulation), dass die Amplituden der digitalisierten Sprache auf eine endliche Menge diskreter Werte abbildet (Quantifizierung). Die zweite Möglichkeit sind sogenannte Vocoder (Voice Coders). Sie versuchen aus der digitalisierten Sprache ein Signal zu berechnen, aus dem sich die gesprochene Sprache wieder rekonstruieren lässt.

Der in Telefonen eingesetzte Codec (Coder/Decoder) heisst G.711 PCM. Da dieser keine Kompression verwendet, benötigt er eine Bandbreite von 64 kBit pro Sekunde. Dieser Codec wäre natürlich für eine Modem-Übertragung uneffektiv. Der erste Ansatz zu einem komprimierenden Codec-Design war der G.726 ADPCM (Adaptive Differential PCM). Hier wird angenommen, dass die abgetasteten Sprachsignale nur geringfügig von einander unterscheiden. Also wird ein Grundsignal und die Abweichungen dieses Wertes übertragen. Kompressionen bis 50 Prozent können so leicht erzielt werden, auch wird der CPU nicht viel abverlangt (lediglich eine Rechenleistung von ewa 8 Mips). Ein noch effektiveres Verfahren stellt die CELP-Technologie (Codebook Excited Linear Predictive Coding). Hier stellt ein mathematische Modell des menschlichen Sprachsystems die Grundlage dar. Ein Transmitter vergleicht den Sprachstrom mit diesem Modell und erzeugt so einen Code. CELP kann die PCM-Qualität fast erreichen, erzeugt aber nur einen 16 kBit-Datenstrom pro Sekunde. Die dafür benötigte CPU-Last ist jedoch mit 20-40 Mips erheblich grösser. In IP-Netzen wird der ITU-Standard G.728 LD-CELP (Low Delay CELP) verwendet. Neu dabei ist der Standard G.729 CSA-CELP (Conjugate-Stucture-Algebraic-CELP). Er führt noch aufwendige Analysen beim Vergleich mit dem Sprachmodell durch und kann so die nötige Bandbreite noch halbieren. Einig ist man sich mittlerweile auf eine Weiterentwicklung geworden, dem Dual-Rate Speech Coding Standard G.723. Dieser Standard findet heute bereits Verwendung bei der Sprach- und Video-Übertragung in analogen Systemen.

Eine weitere Verfeinerung stellt die Silence Surpression dar, so dass in Momenten, in denen nichts gesprochen wird, auch keine Daten verschickt werden. Hier wird einfach ein Steuercode für die Schweigepause definiert und so sehr viel Bandbreite gespart. [uCis98] [Rohr98a]

Audio-Codecs-Übersicht				
Code-Typ	Übertragungsrate	Prozessorlast	Sprachqualität	Verzögerung
G.711 PCM	64 kbps	-	sehr gut	unwesentlich
G.726 ADPCM	40/32/24/16 kbps	8 Mips	gut bis schlecht	sehr gering
G.729 CS-ACELP	8 kbps	30 Mips	gut	gering
G.729A CA-ACELP	8 kbps	20 Mips	zufriedenstellend	gering
G.723 MP-MLQ	6,4/5,3 kbps	20 Mips	gut bis schlecht	hoch
G.723.1 MP-MLQ	6,4/5.3 kbps	20 Mips	gut bis schlecht	hoch
G.728 LD-CELP	16 kbps	40 Mips	gut	gering

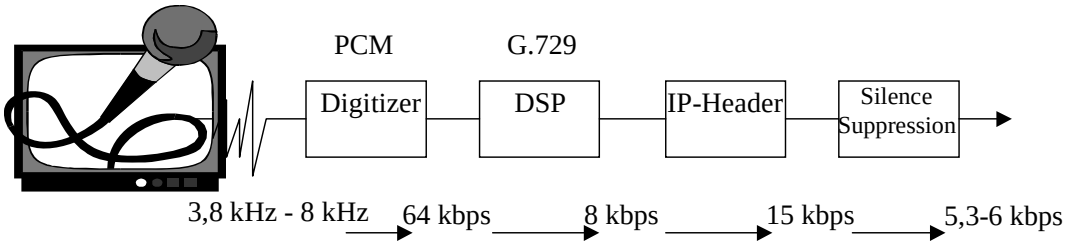

Abbildung 4: Bandbreiten

5 Der wirtschaftliche Aspekt

Voice-over-IP bringt sehr viele Vorteile mit sich, vor allem für Firmen mit einem internen Netz. So liesse sich eine Telefonanlage vollständig ersetzen, das firmeneigene Netz könnte besser ausgelastet werden. Man könnte von den Vorzügen der Technologie profitieren und zum Beispiel Datenaustausch beim Telefonieren betreiben. Die Firma kann viel Geld einsparen, da nur noch ein Netz zu betreuen ist und sie nun eine bessere Kommunikationsinfrastruktur besitzt, die sehr leicht erweiterbar und ausbaubar ist. Bereits nach etwa 14 Monaten ist die gesamte Investition amortisiert. So lassen sich kostengünstig alle Filialen und Standorte der Firma verbinden, es entstehen keine Telefonkosten. [Wess98] [uCis98] [Crue98]

Soll allerdings nach ausserhalb des eigenen Netzes telefoniert werden, so muss man den kostenpflichtigen Dienst eines Carriers oder Internet-Service-Providers in Anspruch nehmen. Durch den nun offenen, liberalisierten Telefon-Markt herrscht ein grosser Preiskampf zwischen den vielen Anbietern. Da Voice-over-IP noch sehr jung ist, existiert noch nicht sehr grosse Konkurrenz. Meist handelt es sich bei ihnen noch um Pilotprojekte, die sich im Aufbau befinden.

6 Systeme auf dem Markt

Im folgenden sollen die jeweils drei wichtigsten Produkte in ihren Möglichkeiten und Vorteilen vorgestellt werden.

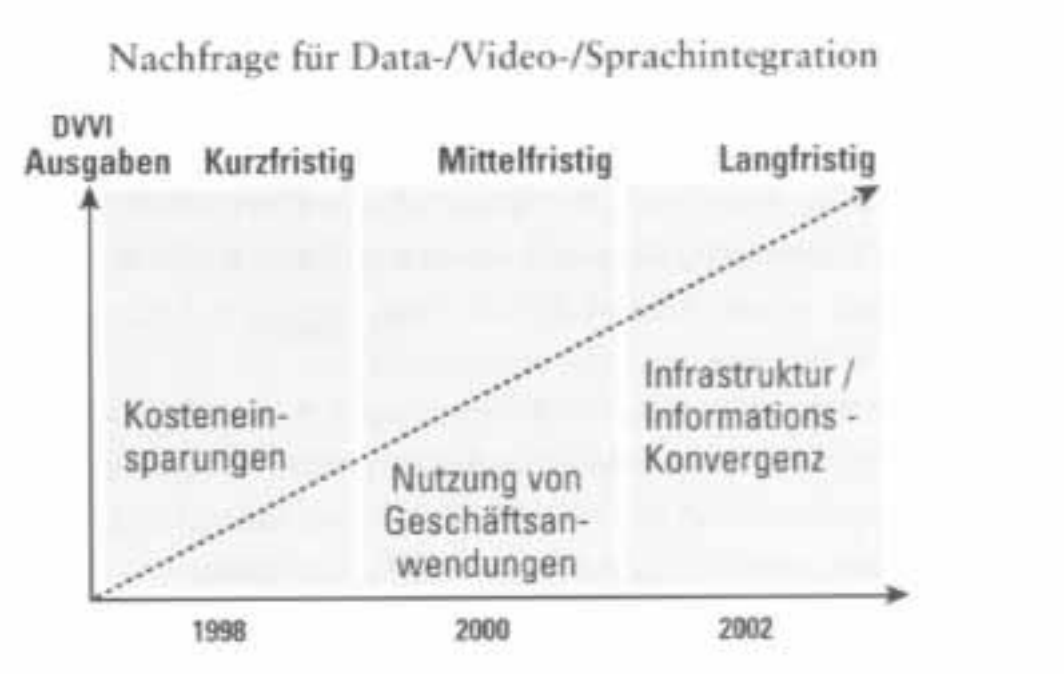

Abbildung 5: Nachfrage nach Voice-over-IP

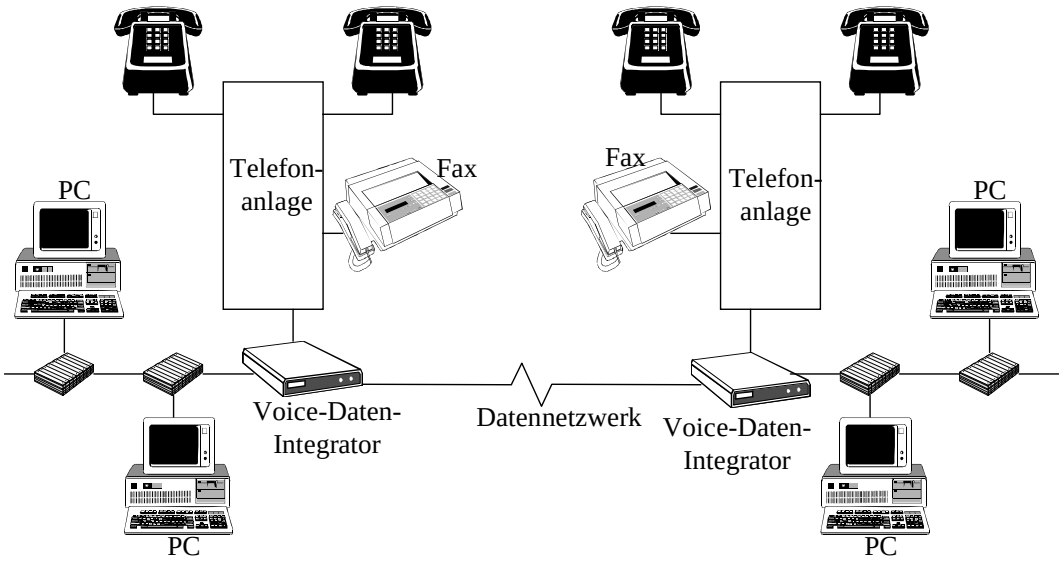

Abbildung 6: Einbindung von Voice-over-IP

6.1 Hardware

6.1.1 Siemens Interxpress

Siemens brachte das erste Komplettpaket auf den Markt, bestehend sowohl aus Hard- als auch aus Software. Gemäss ITUs H.323-Standard werden die Codecs und die Dienste genutzt, weitere Dienste sind modular nachrüstbar (wie zum Beispiel Call Center oder Least Cost Routing). Abrechnungen können individuell erstellt werden. Siemens hat eine hervorragende Sprachqualität ermöglichen können und Interxpress soll sogar schon ab einem Modem mit 14.4 KBit/s funktionieren.

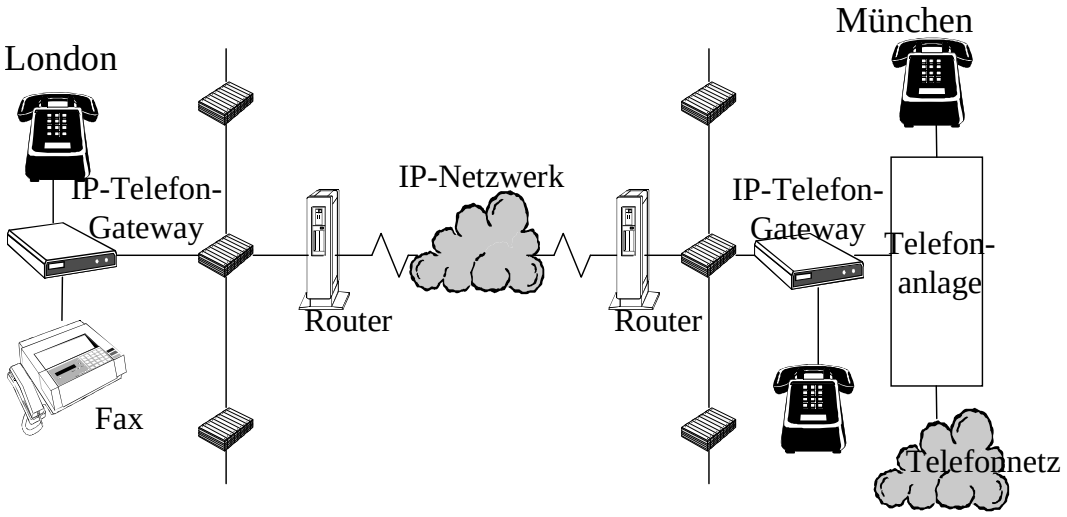

Abbildung 7: Sprachintegration in IP-WANs

6.1.2 Lucent Internet Telephony Server For Enterprises

Wie der Name schon sagt eignet sich diese Lösung lediglich für Grossfirmen. Lucent benutzt bei der Sprachübertragung ein eigenes Kompressionsformat, die Abrechnung erfolgt wie bei Siemens softwareseitig. ITSFE ist ebenfalls kompatibel zu H.323.

6.1.3 Ericsson Gatekeeper

Ericsson unterstützt als einer der ersten das H.323v2-Protokoll. Der Gatekeeper ist Teil einer ganzen Multimedia-Komplettlösung. Abgerechnet wird hier sogar hardwareseitig über einen Abrechnungs-Server. Die Besonderheit ist, dass sich von jedem beliebigen Punkt des Netzes eine Überwachung einrichten lässt, Fehlfunktionen werden an einer Konsole gemeldet.

[Hass98a]

6.2 Software

6.2.1 VocalTec iPhone (InternetPhone)

1. - PC-2-Phone-Communication (über Internet Telephony Service Provider (ITSP))
2. - Audio-Multiconferencing mit bis zu 100 Teilnehmern
3. - TextChat
4. - Full-Duplex
5. - Cross-Platform
6. - Automatic Voice Activation (passt Sprachqualität automatisch der jeweiligen Bandbreite an)
7. - Whiteboarding (Datenaustausch mit mehreren Leuten)

Abbildung 8: VocalTec IPhone

6.2.2 White Pine CUSeeMe

1. H.323-Kompatibilität
2. Liste von Codecs zur individuellen Einstellung je nach Netzleistung
3. Telefonbuch
4. Videomulticonferencing mit bis zu 12 Teilnehmern
5. Online-Detection für User
6. Whiteboarding (Datenaustausch mit mehreren Leuten)

6.2.3 NetSpeak WebPhone

1. - H.323v2-Support
2. - Voice Audio Detection (passt Sprachqualität automatisch der jeweiligen Bandbreite an)
3. - Video-Phone (H.263)
4. - Online/Offline Voice Mail System
5. - TextChat
6. - Telefonbuch

Abbildung 9: White Pine CUSeeMe

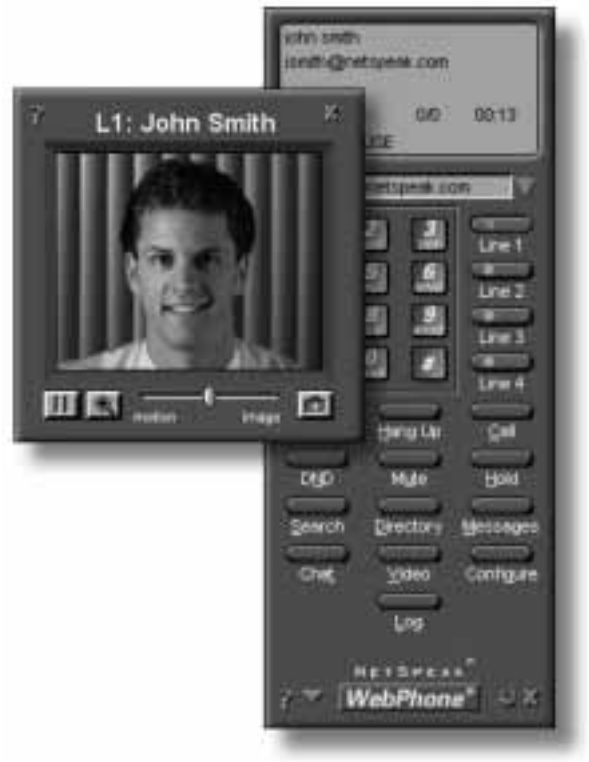

Abbildung 10: NetSpeak WebPhone

Literatur

[Crue98] Marco Crueger. Stark im Internet - Voice over IP im professionellen Einsatz. *Gateway*, Juni 1998.

[Hass98a] Harald Hassenmüller. IP- und Telefonnetze verbinden. *LANline*, Februar 1998.

[Hass98b] Harald Hassenmüller. Kampf in der IP-Telefonie. *LANline*, September 1998.

[ITU98] ITU. Standard H.323 Tutorial. *Internet Draft http://comsoc.org.mx/std_h323.htm*, Oktober 1998.

[KBSS+98] Thomas J. Kostas, Michael S. Borella, Ikhlaq Sidhu, Guido M. Schuster, Jacek Grabiec und Jerry Mahler. Real-Time Voice Over Packet-Switched Networks. *IEEE Network*, Januar 1998.

[Rohr98a] Kai Rohrbacher. Die Multimedia-Falle. *iX*, September 1998.

[Rohr98b] Kai Rohrbacher. Weltweit zum Ortstarif. *iX*, August 1998.

[uCis98] Rupert Goodwins und Cisco Systems. Tech Guide - Telefonieren im IP-Netz. *PC Professionell*, Dezember 1998.

[Wess98] Berthold Wesseler. Mit 58 Pfennig in die USA. *Gateway*, Oktober 1998.

Differentiated Services: Neue Ansätze für Dienstgüte im Internet

Paul Burczek

Kurzfassung

Die Anforderungen ans Internet sind in den letzten Jahren enorm gestiegen. Immer mehr Anwendungen verlangen nach einem besseren Dienst als dem Best-effort-Dienst. Diese Seminarausarbeitung beschreibt die Vorschläge der Diffserv Working Group und der Internet Engineering Task Force für Dienstarchitekturen, die dem Dienstnehmer mehr Dienstqualität anbieten können.

1 Einführung

1.1 Probleme des heutigen Internet

Mit der schnell wachsenden Popularität des Internets wachsen auch die Ansprüche, die dessen Benutzer bezüglich der Übertragungsrate und der Verläßlichkeit der angebotenen Dienste stellen. Der zunehmende Einsatz von Anwendungen mit großen Anforderungen an Übertragungsgeschwindigkeit und Voraussagbarkeit der Dienstgüte, wie z.B. Business- oder Multimedia-Anwendungen, verlangt nach höherer und voraussagbarer Servicequalität. Der Best-Effort-Dienst des heutigen Internets ist mit solchen Anforderungen überfordert.

1.2 Alternative Modelle

1.2.1 Adaptive Methoden

Ein pragmatischer Ansatz zum Erreichen einer guten Servicequalität ist der adaptive Design von Anwendungen. So entworfene Anwendungen passen sich den wechselnden Charakteristiken des Netzes an. Zum Beispiel wird, unmittelbar nach der Entdeckung einer Überlastung des Netzes, die Übertragungsrate mittels einer höheren Komprimierung der Daten gesenkt. Zu diesem Zweck wird eine Überwachung der Servicequalität benötigt. Diese Überwachungsfunktionen werden z.B. durch das RTP (Real-Time Transport Protocol) und das RTCP (Real-Time Control Protocol) bereitgestellt. Diese Protokolle benutzen Signalisierungsnachrichten um ihre Funktion zu erfüllen. Adaptive Methoden stoßen allerdings an ihre Grenzen , wenn Applikationen eine gewisse minimale Bandbreite benötigen, um vernünftige Servicequalität zu erreichen.

1.2.2 Integrated Services

Der erste Schritt zu einem besseren Dienst als den bis jetzt angebotenen Best-Effort-Dienst, ist unter anderem die Integrated-Services-Architektur mit dem RSVP-Protokoll. Hier wird eine

minimale Servicequalität durch Reservierung von Ressourcen garantiert. Integrated Services werden für sogenannte Flows angeboten, die Datenströme von einzelnen Anwendungen zwischen Endsystemen repräsentieren. Die Ressourcen für Flows werden in den Endsystemen und den Routern mit Hilfe von Signalisierungsprotokollen (RSVP - Resource Reservation Protocol) reserviert. Bei einem Reservierungsvorgang müssen entlang eines Kommunikationspfades Netzwerkelemente wie Router, Knoten und sogar die Betriebssysteme der Endsysteme prüfen, ob genügend CPU-Zeit, Speicher und Netzwerkbandbreite zur Verfügung steht, um einen angeforderten Dienst erfüllenn zu können.

1.2.3 Andere Modelle

Die Differentiated Services Working Group (im folgenden Diffserv Working Group genannt) führt noch folgende alternative Modelle an [DSME+98], auf die hier nicht weiter eingegangen wird:

- relatives Prioritätsmodell (relative priority model)
- Virtual Circuit Model
- Service Marking Model

Zusammenfassend läßt sich feststellen, daß Dienstarchitekturen, die das explizite Reservieren von Ressourcen zum Prinzip haben und mit Flows zwischen einzelnen Anwendungen arbeiten (wie Integrated Services), die an sie im realen Internetbetrieb gestellten Anforderungen nicht erfüllen können. Eine große Anzahl von Internetprovidern hat Bedenken bezüglich der rechnerischen und speichertechnischen Kosten, als auch anderer Systemressourcen zum Verwalten von tausenden oder sogar hunderttausenden Flows geltend gemacht [Ferg98].

2 Architektur der Differentiated Services

Das Internet zeichnet sich durch ein kontinuierliches Wachstum in der Anzahl der Hosts, der Anzahl und Vielfalt der Anwendungen und der Kapazität der Netzwerkinfrastruktur aus. Es ist zu erwarten, daß dieses Wachstum für absehbare Zeit anhält. Eine skalierbare Architektur für Dienstdifferenzierung muß für dieses kontinuierliche Wachstum gewappnet sein. Angesichts der Probleme und des schnellen Wachstums des heutigen Internets tauchen folgende Anforderungen an diese Architektur auf [DSME+98]:

- sie muß ein großes Spektrum an Dienstverhalten (service behavior) Dienstzuteilungsmöglichkeiten beinhalten
- sie muß es erlauben, das Dienstverhalten von den verwendeten Anwendungen zu entkoppeln
- sie muß mit existierenden Anwendungen arbeiten
- sie muß Verkehrsbeeinfulßung- (traffic conditioning) und Dienstvergabefunktionen (service provisioning) vom Weiterleitungsverhalten entkoppeln, das in den inneren Knoten des Netzwerks implementiert ist
- sie darf nicht von Hop-by-Hop Anwendungssignalisierung abhängen

- sie darf nur eine kleine Menge von Verhaltensmustern zur Weiterleitung erforderlich machen, deren Komplexität nicht die Kosten für eine Netzwerkeinrichtung (network device) dominiert, und die kein Flaschenhals für zukünftige high-speed Systemimplementationen darstellen wird
- sie muß microflow- und kundenspezifische Zustände im Netz-werkinnern vermeiden
- sie darf im Netzwerkinnern nur zusammengefaßte Klassifikationszustände (aggregated classification state) benutzen
- sie muß einfache Durchführung der Paketklassifikation in den Routern des Netzinnern erlauben
- sie muß einfache Zusammenarbeit mit Netzwerkknoten erlauben, die diese Dienstarchitektur nicht unterstützen (non-compliant network nodes)
- sie muß unter den Bedingungen einer schrittweisen Einführung anwendbar sein

2.1 Grundlegende Merkmale

Die Idee der Differentiated Services (im folgenden Diff-Serv genannt) basiert auf der Zusammenfassung von Flows. Reservierung von Ressourcen geschieht also nicht für einzelne Flows, sondern für eine Menge, auf eine bestimmte Weise zusammenhängender Flows (z.B. alle Flows zwischen zwei Subnetzen).

Die Architektur der Diff-Serv setzt sich aus einer Menge von Funktionselementen zusammen, die in den Netzwerkknoten implementiert sind. Zu diesen Funktionselementen zählt eine kleine Menge von wohl definierten per-hop Forwarding Verhaltensmustern (forwarding behaviors) und Verkehrsbeeinflussungsfunktionen, die wiederum Klassifikation, Messung von Vehrkehrsstromeingenschaften, Markierung, Formung und Überwachung beinhaltet. Die Architektur erreicht Skalierbarkeit durch Implementierung der komplexen Verkehrsbeeinflussungsfunktionen nur an den Eckknoten des Netzwerkes.

2.1.1 Dienst

Unter einem Dienst (*Service*) versteht die Diffserv Working Group in diesem Zusammenhang einige signifikante Charakteristiken der Paketübertragung durch Pfade innerhalb eines Netzwerks [DSME+98]. Diese charakteristischen Merkmale können sein: Durchsatz, Verzögerung, Jitter oder Paketverlust. Sie können auch durch relative Prioritäten für den Zugang zu Netzwerkressourcen angegeben werden.

2.1.2 Architektur

Die Diff-Serv-Architektur hat zum Ziel, skalierbare Dienstunterscheidung (service differentiation) im Internet zu bieten, ohne Zustände für jeden Flow und Signalisierung an jedem Hop zu benutzen. Dieser Ansatz benutzt eine kleine, wohldefinierte Menge von „Bausteinen“ (building blocks), mit denen sich eine Vielzahl von Diensten bilden läßt. Die Architektur der Diff-Serv basiert auf einem einfachen Modell, bei dem der in ein Netzwerk eintretende Datenverkehr an den Rändern des Netzwerks angepaßt wird (conditioning) und entsprechenden Verhaltensaggregaten (behavior aggregate) zugewiesen wird. Jedem Verhaltensaggregat ist eine eindeutige Diff-Serv Kennzahl zugeordnet (wird im folgenden DS-Kennziffer genannt). Im Innern eines Netzwerks werden Pakete entsprechend dem Per-Hop-Verhaltensmuster weitergeleitet, das durch ihre DS-Kennzahl bestimmt ist. Die DS-Kennzahl ist im IP-Kopf eines jeden

Pakets untergebracht. Sie befindet sich im TOS-Feld bei IPv4 bzw. im Class-Feld bei IPv6. IP Pakete werden entweder vom Benutzer (in einem Endsystem oder in einem Router) oder vom Dienstprovider entsprechend gekennzeichnet.

2.1.3 Per-Hop-Verhaltensmuster

Im Modell der Diff-Serv verfügt jeder Router über eine Menge von Parametern zur Kontrolle über das Verteilen der Pakete auf das Ausgabeinterface (z.B. N getrennte Warteschlangen mit variablen Prioritäten, Warteschlangenlängen, Round-Robin Gewichtungen, Drop-Algorithmen, Drop-Schwellen etc.). Die Möglichkeiten der Router und ihre aktuelle Konfiguration bestimmen die verschiedenen Behandlungsarten für Pakete. Zwei Per-Hop-Verhaltensmuster sind weitverbreitet und von der Diffserv Working Group als Standard vorgeschlagen: Default und Expedited Forwarding [Nich98].

Default: Hier handelt es sich um das allgemeine best-effort Weiterleiten, wie es im heutigen Internet zu finden ist. Ein ankommendes Paket wird an das Ende der Warteschlange angehängt, die als FIFO organisiert ist. Pakete kommen also in derselben Reihenfolge raus, wie sie angekommen sind. Das Default-Verhaltensmuster ist mit dem Ziel entworfen worden, möglichst gut das best-effort Verhalten herkömmlicher Router nachzubilden.

Expedited Forwarding: Dieses Verhaltensmuster ist durch hohe Priorität gekennzeichnet und wird vorwiegend für Kontrollfunktionen wie z.B. Routing-Updates verwendet. Ein so gekennzeichnetes Paket wird an das Ende derjenigen Warteschlange angehängt, die relativ kurz ist und somit am schnellsten die Gelegenheit bekommt dieses Paket zu senden.

3 Dienste der Differentiated Services

3.1 Dienste mit Angabe einer absoluten Bandbreite

3.1.1 Premium-Dienst

Dienstdefinition

Der Premium-Dienst ist ein Dienst mit einer extrem kleinen Verzögerung, der Bursts nur im begrenztem Umfang zuläßt und sich mit einer gemieteten Linie vergleichen läßt. Der Kunde handelt mit dem Internet Service Provider (im folgenden ISP genannt) eine maximale Bandbreite aus, um Pakete durch das ISP-Netzwerk zu schicken. Der Aggregatflow wird durch die Ursprungs- und Zieladressen identifiziert.

Dienstarchitektur

First-Hop-Router der Kunden haben die Aufgabe, die Pakete, die vom Endsystem kommen, zu klassifizieren, d.h. zu analysieren, ob die Pakete Premium-Dienst berechtigt sind oder nicht. Wenn ja, werden die Pakete als Premium-Dienst gekennzeichnet. Anschließen wird der Datenstrom entsprechend der vereinbarten maximalen Bandbreite geformt. Wird der Premium-Dienst von mehreren Benutzern des Kundennetzwerks in Anspruch genommen, so muß der Grenzrouter des Kundennetzwerks den Premium-Aggregatstrom des Kundennetzwerks vor dem Weiterleiten zum ISP-Grenzrouter zurückformen. Der ISP-Grenzrouter führt auf dem Premium-Aggregatflow Policingfunktionen durch, d.h. es wird überprüft, ob der Aggregatflow die in der Dienstvereinbarung (im folgenden Service Level Agreement - SLA - genannt) getroffenen Vereinbarungen verletzt. Ist dies der Fall, so können die überzähligen Pakete entweder verworfen werden oder solange zurückgehalten werden, bis sie keine Verletzung des SLA mehr darstellen. Alle First-Hop- und Grenz-Router besitzen zwei Warteschlangen, eine für die

Premium-Dienst-Pakete und eine für alle anderen Pakete. Pakete, die sich in der Premium-Dienst-Warteschlange befinden, werden bevorzugt gesendet. Besitzen alle Router im Kunden- und ISP-Netzwerk die beiden oben beschriebenen Warteschlangen, so haben wir es mit der Realisierung eines virtuellen Netzwerkes für den Premium-Dienst-Verkehr zu tun.

3.1.2 Assured-Dienst

Dienstdefinition

Der Assured-Dienst wird durch ein Burst-Profil charakterisiert [Nich98]. Er offeriert einen Dienst, der keine Bandbreite garantieren kann, der allerdings eine hohe Wahrscheinlichkeit bietet, daß Pakete mit einer hohen Priorität zuverlässig übertragen werden. Der Benutzer handelt mit dem ISP ein Dienstprofil aus, das z. B. die maximale Rate an Paketen mit hoher Priorität bestimmt.

Dienstarchitektur

Pakete, die das SLA verletzen, unterliegen einer größeren Wahrscheinlichkeit verworfen zu werden, bleiben aber in Sendereihenfolge bezüglich der Pakete, die das SLA nicht verletzt haben, wenn sie nicht verworfen werden. Die Wahrscheinlichkeit mit der Pakete zuverlässig transportiert werden, hängt von der Kapazität des Netzes ab. Ein ISP kann die Zuverlässigkeit des Assured-Dienstes auch dadurch unterstützen, daß er die Summe aller Bandbreiten der Assured-Dienste so wählt, daß sie unter der Bandbreite des schwächsten Links bleibt. Der Benutzer kann seine Pakete innerhalb des Endsystems oder des First-Hop-Routers als Assured-Dienst-Pakete kennzeichnen, indem jedes Paket mit einer entsprechenden DS-Kennzahl markiert wird. Möchte man Modifikationen am Endsystem vermeiden, so kann man den First-Hop-Router die Analyse der Pakete anhand der IP-Adresse und des UDP-/TCP-Ports vornehmen lassen. Der First-Hop-Router weist dann jedem Paket, das den Assured-Dienst in Anspruch nehmen soll, die entsprechende DS-Kennzahl zu. Im First-Hop-Router und im Grenzrouter des Benutzers wird dann eine (Re-)Klassifikation vorgenommen um zu garantieren, daß die maximale Rate der Pakete mit hoher Priorität nicht überschritten wird. Der ISP sollte jedoch auch überwachen, ob der Kunde unter der vereinbarten maximalen Übertragungsrate sendet. Im Falle einer Verletzung des SLAs muß er Korrekturmaßnahmen wie Policing anwenden. Bursts können abgefangen werden, indem Pufferkapazität zur Verfügung gestellt wird, in der Burstdaten gespeichert werden können.

Ein großer Vorteil des Assured-Dienstes liegt darin, daß der Benutzer die Reservierung der Ressourcen nicht für eine lange Zeit vornehmen muß. Der Benutzer kann bei ISDN oder ATM unter Umständen die reservierte Bandbreite nicht nutzen, wenn sein Datenverkehr Bursts aufweist. Der Assured-Dienst erlaubt hingegen die Übertragung von kurzzeitigen Bursts.

Empfänger orientiertes Szenario

Die Aushandlung eines Dienstprofils zwischen dem Kunden und dem ISP stellt ein Problem des Assured-Dienstes da. Wenn ein Internetbenutzer z.B. eine Verbindung zu einem Server aufbaut, sollte er in der Lage sein, die Dienstqualität zu bestimmen. Aus diesem Grunde sollte es dem Empfänger möglich sein, ein Benutzerprofil mit dem ISP auszumachen. An der Grenze zwischen dem ISP und dem Netzwerk des Benutzers befindet sich ein Grenzrouter, der das Benutzerprofil kennt und entsprechend diesem Profil den Datenverkehr zwischen dem Server und dem Endsystem des Benutzers gestaltet.

Anpassung von Anwendungen an die Netzauslastung

Der Assured-Dienst kann mit dem Konzept der Adaption von Anwendungen kombiniert werden [BaBH]. Mittels RTP/RTCP können Durchsatz und Paketverlustrate überwacht werden.

Abhängig von Ergebnissen dieser Überwachungsmaßnahmen kann eine größere oder kleinere Anzahl von Paketen als Assured-Dienst-Pakete gekennzeichnet werden. Wenn das Internet nicht ausgelastet ist, kann eine größere Anzahl von Best-Effort-Paketen verschickt werden, womit eine Kostenersparnis einhergehet. Andernfalls muß die Anzahl von Paketen mit hoher Priorität erhöht werden, wenn ein großer Verlust von Best-Effort-Paketen auftritt.

3.1.3 Routerimplementierung

Die Implementierung der Assured- und Premium-Dienste verlangt einige Modifizierungen der Router. Router müssen im Zusammenhang mit diesen Diensten hauptsächlich die zusätzlichen Aufgaben der Klassifizierung, des Shapings und des Policings übernehmen. Diese Funktonen fallen an den Grenzen zwischen zwei Netzwerken an.

First-Hop-Router

In den First-Hop-Routern muß im allgemeinen die Klassifizierung der Pakete vorgenommen werden. Als Parameter für die Klassifikation der Pakete kann die Ursprungs- und Zieladresse oder z.B. die Portnummer verwendet werden. Die Pakete werden dann entsprechend dem für sie bestimmten Dienst Aggregatflows zugewiesen. Best-Effort-Pakete und Assured-Dienst-Pakete werden an die sogenannte RIO-Warteschlange angehängt, die weiter unten beschrieben wird [BaBH]. Die Assured-Dienst-Pakete müssen auf ihre Übereinstimmung mit dem ausgehandelten Verkehrsprofil überprüft werden. Assured-Service-Pakete, die dieses Profil nicht einhalten, werden als Best-Effort-Pakete markiert. Pakete die für den Assured-Dienst bestimmt sind, bekommen aber nur dann die Assured-Dienst-DS-Kennzahl, wenn sich im Assured-Dienst-Behälter (Assured Service Bucket) noch Marken (Token) befinden. Abbildung 1 veranschaulicht den Sachverchalt. Jedem Assured-Dienst-Paket wird dabei eine Marke aus diesem Behälter zugeordet. Die Marken werden entsprechend dem Verkehrsprofil nachgefüllt. Das RIO-Warteschlangenmodell garantiert, daß im Falle einer Kapazitätüberlastung bevorzugt Best-Effort-Pakete verworfen werden. Für die Premium-Dienst-Pakete ist eine eigene Warteschlange vorgesehen. Die Übertragungsrate der Premium-Dienst-Pakete wird ähnlich wie bei Assured-Dienst-Paketen durch einen Premium-Dienst-Behälter mit Marken geregelt.

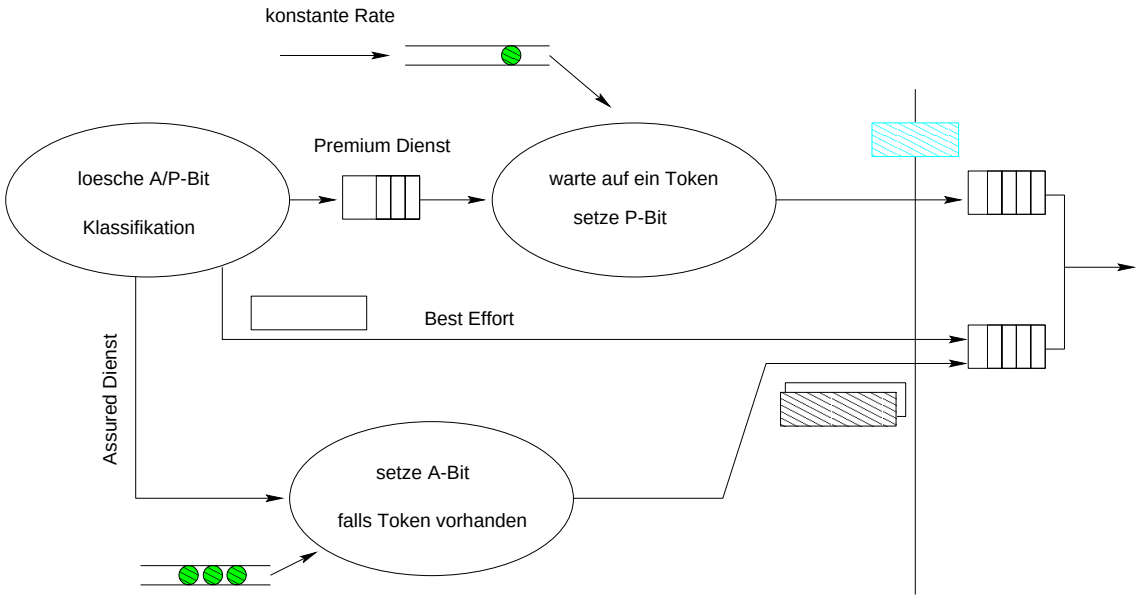

Abbildung 1: First Hop Router für Premium- und Assured-Dienste

Grenzrouter

Grenzrouter übernehmen unter anderem die Aufgabe des Shapings, um zu garantieren, daß nur die per SLA zugelassene Paketrate zum ISP übertragen wird. Insbesondere werden Premium-Service-Pakete und Assured-Dienst-Pakete, die mit dem SLA nicht übereinstimmen, verworfen bzw. als Best-Effort-Pakete markiert.

Warteschlangenmanagement

Ein wichtiges Element in der Implementierung des Premium- und Assured-Dienstes ist eine geeignete Prozedur zum Verwerfen von Paketen im Falle einer Überlastung. Um in einem solchen Fall die vorhandene Bandbreite fair unter den konkurrierenden Datenströmen zu verteilen, wird empfohlen, Pakete aggressiver Datenströme zu verwerfen. Ein fundamentaler Mechanismus, der diese Aufgabe verrichten kann, ist der Random Early Detection Mechanismus (RED). In herkömmlichen Warteschlangen werden ankommende Pakete so lange wie möglich akzeptiert. Wenn die Warteschlange keine weiteren Pakete aufnehmen kann, werden die ankommenden Pakete verworfen.

RED Mechanismus

RED ist ein Mechanismus, der die Länge einer Warteschlange unter einer gewissen Schwellenlänge zu halten versucht, um Kapazitäten für Bursts bereitzuhalten. Dieses Prinzip läßt sich dadurch verwirklichen, daß Pakete auch dann verworfen werden, wenn die Länge der Warteschlange noch relativ klein ist. Unter einer gewissen Schwelle bleiben alle ankommenden und in der Warteschlange befindlichen Pakete erhalten. Je mehr die Länge der Warteschlange über diese minimale Schwelle hinausgeht, desto größer die Wahrscheinlichkeit, daß ankommende Pakete verworfen werden. Das Verwerfen eines Paketes geschieht zufällig, um zu verhindern, daß die Pakete eines und derselben Datenstroms verworfen werden. Wenn die Warteschlange eine bestimmte maximale Schwellenlänge erreicht, wird kein ankommendes Pakete mehr akzeptiert. Der RED-Mechanismus hat die folgenden Vorteile [BaBH]: Bursts werden besser abgefangen, weil für sie immer eine gewisse Kapazität reserviert ist. Zusammen mit der durchschnittlichen Länge der Warteschlange werden auch die Verzögerungen der Pakete reduziert, was eine bessere Unterstützung von Echtzeitanwendungen nach sich zieht.

RIO Mechanismus

RIO (RED with In and Out) ist eine Erweiterung des RED-Mechanismus. Es wird eine einzige Warteschlange eingerichtet, die gleichermaßen out-of-profile und in-profile Pakete annimmt, also Pakete, die das SLA verletzen bzw. SLA konform sind. Die Pakete werden jedoch je nach Klasse einer unterschiedlichen Verwerfungsprozedur (Verwerfer, Dropper) unterzogen. Der Verwerfer für Out-Of-Profile-Pakete verwirft seine Pakete früher, d.h. ab einer kleineren Länge der Warteschlange als der In-Profile-Verwerfer. Hinzu kommt, daß die Wahrscheinlichkeit für das Verwerfen eines Pakets bei dem Out-Of-Profile-Verwerfer schneller steigt als bei dem In-Profile-Verwerfer. Dadurch wird versucht, die Wahrscheinlichkeit für das Verwerfen eines Pakets, das das SLA erfüllt, klein zu halten. Der RIO-Mechanismus für bevorzugt für den Assured-Dienst benutzt. 2 illustriert dieses Verhalten.

Bei Routern, die Implementierungen von verschiedenen Typen von Diensten unterstützen, müssen mehrere Warteschlangen realisiert werden, z.B. Warteschlangen für den Premium-Dienst oder den Assered-Dienst.

3.2 Dienste mit variabler Bandbreite

3.2.1 User-Share Differentiation

Bei der User-Share Differentiation werden keine absoluten Bandbreiten ausgehandelt, sondern relative Bandbreitenanteile. Einem Benutzer kann nur ein relativer Anteil der verfügbaren

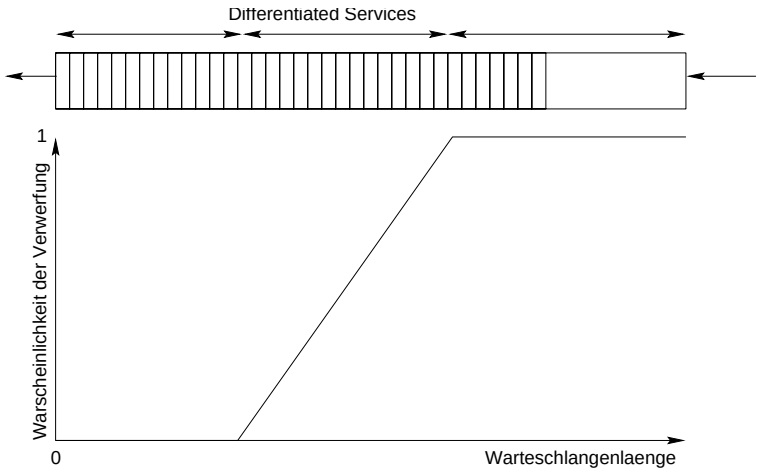

Abbildung 2: Das Verhalten der Warteschlange beim RIO-Algorithmu

Bandbreite in einem ISP-Netzwerk garantiert werden. 1 skiziert einen First-Hop-Router für den Premium- und Assured-Dienst.

Olympic-Dienst

Der Olympic-Dienst weist drei Dienststufen aus: Gold, Silber und Bronze, die sich in abfallender Reihenfolge die Bandbreite während einer Überlastungssituation des Netzwerkes teilen. Der Einsatz dieses Dienstes erfordert ein Verteilerverhalten an jedem Hop, das auf verhältnismäßiger Linkteilung basiert (rate-based link share scheduler). Im Falle einer Überlastung des Netzes bekommen Pakete des „Olympic Gold-Dienstes“ anteilsmäßig mehr Bandbreite als die Pakete des „Olympic Silber-Dienstes“, die wiederum mehr Bandbreite als die Pakete des „Olympic Bronze-Dienstes“ bekommen. Herrscht keine Überlastungssituation und werden keine Gold- und Silber-Pakete gesendet, so bekommen folglich die Bronze-Pakete die volle Bandbreite.

4 Kooperation zwischen Integrated und Differentiated Services

Einige Anwendungen im Internet verlangen nach einer Dienstgüte, die die Anforderungen der Dienstnehmer stärker berücksichtigt, als es die Diff-Serv tun (end-to-end Quality of Service). Zu diesen Anwendungen gehören z.B. Internettelefonie, Video-On-Demand-Anwendungen und andere nicht multimediale Anwendungen, deren Internettraffic im gewissen Maße voraussagbares Verhalten aufweisen muß. Auf den ersten Blick scheint die Integrated-Services-Architecture mit dem RSVP-Protokoll diesen Anforderungen zu genügen. Wenn man jedoch berücksichtigt, welche Nachteile diese Dienstarchitektur in großen Netzwerken mit sich bringt, stellt sich heraus, daß auch diese Dienstarchitektur nicht den oben beschriebenen Anforderungen entspricht.

Die Internet Engineering Task Force (im folgenden IETF genannt) schlägt eine Grundstruktur für Dienste vor, in der Integrated Services und Diff-Serv koexistieren [YRPF$^+$98]. Sie zielt auf die Bedürfnisse großer ISPs, die Transitnetzwerke im Internet betreiben, als auch auf die Anforderungen der Benutzter von - Dienstgüte verlangenden - Anwendungen.

4.1 Voraussetzungen

Die IETF legt eine allgemeine Netzwerktopologie zugrunde, die kleinere Int-Serv-Netzwerke mit RSVP als Randnetzwerke (stub networks) vorsieht, die mit größeren Diff-Serv Netzwerken als Transitnetzwerke verbunden sind. Abbildung 3 enthält eine Skizze dieser Topologie.

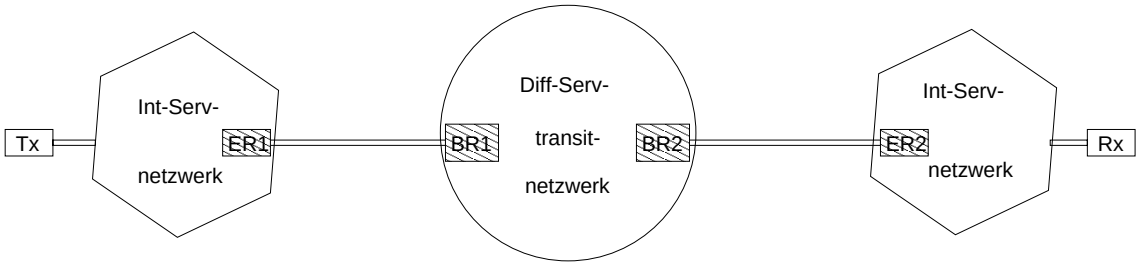

Abbildung 3: Beispiel einer Netzwerkkonfiguration

Ein Netzwerk, das Dienstgüte für den Datenverkehr zwischen einzelnen Anwendungen anbieten soll, muß gewisse Voraussetzungen erfüllen, die von dem Netzwerkbetreiber als auch von den Anwendungen gestellt werden. Im folgenden werden Voraussetzungen beschrieben, die die IETF in diesem Zusammenhang aufstellt [YRPF+98].

4.1.1 Definition einer Menge von Diensten

Es sollte eine Menge von sinnvollen Diensten für die Kommunikation zwischen einzelnen, Dienstgüte erfordernden Anwendungen geben. In Diff-Serv-Netzwerken können diese Dienste durch Konkatenation von gewissen wohldefinierten PHBs gewonnen werden. Es wird vorausgesetzt, daß Netzwerke mit Integerated Services diese Dienste entsprechend ihrer Charakteristiken erkennen und fortführen.

4.1.2 Zuweisung von Diff-Serv-Dienststufen zu spezifischen Flows

Anwendungen, die für ihre Flows Dienste mit einer Dienstgüte beanspruchen, muß es möglich gemacht werden, ihren Flows unterschiedliche Dienste zuzuweisen. Innerhalb der Int-Serv Netzwerken sollten Anwendungen die Möglichkeit haben, mittels RSVP MF-Klassifizierer zu konfigurieren, die anhand von IP-Adressen und Portnummern ihre Aufgabe erfüllen. Innerhalb der Diff-Serv Netzwerke geht die Dienstzuweisung anhand der DS-Bytes im Paketkopf vonstatten.

Daraus ergibt sich die Notwendigkeit der Einflußnahme von Anwendungen auf die Markierung der DS-Bytes von IP-Paketen, die einem Diff-Serv-Netzwerk übergeben werden. Hierbei gibt es zwei grundsätzliche Mechanismen:

1. Hosts markieren direkt die DS-Bytes in den IP-Paketen der Anwendungen, die einen Dienst mit einer Dienstgüte in Anspruch nehmen.

2. Router, die außerhalb eines Diff-Serv-Netzwerkes liegen, können das DS-Byte für die Anwendung, anhand von MF-Klassifizierern, markieren.

Im ersten Fall geschieht die Markierung auf der Grundlage der Konfiguration des Hosts. Im zweiten Fall geschieht die Markierung anhand der Konfiguration des MF-Klassifizierers des markierenden Routers. Die Konfiguration des MF-Klassifizierers kann manuell oder mittels

einer standardisierten Signalisierung zwischen der dienstnehmenden Anwendung und dem MF-Klassifizierer bzw. Marker des markierenden Routers erfolgen.

Welcher Mechanismus zur Markierung gewählt wird, hängt vom minimalen Managementaufwand, der „Granularität“ der Zuweisung und von den Informationen, die man für eine solche Zuweisung benötigt, ab.

4.1.3 Zugangskontrolle

Um den Zugang zu einem Int-Serv-Netzwerk zu erbitten, benutzen Anwendungen explizit das RSVP. Wenn eine Anfrage einer Anwendung abgelehnt wurde, sendet die Anwendung keine IP-Pakete, oder sie nimmt nur den Best-Effort-Dienst in Anspruch.

In Diff-Serv-Regionen des Netzwerkes geschieht die Zugangskontrolle implizit beim Policing in einem Netzwerkrandrouter. Die implizite Zugangskontrolle in Diff-Serv-Regionen stellt ein Problem dar, denn sie bricht die Gültigkeit der expilziten Zugangskontrolle auf. Insbesondere kann eine Anwendung mittels RSVP-Signalisierung den Zugang erhalten, obwohl keine Ressourcen in der Diff-Serv Region für die Flows der Anwendung vorhanden sind. Dienstgüte für die Kommunikation zwischen einzelnen Anwendungen in Endsystemen erfordert, daß dienstnehmende Anwendungen und RSVP-fähige Int-Serv-Knoten über einen Mißerfolg beim Erbitten des Zugangs zu einer Diff-Serv-Region informiert werden. Es ermöglicht ihnen regulirende Maßnahmen einzusetzen und das Diff-Serv-Netzwerk vor Überlastung zu schützen.

4.1.4 Unterstützung des Policings

Policing verläuft innerhalb der Diff-Serv-Regionen auf Kundenbasis. Wenn der Kunde ein ganzes Int-Serv-Netzwerk repräsentiert, muß er selbst in seinem Netzwerk Policing durchführen, um sicherzustellen, daß jedem individuellen Host in seinem Netzwerk entsprechende Ressourcen zugewiesen werden.

4.2 Beispiel einer Kooperation

Im folgenden wird beschrieben wie ein Dienst mit einer Dienstgüte, im oben beschriebenen Sinne, von zwei Anwendungen in Anspruch genommen wird. Der Aufbau des Netzes ist in 3 dargestellt.

1. Ein Prozeß des sendenden Hosts generiert eine RSVP PATH-Nachricht. Diese charakterisiert den Datenstrom, der von einer Anwendung, die einen Dienst mit einer bestimmten Dienstgüte anfordert, gesendet werden soll.

2. Die PATH-Nachricht wird zu dem adressierten Host übertragen. Dabei wird im Int-Serv-Netzwerk des sendenden Hosts in allen RSVP-fähigen Hosts das übliche RSVP-Verfahren duchgeführt.

3. Die PATH-Nachricht wird im Netzwerkrandknoten ER1 dem standardmäßigen RSVP-Verfahren unterzogen, und es wird ein PATH-Zustand eingerichtet. Die PATH-Nachricht wird in das Transitnetzwerk weitergeleitet.

4. Die PATH-Nachricht wird transparent durch das Transitnetzwerk übertragen. Im empfängenden Int-Serv-Netzwerk löst sie das entsprechende herkömmliche RSVP-Verfahren aus.

5. Im empfängenden Host generiert ein Prozeß eine RSVP RESV-Nachricht, die Interesse an dem angebotenen Datenstrom innerhalb des bestimmten Dienstes anzeigt.

6. Die RESV-Nachricht wird zurück zum sendenden Host übertragen. Entsprechend den herkömmlichen RSVP-Regeln, kann sie unterwegs im einem der RSVP-fähigen Knoten des empfängenden Netzwerkes abgewiesen werden, wenn die benötigten Ressourcen nicht zur Verfügung stehen.

7. Die RESV-Nachricht wird im Netzwerkrandknoten ER2 dem üblichen RSVP-Verfahren unterworfen. Sie kann zurückgewiesen werden, wenn die Ressourcen auf der Seite des Int-Serv-Netzwerkes nicht zur Verfügung gestellt werden können. Wenn sie nicht abgewiesen wird, wird sie transparent zum Netzwerkrandknoten ER1 übertragen.

8. Hier tritt der Zugangskontrolldienst auf den Plan. Er vergleicht die Ressourcen die gefordert werden, mit den Ressourcen, die vom Diff-Serv-Transitnetzwerk bereitgestellt worden sind.

9. Wenn die erforderliche Kapazität zur Verfügung steht, wird die RESV-Nachricht zugelassen und zum sendenden Host übertragen. Im anderen Fall wird sie abgewiesen.

10. RSVP-fähige Hosts können sie unterwegs nach dem üblichen RSVP-Verfahren abweisen. Wenn sie unterwgs nicht abgewiesen wurde, gelangt sie zum sendenden Host.

11. Im sendenden Host wird sie von der Anwendung empfangen. Sie interpretiert diese Nachricht als die Bestätigung, daß ihr Datenstrom in der gewünschten Dienstgüte zugelassen wurde. Sie fängt an, in den IP-Paketköpfen das DS-Byte zu setzen, das dem Int-Serv-Dienst entspricht, der mit der RESV-Nachricht durch die Int-Serv-Netzwerke und das Transitnetzwerk zugelassen wurde.

5 Definitionen

DS-Feld: Ipv4 Oktett oder Ipv6 Traffic-Class Oktett, das das Per-Hop-Verhaltensmuster eines Pakets bestimmt.

DS Domain: Eine Menge von benachbarten Diff-Serv-Netzwerkknoten, mit gleichen Charakteristiken bzg. der Diff-Serv.

DS-Kennzahl: Ein spezifisches Bitmuster des DS-Feldes.

Diff-Serv-Region: Eine Menge benachnarter DS Domains, die Differentiated Services auf Pfaden durch diese Domains anbieten.

Flow: Anwendungsdatenstrom zwischen Endsystemen.

Int-Serv-Region: Eine Menge benachbarter Int-Serv-Domains.

Klassifizierer: Ein logisches Element der Verkehrbeeinflussung, das Pakete anhand des Inhalts ihrer Paketköpfe gemäß einiger definierter Regeln selektiert.

MF Klassifizierer: Multi-Field Klassifizierer. Siehe Klassifizierer.

Microflow: Eine einzige Instanz eines Paketstroms zwischen zwei Anwendungen, die durch Ursprungsadresse, Ursprungsport, Zieladresse, Zielport und Protokollkennzahl identifiziert wird.

Netzwerkrandknoten: Ein besonderer Knoten, der an der Grenze zu einem Netzwerk ohne Diff-Serv liegt.

Per-Hop-Verhaltensmuster: Die Behandlung, die ein Paket beim Weiterleiten in einem Netzwerkknoten erfährt (PHB Per-Hop-Behavior).

Überwachung (Policing): Der Prozeß der Anwendung von Verkehrsbeeinflussungsfunktionen auf Verkehrsströme, wie Marking oder Verwerfen von Paketen, im Einklang mit dem Zustand der korrespondierenden Messeinrichtung.

Shaper: Ein logisches Element der Verkehrsbeeinflussung, das Pakete innerhalb eines Verkehrsstromes verzögert, um sie gewissen definierten Verkehrseigenschaften anzupassen.

Verkehrsstrom: Eine administrativ signifikante Menge von einem oder mehreren Microflows, die ein Pfadsegment durchqueren. Ein Verkehrsstrom kann aus einer Menge von aktiven Microflows bestehen, die durch einen Klassifizierer selektiert wurden.

6 Ausblick

Die beschriebenen Vorschläge der Differentiated Services Working Group und der Internet Engineering Task Force werden ständig überarbeitet und die dort vorgestellten Modelle und Strukturen weiterentwickelt. Das führt dazu, daß die vorliegende Seminarausarbeitung mit der Zeit an Aktuallität einbüßen wird. Die Grundstrukturen der beschriebenen Vorschläge mögen jedoch bis zu ihrer Implementierung bestehen. Die aktuellen Internet-Drafts befinden sich auf dem folgenden FTP-Server: ftp.nordu.net.

Literatur

[BaBH] F. Baumgartner, T. Braun und P. Habegger. Differentiated Services: A new Approach for Quality of Service in the Internet. University of Berne, Institute of Computer Science and Applied Mathematics.

[DSME+98] Black D., Blake S., Carlson M., Davies E., Wang Z. und Weiss W. An Architecture for Differentiated Services. Internet-Draft, Mai 1998.

[Ferg98] P. Ferguson. Simple Differential Services: IP TOS and Precedence, Delay Indication, and Drop Preference. Internet-Draft, Marz 1998.

[Nich98] K. Nicholas. Differentiated Services Operational Model and Definitions. Internet-Draft, Februar 1998.

[YRPF+98] Bernet Y., Yavatkar R., Ford P., Baker F. und Zhang L. A Framework for End-to-End QoS Combining RSVP/Intserv and Differentiated Services. Internet-Draft, Marz 1998.

Pricing und Tarifierung im Internet

Joachim Moser

Kurzfassung

Diese Arbeit behandelt den Bereich des Pricing von Transportdiensten im Internet. Durch das rasante Wachstum des Internet sind die bisherigen größtenteils nutzungsunabhängigen Tarifsysteme nicht länger geeignet, um eine sinnvolle und effiziente Nutzung der Ressource "Internet", die den Dienst "Übertragung von Information" bereitstellt, zu gewährleisten. Desweiteren wird durch neue bandbreitenintensive Anwendungen und die Möglichkeit der Reservierung von Ressourcen die Notwendigkeit von nutzungsabhängigen Pricingmodellen, die die knappe Ressource möglichst optimal aufteilen, immer offensichtlicher. In der Literatur wurden schon einige ökonomische Modelle zur Lösung dieses Problems vorgeschlagen. Stellvertretend werden in dieser Arbeit zwei Modelle vorgestellt: das Smart Market Modell und das Markt Modell. Das Hauptproblem bei den meisten ökonomischen Modellen liegt zum einen in ihren vereinfachenden und sehr theoretischen Annahmen und zum anderen in der meist sehr komplexen Berechnung des optimalen Preises, für die meist die Kenntnis der Nutzenfunktionen der Nutzer erforderlich ist. So gilt auch für die beiden hier vorgestellten Modelle, daß sie wohl nicht implementierbar sind. Als Alternative zu den rein ökonomischen Modellen wird nachfolgend eine auf RSVP basierte Pricingumgebung vorgestellt, die sich auch schon in einer realitätsnahen Testumgebung bewährt hat. Es zeigt sich, daß das Gebiet des Pricing im Internet noch viel, vor allem interdisziplinärer Forschung bedarf, um eine möglichst optimale, umsetzbare Lösung zu finden, die auch die technologische Entwicklung des Internet miteinbezieht.

1 Einleitung

Durch neue Multimedia Anwendungen und die Entwicklung des Internets hin zu einem Integrated Services Netzwerk wird das ohnehin schnelle Wachstum des Internets noch verstärkt. Dadurch wird die Übertragungskapazität des Netzwerks immer häufiger zum Engpaß. Auch stellen neue Anwendungen neue höhere Anforderungen an die Dienstgüte und die Garantien der Übertragung. Das bisher vorherrschende Abrechnungsmodell, bei dem die Kosten unabhängig vom Grad der Ressourcenbeanspruchung sind, hat für das bisherige best- effort Internet noch akzeptabel funktioniert, ist aber für diese neuen Entwicklungen ungeeignet und führt nicht zu einer angemessenen Nutzung der Netzwerkressourcen (Motto: "Warum nicht immer die beste Dienstgüte wählen, wenn der Preis dafür nicht höher ist als bei best-effort."). Die heutige Situation im Internet, in der lange Wartezeiten selbst das Websurfen oft zum Geduldsspiel machen, verlangt nach neuen Abrechnungsmodellen (Pricingmodelle) für das Internet, die den sich ändernden Gegebenheiten gerecht werden. Diese neuen Modelle versuchen den Grad der Nutzung der Netzwerkressource für die Preisbestimmung (usage-based) zu verwenden, um damit die Ressourcenallokation im Netzwerk möglichst effizient zu gestalten.

Diese Arbeit versucht das Thema "Pricing im Internet" näher zu beleuchten, einige Modelle näher vorzustellen und die Probleme bei der Umsetzung der Modelle in die Realität zu skizzieren.

2 Pricing

In den Wirtschaftswissenschaften wird ein knappes Gut über den Preis auf die Verbraucher aufgeteilt: je mehr Nutzen das Gut einem Verbraucher stiftet, desto mehr ist er gewillt zu zahlen. Der Preismechanismus führt zu einer ressourcenoptimalen Aufteilung. Dabei sollen gemeinhin zwei Ziele erreicht werden: Paretooptimalität und Preisstabilität. *Paretooptimalität* bedeutet, daß die begrenzten Ressourcen so aufgeteilt werden, daß kein Verbraucher durch Ressourcenmehrverbrauch seinen Nutzen erhöhen kann, ohne den Nutzen eines anderen zu schmälern. *Preisstabilität* bedeutet, daß der Preismechanismus bei Veränderung von Angebot oder Nachfrage wieder in einen Gleichgewichtszustand führt. Ein optimaler Preismechanismus erzeugt einen Preis für ein knappes Gut, der die ressourcenoptimale Aufteilung des Gutes gewährleistet. Man sieht: Preisfestsetzung und Ressourcenallokation sind zwei Seiten derselben Medaille. Im folgenden wird unter dem Term *"Pricing"* die Methode der Abrechnung von Transportdiensten im Internet und damit die Preisbestimmung verstanden. Das Internet ist dabei die Ressource die den Dienst "Übertragung von Information" bereitstellt. Dieser Dienst ist das Gut für das ein Preis bestimmt werden muß. Dabei sollte in die Preisbestimmung die Charakteristik des Dienstes, zum Beispiel die Bandbreite, die Verzögerung, Garantien usw., einfließen.

2.1 Charakteristik der Ressource

Das Pricing eines Gutes hängt maßgeblich von dessen Charakteristik ab. Im folgenden Abschnitt sollen die wesentlichen Merkmale des Internets dargestellt werden.

2.1.1 Technische Entwicklung

Das Internet als dezentrales, heterogenes Netz von Netzwerken, deren Hosts über dasselbe Netzwerkprotokoll TCP/IP kommunizieren wird von keiner zentralen Instanz verwaltet. Das aus einem Forschungsprojekt des US-amerikanischen Verteidigungsministeriums hervorgegangene Internet wurde geprägt durch die Fokussierung auf technische Gesichtspunkte. Ökonomische Gesichtspunkte des Internets fanden zumindest bis Anfang der 90er Jahre wenig Beachtung.

Bei einer Telefonverbindung findet eine verbindungsorientierte Kommunikation statt, das heißt für ein Gespräch wird ein dezidierter physikalischer Link aufgebaut. Somit kann eine feste Übertragungsbandbreite garantiert werden und keine andere Verbindung kann die belegte Ressource nutzen. Im Gegensatz dazu ist das Internet paketorientiert. Die zu übertragende Information wird in Paketen übertragen, wobei jedes Paket alle notwendige Information enthält, um es an die Zieladresse zu leiten. Das Internet Protokoll IPv4 liefert nur bestmöglichen Service (best-effort), das heißt daß ohne zusätzliche Mechanismen die Übertragungsdauer, der Übertragungsweg, ja selbst die korrekte Übertragung nicht garantiert werden kann: durch Stau in einzelnen Routern können Pakete aufgehalten oder gar verworfen werden. Der große Vorteil eines paketorientierten Netzwerkes ist, daß theoretisch unendlich viele Verbindungen gleichzeitig unterhalten werden können, dies ist der Vorteil des statistischen Multiplexen einer Übertragungsleitung. In Zeiten in denen viele Übertragungen und deren Übertragungsgarantien zu Engpässen führen, kann man das paketvermittelnde Netzwerk als knappe (congestible) Ressource betrachten, die damit also einen Preis besitzt. Engpässe auf Übertragungsleitungen wurden bisher dadurch gelöst, daß die Kapazität erhöht wurde (overprovisioning). Dies hat bisher gut funktioniert, doch mit der Einführung von IPv6 und dem Reservierungsprotokoll RSVP und der damit erreichten Einführung von garantierter Dienstgüte müssen über Preise die verschiedenen Güter differenziert werden. Eine höhere Dienstqualität muß in einem höheren Preis resultieren, garantierte Dienste müssen teuerer sein als best-effort Dienst.

2.1.2 Kosten des Internet

Eine wichtige Eigenschaft von Telekommunikationsnetzen ist, daß die Kosten für ihre Unterhaltung (operating costs) fast vollständig unabhängig sind von der Nutzung der Ressource [MMVa94d]. Der größte Teil der anfallenden Kosten, die Kosten für Übertragungsleitungen, für Router und die Netzwerkverwaltung, ist fix und die Kosten für das Versenden eines weiteren, zusätzlichen Pakets, die marginalen Kosten sind nahezu Null. Fixkosten sollten über eine feste Grundgebühr abgerechnet werden, eine Proportionalisierung dieser Kosten widerspräche deren Ursprung. MacKie-Mason und Varian [MMVa94b, MMVa94c] zeigen, daß aber soziale Kosten, sogenannte "congestion costs", signifikant sind. In Zeiten von Übertragungsengpässen müssen diese sozialen Kosten, die durch die Nutzung der Ressource anderen Anwendern dadurch entstehen, daß sie von der Nutzung abgehalten oder beeinträchtigt werden, in die Preisbestimmung mit einfließen. Das Problem einer gemeinsam genutzten Ressource wird in der Literatur als "classical problem of the commons" [Hard68] bezeichnet: solange die Nutzer unbegrenzten Zugang zu einer Ressource haben, wird diese nicht effizient genutzt, da die Nutzer nicht wirklich nach ihren Bedürfnissen die Ressource einsetzen (wenn es nichts kostet, nimmt man unabhängig von der Notwendigkeit immer das Meiste/Beste). Man muß also in die Preisberechnung die negativen externen Effekte (negative externalities), bei einem Netzwerk in Form von Wartezeiten, schlechter Dienstqualität oder Ausschluß von der Übertragung, einbeziehen. Dies gewährleistet, daß die Ressource jenen Anwendern verfügbar gemacht wird, die aus der Nutzung der Ressource den höchsten Nutzen erhalten und damit auch gewillt sind, mehr für deren Nutzung zu bezahlen. In diesem Zusammenhang müssen auch jegliche Arten von Übertragungsgarantien gesehen werden, die über Reservierung oder andere Mechanismen gegeben werden: jede Form von besserem Service muß einen höheren Preis haben als normaler Service, denn "mehr kostet mehr".

2.2 Preiskomponenten

Pricing Modelle im Internet können aus folgenden drei grundlegenden Elementen bestehen (siehe Abbildung 1, vgl. [FSPW98] S.4), wobei diese Preiskomponenten vollständig oder teilweise umgesetzt sein können:

- *feste monatliche Zugangsgebühr (flat-rate/access pricing)*; wird für die Bereitstellung eines Zugangs mit bestimmter Bandbreite und Konfiguration zum Netzwerk berechnet.
- *Verbindungsgebühr (connection pricing)*; wird pro Verbindung/Reservierung in verbindungsorientierten Netzen oder in verbindungslosen Netzen mit Reservierung abgerechnet.
- *nutzungsabhängige Gebühr (usage-based pricing)*; Gebühr auf Basis der Ressourcenbeanspruchung. Dies erfordert, daß die Parameter für die Berechnung der Gebühr gesammelt werden müssen (siehe Kapitel 2.4 Accounting). Ein in der Literatur sehr bekanntes Beispiel für nutzungsabhängige Abrechnung ist Neuseeland, wo eine teure Satellitenverbindung in die USA nutzungsabhängig abgerechnet wird [CaGu94].

Ein Problem, das sich bei einer nutzungsbasierten Abrechnung ergibt, ist, die Grundlage für das Pricing zu bestimmen (zeit-, volumen-, QoS-basiert): die für das Pricingmodell benötigten Inputparameter müssen im Netzwerk beobachtbar sein. Ein weiteres Problem ergibt sich durch die hohe Abhängigkeit des Pricingmodell von der zugrundeliegenden Technologie: Veränderungen der Technologie des Netzwerkes, die zu neuen Diensten führen, müssen sich auch im Pricingmodell wiederspiegeln. So muß bei einem Netzwerk, das Übertragungsgarantien geben kann, das Pricingmodell in der Lage sein, diese Garantien zu bewerten.

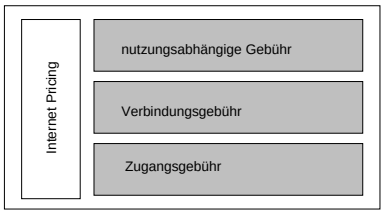

Abbildung 1: Komponenten des Internet Pricing

2.3 Gewünschte Eigenschaften und Ziele des Pricing

Ökonomische Modelle werden benötigt, um die Abhängigkeit zwischen Mechanismen, die den Preis für einen Dienst in einer bestimmten Situation berechnen, und Parametern, die technologisch im Netzwerk beobachtbar sind und diese Situation spezifizieren, zu bestimmen. Wie oben erwähnt müssen ökonomische Modelle für Pricing im Internet auf Netzwerkmodellen basieren, denn diese stellen die Dienste zur Verfügung, die diese Modelle bewerten sollen.

Als Eigenschaften, die von einem optimalen Pricingmodell erfüllt werden sollten, können folgende Punkte angeführt werden (wobei für manche Eigenschaften ein Tradeoff erforderlich ist):

- Die erzeugten Preise sollten zu einer optimalen Ressourcenallokation führen. Auch sollte die Ressource durch ein Pricingmodell gleichmäßiger genutzt werden (MacKie-Mason und Varian [MMVa94d] nennen als durchschnittliche Nutzung des Internets nur 5% der gesamten Übertragungskapazität; Kapazitätsengpässe treten vor allem zu Spitzenzeiten auf.).
- Preise müssen die aktuelle Knappheit der Ressource widerspiegeln. Ein höherer Preis gewährleistet, daß die Ressource jenen Anwendern uneingeschränkt zur Verfügung steht, die aus dem Service einen so großen Nutzen ziehen, daß sie gewillt sind, den entsprechenden Preis zu bezahlen.
- Das Pricingmodell sollte alle vom Netzwerk lieferbaren Dienste bewerten können, nicht nur die Dienstgüte in Bezug auf die Bandbreite, sondern auch in Bezug auf Garantien und anderen QoS Parametern. Die für das Pricing benötigten Parameter sollten vom Netzwerk her verfügbar sein.
- Pricing sollte die richtigen ökonomischen Anreize für den Ausbau des Netzwerkes liefern und das Wachstum des Netzwerkes fördern. Jene Teile des Netzwerkes, die besonders stark beansprucht werden, sollten mit den für sie erzielten höheren Einnahmen ausgebaut werden.

Zusätzlich zu diesen theoretischen Anforderungen muß auch die Umsetzung des Pricingmodells in der Praxis möglichst folgende Anforderungen erfüllen:

- Der durch das Pricingmodell erzeugte Protokoll- und Verarbeitungsoverhead sollte möglichst gering sein.
- Die Preisbestimmung sollte dezentral vorgenommen werden und so dem Netzwerkprovider erlauben, das für sein Netzwerk gültige Preismodell zu wählen. Dabei muß aber die Interoperabilität zwischen den Netzwerken gewährleistet bleiben.
- Bei Einführung von Pricingmodellen muß eine inkrementelle Implementierung möglich sein, da global betriebene Netzwerke nicht über Nacht geändert werden können.

- Bei der Abrechnung von Internetdiensten sollte die Aufteilung der Gebühr auf Sender und Empfänger möglich sein, auch die Frage der Abrechnung von Multicastverbindungen muß gelöst werden.

Diese Liste der gewünschten Eigenschaften ist in den Vorschlägen, die bis zum heutigen Zeitpunkt entwickelt wurden, nur teilweise umgesetzt worden, was sicherlich auch auf die Komplexität der Thematik zurückzuführen ist. Es gibt viele Gründe, warum die Nutzung des Internets noch nicht nach neuen, nutzungsbasierten Preismodellen abgerechnet wird. Ein Hauptproblem liegt sicherlich in der Aufgabe Ingenieurwissenschaften und Wirtschaftswissenschaften zusammenzubringen. Bei vielen rein ökonomischen Ansätzen wurde die Technologie und damit die Umsetzbarkeit des Vorschlags außer acht gelassen. Die mehr technisch orientierten Vorschläge lassen die ökonomischen Gesichtspunkte größtenteils außer acht. Was meist fehlt ist die integrierte Sichtweise des Problems. Weiterhin nennen Fankhauser, et al. [FaSP97, FSPW98] folgende Gründe:

- Man glaubte, daß durch den stetigen Ausbau der Übertragungsleistung der Netzwerke die Kapazität der Ressource irgendwann kein Problem mehr sein wird.
- Das Internet als ursprüngliches Forschungsnetz wurde durch staatliche Subventionen finanziert. Bei dessen Entwicklung wurde deshalb der Schwerpunkt nicht auf die ökonomischen Aspekte des Netzwerks gelegt.
- Man fürchtete die entstehenden Kosten und den Overhead einer Einführung von nutzenbasierter Abrechnung und die sich daraus ergebende Verringerung der Effizienz des Netzwerks.
- Das bisherige best-effort Internet unterstützte nur eine Dienstklasse aber keine garantierten Serviceklassen für bestimmte Dienstgüte. Dies war für die ursprünglichen Internetanwendungen, wie e-Mail, telnet, ftp, ausreichend, es fehlten Anwendungen, die Garantien bezüglich der Dienstgüte benötigen.
- Die schnelle technologische Entwicklung macht die Entwicklung von nutzungsbasierten Preismodelle schnellebig, da die Technologie des Netzwerks die Parameter und die Güter bestimmt, für die ein Preis festgesetzt werden muß.
- Eine nutzungsabhängige Abrechnung wurde durch fehlende elektronische Zahlungssysteme erschwert.

Seit einigen Jahren wird der Trend hin zu einem Integrated Services Internet immer deutlicher. Neue Anwendungen (Multimedia, Internettelefonie) mit ihren strikten Dienstgüteanforderungen und hohen Datenraten gewinnen immer mehr an Bedeutung. Die bisherigen in Bezug auf Bandbreite und Übertragungsgarantien sehr genügsamen Anwendungen treten bezüglich ihres Anteils an der gesamten Ressourceninanspruchnahme (siehe Kapitel 2.1 zum Thema Ressource) immer mehr in den Hintergrund. Trotz des rasanten Anstiegs der Bandbreitenkapazität der Links und der schnelleren Verarbeitungsleistung der Router bleibt die Übertragungskapazität ein Engpaß. Diese erwähnten Veränderungen des Internet und seiner Anwendungen begründen den Bedarf von nutzungsbasierten Tarifmodellen, um ein für den Nutzer geeignetes, stabiles Netzwerk zu gewährleisten. Das Problem mit dem bis heute vorherrschenden flat-rate Pricing ist, daß es keine ökonomische Ressourcenallokation erzeugt. Fortschritte in der Ressourcenreservierung (z.B. das RSVP Reservierungsprotokoll) verstärken noch den Bedarf an nutzungsabhängigen Pricingmodellen: es soll verhindert werden, daß der Anwender automatisch die höchste Dienstgüte reserviert, obwohl er sie nicht braucht. Die Möglichkeit

der Ressourcenreservierung ohne die Verwendung eines Preisanreizes macht keinen Sinn. Desweiteren können über nutzungsabhängiges Pricing die Möglichkeiten des Feedbacks, das der Anwender dem Netzwerkbetreiber geben kann, erhöht werden. Bisher kann der Anwender entscheiden, ob er den Dienst mit der gegebenen Dienstgüte nutzen will oder nicht. Zukünftig kann er über den Preis und die "verbrauchte Menge" abgelesen werden, was dem Anwender die Kommunikation mit einer bestimmten Dienstgüte wert ist.

2.4 Funktionale Komponenten eines Abrechnungssystems

Grundvoraussetzung für eine Abrechnung der Ressourcennutzung ist die Existenz eines Abrechnungssystems. Abbildung 2 (vgl. [FaSP98] S.1) zeigt die hierfür notwendigen Komponenten.

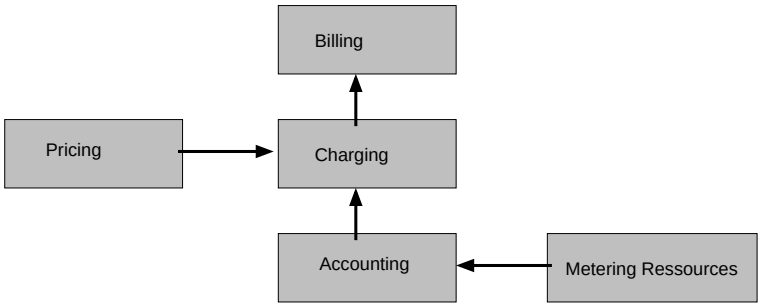

Abbildung 2: Funktionale Komponenten eines Abrechnungssystems

Accounting sammelt im Zeitablauf Informationen bezüglich der Ressourcennutzung (*metering ressources*) eines Anwenders, d.h. Accounting definiert eine Funktion, die den Grad der Ressourcennutzung in technische Größen (z.B. Dauer einer Reservierung, Länge eines benutzten Übertragungsweges, reservierte Bandbreite) überführt. Diese Größen werden in einem *Accounting Record* gesammelt, der die Grundlage für Charging und Billing bildet.

Charging ist der Prozeß der Berechnung der Kosten eines Accounting Records, d.h. Charging definiert eine Funktion, welche technische Größen in monetäre umwandelt. Diese Information wird in einem *Charging Record* gesammelt.

Pricing (siehe auch Kapitel 2) ist die Festlegung eines Preises für die Nutzung der Ressource, diese Funktion ist die fundamentale Determinante eines Abrechnungssystems.

Billing ist der Prozeß, der die gesammelte Charginginformation zu einer Rechnung für den Kunden zusammenstellt und den Gesamtpreis für den jeweiligen Abrechnungszeitraum berechnet.

Schließlich muß dafür gesorgt werden, daß die Rechnung bezahlt werden kann. Hierzu können traditionelle (Lastschrifteinzug, Überweisung) oder neue elektronische Abrechnungssysteme (Kreditkartenzahlung mit Secure Electronic Payments) verwendet werden. Zukünftig wird sicherlich der gesamte Prozeß der Abrechnung von Transportdiensten mit der Abrechnung anderer Serviceleistungen (wie z.B. Informationsdienste, Online-Bestellungen) integriert werden, um das Abrechnungssystem möglichst effizient zu gestalten. Der Verwaltungsoverhead für Billingsysteme beträgt im Falle der Telefontelekommunikation ungefähr 50% der Telefonrechnung [McBa98].

3 Ökonomische Ansätze zur Lösung

In der Literatur wurden verschiedene Modelle diskutiert, die sich sowohl in ihren ökonomischen und technischen Annahmen als auch in der Anwendungsnähe unterscheiden. Die Grundstruk-

tur der ökonomischen Ansätze ist ähnlich. Man versucht das Netzwerk, die Anwender und die vom Netzwerk gelieferten Dienste in einem Modell abzubilden, um einen Preismechanismus herzuleiten, der eine Optimalitätsbedingung erfüllt. Dies kann zum Beispiel die Maximierung des Gesamtnutzens aller Anwender sein oder auch die Minimierung der Wartezeit für den Zugang zum Netz. Hierzu müssen Annahmen über das Verhalten und die Nutzenfunktion der Anwender sowie über die Art der Ressource und der von ihr angebotenen Dienste getroffen werden. Diese Annahmen sind die grundlegenden Determinanten, die die Unterschiede der einzelnen Modelle und auch ihre Realitätsnähe bestimmen.

Im folgenden soll nun das Smart Market Modell von MacKie-Mason und Varian, das Markt Modell von Fulp et al. und ein Basispreis Modell von Fankhauser et al. näher vorgestellt werden.

3.1 Smart Market Modell (MacKie-Mason und Varian, 1994)

MacKie-Mason und Varian [MMVa94c] betrachten in ihrem Smart Market Modell die Kosten, die Anwender durch die kostenlose Nutzung der gemeinsamen Ressource bei anderen Anwendern verursachen. Dies ist ein gutes Modell, um Einblick in die Struktur des Problems des Pricing von Netzwerkressourcen zu bekommen. Normalerweise kann eine gemeinsame Ressource durch die Etablierung von sozialen Normen und der damit einhergehenden Bestrafung von unsozialem Verhalten gerecht unter den Nutzern aufgeteilt werden. Dieser Ansatz funktioniert aber nur in kleinen Gruppen, nicht in einem weltweiten Informationsnetz mit anonymen Anwendern. MacKie-Mason schlägt zur Lösung dieses Problems einen Preismechanismus vor. Als wesentlichen Vorteil von Preismechanismen sehen sie die Möglichkeit, Einnahmen zu erzielen, die einerseits die Kosten decken und andererseits Überschüsse erwirtschaften, um die Kapazitäten bedarfsgerecht auszubauen. “In einem Smart Market geben die Nutzer nur den maximalen Betrag an, den sie gewillt sind, für den Netzwerkzugang zu zahlen. [...] Der Router wertet das Gebot, das in jedem Paket übertragen wird, aus und läßt alle Pakete zu, die ein Gebot größer einem bestimmten Cutoff Wert haben.” [MMVa94c] Meist ist das Netzwerk nicht überlastet, in dieser Zeit wird dem Anwender keine Nutzungsgebühr berechnet. Wenn aber das Netzwerk überlastet ist, werden Pakete verzögert oder gar verworfen. Die Warteschlange im Router soll jetzt nicht mehr nach dem FIFO Prinzip, sondern nach der Höhe der Gebote abgebaut werden. Die Anwender bezahlen nicht die Höhe ihres Gebotes, sondern die Höhe des Gebots, das gerade nicht mehr berücksichtigt werden konnte. D.h. der Nutzer bezahlt die Kosten, die er jenem Nutzer verursacht, der gerade nicht mehr berücksichtigt werden konnte. Die Verfasser bezeichnen dies als “internalizing the externalities”. Die Nutzer, deren Pakete übertragen wurden, erhalten als “Gewinn” die Differenz aus ihrem Nutzen und den von ihnen verursachten und zu zahlenden sozialen Kosten. Diese Art einer Auktion (Vickrey Auktion genannt) hat einige interessante Eigenschaften (siehe [MMVa94b]): sie bewirkt, daß Anwender ihre wahren Präferenzen bekannt geben müssen, da dies die optimale Strategie ist, das heißt mogeln bringt keinen Vorteil. Dies sei an folgendem Beispiel erläutert: man nehme an, es gäbe eine Einheit eines Gutes und zwei Verbraucher $i = 1, 2$, die jeweils ein Gebot b_i für das Gut abgeben. Das Ziel, Effizienz zu erreichen, fordert, daß jener Verbraucher mit dem höchsten wahren Nutzen v_i das Gut erhält. Der erwartete Payoff von Verbraucher 1 ist das Produkt aus der Wahrscheinlichkeit, daß er die Auktion gewinnt und der dann daraus resultierenden Auszahlung:

$$Pr(b_1 > b_2) * [v_1 - b_2] \tag{1}$$

Angenommen Verbraucher 1 sagt die Wahrheit, das heißt $b_1 = v_1$: dann erhält Verbraucher 1 immer dann das Gut, wenn sein Payoff positiv ist, d.h. $v_1 - b_2 > 0$, und niemals wenn er negativ ist. Dies ist klar eine dominante Strategie und da beide Verbraucher diese Strategie

verfolgen, geht das Gut immer an denjenigen, der den höchsten wahren Nutzen hat. Daraus folgt, daß jene Anwender, die die höchsten Verzögerungskosten hätten, zuerst bedient werden. Man kann zeigen, daß die resultierende Ressourcenallokation paretooptimal ist, der soziale Nettowohlstand wird maximiert. Falls der Wert der nicht zur Übertragung zugelassenen Pakete die Kosten für die Erweiterung der Kapazität übersteigt, ist es sinnvoll die Kapazität des Netzwerks auszubauen.

Die theoretisch attraktive Idee an jedem Knoten Auktionen für individuelle Pakete mit Geboten durchzuführen, führt aber in der Praxis zu einem inakzeptablen Verarbeitungsoverhead und zu Verzögerungen. Gerade zu Überlastzeiten werden die Router mit zusätzlichem Rechenaufwand für die Durchführung der Auktionen belastet. Auch lassen die Autoren offen wie oft die Auktionen durchgeführt werden. Dabei muß beachtet werden, daß das Sammeln von Geboten für die nächste Auktion die Verzögerung der Übertragung erhöht. Gupta et al. [GJPS+97] vertreten gar die These, daß sowohl die stochastische Umgebung als auch die technologischen Eigenschaften von Internetverkehr dazu führen, daß Auktionsmechanismen im allgemeinen ungeeignet für öffentliche Netzwerke sind.

Das bisher vorgestellte Preismodell ist in dieser Form nur für best-effort Netze ohne QoS und Übertragungsgarantien anwendbar. In einem weiteren Artikel haben MacKie Mason und Varian [MacK97] versucht das Smart Market Modell auf Netzwerke mit QoS zu verallgemeinern. Das Ergebnis ist aber ein sehr komplexes Modell, das in seiner Form, das geben auch die Verfasser zu, nicht implementierbar ist.

3.2 Markt Modell (Fulp et al., 1997)

Fulp et al. [FORR98] schlagen ein Markt Modell für das Netzwerk vor . Das Netzwerkmodell besteht aus einer beschränkten Ressource (der Bandbreite), Verbrauchern und Produzenten. Eine *Ressource* ist ein Gut (oder ein Dienst), das für die Marktteilnehmer in der Wirtschaft einen Wert hat. Da das Gut knapp ist, gibt es nie genug um alle zufriedenzustellen. Deshalb müssen Allokationsentscheidungen getroffen werden. *Verbraucher* streben nach Ressourcen, um ihre Bedürfnisse zu befriedigen. *Produzenten* erzeugen oder besitzen die gewünschten Ressourcen. Sie treffen sich am Markt, wo sie Ressourcen kaufen oder verkaufen. Normalerweise wird diese Börse nicht über Tausch realisiert sondern über das Medium Geld und der Wechselkurs einer Ressource ist deren Preis. Preise ergeben sich aus dem Zusammenspiel von Angebot und Nachfrage, der Preis steigt, falls die Nachfrage größer als das Angebot ist. Falls Angebot gleich Nachfrage ist der Markt im Gleichgewicht, der Preis ist der Gleichgewichtspreis. Die resultierende Allokation der Ressource ist dann paretooptimal.

Es existieren 3 Komponenten im Netzwerkmodell: User (jene die Netzwerkanwendungen ausführen), Netzwerk Broker und Switches. Das heißt *User* entsprechen den Verbrauchern, *Switches* den Produzenten und *Netzwerk Broker* sind die Intermediäre, die den Austausch von Ressourcen im Markt erleichtern. Um das Modell zu vereinfachen betrachten Fulp et al. als Ressource nur die Bandbreite einer Übertragungsleitung (eines Links).

3.2.1 Switch

Das Netzwerk besteht aus mehreren Switches, die über Übertragungsleitungen (Links) miteinander verbunden sind (siehe Abbildung 3, vgl. [MMVa94a] S.10)). Für einen Link wird der sendende Switch als Eigner der Bandbreite des Links angesehen. Jeder Switch bestimmt lokal für jeden Output Port den Preis für die Bandbreite abhängig von Angebot und Nachfrage für diesen Link.

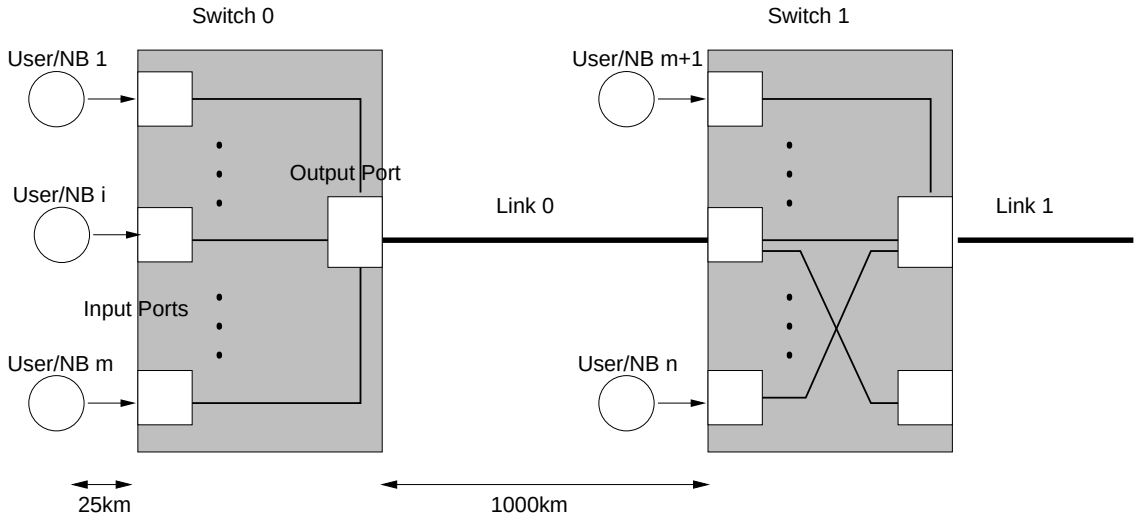

Abbildung 3: Netzwerkaufbau

Das gesamte Netzwerk kann als Wirtschaft mit mehreren Märkten (ein Markt pro Link) betrachtet werden, die unabhängig voneinander funktionieren. Das heißt es ergibt sich eine dezentralisierte Wirtschaft, in der der Ausfall eines Marktes (Links) nicht zum Ausfall des gesamten Pricingmodells führt.

Die Preisberechnung am Switch wird zu diskreten Zeitintervallen durchgeführt. Am Ende des Preisintervalls ${P_n}^i$ berechnet der Switch den neuen Preis ${p_{n+1}}^i$ [DM/Sek] für Link i mittels folgender Gleichung:

$$ {p_{n+1}}^i = {p_n}^i + c \cdot \left(\frac{{d_n}^i - \alpha \cdot S^i}{\alpha \cdot S^i} \right) \tag{2} $$

Der neue Preis ${p_{n+1}}^i$ wird für das neue Zeitintervall ${P_{n+1}}^i$ konstant gehalten. Diese Form einer Preisgleichung wird als Tâtonnement Prozeß [Walr54] bezeichnet, der neue Preis ist gleich dem alten plus einer Korrekturfunktion. Die Korrekturfunktion erzeugt ein Feedback basierend auf der Nachfrage ${d_n}^i$ (erhaltener Verkehr) und dem konstantem Angebot $\alpha \cdot S^i$ (verfügbare Bandbreite). α bewirkt, daß der Preis steigt, sobald α Prozent der maximalen Bandbreite erreicht sind. Aus der Konstruktion der Korrekturfunktion erkennt man, daß der Preis sinkt (steigt), wenn die Nachfrage abnimmt (steigt). Der Gleichgewichtspreis ${p_*}^i$ an Link i ist erreicht, wenn das Angebot gleich der Nachfrage ist, dann ist der Markt geräumt und die Allokation ist paretooptimal. Die Konstante c verstärkt das Feedbacksignal, ihre Größe steuert, wie schnell der Preis sich anpaßt. Nachdem der neue Preis ${p_{n+1}}^i$ berechnet wurde, wird die neue Preisquotierung ${q_{n+1}}^i$ allen Netzwerk Brokern gemeldet, die diesen Link benutzen. Die Preisquotierung besteht aus ${p_{n+1}}^i$, ${d_n}^i$, S^i, c und α. Der Netzwerk Broker verwendet alle diese Informationen, um die zu kaufende Bandbreite zu bestimmen.

3.2.2 User

Ein User, der Netzwerkanwendungen ausführen will, benötigt dafür Übertragungsbandbreite. Die Anwendung habe variable Bandbreitenanforderungen, die zu bestimmten Zeitpunkten angepaßt werden. b_m sei die im Zeitablauf m-te Bandbreitenanforderung. Abhängig vom Preis für die Bandbreite und vom Wohlstand kann sich ein User einen bestimmte Bandbreite leisten. Eine Nutzenfunktion $U(x)$ bildet die Ressourcenhöhe auf eine reelle Zahl ab, die dem Grad der Bedürfnisbefriedigung entspricht: eine Ressourcenhöhe wird einer anderen bevorzugt, $x \succ y$,

falls $U(x) > U(y)$. Fulp et al. verwenden als Nutzenfunktionen QoS Profile. Abbildung 4 (vgl. [MMVa94a] S.9) zeigt beispielhaft ein solches QoS Profil.

Abbildung 4: QoS Profil

Die horizontale Achse mißt das Verhältnis aus allokierter zu gewünschter Bandbreite b_m, die vertikale Achse die Zufriedenheit auf einer Skala von 0 (gering) bis 5 (hoch). Im Schaubild ist eine stückweise lineare Funktion gezeigt, wobei die Steigung den zusätzlichen Nutzen bei Erhöhung des Verhältnisses aus zugeteilter und gewünschter Bandbreite um eine Einheit wiedergibt. Der User wird kontinuierlich für die Dauer einer Verbindung abgerechnet. Um für diese Kosten aufzukommen wird angenommen, daß der User eine konstante Budgetrate W [DM/Sek] zur Verfügung hat.

3.2.3 Network Broker

Die User können das Netzwerk nur über einen Netzwerk Broker benutzen. Dieser fungiert als Intermediär für den User und nimmt folgende Aufgaben wahr: (a) Der Netzwerk Broker steuert den Netzwerkzugang, indem er sicherstellt, daß alle User genügend Wohlstand haben, um sich eine "angemessene" QoS leisten zu können. Fulp et al. begründen dies damit, daß der soziale Wohlstand in einem Netzwerk mit wenigen Usern, die sich "gute" QoS leisten können, besser ist als in einem Netzwerk mit vielen Usern, die sich nur "mäßige" QoS leisten können. Dies ist eine sicher nicht unumstrittene Annahme. (b) Außerdem überwacht der Netzwerk Broker die User und die Preise, indem er Informationen über diese sammelt und speichert. Für jeden User sind dies das QoS Profil, b_m, W und die Übertragungsroute R von der Quelle zum Ziel. R besteht aus den Links $\{l^i, i = 1, \ldots, v\}$, wobei $\vec{q} = \{q^i, i = 1, \ldots, v\}$ den Vektor der aktuellen Preise auf diesen Links darstellt. Der Netzwerk Broker teilt die Budgetrate W in einen Vektor $\vec{w}$ von v Budgetraten auf, mit $\vec{w} = \{w^i, i = 1, \ldots, v\}$. Fulp et al. nehmen diese Aufteilung, die bestimmt, welcher Anteil des Gesamtbudgets für einen Link aufgewendet wird, als gegeben an. Mit diesen Informationen rechnet der Netzwerk Broker die Ressourcennutzung des Users ab. (c) Schließlich bestimmt der Netzwerk Broker die zu kaufende Bandbreite. Dieser Wert wird auf Grundlage von Budgetrate, Preis und QoS Profil des Users bestimmt.

3.2.4 Bestimmung der zu kaufenden Bandbreite

Sei u_r die r-te im Zeitablauf zu kaufende Menge von Bandbreite. Zur Bestimmung der nächsten Menge zu kaufender Bandbreite berechnet der Netzwerk Broker die maximale und minimale Bandbreite, die gekauft werden kann bzw. muß. Die maximale Bandbreite $\hat{b}_{max}$ ergibt sich aus

$$b_{max}{}^i = \frac{w_i}{p_i}, i = 1, \ldots, v \tag{3}$$

$$\hat{b}_{max} = \min_{i=1,\ldots,v} \{{b_{max}}^i\} \tag{4}$$

Die minimale Bandbreite b_{min} ergibt sich aus dem QoS Profil und dem sich daraus ergebenden niedrigsten QoS Score, der für den User gerade noch akzeptabel ist. Falls $\hat{b}_{max} < b_{min}$ muß der User entweder die geringere QoS akzepieren, seine Budgetrate erhöhen oder die Verbindung abbrechen. Das folgende Vorgehen bestimmt nun die maximale mögliche Bandbreite abhängig von den aktuellen Preisen und Budgets.

$$u_{r+1} = \begin{cases} b_m & , \text{ falls } \hat{b}_{max} \geq b_m \\ \hat{b}_{max} & , \text{ falls } \hat{b}_{max} < b_m \text{ und } \hat{b}_{max} \leq b_m \\ 0 & , \text{ sonst } (b_{min} \text{ konnte nicht gekauft werden}) \end{cases} \tag{5}$$

Der Netzwerk Broker muß jetzt noch bestimmen, ob u_{r+1} eine Preisänderung verursacht, die sich der User nicht leisten kann. Der höchste Preis den der User an Link i sich leisten kann ist

$$\frac{w^i}{u_{r+1}} \tag{6}$$

Der neue von u_{r+1} verursachte Preis an Link i ist

$$p^i + c \cdot \left(\frac{u_{r+1} + {d_n}^i - \alpha \cdot S^i}{\alpha \cdot S^i} \right) \tag{7}$$

Dieser neue Preis darf nicht den maximalen Preis, den sich der User leisten kann (siehe Gleichung 6) übersteigen. Die folgende Ungleichung gibt eine Grenze für zulässige Werte von u an:

$$w^i \stackrel{!}{\geq} u_{r+1} \cdot \left[p^i + c \cdot \left(\frac{u_{r+1} + {d_n}^i - \alpha \cdot S^i}{\alpha \cdot S^i} \right) \right] \tag{8}$$

Indem man diese Gleichung nach u_{r+1} auflöst, erhält man die Bandbreite an Link i die der User sich leisten kann. Sobald u_{r+1} bestimmt wurde, startet der Netzwerk Broker sofort mit der Übertragung in Höhe dieser Rate.

Es kann gezeigt werden, daß dieses Vorgehen eine paretooptimale Lösung erzeugt und Preisstabilität gewährleistet ist. Fulp et al. untersuchen ihren Vorschlag in einer Simulation. Das Netzwerk bestand dabei aus 55 Usern/Netzwerk Brokern, 3 Switches und 3 Links. Über jeden Output Port liefen Verbindungen von 30 Usern. Die Übertragungsstrecken der User hatten eine Länge von 1 bis 3 Hops, die User benutzten das Netzwerk zu zufälligen Zeiten (normalverteilt). Das Preismodell wurde mit den Werten $\alpha = 90\%$ und $c = 50$ initialisiert. Es zeigte sich daß dieses Modell erfolgreich die Linkbandbreite preisen kann. Der Nutzungsgrad der Ressource betrug über 90%, der durchschnittliche QoS Score betrug 98% des optimalen Wertes und die Verteilung der Link Bandbreite war zu 92% optimal, gemessen in einem von Fulp et al. definierten Fairnessindex. Auch ergab sich, daß die Preismethode einem Netzwerk ohne Preise überlegen war.

Trotz dieser scheinbar ausnahmslos positiven Ergebnisse ist aber auch Kritik angebracht: wie schon beim Smart Market Modell sind keine Übertragungsgarantien und keine anderen Parameter außer der Bandbreite im Modell integriert. Desweiteren wurde die eigentliche Hauptaufgabe der Netzwerk Broker, nämlich das zu Verfügung stehende Budget für eine unter Kostengesichtspunkten optimale Übertragungsstrecke zu verwenden, nicht gelöst und als

gegeben angenommen. Auch macht die Verwendung von QoS Profilen im Falle von nur einem Parameter (der Bandbreite) wenig Sinn. Es ist klar, daß der User möglichst viel Bandbreite für möglichst wenig Geld erhalten will. Wie die Nutzenfunktion genau aussieht, ist für die Bestimmung des Preises in diesem Modell nicht relevant. Dies würde sich ändern, wenn Entscheidungen getroffen werden müßten, bezüglich verschiedener Kombinationen von Dienstgüteparametern (z.B.: Ist eine Bandbreite von 1 Mbit/Sek und eine Verzögerung von 1 ms gleichwertig zu einer Bandbreite von 2 Mbit/Sek und einer Verzögerung von 2 ms?).

3.3 Probleme mit ökonomischen Modellen

Die meisten in der Literatur behandelten Vorschläge geben gute Denkansätze zum Pricing des Internets. Meist jedoch sind die Modelle zu abstrakt formuliert und aus verschiedenen Gründen weit von einer umsetzbaren Implementierung entfernt: die Annahmen sind unrealistisch, die Vorschläge sind nicht ohne weiteres skalierbar, die benötigten Daten sind gar nicht oder nur näherungsweise vom Netzwerk zu erhalten, oder der erzeugte Overhead ist zu groß. Ein weiteres Problem besteht darin, daß ein ökonomisches Modell, soll es umsetzbar sein, auf einem Netzwerkmodell basieren muß, das die Gegebenheit in der "Ökonomie" widerspiegelt. So ist es häufig so, daß frühe Modelle heute nicht mehr anwendbar sind und oft auch nicht erweitert werden können, da sie z.B. Möglichkeiten der Reservierung oder differenzierter QoS Garantien nicht abbilden können.

4 Experimentelle Pricing Umgebung

Egal wie gut ein ökonomisches Modell theoretisch begründet werden kann, seine wirkliche Güte zeigt sich erst nach der Implementierung unter realen Bedingungen. Erst dann läßt sich die Plausibilität der gemachten Annahmen und die Umsetzbarkeit des Ansatzes überprüfen. Fankhauser, et al. haben sich in vier Artikeln [FaSP97, FSVP98, FaSP98, FSPW98] mit diesem Problem befaßt. Ausgangspunkt ist die Überlegung, daß ökonomische Modelle in der Theorie nicht praxisnah verifiziert werden können, da das Verhalten der Internetuser, das durch ihre Präferenzen und Nutzenfunktionen bestimmt wird, nicht bekannt ist. Fankhauser et al. schlagen ein auf dem Ressourcenreservierungsprotokoll RSVP basierendes Charging- und Accountingprotokoll für reservierte Ressourcen vor. Für dieses wird untersucht, wie sich verschiedene Preismodelle auf die Leistungsfähigkeit auswirken.

4.1 Einführung in flowbasierte Abrechnung

RSVP nimmt Reservierungen für Flows vor. Als Flow wird eine Menge von Datenpaketen bezeichnet, die dieselbe Zieladresse haben und für die bestimmte QoS Garantien festlegt und garantiert werden sollen. Alle zu einem Flow gehörigen Pakete sind durch ein Flowlabel im IPv6 Header identifiziert und legen denselben Weg durchs Netz zurück. Eine RSVP Reservierungsanfrage enthält einen "flow descriptor", der sich aus der "flowspec" und der "filterspec" zusammensetzt. Die "flowspec" spezifiziert die für den Flow gewünschte Dienstgüte. Die "filterspec", zusammen mit der RSVP Session Spezifikation, definiert die Menge der Datenpakete (den Flow), die die in der "flowspec" definierte Dienstgüte erhalten soll. Die Verwendung von reservierten Ressourcen für das Pricing hat den Vorteil, daß das Problem der Quantität von Accountingdaten drastisch reduziert werden kann, da eine Reservierung über längere Zeit konstant gehalten wird. Im Gegensatz dazu müßte bei einer paketbasierten Abrechnung jedes einzelne Paket für die Abrechnung des Dienstes herangezogen werden. Als weiteren Grund für diese Vorgehensweise nennen Fankhauser et al., daß genau jene Verbindungen abgerechnet

werden, die feste Garantien benötigen und die damit einen signifikanten Anteil der Ressourcen exklusiv belegen. Ein Nachteil ist, daß dieser Ansatz nicht für die Abrechnung von best-effort Verbindungen verwendet werden kann, da er allein auf der Abrechnung von reservierter Kommunikation basiert.

4.2 Erweiterung des RSVP Protokolls

Das Ressourcenreservierungsprotokoll RSVP wird als Grundlage für die Übertragung von Charging- und Accountinginformation verwendet. Abbildung 5 (vgl. [FSVP98] S.1) zeigt den Aufbau von Hosts und Routern.

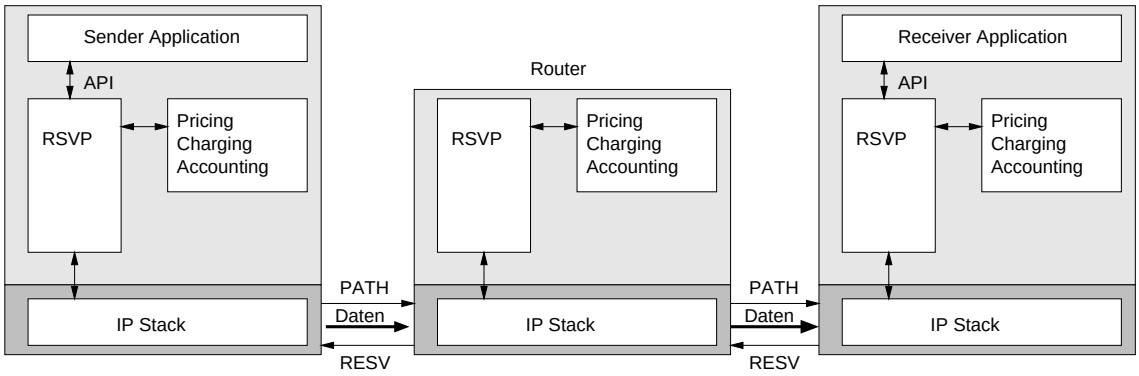

Abbildung 5: RSVP als Basis für die Übertragung von Charging- und Accounting Information

Das RSVP API (Application Programming Interface) muß um folgende grundlegenden Chargingfunktionen erweitert werden:

- Preisanfragen und -mitteilungen müssen möglich sein, um den Anwender über die aktuelle Marktsituation zu informieren.
- Der Anwender muß spezifizieren können, was er gewillt ist, für eine Reservierung zu zahlen (willingness to pay). Im folgenden wird von einem kreditbasierten Ansatz ausgegangen, das heißt der spezifizierte Wert wird auch als Zahlungsversprechen interpretiert.

Die Funktionalität der Router muß um folgende Punkte erweitert werden:

- Der aktuelle Marktpreis muß auf Anfrage quotiert werden können. Dabei muß gewährleistet sein, daß alle Preise in einheitlicher Währung angegeben sind, oder falls nicht, Umrechnungstabellen verfügbar sind. Dies stellt sicher, daß für die Quotierung des Marktpreises einer Verbindung der lokale Preis an jedem Router ohne Probleme aufsummiert werden kann (siehe Abbildung 7).
- Bei einer Reservierungsanfrage muß das willingness-to-pay Feld ausgewertet werden, um zu entscheiden, ob ein Flow zugelassen werden kann oder nicht. Für einen auktionsbasierten Ansatz muß zusätzlich noch das Gebot für die Auktion übertragen werden, das als Prozentsatz des aktuellen Marktpreises spezifiziert wird und dessen Höhe als Wahrscheinlichkeit interpretiert werden kann, mit der die Auktion gewonnen werden kann. Wie man sieht, muß jedes Pricing Modell spezifisch umgesetzt werden, um seinen Anforderungen gerecht zu werden.
- Falls die Reservierung erfolgreich ist, wird das Accounting und Charging durchgeführt. Abhängig vom Pricingmodell wird sofort ein neuer Marktpreis bestimmt, um dessen Betrag das willingness to pay Feld verringert wird.

Die folgenden RSVP Messages werden mit chargingrelevanter Information modifiziert, wobei die Bedeutung einzelner Felder auch vom verwendeten Pricingmodell abhängt:

- PATH

  wird zum Aufbau eines Pfades vom Sender zum Empfänger verwendet, damit die RESV Messages des Empfängers dieselbe Route zurück zum Sender nehmen, und kann eine Anfrage zur Quotierung eines Marktpreises (QRQ) oder eine vom Sender bereitgestellte Zahlung (S_PAY) enthalten.

- RESV

  die Information der PATH Message wird vom Empfänger an den Sender in einer RESV Message zurückgeschickt; sie enthält zusätzlich Quote Messages (QTE) zur Mitteilung des aktuellen Verbindungspreises oder Informationen über Zahlungen des Empfängers (R_PAY).

- RESVCONF (optional)

  kann zum Empfänger zurückgesendet werden, um eine Reservierung zu bestätigen, oder auch um dem Empfänger das Ergebnis einer Preisquotierung mitzuteilen.

- PATHTEAR und RESVTEAR

  werden zum sofortigen Abbau von Reservierungen benutzt, um Fehler wie z.B. nicht ausreichend verfügbare Ressourcen oder nicht ausreichende Zahlungen anzuzeigen; diese Messages werden nicht modifiziert.

Wie in Abbildung 6 dargestellt, haben alle Messages dieselbe PDU (Protocol Data Unit) Struktur, wobei die RSVP PDU Struktur um zusätzliche Felder ergänzt wurde (vgl. [FSVP98] S.4):

Abbildung 6: PDU Struktur (unterlegte Felder wurden der RSVP PDU hinzugefügt)

Im Feld "msg type" wird die Art der Message spezifiziert (PATH, RESV, ...), im Feld "c&a flags" werden die für die jeweilige Message möglichen Optionen angegeben (QRQ, QTE, S_PAY, R_PAY). Übliche Operationen beinhalten Marktpreis- und Reservierungsanfragen, die durch Anwendungen mittels eines erweiterten Reservierungsprotokoll API initiiert werden.

Wie oben erwähnt, werden PATH Messages dazu benutzt, einen Pfad aufzubauen, über den dann die RESV Nachricht zurück übertragen wird. PATH Messages können eine Anfrage bezüglich des Marktpreises oder eine Sender Zahlung enthalten. Diese Information wird vom Empfänger ausgewertet, dieser reagiert in einer RESV Message mit Zahlungsinformation und Geboten. Dieses Round-Trip-Messaging ermöglicht, daß entweder Sender oder Empfänger für die Reservierung bezahlen.

Den Ablauf zur Quotierung des Marktpreises zeigt Abbildung 7. Ein QRQ/QTE-Roundtrip wird dabei in einem regulären PATH/RESV-Roundtrip durchgeführt. Dabei wird an jedem

Router zum Preisfeld, das anfangs zu Null gesetzt wurde, der an diesem Router gültige aktuelle Marktpreis für die geforderte QoS addiert. Schließlich erhält der Sender die Preisquotierung für die reservierte Verbindung zum Empfänger. Diese kann in einer RESVCONF Message an den Empfänger übermittelt werden.

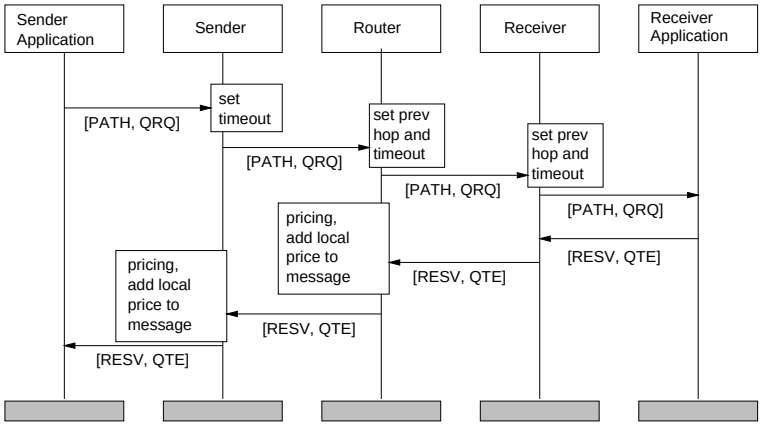

Abbildung 7: Message Sequence Chart (MSC) für die Quotierung des Marktpreises

In Abbildung 8 wird der Ablauf eines normalen PATH/RESV-Roundtrip mit Zahlungsaushandlung zwischen Sender und Empfänger und auktionsbasiertem Pricing dargestellt. Man sieht, daß die Reservierung mittels der RSVP Message jeweils lokal für jeden Link abgerechnet wird, das heißt der Geldbetrag wird bei jedem Router, um den dort gültigen Marktpreis verringert.

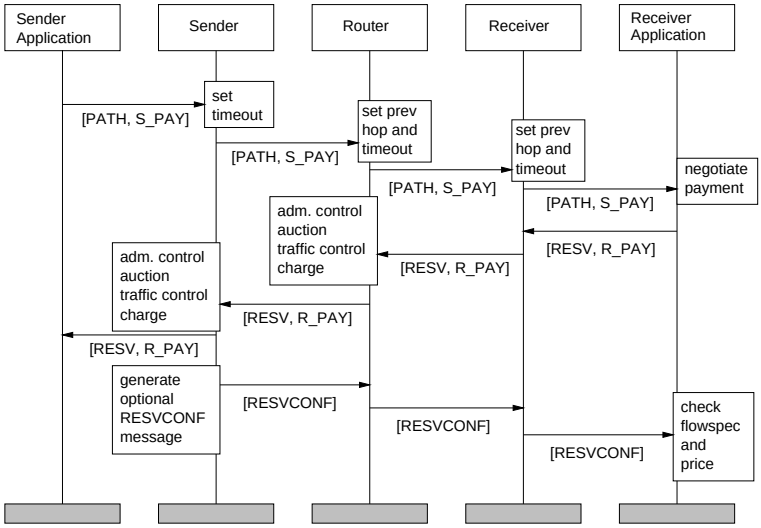

Abbildung 8: MSC für bezahlte Reservierung

Die Integration von Reservierungs- und Chargingprotokoll hat die folgenden positiven Eigenschaften:

- die Reservierung kann auf Grundlage der "flowspec" zum jeweiligen aktuellen Marktpreis am Router abgerechnet werden. Da RSVP die in der "flowspec" spezifizierte Dienstgüte garantiert, muß die aktuelle Ressourcennutzung nicht gemessen werden.
- durch Piggybacking von Charging – in Reservierungsmessages wird der Protokolloverhead reduziert.

- die Feinheit des Chargingprozesses kann durch die Häufigkeit der Auffrischung der Reservierung beeinflußt werden.
- RSVP Messages werden in jedem Router hop-by-hop verarbeitet. Dies ermöglicht es jedem Provider, die Nutzung seines Netzwerkes getrennt abzurechnen. Damit sind lokale Pricingmodelle möglich und die bisher üblichen Interproviderverträge werden größtenteils nicht mehr benötigt.

4.3 Ein Basispreis Modell

Fankhauser et al. [FaSP97] schlagen ein neues Basispreis Modell vor, das auf Dienstklassen basiert. Die Verfasser betrachten vier Dienstklassen: deterministisch garantierter Dienst, statistisch garantierter Dienst und best-effort Dienste mit hoher und niedriger Priorität. Das Modell ist ein eher pragmatischer Ansatz, der nicht versucht, eine theoretisch begründete Preisgleichung herzuleiten. Der Preis für den Transportdienst hängt vom Preis für die Anwendung und im Falle der Netzwerküberlast von einem zeitvariablen Verkehrsfaktor ab. Der Grundpreis für eine Anwendung A ergibt sich aus dem Produkt aus Basispreis und Datenvolumen:

$$Preis_A = Basispreis_{SC} * Durchsatz_A * Verbindungsdauer_A \tag{9}$$

wobei $Basispreis_{SC}$ [DM/Bit] der Basispreis für eine bestimmte Serviceklasse SC ist. Die Basispreise sollen vom Netzwerkprovider auf Grundlage von Geschäfts- und strategischen Marktentscheidungen, auch tageszeitabhängig, festgelegt werden. Der endgültige Preis einer Anwendung A zum Zeitpunkt t ergibt sich wie folgt:

$$Preis_{A,t} = Verkehrsfaktor_{SC(A),t} * Preis_A \tag{10}$$

Der Verkehrsfaktor ist eine Funktion der Differenz $\Delta Bandbreite_{SC}$ zwischen dem aktuellen Durchsatz in einer Serviceklasse und der dieser Serviceklasse allokierten Bandbreite zur Zeit t.

$$Verkehrsfaktor_{SC} = \begin{cases} Straffunktion(\Delta Bandbreite_{SC}) & \text{, falls } \Delta Bandbreite_{SC} > 0 \\ 1 & \text{, falls } \Delta Bandbreite_{SC} \leq 0 \end{cases} \tag{11}$$

Als Straffunktion kann zum Beispiel die Funktion $(x+1)^2$ verwendet werden. Da die Allokation der Bandbreite mit den deterministisch garantierten Serviceklassen startet und mit Serviceklassen niedriger Priorität endet, ist es möglich, daß der aktuelle Durchsatz in einer bestimmten Serviceklasse von der anfänglich zu dieser Serviceklasse allokierten Bandbreite abweicht und sich die Differenz $\Delta Bandbreite_{SC}$ ergibt.

$$\Delta Bandbreite_{SC} = aktueller\ Durchsatz_{SC} - allokierte\ Bandbreite_{SC} \tag{12}$$

Um das Netzwerk vor Überlast zu schützen, tritt bei $\Delta Bandbreite_{SC} > 0$ die Straffunktion in Kraft, welche eine Erhöhung des Verkehrsfaktors bewirkt, also den Dienst verteuert.

Die zu einer Serviceklasse allokierte Bandbreite ergibt sich aus einem für alle Serviceklassen gleichen Anteil der angeforderten Bandbreite. Der "Offset" Wert bestimmt den Punkt auf der Skala der Bandbreite, ab dem die Straffunktion angewendet werden soll.

$$allokierte\ Bandbreite_{SC} =$$

$$angeforderte\ Bandbreite_{SC} * \frac{gesamte\ verfügbare\ Bandbreite - Offset}{gesamte\ Nachfrage} \quad (13)$$

Dieses Preismodell ist vom Konzept her einleuchtend und verwendet als preisrelevante Parameter die Bandbreite und die Serviceklasse. Fankhauser et al. verwenden diesen Ansatz zur Überprüfung der Performanceauswirkungen des von ihnen vorgeschlagenen Charging- und Accountingprotokolls.

4.4 Ergebnisse

Fankhauser et al. haben den durch den Chargingmechanismus verursachten Overhead in einer Testumgebung aus Crossbow Routern und Hosts untersucht (der genaue Aufbau des verwendeten Netzwerks wurde in ihren Papers nicht spezifiziert). Der Overhead wurde bezüglich der zusätzlich benötigten Bandbreite, der Verzögerung und des Speicherplatzbedarfs im Router untersucht.

In einem ersten Szenario wurden für IP Telefonstreams mit sehr kurzen Reservierungsperioden (5 Sek.) und einer konstanten Bitrate von 64 kbit/s die Auswirkungen untersucht. Wie Tabelle 1 zeigt, beträgt der chargingrelevante Anteil am Speicherplatzbedarf im RSVP Dämon 28% der gesamten Flowstate Information (vgl. [FSVP98] S.6).

	[Byte]	[%]
Flow State	120	62
Timer Einträge	20	10
Pricing Einträge	14	7
Account	12	6
Authentifizierungsdaten	28	15
Gesamt	194	100

Tabelle 1: Speicherplatzbedarf für einen Flow im Router

Der bezüglich der Bandbreite erzeugte Overhead ist nach Einschätzung der Verfasser derjenige, der am wichtigsten ist, da die für das Chargingprotokoll aufgewendete Bandbreite ansonsten verkauft werden könnte. Tabelle 2 (vgl. [FSVP98] S.6) zeigt, daß die chargingrelevante Information für diesen Stream nur 0,74% der gesamten Flowbandbreite beansprucht: während einer Reservierungperiode werden 500 Datenpakete und nur ein Messageroundtrip (2 RSVP Messages) zur Preisbestimmung und die Erneuerung der Reservierung benötigt.

Es ist offensichtlich, daß je höher die Bandbreite der Flows und je länger die Reservierungsperioden sind, desto geringer der Protokolloverhead ist.

Die Verarbeitungszeit im Router wurde für verschiedene Pricing Mechanismen untersucht: für einen auktionsbasierten Ansatz (ähnlich dem Smart Market Modell, jedoch mit permanent stattfindenden Auktionen) und das oben vorgestellte Basispreis Modell. Das Ergebnis für den Fall, daß die Router 100000 aktive Flows gleichzeitig verwalten müssen (das heißt unter realistischer Last), ist in Abbildung 9 (vgl. [FaSP98] S.4) dargestellt: je nach gewähltem Pricing Modell kann der Verarbeitungsaufwand signifikant werden.

	[Byte/Paket]	[Pakete]	Summe [Byte]	[%]
Nutzdaten	80	500	40000	73,2
IP/UDP Header	28	500	14000	25,6
RSVP Messages	96	2	192	0,4
Charging Information	12	2	24	0,04
Preisanfragen	108	2	216	0,4
Authentifizierungsdaten	28	2	56	0,1
Optional: RESVCONF	136	1	136	0,2
Gesamt	-	-	54624	100

Tabelle 2: Protokolloverhead für einen IP Telefonstream bei Delta Auktion

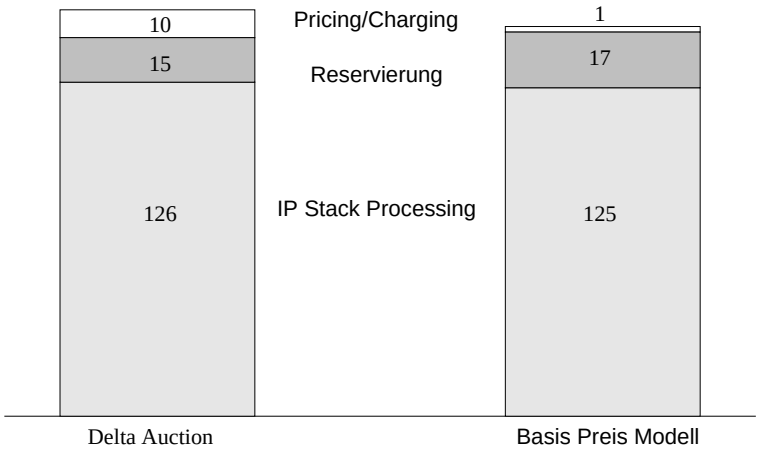

Abbildung 9: Processingzeit für verschiedene Pricingmodelle [μs]

Zusammenfassend läßt sich also sagen, daß der vorgeschlagene flowbasierte Ansatz nur geringen Processingoverhead verursacht und nur wenig Bandbreite benötigt. In diesem implementierten Chargingmodell wurde also gezeigt, daß die Einbindung von Charging- und Accountingfunktionaltät in bestehende Netzwerke möglich ist, ohne daß der Overhead inakzeptabel hoch wird. Der Schlüssel hierzu war die Verwendung von Flows als Grundlage für das Accounting. Außerdem ist die flexible Aushandlung der Aufteilung der Kosten einer Verbindung zwischen Sender und Empfänger möglich. Das Modell unterstützt außerdem eine inkrementelle Implementierung, da der Mechanismus auch funktioniert, wenn nicht an jedem Router Pricingfunktionalität gegeben ist.

4.5 Weiterentwicklungen

Fankhauser et al. sehen zukünftig weiteren Bedarf an Forschung für die Einführung neuer Routing Modelle, die QoS und Pricing Information verwenden, um das Routing auf den Nutzer abzustimmen (will man eine schnelle teuere Verbindung oder eine etwas langsamere, aber dafür günstigere Verbindung). Ein weiteres noch zu lösendes Problem ist die Integration von best-effort Verbindungen in die Architektur: der gegenwärtige Vorschlag stützt sich allein auf das Charging von reservierter Kommunikation. Auch eine mögliche Kostenteilung von Sender und Empfänger oder von Empfängern bei Multicastverbindungen muß noch gelöst werden.

5 Zusammenfassung

Zusammenfassend läßt sich sagen, daß bisher noch keine optimale (vor allem in der Frage der Umsetzbarkeit) Lösung für das Pricing im Internet gefunden wurde. Dies liegt an der Komplexität der Aufgabe und der schnellen Entwicklung neuer Technologien im Netzwerk. Das Internet als Netz von Netzwerken verlangt nach einer Implementierung, die Interoperabilität gewährleistet. Deshalb wird es sicher zunächst zu einem einfachen, standardisierten Modell kommen, um proprietäre Lösungen zu verhindern, die zu signifikanten Mehrkosten und Problemen führen können.

Aber selbst die These, daß mit dem Übergang vom best-effort Internet zu einem Integrated Services Internet mit variablen Dienstklassen und – garantien die Abkehr von der flat-fee Abrechnung unausweichlich ist, ist nicht unumstritten. Kritische Stimmen warnen vor einer Verkomplizierung des Internet, so daß der gewonnene Vorteil durch das nutzungsabhängiges Pricing durch den erhöhten Wartungs- und Programmieraufwand aufgehoben wird. Odlezky [Odly98] erhebt die These, daß der weitere Ausbau der Übertragungskapazitäten Internets zunächst nicht die billigste, aber auf die lange Sicht vielleicht die beste Lösung sein kann, da die Einfachheit des Netzes gewährleistet bleibt.

Das Problem besteht also darin die optimale Balance zwischen ökonomischer und technischer Effizienz zu finden. Es bleibt festzuhalten, daß es auf dem Gebiet des Pricing noch viel, vor allem an interdisziplinärer Forschung bedarf. Die von Fankauser et al. [FSPW98] formulierte These könnte aber in nicht allzu ferner Zukunft Realität werden: "... die Entwicklung des Internet von einem auf die Technologie fokussierten Netzwerk hin zu einem ökonomisch gesteuerten, effizienten globalen Informationssystem scheint unausweichlich."

Literatur

[CaGu94] Carter und Guthrie. Pricing Internet: The New Zealand Experience. *Technical Report, University of Canterbury, Christchurch, New Zealand* Band verfügbar unter URL: http://www.press.available, 1994.

[FaSP97] Fankhauser, Stiller und Plattner. Arrow: A flexible Architecture for an Accounting and Charging Infrastructure in the Next Generation Internet. *Berlin Internet Economics Workshop*, Oktober 1997.

[FaSP98] Fankhauser, Stiller und Plattner. Charging of Multimedia Flows in an Integrated Services Network. *Working paper*, 1998.

[FORR98] Fulp, Ott, Reininger und Reeves. Paying for QoS: An Optimal Distributed Algorithm for Pricing Network Resources. *Proceedings of the IWQOS'98 Workshop, Nappa Valley, CA*, Mai 1998.

[FSPW98] Fankhauser, Stiller, Plattner und Weiler. Charging and Accounting for Integrated Services - State of the Art, Problems, and Trends. *INET'98: The Internet Summit, Genf, Schweiz*, Juli 1998.

[FSVP98] Fankhauser, Stiller, Vögtli und Plattner. Reservation-based Charging in an Integrated Services Network. *4th INFORMS Telecommunications Conference, Boca Raton, Florida, USA*, März 1998.

[GJPS+97] Gupta, Jukic, Parameswaran, Stahl und Whinston. Streamlining the Digital Economy - How to Avert a Tragedy of the Commons. *CREC, University of Texas, Austin*, 1997.

[Hard68] Hardin. *Tragedy of the Commons.* Science. 1968.

[MacK97] MacKie-Mason. A Smart Market for Resource Reservation in a multiple Quality of Service Information Network. *University of Michigan*, September 1997.

[McBa98] McKnight und Bailey. An Introduction to Internet Economics. *MIT Workshop on Internet Economics*, März 1998.

[MMVa94a] MacKie-Mason und Varian. Pricing Congestible Network Resources. *University of Michigan*, 1994.

[MMVa94b] MacKie-Mason und Varian. Pricing the Internet. *University of Michigan*, 1994.

[MMVa94c] MacKie-Mason und Varian. Some Economics of the Internet. *University of Michigan*, 1994.

[MMVa94d] MacKie-Mason und Varian. Some FAQs about Usage-Based Pricing. *University of Michigan*, September 1994.

[Odly98] Odlyzko. The economics of the Internet: Utility, Utilization, Pricing, and Quality of Service. *AT&T Labs Research*, 1998.

[Walr54] Walras. *Elements of Pure Economics.* Richard D. Irwin. 1954.

Virtuelle private Netze — weltweite LANs

Tobias Zimmer

Kurzfassung

Virtuelle private Netze stellen eine neue Entwicklung auf dem Netzwerkmarkt dar. Obwohl die grundlegenden Techniken, auf denen sie beruhen, seit längerem bekannt sind und in verschiedenen Bereichen verwendet werden, sind sie eine Neuheit. Die vorliegende Arbeit beinhaltet eine Einführung in die Technik virtueller privater Netze, ihre Funktion und ihre praktischen Anwendung. Es werden Beispiele für den Einsatz dieser Netze angeführt und die zugrunde liegenden Protokolle und Standards erläutert, um einen Einblick in die vielfältigen Einsatzmöglichkeiten dieser neuen Technik zu gewähren und ihre Vorteile gegenüber klassischen Lösungen herauszustellen. Weiterhin werden auch die Probleme behandelt, zu denen es beim Einsatz virtueller privater Netzwerke kommen kann und wie diese in Zukunft gelöst werden könnten.

1 Einführung

1.1 Was sind virtuelle private Netzwerke?

Ein virtuelles privates Netzwerk (Virtual Private Network, VPN) bietet die gleiche Funktionalität wie jedes andere private Netzwerk. Das heißt, die Daten, die zwischen den Stationen des Netzes ausgetauscht werden, sind sicher vor Angriffen von außen. Der Unterschied zu einem privaten lokalen Netz (Local Area Network, LAN) oder privaten Weitverkehrsnetz (Wide Area Network, WAN) besteht darin, daß das VPN die LAN-Struktur auf einem öffentlichen WAN, wie dem Internet, nachbildet. Hierzu werden virtuelle Verbindungen (Tunnel) verwendet (siehe Abschnitt 2.1).

1.2 Anwendungsgebiete für VPNs

Die Einsatzmöglichkeiten von VPNs entsprechen denen anderer privater Netzwerke, wobei einige Anwendungen erheblich vereinfacht werden und sogar neue hinzukommen, die mit klassischen Netzstrukturen nicht oder nur unter großem Aufwand zu realisieren sind, wie die

- Verbindung von LANs an verschiedenen Standorten eines Unternehmens;
- Anbindung von Außendienstmitarbeitern an interne Firmennetze;
- Erweiterung von Firmennetzen auf Zulieferer und Geschäftspartner (E-Commerce);
- sichere Datenübertragung für Online–Banking Kunden zum Bankrechner.

Mit der Konfiguration der VPNs für die hier angeführten Anwendungen und Beispielen für deren Einsatz beschäftigt sich Abschnitt 3.

1.3 Vorteile des Einsatzes von VPNs

Aus der Sicht des Anwenders liegen die Hauptvorteile des Einsatzes von VPNs in den, im Vergleich zu Direktverbindungen, geringen Unterhaltskosten und in der erheblich vereinfachten Administration des Gesamtnetzwerks. Hinzu kommt, daß das VPN mit geringem Aufwand beliebig erweiterbar ist und vorhandene LAN–Strukturen beim Aufbau übernommen werden können.

Das VPN ersetzt zum Beispiel teure angemietete Leitungen zwischen verschiedenen Standorten durch virtuelle Verbindungen, die bei Bedarf aktiviert werden können. So entstehen keine Kosten für ungenutzte Kapazitäten. Für die Anbindung von Außendienstmitarbeitern wird keine eigene Modem–Bank mit Remote Access Server für Einwahlverbindungen benötigt, da sich diese Mitarbeiter über einen beliebigen Einwahlknoten (Point of Presence, POP) ihres Internet-Dienstanbieters (Internet Service Providers, ISP) mit dem firmeneigenen Netz verbinden können. Für die Internet– und VPN–Anbindung können dieselben Hardware–Komponenten verwendet werden, wodurch der Administrationsaufwand und die Anschaffungskosten minimiert werden.

Zusammenfassend ergeben sich folgende Vorteile:

- geringere Unterhaltskosten als angemietete Leitungen;
- einfachere Administration;
- beliebige Erweiterbarkeit unter Erhaltung vorhandener Teilnetzstrukturen;
- eigene Modem–Bänke werden unnötig;
- vorhandene Internet–Hardware kann verwendet werden, um ein VPN aufzubauen.

Es wird geschätzt, daß der Einsatz von VPNs, gegenüber klassischen Lösungen, eine Kostenersparnis von 20–60% [Full98, Asce97] zur Folge hat.

1.4 Anforderungen

Der Einsatz von VPNs im professionellen Umfeld bedingt einige wichtige Anforderungen an die Dienstmerkmale dieser Netze. Im folgenden werden diese kurz zusammengefaßt.

Datensicherheit: Der Schutz der Daten auf ihrem Weg durch das Internet ist eine der Hauptaufgaben einer VPN–Implementierung. Dieser Schutz wird durch Techniken wie das Tunneln (Tunneling), Kapselung und Verschlüsselung realisiert.

Verfügbarkeit und Dienstgüte (Quality of Service, QoS): Die virtuellen Verbindungen eines VPN müssen bei Bedarf jederzeit zur Verfügung stehen. Anwendungen wie Netztelefonie und Videokonferenz stellen Qualitätsanforderungen an die Datenverbindungen in Bezug auf ihre Bandbreite und die Übertragungsgeschwindigkeit.

Kompatibilität: Ein VPN sollte mit den vorhandenen Anwendungsprogrammen des Benutzers kompatibel sein, um Neuanschaffungen und das Erlernen neuer Programme zu vermeiden. Das heißt, die Implementierung sollte für den Kunden möglichst transparent geschehen.

Adressierung: Die Adressierung innerhalb eines VPN sollte unabhängig von Internet–Adressen sein, da sonst eine komplette Neukonfiguration aller angeschlossenen Teilnetze in den meisten Fällen unumgänglich wäre.

Standards: Die Implementierungen von VPNs sind zur Zeit noch sehr herstellerspezifisch. Standards existieren nur für einzelne Komponenten, aber noch nicht für vollständige VPN–Implementierungen, was für den Anwender, zum Beispiel bei einem Wechsel seines ISPs, zu Problemen führen kann.

Wie diese Anforderungen bei der Implementierung von VPNs umgesetzt werden, zeigt Abschnitt 2.

2 Technische Grundlagen von VPNs

Dieser Abschnitt behandelt die Techniken, Protokolle und Standards, die der Implementierung von VPNs zugrunde liegen und zeigt, wie mit diesen den Anforderungen aus Abschnitt 1.4 Rechnung getragen wird.

2.1 Tunneling

Das Tunneling oder Kapselung ist eine Technik, die es erlaubt, beliebige Datenpakete aus einem LAN über ein anderes Netzwerk zu verschicken. Dabei spielt die Adressierung und das im LAN verwendete Übertragungsprotokoll keine Rolle. Das heißt, durch das Tunneling ist es möglich, zwei oder mehrere LANs transparent über ein WAN zu koppeln (siehe Abbildung 1).

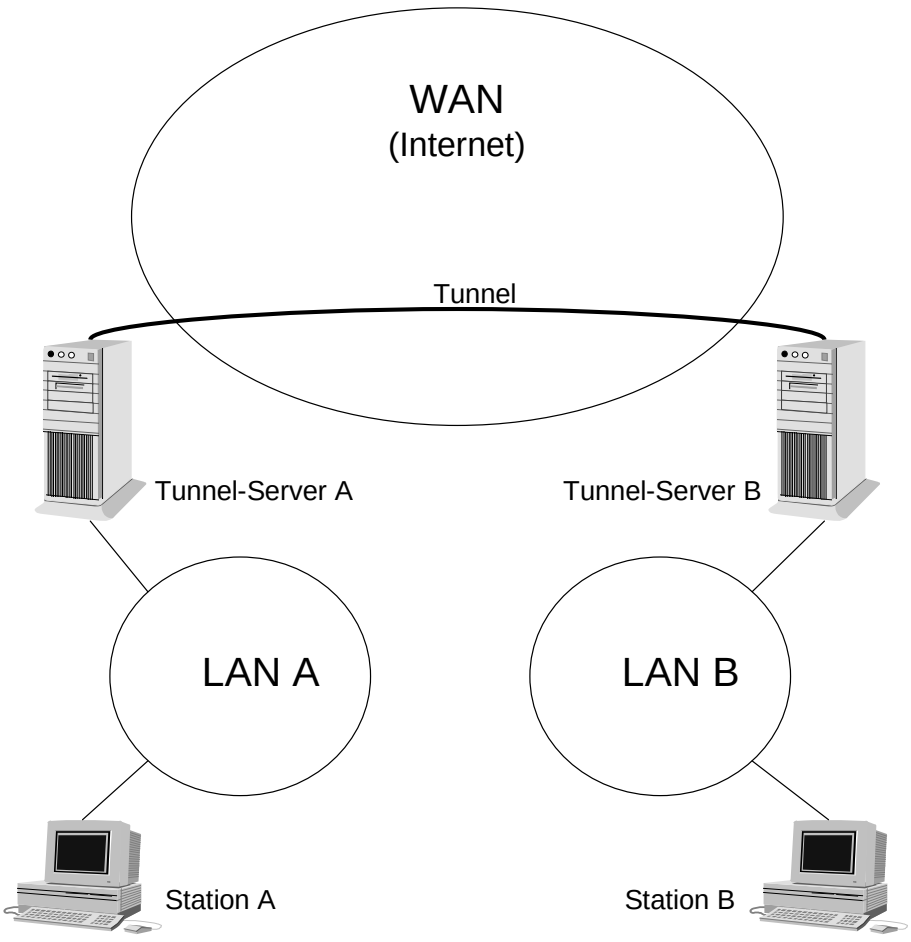

Abbildung 1: Koppelung von zwei LANs durch einen Tunnel

Tranzparenz bedeutet hierbei, daß die kommunizierenden Stationen in den verbundenen LANs nicht mit der Verwaltung und dem Aufbau des Tunnels betraut sind. Diese Aufgabe wird in jedem LAN von einem extra Tunnel-Server übernommen. Die Stationen in den LANs arbeiten so, als ob sie alle an einem einzigen LAN angeschlossen wären.

IP-Tunneling über das Internet beruht darauf, daß dem zu transportierenden Paket ein neuer IP–Kopf vorangestellt wird (IP in IP, RFC 2004 [Inte99]). Dieser Kopf wird in einem Server des LANs oder des ISPs erzeugt, der den Ausgangspunkt des Tunnels bildet. Der Kopf enthält als Quelladresse die Adresse dieses Rechners und als Zieladresse einen Server, der den Endpunkt des Tunnels bildet und das transportierte Paket wieder entpackt, also den Tunnel–Kopf entfernt. Dieses Paket wird dann wie gewohnt im Ziel–LAN seinem Empfänger zugestellt.

Der Tunnel verhält sich also wie eine bidirektionale Direktverbindung zwischen den beiden Tunnel–Servern.

Das Tunneling–Verfahren ist in Schicht 3 des ISO/OSI–Basisreferenzmodells angesiedelt. Dadurch stellt es selber keine Zugriffskontrollmechanismen zur Verfügung. Es bildet aber die Grundlage für einige Schicht–2–Protokolle, die diese Mechanismen implementieren (siehe Abschnitt 2.2).

Ein erster Standard für das Tunneling ist Generic Routing Encapsulation (GRE), RFC 1701 und RFC 1702 [Inte99]. Dabei handelt es sich um eine Richtlinie, wie die Tunnel–Pakete aufgebaut sein sollen.

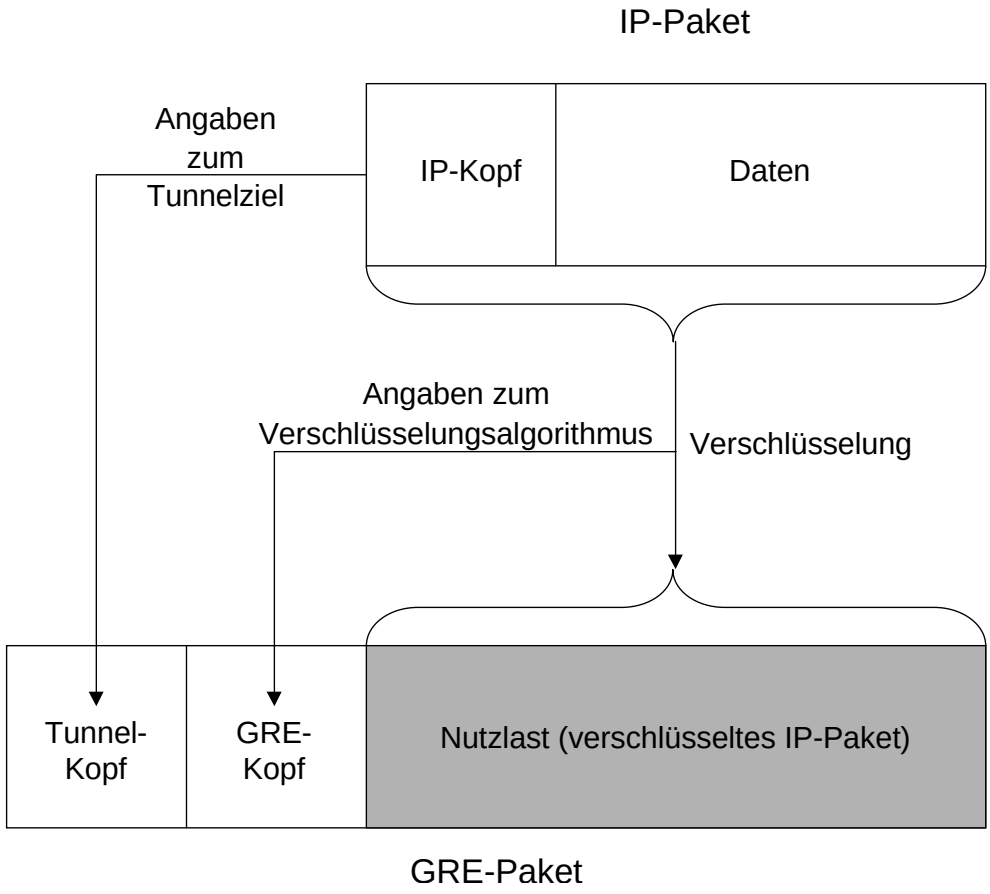

Abbildung 2: Aufbau eines GRE–Paketes zum Transport von IP–Paketen

In einem GRE-Paket werden drei Abschnitte unterschieden: ein Tunnel–Kopf, der das Tunnelziel enthält, ein GRE–Kopf, der Informationen über das verwendete Tunnel–Protokoll und Verschlüsselungsalgorithmen enthält, und die Nutzlast (Payload), also das zu transportierende

LAN–Paket. Abbildung 2 zeigt den Aufbau eines solchen GRE–Paketes. Als Beispiel ist hier die Kapselung eines IP–Paketes gewählt. Mit GRE–Paketen lassen sich aber auch beliebige andere Netzwerkprotokolle tunneln.

2.2 PPTP, L2F und L2TP

Die Protokolle, die in diesem Abschnitt vorgestellt werden, arbeiten auf Schicht 2 des ISO/OSI–Basisreferenzmodells. Somit sind sie in der Lage Zugriffskontrollmechanismen bereit zu stellen, die eine Sicherung des Datenverkehrs in einem VPN ermöglichen.

Das Point–to–Point Tunneling Protocol (PPTP) [Micr98] das von Microsoft und anderen führenden Unternehmen der Netzwerkbranche entwickelt wurde, wurde 1996 der Internet Engineering Task Force (IETF) als Standardprotokoll für das Internet–Tunneling vorgeschlagen [Full98]. PPTP ist eine Erweiterung des Point–to–Point Protocol (PPP). PPTP kapselt PPP–Pakete in IP-Paketen, so können Protokolle wie IP, IPX und NetBEUI über das Internet getunnelt werden. Für die Zugangskontrolle werden das Password Authentification Protocol (PAP) und das Challenge Handshake Protocol (CHAP) verwendet. Als Verschlüsselungsalgorithmen dienen die Rivest´s Cipher 4 (RC4) und der Data Encryption Standard (DES) mit Schlüsseln zwischen 40 und 128 Bit Länge [Jach97].

PPTP ermöglicht also den Aufbau eines sicheren Tunnels, in dem die Daten verschlüsselt transportiert werden. Da PPTP mit PAP und CHAP auch einen gesicherten Verbindungsaufbau und Authentifizierung unterstützt, kann es sowohl auf der Seite eines ISP, zur Verbindung von LANs, als auch auf Anwenderseite zur Anbindung von mobilen Rechnern, verwendet werden. Dabei kann der Anwender eine PPP–Verbindung zu seinem ISP aufbauen, die noch nicht gesichert ist. Dann wird entweder der Tunnel vom ISP aufgebaut, wenn dieser PPTP unterstützt, oder der Anwender kann, wenn PPTP auf seinem eigenen Rechner installiert ist, den Tunnel selbst aufbauen. Nach erfolgreicher Initialisierung des Tunnels nimmt PPTP die Quellpakete entgegen, verschlüsselt sie und gibt sie dann gemäß der GRE (siehe Abschnitt 2.1) weiter.

Ein PPTP–Paket setzt sich aus vier Schichten zusammen. Die oberste Schicht bildet ein Zustellungs–Kopf, der aus dem Netzwerkprotokoll des WAN besteht, über das das VPN aufgebaut wird. Darauf folgt als zweite Schicht ein IP–Kopf, der grundlegende Informationen über das IP–Datagramm enthält, wie die Paketlänge und die Absender– und Empfängeradresse. Die dritte Schicht enthält einen GREv2–Kopf. GREv2 stellt eine für PPTP entwickelte Erweiterung des GRE–Kopfes dar. Er enthält Informationen über die Art der Pakete, die gekapselt wurden und PPTP spezifische Daten über die Verbindung zwischen dem Client und dem Server. Die letze Schicht, das Nutzlast–Datagramm, enthält die eigentlichen Datenpakete. Im Fall von PPP sind das die PPP–Pakete, die zwischen Client und Server ausgetauscht werden. In diesen PPP–Paketen befinden sich dann die zu transportierenden IP–, IPX– oder NetBEUI–Pakete. [ScWE98] Zur Veranschaulichung zeigt Abbildung 3 die aktiven Protokollschichten während einer PPTP–Verbindung.

Das Layer 2 Forwarding (L2F) von der Firma Cisco Systems stellt ein ähnliches Protokoll dar, das mit PPTP die Grundlage für das Layer 2 Transport Protocol (L2TP) eine Weiterentwicklung beider Systeme bildet [Aven98]. L2F unterstützt verschiedene Protokolle und mehrere unabhängige, parallele Tunnel. Die Benutzeridentifizierung ist allerdings etwas schwächer als bei PPTP und eine extra Verschlüsselung der Daten ist nicht vorgesehen [Cisc96].

L2TP [Cisc98b] unterscheidet sich nur in wenigen Punkten von PPTP. Zum einen ist hier zu nennen, daß L2TP, wie das L2F, mehrere Tunnel unterstützt, zum anderen liegt die Kontrolle über den Endpunkt eines Tunnels nicht wie bei PPTP beim Anwender, sondern wird vom ISP vorgegeben. Eine ausführliche Erläuterung der Unterschiede zwischen PPTP und L2TP findet sich in [FeHu98].

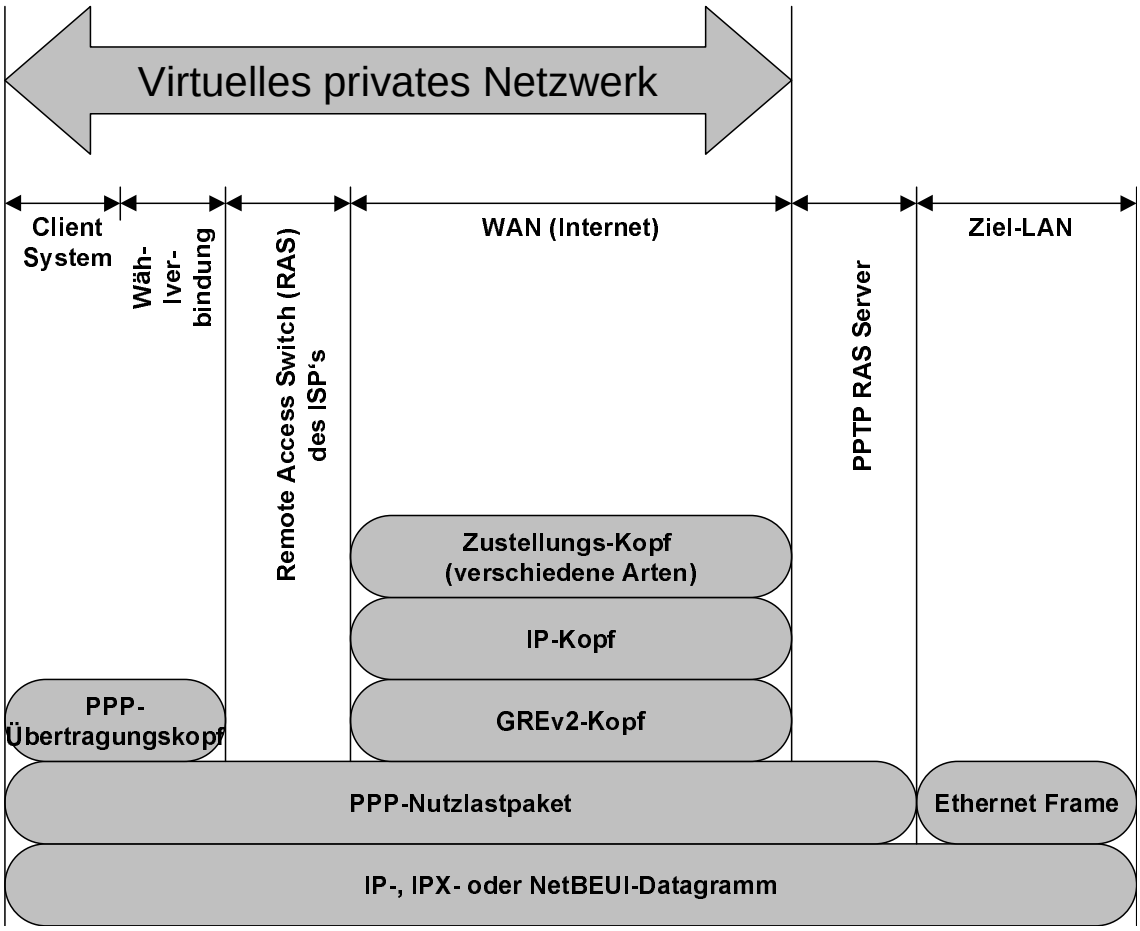

Abbildung 3: Aktive Protokollschichten während einer PPTP–Verbindung

2.3 IPSec

IP Security (IPSec) ist eine neuere Technik, die PPTP langfristig als VPN-Standard ablösen soll, da sie ein höheres Maß an Sicherheit als PPTP garantieren kann. IPSec arbeitet auf IPv4 und soll fester Bestandteil von IPv6 werden. Bei IPSec handelt es sich um ein Paket von Protokollen (RFC 1825 – 1829) [Cisc98a, Inte99], die für Authentifizierung, Datenintegrität, Zugriffskontrolle und Vertraulichkeitsbelange innerhalb des VPN zuständig sind. IPSec besitzt zwei verschiedene Betriebsmodi: den Transportmodus und den Tunnelmodus.

Transportmodus: Im Transportmodus verschlüsselt IPSec nur den Datenteil des zu transportierenden IP–Paketes. Der Original–IP–Kopf bleibt dabei erhalten und es wird ein zusätzlicher IPSec–Kopf hinzugefügt (siehe Abbildung 4). Der Vorteil dieser Betriebsart ist, daß jedem Paket nur wenige Bytes hinzugefügt werden. Dem gegenüber steht, daß jede Station im VNP IPSec beherrschen muß, was eine Neukonfiguration von bestehenden Netzen nötig macht. Außerdem ist es für Angreifer möglich, den Datenverkehr im VNP zu analysieren, da die IP–Köpfe nicht modifiziert werden. Die Daten selbst sind aber verschlüsselt, so daß man nur feststellen kann, welche Stationen wieviele Daten austauschen, aber nicht welche Daten.

Tunnelmodus: Im Tunnelmodus wird das komplette IP–Paket verschlüsselt und mit einem neuen IP–Kopf und IPSec–Kopf versehen. Dadurch ist das IPSec–Paket größer als im Transportmodus. Der Vorteil besteht hier darin, daß in den LANs, die zu einem VPN verbunden werden sollen, je ein Gateway so konfiguriert werden kann, daß es IP–Pakete

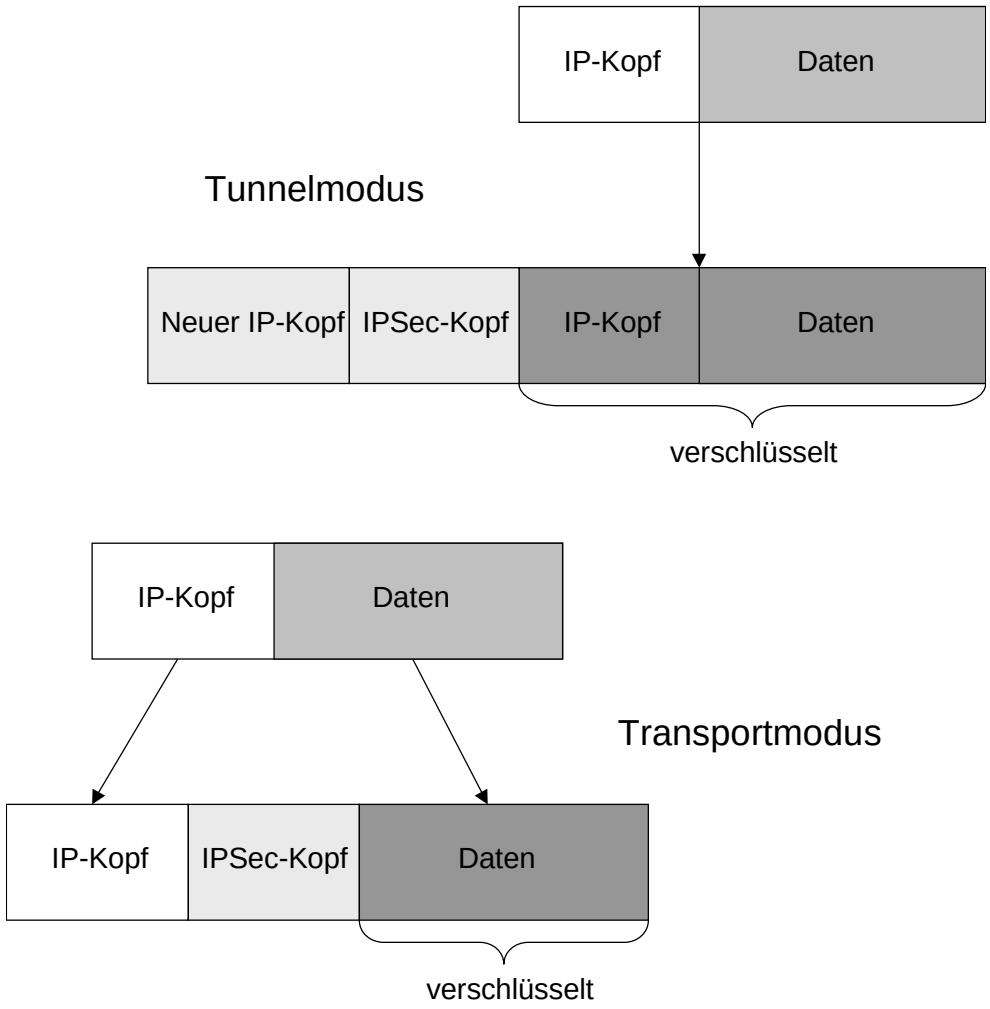

Abbildung 4: Aufbau von IPSec–Paketen in den verschiedenen Betriebsmodi

annimmt, sie in IPSec–Pakete umwandelt und dann über das Internet dem Gateway im Zielnetzwerk zusendet, das das ursprüngliche Paket wiederherstellt und weiterleitet. Dadurch wird eine Neukonfiguration der LANs umgangen, da nur in den Gateways IPSec implementiert sein muß. Außerdem können Angreifer so nur den Anfangs– und Endpunkt des IPSec–Tunnels feststellen.

Wie Abbildung 4 zeigt, wird der IPSec–Kopf hinter dem IP–Kopf eingefügt. Er kann zwei Komponenten enthalten, die einzeln, unabhängig voneinander oder zusammen eingesetzt werden können: den Authentifizierungskopf (Authentification Header, AH) und den Encapsulating Security Payload (ESP). Der AH sichert die Integrität und Authentizität der Daten und der statischen Felder des IP–Kopfes. Er bietet jedoch keinen Schutz der Vertraulichkeit. Der AH benutzt eine kryptographische Hashfunktion (keyed–hash function) und keine digitale Signatur, da diese Technik zu langsam ist und den Datendurchsatz im VPN stark reduzieren würde. Der ESP schützt die Vertraulichkeit, die Integrität und Authentizität von Datagrammen. Er schließt aber die statischen Felder des IP–Kopfes bei einer Integritätsprüfung nicht ein.

IPSec verwendet das Diffie–Hellman Schlüsselaustauschverfahren zur Identitätsprüfung. Die benutzten kryptographischen Hashfunktionen sind unter anderem HMAC, MD5 und SHA. Als Verschlüsselungsalgorithmen dienen zum Beispiel DES und IDEA, Blofish und RC4. Weiterführende Informationen und genaue Beschreibungen dieser Verfahren finden sich in [Jach97].

2.4 SOCKS v5

SOCKS v5 ist eigentlich das von der IETF eingeführte Standardprotokoll zum sicheren Passieren einer Firewall. In Kombination mit der Secure Socket Layer (SSL) bildet es die Grundlage für den Aufbau hochsicherer VPNs, die mit jeder Firewall kompatibel sind [Aven98].

SOCKS v5 arbeitet auf Schicht 5 des ISO/OSI–Basisreferenzmodells. Aus diesem Grund bietet es weit bessere Zugriffskontrollmöglichkeiten als Protokolle, die auf tieferen Schichten arbeiten, da es mehr Informationen über die laufenden Anwendungen zur Verfügung hat (siehe Abbildung 5).

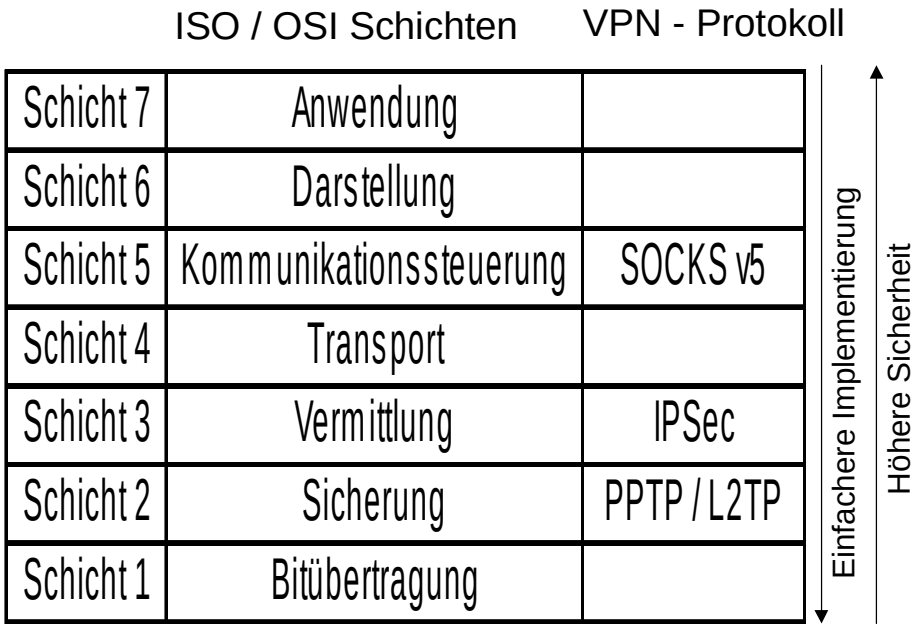

Abbildung 5: Einordnung der VPN–Protokolle im ISO/OSI–Basisreferenzmodell

SOCKS v5 identifiziert einzelne Benutzer und leitet den gesamten Datenverkehr über eine Firewall. So ist es möglich, die Zugriffsrechte innerhalb des VPN für jeden Benutzer individuell zu konfigurieren, ohne neue Anwendungen extra anpassen zu müssen.

Durch ihre Ansiedlung in Schicht 5 des ISO/OSI–Basisreferenzmodells sind SOCKS v5 und SSL die einzigen Protokolle, die mit VPN–Protokollen niedrigerer Schichten zusammenarbeiten können.

Nachteile des Einsatzes von SOCKS v5 sind die geringere Geschwindigkeit, da alle Daten eine Firewall passieren müssen, und die Notwendigkeit entsprechender Programme auf jedem Rechner im VPN, die einen Verbindungsaufbau durch die Firewall ermöglichen.

2.5 RADIUS (Remote Authentication Dial–In User Service)

RADIUS (RFC 2058, RFC 2059) [Cisc97, Inte99] ist kein VPN–Protokoll im eigentlichen Sinne, sondern ein zusätzlicher Dienst, der die Verwaltung und Sicherung von Wählzugängen zu einem VPN erleichtert und verbessert [Davi98]. Den Aufbau eines VPN mit RADIUS–Servern zeigt Abbildung 6. RADIUS arbeitet mit einer Client–/Server–Architektur, wobei RADIUS den Server darstellt und der ISP–Server oder der Firmen–Server den Client.

RADIUS stellt Mechanismen zur Benutzeridentifizierung über PAP und CHAP, zur Zugriffskontrolle über eine eigene RADIUS–Datenbank und zur Verwaltung von dynamischen IP–Adressen bereit [Asce97]. Zur Kommunikation zwischen dem RADIUS–Server und dem ISP–

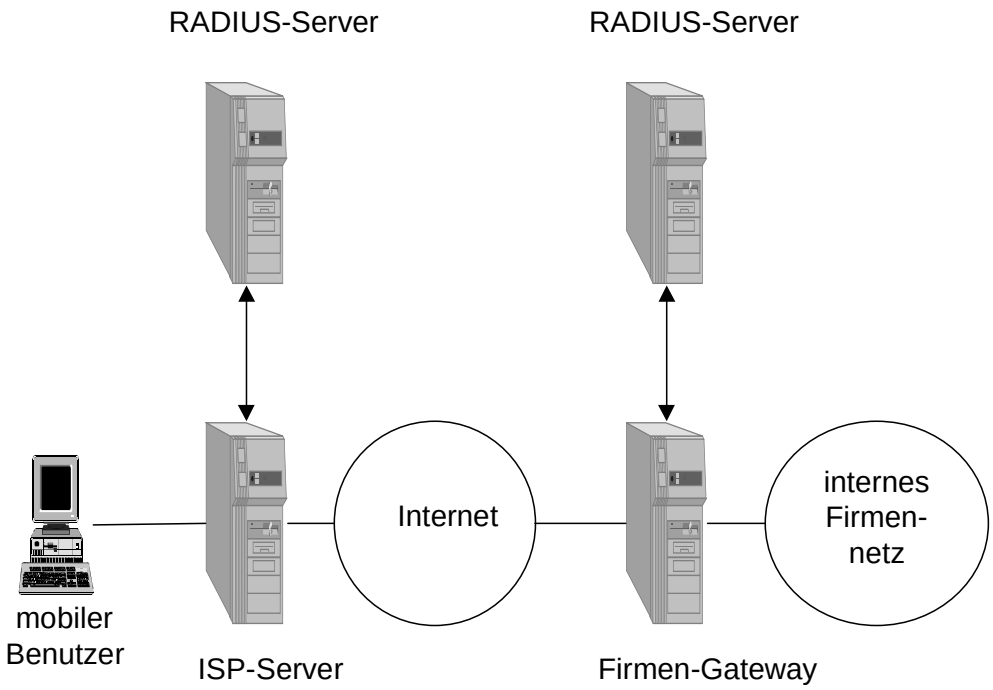

Abbildung 6: Aufbau eines VPN mit RADIUS–Servern

Server wird das User Datagram Protocol (UDP) benutzt [Cisc97]. Das Format der RADIUS–Pakete ist in RFC 2058 [Inte99] beschrieben.

RADIUS wird im allgemeinen in Kombination mit anderen VPN–Protokollen wie zum Beispiel L2F eingesetzt. Eine ausführliche Beschreibung der Zusammenarbeit dieser beiden Protokolle findet sich bei [Cisc97].

3 Konfigurationen von VPNs

Dieser Abschnitt befaßt sich mit der Konfiguration und dem Aufbau von VPNs für verschiedene Anwendungsbereiche. Anhand von Beispielen soll gezeigt werden, welche Netzwerkstrukturen sich für welche Einsatzgebiete besonders gut eignen. Ferner werden die Einsatzmöglichkeiten der in Abschnitt 2 beschriebenen Protokolle unter Einbeziehung des Sicherheitsaspektes angeführt.

3.1 End–to–End–VPNs

End–to–End–VPNs stellen eine direkte Verbindung zwischen mehreren Arbeitsrechnern dar. Eingesetzt werden kann diese Art der VPNs zum Beispiel, um Bankkunden über das Internet sicher mit einem Buchungsrechner zu verbinden, oder um mehreren Wissenschaftlern an verschiedenen Standorten die Arbeit an einem gemeinsamen Projekt zu erleichtern (siehe Abbildung 7).

Zu beachten ist hierbei, daß auf jedem der an das VPN angeschlossenen Rechner ein entsprechendes VPN–Protokoll installiert sein muß, da die Arbeitsrechner direkt untereinander und nicht über zwischengeschaltete VPN–Server verbunden werden.

Besonders geeignete Protokolle für den Aufbau von End–to–End–VPNs sind L2F, L2TP und IPSec, wobei IPSec für Anwendungen, die ein Höchstmaß an Sicherheit erfordern, am besten geeignet ist. Bei dieser Konfiguration ergibt sich aber immer das Problem der Verwaltung des

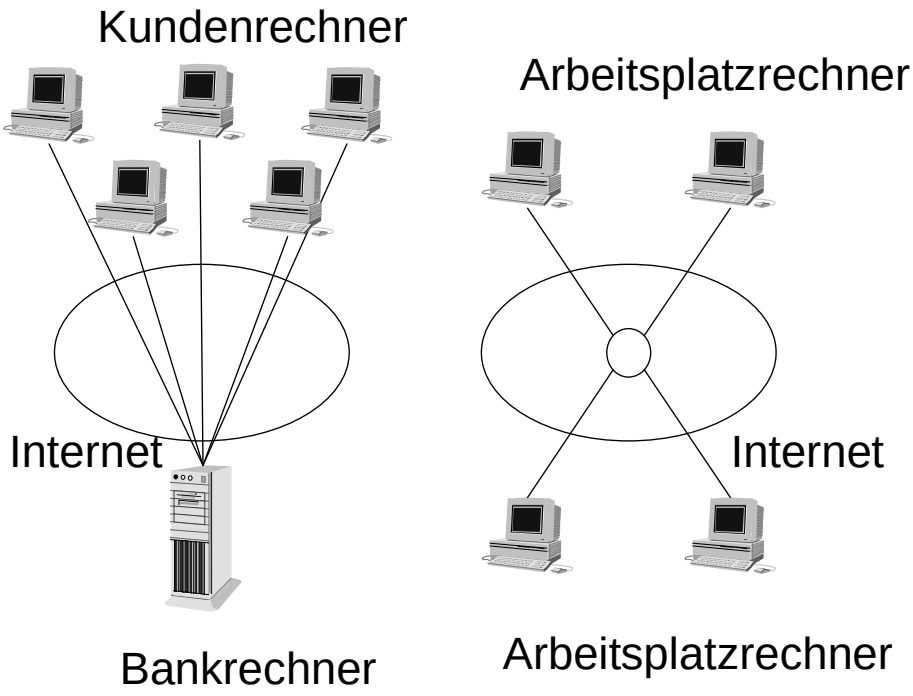

Abbildung 7: Zwei Beispiele für den Aufbau von End–to–End–VPNs

Netzwerks. Im Fall der Online–Banking–Anwendung wird die Verwaltung vom Bankrechner übernommen, da keine Notwendigkeit des Datenaustausches einzelner Kunden untereinander besteht. Im Fall der verteilten Projekte dagegen muß jede der angeschlossenen Stationen die Zugriffe von allen anderen Rechnern selbst verwalten, da der Austausch von Daten der einzelnen Projektteilnehmer untereinander möglich sein muß.

3.2 Site–to–Site–VPNs

Site–to–Site–VPNs stellen die klassische VPN–Variante dar. Hierbei werden mehrere LANs an verschiedenen Standorten verbunden. Diese Konfiguration eignet sich zum Beispiel, um Firmennetze zusammenzuschließen (Abbildung 8), Krankenhäuser zum Datenaustausch zu verbinden, oder Forschungsnetze mit mehreren Forschungsgruppen aufzubauen.

Bei Site–to–Site–VPNs unterscheidet man zwischen Intranet VPNs und Extranet VPNs, die verschiedenen Sicherheitsanforderungen genügen müssen.

3.2.1 Intranet VPNs

Unter Intranet VPNs versteht man Netze, die zur Erweiterung interner LANs dienen. Ein typisches Beispiel ist die in Abbildung 8 gezeigte Anwendung. Hierbei wird davon ausgegangen, daß jede der angeschlossenen Parteien den anderen voll vertraut, und daß alle Ressourcen im Netz allen Parteien zugänglich sein sollen. Daher wird bei diesem VPN–Typ, bei einem Mindestmaß an Sicherheit, großer Wert auf die Geschwindigkeit gelegt. Um die Datensicherheit zu erhöhen, können Zugriffsbeschränkungen auf Benutzerebene eingesetzt werden.

Als Protokoll kann hier zum Beispiel IPSec im Transportmodus eingesetzt werden. Dabei sind die transportierten Daten auf ihrem Weg durch das Internet durch eine Verschlüsselung geschützt und es werden nur wenige zusätzliche Byte für den IPSec–Kopf benötigt.

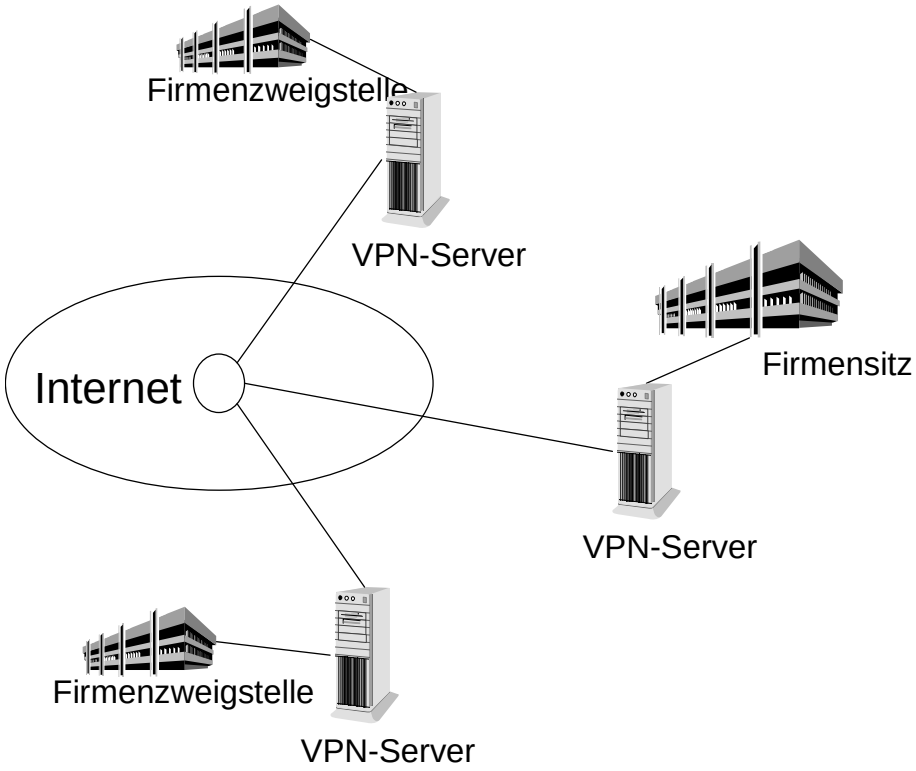

Abbildung 8: Site–to–Site–VPN zur Verbindung verschiedener Firmenstandorte

3.2.2 Extranet VPNs

Bei Extranet VPNs legt man im Vergleich zu Intranet VPNs weit größeren Wert auf die Sicherheit. Extranet VPNs werden zum Beispiel eingesetzt, um das interne Netzwerk einer Firma mit den Netzen von Geschäftspartnen und Zulieferern zu verbinden. Hierbei muß das VPN gewährleisten, daß jeder Teilnehmer nur auf die für ihn bestimmten Ressourcen Zugriff erlangen kann.

Das Datenaufkommen in Extranet VPNs ist im allgemeinen auch geringer als in Intranet VPNs, so daß man zur Realisierung ohne weiteres Lösungen einsetzen kann, die bei geringerer Geschwindigkeit ein Höchstmaß an Sicherheit bieten. Hierzu kann SOCKS v5 und SSL verwendet werden, da diese Kombination in Verbindung mit einer geeigneten Firewall auch Kontrolle über die Zugriffe einzelner Anwendungen erlaubt.

3.3 End–to–Site–VPNs

End–to–Site–VPNs oder Remote–Access VPNs dienen in erster Linie zur Anbindung von Außendienstmitarbeitern an ein internes Firmennetz. Eine solche Konfiguration zeigt Abbildung 9. Der Hauptvorteil eines solchen Netzes besteht darin, daß sich die Mitarbeiter über einen beliebigen POP des ISPs der Firma in das Netz einwählen können. Dadurch können die meist sehr hohen Kosten für Fernverbindungen reduziert werden, und das Unternehmen ist nicht gezwungen, eigene Modem–Bänke zu unterhalten und zu administrieren.

Für den Aufbau von End–to–Site–VPNs eignen sich im besonderen adressunabhängige VPN–Protokolle wie PPTP, da der Großteil der ISPs mit dynamischen IP–Adressen arbeitet. Auf Seiten der Sicherheit wird bei diesem VPN–Typ großer Wert auf die Identifizierung der einzelnen mobilen Mitarbeiter gelegt, um das Firmennetz gegen Angriffe Dritter abzusichern. Hierzu kann ein RADIUS–Server verwendet werden, der dann unabhängig vom benutzten

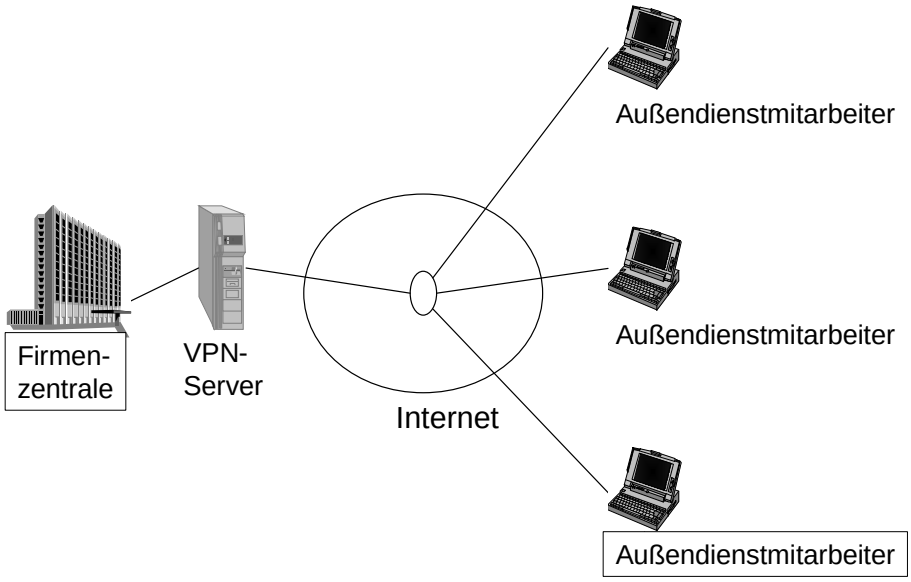

Abbildung 9: End–to–Site–VPN zur Anbindung von mobilen Mitarbeitern an ein Firmennetz

VPN–Protokoll eine zusätzliche Benutzeridentifizierung anhand einer eigenen Datenbank vornehmen kann. Alternativ ist auch hier eine Konfiguration mit SOCKS v5 in Kombination mit einem solchen RADIUS–Server vorstellbar.

4 Ausblick

VPNs versetzen Unternehmen in die Lage, auf einfache und kostengünstige Weise Netzwerke aufzubauen, bestehende Netze zu erweitern und Außendienstmitarbeiter anzubinden und dabei bestehende WAN wie das Internet zu nutzen. VPNs stellen eine billigere Alternative zu klassischen Wählleitungen dar und vereinfachen so die Administration von Netzwerken, da sie die sonst nötigen Modem–Bänke ersetzen können.

Aber trotz all dieser Vorteile können die Sicherheitsfragen, die diese neuen Netze aufwerfen nicht unbeachtet bleiben. Bei einem Datenaustausch über ein öffentliches Netz, wie dem Internet, besteht immer die Gefahr von Angriffen. Es ist also immer nötig, die Daten zu verschlüsseln und die Zugangspunkte zu den VPNs abzusichern.

Hier zeigt sich, wo zur Zeit noch die Schwächen der bestehenden VPN–Implementierungen liegen. Eine Betrachtung der auf dem Markt befindlichen Protokolle erweckt den Eindruck, daß jeder Hersteller seine eigenen Verschlüsselungsalgorithmen, Schlüsselaustausch– und Benutzeridentifizierungsverfahren verwendet. Die Kompatibilität scheint dabei unbeachtet zu bleiben. Und tatsächlich ist diese Inkompatibilität der Systeme das Argument, das heute viele Unternehmen vom Einsatz moderner VPN–Lösungen abhält.

Die aussichtsreichsten Anwärter als VPN–Standards sind PPTP und IPSec. Viele Experten bescheinigen vor allem IPSec beste Zukunftschancen im Hinblick auf die bevorstehende Einführung von IPv6.

Literatur

[Asce97] Ascend Communications INC. Virtual Private Networks Resource Guide. Internet, http://www.ascend.com, 1997.

[Aven98] Aventail Corporation. Making Sense of Virtual Private Networks. Internet, http://www.aventail.com, September 1998.

[Cisc96] Cisco Systems. Solutions for Virtual Private Dialup Networks. Internet, http://www.cisco.com, 1996.

[Cisc97] Cisco Systems. Cisco IOS Technologies: RADIUS Support in Cisco IOS Software. Internet, http://www.cisco.com, 1997.

[Cisc98a] Cisco Systems. IPSEC White Paper. Internet, http://www.cisco.com, 1998.

[Cisc98b] Cisco Systems. Layer Two Tunnel Protocol (L2TP). Internet, http://www.cisco.com, 1998.

[Davi98] I. Davies. An Introduction to Virtual Private Networks. Internet, http://www.cs.uct.ac.za/home/idavies/Security/Security.html, April 1998.

[FeHu98] Paul Ferguson und Geoff Huston. What is a VPN? Internet, http://www.employees.org:80/ ferguson/vpn.pdf, April 1998.

[Full98] Fullerton University. Virtual Private Networks. Internet, http://amir.fullerton.edu/msis410/Projects/Group12/vpnpaper.htm, 1998.

[Inte99] Internet Engineering Task Force. Homepage der Internet Engineering Task Force. Internet, http://www.ietf.org, 1999.

[Jach97] Jörn Jachalsky. Untersuchung kryptografischer Verfahren in der TCP/IP-Protokollarchitektur. Studienarbeit, Universität Hannover Lehrgebiet Rechnernetze und Verteilte Systeme, http://www.rvs.uni-hannover.de/arbeiten/studien/sa-jacha.html, April 1997.

[Micr98] Microsoft INC. PPTP and Implementation of Microsoft Virtual Private Networking. Internet, http://www.microsoft.com/windows/common/nrpptp.htm, 1998.

[ScWE98] Charlie Scott, Paul Wolfe und Mike Erwin. *Virtual Private Networks.* O´Reilly. 1. Auflage, März 1998.

Management by Delegation

Christian Schneider

Kurzfassung

Aufgrund der gestiegenen Anforderungen moderner Netze an das Management ist die klassische zentrale Struktur des SNMP für viele Zwecke nicht mehr ausreichend. Es werden die Grundstrukturen des zentral aufgebauten SNMP und verschiedene Anwendungsgebiete vorgestellt, an denen dieses Modell an seine Grenzen stößt. Das Konzept des Management by Delegation wird als mögliche Lösung dieser Probleme in seiner allgemeinen Struktur beschrieben. Die beiden Implementierungen nach IETF bzw. OSI werden schließlich genauer betrachtet und miteinander verglichen.

1 Einleitung

Aufgrund der immer stärkeren Ausweitung der zu verwaltenden Netzwerke und den wachsenden Anforderungen an die Verfügbarkeit ergibt sich die Notwendigkeit, Manager flexibler zu gestalten. Die einfachste Form eines zentralen Managements ist hier oftmals nicht mehr ausreichend. Management by Delegation ermöglicht durch verteilte Abwicklung von Managementaufgaben auch kompliziertere Netzwerke zu verwalten.

Die Ausarbeitung beginnt mit der Vorstellung des klassischen SNMP Modells und seiner Probleme. Dann wird das Konzept des verteilten Managements beschrieben und anhand seiner Ausprägungen in den IETF und OSI Standards verdeutlicht. Während der OSI Standard, wie in vielen anderen Standardisierungen, eine möglichst große Funktionalität und Universalität zu erreichen versucht, ist der IETF Standard eine pragmatische Erweiterung des SNMP, um die nötigen Konstrukte zur verteilten Ausführung von Skripten zu schaffen.

2 Klassisches SNMP Modell

2.1 Grundgedanke des zentralen Modells

Das klassische zentrale SNMP Modell basiert auf der Annahme, daß ein Manager eine möglichst einfache Struktur besitzen sollte, um eine Integration in möglichst viele verschiedene Arten von Geräten zu ermöglichen. Daher auch der Name Simple Network Management System.

SNMP kennt zwei verschiedene Arten von Systemen, Agenten und Management Stationen. Ein SNMP Agent ist sehr einfach aufgebaut und reagiert normalerweise nur auf Anfragen der Management Station. Das Angebot an Informationen, die ein Agent der Management Station bereitstellen muß, ist in den Definitionen von MIBs (Management Information Bases) exakt festgelegt.

Eine MIB ist in einer Baumstruktur aufgebaut, so daß eine Management Station durch Angabe des Pfades in diesem Baum exakt einen Wert selektieren kann. Der Aufbau dieser Struktur und

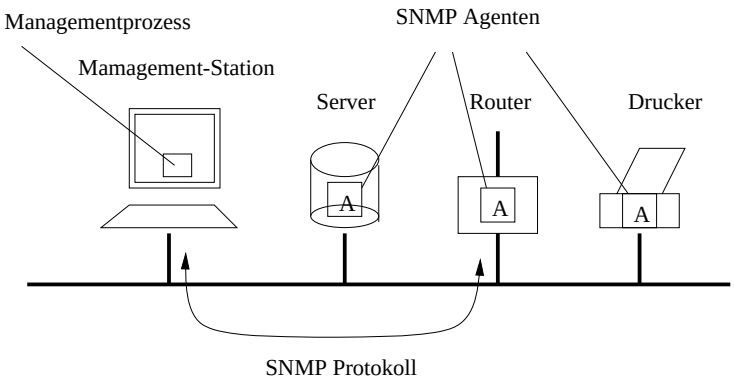

Abbildung 1: Aufbau des klassischen SNMP

der Typ der selektierbaren Objekte sind eindeutig festgelegt und müssen von jedem Agenten, der diese MIB unterstützt, exakt eingehalten werden. Den Begriff Objekt sollte man allerdings nicht zu ernst nehmen. SNMP Objekte sind nichts anderes als einfache Variablen, deren Typ nur ein Skalarwert oder eine Zeichenkette sein kann.

Das SNMP Protokoll enthält verschiedene Kommunikationsmöglichkeiten zwischen Management Station und Agent :

- Get Request : Abfrage eines Objektes (Manager/Agent)
- Get Next Request : Abfrage des in der Baumstruktur folgenden Objektes (Manager/Agent)
- Get Bulk Request : Abfrage einer Reihe von Objekten (Manager/Agent)
- Set Request : Veränderung eines Objektes (Manager/Agent)
- Inform Request : Nachricht mit einer Beschreibung der lokalen MIB (Manager/Manager)
- SNMPv2 Trap : Meldung eines besonderen Ereignisses (Agent/Manager)

Ein Agent ist, mit Ausnahme der SNMP Trap passiv und liefert nur die gewünschten Informationen bzw. führt die gewünschten Veränderungen aus. Eine Trap ist ein Signal, das der Management Station mitteilt, daß ein bestimmtes Ereignis eingetreten ist. Die Management Station muß danach die dieses Ereignis betreffenden Objekte abfragen.

2.2 Probleme

Ein grundlegender Nachteil dieses zentralen Aufbaus ist, daß beim Verlust der Verbindung zwischen Agent und Management Station jegliche Möglichkeit der Steuerung oder Überwachung des Netzes verloren geht. Außerdem erfordern einige Managementaufgaben hohe Bandbreiten, da jede über das Angebot der MIB Daten hinausgehende Berechnung vom Manager durchgeführt werden muß. Die einzige Möglichkeit eine Berechnung nach diesem Modell auf den Agenten auszulagern besteht darin, eine neue MIB zu definieren, die alle benötigten Berechnungsergebnisse vefügbar macht.

Eine solche MIB kann entweder eindeutig standardisiert werden, was sehr zeitaufwendig und unflexibel ist, oder herstellerspezifisch definiert werden. Ein Beispiel einer standardisierten MIB ist die im nächsten Kapitel beschriebene RMON MIB.

am besten geeignetes Management Modell	Zentralisiertes SNMP	MbD
Anforderungen an verteilte Intelligenz	gering	hoch
benötigte Abfrage-Frequenz	niedrig	hoch
Verhältnis von Netzwerk Durchsatz zur Menge an Managementinformationen	Groß	Klein
Komplexität und Häufigkeit des Informationsaustauschs	einfach, selten	hoch, häufig

Tabelle 1: Metriken für Dezentralisierung

3 Dezentrales Modell (MbD)

3.1 Motivation

Das dezentrale Modell geht davon aus, daß die zu überwachenden Systeme immer leistungsfähiger werden. Es entsteht also die Möglichkeit, immer mehr Überwachungs- und Kontrollaufgaben dezentral durchführen zu lassen.

Außerdem gewinnen in Unternehmen die Wide Area Networks (WAN) eine immer größere Bedeutung. Diese Verbindungen können aus Kostengründen oft nicht redundant ausgelegt werden. Daher benötigen die einzelnen Netzwerksegmente eine autarke Verwaltung, um auch beim Ausfall der Verbindung zur zentralen Managementstation gewisse Kontroll- und Steuerungsfunktionen ausführen zu können.

Desweiteren bieten WAN Verbindungen eine geringere Bandbreite als lokale Netze. Bei einem festen Transfervolumen an Management- Informationen werden diese Verbindungen bei einem zentralen Modell oft schon allein durch die Managementinformationen ausgelastet. Daher versucht man im dezentralen Modell möglichst viele Berechnungen und Kontrollfunktionen auf den zu überwachenden Systemen selbst auszuführen. Eine wichtige Auswirkung der geringeren Belastung der Managementstation ist die höhere Skalierbarkeit des Systems. Während in zentralen Systemen jeder Ausbau des Netzes eine große zusätzliche Belastung des Managers darstellt, kann dieser zusätzliche Aufwand beim MbD auf die lokalen Teilnetze ausgelagert werden.

3.2 Metriken für Dezentralisierung

Gérman Goldszmidt, einer der Begründer der Idee des verteilten Managements, entwickelte verschiedene Meßgrößen für die Eignung eines Netzwerkes in Bezug auf MbD. Demnach eignen sich besonders komplexe, weit ausgedehnte Netze für ein verteiltes Management.

3.3 Typische Aufgabenstellungen

Einfache Manager stellen typischerweise für verschiedene Details der zu verwaltenden Geräte Zähler bereit. Ein solcher Zähler repräsentiert die Aufsummierung einer operativen Variable. Für das Netzwerkmanagement ist diese Summe aber oft nicht besonders aussagekräftig. Viel nützlicher ist dagegen die Differenz des momentanen Zählerwerts zu einem vorherigen Wert. Auf diese Weise wird z.B. der Netzwerkdurchsatz aus der Summe der übertragenen Bytes berechnet. Eine andere typische Berechnung ist die Erstellung von Mittelwerten oder die Sortierung von Listen. Ein dezentrales Management führt solche Berechnungen auf den einzelnen verwalteten Geräten durch. Die Managementstation muß dann nur noch wenige vorberechnete Werte abfragen.

3.4 Designkriterien für dezentrales Management

Dezentrales Netzwerkmanagement orientiert sich an der Maxime, Information möglichst schon an der Quelle zu komprimieren. Darunter versteht man eine weitgehende Vorverarbeitung der Information vor Ort, um die Rechenkapazität der Managementstation und die Übertragungswege zu schonen. Dies wird durch eine dynamische Auslagerung von Berechnungen auf die zu verwaltenden Geräte erreicht.

Ein dezentraler Manager muß also die nötigen Komponenten enthalten, um eine dezentrale Ausführung der Managementaufgaben zu ermöglichen. Zusätzlich zu SNMP, das nur die Übertragung von Informationen von und zum Agenten erlaubt, müssen in einem dezentralen System auch Programmteile übertragen werden. Weiterhin werden Routinen zur Fernsteuerung dieser Programme benötigt. Diese Funktionen sollten durch leistungsfähige Authentisierungs- und Verschlüsselungssysteme abgesichert werden.

Das Verteilungsprotokoll kann dabei auf existierenden Protokollen basieren oder ein eigenständig implementiertes Modell sein. Es kann ein Manager Push Modell, ein Agent Pull Modell oder beides ermöglichen. Die Ergebnisse können gleichfalls entweder vom Agent geliefert oder von der Managementstation abgefragt werden.

Die Management-Sprache kann speziell entwickelt oder von einer existierenden Sprache abgeleitet werden. Die Sprachimplementation kann entweder in Form eines Compilers oder Interpreters erfolgen. Der Compiler kann sich entweder auf dem Agent oder auf der Management Station befinden.

Managementfunktionen benötigen üblicherweise Parameter und liefern Ergebnisse zurück. Diese können einfach strukturiert sein, wie bei einem Kommandozeilen-Interface oder komplexe Typen enthalten, die in Form einer MIB dargestellt werden. Die Aktivierung der Funktionen kann zeitgesteuert, ergeignisbasiert oder von der Managementstation ausgelöst werden.

3.5 Anwendungsbereiche des dezentralen Ansatzes

Folgende Anwendungsbereiche für dezentrales Management werden in [Gold95] genannt:

3.5.1 Verteilte Einbruchserkennung

Unter Einbruchserkennung versteht man die automatische Entdeckung von Sicherheitsverletzungen. Gegebenenfalls können sogar direkt Gegenmaßnahmen wie die Umleitung von Ports auf einen Spoofingserver eingeleitet werden.

Die Verfahren zur Erkennung von Sicherheitsverletzungen basieren auf der Annahme, daß eine Attacke aus auffindbaren Sicherheitsrelevanten Ereignissen wie Einlogversuchen, Portscans und u.a. besteht.

Die Aufzeichnung und Filterung all dieser Ereignisse kann in einem zentralen Modell zur Übertragung riesiger Datenmengen führen. Z.B. erzeugt eine Sun bei voll aktiviertem Logging 20 MB Rohdaten pro Stunde. Die Filterung einer solchen Datenmenge kann nur auf dem lokalen System mit vertretbarem Aufwand realisiert werden.

Gegenüber bisherigen Techniken erlaubt SNMP eine standardisierte Einbruchserkennung. Banning [Bann91] schlägt vor, die von einem Agenten verwalteten Objekte in einer MIB zu speichern und auf dieser einen Agenten aufzusetzen, der diese Objekte abhört, relevante Informationen herausfiltert und weiterleitet. Dieser könnte dann über ein standardisiertes Protokoll wie CMIP verwaltet werden.

3.5.2 Fernabfrage von Teilnetzen (RMON)

Die Remote Monitoring MIB stellt einen ersten Ansatz zur Dezentralisierung dar. Sie enthält Gruppen zur Überwachung verschiedener Statistiken im Segment, sowie Gruppen, um Pakete aufzunehmen und Traps auszulösen. Allerdings werden hierbei keine Skripte zur Laufzeit auf die Agenten ausgelagert, sondern nur einige feste Funktionen implementiert, die nur benutzt, aber nicht verändert werden können. RMON führt vor allem Sammlungs- und Sortierfunktionen aus, um der Managementstation die Abfrage der kompletten Tabelle zu ersparen. Beispiele für solche vorsortierten Tabellen ist die Top N Funktion. Diese erzeugt zum Beispiel eine geordnete Liste der 20 Rechner, die am häufigsten Pakete senden oder die meisten Kollisionen bzw. Übertragungsfehler verursachen.

3.5.3 Zustandsüberwachung von Teilnetzen

Die Zustandsüberwachung von Teilnetzen ist die Weiterführung des RMON Ansatzes. Die Managemenstation kann dynamisch entscheiden, in welchem Umfang die Funktionen der Zustandsberechnung auf erweiterte RMON Agenten ausgelagert werden. Diese Skalierung kann von einer reinen Abfrage der Standard RMON Variablen über eine teilweise Vorberechnung mit RMON Funktionen bis zum Laden von neuen Überwachungsfunktionen auf den RMON Agent reichen.

3.5.4 Management belasteter Netzwerke

Ein wichtiges Anwendungsgebiet ist die Verwaltung belasteter Netze. Ein Netzwerk, das am Rande seiner Leistungsfähigkeit betrieben wird, verhält sich in verschiedener Hinsicht anders als ein wenig belastetes Netz. Damit verbundene Auswirkungen sind z.B. längere Antwortzeiten, geringere Erreichbarkeit und weniger verläßliche Rückmeldungen.

Eine übliche Charakteristik einer extremen Belastung ist die Tendenz, daß Probleme, die nicht bearbeitet werden, sich ausweiten. Daher müssen Algorithmen zur Verwaltung dieser Probleme extrem schnell und akkurat reagieren, um Probleme schnell einzudämmen. Die geforderten kurzen Antwortzeiten kann nur ein lokales Programm erreichen. Im Fall einer Überlastung durch ein defektes Gerät kann die Managementstation auch oft die lokalen SNMP Agenten nicht mehr erreichen.

4 IETF Ansatz zur dezentralen Verwaltung

4.1 Entwicklung und Erweiterungen gegenüber dem klassischen SNMP

Das MbD nach IETF basiert auf SNMP und stützt sich auf die Struktur der MIB und Set bzw. Get Anfragen. Gegenüber dem klassischen SNMP enthält das MbD nach IETF einige wichtige Erweiterungen. Das Konzept der Area Agents erlaubt die lokale Ausführung beliebiger Skripte. Ein Area Agent enthält eine standardisierte MIB Erweiterung, die sogenannte Script-MIB. Diese erlaubt einer MS die Verteilung und Ausführung der Skripten auf dem Agenten.

4.1.1 Area Agents

Area Agents ermöglichen die lokale Kontrolle von Netzwerksegmenten. Sie bekommen ihre Kommandos zwar immer noch von einer zentralen MS, können dann aber selbständig Berechnungen und Abfragen durchführen. Insbesondere verringert sich durch den Einsatz von Area

Agents die Netzlast zum zentralen Skriptserver, da nur noch die Ergebnisse von umfangreichen Analysen übertragen werden müssen.

4.1.2 Script-MIB

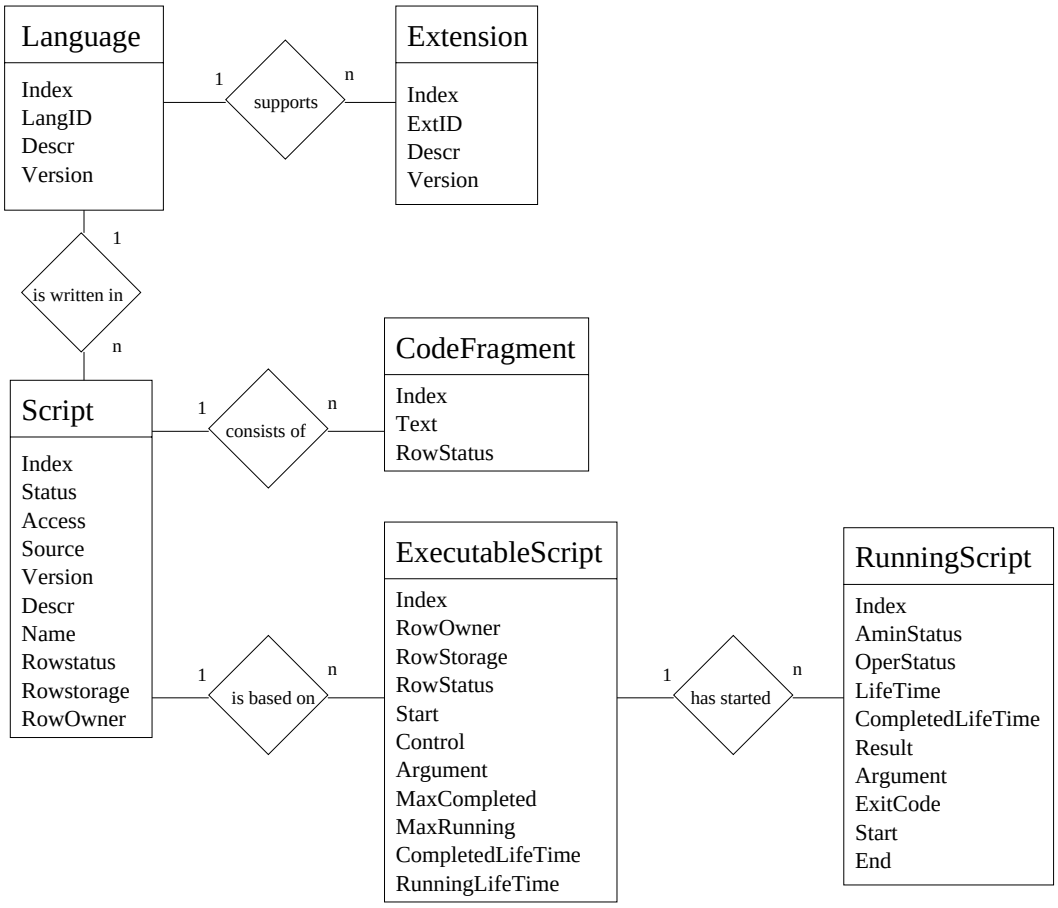

Abbildung 2: Aufbau der Script-MIB

Die Script-MIB ist das wichtigste Element des MbD nach IETF. Diese MIB wurde nach verschiedenen Kriterien erstellt. Sie sollte unabhängig von der verwendeten Skriptsprache sein. Die Script MIB sollte Versionsprobleme der Skripte vermeiden Die MIB muß SNMP MIB Schnittstellen für alle zum Verteilen der Management Skripte benötigten Funktionen beinhalten. Die Script-MIB unterstützt das Laden, Starten, Anhalten, Konfigurieren und Entfernen von Skripten.

4.2 Dienste

Für das verteilte Management wurden zusätzliche Dienste definiert :

Der Known Systems Dienst definiert eine Standard-MIB zur Abfrage und Konfiguration der Systeme, die einer verteilten Managementstation bekannt sind. Dabei kann die Liste der bekannten Systeme durch einen Entdeckungsalgorithmus oder von einem entfernten Manager erstellt werden.

Der Management Domains Dienst erlaubt, Gruppen aus der Liste der bekannten Systeme zu erstellen, auf die dann Management Operationen angewendet werden können. Der Scheduling Dienst erlaubt die Ausführung von Skripten zu bestimmten Zeiten, periodisch oder in Abhängigkeit von anderen Ereignissen.

init	Wird beim initialisieren des Skripts aufgerufen. Das Skript kann in der zugeordneten Funktion die Programmausführung vorbereiten.
start	Wird beim Aktivieren des Skripts ausgelöst.
stop	Hält den Skriptablauf an. Das Skript kann nur durch ein resume Ereignis wieder aktiviert werden. Andere Ereignisse werden ignoriert.
resume	Das Ereignis resume reaktiviert die anderen Ereignisfunktionen.
exit	Beendet den Skriptablauf. Das Skript kann hierbei noch Variablen sichern.

Tabelle 2: Ereignisse zur Steuerung des Skriptablaufs

Der Notification and Logging Dienst ermöglicht, auf das Logging und die Meldung von Ereignissen Einfluß zu nehmen.

Der Delegation Control Dienst verwaltet die Ressourcen eines verteilten Management Systems. Dadurch kann der Zugriff auf Ressourcen durch die Skripte begrenzt werden.

4.3 Ereignisgesteuerte Funktionen

Mit Hilfe der Script-MIB können Skripte auf Area Agents geladen werden.

Die Ausführung dieser Skripte erfolgt nicht automatisch, sondern ist von verschiedenen Ereignissen abhängig. Diese unterteilen sich grundsätzlich in Ereignisse, die von externen Anfragen der MS bzw. SNMP Traps ausgelöst werden und in interne Ereignisse, die durch das Kernsystem des Area Agents erzeugt werden.

Zur externen Einwirkung auf den Skriptablauf existieren fünf Ereignisse, für die das Skript Funktionen registrieren kann :

4.4 Sicherheitsüberlegungen

Die erste Version des SNMP Protokolls enthielt noch einige große Sicherheitslücken. So wurden zum Beispiel Passwörter und die gesamte Information im Klartext übertragen. Eine zweiseitige Authentisierung war ebenfalls nicht möglich.

SNMPv2 [Bann91] enthält dagegen sowohl effektive Verschlüsselung als auch Authentisierung. Auch eine bessere Festlegung der Zugriffsrechte ist nun möglich.

5 OSI Management by Delegation

5.1 Aufbau

Das OSI Management basiert im Gegensatz zum SNMP schon grundsätzlich auf dem Ansatz der verteilten Ausführung von Management-Operationen. Das zentrale Instrument zur Auslagerung von Skripten ist der Delegation Agent (DA). Diese Software regelt die Verteilung der Skripte an Elastic Server(ES) auf den zu steuernden Geräten. Das dazu verwendete Remote Delegation Protocol(RDP) unterstützt verschiedene Funktionen, um die Skripte auf

den Elastic Servern zu steuern. Sehr ähnlich zur Skript MIB Erweiterung bei SNMP sind die Funktionen zur Verteilung, Initialisierung, zum Anhalten und Fortsetzen der Ausführung und zum Beenden der Programme.

Ein auf einem Elastic Server liegendes Programm nennt sich Delegated Program(DP). Von einem DP können durch die Management Clients verschiedene Instanzen aktiviert werden, diese werden als Delegated Program Instatiations (DPI) bezeichnet.

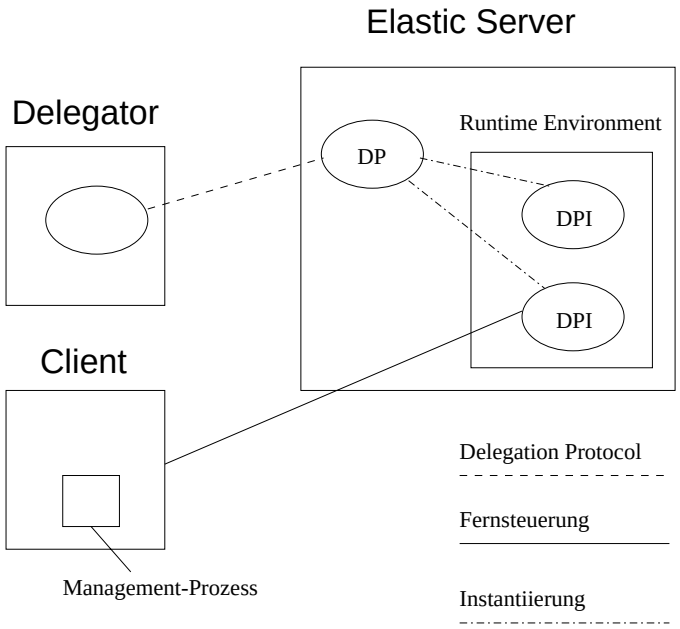

Abbildung 3: Delegation und Ausführung von Programmen

5.2 Delegated Programs

Delegated Programs können in verschiedenen Skriptsprachen aber auch in kompilierter Form auf einem Elastic Server ausgeführt werden. Aufgrund der hauptsächlich ereignisgesteuerten Ausführung werden bevorzugt objektorientierte Ansätze zur Programmierung verwendet. Die Ausführung der Programme kann völlig autonom erfolgen, um z.B. im Fall des Ausfalls der Kommunikationsverbindung zur Managementstation weiterhin die Funktionsfähigkeit des Netzes zu erhalten.

5.3 Remote Delegation Protocol (RDP)

Das Remote Delegation Protocol wird zur Verteilung und Steuerung der Delegated Programs verwendet. Die wichtigste Aufgabenstellung bei der Entwicklung des RDP war sicherzustellen, daß durch die weitreichenden Möglichkeiten des verteilten Managements keine neuen Sicherheitslücken in den zu überwachenden Netzen entstehen.

Die Möglichkeit, auf zu überwachende Geräte beliebige Programme aufzuspielen und auszuführen, würde es einem Eindringling erlauben, das Verhalten der kompletten Anlage zu verändern und damit bestehende Sicherheitskonzepte zu umgehen. Inzwischen unterstützt das Remote Delegation Protocol verschiedene Authentisierungs-Protokolle und Verschlüsselungsverfahren, um einen solchen Mißbrauch zu verhindern.

5.4 Elastic Servers

Ein Elastic Server bildet die Umgebung zur verteilten Ausführung der Management-Prozesse. Die verschiedenen Programme werden in einer multithreading Umgebung voreinander geschützt ausgeführt. Das Konzept der Elastic Servers enthält auch eine Zugriffs-Beschränkung auf die Systemfunktionen, um Skripte mit verschiedenen Sicherheitsleveln zu ermöglichen. Beschränkbare Ressourcen sind der Lese- bzw. Schreibzugriff auf Variablen, der Zugriff auf Funktionen und die maximal zugeteilte Rechenzeit.

6 Vergleich ISO und IETF Modell

6.1 Mächtigkeit und Realisierungsaufwand

Die Script-MIB ermöglicht die Ausführung von Skripten auf SNMP Agents. Allerdings können diese nicht in kompilierter Form vorliegen und unterliegen sehr beschränkten Zugriffsmöglichkeiten auf die Hardware. Die einfache Baumstruktur von SNMP erlaubt nicht die Definition komplexerer Datenstrukturen. Das MbD nach OSI erlaubt dagegen sowohl den Einsatz kompilierter Programme als auch direkten Zugriff auf die Hardware. Auch die Datenstrukturen sind weitaus flexibler und mächtiger.

Gerade durch seine beschränkte Funktionalität ist allerdings der Realisierungsaufwand bei SNMP wesentlich geringer als bei OSI MbD.

6.2 Marktbedeutung

Aufgrund seiner Einfachheit hat sich das SNMP Protokoll inzwischen trotz seiner beschränkten Fähigkeiten stark verbreitet. Inzwischen sind auch schon relativ preisgünstige Geräte, wie HUBs, mit SNMP Fähigkeiten ausgestattet und es gibt für nahezu jede Rechner-Plattform Implementierungen eines SNMP Agents.

Zu einem großen Problem haben sich allerdings die vielen herstellerspezifischen MIBs entwickelt. Es gibt keine Management-Software, die alle diese MIBs unterstützt, so daß man in verschiedenen Fällen auf die Tools des Herstellers zurückgreifen muß, um die erweiterten Fähigkeiten der Produkte zu nutzen.

Das OSI Management by Delegation ist zwar einfacher erweiterbar, jedoch verhinderte die komplizierte Grundimplementierung bisher eine größere Marktbedeutung. Es gibt keinen kompletten Manager auf OSI Basis, der sich bisher am Markt durchsetzen konnte. Allerdings existieren einige Implementierungen, die SNMP zur Ein- und Ausgabe der Prozessdaten verwendet und so die Kompatibilität zu SNMP basierten Management Systemen herstellen.

6.3 Ausblick auf die zukünftige Entwicklung

Aufgrund seiner Einfachheit wird sich SNMP weiter durchsetzen. Die wachsende Rechenleistung auch einfachster Netzwerkkomponenten ermöglicht die Implementierung von SNMP auf immer mehr Geräten. Erweiterungen wie die Skript MIB ermöglichen SNMP den Vorstoß in Netzwerksysteme, die größere Anforderungen an die Verfügbarkeit stellen. Allerdings stößt SNMP an seine Grenzen, wo Echtzeitfähigkeit gefragt ist oder sehr große Datenmengen zu bewältigen sind.

Die entstehenden Hochleistungsbackbones könnten eine Chance für das leistungsfähigere OSI Management bieten. Wo eine extrem schnelle Reaktion auf Veränderungen nötig ist, liegt

die Domäne dieses Modells. Die Einbindung des OSI MbD in bestehende SNMP Systeme ermöglicht aber auch einen problemlosen Mischbetrieb der beiden Systeme, so daß auf SNMP basierende Manager Applikationen auch weiterhin einsetzbar sind.

Vorstellbar ist so eine gewisse Aufteilung des Marktes. SNMP wird sicherlich weiterhin am Markt der preisgünstigen Netzwerksysteme dominieren. Im Bereich der großen Backbone Netze und in Echtzeit-Anwendungen ist aber eine größere Verbreitung des OSI MbD zu erwarten. Allerdings setzt dies brauchbare Implementierungen von Seite der Softwareproduzenten voraus.

Literatur

[Bann91] D. Banning. *Auditing of Distributed Systems.* In Proceedings of the 14th National Computer Security Conference, Waschington D.C. 1991.

[Gold93] Gérman Goldszmidt. *On Distributed system Management.* Computer Science Department, Columbia University, New York City, NY 10027. 1993.

[Gold95] Gérman Goldszmidt. *Decentralized Control And Intelligence In Network Management.* In Proceedings of the 4th International Smyposium on Integrated Network Management Santa Barbara. 1995.

[Gold98] Gérman Goldszmidt. *Delegated Agents for Network Management.* IBM Thomas J. Watson Research Center, Computer Science Department, Columbia University, New York City, NY 10027. 1998.

[GoYe93] Gérman Goldszmidt und Yechiam Yemini. *Evaluating Management Decisions via Delegation.* Computer Science Department, Columbia University, New York City, NY 10027. 1993.

[GoYe95] Gérman Goldszmidt und Yechiam Yemini. *Distributed Management By Delegation.* Computer Science Department, Columbia University, New York City, NY 10027. 1995.

[Kooi95] R. Kooijman. *Divide And Conquer In Network Management Using Event-Driven Network Area Agents.* 1995.

[Schö96] J. Schönwälder. *Network Management By Delegation From Research Prototypes Towards Standards.* Proceedings JENCS. 1996.

Moderne Satellitenkommunikationssysteme

Martin Dinkloh

Kurzfassung

Satellitenkommunikationssysteme waren in der Vergangenheit der Vermittlung von interkontinentalen Telefonaten und Fernsehkanälen vorbehalten, in der mobilen Telekommunikation aber lediglich in der Schifffahrt zu finden. Aktuell nehmen aber insbesondere Satellitensysteme in der Telekommunikation den Betrieb auf, die in ihrer Konzeption auf Endverbraucherpreise ausgerichtet sind, die es jedermann erschwinglich machen, an fast jedem Ort der Welt erreichbar zu sein. Die Integration in vorhandene Mobilfunknetze und stationäre Telekommunikationsnetze wird diese Systeme durch eine Senkung des Preises noch attraktiver machen. Dieser Vortrag stellt die vorhandenen und geplanten Systeme vor und erläutert Aspekte von Satellitensystemen wie Übertragungsverfahren, Bahnen und Abdeckung sowie eine Strategie der Zelleneinteilung eines Satellitensystems [Pris97].

1 Vorstellung vorhandener und geplanter Satellitenkommunikationssysteme

1.1 Charakteristika

Ein Satellitensystem besteht grob skizziert aus den Satelliten und den Bodenstationen (Earth Station, ES) bzw. Mobilen Bodenstationen (Mobile Terminal, MT). Je nach Höhe des Satelliten und seiner Bahn unterscheidet man zwischen LEO: Low Earth Orbit, MEO: Medium Earth Orbit und GEO: Geostationärer Orbit. Die Satelliten kreisen dabei auf einer oder mehreren Umlaufbahnen (Planes). Die Ellipsen dieser liegen jeweils auf einer Ebene. Die Verbindung zwischen einer Bodenstation und dem Satelliten wird Uplink, die umgekehrte Verbindung Downlink bezeichnet. Dabei kommen für die Verbindungen die Übertragungsverfahren CDMA, TDMA und FDMA in Frage, auf die in Abschnitt 2 noch näher eingegangen wird. Haben die Satelliten auch noch die Fähigkeit untereinander zu kommunizieren, so nennt man diese Verbindungen Inter Satellite Links (ISL). Den minimalen Winkel zwischen der Ebene durch den Äquator und der Ebene des Orbits wird Minimum Elevation Angle (MEA) genannt (δ in Abb. 1). Handelt es sich um einen elliptischen Orbit, so kann man die Ellipse durch die Lage des erdnächsten Punkts der Bahn beschreiben (ω in Abb. 1). Je nach Wahl des Bahnen ist es üblich, die Abdeckung in Prozent der Erdoberfläche (Coverage) oder in dem maximalen Breitengrad (Latitude Range), der noch erreicht wird, angeben. Um über stark frequentierten Gebieten das Satellitensystem effizienter auszunutzen bzw. Engpässe zu umgehen, können die Satelliten die Fähigkeit haben, ihre Antennen von den üblichen 90 Grad bezüglich ihrer Tangente auf Ballungsgebiete auszulenken (Point Antennas off Nadir, PON). In vielen Satellitensystemen spricht der einzelne Satellite nicht einfach ein ganzes Gebiet an, sondern die Abstrahlung ist in sogenannte spot-beams unterteilt, um z.B. Frequenzen in verschiedenen Ländern unterschiedlich zu nutzen zu können. Das Gebiet, daß durch einen spot-beam abgedeckt wird, nennt man footprint.

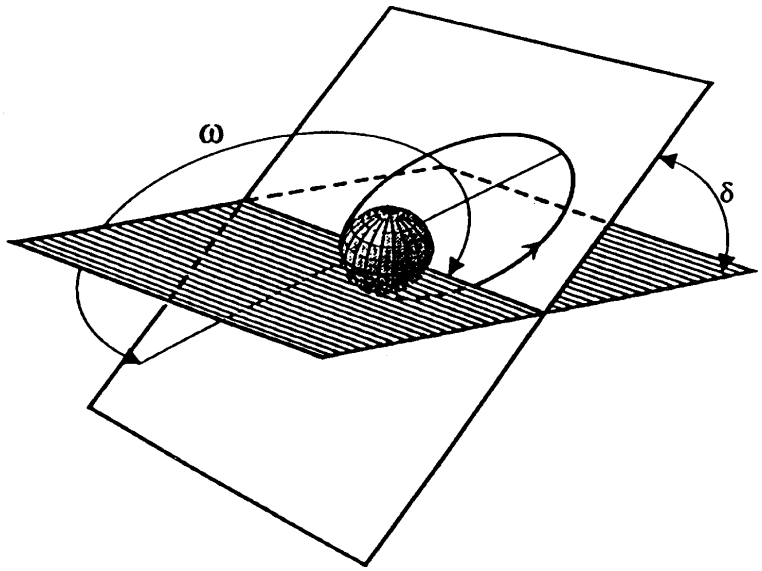

Abbildung 1: Beschreibung eines elliptischen Orbits durch Inklination und Lage des erdnächsten Punkts [ABWe95]

Die Kapazität eines Telekommunikationssatelliten wird in Gesprächsverbindungen gemessen (Capacity in Voice Circuits per Satellite, VCS). Bei Telekommunikationssystemen ist auch der angestrebte Preis für den Endkunden in US Dollar pro Minute und die angestrebte Grundgebühr interessant (Price per Minute, PPM / Base Rate, BR). Ein ganz wesentlicher Aspekt hinsichtlich des Stands der Realisierung eines Satellitensystems ist die Vergabe der nutzbaren Frequenzbänder durch die Regulierungsbehörden der verschiedenen Länder. Weiterhin spielen die Investoren, sowie die geplante Fertigstellung eine große Rolle in der Realierbarkeit und Marktstellung des jeweiligen Systems.

1.2 Gegenüberstellung geplanter und existierender Systeme [Jond98], [ABWe95], [Nico], [AbSi97]

1. *INMARSAT* (International Maritime Telecommunications Satellite Organization) Diese Satellitensysteme werden hauptsächlich zur maritimen Kommunikation eingesetzt. Angebotene Dienste sind Sprache, Daten, Telex und Fax. Nach analogen Systemen wie INMARSAT-A und digitalen wie -B und den Weiterentwicklungen hinsichtlich der Endgerätegröße -M und -C ist nun INMARSAT-3 das am weitest entwickelte System der dritten Generation dieser Reihe. INMARSAT-M verwendet eine Single Channel per Carrier Strategie mit FDMA im Uplink und TDMA im Downlink. Damit werden Übertragungsraten von 3 bis 8 kbit/s erzieht. INMARSAT-P21 ist das aktuellste Projekt der Organisation. Nach sechs verschiedenen Studien namhafter Firmen soll auch dieses Satellitensystem aus ökonomischen und technischen Gründen ein GEO-System werden.[Jond98]

2. *IRIDIUM* Mit der gleichen Anzahl von Satelliten wie die Stelle des Element Iridium im Periodensystem sollte dieses System starten. Wegen technischer Schwierigkeiten und Startschwierigkeiten der Ariane-Trägerraketen ging es letztes Jahr im August mit 66 Satelliten auf 6 statt auf 7 polaren Kreisbahnen in 780 km Höhe in Betrieb. Es ist als Ergänzung zu terrestrischen Mobilfunknetzen gedacht und nutzt das Band bei 1,6 GHz sowohl im FDMA-Verfahren als Uplink, als auch im TDMA-Verfahren als Downlink. Die Vermittlung der Gespräche kann sowohl über ESs als auch über ISLs bei 23 GHz erfolgen. Angebotene Dienste sind Telephonie, Daten, Fax und RDSS (Radio Determination Satellite Services: Positionsbestimmung).

3. *ODYSSEY* Die angebotenen Dienste sind die gleichen wie bei Iridium, während dieses MEO-System allerdings mit nur 12 Satelliten auf 4 Bahnen auskommt. Es arbeitet massiv mit der Steuerbarkeit der Satellitenantennen, um die Footprints stationär zu halten. Wie auch Inmarsat-P21 und Iridium ist Odyssey als Ergänzung terrestrischer Netze gedacht. Die Verbindung zum MT erfolgt im L- und S-Band über CDMA, während die 10 bis 11 ESs bei 20/30 GHz arbeiten.

4. *GLOBALSTAR* Die Dienste sind wieder identisch zu den vorgenannten MSSs. Wie auch Odyssey arbeitet dieses LEO/ICO-System im L- und S-Band Über CDMA, allerdings kommuniziert es bei 6,5 GHz Uplink und 5,2 GHz Downlink mit den ESs.

5. *TELEDESIC* Hinter diesem Namen verbirgt sich ein Projekt, daß den Rahmen der bisherigen MSS mit dem ungefähr doppelten Etat bei weitem sprengt. Es bietet auf ATM Basis Vielfache von einzelnen Kanälen von 16 kbit/s bis zu 2 Mbit/s. Für sogenannte Gigalink-Terminals stehen auch Kanäle von 155 Mbit/s bis zu 1,2 Gbit/s zur Verfügung. Die möglichen Dienste sind vielfältig und nicht genau spezifiziert, sie decken jedoch den Rahmen der bisherigen Systeme komplett ab. Das System nutzt 21 Kreisbahnen in einer Höhe von ca. 700 km, auf denen sich je 40 in Betrieb befindliche und 4 Ersatz-Satelliten befinden. Mit über 800 gleichzeitig im Orbit befindlichen Satelliten stellt dieses System eine neue Generation von MSS dar. Die Orbits verlaufen über die Polkappen und sind sonnensynchron, ihre Bahnen haben relativ zur Sonne einen konstanten Winkel. Die Vermittlung erfolgt paketorientiert an Bord der Satelliten, diese werden zunächst über ISLs an einen der 8 benachbarten Satelliten über den vermutlich kürzesten Weg zum Ziel befördern. Das Protokoll ist verbindungslos, so daß verschiedene Pakete verschiedene Wege durch das Netz nehmen können. Diese müssen dann vom Empfänger in der richtigen Reihenfolge wieder zusammengesetzt werden. Die Pakete werden zum Schutz vor unerwünschtem Mithören auf Paketbasis verschlüsselt. Die Sendeleistung wird dynamisch den Witterungsbedingungen angepaßt. Da die Satelliten sich sehr schnell bezüglich der Erdoberfläche bewegen und daher ständig ein Zellenwechsel erforderlich wäre, arbeitet das System mit festen Zellen auf der Erdoberfläche. Die Erdoberfläche ist in 160 km breite Quadrate, sogenannte Superzellen aufgeteilt, von denen es ca. 20 000 zur Abdeckung der Erdoberfläche bedarf. Diese sind weiterhin in je 9 Zellen aufgeteilt. Die Zellen bilden Bänder parallel zum Äquator. Das Zugriffsverfahren ist ein kombiniertes. Die Zellen einer Superzelle werden periodisch gescannt und damit einem von 9 Zeitschlitzen zugeteilt (SDMA, Raummultiplex). Alle Satelliten des Systems sind so synchronisiert, daß die Zellen n ($n = 1, 2, ..., 9$) gleichzeitig abgetastet werden. Ebenso senden alle Terminals zur gleichen Zeit zum Satelliten, wenn dieser eben ihre Zelle abtastet. Die Interferenz mit benachbarten Zellen wird durch abwechselnde links- und rechtsseite Polarisation des Signals vermieden. Innerhalb des Zeitschlitzes erfolgt die Übertragung über den Uplink in FDMA und über den Downlink in TDMA (Abschnitt 2.2.

2 Übertragungsverfahren für Vielfachzugriff [Jond98], [uH.-97], [MaBo98]

Bei der Übertragung zwischen Bodenstation und Satellit finden verschiedene Übertragungsverfahren Verwendung, die den Zugriff mehrerer Stationen auf den gleichen Satelliten ermöglichen. Die Empfangs- und Sendeeinheit eines Satelliten ist in mehrere Kanäle, die sogenannten Transpondern, eingeteilt. Bei der Betrachtung des Vielfachzugriffs muß also im folgenden zwischen dem Vielfachzugriff auf die Empfangseinheit und den Vielfachzugriff auf den Transponder unterschieden werden.

Name	Odyssey	Globalstar	Iridium	Teledesic	Inmarsat-P
No. of ES		100-210			
No. of S.	12	48	66	840-924	10
Services	Tel., Data, Pag., RDSS	Tel., RT-Data, Pag., Pos.	Tel., Data, Pag., Pos.	High Bandwidth Data, Tel.	Tel., Fax, Data, Pag. Pos.
No. Circ./S.	2800	2700	4000	2500	5300
Type	MEO	LEO	LEO	LEO	MEO
Planes	3	8	6	21	2
Inklination	55°	52°	86°	98.2°	45°
Feeder Up	Ka	FDM			
Feeder Down	FDMA, Ka	FDMA			
Mobile Up	CDMA	CDMA	TDMA/FDMA	S/FDMA, Ka	FDM/TDMA
Mobile Down	CDMA, S	CDMA	TDMA/FDMA	S/ATDMA, Ka	FDM/TDMA
ISL	-	-	4	8	-
Coverage	100%	100%/25 – 50°	100%	100%	
Min. El.	20°	20°	8°	40°	20°
Path Div.	-	3			
Min. No. S. in View	2			2	
PON	+		+	+	
Rate	$0.7	$0.65 + terr. Geb.	$3 + terr. Geb.	k.a.	$2
Base Rate	$29	$20	$50	k.a.	
Cost of System	$1800 Mio.	$1600 Mio.	$3400 Mio.	$9000 Mio.	
Completion	1998	1997 (USA) / 1998 (global)	1998	2001	1999/2000
Payload	Transparent	Transparent	Regenerativ	Regenerativ (ATM)	Transparent
Organisation	TRW	Loral Qualcomm	Iridium Inc. / Motorola	Teledesic Corp.	Inmarsat

Tabelle 1: Vorhandene und geplante Satellitensysteme im Vergleich

Grundsätzlich läuft die Funkübertragung der Daten durch Modulierung des Datensignals auf ein Trägersignal. Um mehrere Signale möglichst zur gleichen Zeit über das gleiche Medium zu übermitteln, gibt es nun zwei Routingstrategien:

1. Der Satellit kann nun einer Sendestation bei der Weiterleitung ihrer Daten für jede Verbindung einen neuer Träger zur Verfügung stellen (One carrier per link, OCL) oder aber

2. der gleiche Träger für alle Verbindungen dieser Sendestation verwendet werden (One carrier per transmitting station, OCTS).

2.1 Frequenzmultiplex (FDMA)

Beim Frequenzmultiplex-Verfahren läuft die Übertragung der Daten durch die Modulierung des Signals auf mehrere Trägerfrequenzen ab. Das von jedem dieser Kanäle benutze Frequenzband wird von den anderen Kanälen durch ein Schutzband (guard band) getrennt. Hierdurch werden Ungenauigkeiten in Oszillatoren und Filtern ausgeglichen.

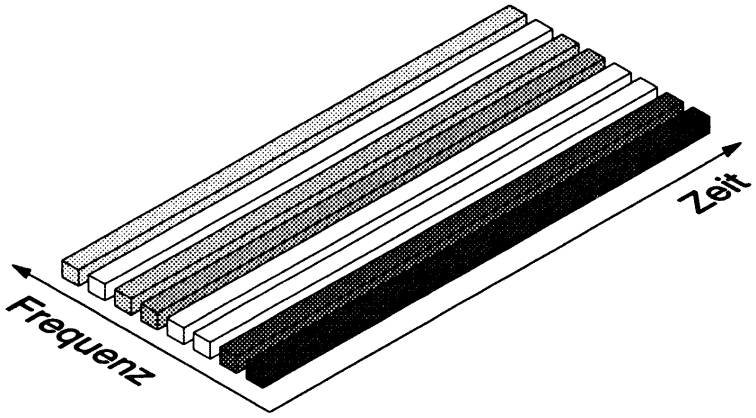

Abbildung 2: Frequenzmultiplex (FDMA) [Jond98]

Gängige Übertragungsschemata bei Frequenzmultiplexsystemen sind

- FDM/FM Wird bei analogen Signalen zumeist verwendet. Diese Signale werden mittels Frequenzmultiplex (Frequency Division Multiplex FDM) zu einem Signal zusammengefaßt und mit Frequenzmodulation (FM) auf eine Trägerfrequenz moduliert. Da hier von der sendenden Station alle Signale am Ende auf einen einzigen Träger moduliert werden, handelt es sich um die Routingstrategie OCTS.
- TDM/PSK Die Signal sind hierbei digital und können daher leicht per Zeitmultiplex (Time Division Multiplex TDM) zusammengefaßt werden. Dieses Signal moduliert schließlich mittels Phasenumtastung (Phase Shift Keying PSK) die Trägerfrequenz. Auch hier handelt es sich um die Routingstrategie OCTS.
- SCPC (Single Channel per Carrier) Jedes Eingangssignal wird auf einen anderen Träger moduliert. Die Routingstrategie ist hier OCPS.

Wird ein FDMA-kodiertes Signal verstärkt, so entstehen neben den gewünschten Frequenzen in dem „Frequenzgemisch“ auch ungewünschte Intermodulationsprodukte, welche eine Linearkombination der anderen Frequenzen sind. Die Summe der Faktoren wird Ordnung genannt. Ist das Verhältnis zwischen dem Frequenzbereich des verstärkten Bandes und dessen mittlerer Frequenz hoch, so fallen nur Intermodulationsprodukte ungerader Ordnung an.

2.2 Zeitmultiplex (TDMA)

Zu einem bestimmten Zeitpunkt sendet immer nur eine Station, d.h. der Träger belegt den Kanal exklusiv. Um trotzdem über eine längere Zeit hinweg mehrere Stationen bedienen zu können, senden die Stationen abwechselnd. Die Aussendungen bezeichnet man als Bursts. Diese werden zu einer periodischen Struktur, dem Rahmen, zusammengefaßt. Bei der Routingstrategie „ein Träger pro Verbindung“ mit N Stationen im System sendet jede Station

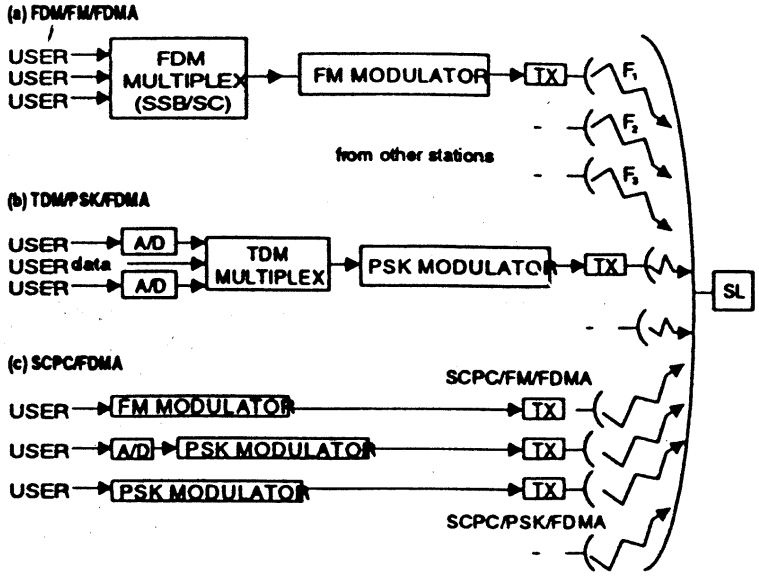

Abbildung 3: FDMA Übertragungsschemata [uH.-97]

also N-1 Bursts. In einen Rahmen fallen in diesem Fall also $P = N(N-1)$ Bursts. Bei „ein Träger pro Station“ ist $P = N$.

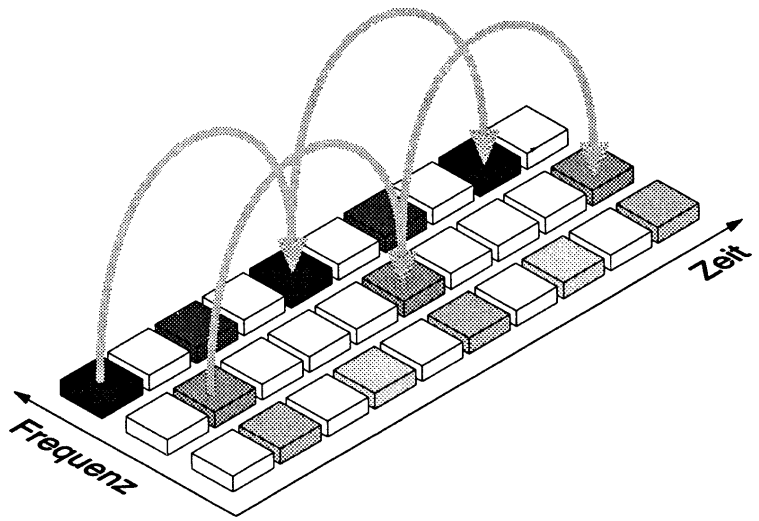

Abbildung 4: Zeitmultiplex (TDMA) [uH.-97]

Die Signale müssen von der sendenden Station also jeweils für maximal eine Rahmenlänge gepuffert werden. Daher resultiert, daß dieses Verfahren vornehmlich für digitale Signale geeignet ist, da die Pufferung hier sehr einfach ist. Bei analogen Signalen ist dies nicht ohne weiteres möglich. Weiterer Nachteile von TDMA sind die Tatsache, daß um Synchronisationsungenauigkeiten auszugleichen, Schutzzeiten zwischen den Bursts eingefügt werden müssen. Außerdem muß es zur Synchronisation mindestens eine, besser zwei Referenzstationen geben, die Referenzbursts aussenden. Der Durchsatz ist mit typischerweise über 80% sehr hoch und bleibt dies auch bei großer Netzteilnehmerzahl. Da immer nur ein Träger gleichzeitig auf dem Kanal ausgesendet wird, entfallen auch die bei FDMA störenden Intermodulationsprodukte. Da der Träger immer auf der gleichen Frequenz bleibt, ist die Abstimmung von Sender und Empfänger auch sehr leicht. Diese Vorteile werden sich durch die Erforderlichkeit einer Syn-

chronisation des Systems und die Notwendigkeit der Fähigkeit, hohe Bitraten zu verarbeiten, erkauft.

2.3 Codemultiplex (CDMA)

Bei CDMA wird das Frequenzband von allen Stationen gleichzeitig verwendet. Die Unterscheidung der verschiedenen Sender geschieht mit Hilfe einer sogenannten Signatur. Da ein im Vergleich eine zu z.B. FDMA stark vergrößerter Frequenzbereich benötigt wird, spricht man auch von Bandspreizübertragung (Spread Spectrum Transmission).

Es werden zwei verschiedene Techniken beim Zugriff auf das Übertragungsmedium benutzt:

2.3.1 Direct Sequence Spread Spectrum (DSSS)

Hierbei wird die zu übertragende Bitfolge m(t) mit einer zweiten Bitfolge p(t) (Signatur) multiplikativ verknüpft und mit PSK auf den allen Stationen gemeinsamen Träger moduliert. Das dabei entstandene Signal ist

$s(t) = m(t) * p(t) * cos(\omega_C) * \dot{t}$

Da p(t) NRZ-kodiert ist und daher nur die Werte +-1 annehmen kann, ist das Signal leicht durch Multiplikation des phasenrichtigen p(t) zurückzugewinnen

$x(t) = m(t) * p^2(t) = m(t)$

Um gegen Störungen wie Mehrwegeausbreitung und Interferenz mit anderen Systemen geschützt zu sein, ist es wichtig, daß die Signatur günstige Korrelationseigenschaften besitzt. Sie muß gegenüber zeitverschobenen Versionen und allen anderen benutzten Signaturen leicht unterscheidbar sein.

2.3.2 Frequency Hopping (FH)

Das FH arbeitet mit einem Träger, dessen Frequenz von einem Synthesizer erzeugt wird, der durch einen binären Code gesteuert wird. Auf der Empfangsseite wird das Signal durch Multiplikation mit dem Träger wieder demoduliert. Hierbei ist eine gute Synchronisation zwischen Sender und Empfänger erforderlich. Je nach Verhältnis zwischen Sprung- und Bitrate spricht man von Slow und Fast Hopping.

2.3.3 Vor- und Nachteile

Ein CDMA-System hat einen mit ca. 10% sehr geringen Durchsatz, der durch die hohe Störsicherheit durch die Bandspreizung erkauft wird. Synchronisation muß nur auf die Signatur erfolgen, nicht aber direkt zwischen den Stationen, dadurch ist das Netz einfach zu betreiben.

3 Bahnen und Abdeckung

Die Umlaufbahnen werden abhängig von der Höhe und der Postition bezüglich des Äquators in folgende Klassen eingeteilt.

Den Bereich zwischen 2.000 und 6.000 km ist einer der beiden Van-Allen Gürtel. Der zweite liegt im Bereich 15.000 bis 30.000 km, wie auch in Bild 6 zu sehen. Es sind Bereiche mit einer so hohen Dichte von stark-geladenen Partikeln, daß die Elektronik von Satelliten Schaden nehmen würde. Diese Gürtel entstehen durch die Interaktion von Partikel aus dem Solarwind mit dem elektromagnetischen Feld der Erde. [MaBo98]

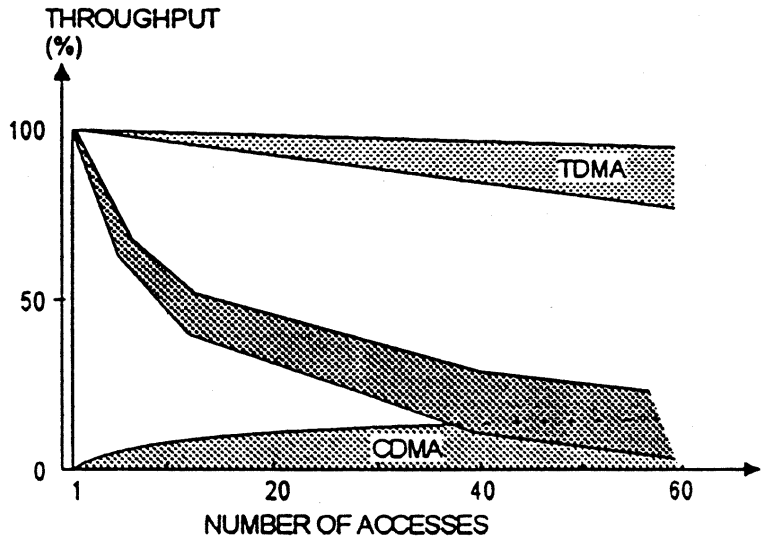

Abbildung 5: Vergleich des Durchsatzes bei TDMA, FDMA und CDMA [Jond98]

Bez.	Höhe Über Erdoberfläche	Bemerkungen
GEO	Geostationary Orbit, d.h. direkt über dem Äquator. In 35786 km beträgt die Dauer eines Erdumlaufes genau 24 Stunden, d.h. der Satellit bewegt sich relativ zu einem Punkt auf der Erdoberfläche nicht.	Ausleuchtungswinkel nur bis zum 50. Breitengrad. Drei Satelliten genügen für eine komplette Erdabdeckung.
LEO	Low Earth Orbit, 700–2.000km	Mehrere Satelliten sind nötig, da sie sich zeitweise außerhalb der Reichweite des Senders am Boden befindet. Je niedriger die Bahnhöhe, desto mehr Satelliten werden benötigt.
MEO	Medium Earth Orbit, 6.000-20.000km	
ICO	Intermediate Circular Orbit	
HEO	Highly Elliptical Orbit	

4 Zelleneinteilung und -wahl (Ansatz von F.D. Priscoli) [Pris97]

Eine Zelle nenne ich im folgenden passend zu einem MT, wenn in dem Aufenthaltsbereich des MT die Empfangskriterien des Systems erfüllt sind. Alle Satellitensysteme, ebenso wie Mobilfunksysteme, sprechen das MT zunächst mit Hilfe eines Broadcast-Channels an, also eines Kanals, den zunächst jedes MT in der Zelle empfängt. Es gibt also eine eindeutige Beziehung zwischen Zelle und Broadcast-Channel. Nach einem Zellenwechsel muß also eine Zellen-Neuwahl erfolgen (cell reselection). Das Wechseln des Kanals eines MTs während eines Gesprächs nennt man ein Handover.

Ein weiterer Begriff ist der des Aufenthaltsorts (location area) eines MT. Hiermit ist der Bereich gemeint, in dem sich ein MT frei bewegen kann, ohne seinen Aufenthaltsort dem System neu mitteilen zu müssen. Eine location area kann aus mehreren Zellen bestehen. Liegt ein Gespräch für ein MT vor, so muß das System das MT in allen Zellen der location area suchen (paging), man muß also zwischen des Aufwands eines location updates und des Aufwands des pagings abwägen. Dafür ist eine intelligente Aufteilung des Abdeckungsgebietes eines Satellitensystems in Zellen wichtig, um cell reselection, paging und handover effizient zu halten.

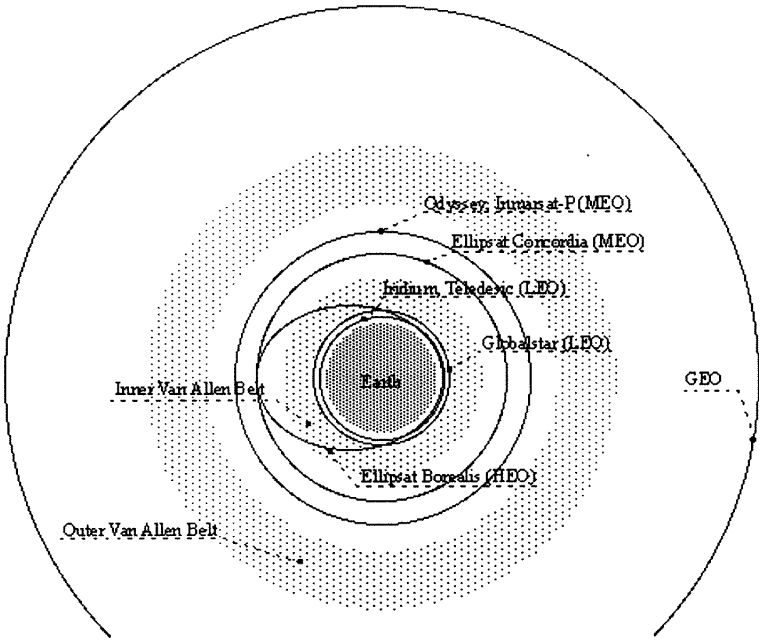

Abbildung 6: Orbits und Van-Allen Gürtel [Nico]

Im folgenden betrachten wir ein Satellitensystem mit N ESs und M spot-beams. i sei der Index für die ESs und j der für die spot-beams. Da sich zu einem Zeitpunkt t mehrere ES in einem spot-beam aufhalten können, ist eine Zelle nicht allein durch den spot-beam, sondern erst durch ein Paar (i, j) identifiziert. Dabei ist j die ES, die den broadcast-channel für die Zelle ausstrahlt. Sei jetzt $C(i, j, t)$ eine binäre Funktion, die zu einem Zeitpunkt t angibt, ob ES i in spot-beam j liegt. Analog sei $B(i, j, t)$ eine binären Funktion, die angibt, ob ES i zum Zeitpunkt t tatsächlich mit spot-beam j verbunden ist. Es gilt also

$$B(i, j, t) \leq C(i, j, t) \tag{14}$$

Die Funktion C ist vorgegeben, B kann durch das System gewählt werden und beschreibt damit die Zelleneinteilung des Systems. Weiterhin seien $C_{sat}(t)$, $C_{ES}(i, t)$ und $C_{spot}(j, t)$ die Anzahl der Zellen im gesamten System, die Anzahl der Zellen, die eine ES zum Zeitpunkt t bedienen muß und die Anzahl der Zellen im spot-beam j zum Zeitpunkt t. Damit gilt

$$B(i, j, t) \leq C(i, j, t) \tag{15}$$

$$C_{sat}(t) = \sum_{i=1}^{N} B(i, j, t) \tag{16}$$

$$C_{ES}(i, t) = \sum_{j=1}^{M} B(i, j, t) \tag{17}$$

$$C_{spot}(j, t) = \sum_{i=1}^{N} B(i, j, t) \tag{18}$$

Sei nun $A(j, t)$ das Gebiet auf der Erdoberfläche, daß vom spot-beam j zum Zeitpunkt t abgedeckt wird. $A_{potential}(i, t)$ sei das Gebiet, daß von der ES i potentiell abgedeckt werden könnte. Dieses ergibt sich aus der Vereinigung aller $A(j, t)$. Analog sei A_{actual} der Bereich, den eine ES tatsächlich abdeckt und A_{target} der Bereich, den sie versucht abzudecken. Für diese Werte gilt

$$A_{potential}(i,t) = \bigcup_{j=1}^{M} A(j,t)C(i,j,t) \tag{19}$$

$$A_{actual}(i,t) = \bigcup_{j=1}^{M} A(j,t)B(i,j,t) \tag{20}$$

$$A_{target}(i,t) \subseteq \bigcup_{j=1}^{M} A(j,t)B(i,j,t) \tag{21}$$

$$A_{potential}(i,t) \supseteq A_{target}(i,t) \tag{22}$$

Gleichung 19 und 20 gelten nach Definition, Gleichung 21 folgt aus der Voraussetzung, daß das Zielgebiet nicht die tatsächliche Abdeckungsgebietgröße überschreiten darf und Gleichung 22 folgt aus 15, 19 und 20.

Daraus folgt, daß die Funktionen $C(i,j,t)$ und $A(j,t)$ sowie $A_{potential}$ Charakteristiken des betrachteten Satellitensystems sind, die mit Hilfe von Daten wie des Orbits, der Payload des Satelliten und den Positionen der Earth Stations berechnet werden können. Die ES mössen dann ihr gewünschtes Abdeckungsgebiet wählen mit den Einschränkungen von Gleichung 22 und anderen Kriterien. Die Zellenaufteilung $B(i,j,t)$ kann sodann aus der Gleichung 21 berechnet werden.

5 Ausblick

Mit Iridium ist erstmals ein attraktives Angebot im Universal Telecommunication Mobile System-Markt seit Ende letzten Jahres im Handel, deren Endgeräte sich der Größe von denen terrestrischer Mobilfunkgeräte annähern. Die Entwicklung wird sich immer mehr zu immer komplexeren LEO-Systemen mit immer mehr Satelliten und Inter Satellite Links bewegen. Hierbei wird die Datenübertragung auch eine sehr große Rolle spielen, wie man an dem sehr ehrgeizigen Projekt Teledesic (Abschnitt 5) erkennen kann. Dennoch zeigt die Verzögerung des Starts von Iridium im letzten Jahr, daß es noch technische Schwierigkeiten bei diesen Systemen gibt. Dies zeigt auch die Entscheidung der Inmarsat Organisation, ihr neuestes System, Inmarsat-P, als MEO auszulegen. (Abschnitt 1)

Literatur

[AbSi97] Farrokh Abrishamkar und Zoran Siveski. PCS Global Mobile Satellites. *IEEE Communications Magazine*, September 1997, S. 132–136.

[ABWe95] A. Jahn A. Böttcher und M. Werner. Mobile Satellitenkommunikation – Grundlagen und Orbits Teil 1–3. *Gateway*, April, Mai, June 1995.

[AkJe97] Ian F. Akyildiz und Seong-Ho Jeong. Satellite ATM Networks: A Survey. *IEEE Communications Magazine*, July 1997, S. 30–42.

[AnVa95] F. Ananasso und F. Vatalaro (Hrsg.). *Mobile and Personal Satellite Communications*. Springer, 1995.

[Auth] Verschiedene Authoren. Small Satellites Home Page, http://www.ee.surrey.ac.uk/CSER/UOSAT/SSHP/. Technischer Bericht.

[Helb96] Dieter Helbig. Satellitenfunk – Eine Einführung in Technik und Betrieb bei der Deutschen Telekom. *Telekom Unterrichtsblätter*, 1996, S. 460–479.

[Jond98] Friedrich K. Jondral. Folien und Mitschrift zur Vorlesung „Satellitenkommunikation“. 1998.

[MaBo98] G. Maral und M. Bousquet. *Satellite Communications Systems*. Wiley. 1998.

[Nico] Th. Nicolay. Review of Big LEO Systems. Technischer Bericht.

[Pris97] Francesco Delli Priscoli. Functional Areas for Adanced Mobile Satellite Systems. *IEEE Personal Communications*, December 1997, S. 34–40.

[Seid96] Lawrence P Seidman. Satellites for Wideband Access. *IEEE Communications Magazine*, October 1996, S. 108–111.

[uH.-97] J. Eiberspächer und H.-J. Vogel. *GSM – Global System for Mobile Communication*. Teubner. 1997.

Sichere Mobilkommunikation im Internet - Trend in Mobile IP

Christoph Weser

Kurzfassung

Aufgrund der Forderung nach mobilen Rechnersystemen, mußte die Spezifikation des Internet Protocols, kurz IP, erweitert werden. Diese Erweiterung heißt Mobile IP und wurde bereits als Standard verabschiedet. In der nachfolgenden Arbeit werden die Problematik die hinter diesem Gebiet stehen, die Funktionsweise von Mobile IP, sowie die Sicherheitsaspekte, die gerade bei mobilen Knoten, wie z.B. Datenübertragungen über Funkstrecken, besonders wichtig sind, aufgezeigt und erklärt. Zum Schluß werden noch die wesentlichen Unterschiede zwischen IPv4, dem Internet Protocol Version 4, der den aktuellen Standard darstellt und IPv6, dem bereits verabschiedeten neuen Standard des Internet Protokolls in der Version 6 aufgezeigt.

1 Problematik der mobilen Kommunikation

Die Forderung nach Mobilität wird in unserer globalisierten Welt immer wichtiger. [Huit96] Dies zeigt schon allein die ständig wachsende Zahl der Laptops, Palmtops und Mobiltelefone. Die auf das IP-Protokoll aufsetzende Erweiterung *Mobile IP*, die durch die *RFC 2002* [Perk96a] spezifizert wurde, soll nun gewährleisten, daß man z.B. mit dem Internet mittels Laptop und Funkmodem verbunden bleiben kann, während man sich aber physikalisch an einen anderen Ort bewegt. Diese Erweiterung wurde notwendig, da normales IP diesen Service nicht bietet. So hat ein Rechner im normalen IP-Protokoll eine feste Adresse, die sogenannte IP-Adresse. Man geht davon aus, daß sich der Computer gar nicht bzw. nur sehr selten physikalisch bewegt, und sich so immer im gleichen Subnetz aufhält. In diesem ist er auch ständig über eben diese IP-Adresse zu erreichen und die für ihn bestimmten Pakete können leicht an ihn *geroutet* werden. Bewegt sich der Rechner, so kann er unter Umständen sein Subnetz verlassen und ist deshalb auch nicht mehr über seine feste IP-Adresse zu erreichen, und ein *Routing* wird unmöglich. Dies eben doch möglich zu machen, ist die Aufgabe der *Mobile IP*-Erweiterung, sodaß die Pakete an seinen aktuellen Aufenthaltsort transparent für den Sender weitergeleitet werden. Die Einsatzgebiete ergeben sich natürlich klar für diejenigen Menschen, die ständig unterwegs sind, wie Manager, Vertreter, usw. Selbstverständlich soll das Routing möglichst effizient sein und dabei auch so sicher wie möglich. Wie dies bewerkstelligt werden kann, wird im folgenden näher erläutert.

2 Funktionsweise

Jeder mobile Rechner *(Mobile Host, MH)* hat eine feste IP-Adresse. Alle Pakete, die für ihn bestimmt sind, laufen direkt an ihn, solange er sich in seinem Heimatnetzwerk *(Home Network, HN)* aufhält. Ist nun aber der *MH* unterwegs, so wird der Heimatagent *(Home Agent, HA)* für dessen Pakete verantwortlich. Er muß dafür Sorge tragen, daß der *MH* die für ihn bestimmten Pakte auch erhält, und muß diese an ihn weiterleiten. Hierfür werden jedoch eine ganze Reihe Protokolle benötigt, die im folgenden erklärt werden.

So wird das *Agent Discovery Protocol* benötigt, welches auf dem *MH* implementiert ist. Dieses Protokoll lokalisiert Agenten, die *Mobile IP Support* zur Verfügung stellen. Jeder Agent schickt sogenannte *Advertisements* weg, in denen er allen mitteilt, welche Dienste er zur Verfügung stellt, also ob er als Heimatagent, als Fremdagent *(Foreign Agent, FA)*, oder als beides dienen kann. Ein *MH* fängt eben diese *Advertisements* mittels des *Agent Discovery Protocols* ab und kann anhand derer feststellen, ob er sich noch im gleichen Netz befindet, ob er in einem neuen Subnetz ist, oder ob er wieder in sein *HN* zurückgekehrt ist. Befindet er sich in einem neuen Netz, so kann er versuchen, sich bei eben diesem Host, von dem er ein *Advertisement* empfangen hat, zu registrieren. Empfängt er selbst keine *Advertisements*, so schickt er selbst welche aus, um einen Agenten zu finden, bei dem er sich registrieren kann. Findet er auch auf diesem Weg keinen *FA*, so stellt diese Subnetz keine *Mobile IP*-Unterstützung zur Verfügung.

Ist der *MH* fündig geworden, wird ein weiteres Protokoll benötigt, das *Registration Protocol*. Dieses Protokoll ermöglicht es dem *HA* herauszufinden, wo sich der *MH* gerade befindet, aber es ermöglicht auch dem *FA* herauszufinden, ob er dem *MH* in seinem Subnetz Zugang gewähren soll. Der *MH* muß sich nun mittels einer *Registration Request message* registrieren. Mit dieser schickt er seine *Care-of-Address (CoA)*, welche üblicherweise die Adresse des *FA* ist, direkt an den *HA*. Anstatt die *Registration Request message* direkt an den *HA* zu schicken, kann auch der Weg über den *FA* gewählt werden, der dann wiederum die Nachricht an den *HA* weiterleiten muß, wie dies in Abbildung 1 dargestellt ist. Hiernach weiß der *HA*, wo sich der *MH* befindet. Nun schickt der *HA* eine *Registration Reply message* an den *FA*, in der alle wichtigen Informationen, wie z.B. die Lebensdauer der Registrierung, usw. stehen. Dieser wiederum schickt diese *Registration Reply message* an den *MH*, damit dieser weiß, daß die Registrierung komplett ist. Von nun an, kann der *HA* Pakete, die für den *MH* bestimmt sind, an den *FA*, bei dem der *MH* gerade registriert ist, weiterleiten, und dieser wiederum leitet sie an den *MH* weiter. Diese Verbindung nennt man *Mobility Binding*. Jedoch ist zu beachten, daß eine solche Registrierung nur eine ganz bestimmte Zeit gültig ist. Ist diese Zeit überschritten, ohne daß die Registrierung erneuert wurde, so hat er *MH* keinen Zugriff mehr auf das Netz des *FA*. Man benutzt einen solchen *Timeout* deshalb, damit die Registrierungstabellen eines *FA* einigermaßen aktuell bleiben, falls ein *MH* das Netz verläßt, ohne sich ordnungsgemäß abzumelden.

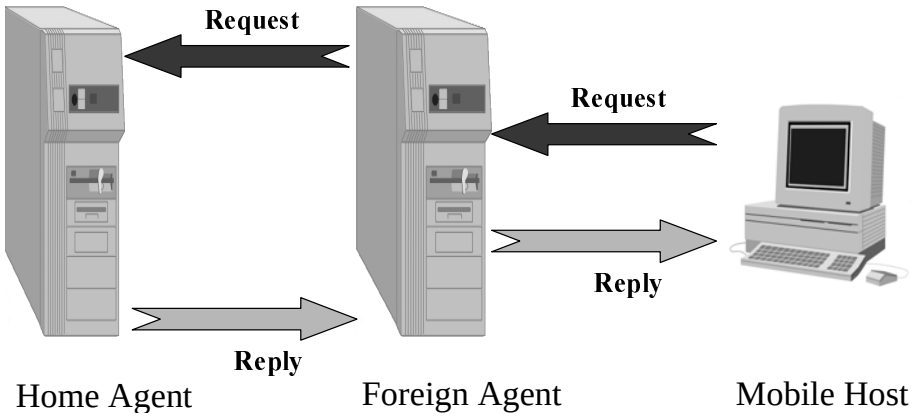

Abbildung 1: Ablauf der Registrierung eines *MH*

Ist nun die Registrierung geglückt, so kann mit der eigentlichen Datenübertragung begonnen werden. Fängt also ein *HA* nun ein Paket ab, das für den *MH*, der gerade unterwegs ist, bestimmt ist, sieht dieser in seinen Tabellen nach, wo sich der *MH* gerade befindet. In diesen Tabellen steht die *CoA*, unter der der *MH* zu erreichen ist. Nun wird das ganze Paket mittels *IP-in-IP* in ein anderes Paket, das an den, für den *MH* zuständigen *FA* adressiert ist, eingekapselt und an diesen übermittelt. Die genaue Funktionsweise von *IP-in-IP* [Perk96b] wird im weiteren Verlauf anhand der Abbildung 4 erläutert. Das zu übermittelnde Paket wird einfach

als *Payload* in einem neuen IP-Paket verschickt. Der Aufbau der *IP-Header* sind im großen und ganzen gleich, außer daß im äußeren Paket ein Flag gesetzt ist, an dem sich erkennen läßt, daß der *Payload* ein gekapseltes Paket ist. Der *FA* entkapselt nun dieses Paket und kann dann das ursprüngliche Paket an den *MH* weiterleiten. Dieses Verfahren der Einkapselung ist für den Sender vollkommen transparent. Die Pakete vom *MH* zurück zum korrespondierenden Rechner *(Correspondent Node, CN)* werden auf direktem Wege zwischen beiden ausgetauscht, ohne daß irgendein Agent benötigt wird. Als Absender trägt das Pakte vom *MH* dessen feste IP-Adresse.

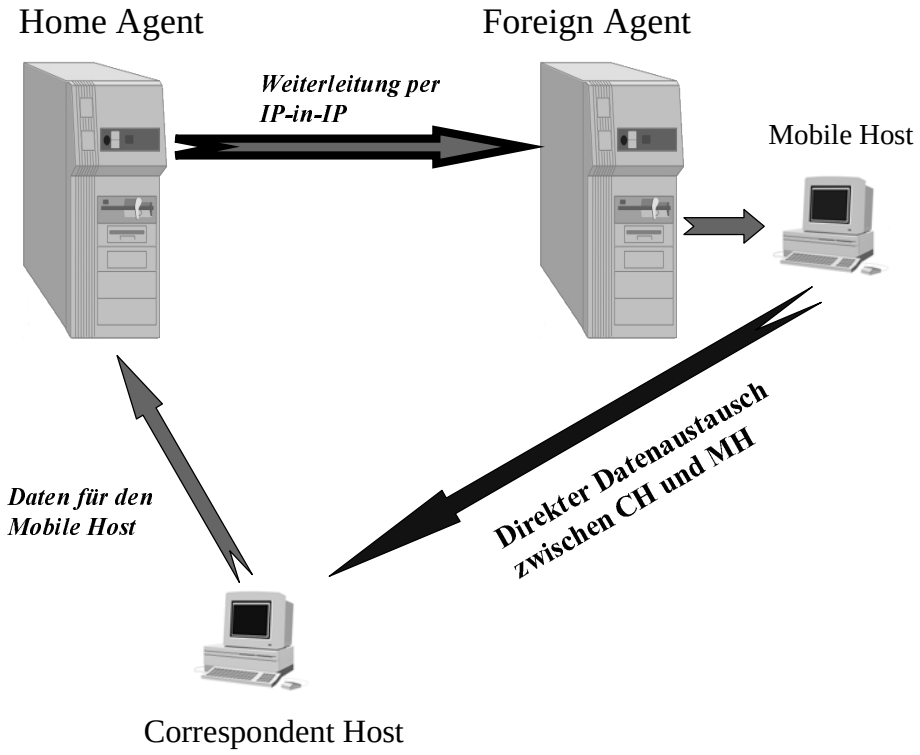

Abbildung 2: Datenfluß bei der Übertragung zum *MH*

3 Optimierung dieses Ablaufs

Ursprünglich war *Mobile IP* dazu gedacht, die Daten immer auf die gleiche Weise, also einem festen Pfad folgend, weiterzuleiten. Aber was ist, wenn sich der *MH* zufällig im gleichen Subnetz aufhält wie der *CN*, also der Rechner, der dem *MH* etwas schicken will?

Hier würde das herkömmliche Verfahren bei weitem mehr Netzlast erzeugen, als eigentlich nötig wäre, da die gesamten Daten zuerst an den *HA* des *MH* gehen würden und erst von dort an den *FA* weitergeleitet werden würden. Der komplette Datentransfer zwischen *HA* und *FA* stellt also einen vermeidbaren *Overhead* dar, gegen den die *Optimization Messages* vernachlässigbar gering sind. Um solchen zusätzlichen Aufwand zu vermeiden, wurden die *Route Optimization Extensions* eingeführt. Mit diesen Erweiterungen werden vier Nachrichtentypen zur Verfügung gestellt, mit denen das Routing optimiert werden kann. Durch diese neuen Nachrichten erhält der *CN* direkt Auskunft darüber, wo sich der *MH* gerade aufhält, und kann somit die für den *MH* bestimmten Pakete direkt per *IP-in-IP* tunneln, ohne den Umweg über den *HA* machen zu müssen.

Will also ein *CN* an einen *MH* etwas senden, so schickt er als erstes einen *Binding Request* an den *HA* des *MH*. Dieser teilt ihm dann die Informationen über den augenblicklichen Aufenthaltsort des *MH* mit. Diese Mitteilung des *HA* wird *Binding Update message* genannt.

Es ist aber auch möglich, daß der *HA* dem *CN* von sich aus eine solche Mitteilung schickt, und zwar nachdem der *HA* das erste Paket, das für einen *MH* bestimmt ist, abgefangen hat. Hiermit versucht er also, sich selbst zu entlasten. Genauso können die *Binding Updates* auch dazu eingesetzt werden, um den *FA* eines *MH* über dessen Umzug zu informieren, damit der *FA* seine Listen aktualisieren kann und nicht auf einen Timeout warten muß. Dies ist aber optional. Diese Updates müssen natürlich auch gesichert werden, da sich sonst ein Angreifer einen Zugang erschleichen könnte, indem er ein *Binding Update* fälscht, und so einen Umzug vortäuscht. Nun bekommt der Angreifer die für den *MH* bestimmten Pakete, da nach dem Update ja zu dem neuen Aufenthaltsort *geroutet* wird. Ein weiterer Nachrichtenyp ist die *Binding Acknowledge message*. Diese Nachricht hat den Zweck, den Erhalt eines *Binding Updates* zu bestätigen. Sie wird aber nur dann verschickt, wenn die *Binding Update message* dies explizit erfordert. Der vierte und letzte Nachrichtentyp für die Optimierungen ist die *Binding Warning message*. Sie wird nur in Implementierungen mit *IPv4* benötigt. Sie werden verschickt, falls ein Knoten eine unzulässige Bindung entdeckt. Solche Meldungen werden vom *FA* oder aber auch von anderen Knoten verschickt, aber nie vom *CN*. So kann z.B. ein Knoten, den ein nicht für ihn bestimmtes Paket erhält, das aber seine Adresse trägt, eine solche Meldung verschicken. Sie sagt dann dem *HA* des *MH*, das ein Knoten versucht eben diesen zu erreichen, aber das nicht kann. Es kann aber auch sein, daß der für einen *MH* zuständigen *FA* eine solche Meldung an den *HA* des *MH* verschickt, um ihn darüber in Kenntnis zu setzen, daß der *MH* nun das Netz des *FA* verlassen wird bzw. dies schon getan hat. Auch diese Meldungen sind optional und erfordern keinerlei Bestätigung des *HA*. So kann ein Knoten, der diese Meldung verschickt hat höchstens erneut eine solche Meldung verschicken, falls ihn weiterhin falsche Pakete erreichen. Hierzu siehe auch [ADSc97]

Zwischen den Implementierungen dieser Erweiterung von *IPv4* und *IPv6* gibt es einige Unterschiede. So gibt es in *IPv6* keine *Binding Warning message*, da der *MH* den *CN* selbst über seine Bewegungen informiert, indem er die Meldung selbst verschickt und nicht mehr wie bei *IPv4* durch den *HA* des *MH*. Bei *IPv4* muß der *CN* einfach dem *HA* glauben, daß der jeweilige *MH* umgezogen ist. Näheres zu *IPv6* findet sich in Abschnitt 5.

Aber egal ob *IPv4* oder *IPv6*: Durch diese Optimierungserweiterungen wird die Netzlast ganz immens verringert.

4 Sicherheitsaspekte

4.1 Sicherheitsproblematik

In den meisten Fällen passiert ein Paket auf seinem Weg zum Empfänger eine Vielzahl von Knoten, die das Paket weiterleiten. Jeder dieser „Verteilerknoten“ stellt einen möglichen Angriffspunkt dar. Dies kann das Mitlesen der Daten (passiver Angriff) sein, oder aber auch das Manipulieren der Daten (aktiver Angriff). Dies soll natürlich weitestgehend vermieden werden. Beim *Mobile IP* kommt noch eine weitere Forderung hinzu: Es soll unmöglich gemacht werden, mittels einer Verkehrsflußanalyse ein sog. Bewegungsprofil des *MH* zu erstellen. So kann man also zusammenfassend von sechs Anforderungen sprechen, die an die Sicherheit des *Mobile IP* gestellt werden.

- Integrität (*Integrity*)

  Es soll unmöglich sein, ein Paket so verändern, ohne daß dies der Empfänger bemerkt. Bemerkt er dies, kann er das Paket verwerfen und es nochmals anfordern.

- Authentizität (*Authentication*)

  Es soll festzustellen sein, daß der angegebene Sender auch der tatsächliche Sender war.

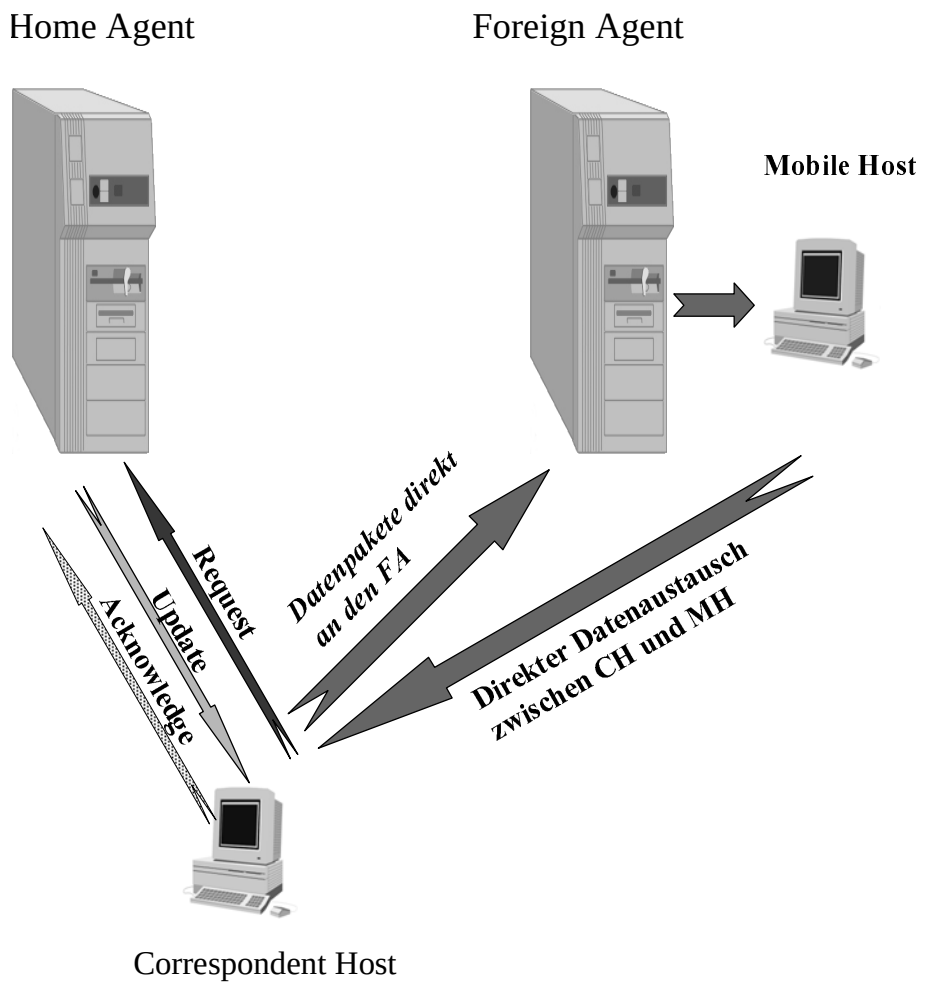

Abbildung 3: Datenfluß der Optimierungsnachrichten

- Vertraulichkeit (*Confidentiality*)

  Es soll nur dem Sender und dem Empfänger, aber keinem der dazwischen liegenden Knoten möglich sein, die übertragenen Daten zu lesen.

- Nicht-Zurückweisbarkeit (*Non-Repudiation*)

  Es soll garantiert werden, daß der Sender nicht leugnen kann, die Daten gesendet zu haben.

- Bewegungsprofil durch Verkehrsanalyse (*Traffic Analysis*)

  Die Erstellung eines eben solchen soll unmöglich gemacht werden.

- Rückspielsicherung (*Replay Protection*)

  Es soll unterbunden werden, daß abgefangene Registrierungen wiederverwendet werden können. Wird eine Registrierung als solche erkannt, so soll sie verworfen werden.

4.2 Sicherung der Registrierung

Beim *Mobile IP* bietet schon die Registrierung des *MH* bei seinem *HA* den ersten Angriffspunkt, da ein Angreifer die Registrierung abfangen könnte, und sich selbst als *MH* anmelden könnte. Ist der Angriff gut durchgeführt, leitet der Angreifer alles an den echten *MH* weiter,

und dieser würde, abgesehen von einer kleinen Verzögerung, nicht mal bemerken, daß er angegriffen wird. Also muß auch die Registrierung auf jeden fall authentifiziert werden, wie dies in [Perk96a] gefordert wird. Vor der Registrierung wird in einer *Mobile Security Association* festgelegt, welche Parameter zur Sicherung verwendet werden sollen. Diese Vereinbarung wird zwischen dem *HA*, dem *FA* und dem *MH* getroffen. Folgende Parameter müssen ausgehandelt werden.

- IP-Adresse
- SPI (*Security Parameter Index*)

  Dies ist eine 4 Byte lange Zufallszahl. Zusammen mit der IP-Adresse identifiziert sie eine *Security Association*, die zwischen zwei Knoten getroffen wurde, eindeutig. Nur wenn jede Authentisierungsnachricht zwischen zwei Knoten diese sorgfältig gewählte Zufallszahl enthält, wird die Nachricht akzeptiert.
- Algorithmustyp

  Hier gibt es zwei Möglichkeiten, die in [Schw97] angesprochen werden. Zum einen ist es möglich, MD5 zu verwenden, bei dem es einen geheimen Schlüssel gibt, der über die *Security Association* spezifiziert wird. Besser aber ist ein asymetrisches Verfahren, wie z.B. das RSA-Verfahren von Rivest, Shamir und Adleman, das einen geheimen und einen öffentlichen Schlüssel benützt.
- Modus (präfix/suffix)
- Schlüssel
- Rückspielsicherung

  Dies wird durch Zeitstempel (*Time Stamps*) und Einmalwerte, sog. *nonces*, realisiert. Die genaue Vorgehensweise muß hier ausgehandelt werden, damit beide Knoten darin absolut übereinstimmen und es zu keinen Mißinterpretationen kommt. Näheres dazu in Abschnitt 4.2.1 und in Abschnitt 4.2.2.

Durch die drei Erweiterungen *Mobile-Home-Authentication*, *Mobile-Foreign-Authentication* und *Foreign-Home-Authentication* wird dies, wie im folgenden gezeigt wird, erreicht. Je nach Kommunikationsweg wird die *Mobile-Home-Authentication*, die *Mobile-Foreign-Authentication* oder die *Foreign-Home-Authentication* an die Registrierungsnachricht angehängt. Der Empfänger überprüft dann die Erweiterung auf ihre Richtigkeit. Bei der Registrierung errechnet der *FA* aus der *Mobile-Foreign-Authentication* die *Foreign-Home-Authentication*. Die *Mobile- Home-Authentication* darf vom *FA* nicht verändert werden.

Wie oben genannt, werden für die Rückspielsicherung Zeitstempel und Einmalwerte benutzt, wobei die Verwendung von Einmalwerten optional ist.

4.2.1 Rückspielsicherung durch Zeitstempel

Damit diese Methode funktionieren kann, müssen natürlich die Systemuhren der miteinander kommunizierenden Systeme synchronisiert sein. Werden Zeitstempel verwendet, so ist auch eine Länge von 64 Bit für das Identifikationsfeld der Authentisierungsnachricht verbindlich. Die unteren 32 Bit des Identifikationsfeldes werden mit dem Zeitstempel gefüllt. Die oberen 32 Bit werden mit einer Zufallszahl gefüllt. Der Wert des Identifikationsfeldes muß nach [Perk96a] grösser sein, als der Wert des vorhergehenden Feldes, da er als Sequenznummer dient. Ist der Wert grösser, und der Zeitstempel nur wenig älter als der aktuelle Wert, so ist die Registrierung in Ordnung, und der *HA* kopiert das Identifikationsfeld einfach in das Reply. Ist es jedoch nicht in Ordnung, werden nur die unteren 32 Bit kopiert und in die oberen 32 Bit wird der aktuelle Zeitstempel eingefügt. Hier erhält der Reply, der vom *HA* verschickt wird, einen Fehlerrcode.

4.2.2 Rückspielsicherung durch Einmalwerte (*nonces*)

Hierbei nimmt der Sender A eine Zufallszahl als Einmalwert, welche aber generell unterschiedlich zu vorher bereits verwendeten Werten ist, und sendet diesen Einmalwert in seinen Nachrichten an den Empfänger B mit. Die Registrierung kann nur dann gültig sein, falls bei der Antwort wieder der gleiche Einmalwert von B an A zurückgeschickt wird. Gleichzeitig kann aber auch B an A seinen eigenen Einmalwert mitschicken, um so die Sicherheit zu haben, daß A überhaupt neue Nachrichten empfängt. Da beide Meldungen durch Authentisierungscodes geschützt sind, können sie auch sicher sein, daß die Meldungen nicht verändert wurden. Der *HA* kopiert jeweils die unteren 32 Bit des *Requests* in den *Reply* und generiert die oberen 32 Bit neu. Der *MH* wiederum, der den *Reply* empfängt, kopiert die oberen 32 Bit aus der Nachricht, um diese beim nächsten *Request* wieder einzufügen. Er generiert dann die unteren 32 Bit neu.

4.3 Sicherung der IP-Pakete

Da nun die Registrierung durch diesen Sicherheitsmechanismus gesichert wird, kann es nach geglückter Registrierung zum eigentlichen Datenaustausch durch *IP-in-IP* kommen. Für die genaue Spezifikation der Einkapselung mittels *IP-in-IP* wende man sich an die unter [Perk96b] aufgeführte RFC.

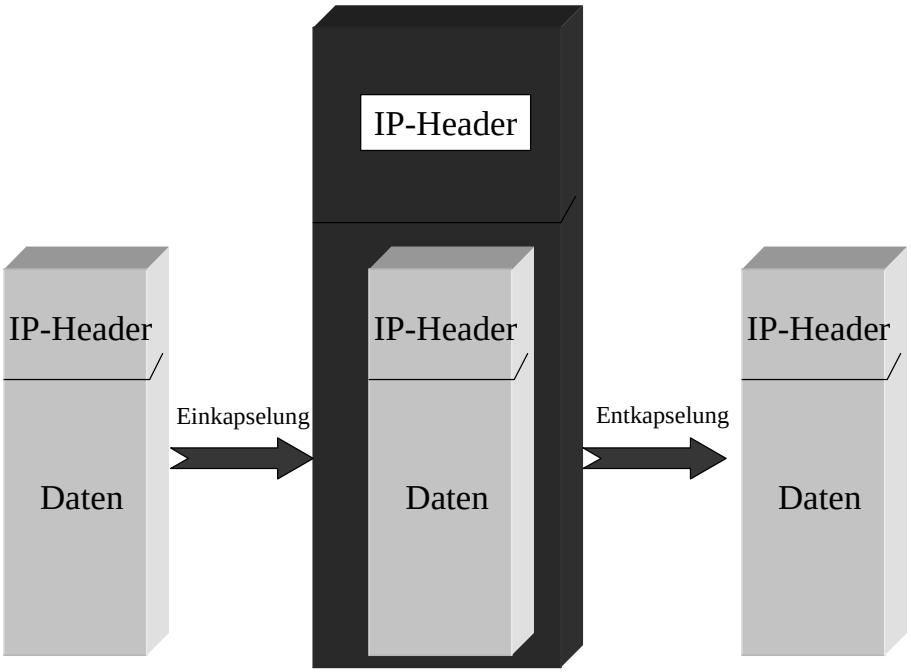

Abbildung 4: Einkapselung eines IP-Paketes

Aber auch hier muß vor der Datenübertragung eine *Security Association* ausgehandelt werden, die im grossen und ganzen der *Mobile Security Association* entspricht, ausser, daß hier keine Rückspielsicherung nötig ist, aber dafür zusätzlich folgende Punkte vereinbart werden müssen:

- Lebensdauer der Schlüssel

  Wie lange die Schlüssel eine Gültigkeit besitzen, bevor sie erneuert werden müssen.

- Lebensdauer der *Security Association*

  Wie lange die *Security Association* gilt.

- Sicherheitsstufe

  Ist die Nachricht streng geheim, geheim, oder nicht näher klassifiziert?

Für die Sicherung der IP-Pakete werden zwei besondere Header definiert: den *Authentication-Header* und den *Encapsulation Security Payload-Header*, kurz *ESP-Header*. Der *Authentication-Header* ist für die Zusicherung der Authentisierung und der Integrität zuständig. Der *ESP-Header* ist auch für die Zusicherung der Integrität, aber vor allem für die Zusicherung der Vertraulichkeit zuständig.

4.3.1 Authentication-Header

Der *Authentication-Header* steht im Protokollkopf direkt hinter dem *IP-Header*.

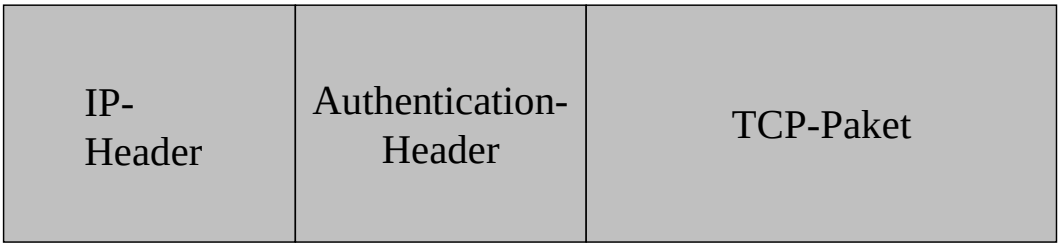

Abbildung 5: Plazierung des *Authentication-Headers*

Mittels des MD5-Algorithmus im Präfix und Suffix-Modus wird die Integrität und Authentisierung gewährleistet. Dieser Algorithmus berechnet einen bestimmten 128-bit *message digest* aus dem geheimen Schlüssel und dem gesamten IP-Paket. Hieraus ergibt sich ein einmaliger, individueller Fingerabdruck, der im Authentisierungsfeld des *Authentication-Headers* abgelegt wird. Kommt nun dieses Paket beim Empfänger an, errechnet dieser ebenfalls diesen Fingerabdruck, da er ja auch über den geheimen Schlüssel verfügt, der in der *Security Association* ausgehandelt wurde. Nur wenn beide Fingerabdrücke identisch sind, ist die Integrität und die Authentisierung voll gewährleistet. Felder, die während des Transportes ihren Wert ändern, wie z.B. das *TTL-Feld*, das bei jedem „Verteiler“ um eins erniedrigt wird, werden vor der Berechnung auf Null gesetzt, damit sie nicht das Ergebnis verfälschen können. Wird anstelle des MD5-Algorithmus sogar ein asymetrisches Verschlüsselungsverfahren verwendet, die z.B. der RSA-Algorithmus, so läßt sich im *Authentication-Header* sogar die Nicht-Zurückweisbarkeit realisieren, da hier der Sender die Nachricht mit seinem geheimen Schlüssel signiert, den ja nur er kennt. Schutz der Vertraulichkeit und vor einer Verkehrsflussanalyse bietet aber dieser Header nicht.

4.3.2 Encapsulation Security Payload-Header

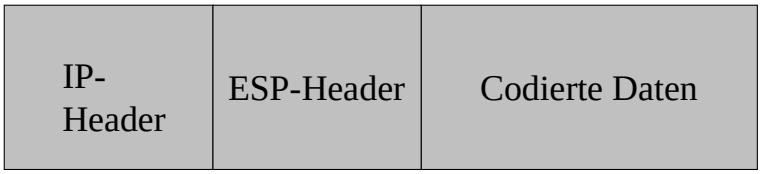

Abbildung 6: Plazierung des *ESP-Header*

Durch diesen Header wird die Vertraulichkeit garantiert, da das komplette Paket verschlüsselt wird. Vor dieses verschlüsselte Paket wird ein *ESP-Header* gestellt, der selbst zu einem Teil

verschlüsselt ist. Näheres über die Verschlüsselung durch den *ESP-Header* läßt sich in [Schw97] nachlesen. Wiederum davor wird ein neuer *IP-Header gestellt*, der nur die Quelladresse und die Zieladresse enthält, also im Normalfall die Adresse des *HA* und die des *FA*. Vorteil dabei ist natürlich, daß ein Angreifer zwar den Datenfluß zwischen *FA* und *HA* abhören kann, er aber nicht weiß, daß das eigentliche Paket für den *MH* bestimmt ist, da es für ihn wie eine ganz normale Übertragung zwischen *FA* und *HA* aussieht; d.h., daß dieser Header auch einen Schutz vor einer Flußanalyse darstellt.

5 Änderungen in *IPv6* nach [Perk97]

Mit *IPv6* kommt die nächste Version des IP-Protokolls, welche die alte Version *IPv4* in absehbarer Zeit ablösen wird. Dieses neue Protokoll wurde im Dezember 1998 in einer RFC verabschiedet. *IPv6* wartet mit einer ganzen Menge Verbesserungen und Neuerungen im Gegensatz zu *IPv4* auf, wie z.B.:

- Der Adreßraum wurde von 32 Bit auf 128 Bit vergrößert.
- Erweiterungen für die Authentisierung und Datenintegrität werden nun direkt im IP-Header bereitgestellt.
- Der Mobilitätssupport ist bereits Bestandteil von *IPv6*. Was dies für Auswirkungen im allgemeinen Ablauf hat, wird im folgenden kurz dargelegt.

Für die komplette Spezifikation wende man sich an [Deer98].

Der prinzipielle Ablauf, also daß der *HA* die für den *MH* bestimmten Pakete an den *FA* weiterleitet, bleibt auch bei *IPv6* der gleiche. Auch wird sich bei der Einkaspelung der Pakete vom *HA* zur *CoA* des *MH* nicht viel ändern.

Neu ist, daß der *MH* die Möglichkeit hat, eine eigene *CoA* zu bekommen, was dazu führt, daß der *FA* unnötig wird, und so folglich aus dem Protokoll für *IPv6* gestrichen wurde.

Desweiteren werden die *Binding Update messages* unnötig, da bei *IPv6* durch die neu eingeführten *Destination options* diese Informationen gleich jedem Paket direkt mitgegeben werden können. Dies setzt nicht die Performance herab, da diese *Destination options* nur direkt vom Empfänger, und nicht von den dazwischen liegenden Routern ausgewertet werden. Dadurch wird also der durch die ganzen *Binding Update messages* entstandener Overhead vollständig eliminiert. Weiß ein *CN* noch nichts von einem Update, so wird das Paket im *HN* eingekapselt und an den *MH* weitergeleitet. Dieser verpackt dann das Update in das nächste Datenpaket an den *CN*. Natürlich müssen auch bei *IPv6* diese Updates authentisiert werden. Dies geschieht aber automatisch, da sowieso jedes *IPv6*-Paket einen *Authentication-Header* besitzt. Ausserdem ist bei *IPv6* ein mobiler Knoten der einzige, der solche Updates verschicken darf.

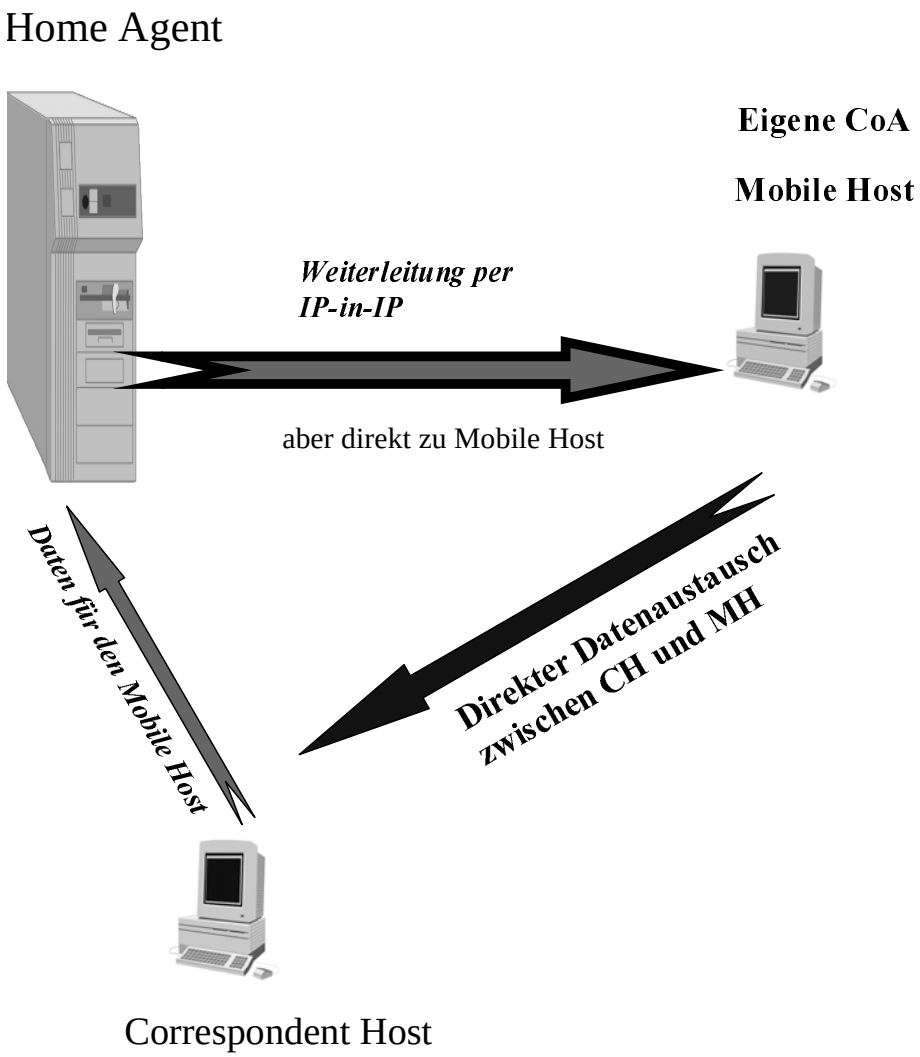

Abbildung 7: Datenfluß bei der Übertragung mittels *IPv6P*

Literatur

[ADSc97] Jody Crawford Allison Dailey, Angela Adams und Jeffery Schilling. Mobile IP. http://www.seas.upenn.edu/ jlc/MobileIP.html, 1997.

[Deer98] S. Deering (Hrsg.). Request for Comments: 2460 - Internet Protocol, Version 6. Standards track, Network Working Group, 1998.

[Huit96] Christina Huitema. *Routing im Internet*. Prentice Hall. 1996.

[Perk96a] C. Perkins (Hrsg.). Request for Comments: 2002 - IP Mobility Support. Standards track, Network Working Group, 1996.

[Perk96b] C. Perkins (Hrsg.). Request for Comments: 2003 - IP Encapsulation in IP. Standards track, Network Working Group, 1996.

[Perk97] Charles E. Perkins. Mobile IP. *IEEE Communications Magazine*, Marz 1997.

[Schw97] Silke Schwaas. IP, 1997.

[Thom96] Norbert Diehl und Alexander Schill Thomas Ziegert. Mobile IP: Ueberblick und Systemvergleich. *PIK*, 1996.

Drahtloses ATM - Handover und Routing

Mark Arnold

Kurzfassung

Drahtloses ATM stellt eine Technologie dar, die die normale ATM-Technik um Faktoren zur drahtlosen und mobilen Funkkommunikation erweitert. Dabei werden Dienstqualitätsparameter, die für normale ATM-Verbindungen festgelegt werden können, übernommen. Der mobile Rechner ist dabei per Funk über eine Basisstation an das ATM-Netz angebunden. Vor allem zur Gewährleistung der Mobilität sind einige Probleme zu lösen, so ist etwa bei den Routingverfahren sicherzustellen, daß die Verbindung aufgebaut werden kann, egal wo sich der mobile Rechner gerade befindet. Handover (der Wechsel der Basisstationen) müssen durchgeführt werden, ohne daß Übermittlungsfehler, Datenverluste oder Reihenfolgeverletzungen auftreten oder gar die Verbindung abbricht. Spezielle Protokolle übernehmen dieses Aufgaben.

1 Einleitung

1.1 Was ist drahtloses ATM?

Drahtloses ATM ("wireless ATM" – WATM) ist eine Erweiterung der Hochleistungskommunikationstechnologie ATM (*asynchronous transfer mode*) dahingehend, daß die Kommunikationspartner nicht statisch an einem Netzzugangspunkt angeschlossen sein müssen, sondern mobil sein können. Das heißt, die Netzteilnehmer können sich – in gewissen Grenzen, die beispielsweise durch die Funkabdeckung gegeben sind – frei bewegen und trotzdem per Funk über ATM-Netze kommunizieren.

WATM kann sowohl zum Transfer von Daten als auch für zeit- und leistungskritische Übertragungen wie etwa Sprache oder Video in Echtzeit für Videokonferenzen benutzt werden und bietet – wie ATM – hohe Datenraten und Dienstqualitätszusicherungen (Quality-of-Service – QoS).

1.2 Argumente für drahtloses ATM

Die großen Chancen dieser Technologie liegen vor allem darin begründet, daß sie keine komplett neue Technik darstellt, sondern auf eine bereits verbreitete Technologie – nämlich ATM – aufsetzt und diese um mobilkommunikationsspezifische Funktionen erweitert. Die Vorzüge von ATM, wie etwa die hohe Datenrate oder Dienstqualitätsgarantieen sind damit auch im drahtlosen ATM wiederzufinden. Die Hochleistungskommunikationstechnologie ATM wird beispielsweise zur Realisierung von B-ISDN eingesetzt.

Die Tatsache, daß Multimedia immer gefragter wird und durch WATM multimediale Kommunikation nicht mehr nur zu Hause im Wohnzimer, sondern auch unterwegs stattfinden kann, ist ein weiterer Pluspunkt für WATM. Da bereits bestehende Mobilfunknetze bei weitem nicht

die für Multimedia-Anwendungen benötigte Bandbreite erbringen, ist hier eine neue Technologie wie WATM erforderlich.

Ein Beispiel für die Nachfrage nach Mobilkommunikationstechnologieen ist beispielsweise der überall sichtbare "Handyboom".

2 Grundlagen

2.1 Die Technik des ATM

2.1.1 Das Übertragungsmedium

ATM ist eine verbindungsorientierte Übertragungsart, das heißt, zu Beginn der Kommunikation wird eine Verbindung aufgebaut, über die alle Daten dieser Kommunikationssitzung geleitet werden; ist die Sitzung beendet, wird die Verbindung wieder abgebaut. In ATM wird eine solche Verbindung durch sogenannte *virtuelle Kanäle* ("virtual channels" – VC) realisiert, über die die Daten unidirektional übertragen werden. Mehrere solcher Kanäle werden zwischen den einzelnen Netzknoten zu sogenannten *virtuellen Pfaden* ("virtual paths" – VP) zusammengefasst. Diese Kanäle und Pfade werden anhand eines *virtual channel identifiers* (VCI) bzw. *virtual path identifier* (VPI) identifiziert (siehe auch Abb.1). Im Gegensatz zu anderen verbindungsorientierten Protokollen werden die Daten jedoch nicht als Datenstrom Bit für Bit übertragen, sondern in Zellen zusammengefasst und so in kleinen Häppchen gesendet. Eine Zelle besteht dabei aus 53 Byte (5 Byte Zellkopf, 48 Byte Nutzdaten). Eine Zelle wird einer bestimmten Verbindung zugeordnet, indem in ihrem Zellkopf der VPI und VCI des zur Verbindung gehörenden Kanals bzw. Pfades eingetragen wird.

Die Zellen werden auf das Medium (z.B. Glasfaserkabel) "gemultiplext", d.h. die Zellen aller virtuellen Kanäle (bestehnde Verbindungen) werden in einem Puffer gesammelt und der Reihe nach übertragen. Ist der Puffer leer, d.h. sind gerade keine Daten zu übertragen, so werden besonders gekennzeichnete Leerzellen übertragen. Die Asynchronität bezieht sich bei ATM nicht auf die Signalübertragung, sondern auf die Zellen. So werden Zellen, die zu einer bestimmten Anwendung gehören, je nach Verkehrssituation nicht periodisch, sondern ohne bestimmten Rhythmus abwechselnd ($\Rightarrow$ asynchron) mit Zellen anderer Verbindungen übertragen. Der Zellstrom auf dem Medium ist aber synchron, was bei einem Leerlauf durch die Leerzellen erreicht wird.

Die Übertragung von Daten in Zellen fester Länge macht eine relativ einfache Hardwarearchitektur der Netzknoten möglich, was neben dem Verzicht auf aufwendige Fehlerkorrekturmaßnahmen auf der Hardwareebene den hohen Datendurchsatz von ATM (155 Mbit/s bis zu 2,4 GBit/s) ermöglicht.

2.1.2 Wesentliche Eigenschaften von ATM

ATM unterstützt verschiedene Arten von Daten. Es können sowohl zeitunkritische Daten – wie etwa Dateien – übertragen werden, als auch zeitkritische Daten für Audio- oder Videoübertragungen. ATM stellt dazu verschiedene Dienstklassen bereit, die nach der Art der zu übertragenden Daten aufgeteilt sind:

- *AAL-1*: Daten mit konstanter Bitrate, zeitkritisch. Bsp.: unkomprimierte Sprache/Video
- *AAL-2*: Daten mit variabler Bitrate, zeitkritisch. Bsp.: komprimierte Audio-/Videodaten

- *AAL-3/4*: Daten mit variabler Bitrate, zeitunkritisch, Fehlererkennung. Bsp.: Dateien
- *AAL-5*: Daten mit variabler Bitrate, zeitunkritisch, keine Fehlererkennung ⇒ höherer Durchsatz als AAL-3/4. Bsp.: Dateien

Diese unterschiedlichen Dienstklassen stellen unterschiedliche Anforderungen bezüglich Durchsatz, Bandbreite und andere Kriterien an das Netz. Damit diese Anforderungen eingehalten werden und eine Anwendung auch die benötigte Übertragungseigenschaften bekommt, existieren bei ATM verschiedene Qualitätsparameter (Quality-of-Service-Parameter). Diese Qualitätskriterien werden beim Verbindungsaufbau festgelegt und für die Dauer der Verbindung zugesichert. Solche Qualitätskriterien sind:

- *Cell Transfer Delay*: Verzögerungszeit zwischen Abschicken und Ankunft einer Zelle. Setzt sich aus Codierungszeit, Zeit zum Packen der Zelle, Übertragungszeit, Schaltzeit der Netzknoten, Pufferverzögerung und ähnlichen Verzögerungen zusammen.
- *Cell Delay Variation*: auch Jitter genannt. Die Varianz zwischen den verschiedenen Verzögerungszeiten der einzelnen Zellen.
- *Cell Loss Ratio*: Zellverlustrate; Verhältnis der verlorenen oder verworfenen Zellen zur Gesamtzahl der gesendeten Zellen.

Neben Verbindungen mit spezifizierten QoS-Anforderungen gibt es aber auch sogenannte "best-effort"-Verbindungen, die keine Mindestdienstgarantieen fordern.

Für die Festlegung und Überwachung der QoS-Anforderungen auf den Teilstücken einer Verbindung sind verschiedene QoS-Protokolle zuständig:

- *UNI* (User-to-Network-Interface): Schnittstelle zwischen Netzteilnehmer und Netz. Festlegung der Ende-zu-Ende-Qualitätsparameter.
- *P-NNI* (Network-to-Network-Interface): Schnittstelle zur Kommunikation zwischen Netzknoten im selben Subnetz.
- *B-ICI* (Broadband-Intercarrier-Interface): Kommunkation zwischen Netzknoten unterschiedlicher Subnetze; falls Verbindung sich über mehrere Subnetze oder Netzhierarchien erstreckt.

Außer normalen Punkt-zu-Punkt-Verbindungen zwischen zwei Kommunikationspartnern werden auch Punkt-zu-Mehrpunkt-Verbindungen (bsp. Radio- oder Fernsehübertragungen) oder Mehrpunkt-zu-Mehrpunkt-Verbindungen (Konferenzen mit mehr als zwei Teilnehmern) durch spezielle Übertragungstechniken unterstützt. Solche Verbindungen werden aber im Rahmen dieser Ausarbeitung nicht besprochen.

2.1.3 Der ATM-Protokollturm

Wie fast alle Kommunikationsmodelle ist auch das ATM-Modell in hierarchische Schichten aufgeteilt. Das ATM-Referenzmodell basiert auf dem ISO/OSI-Referenzmodell und besitzt die folgenden drei Ebenen:

- *Physikalische Schicht*: Diese Schicht – auch Bitübertragungs-Schicht genannt – beinhaltet Funktionen zur Bitübertragung. Sie ist unter anderem verantwortlich für die Festlegung der Bitrate, die Umsetzung der Daten auf den Signalcode und die Synchronisation.

Außerdem übernimmt sie die Pufferung der ATM-Zellen und das Multiplexen der Zellen auf das Medium. Da bei einem Pufferüberlauf die neu ankommenden Zellen verloren gehen, muß der Puffer so ausgelegt sein, daß statistisch gesehen die Verlustrate bzw. die Wahrscheinlichkeit für den Verlust einer Zelle einen bestimmten Wert (10^{-9}) nicht überschreiten.

- *ATM-Schicht*: Die ATM-Schicht sorgt für den Transport und die Vermittlung der ATM-Zellen. Dazu gehören das Erstellen des Zellkopfes am Startknoten bzw. das Auswerten des Kopfes am Ziel- und in den Zwischenknoten, die Sicherung der Zellkopfinformationen, das Einfügen und Kennzeichnen von Leerzellen und die Überwachung der Übertragungsrate.
- *ATM-Anpassungs-Schicht* (ATM-Adaption-Layer – AAL): Diese Schicht übernimmt die Abbildung der zu übertragenden Nutzdaten auf ATM-Zellen bzw. die Rückgewinnung der Daten aus den ankommenden Zellen. Hier erfolgt auch die je nach Dienstklasse (siehe 2.1.2) und QoS-Anforderungen unterschiedliche Bearbeitung der Daten.

2.1.4 Switching bei ATM

Da in einem Netz typischerweise nicht jeder Rechner mit jedem anderen Rechner direkt verbunden ist, gehen Verbindungen nicht direkt vom Start- zum Zielknoten, sondern die Pfade erstrecken sich über mehrere Netzknoten. Alle Netzknoten haben mehrere Eingänge, über die Daten von verschiedenen Nachbarknoten ankommen und Ausgänge, über die Daten an Nachbarknoten weg- oder weitergeschickt werden. Soll nun eine Verbindung von einem Startrechner zu einem Zielrechner aufgebaut werden, so muß entschieden werden, über welche Zwischenknoten die Verbindung geht (siehe 2.1.5 und 2.3). Diese Verbindung wird dann durch mehrere aufeinanderfolgende virtuelle Kanäle realisiert, die von einem Netzknoten zum nächsten gehen. Die Zellen dieser Verbindung verlassen den Startrechner über den entsprechenden Kanal, erreichen den ersten Zwischenknoten und werden dort auf das nächste Teilstück der Verbindung weitergeleitet. Dieses Weiterleiten nennt man “switching” oder “Vermitteln”.

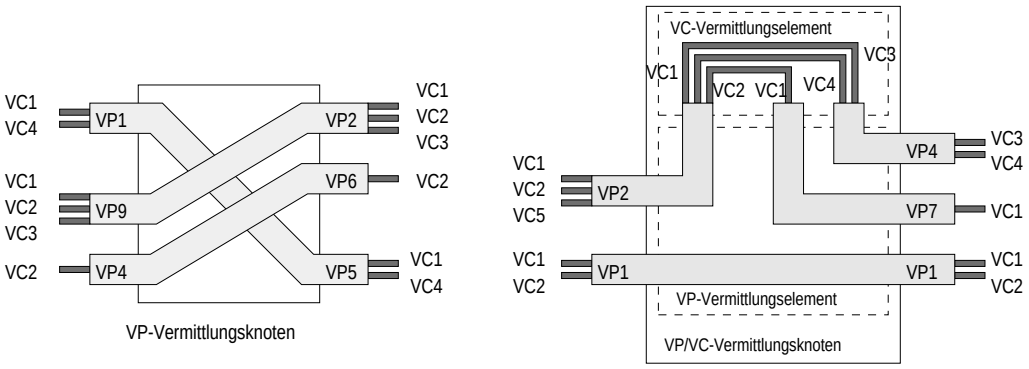

Abbildung 1: VP- und VP/VC-Vermittlungsknoten [Schm98]

Jeder Netzknoten (auch “Switch” oder “Vermittlungsknoten” genannt) hat eine Wegetabelle pro Eingang, in der zu jeder Verbindung (identifiziert durch VCI und VPP), die auf diesem Eingang ankommt, der Ausgang steht, auf den die Verbindung weitergeleitet wird. Kommt nun eine Zelle bei einem Switch an, wird zuerst die VCI/VPI-Kennung ausgewertet. Es wird geschaut, über welchen Ausgang die Zelle weitergeleitet werden muß. Außerdem werden VPI und VCI im Zellkopf umgeschrieben, da das nächste Teilstück eventuell eine andere logische Pfad- und/oder Kanalnummer hat. Dann wird die Zelle über den entsprechenden Ausgang weitergeleitet. Diese Vermittlung ist Aufgabe der ATM-Schicht, die somit in jedem Vermittlungsknoten realisiert sein muß.

In ATM-Netzen werden zwei Arten von Vermittlungsknoten unterschieden: *VP-Switches* vermitteln nur komplette Pfade, d.h. alle Kanäle, die zu einem ankommenden Pfad gehören, bilden zusammen auch wieder einen abgehenden Pfad, der nun aber eine andere Pfadnummer haben kann. Bei Zellen, die einen solchen Knoten durchlaufen, muß also nur das VPI-Feld des Zellkopfes geändert werden. Bei *VP/VC-Switches* dagegen werden Pfade und Kanäle neu vermittelt, es ändern sich also für zwei Teilstücke einer Verbindung eventuell sowohl VCI als auch VPI.

Vermittlungsknoten können sowohl mit automatischer Vermittlung als auch mit manueller Vermittlung realisiert sein. Bei automatischer Vermittlung wird die Verbindung durch Steuerinformationen, die in der Verbindungsanfrage enthalten sind, automatisch geschaltet und die Vermittlungstabelle aktualisiert, bei manueller Vermittlung, muß die Schaltung von Hand erfolgen. Manuelle Vermittlung ist also nur dann sinnvoll einsetzbar, wenn es sich um lange aufrechtzuerhaltende Verbindungen oder Standleitungen handelt, da sie sehr aufwendig zu schalten sind.

2.1.5 Prinzipien zur Verbindungsverwaltung

Die Verbindungsverwaltung dient dazu, den momentanen Zustand des Netzes bzw. Subnetzes zu protokollieren und zu analysieren und daraufhin in angemessener Weise zu reagieren. So wird über alle bestehenden Verbindungen Buch geführt; es wird protokolliert, welche Verbindung über welche Knoten geht, welche QoS-Anforderungen sie hat, welche Ressourcen sie belegt und welcher Netzknoten wieviele Ressourcen noch frei hat und zur Verfügung stellen kann. Beim Aufbau einer neuen Verbindung wird aufgrund der QoS-Anforderung und der aktuellen Ressourcenauslastung der jeweiligen Knoten entschieden, über welche Knoten die Verbindung aufgebaut wird, bzw. ob die Verbindung – im schlimmsten Fall – abgelehnt werden muß, weil keine Ressourcen mehr frei sind. Es gibt zwei mögliche Prinzipien, wie diese Netz- und Verbindungsverwaltung realisiert werden kann:

Zentralisierte Verwaltung Bei diesem Prinzip gibt es im Netz einen ausgezeichneten Server – den sogenannten "Connection Server" – der alle Informationen über Netz-, Knoten- und Verbindungszustände verwaltet. Beim Aufbau einer Verbindung wird der Connection Server kontaktiert, der dann anhand der Adresse des Start- und Zielrechners und der QoS-Anforderungen abhängig von der momentanen Netzsituation eine Route bestimmt und die daran beteiligten Knoten anweist, die entsprechenden Ressourcen zu reservieren. Sind alle Teilstrecken "geschaltet", werden die beiden Verbindungspartner über den Verbindungsaufbau informiert und der Connection Server aktualisiert seine Zustandstabellen. Ebenso müssen die Zustandsdaten beim Verbindungsabbau aktualisiert werden, da dabei reservierte Ressourcen wieder frei werden. Der Vorteil diese Verfahrens ist, daß alle benötigten Informationen an einer zentralen Stelle gesammelt werden, die dann anhand dieser Informationen Entscheidungen trifft. Die einzelnen Netzknoten müssen weder Logik noch Speicher oder ProzessorRessourcen für die Verwaltung von Routingtabellen oder das Ermitteln neuer Routen aufbringen und können so relativ einfach realisiert werden. Außerdem werden nie Fehlentscheidungen aufgrund inkonsistenter Netzzustandsinformationen getroffen werden, da nur eine zentrale Stelle die Informationen besitzt und Entscheidungen trifft. Ein weiterer Pluspunkt dieses Prinzips ist die Tatsache, daß die Reservierung von Ressourcen in den einzelnen Knoten parallel erfolgen kann, nachdem der Connection Server eine entsprechende Nachricht an alle beteiligten Knoten gesendet hat. Die Berechnung des Weges in einer Zentralstelle erspart auch den Signalisierungsverkehr zwischen den einzelnen Knoten, der sonst zur Wegfindung anfallen würde. Der Nachteil der Zentralisierung liegt in der Skalierbarkeit des Netzes. Je mehr Knoten das Netz umfasst, desto mehr Informationen müssen vom Server gespeichert, verwaltet und ausgewertet werden, was den Berechnungsaufwand für eine neue Verbindung drastisch erhöht.

Außerdem nimmt – statistisch gesehen – die Anzahl der Verbindungsanfragen pro Zeiteinheit normalerweise mit der Anzahl der Netzknoten zu, da mehr Netzteilnehmer auch mehr Netzaktivität mit sich bringen. Es werden also mit wachsendem Netz in der selben Zeit immer mehr Anfragen gestellt, die pro Anfrage immer mehr Berechnungsaufwand durch steigende Datenmengen verursachen. Das Netz wird also nicht beliebig wachsen können, da früher oder später der Connection Server überlastet wird und damit die Netzauslastung einbricht.

Verteilte Verwaltung Bei der verteilten Verbindungsverwaltung sind alle benötigten Informationen über Knoten und Verbindungen in jedem Knoten selbst neu gespeichert. Benötigt werden hier außer den obligatorischen Routingtabellen vor allem auch ATM- spezifische Daten, wie Informationen über die Verbindungen, an denen ein Knoten beteiligt ist, deren QoS-Anforderungen und freie Ressourcen des eigenen Knotens und der Nachbarknoten. Bei einem Verbindungsaufbau wird ausgehend vom Startrechner in jedem einzelnen Netzknoten geprüft, ob die Verbindungsanforderungen erfüllt werden können. Wenn ja werden die entsprechenden Ressourcen belegt und durch Routingverfahren ermittelt, welcher Nachbarknoten als nächster Knoten für die Verbindung in Frage kommt. An diesen wird dann die Verbindungsanfrage weitergeleitet und die Prüfung beginnt dort von neuem. Kann ein Knoten eine Verbindungsanforderung etwa aufgrund mangelnder Ressourcen nicht erfüllen, so lehnt er den Verbindungsaufbau ab und es muß ein Alternativpfad bestimmt oder im schlimmsten Fall die Verbindung zurückgewiesen werden. In diesem Fall kann der Verbindungsaufbau entweder neu probiert werden oder er muß abgewiesen werden. Eine Verbindung gilt dann als aufgebaut, wenn Ressourcen für alle Teilstrecken reserviert sind und der Startrechner eine Verbindungsaufbau-Bestätigung vom Zielrechner bekommen hat. Vorteile dieser Methode sind der Wegfall des Connection Servers und eine Verteilung der Datenmengen auf die einzelnen Rechner. Zwar muß immer noch ein Teil der Daten von allen Knoten in jedem einzelnen Knoten gehalten werden, bei vielen Daten genügt es aber auch, nur Kenntnisse über die Nachbarknoten zu haben. Die Skalierbarkeit steigt damit zwar nicht ins Unendliche, wächst aber gegen die zentralisierte Methode beträchtlich. Nachteilig wirkt sich hier aus, daß die Ressourcenreservierung beim Verbindungsaufbau nicht mehr parallel, sondern Knoten für Knoten erfolgt, was eine längere Dauer der Aufbauprozedur nach sich zieht. Des Weiteren bringt die Kommunikation zwischen den einzelnen Netzknoten zur Routenplanung zusätzlichen Signalisierungsverkehr mit sich. Das größte Problem stellt jedoch der Aufwand zur Konsistenzhaltung und Aktualisierung der Zustandsdaten dar. Benachbarte Server müssen ständig Informationen austauschen, was zum Einen einen erhöhten Kommunikations- und damit auch Ressourcenaufwand darstellt, zum Anderen Rechenzeit zur Auswertung der neu erhaltenen Informationen fordert. Weiterhin existiert immer ein gewisser Verzögerungsfaktor zwischen Eintreten eines Zustandes und der Verbreitung der Informationen darüber, wodurch Reaktionen auf Ereignisse immer nur verzögert erfolgen können.

Da beide Prinzipien nicht beliebig skalierbar sind, muß ein ATM-Netz, das über eine bestimmte Größenordnung hinausgeht, in Subnetze aufgespalten werden. Die Subnetze können jeweils nach einem der beiden Prinzipien realisiert sein; zusätzlich werden dann noch Instanzen benötigt, die zwischen den einzelnen Subnetzen vermitteln, da die Knoten und Connection Server jeweils nicht über die Grenzen ihres Subnetzes “hinausschauen” können. Insbesondere nationale und internationale Netze sind in Hierarchien und parallele Subnetze aufgeteilt.

2.2 Drahtloses ATM

2.2.1 Netztopologie

Zentraler Bestandteil von WATM ist der Mobile Rechner (“Mobile Host” – MH), mit dem der Benutzer arbeitet und der per WATM in ein ATM-Netz angebunden werden soll. Er besteht

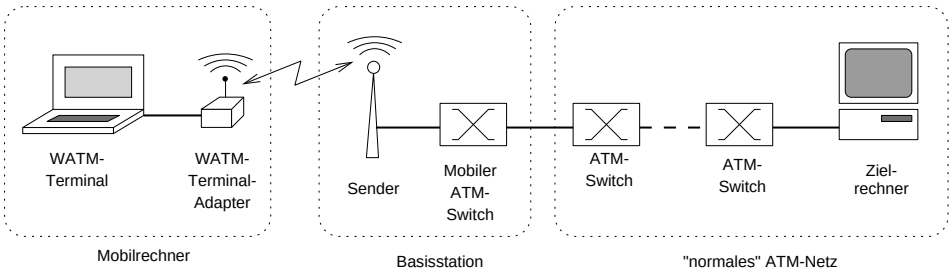

Abbildung 2: Netztopologie eines ATM-Netzes mit mobilem ATM-Rechner

aus einem *Mobile Terminal* (Rechner o.ä.), der alleine keinerlei Netzverbindung aufweist und einem "wireless terminal adapter" (WTA), dem Funkmodul, das für die drahtlose Anbindung ans Netz sorgt. Der WTA ist per Funk mit einer Basisstation (*Base Station* – BS) verbunden, die das Verbindungsglied zur "restlichen normalen Netzwelt" darstellt. Diese Basisstationen können je nach Ressourcenausstattung eine unterschiedliche Anzahl von Mobilrechnern versorgen. Sie unterscheiden sich in ihrer sonstigen Verhaltensweise gegenüber dem restlichen Festnetz in nichts von den normalen Netzknoten. Die Kommunikation zwischen einem Mobile Host und einem Festrechner unterscheidet sich also nur durch den letzten Teilpfad zwischen Mobile Host und Basisstation vom Kommunikationsablauf zwischen zwei Festrechnern. Die Kommunikation zwischen zwei Mobilrechnern findet ebenfalls immer über Basisstationen und – falls nicht beide Rechner von derselben Basisstation betreut werden – Festnetz statt, auch wenn vom Funkkontakt her eine direkte Kommunikation möglich wäre.

2.2.2 Zusatzanforderungen für drahtloses ATM

Die Realisierung von drahtlosem ATM erfordert eine Reihe von Zusatzfunktionalitäten, die sich aus den zwei Hauptaspekten des drahtlosen ATM ergeben; nämlich zum Einen aus der Drahtlosigkeit, bzw. der Kommunikation per Funk und zum Anderen aus der damit erreichten Mobilität des Endgerätes und des Benutzers. Diese Zusatzanforderungen werden durch eine Reihe spezieller Protokolle realisiert.
Unter den Gesichtspunkt der Mobilität fallen hierbei:

- *Mobile Connection Management Protocol* (MCMP): Regelt den Verbindungsaufbau, QoS-Vereinbarungen, Reservierung und Freigabe von Ressourcen und virtuellen Kanälen sowohl auf der drahtlosen als auch auf der festen Teilstrecke. Außerdem wird das Protokoll bei einem anstehenden Handover benötigt (siehe 2.4.1).

- *Mobile Handover Management Protocol* (MHMP): Verantwortlich für Durchführung des Handovers (siehe 2.4.1).

- *Mobile Location Management Protocol* (MLMP): Regelt die Standortverwaltung des Mobilrechners. Aufgaben sind das Protokollieren des physikalischen Standortes des Benutzers, die momentane Basisstation des Mobilrechners und das Subnetz, dem der Rechner momentan angegliedert ist. Beim Booten des Rechners muß sich dieser bei einer Basisstation anmelden und dann seinen Standort an den *Home Agent* melden (siehe 2.3).

- *Mobile Routing Protocol* (MRP): Protokoll für Routing-Aufgaben (siehe 2.3).

- *Mobile Media Access Control Protocol* (MMACP): Da eine Basisstation theoretisch mehrere Mobilrechner versorgen kann, praktisch aber nur beschränkte Ressourcen zur Verfügung hat, muß der Zugriff auf diese Ressourcen verwaltet werden, um die QoS-Anforderungen bestehender oder neuer Verbindungen zu erfüllen. Zum Einsatz kommen

Prinzipien wie TDMA (Zeitmultiplex), FDMA (Frequenzmultiplex) und CDMA (Codemultiplex).

- *Mobile Data-Link Control Protocol* (MDLCP): Durch Funkübertragung zusätzlich zu normalen Data-Link-Protokollen benötigte Funktionen wie Datenflußkontrolle, Signalrückgewinnung, Reihenfolgeerhaltung u.a.

- Radio Access Layer (RAL): Regelt Kanal- bzw. Frequenzvergabe, übernimmt Aufgaben der ISO/OSI-Sicherungsschicht (Schicht 2) wie etwa Fehlererkennung und -behandlung speziell auf dem Teilstück Mobilrechner $\Leftrightarrow$ Basisstation.

2.3 Routing bei Drahtlosem ATM

Vor dem Verbindungsaufbau muß zunächst einmal entschieden werden, über welche Zwischenknoten eine Verbindung gehen soll. Meist gibt es hier mehrere verschiedene Möglichkeiten, aus denen nach unterschiedlichen Gesichtspunkten eine ausgewählt wird. Diese Wegewahl beim Verbindungsaufbau nennt man *Routing*.

Neben Routingkriterien wie Entfernung zwischen den Netzknoten, Verbindungskosten oder Anzahl der Zwischenknoten vom Start zum Ziel, die auch in "normalen Netzen" (z.B. Internet) eine Rolle spielen, müssen bei ATM vor allem Ressourcenbezogene Aspekte berücksichtigt werden. So kann eine Verbindung nur über Knoten geleitet werden, die genügend freie Ressourcen haben, um die benötigten QoS-Anforderungen zu erfüllen. Kann kein solcher Weg gefunden werden, so müssen die QoS-Anforderungen zurückgeschraubt werden, oder der Verbindungsaufbau muß abgelehnt werden. Es ist sinnvoll, einen Pfad zu wählen, der möglichst wenig Zwischenknoten enthält, um die Zellverzögerung, die über die einzelnen Knoten aufsummiert wird, gering zu halten.

Bei drahtlosem ATM kommen durch die Mobilität weitere Aufgaben, die das Routing betreffen hinzu. So muß ständig bekannt sein, wo sich ein Mobilrechner befindet und über welches Subnetz und welche Basisstation er erreichbar ist, um eventuell eine von einem Kommunikationspartner ZR gewünschte Verbindung zu diesem Rechner aufbauen zu können (siehe 2.2.2, MLMP). Dazu muss mindestens ein bestimmter Rechner im Netz über diese Informationen verfügen. In verteilten Netzen ist dies der *Home Agent*, dessen Adresse als erste Kontaktadresse für Verbindungen mit dem MH benutzt wird. Dieser Rechner kann dann entweder alle Daten von ZR an MH weiterleiten (*triangular routing*), was aber einen Umweg und somit zusätzliche Übertragungszeit bedeutet; oder er kann ZR die Adresse der Basisstation BS mitteilen, über die MH gerade erreichbar ist, und die Verbindung wird dann direkt von ZR über BS zu MH aufgebaut. Bei zentral verwalteten Netzen kann die Information über den Aufenthaltsort des MH auch beim Connection Server gespeichert sein. Aufgaben des mobilen Routing werden durch das Mobile Routing Protocol (MRP) geregelt.

Im folgenden werden verschiedene konkrete Routingverfahren kurz vorgestellt:

2.3.1 Link State Routing

Jeder Knoten hat eine Routingtabelle, in der für jeden anderen Knoten im (Sub-)netz eingetragen ist, über welchen Ausgangsport (also über welchen Nachbarknoten) dieser erreichbar ist. Beim Auf- oder Abbau von Verbindungen bzw. nach Ablauf eines Zeitzählers werden die Tabellen aktualisiert, um auf aktuelle Gegebenheiten im Netz reagieren zu können. Die Berechnung der Tabellen – also die Entscheidung, welcher Knoten am günstigsten über welchen Port erreicht wird – erfolgt z.B. durch den Dijkstra-Algorithmus. Kriterien hierbei können Verzögerungszeiten, Verfügbarkeit/Zuverlässigkeit von Netzknoten oder Verbindungskosten

sein. Da jeder Knoten seine eigene Routingtabelle hat, ist diese Routingvariante für verteilt verwaltete Netze gedacht. [Toe97]

2.3.2 Minimum-Hop Routing

Dieses Routingverfahren funktioniert wie das *Link-State-Routing*-Verfahren, allerdings werden die Routingtabellen nicht nach Kosten, sondern nach der Anzahl der Zwischenknoten (Hops) vom Start- zum Zielrechner berechnet. Es ist also sichergestellt, daß der vom Routingverfahren ausgewählte Weg der Weg mit den wenigsten Zwischenknoten ist. [Toe97]

2.3.3 Distance-Vector Routing

Dieses Verfahren ist ebenfalls auf die geringste Knotenanzahl optimiert. Jeder Rechner hat eine Routingtabelle, die die Anzahl der Zwischenknoten zu den jeweiligen Rechnern und den dazugehörenden Port beinhaltet. Bei der Initialisierung werden die Entfernungswerte für den eigenen Knoten auf 0 gesetzt, für alle anderen auf ∞. Die Tabellen werden dann an alle Nachbarknoten weitergeschickt, die nun ihre noch unbekannten Entfernungswerte (die mit ∞) mit den bekannten Werten der fremden Tabellen aktualisieren. Indem die fremden Werte vor der Übernahme um 1 erhöht werden, erhält so jeder Knoten Schritt für Schritt alle Informationen über Port und Entfernung zu den restlichen Netzknoten. Bei einer Änderung im Netz oder nach einem Zeitintervall werden die aktualisierten Informationen erneut ausgetauscht.

Im Gegensatz zu den drei oben vorgestellten Routingverfahren, die keine Ressourcenauslastung mit in die Routenbestimmung mit einbeziehen, sind die folgenden Verfahren auch für ATM-Netze geeignet, da sie – falls die Netzsituation dies zuläßt – die QoS-Anforderungen einer neuen Verbindung berücksichtigen.

P-NNI Routing Dieses Verfahren ist aus dem *Link-State-Routing*-Verfahren abgeleitet; zusätzlich zu den Kosten werden aber für jeden Rechner noch Informationen über Ressourcenauslastung gespeichert. Beim Aufbau einer neuen Verbindung kann so ein Weg gewählt werden, der nur über Knoten führt, die die geforderten QoS-Kriterien erfüllen können. [Toe97]

2.3.4 Bandwidth Control Algorithm

Bei diesem Verfahren beinhaltet die Routingtabelle eines Netzknotens für jedes mögliche Ziel des (Sub-)netzes eine Liste aller Ports, über die dieses Ziel erreichbar ist, zusammen mit Ressourceninformationen des Nachbarrechners, der an diesem Port angeschlossen ist. Beim Verbindungsaufbau wird ausgehend vom Startrechner der Nachbarknoten als nächster Knoten gewählt, der die meisten freien Ressourcen hat. Dann wird der Teilpfad zu diesem Nachbarknoten aufgebaut. Von dort wird wieder der nächste Knoten nach den gleichen Gesichtspunkten gewählt. Dies setzt sich so lange fort, bis entweder der Zielknoten erreicht ist, oder der Pfad in eine Sackgasse mündet, weil alle Nachbarknoten eines Knotens nicht genügend Ressourcen aufweisen können. In diesem Fall muß ein Alternativpfad gesucht werden. [Lehm97]

2.3.5 Progressive Shortest Path Routing

Dieses Routingverfahren arbeitet mit statischen Tabellen, die bei der Initialisierung der Netzknoten einmal erstellt werden und dann bis zum nächsten Systemstart des Knotens benutzt werden. Die Routingwahl bei der Initialisierung erfolgt nach den gleichen Kriterien wie beim Bandwidth Control Algorithm. [Lehm97]

2.3.6 Progressive Pure Alternate Routing

Dieses Verfahren ist ebenfalls statisch und arbeitet nach dem gleichen Prinzip wie das *Progressive Shortest Path*-Verfahren. Hier wird allerdings zu jedem Pfad ein Alternativpfad gespeichert. Beim Verbindungsaufbau wird dann per Zufall ein Weg ausgewählt, wobei die Gewichtung der einzelnen Pfad sich nach ihrer Länge richtet (je kürzer desto mehr Gewicht). [Lehm97]

2.3.7 Progressive Overflow Alternate Routing

Der Ablauf gleicht dem des *Progressive Pure Alternate Path*-Verfahrens, hier wird jedoch nicht per Zufalls sondern direkt der Länge nach der Pfad ausgewählt. Ist ein Pfad blockiert, weil einer der Knoten nicht genügend freie Ressourcen hat, wird der nächst längere Pfad ausgewählt.
[Lehm97]

Bei Auf- und Abbau von Verbindungen ändert sich die Auslastung der Ressourcen in den einzelnen Knoten. Daher werden bei den dynamischen Routingverfahren beim Verbindungsauf- und -abbau oder bei veränderten QoS-Anforderungen erneut die aktuellen Knotenzustandsinformationen ins Netz gesendet. Der Vorteil der dynamischen Routingverfahren gegenüber den statischen liegt auf der Hand: Da ständig Informationen über Netzzustandsänderungen ausgetauscht werden, wird immer der Pfad ausgewählt, der zum Zeitpunkt des Verbindungsaufbaus auch wirklich der bestmögliche ist. Im Extremfall kann bei Verfahren mit statischen Tabellen der Fall auftreten, daß eine Route ausgewählt wird, die über einen Knoten führt, der zwischenzeitlich gar nicht mehr funktionstüchtig ist.
Der Nachteil der dynamischen Verfahren ist ein erheblich höherer Aufwand zur Wegewahl beim Verbiundungsaufbau und zur Aktualisierung der Informationen in den einzelnen Knoten, die außerdem einen nicht unerheblichen Signalisierungsverkehr mit sich bringt. Die drei statischen Verfahren existieren aber auch in adaptiven Versionen, die sich dynamisch an die Netzgegebenheiten anpassen.

2.4 Handover

2.4.1 Aufgaben beim Handover

In diesem Abschnitt wird davon ausgegangen, daß eine Verbindung zwischen einem Mobilrechner MH und einem Zielrechner ZR existiert. MH ist dabei über eine Basisstaion BS_{alt} an das ATM-Netz angebunden. Beim Handover wird der Mobilrechner von der Basisstation (BS_{alt}) an eine andere Basisstation (BS_{neu}) übergeben, etwa weil der Rechner im Begriff ist, sich aus dem Empfangsbereich von BS_{alt} hinaus in den Empfangsbereich von BS_{neu} hinein zu begeben.

Der prinzipelle Ablauf des Handovers sieht folgendermaßen aus: Wenn die neue Basisstation bestimmt ist, wird durch ein Routingverfahren je nach Art des Handover (vgl. 2.4.2) eine Route von BS_{neu} zu ZR oder einem Crossover-Knoten bestimmt. Die neue Basisstation wird über den Handover informiert und reserviert die erfoderlichen Ressourcen. Wenn MH auf die neue Basisstation umschaltet, werden die Zellen auf den neuen Weg umgeleitet und der alte Pfad abgebaut. Das *Mobile Handover Management Protocol* (MHMP) sorgt dabei dafür, daß keine Zellen verloren gehen. Dies könnte beispielsweise dann passieren, wenn MH auf die neue Basisstation umschaltet, obwohl noch Zellen für MH über BS_{alt} unterwegs sind. Außerdem gewährleistet das MHMP, daß Zellen, die über den neuen Pfad an MH geleitet werden, nicht vor Zellen, die über den alten Pfad kommen, von MH ampfangen werden. Dies ist wichtig, um die von ATM garantierte Reihenfolgetreue einzuhalten.

2.4.2 Verschiedene Versionen des Handover

Die Durchführung eines Handovers bedeutet eine Änderung bzw. Erweiterung der bestehenden Verbindung MH↔ZR, bei der die neue Basisstation in den bestehenden Verbindungspfad aufgenommen wird. Dieser Handover kann auf verschiedene Arten erfolgen:

Kompletter Neuaufbau der Verbindung Die Verbindung zwischen BS_{alt} und ZR bleibt bestehen, zusätzlich wird ein zweite Verbindung von ZR zu BS_{neu} geschaltet, die beim Handover den mobilen Rechner "auffängt". Dabei besteht für ein kurze Zeit eine doppelte Verbindung, was eine doppelte Ressourcenreservierung bedeutet. Vor allem dann, wenn sich der alte und neue Pfad nur durch BS_{alt} und BS_{neu} unterscheiden, sonst aber über dieselben Knoten gehen, ist diese Doppelbelegung unnötig. Da beide Verbindungen jedoch nur für eine relativ kurze Zeit parallel bestehen, ist die Doppelreservierung von Ressourcen in manchen Netzen möglicherweise zu verkraften. Diese Methode des HJandovers ist relativ einfach zu implementieren.

Erweiterung der bestehenden Verbindung Da BS_{alt} und BS_{neu} räumlich relativ nahe beieinander liegen, ist anzunehmen, daß es eine direkte Verbindung oder zumindest eine sehr kurze indirekte Verbindung zwischen den beiden Basisstationen gibt. Es ist also möglich einfach das neu benötigte Teilstück zur neuen Basisstation an die schon bestehende Verbindung anzuhängen und so die Verbindung aufrechtzuerhalten. Die Nachteile dieser Lösung liegen auf der Hand: zum Einen wird die Kette der beteiligten Knoten immer länger, jeder neu aufgenommene Knoten bedeutet eine zusätzliche Verzögerungszeit bei der Paketübermittlung. Außerdem gäbe es mit ziemlicher Wahrscheinlichkeit eine kürzere direkte Verbindung von ZR zu BS_{neu}, vor allem wenn der Verbindungspfad schon mehrere Male erweitert wurde; das heißt, es werden NetzRessourcen unnötigerweise weiterhin für die Verbindung reserviert. Wenn der Mobile Rechner im Laufe der Verbindung mehrmals zur selben Basisstation weitergeleitet wird – etwa bei einer Hin- und Herbewegung – bilden sich zudem Schleifen, die unnötigerweise aufrechterhalten werden und zusätzliche NetzRessourcen verbrauchen und die Verzögerungsrate erhöhen.

Teilweiser Neuaufbau der Verbindung Diese Version des Handover ist bezüglich Verzögerungszeiten und Pfadlänge / Ressourcenreservierung die optimale Lösung, bringt aber einen höheren Implementierungs- und Durchführungsaufwand mit sich.Es kann davon ausgegangen werden, daß bei einem Handover durch kompletten Neuaufbau die alte Verbindung und eine neu Aufgebaute zum größten Teil über die gleichen Netzknoten gehen – oder zumindest gehen würden, wenn die Knoten genügend Ressourcen frei hätten – und sich die beiden Pfade erst kurz vor dem Ziel gabeln. Der Knoten, der sich an dieser Gabelung befindet, wird CrossoverSwitch (CX) genannt. Man kann also angefangen von diesem Knoten eine neue Teilverbindung von CX zu BS_{neu} aufbauen und so tatsächlich für einen kurzen Zeitraum diese Gabel realisieren. Die Pakete werden bis zum Übergabezeitpunkt des MH auf der alten Verbindung weitergeleitet, der neue Teilpfad liegt noch "brach". Vom Zeitpunkt der Übergabe des MH von BS_{alt} an BS_{neu} an werden die Pakete dann über das neue Teilstück direkt an BS_{neu} geleitet und der alte Restpfad von CX zu BS_{alt} abgebaut bzw. freigegeben. Damit wird die alte Verbindung zum größten Teil weiterverwendet und es erfolgt keine unnötige Doppelreservierung von Ressourcen auf den Teilstücken, die alter und neuer Pfad gemeinsam haben, wie es beim kompletten Neuaufbau der Fall ist. Der erhöhte Durchführungsaufwand beim Handover entsteht durch die Bestimmung des CX-Knotens. Es existieren verschiedene Ideen und Algorithmen zur geschickten Wahl des CrossoverSwitches, die sich nach unterschiedlichen Gesichtspunkten richten und somit auch je nach Algorithmus unterschiedliche CX-Knoten für den selben Fall ergeben können. Einige davon werden im folgenden Abschnitt genauer erklärt.

2.4.3 Verschiedene Arten der CrossoverSwitch-Ermittlung

In diesem Abschnitt wird auf verschiedene Verfahren zur Bestimmung des CrossoverSwitches bei einem Handover eingegangen. Es wird des Öfteren der Begriff "Länge" eines Weges oder Pfades verwendet werden. Soweit nicht anders angegeben, bezieht sich der Ausdruck "Länge" hier auf die Anzahl der Knoten, über die sich der Pfad erstreckt.

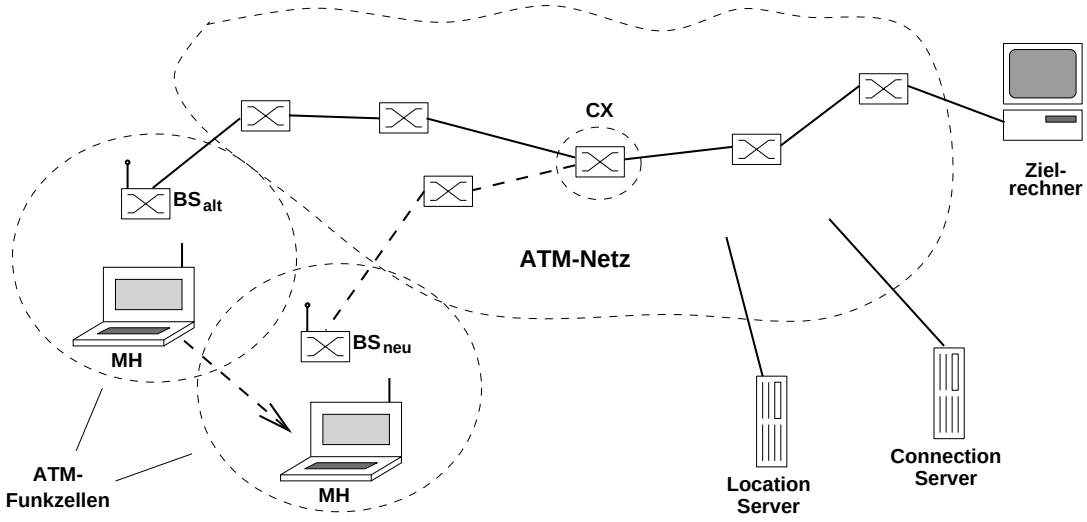

Abbildung 3: CX-Knoten-Ermittlung durch das *Loose-Select*-Verfahren

Loose Select CX Discovery Dieses Verfahren stellt ein von der Algorithmus-Seite gesehen relativ einfaches Verfahren dar. Bei einem anstehenden Handover wird der komplette Weg von ZR zu BS_{neu} in der gleichen Weise berechnet, wie wenn die Verbindung neu aufgebaut würde. Der alte Pfad wird dabei nicht berücksichtigt. Anschließend wird geprüft, ob ein Teil des neuen Pfades mit dem alten Pfad übereinstimmt. Ist dies der Fall, so ist der Knoten, an dem sich die beiden Pfade gabeln, der CrossoverSwitch. [Toe97]

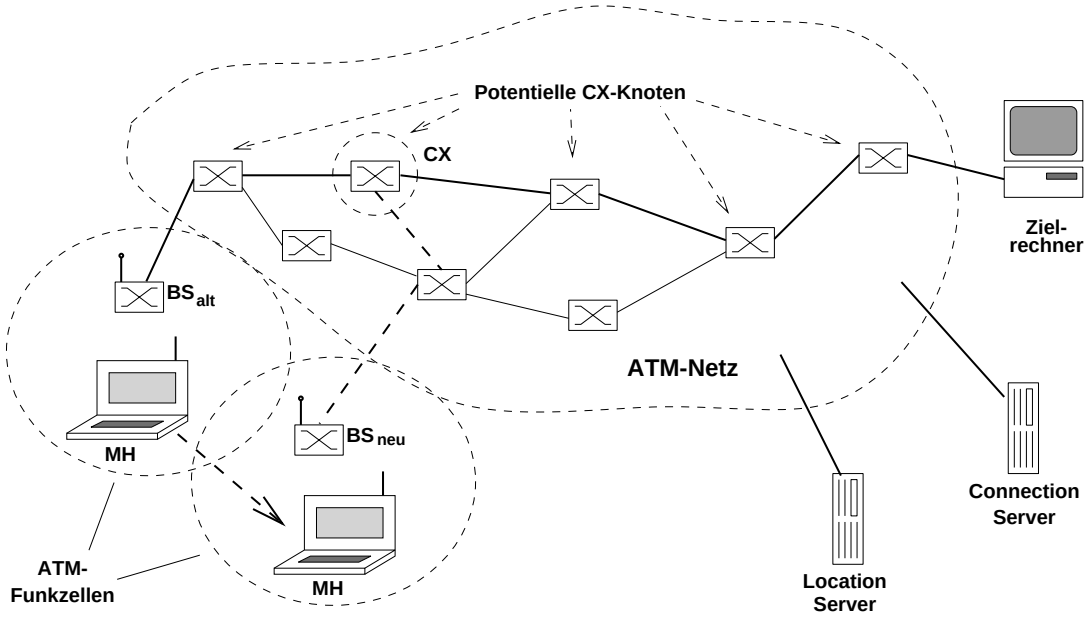

Abbildung 4: CX-Knoten-Ermittlung durch das *Prior Path Knowledge*-Verfahren

Prior Path Knowledge CX Discovery Dieses Verfahren geht von einer zentralen Verbindungsverwaltung aus. Wie der Name sagt, wird bei der Wahl des neuen CX der bisherige Pfad der Verbindung berücksichtigt. Zu Beginn werden alle Wege von BS_{neu} zu den Knoten des bisherigen Pfades berechnet und für jeden Knoten der kürzeste Weg bestimmt. Der CrossoverSwitch ist der Knoten, der den kürzesten Teilpfad zu BS_{neu} aufweist. Haben mehrere Wege die gleiche Länge, so wird derjenige unter diesen Wegen ausgewählt, dessen Knoten am nächsten bei der alten Basistation liegt. Dieses Verfahren hat zwar einen wesentlich komplexeren Algorithmus als das Loose Select Verfahren, dafür werden jedoch die Ressourcen optimal ausgenutzt, da keine der Teilstrecken unnötigerweise doppelt belegt wird. Es ist somit vor allem für (Sub-)Netze mit hoher anzunehmender Ressourcenauslastung oder wenig verfügbaren Ressourcen geeignet. [Toe97]

Prior Path Optimal Resultant CX Discovery Dieses Verfahren ist wie das Prior Path Knowledge Verfahren ein Verfahren für Netze mit einem zentralen Connection Server. Anfangs wird wieder für jeden Knoten des alten Pfades der kürzeste Weg zu BS_{neu} bestimmt.Ein Knoten ist ein potentieller CrossoverSwitch, wenn die Anzahl der Knoten der kompletten neuen Verbindung kleiner oder gleich der Anzahl der Knoten des alten Pfades ist. Als tatsächlicher CrossoverSwitch wird der Knoten mit der kleinsten Gesamtlänge vom Zielknoten zu BS_{neu} gewählt. Existieren mehrere Pfade mit der gleichen Gesamtlänge, wird der Knoten als CrossoverSwitch gewählt, der am nächsten bei BS_{alt} liegt. Falls alle möglichen CrossoverSwitches eine größere Gesamtpfadlänge als der alte Pfad ergeben würden, wird auf das Prior Path Knowledge Verfahren zurückgegriffen.Dieses Verfahren zeichnet sich dadurch aus, daß es immer einen neuen Pfad als Ergebnis hat, der kürzer oder gleich lang wie der aktuelle Pfad ist. Das Optimierungskriterium ist hier nicht die Länge des neu aufzubauenden Teilpfades, sondern die Länge des resultierenden Gesamtpfades (⇒"optimal resultant"). Abgesehen vom Auswahlkriterium für den CrossoverSwitch ist das Verfahren identisch zum Prior Path Knowledge Verfahren. [Toe97]

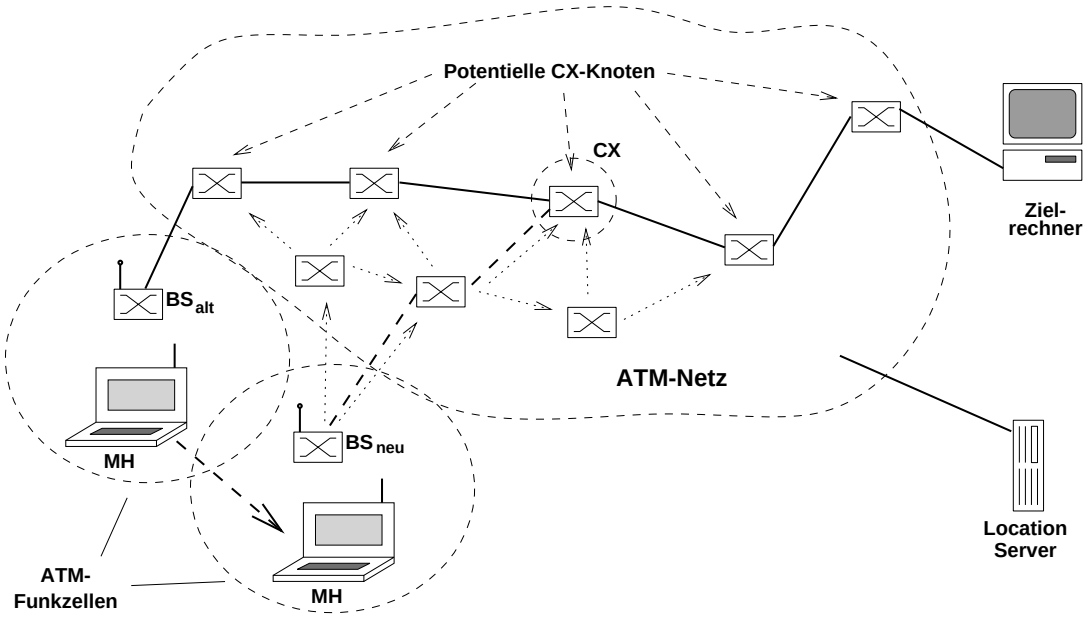

Abbildung 5: CX-Knoten-Ermittlung durch das *Distributed Hunt*-Verfahren

Distributed Hunt CX Discovery Diesem Verfahren wird ein Netz mit verteilter Verbindungsverwaltung zugrunde gelegt (⇒"distributed"). Wenn eine Basisstation darüber informiert wird, daß sie durch einen bevorstehenden Handover neue Basis-Station für einen Mobile

Host wird, sendet sie eine Broadcast-Anfrage nach möglichen CX-Knoten für die betreffende Verbindung ins Netz. Dieser Broadcast richtet sich an alle Knoten, die am aktuellen Verbindungspfad beteiligt sind, die restlichen Knoten im Netz ignorieren die Nachricht. Kann ein Knoten die geforderten QoS-Anforderungen erfüllen, so sendet er eine Antwort an BS_{neu}. Wie beim Prior Path Knowledge Verfahren wird der Knoten als CX-Knoten gewählt, für den die kürzeste neue Teilstrecke aufgebaut werden muß. Bei mehreren Knoten mit gleicher Länger der neuen Strecke wird entweder per Zufallsgenerator willkürlich oder nach anderen Optimierungsmethoden ein Knoten ausgewählt. Es ist zu erwarten, daß diese Methode eine größere Verzögerungszeit haben wird, als die vorher genannten, da die neue Basisstation auf jeden Fall eine bestimmte Zeit auf Antworten auf ihre Broadcast-Anfrage warten muß. Außerdem ist mit dem Broadcast und den Antworten ein höherer Signalisierungsaufwand nötig als bei zentral verwalteten Netzen. Dafür kommt diese Methode ohne zentralen Connection Server aus. [Toe97]

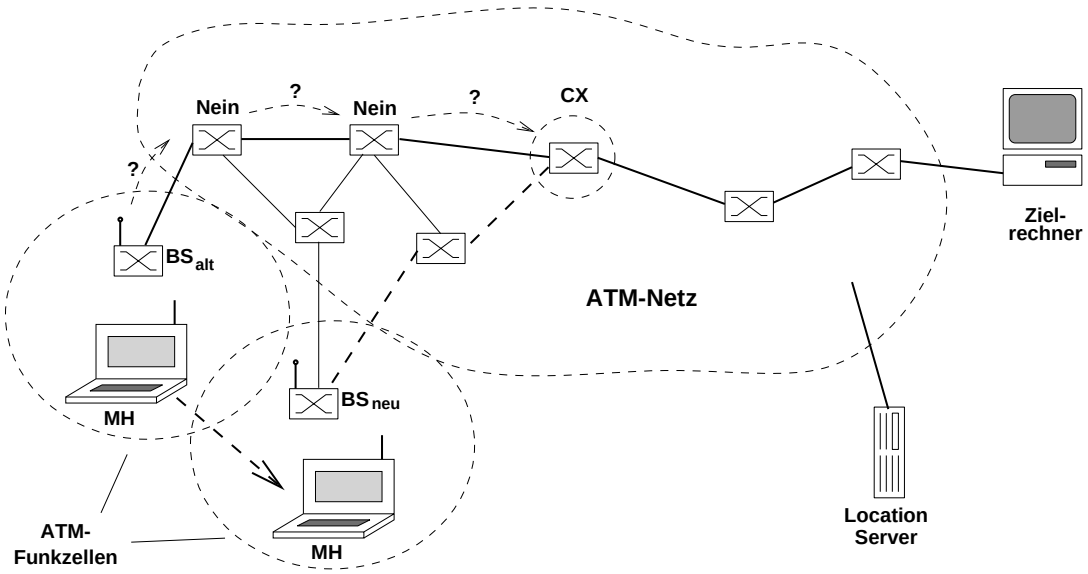

Abbildung 6: CX-Knoten-Ermittlung durch das *Backward Tracking*-Verfahren

Backward Tracking CX Discovery Bei diesem Verfahren prüft jeder Knoten ausgehend von BS_{alt}, ob er als CX für die neue Route in Frage kommt. Dies ist dann der Fall, wenn der Knoten, der einen Schritt weiter in Richtung ZR liegt, BS_{alt} und BS_{neu} über den gleichen Port erreicht. Da dieses Verfahren auf Routinginformationen aufbaut, kann es nur sinnvolle Ergebnisse liefern, wenn ein entsprechendes Routingverfahren angewandt wird. Dieses Verfahren ist sowohl für verteilte als auch für zentral verwaltete Netze anwendbar, die Prüfung muß dann jeweils in den einzelnen Knoten (verteiltes Netz) oder für alle Knoten beim Connection Server (zentralisiert) vorgenommen werden. [Toe97]

2.4.4 Ablauf des Handovers

In diesem Abschnitt wird zusammenfassend ein kompletter Handoverablauf von Anfang bis Ende beschrieben. Es wird auf den Normalfall des Handovers mit Radio Hint eingegangen und anschließend die abweichende Spezialversion eines Handovers ohne Radio Hint, bespielsweise bei Ausfall der Basisstation, beschrieben.

Mit Radio Hint Radio Hints sind kurze Funksignale, die in periodischen Abständen zwichen dem Mobilrechner und allen erreichbaren Basisstationen ausgetauscht werden. Sie dienen

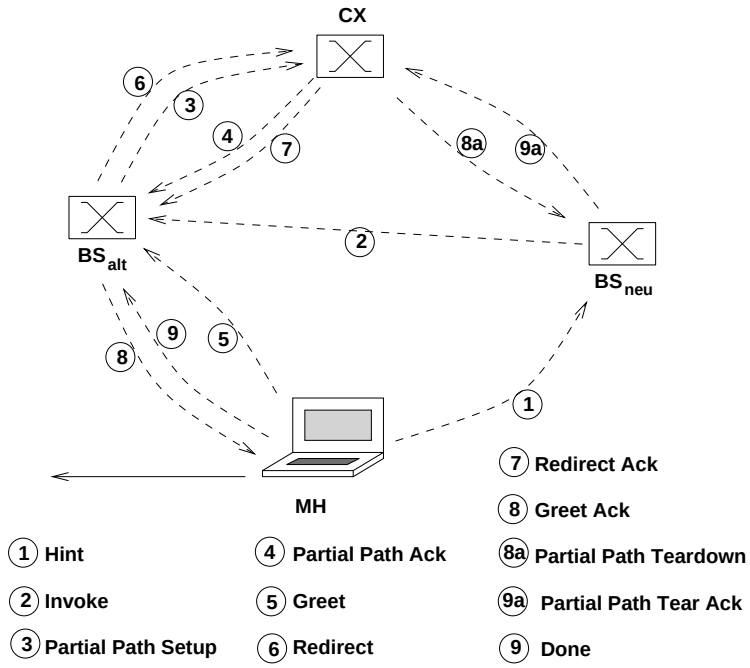

Abbildung 7: Handover mit Radio Hint

zum Einen dazu, festzustellen, welche Basisstationen vom Mobilrechner erreichbar sind und zum Anderen dazu, die Stärke der beim Mobilrechner bzw. bei den Basisstationen ankommenden Signalen zu ermitteln. Die Signalstärke des Mobilrechnersignals wird in den Basisstationen, die dieses Signal empfangen können, gemessen und als Antwort an den Mobilrechner zurückgeschickt. Der Mobilrechner kann seinerseits feststellen, wie stark die Signale der einzelnen Basisstationen bei ihm ankommen, außerdem weiß er durch die Antworten, wie seine Signale bei den Basisstationen empfangen werden. Aufgrund dieser Informationen kann der Mobilrechner entscheiden, wann das Signal der aktuellen Basisstation schwächer wird und ob es sinnvoll wäre, zu einer anderen Basisstation zu wechseln, bei der der Empfang besser ist.
Ist dies der Fall, so sendet der Mobilrechner ein ein *hint*-Signal (1) mit der Adresse von BS_{neu} an BS_{alt}. BS_{alt} benachrichtigt daraufhin BS_{neu} mittels *invoke* (2) über den Handover-Wunsch und übergibt gleichzeitig eine Liste mit allen Verbindungen und deren QoS-Anforderungen, die der Mobilrechner zur Zeit unterhält. Falls BS_{neu} nicht genügend Ressourcen reservieren kann, um die Verbindungen von MH zu übernehmen, muß eine andere Basisstation gefunden werden; ansonsten kann mit der Handover-Prozedur fortgefahren werden. Als nächstes muß mittels einer der oben beschriebenen CX-Ermittlungsverfahren ein CrossoverSwitch bestimmt werden. Der CX wird dann über den bevorstehenden Handover benachrichtigt (*partial path setup* (3)) und das neue Verbindungsteilstück CX $\Rightarrow$ BS_{neu} aufgebaut. Der Verbindungsaufbau wird mit *partial path ack* (4) bestätigt.
BS_{neu} ist nun zur Übernahme des Mobilrechners bereit und muß warten, bis dieser mittels *greet* das Signal zur Durchführung des Handovers gibt. Sobald das *greet*-Signal empfangen wird (5), schickt BS_{neu} ein *redirect*-Signal an CX (6), der daraufhin mir der Umleitung der Daten auf das neue Teilstück beginnt. CX sendet eine *redirect-ack*-Bestätigung (7) an BS_{neu}; gleichzeitig wird eine *partial path teardown*-Nachricht (8a) an BS_{alt} geschickt, um der Station mitzuteilen, daß sie nicht länger Basisstation für MH ist und die reservierten Ressourcen wieder freigegeben werden können. Als Bestätigung schickt BS_{alt} ein *partial path tear ack* an CX (9a). Während der Verbindungsabbau des alten Teilpfades erfolgt, wird MH von BS_{neu} mittels *greet-ack* (8) über die erfolgreiche Umleitung der Daten informiert. Ein bestätigendes *done* von MH an BS_{alt} (9) schließt die Handover-Prozedur ab. [Toe97]

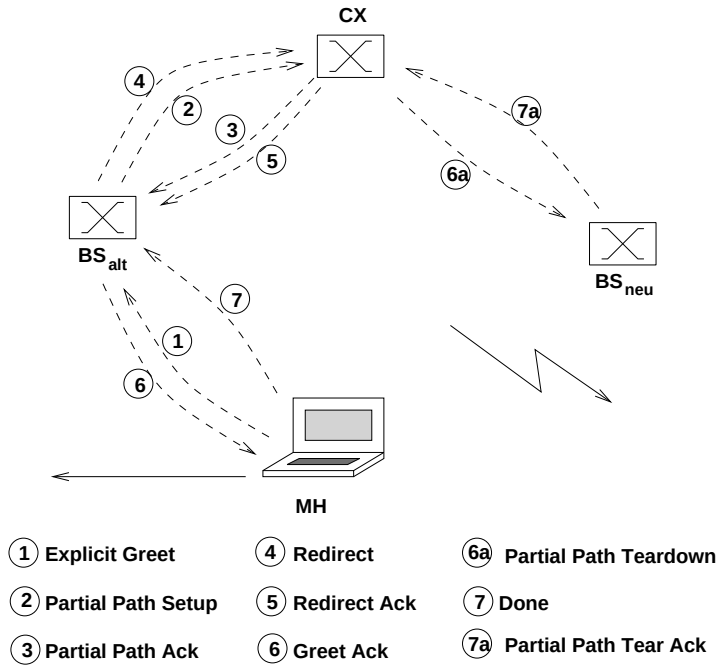

Abbildung 8: Handover ohne Radio Hint

Ohne Radio Hint Normalerweise wird ein Handover per *hint*-Signal an BS_{alt} eingeleitet. BS_{alt} veranlasst daraufhin den Aufbau des neuen Teilpfades der Verbindung, der zu dem Zeitpunkt, zu dem MH den endgültigen Wechsel zu BS_{neu} beschließt, schon aufgebaut ist. Durch einen Ausfall von BS_{alt} oder eine Störung des Funksignals kann jedoch der Fall eintreten, daß BS_{alt} nichts vom bevorstehenden Handover mitbekommt und BS_{neu} plötzlich durch das *greet*-Signal von MH überrascht wird. In diesem Fall muß MH eine *explicit-greet*-Nachricht (1) an BS_{neu} schicken, die nun alle Daten über die momentanen Verbindungen von MH enthält. Diese Daten hätte BS_{neu} ja normalerweise von BS_{alt} erhalten.
BS_{neu} schickt dann eine *partial path setup*-Nachricht an den von ihr ermittelten CX-Knoten (2), um den neuen Teilpfad aufzubauen. CX bestätigt den Aufbau mit *partial path ack* (3). Daraufhin leitet BS_{neu} per *redirect* (4) sofort die Umleitung der Daten ein, die von CX per *redirect-ack* (5) bestätigt wird. BS_{neu} teilt MH mittels *greet-ack* die Durchführung des Handover mit (6), was von MH nochmals mittels *done* bestätigt wird (7). Parallel dazu wird das alte Teilstück CX $\Leftrightarrow$ BS_{alt} wie oben per *partial path tear-down* (6a) und *partial path tear ack* (7a) abgebaut. [Toe97]

Literatur

[Lehm97] Volker Lehmann. Rerouting-Verfahren für ATM-Netze mit mobilen Endsystemen. *Diplomarbeit am Institut für Telematik, Universität Karlsruhe*, 1997.

[Schm98] Dr. Claudia Schmidt. Hochleistungskommunikation. *Folien zur Vorlesung am Institut für Telematik, Universität Karlsruhe*, 1998.

[Sieg93] Gerd Siegmund. *ATM - Die Technik des Breitband-ISDN.* R. v. Decker. 1993.

[Toe97] C-K Toe. *Wireless ATM and Ad-hoc Networks - Protocols and Architectures.* Kluwer Academic Publishers. 1997.

Evolution von GSM - Datentransfer mit HSCSD und GPRS

Erik-Oliver Blaß

Kurzfassung

Mit den heutigen GSM[1]-Netzen wie den deutschen D1/D2 und Eplus/E2 kann nicht nur Sprache übertragen werden - nein, *beliebige* Daten sind austauschbar.
Trotz des eigentlich guten Ansatzes - nämlich Zugriff auf Datendienste, insbesondere das Internet, von jedem Ort der Welt aus zu ermöglichen, nur mit Laptop, Handy und unabhängig von jeder Telefondose - ist der Datendienst in den heutigen GSM-Netzen kaum zu benutzen: die Übertragungsrate liegt nur bei 9,6 kbit/s, was ernsthaftes Arbeiten, geschweige denn gar Multimediaanwendungen wie Videokonferenzen, doch stark einschränkt.
Zwei neue Standards - "HSCSD" und "GPRS" - sollen hier abhelfen und dem vorhandenen GSM-Netz zu Datenraten von bis zu 164 kbit/s verhelfen.
Wie funktioniert ein modernes GSM-Netzwerk, und was verändert HSCSD und GPRS ?

1 GSM heute

Um den Fortschritt von HSCSD[2] und GPRS[3] gegenüber GSM zu verstehen, folgt hier zunächst eine Einführung in GSM:

GSM ist ein Standard für ein digitales, zelluläres Mobilfunknetzwerk, der 1982 von einem Ausschuß (Groupe Special Mobile - daher eigentlich der Name) der CEPT[4] begründet und 1989 an das ETSI[5] weitergegeben wurde. Das digitale GSM-Netz und damit auch seine deutschen Vertreter wie D-Netze (GSM900) und E-Netze (GSM1800) fällt in die sogenannte 2. Generation der Mobilfunknetz-Entwicklung [Mise98], die 1. Generation waren oder sind analoge Netze, wie z.B. das deutsche C-Netz.
Zur 3. Generation gehören Netze wie das UMTS, auf das noch ganz kurz am Ende eingegangen wird.

2 Komponenten im GSM-Netz

In Abbildung 1 sind zunächst Aufbau und Systemarchitektur sowie die Komponenten, Hierarchien und Datenflüsse eines solchen GSM-Netzes dargestellt.

- MS[6]: die MS ist das Endgerät eines Benutzers, also z.B. ein Handy oder ein Terminal.

[1] Global System for Mobile Communication
[2] High Speed Circuit Switched Data
[3] General Packet Radio Service
[4] Conference of European Posts and Telegraphs
[5] European Telecommunications Standards Institute
[6] Mobile Station

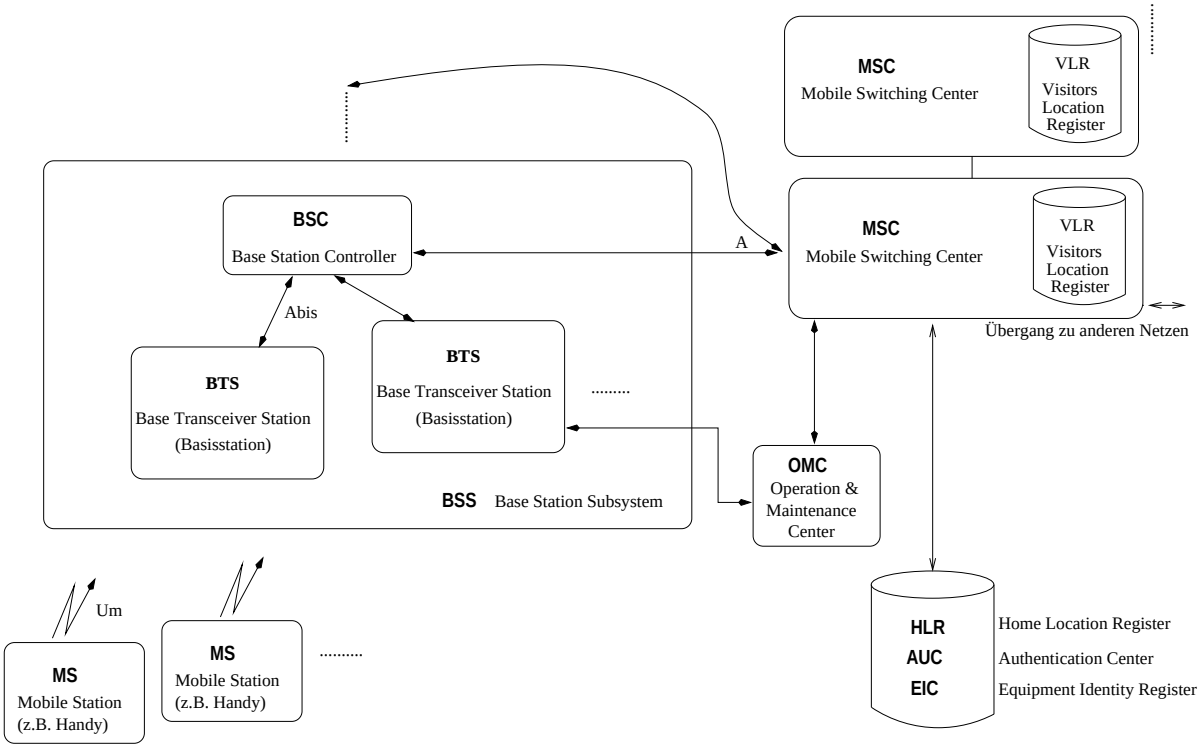

Abbildung 1: Komponenten im GSM-Netz, aus [Rohr]

- BTS[7]: "Basisstation"; die Basisstation ist der Kommunikationspartner der MS, MS und BTS kommunizieren über den sogenannten Radio-Path U_m, der in 3.1 und 3.2 noch genau erklärt wird. Eine Basisstation hat eine Reichweite von bis zu 37,8 km, jedoch ist es aus verschiedenen Gründen sinnvoller, *mehrere* Basisstationen mit *geringer* Sendeleistung zu verwenden (siehe 3.1.1). Eplus z.B. betreibt derzeit 6000 Basisstationen in Deutschland [Rohr], E2 verfügt im Moment über 1200, will aber sein Netz noch auf 10000 ausbauen.

- BSC[8]: mehrere benachbarte Basisstationen werden von einer übegeordneten Kontroll- bzw. Verwaltungsinstanz, dem BSC, gesteuert. Das BSC und seine BTSe nennt man auch Base Station Subsystem (BSS).

- MSC[9]: MSCs fassen mehrere BSCs zusammen, sie sind die obersten Verwaltungsinstanzen in einem GSM-Netz - sie vermitteln die Gespräche zwischen Teilnehmern in verschiedenen Base Station Subsystemen und vermitteln bzw. verwalten auch den Zugang zu *anderen* Mobilfunk- und Festnetzen.

- Die Schnittstelle zwsichen MSC und BSC heißt A, die innerhalb eines BSS zwischen BSC seinen BTS heißt A_{bis}. Dies sind in der Praxis meist Telekom-Mietleitungen, (eigene) Richtfunkstrecken oder sonstige (eigene) Leitungen [Rohr].

- OMC[10]: diese Komponente dient der Überwachung aller anderen Komponenten im Netz.

2.1 Datenbanken

Außerdem benötigt jedes GSM-Netz folgende Datenbanken:

[7] Base Transceiver Station
[8] Base Station Controller
[9] Mobile Switching Center
[10] Operation & Maintenance Center

- HLR[11]: hier stehen alle Teilnehmerdaten, wie Name, Nummer, freigeschaltete Dienste (Rufumleitung, Anklopfen, Anrufbeantworter, usw.) oder der aktuelle Aufenthaltsort des Nutzers im Netz. Das HLR gibt es nur einmal pro Dienst-Anbieter (D1, D2, Eplus...). Jeder Nutzer hat einen Eintrag in einem HLR in seinem jeweiligen GSM-Netz.

- VLR[12]: aus Effektivitätsgründen steht in jedem MSC eine Kopie des HLR, jedoch nur über diejenigen Teilnehmer, die sich gerade im Kontrollbereich dieses MSCs aufhalten. Diese Datenbank des MSCs heißt VLR.

- AUC[13]: dies ist meist implementiert als ein Teil des HLR [Rohr]. Im AUC stehen sensible Zugangsdaten, wie die geheimen SIM-Karten-Codes der einzelnen Nutzer zur Verschlüsselung einer Verbindung. (Die SIM-Karte eines Nutzers enthält Informationen über seine Identität, seine Zugangs-Codes usw. Die MS kann diese Karte auslesen. Da die geheimen Codes auf diese Weise nur MS und BS kennen, ist die Übertragung theoretisch sicher.)

3 Funk-Schnittstelle von GSM

GSM benutzt verschiedene Verfahren, um vorhandene Ressourcen, wie Frequenzen, Zeit und auch Raum möglichst optimal auszunutzen.

Das vorhandene Frequenzspektrum des GSM-Netzes wird nach dem FDMA[14]- und dem TDMA[15]-Verfahren aufgeteilt.

3.1 FDMA

(s. Abbildung 2)
Unterschieden wird zunächst zwischen GSM900 und GSM1800:

3.1.1 GSM900

Reserviert ist das Frequenz-Spektrum von 890,2 MHz bis 959,8 MHz (+ obere und untere Schutzbänder), aufgeteilt in zwei Teile, nämlich einen Teil für Uplink- und einen für Downlink-Kanäle, mehrere MS teilen sich einen solchen Kanal (s. 3.2). Auf einem Uplink-Kanal schickt die MS Daten zur BTS, umgekehrt sendet auf einem Downlink-Kanal die BTS zur MS. Zu jedem Uplink-Kanal gehört ein Downlink-Kanal. Der Abstand zwischen zueinandergehörendem Uplink und Downlink-Kanal sind genau 45 MHz ("Duplexabstand"). Zwischen zwei aufeinanderfolgenden Kanälen (jeweils Uplink/Downlink) besteht ein Abstand von 0,2 MHz (zur Modulation).
Der erste Uplink-Kanal fängt bei 890,2 MHz an, der erste Downlink entsprechend bei 935,2 MHz.
Das macht bei jeweils 0,2 MHz Abstand zwischen zwei aufeinanderfolgenden Kanälen insgesamt 124 verschiedene Kanäle (jeweils Uplink/Downlink), die man auch "Frequenzträger" oder "bearer" nennt. Die Frequenzen für den i-ten Uplink- bzw. Downlink-Kanal können leicht so errechnet werden:

[11] Home Location Register
[12] Visitor Location Register
[13] Authentication Center
[14] Frequency Division Multiple Access
[15] Time Division Multiple Access

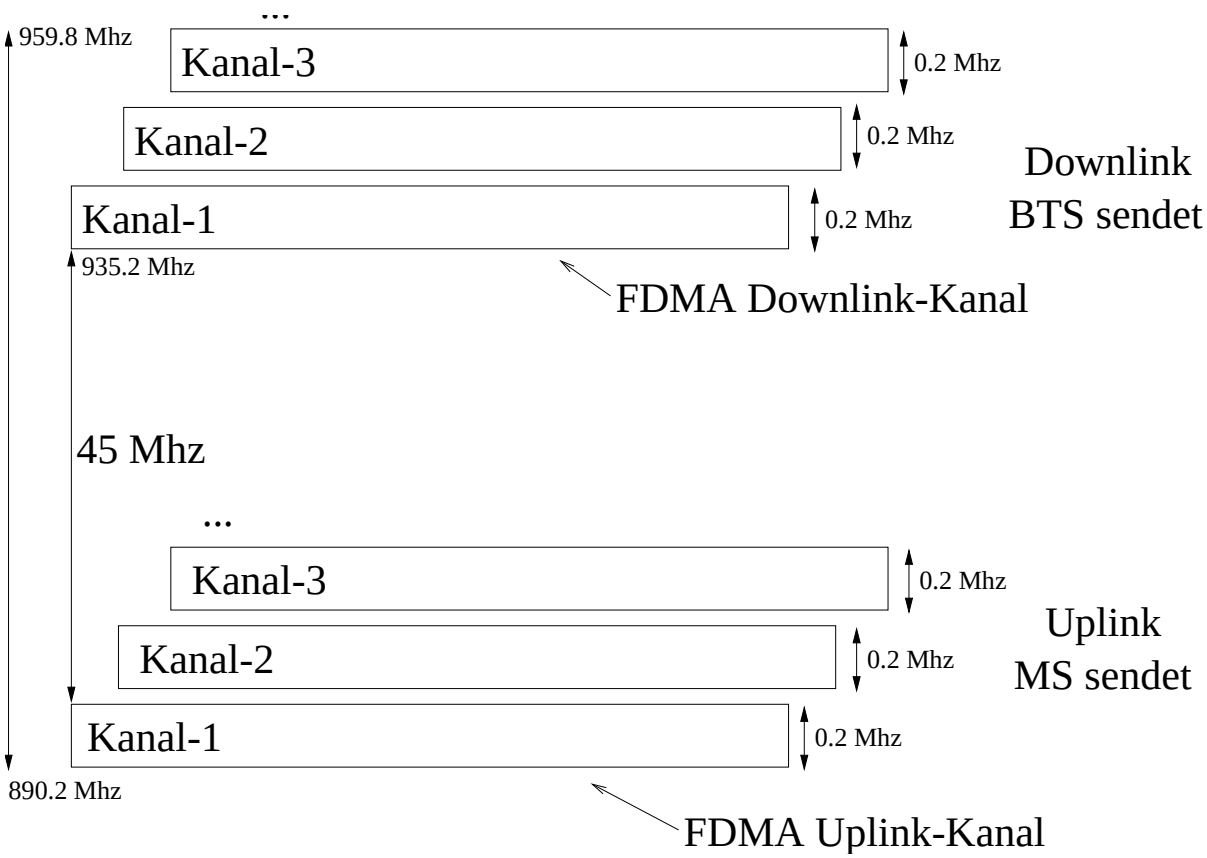

Abbildung 2: FDMA mit GSM900, aus [Smol94]

$f_{Up}(i) = 890$ Mhz $+ i * 0,2$ Mhz, $i \epsilon [1, \ldots, 124]$ "Uplinkfrequenz" des i-ten Kanals

$f_{Down}(i) = f_{Up}(i) + 45$ Mhz, $i \epsilon [1, \ldots, 124]$ "Downlinkfrequenz" des i-ten Kanals

Damit sich zwei benachbarte Basisstationen nicht durch Überlagern stören, dürfen sie nur verschiedene Frequenzen belegen, d.h. um möglichst viele MS gleichzeitig zu bedienen, sollten viele Basisstationen mit geringer Sendereichweite aufgestellt werden (Raummultiplex durch "Zellenbildung").

3.1.2 GSM1800

Analog zu GSM900[16] arbeitet das GSM1800[17]-Verfahren. Die Unterschiede zu GSM900 sind schnell erklärt:

- der Uplink beginnt bei 1710,2 MHz, der Downlink bei 1805,2 Mhz
- 95 MHz Duplexabstand
- d.h. insgesamt stehen 374 Trägerfrequenzen zur Verfügung
- $f_{Up}(i) = 1710$ MHz $+ i * 0,2$ MHz, $i \epsilon [1, \ldots, 374]$ "Uplinkfrequenz" des i-ten Kanals
  $f_{Down}(i) = f_{Up}(i) + 95$ Mhz, $i \epsilon [1, \ldots, 374]$ "Downlinkfrequenz" des i-ten Kanals

[16] in Deutschland sind D1 und D2 GSM900 Netze
[17] früher: DCS 1800; in Deutschland durch Eplus und E2 vertreten

3.2 TDMA

Jeder Uplink- bzw. Downlink-Kanal wird nun noch weiter unterteilt - und zwar in der Zeit nach dem TDMA-Verfahren (s. Abbildung 3).

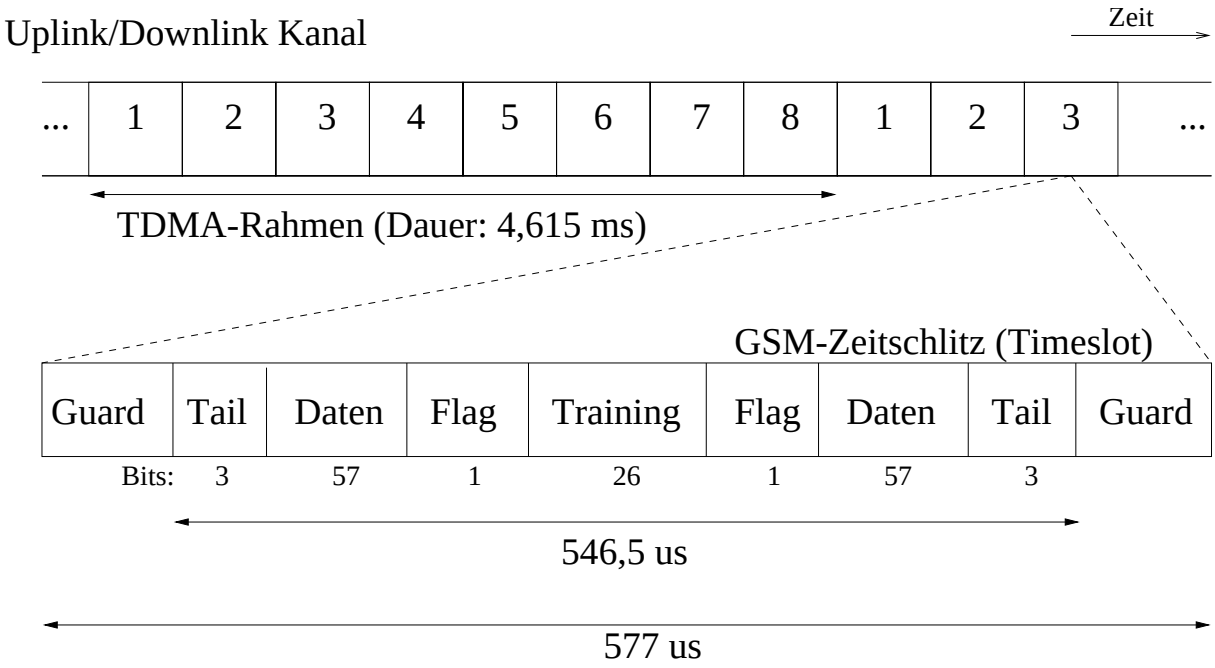

Abbildung 3: TDMA

Die Zeit wird in 4,615 ms lange Rahmen ("Frames") eingeteilt: TDMA-Rahmen. Jeder Rahmen besteht aus 8 Zeitschlitzen ("Timeslots"), von je $\frac{4{,}615\ ms}{8} = 577\ \mu s$ Dauer.
Ein solcher Timeslot ist nun ein physikalischer Datenkanal, in dem Nutz- und Steuerdaten von einer MS zur BTS (Uplink) oder umgekehrt (Downlink) gesendet werden können.
D.h. pro Trägerfrequenz stehen also 8 Kanäle für 8 mögliche MS zur Verfügung, macht $124 * 8 = 992$ mögliche MS pro BTS.
Ein Rahmen besteht aus:

- Guard: Dies ist ein variabler Schutzabstand von bis zu je 15 μs zum nächsten, bzw. vorhergehenden Timeslot.
- Daten: Hier stehen die eigentlichen Steuer-/Nutzdaten der Übertragung.
- Flag: Das Flag gibt an, ob es sich beim benachbarten Datenfeld um Steuer- oder Nutzdaten handelt.
- Trainingsfeld: Dies ist eine der MS und der BTS bekannte Bit-Folge, die der Erkennung der Qualität der empfangenen Übertragung und zur Synchronisation dient.
- Tail: Das Tail kann zur Erhöhung der Empfangsqualität eingesetzt werden.

In einem Timeslot können also während eines Übertragungsbursts (so nennt man das Senden bzw. Empfangen eines Timeslots) 156 Bit Steuer-/Nutzdaten übertragen werden. Auf den zueinandergehörenden Uplink-/Downlink-Kanälen werden zusammengehörende Timeslots (also Timeslots für die selbe MS) um 3 Timeslots zeitversetzt gesendet. D.h. sendet die MS in dem für sie reservierten Timeslot Nummer n im Uplink-Kanal, dann empfängt sie auf dem Downlink-Kanal 3 Timeslots $= 3 * 577\ \mu s = 1731\ \mu s$ später, wenn der Uplink-Kanal gerade Timeslot $n + 3$ durchläuft.

Dies bedeutet eine einfache Implementierung der Sende-/Empfangselektronik der MS: denn die MS muß nur Halb-Duplex fähig sein, und hat "genug" Zeit zum Umschalten zwischen Senden und Empfangen.

Jede MS belegt einen Timeslot für Uplink und einen für Downlink während einer *Übertragung*. Im Idle oder Standby-Modus "lauscht" die MS nur auf bestimmten Control Channels, wie dem BCCH[18], PCH[19] oder RACH[20] auf Kontroll-Informationen, die die Basisstation aussendet.

Außerdem interessant, aber für das weitere Verständnis nicht besonders wichtig, dafür in der angegebenen Literatur (besonders [Rohr],[Smol94],[Scou97]) nachzulesen:

- Wie ist das Trainigsfeld aufgebaut ? Wie wird Sprache in GSM mit GSMK und dem Viterbialalgorithmus moduliert ?
- Was passiert beim Verbindungsaufbau, wie synchronisieren sich MS und BTS aufeinander ?
- Was passiert beim "Frequency Hopping", wenn einzelne Frequenzen zu stark gestört sind ?

Fazit: durch die relativ hohe Fehleranfälligkeit von Funkübertragungen definiert GSM nur Übertragungsgeschwindigkeiten von 9,6 kbit/s, bzw. nach Verabschiedung von GSM Phase 2+ 14,4 kbit/s (durch teilweises Weglassen von Fehlerkorrektur [Timo98]), also für moderne Multimedia viel zu wenig.

4 HSCSD

Die Entwicklung von HSCSD begann im Februar 1997 und ist seit Juli 1998 abgeschlossen [Euro]. Die Idee von HSCSD ist relativ einfach als "Kanalbündelung" zu verstehen, d.h. eine MS darf nicht nur *einen* Timeslot pro Rahmen auf Uplink- bzw. Downlink-Kanal belegen, sondern mehrere - nicht unbedingt aufeinanderfolgende. Es müssen nicht nur symmetrisch viele, d.h. die gleiche Anzahl von Timeslots im Uplink- und Downlink-Kanal, belegt werden, sondern es können unterschiedlich viele allokiert werden [Euro98e].
n+m Timeslots können reserviert werden, n Uplink-Kanäle, m Downlink-Kanäle, $1 \leq n \leq m \leq 8$. Dies spiegelt die tatsächliche Anwendungssituation wieder, daß nämlich mehr Daten von der BTS zur MS fließen, als umgekehrt [Timo98]. Die Übertragung auf den jeweiligen Timeslots soll weiterhin nach den bekannten Verfahren wie FDMA und TDMA unabhängig voneinander geschehen.
Zwei Modi sind in [Euro98e] und [Euro98d] definiert, transparent und nicht-transparent.
Transparent bedeutet, daß beim Verbindungsaufbau eine Anzahl von Timeslots reserviert wird, die sich danach während der Übetragung nicht mehr ändert. Dies ist wohl einfach zu implementieren, hat jedoch ein Problem beim dem sogenannten "Handover": wenn sich eine MS aus dem Versorgungsbereich ihrer BTS entfernt, wird die MS zur nächst günstigsten BTS weitergereicht ("Handover"). Wenn die neue BTS jedoch nicht mehr die Anzahl von Timeslots frei hat, die von der MS benötigt werden, muß die Verbindung abgebrochen werden [Euro98e].

[18] Broadcast Control Channel
[19] Paging Channel
[20] Random Access Channel

Dahingegen kann bei der nicht-transparenten Verbindung auch während des Datenaustausches die Anzahl der belegten Timeslots verhandelt werden.
Nach [Euro98d] werden bei Verbindungsaufbau unter anderem folgende Informationen ausgehandelt:

- AIUR[21]: Dies ist die gewünschte Geschwindigkeit, die das Netz bereitstellen soll, aber nicht überschreiten darf, außer die höhere Geschwindigkeit wird durch eine geringere Anzahl von Timeslots eines schnelleren Kanals erreicht, z.B. AIUR = 38 kbit/s, dann wähle 3*14,4 kbit/s, statt 4*9,6 kbit/s, der Benutzer zahlt nämlich pro belegtem Timeslot an den Provider [Euro98e].

- max. TCH[22]: definiert die maximale Anzahl von Timeslots, die die MS aktzeptiert, sie darf *nicht* überstiegen werden.

Wichtig ist außerdem([Euro98d], [Euro98e]):

- sowohl MS also auch BTS müssen einen Datenstrom in n-Teile spalten, übertragen und wieder zusammenführen können

- QoS[23]: die Fehlerrate pro belegtem Timeslot bleibt gleich, jedoch darf die Overall HSCSD Bit Error Rate durch den höheren Verwaltungsaufwand steigen.

- Call setup-delay: die Dauer, bis eine Verbindung zustande kommt, und Nutzdaten ausgetauscht werden können (3s bei GSM) darf steigen.

- Verschlüsselung: die n-Datenkanäle dürfen nicht alle mit dem selben Schlüssel übertragen werden, eine neue Verschlüsselung wird benötigt.

- Roaming soll auch weiterhin möglich sein. (Roaming ist die Möglichkeit, sich in einem fremden Netz einzubuchen. Der Nutzer, soll so seine MS auch in anderen (fremden) Netzen - also von anderen Providern - z.B. im Ausland ohne grossen Aufwand weiternutzen können. Der Nutzer ist ausserdem im "Fremd-Netz" unter seiner alten Rufnummer zu erreichen.)

Die Bezahlung soll - wie oben erwähnt - abhängig von der Anzahl der belegten Timeslots sein, d.h. bei transparenten Verbindungen, bei denen sich die Anzahl der Kanäle während der Verbindung ändern darf, müssen zu jeder solchen Veränderung die Time-Stamps für Start- und Stop-Zeiten und die Anzahl der belegten Timeslots gespeichert werden.
Die erste Implementierung der Firma Nokia [Timo98] benutzt übrigens der Einfachheit halber nur Timeslot-Belegungen mit weniger als 4 gleichzeitig belegten Timeslots - wir erinnern uns, daß nach 3 Timeslots die MS zwsichen Sendemodus und Empfangsmodus umschalten muß. Bei mehr als 3 Timeslots müßte sonst die MS seperate/unabhängige Empfangs- und Sendeeinheiten beeinhalten.

Welches Fazit können wir über HSCSD ziehen:

- Pro

[21] Air Interface User Rate
[22] Traffic Channel
[23] Quality of Service

  - der Umstieg auf HSCSD, bzw. die "Erweiterung" eines vorhandenen GSM-Netzes auf HSCSD ist für einen Service-Provider relativ einfach: zunächst muß nur die Software der BTS verändert werden.
  - Dies bedeutet insbesondere, daß der Umstieg ist billig ist.
  - Der HSCSD Standard ist bereits verfügbar.
  - HSCSD ist um ein Vielfaches schneller als GSM, theoretisch möglich sind $8 * 9,6$ kbit/s = 76,8 kbit/s.

- Contra
  - HSCSD belegt (so wie standard GSM natürlich auch) permanent Kanäle für die Datenübertragung, also auch wenn aktuell keine Daten übetragen werden sollen ("verbindungsorientiert"). Dies spiegelt nicht die typische Übertragungssituation von Computer Anwendungen wieder, bei der es eher zu "burst"-artigen Übertragungen kommt, d.h. Leitungen lange Zeit frei sind und dann schubweise belegt werden.

5 GPRS

General Packet Radio Service ist ein recht neuer Standard, sein letzter *Draft(!)* stammt noch vom August 1998 [Euro98c], und erst im Jahre 2000 sollen die ersten GPRS Netze getestet werden - man rechnet nicht vor 2003 damit, daß GPRS Einzug in den "Mass Market" hält [Sivu98].
Die Idee hinter GPRS: Statt der verbindungsorientierten Verfahren zur Kommunikation, wie GSM und HSCSD, soll ein paketorientierter Netzdienst eingführt werden, d.h. der zu übertragende Datenstrom wird in einzelne Pakete verpackt und die Pakete jeweils für sich übertragen. Dadurch fällt die Ein- bzw. Anbindung von anderen, bekannten paketorientieren Netzen (wie das IP basierte Internet!) leichter. Konkret ist das Ziel, daß das GPRS-Netz aus dem Internet heraus nur wie ein weiteres Subnetz aussieht [Rohr98]. Ein Teilnehmer, der sich eingewählt hat, bekommt eine dynamische IP-Adresse zugewiesen. Außerdem soll durch die Paketorientierung eine Leitung nicht permanent belegt werden, sondern die Leitung wird nur in dem Moment der eigentlichen Datenübertragung besetzt aber danach gleich wieder freigegeben ("capacity-on-demand").

In Abbildung 4 wird dargestellt, wie ein GSM-Netz um GPRS-Funktionalität erweitert wird. Die wichtigsten Komponenten sind:

- GGSN[24]: sichert den Zugang zu anderen paketvermittelten Netzen
- SGSN[25]: übernimmt die Übertragung der Daten zu den MS, dies kann mit Hilfe einer BTS in einem BSS geschehen. Das SGSN kann die eigentliche Übertragung allerdings auch selbst vornehmen, dies ermöglicht, daß ein Handy z.B. *gleichzeitg* Daten *und* Sprache überträgt.
- GPRS-Backbone: Datenleitungen, TCP/IP basierend, transportieren alle GPRS relevanten Daten
- Durch diesen Aufbau ist GPRS ein Netz im (GSM-) Netz

[24] Gateway GPRS Support Node
[25] Serving GPRS Support Node

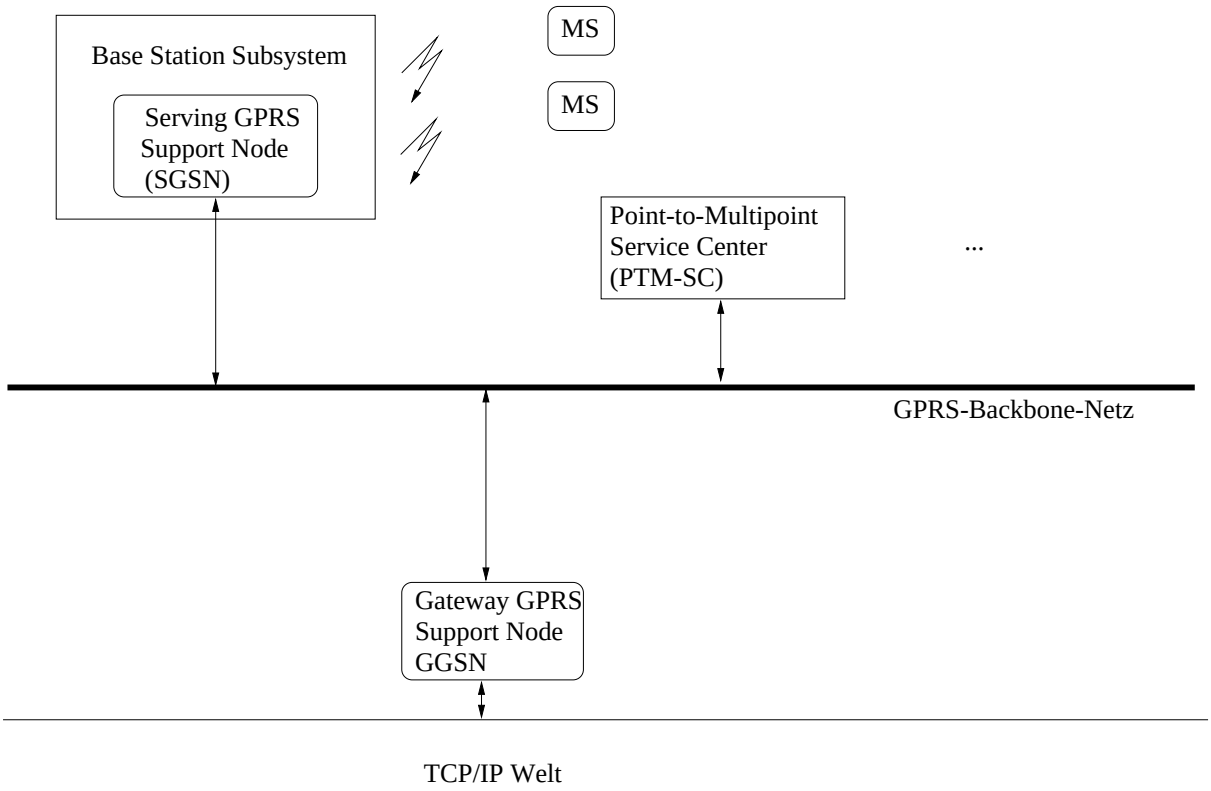

Abbildung 4: Einbindung von GPRS in ein GSM-Netz, aus [Rohr]

Ein wichtiger Punkt ist darüberhinaus, daß GPRS *auch* unabhängig von einem bestehenden GSM-Netz aufgebaut werden kann. D.h. ein Service Provider kann *nur* Datendienste anbieten, aber keine Sprache. Dies bedeutet natürlich, daß GPRS wichtige Informationen (redundant zum HLR) selber verwalten muß, so wie das Mobility Management [Euro98c]. Das HLR wird zudem noch um Informationen erweitert, wie die Priorität (High/Normal/Low, High verdrängt alle anderen Pakte, Normal nur "Low"-Pakete) und die zugesicherte Zuverlässigkeit ("Reliability") (wieviel Fehler pro Sekunde treten maximal auf, zwischen 10^{-2} und 10^{-9} pro Sekunde) des Benutzers [Euro98b].

Die eigentliche Datenübertragung funktioniert folgendermaßen: Liegen Daten im Ausgangs-Puffer ("Output Buffer") der MS (oder BTS), so wird zunächst auf bestimmten PacketControlChannels verhandelt, wieviele Timeslots auf Up- und auf Downlink-Kanal benutzt werden sollen (abhängig von der benutzerspeziefischen "wanted-throughput"). Die Timeslots müssen nicht hintereinanderliegen und es dürfen auch mehr als 8 Timeslots belegt werden, d.h. über ein TDMA Frame hinaus [Euro98c], die sogenannte "Multiframe"-Struktur. Dann werden die Datenpakete auf die allokierten Timeslots aufgeteilt und gesendet. Schließlich werden die Timeslots freigegeben.

Außerdem sind folgende Neuerungen vorgesehen:

- anonyme Verbindungen sollen möglich sein, d.h. ein Benutzer kann sich ohne zu identifizieren an einem GPRS-Netz anmelden und bestimmte Dienste nutzen - außerdem muß er für die Verbindung *nichts* zahlen, also ähnlich wie eine 0800/0130er Nummer im Festnetz der Telekom [Euro98b].

- eine andere Verschlüsselung
- verschiedene MS-Typen sind definiert:
  - Class A: GSM und GPRS Dienste sind *gleichzeitig* benutzbar.
  - Class B: die MS kann sich bei beiden Diensten anmelden, sie aber nur getrennt voneinander benutzen [Euro98b].
  - Class C: beide Dienste sind grundsätzlich nur hintereinander benutzbar.
- Es wird im GPRS unter anderem folgende neue Broadcast-Dienste geben [Rohr98], diese funktionieren nur in Richtung BTS $\rightarrow$ MS:
  - PTMM[26]: Textnachrichten werden zu allen Handys einer bestimmten Region geschickt.
  - PTMG[27]: wie PTMM, nur werden die Informationen an die Benutzer geschickt, die Mitglied einer bestimmten Gruppe sind. Ähnlich wie bei den bekannten Mailinglisten können sich die Benutzer selbst bei diesem Dienst anmelden und auch abmelden.
- Reverse Charging: d.h. der Angerufene zahlt die Verbindungskosten.
- auch hier soll Roaming weiterhin möglich sein.
- die Zeit, die vergeht, bis eine Verbindung aufgebaut wird, soll von $<$3s (GSM) auf $<$1s fallen
- Screening: bestimmte Datenpakete, von bestimmten Benutzern sollen ausgefiltert werden können

Welches Fazit können wir über GPRS ziehen:

- Pro
  - GPRS bietet eine einfache Anbindung an packet-switched Netze wie das Internet.
  - GPRS optimiert die Verteilung der Kapazitäten durch die burst-artige Übertragungsart auf mehrere Nutzer.
  - GPRS ist deutlich schneller noch als HSCSD, spezifiziert sind bis zu 115 kbit/s [Rohr98].
  - GPRS ermöglicht eine "gerechtere" nämlich volumenorientierte Abrechnung.
  - GPRS erweitert die Funktionalität von GSM um obige Broadcast-Dienste.
  - GPRS kann unabhängig von GSM aufgebaut werden.
- Contra
  - Die aufwendige Erweiterung des GSM-Netzes, nicht nur um Software, sondern auch Hardware ist entsprechend kostspielig.
  - GPRS ist erst sehr spät verfügbar (2003), d.h. es fällt mit neueren konkurrierenden Technologien wie UMTS zusammen.

[26] Point To Multipoint Multicast
[27] Point To Multipoint Group-Call

6 Ausblick

Sowohl Eplus, als auch D1 wollen dem Nutzer Mitte 1999 HSCSD anbieten. D2 und E2 planen HSCSD und GPRS, D2 nennt allerdings erst 2002 als Startpunkt für HSCSD und GPRS. Eplus verzichtet auf die Einführung von GPRS, da es zeitlich zu nahe mit UMTS zusammenfällt [Rohr].
Die Firma SingTel Mobile aus Singapur ist im Moment dabei ihr GSM-Netz auf HSCSD (bis 38,4 kbit/s) mit Hilfe der Firma Ericsson aufzurüsten - für 17 Millionen Dollar [cpre98].

UMTS[28] gehört zur 3. Mobilfunkgeneration, es beinhaltet Satellitenfunk und erlaubt Datenraten von bis zu 2048 kbit/s und soll auch bei höheren Relativ-Geschwindigkeiten (zwischen MS und BTS) als GSM (250 km/h) arbeiten. UMTS soll die (parallele) Übertragung von z.B. Audio oder Video direkt unterstützen. Erste UMTS Netze sollen 2002 aufgebaut werden [Mise98].

[28] Universal Mobile Telecommunications System

Literatur

[cpre98] SingTel Mobile company press release. SingTel Mobile upgrades its data services to High Speed Circuit Switched Data (HSCSD). *URL: http://www.gsmdata.com/*, Mai 1998.

[Euro] European Telecommunications Standards Institute (ETSI). ETSI Standards Monitoring. URL: http://www.etsi.org/, European Telecommunications Standards Institute (ETSI).

[Euro98a] European Telecommunications Standards Institute (ETSI). General Packet Radio Service (GPRS), Overall description of the GPRS radio interface; Stage 2, GSM 03.64 version 6.1.0, Release 1997. GSM Technical Specification (GTS), European Telecommunications Standards Institute (ETSI), Oktober 1998.

[Euro98b] European Telecommunications Standards Institute (ETSI). General Packet Radio Service (GPRS), Service Description; Stage 1, GSM 02.60 version 6.1.0. Draft, European Telecommunications Standards Institute (ETSI), Juli 1998.

[Euro98c] European Telecommunications Standards Institute (ETSI). General Packet Radio Service (GPRS), Service Description; Stage 2, GSM 03.60 version 6.1.1. Draft, European Telecommunications Standards Institute (ETSI), August 1998.

[Euro98d] European Telecommunications Standards Institute (ETSI). High Speed Circuit Switched Data (HSCSD) - Stage 1 (GSM 02.34 version 5.2.1). GSM Technical Specification (GTS), European Telecommunications Standards Institute (ETSI), Juli 1998.

[Euro98e] European Telecommunications Standards Institute (ETSI). High Speed Circuit Switched Data (HSCSD) - Stage 2 (GSM 03.34 version 5.1.0 Release 1996). GSM Technical Specification (GTS), European Telecommunications Standards Institute (ETSI), Juli 1998.

[Kevi98] Kevin Holley & Tim Costello. The Evolution of GSM Data Towards UMTS. Paper, GSM Data Today http://www.gsmdata.com/, Fall/Winter 1998.

[Mise98] Rainer Miserre. Schöne neue Welt. *Gateway*, Oktober 1998, S. 66–72.

[Rohr] Kai Rohrbacher. GSM-Technik. *URL: http://sites.inka.de/sites/maya/gsmtech.html, inzwischen (Jan. 1999) hat der Autor diese Seiten vom Netz genommen.*

[Rohr98] Kai Rohrbacher. Dampf fürs Drahtlose. *iX*, März 1998, S. 110–117.

[Scou97] John Scourias. Overview of the Global System for Mobile Communications. *URL: http://www.gsmdata.com/*, Oktober 1997.

[Sivu98] Timo Sivula. General Packet Radio Service GPRS, Ver. V1.0, Nr.: 981041. White Paper, NOKIA, Mai 1998.

[Smol94] Peter Smolka. *GSM-Funkschnittstelle aus GSM-Mobilfunk-Übertragungstechnik*, S. 32–52. Schiele & Schön. Herausgeber: Heinz Preibisch, 1994.

[Timo98] Timo Sivula, Kaj Hagros. High Speed Circuit Switched Data, Ver. V1.0, Nr.: 981021. White Paper, NOKIA, Juli 1998.

Deregulierung - neue Telefongesellschaften, neue Märkte

Jan Gerke

Kurzfassung

Auf EU-Beschluß mußte der deutsche Telekommunikationsmarkt zum 1.1.1998 privaten Anbietern vollständig geöffnet werden. Der neue Markt wird bestimmt von der Deutschen Telekom AG und drei weiteren „global players". Außerdem tummeln sich zahlreiche kleinere Unternehmen auf dem Markt, über den die Regulierungsbehörde für Telekommunikation und Post wacht. Zwischen allen Anbietern herrscht ein reger Preiskampf. Ihre Zukunft wird jedoch vor allem auch durch die angebotenen Dienste, die Nutzung neuer Technologien und die Bereitstellung eines vernünftigen Internet-Zugangs bestimmt werden.

1 Einleitung

Diese Ausarbeitung, die im Rahmen des Seminars „Netzwerkmanagement und Hochleistungskommunikation" im Wintersemester 98/99 entstand, beschäftigt sich mit der Situation des Telekommunikationsmarkts in Deutschland nach dessen Öffnung für private Anbieter. Auf den ersten Blick scheint dieses Thema vielleicht für Informatiker uninteressant und hier damit am falschen Platz zu sein, doch ist es dies keineswegs. Schließlich ist es für Informatiker, insbesondere für Telematiker, von höchster Bedeutung, wodurch der deutsche Telekommunikationsmarkt in den nächsten Jahrzehnten bestimmt wird. Zur Zeit befindet sich der Markt gerade im Umbruch, wodurch das Thema noch Bedeutung gewinnt, da jetzt die Weichen für die Zukunft gestellt werden, insbesondere auch durch Gesetze, die die Grundlage für einen liberalen Telekommunikationsmarkt bilden sollen.

Im einzelnen beschäftigt sich diese Ausarbeitung zunächst mit der rechtlichen Seite und vor allem auch der Durchsetzung der geltenden Gesetze durch die Regulierungsbehörde für Telekommunikation und Post. Dabei wird insbesondere auf die Probleme eingegangen, die dadurch entstehen, daß die Regulierungsbehörde Teil des Bundes ist, der aber auch gleichzeitig den größten Anteilseigner der Deutschen Telekom AG [Tele98] darstellt.

Anschließend wird auf die neuen Konkurrenten der Deutschen Telekom AG eingegangen. Dabei werden als erstes die gängigen Möglichkeiten, beim Telefonieren auf diese Gesellschaften zurückzugreifen, vorgestellt. Danach wird näher auf die drei größten Konkurrenten der Deutschen Telekom AG eingegangen. Als letztes werden die weiteren, kleineren Gesellschaften vorgestellt und ein Tarifvergleich vorgenommen.

Nachdem bis dahin nur auf den momentanen Telekommunikationsmarkt eingegangen wird, werden nun die Faktoren vorgestellt, die vermutlich den Markt der Zukunft bestimmen werden. Dabei wird sowohl versucht, eine Vorhersage über das Aussehen der Telekommunikationsnetze und -dienste als auch über ihre Betreiber und Anbieter zu treffen.

2 Deregulierung

2.1 Öffnung des Telekommunikationsmarkts

Nach einem Beschluß der EU mußten bis zum 1.1.1998 in sämtlichen EU-Mitgliedsstaaten die staatlichen Telekommunikationsgesellschaften privatisiert und der Telekommunikationsmarkt unabhängigen Konkurrenten geöffnet werden. Um die rechtlichen Grundlagen dieses freien Markts festzulegen, wurde in Deutschland am 25.7.1996 das Telekommunikationsgesetz (TKG) [Bund96] verabschiedet, welches am 17.12.1997 abgeändert wurde. Erklärtes Ziel war es dabei, einen der liberalsten Telekommunikationsmärkte der Welt zu schaffen.

Der offizielle Zweck des Gesetzes ist es, „durch Regulierung im Bereich der Telekommunikation den Wettbewerb zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten sowie eine Frequenzordnung festzulegen." (siehe TKG, §1).

Ferner wird festgelegt, daß für diese Aufgaben der Bund zuständig ist, wobei aber die Zuständigkeiten des Verteidigungsministers unverändert bestehen bleiben. Der Bund hat dabei folgende Ziele zu verfolgen, außer wenn diese gegen das Gesetz gegen Wettbewerbsbeschränkungen verstoßen:

- Wahrung der Interessen der Nutzer
- Sicherstellung eines chancengleichen Wettbewerbs
- Sicherstellung einer flächendeckenden Grundversorgung zu erschwinglichen Preisen
- Förderung der Telekommunikation in öffentlichen Einrichtungen
- Sicherstellung einer vernünftigen Nutzung der Übertragungsfrequenzen
- Wahrung der öffentlichen Sicherheit

2.2 Regulierungsbehörde

Die *Regulierungsbehörde für Telekommunikation und Post* (Reg TP) [fTuP98] wurde zum 01.01.98 als Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft mit Sitz in Bonn errichtet. Die Regulierungsbehörde hat insoweit die Aufgaben des bisherigen Bundesministeriums für Post und Telekommunikation (BMPT) übernommen, das zum Jahresende 1997 aufgelöst wurde. Außerdem wurde das bisherige Bundesamt für Post und Telekommunikation (BAPT), das neben Ausführungsaufgaben nach dem TKG auch weitere Aufgaben (z. B. nach dem Gesetz über die elektromagnetische Verträglichkeit von Geräten) wahrzunehmen hat, in die Regulierungsbehörde integriert.

Laut TKG dient die Reg TP der „Wahrnehmung der sich aus diesem Gesetz und anderen Gesetzen ergebenden Aufgaben" (siehe TKG, §66, 1). Die Reg TP selbst sieht ihre Aufgaben wie folgt:

- Sicherstellung eines fairen Wettbewerbs
- Gewährleistung der notwendigen technischen Kooperation der Anbieter und Verhinderung von Diskriminierungen
- Berücksichtigung von Ökonomie und technischem Fortschritt bei den Regulierungsentscheidungen, um Fortschritt und Marktwachstum zu fördern

- Sicherung eines flächendeckenden und ausreichenden Angebotes an Kommunikations- und Postdienstleistungen

Teil der Reg TP ist der sogenannte *Beirat*, der sich aus jeweils neun Mitgliedern des Bundestags und des Bundesrats zusammensetzt und der weitreichende Kontrollfunktion hat, aber auch den Präsidenten und die Vizepräsidenten der Reg TP vorschlägt. Die täglichen Beschlüsse jedoch werden in sogenannten *Beschlußkammern* gefällt, die „nach Bestimmung des Bundesministeriums für Wirtschaft gebildet" werden (siehe TKG, §73, 2).

Kritiker sehen darin das wesentliche Problem der Reg TP. Einerseits ist die Reg TP Teil des Bundes und als solches auch direkt dem Bundeswirtschaftsminister unterstellt. Andererseits trifft sie Entscheidungen, die direkt oder indirekt die Deutsche Telekom AG (DTAG) betreffen, deren Hauptanteilseigner wiederum der Bund ist, da die DTAG aus der staatseigenen Post hervorgegangen ist und noch nicht vollständig privatisiert ist.

Es liegt nahe, zu unterstellen, daß der Bund bei der Regulierung des Telekommunikationsmarktes sehr eigene Interessen verfolgt. Tatsächlich haben sich sowohl Theo Waigl als auch Oskar Lafontaine in ihrer Funktion als Bundesfinanzminister verschiedentlich zu Regulierungsverfahren der Reg TP geäußert. Dabei ging es stets um die Höhe von Geldbeträgen, die die DTAG-Konkurrenten für die Nutzung bestimmter, durch die DTAG bereitgestellter, Leistungen zu zahlen hatten. Die Bundesfinanzminister forderten dabei stets einen höheren als den sich abzeichnenden Betrag.

Davon hätte die DTAG profitiert und damit auch der Bund. Schließlich hat dieser vor, als Abschluß der Post-Privatisierung seine verbliebenen DTAG-Anteile zu veräußern, die einen bedeutenden Wert darstellen, den man natürlich nicht gerne durch Entscheidungen der eigenen Regulierungsbehörde geschmälert sieht. Böse Zungen sprechen in diesem Zusammenhang von „Kohle für Lafontaine" und unterstellen dem Bundesfinanzminister, daß er durch den Verkauf der DTAG-Aktien seine Finanzen aufpolieren wolle.

2.3 Letzte Meile

Viel im Gespräch waren die Reg TP und vor ihr das BMPT vor allem durch das Regulierungsverfahren die viel diskutierte *letzte Meile* betreffend. Also solche bezeichnet man die Leitung, die von einer Ortsvermittlungsstelle zum Endteilnehmer geht, die *Teilnehmeranschlußleitung*. Die DTAG verfügt dabei über ein großes und dichtes Netz (eigentlich sehr viele einzelne Ortsnetze), an das praktisch alle Haushalte bereits angeschlossen sind oder problemlos angeschlossen werden können. Für ihre Konkurrenten ist es fast unmöglich, ein solches Netz aufzubauen, da hierzu umfangreiche, langwierige und kostenintensive Arbeiten nötig wären. Es wurden im Laufe der Jahre verschiedene Ansätze, wie zum Beispiel Funkübertragung, diskutiert, um das Problem der letzten Meile zu lösen, aber alle wurden bisher als unpraktikabel verworfen. Somit waren Regelungen notwendig, die es den DTAG-Konkurrenten ermöglicht, die bestehenden DTAG-Leitungen zu nutzen. Da dies von elementarer Bedeutung für den Telekommunikationsmarkt ist, werden im folgenden die entstandenen Lösungen vorgestellt, da sich anhand dieser feststellen läßt, wie der Bund den Telekommunikationsmarkt reguliert.

2.3.1 Gebühren

Die Regulierung sieht zwei mögliche Verfahren vor. Zum einen können einzelne Gespräche über einen DTAG-Konkurrenzgesellschaft geführt werden, wobei eine Gebühr auf Grundlage des sogenannten Interconnection-Tarifs fällig wird, den der Konkurrent an die DTAG zu entrichten hat. Zum anderen ist es möglich, daß der Kunde mit seinem Anschluß komplett

zu einem Konkurrenten wechselt und dieser eine monatliche Miete für den Netzzugang an die DTAG abführt. In der folgenden Tabelle 1 werden die Preisvorstellungen der DTAG und ihrer Konkurrenten für diese Dienste sowie eine relativ neutrale Kostenbewertung und die letztendliche Festsetzung durch BMTP bzw. Reg TP vorgestellt.

	Interconnection-Tarif	Miete des Netzzugangs
DTAG	6 Pf/min	47,26 DM/Monat
DTAG-Konkurrenz	2 Pf/min	12,50 DM Monat
Neutrale Bewertung	0,84 Pf/min (EU-Gutachten)	14,30 DM/Monat (Bundeskartellamt)
BMTP bzw. Reg TP	2,7 Pf/min	20,65 DM/Monat (vorläufig)

Tabelle 1: Gebührenvorstellungen

Zunächst fällt auf, daß die letztendliche Festsetzung in beiden Fällen Gebühren vorsieht, die sich zwischen den Forderungen der DTAG und ihrer Konkurrenten bewegen und sogar näher an den Vorstellungen der Konkurrenten liegen. Allerdings muß man andererseits feststellen, daß die Forderungen der DTAG in der Presse häufig als maßlos überhöht angesehen wurden. Zudem liegen die festgesetzten Gebühren jeweils auffallend weit über den Bewertungen durch relativ neutrale Institutionen. Es stellt sich die Frage, ob die Gebührenbeschlüsse nicht doch mit Rücksicht auf den Wert der DTAG-Aktie gefällt wurden.

Natürlich gelten diese Tarife nicht nur bei der Nutzung eines DTAG-Netzzugangs, sondern ebenso auch für die Netzzugänge aller anderen Telekommunikationsgesellschaften. Es ist jedoch so, daß zur Zeit praktisch nur die DTAG über Netzzugänge verfügt und daß hohe Gebühren für deren Nutzung dazu führen, daß nur Gesellschaften, die über sehr viel Kapital verfügen, um eigene Netzzugänge einrichten zu können, konkurrenzfähig zur DTAG sein könnten.

Zur besseren Beurteilung der festgelegten Gebühren folgt hier der Paragraph 24 des TKG, der die Maßstäbe der Entgeltregulierung festlegt:

> §24 Maßstäbe der Entgeltregulierung
>
> 1. Entgelte haben sich an den Kosten der effizienten Leistungsbereitstellung zu orientieren und den Anforderungen nach Absatz 2 zu entsprechen. Die Regelungen des §17 Abs. 1 und 2 und der auf Grund des §17 Abs. 2 erlassenen Rechtsverordnung bleiben unberührt.
> 2. Entgelte dürfen
>   (a) keine Aufschläge enthalten, die nur auf Grund der marktbeherrschenden Stellung nach §22 des Gesetzes gegen Wettbewerbsbeschränkungen eines Anbieters auf dem jeweiligen Markt der Telekommunikation durchsetzbar sind,
>   (b) keine Abschläge enthalten, die die Wettbewerbsmöglichkeiten anderer Unternehmen auf einem Markt der Telekommunikation beeinträchtigen, oder
>   (c) einzelnen Nachfragern keine Vorteile gegenüber anderen Nachfragern gleichartiger oder ähnlicher Telekommunikationsdienstleistungen auf dem jeweiligen Markt der Telekommunikation einräumen,
>
> es sei denn, daß hierfür ein sachlich gerechtfertigter Grund nachgewiesen wird.

2.3.2 Verlauf der Regulierung

Nachdem in Abschnitt 2.3.1 die zu entrichtenden Gebühren bei der Nutzung des Netzanschlusses eines Konkurrenzunternehmens vorgestellt wurden, soll im folgenden anhand des

noch laufenden Verfahrens zur endgültigen Feststellung des monatlichen Mietpreises für den Netzanschluß der Verlauf eines solchen Verfahrens geschildert werden ([Ditt98]):

- 1997: Das Bundespostministerium trifft die Entscheidung, den neuen Wettbewerbern entbündelten Zugang zu den Teilnehmeranschlußleitungen der DTAG zu gewähren. Die DTAG schließt daraufhin Verträge über den entbündelten Zugang zur Teilnehmeranschlußleitung.

- 14.01.1998: Die Regulierungsbehörde erteilt die vorläufige Genehmigung der Entgelte von 19 verschiedenen Zugangsmöglichkeiten zur Teilnehmeranschlußleitung (z.B. 28,80 DM monatlich für die Überlassung einer einfachen Kupferdoppelader). Die Genehmigung erfolgt vorbehaltlich einer abschließenden Prüfung der Entgelte anhand der von der DTAG eingereichten Kostenunterlagen.

- 10.03.1998: Der Antrag der DTAG über die Entgelte für den Zugang zur Teilnehmeranschlußleitung wird in seinen wesentlichen Punkten abgelehnt. Die Prüfung hat ergeben, daß nur ein Betrag von maximal DM 20,65 für die Überlassung der einfachen Kupferdoppelader genehmigungsfähig ist. Dieses Entgelt ergibt sich aus den von der DTAG selbst geltend gemachten Kosten. Die Reg TP setzt das Entgelt vorläufig auf 20,65 DM fest und fordert die DTAG auf, bis zum 22.05.1998 einen erneuten Antrag auf Entgeltgenehmigung vorzulegen, der die Prüfungsergebnisse berücksichtigt.

- 22.05.1998: Die DTAG beantragt eine Fristverlängerung. Die Reg TP verlängert daraufhin die Abgabefrist auf den 05.06.1998.

- 05.06.98: Die DTAG legt einen neu formulierten Antrag vor. Eine Entscheidung über das Entgelt für die Überlassung der Teilnehmeranschlußleitung ist nun bis zum 17.08.98 zu treffen. Die DTAG fordert in ihrem Antrag 47,26 DM für eine einfache Kupferdoppelader.

- DTAG und Reg TP einigen sich darauf, daß die DTAG ihren Antrag wieder zurückzieht und zu einem späteren Zeitpunkt erneut einreicht, um der Reg TP genügend Zeit zur Prüfung des Antrags zu geben. Das vorläufige Entgelt von 20,65 DM wird bis zum 30.11.1998 verlängert.

- 27.11.1998: Die DTAG zieht auf Empfehlung des Bundeswirtschaftsministers Müllers überraschend ihren inzwischen neu eingereichten Antrag zurück. Die Reg TP verlängert daraufhin das vorläufige Entgelt von 20,65 DM bis zum 30.4.1999.

3 Konkurrenten der Telekom

Seit Anfang dieses Jahres unterscheidet man insbesondere zwei Arten von Telefongesellschaften. Der *Teilnehmernetzbetreiber* ist dabei die Gesellschaft, die die Rechte an der Verkabelung des Telefonanschlusses selbst hat. Über ihn laufen sämtliche Ortsgespräche. In den meisten Fällen ist dies auch 1998 die Deutsche Telekom AG. In diesen Markt dringen die neuen Anbieter nur sehr zaghaft vor, da sie mit gewaltigen Investitionskosten rechnen müssen. Dennoch gibt es in einigen Städten bereits alternative Anbieter. Diese verkabeln im Augenblick jedoch bevorzugt Geschäftskunden mit großem Umsatz.

Ein *Verbindungsnetzbetreiber* hingegen bietet die Nutzung seiner Leitungen für Gespräche zwischen zwei verschiedenen Orten an. Viele Gesellschaften dieser Art ermöglichen im Augenblick jedoch nur registrierten Kunden einen Zugang zu ihren Leistungen.

3.1 Ansprüche des Kunden

Die Festlegungen der Ansprüche der Kunden gegenüber den Telekommunikationsanbietern verteilen sich über eine Reihe von Gesetzen und Verordnungen, vor allem das Telekommunikationsgesetz, die Telekommunikations-Kundenschutzverordnung, Telekommunikations-Entgeltregulierungsverordnung sowie die Telekommunikations-Universaldienstleistungsverordnung.

Darin werden zunächst die sogenannten *Universaldienstleistungen* definiert, die zur Grundversorgung gehören und damit jedem Kunden zu einem erschwinglichen Preis zugänglich sein müssen. Das bedeutet nicht, daß alle Telekommunikationsunternehmen diese Dienste anbieten müssen, sondern nur, daß an jedem Ort Deutschlands diese Dienste von mindestens einem Anbieter erbracht werden müssen. Ist dies nicht der Fall, kann die Reg TP die Erbringung erzwingen. Zu den Universaldienstleistungen gehören Sprachtelefonie, Fax- und Datenkommunikation, Dienste wie Anklopfen, Anrufweiterschaltung, Entgeltanzeige und Makeln. Außerdem hat der Kunde das Recht, in einem Telefonbuch aufgeführt zu werden und ihm muß eine Telefonauskunft zur Verfügung stehen.

Schließlich hat der Kunde noch spezielle Rechte gegenüber seinem Netzanbieter. Dieser ist verpflichtet ihm eine Rechnung auszustellen, in der auch sämtliche Ansprüche anderer Anbieter gegenüber dem Kunden aufgeführt sind. Der Kunde erhält also nur eine Rechnung und muß auch nur diese begleichen. Zudem hat er das Recht einen Einzelverbindungsnachweis zu fordern und er kann sogar eine Rechnungshöhe festlegen, die nicht ohne seine ausdrückliche Genehmigung überschritten werden kann. Außerdem kann der Kunde bestimmte Arten von Rufnummern sperren lassen, so daß diese von seinem Anschluß nicht mehr angewählt werden können.

3.2 Momentane Leistungen

Das Leistungsspektrum der verschiedenen Anbieter ist zur Zeit noch sehr unterschiedlich und meist auch sehr dünn. Abgesehen von Spezialleistungen, wie Anrufbeantwortern im Netz, existieren zur Zeit folgende Möglichkeiten, das Angebot der DTAG-Konkurrenten zu nutzen:

- Call-by-Call
  Mit *Call-by-Call* bezeichnet man ein Verfahren, das es ermöglicht, ein einzelnes Gespräch über den Anbieter seiner Wahl zu führen. Dazu wählt man vor der gewohnten Nummer zusätzlich eine sogenannte *Verbindungsnetzbetreiberkennzahl*, die stets mit 010 beginnt. Bei diesem Verfahren bindet man sich nicht an einen einzelnen Anbieter, sondern kann immer (abhängig von der Tageszeit und der Entfernung) den billigsten Anbieter benutzen. Um diesen Vorteil nutzen zu können, sollte man jedoch gut über die aktuellen Tarife informiert sein.

- Preselection
  Mit *Preselection* bezeichnet man ein Verfahren, das es ermöglicht, jedes Gespräch über einen bestimmten Anbieter seiner Wahl zu führen, ohne daß man dabei anders wählen müßte als bisher. Anfang 1998 war dies bei allen Telefonkunden die DTAG. Die meisten Anbieter versuchen derzeit, ihre Kunden mit langen Vertragslaufzeiten zu binden. Es scheint jedoch fraglich, ob es sinnvoll ist, sich im Moment an eine Gesellschaft zu binden, da der neue Telekommunikationsmarkt noch sehr jung ist und sich die Tarife der Anbieter in nächster Zeit sicherlich noch ändern werden.

- Callback
  Um mit *Callback* zu telefonieren, muß man zuerst einen sogenannten Lockruf absetzen.

Dazu wählt man eine von der Telefongesellschaft zugeteilte Telefonnummer und läßt es einmal klingeln, wobei keine Kosten entstehen. Der Computer der Gesellschaft registriert jedoch den Anruf, ruft einige Sekunden später zurück und bietet ein Freizeichen, das man nun als Angerufener zum Wählen nutzen kann. Dieser Service wird insbesondere im Mobilfunkbereich gerne genutzt, da die Tarife grundsätzlich auch für von Handies aus geführte Gespräche gelten, die bei anderen Anbietern häufig recht teuer sind. Allerdings berechnen die meisten Gesellschaften auch die Zeit, die man zum Wählen benötigt, was insbesondere kurze Gespräche recht teuer machen kann.

- Call-Through
  Um mit *Call-Through* zu telefonieren, ruft man ebenfalls eine gebührenfreie Nummer an und erhält dort, nach Eingabe einer persönlichen Identifikationsnummer, ein Freizeichen. Ebenso wie beim Callback ist dieser Service bei Handybenutzern recht beliebt, da auch hier häufig die gleichen Tarife gelten wie fürs Festnetz. Für innerdeutsche Gespräche innerhalb des Festnetzes ist dieser Service in der Regel jedoch nicht attraktiv.

Bei manchen dieser Verfahren, wie zum Beispiel bei Call-by-Call, wird vor dem Anruf kein Vertrag unterzeichnet und der Kunde erfährt auch beim Anruf nicht, zu welchem Tarif er telefoniert. Um sicherzustellen, daß der Kunde trotzdem über die ihm entstehenden Kosten informiert ist, bzw. zumindest sicherzustellen, daß er sich darüber informieren kann, gelten die in Paragraph 29 der Telekommunikations-Kundenschutzverordnung (TKV) festgelegten Veröffentlichungsfristen:

> §29 Veröffentlichungsfristen
>
> 1. Änderungen von Entgelten und entgeltrelevanten Bestandteilen Allgemeiner Geschäftsbedingungen marktbeherrschender Anbieter von Sprachtelefondienst und von Übertragungswegen treten frühestens einen Monat nach ihrer Veröffentlichung in Kraft. Die Frist gilt nicht für kurzzeitige ereignisbezogene Sondertarife. Informationen über neue Angebote marktbeherrschender Anbieter von Übertragungswegen sind so bald wie möglich zu veröffentlichen. Die Regulierungsbehörde kann eine Abweichung von der Frist nach Satz 1 in Einzelfällen genehmigen.
> 2. Bei genehmigungspflichtigen Entgelten und entgeltrelevanten Bestandteilen Allgemeiner Geschäftsbedingungen darf die Veröffentlichung nach Absatz 1 nicht vor Erteilung der Genehmigung erfolgen.

Allerdings gilt dieser Paragraph nur für marktbeherrschende Anbieter, wie auch viele andere Bestimmungen der verschiedenen den Telekommunikationsmarkt regelnden Gesetze. Von diesen Bestimmungen ist daher zur Zeit nur die DTAG betroffen, was einen erheblichen Nachteil für sie darstellt.

3.3 Major Players

Unter den Konkurrenten der DTAG stechen besonders drei durch ihre Größe hervor. Dies sind ARCOR, o.tel.o und VIAG InterKom. Interessant ist in diesem Zusammenhang, woher das Kapital dieser Unternehmen kommt, das heißt, wer die Anteilseigner sind. Diese sind in Tabelle 2 aufgeführt.

Als erstes fällt auf, daß sowohl ARCOR als auch VIAG InterKom große Telekommunikationsunternehmen wie AT & T und British Telecommunications als Anteilseigner bzw. als anteilslose Konsortialpartner haben, um sich so das nötige Know-How zu sichern, das nötig ist, um der DTAG in großem Maßstab Konkurrenz machen zu können.

ARCOR		o.tel.o		VIAG InterKom	
Mannesmann AG	74,9 %	VEBA AG	48.75 %	VIAG AG	45 %
Deutsche Bahn AG	25,1 %	RWE AG	51,25 %	British Telecommunications	45 %
Deutsche Bank AG				TELENOR AG	10 %
Unisource					
AT & T					
AirTouch					

Tabelle 2: Anteilseigner der drei großen DTAG-Konkurrenten

Zu diesem Zwecke noch wichtiger ist allerdings das Vorhandensein des nötigen Kapitals. Bei den Hauptkapitalgebern handelt es sich sämtlich um große Aktiengesellschaften. Interessanterweise sind darunter mehrere, die sich mit der Rolle des Monopolisten, die die DTAG einst einnahm, gut auskennen, nämlich die Deutsche Bahn AG sowie die Stromerzeuger VEBA AG und RWE AG.

Die Gründe für das Engagement dieser drei Unternehmen liegen in dem Wunsch mögliche Synergieeffekte zu nutzen. Als die Öffnung des Telekommunikationsmarkts abzusehen war, machten sich die zukünftigen Konkurrenten der DTAG unter anderem darüber Gedanken, wie man am einfachsten, kostengünstigsten und vor allem auch schnellsten ohne lange Rechtsstreits Kabel verlegen könne, um ein eigenes Telekommunikationsnetz aufzubauen. Recht schnell kam man auf die Idee, bestehende Verbindungen, wie zum Beispiel das Gleisnetz der Deutschen Bahn AG oder die Stromnetze der Stromerzeuger VEBA AG und RWE AG, zu diesem Zwecke zu nutzen. So wurden Verträge mit diesen Unternehmen geschlossen, bzw. diese Unternehmen gründeten eigene Telekommunikationsgesellschaften.

Von manchen Leuten wir o.tel.o allerdings keine große Chance am Markt eingeräumt, da sie den Stromerzeugern unterstellen, keine Erfahrung im Umgang mit den Endkunden zu haben und so deren Betreuung zu vernachlässigen. Bei eingehender Betrachtung erscheint dieses Argument allerdings falsch. Zum einen bringen sie sehr wohl Erfahrung in der Kundenbetreung mit, erstens durch die Vorgängerfirmen Meganet und Lion und zweitens durch das Mobilfunknetz E-Plus. Zum anderen ist auch die DTAG nicht gerade für ihre gute Kundenbetreuung bekannt, schließlich mußte man sich als Monopolist darum bisher nicht besonders kümmern, da die Kunden ja auf einen angewiesen waren.

In Tabelle 3 findet sich als Abschluß ein Vergleich zwischen der DTAG und ihren drei Hauptkonkurrenten. Dabei wird zum einen deutlich, daß es im Telekommunikationsmarkt um Milliardenbeträge geht. Zum anderen zeigt der Vergleich aber auch, daß zwischen den einzelnen Gesellschaften sehr große Unterschiede in der Investitionshöhe bestehen und die DTAG noch weit vor ihrer Konkurrenz liegt. Anzumerken ist noch, daß, während die DTAG-Konkurrenten sich noch im Aufbau befinden und Mitarbeiter einstellen, die DTAG damit beschäftigt ist, ihre Struktur zu verschlanken, und daher versucht ihren Mitarbeiterstamm abzubauen.

3.4 Weitere Konkurrenten

Vor der Öffnung des deutschen Telekommunikationsmarkts rechneten die meisten Gesellschaften damit, daß sich das bestehende Monopol in ein Oligopol, also in einen Markt, der von wenigen großen Unternehmen beherrscht wird, wandelt. Diese Vorstellung stellte sich als falsch heraus. Durch die Interconnection-Tarife war es nicht mehr nötig, große Geldsummen in den Aufbau von neuen Ortsnetzen zu investieren. Dies ermöglichte auch kleineren Unternehmen

	Telekom	ARCOR	o.tel.o	VIAG InterKom
Festnetz(km)	686.000	40.000	11.000	k.A.
Mobilfunkkunden	D1	D2	E-Plus (30%)	E 2 (Start 6/98)
(in Millionen)	2,4	2,5	0,5	k.A.
Investitionen	100 Mrd.	4 Mrd.	7 Mrd.	7 Mrd.
(bis zum Jahr)	2001	2001	2005	2007
Umsatz	63 Mrd.	Gewinn	7-9 Mrd. im	10-11 Mrd. im
	(1996)	ab 2000	Jahr 2005	Jahr 2007
Mitarbeiter	ca. 190.000	7.000	2.500	450

Tabelle 3: Vergleich zwischen der DTAG und ihren Hauptkonkurrenten

ACC	Hutchison	NetNet	Telepassport
Arcor	Interoute	NewTel	Tesion
Citycom	Isis	Nikoma	UPX
Deutsche Telekom AG	KDD-CONOS	O.Tel.O	VEW Telnet
EWE Tel	KielNet	RSL Com	Viag Interkom
Debitel	KomTel	Star Telecom	Viatel
DPLus	Microcall	Talkline	Victor Vox
First Telecom	Mobilcom	TelDaFax	Westcom
GermanBusinessNet	Mox Telecom	Tele2	Worldcom
HanseNet	Netcologne	TeleBridge	

Tabelle 4: Telekommunikationsanbieter

mit weniger Kapital, den Endkunden Telekommunikationsdienste anzubieten. Die Tabelle 4 zeigt eine (unvollständige) Liste der Anbieter.

Abgesehen von der DTAG und ihren in 3.3 vorgestellten drei großen Konkurrenten handelt es sich bei diesen Anbietern meist um Unternehmen mit geringem Kapital, die weitgehend auf das Verlegen eigener Leitungen verzichten, sondern von den großen Unternehmen Übertragungskapazitäten mieten. Diese nutzen sie fast ausschließlich zur Sprachübertragung und verzichten auf das Anbieten weiterer Leistungen. Wie Tabelle 5 zeigt, liegen ihre Gebühren dabei allerdings meist weit unter denen der DTAG.

	R50	R50 (DTAG)	Fern	Fern (DTAG)
21 - 2 Uhr	7,5 (Arcor)	12,1	9 (Talkline)	20,2
2 - 5 Uhr	6,1 (DTAG)	6,1	6,1 (DTAG)	6,1
5 - 9 Uhr	9 (Talkline)	16,1	9 (Talkline)	32,3
9 - 12 Uhr	14 (TeleBridge)	27,9	16 (Viatel)	55,8
12 - 18 Uhr	14 (TeleBridge)	24,2	16 (Viatel)	51,9
18 - 21 Uhr	9 (Viatel)	16,1	9 (Viatel)	32,2

Tabelle 5: Gebühren in Pf/min (Stand vom 24.12.1998)

Eine besondere Rolle nehmen lokale Anbieter, wie zum Beispiel Netcologne ein. Ihr Angebot ist meist auf einen städtischen Ballungsraum beschränkt. Dort versuchen sie, bereits verlegte Leitungen, die nicht im Besitz der DTAG, sondern zum Beispiel der Stadt sind, zu nutzen. Im Gegensatz zu anderen DTAG-Konkurrenten können sie so auch günstige Ortsgespräche und Internetzugänge anbieten. Solche Anbieter existieren unter anderem in Köln und Berlin,

weitere werden wohl noch folgen. Auch in der Region Karlsruhe steht ein Anbieter (Telemaxx) in den Startlöchern, bei dem die Kommunen eine tragende Rolle spielen wollen.

3.5 Vergleichende Umfrage

Vom 23. Juli 1998 bis zum 31. August 1998 führte www.billiger-telefonieren.de zusammen mit der Zeitschrift 0-800 eine Umfrage durch, um die Leistungen der neuen Anbieter im Vergleich zur DTAG zu beurteilen. Bewertet wurden dabei:

- Verfügbarkeit der Leitungen
- Verständlichkeit der Tarife und Preis-/Leistungsverhältnis
- Erreichbarkeit der Hotline, sowie Kundenfreundlichkeit und Kompetenz ihrer Mitarbeiter
- Korrektheit und Verständlichkeit der Abrechnung

Dabei schnitten die neuen Anbieter weit besser ab als die DTAG, die einzig in der Verfügbarkeit der Leitungen ihre Konkurrenten schlagen konnte. In fast allen anderen Bereichen nahm die DTAG den letzten Platz ein, teilweise sogar weit abgeschlagen. Allerdings sollte berücksichtigt werden, daß die Verfügbarkeit der Leitungen für die meisten Kunden das wichtigste Bewertungskriterium sein dürfte. Schließlich hilft ein günstiger Tarif nichts, wenn aus dem Telefonhörer nur das Besetztzeichen klingt. Auffallend ist, daß gerade die günstigsten Anbieter auch die schlechtesten Leitungsverfügbarkeiten aufwiesen. Ähnlich gut wie die DTAG schnitten hier vor allem die zwei großen Anbieter o.tel.o und Arcor ab, deren Tarife allerdings nicht zu den günstigsten zählen, wenn sie auch einiges unter denen der DTAG liegen.

Ein weiteres interessantes Ergebnis der Umfrage ist, daß in der Bewertung der Hotline ausgerechnet o.tel.o, denen Kritiker ja mangelnde Erfahrung in der Kundenbetreuung unterstellen, eindeutiger Sieger in allen drei Kategorien wurde.

Als Gesamtsieger der Umfrage kann man wohl o.tel.o und Arcor betrachten, da diese in fast allen Bereichen unter den vorderen Plätzen zu finden sind. Der eindeutige Verlierer hingegen ist die DTAG.

4 Der Markt von Morgen

4.1 Bestimmende Elemente

Aus technischer Sicht wurde die Entwicklung des Telekommunikationsmarkts in Deutschland in den letzten Jahren von der Digitalisierung des Netzes bestimmt. Damit sind Sprach- und Datennetze nahe zusammengerückt, es besteht praktisch kein Unterschied mehr zwischen ihnen.

Das digitale Netz ermöglicht nun völlig neue Angebote. In Zukunft werden dem Kunden neben der herkömmlichen Sprachtelefonie auch Dienste wie Sprachvermittlung, Fernsteuerung von Hausfunktionen, universelle Mailboxen oder Mobilfunknavigation geboten werden. Für Unternehmen werden weitere Angebote wie virtuelle Privatnetze oder die Auslagerung von Funktionalitäten der bisherigen Nebenstellenanlagen zum Telekommunikationsanbieter hinzukommen. Der Konkurrenzkampf zwischen den Anbietern wird sich auf diese Angebote ausweiten.

Marktbestimmend werden auch neue Übertragungstechniken sein. Insbesondere kann durch die Nutzung von Stromkabeln oder dem TV-Kabelnetz zur Datenübertragung das Problem der letzten Meile gelöst werden. Unternehmen könnten dann unabhängig von der DTAG Ortsnetzzugänge zu vernünftigen Preisen anbieten.

Dies ist besonders auch durch die immer weiter steigende Bedeutung des Internets interessant. Ein günstiger Zugang zum Internet wird immer mehr zum Entscheidungskriterium bei der Auswahl eines Telekommunikationsanbieters werden. Das Internet macht jedoch keinen Unterschied zwischen Nah- und Ferngesprächen. Wichtig ist allein eine günstige Verbindung zu einem günstigen Provider. Vor allem ist es auch möglich, über das Internet zu telefonieren (Stichwort: iphone). Eine Verbreitung der Internettelefonie würde einen Einheitstarif für Telefongespräche bedeuten, so daß von vielen der „Kampf ums Ortsnetz" mit dem Kampf um den ganzen Telekommuikationsmarkt gleichgesetzt wird.

4.2 Firmen

Bis auf weiteres wird die DTAG ihre marktbeherrschende Stellung wohl nicht verlieren. In der Vergangenheit hat sie die Telefongebühren kaum gesenkt und ihren beträchtlichen Gewinn (1997 ca. 50 Mrd DM Umsatz und 10 Mrd DM Gewinn!) stattdessen in den Ausbau des eigenen Netzes gesteckt. Nun besitzt sie das vermutlich modernste Telekommunikationsnetz der Welt, während ihre Konkurrenten immer noch über keine nennenswerten Netze verfügen. Anscheinend beginnt die DTAG daher jetzt damit, auch die Gebühren denen der anderen Anbieter anzugleichen. Zum 1.1.1999 erfolgt eine erste, inzwischen von der Reg TP genehmigte, Gebührensenkung, bei der die Preise bis zu 65% fallen.

Dies ist auch nötig, da die DTAG sonst das Risiko eingeht, daß zu viele ihrer Kunden zu den neuen, billigeren Anbietern wechseln, die später schwer zurückzugewinnen sind. Der Telekommunikationsmarkt in Deutschland befindet sich zur Zeit in einem andauerndem Preiskampf. Immer wieder tauchen Preisbrecher auf, die die Konkurrenten zwingen, ebenfalls Gebührensenkungen vorzunehmen. Insbesondere lokale Anbieter können ihren Kunden oft Preise offerieren, die weit unter den bisherigen liegen.

Dieser stetige Preiskampf wird dazu führen, daß viele der momentan vorhandenen Anbieter vom Markt verschwinden. Manchen von ihnen wird es gelingen, in Nischen zu überleben, doch wird es ihnen auf Dauer nicht möglich sein, in allen Bereichen des Markts der Konkurrenz zu trotzen. Die besten Chancen haben die großen Firmen, da diese über das nötige Kapital verfügen, auch einen längeren Preiskampf durchzustehen. Experten erwarten jedoch, daß auch ihre Zahl von vier auf höchstens drei schrumpfen wird. Sie vermuten, daß die DTAG, Arcor und einer der beiden anderen Anbieter überleben wird. Der Vergleich der großen Anbietern in Abschnitt 3.3 und die in Abschnitt 3.5 vorgestellte Umfrage legen nahe, daß dies o.tel.o sein wird.

Schwer vorhersagbar, aber recht wahrscheinlich, ist das Auftauchen völlig neuer Anbieter. In Amerika drängen jetzt schon Unternehmen wie Cisco, die bislang nur als Netztechnik-Hersteller fungierten, in den gesamten Telekommunikationsmarkt. Neue Technologie wird den Kampf um die Telekommunikationsmärkte der ganzen Welt stark beeinflussen und die Anbieter dieser Technologie werden an Bedeutung gewinnen.

Doch die großen Unternehmen stehen auch dieser Entwicklung wesentlich sicherer gegenüber als die kleinen. Schließlich verfügen sie über das nötige Kapital, um technisches Know-How in Form von ganzen Unternehmen einfach aufzukaufen. Dies ist schon häufig geschehen, man denke nur an den Software-Giganten Microsoft.

5 Resumé

Die Liberalisierung des deutschen Telekommunikationsmarkts ist weitgehend abgeschlossen, zahlreiche Anbieter tummeln sich auf dem entstandenen Markt. Die Regulierung des Netzzugangs steht allerdings immer noch aus. Generell kann man sagen, daß die Motivation der Reg TP zweifelhaft ist. Sie hat in der Vergangenheit mehrere Entscheidungen gefällt, die vermutlich stark an den Interessen der DTAG und damit des Bundes orientiert waren. Dies kann man nicht gerade als Zeichen eines liberalen Markts werten, die Liberalisierung kann also erst dann wirklich als abgeschlossen gelten, wenn der Bund seine Anteile an der DTAG veräußert hat.

Die neuen Anbieter bestehen aus zwei Gruppen. Zum einen sind dies die drei major players, Arcor, o.tel.o und Viag Interkom, die versuchen, der DTAG auf allen Gebieten Konkurrenz zu machen. Zum anderen existieren zahlreiche kleine Unternehmen, die sich hauptsächlich gemieteter Übertragungskapazitäten bedienen und sich auf die Sprachtelefonie beschränken. Eine gewisse Sonderstellung haben einige Unternehmen inne, die ihre Dienste nur regional anbieten, meist auf ein Ballungszentrum wie Köln oder Berlin beschränkt.

Grundsätzlich hat ein Kunde zwei verschiedene Möglichkeiten zu telefonieren. Entweder er bindet sich fest an einen Anbieter oder er wählt bei jedem Gespräch den Telekommunikationsanbieter neu aus. Bei der festen Bindung (Preselection) versuchen die Unternehmen jedoch meist, Verträge mit langen Laufzeiten abzuschließen. Zur Zeit tobt aber noch ein heftiger Preiskampf zwischen den Unternehmen und es scheint nicht ratsam, sich zu diesem Zeitpunkt schon auf einen Anbieter festzulegen.

Ein Vergleich der derzeit existierenden Anbieter zeigt, daß das Angebot der neuen Anbieter dem der DTAG offenbar überlegen ist. Insbesondere Arcor und o.tel.o schneiden dabei gut ab. Die DTAG hat jetzt jedoch auch damit begonnen, recht massiv ihre Preise zu senken. Der momentan herrschende Preiskampf wird vermutlich dazu führen, daß viele Unternehmen vom Markt verschwinden oder in Nischen gedrängt werden.

Andererseits ist es auch wahrscheinlich, daß noch völlig neue Unternehmen auf den Markt drängen werden, insbesondere Unternehmen, die über moderne Übertragungstechnologie verfügen. Der Markt der Zukunft wird wesentlich von neuer Technologie, neuen Diensten und auch der Verknüpfung mit dem Internet gestaltet werden. Die genaue Entwicklung des Markts ist leider nur sehr schwer absehbar, da sie sehr stark von neuen Technologien abhängt, die zur Zeit noch gar nicht existieren, und da die Telekommunikationstechnik sich allgemein sehr schnell entwickelt. Auch hier gilt Moore's Law: Alle 18 Monate kommen neue Produkte auf den Markt, deren Preis-Leistungs-Verhältnis sich um das Vierfache verbessert.

Nur eines scheint sicher: Wer den Telekommunikationsmarkt beherrschen will, oder sich zumindest als großer Anbieter etablieren will, braucht viel Kapital.

Literatur

[Arco98] Mannesmann Arcor. *Homepage von Mannesmann Arcor, http://www.arcor.de.* 1998.

[Bund96] Bund. *Telekommunikationsgesetz (TKG), http://www.regtp.de/Rechtsgrundlagen/tkg1.pdf.* 1996.

[Bund97a] Bund. *Telekommunikations-Kundenschutzverordnung (TKV), http://www.regtp.de/Rechtsgrundlagen/tkv.pdf.* 1997.

[Bund97b] Bund. *Telekommunikations-Universaldienstleistungsverordnung (TUDLV), http://www.regtp.de/Rechtsgrundlagen/tudlv.pdf.* 1997.

[Bund98] Bund. *Telekommunikations-Entgeltregulierungsverordnung (TEntgV), http://www.regtp.de/Rechtsgrundlagen/Tentgv.pdf.* 1998.

[Ditt98] Karl Heinz Dittberner. *Telekom-Offline, http://userpage.fu-berlin.de/~dittbern/Telekom.* 1998.

[fTuP98] Regulierungsbehörde für Telekommunikation und Post. *Homepage der RegTP, http://www.regtp.de.* 1998.

[Inte98] Viag Intercom. *Homepage von Viag Intercom, http://www.viagintercom.de.* 1998.

[Maga98a] Manager Magazin. *Diener aus der Steckdose.* September 1998.

[Maga98b] Manager Magazin. *Jeder gegen jeden.* September 1998.

[Maga98c] Manager Magazin. *Kampf ums Netz.* September 1998.

[O.te98] O.tel.o. *Homepage von O.tel.o, http://www.o-tel-o.de.* 1998.

[Salm98] Thilo Salmon. *Billiger telefonieren, http://www.billiger-telefonieren.de.* 1998.

[Tele98] Telekom. *Homepage der Deutschen Telekom AG, http://www.dtag.de.* 1998.

[Wess98] Holger Wess. *Telefongeschichte, http://stud.fbi.fh-darmstadt.de/~wess.* 1998.