Universität Karlsruhe
Fakultät für Informatik
Institut für Telematik
76128 Karlsruhe

Netzwerk-Management und Hochgeschwindigkeits-Kommunikation

Teil XV

Seminar WS 1996/97

Herausgeber:
Roland Bless
Elmar Dorner
Markus Hofmann
Claudia Schmidt
Jochen Seitz

Universität Karlsruhe
Institut für Telematik

Interner Bericht 5/97
ISSN 1432–7864

Zusammenfassung

Der vorliegende Interne Bericht enthält die Beiträge zum Seminar „Netzwerk-Management und Hochgeschwindigkeits-Kommunikation“, das im Wintersemester 1996/97 zum fünfzehnten Mal stattgefunden hat.

Die Themenauswahl kann grob in folgende vier Blöcke gegliedert werden:

1. Ein Block ist der Mobilkommunikation gewidmet. Hier werden die aktuellen Entwicklungen zuerst anhand von *UMTS* aufgezeigt, einem europäischen Projekt zur Standardisierung eines umfassenden Mobilfunksystems der 3. Generation. Anschließend folgen Beiträge zur Technik des digitalen Radiosystems *DAB* (das auch als Datenverteildienst genutzt werden kann) sowie zum *„Drahtlosen ATM“*.

2. Ein zweiter Block beschäftigt sich mit grundlegenden Techniken in ATM-Netzwerken. Hier werden zum einen *Routing-Mechanismen* vorgestellt und zum anderen der *ABR-Dienst* erläutert.

3. Der dritte Block umfaßt den Themenbereich *Internet*. Hier werden neuere Entwicklungen anhand von *IPv6* und *TCPng* aufgezeigt. Schließlich werden noch Charakteristiken des *Multicast Backbone* (MBone) untersucht.

4. Im vierten Block werden Netztechnologien im LAN/MAN-Bereich vorgestellt. Hier werden die Standards zum *Fast Ethernet* und Grundlagen zum Thema *„Corporate Networks“* präsentiert.

Abstract

This Technical Report includes student papers produced within small lessons called seminar of “Network Management and High Speed Communications”. For the fifteenth 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 mobile communication. At first, a European standardization project for mobile systems of the third generation called *UMTS* is presented. Subsequently, a description of a European standard for digital audio broadcasting called *DAB* follows. The last topic of this block is about *„Wireless ATM“*.

2. A second block deals with *routing mechanisms* and the *ABR service* in ATM networks.

3. The third block contains topics grouped around the *Internet*. Current developments such as *IPv6* and *TCPng* are described as well as characteristics of the *multicast backbone* (MBone).

4. The fourth area covered by the seminar deals with LAN/MAN technologies. At first, standards for *fast ethernet*, and, finally fundamentals of *corporate networks* are presented.

Inhaltsverzeichnis

Vorwort

Das Seminar „Netzwerk-Management und Hochgeschwindigkeits-Kommunikation“ erfreute sich in den letzten Jahren immer größerer Beliebtheit. Gerade heutzutage sind Stichworte wie „ATM“, „Quality of Service“, „Mobil-Kommunikation“ oder „Internet“ in aller Munde. Daher sind die Forschungsgebiete in diesen Bereichen auch von allgemeinem Interesse, so daß sie eine derartige Vielzahl von innovativen Arbeiten aufweisen können, deren Behandlung in anderen Lehrveranstaltungen so detailliert nicht möglich ist.

Jetzt liegt auch der nunmehr fünfzehnte 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 ausgesprochen gute Resonanz bei den Studenten hat uns veranlaßt, auch im Sommersemester 1997 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:

UMTS - Universal Mobile Telecommunication System

Mit zunehmender Bedeutung der weltweiten Rechnerkommunikation wächst auch der Wunsch zur Mobilität. Was beim Telefon mittlerweile schon zu einer Selbstverständlichkeit geworden ist – die weltweite Erreichbarkeit – befindet sich im Bereich der Datenkommunikation noch im Anfangsstadium. Die Entwicklung von UMTS soll die Integration von traditionellem drahtlosen Telefondienst und Datenkommunikation im mobilen Umfeld erreichen. Der vorliegende Beitrag beschreibt die Einsatzgebiete und deren Anforderungen an ein zukünftiges drahtloses Kommunikationssystem.

Drahtloses ATM

Das B-ISDN-Netz wir als diensteintegrierendes, multimediafähiges Netz verstanden. Das zugrundeliegende ATM-Vermittlungskonzept unterscheidet verschiedene ATM-Dienstklassen, die abhängig von den Bedürfnissen der jeweiligen Anwendung gewählt werden können. Die Vorteile von ATM sollen nun auch in zukünftige drahtlose Netze Eingang finden. Dieser Beitrag beschreibt das neue Konzept „drahtloses ATM“ und grenzt es gegenüber bestehenden drahtlosen Kommunikationssystemen ab.

Digital Audio Broadcasting – Grundlagen

Der UKW-FM-Rundfunk wurde bei seiner Entwicklung vor ca. 40 Jahren für den stationären Empfang mit einer Antenne in 10m Höhe konzipiert. Die Wiedergabe ist im Vergleich zur CD deutlich hörbar schlechter und nimmt beim mobilen Empfang weiter

ab. DAB wurde entwickelt, um unter anderem eine mit der CD vergleichbare Wiedergabequalität zu ermöglichen. Weitere Aspekte waren ein breiteres Programmangebot und die Möglichkeit, Datenprogramme anbieten zu können. Im Rahmen dieses Beitrags sollen die physikalisch/technischen Grundlagen von DAB näher beleuchtet werden.

Routing in ATM- und „Multiprotokoll über ATM“-Netzwerken

Für private ATM-Netzwerke wurde innerhalb des ATM-Forums das PNNI-Protokoll als flexibles und mächtiges Routingprotokoll entwickelt. Zusätzlich muß jedoch in heterogenen Netzwerken das Routing von mehreren Vermittlungsschichtprotokollen wie beispielsweise IP, IPv6 oder CLNP über ATM betrachtet werden. Diese Protokolle sind in der Regel verbindungslos und daher muß in den Routern für jedes einzelne Paket eine Routingentscheidung getroffen werden. Im Gegensatz dazu werden in ATM-Netzwerken virtuelle Verbindungen aufgebaut, welche den Datenpfad für alle Zellen der Verbindung festlegen. In dem vorliegenden Beitrag wird zunächst das PNNI-Routingprotokoll vorgestellt. Anschließend werden die Probleme einer „Multiprotokoll über ATM-Umgebung“ und erste Lösungsansätze für diesen Bereich diskutiert.

Der ABR-Dienst und Mechanismen zur Verkehrskontrolle in ATM-Netzwerken

In ATM-basierten Netzwerken wird beim Verbindungsaufbau die Dienstqualität über mehrere Qualitätsparameter ausgehandelt und in einem Dienstvertrag festgelegt. Im Gegensatz zu Audio und Video, ist bei Datenübertragungen das Verkehrsaufkommen nicht direkt spezifizierbar, wobei aber oftmals auch keine Garantie von Durchsatz und Verzögerung erforderlich ist. Vor diesem Hintergrund wurde der ABR-Dienst (Available Bit Rate) definiert, der speziell den Datenanwendungen die aktuell verfügbare Bandbreite anbietet. Mechanismen zur Verkehrskontrolle dienen dabei zum Austausch der für den ABR-Dienst benötigten Informationen. In diesem Beitrag werden zunächst die Charakteristiken des ABR-Dienstes im Vergleich mit weiteren ATM-Diensten beschrieben und anschließend Verfahren zur Verkehrskontrolle vorgestellt.

IPv6 - Das Internet Protokoll der nächsten Generation

Mit zunehmender Bedeutung der weltweiten Rechnerkommunikation wächst die Anzahl der Kommunikationsteilnehmer und der zu verbindenden Netzsegmente im Internet. Der Einsatz etablierter Protokollarchitekturen, wie beispielsweise TCP/IP, führt in diesem Zusammenhang zu Problemen im Bereich der Adressierung und der Vermittlung von Datenpaketen. Aus diesem Grunde wurde von der IETF, der Internet Engineering Task Force, ein neues Internet-Protokoll mit der Bezeichnung IPv6 standardisiert. Im Rahmen des Beitrages werden dessen Merkmale und mögliche Migrationsstrategien aufgezeigt.

TCPng - Aktuelle Entwicklungen im Transportbereich des Internet

Mit der Einführung des neuen Internet Protokolls IPv6 müssen zwangsläufig auch Modifikationen am Transportprotokoll des Internet, dem Transmission Control Protocol (TCP), vorgenommen werden. In diesem Zusammenhang wird in der Internet-Gemeinde derzeit über die Spezifikation einer komplett neuen TCP-Version nachgedacht. Als Alternative werden momentan einige Modifikationen in die bewährte Protokollversion eingearbeitet. Der Beitrag zeigt zunächst auf, warum das derzeitige TCP nur eingeschränkt für den Einsatz in modernen Hochleistungsnetzen geeignet ist und stellt darauf aufbauend konkrete Lösungsansätze vor.

Charakteristiken des Multicast Backbone (MBone)

Mit dem Aufkommen computergestützter Teamarbeit kommt der Entwicklung und Implementierung von Multicast-Protokollen einer Schlüsselrolle in der modernen Rechnerkommunikation zu. Neuartige Protokolle müssen sowohl den Anforderungen der Benutzer als auch den technologischen Gegebenheiten der zugrundeliegenden Netzdienste gerecht werden. Aus diesem Grunde wurde mit dem Multicast Backbone (MBone) ein prototypisches Netzwerk etabliert, welches die Bewertung der Gruppenkommunikation im Internet ermöglicht. Der Beitrag stellt überblickartig die Architektur und die Funktion des MBone dar und erläutert die derzeitige Fehlercharakteristik des Netzes und das Verhalten der MBone-Benutzer.

FastEthernet - Die Standards

Obwohl der Asynchrone Transfer Modus als Hochgeschwindigkeitsstandard für alle Netztopologien konzipiert ist, gibt es derzeit Probleme, ihn in heterogenen lokalen Netzen einzusetzen. Dort halten Weiterentwicklungen des CSMA/CD-Standards ihren Einzug. Leider existieren unterschiedliche Standards (100Base-T4, 100Base-TX/FX, 100VG-AnyLAN), die zudem noch in der verwendeten Kabeltechnik variieren können. Diese Standards und weitere Möglichkeiten zur hochleistungsfähigen Vernetzung im lokalen Bereich sind Thema dieses Beitrags.

Corporate Networks

Weg vom lokalen hin zum globalen Rechnernetz führt der abschließende Beitrag. Um der Tatsache Rechnung zu tragen, daß in expandierenden Unternehmen, deren Niederlassungen über die gesamte Weltkugel verstreut sind, dennoch effizient und kostengünstig Informationen ausgetauscht werden können, werden Dienste für sogenannte „Corporate Networks“ angeboten. Diese Netzwerke stellen Voraussetzungen sowohl an die Unternehmen, die solche Netze betreiben wollen, als auch an die Anbieter der Dienste, insbesondere, wenn ein weltweites Unternehmen ein sogenanntes „International Virtual Private Network“ betreiben will.

UMTS - Universal Mobile Telecommunication System

Christian Trefz

Kurzfassung

Die Mobilkommunikation und ihre Anwendungen stecken noch in den Kinderschuhen. Die Mobilität mit dem Computer bringt in vielen Bereichen neue Freiheiten und Möglichkeiten mit sich. Die Leistungskenndaten im Bereich der Mobilkommunikation unterscheiden sich jedoch um Größenordnungen von denen herkömmlicher Festnetze. Die Übertragungskapazitäten in Mobilnetzen sind, bei wesentlich höheren Fehlerraten, wesentlich niedriger als in traditionellen Festnetzen. Aus diesem Grund entsteht wohl der Bedarf an neuen bzw. angepaßten Anwendungen, die den Faktor Mobilität entsprechend berücksichtigen.

In diesem Beitrag sollen die einzelnen Überlegungen und Vorschläge zum Thema UMTS vorgestellt werden. Von besonderem Interesse sind dabei die Anforderungen, die an das neue System gestellt werden und welche Erfahrungen damit verbunden sind.

1 Einleitung

Es wird allgemein angenommen, daß zur Jahrtausendwende jeder zweite Anruf mit einem mobilen Endgerät geführt wird. Die zur Verfügung stehenden breitbandigen Festnetzdienste werden die Nutzer auch mobil nutzen wollen. Es werden verschiedene Arten von mobilen Endgeräten zum Einsatz kommen, vom einfachen Handy bis zum kompletten Terminal für Video- und Datendienste. Notebooks und Palmtop-Computer sind der erste Schritt auf dem Weg zur ortsunabhängigen Kommunikation. Mobilfunkgeräte und Funkmodem stellen einen weiteren Schritt dar, d.h. den Übergang zur mobilen persönlichen Kommunikation (PCN, Personal Communication Network). PCN bedeutet für den Benutzer:

- Rufnummern werden nicht mehr Endgeräten, sondern Personen zugeordnet.
- Jeder Teilnehmer hat mindesten eine persönliche Rufnummer, unter der er prinzipiell immer und überall erreichbar ist.
- Das Netz ist in der Lage, automatisch den Aufenthaltsort eines Teilnehmers zu lokalisieren und ihm dort die persönlichen Leistungs- und Dienstmerkmale zur Verfügung zu stellen.

Allerdings sind die Mobilfunksysteme der 2. Generation[1] den obigen Anforderungen nicht gewachsen.

Deshalb wurde 1992 auf der *World Administrative Radio Conference*[2] (WARC) eine Bandbreite von 230 MHz bei dem Frequenzband um 2 GHz[3] ab dem Jahr 2000 für Mobilfunksysteme der 3. Generation zur Verfügung gestellt. Ein Konsortium von 26 europäischen Institutionen hat daraufhin mit der Entwicklung des *Universal Mobile Telecommunications System* (UMTS) begonnen. Unter der Leitung der Europäischen Union (EU) beschäftigt man sich im *European Telecommunications Standards Institute* (ETSI) und der *Commission of the European Community* (CEC) mit den entsprechenden Standardisierungen und Produkten.

Im Rahmen dieses *Research into Advanced Communication in Europe* - Programms (RACE) wurden folgende Projekte ins Leben gerufen:

- **MONET** – Rahmenarbeit über Netzwerkstandards
- **CODIT** – Einsatz des Code Division Multiple Access (CDMA) - Verfahrens
- **ATDMA** – Einsatz des Time Division Multiple Access (TDMA) - Verfahrens
- **MAVT** – Entwicklung neuer Video- und Audio-Kodieralgorithmen
- **TSUNAMI** – Anpassung der Antennensysteme an UMTS
- **SAINT** – Integration von Satelliten in UMTS

Beteiligt an den Projekten sind sowohl Universitäten und Forschungsinstitute als auch Betreiber von Telekommunikationsdiensten und Hersteller von Mobilfunksystemen. Ziel dieser Projekte ist es, ein universelles Mobilkommunikationsnetz zu schaffen und die Entwicklung entsprechender Endgeräte voranzutreiben.

Parallel zu UMTS, das europaweit entwickelt wird, erfolgt eine weltweite Standardisierung unter dem Namen *Future Public Land Telecommunication System*[4] (FPLMTS) durch die *International Telecommunications Union* (ITU).

2 UMTS aus Sicht des Benutzers

UMTS wird als allgemeines Mobilkommunikationsnetz der Zukunft bezeichnet. Dabei ist die Gestaltung von UMTS noch nicht fest definiert. Daher macht es durchaus Sinn, derzeitige Probleme zu betrachten und daraus ein Benutzerprofil und Anwendungsmerkmale für UMTS zu erarbeiten. Es soll — ähnlich wie ATM im Festnetz bestehende Netzwerktopologien vereint — als technologieübergreifendes Kommunikationssystem folgende Probleme lösen:

[1] GSM, DCS (Digital Cellular System), DECT (Digital European Cordless Telephone), CT1/2 (Cordless Telephone), usw., siehe auch Seite 3

[2] WARC ist eine ITU-Konferenz, die zuletzt 1992 stattfand und Entscheidungen bezüglich der Frequenz-Zuweisung bis zum Jahr 2010 getroffen hat.

[3] genauer: 1885 - 2025 MHz und 2110 - 2200 MHz

[4] wurde mittlerweile in *International Mobile Telecommunication 2000* (IMT-2000) umbenannt

- Daten- und Telekommunikation sind immer noch zwei Welten. Es gibt aber Ansätze, in denen Modems im Scheckkartenformat (PCMCIA) für Notebooks genutzt werden, mit denen sich Daten aus dem GSM-Netz empfangen und senden lassen. Dadurch ist eine Sprach- und Datenübertragung möglich.
- Es fehlen Universalgeräte für das Senden und Empfangen von Daten, Sprache und Bildern. Die aktuellen Personal Digital Assistants (PDAs) und mobile audiovisuelle Terminals (MAVTs) stellen einen ersten Ansatz für Universalität dar.
- Für jeden Kommunikationsdienst erhält der Benutzer eine eigene Nummer beziehungsweise Zugangscode. Die Übersichtlichkeit geht somit bei der Benutzung von mehreren Diensten völlig verloren.
- Die Datenraten der vorhandenen Funknetze sind zu niedrig: Multimedia-Anwendungen sind über Funknetze daher bislang nicht in akzeptabler Qualität möglich.
- Die Lokalisierung eines Anwenders und die Übergabe in eine andere Funkzelle machen heute aufgrund unterschiedlicher Standards noch große Schwierigkeiten.
- Die höchstmögliche Erreichbarkeit der Teilnehmer muß garantiert werden.
- Bestehende Mobilkommunikationsgeräte und -systeme der 2. Generation nutzen noch eine zu geringe Bandbreite .
- Anwender wie Hersteller müssen sich mit einer Vielzahl von Standards herumschlagen, die größtenteils inkompatibel zueinander sind:
  - Zellularfunk-Systeme (GSM900, DCS1800)
  - schnurlose Telefone mit kurzer Reichweite, Telepunktsysteme (DECT, CT1/2)
  - Pager (ERMES – European Radio Message Service)
  - Bündelfunksysteme (TETRA, Iridium[5])
  - Funk-LANs (HYPERLAN)
  - Festnetze (PSTN – Public Switched Telecommunications Network, ISDN – Integrated Service Digital Network)

Trotz Einführung und Entwicklung neuer Geräte der 3. Generation möchte der Anwender bestehende Infrastruktur, Anlagen und Geräte so weit wie möglich weiterverwenden.

Idealerweise sollte der Anwender keinen Unterschied in der Dienstqualität zwischen Fest- und Mobilfunknetzen bemerken. Die Benutzung erfolgt vollkommen transparent. Auch bei der Auswahl seiner Anwendung möchte der Benutzer nicht eingeschränkt werden und mit einer Vielzahl an Kommunikationsgeräten und -diensten arbeiten müssen. Ferner darf der Aufenthaltsort des Teilnehmers kein Hindernis mehr für ein Kommunikationssystem des 21. Jahrhunderts sein. Zusammenfassend läßt sich sagen: *„In contact anytime, anywhere, with anyone“* kann als das Schlagwort für UMTS bezeichnet werden.

[5] zukünftiges Satellitensystem, das mit 77 Satelliten in erdnaher Umlaufbahn ausgestattet sein wird

3 Allgemeine Eigenschaften und Anforderungen an UMTS

Aus den obigen Problemen und Benutzerwünschen lassen sich Anforderungen und erste Eigenschaften von UMTS ableiten.

Der Teilnehmer soll nicht mehr zwischen mobilen und terrestrischen Netzen unterscheiden können, d.h. die Bandbreite sollte sich nicht verringern, wenn mit mobilen Endgeräten kommuniziert wird. Dies bedeutet eine ganze Menge von Diensten, die unabhängig von

- der Art des Zugriffs (Festnetz oder Mobilnetz)
- den Anwendungen (zellular, schnurlos, Paging, Satellit, etc.)
- der Dienstart (öffentlich oder privat)
- der Umgebung (Haus, Straße, Transport, Büro, Betrieb, etc.)
- der Örtlichkeit (Stadt, Land, bergisches Gelände)

zur Verfügung stehen müssen.

Weiterhin ist UMTS bestrebt, Innovationen, Wettbewerb und Verantwortlichkeiten für die mobilen Telekommunikationsdienste zu fördern. Um dieses zu erreichen, müssen die öffentlichen Dienste von UMTS standardisiert und Kompatibilät zu bestehenden Diensten bewahrt werden. Nur so kann UMTS schnell auf Marktentwicklungen reagieren und Dienstlösungen und Besonderheiten sowohl in Endterminals als auch in Dienstknoten berücksichtigen.

Weitere Forderungen, die UMTS deutlich von bestehenden 2. Generations-Standards unterscheiden:

- Untergrenze der Datenrate im gesamten Versorgungsgebiet beträgt 64 kBit/s
- Angebot von Diensten mit Datenraten bis zu 2 MBit/s
- Unterstützung von *Universal Personal Telecommunication Service* (UPT)
- Zugang zu Breitbandnetzwerken durch Integration von UMTS in B-ISDN und Nutzung des *Asynchronous Transfer Mode* (ATM)
- breites Angebot an Anwendungen (Voice, Fax, Data, Multimedia, etc.) und Diensten (handover, roaming, etc.), aus denen der Benutzer nach seinen Vorlieben und Bedürfnissen auswählen kann
- Annäherung bzw. Vereinigung der derzeit bestehenden mobilen Systeme (DECT, GSM900, DCS1800)
- Flexibilität, Schnelligkeit und jederzeitige Verfügbarkeit bei den unterschiedlichsten Übertragungsanforderungen

- vergleichbare Qualität der Dienste zu denen in Festnetzen (Störfestigkeit)
- Bewahrung der Kompatibilität zu FPLMTS
- Angebot einer Palette von Mobilfunkgeräten (von einem preiswerten Handheld-Telefon bis zu einem hochentwickelten Endgerät, welches Video- und Datendienste unterstützt)

4 Die Architektur von UMTS

4.1 Entwurfsmöglichkeiten für UMTS

Man unterscheidet folgende Möglichkeiten:

- **Eigenständiges UMTS-Netzwerk** – Das System wird ohne Nutzung von Komponenten anderer Netze entwickelt. Verbindungswünsche zu Festnetzwerken oder anderen Mobilfunknetzen werden über ein Gateway weitergeleitet. Dieses Gateway realisiert notwendige Dienst- und Protokollumsetzungen. In Abbildung 1 wird dies schematisch dargestellt. Von Vorteil ist, daß hierbei keinerlei Restriktionen bestehen. Der mobile Zugriff kann hier am besten optimiert werden. Nachteilig sind die hohen Kosten.

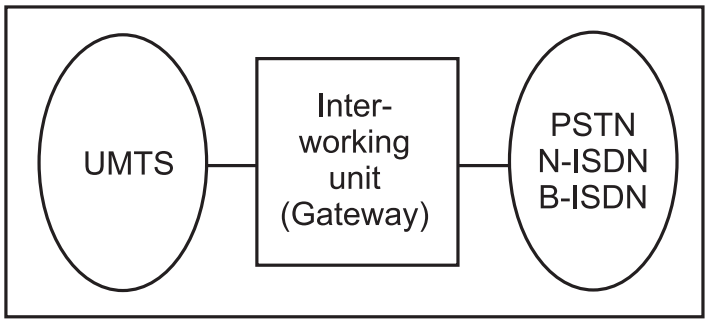


Abbildung 1: Eigenständiges UMTS-Netzwerk

- **Entwicklung aus einem Mobilfunknetz der 2. Generation** – Hierbei wird die Infrastruktur eines Mobilfunknetzes der 2. Generation, zum Beispiel *Global System for Mobile Communication* (GSM), genutzt, um UMTS-Dienste anzubieten. Von Vorteil sind niedrigere Kosten und die schon zur Verfügung stehende Infrastruktur. Von großem Nachteil ist die notwendige Anpassung der UMTS-Funktionalität an die schon bestehende Implementierung des Systems der 2. Generation.
- **Integration in ein Festnetzwerk** – Eine dritte Möglichkeit ist die Integration mit einem Festnetzwerk. Infrastruktur, Dienste und Funktionen könnten von beiden Systemen gemeinsam genutzt werden. Das würde Kosten reduzieren, sowohl bei der Implementierung als auch beim Betrieb und der Wartung. Abbildung 2 zeigt eine schematische Realisierung. Ein weiterer Vorteil wäre, daß ein integriert entworfenes UMTS auch als *stand-alone* Netzwerk implementiert werden kann[6].

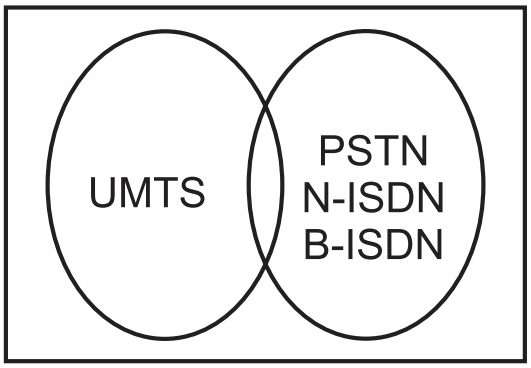


Abbildung 2: UMTS integriert in ein Festnetz

Wenn die Vor- und Nachteile der einzelnen Realisierungsmöglichkeiten gegenübergestellt werden, so kommt man zu dem Ergebnis, daß die Integration in ein Festnetz die einzig akzeptable Lösung darstellt.

Als Festnetze werden dabei N-ISDN und B-ISDN vorgeschlagen. N-ISDN ist insofern interessant, da es schon zur Verfügung steht. Bleibt die Frage, ob B-ISDN Dienste überhaupt unterstützt werden sollten und N-ISDN Dienste nicht ausreichend sind. Aber in allen Artikeln, die ich zu diesem Thema gefunden habe, wird B-ISDN als mögliches Festnetzwerk favorisiert oder dessen Einsatz sogar vorausgesetzt.

Im folgenden werde ich mich auf die Realisierung eines in das Festnetz B-ISDN integriertes UMTS beziehen.

4.2 Die Netzwerk-Struktur von UMTS

Es gibt drei eigenständige Komponenten, die zusammen UMTS bilden. Das sind das *access network* (Zugriffsnetzwerk), das *intelligent network* (IN, Intelligentes Netzwerk) und das *fixed (core) network* (Festnetzwerk oder inneres Netzwerk). Dabei lassen sich deren Aufgaben wie folgt unterscheiden:

- *access network* – Das *mobile terminal* (MT, mobiles Terminal) greift auf UMTS über das *access network* zu. Dies stellt dazu alle für den Funkkontakt notwendigen Komponenten bereit. Es besteht aus einer Menge von *base stations* (Basisstationen).
- *fixed (core) network* – Dieser Teil von UMTS beinhaltet Funktionen für die Verbindung, Übertragung und Zusammenarbeit mit anderen Netzwerken. Ein Beispiel für ein solches Netzwerk ist das oben bereits erwähnte B-ISDN.
- *intelligent network* – Das IN stellt Funktionen zur Verfügung, die spezifisch sind für mobile Nutzer, z.B. Zugangskontrolle, Benutzerlokalisierung, *roaming*[7] und

[6] UMTS muß *stand-alone* betrieben werden, wenn kein geeignetes Festnetz zur Verfügung steht oder Reglementierungen und Gesetze eine gemeinsame Nutzung der Infrastruktur nicht zulassen. Die bei einer Integration gemeinsam genutzte Infrastruktur ist in diesem Fall für das Mobilfunknetz alleine aufzubauen, und die normalerweise vom Festnetz zur Verfügung gestellte Funktionalität ist nachzubilden.

[7] Übergang von einem GSM-Netz in den Bereich eines anderen GSM-Betreibers ohne Gesprächsunterbrechung

handovers[8]. Die IN-Komponenten interagieren dabei mit dem *access network*, dem *fixed network* und dem *mobile terminal*.

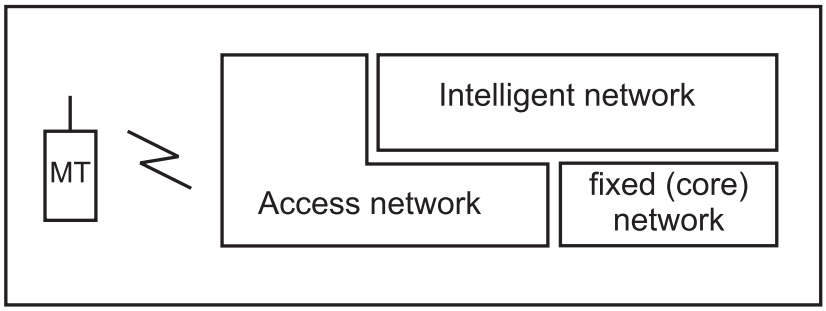


Abbildung 3: Die Grundstruktur von UMTS

Bei dieser Struktur ist nur das *access network* spezifisch für UMTS. Damit weicht dieses System von dem bisher üblichen *stand-alone*-Prinzip für Mobilfunknetze ab.

4.3 Einsatzmöglichkeiten eines UMTS-Terminals

Grundsätzlich lassen sich zwei Typen von Mobilität unterscheiden:

- *Terminal mobility* – als die Möglichkeit, mit einem Terminal von verschiedenen Orten oder wenn man sich in Bewegung befindet, Telekommunikationsdienste zu nutzen. Dazu muß das Mobilkommunikationsnetz in der Lage sein, das Terminal zu lokalisieren und zu identifizieren.
- *Personal mobility* – als die Möglichkeit, daß der Nutzer von verschiedenen Terminals aus kommunizieren oder andere Dienste nutzen kann. Das Netz muß dazu diese Dienste unterstützen und die Gebühren dem Gebührenkonto des Nutzers zuschreiben.

UMTS unterstützt beide Arten der Mobilität. *Personal mobility* wird mittels *Universal Personal Telecommunication service* (UPT) realisiert. Bei UPT erfolgt die Identifizierung eines Nutzers über eine eindeutige Nummer.

Im Rahmen der *terminal mobility* gibt es bei UMTS verschiedene Mobilitätsstufen — auch Umgebungen genannt—, in denen das Terminal eingesetzt werden kann:

1. *Home environment (Häusliche Umgebung)* – Es gibt eine *personal base station* (persönliche Basisstation) für jede Wohnung. Zu dieser Basisstation haben nur autorisierte Nutzer Zugriff und es besteht keine Möglichkeit, ein *handover* zu initiieren. Die *personal base station* ist entweder direkt mit dem Festnetz oder über eine externe UMTS Funkschnittstelle mit einer *public base station* (öffentlichen Basisstation) verbunden. Die Reichweite der persönlichen Basisstation ist begrenzt. Sie entspricht in etwa der eines schnurlosen Telefons.

[8]Gesprächsumschaltung

2. *Office / Business environment (Geschäftliche Umgebung)* – Für Unternehmen, Betriebe und Bürogebäude gibt es eine an die *Private Branche Exchange* (PBX, private Nebenstelle) des ISDN angelehnte Variante, welche als geschäftliche Umgebung bezeichnet wird. Dieses sogenannte *Customer Premises Network* (CPN, Kunden-Haus-Netzwerk) ist ein Netzwerk aus mehreren *lowpower base stations* (Basisstationen mit geringer Sendeleistung). Es besteht die Möglichkeit für ein *handover* in eine andere Funkzelle einer geschäftlichen, aber auch öffentlichen Umgebung. Das CPN ist mittels einer Glasfaserleitung oder über einen eigenen Funkkanal mit einem *mobile switching center* (MSC) verbunden.

3. *Public environment (Öffentliche Umgebung)* – Die oberste Stufe der Mobilität bildet ein Netz von *public base stations* (öffentliche Basisstationen). Dieses Netzwerk wird auch als öffentliche Umgebung bezeichnet. Wie schon bei der geschäftlichen Umgebung angedeutet wurde, besteht die Möglichkeit, ein *handover* auszulösen.

4. *Weitere* – Zusätzlich gibt es noch *base stations* in beweglichen Objekten, wie zum Bespiel in Bussen und in Zügen. In Gebieten, welche nicht die notwendige Infrastruktur aufweisen, sollen Satelliten-Komponenten eingesetzt werden.

In Anlehnung an oben läßt sich in der Literatur auch folgende Zelleneinteilung finden:

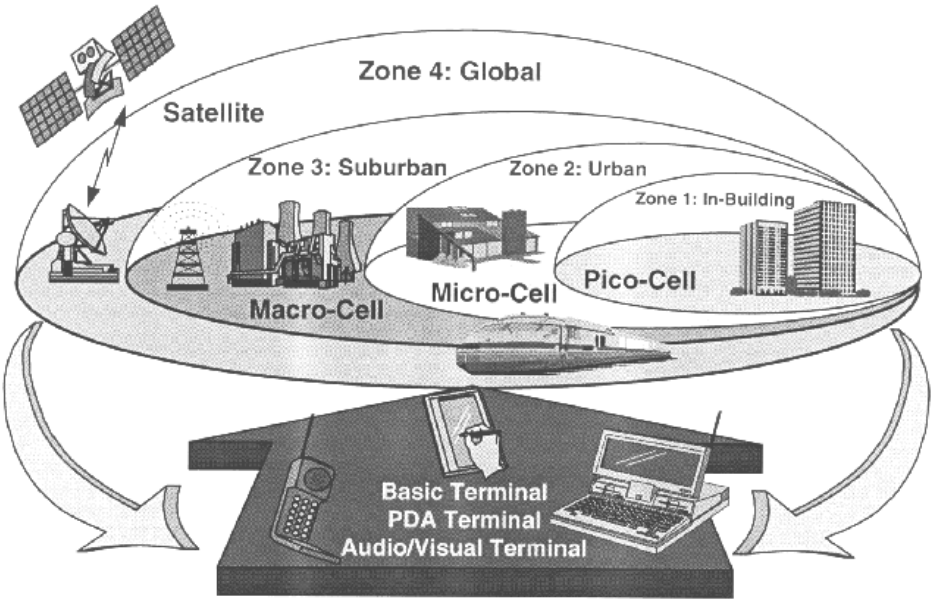


Abbildung 4: UMTS Telekommunikationsumgebungen

UMTS zeichnet sich also besonders dadurch aus, daß komplexe Zellenstrukturen eine effektive Ausnutzung der zur Verfügung stehenden Bandbreiten erlauben. Dabei bieten lokale, begrenzte Zellen sehr hohe Datenraten, wohingegen mobile Satellitensysteme die Lösung für die ökonomische Einbindung großer Gebiete darstellen.

4.4 Realisierungsmöglichkeiten der Funkschnittstelle

Um vor allem letzteres zu erreichen, bedarf es dreier Ebenen der Integration:

- **Netzwerkintegration**, wodurch terrestrische und mobile Netzwerke unabhängig voneinander betrieben werden können.
- **Equipment-Integration**, wodurch gemeinsame Standarddienste erforderlich sind sowie die Übereinstimmung in den Übertragungsparametern und der Funkschnittstelle zwischen den Satelliten- und terrestrischen Implementationen.
- **Systemintegration**, in der der Satellit ein wesentlicher Bestandteil des terrestrischen Netzwerks ist und in der Lage sein wird, *handovers* zwischen den terrestrischen Zellen und Satellitenzellen zu unterstützen.

Dabei wird die GSM-Technik weiterhin Technologieträger für das zukünftige UMTS bleiben. Weiterentwicklungen der 2. Generation wird es parallel zur Entwicklung von UMTS geben. Allerdings könnten CDMA-Zugriffsverfahren — durch CODIT vorangetrieben — das zur Zeit intensiv verwendete Multiplexverfahren FDMA/TDMA bzw. das neuentwickelte FDMA/ATDMA- Verfahren verdrängen.

Hauptaufgaben dieses CODIT-Projektes sind:

- die Schaffung eines breitbandigen Systemkonzepts, welches auf CDMA basiert.
- das Entwickeln und Erstellen eines Systemdemonstrators (Testbed), einschließlich Mobilfunkstationen, Funkbasisstationen, Funknetzwerkcontroller sowie Kanalsimulator.
- die Erstellung eines Simulators, damit die Ergebnisse des Systemkonzepts besser mit anderen Zugriffstechniken verglichen werden können.

Das Hauptproblem stellt dabei das Konzept der Funkschnittstelle von CODIT dar, um die geforderten 2 MBit/s zur Verfügung zu stellen. CMDA wurde als Zugriffsmethode ausgewählt, da hier die größte Effektivität für die Bereitstellung der UMTS-Anfordungen vermutet wurde.

Code Division Multiple Access ist ein Verfahren, das mehreren Benutzern den Zugriff auf den Übertragungskanal ermöglicht. Das heißt, es belegen zwar alle Teilnehmer denselben Frequenzbereich, jedoch wird das Nutzsignal für jeden Teilnehmer unterschiedlich codiert, wodurch die jeweiligen Daten im Übertragungskanal klar voneinander unterschieden werden können. Somit ist der größte Vorteil von CDMA, daß zur Verfügung stehende Bandbreite besser genutzt wird[9] und eine größere Anzahl von Teilnehmern Zugriff auf das Übertragungsmedium hat als beim FDMA- oder TDMA-Verfahren. Durch die dynamische Kanalzuordnung ist keine feste Zuordnung der nutzbaren Frequenzkanäle nötig. Dies bedeutet, daß keine Frequenzplanung mehr erforderlich ist, das Netzprotokoll vereinfacht sich. Ein weiterer Vorteil gegenüber TDMA ist die niedrigere konstante Sendeleistung.

Das *Time Division Multiple Access*-Verfahren stellt ein Zeitmultiplexverfahren dar, bei dem jedem Knoten eine feste Anzahl von Zeitschlitzen pro Umlauf zugeordnet wird. Die Zeitschlitze können nach den Bedürfnissen der einzelnen Stationen ausgerichtet sein. Sind diese Bandbreiten bekannt, so führt TDMA zu einer hohen Auslastung. Es versagt

[9] eine der Hauptschwächen der 2. Generations-Geräte

allerdings bei schwankenden Benutzeranforderungen, da es nicht angemessen reagieren kann und disqualifiziert sich somit für die Forderungen von UMTS nach Flexibilität und Effizienz. Ein weiterer Nachteil von TDMA ist die notwendige Synchronisation der Stationen, die bei CDMA entfällt. Dies trägt ebenfalls zur Protokollentlastung von CDMA bei.

Aus diesen Gründen bezeichnen viele Fachleute inzwischen CDMA als das Zugriffsverfahren für UMTS. Dagegen gilt TDMA als technisch ausgereifter, da man auf Erfahrungen bei GSM zurückgreifen kann. Welches Verfahren sich letztendlich durchsetzt, wird die endgültige Standardisierung von UMTS bringen. Möglich kann auch eine Hybridstruktur sein, die je nach Zellstruktur TDMA- oder CDMA-Verfahren anbietet.

4.5 Aufbau Intelligenter Netzwerke und Integration in UMTS

Intelligente Netzwerke unterscheiden sich zu anderen Netzen durch eine erweiterte Dienstpalette, die sich in drei Kategorien einteilen läßt:

- **personenbezogen:** persönliche Rufnummer, landesweite Rufnummer, virtuelles Privatnetz
- **informationsbezogen:** Notrufdienst, Tele-Info-Dienst, Wide Area Centrex
- **integrierte Fremdfunktionen:** Telefonieren mit Kontokarte, Televotum, alternative Gebührenberechnung

Entscheidende Merkmale für IN-Strukturen sind allerdings

- die Möglichkeit der einfachen und schnellen Einführung von neuen Diensten
- eine flexible Dienstverwaltung
- bessere Kontrollmöglichkeiten der Dienstparameter durch die Teilnehmer

Somit handelt es sich bei IN-Strukturen um ein offenes Kommunikationsnetz, das mehr Flexibilität bei gleichzeitiger Steigerung der Dienstqualitäten erlaubt. Intelligente Netzstrukturen sollen aus Sicht des Benutzers unterschiedliche Teilnetze zusammenführen. Darüber hinaus versetzen sie den Netzbetreiber und Service Provider in die Lage, neue Kommunikationsdienste schnell und einfach, das heißt unabhängig vom verwendeten Transportnetz, realisieren zu können. IN-Dienste stellen also eine sinnvolle und attraktive Ergänzung zum ISDN im Festnetz sowie zu GSM im Mobilfunkbereich dar und bilden somit eine optimale Grundlage zur Vereinigung bzw. Annäherung der Netze via UMTS.

Dabei kann man sich die Integration von IN in ein Festnetzwerk — hier B-ISDN — wie folgt vorstellen:

Dabei ist die Grenze zwischen den beiden Systemen so tief wie möglich anzusiedeln, um möglichst wenig notwendige Erweiterungen des B-ISDN und viel Funktionalität im IN zu erhalten.

Dabei läßt sich die IN-Architektur, die auch als Dienste-Kontroll-Architektur bezeichnet wird, wie in Abbildung 6 in drei Ebenen unterteilen:

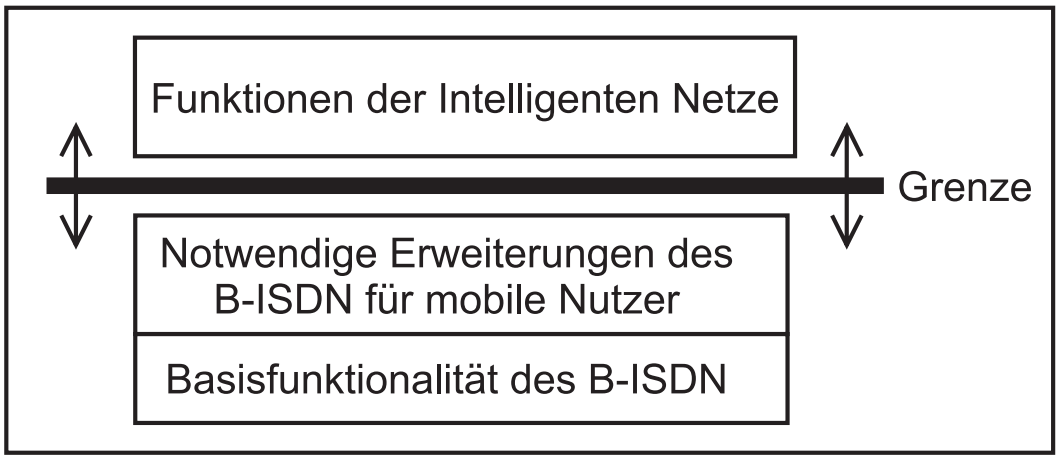


Abbildung 5: Relation zwischen B-ISDN und IN-Erweiterungen

- **Teilnehmerebene (accesss domain)** – sie stellt die standortgebundenen und mobilen Endgeräte sowie deren spezifische Netze dar.
- **Dienstvermittlungsebene (network domain)** – sie hat die Aufgabe, bei einer Anfrage zu überprüfen, ob sie den Dienst bereitstellen kann.
- **Service Control Point (PSCS) und Dienstmerkmalsverwaltung (Application services)** – hier sind die Anwendungen und Daten zusammengefaßt, die für das Zusammenspiel der Dienstvermittlungsstellen mit den Endgeräten erforderlich sind. Ferner steuert und verwaltet die Dienstmerkmalsverwaltung das gesamte System.

Manche Autoren unterscheiden hier vier Ebenen. Dabei wird die letzte auf zwei Ebenen aufgeteilt, wobei die Dienstmerkmalsverwaltung die oberste Schicht darstellt.

Eine Weiterführung des Architekturmodells würde hier den Rahmen sprengen, zumal noch kein endgültiges Architekturmodell von UMTS existiert. Als Referenzmodell allerdings kann das des MONET-Projekts angesehen werden.

5 Faktoren für den Erfolg von UMTS

Der Erfolg eines modernen Telekommunikationssystems ist abhängig von einer Reihe von Faktoren, die sich wie folgt gliedern lassen:

- **Verfügbarer Massenmarkt** – Eine Reihe neuer Dienste, Anwendungen und Fähigkeiten werden nach Marktananlysen in den ersten drei Jahren bis zu 3 Millionen und in den ersten zehn Jahren sogar bis zu 60 Millionen neuer mobiler Terminals hervorbringen.
- **Regelung und Lizensierung** – Es werden klare Stellungnahmen, Gesetze, Reglementierungen und einheitliche Lizensierungen von Seiten der Politik in Richtung Telekommunikationstechnik benötigt. Derart massive Investitionen für die

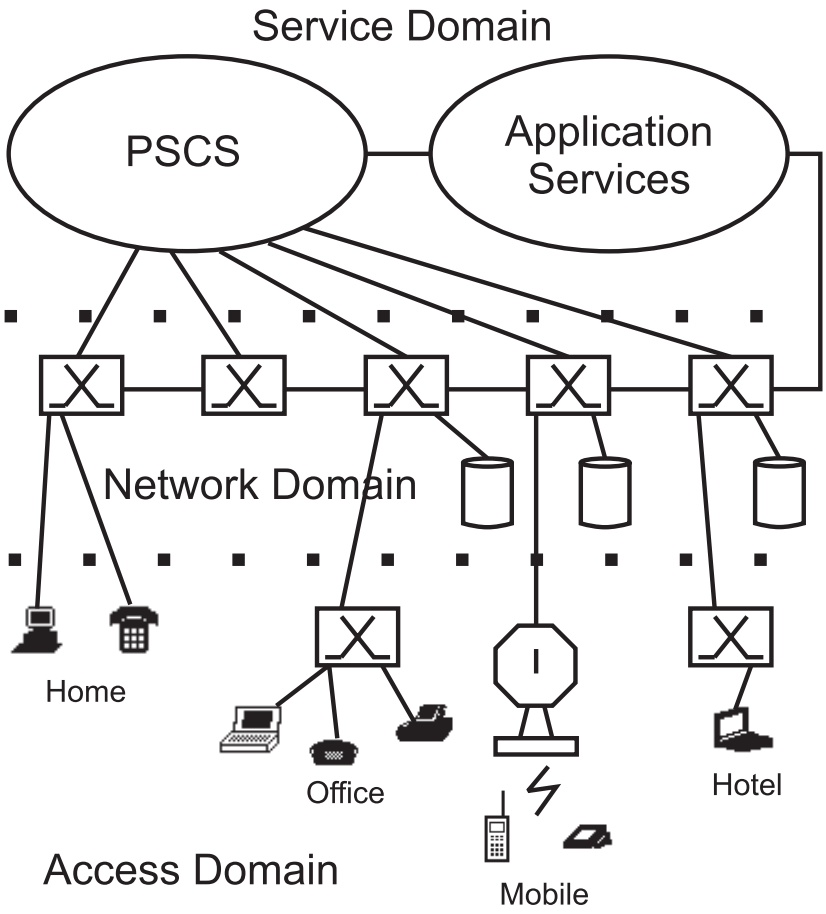


Abbildung 6: Architektur der Intelligent-Network-Struktur

Entwicklung von UMTS von Seiten der Industrie bedürfen einer stabilen politischen Grundlage, die durch europäische und internationale Gremien und Standards gegeben werden könnten, zumal durch das Zusammenwachsen der beteiligten Länder zur EU eine geeignete Plattform im Begriff ist, zu entstehen.

- **Standards** – Obwohl UMTS als offenes System verstanden und implementiert wird, müssen einheitliche Standards verabschiedet werden. Offene Schnittstellen für alle Verbindungen nach außen und die inneren Netzwerkfunktionen bilden dabei das Fundament der Entwicklung und schnellen Einführung von UMTS. Die dabei verwendeten Protokolle müssen offengelegt werden und standardisiert sein.

- **Technologie** – Die Weiterverwendung von 2. Generations-Systemen und Infrastruktur erlaubt dem Benutzer eine schrittweise Wandelung zu UMTS. Die dabei entstehenden Geräte der erweiterten 2. Generation kombinieren dann eventuell schon bestehende Standards wie GSM900, DCS1800 und DECT auf ihrem Weg zur dritten Generation.

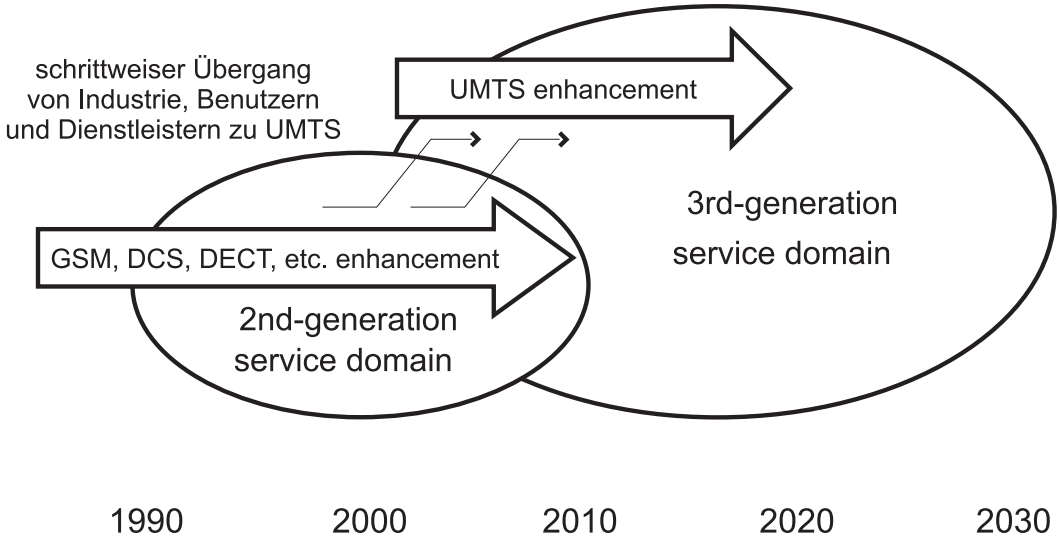


Abbildung 7: Wandelung von Systemen der 2. zu Systemen der 3. Generation

- **Erfolg der GSM-Familie** – Nicht zuletzt sollten die Erfahrungen aus den Erfolgen durch GSM-Produkte der Entwicklung und Standardisierung von UMTS behilflich sein. GSM wird — wie in Abschnitt 4.4 bereits erläutert — eine wichtige Rolle für bzw. parallel zu UMTS spielen.

6 Schlußbemerkungen

Durch ein Zusammenspiel all dieser Faktoren steht dem Erfolg von UMTS nichts mehr im Weg. In UMTS ist die Schaffung einer gemeinsamen Plattform für existierende Systeme (GSM, DECT, DCS, ERMES, etc.), sowie die Integration neuer Systeme geplant und zum Teil schon realisiert. Dennoch bleibt abzuwarten, wie schnell das „neue System“ von der Industrie und vor allem von den Verbrauchern angenommen und weiterentwickelt wird[10]. Bis es soweit ist, bedarf es noch immenser Entwicklungen und

[10] Auch ATM bescheinigt man schon seit längerer Zeit, das Universalrezept für Festnetze zu sein.

Neuerungen in der Netzwerk und Funktechnik und auf dem Dienste-Sektor. UMTS entsteht nicht durch eine einzelne sensationelle Entdeckung oder Entwicklung auf dem Telekommunikationssektor, sondern zeigt sich — wie in Abbildung 7 bereits angedeutet — als langwierigen Entwicklungs- und Wandelungsprozeß bis weit ins nächste Jahrtausend hinein.

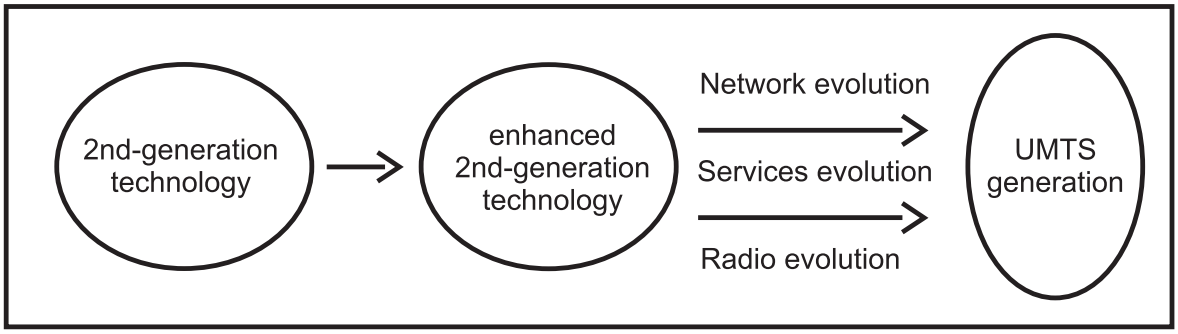


Abbildung 8: Entwicklung von UMTS

Solange aber muß der tüchtige Geschäftsmann wohl oder übel noch mit Handy, Laptop, Modem und Filofax bepackt durch die Lande ziehen.

Literatur

[Det96a] Kai-Oliver Detken. Intelligente Netze: Architektur - Vergleich zu GSM - Probleme. *Gateway*, April 1996, Seite 110–114.

[Det96b] Kai-Oliver Detken. PCN: Personenbezogenes Kommunikationsnetz der Zukunft. *Gateway*, Mai 1996, Seite 76–84.

[Det96c] Kai-Oliver Detken. Verschmelzung der Systeme. *Gateway*, Juni 1996, Seite 104–111.

[FJKP95] H. Federrath, A. Jerichow, D. Kesdogan und A. Pfitzmann. Technischer Datenschutz in öffentlichen Mobilkommunikationsnetzen. *Wissenschaftliche Zeitschrift der TU-Dresden*, 1995. Heft 6.

[GMM95] D. Grillo, N. Metzner und E. D. Murray. Testbeds for Accessing the Performance of a TDMA-Baesd Radio Access Design for UMTS. *IEEE Personal Communications*, April 1995, Seite 36–45.

[INT96] Struktur künftiger Mobilfunknetze. Internet, 1996.

[KST96] J. A. Korinthios, E. D. Sykas und M. E. Theologou. Numbering and Adressing Aspects of the UMTS's Integration into the Fixed Network Infrastrucure. *IEEE Personal Communications*, April 1996, Seite 62–71.

[Mit94] Hakan Mitts. *Universal Mobile Telecommunication System - Mobile access to Broadband ISDN*. Elsevier Science B.V. 1994. Broadband Islands'94: Connecting with the End-User, 1994.

[MLKN96] H. Mitts, G. Luijten, J. A. Korinthios und J. Nelson. Connectionless Signalising Network Layer in UMTS. *IEEE Personal Communications*, June 1996, Seite 44–53.

[Ref95] Bernd Refer. Trends bei Mobilkommunikation. *Gateway*, Dezember 1995, Seite 68–71.

[Rö96] Dirk Römhild. Das Universal Mobile Telecommunication System (UMTS) aus der Sicht des Technisches Datenschutzes, 25. September 1996.

[Swa] R. S. Swain. UMTS - A 21st Century System. A RACE Mobile Project Line Assembly Vision.

[UMT96] *UMTS Task Force Report*, Brüssel, 1. März 1996.

Abbildungsverzeichnis

Digital Audio Broadcasting – Grundlagen

Oliver Kreylos

Kurzfassung

Nach dem Siegeszug digitaler Systeme zur Aufzeichnung und Wiedergabe im kommerziellen Audiobereich soll nun auch die Funkübertragung zu stationären oder mobilen Empfängern der Digitalisierung anheimfallen.

Dieser Artikel soll zeigen, welche Nachteile des herkömmlichen, analogen AM/FM-Radios durch den Übergang zur Digitaltechnik aufgehoben werden können; ferner wird eine Übersicht über weitere Datendienste gegeben, die den digitalen Rundfunk als Medium zur transparenten, gesicherten Übertragung beliebiger Bitströme verwenden.

Im besonderen wird dabei auf die Struktur und das Übertragungsverfahren des Digital Audio Broadcasting Systems (DAB) nach Eureka-Projekt 147 eingegangen, da dieses den momentan am weitesten gediehenen Ansatz darstellt.

1 Einleitung

Dieser Abschnitt beschreibt die Vorteile, die sich bei der Umstellung der Radioübertragung auf Digitaltechnik ergeben.

1.1 Nachteile des analogen AM/FM-Rundfunks

Beim herkömmlichen analogen Radio wird das (z. B. über ein Mikrofon aufgenommene) niederfrequente Tonsignal direkt auf einen hochfrequenten Träger aufmoduliert – beim Lang-, Mittel- und Kurzwellenfunk per Amplitudenmodulation, beim Ultrakurzwellenfunk per Frequenzmodulation. Die modulierte Trägerfrequenz wird über die Sendeantenne abgestrahlt und von der Empfangsantenne aufgenommen. Im Empfänger wird das ursprüngliche Tonsignal wieder von der Trägerfrequenz abgenommen, verstärkt und wiedergegeben.

Durch diese Vorgehensweise der direkten Trägermodulation entstehen eine Reihe von Nachteilen:

- Durch die direkte Modulation des Tonsignals ist die Übertragung völlig ungesichert. Jede Störung der Übertragung schlägt sich sofort in einer Störung des wiedergegebenen Tonsignals wieder (Knackser, Rauschen, etc.); insbesondere hat der Empfänger keine Möglichkeit, Übertragungsfehler zu erkennen oder gar zu korrigieren.

- Aus der obigen Betrachtung folgt, daß die hörbaren Effekte von Störsignalen nur durch eine Erhöhung der Sendeleistung gemildert werden können, da dann das Tonsignal (und damit auch die Störungen) beim Empfänger nicht mehr so stark verstärkt zu werden braucht.

- In einer realen Umgebung gibt es durch Reflexion oder Beugung stets mehrere, verschieden lange Wege, die die Funkwellen von der Sende- zur Empfangsantenne zurücklegen können ("Mehrwegeausbreitung", siehe auch Bild 1). Durch

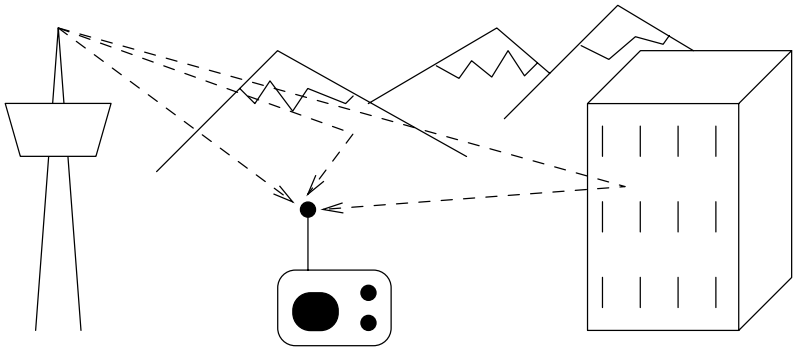


Abbildung 1: Mehrwegeausbreitung

  die Interferenz der eintreffenden Wellen kommt es zu ortsabhängigen Störungen, bei denen einzelne Frequenzbereiche des Tonsignals ausgelöscht werden können ("selektiver Frequenzschwund"). Diese Effekte sind bei stationären Empfängern durch geeignete Wahl des Antennenstandpunkts zu umgehen, dies ist bei mobilen Empfängern nicht möglich; bei diesen kommt neben der zeitlichen Veränderung der Empfangsbedingungen sogar noch eine weitere Frequenzverzerrung durch den Dopplereffekt hinzu.

- Die Reichweite von Sendern ist durch Abschattung begrenzt. Um also ein größeres Sendegebiet mit einem Radioprogramm zu versorgen, müssen viele Sendestationen ("Relais") zu einem Sendenetz zusammengeschaltet werden. Aus der obigen Betrachtung folgt aber, daß benachbarte Relaisstationen nie auf der gleichen Trägerfrequenz senden dürfen, da sonst Interferenzen aufträten. Das führt aber dazu, daß die zur Verfügung stehenden Frequenzbereiche (eine immer knapper werdende Ressource) nicht effizient genutzt werden können, da alle Relaisstationen, deren Sendebereiche sich überschneiden, das gleiche Programm auf verschiedenen Trägerfrequenzen ausstrahlen müssen. Weiterhin muß bei mobilem Empfänger beim Übergang zwischen den Sendebereichen zweier benachbarter Relaisstationen die Empfangsfrequenz gewechselt werden.

- Die Übertragung nichtakustischer Zusatzdaten ist zwar möglich, aber aufwendig und nicht in die Audioübertragung direkt integrierbar: Solche Zusatzdaten stellen einen zusätzlichen digitalen Kanal dar, der mit dem primären analogen Kanal in keinem direkt ersichtlichen Zusammenhang steht. Beim Radiodatensystem (RDS) zum Beispiel werden die digitalen Zusatzdaten auf eine eigene Trägerfrequenz moduliert, die nach Konvention 57 kHz oberhalb der eigentlichen Trägerfrequenz liegt (der RDS-Kanal hat übrigens nur eine Übertragungskapazität von unter 1200 bit/s).

1.2 Anforderungen an digitale Radioübertragung

Um die oben angeführten Nachteile des herkömmlichen Rundfunks zu überwinden, wurden folgende Anforderungen an zu entwickelnde digitale Übertragungssysteme formuliert:

- Audioübertragung in (annähernd) CD-Qualität
- Weitgehende Immunität gegen Mehrwegausbreitung und andere Störeinflüsse
- Minimale Störung bereits existierender Rundfunkdienste
- Minimierung sowohl der Übertragungskosten als auch der Komplexität und Kosten der Empfänger
- Fähigkeit zur Übertragung zusätzlicher Daten
- Minimale Verzerrung der Tonsignale bei schwächer werdendem Empfang

Wie diese Anforderungen erfüllt werden können, wird im nächsten Abschnitt anhand des Eureka-147-Systems, das den momentan am weitesten fortgeschrittenen Standard zur digitalen Funkübertragung darstellt, näher beleuchtet.

2 Das Eureka-147-DAB-System

Das Eureka-147-Projekt wurde 1987 ins Leben gerufen, um ein System zur digitalen Rundfunkübertragung (Digital Audio Broadcasting, DAB) zu entwickeln, das den im letzten Abschnitt aufgeführten Anforderungen genügt. Dieses System wurde schließlich im September 1994 vom European Telecommunications Standards Institute (ETSI) als Standard übernommen.

Wie werden nun die im letzten Abschnitt genannten Anforderungen vom DAB erfüllt?

- Die zu übertragenden Tonsignale werden wie in der digitalen Studiotechnik üblich abgetastet (PCM, 16 Bit Auflösung, 48 kHz Abtastrate, stereo). Um die Datenmenge zu reduzieren, werden die digitalisierten Tonsignale noch einer Kompression unterworfen, die auch im MPEG-Standard zur Videokompression verwendet wird; diese nutzt die Funktionsweise des menschlichen Gehörs aus, um ohne hörbaren Qualitätsverlust Kompressionsraten von etwa 1:10 zu erreichen.
- Um das komprimierte Tonsignal gegen Übertragungsfehler zu sichern, werden Schutzbits eingefügt (etwa eins pro Nutzbit), so daß der Empfänger Fehler erkennen und sogar korrigieren kann. Da bei Funkübertragung häufig Bündelfehler auftreten (mehrere fehlerhafte Bits folgen direkt aufeinander), werden die Bits des digitalisierten Tonsignals vor der Übertragung nach einem festen Schema durcheinandergewürfelt, dadurch werden zusammengehörende Bits zeitlich weit auseinandergesetzt, und bei der Rückverwürfelung im Empfänger werden aus einem Bündelfehler mehrere – korrigierbare – Einzelfehler.

- Digitale Daten werden grundsätzlich als Folge von Symbolen (z. B. Bits) auf dem Kanal übertragen. Um die Übertragung gegen Mehrwegausbreitung und ähnliche Störungen zu sichern, wird beim DAB statt einer schnellen Folge kurzer Symbole eine Folge langer Symbole gesendet, die durch Schutzintervalle voneinander getrennt sind. Werden diese so lang gewählt, daß alle durch Reflexion verzögert eintreffenden Symbole in das Schutzintervall fallen, so stören sich benachbarte Symbole nicht (siehe auch Bild 2). Natürlich muß bei Verringerung der

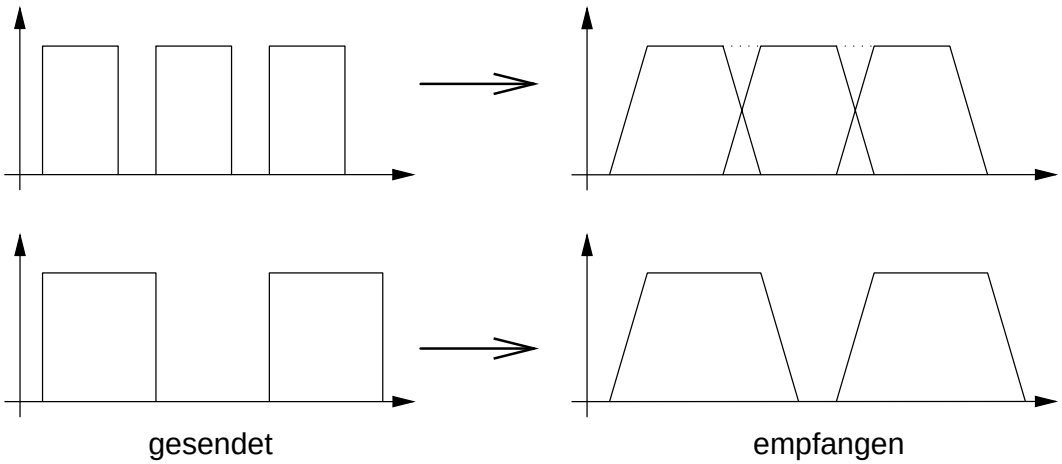


Abbildung 2: Verschieden schnelle Schrittfolgen

  Schrittgeschwindigkeit der Symbolvorrat entsprechend vergrößert werden, damit die Übertragungskapazität konstant bleibt.

- Um Störungen bei Auftreten von selektivem Frequenzschwund zu minimieren, sollte das DAB-Signal die zur Verfügung stehende Bandbreite gleichmäßig ausnutzen, es sollte also einem weißen Rauschen gleichen. Dies wird durch Verwendung des OFDM-Verfahrens (Orthogonal Frequency Division Multiplex) beim DAB erreicht.

- Die Unempfindlichkeit des DAB-Signals gegenüber Mehrwegeausbreitung hat schwerwiegende Konsequenzen für die Planung eines DAB-Funknetzes: Es ist nämlich möglich, daß benachbarte Relaisstationen auf exakt der gleichen Trägerfrequenz senden, sofern sie nicht zu weit auseinanderstehen. Man kann also beliebig erweiterbare Netze bei Verwendung nur einer Trägerfrequenz errichten – sogenannte Gleichwellennetze (Single Frequency Networks, SFN). Dadurch können die zur Verfügung stehenden Frequenzbereiche optimal genutzt werden.

- Mit Gleichwellennetzen ist es sogar möglich, ein Sendenetz für viele Regionalprogramme mit jeweils mehreren Relaisstationen aufzubauen, das insgesamt nur vier Frequenzbänder benötigt (siehe auch das sogenannte Vierfarbenproblem: Eine allgemeine Unterteilung der Ebene in Gebiete kann mit vier Farben so eingefärbt werden, daß je zwei benachbarte Gebiete verschieden gefärbt sind); diese lassen sich bequem innerhalb eines (7 MHz breiten) Fernsehkanals unterbringen (beim DAB-Pilotversuch in Baden-Württemberg ist dies der Fernsehkanal 12 im VHF-Band, die vier Kanäle werden als DAB-Kanäle A bis D bezeichnet, siehe auch Bild 3). Bei dieser Netzplanung senden alle Relaisstationen eines Regionalsenders auf der gleichen Frequenz (Kanal A, B, C oder D), benachbarte Regionalsender

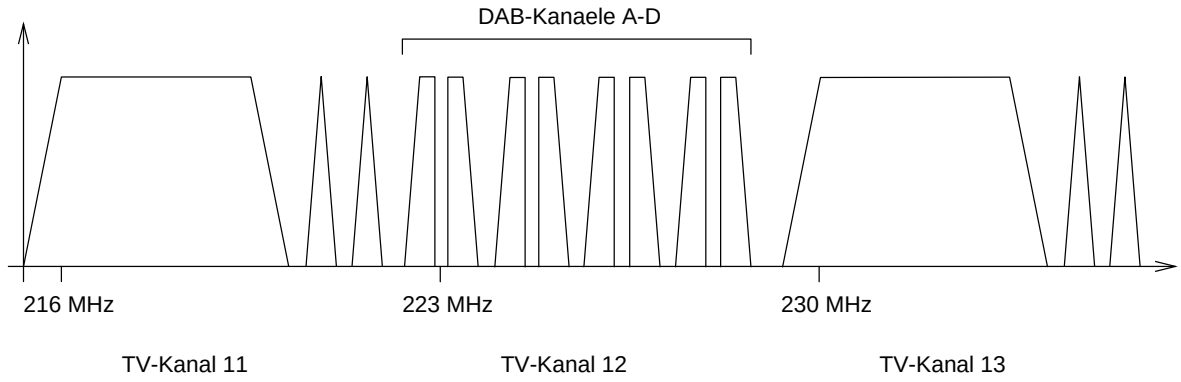


Abbildung 3: DAB-Kanäle A bis D im TV-Kanal 12

benutzen verschiedene Frequenzen so, daß sich keine zwei benachbarten Regionalsender gegenseitig stören (siehe auch Bild 4).

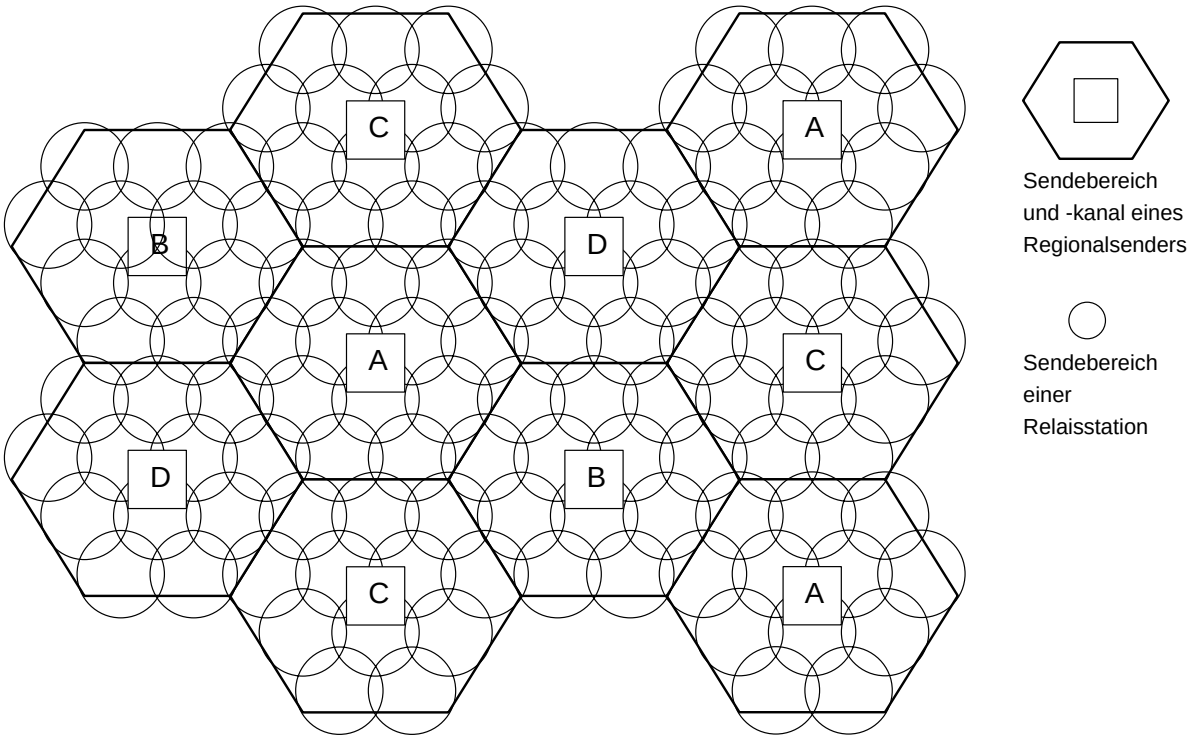


Abbildung 4: Regionalsender in Gleichwellennetzen

- Durch die Kompression der zu übertragenden Tonsignale mit wählbaren Kompressionsraten und die Möglichkeit, einen DAB-Kanal durch Multiplexen in mehrere digitale Kanäle aufzuteilen, können die Frequenzbänder noch effizienter genutzt werden. So können über einen DAB-Kanal bis zu sechs Radioprogramme in CD-Qualität oder bis zu 80 Programme geringerer Qualität übertragen werden.

- Da auf dem Kanal nur digitale Signale übertragen werden, kommt man im Vergleich zum analogen Rundfunk mit einem geringeren Signal-/Rauschabstand aus – es wird also nur eine geringere Sendeleistung benötigt. Weiterhin hat eine Verringerung der Empfangsstärke keinen direkten Einfluß mehr auf die Tonqualität: Bis zu einer gewissen Minimalempfangsstärke hat man fast gleichbleibende

Tonqualität, darunter ist überhaupt kein Empfang mehr möglich (Deshalb heißt es auch "Digitale Übertragung": Man hat entweder exzellenten oder gar keinen Empfang).

In den folgenden Abschnitten werden die Verarbeitungsschritte dargestellt, die ein Tonsignal (oder ein anderes digitales Signal) von der Einspeisung im Sender bis zur Wiedergabe im Empfänger eines DAB-Systems durchläuft. Eine wesentlich detailliertere Darstellung dieser Schritte, mit besonderer Gewichtung der einzelnen verwendeten Modulationsverfahren, findet sich in [Wen96a, Wen96b, Wen96c].

2.1 Audiocodierung im DAB

In diesem Abschnitt soll die beim DAB verwendete Quellencodierung für Tonsignale genauer betrachtet werden. Der Quellencodierer gliedert sich in drei Funktionsblöcke:

- Den MUSICAM-Encoder
- Die Faltungscodierung
- Das Time-Interleaving

2.1.1 Der MUSICAM-Encoder

Dieser Funktionsblock dient zur Komprimierung des zu übertragenden Tonsignals. An seinem Eingang wird das Tonsignal in PCM-codierter Form (16 Bit Auflösung, 48 kHz Abtastrate, stereo) angeliefert.

Die im MPEG-Layer-II-Standard genormte MUSICAM-Codierung (Masking pattern Universal Subband Integration Coding And Multiplexing) benutzt psychoakustische Effekte, um hohe Kompressionsraten (um 1:10) bei nicht hörbaren Qualitätsverlusten zu erzielen.

Hierbei wird die Tatsache benutzt, daß das menschliche Ohr in verschiedenen Frequenzbereichen verschieden empfindlich ist (Ruhehörschwelle), und daß ein lauter Ton in einem Frequenzbereich die Hörschwelle in benachbarten Frequenzbereichen nach oben verschiebt (Mithörschwelle, siehe auch Bild 5). Dieser Effekt bewirkt, daß Töne, de-

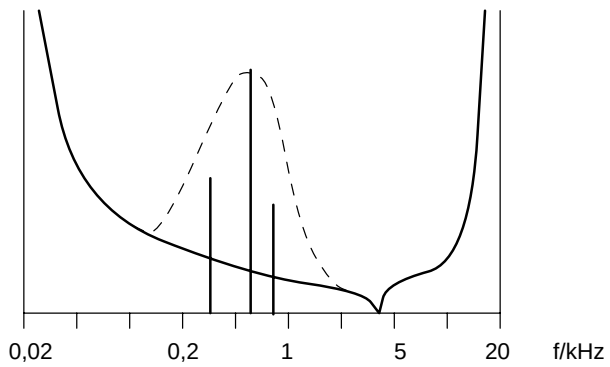


Abbildung 5: Ruhehörschwelle und verdeckte Töne

ren Lautstärke über der Ruhehörschwelle läge, trotzdem nicht wahrgenommen werden, wenn in einem benachbarten Frequenzbereich ein lauter Ton vorhanden ist – die leiseren Töne werden von dem lauten Ton verdeckt.

Bei der Codierung wird das Spektrum des Tonsignals von 24 kHz in 32 Bänder von je 750 Hz unterteilt. Innerhalb dieser Bänder werden verschiedene Abtastauflösungen so gewählt, daß das Quantisierungsrauschen unterhalb der Hörschwelle bleibt – hierbei wird auch die Anhebung der Mithörschwelle durch laute Töne in einem benachbarten Frequenzbereich berücksichtigt.

Die einzelnen Frequenzbänder des Tonsignals werden also getrennt voneinander mit jeweils optimalen Abtastauflösungen – also Wortbreiten – codiert. Die Information über die in jedem Band verwendeten Wortbreiten wird mit dem Signal übertragen, so daß der Empfänger das Ursprungssignal mit relativ geringem Aufwand rekonstruieren kann.

Durch die Kompression sinkt die Datenrate des Tonsignals von etwa 1,5 MBit/s (48.000 Rahmen/s · 16 Bit/Sample · 2 Sample/Rahmen) je nach gewählter Kompressionsrate auf 192 kBit/s bis hin zu 16 kBit/s (bei entsprechend schlechterer Qualität).

2.1.2 Die Faltungscodierung

Durch die Kompression des Tonsignals im MUSICAM-Encoder steigt die Entropie, also die durchschnittliche Informationsmenge pro übertragenem Bit. Um die Übertragung gegen Fehler, die sich im komprimierten Signal wesentlich stärker auswirkten, zu sichern, wird in diesem Baustein wieder kontrollierte Redundanz in Form von Schutzbits hinzugefügt. Die Qualität des Schutzes ist dabei wählbar, es werden pro Nutzdatenbit durchschnittlich – je nach Wunsch – 0,33 bis 2 Schutzbits hinzugefügt. Bei Tonsignalen kommt in der Regel ein Schutzbit auf ein Nutzbit.

2.1.3 Das Time-Interleaving

Die im vorigen Abschnitt beschriebene Faltungscodierung kann das Tonsignal effektiv gegen Einzelbitfehler absichern, d. h. bei auftreten einzelner Bitfehler kann der Empfänger den Fehler erkennen und korrigieren.

Da bei Funkübertragung jedoch meistens Bündelfehler auftreten, werden die Bits des Tonsignals in diesem Baustein nach einem festgelegten Muster durcheinandergewürfelt, wodurch zusammengehörige Bits zeitlich weit auseinandergerückt werden. Wird diese Verwürfelung im Empfänger wieder rückgängig gemacht, werden die Bündelfehler ihrerseits zu mehreren Einzelfehlern auseinandergezogen, die dann per Faltungsdecodierung erkannt und korrigiert werden können.

Ein Nachteil des Time-Interleaving ist, daß für den Umsortierungsvorgang Daten über einen längeren Zeitraum (mehrere Millisekunden) gesammelt werden müssen. Das führt zum einen zu einem erhöhten Speicherbedarf sowohl auf Sender- als auch auf Empfängerseite, zum anderen wird durch diese Pufferung aber auch die gesamte Zeitverzögerung des DAB-Systems erhöht. Zum Glück ist Rundfunk ein unidirektionales Medium, bei dem solche Verzögerungen keine große Rolle spielen (ausgenommen sind vielleicht Zeitansagen: “Bei Ihnen ist es jetzt fünf Millisekunden nach drei Uhr, hier sind die Nachrichten...”).

2.1.4 Eingebette Daten

Innerhalb eines Audiosignals können beim DAB noch andere Daten übertragen werden, die mit dem Audiosignal in einem engen Zusammenhang stehen (Program Associated Data, PAD). Solche Zusatzdaten könnten z. B. Senderkennungen, Aussteuerungssignale oder tonsynchron gesendete Liedtexte (vielleicht für Karaoke?) umfassen.

Die Übertragungskapazität für die Zusatzdaten ist wählbar (mindestens 667 bit/s), aber da Audiosignal und PAD im gleichen Kanal übertragen werden, geht eine hohe PAD-Kapazität auf Kosten der Tonqualität.

2.2 Übertragung anderer Daten

Anstatt eines digitalen Tonsignals können auch beliebige andere Daten per DAB übertragen werden. Hierzu stellt das DAB-System einen Dienst zur transparenten, gesicherten Übertragung beliebiger Bitströme zur Verfügung. Die Sicherung erfolgt wie bei der Audioübertragung durch Faltungscodierung und anschliessendes Time-Interleaving; die Qualität der Sicherung, d. h. die Anzahl der eingefügten Schutzbits pro Nutzbit, kann dabei vom Dienstbenutzer bestimmt werden.

Die Vielzahl möglicher Datendienste, die auf dem DAB-System aufbauen, ist Thema einer eigenen Abhandlung; hier seien nur einige Beispiele angeführt:

- Aktuelle Wetterberichte mit Wetterkarte und/oder aktuellen Satellitenbildern
- Aktuelle Verkehrszustandsmeldungen, die dann von einem Navigationssystem berücksichtigt werden können
- Übertragung von Stand- oder Bewegtbildern (bei geeigneter Kompression ist sogar Fernsehübertragung möglich)
- Ausstrahlung des Seitenangebots eines Web-Servers, hierbei werden dann alle Seiten zyklisch gesendet

Die Möglichkeit, beliebige Daten schnell an mobile Empfänger übertragen zu können, ist eine wesentliche Neuerung des DAB-Radios gegenüber dem herkömmlichen analogen Rundfunk. Um dieser Neuerung zum Durchbruch zu verhelfen, müssen Standards geschaffen werden, die die Struktur der übertragenen Daten – über die einfache Bitübertragung hinaus – festlegen.

2.3 Der DAB-Übertragungskanal

Dieser Abschnitt behandelt die nötigen Verarbeitungsschritte, um mehrere wie im letzten Abschnitt quellencodierte Tonsignale und/oder andere digitale Datenströme zusammenzufassen und so auf eine Trägerfrequenz zu modulieren, daß sie beim Empfänger möglichst fehlerfrei rekonstruiert werden können.

Das Hauptaugenmerk beim DAB liegt auf der Bereitstellung eines möglichst sicheren Übertragungskanals, die Sicherung der Quellensignale mit Schutzbits stellt also nur eine flankierende Maßnahme dar.

2.3.1 Die drei DAB-Modi

Um eine größtmögliche Flexibilität bei der Wahl der Frequenzbereiche für DAB-Sender zu erreichen, wurden bei der Standardisierung drei Übertragungsmodi festgelegt:

Modus I Dieser Modus ist für die Übertragung in terrestrischen Gleichwellennetzen bei Frequenzen bis 375 MHz vorgesehen. Er benutzt einen sehr großen Symbolvorrat (2^{3072} Symbole), um die erforderte Kapazität bei geringer Schrittgeschwindigkeit (1,25 ms) und langen Schutzintervallen (0,25 ms) zu ermöglichen. Damit wird erreicht, daß benachbarte Relaisstationen in Gleichwellennetzen bis zu 96 km voneinander entfernt sein dürfen.

Modus II Dieser Modus ist für lokale Radioprogramme gedacht, die nur eine Sendestation umfassen. Er benutzt einen kleineren Symbolvorrat (2^{768} Symbole) und schnellere Schritte (312 μs), um bei höheren Sendefrequenzen bis 1,5 GHz die dort stärker auftretenden Störeinflüsse durch Dopplereffekte bei bewegten Empfängern zu reduzieren.

Modus III Dieser Modus wird bei Satellitenübertragung oder Übertragung in Kabelnetzen eingesetzt. Er ist für Sendefrequenzen bis 3 GHz ausgelegt und benutzt den kleinsten Symbolvorrat (2^{384} Symbole) und die höchste Schrittgeschwindigkeit (156 μs), da bei Kabel- bzw. Satellitenübertragung Mehrwegausbreitung kaum auftritt.

Alle drei Modi haben eine Bandbreite des DAB-Kanals von 1,536 MHz und eine (Brutto-)Übertragungskapazität von 2,4 MBit/s gemeinsam.

2.3.2 Das DAB-Rahmenformat

Beim DAB wird der zu übertragende Bitstrom in Pakete fester Länge – die sogenannten DAB-Rahmen – unterteilt. Dabei besteht ein DAB-Paket aus drei Teilen (siehe auch Bild 6):

Synchronisationsteil (Synchronisation Channel, SC): Dieser dient zur Synchronisation und Regelung des DAB-Empfängers und enthält in jedem Rahmen die gleichen Daten: Ein Nullsymbol zur Markierung des Rahmenbeginns und ein Referenzsysmbol zur Abstimmung des Empfängers.

Steuerungsteil (Fast Information Channel, FIC): Dieser enthält Informationen über die Art und die Struktur der Daten im MSC.

Datenteil (Main Service Channel, MSC): Dieser enthält schließlich die Nutzinformationen selbst. Um die Daten mehrerer Radioprogramme oder sonstige Dienste im MSC zusammenzustellen, wird ein Multiplexer benutzt, der die Daten aller zu übertragenden Quellen sammelt und an den Übertragungskanal weitergibt; am Ausgang des Multiplexers fällt eine konstante Datenübertragungsrate von 2,4 MBit/s an. Die Information über die aktuelle Programmzusammensetzung des DAB-Signals, das der Multiplexer liefert, wird durch die Multiplex Configuration Information (MCI) festgelegt, die im FIC übertragen wird.

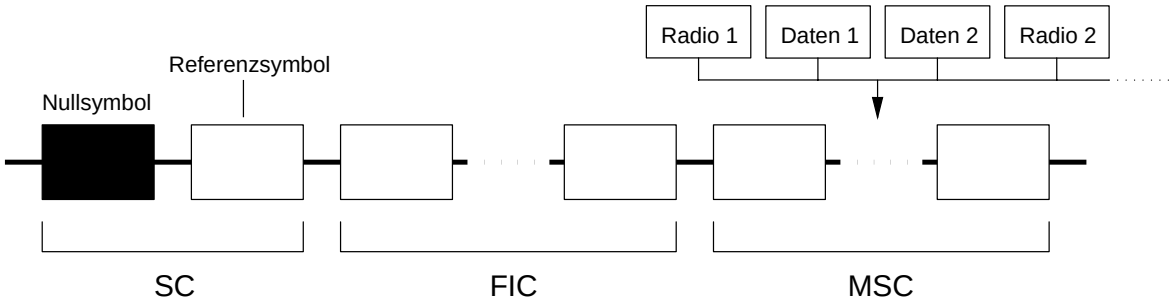


Abbildung 6: Die Struktur des DAB-Rahmens

2.3.3 Die spektrale Codierung

Genauer betrachtet besteht ein DAB-Rahmen aus einer Folge von Symbolen, von denen jedes genau einem Rahmenteil zugeordnet ist. Um die Übertragung gegen Störungen durch Mehrwegausbreitung zu sichern, wird statt einer schnellen Folge kurzer Symbole eine Folge langer Symbole gesendet, zwischen denen Schutzintervalle eingeschoben werden.

Um trotz der geringen Schrittgeschwindigkeit eine hohe Übertragungskapazität zu erreichen, wird ein sehr großer Symbolvorrat verwendet (je nach Übertragungsmodus 2^{384}–2^{3072} mögliche Symbole, d. h. pro Schritt werden 384–3072 Bit übertragen).

Zur Codierung der Symbole wird ein spezielles Verfahren verwendet, bei dem sehr viele Trägerfrequenzen (192–1536) gleichzeitig gesendet werden (Orthogonal Frequency Division Multiplex, OFDM); jede einzelne Trägerfrequenz wird dabei per differentieller Phasenmodulation (Differential Phase Shift Keying, DPSK) moduliert und überträgt 2 Bit Information pro Schritt (siehe auch Bild 7).

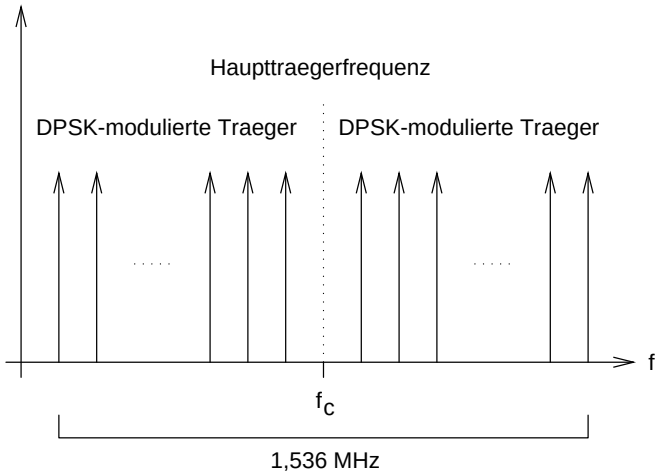


Abbildung 7: Spektrum des Sendesignals bei OFDM-Codierung

Differentielle Phasenmodulation bedeutet, daß die Phase jeder Trägerfrequenz – je nach Bitmuster – zwischen zwei Schritten um 45°, 135°, 225° oder 315° verschoben wird (4-DPSK). Da das Bitmuster bei diesem Verfahren nur durch den Phasenwechsel zwischen zwei Schritten bestimmt ist, muß zwischen Sender und Empfänger keine Referenzphasenlage übertragen werden; es genügt, in gewissen Abständen ein Symbol mit definierten Phasenlagen zu übertragen – genau dazu dient das Referenzsymbol am Anfang jedes DAB-Rahmens.

Die K Einzelträgerfrequenzen sind dabei so um die Hauptträgerfrequenz f_c gruppiert, daß ihre Frequenzen $f_k = f_c + k \cdot \triangle f$ sind, mit $k \in \{\pm 1, \pm 2, \ldots, \pm K/2\}$ (bei f_c selbst liegt keine Einzelträgerfrequenz). Die Frequenz $\triangle f$ ist so gewählt, daß die gesamte Bandbreite des DAB-Signals stets 1,536 MHz beträgt.

Die Sendedauer der Symbole ist mit $T_u = 1/\triangle f$ so gewählt, daß sie ein ganzzahliges Vielfaches der Periodendauer jeder einzelnen Trägerfrequenz ist. Zwischen zwei Symbolen wird ein Schutzintervall der (ungefähren) Länge $T_\triangle = 0,25 T_u$ eingefügt; die Summe aus Symboldauer und Schutzintervalllänge ergibt die Schrittgeschwindigkeit T_s der Übertragung.

2.3.4 Die HF-Modulation

Um die Vielzahl der möglichen OFDM-Symbole handhaben zu können, werden diese nicht gespeichert, sondern bei Bedarf aus den phasenmodulierten Trägerfrequenzen zusammengesetzt. Der Einfachheit halber erfolgt diese Synthese im Frequenzbereich; als nächstes muß das konstruierte Spektrum des OFDM-Symbols also per inverser Fouriertransformation in den Zeitbereich übertragen werden.

Diese Transformation liefert im allgemeinen eine komplexwertige Zeitfunktion der Periodendauer T_u. Wichtig ist hierbei, daß diese Zeitfunktion nicht nur während der Symboldauer T_u, sondern durch periodische Fortsetzung während der gesamten Schrittdauer T_s, also auch im Schutzintervall, gesendet wird. Dies geschieht, damit der Empfänger während eines Abtastzeitraums der Länge T_u auch dann eine volle Periode des OFDM-Symbols abtastet, wenn der Empfangstakt gegenüber dem Sendetakt verschoben ist. Die Abtastung einer vollen Periode ist wesentlich, da sonst das gesendete OFDM-Symbol nicht rekonstruiert werden kann.

Die fortgesetzte Zeitfunktion wird dann per Quadraturamplitudenmodulation (QAM) mit Real- und Imaginärteil einer Zwischenfrequenz aufgeprägt. Die am Ausgang des QA-Modulators anfallende rein reellwertige Zeitfunktion wird durch einen D/A-Wandler "analogisiert", in den Bereich der Hauptträgerfrequenz verschoben und dann endlich über Antenne abgestrahlt.

Durch die spezielle Art der Modulation ergibt sich ein Signal, das innerhalb seines Frequenzbandes einem weißen Rauschen ähnelt (alle Frequenzanteile sind gleichstark vertreten). Diese Eigenschaft bewirkt, daß einzelne bei der Übertragung gestörte Frequenzen (selektiver Frequenzschwund) nur einen gleichmäßig kleinen Teil des Signals stören.

Bei den im Moment laufenden Pilotprojekten liegt die Hauptträgerfrequenz im Bereich des TV-Kanals 12, also zwischen 223 MHz und 230 MHz. In diesem Bereich finden vier Kanäle der Breite 1,536 MHz Platz, die durch Schutzbänder der Breite 0,2 MHz getrennt sind; diese werden als DAB-Kanäle A bis D bezeichnet.

2.3.5 Die HF-Demodulation

Die erste Stufe des DAB-Empfängers funktioniert genauso wie beim herkömmlichen analogen Rundfunk: Mittels eines Bandpaßfilters wird die gewünschte Hauptträgerfrequenz aus dem empfangenen "Wellensalat" extrahiert und danach in den Bereich der Basisfrequenz verschoben.

Im zweiten Schritt wird die empfangene Zeitfunktion mit einem A/D-Wandler abgetastet und an den QA-Demodulator übergeben, der die (komplexwertige) Zeitfunktion des OFDM-Symbols rekonstruiert. Diese wird mittels Fouriertransformation in den Frequenzbereich transformiert.

Von entscheidender Bedeutung ist hierbei, daß die komplexwertige Zeitfunktion am Ausgang des QA-Demodulators nur während eines Zeitfensters der Länge T_u abgetastet wird. Da das OFDM-Symbol vom Sender während der gesamten Schrittdauer T_s abgestrahlt wird, hat der Empfänger die Freiheit, das Abtastfenster innerhalb der Schrittdauer zu verschieben. Dies kann genutzt werden, diejenige Position zu wählen, die die geringsten Störungen durch Nachbarimpulse enthält (siehe auch Bild 8). Diese Position kann für jeden DAB-Rahmen anhand des empfangenen Referenzsymbols

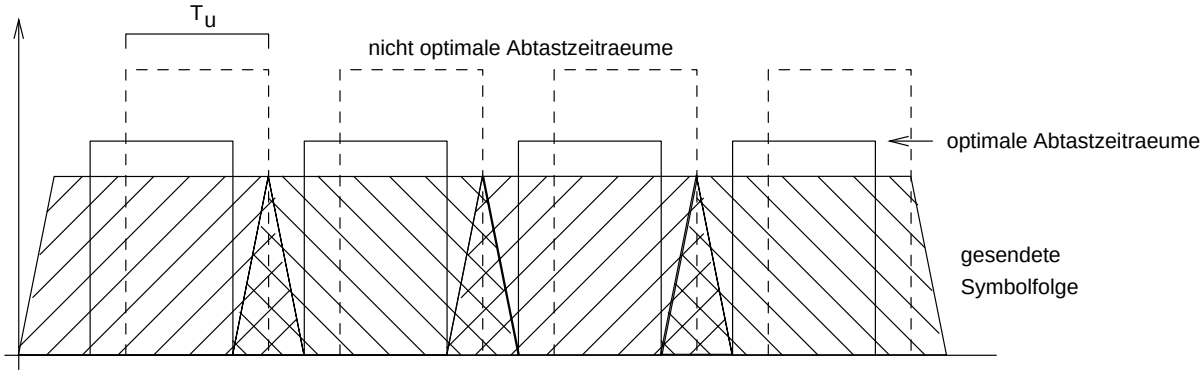


Abbildung 8: Abtastung der gesendeten OFDM-Symbole

berechnet werden.

Die Abtastung einer Zeitfunktion innerhalb eines Zeitfensters entspricht der punktweisen Multiplikation der Zeitfunktion mit einer Rechteckfunktion, die nur im Zeitfenster ungleich Null ist. Im Frequenzbereich bedeutet dies eine Faltung des Spektrums mit einer sinc-Funktion ($x \mapsto \sin x/x$). Da das Spektrum eines ODFM-Symbols aus Linien der Abstände $\triangle f$ besteht und da $T_u = 1/\triangle f$ ist, hat die zu einer Trägerfrequenz gehörende sinc-Funktion ihre Nullstellen gerade an den Stellen der anderen Trägerfrequenzen. Durch diesen "glücklichen" Umstand können die Phasen (und auch die Amplituden) aller Trägerfrequenzen durch Abtastung des Spektrums der empfangenen Zeitfunktion an den entsprechenden Stellen rekonstruiert werden. Die Orthogonalität der einzelnen Trägerfrequenzen entsteht also erst durch geschickte Wahl der Abtastdauer T_u auf Empfängerseite.

2.3.6 Die spektrale Decodierung

Nach der Berechnung des Spektrums wie oben angeführt, können die Phasen aller Trägerfrequenzen einfach bestimmt werden. Nun gilt es nur noch, den Phasensprung gegenüber dem zuletzt empfangenen Symbol zu berechnen, und daraus anhand einer Schwellwertentscheidung die gesendete Bitkombination zu rekonstruieren.

Um die Sicherheit der Übertragung zu erhöhen, wird bei der Schwellwertentscheidung ebenfalls berücksichtigt, wie nah die berechneten Phasendifferenzen den Entscheidungsschwellen waren: Je näher, desto wahrscheinlicher ist eine falsche Entscheidung. Anhand mehrerer empfangener Symbole kann dann diejenige Bitfolge berechnet werden,

die mit größter Wahrscheinlichkeit der gesendeten entspricht (Maximum-Likelihood-Decodierung).

3 Zusammenfassung und Ausblick

Die vorliegende Abhandlung hat aufgezeigt, welche Probleme des herkömmlichen analogen Rundfunks mit einer Umstellung auf digitale Übertragung in den Griff bekommen werden können; dies betrifft im besonderen die Bereiche Tonqualität und Flexibilität.

Momentan (Stand Mitte 1996) existieren fünf Ansätze für digitale Rundfunksysteme, die natürlich zueinander inkompatibel sind. In Europa wurde das im Rahmen dieser Abhandlung genauer dargestellte System nach Eureka-Projekt 147 zum Standard erhoben; in Großbritannien und Schweden gibt es bereits reguläres digitales Radio nach diesem Standard, in der Bundesrepublik laufen wenigstens Pilotprojekte (eins davon in Baden-Württemberg). Kanada setzt ebenfalls auf das Eureka-147-System, die Rundfunkbehörden der USA und Japans befinden sich noch in der Testphase der einzelnen Systeme.

Ob und wie schnell sich das digitale Radio gegenüber dem analogen Rundfunk durchsetzen kann, hängt wohl vor allem davon ab, wann die erforderlichen Empfänger zu vernünftigen Preisen und in Stückzahlen erhältlich sind (man beachte nur den Übergang von der Schallplatte zur CD im Heimaudiobereich). Eine weltweite Einigung auf einen gemeinsamen DAB-Standard ist zwar unwahrscheinlich, wäre dem Durchbruch dieser neuen Technologie aber sicher nicht hinderlich.

Literatur

[Wen96a] Dietmar Wenzel. Digital Audio Broadcasting, Teil 1: Grundlagen des digitalen Tonrundfunks. *ELRAD*, Januar 1996, Seite 83–88.

[Wen96b] Dietmar Wenzel. Digital Audio Broadcasting, Teil 2: Kanalkodierung etwas näher betrachtet – das OFDM-Verfahren. *ELRAD*, Februar 1996, Seite 104–108.

[Wen96c] Dietmar Wenzel. Digital Audio Broadcasting, Teil 3: Kanalkodierung und Betriebs-Modi. *ELRAD*, April 1996, Seite 85–88.

Abbildungsverzeichnis

Drahtloses ATM

Verena Rose

Kurzfassung

Seitdem Mobiltelefone und tragbare Computer immer größere Verbreitung finden, steigt auch das Interesse an mobilen Datennetzen. So sollen außer Sprache auch Texte, Bilder, Videos, kurz gesagt „Multimedia-Daten“ über Mobilnetze übertragen werden. Jedoch sind die Übertragungsraten in Mobilnetzen wesentlich geringer als in „traditionellen“ Festnetzen. Aufgrund dieser Tatsache müssen an diese Anforderungen angepaßte Kommunikationsprotokolle neu standardisiert werden.

Eine Lösung bietet eine Protokolldefinition, die auf ATM als Technologie, die variable und konstante Übertragungsraten anbietet, basiert. In dieser Ausarbeitung sollen daher die Konzepte und die Anforderungen, die ein ATM-kompatibles diensteintegrierendes Mobilnetz beinhaltet, dargestellt werden. Zu den Problemen, die sich auf den verschiedenen Schichten aufgrund der Gegebenheiten des Mediums ergeben, haben einzelne Arbeitsgruppen verschiedene Lösungsansätze entwickelt. Die experimentelle Architektur einer dieser Forschungsgruppen wird in diesem Artikel ausführlicher vorgestellt.

1 Einleitung

ATM (Asynchronous Transfer Mode) verspricht in Festnetzen die Technologie der Zukunft zu werden, da ATM „alles“ bietet: ATM ist ideal für lokale, nationale, internationale, private und öffentliche Netzwerke; ATM ist skalierbar in der Geschwindigkeit; ATM unterstützt sowohl isochronen Verkehr als auch Burstdaten; ATM bietet konstante und variable Bitraten, und ob Telefongespräch, Videokonferenz oder Dateien - alles kann übertragen werden [Hun96].

Der Begriff „ATM“ ist zunächst von Telefongesellschaften eingeführt worden: Asynchron bedeutet, daß die Daten nicht mehr in festen Zeitschlitzen pro Teilnehmer transportiert werden müssen. Das Attribut „asynchron“ bezieht sich also auf das Multiplexen, nicht auf die Übertragung der Daten.

ATM wird manchmal als schnelle Paketvermittlungstechnologie bezeichnet, dieser Begriff ist allerdings etwas irreführend, da es bei ATM ausschließlich Zellen fester Länge (53 Bytes) gibt. Aus der festen Zellänge resultiert auch die Geschwindigkeit, da Vermittlungsknoten einfacher implementiert werden können. ATM ist somit eine Zellstruktur und eine Vermittlungstechnologie.

ATM hebt die Grenze zwischen lokalen und internationalen Netzwerken auf, das hat zur Konsequenz, daß Übergänge von Protokollen und Geschwindigkeiten, die sonst in Routern implementiert sind, nun in der Infrastruktur von ATM enthalten sind. Dies macht ATM zu einer Spezifikation für die Schnittstelle zwischen WAN und LAN.

ATM ist auf den Schichten 1 und 2 des OSI-Referenzmodells definiert, jedoch werden die ATM-Zellen heute in den meisten Fällen noch über synchrone Architekturen wie SONET und SDH transportiert. Dies soll sich in Zukunft ändern, so daß die ATM-Zellen auch auf der physikalischen Schicht als reine ATM-Zellen übertragen werden. Damit ist ATM auch eine Spezifikation für die Bitübertragung [Hun96].

Im Bereich der drahtlosen Kommunikation gibt es heute zwei große Anwendungsbereiche: Systeme für persönliche Kommunikation (PCNs = Personal Communications Networks), die ihren Ursprung in den Mobiltelefonen haben, und drahtlose lokale Netzwerke (WLANs = Wireless Local Area Networks), die vor allem zur Datenübertragung genutzt werden. Diese beiden Linien entwickeln sich zu anspruchsvolleren Anwendungen hin, d.h. über beide Systeme sollen multimediale Anwendungen laufen können [RW92]. Aus diesem Grund ist es durchaus sinnvoll, eine Technologie zu nutzen, die beide Systeme integriert. Der Unterschied zwischen einem mobilen Kommunikationssystem in Fahrzeugen und einem drahtlosen Netz in einem Bürogebäude liegt hauptsächlich in der Funkübertragungstechnik, es müssen verschiedene Funkausbreitungsmodelle, Antennen, Störquellen etc. berücksichtigt werden. Allerdings gibt es auch Einschätzungen, daß ein Unterschied zwischen mobilen Kommunikationssystemen und WLANs bestehen bleiben wird, wobei das drahtlose ATM für WLANs konzipiert ist und Mobilkommunikationssysteme der dritten Generation für PCNs genutzt werden [Mik96].

In einem drahtlosen ATM-Netzwerk gibt es kleine Mikro- (Ausdehnung bis 500m) und Piko-Zellen (Ausdehnung bis 100m), in denen sich die Mobilstationen bewegen. Eine Basisstation pro Zelle bedient alle drahtlosen Stationen, physikalisch existiert hier also eine Punkt-zu-Mehrpunkt-Verbindung. Die Basisstationen selber sind über ein hierarchisches ATM-Festnetz verbunden. Die Mobilstationen kommunizieren miteinander ausschließlich über die Basisstationen. Alle Basisstationen arbeiten auf derselben Frequenz. Dies bedeutet, daß auf der physikalischen Ebene keine Übergabe stattfinden muß, wenn eine Mobilstation eine Zelle verläßt und in eine andere wechselt. Auf der Ebene der (virtuellen) Verbindungen muß dieser Übergabemechanismus jedoch stattfinden, was gegenüber Festnetzen eine hohe Komplexität bedeutet [PH94].

Die Anforderungen, die an ein drahtloses ATM-Netzwerk gestellt werden, beinhalten unter anderem die Kompatibilität zu Breitbandnetzen der Zukunft, die konstante und variable Bitraten und die Möglichkeit, burstartige Daten zu transportieren, anbieten. Zu den Diensten, die angeboten werden sollen, gehört keinesfalls nur die Hochgeschwindigkeitsübertragung, sondern auch eine flexible Bandbreitenzuteilung und die Garantie, bestimmte Dienstgütemerkmale einzuhalten. Diese Anforderungen werden durch die ATM-Technologie in Festnetzen erfüllt, doch in drahtlosen Netzwerken gibt es wesentlich geringe Übertragungsgeschwindigkeiten bei gleichzeitig höheren Fehlerraten, so daß eine quantitative Äquivalenz mit Netzen, die auf der Glasfaser-Technologie basieren, derzeit nicht verwirklicht werden kann. Dennoch sollten qualitativ die oben genannten Anforderungen erfüllt werden können [RW92].

Da die drahtlose Komponente vor allem eine Ergänzung des ATM-Festnetzes sein soll, muß sie transparent für die Benutzer des Netzes sein. Dies bedeutet, daß es einem Nutzer möglichst verborgen sein sollte, mit welchen Stationen (Mobil- oder Feststationen)

er innerhalb des Netzes kommuniziert. Dazu ist außer den schon genannten Anforderungen vor allem erforderlich, daß der Protokollturm für ein drahtloses ATM nur eine Ergänzung des ATM-Protokollturmes sein sollte. Speziell für die drahtlose Komponente werden physikalische Spezifikationen, die durch das Funkmedium bestimmt sind, und Funktionen zum Zugriff auf das Medium und zur Fehlersicherung und Flußkontrolle benötigt. Dies bedeutet, daß höhere Schichten, also z.B. die virtuelle Kanal- oder Pfadadressierung, mit der ATM arbeitet, nicht betroffen sind. Zur Netzwerkschicht müssen zusätzlich nur Funktionen zum Auffinden der Mobilstationen implementiert werden, die aber in der Infrastruktur der drahtlosen Komponente enthalten sind und somit keine Änderung bei der Vermittlung im ATM-Festnetz erfordern.

2 Nur ein weiteres drahtloses LAN?

Fast zu jedem Local Area Network (LAN) gibt es eine drahtlose Erweiterung. Ist ein drahtloses ATM also nur „eins unter vielen“, zumal, da die Anwendungen, die ein Multimedia-Mobilnetz benötigen, noch in relativ geringer Zahl vorhanden sind?

Schon bei ATM für traditionelle Festnetze stellt sich die Frage, ob ATM wirklich die Netzwerkwelt revolutioniert (was erheblichen Aufwand bei der Umstellung der Software verursachen würde), oder ob ATM nur eine LAN-Technologie unter vielen darstellt, die in wenigen Jahren schon wieder überholt sein kann.

Kriterien, die über die „Gewinner“ bei den verschiedenen Technologien entscheiden, beinhalten unter anderem [Wob96]:

- wie schnell verschiedene Produkte auf den Markt gebracht werden,
- wie schnell sich der Standard stabilisiert und etabliert,
- wieviel die Endsysteme kosten,
- die Notwendigkeit, neue Netzwerksoftware, eventuell bis zur Anwendungsschicht, zu implementieren,
- die Fähigkeit, LANs und WANs zu integieren,
- die Fähigkeit, den Kunden verschiedene Dienste zu einem geringeren Preis anzubieten.

Vom technischen Aspekt aus gesehen kann ATM viele Beschränkungen, denen heute weit verbreitete LANs unterworfen sind, aufheben. Deshalb kann auch eine zusätzliche drahtlose Komponente, wenn sie qualitativ den Anforderungen genügt, Vorteile für die Verbreitung bringen. Da aber viele Anbieter und Kunden eher das am weitesten verbreitete als das beste Produkt möchten, müssen Anstrengungen im Bereich Standardisierung möglichst schnell vorgenommen werden, um ATM tatsächlich in dem Maße zu verbreiten, wie z.B. Ethernet heute genutzt wird. Die große Verbreitung eines drahtlosen ATM-Netzwerkes kann nur Hand in Hand mit der Verbreitung des ATM/B-ISDN gehen.

3 Anforderungen für ein drahtloses ATM

Die drahtlosen LANs, die heute auf dem Markt sind, unterstützen entweder nicht mehrere Verkehrstypen oder benutzen hybride Systeme, die die Bandbreite in Reservierungs- und Kollisionsintervalle aufteilen [PH94].

Dagegen sollte das zu konzipierende drahtlose ATM-Netzwerk eine transparente, nahtlose und effiziente Ergänzung zu einem auf Glasfaser basierendem ATM- oder B-ISDN-Netzwerk sein. Heutige Anwendungen umfassen eine ganze Spanne von Dienstklassen, Dienstgütemerkmalen und Übertragungsraten. Die Dienstgütemerkmale, auch Quality-of-Service-(QoS-)Parameter genannt, beinhalten zum Beispiel die maximale Verzögerung, den maximalen Jitter oder auch die maximale Zellverlustrate.

Eine Übersicht über zusammengehörige Dienstklassen mit ihren Merkmalen zeigt Bild 1 [RW92]:

Anwendung / Parameter	Sprache	Digitales Radio	HDTV	Digitales Video	Daten	E-mail	Hochgeschw.-Daten (Multimedia)
Bitrate	konstant			variabel			
	2,4 - 32 kbit/s	128-512 kbit/s	15-20 Mbit/s	1-6 Mbit/s	0,1-1 Mbit/s	9,6 - 128 kbit/s	1 - 10 Mbit/s
Verbindungsart	verbindungsorientiert				verbindungslos		
erlaubter Zellverlust	niedrig - mittel	niedrig	niedrig - mittel	niedrig - mittel	niedrig	niedrig	sehr niedrig
erlaubte Verzögerung	-	niedrig	niedrig	niedrig	mittel	hoch	mittel

Abbildung 1: Dienste im ATM-Netz

Allgemein sollte eine Netzwerkarchitektur zwischen (Dienst-) Leistung, Netzwerkgüte und den Kosten für die Endsysteme ausgewogen sein. Die einzelnen Forderungen, die an den Systementwurf eines Netzwerkes für die Mobilkommunikation gestellt werden, beinhalten daher [RW92]:

- Flexibel anforderbare Dienste (Sprache, Daten, Multimedia-Anwendungen,...),
- Dienstgütegarantien für verschiedene Dienstklassen,
- hohe Kompatibilität zu Breitbandnetzwerken,
- niedrige Endsystemkosten,
- geringer Stromverbrauch (im Mobilbereich sehr wichtig!),
- hohe Bandbreiteneffizienz,
- skalierbare, effiziente Netzwerkarchitektur mit moderaten Kosten,
- Erfüllung von Beschränkungen, z.B. im Bereich der Frequenzzuweisung.

4 Architektur des drahtlosen ATM-Systems

Das „Herzstück“ eines ATM-Netzwerkes ist die ATM-Zelle. Sie hat stets die Länge 53 Bytes, wobei 48 Bytes Nutzdaten (Payload) und 5 Bytes Header (mit Routing-Information) sind. An dieser Zellstruktur soll sich in einer mobilen Umgebung auch möglichst nichts ändern, damit der Aufwand für z.B. Segmentierungen beim Übergang zum Festnetz gering ist.

Die kleine Zellgröße ist auch günstig für ein Mobilnetz, da sporadisch auftretende Fehler nur kleine Datenblöcke betreffen. So schlagen Raychaudhuri und Wilson sogar vor, die Zellgröße auf 24 oder 12 Bytes Nutzdaten zu beschränken, falls die Bitfehlerraten des Mobilnetzes dies erfordern [RW92].

Der Header unterscheidet sich bei den drahtlosen Architekturen von dem ATM-Header im Festnetz. So werden Funktionen zur Sicherung und Flußkontrolle hinzugefügt, während der Rest des Headers komprimiert wird. Bild 2 [PH94] zeigt den Unterschied zwischen den Headern beim RATM (Radio ATM) und Festnetz.

In den nächsten Abschnitten wird die Struktur der drahtlosen Komponente des ATM-Netzwerkes erläutert, darauf aufbauend wird der Protokollturm für drahtloses ATM gezeigt.

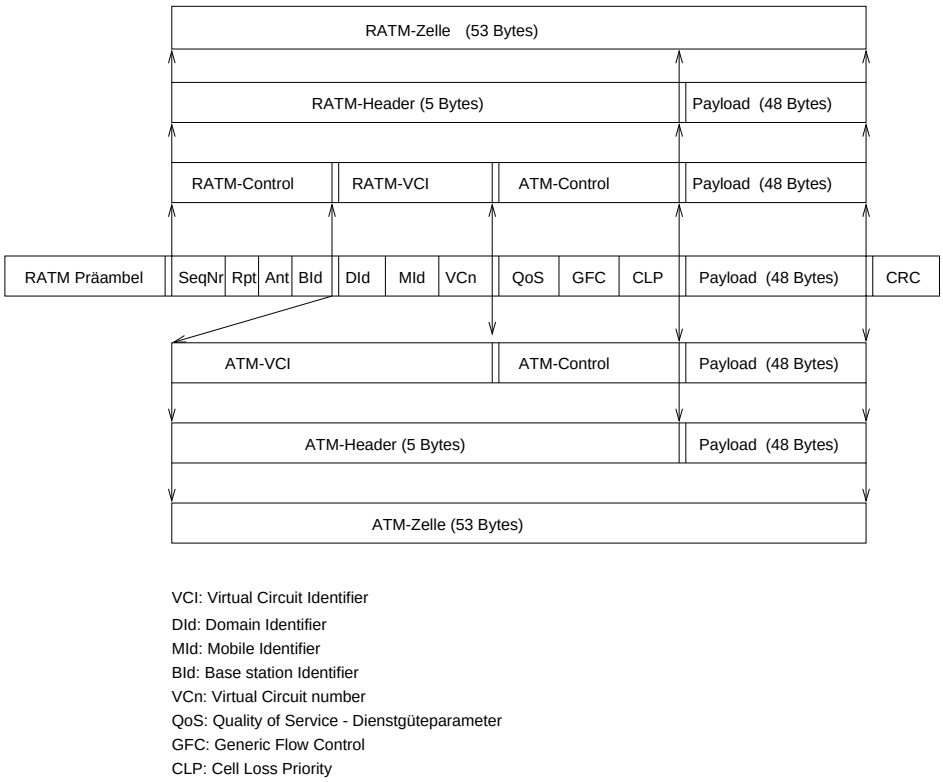


Abbildung 2: Vergleich von RATM-Zelle und ATM-Zelle

4.1 Struktur des drahtlosen Kommunikationsnetzwerkes

Das mobile Netzwerk besteht aus einer großen Zahl kleiner Übertragungsbereiche, den Piko-Zellen oder Mikro-Zellen. Jede Zelle wird von einer Basisstation bedient. Die

Basisstationen sind über das ATM-Festnetz miteinander verbunden. Auf der Mobilseite arbeiten sie alle auf derselben Frequenz, so daß es keine harten Grenzen zwischen den Piko-Zellen gibt und diese sich überlappen können. Die Basisstationen übersetzen die Header-Formate von drahtlosem ATM-Netzwerk zum ATM-Festnetz, da an der Struktur und Größe der ATM-Zelle nichts geändert wird, können die Basisstationen hardwaremäßig einfach gehalten werden.

Die Ausdehnung der Zellen (und damit die Anzahl der benötigten Basisstationen) wird von einzelnen Arbeitsgruppen unterschiedlich gehandhabt. Kleinere Zellen, die sich eventuell sogar auf einen einzigen Raum in einem Gebäude beschränken, können zur Lösung der Probleme drahtloser Netzwerke in Gebäuden (WLANs) beitragen, da es dann Sichtverbindungen gibt und Mehrwegeausbreitung vermieden wird. Doch kleinere Zellen haben auch Nachteile, so befinden sich sehr wenige Mobilstationen in Reichweite einer Basisstation, so daß deren Kosten und Verbindungen kritisch werden. Dies gilt vor allem für PCN-Systeme. Des weiteren wird die Häufigkeit der Übergaben der Mobilstationen zwischen den Basisstationen erhöht. Da die Piko-Zellen sich aber überlappen können, gibt es keinen speziellen Zeitpunkt, an dem die Übergabe stattfinden muß [PH94]. Für die Integration von WLANs und PCN-Systemen ist auch eine Mischstruktur denkbar, bei der in Gebäuden Piko-Zellen und für Mobilkommunikation Mikro-Zellen genutzt werden [Sin96].

Das drahtlose ATM-Netzwerk kann einfach erweitert werden, neue Piko-Zellen können einfach durch Hinzufügen einer neuen Basisstation eingerichtet werden. Dabei wird die Basisstation nur bei der Managementeinheit registriert, es muß nicht das ganze Netzwerk rekonfiguriert werden [PH94].

Bild 3 zeigt die grobe, sehr allgemeine Struktur der mobilen Umgebung. Das Management der Mobilstationen beispielsweise wird hier vernachlässigt, da es sehr architekturabhängig ist und später an einem Beispiel erläutert wird.

4.2 Der Protokollturm für drahtloses ATM

Der ATM-Protokollturm wird für die drahtlose Kommunikation um eine spezielle physikalische Schicht für Funkkanäle, um eine MAC- und um eine Datensicherungsschicht unterhalb der ATM-Vermittlungsschicht ergänzt. Die regulären Dienste der ATM-Vermittlungsschicht bleiben dabei erhalten und werden nur insoweit ergänzt, als es z.B. für das Auffinden der Mobilstationen im Netzwerk erforderlich ist [RW92].

Bild 4 zeigt die Benutzersäule (U-Plane) und die Signalisierungssäule (C-Plane) des ATM-Protokollturms. Die Zusätze, die für die drahtlose Komponente nötig sind, sind in gestrichelten Linien eingefügt.

4.2.1 Die physikalische Schicht (Physical Layer)

Bei drahtloser Kommunikation ist das physikalische Medium die Luft, und die Daten müssen über dieses Medium so übertragen werden, daß möglichst hohe Übertragungsgeschwindigkeiten erreicht werden. Neben der Frage, welches Modulationsverfahren benutzt werden soll, sind auch die zu nutzenden Frequenzbänder Gegenstand der Forschung.

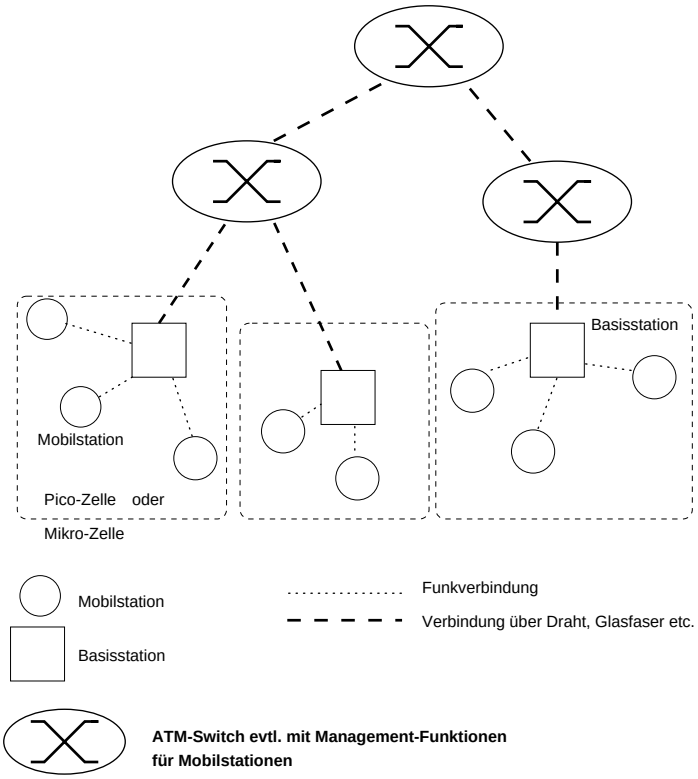


Abbildung 3: Grobstruktur des drahtlosen ATM-Netzwerkes

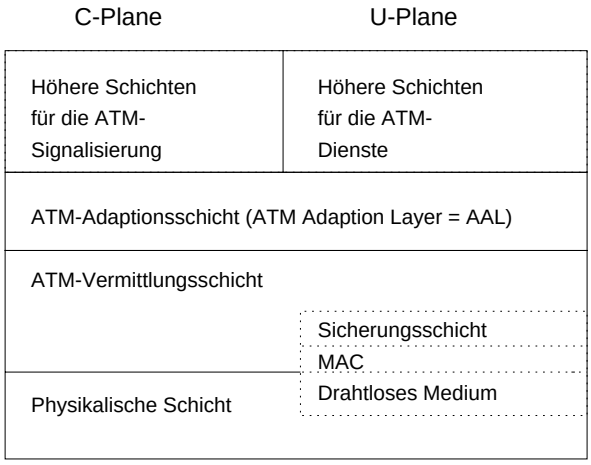


Abbildung 4: Protokollturm (C-Plane und U-Plane) des drahtlosen ATM

Einige Autoren propagieren Frequenzen um 60 GHz als für Breitbandnetze gut geeignete Bereiche [YBHD93]. Dort sind große Bandbreiten nutzbar, wobei nur wenig Störungen zu erwarten sind. Allerdings ist auf höheren Frequenzen die Abschwächung größer.

Porter und Hopper haben ein experimentelles drahtloses ATM-Netzwerk auf 2,4 GHz aufgebaut, andere Gruppen tendieren zu Bereichen um 17 GHz [Mik96].

Als Modulationsverfahren kommen prinzipiell sowohl Spread-Spectrum- als auch Schmalbandverfahren in Frage.

Spread-Spectrum hat den großen Vorteil, daß es extrem störunanfällig ist. Schmalbandstörer von anderen Systemen werden gespreizt, so daß das Nutzsignal immer noch gut dekodiert werden kann. Außerdem hat das Verfahren einen inhärenten Schutz gegen Mehrwegeausbreitung, die vor allem in Gebäuden sehr große Probleme verursacht.

Der Nachteil des Spread-Spectrum-Verfahrens ist, daß bei einer gegebenen Bandbreite die Benutzerdatenrate auf ein relativ niedriges Niveau beschränkt ist. So ist bei einer Bandbreite von 50 MHz und einem Spreizfaktor von 512 die Benutzerdatenrate auf ca. 100kb/s beschränkt [RW92]. Daher sind Spread-Spectrum-Verfahren eher für einzelne Zugangspunkte in Gebieten, in denen es schwer ist, überhaupt ein Glasfasernetz zu installieren, ausgelegt.

Schmalbandmodulationsverfahren sind heute schon sehr gut erforscht, am bekanntesten sind QPSK- und QAM-Verfahren. Als neues Verfahren wird das COFDM (Coherent Orthogonal Frequency Division Multiplex) vorgeschlagen, das sowohl eine gute Bandbreiteneffizienz als auch Schutz gegen Störungen bietet [RW92].

Maßnahmen gegen die Probleme mit Mehrwegeausbreitung können auch durch Antennen-Diversity-Verfahren getroffen werden. Dabei werden die Signale von verschiedenen Antennen ausgestrahlt, die weniger als eine Wellenlänge voneinander entfernt sind [PH94].

4.2.2 Zugriff zum Medium (Media Access Control)

Bei drahtloser Kommunikation gibt es einen Wettbewerb um das Medium, da die Stationen nicht alle miteinander, sondern nur mit der jeweiligen Basisstation kommunizieren. Es muß festgelegt werden, wie der Zugriff auf das Medium zu erfolgen hat. Die beiden Verfahren des Code Division Multiple Access (CDMA) und Time Division Multiple Access (TDMA) haben sich laut der Veröffentlichungen zu diesem Thema als Lösungsmöglichkeiten herausgestellt. Hier sollen Vor- und Nachteile gegenübergestellt werden.

Wenn als Modulationsverfahren Spread-Spectrum benutzt wird, muß normalerweise CDMA benutzt werden, damit die beschränkte Datenrate durch das Zugriffsverfahren verbessert wird.

Bei CDMA senden alle Stationen gleichzeitig und im selben Band, d.h. die Sendungen überlagern sich. Die einzelne Sendung ist durch eine Signatur (Spreizcode) charakterisiert. Im Empfänger wird die gewünschte Sendung durch Code-Korrelation herausgefiltert. Für die nutzbaren Codefamilien bedeutet dies, daß jeder Code von jedem

anderen einfach unterscheidbar und jeder Code auch von seinen zeitverschobenen Versionen leicht trennbar sein muß.

Bei TDMA wird dem Nutzer über eine Zeitdauer hinweg der gesamte Frequenzbereich zur Verfügung gestellt. Da zu jedem Zeitpunkt nur ein Träger auf dem Kanal ist, gibt es keine Intermodulationsprodukte. Ein weiterer Vorteil ist, daß der Durchsatz auch bei größerer Teilnehmerzahl hoch bleibt.

Porter und Hopper verwenden bei ihrer experimentellen Architektur Slotted ALOHA mit einer Slotlänge, die genau der Länge der ATM-Zelle entspricht. Die Slotstruktur wird dabei erreicht, indem die Mobilstationen bei jeder empfangenen Sendung mit der Basisstation synchronisiert werden. Slotted ALOHA ist im Gegensatz zu CSMA auch robust gegen Störungen angrenzender Zellen, da der Zustand des Empfängers entscheidend ist [PH94].

Younger et al. argumentieren dagegen, daß Slotted Aloha und seine Abkömmlinge ausgeschlossen sind, da sie zu geringen Durchsatz ermöglichen [YBHD93].

Andere Ansätze favorisieren CSMA/CA (Collision Avoidance), ein Verfahren, daß prinzipiell ähnlich dem CSMA/CD des Ethernet ist, aber darauf bedacht ist, Kollisionen zu vermeiden, indem ein gewisses Intervall abgewartet wird, falls der Sendewunsch nicht erfüllt wird. Auf einem Funkmedium ist es ohne weiteres nicht möglich, Kollisionen zu erkennen, da der Sender sich selber immer am stärksten hört. Allerdings benutzt diese Architektur ein Spread-Spectrum-Verfahren zur Modulation, so daß scharfe Grenzen zwischen den Piko-Zellen gezogen werden und keine Störungen auftreten [ES96].

Mehr aus der Satellitenkommunikation stammt der Vorschlag, ein DAMA-Zugriffsprotokoll zu implementieren. Bei diesem Verfahren werden die Stationen nacheinander nach Sendewünschen befragt. Das Verfahren kann durch Prioritätenzuweisung und Aufteilung der leeren Slots entsprechend verfeinert werden [Was95].

Fazit ist, daß es sehr viele Möglichkeiten zum geteilten Zugriff auf das Funkmedium gibt. Welche die beste ist, müssen Forschungsarbeiten und Experimente zeigen. Raychaudhuri und Wilson geben die Einschätzung ab, daß sowohl CDMA- als auch TDMA-Lösungen nebeneinander existieren könnten, da für verschiedene Ausbreitungscharakteristika (in bzw. außerhalb von Gebäuden) auch verschiedene Lösungen optimal sein können.

4.2.3 Die Datensicherungsschicht (Data Link Layer)

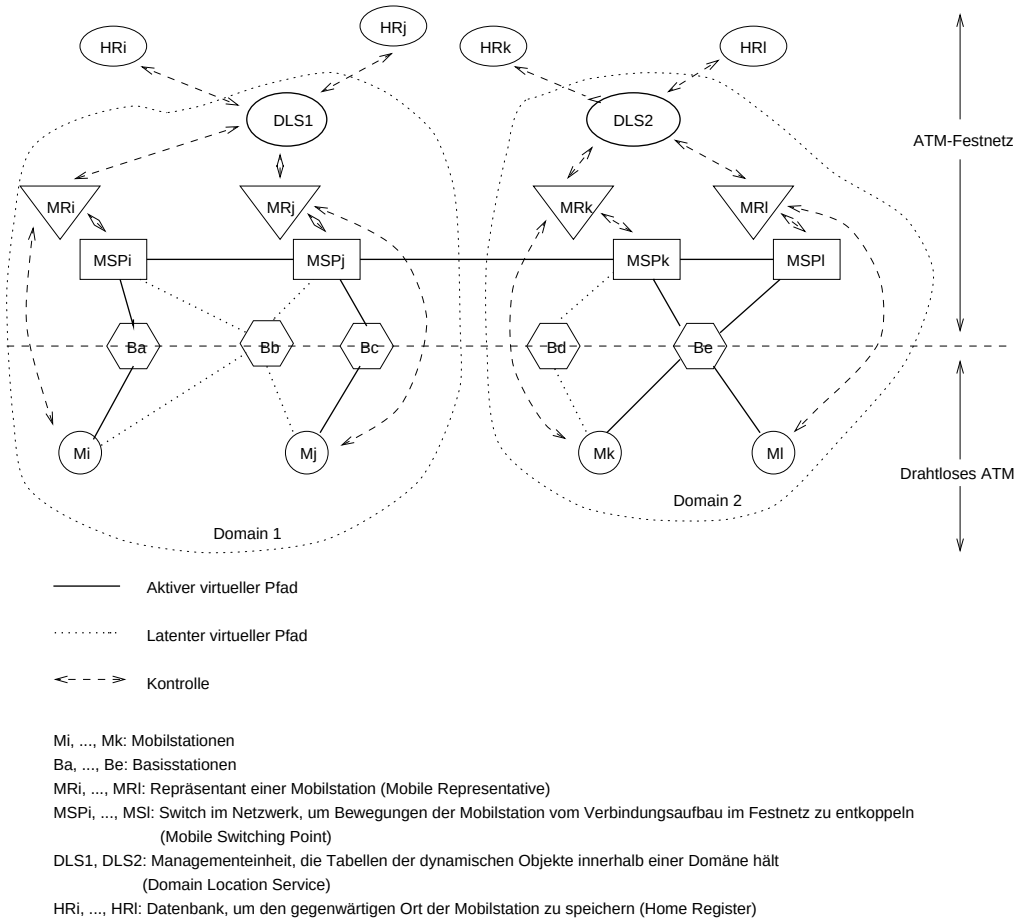
Da in einem drahtlosen Kommunikationsnetz relativ hohe Fehlerraten auftreten, gilt es, die höheren Schichten vor auftretenden Fehlern, Verzögerungen und Stausituationen zu sichern.

Zur Fehlersicherung werden in dem Header der drahtlosen Komponente Folgenummern eingeführt. Wenn mit Quittierungen gearbeitet wird und die Quittung verloren geht, wird die Zelle dupliziert und nochmals gesendet. Die doppelte Zelle wird erst von der ATM-Adaptionsschicht erkannt, was in manchen Fällen zum Verlust des assoziierten Blocks, in jedem Fall aber zu einer Leistungsminderung führt. Deshalb werden Folgenummern dazu benutzt, so duplizierte Zellen zu erkennen und entsprechend zu behandeln [PH94].

4.2.4 Die ATM-Vermittlungsschicht (ATM Network Layer)

Ähnlich wie bei Drahtnetzen stellt sich die Frage, welche Verfahren zur Wegewahl zu entfernten Knoten zu verwenden sind. Dazu kommt für ein drahtloses ATM-Netz noch das Problem, daß Mobilstationen sich an andere Orte bewegen und damit auch an ganz anderen Basisstationen aufzufinden sind.

Porter und Hopper geben im Rahmen ihrer Versuche zu drahtlosem ATM eine genauere Definition der Funktionen der Vermittlungsschicht an [PH94]:



Mi, ..., Mk: Mobilstationen
Ba, ..., Be: Basisstationen
MRi, ..., MRl: Repräsentant einer Mobilstation (Mobile Representative)
MSPi, ..., MSl: Switch im Netzwerk, um Bewegungen der Mobilstation vom Verbindungsaufbau im Festnetz zu entkoppeln (Mobile Switching Point)
DLS1, DLS2: Managementeinheit, die Tabellen der dynamischen Objekte innerhalb einer Domäne hält (Domain Location Service)
HRi, ..., HRl: Datenbank, um den gegenwärtigen Ort der Mobilstation zu speichern (Home Register)

Abbildung 5: Komponenten für das Management der Mobilstationen

Management der Mobilstationen: Die Kontrolle und das Management der Mobilstationen muß über das Festnetz erfolgen, da die Mobilstationen selbst möglichst einfach aufgebaut sein sollen.

Jeder Mobilstation wird ein Mobile Representative (MR) zugeordnet, wenn sie innerhalb einer Domäne registriert wird. Der MR ist ein Softwareobjekt, das logisch den Ort der Mobilstation im Festnetz definiert. Er stellt der Mobilstation einen Signalisierungskanal bereit, über den die Kontrolle ausgeübt und die Kommunikation mit dem Domain Location Service (DLS) und den Basisstationen, die sich in der Reichweite der Mobilstation befinden, geführt wird.

Da nicht alle virtuellen Verbindungen bei jeder Übergabe zwischen Piko-Zellen neu aufgebaut werden sollen, wird ein Mobile Switching Point (MSP) eingerichtet. Der

MSP ist eine Stelle, durch die alle virtuellen Verbindungen zur Mobilstation vermittelt werden. Von dem MSP aus gibt es eine Anzahl potentieller Basisstationen, die die Mobilstation erreichen kann. Diese virtuellen Verbindungen von einer Basisstation zu einer Mobilstation bilden virtuelle Pfade, die durch ein einziges Signalisierungskommando am MSP geändert werden können. Wenn ein virtueller Pfad aktiv ist, sind auch seine zugeordneten virtuellen Verbindungen aktiv, die anderen virtuellen Pfade sind latent, es fließt kein Verkehr über sie.

Übergabe zwischen Piko-Zellen: Dadurch, daß alle virtuellen Verbindungen einer Mobilstation gemeinsam kontrolliert werden können, werden bei einer Übergabe zwischen Piko-Zellen die virtuellen Verbindungen auf latente virtuelle Verbindungen abgebildet, indem der virtuelle Pfad geändert wird.

Eine Übergabe der Mobilstation von der Basisstation B_i zur Basisstation B_j läuft nach Vorschlag von Porter und Hopper folgendermaßen ab:

1. Der Mobile Switching Point wird aufgefordert, die virtuellen Pfade zu ändern.

2. Die Basisstation B_i muß die Übermittlung an die Mobilstation beenden, alle gepufferten Zellen werden verworfen.

3. Die Basisstation B_j nimmt die Übermittlung an die Mobilstation auf.

4. Die Mobilstation wird über die Übergabe informiert.

5. Die Basisstation B_i beendet den Empfang von der Mobilstation.

Diese Abfolge wird gewählt, um die Komplexität der Übergabe und die Wahrscheinlichkeit, daß Zellen falsche Wege nehmen, zu vermindern. Die bei der alten Basisstation gepufferten Zellen werden so nicht gesendet, sondern verworfen. Die neue Basisstation kann sofort die Übermittlung beginnen, da die Mobilstation Zellen von jeder Basisstation bekommen kann, die die Identifikation der Mobilstation und der Domäne im Header richtig setzt.

Auffinden der Mobilstation im Netzwerk: Um eine Verbindung zu einer Mobilstation aufbauen zu können, muß diese im Netzwerk aufgefunden werden. In kleinen Systemen können Broadcasts ausgesendet werden, um die Station zu finden, im allgemeinen muß ein Objekt sich jedoch selber bei einem bestimmten Registrierungspunkt, der aus einer Datenbank besteht, an die dann die Anfragen gerichtet werden, anmelden.

Porter und Hopper schlagen ein hierarchisches Registrierungssystem vor. Innerhalb einer Domäne wird eine Mobilstation bei dem Domain Location Server (DLS) der Domäne registriert. Dieser meldet dann die Mobilstation bei ihrem Home Register (HR) an, der die Information behält, welcher DLS gerade zu der Mobilstation gehört. Die Mobilstation hat eine statische Home-Adresse, die auf die Adresse des HR abgebildet wird und äquivalent etwa einer IP-Adresse ist, so daß bei einer Anfrage nach der Mobilstation ein traditioneller Name-Server benutzt werden kann.

5 Beispiel einer experimentellen Architektur

Die umfassendste experimentelle Arbeit zu diesem Thema, in obigen Abschnitten schon mehrmals erwähnt, haben John Porter und Andy Hopper bei Olivetti geleistet [PH94]. Sie haben das System RATM (Radio ATM) um eine Reihe kleiner ATM-Switches aufgebaut. Dazu haben sie Switches gewählt, die eine flexible Kontrolle der Managementinformationen und der Daten ermöglichen. Mit einer gewissen Leistungsverminderung ist es möglich, die QoS-Mechanismen in Software auszulagern. Die übliche Leistung eines Switches beträgt 1 Million Zellen pro Sekunde, wenn keine zusätzlichen Kontrollfunktionen ausgeübt werden.

An die Hardware können auch Peripheriegeräte direkt angeschlossen werden. Die Hardware-Komponente eines Switches besteht aus Netzwerkmodulen, die üblicherweise bei 100 Mbit/s arbeiten, und mehreren Schnittstellen zum Anschluß der Geräte, eventuell weiterer Switches und des Funkmoduls, das die Funktion einer Bridge zwischen Festnetz und drahtlosem Netz wahrnimmt.

Die Trägerfrequenz des Systems liegt bei 2,45 GHz und nutzt 10 MHz Bandbreite. In Großbritannien kann dieses Band unlizenziert für Verbindungen mit kleiner Reichweite in Gebäuden genutzt werden. Die Übertragungsleistung beträgt 10 dBm, was für Pikozellen mit einem Radius von 10 m ausreicht. Als Modulationsverfahren wird QPSK mit einer Bitrate von 10 Mbit/s benutzt, um innerhalb der gewünschten Bandbreite zu bleiben.

Um Störungen auszublenden, wird ein Antennen-Diversity-Verfahren angewendet. Ein Antennen-Switch wählt vor jeder Aussendung eine spezielle Antenne aus, und jedes Mal, wenn eine ATM-Zelle wiederholt wird, wird die Antenne neu gewählt.

Ein wichtiger Parameter in einem Funkmodul ist die Umschaltzeit zwischen Empfang und Sendung, diese beträgt 2 Mikrosekunden, wobei die Übertragungszeit einer Zelle 50 Mikrosekunden beträgt. Dies kann als tolerierbare Verzögerungszeit angesehen werden.

Als MAC-Protokoll wird — wie bereits erwähnt — Slotted ALOHA benutzt, wobei der Sender bei Erhalt einer Synchronisationszelle auf den Empfänger synchronisiert werden kann, um die Slotlänge von 53 Bytes zu erhalten. Das Protokoll ist auf einem reprogrammierbaren Xilinx-Gate-Array implementiert, so daß mit Parametern des Protokolls experimentiert werden kann.

Das Auffinden der Mobilstationen wird wie im Abschnitt 4.2.4 erklärt durchgeführt. Zu dem RATM-System gehören auch Hardware-Komponenten wie Speicher, Video- und Audiomodule und einfache Bildschirme. Mit diesen Peripheriegeräten werden Anwendungen wie Videokonferenzen oder permanente Videoverbindungen untersucht. Durch die Funktechnologie können innerhalb des Systems mobile Versionen dieser Anwendungen untersucht werden.

6 Bewertung

Singh kritisiert den Ansatz, ein mobiles Netzwerk als Erweiterung des ATM-/B-ISDN-Netzwerkes zu implementieren. Seiner Ansicht nach hat ein drahtloses ATM folgende Nachteile [Sin96]:

- Wenn sich Mobilstationen in andere Mikrozellen begeben, können ATM-Zellen außerhalb der Reihenfolge übermittelt werden, da die alte Basisstation alle Zellen an die neue ausliefert. Falls die neue Basisstation alle Zellen von der alten holen soll, führt dies zu Verzögerungen, die abhängig von der Anwendung evtl. nicht akzeptabel sind.
- Es gibt keine einfache Kommunikation in Gruppen von Mikrozellen, da nicht entschieden kann, welche Gruppen von Mikrozellen für die Multicast-Übertragung geeignet sind, wenn die Benutzer sich fortbewegen.
- Wenn Benutzer sich in andere Zellen bewegen, müssen die Pfade, das heißt, die Tabellen in den ATM-Switches, erneuert werden.
- Wenn ein Benutzer mit seinen Verbindungen in eine Zelle kommt, in der die Bandbreite ausgelastet ist, führt dies dazu, daß die QoS-Parameter für seine Verbindungen nicht mehr eingehalten werden können. Der Benutzer muß dann die QoS-Parameter für diese Verbindungen fast jedes Mal, wenn er die Grenzen der Mikrozelle überquert, neu verhandeln.

Diese Kritik bezieht sich hauptsächlich auf das Papier von Raychaudhuri und Wilson, in dem die Funktionen der Vermittlungsschicht nicht genau spezifiziert worden sind. Porter und Hopper bieten mit der im vorigen Abschnitt genannten Architektur Lösungen für die Probleme, die sich im Zusammenhang mit der Bewegung der Mobilstationen ergeben. So unterscheidet sich deren Lösungsvorschlag hauptsächlich in dem Punkt von der Architektur Singhs, daß dieser variable Paketlängen statt der festen Zellgröße der ATM-Zelle benutzt.

Durch den Mechanismus bei der Übergabe der Mobilstation, daß die neue Basisstation zuerst über die Übergabe informiert wird, werden kaum ATM-Zellen außerhalb der Reihenfolge an die Mobilstation gesendet. So werden auch wenig Zellen doppelt gesendet.

Durch die latenten virtuellen Pfade wird die Übergabe zwischen den Zellen auch sehr beschleunigt und vereinfacht.

Es gibt in der Architektur des drahtlosen ATM auch die Möglichkeit, daß Gruppen von Mikro-/Piko-Zellen als Domäne definiert werden, allerdings überlappen sich die Domänen nicht, so daß die Bewegung in andere Domänen hinein komplizierter zu handhaben ist.

Das größte Problem ist das der evtl. nicht mehr erfüllbaren QoS-Parameter, da dies die qualitativen Anforderungen an das drahtlose ATM stark betrifft. Die Übergabe zwischen den Zellen kann zwar herausgezögert werden, da die Zellen sich überlappen, dennoch wird in vielen Fällen eine neue Verhandlung der QoS-Parameter nötig sein. Mit Hilfe der Prioritätsangabe kann entschieden werden, welche Verbindung auf jeden Fall ihre Dienstqualität beibehalten muß. Dies werden vor allem Anwendungen mit konstanten Bitraten sein, da dort die Anwendung eingreifen muß, wenn die QoS-Parameter nicht einzuhalten sind.

Eine feste Zellgröße ist für ein Mobilnetz dagegen durchaus von Vorteil, da das MAC-Protokoll einfacher gestaltet werden kann. Der Header kann in der drahtlosen Komponente auch mit Funktionen der Sicherungsschicht ergänzt werden, da er in der Basisstation einfach in einen ATM-Header übersetzt werden kann.

7 Abschließende Bemerkungen

ATM zieht zur Zeit wachsendes Interesse auf sich, und es ist für Festnetze klar, daß ATM ideal für die Übermittlung von Sprache, Video und konventionellen Daten ist [Hun96]. Doch auch dort ist die Standardisierung noch nicht abgeschlossen.

Im Oktober 1995 ist der Vorschlag eines drahtlosen ATM-Systems erstmals in ein Standardisierungsgremium gebracht worden. Das Sub-Technical Committee der ETSI RES10 beschäftigt sich seitdem damit, einen Standard für die Bitübertragungsschicht zu entwerfen. Im April 1997 soll der erste Entwurf eines Standards erscheinen, der dann bis Dezember 1997 durch das Sub-Technical Committee und das Technical Committee gebilligt werden soll.

Das ATM-Forum, ein Zusammenschluß von Firmen, beschäftigt sich seit dem Treffen im Oktober 1995 ebenfalls mit den drahtlosen Aktivitäten im ATM-Bereich.

Um die Standardisierung einheitlich zu gestalten, könnte sich dabei das ATM-Forum auf die Festnetzseite konzentrieren, während RES10 die Schnittstelle der drahtlosen Komponente spezifiziert. Das ATM-Forum sollte dabei jedoch berücksichtigen, daß die physikalische Schicht des ATM-Netzwerks nicht immer zuverlässig ist und die Endsysteme auch Mobilstationen sein können [Mik96].

Das Problem bei der Einführung eines drahtlosen ATM-Netzwerks ist hauptsächlich die Frage, inwieweit sich ATM in Festnetzen durchsetzen wird. Die Kompatibilität von einem drahtlosen System zu einem Festnetz ist ein wichtiger Faktor, da so die Transparenz für die Benutzer fast ohne jeden Übersetzungsaufwand gewährleistet werden kann.

Daneben wird auch noch einige Forschungsarbeit geleistet werden müssen, um zu zeigen, daß drahtloses ATM zumindest qualitativ den Anforderungen an ein diensteintegrierendes Netz der Zukunft genügen kann. Dazu gehört, wie in den obigen Abschnitten erwähnt, Entscheidungen über die genaue Spezifikation der Mobilkomponente wie auch über ihr Management zu treffen. Forschungsprojekte, die zum Teil auch von der Europäischen Union unterstützt werden, sind z.B. The Magic WAND (Wireless ATM Network Demonstrator), das eine Übertragungsrate von 20 Mbit/s bei 17 GHz erreichen möchte, während sich MEDIAN das Ziel gesetzt hat, 155 Mbit/s bei 60 GHz zu erreichen [Mik96].

Nach der Spezifikation wird der Hauptaufwand jedoch in den Standardisierungsgremien in Zusammenarbeit mit Anwendergruppen geleistet werden müssen, damit (drahtloses) ATM nicht nur ein großes Forschungsprojekt bleibt, sondern eine ebenso weite Verbreitung findet wie sie heute z.B. Ethernet hat.

Literatur

[ES96] David Eckhardt and Peter Steenkiste. Measurement and Analysis of the Error Characteristics of an In-Building Wireless Network. *ACM SIGCOMM*, pages 243–254, Aug 1996.

[Hun96] Ray Hunt. Tutorial: ATM - protocols and architecture. *Computer Communications*, 19:597–611, 1996.

[Mik96] Jouni Mikkonen. Wireless ATM Overview. *Nokia, http://www.club.nokia.com/library*, 1996.

[PH94] John Porter and Andy Hopper. An ATM based Protocol for Wireless LANs. *Olivetti Research Limited*, Apr 1994.

[RW92] Dipankar Raychaudhuri and Newman D. Wilson. ATM-Based Transport Architecture for Multiservices Wireless Personal Communication Networks. *IEEE Journal on Selected Areas in Communications*, 12(8):1401–1414, Oct 1992.

[Sin96] Suresh Singh. Quality of service guarantees in mobile computing. *Computer Communications*, 19:359–371, 1996.

[Was95] Atif S. Wasi. Wireless ATM. *Seminar, http://www.cis.ohio-state.edu/~jain/cis788/wireless_atm/index.html*, 1995.

[Wob96] John Wobus. LAN Technology Scorecard. *http://web.syr.edu/ jmwobus/comfaqs/lan-technology*, Oct 1996.

[YBHD93] E.J. Younger, K.H. Bennett, and R. Hartley-Davies. A model for a broadband cellular wireless network for digital communications. *Computer Networks and ISDN Systems*, 26:391–402, 1993.

Abbildungsverzeichnis

Routing in ATM- und „Multiprotokoll über ATM“-Netzwerken

Matthias Korkisch

Kurzfassung

ATM, der Asynchrone Transfer Mode, ermöglicht den Aufbau hochleistungsfähiger dienstintegrierender Netzwerke. Für private Netzwerke wurde vom ATM-Forum das PNNI-Protokoll als flexibles und mächtiges Routingprotokoll entwickelt. Es erlaubt eine weitgehend automatische und dynamische Konfiguration des Netzes. Mit einer hierarchischen Struktur ermöglicht es auch den Aufbau sehr großer Netze. Zusätzlich muß jedoch in heterogenen Netzwerken das Routing von mehreren Vermittlungsschichtprotokollen wie beispielsweise IP über ATM betrachtet werden.

Im ersten Teil dieses Beitrages wird das *PNNI-Routingprotokoll* vorgestellt. Danach werden Probleme und verschiedene Lösungen beim *Routing in „Multiprotokoll über ATM“-Netzwerken* präsentiert.

1 ATM und PNNI

ATM-Netze sind *verbindungsorientierte Hochgeschwindigkeitsnetze*. Die Verbindungen zwischen Endsystemen heißen virtuelle Kanäle (Virtual Channel, VC). Auf diesen Kanälen werden die Daten in 53 Byte langen Zellen übertragen. Beim Verbindungsaufbau eines VC wird für jeden Abschnitt zwischen zwei ATM-Geräten ein nur lokal eindeutiger VCI (Virtual Channel Identifier) festgelegt. In einem Switch werden für jeden VC zwei VCIs , der eine VCI für den eingehenden, der andere für den ausgehenden Verbindungsabschnitt in einer Tabelle gespeichert. Der VCI wird im 5-Byte-Kopf jeder Zelle einer Verbindung vermerkt. An diesem VCI erkennt der Switch die zu der Zelle passende Verbindung und wechselt den VCI im Kopf der Zelle gemäß der Tabelle aus, bevor die Zelle weitergeleitet wird. Zwischen Vermittlungsknoten (Switches) können mehrere Kanäle, die zum gleichen Ziel führen, in virtulle Pfade (Virtual Path, VP) zusammengefaßt werden. Die VPs bekommen wie die VCs einen Bezeichner (VPI, Virtual Path Identifier) zugewiesen. Ein VC-Switch muß sowohl den VCI als auch den VPI einer Zelle auswerten und vor dem Weiterleiten ändern.

PNNI (Private Network to Network Interface oder Private Network Node Interface) ist ein *Routing-Protokoll* für private ATM-Switches oder Gruppen davon; öffentliche Netze können es auch benutzen. Der erste Teil dieses Beitrages über *PNNI* basiert auf den Kapiteln 3 und 4 aus [For96]. Zwei wesentliche Aufgaben erfüllt PNNI. Zum

einen ermöglicht es den Switches, die *Topologie des Netzes kennenzulernen.* Besonders zur Zusicherung von Verbindungseigenschaften (Quality of Service, QoS) ist eine genaue Kenntnis des Netzes und den Eigenschaften der Links (z. B. der verfügbaren Bandbreite) wichtig. Zum anderen kann man mit PNNI die eigentlichen *Verbindungen aufbauen.* Dazu erweitert PNNI eine Teilmenge von *UNI 4.0 (User to Network Interface)*, das auch zur Signalisierung zwischen Endgeräten und dem ATM-Netz dient.

1.1 Die Topologie

Die Switches eines ATM-Netzes erhalten durch PNNI die zum Aufbau von Verbindungen nötige Information über die Struktur des Netzes weitgehend automatisch. Sie tauschen laufend Managementinformationen mit ihren Nachbarn aus. So hat jeder Switch eine aktuelle Sicht des Netzes. PNNI faßt Switches in Gruppen zusammen und kann daraus eine Routing-Hierarchie bilden. Damit lassen sich auch sehr große Netze sinnvoll konfigurieren.

1.2 Eine Peer Group (PG)

Eine Peer Group ist die kleinste logische Zusammenfassung von Switches oder Gruppen davon. Auf der hier betrachteten Ebene besteht eine Peer Group aus *Knoten (Switches)* und dazwischenliegenden *Physical Links.* Man beachte, daß in Abbildung 1 keine Endsysteme vorkommen, da PNNI ein Protokoll für die Vermittlungssysteme ist.

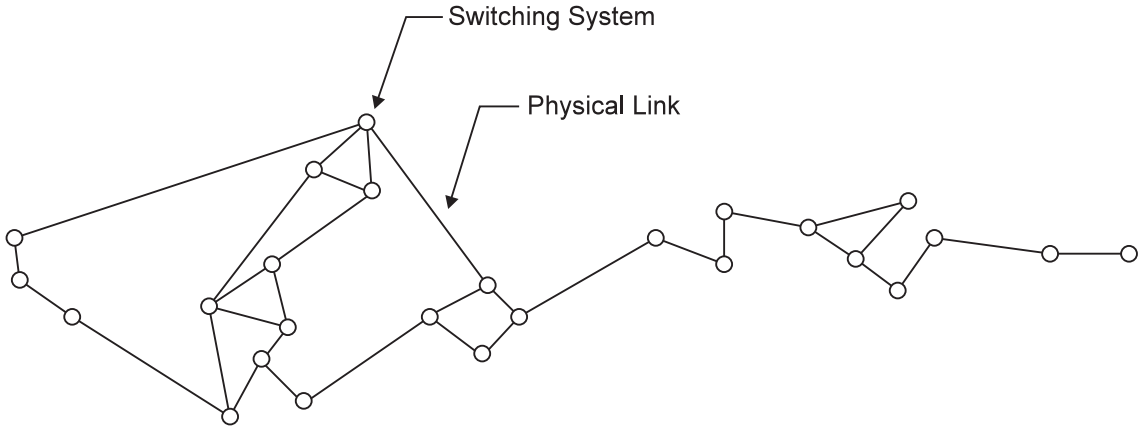


Abbildung 1: ATM-Netz aus Switches und Links

Jeder Physical Link wird durch zwei Parametersätze beschrieben; für jede Übertragungsrichtung einen. Innerhalb einer PG erreicht PNNI, daß alle Knoten die gleiche Sicht des Netzes haben. Da PNNI das Konzept der Hierarchie unterstützt, sind die Knoten und Links auf höherer Ebene nicht mehr physikalisch, sondern nur noch logisch vorhanden. Ein *Logical Node* kann ein Switch oder auf höherer Ebene eine ganze Gruppe davon sein. *Logical Links* können *Physical Links* oder *VPs* sein. Jede PG hat einen *Peer Group Leader (PGL).* Falls es mehrere PGs gibt, heißen die Knoten, die einen Link zu einer anderen PG haben, *Border Nodes.*

Abbildung 2 zeigt die unterste PNNI-Hierarchieebene. Die Knoten sind in *Peer Groups* eingeteilt. Die PGs werden mit dem Präfix der Adressen der dazugehörenden Knoten bezeichnet. So bilden z. B. die Knoten A.1.1, A.1.2 und A.1.3 die PG(A.1).

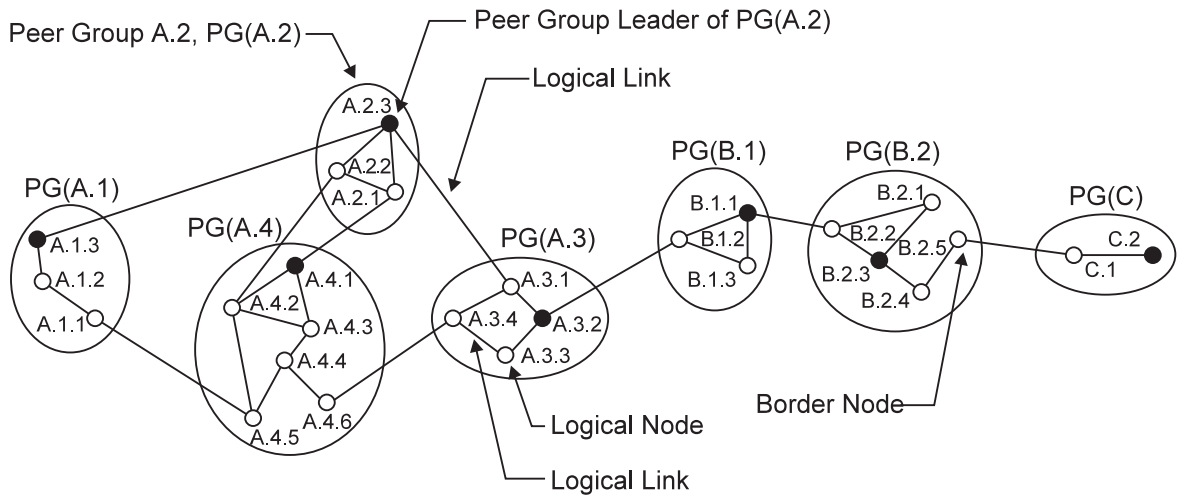


Abbildung 2: Die unterste Ebene der PNNI-Hierarchie

1.3 Peer Group Leader (PGL)

Zur Repräsentation einer PG auf der nächsthöheren Ebene der Hierarchie wird in jeder PG ein PGL gewählt. Jeder Knoten hat eine *Leadership Priority*. Sie wird wie die Topologieinformation ausgetauscht. Der Knoten mit dem höchsten Wert gewinnt und wird PGL. Bei Gleichstand gibt die Node-ID den Ausschlag. Der gewählte PGL erhöht seinen Wert, damit das Verfahren stabil bleibt. Der Wahlvorgang wird laufend wiederholt, so daß ein neuer Knoten mit höchster *Leadership Priority* automatisch PGL wird. In den Abbildungen sind die PGLs mit schwarz ausgefüllten Kreisen gekennzeichnet.

1.4 Das Hello-Protokoll

Alle Knoten senden periodisch *Hello-Pakete* an ihre Nachbarknoten aus. Sie enthalten die ATM-Adresse, die ID des Knoten selbst, die Port-ID des Links zum Nachbarknoten und die ID der PG. Damit können Knoten feststellen, wer ihre direkten Nachbarn sind. Anhand der PG-ID erkennen sie auch gleich, ob sie derselben PG angehören. Links in derselben PG heißen *Horizontal Links*, Links zwischen verschiedenen PGs *Outside Links*. Das Hello-Protokoll läuft dauernd. Es ermöglicht damit eine dynamische Konfiguration, wenn neue Knoten oder Links dazukommen. Falls andere Mechanismen versagen, kann es auch Fehler (z. B. den Ausfall eines Physical Links) feststellen.

1.5 PNNI Topology State Element (PTSE)

Mit dem *Hello-Protokoll* erhält ein Knoten nur die Informationen über direkte Nachbarn und die Links dorthin. Diese Informationen müssen nun innerhalb der gleichen PG vollständig verbreitet werden. Dazu wird die Topologie-Information in sogenannte *PTSEs* gepackt, die dann innerhalb der PG *zuverlässig geflutet* werden. Die Knoten sammeln alle erhaltenen PTSEs und tragen die Information in ihre *Topologie-Datenbank* ein, wenn sie aktueller als die bisherige ist. Dadurch erhalten sie die vollständige Information über alle Knoten und Links ihrer PG. Der Inhalt der *Topologie-Datenbanken* ist also bis auf kurze Verzögerungen und Fehler in allen Knoten einer PG gleich. Für

die Übertragung werden die PTSEs in *PNNI Topology State Packets (PTSP)* verpackt. Der Empfang der Pakete wird bestätigt. PTSEs werden sowohl zyklisch als auch ereignisgesteuert verschickt. Wenn sich eine signifikante Änderung im Netz, z. B. der verfügbaren Bandbreite, ergibt, sollte sie verbreitet werden. Es dürfen aber auch nicht zu viele PTSEs erzeugt werden, die das Netz nur sinnlos belasten. Bei der Initialisierung eines Knotens werden zuerst nur die Kopfinformationen (Header) der PTSEs verschickt und nur die benötigten PTSEs nach Aufforderung zugesandt.

Ein PTSE enthält *Zustandsparameter der Topologie*, welche die Eigenschaften von Links beschreiben. Manche davon sind *Attribute*, andere *Metriken*. *Attribute* werden bei Routingentscheidungen immer einzeln betrachtet. Ein Attribut über die Sicherheit eines Links oder eines Knotens kann z. B. dazu führen, daß eine wichtige Verbindung nicht über einen solchen Knoten führen darf. *Metriken* werden dagegen entlang der Strecke eines Ende-zu-Ende-Pfades aufaddiert; z. B. müssen Verzögerungszeiten summiert werden. Viele Parameter ändern sich ständig. Die noch verfügbare Bandbreite schwankt bei jeder neu aufgebauten Verbindung. Andere Parameter, die z. B. durch manuelle Konfiguration festgelegt werden, bleiben längere Zeit konstant. Die Parameter werden jedoch gleich häufig ausgetauscht. Die zweite wichtige Information eines PTSEs neben den Zustandsparametern der Topologie ist die *Erreichbarkeits-Information*. Sie beschreibt, zu welchen Adressen Zellen weitergeleitet werden können.

2 Die Routing-Hierarchie

In großen Netzen steigen der Overhead, der durch den Austausch der Topologie-Information ensteht, und die Zeit, bis die Topologie-Datenbanken wieder synchronisiert sind, an.

Dann ist es sinnvoll, mehrere PGs zu bilden und sie über eine *Routing-Hierarchie* zu verbinden. Eine PG wird auf der nächsthöheren Ebene durch ihren PGL vertreten. Er heißt auf der höheren Ebene *Logical Group Node (LGN)*. Die Funktionen des LGNs führt ein PGL auf unterster Ebene aus.

Die *Logical Group Nodes* werden auf der höheren Ebene wieder in PGs zusammengefaßt. Zwischen ihnen läuft das gleiche Protokoll mit Hello-Paketen und PTSEs wie auf der unteren Ebene ab. Die Adressen verkürzen sich entsprechend der Hierarchieebene. In Abbildung 3 werden z. B. die Knoten der PG(B.1) auf der nächsthöheren Ebene durch ihren LGN B.1 vertreten. Die Aufgaben dieses LGN übernimmt der PGL B.1.1. Alle LGNs, deren Bezeichnungen mit B beginnen, werden wiederum in einer PG organisiert. Sie heißt entsprechend PG(B).

2.1 Uplinks

Wenn mit dem *Hello-Protokoll* festgestellt wird, daß zwei benachbarte Knoten in unterschiedlichen PGs liegen, tauschen diese Knoten keine PTSEs aus. Stattdessen erweitern die *Border Nodes* das *Hello-Protokoll*, um den Bezeichner des Logical Group Nodes und seiner PG zu erhalten, der den Nachbarknoten auf einer höheren Hierarchieebene repräsentiert. Damit erfahren die Knoten, eventuell durch rekursives Aufrufen durch mehrere Hierarchiestufen hindurch, ihre unterste gemeinsame PG, in der sie vertreten

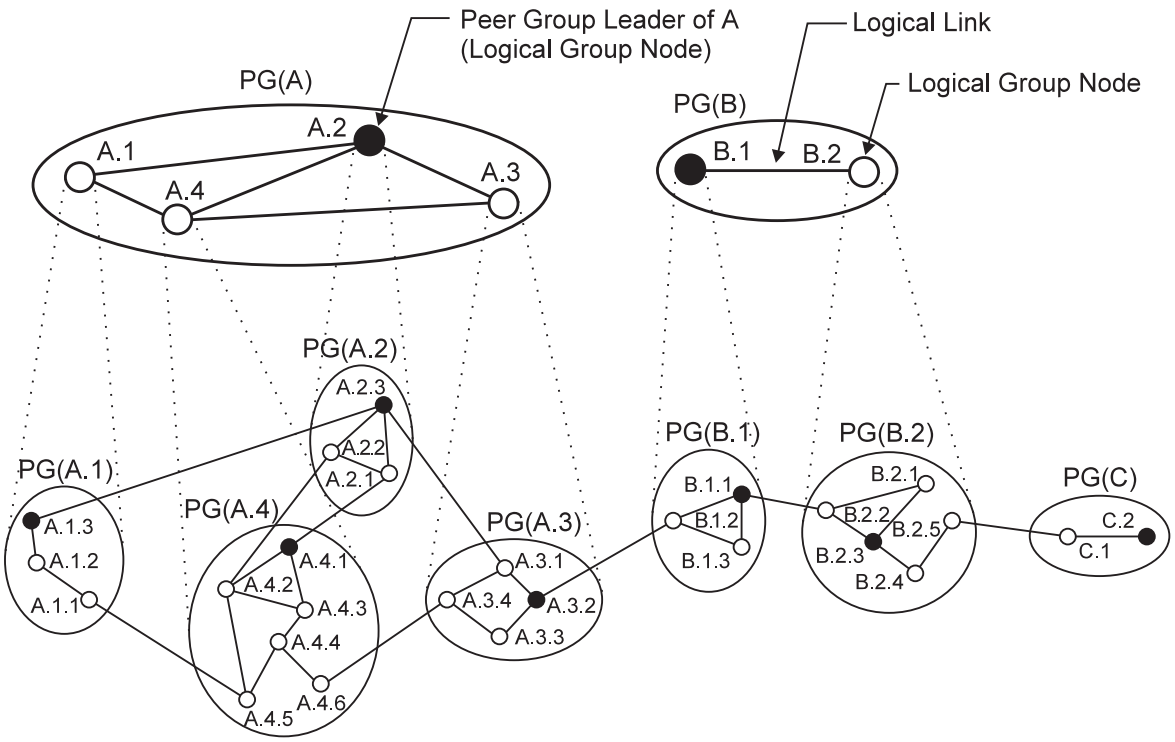


Abbildung 3: Die zwei untersten Ebenen der PNNI-Hierarchie

sind. *Uplinks* sind Links zu dem LGN, der den direkten Nachbarn auf höherer Ebene darstellt.

In Abbildung 4 repräsentiert der *Uplink* (A.3.4–A.4) die Verbindung vom Knoten A.3.4 zur PG(A.4), die den *Physical Link* von A.3.4 zu A.4.6 darstellt.

2.2 Die vollständige Routing-Hierarchie

Es werden so viele *Routing-Hierarchieebenen* gebildet, bis alle Knoten in einer einzigen obersten PG durch ihre LGNs vertreten sind. In der obersten PG wird kein PGL bestimmt, da kein weiterer Stellvertreter zur Repräsentation der PG auf höheren Ebenen benötigt wird.

Eine ATM-Adresse ist 20 Byte lang. Eine PG wird mit einem maximal 13 Oktett langen *Adreßpräfix* bezeichnet. Damit kann man $13 \cdot 8 = 104$ Hierarchiestufen bilden. Bei jedem Aufsteigen in der Hierarchie wird das *Adreßpräfix* kürzer.

In Abbildung 5 wird die komplette *Routing-Hierarchie* des Beispielnetzwerkes gezeigt. Der Knoten A.4.5 in der PG(A.4) wird auf der nächsthöheren Ebene durch den LGN A.4 repräsentiert. Auf der obersten Ebene wird er vom LGN A vertreten. Die Ebenen der *Routing-Hierarchie* müssen nicht gleichartig aufgebaut sein. So stellt der LGN C direkt die zwei unteren Knoten C.1 und C.2 dar, während zwischen den Knoten A und A.1.1 die PG(A) liegt.

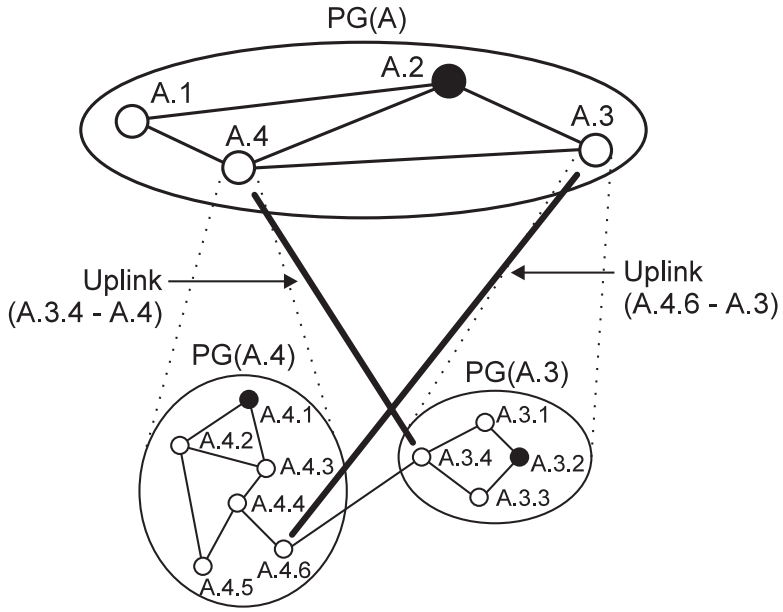


Abbildung 4: Uplinks

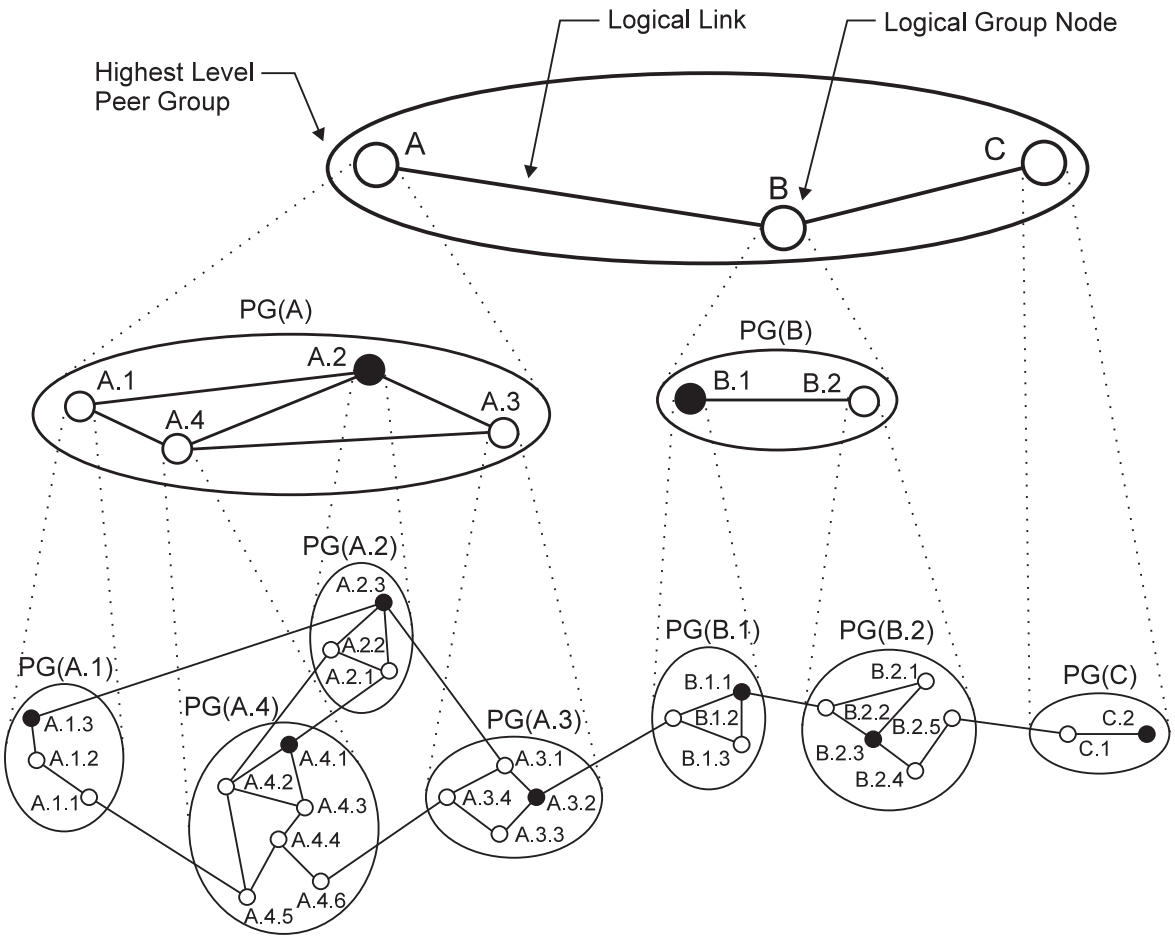


Abbildung 5: Die vollstndige Routing-Hierarchie

2.3 Informationsaustausch über mehrere Ebenen

Um einen echten Vorteil aus der Struktur der Hierarchie zu gewinnen, darf nicht die gesamte Information der unteren Ebene weitergegeben werden. Die Information muß zusammengefaßt und der Informationsumfang dadurch beschränkt werden. Innerhalb einer PG werden alle PTSEs geflutet, damit erhalten alle Knoten einer PG die gleiche Information. Beim Weiterleiten an eine höhere Ebene wird die Information dagegen zusammengefaßt. Dazu erzeugt der LGN, der als PGL die genaue Topologie der unteren Ebene kennt, neue PTSEs, die nur eine summarische Beschreibung der darunterliegenden PG enthalten. In umgekehrter Richtung, also zu den unteren Ebenen, werden alle PTSEs direkt weitergegeben. PTSE fließen in horizontaler Richtung und nach unten, nie aber nach oben.

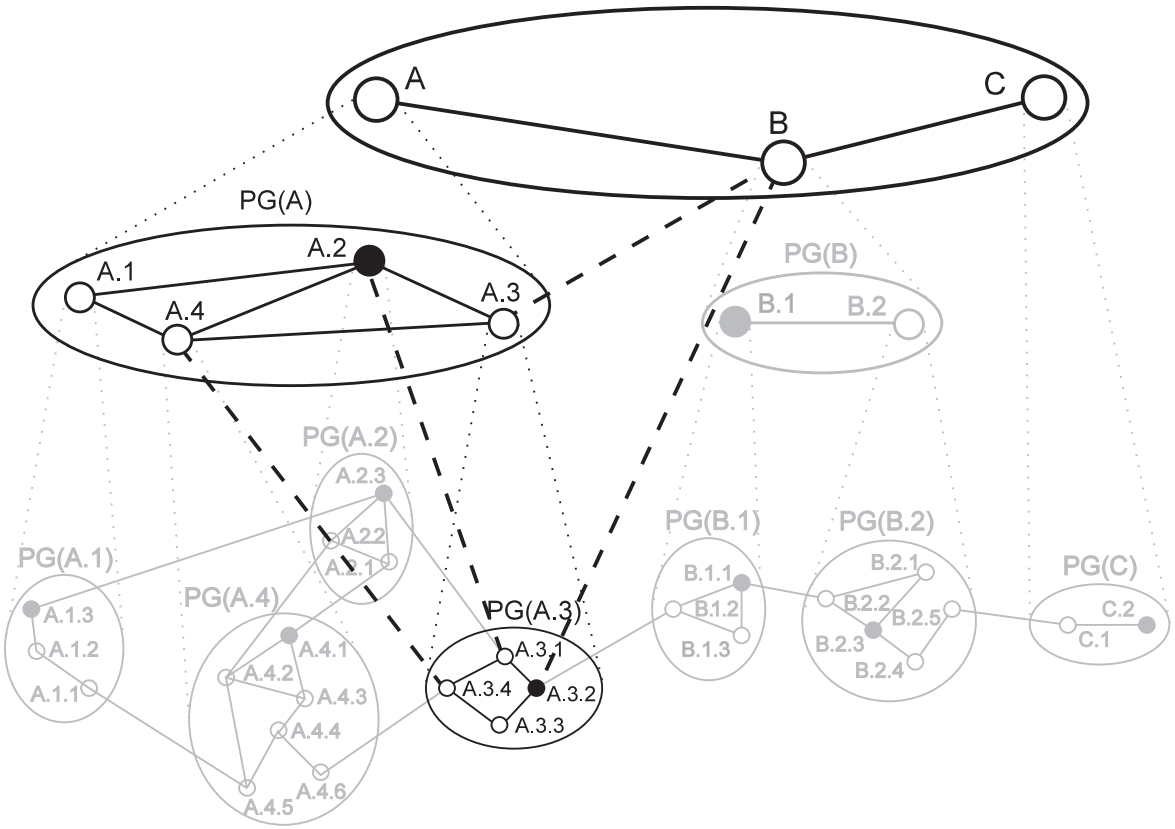


Abbildung 6: Die Sicht des Netzes von Knoten A.3.3 aus

Der Knoten A.3.3 in Abbildung 6 die genaue Topologie seiner PG. Von den PGs A1, A2 und A3 kennt er nur die zusammengefaßte Information. Die gestrichelten Links, z. B. von A.3.1 zu A.2 sind Uplinks, die der entsprechende Knoten A.3.1 in seiner PG mit PTSEs verbreitet hat. Von den über ihm liegenden PGs, hier PG(A) und der obersten PG erhält Knoten A.3.3 alle PTSEs. Aber z. B. von der PG(A.1) erreichen ihn über die PG(A) nur die zusammengefaßten Informationen. In Abbildung 6 hat der Knoten A.3.3 von den schwarz gezeichneten PGs alle PTSEs direkt erhalten, von den grau gezeichneten PGs nur indirekt PTSEs, die ein Knoten auf gemeinsamer höherer Ebene mit zusammengefaßter Information erzeugt hat.

2.4 PNNI Routing Control Channel

Auf der untersten Ebene benutzen die physikalischen Knoten reservierte VCCs (Virtual Channel Connection) zum Austausch ihrer Routing-Information. Zwischen Logical Group Nodes auf höherer Ebene gibt es diese Verbindungen nicht. Sie müssen deshalb erst einen SVCC (Switched VCC) aufbauen. Über diese Verbindung werden dann die gleichen PTSEs geschickt wie auf der unteren Ebene.

2.5 Zusammenfassen der Topologie-Information

Ein LGN muß die Information der PG, die er repräsentiert, für die Darstellung der PG auf höherer Ebene zusammenfassen. Dazu stellt er die PG in einer sternförmigen Struktur wie in Abbildung 7 dar.

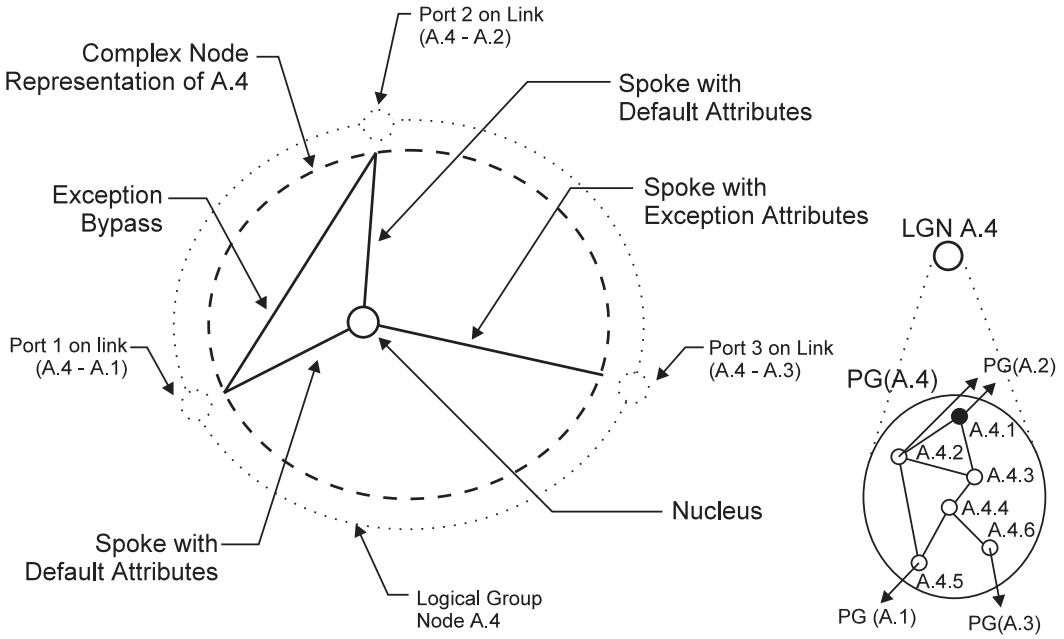


Abbildung 7: Zusammenfassen der Topologie von LGN A.4

Alle Knoten und die Links zwischen ihnen werden durch den *Kern (Nucleus)* repräsentiert. Links zu anderen PGs werden auf eine radiale Linie *(Speiche, spoke)* abgebildet. Diese Links werden mit *Standard-Attributen (Default Attributes)* oder, falls sie Besonderheiten wie z. B. eine hohe Verzögerung haben, mit *Ausnahme-Attributen (Exception Attributes)* gekennzeichnet. Einen *Exception Bypass* wie in Abbildung 7 kann man dazu benutzen, eine besonders schnelle Verbindung zwischen den Knoten A.4.2 und A.4.5 darzustellen. Eine Verbindung durch eine solche Repräsentation einer PG kann aus maximal zwei Teilverbindungen bestehen.

2.6 Zusammenfassen von Adressen

Wie die Topologie müssen auch die erreichbaren Adressen zusammengefaßt werden. Wenn mehrere Adressen oder *Adreßpräfixe* gleich beginnen, könnnen sie mit dem gemeinsamen kürzeren *Adreßpräfix* beschrieben werden.

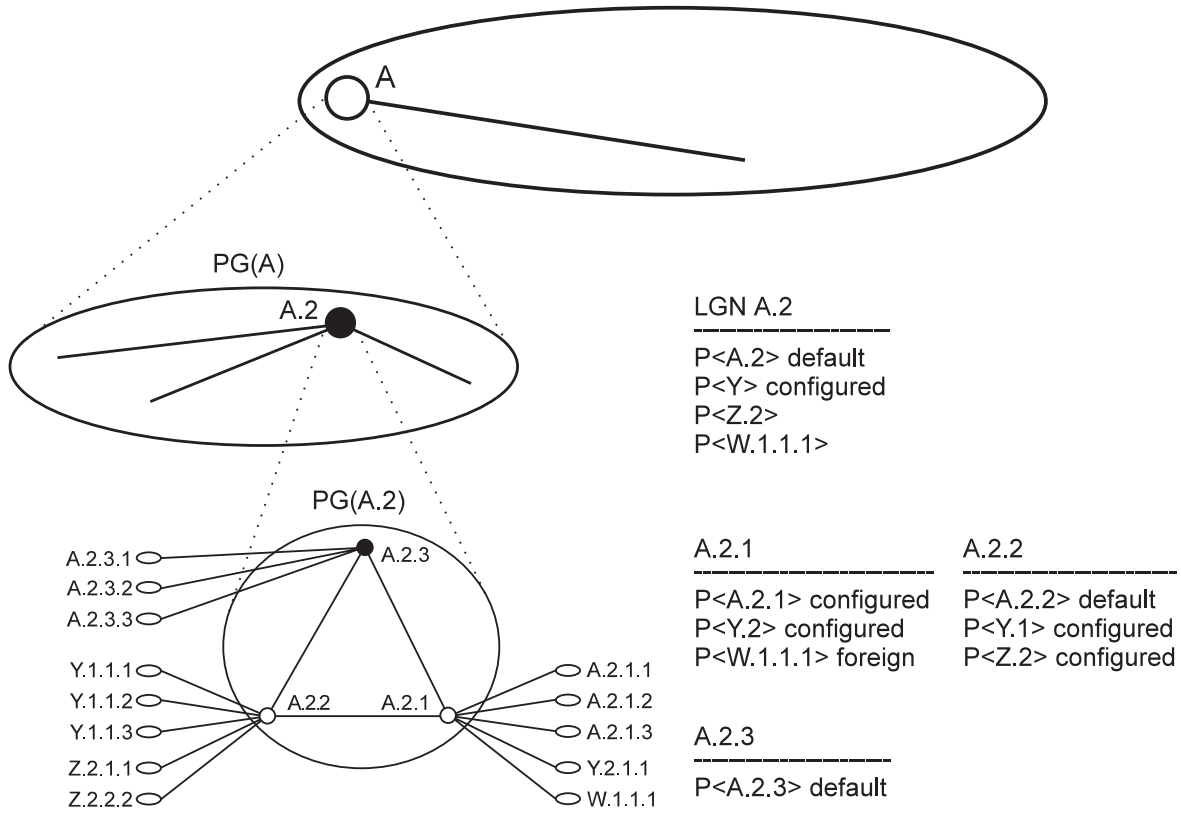


Abbildung 8: Zusammenfassen von Adressen

Endsystemadressen, die so beginnen wie die Adresse des Switches, an den sie angeschlossen sind, können also zu einem einzigen *Adreßpräfix* zusammengefaßt werden. So sind in Abbildung 8 alle an Switch A.2.3 angeschlossenen Endgeräte mit dem *Adreßpräfix* P<A.2.3> erfaßt. Am Knoten A.2.2 sind zusätzlich die *Adreßpräfixe* P<Y.1> und P<Z.2> konfiguriert, mit denen die Endgeräte Y.1.1.1, Y.1.1.2, Y.1.1.3, Z.2.1.1 und Z.2.2.2 erfaßt werden können. Wenn Endgeräte an einen Switch angeschlossen sind, deren *Adreßpräfixe* weder in den *Standardadressen (default)* noch in den manuell *konfigurierten (configured)* enthalten sind, werden sie wie im Knoten A.2.1 das Gerät W.1.1.1 automatisch als *fremd (foreign)* eingetragen. Auf der nächsthöheren Ebene werden die *Adreßpräfixe* wiederum zusammengefaßt.

3 Signalisierung

Die *ATM-Signalisierung* dient der Suche nach einem passenden Weg für eine Verbindung und dem anschließenden Aufbau derselben. Die Signalisierung bei PNNI basiert auf *UNI 4.0*, das auch von den Endsystemen zur Signalisierung benutzt wird. Allerdings ist einerseits nicht alles davon implementiert, auf der anderen Seite gibt es auch Erweiterungen.

3.1 Auswahl eines Pfades

ATM ist *verbindungsorientiert*. Dienstqualität und Bandbreite einer Verbindung sollen garantiert werden. Deshalb muß bei der Wegewahl besonders sorgfältig vorgegangen

werden. Die Informationen über das Netz, die in der Topologie-Datenbank vorliegen, ermöglichen es, eine Verbindung mit den gewünschten Eigenschaften zu finden. Bei PNNI wird für die Verbindungsaufbauphase *Source-Routing* verwendet. Der Initiator einer Verbindung wählt also gemäß seiner Sicht auf das Netz den gesamten Weg. Wenn der Initiator einer Verbindung einen Weg gefunden hat, wird der Weg in eine *Designated Transit List (DTL)* verpackt. Sie enthält die Folge aller Node-IDs und eventuell auch die Port-IDs, durch die die Verbindung führen soll.

Wenn es eine Hierarchie gibt, kennt der Initiator nur seine PG vollständig. Er kann deshalb keine komplette Beschreibung der Verbindung durch alle Knoten aufstellen und erzeugt stattdessen für jede Hierarchieebene eine eigene DTL und organisiert die DTLs in einem Stapel. Die DTLs für höhere Hierarchieebenen enthalten zunächst nur die LGNs, welche die zu durchquerenden PGs repräsentieren. Der erste Knoten einer PG entlang einer Verbindung übernimmt dann das Routing durch seine PG und ersetzt in einer DTL die LGNs mit Knoten einer tieferen Hierarchieebene.

3.2 Crankback

Wenn die Datenbasis, anhand derer eine DTL erzeugt wurde, nicht aktuell war, kann es sein, daß ein Knoten auf dem Weg eine Verbindung mit den gewünschten Eigenschaften nicht aufbauen kann. Er sendet dann eine *Crankback-Nachricht* zum Erzeuger der aktuellen DTL zurück. Dieser kann innerhalb seiner PG einen anderen Weg suchen oder auch eine *Crankback-Nachricht* zum Erzeuger der vorhergehenden DTL schicken. Falls der Initiator der ganzen Verbindung ein *Crankback* bekommt, ist der ganze Verbindungsaufbau gescheitert und er kann versuchen, eine andere Verbindung aufzubauen.

4 Routing in „Multiprotokoll über ATM“-Netzwerken

Die Installation von ATM-Netzen erfolgt meistens nur schrittweise und ersetzt nur Teilstücke eines schon bestehenden Netzwerkes. Man setzt ATM z. B. nur im Backbone-Bereich ein, behält aber die bestehende Vernetzung der Arbeitsplatzrechner, beispielsweise mit Ethernet, bei. Dann muß man das ATM-Netz in diese heterogene Umgebung integrieren. Dabei gibt es viele Probleme, aber auch bereits Lösungen. Das verbindungsorientierte Konzept von ATM widerspricht dem traditioneller Kommunikationsnetze, die auf Vermittlungsschichtebene meist verbindungslos arbeiten. Deshalb unterscheiden sich die Protokolle für diese Ebene deutlich. Es ist nicht effizient möglich, für jedes Paket einen VC aufzubauen, es in Zellen zu zerlegen, über das ATM-Netz zu transportieren und die Verbindung dann wieder abzubauen. Deshalb müssen genügend Verbindungen bereitgestellt werden, die bei Bedarf ohne neuen Verbindungsaufbau genutzt werden können. Die ATM-Adressen sind hierarchisch strukturiert, wohingegen die ebenfalls hierarchischen IP-Adressen in flach organisierte MAC-Adressen umgewandelt werden. Viele Möglichkeiten wie die Unterstützung von Dienstqualitäten, die ATM bietet, kennen traditionelle Kommunikationsnetze gar nicht.

4.1 Beispielkonfiguration

In Abbildung 9 ist ein einfaches Netz aus drei ATM-Switches (A, B und C) und zehn traditionellen Routern (R1 bis R10) dargestellt. Die Router können z. B. IP-Router sein. Sie müssen über aufgebaute und mögliche Verbindungen durch das ATM genügend wissen, um über die ATM Switches routen zu können. Im einfachsten Fall benutzt man einzelne Verbindungen des ATM-Netzes als Standleitungen, die als *Permanent Virtual Channels* fest aufgebaut sind. Damit nutzt man allerdings keine Fähigkeit von ATM aus. Weder konfiguriert sich das ATM-Netz automatisch, noch passen sich die Verbindungen an die Last an, indem neue SVCs aufgebaut werden. Im Folgenden werden drei unterschiedliche Möglichkeiten dargestellt, wie das Beispielnetz besser genutzt werden kann. Sie werden wie in [Jef96] beschrieben vorgestellt.

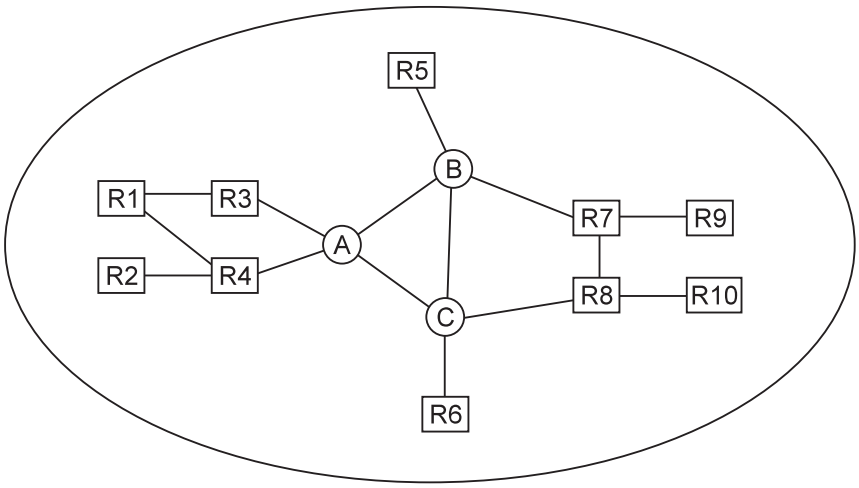


Abbildung 9: Netzwerk aus ATM-Switches und traditionellen Routern

Bisher werden meist zwei Konzepte zur Kopplung von ATM-Netzen und traditionellen LANs genutzt. Bei *LAN-Emulation* wird über die ATM-Adaptions-Schicht (AAL) von ATM, die schon unterschiedliche Transportdienste und Konvergenzfunktionen unterstützt, das LAN-Emulationsmodul gelegt. Es gestattet, das ATM-Netz als einfache MAC-Schicht (Medium-Access-Layer) zu benutzen. Damit kann man die darüberliegende LLC-Schicht (Logical Link Control) und alle höheren Schichten (auf Schicht 3 z. B. IP) beibehalten. Ein *LAN-Emulations-Server* übernimmt die Konfigurationsverwaltung des Netzes, die Auflösung der MAC-Adressen in ATM-Adressen und die Bereitstellung von Multicastverbindungen.

Bei *IP über ATM* wird IP mit Hilfe der Konvergenzschicht auf das AAL von ATM aufgesetzt. ATM übernimmt die Aufgaben der Sicherungsschicht. Es wird ein *Logisches IP-Subnetz (LIS)* über das ATM-Netz aufgebaut. Kurze Verbindungen werden über diese Defaultwege des *LIS* geleitet. Mit dem *NHRP (Next Hop Resolution Protocol)* können für größere Übertragungen zusätzliche ATM-Verbindungen aufgebaut werden. Dazu benutzt NHRP zur Adreßauflösung von IP- in ATM-Adressen das *ATM-Address-Resolution-Protokoll (ATMARP)*. Die Dienste dieses Protokolls werden von einem speziellen Server angeboten.

4.2 Layered Routing

Das Hauptziel von Layered Routing ist es, einige ATM-Geräte in ein bestehendes Netzwerk möglichst so zu integrieren, daß nur wenige Veränderungen an dem vorhandenen Netz und der Software notwendig sind. Deshalb werden die normalen Routing-Methoden auf das ATM-Netz erweitert. Das Routing-Protokoll des ATM-Netzes ist völlig getrennt von dem der Router. Die Router wissen gar nichts über die Struktur des ATM-Netzes. Man baut per Konfiguration bei der Initialisierung einfach PVCs im ATM-Netz auf, die dann von den Routern als hochleistungsfähige Punkt-zu-Punkt-Verbindung genutzt werden.

Es ist klar, daß dieser Ansatz nur bei relativ kleinen Anteilen von ATM am Gesamtnetz sinnvoll ist. Es müssen die VCs konfiguriert werden. Die dynamische Konfiguration wird nicht genutzt, so daß keine Geräte während des Netzbetriebes hinzukommen oder außer Betrieb gehen können. Es gibt keine Möglichkeit, die Wartung und Installation durch ein hierarchisches Konzept zu erleichtern. Die Vorteile von ATM wie Reservierung von Ressourcen und die Unterstützung von Verbindungseigenschaften werden nicht genutzt. Die Emulation des logischen Netzes und die Umwandlung der Protokolle belasten die Rechner und Geräte im Netz stark. Dafür muß man sich mit ATM kaum befassen und kann mit seinen gewohnten Protokollen arbeiten. Wenn man nur wenige ATM-Verbindungen in ein bestehendes Netz einfügt, ist diese Lösung wohl am einfachsten.

4.3 PNNI Augmented Routing

Dieses Verfahren nutzt zwei getrennte Protokolle für das ATM-Netz und das restliche Netz. Auf dem ATM-Netz und auf den Routern mit ATM-Anschluß wird PNNI genutzt. Damit erhalten diese Router Kenntnis über die Topologie des ATM-Netzes. Auf den Routern läuft außerdem ein normales Routing-Protokoll wie OSPF (Open shortest Path first) oder RIP (Routing Information Protocol).

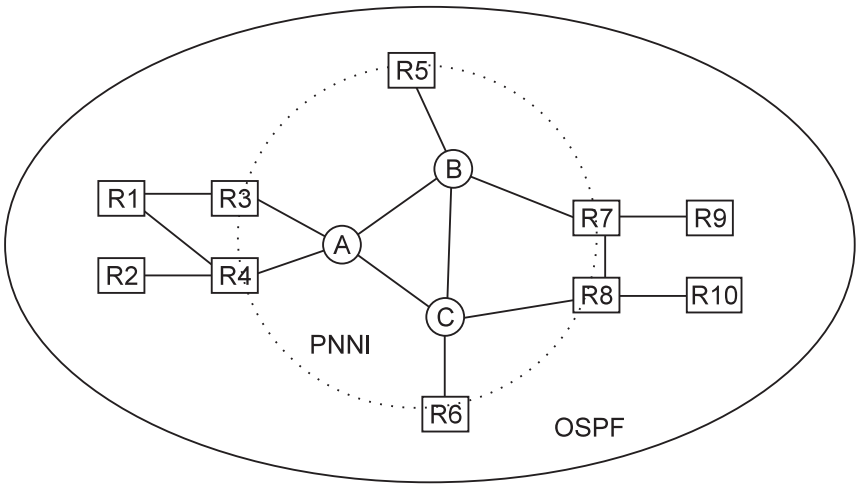


Abbildung 10: PNNI Augmented Routing

Die von PNNI erhaltenen Informationen ermöglichen es, daß bei der Netzwerk-Initialisierung automatisch genügend SVCs aufgebaut werden, so daß alle Router miteinander

Kontakt haben. Damit entfällt der manuelle Aufbau von VCs, und bei Veränderungen am ATM-Netz ist keine Neukonfiguration nötig. Die Router mit ATM-Anschluß werden in PNNI als *Transit Restricted* ATM-Switches betrachtet, d. h. SVCs können dort beginnen oder enden, nicht aber in das traditionelle Kommunikationsnetz hineinführen. Nachdem das ATM-Netz SVCs aufgebaut hat, können diese von den normalen Routing-Protokollen benutzt werden. Die Router mit ATM-Anschluß können mit Erweiterungen von PNNI, die von ATM-Switches ignoriert werden, ihre unterstützten Protokolle und ihre Router-ID weiterleiten.

PNNI Augmented Routing vereinfacht die Konfiguration eines Netzes mit größerem ATM-Anteil erheblich, da die benötigen SVCs automatisch aufgebaut werden. Die Anpassung an Veränderungen der Netzstruktur ist wesentlich leichter. Das ATM-Netz kann sich der Last anpassen, indem neue SVCs aufgebaut werden. Auf der anderen Seite muß man zwei verschiedene Routing-Protokolle benutzen, und die Router mit ATM-Anschlüssen werden deutlich aufwendiger, da sie beide Protokolle verwenden. Wenn in einem Netz der ATM-Anteil wächst, ist es jedoch sinnvoll, von *Layered Routing* auf *Augmented Routing* zu wechseln.

4.4 Integrated PNNI (I-PNNI)

Bei diesem Verfahren wird PNNI als einziges Routing-Protokoll benutzt. Es läuft sowohl im ATM-Netz als auch auf allen Routern.

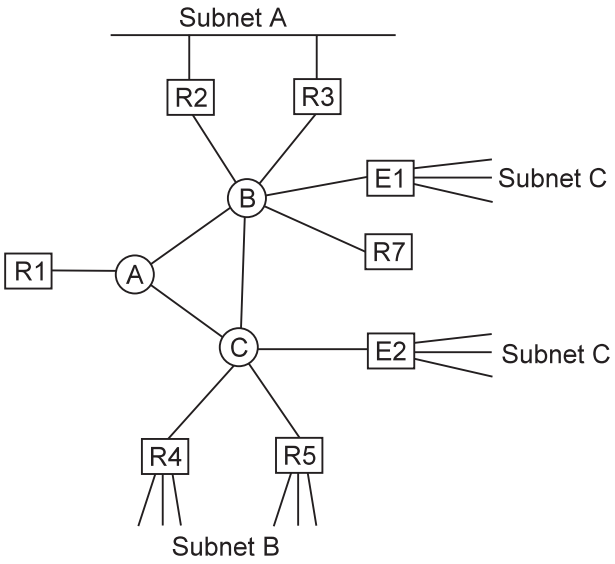


Abbildung 11: Logische Subnetze bei I-PNNI

Alle Router und Switches erscheinen in den Topologie-Datenbanken als Knoten. Sie benutzen grundsätzlich die üblichen Verfahren von PNNI. So tauschen die Knoten gemäß PNNI Hello-Pakete und PTSEs aus. Für die Beschreibung der Router und der Verbindungen des traditionellen Kommunikationsnetzes müssen geeignete Zustandsparameter (Attribute und Metriken) gefunden werden. Die Erreichbarkeit von Routern und Endgeräten kann mit einer Erweiterung von PNNI verbreitet werden. Damit lassen sich z. B. IP-Adressen und IP-Subnetzmasken weitergeben. Mit I-PNNI kann man viele Vorteile von ATM nutzen.

Die Router R1, R2 und R3 in Abbildung 11 benutzen I-PNNI, NHRP und leiten IP-Pakete normal weiter. Das Subnetz A ist über die Router R2 und R3, das Subnetz B teilweise über R4, teilweise über R5 erreichbar. Wenn ein Paket von R1 zum Subnetz A weitergeleitet werden soll, kann dies direkt geschehen, weil das ganze Subnetz direkt erreichbar ist. Wenn man aber besonders große Datenmengen von R1 zum Subnetz C schicken will, kann es sinnvoll sein, zuerst eine Anfrage zu stellen, um eine geeignete Verbindung über das ATM-Netz aufzubauen.

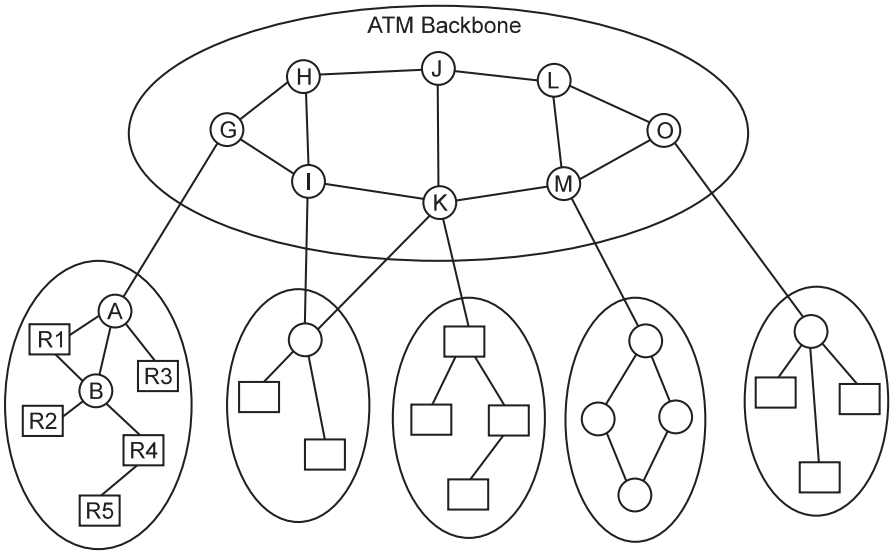


Abbildung 12: Hierarchie bei I-PNNI

Wenn das Netzwerk wie bei einer Universität oder einem Unternehmen sehr groß wird, kann man das hierarchische Konzept von PNNI wie in Abbildung 12 vollständig nutzen. Mit einigen Ebenen kann man praktisch jedes Netzwerk sinnvoll gliedern.

In Abbildung 12 bilden die Switches G bis O das ATM-Backbone. Daran sind Gruppen von ATM-Switches und Router angeschlossen. Die Router und Switche der unteren Hierarchieebene müssen so konfiguriert sein, daß ein geeigneter ATM-Switch PGL wird, der die untere PG als LGN in der höheren PG repräsentiert. Diese PG besteht dann aus den hochleistungsfähigen ATM-Switches des Backbones.

4.5 Vergleich

Die verschiedenen Konzepte zur Verbindung von traditionellen und ATM-Netzen haben alle ihre Vorteile. Wenn nur sehr wenige ATM-Switches vorhanden sind, hat *Layered Routing* nur geringen Aufwand und braucht wenige Änderungen im bestehenden Netz. *Augmented Routing* bietet Vorteile bei der Konfiguration, sobald der ATM-Anteil am Netz größer wird. Dafür wächst der Aufwand für die Verwaltung von zwei Protokollen. *I-PNNI* hat zweifellos die größten Möglichkeiten der hier beschriebenen Verfahren. Allerdings muß auch auf allen bestehenden Routern das Protokoll geändert werden. Die Implementierung von *PNNI* auf traditionellen Routern bereitet natürlich einige Schwierigkeiten.

Für die Verbreitung von ATM ist die Verknüpfung mit traditionellen Netzen existentiell wichtig. Fast niemand würde auf ATM umsteigen, wenn er sein ganzes bisheriges

Netz austauschen müßte. Die bereits bestehenden Konzepte für heterogene Netze mit ATM bieten für verschiedene Anwendungsfälle funktionierende Lösungen. Wenn man seine Anforderungen an das Netz kennt, kann man eine geeignete wählen. Die eigentlichen Vorteile von ATM, wie z. B. die Unterstützung von Dienstqualitäten, lassen sich in heterogenen Netzen prinzipiell aber nur beschränkt nutzen. Die Unterschiede zwischen traditionellen Computernetzen und ATM lassen eine so große Lücke, daß sie mit verschiedenen Lösungen überbrückt werden kann. So decken die bereits vorhandenen Verfahren die prinzipell denkbaren Lösungen ab, aber sie lassen sich noch wesentlich verbessern.

Literatur

[For96] ATM Forum. *Private Network-Network Interface Specification 1.0, PNNI 1.0, ATM Forum af-pnni-0055.0000.* ATM Forum. 1996.

[Jef96] R. W. Callon J. Hapern J. Drake H. Sandick J. Jeffords. Routing in a Multiprotocol over ATM Environment. *Connexions* Vol. 10(No. 3), March 1996, Seite 34–48.

Abbildungsverzeichnis

Der ABR-Dienst und Mechanismen zur Verkehrskontrolle in ATM-Netzwerken

Jochen Ernst

Kurzfassung

Im Hinblick auf die Dienstintegration stellen ATM-basierte Netzwerke unterschiedliche Kommunikationsdienste zur Übertragung von Sprache, Video und klassischen Daten zur Verfügung. Beim Verbindungsaufbau wird die Dienstqualität über mehrere Qualitätsparameter wie Durchsatz und Verzögerung ausgehandelt und in einem Dienstvertrag festgelegt. Im Gegensatz zu Audio und Video, ist bei Datenübertragungen das Verkehrsaufkommen nicht direkt spezifizierbar, wobei aber oftmals auch keine Garantie von Durchsatz und Verzögerung erforderlich ist. Vor diesem Hintergrund wurde der ABR-Dienst (Available Bit Rate) definiert, der speziell den beschriebenen Datenanwendungen die verfügbare Bandbreite anbietet. Mechanismen zur Verkehrkontrolle dienen dabei zum Austausch der für den ABR-Dienst benötigten Informationen.

1 Einleitung

Die rasche Weiterentwicklung im Bereich der Telekommunikations-Netzwerke bringt immer schnellere aber auch komplexere Übertragungsmöglichkeiten hervor. Im Bereich der Breitband-Netzwerke ist eines davon das Breitbandübermittlungsverfahren (B-ISDN) mit ATM (Asynchronous Transfer Mode) als Übermittlungsverfahren. ATM selbst stellt eine Fülle von verschiedenen Diensten zur Verfügung. Unter anderem auch den ABR-Dienst. In diesem Beitrag sollen zunächst die Charakteristiken des ABR-Dienstes im Vergleich mit weiteren ATM-Diensten beschrieben werden. Anschließend werden die unterschiedlichen Verfahren zur Verkehrskontrolle und insbesondere die Unterschiede zwischen fenster- und raten-basierten Verfahren dargestellt.

2 ATM-Netzwerke

2.1 Grundprinzipien vom ATM

ATM wird als ein spezieller, paketorientierter Übertragungsmodus angesehen, der auf asynchronem Zeitmultiplex und dem Einsatz von Zellen, das sind Pakete fester Länge, beruht. Jede Zelle besteht aus einem Datenfeld und einem Datenkopf. Der Kopf wird vor allem zur Identifikation von Zellen benutzt, die zur Verbindung, einem sogenannten

virtuellen Kanal, gehören und für die Durchführung der entsprechenden Wegefestlegung dienen. Die Integrität wird über einen virtuellen Kanal bewahrt. Das Datenfeld von ATM-Zellen bleibt beim Transport durch das Netzwerk transparent. Alle Dienste (Ton, Bild, Daten usw.) können mittels ATM befördert werden, einschließlich der verbindungslosen Dienste. Abbildung 1 gibt einen Überblick der Anforderungen an die Leistungsfähigkeit von Netzwerken. Die Bitraten der verschiedenen Dienste reichen von wenigen Bits/s bis hin zu mehreren Mbits/s. Auch die Zeitdauer der Übertragung erstreckt sich von einigen Sekunden bis Stunden. Alle diese Dienste müssen über das zukünftige Breitbandnetz übertragen werden [DeP96].

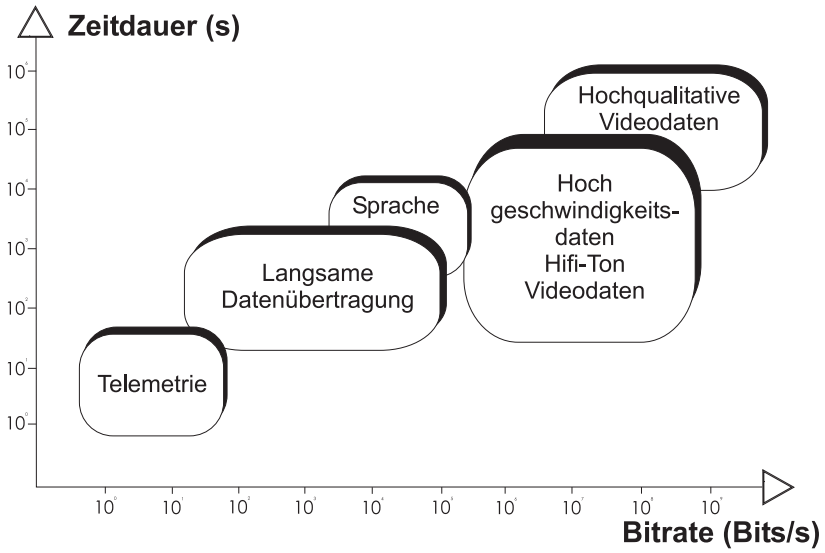


Abbildung 1: Erwarteter Dienstumfang in Breitbandnetzen

Um verschiedene Dienste unterbringen zu können, wurden je nach Art des Dienstes mehrere Arten von ATM-Anpassungsschichten (ATM-Adaptions Layer, AAL) festgelegt, um die Daten auf die ATM-Zellen abzustimmen und diensttypische Funktionen (z.B. Taktauffrischung, Ausgleich von Zellverlusten usw.) zur Verfügung zu stellen. Die AAL-eigene Information ist im Datenfeld der ATM-Zelle enthalten [DeP96]. Die Asynchronität von ATM bezieht sich auf das Multiplexen von Daten auf das Medium. Daher ist die Übertragung in periodischen Übertragungsrahmen, in die die Zellen asynchron gemultiplext werden, möglich. ATM-Zellen werden auf der Leitung kontinuierlich gesendet. Stehen keine Zellen zur Verfügung, werden Leerzellen gesendet.

2.1.1 Aufbau von ATM-Zellen

ATM-Zellen bestehen aus 48 Byte Nutzdaten und 5 Byte Kontrollinformationen. Sie werden in sogenannten virtuellen Kanälen auf virtuellen Pfaden transportiert. Obwohl das Verhältnis von Kontrollinformation zu Nutzdaten relativ hoch ist (etwa 9 Prozent), müssen die Netzknoten verhältnismäßig wenig Daten für die Adressierung und Wegewahl berechnen [Har96].

Auf die einzelnen Parameter wird im folgenden noch eingegangen. Der Parameter GFC (Generic Flow Control, allgemeine Flußsteuerung) wird zur Flußsteuerung benötigt. Dazu können im Datenkopf einige zusätzliche Bits erforderlich sein. Die Anzahl

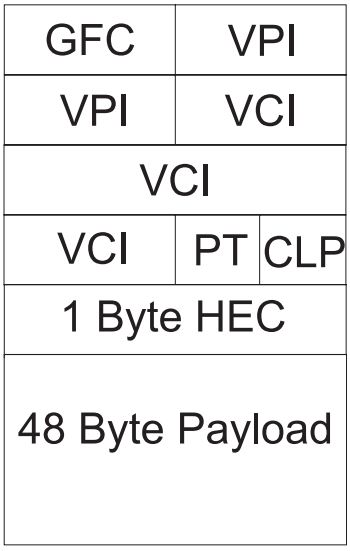


Abbildung 2: Aufbau von ATM-Zellen

der zur Ausführung dieser Funktion benötigten Bits liegt je nach verwendeter Medienzugriffssteuerung (MAC, Medium Access Control) zwischen null und acht Bits [DeP96]. Die Parameter VCI (Virtual Channel Identifier,virtuelle Kanalkennung) und VPI (Virtual Path Identifier, virtuelle Pfadkennung) dienen zur Vermittlung der Zellen. Um das gesamte Netzwerk zu warten und den Durchsatz der ATM-Verbindungen zu überwachen, wurde der PT-Parameter (Payload Type Identifier, Nutzlastarterkennung) entwickelt. Er ermöglicht auf jeder virtuellen Verbindung das Einfügen spezieller Zellen, die wie normale Zellen weitergeleitet werden, aber besondere Wartungsdaten enthalten.Über das Cell-Loss-Priority-Feld (CLP, Zellverlustpriorität) kann der Zelle eine Priorität gegeben werden. Der Parameter HEC (Header Error Check) enthält eine Prüfsumme über den Zellkopf. Dieses Zellcodierverfahren nutzt die Wechselbeziehung zwischen den zu überwachenden Datenkopfbits und den dazu von der HEC in den Datenkopf eingefügten Bits, die mittels eines zugehörigen Generatorpolynoms erzeugt wurden [DeP96].

2.1.2 Vermittlung

Zellen werden über die virtuelle Kanalkennung und die virtuelle Pfadkennung im Zellkopf ihren Verbindungen zugeordnet. Die Kanäle (Virtual Channel, VC) werden auf Pfaden (Virtual Path, VP) gebündelt und von Netzknoten (ATM-Switch) zu Netzknoten geschaltet. Eine Verbindung (Virtual Channel Connection, VCC) zwischen zwei Endsystemen setzt sich also aus einzelnen Kanälen zwischen den ATM-Switches zusammen. Dynamische, vom Netz geschaltet virtuelle Kanalverbindungen nennt man Switched Virtual Connection (SVC), permanente Kanalverbindungen nennt man Permanent Virtual Connection (PVC). Ein ATM-Switch schaltet virtuelle Kanäle über seine Ports mittels einer Switching-Matrix. Sie enthält für jeden Kanal einen Eintrag für Eingangs-Port, -Pfad, -Kanal sowie für Ausgangs-Port, -Pfad, -Kanal. Beim Schalten der Zellen zwischen den Ports ändert der Switch die Werte für die Kanal- und Pfad-Kennung jeder Zelle. Anfangs ist eine solche Matrix unidirektional, so daß für einen bidirektionalen virtuellen Kanal der entsprechende Eintrag auch für die Rückrichtung existieren muß. Dafür werden in der Regel die gleichen VPI/VCI-Kombinationen ver-

wendet. Für eine Punkt-zu-Mehrpunktverbindung existieren an der Gabelung mehrere Einträge für Ausgangs-Port, -Pfad, -Kanal [Har96].

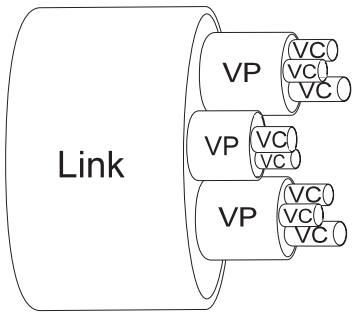


Abbildung 3: Virtuelle Kanäle und Pfade auf einem Link

2.2 Verkehrsvertrag

Beim Verbindungsaufbau entscheidet die Zugangskontrolle (Call Admission Control, CAC), ob das Netz in der Lage ist, die gewünschte Dienstqualität bereitzustellen. Wird die Verbindung aufgebaut, so schließen Endsystem und Switch einen Verkehrsvertrag ab, der die vereinbarten Dienstklassen umfaßt. Anhand dieses Verkehrsvertrages überwacht die Verkehrssteuerung die Einhaltung der Parameter. Diese Steuerung setzt sich aus der Nutzungskontrolle (Usage Parameter Control, UPC) auf der Netzseite und der Verkehrskontrolle (Traffic Shaper) im Endsystem zusammen. Die Verkehrskontrolle dient dazu, den Verkehrsvertrag von Seiten des Endsystems aus einzuhalten, er gleicht also eventuelle Spitzen (Bursts) aus. Erst bei Verletzung des Verkehrsvertrages, beispielsweise bei Überschreitung der vereinbarten Bandbreite, verwirft die Nutzungskontrolle die entsprechenden Daten. So kann garantiert werden, daß vom Netz zugesicherte Dienstqualitäten eingehalten werden.
Anstatt Zellen gleich zu verwerfen, können sie auch über das Cell-Loss-Priority-Feld im Zellkopf markiert werden. Ein ATM-Switch erkennt durch dieses Feld, ob die entsprechende Zelle übertragen werden muß oder nicht. Zellen mit der Dienstklasse UBR (Unspecified Bit Rate) (siehe Tabelle 1.) sind durch dieses Feld entsprechend markiert. ATM-Switches, die an ihre Belastungsgrenzen gelangen, können nun all die Zellen verwerfen, die das CLP-Bit gesetzt haben, ohne vereinbarte Verkehrsverträge zu verletzen.

2.3 Dienstklassen

Die Dienstqualität einer Verbindung (Quality of Service, QoS) bezieht sich auf den Zellverlust (Cell Loss) und die Verzögerung (Cell Delay) der Zellen innerhalb eines ATM-Netzwerks. Die Dienstqualität ist eng verbunden mit der verwendeten Bandbreite. Stehen nur begrenzte physikalische Ressourcen zur Verfügung, erhöht die Verwendung einer höheren Bandbreite die Zellverluste, sowie die Verzögerung (Cell Delay Variation, CDV) und die Fehlerrate (Cell Error Rate, CER) [DeP96].
Derzeit sind vier Dienstqualitätsklassen (QoS Class) entsprechend den Dienstklassen definiert [Kya95] (siehe Tabelle 1.). Der CBR-Dienst (Constant Bit Rate, CBR) liegt in der am höchsten priorisierten Klasse (QoS Class 1). Er spezifiziert einen verbindungsorientierten, isochronen Dienst mit konstantem Durchsatz für die Sprachübertragung.

Dienstklasse	A	B	C	D
Zeitverhalten	isochron	isochron	nicht isochron	nicht isochron
Bitrate	konstant	variabel	variabel	variabel
QoS	CBR	rt-VBR	nrt-VBR	UBR, ABR
QoS-Parameter	CTD, CDV CLR	CTD, CDV CLR	CLR	-
Art	verbindungs-orientiert	verbindungs-orientiert	verbindungs-orientiert	verbindungslos
Anpassungs-schicht	AAL1	AAL2	AAL3/4, AAL5	AAL3/4, AAL5
Dienste (z.B.)	Sprache, unkomp. Video	kompr. Video	Filetransfer	LAN-Protokolle
Verkehrs-parameter	PCR, CDVT	PCR, CDVT, SCR, MBS	PCR, CDVT, SCR, MBS	PCR, CDVT, MCR

Tabelle 1: Die Dienstklassen von ATM

Die Klasse 2, oder auch rt-VBR (Realtime Variable Bitrate), unterscheidet sich von Klasse 1 nur durch einen variablen Datenstrom. Dies wird zum Beispiel für Audio- und komprimierte Videoübertragungen in Multimedia-Anwendungen verwendet. Die Klasse 3 (nrt-VBR, non-realtime VBR), etwa für Frame Relay, stellt eine gesicherte Datenübertragung mit variabler Datenrate dar. In der Klasse 4 sind verbindungslose Datenübertragungsdienste wie zum Beispiel ABR, IP oder SMDS (Switched Multimegabit Data Services) zusammengefaßt. Neben diesen spezifizierten QoS-Klassen, gibt es noch die sogenannte unspezifizierte QoS-Klasse, die keinerlei Garantien beinhaltet. Der ABR-Dienst ist ein Mechanismus, bei dem nicht das Endsystem eine bestimmte Bandbreite und QoS-Klasse anfordert, sondern das Netz dem Endsystem mitteilt, wieviel Bandbreite zur Verfügung steht [Har96].

Die Fähigkeit, konstante und variable Bitraten aufrechtzuerhalten, wurden vom ATM-Forum für Verbindungen definiert, die besondere Qualitätsanforderungen an die Dienstklasse stellen, wie z.B. Zellverlustrate oder Zellenübertragungsverzögerung. Diese QoS-Garantien können durch das Netzwerk durch die Reservierung von Bandbreiten eingehalten werden, die bei der Einrichtung der Verbindung vorgenommen wird [DeP96].

2.3.1 CBR

Echtzeitanwendungen akzeptieren meist keine oder nur sehr geringe Schwankungen bei der Verzögerung des Ausgangssignals. Diese Dienste werden CBR oder isochron genannt. Als Verkehrsparameter sind vor allem die Spitzenzellrate (Peak Cell Rate, PCR) für jede Verbindung zwingend notwendig, die eine obere Grenze der Zellrate festlegt. Tabelle 1 stellt die einzelnen Dienstklassen und ihre Parameter gegenüber. Für die Bestimmung der Dienstqualitätsklasse A (QoS Class 1) sind noch die folgenden Parameter von Bedeutung:

- CTD (Cell Transfer Delay) Zellübertragungsverzögerung
- CDV (Cell Delay Variation) Zellverzögerungsvariation

- CDVT (Cell Delay Variation Tolerance) Zellverzögerungsvariationstoleranz
- CLR (Cell Loss Ratio) Zellverlustrate

2.3.2 VBR

Der VBR Dienst (Variable Bit Rate) stellt Verbindungen eine Bandbreite bis hin zur Spitzenzellrate zur Verfügung. Dabei unterscheidet man noch zwischen rt-VBR und nrt-VBR. Während für rt-VBR in der Dienstklasse B die gleichen Parameter wie in Dienstklasse A verwendet werden, ist für nrt-VBR nur der Parameter CLR von Bedeutung.

2.3.3 UBR

In der am niedrigsten priorisierten Klasse (QoS Class 4) liegt der UBR-Dienst Er bietet keine Dienstqualität einer Verbindung an. Daher werden auch keine Parameter für den UBR-Dienst verwendet. Die Dienstklasse wird manchmal auch als 'Best Effort' bezeichnet.

2.3.4 ABT

Der ABT-Dienst (Asynchronous Block Transfer, ABT) ist in keine Dienstklasse eingeteilt, wurde jedoch auch vom ITU-T genormt. Dieser Dienst ist in gewisser Weise dem von ABR ähnlich. Auch er kann die unterschiedlichsten Datenapplikationen bedienen und verwendet auch RM-Zellen (Resource Management, RM) zur Flußsteuerung. RM-Zellen dienen zur Verkehrskontrolle in ATM-Netzwerken. Im Gegensatz zu ABR ist ABT eine Methode, die es der Datenquelle ermöglicht, eine bestimmte Bandbreite aufgrund von Blöcken von Zellen reservieren zu können. Ein Block wird durch zwei RM-Zellen begrenzt. Der größte Nachteil von ABT ist die erweiterte Leistung die jeder Vermittlungsknoten (Switch) aufbringen muß, um die zusätzlichen RM-Zellen zu produzieren. Auch die schnelle Entscheidung über verfügbare Bandbreite und ihre Reservierung setzt sehr schnelle Hardware voraus [DeP96].

3 Der ABR-Dienst in ATM-Netzwerken

3.1 Charakteristiken und Funktionsweise des ABR-Dienstes

Obwohl einige Anwendungen sich auf eine feste Bandbreite verlassen, können sich einige Anwendungen an zeitlich variierende unbenutzte Bandbreiten anpassen. Da Datenanwendungen Zellverlusten gegenüber empfindlich, zeitlichen Verzögerungen gegenüber jedoch toleranter sind, ist es für das Netzwerk unumgänglich, den Anwender über eine Überlastung im Netzwerk zu informieren und die Möglichkeit von Zellverlusten anzukündigen. Aus diesem Grund sind Managementfunktionen in der ATM-Schicht notwendig. Diese sorgen dafür, daß das Verkehrsaufkommen effizient von

den Quellen eines ATM-Netzwerks übertragen wird. Auf diese Weise können Netzwerkbetreiber die maximale Bandbreite der Übertragungsstrecke nutzen, ohne die Leistung der CBR- oder VBR-Verbindung zu beeinträchtigen. Hier definierten das ATM-Forum und die ITU-T eine neue Dienstklasse für die ATM-Schicht, Available Bit Rate (ABR) genannt [DeP96]. ABR ist eine Funktion der ATM-Schicht, mit der beschränkte Übertragungscharakteristika, (z.B. der Durchsatz), die vom Netzwerk bereitgestellt werden, während der Datenübertragung verändert werden können. Der ABR-Dienst ist nicht für Echtzeit-Anwendungen geeignet, aufgrund der veränderlichen ATM-Übertragungscharakteristika. Bei Einrichtung einer ABR-Verbindung legt der sendende Teil, vom ATM-Forum Source End System (SES) genannt, eine maximal geforderte Bandbreite fest, die als Spitzenzellrate bekannt ist, sowie die minimal geforderte Bandbreite, die minimale Zellrate (Minimal Cell Rate, MCR). Die Spitzenzellrate wird zwischen den Endsystemen und dem Netzwerk ausgehandelt, ebenso die minimale Zellrate, die aber auch Null sein kann. Die über das Netzwerk erhältliche Bandbreite darf bis zum Wert der minimalen Zellrate absinken. Die Bandbreite und gleichzeitig die Zellrate einer ABR-Verbindung dürfen folglich zwischen dem Wert der minimalen Zellrate und der Spitzenzellrate schwanken. Eine ABR-Funktion kann für eine virtuelle Kanalverbindung oder eine virtuelle Pfadverbindung eingerichtet werden. Der ABR-Dienst einer virtuellen Kanalverbindung innerhalb einer virtuellen Pfadverbindung teilt sich die Kapazität mit der entsprechenden virtuellen Pfadverbindung. Diese VPC kann entweder mit einer statischen Bandbreite oder der VPC-Bandbreite, die sich mit dem ABR-Mechanismus dynamisch ändert, definiert werden. Siehe dazu auch Abbildung 4. Eine wichtige Voraussetzung für den ABR-Dienst ist, daß die Ressource Bandbreite, die für eingerichtete CBR- und VBR-Verbindungen reserviert wurde, beim Abbau von CBR- und VBR-Verbindungen wieder freigegeben wird. Dabei wird die nicht reservierte Bandbreite, wenn möglich, für andere ABR-Verbindungen bereitgestellt.
Die folgenden wünschenswerten Kriterien werden vom ATM-Forum und ITU-T unterstützt und sollten grundlegende Eigenschaften jedes Netzwerkmechanismus in der ABR-Funktion der ATM-Schicht mit Feedback-Information sein [DeP96],[BF95]:

- Invarianz des Zeitrahmens: Der Feedback-Mechanismus sollte gut zur Netzgröße und den Verbindungsraten passen.
- Fairneß: Obwohl alle verfügbaren Ressourcen gemäß der vom Netzbetreiber festgelegten Politik zwischen allen ABR-Verbindungen einer bestimmten Schnittstelle aufgeteilt werden sollten, darf keine Art von ABR-Verbindung zufällig oder systematisch einer anderen Art vorgezogen werden.
- Robustheit: Die Funktionsbereitschaft des ATM-Netzwerks sollte nicht auf der Bereitschaft der Anwender beruhen, den bereitgestellten Steuerungsinformationen Folge zu leisten.
- Stabilität: Die Netzlast sollte gleichmäßig mit nur wenigen und beschränkten Schwankungen sein.

3.2 ABR-Flußsteuerungsmechanismen

Das ATM-Forum hat einen zellratenbasierten Flußsteuerungsansatz für die Ende-zu-Ende-ABR-Funktion entwickelt. Dieser ABR-Flußsteuerungsmechanismus erlaubt es

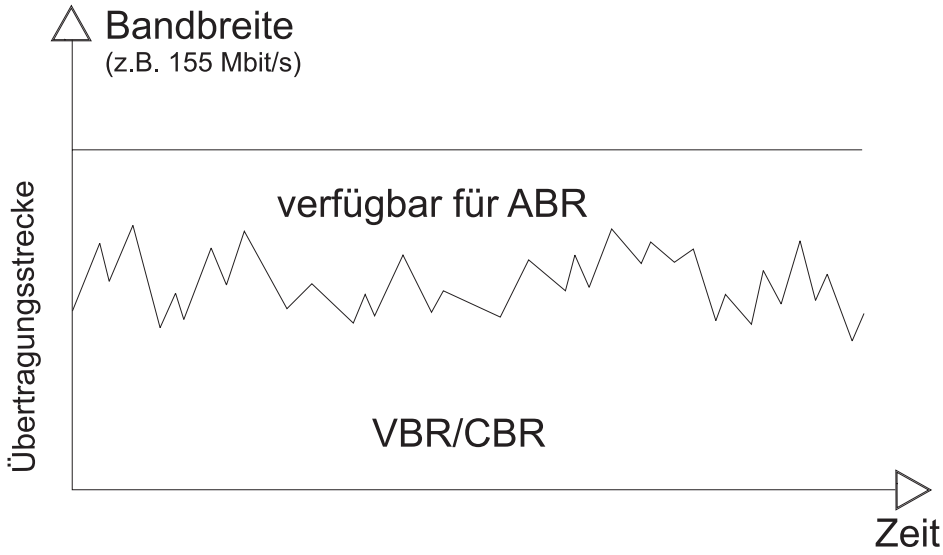


Abbildung 4: Beispiel der zur Verfügung stehenden Bandbreiten für ABR

dem Source End System, die Zellsenderate auf Basis von Feedback- Informationen des Netzwerks über den Verfügbarkeitsstatus von Bandbreitenressourcen dynamisch anzupassen. Abbildung 5 zeigt die Ende-zu-Ende-Feedback-Steuerung. Da dieser Algorithmus und einige Varianten davon, dem ATM-Forum als zufriedenstellend und praktikabel erschien, soll dieser hier etwas genauer beschrieben werden.

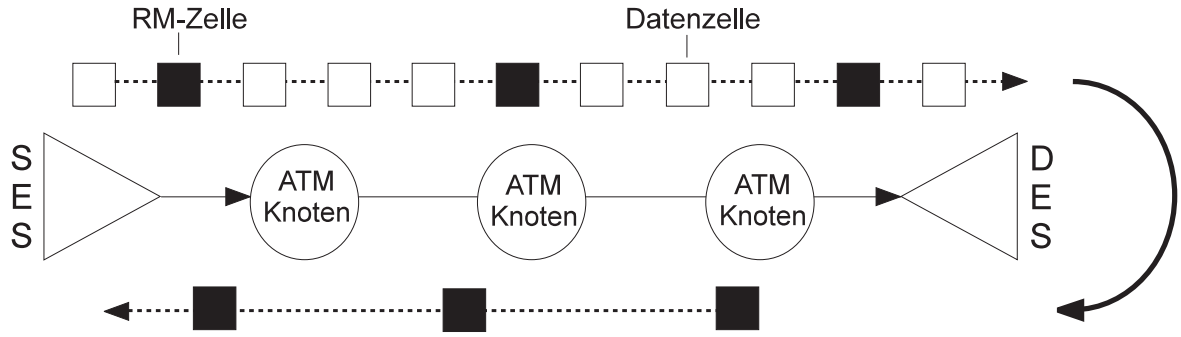


Abbildung 5: Feedback Steuerung in ATM

Dieser Algorithmus entspricht im wesentlichen dem EPRCA-Algorithmus, der weiter unten noch einmal erläutert wird. Die RM-Zellen sind durch die ITU-T genormt und haben ein auf Null gesetztes CLP-Bit. Sie werden durch die virtuelle Kanalkennung von 6 (VCI=6) über einen virtuellen Pfad oder über den Nutzlastarterkennung von 110 (PT=110) über eine virtuelle Kanalverbindung gekennzeichnet [CLS96]. Dazu vergleiche man Abbildung 2. Ein ABR-Flußsteuerungsmechanismus, der auf einer reinen Ende-zu-Ende-Basis funktioniert, erhält die RM-Zellen vom Zielsystem (Destination End System, DES) zurück, wodurch der Informationskreis in Richtung SES geschlossen wird. Man bezeichnet den ABR-Dienst auch als 'closed-loop control'. Es entstehen also zwei RM-Zellströme, einer in Vorwärtsrichtung von SES nach DES und ein zurücklaufender von DES zu SES. Die Richtung der RM-Zelle wird durch den Richtungsindikator (DIR) im Informationsfeld der RM-Zelle festgelegt. Das ratenbasierte Verfahren der RM-Zellen bietet außerdem die Möglichkeit, zwischen zwei ATM-Knoten eine sogenannte Segmentierung einzusetzen. Die Segmentierung ermöglicht es Netzbetreibern,

besonders solchen in öffentlichen Netzen, den ABR-Verkehr im Netzwerk schneller zu regeln. Die Einführung eines virtuellen Ziels und einer virtuellen Quelle hat den Vorteil, daß die Informationsrückführung praktisch an jedem gewünschten Punkt entlang des Ende-zu-Ende-Pfads segmentiert werden kann. Ein zwischengeschaltetes Netzwerk hat dann die Möglichkeit, bei jeder ABR-Verbindung einen eigenen, internen Informationsfluß zu erzeugen, in dem die Schleife abgeschlossen wird [KM95],

- indem beim Eintritt über ein virtuelles Ziel zur Außenwelt (d.h. in Richtung SES) die empfangenen RM-Zellen in Rückrichtung an das SES gesendet wird.
- oder indem beim Austritt über eine virtuelle Quelle zur Außenwelt (d.h. in Richtung DES) die RM-Zellen nicht nur in Vorwärtsrichtung eingefügt werden, sondern diese auch aus dem Zellstrom in Rückrichtung entfernt werden.

Ein Schlüsselelement des zellbasierten RM-Steuermechanismus der ABR-Funktion, das das SES-Musterverhalten betrifft, wird 'positiv feedback' genannt [KM95]. Daneben gibt es noch 'negative feedback', 'explicit feedback' und Kombinationen daraus [CLS96].Das Referenzverhalten das SES legt folgendes fest:

- Fehlen die zurücklaufenden RM-Zellen, sollte das SES die Senderate gleichmäßig verringern.
- Das SES darf die Senderate nur dann erhöhen, wenn dazu eine explizite Genehmigung durch eine zurückgesandte RM-Zelle vorliegt.
- Beim Empfang zurückgesandter RM-Zellen ohne explizite Genehmigung sollte das SES die Zellrate weiter verringern.

4 Mechanismen zur Verkehrskontrolle in ATM

4.1 Fenster-basierte und Raten-basierte Verfahren

Um den ABR-Dienst zu unterstützen, braucht das Netzwerk einen Mechanismus, der ihm Auskunft über seinen momentanen Zustand gibt. Das Netzwerk benötigt Informationen für die einzelnen Datenquellen um ihnen mitteilen zu können, wieviel Daten sie gerade senden dürfen. Die zwei wohl bekanntesten Verfahren sind das fenster-basierte Verfahren (Credit Based Flow Control) oder auch 'link-by-link credit-based control' genannt. Das andere ist das raten-basierte Verfahren (Rate Based Flow Control) oder auch 'end-to-end rate-based control' genannt. Im September 1994 entschied sich das ATM-Forum für das raten-basierte Verfahren [KM95]. Beide Verfahren bieten jedoch bestimmte Vor- und Nachteile in den jeweiligen Netzwerkumgebungen.

4.2 Charakteristik des fenster-basierten Verfahrens

Es ist dem Flußkontrollverfahren mit Sliding Window Technik ähnlich. Eine Datenquelle kann solange keine Daten senden, bis die Datensenke, welche die Daten empfangen

soll, ihr dafür die Berechtigung (Credit) gibt, in Form von sogenannten Credit-Cells, die der Datenquelle die Verfügbarkeit von freiem Pufferspeicher signalisieren. Es ist daher aber immer garantiert, daß genügend freier Pufferspeicher für die zu empfangenden Daten vorhanden ist. Dies kann natürlich in unterschiedlichen Zeitabständen geschehen [KM95].
Das fenster-basierte Verfahren bietet einige Vorteile, wie zum Beispiel Fairneß, Robustheit und garantiert eine Zellverlustrate von Null. Da das Fenster-basierte Verfahren zur Datenflußsteuerung keine RM-Zellen verwendet, wie das Raten-basierten Verfahren, treten auch keine großen Verzögerungszeiten auf. Daher eignet sich dieses Verfahren für den Einsatz in einer LAN-Umgebung.
Der Nachteil diese Verfahrens besteht darin, daß für jede einzelne Verbindung eine Warteschlange oder auch Puffer vorhanden sein muß. Dies macht dieses Verfahren für den Einsatz in WANs unbezahlbar [CLS96].

4.3 Charakteristik des raten-basierten Verfahrens

Obwohl dieses Verfahren keine Zellverlustrate von Null garantieren kann, ist es doch flexibler und für die Implementierung der ATM-Knoten von Vorteil [CLS96]. Das Grundprinzip besteht darin, durch sogenannte RM-Zellen Informationen über den momentanen Zustand des Netzwerks, insbesondere durch das Verkehrsaufkommen von Daten beeinflußt, zu erhalten. Aufgrund dieser Information ist es dann der Datenquelle möglich, ihre Senderate zu variieren. Dieses Verfahren kontrolliert besser das Pufferüberlauf-Problem und damit auch die Speicheranforderungen, da es ständig neue Informationen über den Netzzustand durch den Empfang von RM-Zellen erhält. Es eignet sich besser für den Einsatz in Hochleistungs-Protokollen [KM95].
Der Nachteil dieses Verfahrens ist, daß bei Verzögerung oder gar Verlusten von RM-Zellen der Verkehrsfluß nicht mehr optimal geregelt werden kann [KM95]. Messungen haben gezeigt, daß die durchschnittliche Dateilänge unter UNIX bei ca. 22 kByte liegt und die meisten Dateien kleiner als 2 kByte sind. Das raten-basierte Verfahren benötigt für die Übertragung der Zustandsinformation einfach zu viel Zeit. Es eignet sich daher nicht optimal für ein Hochleistungsnetzwerk [CLS96]. Das raten-basierte Verfahren eignet sich besser für den Einsatz in einem WAN (Wide Area Network, WAN), da hier weite Strecken überbrückt werden müssen und durch die begrenzte physikalische Ausbreitungszeit, gewisse Laufzeiten entstehen, die größer sind, als die Warteschlangenverzögerungen [RN95].
Eine andere Idee, nämlich die Kombination beider Verfahren zeigt Abbildung 6. Dabei wird die Flexibilität des raten-basierten Verfahrens mit der Leistung des kredit-basierten Verfahrens kombiniert. Dabei wurde vorgeschlagen, daß zum Beispiel das raten-basierte Verfahren als Standardverfahren eingesetzt wird, und optional auch noch zusätzlich das Kredit-basierte Verfahren. Oder, daß das Raten-basierte Verfahren in WANs, und das Kredit-basierte Verfahren in LANs eingesetzt wird [RN95]. Das gezeigte Netz-Interface fungiert dabei als virtuelle Datenquelle und als virtuelles Ziel. Dieser Vorschlag würde sich besonders für den ABR-Dienst eignen [RN95], aber auch für VBR oder CBR.

Das ATM-Forum hat das Referenzverhalten von Source End System und Destination End System zur Rückmeldung der Übertragungsrate in einem einzelnen Algorithmus zusammengefaßt. Es gibt jedoch mehrere Verfahren, das Anheben/Absenken der Senderate optimal zu bestimmen.

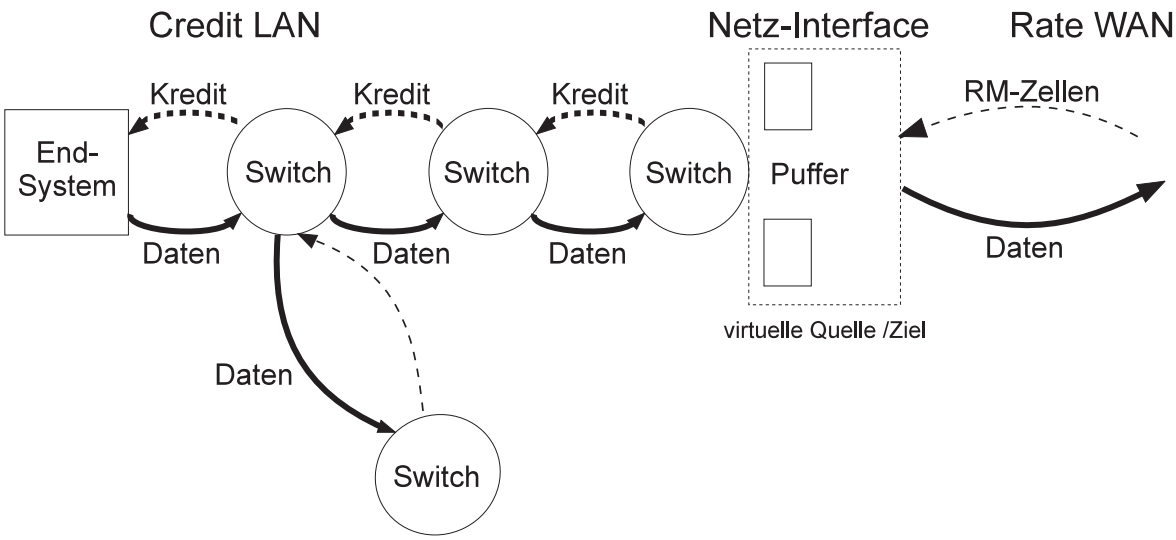


Abbildung 6: Netzwerk-Interface zwischen LAN mit Kredit-basierten Verfahren und WAN mit Raten-basierten Verfahren

Die folgenden Verfahren sind alles Raten-basierte Verfahren:

4.3.1 EFCI

Der EFCI-Mechanismus (Explicit Forward Congestion Indication) ist ähnlich zum DEC-Bit-Schema und dem FECN (Forward Explicit Congestion Notification). Ursprünglich wurde dieses Verfahren für den VBR-Dienst verwendet, wurde dann jedoch auch für den ABR-Dienst entdeckt [CLS96].Der EFCI-Mechanismus funktioniert wie folgt:
Das SES sendet alle Datenzellen mit dem Parameter EFCI=0 (keine Blockierung vorgekommen), und zwischenliegende ATM-Knoten melden dies an das DES der ABR-Verbindung, sofern keine Blockierung aufgetreten ist. Das DES überwacht den Blockierungszustand der Netzknoten, indem der EFCI-Status der empfangenen Datenzellen, der durch jeden Knoten aktualisiert werden kann, ausgewertet wird. Gleichzeitig wird der Status der rückläufigen RM-Zelle weitergegeben. Ist eine Blockierung aufgetreten wird das CI-Bit (Congestion Indikation) der RM-Zellen, die der Knoten selbst zurückschickt, auf 1 gesetzt.
Weiter wird das CI-Bit der RM-Zellen, die der Knoten selbst zurückschickt, immer dann auf 1 gesetzt, wenn der EFCI-Status der letzten empfangenen Datenzelle eine Blockierung in Flußrichtung anzeigt (EFCI=1). Dadurch imitiert der Knoten das DES-Verhalten für dieses Netzwerk in Flußrichtung [DeP96]. Der EFCI-Mechanismus verwendet das 'negative feedback', d.h. das SES erhöht die Senderate automatisch nach Definition und verringert diese nur, wenn eine entsprechende RM-Zelle eine Blockierung meldet. Der Nachteil dieses Verfahrens besteht in der Laufzeit der RM-Zellen sowie deren möglichen Verlust.

4.3.2 PRCA

Eine andere Version eines Steuerungsmechanismus ist der Proportional Rate Control Algorithm Mechanismus. Im Vergleich zur EFCI-Methode, wird hier das 'positiv feed-

back' verwendet. Das bedeutet, daß RM-Zellen nur dann gesendet werden, wenn eine geringe Verkehrsdichte erkannt wird und diese der SES anzeigt, die Datenrate zu erhöhen. Ansonsten verringert das SES exponentiell die Rate. Weiter werden die RM-Zellen proportional zur Senderate erzeugt.
Der Nachteil dieses Verfahrens besteht darin, nicht mehr konsistent gegenüber EFCI zu sein und die Anstiegsrate ist nicht mehr linear, aufgrund der RM-Zellen. Es hat sich auch gezeigt, daß es sich in bestimmten Situationen unfair gegenüber Verbindungen verhält, die permanent ihre Datenrate in Richtung des MCR-Parameters verringern [CLS96].

4.3.3 EPRCA

Neben dem beschränkten Ansatz des Anhebens/Absenkens der Rate, der durch die Option des binären Feedbacks festgelegt ist, hat das ATM-Forum einen erweiterten Steuerungsmechanismus für die Rate vorgesehen. Dieser beruht auf der expliziten Rückgabe der Rate. Der Enhanced Proportional Rate Control Algorithm ist eine Erweiterung der bestehenden PRCA-Methode, jedoch um die Option der expliziten Rückgabe der Datenrate erweitert. Man übernahm wieder die Funktionen aus dem EFCI-Mechanismus: EFCI=0 bedeutet keine Blockierung, entsprechend EFCI=1 bedeutet eine Blockierung. Vorwärtslaufende RM-Zellen werden von dem SES erzeugt. Ein explizites Feld für die Rate der RM-Zelle wurde definiert, in dem die zwischenliegenden Übertragungsknoten explizit die gewünschte SES-Zellenübertragungsrate angeben können [DeP96]. Wichtige Felder der RM-Zelle sind:

- DIR: welche die Laufrichtung der RM-Zelle enthält
- CI: welches anzeigt, ob ein hohes Verkehrsaufkommen vorliegt (CI=1) oder nicht (CI=0)
- ER: enthält die explizite Rate, initialisiert auf den Wert des PCR-Parameters
- ACR: (Allowed Cell Rate) auch Intelligente Marken genannt [DeP96] welche sich aus den Parametern der minimalen Zellrate und der aktuellen Zellrate (current cell rate, CCR) ergibt.

5 Ausblick

Derzeit sind Applikationen und Betriebssysteme noch nicht für verbindungsorientierte Netze wie ATM optimiert. Erst für die kommenden Jahre sind hierfür Lösungen in Sicht. Durch die Standardisierungsbemühungen des ATM-Forums sind die Spezifikationen inzwischen jedoch so weit gediehen, daß für jeden Anwendungsfall ATM-Geräte und -Adapter zur Verfügung stehen. Die LAN-Emulation schafft zwar eine praktikable Verbindung zwischen derzeit eingesetzten Applikationen und ATM-Netzen, kann jedoch die Leistungsfähigkeit von ATM nicht voll ausnutzen. Daher gilt es, möglichst bald die noch offenen Fragen, wie zum Beispiel das Zusammenspiel von TCP und dem ABR-Dienst, zu klären.
Aufgrund der Spezifikationen sollte auch das Zusammenspiel zwischen den Geräten

verschiedener Hersteller kein Problem darstellen, was sich jedoch nach aktuellen Angaben aus dem Internet nicht ganz bewahrheitet. Trotzdem ist der ABR-Dienst ein sehr interessanter und vielseitiger Dienst, der besonders für Netz-Provider von Bedeutung sein dürfte. Diese können mit dem ABR-Dienst ihre noch frei zur Verfügung stehende Bandbreite besser für weitere Verbindungen nutzen. Als Anreiz können sie den Konsumenten eine sehr geringe Zellverlustrate anbieten. Der Kommunikationsbedarf der meisten privaten Haushalte beschränkt sich heute meist noch auf Telefon und Fernsehen. Doch gerade durch den Einsatz von ATM, das mit einer Fülle von neuen Diensten aufwartet, könnten schon bald Schlagworte wie Video on Demand (VOD, d.h. der Abruf von Videofilmen beliebiger Wahl) in greifbare Nähe rücken.

Literatur

[BF95] F. Bonomi and K.W. Fendick. The Rate-Based Flow Control Framework for the Available Bit Rate ATM Service. *IEEE Network*, Vol. 9(No. 2):25–39, March/April 1995.

[CLS96] T.M. Chen, S.S. Liu, and V.K. Samalam. The Available Bit Rate Service for Data in ATM Networks. *IEEE Communications Magazine*, Vol. 34(No. 5):56–71, May 1996.

[DeP96] Martin DePrycker. *Asynchronous transfer mode: ATM/M.* Prentice Hall, 1996.

[Har96] Rüdiger Hartmann. Netz ohne Grenzen. *c't Computer Technik*, 1996(Nr. 10):346–354, Oktober 1996.

[KM95] H.T. Khung and R. Morris. Credit-Based Flow Control for ATM Networks. *IEEE Network*, Vol. 9(No. 2):40–48, March/April 1995.

[Kya95] Othmar Kyas. *ATM-Netzwerke: Aufbau, Funktion, Performance.* DATACOM-Fachbuchreihe, 1995.

[RN95] K.K. Ramakrishnan and P. Newman. Integration of Rate and Credit Schemes for ATM Flow Control. *IEEE Network*, Vol. 9(No. 2):49–56, March/April 1995.

Abbildungsverzeichnis

Tabellenverzeichnis

IPv6 - Das Internet Protokoll der nächsten Generation

Bernhard Thurm

Kurzfassung

Das neue Internet Protokoll IPv6 soll in naher Zukunft das alte IPv4 ersetzen. Anlaß für die neue Version war hauptsächlich die absehbare Erschöpfung des Adreßraumes, der mit den 128-Bit langen IPv6-Adressen begegnet werden soll. Die vorliegende Ausarbeitung untersucht die Gründe für die IPv4-basierten Probleme der Adressierung und geht dann ausführlich auf die Möglichkeiten der neuen Adressierung (Unicast-/Anycast-/Multicast-Adressen) und die neuen Datenformate (IPv6-Header, Erweiterungs-Header) ein. Im weiteren wird die daraus resultierende neue Funktionalität beschrieben: Echtzeit-Datenverkehr und Stau-/Lastkontrolle mittels Flow-Labels und Prioritätsvergabe, automatische Systemkonfiguration durch das Neighbor Discovery-/Dynamic Host Configuration-Protocol, Unterstützung mobiler Endsysteme, Authentifizierung und Verschlüsselung sowie Strategien zum Übergang von IPv4 nach IPv6.

1 Einleitung

Das Wachstum des Internet hat in den letzten Jahren eine Geschwindigkeit erreicht, die selbst die kühnsten Prognosen bei weitem übertroffen hat (Abb. 1). Ursprünglich aus rein militärischen Zwecken entwickelt und auf 4 Rechner beschränkt, verbindet es mittlerweile Millionen von Systemen auf der ganzen Welt. Neue Technologien wie ATM oder Glasfaser ermöglichen immer höhere Übertragungsraten (z.b. für Videokonferenzen) und ziehen - im Verbund mit den sinkenden Kosten - immer mehr Nutzer an. Doch dieses Wachstum hat auch seinen Preis: man geht davon aus, daß der vorhandene Adreßraum in den Jahren 2005-2011 erschöpft sein wird. Diese Entwicklung wurde von der IETF (Internet Engineering Task Force) Anfang der 90'er Jahre erkannt: 1992 fiel die Entscheidung, das vorhandene IP durch eine neue Version zu ersetzen. In der neu eingerichtetetn IPng-Area (IP Next Generation Area) fand eine Bewertung und Diskussion der Proposals statt, ehe 1995 im RFC 1752 [S.B95] die Empfehlung für das Internet Protokoll der nächsten Generation gegeben wurde. Dieses neue Protokoll, IPv6, stellt nicht nur einen erweiterten Adreßraum zur Verfügung, sondern beseitigt auch Schwächen in bisher von IPv4 vernachlässigten Bereichen. So bietet es z.b. Unterstützung für Echtzeit-Datenverkehr, eine flexible Stau-/Lastkontrolle, Authentifizierung und Verschlüsselung, automatische Systemkonfiguration, Unterstützung mobiler Endsysteme sowie neue Routing-Mechanismen, die die Zwischensysteme entlasten. Die

vorliegende Ausarbeitung führt zunächst in die neue Adressierung im Internet ein, beschreibt dann im Detail die Änderungen am IPv6-Header sowie die daraus resultierende neue Funktionalität und zeigt Möglichkeiten auf, eine Umstellung von IPv4 auf IPv6 durchzuführen.

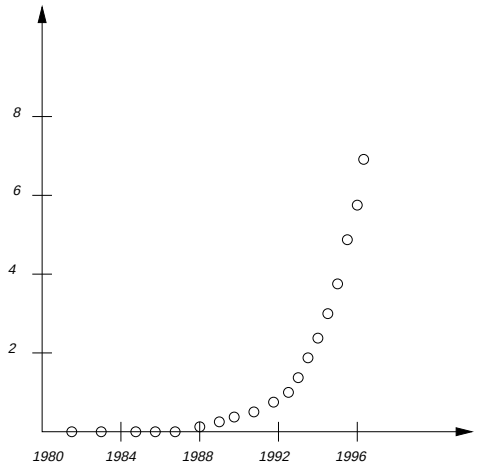


Abbildung 1: Computer im Internet (Millionen).

2 Adressierung in IPv6

Der entscheidende Anlaß, eine neue Version von IP zu entwicklen, war die absehbare Erschöpfung des Adreßraumes: IPv4 bietet zwar 32-Bit Adressen, so daß theoretisch 4 Milliarden ($= 2^{32}$) Systeme adressierbar sind, es gibt jedoch mehrere Gründe, die diese Zahl erheblich einschränken:

- Die - für das Routing benötigte - Einteilung in Class A,B,C,D,E Adressen ist sehr ineffizient, da mit einer Netzwerk-Adresse auch sämtliche zugehörige Host-Adressen reserviert werden (ob benötigt oder nicht). Vor allem die Anzahl der besonders beliebten Class B Netzwerke (theoretisch 16384) ist zu gering.

- Es ist allgemein üblich, Netzwerk-Adressen auch an IP-Netze zu vergeben, die nicht am Internet angeschlossen sind.

- Das enorme Wachstum des Internet: viele Firmen besitzen mehrere Netze; auch kabellose Netze werden in Zukunft eine grössere Rolle spielen. TCP/IP wird in immer neuen Bereichen eingesetzt z.b. bei elektronischem Zahlungsverkehr oder Kabelfernsehen.

- Ein Host ist nicht auf eine Adresse beschränkt, er kann mehrere IP-Adressen besitzen ("Multiple Adressing").

In IPv6 sind für die Adressierung 128 Bit vorgesehen,was einer Vergrößerung des Adreßraumes um den Faktor 2^{96} entspricht (das ist ca. $7.9 * 10^{28}$!).Die Angabe der Adressen erfolgt in der Form a:b:c:d:e:f:g:h ,wobei jede Stelle 16 Bit kodiert.

Eine Adresse wird dabei nicht mehr an einen einzelnen Knoten, sondern an die Netzwerkkarte direkt vergeben, dabei darf eine Karte auch mehrere Adressen besitzen (der Knoten wird dann durch eine beliebige dieser Adressen eindeutig identifiziert). Verhinderte in IPv4 der prinzipielle Aufbau der Adressen ein effizientes Routing (wenig Hierarchiestufen, große Routing-Tabellen) erlauben die neuen - längeren - Adressen, Hierarchien z.b. nach lokalem Netzwerk, Firma, Standort, geographischer Lage zu bilden, was die Größe der Routing-Tabellen verkleinert.

Grundsätzlich unterscheidet man 3 Adreßtypen, die jeweils durch ein Format-Präfix variabler Länge festgelegt werden: Unicast-/Anycast- und Multicast-Adressen [Sta96].

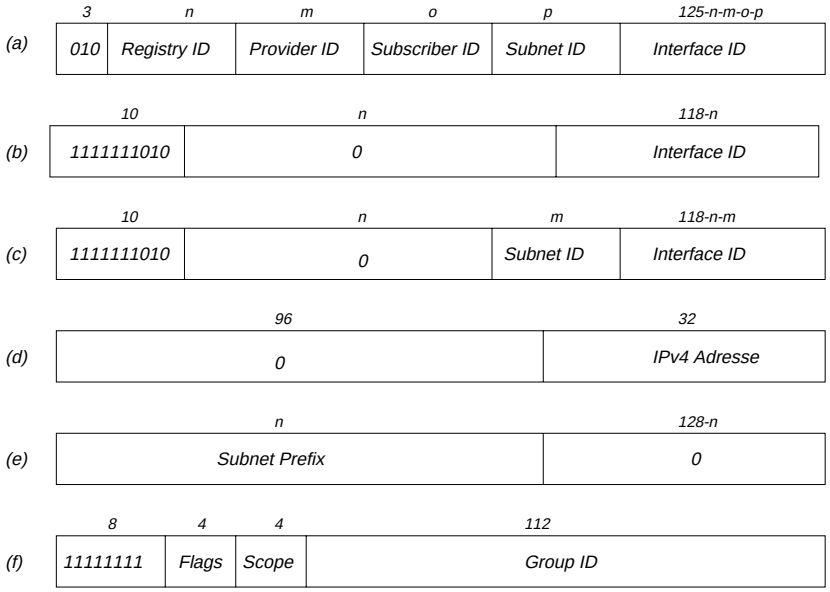


Abbildung 2: Adreßformate.

2.1 Unicast-Adressen

Eine Unicast-Adresse identifiziert eindeutig eine bestimmte Netzwerkkarte, an die die IP-Pakete ausgeliefert werden. Unter den Unicast-Adressen existiert eine weitere Strukturierung:

- **Provider Based Unicast Address** (Abb. 2a): Provider-basierte Unicast-Adressen ermöglichen eine globale Adressierung über den gesamten Adreßraum. Nach dem Präfix folgen mehrere Felder variabler Länge, die eine hierarchische Gliederung ermöglichen: Registry-ID identifiziert die Registrierungsinstanz, die den Provider-Teil der Adresse vergibt, Provider-ID bezeichnet den Netzanbieter, der den Subscriber-Teil der Adresse vergibt. Der Subscriber (Firma, Organisation o.ä.) legt dann wiederum die Subnetz-ID fest. Für eine eindeutige Adressierung muß dann noch eine Kennung für die Netzwerkkarte vergeben werden, z.b. mittels der MAC-Adresse (Ethernet, Tokenring).

- **Link-Local Address** (Abb. 2b): Link[1]-lokale Adressen enthalten neben dem Präfix lediglich eine Kennung für die Netzwerkkarte; sie dürfen nicht über den

[1] z.b. ein/mehrere Ethernet Segmente

Link weitergeleitet werden und können auch nicht in das globale Adressierungsschema integriert werden. Ihre Verwendung liegt im Bereich der automatischen Systemkonfiguration (siehe Kapitel 4).

- **Site-Local Address**(Abb. 2c): Standort-lokale Adressen besitzen neben dem Präfix eine Subnet-ID und eine Interface-ID: dies ermöglicht die lokale Verwendung (ähnlich wie bei Link-lokalen Adressen dürfen Pakete mit solchen Zieladressen nicht über den Standort weitergeleitet werden), eine spätere Integration in das globale Adressierungsschema ist jedoch leicht möglich, in dem der unbenutzte Teil um Registry-ID, Provider-ID und Subscriber-ID ergänzt wird.

Zwei Unicast-Adreßtypen sind speziell für den Übergang von IPv4 nach IPv6 vorgesehen (siehe auch Kapitel 7):

- **IPv4 Compatible Address** (Abb. 2d): IPv4-kompatible Adressen enthalten in den niederwertigen 32 Bit eine IPv4-Adresse, während die höherwertigen 96 Bit 0 sind (z.b. 0:0:0:0:0:0:ab:cd , wennn a.b.c.d eine IPv4-Adresse ist).
- **IPv4 Mapped Address**: IPv4-abgebildete Adressen enthalten ebenfalls in den niederwertigen 32 Bit eine IPv4-Adresse, jedoch sind jetzt die höherwertigen 80 Bit 0 und die 16 darauffolgenden Bit 1 (z.b. 0:0:0:0:0:FFFF:ab:cd).

2.2 Anycast-Adressen

Eine Anycast Adresse identifiziert eine Menge von Netzwerkkarten, die i.a. zu verschiedenen Systemen gehören (diese Systeme werden auch als Gruppe bezeichnet): gibt ein Sender eine solche Anycast-Adresse als Ziel an, bedeutet dies, daß das Datenpaket an mindestens ein (i.a. das nächstliegende) System dieser Gruppe ausgeliefert wird. Da sich Anycast-Adressen syntaktisch nicht von Unicast-Adressen unterscheiden, muß jedes System, das eine solche Adresse besitzt, explizit für die Erkennung dieser Adresse konfiguriert werden (im Gegensatz zum Broadcast). Zusätzlich müssen die Router in der Lage sein, die Anycast-Adresse auf die Hardware-Adresse (MAC-Adresse) einer Netzwerkkarte abzubilden.

Vorläufig sollen Anycast-Adressen nicht als Quelladressen auftreten und auch nur Zwischensysteme identifizieren. Eine mögliche Anwendung wäre z.b. die Weiterleitung eines Paketes über ein bestimmtes Subnetz, indem nicht eine spezielle Router-Adresse angegeben wird, sondern eine Anycast-Adresse, die mehrere Router identifiziert.

- **Subnet Router Address** (Abb. 2e): Die Subnetz-Router-Adresse stellt eine vordefinierte Anycast-Adresse dar: sie enthält ein Präfix für das Subnetz und eine Interface-ID, die jedoch nur aus 0-en besteht. Die Auslieferung erfolgt an einen (beliebigen) Router im Subnetz.

2.3 Multicast-Adressen

Multicast-Adressen (Abb. 2f) ermöglichen es, einer Menge von Netzwerkkarten („Gruppe“) eine Adresse zuzuweisen, eine Auslieferung von Paketen erfolgt dann an alle Gruppenmitglieder. Die Identifizierung einer Gruppe erfolgt dabei durch eine 112 Bit lange Gruppen-ID. Es lassen sich 2 Typen von Multicast-Gruppen unterscheiden:

- **Permanente Gruppen**: Die Adresse permanenter Gruppen wird durch die "Global Internet Numbering Authority Group" vergeben; Gruppen dieses Typs sind dauerhaft gültig.
- **Transiente Gruppen**: Diese Gruppen existieren nur temporär und erhalten auch nur eine temporär gültige Adresse.

Die Unterscheidung erfolgt durch das Feld "Flag": ist das letzte Bit eine 0 handelt es sich um eine permanente Adresse, andernfalls um eine temporäre Adresse.

"Scope"schränkt dabei den Gültigkeitsbereich einer Multicast-Adresse auf zweierlei Art ein: im Falle einer permanenten Multicast-Gruppe wird das Routing der Pakete abhängig vom Wert dieses Feldes durchgeführt (z.b. nicht über Standort hinaus), die Adresse selbst bleibt jedoch global gültig. Dadurch besteht die Möglichkeit, nur bestimmte Teile einer Gruppe anzusprechen. Im Falle einer temporären Gruppe ist die Adresse selbst nur im angegebenen Bereich gültig, was eine Wiederverwendung in einem anderen Bereich ermöglicht (eine Site-lokale temporäre Multicast-Adresse kann z.b. an 2 verschiedenen Standorten verwendet werden). Einige Multicast-Adressen sind bereits vordefiniert, z.b. alle Systeme an einem Link oder alle DHCP[2]-Server (siehe Kapitel 4).

- **Solicited Nodes Address**: Jede Unicast-/Anycast-Adresse wird genau auf eine Solicited-Nodes-Adresse abgebildet: dazu werden die letzten 32 Bit der Adresse an das Präfix FF01:0:0:0:0:1 angehängt (Bsp: 1:2:3:4:5:6:7:8 wird zu FF01:0:0:0:0:1:7:8). Da dieses Präfix eine Multicast-Adresse identifiziert, gehört jeder Knoten automatisch zur Multicast-Gruppe, deren Gruppen-ID seinen niederwertigsten 32 Bit entspricht. Solicited-Nodes-Adressen werden v.a. zu Kontrollzwecken benötigt und in den Protokollen DHCP und ND[3] eingesetzt (siehe Kapitel 4).

3 Datenformate

Eine IPv6-PDU hat im allgemeinen folgenden Aufbau (Abb. 3):

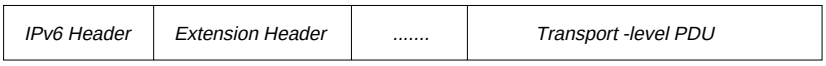


Abbildung 3: IPv6-PDU.

Auf den eigentlichen IPv6-Header können noch sogenannte "Extension"-Header folgen, in denen optionale Informationen übermittelt werden.

3.1 Der IPv6-Header

Vergleicht man den IPv4-Header (Abb. 4) mit dem IPv6-Header (Abb. 5), lassen sich folgene Neuerungen erkennen:

[2]Dynamic Host Configuration Protocol
[3]Neighbor Discovery

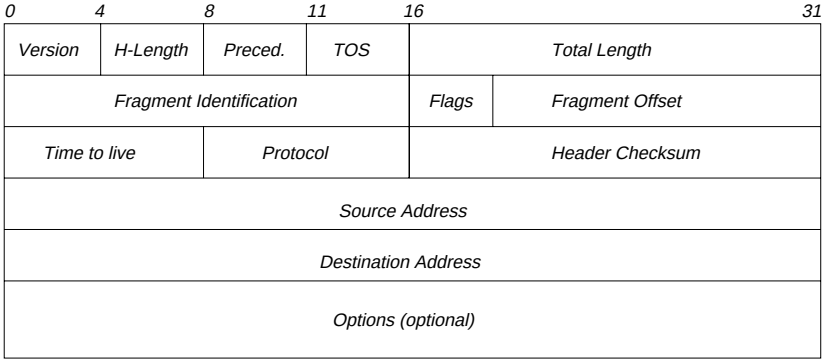


Abbildung 4: IPv4-Header.

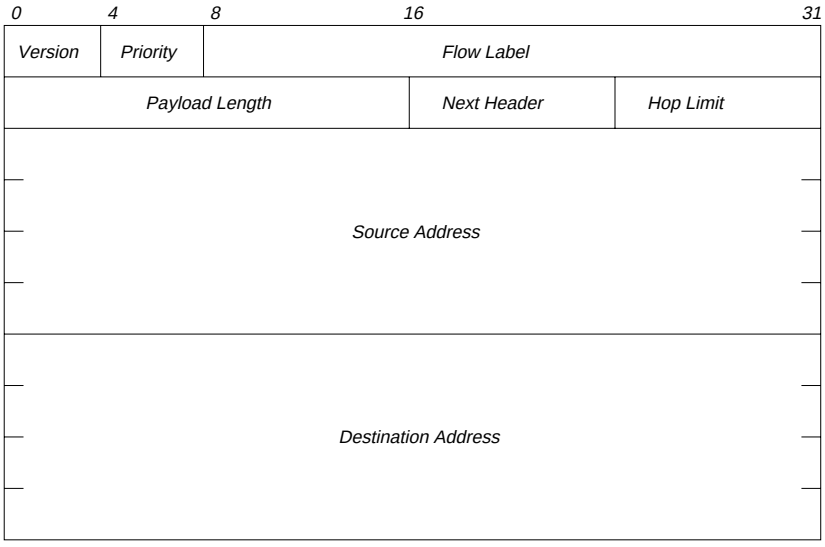


Abbildung 5: IPv6-Header.

- Der IPv6-Header besitzt eine feste Länge von 40 Byte.
- Die Felder Header Length, Header Checksum, Type of Service wurden eliminiert.
- Flags, Fragment Offset und Identification kommen in einen separaten Header, den Fragment-Header.
- Precedence, Total Length, TTL (Time to live) und Protocol werden ersetzt durch Priority, Payload Length, Hop Limit und Next Header.

Das neue Format ermöglicht eine beschleunigte Verarbeitung, da der - den Normalfall darstellenden - IPv6-Header weniger Felder enthält und eine feste Länge besitzt.

- **Version**: Versions Nummer.
- **Priority**: Erlaubt einem Sender, die gewünschte Priorität seiner Pakete anzugeben. Dabei sind 2 Bereiche zu unterscheiden:
  - Priorität 0-7 : Der Sender nimmt eine Staukontrolle vor, d.h. er verzögert das Aussenden seiner Pakete, sobald er bemerkt, daß eine Stausituation vorliegt.
  - Priorität 8-15: Der Sender nimmt keine Staukontrolle vor, z.b. bei Verkehr mit konstanter Datenrate (z.b. Echtzeitdaten).

  Zu bemerken ist noch, daß die Prioritäten beider Verkehrsarten unabhängig voneinander sind, d.h. ein Paket der Priorität 8 ist nicht "wichtiger" einzustufen, als ein Paket der Priorität 7.
- **Flow Label**: Unter einem Fluß versteht man eine Folge von Paketen von einer bestimmten Quelle zu einem bestimmten (Unicast-/Multicast-) Ziel, für die eine besondere Behandlung durch dazwischenliegende Router erwünscht ist. Die Quelle vergibt dazu eine sogenannte Flußmarke, um einen von ihr ausgehenden Fluß zu kennzeichnen (diese Marke zusammen mit der Quelladresse identifiziert den Fluß eindeutig). Eine Quelle darf definitionsgemäß mehrere Flüße unterhalten, wichtig ist jedoch, daß alle Pakete eines Flusses dieselbe Quell- und Zieladresse besitzen. Ein Fluß wird üblicherweise dazu eingesetzt, Pakete einer einzelnen Anwendung zu kennzeichnen, da diese meist dieselben Übertragungsanforderungen besitzen. Denkbar ist aber auch, die Datenströme einer Anwendung in mehrere Flüsse aufzuteilen, z.b. Audio- und Video-Daten einer Multimedia-Konferenz.

  Aus der Sicht eines Routers bestimmt ein Fluß die Art und Weise, wie alle folgenden Pakete eines Flusses behandelt werden sollen, etwa im Hinblick auf Wegwahl, Resourcen-Reservierung, Priorität und Sicherheit (d.h. Quell- und Zieladresse, Routing Header, Hop by Hop Header sollten identisch sein). Die Verarbeitung innerhalb eines Routers läuft dann folgendermaßen ab: Trifft ein Paket mit unbekannter Flußmarke ein, werden dessen - für das Routing relevante - Optionen sowie daraus entstehende Verarbeitungsergebnisse (z.b. Wegwahl) in einer Hash Tabelle unter dem Hash-Wert der Flußmarke gesichert (man spricht auch von einem "Route Cache"). Der Wert der Flußmarke sollte dabei gleichverteilt aus dem Wertebereich gewählt werden, um Ballungen zu vermeiden. Das Routing wird durch dieses Verfahren beschleunigt, da für nachfolgende Pakete des Flusses

die vorberechneten Ergebnisse verwendet werden können. Einträge in der Hash Tabelle bleiben 6 Sekunden gültig, danach ist eine komplette Neuberechnung nötig.

Anstelle des Verfahrens, das erste Paket mit unbekannter Flußmarke für die Generierung eines Eintrags im Cache zu verwenden, ist es auch möglich, eine explizite Vorabreservierung mittels des Kontrollprotokolls RSVP[4] vorzunehmen

- **Payload**: Länge des IPv6-Paketes ohne den IPv6-Header (=Länge aller Erweiterungs Header + Transport PDU). Da Payload eine Länge von 16 Bit besitzt, ist ein normales Datagramm auf 65535+40=65575 Byte beschränkt.

- **Next Header**: Spezifiziert den Typ des nachfolgenden Erweiterungs-Headers. Falls kein IP-Header mehr folgt, gibt dieses Feld an, an welches Protokoll die Daten ausgeliefert werden.

- **Hop Limit**: Gibt die maximale Anzahl von Routern an, die das Paket passieren darf (0=„wird verworfen“).

3.2 Erweiterungs-Header

IPv6 verlagert optionale Felder vom Standard-Header in sogenannte Erweiterungs-Header. Dabei wird der Typ des nachfolgenden Headers im Feld “Next Header” des vorhergehenden Headers angegeben. Jeder Erweiterungs-Header besitzt zur schnelleren Verarbeitung eine Länge mit einem Vielfachen von 8 und darf höchstens einmal in einem Paket vorkommen. Treten mehrere Header auf, ist eine Reihenfolge vorgegeben:

1. IPv6 Header
2. Hop by Hop Header
3. Routing Header
4. Fragment Header
5. Authentication Header
6. Encapsulating Payload Header
7. Destination Options Header

- **Hop by Hop Header**: Der Hop by Hop Header enthält Informationen, die von jedem Router eines Pfades ausgewertet werden müssen. Im IPv6-Standard wurde bisher nur die sogenannte “Jumbo Payload” Option spezifiziert, die aus einer 32 Bit Längenangabe besteht und die Paketlänge in Bytes angibt: damit sind statt $2^{16} - 1$ Byte langen Paketen auch $2^{32} - 1$ Byte lange Pakete möglich.

- **Routing Header** (Abb. 6): Der Routing-Header ermöglicht es einem Sender, ein oder mehrere Router zu spezifizieren, die ein Paket auf seinem Weg zum Ziel passieren soll. Definiert wurde bisher nur Typ 0: Die Adressen innerhalb des Headers bezeichnen die Zwischensysteme, die das Paket noch durchlaufen muß, mit dem endgültigen Ziel als letzte Adresse. Empfängt ein Router solch ein Paket, trägt er die nächste zu durchlaufende Adresse im IPv6-Header ein (als Destination Address) und dekrementiert das “Segments Left”-Feld (was die Anzahl der

[4] Resource Reservation Protocol

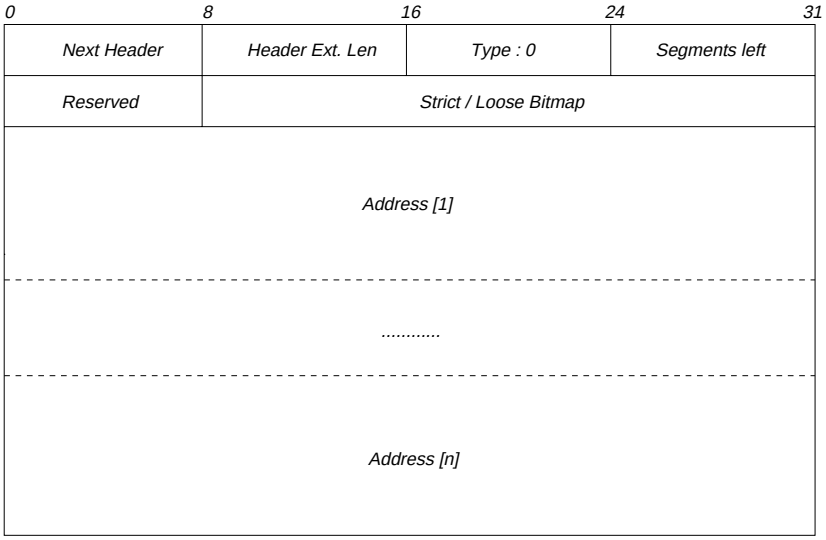


Abbildung 6: Routing-Header.

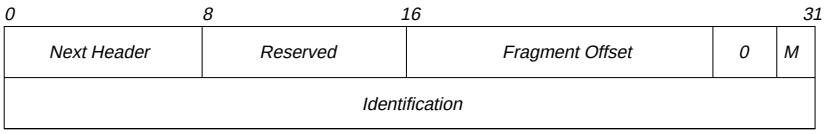


Abbildung 7: Fragment-Header.

restlichen "Hops" angibt). Mittels "Strict/Loose Bitmap" wird bestimmt, ob die nächste Adresse ein Nachbar der vorherigen sein muß, d.h. ob Zwischenschritte erlaubt sind (jedes Bit repräsentiert einen Router).

- **Fragment Header** (Abb. 7): Im Gegensatz zu IPv4 wird in IPv6 nur vom Sender eine Fragmentierung durchgeführt und nur vom Empfänger reassembliert. Aus diesem Grund muß der Sender in der Lage sein, eine Pfad-MTU Erkennung durchzuführen (Pfad-MTU = kleinste Paketgröße auf dem Pfad): das erste Paket wird mit der Größe des ersten (angeschlossenen) Netzwerks gesendet; falls auf dem Weg zum Ziel das Paket die MTU eines Netzes übersteigt, sendet der betreffende Router eine ICMP-Meldung "Message too big" zurück und der Sender paßt seine Paketgröße an und sendet erneut. Dabei beträgt die Mindest-MTU, die jedes Netz unterstützen muß, 576 Byte (zum Vergleich Ethernet ca. 1500 Byte).

  Fragmentierung kommt nur zum Einsatz, falls die IP-Instanz des Senders ein Paket erhält, das inklusive der IP Header die Pfad-MTU überschreitet. Das (zu große) Originalpaket erhält eine eindeutige Identifikation ("Identification") und wird in kleinere Pakete unterteilt. "Fragment Offset" bezeichnet den Beginn eines Fragments im Originalpaket (z.b. 0 für das erste Fragment)."M" (More) gibt an, ob noch weitere Fragmente folgen.

- **Authentication/Encapsulated Payload Header**: Siehe Kapitel 6.

- **Destination Options Header**: Optionale Informationen, die nur vom Ziel ausgewertet werden müssen (bisher noch nicht weiter spezifiziert).

4 Automatische Systemkonfiguration

4.1 Neighbor Discovery

Das Neighbor Discovery Protokoll (ND) erlaubt es - über ICMPv6[5]-Pakete - Kontrollnachrichten auszutauschen. Hauptaufgabe ist die Erkennung anderer Systeme, die sich am gleichen Link befinden. Man kann folgende Funktionen unterscheiden [Bra96]:

- **Router-Erkennung**: Aktive Router senden auf ihren Links periodisch sogenannte "Router-Advertisements" an die All-Hosts Multicast-Adresse, als Quelladresse werden dabei sowohl die eigene Link- wie auch IP-Adresse verwendet. Ein Knoten kann auch explizit ein solches Advertisement anfordern, mittels einer "Router Solicitation Message" an die All-Routers Multicast-Adresse.

- **Präfix-Erkennung/Bestimmung nächster Knoten**: Router-Advertisements enthalten Präfix Listen für den Link, auf dem das Advertisement gesendet wurde. Ein Präfix ist der höherwertige Teil einer IP-Adresse (z.b. die höherwertigsten 64 Bit) und wird von dem - für den Link zuständigen - Router (der ja die gesammelte Adreßinformation über den Link besitzt) festgelegt. Durch Vergleich der Zieladresse mit den Präfixen kann so ein Knoten feststellen, ob sich der gewünschte Zielknoten am gleichen Link befindet. (Bsp: Sämtliche Knoten eines Links besitzen Adressen, die mit 4c00:0:0:1 beginnen, der Router versendet dann das Präfix 4c00:0:0:1 in seinen Advertisements.)

- **Parameter Erkennung**: Router-Advertisements enthalten außerdem noch zusätzliche Informationen, z.b. empfohlene Anzahl Hops ("Max Hops"), Erreichbarkeit des Routers ("Router Lifetime") oder MTU-Größe. Diese Parameter-Erkennung erleichtert das Eingliedern neuer Knoten, da ein Großteil der aufwendigen manuellen Konfiguration entfällt.

- **Adreßauflösung**: Besitzt ein Knoten nur die IP-Adresse eines anderen Knotens, der sich auf demselben Link befindet, muß er zuerst dessen Link-Adresse bestimmen. Zu diesem Zweck sendet er ein sogenanntes "Neighbor Solicitation"-Paket an die (Link-lokale) Solicited-Nodes Multicast-Adresse. Die Antwort ("Neighbor Advertisement") enthält die gesuchte Link-Adresse. Die Verwendung der Solicited-Nodes Multicast-Adresse bewirkt, daß die Anfrage nur an einen kleinen Teil der Knoten eines Links gesendet wird, nämlich an diejenigen Knoten, deren niederwertigste 32 Bit ihrer Unicast-Adresse mit denen des Zielknotens übereinstimmen (Lastreduzierung). Eine Änderung der eigenen Link-Adresse kann ein Knoten durch Senden eines Neighbor-Solicitation-Paketes an die All-Hosts Multicast-Adresse anzeigen. Neighbor Solicitation kann auch zur Erkennung von Adreßduplikaten und zur Erreichbarkeitsbestimmung von Nachbarknoten eingesetzt werden.

- **Zustandslose automatische Adreßkonfiguration** : Hiermit wird die Konfiguration einer Netzwerkkarte mit einer eindeutigen IP-Adresse erleichtert: ein Knoten wartet auf ein Router-Advertisement (oder fordert ein solches an) und konfiguriert seine Adresse aus dem Link-spezifischen Präfix und zusätzlich einer

[5] Internet Control Message Protocol

Kennung für seine Karte (z.b. Hardware-Adresse). Die Eindeutigkeit der Adresse läßt sich dann durch ein Neighbor-Solicitation Paket überprüfen. Ist kein Router vorhanden, werden Link-lokale Adressen verwendet.

- **Zustandsbehaftete automatische Adreßkonfiguration** : Eine flexiblere Methode der Adreßkonfiguration bietet DHCP[6], das auf dem Client-Server Prinzip basiert: Ein Client, der eine IP-Adresse benötigt, sendet eine (Link-lokale) Anfrage an einen DHCP-Server (Unicast, falls dessen Adresse bekannt, andernfalls an eine vordefinierte DHCP-Multicast-Adresse) und erhält von diesem eine Antwort, die IP-Adresse, welche der Client wiederum bestätigt. Die Adresse hat eine begrenzte Gültigkeitsdauer, nach deren Ablauf eine Verlängerung beantragt werden muß (Gültigkeitsdauer bestimmt durch Antwort des DHCP-Servers).

  War bei der zustandslosen Adreßkonfiguration an jedem Link ein Router nötig, der Advertisements verschickt, so wird jetzt nicht an jedem Link ein DHCP-Server benötigt: sogenannte "Relay-Agents" müssen gegebenenfalls die Pakete an den nächsten Server weiterleiten.

- **Redirect** : "ICMP - Redirect"-Meldungen werden von Routern verwendet, um einem Sender einen anderen Pfad für seine Pake an einen bestimmten Empfänger mitzuteilen (z.b. bei 2 Routern an einem Link).

5 Unterstützung mobiler Endsysteme

Mobile-IP ist gekennzeichnet durch 3 Knotentypen:

1. Mobile Host: Das mobile Endsystem.
2. Home Agent: Ein Knoten im Heimatnetz, der dem Mobile Host Pakete nachsendet.
3. Foreign Agent: Ein Knoten am neuen Standort, der Pakete an den Mobile Host weiterleitet.

DHCP vereinfacht es dem Mobile Host, im neuen (fremden) Netz eine eigene temporäre IP-Adresse ("Care Of Address") zu erlangen, wenn er sein Heimatnetz verlassen hat. Mit ND ist es leicht möglich, notwendige Routing Informationen über den neuen Standort abzufragen. Somit wird die Funktion des Foreign Agent in den meisten Fällen obsolet.

War es bisher in IPv4 für den Home Agent nötig, die Pakete an den Mobile Host in ein Paket mit der Care-Of- Adresse einzukapseln ("Tunneling"), kann darauf in IPv6 verzichtet werden: es genügt, die Care-Of Adresse und die Zieladresse im Routing-Header anzugeben. Der Mobile Host ist jetzt zudem mittels der Option "Binding Update" (im Destination-Options-Header) in der Lage, direkt - den an ihn sendenden Systemen - seinen neuen Standort mitzuteilen, so daß der Umweg über den Home Agent entfällt.

Registrierungs-Informationen (nötig, um dem Home Agent den neuen Standort des Mobile Host mitzuteilen) werden in IPv6 nicht mehr über UDP[7], sondern über spezielle ICMPv6 Pakete oder Optionen im Erweiterungs-Header ausgetauscht.

[6] Dynamic Host Configuration Protocol
[7] User Datagramm Protocol

6 Sicherheit in IPv6

Im Internet existieren bereits eine Reihe anwendungsspezifischer Sicherheitsmaßnahmen, z.b. Secure HTTP, Privacy Enhanced Mail; Sicherheitsmaßnahmen auf IP-Ebene ermöglichen jedoch eine neue Qualität: Sicherheit ist künftig für jede Anwendung realisierbar, es müssen keine spezifischen Lösungen entworfen werden.

Grundsätzlich lassen sich 2 Gebiete unterscheiden:

1. **Authentifizierung**: Stellt sicher, daß das Paket wirklich vom angegebenen Sender – ohne Verfälschung – übertragen wurde.
2. **Verschlüsselung**: Verhindert unbefugtes Ausspähen von Daten.

Beide Verfahren basieren auf dem Konzept der Sicherheits-Assoziation: diese Assoziation besteht zwischen Sender und Empfänger und ist nur in einer Richtung gültig. Eindeutig identifiziert wird sie durch die Zieladresse und einen SPI ("Security Parameter Index"), der sich in einem Erweiterungs-Header befindet. Durch den Aufbau einer solchen Assoziation werden u.a. definiert:

- Verschlüsselungs-/Authentifizierungsalgorithmus.
- Ein/mehrere Schlüssel.
- Lebenszeit der Schlüssel/der Assoziation.
- Sicherheitslevel (Top Secret, Secret ...).

6.1 Authentifizierung

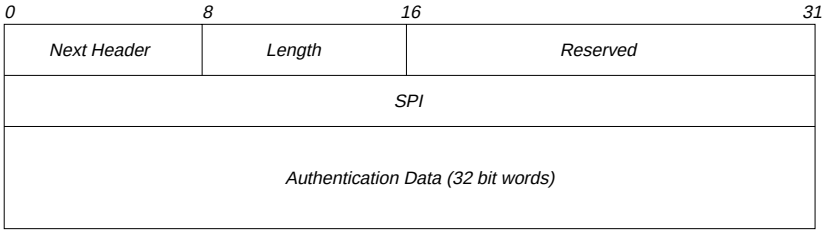


Abbildung 8: Authentifizierungs-Header.

Die Authentifizierung basiert auf dem Authentifizierungs-Header (AH) (Abb. 8). Das Feld SPI definiert dabei (mit der Zieladresse) die Sicherheits-Assoziation, in "Authentication Data" befinden sich die vom Authentifizierungs-Algorithmus berechneten Daten. Die Berechnung erfolgt vor einer möglichen Fragmentierung und geht über das gesamte IP-Paket, ausgeschlossen der Felder, die sich während des Routings ändern können.

Standardmäßig wird MD5 ("Message Digest 5") als Algorithmus eingesetzt: aus dem abzusendenden Paket und einem vorher -zwischen Sender und Empfänger- vereinbarten Schlüssel wird eine 128 Bit Kennung ("Authentication Data") berechnet und im AH eingetragen. Der Empfänger führt auf seiner Seite dieselben Operationen aus: sind seine berechneten Werte mit den übertragenen identisch, war die Authentifizierung erfolgreich. Dieses Verfahren arbeitet nur dann, wenn Sender und Empfänger denselben geheimen Schlüssel besitzen.

6.2 Verschlüsselung

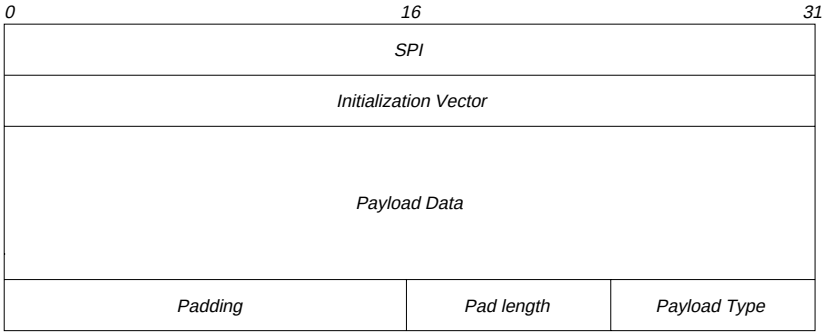


Abbildung 9: ESP-Header.

Verschlüsselung basiert auf dem "Encapsulating Security Payload"-Header (ESP-Header) (Abb. 9). SPI und Initialisierungsvektor sind unverschlüsselt, danach werden - in "Payload Data" - die kodierten Daten eingetragen. Zum Schluß folgen noch - ebenfalls in verschlüsselter Form - Füllbits ("Padding"), deren Länge und der Protokoll-Typ der Daten. IPv6 bietet 2 Modi:

- **Tunnel Modus**: Das gesamte IP-Paket (inkl. aller Header) wird verschlüsselt und ein neuer Header erzeugt. Eine mögliche Anwendung ist, daß der Knoten selbst keine Verschlüsselung vornimmt, nur spezielle Security-Gateways, die den Verkehr filtern.
- **Transport Modus**: Nur die Nutzdaten und der Destination-Options-Header werden verschlüsselt und in Payload-Data eingetragen. Ein Nachteil dieser Methode ist, daß eine Analyse des Datenverkehrs für Außenstehende noch möglich ist.

Jede Implementierung, die den ESP-Spezifikationen folgt, muß den DES-CBC[8]-Algorithmus beherrschen, der von der US Regierung spezifiziert wurde.

6.3 Authentifizierung & Verschlüsselung

Um Authentifizierung und Verschlüsselung gleichzeitig zu verwenden, gibt es 2 Möglichkeiten:

1. **Verschlüsselung vor Authentifizierung**: Die Daten werden normal verschlüsselt, je nach Typ (siehe Kapitel 6.2) wird die Authentifizierung jedoch im Zielknoten (Transport Modus) oder am Endpunkt des Tunnels (Tunnel Modus) durchgeführt.
2. **Authentifizierung vor Verschlüsselung**: Dieses Verfahren ist nur für den Tunnel Modus geeignet (Da der AH nicht im ESP-Header eingeschlossen ist, würde der Empfänger im Transport Modus die Authentifizierung fälschlicherweise über die kodierten Daten durchführen). Der AH wird in das innere Paket eingefügt und dieses dann komplett verschlüsselt.

[8]Data Encryption Standard Cypher Block Chaining

Grundsätzlich sollte man der 2.Variante den Vorzug geben: der AH wird im ESP-Header verschlüsselt, was eine Änderung unmöglich macht und zusätzlichen Schutz bietet.

7 Migration IPv4 nach IPv6

7.1 Adressierung

IPv6 definiert 2 spezielle Unicast-Adreßtypen (siehe Kapitel 2.1), IPv4-kompatible Adressen und IPv4-abgebildete Adressen, die nur dazu dienen, den Übergang IPv4 nach Ipv6 zu erleichtern. Sie bieten folgende Vorteile:

- Beide Typen erlauben eine einfache Umwandlung der IPv6-Adresse in die zugehörige IPv4-Adresse und umgekehrt, z.b. wird 1.2.3.4 zur IPv4-kompatiblen Adresse 0:0:0:0:0:0:0102:0304.
- Die auf IP aufsetzenden Protokolle (TCP, UDP, ICMP) schließen in die Berechnung ihrer Checksumme u.a. die Source-/Destination-Adresse aus dem IP-Header mit ein. Sowohl die IPv4-kompatiblen, wie auch die IPv4-abgebildeten Adressen ergeben die gleiche Checksumme wie ihre zugehörigen IPv4 Adressen. Erst diese Eigenschaft erlaubt Routern eine effiziente Umwandlung von Paketen vorzunehmen, da sie die Checksumme (des darüberliegenden Protokolls) nicht neu berechnen müssen.

7.2 Header-Umwandlung

Aufgrund der Ähnlichkeit der Protokolle ist eine einfache Umwandlung zwischen IPv4- und IPv6-Feldern möglich [Tho96]:

- Die IPv4-Header Länge erhält man aus der Länge der IPv6-Header.
- Verkehr ohne Staukontrolle (Priority größer 7) erhält in IPv4 die Priorität 0.
- TOS[9] in IPv4 wird ignoriert bzw. auf 0 gesetzt, gleichermaßen Flow Labels aus IPv6.
- Die Header-Checksumme in IPv4 muß einmal (bei Umwandlung) berechnet werden.
- Die Fragmentierung läßt sich aus dem Fragment-Header ableiten, bzw. ein fragmentiertes IPv4-Datagramm resultiert in einem IPv6-Paket mit Fragment-Header.

[9] Type of Service

7.3 Vorgehensweise bei der Einführung

In der ersten Zeit der Einführung werden sogenannte "Dual Stack"-Systeme vorherrschen, die sowohl IPv4 als auch IPv6 beherrschen. Durch Abfrage des DNS[10] kann ein solches System feststellen, ob das gewünschte Ziel IPv6 unterstützt. Ist dies der Fall und ist es am selben Link angeschlossen, oder werden IPv6-Router-Advertisements empfangen, kann ohne Einschränkung IPv6 verwendet werden. Ist kein IPv6 Router erreichbar, sollte der Knoten mit Tunneling arbeiten, d.h. das IPv6-Paket in ein IPv4-Paket einkapseln:

- **Automatisches Tunneln**: Basiert auf den IPv4-kompatiblen Adressen. Erreicht ein IPv6-Paket die Grenze eines reinen IPv4 Netzwerks, muß der Router eine Einkapselung in ein IPv4-Paket vornehmen, wobei die IPv4-Zieladresse aus der IPv6-Adresse abgeleitet wird. Das Tunnel-Ende entspricht somit dem Zielknoten, der aus dem IPv4 Paket wieder ein IPv6 gewinnt. Nachteil ist hierbei, daß jeder Knoten zusätzlich eine IPv4-Adresse benötigt.
- **Konfiguriertes Tunneln**: Ist es nicht möglich die IPv4 Adresse aus der IPv6 Adresse abzuleiten, muß der Tunnel zwischen IPv6 Routern aufgebaut werden, d.h. als Tunnel-Ende dient ein weiterer Router. Dieser Router streift den IPv4-Header wieder ab und leitet das IPv6-Paket zum Ziel weiter. Nachteil ist, daß hierzu die Router explizit konfiguriert werden müssen (welche IPv6-Adresse erfordert welchen Tunnel ?).

Ist die Einführung von IPv6 weit genug fortgeschritten, wird ein komplette Umstellung auf das neue Protokoll erfolgen, d.h. die Dual Stack Systeme werden auf Single Stack reduziert. Dennoch wird es immer noch einige reine IPv4-Systeme geben, die durch die IPv4-abgebildeten Adressen gekennzeichnet werden: Wird ein Paket an eine IPv4-abgebildete Adresse gesendet, wird es bis zum Router des Zielnetzes normal weitergeleitet. Dieser nimmt eine Umwandlung des Paketes vor, die IPv4-Zieladresse kann er aus der IPv6 Adresse ableiten.

8 Ausblick

Die Neuentwicklung von IP ist ein Meilenstein in der Geschichte des Internet - waren es bisher meist nur kleinere Änderungen und Verbesserungen ist jetzt die Möglichkeit gegeben, eine komplette Umstellung vorzunehmen. Die treibende Kraft stellt sicher der zu eng werdende Adreßraum dar, der die Notwendigkeit einer Überarbeitung deutlich vor Augen führt. Derzeit werden auf verschiedenen Systemen erste Implementierungen des neuen Protokolls getestet, eine breite Einführung und Verwendung wird für die Jahre 1998-2000 erwartet [Bra95].

[10] Domain Name System

Literatur

[Bra95] S.O. Bradner. *IPng - Internet Protocol Next Generation.* Addison Wesley. 1995.

[Bra96] Torsten Braun. Die Internet Protokollfamilie der nächsten Generation. *Praxis der Informationsverarbeitung und Kommunikation*, Juni 1996, Seite 94–102.

[S.B95] A.Mankin S.Bradner. RFC 1752: The Recommendation for the IP Next Generation Protocol. *Request for Comments 1752*, Januar 1995.

[Sta96] William Stallings. IPv6 : The New Internet Protocol. *IEEE Communications Magazine* 34(7), Juli 1996, Seite 96–108.

[Tho96] S.A. Thomas. *IPng and the TCP/IP Protocols.* Wiley Computer Publishing. 1996.

Abbildungsverzeichnis

TCPng - Aktuelle Entwicklungen im Transportbereich des Internet

Bodo Pfannenschwarz

Kurzfassung

Immer leistungsfähiger werdende Netze erfordern eine Anpassung der verwendeten Protokolle. Mit der Einführung des neuen Internet-Protokolls IPv6 müssen auch Veränderungen an dem im Internet benutzten Transportprotokoll, dem Transmission Control Protocol (TCP), vorgenommen werden.

Diese Seminararbeit beleuchtet die Eigenschaften von TCP und Probleme, die bei der Benutzung in Hochleistungsnetzwerken auftreten, und versucht, Lösungsmöglichkeiten aufzuzeigen.

Im ersten Abschnitt wird das bestehende TCP erläutert und die benutzten Mechanismen vorgestellt. Der zweite Teil zeigt Problemstellen, die bei modernen Netzen zu Leistungsverlusten führen können. Schließlich werden Lösungsansätze vorgestellt und ein Ausblick auf zukünftige Entwicklungsmöglichkeiten wird gegeben.

1 Vorstellung von TCP

1.1 Einbettung in das ISO/OSI-Schichtenmodell

Das im Internet benutzte Transportprotokoll TCP (Transmission Control Protocol) ist im ISO/OSI-Basisreferenzmodell in der Schicht 4, der Transportschicht, anzusiedeln. Die Protocol Data Units (PDUs) der Transportschicht werden auf Ende-zu-Ende-Ebene ausgetauscht.

1.2 Qualität einer TCP-Verbindung

Die Grundidee des TCP ist es, eine zuverlässige Auslieferung von Datenpaketen zu garantieren. Damit unterscheidet es sich von unzuverlässigen Transportprotokollen wie beispielsweise UDP (User Datagram Protocol). Vier Aspekte stehen im Vordergrund dieser Zuverlässigkeit: Fehlerfreiheit, gesicherte Übertragung, Reihenfolgentreue und Schutz vor Duplikaten. Die Fehlerfreiheit soll garantieren, daß beim Empfänger exakt dieselben Daten ausgeliefert werden, die vom Sender an TCP übergeben wurden. Dies wird über ein CRC-Kontrollsummenfeld im TCP-Header realisiert.

Gesicherte Übertragung bedeutet, daß TCP die Verantwortung für die Auslieferung einer von der Applikation übergebenen Nachricht beim Empfänger übernimmt. Selbstverständlich ist dies nicht immer möglich, der Empfänger könnte möglicherweise unerreichbar sein. In diesem Falle wird TCP der Sendeapplikation den aufgetretenen Fehler mitteilen.

Die Aspekte Reihenfolgentreue und Duplikationsschutz stehen in engem Zusammenhang, hier soll erreicht werden, daß - beispielsweise bei Transaktionen - die Abfolge der übermittelten Anweisungen gewahrt bleibt und jeder Befehl nur einmal zur Ausführung kommt.

1.3 Motivation eines Ende-zu-Ende-Transportprotokolls

Es stellt sich die Frage, inwieweit die vorliegenden Forderungen an das Transportprotokoll nicht bereits durch darunterliegende Schichten erfüllt werden, ob hier möglicherweise Overhead eingespart werden kann. Protokolle auf Schicht 3 können ebenfalls Mechanismen zur Fehlererkennung und Duplikationselimination bereitstellen, so daß es nicht offensichtlich ist, daß der Gesamtpfad eines Pakets, welches mehrere für sich korrekt arbeitende Subnetzwerke durchquert, am Ende nicht mehr zuverlässig sein soll.

Eine Quelle für solche Mängel stellen die Verbindungsstücke der einzelnen Netzwerkabschnitte - Router, Bridges oder Gateways - dar. Diese verfügen in der Regel über Pufferspeicher, um eintreffende Pakete zwischenspeichern zu können, falls diese in größerer Menge und Geschwindigkeit ankommen, als es das System verarbeiten kann. Da die Größe des Speichers endlich ist, kann es bei Überlastung passieren, daß Pakete verworfen werden.

Es ist zudem möglich, daß ein Paket mit korrekter Prüfsumme bei einem Router ankommt, dort im Hauptspeicher zwischengelagert und durch Soft- oder Hardwarefehler verändert wird. Da die Prüfsumme für das nächste Netzwerkteilstück erst beim Abschicken neu berechnet wird, ist diese ebenfalls korrekt und der Datenfehler kann vom Vermittlungsprotokoll nicht entdeckt werden.

Um solche Fehler aufdecken zu können, muß das Gesamtpaket an der Quelle einer Punkt-zu-Punkt-Verbindung mit einer Prüfsumme versehen werden, die auf Schicht 3 gekapselt und erst bei Ankunft an der Senke kontrolliert wird. Transportschichtprotokolle wie TCP bieten dieses Merkmal an.

2 Merkmale von TCP

2.1 Verbindungsidentifikation mittels Sockets/Ports

Hinter einem Ende einer Punkt-zu-Punkt-Verbindung befindet sich meist ein Rechensystem, welches mehrere Kommunikationsprozesse parallel abarbeiten kann, beispielsweise einen Datentransport und ein Remote Login gleichzeitig. Daher ist es wichtig, daß TCP Multiplexeigenschaften vorweist, um jeder Applikation die zugehörigen korrekten Daten ausliefern zu können.

Hierzu werden sogenannte Sockets benutzt. Sockets bestehen aus einer IP-Adresse und einer Portadresse, wobei die IP-Adresse das Rechnersystem kennzeichnet und mittels der Portnummer die verschiedenen Applikationen innerhalb dieses Systems unterschieden werden. Somit kann eine Verbindung mittels eines Socketpaars eindeutig identifiziert werden.

Viele Applikationen verwenden vordefinierte Portadressen, die per Vereinbarung zu bestimmten Applikationsprotokollen gehören. Die wichtigsten von ihnen sind in Tabelle 1 [Com88] aufgeführt:

Portnr.	Applikation
20	File Transfer Protocol (FTP) Data
21	FTP Control
23	Telnet Remote Login
53	Domain Name Service (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol (POP)
111	Remote Procedure Call (RPC)
119	Network News Tranfer Protocol (NNTP)

Tabelle 1: Vordefinierte Portadressen

Viele Anwendungen setzen auf einer Client/Server-Architektur auf. In diesem Falle warten Server üblicherweise auf Verbindungen, die ihre vordefinierte Portadresse ansprechen, während Clients die Initiative beim Verbindungsaufbau übernehmen. Hierzu müssen sie sowohl die IP-Adresse des Servers als auch die zugehörige Portadresse kennen. Im Gegensatz dazu benötigt der Server kein Wissen über die Identität des Clients im voraus.

2.2 Verbindungsaufbau / Three-Way-Handshake

Eine TCP-Verbindung ist hergestellt, wenn zwei Systeme den Verbindungsaufbauprozeß erfolgreich abgeschlossen haben. Der Verbindungsaufbau wird üblicherweise mittels eines Three-Way-Handshake durchgeführt. Der Name begründet sich daher, daß für einen erfolgreichen Aufbau drei Pakete ausgetauscht werden müssen: zuerst schickt der Initiator ein Connect-Request-Paket, welches das beantwortende System mittels eines Connect-Confirm-Pakets bestätigt. Dieses wiederum muß vom Initiator mit einem Acknowledge-Paket bestätigt werden. Erst dann können beide Systeme sicher sein, daß die Verbindung zustande gekommen ist.

Der Vorteil gegenüber dem einfacheren Two-Way-Handshake liegt in der Möglichkeit, bereits beim Verbindungsaufbau Verhandlungen über die gewünschten Eigenschaften der Verbindung führen zu können, beispielsweise Fenstergrößen oder Übertragungsgeschwindigkeiten. Zudem ist gewährleistet, daß durch Duplikate von Verbindungsaufbauwünschen keine unbeabsichtigten Verbindungen aufgebaut werden, da in diesem Falle der vermeintlichen Initiator kein Acknowledge-Paket verschickt.

2.3 Sequenznummern / Fehlererkennung / go-back-n

Nach erfolgreichem Aufbau kann die erstellte Verbindung genutzt werden, um Datenpakete über sie auszutauschen. Die Daten werden hierzu in kleine Teilstücke zerlegt und auf TCP-Pakete - sogenannte Segmente - abgebildet. Diese erhalten neben den eigentlichen Daten zusätzlich eine fortlaufende Numerierung, die Sequenznummern. Dadurch wird gewährleistet, daß TCP die korrekte Reihenfolge am Ziel rekonstruieren kann. Kommen mehrere Pakete mit derselben Sequenznummer an, so sind Duplikate aufgetreten, die verworfen werden können. Wird dagegen eine Lücke festgestellt, sind Daten verlorengegangen und es können Maßnahmen ergriffen werden, um diesen Verlust auszugleichen.

Erwähnenswert ist, daß beide an der Verbindung beteiligten Systeme unabhängig voneinander laufende Sequenznummernzähler haben, sie stehen in keiner Relation zueinander.

Um ein erneutes Senden verlorener Daten herbeiführen zu können, muß der Empfänger den Sender explizit über den Verlust informieren. Dies geschieht mittels Sequenznummernbestätigungen. Der Empfänger teilt dem Sender jeweils mit, bis zu welcher Nummer exklusive er die Pakete fehlerfrei empfangen hat. Ist diese Zahl kleiner als die des letzten Pakets, das der Sender verschickt hat, so weiß dieser, daß es zum Verlust von Daten gekommen ist und sendet die Pakete ab der entsprechenden Nummer erneut. Dieses Verfahren wird “go-back-n“ genannt.

2.4 Flußkontrolle / Sliding Window

Zu Datenverlusten kann es auch kommen, wenn der Empfänger die vom Sender geschickten Daten nicht schnell genug verarbeiten kann, und es zum Überlauf des Eingangspuffers kommt. Daher ist ein Flußkontrollverfahren notwendig, um die Senderate den Möglichkeiten des Empfängers anzupassen. Während einer Verbindung teilen sich die Systeme gegenseitig mit, in welchem Umfang sie Daten entgegennehmen können. Damit wird eine Sendefenstergröße spezifiziert. Ist der eingeräumte Sendekredit ausgeschöpft, so muß auf die Bestätigung von Paketen gewartet werden, bis erneut gesendet werden darf.

2.5 Staukontrolle / Slow-Start-Verfahren

Eine Eigenschaft des vorgestellten Sliding-Window-Flußkontrollverfahrens ist, daß zu Beginn einer Verbindung dem Sender der komplette Sendekredit zur Verfügung steht. Dies kann zum sogenannten “Jumping Window Syndrom“ führen: Wird die Maximaldatenmenge sofort gesendet, führt dies zu einer burstartigen Belastung auf dem Netz. Dadurch kann wegen Überlastung eines der Datenpakete verloren gehen, woraufhin der Empfänger keine weiteren Empfangsbestätigungen mehr verschickt. Bis der Sender dies registriert, wird er seinen Sendekredit voll ausgeschöpft haben. Sendet er nun das noch ausstehende Paket, gewährt ihm der Empfänger wiederum den vollen Kredit, da er die restlichen gesendeten Daten korrekt empfangen hat. Dies führt erneut zum Senden eines kompletten Fensters in kurzer Zeit und die Situation wiederholt sich. Dieses

Phänomen wurde häufig im Internet beobachtet und ist unter dem Namen "Congestion Collapse" [Nag84] bekannt.

Als reaktives Verfahren zur Staukontrolle wurde daher das Slow-Start-Verfahren entwickelt, das seit 1989 als fester Bestandteil von TCP akzeptiert ist [Bra89]. Ziel ist es, die Datenmengen zu Beginn eines Transfers und nach Auftreten eines Verlustes zu kontrollieren. Dazu wird neben dem bereits vorhandenen Empfangsfenster ein weiteres Fenster, das Staukontrollfenster eingeführt. Der aktuelle Sendekredit ist dann das Minimum der beiden Werte.

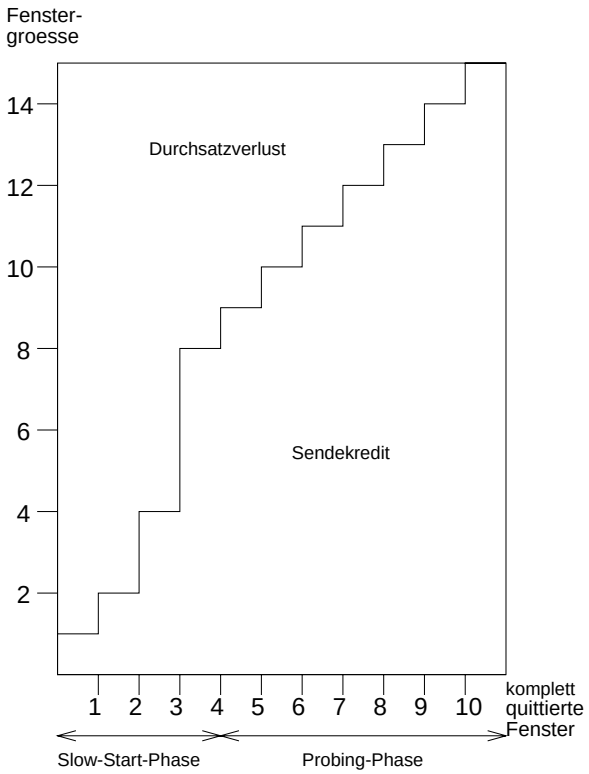


Abbildung 1: Fenstergrößen beim Slow-Start-Verfahren.

Zu Beginn einer Verbindung und nach vermutetem Datenverlust wird das Staukontrollfenster auf eine Größe von 1 gesetzt. Die Erhöhung verläuft dann in zwei Phasen: der Slow-Start-Phase und der Probing-Phase (siehe Abbildung 1). Als Grenzwert gilt die halbe Größe des Sendekredits. In der Slow-Start-Phase verdoppelt sich der Wert des Staukontrollfensters nach jedem komplett erfolgreich versandten und quittierten Fenster, bis der Grenzwert erreicht ist. Dann geht die Verbindung in die Probing-Phase über, dabei wird die Fenstergröße langsamer erhöht, nur noch um jeweils 1 nach komplett empfangenen Fenster. Dieses langsame Anwachsen dient zur sukzessiven Annäherung an die maximal verfügbare Pfadkapazität.

Da diese Erhöhung aber nicht nach oben begrenzt ist, kommt es unweigerlich zu Netzüberlastung und den damit verbundenen Datenverlusten. Dies führt zyklisch zum Zurücksetzen der Fenstergröße auf 1 und einem TCP-typischen sägezahnartigen Verlauf des Durchsatzes.

2.6 Umlaufzeitabschätzung / -messung

Um das Slow-Start-Verfahren zum Einsatz bringen zu können, müssen Datenverluste zuverlässig erkannt werden. Hierzu werden typischerweise Zeitgeber benutzt, nach deren Ablauf man die Daten als verloren betrachtet. Es ist offensichtlich, daß der dabei verwendete Grenzwert kritisch für die Effektivität des Verfahrens ist. Slow-Start reagiert sehr sensitiv gegen zu früh ablaufenden Zeitgeber. Wird fälschlicherweise von einem Verlust ausgegangen, obwohl die Dateneinheit oder Quittung noch unterwegs ist, so führt dies zu häufigem unnötigen Rücksetzen des Staukontrollfensters und zu erhöhter Netzlast, da die Daten erneut gesendet werden.

Ein zu hoch gesetzter Zeitgeber führt ebenfalls zu Durchsatzeinbußen, da tatsächliche Verluste dann zu spät erkannt werden. Um einen guten Wert für den Zeitgeber zu ermitteln, ist es wichtig, die aktuelle Netzumlaufzeit, d.h. die Zeit, die vom Senden der Daten bis zum Empfang der Quittung verstreicht, möglichst akkurat messen zu können. In RFC793 [Pos81], der Originalspezifikation von TCP, ist ein simpler Mechanismus zur Umlaufzeitabschätzung enthalten. Dieser wird heute jedoch nicht mehr eingesetzt, da er gegen Übertragungswiederholungen anfällig ist und daher falsche Werte liefert. Derzeit im Einsatz ist der von van Jacobson entwickelte Algorithmus zur Abschätzung der Umlaufzeit. Er basiert auf der Berechnung einer geglätteten Umlaufzeit SRTT (Smoothed Round Trip Time). Dabei wird die aktuell gemessene Umlaufzeit in Gewichtung mit älteren Werten gesetzt, um Schwankungen auszugleichen.

3 Probleme von TCP in schnellen Netzen

3.1 Verbindungsaufbau

Der Einsatz des Three-Way-Handshake-Mechanismus garantiert zwar einen gesicherten Verbindungsaufbau, jedoch stammt dieser aus einer Zeit mit relativ unzuverlässigen, wenig leistungsfähigen Netzverbindungen. Bei dieser Art von Verbindungsaufbau verstreicht mindestens eine volle Umlaufzeit, bis die ersten Daten übermittelt werden können. Insbesondere in einem Client/Server-Umfeld, in dem relativ oft relativ kurze, voneinander unabhängige Nachrichten ausgetauscht werden, sorgt der jedesmal stattfindende langsame Verbindungsaufbau für drastische Performanceeinbußen.

3.2 Begrenzte Fenstergröße

Im TCP-Header ist ein 16-bit-Feld vorgesehen, um dem Sender die Größe des Empfangsfensters mitzuteilen. Die maximale Größe des Fensters beträgt daher $2^{16} = 65536$ Byte.

Bei Verbindungen mit großem Bandbreite-Verzögerungs-Produkt (BVP) kann jedoch vom Sender eine große Anzahl von Datenpaketen bereits abgeschickt worden sein, bevor das erste davon den Empfänger erreicht. Eine DS1-Satellitenverbindung erreicht beispielsweise ein BVP von mehr als 1 Mbit, auch terrestrische Glasfaserbackbones fallen in diese Größenklasse. Die begrenzte Fenstergröße bildet hier eine obere Grenze für den Maximaldurchsatz.

3.3 Durchsatzeinbruch bei Übertragungsfehlern

Aufgrund des go-back-n-Verfahrens zur Fehlerbehandlung im Falle von Paketverlusten und des Slow-Start-Verfahrens zur Staukontrolle haben Datenverluste bei TCP eine große Verminderung des erzielbaren Durchsatzes zur Folge.

Bis vor kurzem führte jeder Datenverlust zu einem Leerlauf der Datenverbindung und der Durchsatz stieg aufgrund des Slow-Start-Verfahrens nur langsam wieder an. Neue Fast Retransmit / Fast Recovery - Algorithmen [Jac90b] kompensieren zwar einen einzelnen Paketverlust pro Sendefenster, falls dieses jedoch vergrößert wird, um sich der Übertragungskapazität von Hochgeschwindigkeitsnetzen anzupassen, steigt die Wahrscheinlichkeit von mehreren Verlusten pro Fenster, was wiederum einen Timeout und ein Neuanlaufen des Slow-Start-Mechanismus zur Folge hat.

Im Bereich der drahtlosen Kommunikation tritt ein weiteres Problem von Staukontrollverfahren auf. Da hier hohe Paketverlustraten zu erwarten sind, wird das Fenster des TCP-Protokolls fast nie komplett geöffnet, also ist nur ein geringer Durchsatz möglich. Durch die Eigenschaften drahtloser Verbindungen wird hier fälschlicherweise eine Stausituation diagnostiziert.

3.4 Fairneß der Staukontrolle

Das Verhalten einer Verbindung bezüglich Fairneß beim Staukontrollverfahren hängt beim Slow-Start-Verfahren wesentlich von der bei dieser Verbindung gültigen Umlaufzeit ab. Benutzer von kurzen Pfadlängen werden bei der Erkennung von Überlastungssituationen benachteiligt, da deren Umlaufzeit und damit auch ihre Zeitgeber niedrige Werte haben und daher frühzeitig ablaufen. Die Reduzierung der Last bei Lastspitzen geht also auf Kosten der Verbindungen mit kleiner RTT, während die Verbindung mit längerer Umlaufzeit davon unbehelligt bleibt.

Eine gegenteilige Situation ergibt sich bei der Wiedererhöhung eines reduzierten Sendekreditfensters. Eine Verbindung mit großer Umlaufzeit kann ihr Staukontrollfenster nur langsam vergrößern, da die Wartezeit auf die eine Erhöhung auslösenden Quittungen größer ist.

3.5 Sequenznummernüberläufe

Besonders schwerwiegende Fehler können vorkommen, wenn TCP Sequenznummern versehentlich mehrfach auftreten. Dies geschieht meist durch verspätet eintreffende Duplikate, deren Sequenznummer zufällig in das aktuelle Sendefenster paßt. In diesem Falle führt die Überprüfung der Kontrollsumme zu keiner Fehlermeldung, und es kann unbemerkt zur Verfälschung der Daten kommen.

Da für die Sequenznummer ein 32-bit-Feld zur Verfügung steht, ist die Gesamtzahl der Sequenznummern auf 2^{32} begrenzt. Dies hat zur Folge, daß früher oder später jede Sequenznummer wiederbenutzt werden muß. Die Zuverlässigkeit von TCP basiert daher auf einer Begrenzung der Lebenszeit jedes einzelnen Pakets. Ein mehrfaches Auftreten von Sequenznummern kann zwei verschiedene Ursachen haben:

(1) Überreste von früheren Verbindungen

Wird eine Verbindung beendet und sofort danach erneut eine Verbindung mit demselben Socket-Paar aufgebaut, beispielsweise nach einem Hostcrash, so könnte ein verspätetes Paket der beendeten Verbindung ankommen und im neuen Sendefenster als gültig akzeptiert werden.

(2) Sequenznummernüberlauf während einer bestehenden Verbindung.

Ist die Datentransferrate ausreichend hoch, so könnte eine Sequenznummer durch Überlauf des Zählers erneut vergeben werden, während frühere Pakete, durch Warteschlangen verzögert, noch unterwegs sind.

Tabelle 2 gibt ein Beispiel, wie lange es in verschiedenen Netzen dauert, bis der Sequenznummernvorrat aufgebraucht ist, und es zum Überlauf des Zählers kommt.

Netz	Bandbreite	Zeit bis Sequenznummernüberlauf
ARPANET	56 kbit/s	ca. 3,6 Tage
DS1	1,5 Mbit/s	ca. 3 Stunden
Ethernet	10 Mbit/s	ca. 30 Minuten
DS3	45 Mbit/s	6,3 Minuten
FDDI	100 Mbit/s	170 Sekunden
Gigabit	1 Gbit/s	17 Sekunden

Tabelle 2: Sequenznummernüberlaufzeiten in verschiedenen Netzen

Es ist offensichtlich, daß diese Grenze in langsameren Netzen wie Ethernet-LANs keine tragende Rolle spielt. Da die maximale Paketlebenszeit in der TCP-Spezifikation [Pos81] mit 2 Minuten angegeben wird, kommt man bei FDDI oder DQDB-Netzen bereits in einen kritischen Bereich, bei einem Übergang zu Gigabit-Verbindungen wird die Zeit bis zum Überlauf zu klein, um einen zuverlässigen Betrieb zu gewährleisten. Allerdings wird die effektive Bandbreite bei TCP durch das 16-bit-Sendefensterfeld begrenzt auf einen Wert von 2^{16}/RTT, wobei RTT (Round Trip Time) die Umlaufzeit in Sekunden ist.

Falls die Umlaufzeit ausreichend groß ist, wird aufgrund der dann limitierten Bandbreite die Sequenznummernüberlaufzeit keine unsicheren Werte erreichen können. Für die im heutigen Internet auftretenden Verbindungen ist dies der Fall. Problematisch wird es jedoch, wenn man ein räumlich stark begrenztes Hochgeschwindigkeitsnetz betrachtet, beispielsweise ein FDDI-LAN mit einem Durchmesser von 10km. Die RTT berechnet sich hier zu 67 Mikrosekunden, das Bandbreite-Verzögerungs-Produkt beträgt 833 Bytes. Also reicht bereits ein Sendefenster von 833 Bytes aus, um eine Verbindung mit den vollen 100 Mbit/s betreiben zu können. Der Vorrat an Sequenznummern ist dann nach knapp 3 Minuten erschöpft, dies liegt in der Größenordnung der maximalen Paketlebenszeit bei TCP und kann den zuverlässigen Betrieb gefährden.

3.6 Ungenaue Umlaufzeitmessung

Genaue und aktuelle Umlaufzeitmessungen sind wichtig, damit TCP auf sich verändernde Netzbedingungen reagieren kann. Viele TCP-Implementierungen benutzen zur

Umlaufzeitmessung lediglich ein Paket pro Sendefenster. Dies reicht bei kleinen Fenstergrößen völlig aus, führt jedoch in Hochgeschwindigkeitsnetzwerken zu schlechten Schätzungen.

Man kann das Problem der RTT-Abschätzung auf ein Signalverarbeitungsproblem zurückführen. Das Datensignal, welches gemessen werden soll - die Paketrate - wird mit einem Signal niederer Frequenz, der Fensterrate, abgetastet. Da hier Nyquists Theorem verletzt wird, kann es zu Aliasing-Effekten kommen, die die Messung stark verfälschen können.

Die Umlaufzeitmessung gestaltet sich noch schwieriger, wenn Paketverluste auftreten. Zhang [Zha86], Jain [Jai86] und Karn [KP87] haben gezeigt, daß es nicht möglich ist, zuverlässige RTT-Schätzungen durchzuführen, wenn Übertragungswiederholungen in die Schätzung mit einbezogen werden.

Da vor einer Übertragungswiederholung ein komplettes Sendefenster verschickt wird, müssen dessen sämtliche Pakete zuerst bestätigt werden, bevor ein neuer Umlaufzeitwert ermittelt werden kann, was die Abtastrate zusätzlich vermindert.

Wenn die Fehlerrate sich einem Fehler per Sendefenster nähert, beispielsweise in Satellitennetzwerken mit enormen Fenstergrößen und einer Fehlerrate von 10^{-6}/bit, wird es nahezu unmöglich, eine brauchbare Messung der RTT durchzuführen.

3.7 Begrenzte Portnummernzahl durch Time-Wait-Zustand

In Standard-TCP wird eine geschlossene Verbindung in beiden Endpunkten für die doppelte maximale Lebensdauer eines Pakets, also nach der Spezifikation für 4 Minuten, in einen speziellen Zustand, den Time-Wait-Zustand, versetzt. In diesem Zustand gilt die Verbindung als abgebaut, die Kombination der beiden benutzten Portnummern bleibt jedoch für die beteiligten Endsysteme gesperrt. Es kann keine sofortige Neuverbindung mit denselben Portnummern etabliert werden. Damit soll vermieden werden, daß verspätet ankommende Duplikate der beendeten Verbindung zu Datenfehlern bei der neuen Verbindung führen.

Werden also Transaktionen unmittelbar hintereinander ausgeführt, so muß jedesmal eine neue Portnummer verwendet werden. Die Anzahl der Portnummern ist auf 2^{16} begrenzt, so daß die Anzahl der möglichen Transaktionen pro Sekunde auf $2^{16}/240 = 273$ begrenzt ist. Dazu kommt der enorme Aufwand für die große Zahl von offenen Verbindungskontexten, die das System zu führen hat.

4 Lösungsansätze

4.1 Fensterskalierung

Um dem Problem der limitierten Fenstergröße in schnellen Netzen beizukommen, wird die Option Fensterskalierung eingeführt. Dabei wird im Optionsfeld einer SYN-Dateneinheit eine neue Basiseinheit - bisher ein Byte - zur Berechnung der Empfangsfenstergröße definiert. Da SYN-Dateneinheiten beim Verbindungsaufbau verschickt

werden, wird der Skalierungsfaktor bereits bei Beginn einer Verbindung festgelegt. Dies geschieht logarithmisch zur Basis 2, so daß die neue Fenstergröße durch einfache Shift-Operationen schnell berechnet werden kann. Steht im Optionsfeld beispielsweise eine 5, so ist die neue Basiseinheit $2^5 = 32$ Byte. Die maximale Fenstergröße wäre in diesem Fall dann $2^5 * 2^{16} = 2^{21}$ Byte = 2 MByte.

Allerdings ist der Skalierungsfaktor nach oben hin auf 2^{14} limitiert, um einen Sequenznummernüberlauf innerhalb eines Fensters zu vermeiden.

4.2 Umlaufzeitmessung mit Zeitstempeln

Ein Lösungsansatz zur Verbesserung der Genauigkeit und Zuverlässigkeit der Umlaufzeitmessung ist die Einführung der Option Zeitstempel. Der Sender muß dabei jedes Datenpaket mit einem Zeitstempel versehen, dessen Wert vom Empfänger bei der Empfangsbestätigung zurückübertragen wird (siehe Abbildung 2). Mit einer simplen Subtraktion ist es dem Sender so möglich, einen genauen RTT-Wert zu ermitteln. Dies vereinfacht zudem die Entwicklung von Protokollen, da keine aufwendigen Algorithmen implementiert werden müssen. Darüber hinaus ist dieser Mechanismus nicht anfällig bei variablen Fenstergrößen, was eine universelle Einsatzfähigkeit ermöglicht.

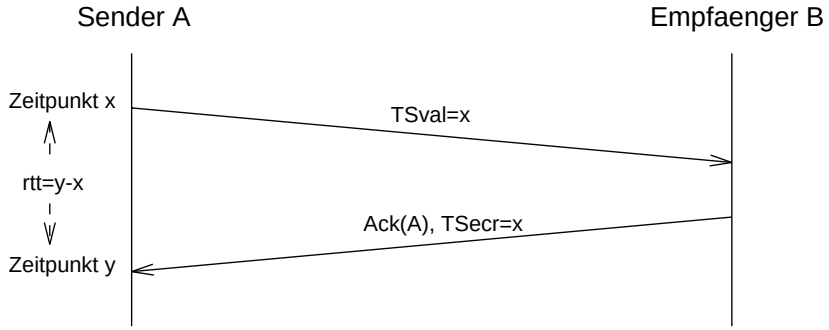


Abbildung 2: Timestamps.

Da TCP ein symmetrisches Protokoll ist, bei dem Daten jederzeit in beide Richtungen übertragen werden können, werden die Felder für den Zeitstempel und seine Rückübertragung aus Effizienzgründen zu einem Optionsfeld zusammengefaßt. Ein Problem tritt auf, wenn einer der Verbindungsteilnehmer nicht kontinuierlich Daten sendet. Nach einer Pause wird im Rückübertragungsfeld ein alter Wert mitgeschickt, der zu überhöhten Messungen führen könnte. Dies wird umgangen, indem nur solche Werte zur Berechnung herangezogen werden, die aus einem Paket stammen, mit dem neue Daten bestätigt wurden, also das ACK-Flag gesetzt ist.

4.3 Schutz gegen Sequenznummernüberlauf

Das PAWS-Verfahren (Protection Against Wrapped Sequence numbers) [JBB92] bietet einen simplen Mechanismus zum Schutz vor verspäteten Duplikaten, die eine TCP-Verbindung stören könnten. PAWS benutzt dieselben Zeitstempel wie die Umlaufzeitmessung und ist daher ohne übermäßigen Zusatzaufwand zu realisieren. Es setzt voraus, daß jedes empfangene TCP-Paket einen Zeitstempel enthält, dessen Werte in

zeitlicher Abfolge monoton steigend sind. Die Grundidee des Verfahrens ist, daß ein Paket als Duplikat erkannt und verworfen werden kann, wenn sein Zeitstempelwert kleiner ist als ein in der aktuellen Verbindung bereits empfangener Wert.

Die beiden auf Zeitstempeln beruhenden Verfahren stellen gewisse Anforderungen an den Generator der Zeitstempelwerte, um eine zuverlässige Funktion zu gewährleisten:

(1) Die Zeitstempeluhr darf nicht zu langsam getaktet sein

Sie muß mindestens einmal pro 2^{31} gesendeten Bytes erhöht werden, damit sie zur Umlaufzeitmessung tauglich ist. Sie muß pro Fenster zumindest einmal erhöht werden, da 2^{31} Bytes auch mit Skalierung der Fenstergrößen mindestens zwei Fenster belegen.

Eine mit 1 Tick/Sekunde getaktete Uhr ist bis zu Geschwindigkeiten von 8 Gbit/s geeignet, um Duplikate als verwerfbar zu erkennen.

(2) Die Zeitstempeluhr darf nicht zu schnell getaktet sein

Ihre Überlaufzeit muß größer sein als die maximale Lebensdauer eines Pakets. Da diese maximal 255 Sekunden beträgt und das Zeitstempelfeld 32 Bit groß ist, errechnet sich die maximal mögliche Uhrenfrequenz zu einem Impuls per 59 ns. Eine mit 1 kHz getaktete Uhr würde nach 24,8 Tagen zum Überlauf führen.

Aus diesen Überlegungen ergibt sich ein sinnvoller Zeitstempeluhrentakt im Bereich zwischen 1 ms und 1 s.

4.4 Header Prediction

Ein wichtiger Aspekt von Hochgeschwindigkeitstransportprotokollen ist die möglichst schnelle Abarbeitung von eintreffenden Datenpaketen. Um dies zu unterstützen, wurde eine spezielle Implementierungstechnik, Header Prediction [Jac90a], entwickelt. Dabei wird der Programmcode für den am häufigsten auftretenden Fall optimiert: korrekt und in richtiger Reihenfolge ankommende Pakete. Bei herkömmlichen Implementierungen beginnt die Abarbeitung eines eintreffenden Pakets mit der Prüfung "Liegt dieses Paket im aktuellen Fenster?". Bei Header Prediction wird dies durch die Prüfung "Ist dies das Paket, welches als nächstes kommen müßte?" ersetzt, dies ist in weniger Maschinenbefehlen zu entscheiden und ermöglicht damit kürzere Verarbeitungszeiten.

4.5 Connection Counter

Aufgrund des langsamen Three-Way-Handshakes und der Begrenzung der Portnummernzahl benutzen Client-Server-Anwendungen eher den unbestätigten Datagrammdienst UDP und fügen die für einen zuverlässigen Datentransport erforderlichen Funktionen selbst hinzu. Da dies keine zufriedenstellende Lösung darstellt, wurde Transaction-TCP (T/TCP) entwickelt, das als rückwärtskompatible TCP-Version eine für Transaktionen zufriedenstellend effiziente Verbindung bieten soll.

T/TCP führt die Option Verbindungszähler (CC, Connection Counter) ein, um den Three-Way-Handshake zu vermeiden. Dieser Zähler wird monoton steigend für jeden aktiven oder passiven Verbindungsaufbau um eins erhöht. Der Server speichert den jeweils zuletzt erhaltenen CC-Wert des Clients. Trifft nun ein SYN-Datenpaket mit

einem größeren Wert als dem gespeicherten ein, so wird das Paket einer neuen Transaktion zugeordnet und die entsprechende Verbindung wird etabliert (siehe Abbildung 3).

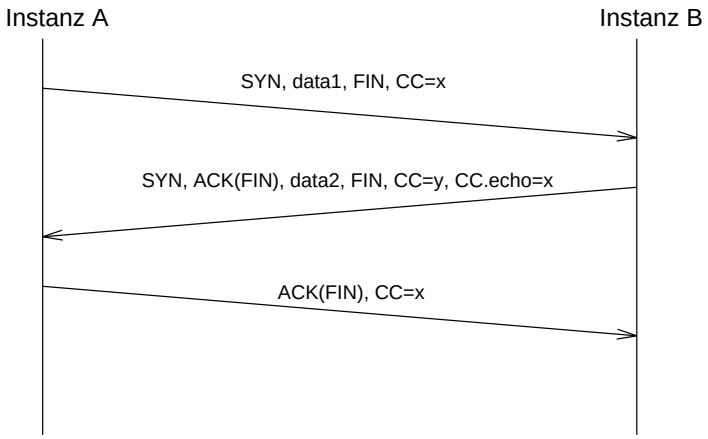


Abbildung 3: Connection Counter bei T/TCP.

Geht ein SYN-Paket mit kleinerem Zählerwert ein, so kann dies von einer Duplizierung oder Reihenfolgevertauschung hervorgerufen worden sein. In diesem Falle wird ein normaler Three-Way-Handshake durchgeführt. In normalen Paketen (SYN=0) wird der Verbindungszähler benutzt, um veraltete Duplikate früherer Verbindungen zu erkennen.

5 Ausblick

5.1 IPv6-bedingte Veränderungen

Aufgrund der rasanten Entwicklung des Internets, die eine Erneuerung des Schicht-3-Protokolls IP zu IPv6 erforderlich gemacht hat, wurde eine Diskussion über eine grundlegende Veränderung des Transportprotokolls angeregt, es sollte ein TCP für die nächste Generation, daher der Name "TCPng", ausgearbeitet werden. Wichtigster Grund für die Veränderung von TCP ist die Änderung des IPv6-Adreßformats, das bei TCP einen neue Pseudoheader zur Berechnung der Paketprüfsumme erforderlich macht.

Viele Experten tendieren aber zu umfassenden Modifikationen des Transportprotokolls, die über die notwendige Anpassung an IPv6 hinausgehen. Erweiterungen wurden dabei über die Einführung neuer Optionen vorgeschlagen, wodurch das Format der Dateneinheit an sich zunehmend an Unübersichtlichkeit zu leiden hatte.

5.2 64-bit-Feldgrößen

Durch eine Erhöhung der Feldgröße für Fenster und Zeitstempel im Header würde die eingeführte Option zur Skalierung der Fenstergröße hinfällig werden. Da das IPv6-Format auf 64-Bit-Felder ausgerichtet wurde, ist es generell sinnvoll, Sequenznummern, Zeitstempel und Fenstergrößen auf 64 Bit auszudehnen. Dies würde auch für schnellere Netze und 64-bit-Prozessoren gut geeignet sein.

5.3 Funktionale Erweiterungen

Da sich seit der Festlegung der Spezifikation von TCP viele Änderungen in Gebrauch und Umfeld von Transportprotokollen ergeben haben, erscheint es sinnvoll, selten benutzte Felder des Segmentheaders - beispielsweise den Urgent-Pointer - als Option zu definieren und dafür andere Felder wie Zeitstempel, die für das Protokollverhalten von zentraler Bedeutung sind, permanent im Kopf der Dateneinheit aufzunehmen.

Eine wirksame Kontrolle der Lebenszeit von Datenpaketen durch TCP gewinnt an Wichtigkeit, da bei IPv6 nicht mehr die Lebensdauer an sich, sondern nur noch die Anzahl der sich im Übertragungspfad befindlichen Stationen kontrolliert wird.

Weitere Änderungsvorschläge sind die Aufnahme von speziellen Bits in Quittungspaketen zur Staukontrolle und die Plazierung der Prüfsumme im Anhang einer Dateneinheit. Dies würde effizientere Implementierungstechniken wie Integrated Layer Processing ermöglichen.

Aufgrund des gestiegenen Erwartungs- und Anwendungshorizontes des Internets werden auch Überlegungen angestellt, TCP um funktionale Aspekte zu erweitern, insbesondere um mobile Endsysteme, Gruppenkommunikation und Transaktionen effizient zu unterstützen.

Literatur

[Bra89] R. Braden. *Requirements for Internet Hosts – Communication Layers, RFC 1122.* Internet Engineering Task Force. 1989.

[Com88] D. Comer. *Internetworking with TCP/IP.* Prentice-Hall. 1988.

[Jac90a] V. Jacobson. *4BSD Header Prediction.* ACM Computer Communication Review. 1990.

[Jac90b] V. Jacobson. *Modified TCP Congestion Avoidance Algorithm.* Message to end2end-interest mailing list. 1990.

[Jai86] R. Jain. *Divergenve of Timeout Algorithms for Packet Retransmissions.* Proc. Fifth Phoenix Conf. on Comp. and Comm., Scottsdale, Az. 1986.

[JBB92] V. Jacobson, R. Braden und D. Borman. *TCP Exensions for High Performance, RFC 1323.* Network Working Group. 1992.

[KP87] P. Karn und C. Partridge. *Estimating Round-Trip Times in Reliable Transport Protocols.* Proc. SIGCOMM '87, Stowe, Vt. 1987.

[Nag84] J. Nagle. *Congestion Control in IP/TCP Internetworks, RFC 896.* FACC. 1984.

[Pos81] J. Postel. *Transmission Control Protocol - DARPA Internet Program Protocol Specification, RFC 793.* DARPA. 1981.

[Zha86] L. Zhang. *Why TCP Timers don't work well.* Proc. SIGCOMM '86, Stowe, Vt. 1986.

Abbildungsverzeichnis

Tabellenverzeichnis

Charakteristiken des Multicast Backbone (MBone)

Dirk Bungard

Kurzfassung

Moderne Kommunikationsnetze sowie die hohe Komprimierung von Audio- und Videodaten ermöglichen die audiovisuelle Kommunikation und das gemeinsame Arbeiten an Dokumenten über das Internet. Neben Punkt-zu-Punkt Verbindungen bietet das MBone (Multicasting-Backbone), das auf der Internet-Infrastruktur basiert, eine effiziente Möglichkeit zur Gruppenkommunikation mit Internetprotokollen. Dieses Seminar soll die technische Realisierung des MBone, die existierenden Applikationen, sowie die Übertragungsverluste im Backbone und das Benutzerverhalten darstellen.

1 Einleitung

Die Video- und Audioübertragung in lokalen Netzen ist heute dank hoher Transferraten kein Problem mehr. Will man jedoch Videokonferenzen mit mehreren Teilnehmern durchführen und größere Distanzen im Internet überbrücken, bedarf es einer effektiven Verteilung der Datenströme in den Netzen, um so eine sichere Verbindung und eine gute Übertragungsqualität gewährleisten zu können. Hierfür wurde das MBone entwickelt, das jedoch keine fertige Lösung darstellt und somit ständig erweitert wird.

2 MBone Infrastruktur

2.1 Multicasting

Der MBone (Multicast-Backbone) ist eine Entwicklung aus den ersten zwei IETF (Internet Engineering Task Force) Audiocast Experimenten (1992), in denen live Audio und Video von der IETF Konferenz zu Empfängern auf der ganzen Welt übertragen wurde. MBone ist ein virtuelles Netzwerk, das das Internet als Basisnetz nutzt. Es werden aber statt Unicast-Paketen Multicast-Pakete übertragen. So ist es möglich, Datagrammme an eine Gruppe von Rechnern zu schicken.

Die Mitgliedschaft in einer Gruppe spezifiziert der Empfänger, wobei Gruppen anhand von Klasse-D-IP-Adressen (Tabelle 1) identifiziert werden die zwischen 224.0.0.0 und 239.255.255.255 liegen.

Durch die Verwendung von Multicast werden vor allem Weitverkehrsnetze weniger belastet als beim Versenden mit Unicast oder Broadcast (Abbildung 1). Daten werden bei diesem Verfahren nicht vom Sender, sondern von den Multicast-Routern repliziert (spart Ressourcen des Senders und der Netze).

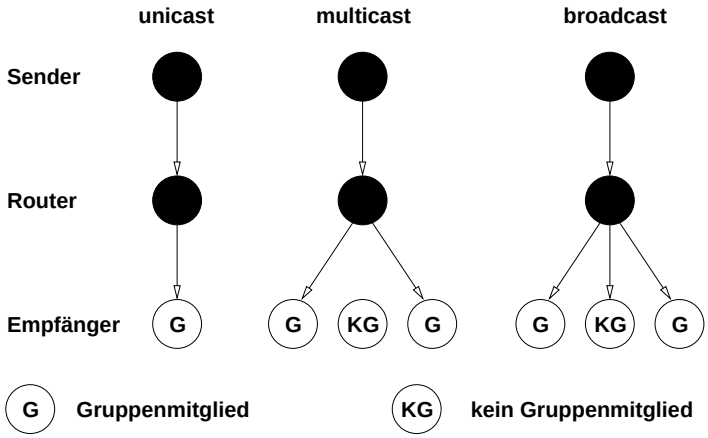


Abbildung 1: unicast, broadcast,multicast

1234 8	16	24	32	bit/Klasse
0 Netz-ID	Host-ID			A
10 Netz-ID		Host-ID		B
110 Netz-ID			Host-ID	C
1110 Host-Group				D

Tabelle 1: Klasse von Internetadressen

2.2 Der Multicast-Router

Das virtuelle Netz setzt sich aus multicastfähigen Teilnetzen zusammen, die über multicastfähige Router mit einer Punkt-zu-Punkt Verbindung über das Internet mittels sogenannter Tunnel verbunden sind (Abbildung 2).

Da herkömmlich verwendete Router im Internet Multicast-Routing zumeist nicht unterstützen, werden Mrouted (Multicast Routing Daemons) eingesetzt, die auf leistungsfähigen Workstations laufen. Hierzu existieren Implementationen für gängige Systeme wie SUN, DEC, HP, SGI, Linux.

Tunnel zwischen diesen Mroutern sind durch verschiedene Parameter spezifiziert:

- Threshold: Der Threshold gibt die maximale TTL an, die ein IP-Paket haben muß, damit es durch einen Tunnel geroutet wird
- Ratelimit: Mit dem Ratelimit wird die für die Übertragung maximal auszuschöpfende Bandbreite limitiert (typischer Wert im Campusbereich/zum nächsten Backbone-Router: 1000Kb/500Kb)
- Tunnel: hier wird der Mrouter angegeben, zu dem ein Tunnel eingerichtet ist.
- Metrik: Kostengewichtung für das Routing (1 für den Dedicated-Link (Haupttunnel) und 3 für den Backup-Tunnel (Reservetunnel bei Ausfall des Haupttunnels)

Wenn ein Sender ein Multicast-Paket versendet, entscheidet der Mrouted, ob er das Paket weiterleiten soll, packt es in ein Unicast-Paket ein und schickt es über einen Tunnel zum nächsten Mrouter. Dieser prüft dann, ob ein Rechner im lokalen Netz das

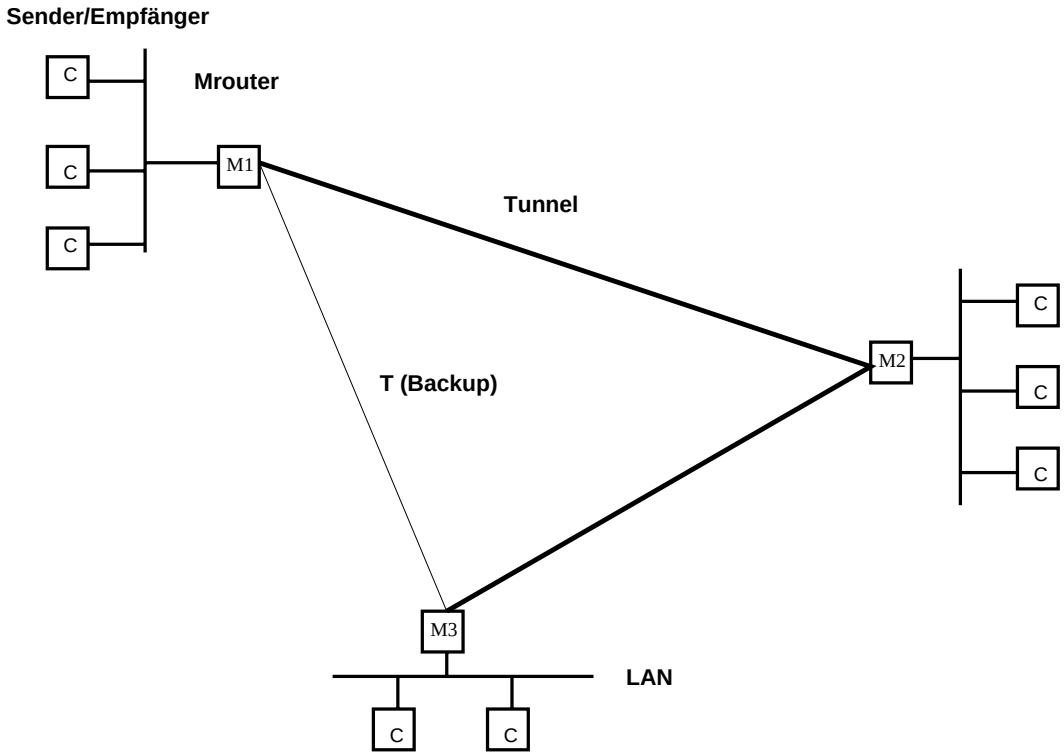


Abbildung 2: Tunnel im Internet

Paket empfangen will und routet es evtl. zum lokalen Netz, bzw. sendet das Paket zu anderen Mroutern.

Die Metrik eines Tunnels spezifiziert eine Routing Kostengewichtung, die in dem Distance-Vector Multicasting Routing Protocol (DVMRP/RFC 1075) benutzt wird. Die Metrik ist so gewählt, daß der primäre Tunnel mit einer 1 und Reservetunnel mit einer 3 gewichtet werden.

Das Threshold ist die minimale Überlebenszeit (TTL = time to live), die ein Multicast Datagramm haben muß, um durch einen gegebenen Tunnel gesendet zu werden. Jedes von einem Sender gesendete Multicast-Paket erhält eine bestimmte TTL, die beim Durchlauf durch jeden Mrouter um 1 erniedrigt wird. Wenn nun die TTL kleiner ist als das Threshold des Tunnels, durch die es vom DVMRP geschickt werden soll, wird es nicht weitergeleitet, um so den Umfang (Reichweite) der Multicast Übertragung zu limitieren. In früheren Versionen gab es Probleme, da alle Pakete zu jedem Mrouter geroutet wurden, heute werden jedoch Pakete, die von keinem Empfänger benötigt werden nicht weitergesendet, und der sendende nahegelegene Mrouted benachrichtigt, daß er keine weiteren Pakete mit dieser Adresse mehr schicken soll (pruning). Werden wieder Pakete benötigt, so fordert der Mrouted-Host dieses bei seinen benachbarten Mroutern an (Abbildung 3).

2.3 Protokolle für Multicast Routing

Um Schleifen zu vermeiden und die effiziente Verbreitung der Multicast-Daten zu erreichen, werden spezielle Multicast-Routing-Protokolle eingesetzt. Das wichtigste Protokoll ist das Distance Vector Multicast Routing Protocol (DVMRP), das auf dem

Distance Vector Algorithmus (DV) mit Reverse-Path Broadcasting (RPB) basiert. Multicast-Pakete werden bei dieser Variante nicht über den Weg, auf dem sie zum Router gekommen sind, weitergeleitet.

Die aktuelle Implementation von DVMRP unterscheidet sich jedoch von der in RFC-1075 spezifizierten Version (unterschiedliches Paket-Format, Tunnel-Format, zusätzliche Paket-Typen,...).

Router sowie Sender und Empfänger im MBone verständigen sich mittels IGMP (Internet Group Multicast Protocol). Der Mrouter sendet periodische Quer-Nachrichten mit der TTL 1 an die All-Host-Gruppe (224.0.0.1), der jeder multicastfähige Rechner zugehört. Diese melden dann per IGMP mit der TTL 1 einen Host-Membership-Report an die angeschlossenen Gruppen. Die anderen Rechner der Gruppe G hören diesen Report und können ihre Timer zurücksetzen. Der Multicast-Router wertet diese Reports aus und legt so z.B. einen Datenstrom auf das lokale Netz, bzw. fordert Daten beim nächsten Mrouter an.

Durch das Versenden von Prune-Nachrichten eines Routers können Zweige erkannt werden, die keinen Bedarf am Empfang einer Gruppe haben (Abbildung 3). Ist wieder Bedarf vorhanden, wird eine Graft-Nachricht versendet, die dem Mrouter signalisiert, daß er wieder Daten senden soll (Abbildung 3).

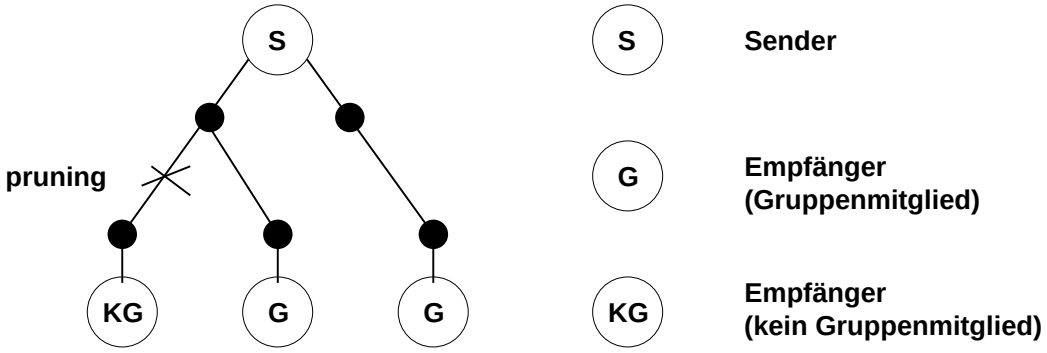


Abbildung 3: Pruning im MBone

Normale Router im Internet, die das Protokoll MOSPF (Multicast Open Shortest Path First, eine Erweiterung zu OSPF) unterstützen, können IP-Multicast-Pakete ohne Tunnel direkt weitersenden (z.B. CISCO Router). MOSPF und DVMRP können zusammen interoperieren. So kann von einem Mrouted direkt ein Tunnel zu einem MOSPF-fähigen Router betrieben werden.

2.4 Probleme im MBone

Bei der Übertragung im MBone werden verbindungslose Protokolle verwendet, bei denen Datenverluste in Kauf genommen werden müssen. Die verwendeten Protokolle (UDP/RTP) nehmen die Bandbreite in Anspruch, die sie benötigen. So kann es zu Engpässen mit anderen Anwendungen im Netz kommen.

Aus Unwissenheit wird die TTL einer Sendung oft zu hoch gesetzt. Es sollten Werte gewählt werden, die die Sendung auf den Zuhörerkreis beschränken, für den die Übertragung interessant ist.

Die einzige Möglichkeit die Ausbreitung von Multicast-Datagrammen zu begrenzen, ist die Verwendung eines Thresholds. Wenn ein Datagramm eine TTL größer als ein Threshold hat, wird es durch den Tunnel gesendet (Thresholds zwischen 0 und 255). So wird eine lokale Konferenz lokal gehalten und die Videobandbreite mehr als die Audiobandbreite begrenzt.

Das MBone erfährt zur Zeit einen starken Boom. Durch den so entstehenden hohen Netzverkehr stoßen viele Multicast-Router an ihre Leistungsgrenzen oder sind bereits überlastet. So kann es vorkommen, daß Pakete beim Ausfall oder Überlastung eines Routers einen sehr ineffizienten Weg nehmen oder ihr Ziel nicht erreichen. Durch die rasche Ausweitung des Netzes müssen Tunnel manuell rekonfiguriert werden. Abhilfe schafft hier die Implementierung von Multicast Routing in normale Internet-Router, die es dem Multicast-Routing ermöglicht dem Unicast-Routing zu folgen.

2.5 MBone Applikationen

Als Transportprotokoll werden im MBone verbindungslose Protokolle mit einem transparenten Transport-Level-Umschlag um ein IP-Paket (UDP/RTP User Datagramm Protocol/Real Time Protocol) verwendet. Bei RTP, entwickelt von der Audio-Video Transport Working Group (IETF intern) erhält jedes Paket eine Timing und Sequencing Information, die einen kontinuierlichen Datenfluß beim Empfänger ermöglichen. Schwankungen im Netz machen sich dadurch nicht so störend bemerkbar.

TCP (Transport Control Protocol) zu verwenden ist weniger sinnvoll, da man um einen gleichmäßigen Datenfluß zu erreichen nicht jedes verlorengegangene IP-Paket beim Sender neu anfordern kann. Um einen sicheren Multicast Transportdienst im MBone zu realisieren, müssen jedoch noch neue Protokolle entwickelt werden.

Traffic type	TTL	Kb per second	threshold
GSM audio 1	255	15	224
GSM audio 2	223	15	192
PCM audio 1	191	75	160
PCM audio 2	159	75	128
Video 1	127	130	96
Video 2	95	130	64
local event audio	63	≥ 250	32
local event video	31	≥ 250	1

Tabelle 2: IETF Transmission Plan

Audiodaten im MBone werden im PCM verfahren (Pulse Code Modulation) mit 8 KHz und 8-bit Auflösung kodiert, was eine Bandbreite von 64Kb ohne Overlay erfordert. Benutzt man den Cellular-Phone Standard (GSM= Group Special Mobile), so kann die Bandbreite bis auf 18 Kb pro Sekunde (incl. Overlay) verringert werden. Video wird überwiegend nach dem CCITT (Consultative Committee of International Telephone and Telegraph) H.261 Standard übertragen (siehe auch Tabelle 2). Für Konferenzen im MBone existieren verschiedene Programme, die mittlerweile für alle gängigen Workstation sowie für Windows verfügbar sind. Bei den vorgestellten Applikationen kann die Übertragung auch verschlüsselt erfolgen.

SDR

Der Session Director (SDR), entwickelt am UCL (MICE/University College London) gibt eine Programmübersicht über Konferenzen. Er zeigt die aktuellen MBone-Sendungen an, ermöglicht das komfortable Ankündigen und Starten einer eigenen Session und startet die entsprechenden Applikationen. Eine MBone-Sendung wird mit dem SDR angekündigt. Dabei werden freie Multicast-Adressen und UDP-Ports für die geplante Sendung reserviert.

2.5.1 VIC

Das Video Conferencing Tool (VIC) ist ein Tool zur Videoübertragung und ermöglicht Videokomprimierung nach dem H.261 Standard. Das Tool bietet eine Vielzahl von Funktionen, wie etwa den Voice-Switched-Mode, bei dem das Videobild des gerade sprechenden Konferenzteilnehmers angezeigt wird.

2.5.2 VAT

Das VAT (visual audio tool) wurde von Steve McCanne und Van Jacobsen am Lawrence Berkley Laboratory entwickelt. Das Audiotool beinhaltet verschiedene Audio-CODEC wie PCM, PCM2, PCM4, und GSM. Neben der Übertragung bietet vat viele Funktionen zur Steuerung der Audioübertragung. Es können z.B einzelne Teilnehmer stummgeschaltet werden und während einer Konferenz kann mit einem Mausklick ein Privatgespräch mit einem Teilnehmer begonnen werden, welches dann unicast übertragen wird.

2.5.3 RAT

Das Robust Audio Tool wurde wie der SDR am University College London entwickelt. Programmautoren sind Vicky Hardman und Isidor Kouvelas. Ein neues, sehr interessantes Feature dieser Anwendung ist die Redundancy (Packet Loss Protection). Bei Paketverlust wird hier nicht ganz stumm geschaltet, sondern es wird ein zweites Audiopaket (mit geringer Bandbreite) abgespielt, das an ein vorheriges Audiopaket angehängt ist. Somit wird die Audioübertragung qualitativ verbessert. Das RAT besitzt auch einen Modus, in dem es voll kompatibel zum VAT 4.0 ist.

2.5.4 WB

Das WB (White Board) entwickelt von Steve McCanne und Van Jacobsen am Lawrence Berkley Laboratory ist ein Tool ähnlich einem Overheadprojektor. Man kann mit ihm alleine oder mit mehreren Teilnehmern in einem Dokument schreiben und zeichnen. Es besitzt Importmöglichkeiten für Text und Postscript-Dokumente, so daß Vortragsfolien importiert werden können, die dann synchron bei allen Teilnehmern angezeigt werden.

3 Sendungen im MBone

Das MBone ist vor allem für die Forschung ein wichtiges Medium geworden. Wissenschaftler aus aller Welt nutzen multimediale Kommunikationsmittel für virtuelle Konferenzen, um Zeit und Reisekosten zu sparen.

Neben der privaten Nutzung wird im MBone eine Vielzahl von Sendungen übertragen, die für ein breites Publikum interessant sind. Zu den Highlights gehören die weltweit ausgesendeten aktuellen Spaceshuttle-Missionen sowie Seminare der IETF (Internet Engineering Task Force).

In Deutschland werden Vorlesungen und Seminare über das MBone übertragen (Teleseminar Digitales Geld zwischen Mannheim, Karlsruhe und Freiburg; Bill Gates an der Uni Karlsruhe und Veranstaltungen aus dem Multimediahörsaal der Uni Karlsruhe). Bei einem Projekt an der Uni Erlangen und Nürnberg werden Vorlesungen die nicht am jeweiligem Ort angeboten werden, abwechselnd übertragen, um so Fahrtkosten einzusparen.

3.1 Wo entsteht Datenverlust?

Um die Fehlerraten von Sendungen im Backbone zu untersuchen, haben Maya Yajnik, Jim Kurose und Don Towsley vom Computer-Science Departement der Universität Massachusetts in Amherst die Fehlerrate bei 17 Empfängern in den USA und Europa bei verschiedenen Audio-Übertragungen ermittelt.

Als Sendungen wurden das World Radio Network (WRN) (5 Kbits Daten pro Audiopaket in 80ms Intervallen), die Übertragung des UC Berkeley Multimedia Seminar (UCB) aus Californien (alle 40ms ein Audiopaket mit 2,5 Kbits pro Paket) und Radio Free VAT (RFV aus Californien) (80ms Intervall am 19.4.1996/40ms Intervall am 8.5.96) ausgesucht.

Um die für die Auswertung nötigen Daten zu erhalten, wurden bei den Empfängern Programme eingesetzt, die auf der entsprechenden Multicast-Adresse und Port lauschten, die ankommenden Vat-Headers der Pakete mit einem Zeitstempel versahen und aufzeichneten. Nach der Aufzeichnung, die durch ein zentrales Programm gestartet wurde, wurden die gesammelten Daten per FTP zu einem zentralen Rechner übertragen.

Insgesamt fanden 14 Experimente mit unterschiedlicher Zeitdauer zwischen 15 und 99 Minuten statt.

Mit den gesammelten Daten lassen sich Aussagen über den Verlust von gleichen Paketen bei verschiedenen Empfängern und den temporären Verlust von Daten bei einzelnen Empfängern machen.

3.2 Auswertung

Man kann 2 unterschiedliche Arten von Datenverlust bei allen Empfängern unterscheiden: 1. Die Anzahl von Empfängern, die kontinuierlich ein gegebenes Paket nicht empfangen. Diese Ergebnisse werden anhand von 3 Netztopologien untersucht. 2. Die

Kovarianz eines verlorengegangenen Paketes für ein Paar von Empfängern. Sie gibt einen räumlichen Zusammenhang im MBone wieder.

Mit Mtrace und Mrinfo wurde der Multicast-Baum für die Sender und Empfänger ermittelt.

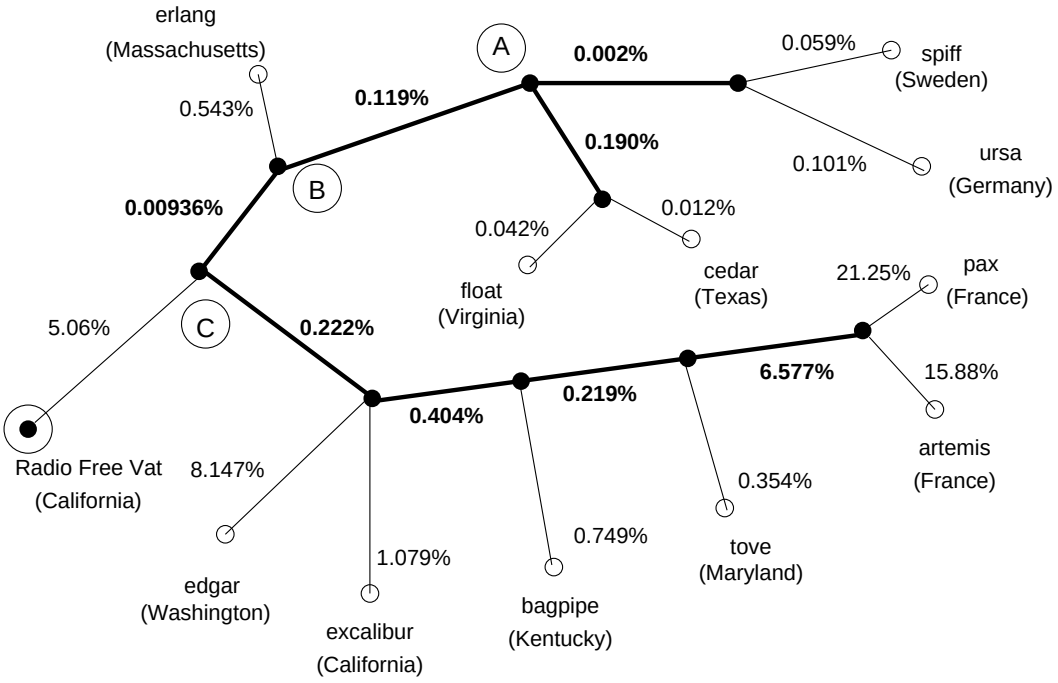


Abbildung 4: Multicast Baum (Fehlerrate auf jedem Link)

Die Wahrscheinlichkeit eines Paketverlustes zwischen einem Punkt A (N_A) und B (B_A) ergibt sich aus:

$p_A = \frac{N_A - N_B}{N - N_B}$

N: Gesamtzahl der gesendeten Pakete
N_A: Anzahl der bei A (abwärts) verlorengegangenen Pakete
N_B: Anzahl der bei B (abwärts) verlorengegangenen Pakete

So läßt sich der Paketverlust für jeden Link im Multicast-Baum errechnen.

Da der durchschnittliche Datenverlust im Backbone mit 2% im Vergleich zum Datenverlust bei den Empfänger (bis zu 21% zwischen USA und Frankreich) recht niedrig liegt, erscheint das Neuanfordern von nicht korrekt empfangenen Paketen bei einem benachbarten Empfänger sinnvoll.

Desweiteren treten periodische Datenverluste in Intervallen von 0,6 s und 30 s auf, wofür das Routingupdate der Multicastrouter verantwortlich ist.

Der Datenverlust zwischen Mrouter und Empfänger im lokalem Netz (Ethernet) kann vernachlässigt werden, da die Fehlerrate hier zwischen 0% - 0,001% liegt.

Ein Test am 19. April, um herauszufinden wie viele Empfänger kontinuierlich ein Paket nicht korrekt empfangen, ergab, daß 47% eines Paketes von mindestens einem Empfänger nicht richtig empfangen wurden. Diese Verteilung der Datenverluste wurde anhand von 3 Modellen untersucht (Abbildung 5).

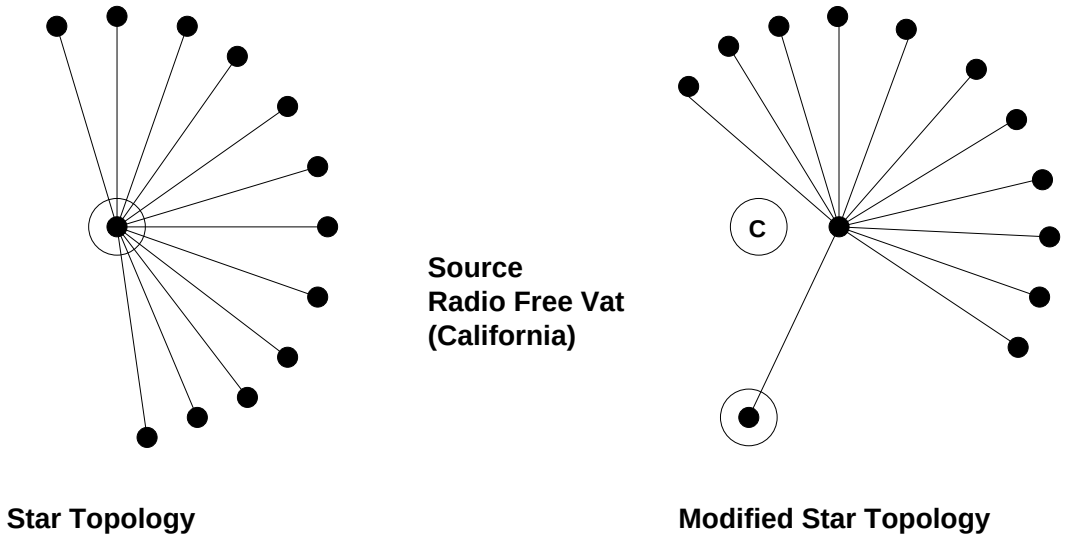


Abbildung 5: Netz-Topologien

1. Star Topology

   Es wird angenommen, daß der Paketverlust räumlich (für mehrere Empfänger) und temporär (Verlust bei einzelnen Empfängern) unabhängig ist. Die gemessene Wahrscheinlichkeit des Datenverlustes der Empfänger wurden benutzt, um die effektive Transferrate des Senders zu errechnen.

2. Full Topology

   Es wird angenommen, daß Paketverluste bei mehreren Empfängern korreliert sind (siehe Abbildung 4). Die effektive Transferrate berechnet sich aus den Verlusten der einzelnen Links (Bottom-UP).

3. Modified Star Topology

   Die Wahrscheinlichkeit für einen Datenverlust vom Sender zum Knoten C setzt sich zusammen aus den Paketverlusten der einzelnen Empfänger. Für den Rest der Verluste nimmt man räumliche Unabhängigkeit an.

Ergebnis:

Das erste Modell scheint ungeeignet, da es stark von der Realität abweicht. Das 2. Modell kommt der Realität sehr nahe und das dritte Modell ist in 9 von 14 Fällen eine gute Annäherung (Abbildung 6). Das bedeutet, daß die MBone Topologie der Modified Star Topologie entspricht und daß die Wahrscheinlichkeiten für Paketverlust im MBone im Vergleich zu Datenverlust nahe dem Sender sehr gering sind.

3.3 Räumliche Zusammenhänge der Datenverluste

Die Kovarianz für ein Paar von Empfängern gibt ein Maß über die Verbindung zwischen ihnen an, und die durchschnittliche Kovarianz für alle Paare von Empfängern in einer Meßreihe ist ein allgemeines Maß für den Verlust der gleichen Pakete im gesamten MBone. Sie ist gleich der Differenz der gemessenen Wahrscheinlichkeit der verteilten

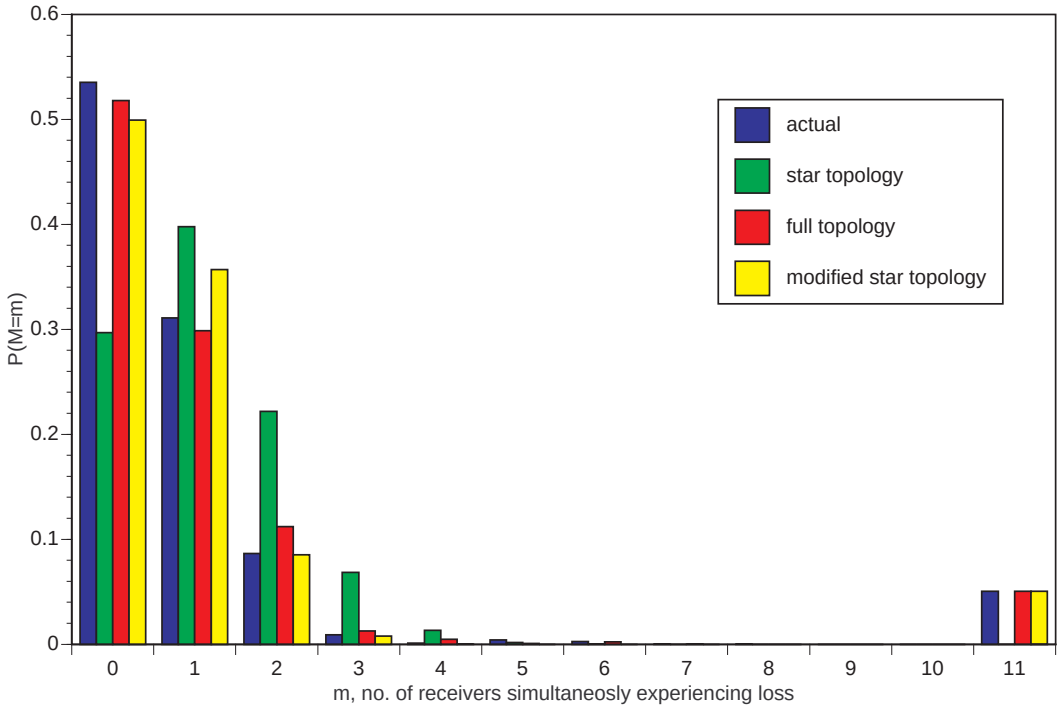


Abbildung 6: Wahrscheinlichkeiten für gleichzeitigen Paketverlust bei mehreren Empfängern

Verluste im Backbone und der berechneten Wahrscheinlichkeit wenn Unabhängigkeit angenommen wird.

Sie ist für 2 Empfänger i und j definiert als:

$$\begin{aligned} cov(X_i, X_j) &= E[(X_i - \overline{X_i})(X_j - \overline{X_j})] \\ &= \frac{S(i,j)}{N-1} - \overline{X_i X_j} \end{aligned}$$

N:	Anzahl der Pakete, die vom Sender gesendet wurden
$S(i,j)$:	Anzahl der Pakete, die von Empfänger i und j nicht korrekt empfangen wurden
X_i:	eine binäre Zufallsvariable 1 für Paket Verlust bei i 0 für korrekter Empfang beim Empfänger i
$\overline{X_i}$:	„let X_i be the mean of the variable X“
$(\overline{X_i X_j})$:	Wahrscheinlichkeit, daß i und j simultan ein Paket nicht empfangen, angenommen, daß die Verluste unabhängig voneinander sind
$cov(X_i, X_j) = 0$:	X_i und X_j sind gewiß unabhängig
$cov(X_i, X_j) > 0$:	Verluste bei i sind positiv korreliert zu Verlusten bei j D.h., daß das Paket, das bei i verlorengeht auch bei j nicht korrekt empfangen wird
$cov(X_i, X_j) < 0$:	bei negativer Korrelation

Ergebnis:
Die durchschnittliche Kovarianz variiert zwischen 0,0118 und 0,0776. Die Kovarianz

ohne den Datenverlust nahe dem Sender nimmt Werte zwischen 0 und 0,0214 an. Zusätzlich weist der Link nahe zum Sender (Abbildung 4) mit 5% Verlustwahrscheinlichkeit einen hohen Wert auf. Daraus läßt sich folgern, daß der größte Anteil der Verluste nahe dem Link zum Sender liegt.

3.3.1 Temporäre Verluste bei einzelnen Empfängern:

Bei der Untersuchung des temporären Verlustes von Paketen bei einem einzelnen Empfänger kann man die beobachteten Werte der Übertragungsverluste in 3 Kategorien einteilen:

1. Länge: 1-6 Pakete: 0,08 s - 0,48 s
2. Länge: 7-10 Pakete: 0,6 s
3. Länge: >100 Pakete: 8 s - 3 min

Die meisten Unterbrechungen dauern nur 1-6 Pakete an. Datenverlust von 7-10 Paketen wurde bei einigen Empfängern beobachtet und Verluste bei Paketlängen größer 100 traten häufig auf.

Diesen Ergebnissen liegen die Daten vom 11. Dezember 1995 zugrunde (WRN/80ms Pakete Intervall)

Machine Name	Loss Rate	No. of Bursts	Avg. Length	Coef. of Var.	Median Length	75 %	99 %	Length of longest burst	perc. of loss in long bursts (>100)
alps	5,93%	3427	1,210	2,912	1	1	3	179	4,3%
anhur	5,15%	3387	1,065	0,253	1	1	2	4	0,0%
cedar	14,22%	7463	1,333	0,826	1	1	8	14	0,0%
collage	9,08%	5508	1,155	2,069	1	1	3	175	2,75%
erlang	10,41%	3793	1,921	21,30	1	1	4	2518	34,6%
float	10,44%	6470	1,129	0,367	1	1	3	7	0,0%
law	12,09%	4983	1,698	21,001	1	1	3	2518	29,8%
pax	16,98%	7633	1,557	19,134	1	1	3	2603	21,9%
tove	5,46%	3486	1,097	0,407	1	1	3	10	0,0%

Tabelle 3: Burstiness of Loss for the WRN source on Dec 11, 1995

Der Variationskoeffizient (Coef. of Var) für die temporären Verluste ergibt sich aus der Standardabweichung geteilt durch den Mittelwert. Er ist ein Maß für die relative prozentuale Streuung der Burstlängen im Vergleich zu ihrem Mittelwert (unabhängig von der Burstlänge).

$$c = \frac{\sqrt{E[(b-\overline{b})^2]}}{\overline{b}}$$

b: Burstlänge oder Anzahl der fortlaufenden Verluste
$\overline{b}$: durchschnittliche Burstlänge

Beide Analysen zeigen, daß für die meisten aufgezeichneten Daten die räumlichen Zusammenhänge der Paketverluste im Netz sehr gering sind. Es gibt allerdings Übertragungseinbrüche von einigen wenigen Sekunden bis hin zu einigen Minuten.

3.4 Benutzerverhalten im MBone

Kevin C. Almeroth und Mostafa H. Ammar der Network Telecommunications Group am College of Computing, Georgia Institute of Technology in Atlanta haben das Benutzerverhalten im MBone mit einem entwickelten Tool untersucht.

Scannen und Filtern von Paketen

Auf einem Rechner in einem Ethernet läuft ein Audiotool (VAT) und auf einem weiteren Rechner im selben Segment das entwickelte Meß-Tool (modifiziertes Etherfind-Tool), das Daten über verschiedene Sessions sammelt und speichert.

Das Tool filtert die Empfänger-IP-Adresse und UDP-Port aus dem Datenstrom heraus und ruft eine Funktion zur Weiterverarbeitung der Daten auf, wenn die Empfänger-Adresse und Port mit der zu überwachenden Session übereinstimmen.

Aufzeichnen von Session-Name Paketen

Für jede aktive Verbindung sammelt das Tool

- die IP-Adresse des Empfängers
- UDP Port und Nummer, auf dem empfangen wird
- Datum und Zeit des Starts
- Status der Verbindung (aktiv/nicht aktiv)
- letztes Datum und Zeit, wann ein Paket zuletzt empfangen wurde
- Anzahl der empfangenen Pakete
- Datum und Zeit beim Beenden

Verbindungsende der Empfänger

Es ist nicht unproblematisch, das Verbindungsende eines Empfängers genau zu ermitteln, da Kontroll-Pakete evtl. verlorengehen oder aber ein Teilnehmer die Konferenzapplikation nicht ordnungsgemäß beendet und so keine Nachricht für das Verlassen der Gruppe gesendet wird. Um dennoch das Verlassen einer Gruppe und erneutes Empfangen zu erkennen, benutzt das Meßtool einen Zeitschwellwert von 1,5 Minuten. Somit wirken sich auch Übertragungsstörungen nicht so stark auf die Meßreihe aus.

Anlegen von Records- und Logfiles

Das Tool führt alle 30 Sekunden ein Update der aufgezeichneten Daten durch. Ist eine Verbindung beendet, wird im Logfile neben Name des Empfängers, der Start und Endzeit, auch die Zeit des letzten Empfangs aufgezeichnet, um so später Rückschlüsse auf Datenverlust im Netz oder das nicht ordnungsgemäße Beenden des Konferenzprogrammes ziehen zu können.

Beim Auswerten der Daten mußte beachtet werden, daß es im MBone zu hohen Datenverlusten auf einigen Übertragungsstrecken kommen kann, Kontroll-Pakete nicht rechtzeitig empfangen werden, Mrouter nicht am Netz sind und daß im MBone viel getestet wird. Um ein gutes Ergebnis zu erzielen wurden die Daten von Empfängern, die sehr häufig einer Gruppe zugehören und sie dann wieder verlassen, herausgefiltert.

Um das Beenden einer Verbindung zu überprüfen, wird das Logfile nach verschiedenen Verbindungsaufzeichnungen mit der selben IP-Adresse und UDP-Portnummer durchsucht. Werden 2 Verbindungen gefunden, bei denen die End- und Startzeit nicht weniger als 5 Minuten betragen, werden die beiden Datensätze für die gleiche Verbindung gewertet.

Werden keine Empfänger mehr angezeigt, läßt das auf den Ausfall eines Links schließen. Problematisch ist auch, daß MBone-Tools häufig mehrmals gestartet werden, da der SD (Session Director) nicht anzeigt, daß die Tools bereits gestartet wurden.

Durch das Ausfiltern von Daten nach oben genannten Kriterien kann man etwa bei der Aufzeichnung der STS-63 Space-Shuttle Mission die Anzahl der beobachteten Verbindungen von 8229 auf 5055 reale Verbindungen reduzieren .

Untersucht wurde das Benutzerverhalten bei der STS-63 Space-Shuttle Mission (3.2.95-13.2.95), dem UCB Multimediaseminar (17.2.95), dem IPNG Working Group Meeting (9.2.95-11.2.95) und beim IMS World Radio Network (21.6.95-31.6.95).

3.5 Auswertung

Benutzerverhalten

STS-63 Space Shuttle Mission Die Spaceshuttle-Missionen gehören zu den beliebtesten MBone-Sendungen. Man beobachtet bis zu 200 Empfänger wobei die Aktivitäten hier während normaler Arbeitsstunden zwischen Montag und Freitag besonders hoch sind und sich periodisch im 24 Stundenzyklus wiederholen.

Besonders viele Zuschauer gibt es bei Landung und Start des Shuttle sowie bei besonderen Ereignissen (Rendevouz Shuttle-Mir).

Bei der räumlichen Betrachtung der Empfänger kann man feststellen, daß das Join/Leave-Verhalten trotz unterschiedlicher Zeitzonen, zeitunabhängig ist (immerhin sind 50% der Zuschauer nicht aus den USA).

Auffällig ist das andauernde Join/Leave-Verhalten, wenn nichts besonderes passiert.

Ein Empfänger sieht die Shuttle-Mission im Durchschnitt 21 Stunden und im Mittel (Median) 62 Minuten lang (4,2 Verbindungen) wobei er pro Verbindung durchschnittlich 5 Stunden und im Mittel (Median) 6,2 Minuten lang die Sendung sieht. Aus der

Differenz der Zeit pro Verbindung und der Gesamtzeit läßt sich schließen, daß Empfänger die sich nur kurz zuschalten, später wiederkehren.

IMS Beim IMS World Radio Network bewegt sich die Zuhörerzahl zwischen 15 und 30 und vom 26. Mai (Freitag) bis 29. Mai (Montag), einem nationalem Feiertag in den USA, gab es eine konstante Zahl von Zuhörern, die diese Sendung ständig empfangen haben.

IPNG Das IPNG Working Group Meeting wurde an 2 Tagen für einige Stunden übertragen. Interessant ist hier, daß die Teilnehmerzahl nach dem ersten Tag zwar abgenommen hat, jedoch viele der Multicastgruppe weiterhin angehören, anstatt sich am nächsten Tag erneut zuzuschalten.

Seltsamerweise waren auch nach dem Ende des zweiten Tages eine größere Anzahl von Empfängern in dieser Multicastgruppe anwesend, obwohl das Meeting beendet war.

UCB Die Übertragung des UCB Multimedia Seminar kann mit einem Kinofilm verglichen werden. Nahezu alle Teilnehmer gehören der Multicastgruppe kurz vor Beginn der Sendung an und verlassen sie am Ende nahezu gleichzeitig.

Während der Übertragung schalten sich einige Empfänger nur für kurze Zeit ein, was sich durch die schlechte Übertragungsqualität und durch die Neugierde der Zuschauer erklären läßt. Jeder Zuhörer dieser Sendung hat sich im Mittel 2,3 mal zugeschaltet. Pro Verbindung sah ein User diese Sendung durchschnittlich 46 Minuten (Median: 7 Minuten) und insgesamt 105 Minuten (Median: 88 Minuten) lang.

Multicast-Baum-Kostengewichtung

Mit den aufgezeichneten Daten (IP-Adresse der Empfänger) lassen sich Aussagen über die Größenänderungen des Multicast-Baumes während einer Sendung machen.

Zusätzlich wurde die Summe aller Paket-Hops zu jedem Empfänger gebildet (mit Mwatch-Tool) , um eine Kostengewichtung des MBone im Vergleich zur Unicast-Übertragung über das MBone und der Multicast-Übertragung von einem anderen Standort aus (Georgia Tech (GT)) machen zu können.

Um etwas über ein in naher Zukunft verfügbares, voll multicast-fähiges Internet aussagen zu können, wurden mit traceroute die kürzesten Wege (Hops) zu jedem Empfänger von Georgia Tech aus ermittelt.

Ergebnis:

IMS

- Trotz starker veränderlicher Zuhörerzahl variiert die Multicast-Kostengewichtung nicht, die Unicast-Kostengewichtung schwankt jedoch beträchtlich.

Session	Mbone Topology Original Source		Mbone Topology GA Tech Source		Internet Topology GA Tech Source	
	Average	Maximum	Average	Maximum	Average	Maximum
IMS	11,0	25	8,6	22	17,3	30
UCB	8,8	21	7,1	14	16,8	23
STS-63	7,1	17	7,5	15	17,4	30

Tabelle 4: Average and maximum path length for the multicast sessions

- Die Kostengewichtung der Multicast-Übertragung über das MBone beträgt nur 35,7% der Kostengewichtung, wenn man unicast über das MBone übertragen würde.
- Wenn man Georgia Tech als Source betrachtet gibt es keine großen Veränderungen, weil IMS nahe GT sendet.
- Die Multicast-Kostengewichtung über das Internet (alle Router sind multicastfähig) wäre 2,0 mal so hoch wie die Übertragung über das vorhandenen MBone.

UCB

- Trotz Verdoppelung der Empfänger steigt die MBone-Multicast-Kostengewichtung nicht stark an.
- Die MBone-Kostengewichtung beträgt nur 22,6% der Unicast-Kostengewichtung.
- Die Internet-Multicast-Kostengewichtung beträgt das 2,4-fache der MBone-Multicast kosten.

3.5.1 STS-63 Space Shuttle

- Die Kosten des Multicast-Baumes betragen 30,1% der Unicast-Kosten (hier größer, da diese Sendung von sehr vielen empfangen wird).
- Die Internet-Multicast-Kostengewichtung beträgt das 2,3-fache der MBone multicast Kosten.

4 Ausblick

Durch immer höhere Übertragungsraten im Internet gewinnt die multimediale Kommunikation in Weitverkehrsnetzen immer mehr an Bedeutung. Multimediale Gruppenkommunikation wird bald für Jedermann möglich sein. In absehbarer Zeit wird das MBone in seiner jetzigen Form jedoch nicht mehr existieren. Normale Router im Internet, die dann Multicast-Routing unterstützen, werden die Aufgabe von heutigen Multicast-Routern (Mrouted) übernehmen.

Literatur

[AA95] K. C. Almeroth und M. H. Ammar. Characterization of Mbone Session Dynamics: Developing and Applying a Measurement Tool. *GIT-CC* 95(22), Juli 1995.

[Bun95] J. Bunn. *MBONE (Multicasting Backbone)*. Geneva University. 1995.

[Eri94] H. Eriksson. MBONE: The multicasting Backbone. *Communications of the ACM* 37(8), August 1994, Seite 54–60.

[MBo] Offizielle MBone-Seite für Deutschland. http://www.mbone.de.

[YKT96] M. Yajnik, J. Kurose und D. Towsley. Packet Loss Correlation in the Mbone Multicast Network. *UMASS CMPSCI Technical Report* 96(32), 1996.

Abbildungsverzeichnis

Tabellenverzeichnis

FastEthernet — Die Standards

Viktor Sauer

Kurzfassung

Dieser Beitrag führt in die zahlreichen FastEthernet Standards ein. Im ersten Teil werden die verschiedenen 802.3u Standards 100Base-T4, 100Base-TX und 100Base-FX vorgestellt, sowie der 802.12 Standard Priority Demand, auch bekannt als 100VG-AnyLAN. Ebenso wird auch Ethernet- oder Packet Switching als mögliche kostengünstige Alternative behandelt. Im zweiten Teil werden die 802.3u Standards und Priority Demand miteinander verglichen und Unterschiede in der Topologie und Technologie weiter vertieft. Dabei wird eine kleine Auswahl von Hubs oder Repeater sowie der entsprechenden FastEthernet-Adapter im Leistungsvergleich vorgestellt. Dabei sind beide Standards (802.3u und 802.12) vertreten.

1 Einleitung

Die rasche Verbreitung von LANs im kommerziellen, wissenschaftlichen und universitären Bereich zog einen steigenden Bedarf an „Bandbreite“ und Zuverlässigkeit nach sich. Während früher LANs häufig dazu benutzt wurden, mehrere Workstations oder PCs den Zugang zu Mail- oder PrintServern zu ermöglichen, sind heute neue Anwendungen mit größerem Bedarf an Übertragungskapazität hinzugekommen. Diese Anwendungen, wie Video- und Audio-Konferenzen, verteilte Netzwerkfilesysteme, Diskless Workstations oder Informationssysteme wie z.B. das WWW sind nur schwer mit den etablierten LAN-Standards wie Ethernet oder Tokenring unter Berücksichtigung der gestiegenen Erwartungen der Benutzer, z.B. im Bereich der Antwortzeiten, zu befriedigen.

Um diese Anforderungen zu erfüllen, wurde eine Reihe von schnellen LAN-Typen entwickelt. Diese enthalten eine Anzahl von Variationen des CSMA/CD-Ethernet-LAN-Standards, da dies der wohl am häufigsten in der Praxis anzutreffende LAN-Typ ist. Das Ziel der Hersteller war die Steigerung der Übertragungskapazität mit nur minimalen Änderungen an der installierten Software und Verkabelung. Eine Variante der bestehenden CSMA/CD-LANs ist bekannt unter dem Namen „Ethernet“- oder „Packet Switching“, die andere unter der Bezeichnung FastEthernet. Eine dritte Variation ist der IEEE 802.12 Standard, auch als Priority Demand bezeichnet. Dieser Standard wurde auch mit dem Ziel entwickelt, die bestehende Verkabelung zu nutzen, benutzt jedoch ein anderes MAC-Protokoll (Priority Demand), um dies zu ereichen.

In Abschnitt 2 werden die verschiedenen 802.3u Standards 100Base-T4, 100Base-TX und 100Base-FX vorgestellt sowie der 802.12 Standard Priority Demand, auch bekannt

als 100VG-AnyLAN. Ebenso wird auch Ethernet- oder Packet Switching als mögliche billige Alternative behandelt. In Abschnitt 3 werden die 802.3u Standards und Priority Demand miteinander verglichen und Unterschiede in der Topologie und Technologie weiter vertieft. Dabei wird eine kleine Auswahl von Hubs oder Repeater, sowie der entsprechenden FastEthernet-Adapter im Leistungsvergleich vorgestellt. Es sind beide Standards (802.3u und 802.12) vertreten.

2 Die neuen 100MBit/s LAN-Standards

In diesem Abschnitt werden die zwei wichtigsten 100MBit/s-Standards FastEthernet mit seinen Spielarten und 100VG-AnyLAN näher erläutert. Im FastEthernet-Bereich wird hier vor allem auf 100Base-T4 Wert gelegt. Auch Packet Switching wird etwas genauer untersucht. Um Mißverständnissen vorzubeugen, sei hier erwähnt, daß Packet Switching genau genommen kein 100MBit/s-Standard ist, sondern eine Art schneller Switch, für Details sei hier auf Abschnitt 2.3 verwiesen.

2.1 FastEthernet/IEEE 802.3u

Das Ziel bei der Entwicklung von FastEthernet war ein signifikanter Geschwindigkeitsgewinn gegenüber dem herkömmlichen Ethernet unter der Randbedingung, daß sowohl die bestehende Verkabelung als auch die MAC-Schicht mit ihrem Paket-Format beibehalten werden kann.

2.1.1 Die MAC-Schicht

Der IEEE 802.3 Standard, also Ethernet, erlaubt eine maximale Kabellänge von 2,5km für ein Segment, einschließlich Repeater und Remote Repeater mit einer Kabellänge von 1000m für die Punkt-zu-Punkt Verbindung. Bei einer Signalausbreitungsgeschwindigkeit von $0,77 \times c$ im Koaxialkabel und $0,65 \times c$ in der Punkt-zu-Punkt Verbindung ergibt sich hier ein sog. „Worst-Case Round-Trip-Delay“ von ca. 50μs. Der Worst-Case Round-Trip-Delay ist die Zeit, die ein Signal von einem Ende der Übertragungsstrecke bis zum anderen und wieder zurück braucht. Diese 50μs entsprechen bei einer Bitrate von 10MBit/s 500 Bit. Hierzu wird ein Sicherheitsfaktor addiert und somit ergibt sich 512 Bit als minimale Paketgröße. Um nun eine Beschleunigung mit CSMA/CD zu erzielen, muß diese maximale Segmentlänge reduziert werden. Dies ist die Basis für die FastEthernet-Standards.

Da in der Praxis bei einem Großteil der Installationen die Strecke zwischen Endadapter und Hub kleiner als 100m ist, ergibt sich 200m für den maximalen Abstand zwischen zwei Endadaptern und damit eine maximale Strecke von 400m für die Kollisionserkennung. Daher kann bei einer Bitrate von 100MBit/s das CSMA/CD MAC-Protokoll und die minimale Paketgröße von 512 Bit beibehalten werden.

2.1.2 Die Physikalische-Schicht

Das eigentliche Problem bei FastEthernet ist, wie man 100MBit/s über 100m nicht abgeschirmte Twisted-Pair-Leitung (Bezeichnung UTP (Unshielded Twisted Pair) oder

VG (Voice Grade)) übertragen kann. Daher wurden zwei Standards entwickelt 100Base T4 für UTP und 100Base TX/FX für abgeschirmte Twisted-Pair Kabel (Bez. STP (Shielded Twisted Pair)) oder Glasfaser. Um diesen verschiedenen Anforderungen gerecht zu werden, wurden in der physikalischen Schicht zwei Unterschichten definiert: zum einen die Konvergenz-Schicht (convergence-layer), die die Schittstelle zur MAC-Schicht darstellt, und zum anderen die vom physikalische Medium abhängige Unterschicht (PMD-layer). Für die Kommunikation zwischen Konvergenz-Schicht und PMD-Schicht wurde das MII (Media-Independent-Interface) definiert. Die Hauptaufgabe der Konvergenz-Schicht besteht in der Konvertierung serieller Datenströme von der MAC-Schicht in 4 Bit Nibbels (Bez. für eine 4 Bit Einheit) für das MII und umgekehrt, sowie die Weiterleitung der Carrier-Sense und Collision-Detect Signale (vgl. Bild 1).

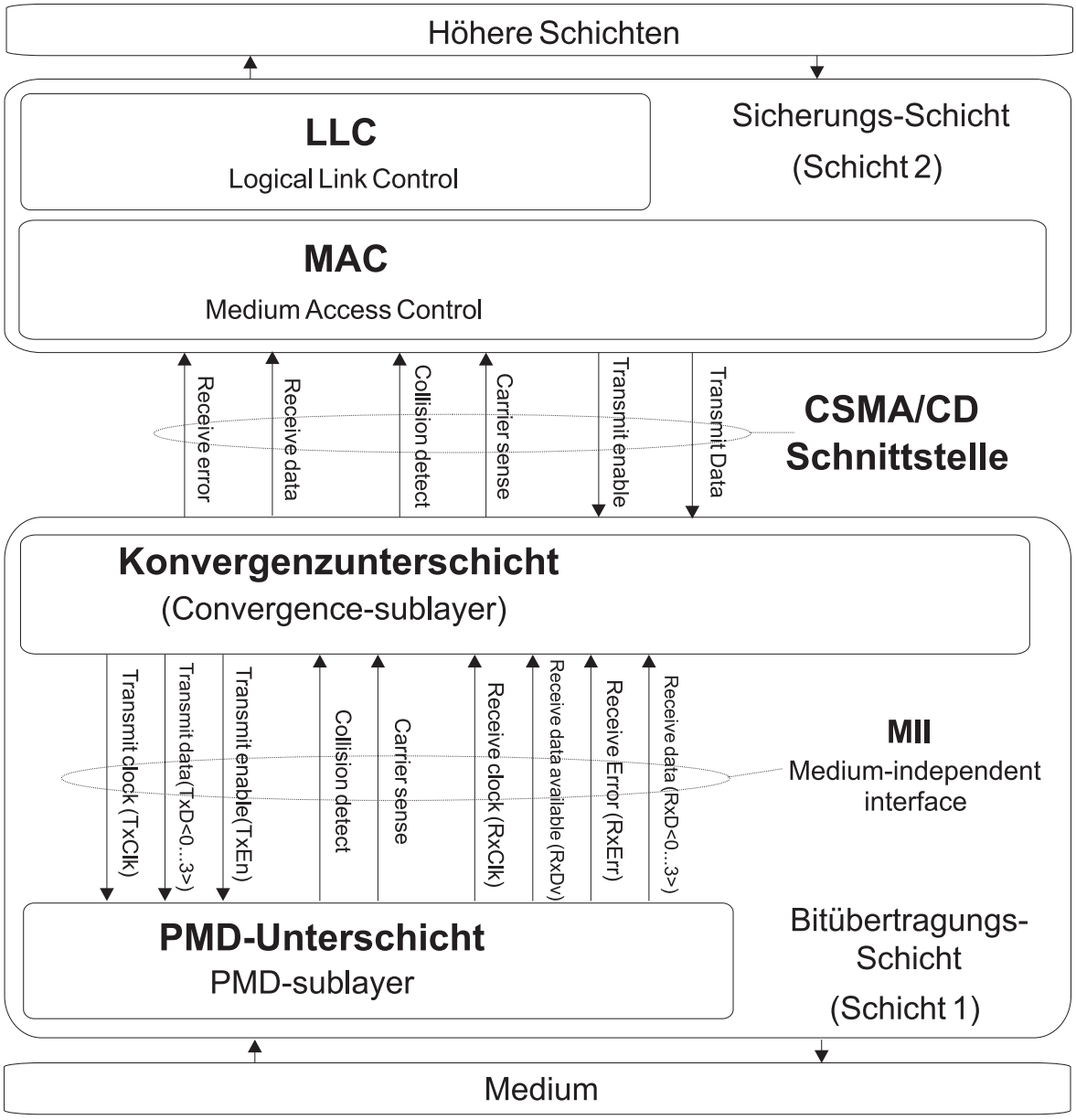


Abbildung 1: 100Base-T Protokollarchitektur.

2.1.3 100Base-T4

Der 100Base-T4-Standard wurde für UTP Kategorie 3, 4 oder 5 oder IBM Type 1 STP Kabel entwickelt. Diese Kabeltypen enthalten 4 separate Leitungspaare. Für die Übertragung von 100MBit/s in beide Richtungen, also von Station-zu-Hub und Hub-zu-Station, werden alle 4 Paare benötigt. Dies ist der Ursprung des 'T4' im Namen.

Bei bestehenden 10Base-T–Installationen werden für die Übertragung nur zwei Leitungspaare benötigt, eines für jede Richtung. Mit CSMA/CD sind alle Übertragungen nur halb-duplex, d.h. eine Kollision kann sehr einfach erkannt werden. Eine Kollision tritt nur genau dann auf, wenn eine Station auf ihrem Sendepaar sendet und auf ihrem Empfangspaar ein Signal empfängt. Diese Art der Kollisionserkennung soll auch bei 100Base-T4 funktionieren. Aus diesem Grund muß das gleiche Sende- und Empfängerpaar wie bei 10Base-T verwendet werden. Die verbleibenden 2 Paare werden gemeinsam für die bidirektionale Übertragung verwendet. Bild 2 soll dies veranschaulichen. Insgesamt folgt somit, daß für jede Übertragungsrichtung 3 Paare zur Verfügung stehen. Dies beutet, daß pro Paar nur noch 33,33MBit/s übertragen werden müssen.

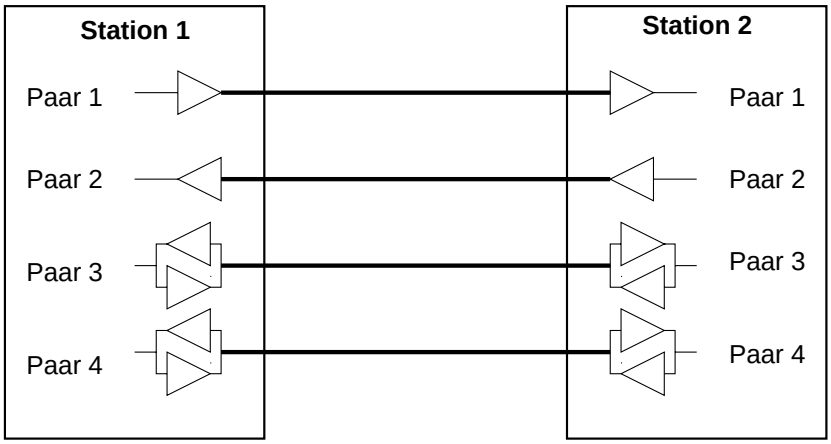


Abbildung 2: Aufteilung der Leitungspaare bei 100Base-T4.

2.1.4 Physikalische mediumunabhängige Schicht

Bei Verwendung eines Biphasen-Codes (z.B. Manchester-Kodierung) benötigt eine Bitrate von 33,33MBit/s eine Bandbreite von 33,33MHz. Diese überschreitet allerdings die maximal zulässige Bandbreite von 30MHz für UTP-Kabel (Kategorie 3). Daher muß die Taktrate gesenkt werden. Zu diesem Zweck wird ein ternärer, also 3-stufiger Code, verwendet (Doppelstromverfahren). Der benutzte Code ist 8B6T, das bedeutet, daß 8Bit in 6 ternäre Symbole übersetzt werden. Bild 3 soll den Zusammenhang verdeutlichen. Mit dieser Kodierung gelingt es, die Taktrate auf 25MHz ($\frac{100MHz*\frac{6}{8}}{3} = 25MHz$) zu senken.

Damit diese Kodierung auch praktisch eingesetzt werden kann, müssen noch zwei Randbedingungen erfüllt werden. Erstens sollte der Code gleichstromfrei sein und zweitens soll eine Rückgewinnung des Taktes, um die Synchronisation zwischen Sender und Empfänger sicherzustellen, möglich sein.

Da pro Codewort 6 ternäre Symbole verwendet werden, gibt es hier (3^6) 729 Möglichkeiten, benötigt werden für die Kodierung von 8Bit jedoch nur 256. Um nun die erste

Bedingung zu erfüllen, werden die Codeworte mit einem Gewicht von 0 oder +1 ausgewählt. Dabei ist das Gewicht eines Codewortes die Summe über die einzelnen Symbole. Jedem Symbol wird dabei ein Gewichtsfaktor, je nach repräsentierter Spannung +V , 0, -V, also +1, 0 oder -1 zu gewiesen. Es erfüllen genau 267 Codeworte diese Bedingung. Für die zweite Bedingung werden alle Codeworte, die weniger als 2 Signalübergänge enthalten und mit 4 Nullen beginnen oder enden, gestrichen. Es bleiben genau 256 Codeworte übrig. (Die Kodierungstabelle ist in [Hal96] Tabelle 7.1 zu finden)

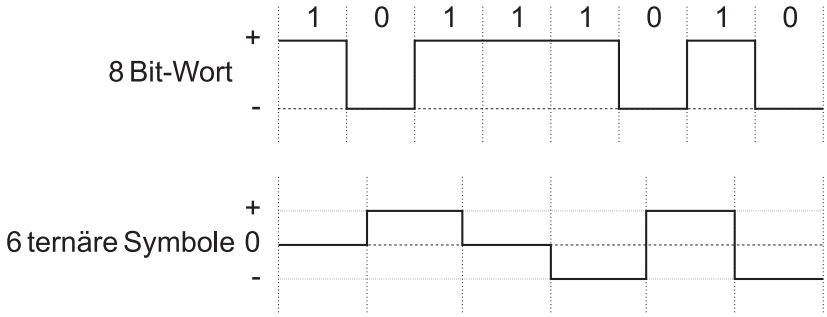


Abbildung 3: 8B6T Code.

2.1.5 Gleichstromfreiheit

Da bei der Codewortwahl auch Worte mit einem Gewicht von +1 zugelassen wurden, kann hier ein Problem auftauchen. Soll eine Folge von Codeworten mit je einem Gewicht von +1 übertragen werden, kann der Signalpegel ganz erheblich vom Grundpegel 0 abweichen. Dies kann wiederum zu einer Fehlinterpretation der Signale führen.

Zur Lösung des Problems wird die Polarität der Signale eines ganzen Codewortes, bei einem Codewortgewicht von +1, alternierend invertiert. Ein Beispiel soll das verdeutlichen. Es soll eine Folge des Codewortes 0+1+1+1-1-1 übertragen werden. Dann wird die folgende Codewortfolge gesendet 0+1+1+1-1-1, 0-1-1-1+1+1, 0+1+1+1-1-1, ... Da der Empfänger das gleiche Verfahren anwendet, werden die Codeworte in ihre ursprüngliche Form dekodiert und die Bedingung der Gleichstromfreiheit ist erfüllt.

2.1.6 Kollisionserkennung

Um Kollisionen zu erkennen, muß der Sender wie schon erwähnt während einer Übertragung sein Empfangspaar auf eingehende Pakete hin überprüfen. Und genau hier kann es zu Problemen kommen, wenn die eigene Übertragung durch Induktion in das Empfängerpaar eine Störung verursacht. Um Fehler durch dieses sog. Übersprechen zu verhindern, wird zu Beginn eines Paketes eine Präambel (start-of-stream sequence) aus binären Signalen gesendet. Dies ermöglicht dem Empfänger eine klare Unterscheidung zwischen Übersprechen und tatsächlicher Kollision.

2.1.7 100Base-X

Der Ansatz von 100Base-X unterscheidet sich auf physikalischer Ebene grundsätzlich von 100Base-T4, da 100Base-X für Kategorie 5 UTP oder STP Kabel und Glasfa-

ser entwickelt wurde. Diese Kabel ermöglichen eine wesentlich höhere Bandbreite als Kategorie 1 bis Kategorie 4 UTP Kabel.

Da auch FDDI den Einsatz von Kupfer- und Glasfaserkabeln gestattet, wurde für 100Base-X ein Teil der FDDI-Technologie übernommen. Dies schließt sowohl die Signalkodierung mit dem 4B5B-Schema als auch die Vollduplex-Signalisierung ein. Jedoch wurde weiterhin auf CSMA/CD als MAC-Protokoll gesetzt.

Bemerkenswert ist hier ebenfalls, daß die 4B5B-Codeworte für 100Base-TX, das 'T' steht wieder für Twisted Pair, in einen ternären Leitungskode für die Übertragung umgesetzt werden. Die Übertragung selbst erfolgt ähnlich wie bei 10Base-T auf nur zwei Leitungspaaren, eines für jede Richtung. Anstelle von Twisted Pair kann hier auch Glasfaser verwendet werden, dabei wird ebenfalls für jede Richtung eine Faser benötigt.

Die Kollisionserkennung funktioniert genau wie bei 10Base-T. Sendet eine Station, so muß sie gleichzeitig ihr Empfängerpaar überprüfen. Falls eine Kollision erkannt wird, wird die Sendung abgebrochen und die Jam-Sequenz übertragen. An dieser Stelle sei auf eine bemerkenswerte Besonderheit von 100Base-X hingewiesen. Es ist auch ein Vollduplex-Betrieb, d.h. das gleichzeitige Senden und Empfangen möglich. Liegen keine Sendewünsche an, so wird im Gegensatz zu 100Base-T4 ein IDLE-Signal ähnlich wie bei FDDI gesendet. Dies hilft zum einen bei der Synchronisation und erleichtert zum anderen die Erkennung eines Paketbeginns oder eines Leitungsfehlers.

2.2 100VG-AnyLAN/IEEE 802.12

Wie FastEthernet (Abschnitt 2.1) wurde auch 100VG-AnyLAN mit dem Ziel entwickelt, den IEEE802.3-Standard „Ethernet“ abzulösen. In Kontrast zu 100Base-T wurde ein anderes MAC-Protokoll entwickelt [WAC+95]. Es wurde bei der Entwicklung besonderen Wert auf die folgenden Punkte gelegt:

- Erhaltung der MAC-Dienstschnittstelle, aus Kompatibilitätsgründen
- Einfacher Aufbau von hierarchischen Strukturen ohne Brücken oder Switches
- Variable Paketgröße, für eine leichtere Migration von bestehenden LANs
- Unterstützung von Realzeiteigenschaften

100VG-AnyLAN unterstützt sämtliche im 10Base-T–Bereich vertretenen Kabeltypen. Dabei ist mit besserer Kabelqualität auch beinahe eine proportionale Steigerung des Abstandes zwischen Station und Hub möglich. Für Kategorie-3-UTP-Kabel beträgt der maximale Abstand 100m. Die erlaubten Kabeltypen sind somit Kategorie 3, 4 oder 5 UTP-Kabel mit 4 Leitungspaaren, sowie STP mit 2 Paaren oder Glasfaser mit 2 Leitungen.

2.2.1 Topologie

Mit 100VG-AnyLAN-Hubs kann jede beliebige hierarchische Baumstruktur aufgebaut werden. Dafür besitzt ein Repeater einen „uplink“-Port für die Verbindung mit einem „Eltern“-Hub und mehrere „downlink“-Ports, an die wahlweise Endstationen oder

andere Hubs angeschlossen werden können. Hubs können so bis zu einer maximalen Länge von bis zu 2,5km verbunden werden, bevor der Einsatz von Brücken nötig ist. Brücken müssen nun allerdings auch das „Demand Priority"-MAC-Protokoll an mindestens einem ihrer Ports unterstützen. Um die Konektivität noch zu steigern, kann das IEEE802.12 Paket-Format entweder das IEEE802.3 (Ethernet) oder das IEEE802.5 (Tokenring) Paket-Format sein. In einem Netz kann jedoch nur eines der Formate zur gleichen Zeit benutzt werden.

2.2.2 MAC-Protokoll — Demand Priority

Das MAC-Protokoll ist ein Polling-basiertes Verfahren. Zwischen Hubs und Stationen besteht eine enge „Verbindung", wobei eine Station auch ein anderer Hub sein kann. Für Übertragungen stehen zwei Prioritätsstufen zur Verfügung. Jeder Hub besitzt eine bestimmte feste Anzahl von Ports, gewöhnlich zwischen 8 und 16, und einen uplink-Port. Jeder Port hat eine Nummer (im folgenden mit PN abgekürzt). Die PN sind aufsteigend beginnend bei 1 durchnumeriert.

2.2.3 Signalisierung

Um den Zugriff auf das Netzwerk zu steuern, wird ein einfaches Signalisierungsverfahren verwendet. Dafür werden je zwei Leitungspaare benutzt, bei STP nur je ein Paar.

Im Grundzustand sendet eine Station spezielle IDLE-Signale, auf die der Hub seinerseits mit IDLE-Signalen antwortet. Um Sendewünsche (SW) abzusetzen, werden 2 REQUEST-Signale definiert: REQH für hochpriore SW (HSW) und REQN für normalpriore SW (NSW). Für Belegung des Netzes durch eine Übertragung wurde das INCOMING-Signal definiert. Zu jeder Zeit darf auf dem Netz nur eine Übertragung laufen. Bild 4 soll das Zusammenwirken der Signale für einen Sendewunsch veranschaulichen.

Station S1 hat einen SW und setzt ein REQUEST ab. Der Hub nimmt den SW entgegen, schaltet seine Übertragung der IDLE-Signale ab und sendet das INCOMING-Signal an alle anderen Stationen. S1 erkennt, daß die Leitung frei ist und beginnt mit der Übertragung. Alle anderen Stationen signalisieren ihre Bereitschaft, indem sie ihr IDLE-Signal abschalten. Der Hub verzögert das Paket (mit einem FIFO-Speicher) nur solange, bis er die Zieladresse ausgewertet hat, hier Station S3, und beginnt dann mit der Weiterleitung. An die unbeteiligten Stationen wird wieder das IDLE-Signal gesendet, worauf diese mit dem IDLE-Signal antworten. Ist die Übertragung beendet, gehen S1 und S3, nachdem das letzte Codewort empfangen wurde, wieder in den IDLE-Zustand über.

2.2.4 Demand Priority

Für die Zuteilung des Senderechtes führt der Hub zwei sog. „next-port pointer" (NPP), einen für jede Prioritätsstufe (normale Priorität: NNPP - Normal NPP; hohe Priorität: HPNPP - High-Priority NPP). Die Reihenfolge der Sendungen für eine Prioritätsstufe wird nach dem sog. „round-robin scheduling"-Algorithmus bestimmt. Der Algorithmus soll hier kurz mit einem NPP erläutert werden. Der NPP enthält die PN des Ports,

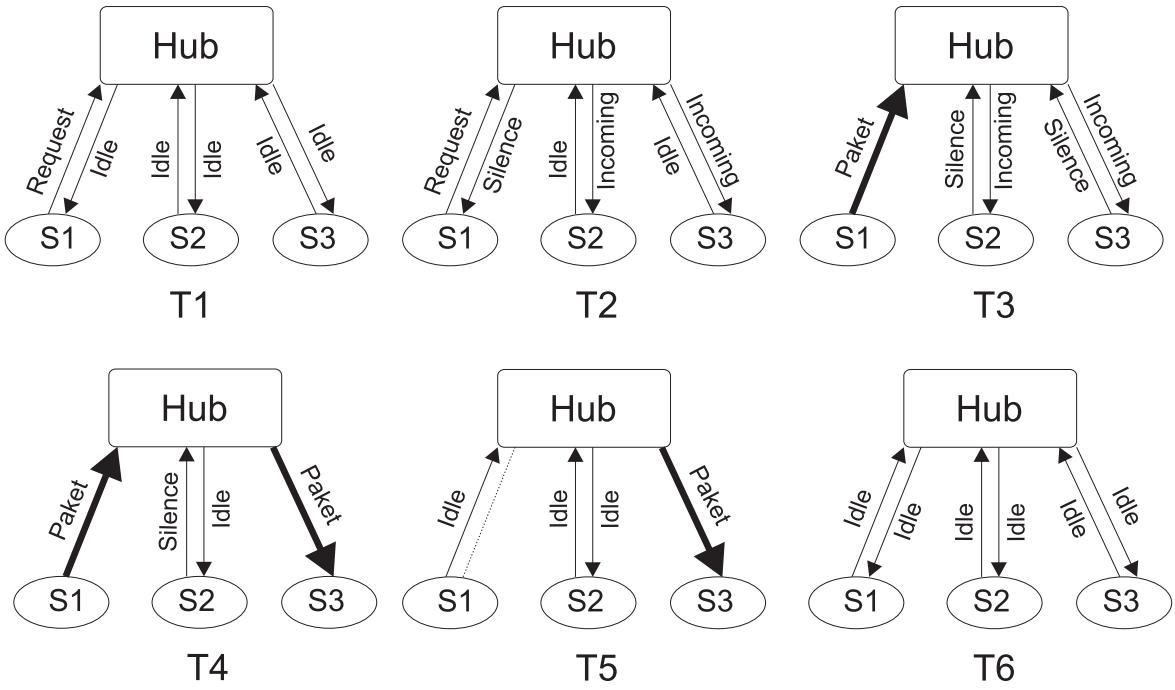


Abbildung 4: Signalisierung eines Sendewunsches.

der als nächster sendeberechtigt ist. Der Hub speichert alle eingehenden SW seiner Ports. Dabei darf nun die Station am nächsten Port mit einer PN größer gleich dem NPP senden. Liegen unter diesen Bedingungen keine SW vor, darf die Station senden, deren PN größer gleich der PN des ersten Ports ist. Im NPP wird die PN des Ports abgelegt, der dem gerade bedienten Port nachfolgt. War der bediente Port der letzte, wird im NPP die PN des ersten Ports gespeichert.

Alle HSW werden zuerst bedient; erst wenn keine mehr vorliegen, werden die NSW abgearbeitet. Dieses Verfahren wird „demand priority scheduling“ gennant; daher auch der Name des MAC-Protokolls. Um die NSW bei vielen HSW nicht zu lange zu verzögern, wird nach einem „time-out“-Intervall von 200ms bis 300ms der NSW wie ein HSW behandelt.

2.2.5 Kaskadierung

Im letzten Abschnitt wurde das Verfahren für eine einfache Sterntopologie beschrieben. Für kaskadierte Strukturen ist das Verfahren etwas anders. Es gibt dann immer einen „Root“-Hub, der die Kontrolle über sämtliche Transaktionen hat. Die Hubs in den unteren Schichten pollen wie im einfachen Fall ihre Ports. Liegt ein SW in einer unteren Schicht vor, so signalisiert der entsprechende Hub dies an seinem uplink-Port. Der SW wird bis an den Root-Hub propagiert. Dieser übergibt die Kontrolle, wenn der betroffene Port an die Reihe kommt, an den signalisierenden Hub. Dieser behält die Kontrolle für einen kompletten „round-robin“-Zyklus und gibt sie dann an eine höhere Ebene in der Hierarchie zurück (Siehe Bild 5).

Empfängt ein Hub eine Sendung, so leitet er diese an alle angeschlossenen Hubs weiter, damit diese eine Belegung oder das Freiwerden des Netzwerkes erkennen können.

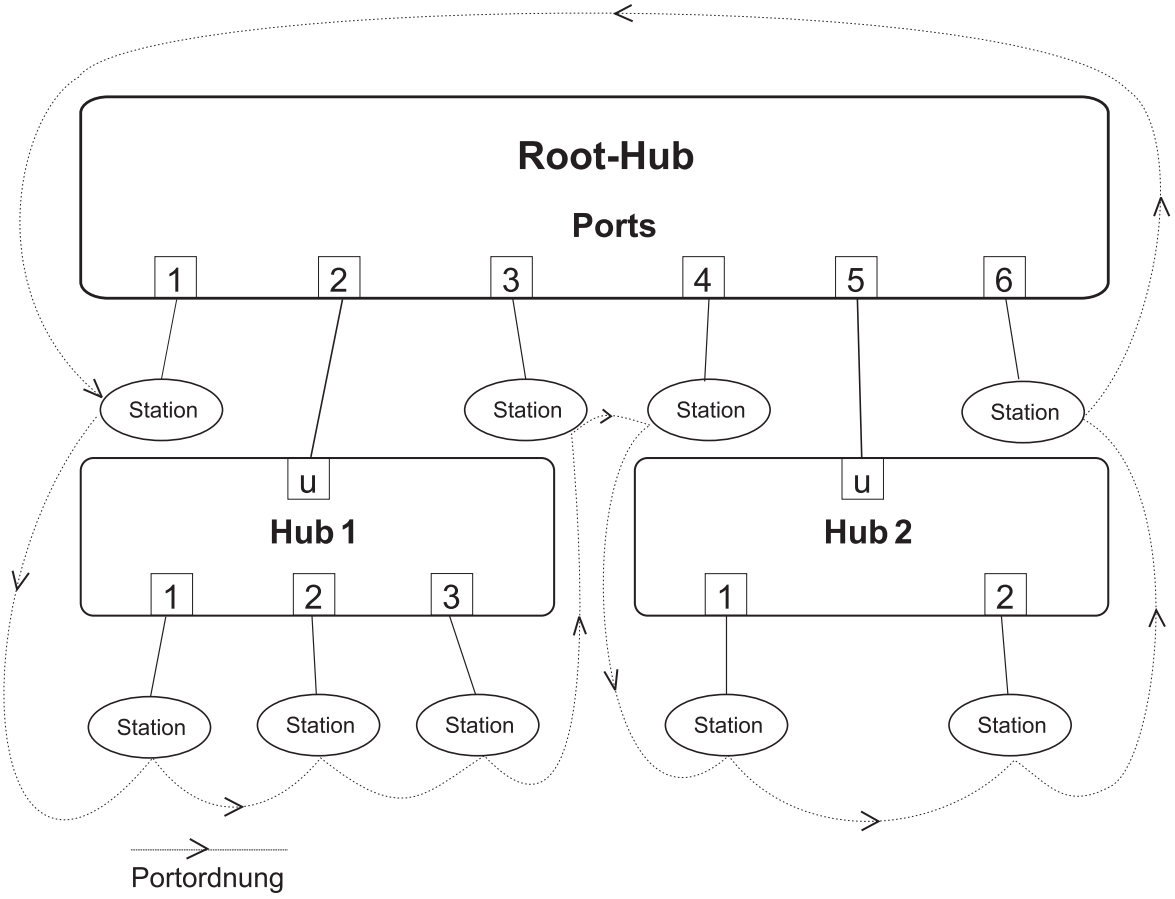


Abbildung 5: Effektive Sendereihenfolge bei kaskadierten Hubs.

Um sicherzustellen, daß HSW auf höheren Schichten auch dann bedient werden, wenn ein Hub aus einer tieferen Schicht die Kontrolle hat und nur NSW bearbeitet, sendet der Root-Hub, wenn die aktuelle Sendung beendet ist, ein „Pre-empt“-Kontrollsignal an alle seine Hubs. Nachdem die Kontrolle wieder beim Root-Hub ist, bedient dieser den HSW nach dem üblichen Verfahren. Danach erhält der unterbrochene Hub die Kontrolle zurück und kann seinen „round-robin“-Zyklus vollenden.

Damit dieses Verfahren funktioniert, muß jeder Hub wissen, ob an seinen Ports eine Station oder ein anderer Hub angeschlossen ist. Dies wird in einer initialen Trainingsphase ermittelt, sobald ein neues Gerät angeschlossen wird.

2.2.6 Physikalische Schicht

Da Demand Priority keine Kollisionserkennung benötigt, können alle zur Verfügung stehenden Leitungspaare benutzt werden. Bei Kategorie 3 UTP sind das 4 Paare, d.h. pro Paar sind 25MBit/s zu übertragen. In der Praxis wird dieser Wert durch eine 5B6B Kodierung auf 30MBit/s erhöht. Die 5B6B Codeworte sind wieder mit Bedacht auf Gleichstromfreiheit und einer minimalen Signalübergangsabhängigkeit ausgewählt worden. Zur Übertragung werden die 5B6B Codeworte so auf die 4 Leitungspaare moduliert, daß sie beim Empfangen ohne größere Verzögerung dekodiert werden können.

2.3 Packet Switching

Im Gegensatz zu FastEthernet und 100VG-AnyLAN ist Packet-Switching keine neue Technologie, sondern vielmehr der Versuch, durch den Einsatz von Switches den Durchsatz bestehender Ethernet-Installationen zu steigern. Ein Switch ist dabei eine Art Multiport-Bridge.

Switches können eingesetzt werden, um unterschiedlich schnelle Netzsegmente zu verbinden oder allgemein, um ein bestehendes Netz zu segmentieren und so die Teilsegmente zu enlasten. Die Leistungssteigerung durch einen Switch ist dabei stark abhängig von dem im Netzwerk vorherschenden Verkehr. Besteht der Verkehr insgesamt aus vielen kleinen Paketen, ist keine nennenswerte Steigerung möglich, da das Medium dann meistens frei vorgefunden wird, vergleiche hierzu [MW96]. Generell läßt sich jedoch sagen, daß mit Switches, die unterschiedlich schnelle Technologien vereinigen, wie z.B. 10Base-T und FastEthernet, eine deutliche Steigerung des Durchsatzes möglich ist. Dabei kann z.B. ein Server an einem FastEthernet-Port betrieben werden und so „gleichzeitig“ mehrere Ethernet-Clients ohne nennenswerte Leistungseinbrüche versorgen, immer vorausgesetzt, der Server ist leistungsfähig genug.

2.3.1 Grundlagen

Die Funktionsweise eines Switches ist im Vergleich zu einem Router recht simpel: Ein Paket wird von seinem Quellport nur zu seinem Bestimmungsport weitergeleitet. Das bedeutet, daß zu einem Zeitpunkt, je nach Leistungsfähigkeit der Backplane des Switches, mehrer Pakete gleichzeitig zwischen unterschiedlichen Ports und somit Netzsegmenten ausgetauscht werden können. Pakete für Endsysteme im gleichen Segment werden nicht auf andere Segmente übertragen.

Um Pakete zielgerichtet zwischen den Ports übertragen zu können, muß ein Switch „wissen“, welche MAC-Adressen an welchem Port zu finden sind. Dies kann ein Switch, da er auf Schicht 2 des ISO/OSI-Modells operiert, im Gegensatz zu einem Router, im laufenden Betrieb ohne zusätzlichen Protokollaufwand ermitteln. Dafür besitzt ein Switch eine Zuordnungstabelle. Bevor ein Paket von einem Port weitergeleitet wird, wird die Quelladresse ausgelesen und ein Eintrag in der Zuordungstabelle gemacht. Ist für eine Zieladresse noch keine Portzuordnung getroffen worden, wird das Paket an alle Ports, außer dem Quellport, gesendet. Die Einträge in der Zuordnungstabelle werden in bestimmten Zeitabständen gelöscht und neu ermittelt. Dies dient der Konsistenzerhaltung, z.B. für Fall, daß eine Station „umgezogen“ ist. Zur Veranschaulichung soll Bild 6 dienen.

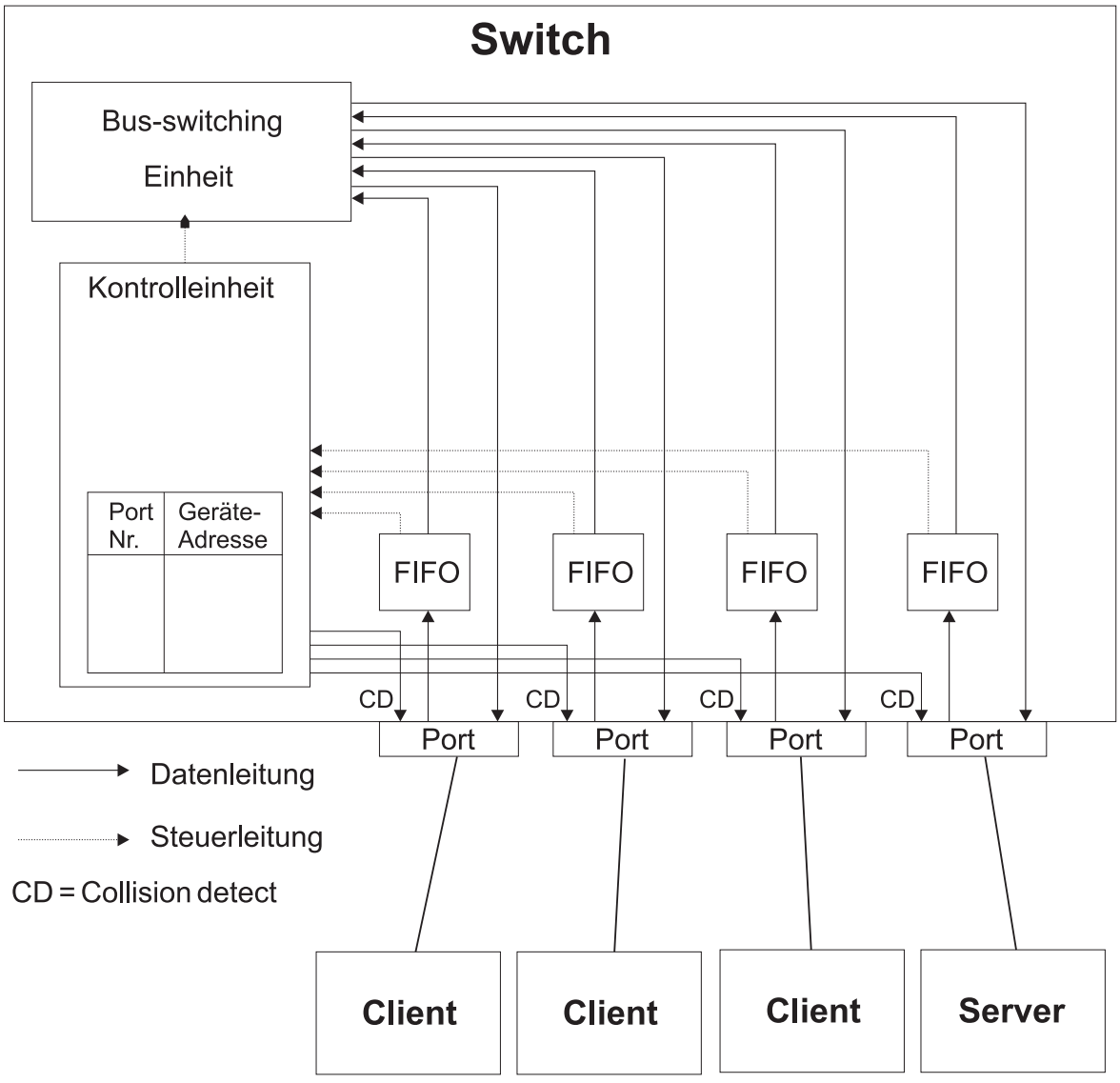


Abbildung 6: Schema eines Switches.

Für die Paketweiterleitung sind zwei allgemeine Vorgehensweisen möglich: „cut-through“ und „store-and-forward“. Bei „store-and-forward“ wird ein Paket zunächst ganz empfangen und dann erst weitergeleitet. Es wird also um ein ganzes Paket verzögert. In der Praxis wirkt sich diese Vorgehensweise jedoch nicht so störend aus, da die gängigen Transportprotokolle meistens einen Schwall von Paketen senden. Dabei ist die

Gesamtverzögerung, bedingt durch den Pipeline-Effekt, ebenfalls nur eine Paketlänge. Bei „cut-through“ wird ein Paket weitergeleitet sobald die Zieladresse (und der Zielport) bekannt ist. Die Verzögerungszeit wird so minimiert. Jedoch kann es durch die frühzeitige Weiterleitung zu Problemen kommen. Es kann passieren, daß unmittelbar nach Beginn der Weiterleitung eine Kollision eintritt und die Sendung unterbrochen wird. Das weitergeleitete Paket ist dann ungültig und eventuell kürzer als die Mindestpaketgröße. In den meisten Fällen stellt dies kein Problem dar, jedoch wird so Bandbreite verschenkt. Eine Möglichkeit, zu kurze Pakete auszuschließen, ist, solange mit dem Weiterleiten zu warten, bis die minimale Paketgröße empfangen wurde. Dies erhöht jedoch die Verzögerungszeit ein wenig. Ein weiterer Nachteil von „cut-through“ ist, daß Pakete nur zwischen Ports mit gleicher Übertragungsrate ausgetauscht werden können.

3 Leistungsvergleich

In diesem Abschnitt sollen die beiden in Abschnitt 2.1 und 2.2 vorgestellten 100MBit/s-Standards FastEthernet und 100VG-AnyLAN miteinander verglichen werden und die Vor- und Nachteile der jeweiligen Technologie aufgezeigt werden.

Topologie

Beide Standards wurden, im Hinblick auf weitgehende Erhaltung bestehender Verkabelung entwickelt. Sowohl 100Base-TX/T4 und 100VG-AnyLAN unterstützen eine Vielzahl der gängigen Kabeltypen. Bei der hierarchischen Unterteilung ist 100VG-AnyLAN deutlich im Vorteil. Hier sind, je nach Hersteller, 5 bis 6 Hierarchie-Stufen ohne den Einsatz von Brücken oder Switches möglich (vgl. [HP95]) und damit eine maximale Distanz von bis zu 4km. Jedoch wird eine so große Schachtelungstiefe aus Leistungsgründen nicht empfohlen. Der Abstand zwichen Hub und Adapter ist bei 100VG-AnyLAN auf maximal 200m mit STP-Kabel beschränkt. Mit 100Base-TX/T4 darf der maximale Abstand von 206m zwischen zwei Endsystemen nicht überschritten werden, wenn ebenfalls auf den Einsatz von Brücken verzichtet werden soll. In dieser Distanz sind 6-10m maximaler Abstand zwischen zwei Hubs bereits enthalten. Die meisten Hersteller empfehlen, die Anzahl von 2 Hubs nicht zu überschreiten. Jedoch sind auch 100Base-TX/T4 hierarchische Strukturen möglich, solange der „round-trip delay“ einschließlich aller durch Hubs hervorgerufenen Verzögerungen unter dem „worst-case round-trip delay“ bleibt.

Konfiguration

Durch den Einsatz gleicher Steckerverbindungen (RJ45-Stecker) bei 100Base-TX/T4, 100VG-AnyLAN und 10Base-T ist für eine „reibungslose“ Zusammenarbeit und leichte Migration der Komponenten ein automatisches Verfahren zur Konfiguration der Adapter und Hubs nötig. Für 100Base-TX/T4 wurde unter dem Namen „Autonegotiation“ ein Verfahren entwickelt, mit dem die maximale Übertragungsrate (10/60/100/200 MBit/s) und Übertragungsart (Voll- oder Halbduplex) ausgehandelt werden kann. Dafür wurde der bei 10Base-T übliche sog. „link integrity test pulse“ durch eine Folge

spezieller Signale ersetzt, damit die Abwärtskompatibilität erhalten bleibt. 100VG-AnyLAN bietet hier ein ähnliches Verfahren an.

Effizienz und Fairneß

Der Durchsatz mit beiden Verfahren ist stark abhängig von der Länge der Pakete. Wie bei allen Netzen, die sich das Medium teilen, nimmt der Durchsatz mit steigender Paketgröße zu und mit längeren Kabelwegen ab. In praktischen Versuchen hat sich gezeigt (vgl. [All95]), daß 100Base-T mit kleineren Paketen, bedingt durch weniger Overhead als bei 100VG-AnyLAN, besser umgehen kann. Bei 802.3-Paketen mit maximaler Länge hingegen gelingt mit 100VG-AnyLAN eine 95%-ige und mit 100Base-T eine 86%-ige Auslastung des Netzes. Bei 100VG-AnyLAN ist in der Praxis vorallem das Zusammenspiel von Hub und Adapter ausschlaggebend. In Tests (vgl. [NL96]) unter Novel Netware 4.10 (auf PC's) mit verfügbaren 100VG-AnyLAN-Adaptern und Hubs ergab sich eine sehr breite Streuung zwischen den einzelnen Testkandidaten im Bereich des Durchsatzes. Insgesamt waren die Karten zum Teil erheblich langsamer als die 100Base-T-Pendanten. Die besten Ergebnisse ließen sich mit dem HP J2410A Hub und einem Compex-Adapter (Enet100VG4/PCI) realisieren. Bild 7 soll den Testaufbau veranschaulichen. Um den Durchsatz im Netz zu ermitteln, wurden LAN-Analyzer eingesetz.

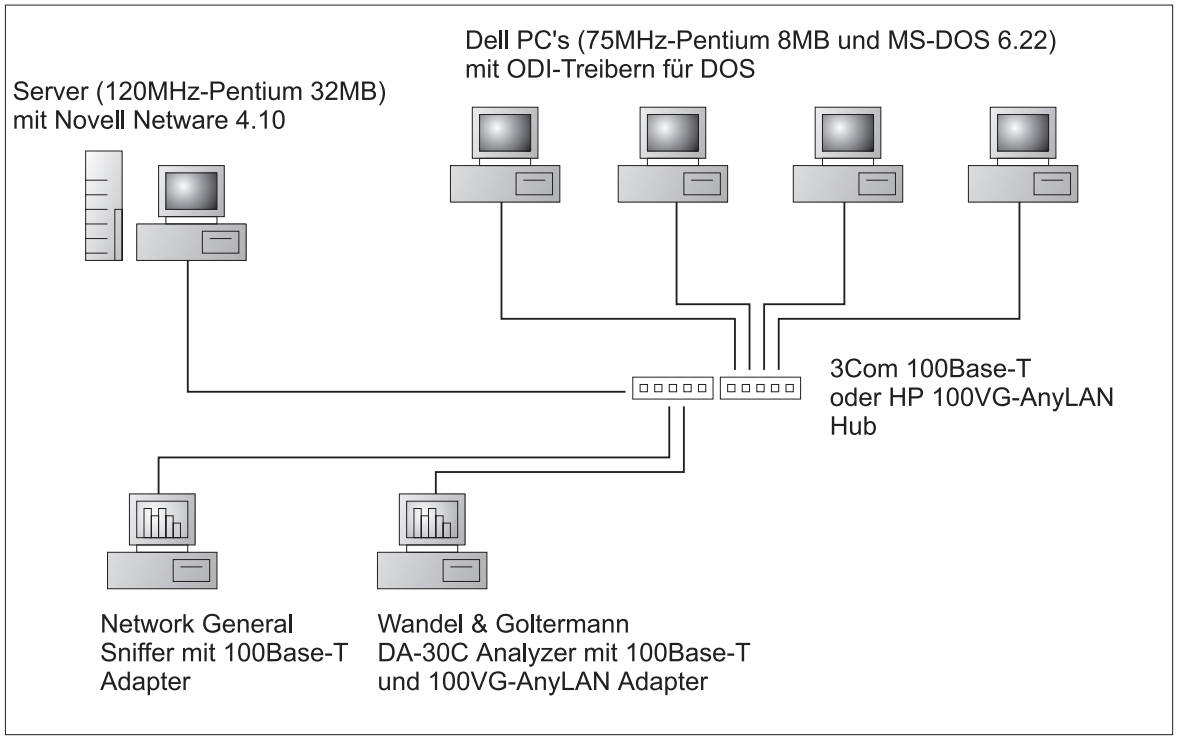


Abbildung 7: Testumgebung.

Bei steigender Netzlast wird CSMA/CD zunehmend unfairer. Durch den BackOff--Algorithmus kann häufiger der Fall eintreten, daß Stationen, die „später“ kommen, früher senden können, als Stationen die schon länger warten. Im schlimmsten Fall, nach 16 aufeinander folgenden Kollisionen, wird das Paket ganz verworfen und ein Fehler angezeigt. 100VG-AnyLAN verhält sich hier mit dem „round-robin schedule“

wesentlich besser. Auch bei hoher Last erhalten Stationen nach einer genau bestimmbaren Zeitspanne die Möglichkeit, ein Paket abzusetzen. Durch dieses deterministische Verfahren kann 100VG-AnyLAN im Gegensatz zu FastEthernet zeitkritischen Anwendungen eine („best-effort“) Auslieferung der Pakete bis zu einem bestimmten Zeitpunkt garantieren. Das wird noch durch die beiden Prioritätsklassen unterstützt, sofern diese von der verwendeten Software überhaupt benutzt werden können.

4 Fazit

FastEthernet und 100VG-AnyLAN erfüllen zum größten Teil die theoretischen Erwartungen. Jeder Standard hat seine Stärken und Schwächen, aber beide, 100Base-T und 100VG-AnyLAN sind bestens geeignet, 10Base-T abzulösen. Die Kosten für beide Standards sind relativ niedrig, im Vergleich zu FDDI oder ATM. In der Praxis scheint ein großer Teil der Hersteller auf 100Base-TX zu setzen und so ist auch zu erklären, daß hier Adapterkarten etwas billiger sind als bei 100VG-AnyLAN. Die Preisdifferenz bewegt sich im Raum von 10-20 Dollar. Die Adapterkartenpreise bewegen sich zwischen 129 bis 200 Dollar für 100VG-AnyLAN und 110 bis 160 Dollar bei 100Base-TX. Die pro-Port-Kosten bei Hubs sind, wenn man bei größeren Netzen unterstellt, daß bei 100Base-TX Brücken zum Einsatz gebracht werden müssen, bei 100VG-AnyLAN je nach Hersteller niedriger (z.B. HP AdvancedStack 100VG Hub 15 (15 Ports) ca. 7000 DM (Gerätepreis) und Grand Junction FastHub 100 (16 Ports) ca. 9500 DM (Gerätepreis)).

Zur Verbesserung des Durchsatzes eignet sich Packet-Switching mit Switches, die 10Base-T und 100VG-AnyLAN oder FastEthernet unterstützen, bestens. So kann durch „strategisch“ richtig plazierte Switches ein bestehendes Ethernet einen deutlichen Leistungszuwachs verzeichnen. Besonders nützlich ist hier die Möglichkeit von 100Base-TX, im vollduplex Betrieb zu arbeiten.

Für die Zukunft bleibt abzuwarten, welcher der beiden Standards in der Gunst der Käufer am höchsten stehen wird. Jedoch steht die Zeit nicht still und mittlerweile ist schon ein GigaEthernet-Standard in Vorbereitung (siehe [All95]).

Literatur

[All95] Gigabit Ethernet Alliance. Gigabit Ethernet Technology FAQ. In *World Wide Web unter http://www.gigabit-ethernet.org/faq.html*. Gigabit Ethernet Alliance, 1995.

[Hal96] F. Halsall. *Data Communications, Computer Networks and Open Systems*. Electronic Systems Engineering Series. Addison-Wesley Publishing Company, Wokingham (England). 1996.

[HP95] Hewlett-Packard. 100VG-AnyLAN: Facts and Myths. In *World Wide Web unter http://www.hp.com/rnd/technol/100vg/factmyth/vgfea2.htm*. Hewlett-Packard Company, Roseville Network Division, 1995.

[MW96] M. Molle und G. Watson. 100Base-T / IEEE 802.12 / Packet Switching. *IEEE Communications Magazine* 34(8), Aug 1996, Seite 64–73.

[NL96] D. Newman und B. Levy. 100Base-T vs. 100VG: The Real Fast Ethernet. *Data Communications International* 25(3), Mar 1996, Seite 67–80.

[WAC+95] G. Watson, A. Albert, J. Curico, D. Dove, S. Goody, J. Grinham, M.P. Spratt und P.A. Thaler. The Demand Priority MAC Protocol. *IEEE Network* 9(1), Jan/Feb 1995, Seite 28–34.

Abbildungsverzeichnis

Corporate Networks

Manfred Tessin

Kurzfassung

Diese Ausarbeitung gibt einen ersten Einblick in die Welt der Corporate Networks. Im ersten Teil wird die Idee des Corporate Networks beschrieben. Neue und weitergehende Anforderungen verschiedener Firmen definieren den Lösungsansatz des Corporate Networks. Anschließend werden kurz die Definition und einige rechtliche Grundlagen beschrieben. Nachfolgend werden Wege zum Corporate Network aufgezeigt. Die verschiedenen Ausprägungen und technischen Grundlagen eines Corporate Networks sind Gegenstand dieser Betrachtungen. Weiterhin werden die verschiedenen Standardisierungsmöglichkeiten im Themenkomplex Corporate Networks diskutiert. Als zukunftsweisender Ausblick wird eine kurze Einführung in die International Virtual Private Networks gegeben. Abschließend werden Gründe für und wider Corporate Networks abgewogen, um einen Anhaltspunkt zu finden, für welche Firmen Corporate Networks sinnvoll sind.

1 Die Idee des Corporate Networks

Mit der Veränderung vieler Firmenstrukturen verändern sich auch die Anforderungen, die an Informationshaltung, Informationsfluß und -verarbeitung gestellt werden.

Während junge Firmen sich zunächst auf einen lokal beschränkten Markt konzentrieren, nimmt die Größe des anvisierten Marktes im Laufe der Zeit immer mehr zu. Somit wachsen auch die Anforderungen, die an das Kommunikationssystem innerhalb einer Firma gestellt werden. Um die Informationen zu verwalten, werden die Rechner einer kleinen Firma in einem Local Area Network (LAN) miteinander verbunden.

Durch die Ausrichtung auf den gesamten Weltmarkt jedoch werden einige neue Anforderungen definiert: Informationen müssen möglicherweise weltweit vorhanden sein. Außerdem muß auf die Informationen zu jedem Zeitpunkt zugegriffen werden können. Das LAN kann die Anforderung des ortsunabhängigen Datenzugriffs nicht mehr erfüllen, so daß ein Wide Area Network (WAN) nötig wird. Typischerweise wurde für die Verbindung weit entfernter Netzwerkknoten auf das vorhandene analoge Telefonnetz und den Datentransfer per Modem gesetzt. In neuerer Zeit wird der Datentransfer verstärkt über das digitale ISDN abgewickelt. Abbildung 1 zeigt die Möglichkeit der Vernetzung einer weltweit operierenden Firma mit mehreren Niederlassungen. Während in Deutschland, der Schweiz, Holland und Frankreich der Datenverkehr über gemietete Standleitungen abgewickelt wird, muß in England, Österreich, Brasilien und Südafrika auf das öffentliche Telefonnetz ausgewichen werden.

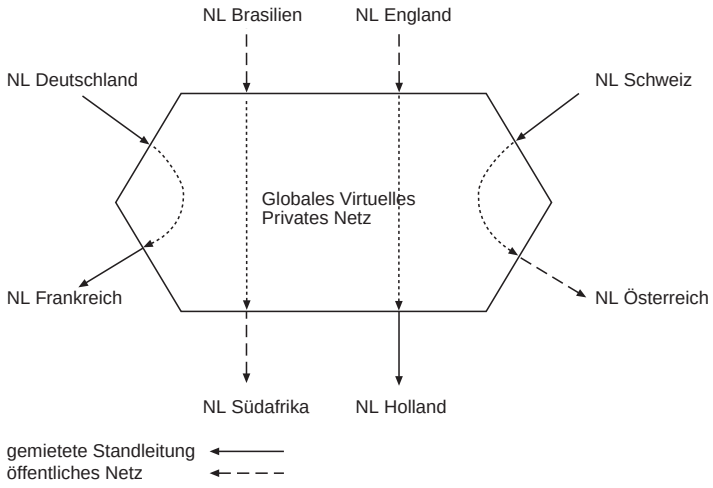


Abbildung 1: Möglichkeiten der internationalen Vernetzung.

Neben der Möglichkeit, auf Informationen zeit- und ortsunabhängig zugreifen zu können, steht aber auch die Bedeutung des Begriffes „Information“ im Vordergrund. Informationen sind die Grundlage, auf der eine erfolgreiche Unternehmung basiert. Doch was sind Informationen wert, wenn sie nicht zu der richtigen Zeit an der richtigen Stelle verfügbar sind? Somit muß eine Grundlage geschaffen werden, den Informationsfluß innerhalb einer Organisation zu optimieren.

Die Relevanz von verfügbaren Informationen erstreckt sich dabei auf jeden Bereich des Unternehmens. Ganz besonders deutlich tritt er im Marketing zu Tage. Marketing, ein wesentlicher Aspekt jeglichen Wirtschaftens für jede Firma, beinhaltet nach Meffert die „Planung, Koordination und Kontrolle aller auf die aktuellen und potentiellen Märkte ausgerichteten Unternehmensaktivitäten. Durch eine dauerhafte Befriedigung der Kundenbedürfnisse sollen die Unternehmensziele im gesamtwirtschaftlichen Güterversorgungsprozeß verwirklicht werden“ [Mef86]. Durch diese Definition wird die Bedeutung, die der Informationsfluß in einer Firma innehat, unterstrichen. Es ist somit leicht nachzuvollziehen, daß eine erfolgreiche Unternehmung einen effizienten Informationsfluß vorweisen muß. Dies wird durch die Ausrichtung auf einen Weltmarkt bestärkt.

Aus diesen Gründen ist als Problemlösung die Vernetzung der Stellen einer Firma, die Informationen speichern, hervorgegangen. Wenn diese Vernetzung auch offen gegenüber den Kunden einer Firma ist, so bringt das einige Vorteile mit sich. Die Beziehung zwischen Anbieter und Kunde ist erheblich enger. Dadurch stehen dem Kunden Informationen über die Firma zur Verfügung (Verfügbarkeit der gewünschten Waren etc.). Aber auch der Anbieter zieht seinen Nutzen aus dieser Beziehung. Durch das Wegfallen vieler Zwischenhändler erhält er ein direktes Feedback auf seine angebotenen Leistungen, welches sich im Kaufverhalten des Kunden äußert. Somit kann er erheblich effizienter planen, welche Waren wann und wo vorhanden sein müssen. Wenn viele solche Informationen vorhanden sind, kann sich das Verhältnis Kunde-Anbieter sogar dahingehend ändern, daß Anbieter zielgerichtet Kunden aufsuchen können, während früher durch das Fehlen dieser Informationen der Anbieter passiv auf seine Kunden warten mußte.

Weitere Veränderungen, die einen neuen Ansatz des Informationsflusses vonnöten machten, spielten sich in der grundlegenden Struktur großer Organisationen ab. Zu-

nächst waren große Firmen durch eine besonders stark ausgeprägte Hierarchie gekennzeichnet. Diese zwar logisch den damaligen Entscheidungsbefugnissen angepaßte Struktur hatte jedoch den Nachteil, daß die Kommunikationswege von den ausführenden zu den entscheidenden Stellen lang und somit wenig flexibel waren. Diese Flexibilität ist aber eine Grundvoraussetzung, um sich auf rasch ändernde Märkte einzustellen. Somit wird versucht, die Struktur der Organisation zu glätten. Der Informationsfluß findet nun im wesentlichen horizontal zwischen verschiedenen Arbeitsgruppen statt.

Als Gesamtlösung der verschiedenen Probleme kristallisiert sich ein firmeneigenes Netzwerk heraus, an das folgende Anforderungen gestellt werden.

1.1 Allgemeine Anforderungen

Durch die große Bedeutung des Informationsflusses ist ein sehr hohes Kommunikationsaufkommen in einer Organisation vorhanden, welches Kosten verursacht. Diese Kosten sollten durch ein eigenes Netzwerk reduziert bzw. minimiert werden. Dabei ist die firmeninterne wie auch die externe Kommunikation betroffen.

Da Informationen vielfältige Formen annehmen können, ist die Kommunikation nicht nur auf Sprache einerseits oder aber auf Daten andererseits auszurichten. Es sollen über das Netzwerk Sprache wie auch Daten übertragen werden können. Dazu gehören auch multimediale Daten wie Bilddaten z.B. einer Videokonferenz.

Das Netzwerk muß weiterhin eine hohe Flexibilität aufweisen, um der Dynamik einer Organisation Rechnung zu tragen. Dies betrifft die Anpassung des Netzwerkes an veränderte Arbeitsabläufe und Restrukturierungen der Firmenorganisation. Ebenso muß das Netzwerk problemlos erweitert werden können.

Außerdem muß das Netzwerk alle Leistungsmerkmale transparent zur Verfügung stellen, unabhängig von der verwendeten Hard- und Software in den einzelnen Netzknoten. Diese Anforderung nennt man *Feature Transparency* [Wit96].

Von Bedeutung sind natürlich auch die Ausfallsicherheit und die Wirtschaftlichkeit. Die Ausfallsicherheit wird durch das redundante Vorhandensein aller relevanten Teile, durch eine automatische Sicherung aller wichtigen Daten (Backup), durch die Möglichkeit, das System von mehr als einer Stelle aus zu konfigurieren, sowie ein sicheres Netzwerkmanagement (z.B. basierend auf dem Simple Network Management Protocol SNMP) erreicht. Die Wirtschaftlichkeit betrifft nicht nur den Betrieb des Netzes, sondern auch die Installation, die Gewährleistung, das Wartungskonzept und den Betreuungsaufwand.

Neben diesen allgemeinen Anforderungen werden sowohl im Sprach- wie im Datenbereich spezielle Anforderungen an das Netzwerk gemacht.

1.2 Anforderungen aus dem Sprachbereich

Die Sprachverbindungen innerhalb des Netzwerks müssen einfach sein. Die Basis sind permanente oder vermittelnde Schaltprinzipien.

Weiterhin ist es sinnvoll, die Unternehmensstruktur auf einen privaten Rufnummernplan abbilden zu können. So wird der Effizienz und der Wirtschaftlichkeit im Betrieb

des Netzes Rechnung getragen. In diesem Zusammenhang ist auch der Einsatz von organisationsweiten Kurzrufnummern und organisationsweiter Ruf-Weiterschaltung zu nennen.

Auch sollen die sogenannten *Supplementary Services* (zusätzliche Dienstmerkmale) unterstützt werden. Zu diesen zählen vom ISDN bekannte Merkmale wie Anklopfen, Durchwahl, Dreierkonferenz und ähnliche.

Außerdem sollte bei Überlastung des Netzes automatisch auf das öffentliche Netz ausgewichen werden, so daß es nicht zu Verbindungsabbrüchen oder -verzögerungen kommt.

Desweiteren kann zur Kostenminimierung das *Least Cost Routing* angewendet werden. Dieses wird durch den effektiven Ein- und Ausstieg zwischen Firmennetzwerk und öffentlichem Netz realisiert.

1.3 Anforderungen aus dem Datenbereich

Die Anforderungen, die an die Datenkommunikation gestellt werden, lassen sich kurz stichwortartig auflisten: [Wit96]

- Unterstützung aller routingfähigen Protokolle
- Ersatzweg über das öffentliche Netz ohne Sitzungsverlust (z.B. bei Überlast)
- Einhaltung bestimmter Netzantwortzeiten
- Routing im Weitverkehr über alternative Wege
- *Bandwidth on Demand* (dynamische Bandbreitenzuordnung zwischen Sprach- und Datenverkehr)
- Datensicherheitsanforderungen
- Bildübertragung
- Multimedia-Anwendungen wie z.B. Desktop-Videoconferencing

Nachdem zunächst die Veränderungen, die ein neues Konzept zur Informationsweitergabe in Organisationen erforderlich machten, sowie die verschiedenen Anforderungen, die an ein solches System zur Informationsweitergabe gestellt werden, aufgezeigt wurden, stellt sich die Frage nach der Definition des Begriffes „Corporate Network“.

2 Corporate Network — Definition und rechtliche Bestimmungen

Den Begriff des Corporate Networks zu definieren, erscheint schwierig, existiert doch derzeit noch keine national oder international anerkannte rechtliche Definition. Somit

läßt sich ein Corporate Network am besten charakterisieren als ein Kommunikationsnetz, das alle Arten von Informationen innerhalb einer Corporation (Unternehmen, Verwaltung) vermittelt und/oder überträgt [Wit96].

Das Corporate Network in seiner idealen Form ermöglicht jedem Benutzer, die existierenden Verbindungen zu den anderen Benutzern zu nutzen. Das Konzept des Corporate Networks ist vergleichbar mit dem nationalen und internationalen Stromnetz. Dabei sollten die einzelnen Mitarbeiter einer Organisation in der Lage sein, überall im Netz beliebig auf verschiedene Ressourcen zugreifen zu können. Dafür ist ein gewisses Maß an Standardisierung notwendig [Val93].

In Deutschland wird der Einsatz von Corporate Networks durch folgende Gesetze und Verfügungen rechtlich abgesichert:

- Fernmeldeanlagengesetz Par. 2 (Befugnis zur Verleihung bzw. Genehmigung von Fernmeldeanlagen, die im Bereich des Telefondienstmonopols liegen)
- Verfügung des Bundesministerium für Post und Telekommunikation (BMPT) 1 und 8/93 (Genehmigungskonzept Corporate Networks; Herstellung der Übereinstimmung zwischen deutschem und europäischem Telekommunikationsrecht hinsichtlich des Telefondienstmonopols)
- Vfg BMPT 9/93 (Allgemeingenehmigung für den Betrieb von Fernmeldeanlagen zum Zwecke der Vermittlung von Sprache für zusammengefaßte Unternehmen –geschlossene Benutzergruppe zusammengefaßter Unternehmen–)
- Vfg BMPT 269/93 (Vorläufige Regelung zur Sprachkomprimierung in komplexen Netzen mit Teilnahme am Telefondienst)
- Vfg BMP 102/93 (Gebührenvorschriften für das Erteilen einer Einzelgenehmigung für das Betreiben von Fernmeldeanlagen zum Zwecke der Vermittlung von Sprache für einen abschließend festgelegten Kreis von Teilnehmern –sonstige geschlossene Benutzergruppe–)

Weiterhin werden folgende Anforderungen an das Corporate Network gestellt:

Die Quelle oder aber die Senke einer Verbindung müssen innerhalb des Corporate Networks liegen. Dabei ist Least Cost Routing zulässig, nicht jedoch die reine Durchleitung von voradressiertem Verkehr.

Hat das Corporate Network Verbindung zum öffentlichen Netz, so ist eine Anschalteerlaubnis erforderlich. Diese soll die Kommunikationsfähigkeit mit den Einrichtungen des Telefonnetzes sicherstellen. Grundsätzlich ist dabei die sogenannte Telefondienstqualität einzuhalten [Wit96].

Wie ein Corporate Network genau eingerichtet wird und welche technischen Ausprägungen vorkommen, wird im nächsten Abschnitt behandelt.

3 Der Weg zum Corporate Network

Zunächst soll an dieser Stelle die Geschichte allgemeiner Netze beleuchtet werden. Aus diesen ersten Anfängen hat sich langsam aber sicher die Idee des Corporate Networks entwickelt.

Anschließend werden einige technische Aspekte der Realisierung eines Corporate Networks herausgegriffen und exemplarisch behandelt.

Den Abschluß dieses Abschnitts bildet eine Zusammenfassung der Vorteile, die durch den Einsatz von Corporate Networks erzielt werden können.

3.1 Die Schritte zur Netzwerklösung

In den frühen Jahren des Rechnereinsatzes in der Wirtschaft fand man weitestgehend Großrechner. Diese Mainframe-to-Terminal-Lösung hatte einige Vorteile: Die Daten wurden wegen der zentralen Speicherung immer konsistent gehalten. Weiterhin konnten die Datensicherheit und Schutz vor unautorisiertem Zugriff recht gut gewährleistet werden. Der größte Nachteil war jedoch, daß diese Datensicherheit durch eine sehr unflexible Datenhaltung erkauft wurde. Durch die starren Strukturen des Systems konnten die Daten zumeist nur angesehen werden; die Verknüpfung mit anderen Dokumenten, der Export auf andere Systeme oder die Konvertierung in andere Dokumentarten konnten aufgrund der einfachen und zentralen Datenhaltung nicht umgesetzt werden.

In den frühen 80er Jahren begannen Personal Computer ihren Einzug in die Wirtschaft. In gleichem Maße gewann die Kommunikation im geschäftlichen Sektor radikal an Bedeutung. Zunächst waren die Computer als Stand-alone-Lösung konzipiert.

Als wesentliche Anforderung zur weiteren Entwicklung im technischen wie wirtschaftlichen Bereich bildete sich der Trend zu Innovation, Miniaturisierung, Standardisierung und umfangreicher Interoperabilität heraus. Gerade die Miniaturisierung ermöglichte, daß immer mehr Geräte kompakter wurden und so eine Verschmelzung verschiedener Aufgaben und Funktionen stattfand. Als Beispiel ist das interne Modem zu nennen.

Diese vorhandene Fähigkeit zur Kommunikation erleichtert das Vernetzen der Computer in LANs und WANs. Es kristallisierte sich eine neue Lösung der Datenhaltung heraus: Client-Server-basierte verteilte Datenhaltung als Ersatz für die Mainframe-Technologie.

Der zentralisierte Ansatz (große Rechenkapazität in wenigen Schlüsselpositionen) hat den Vorteil der einfachen Erweiterung und der geringen Kosten bei Erweiterungen. Nachteilig wirken sich die schlechten Antwortzeiten bei entferntem Datenzugriff aus. Der dezentralisierte Ansatz hat als Hauptnachteil relativ hohe Kosten, da recht leistungsfähige Rechner an vielen Stellen im System vorhanden sind, diese aber möglicherweise nicht gut ausgelastet sind. Der Client-Server-Ansatz vereint die Vorteile beider Systeme und koppelt die zentralen und dezentralen Aspekte in einem Netzwerk.

Bemerkenswert ist die Rolle, die eine Regierung auf das Vorantreiben und Etablieren neuer Technologien und Infrastrukturen haben kann. Als deutliches Beispiel mag hierzu das allen bekannte Internet dienen. Ursprünglich als Netzwerk aus dem Bereich der Verteidigungspolitik konzipiert, wurde es immer mehr an die zivilen Bedürfnisse

angepaßt. Die nächste Stufe war ein Informationsnetzwerk aus dem Bereich Erziehung und Wissenschaft. Erst in jüngster Vergangenheit wurde das Internet immer kommerzieller, so daß sich die Anwendungsmöglichkeiten auch auf den wirtschaftlichen Bereich erstrecken. Somit läßt sich das Internet als Vorstufe zum Netz der Zukunft sehen.

3.2 Technische Eigenschaften eines Corporate Networks

Wesentliche Eigenschaft eines Corporate Networks ist die Möglichkeit, Telekommunikationsanlagen zu verbinden. Bei dieser Vernetzung werden einige technische Möglichkeiten gefordert, die im folgenden näher betrachtet werden.

3.2.1 Sprachkompressionsverfahren.

Es ist bei firmeninternen Netzen oftmals nicht notwendig, Sprache in Telefondienstqualität zu übertragen. Diese Übertragung erfordert eine Übertragungsrate von 64 kbit/s. Statt dessen wird die Sprache mit Datenraten zwischen 6 und 32 kbit/s übertragen. Die reduzierte Datenrate ermöglicht es, gleichzeitig bei gegebener Bandbreite der Übertragungsleitung auf mehreren Sprachkanälen zu kommunizieren. Dies wird durch Sprachkompressoren, sogenannte Codecs, ermöglicht. Ihr Einsatz und ihre Wirkungsweise werden durch die folgende Abbildung demonstriert. Der verwendete Codec komprimiert die Sprache um den Faktor vier, so daß auf einer Leitung mit einer Bandbreite von 64 kbit/s gleichzeitig vier verschiedene Gespräche übertragen werden können.

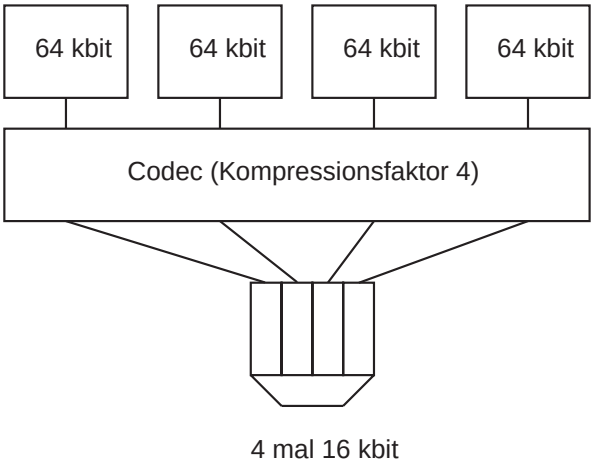


Abbildung 2: Schematische Darstellung der Bandbreiteneinsparung durch Verwendung eines Codecs.

Wesentliche Charakteristika der verschiedenen Sprachkompressionsverfahren sind [Wit96]:

- erzielbare Sprachqualität
- Kompressionsfaktor bzw. Bitrate
- Art des Kompressionsalgorithmus

- Komplexität / Kosten
- Verträglichkeit gegenüber Modemsignalen (Daten, Fax)
- Empfindlichkeit gegen mehrfache Analog-/Digital-Wandlungen und Bitfehler
- Signalverzögerung

Die Sprache kann bei den Standards G.721 (32 kbit/s- Adaptive Differential Puls Code Modulation) und G.728 (Low Delay Codebook Excited Linear Prediction) annähernd in Telefondienstqualität übertragen werden. Diese beiden Standards können auch in mehreren Abschnitten hintereinander geschaltet werden. Bei anderen Codecs, die mit 16 kbit/s oder weniger operieren, ist dementsprechend eine deutlich geringere Sprachqualität vorhanden.

Ebenso sind die erstgenannten Standards G.721 und G.728 gegenüber Modem- und Faxsignalen einer Übertragungsrate von bis zu 9600 kbit/s relativ unempfindlich.

Für die Empfindlichkeit gegenüber mehrfacher A/D-Wandlungen gibt es das Maß der Zahl der Quantisierungsverzerrungen (QVE). Sie sollte für jeden Codec-Standard spezifiziert werden und ist national aufgrund internationaler Vereinbarungen auf maximal vier QVEs festgelegt.

Der Einsatz von Codecs bedingt eine Verzögerung von bis zu 30 Millisekunden.

Eine weitere Möglichkeit zur Einschränkung der benötigten Bandbreite bei Sprachübertragung ist die sogenannte Sprechpausenunterdrückung (*Speech Detection*). Dabei wird das übliche menschliche Kommunikationsverhalten ausgenutzt, daß meist nur ein Sprecher zu einem bestimmten Zeitpunkt spricht. Dieses Verfahren teilt nur dem jeweils aktiven Sprecher einen Übertragungskanal zu und kann somit technisch als Halbduplexverfahren betrachtet werden. Bereits diese einfache Form der Bandbreitenreduzierung ermöglicht bei normalen Sprachübertragungen eine Einsparung von bis zu 50% der benötigten Bandbreite.

3.2.2 Sprach-Datenmultiplexer.

Die Sprach-Datenmultiplexer sind speziell für den Einsatz in Corporate Networks entwickelt worden. Sie weisen viele Eingangsschnittstellen für den Anschluß von Telekommunikationsanlagen (auch alter analoger Anlagen), LANs und Endeinrichtungen wie Faxgeräte als auch viele Ausgangsschnittstellen für Standardfestverbindungen, ISDN, DDV (Datendirektverbindungen), LANs u.a. auf.

Ein mittels Sprach-Datenmultiplexer realisierter Zugangsknoten weist eine QSIG-Komponente (Signalling Protocol at Reference Point Q, auch Private Integrated Signalling System Number One - PSS1) auf. Diese ermöglicht die Signalisierung und die Nutzung von zusätzlichen Diensten zwischen den Telekommunikationsanlagen. Statt dieser QSIG-Komponente können auch andere Standards wie der englische Industriestandard DPNSS oder das von Siemens entwickelte Cornet verwendet werden.

QSIG ist ein herstellerneutrales Protokoll zur Vernetzung von Telekommunikationsanlagen. Die Signalisierungsgrundfunktionen Verbindungsauf- und -abbau basieren auf

dem Q.931-Standard. Als Erweiterung kam die Möglichkeit hinzu, mit einem Signalisierungskanal mehr als 30 Übertragungskanäle zu steuern. Weiterhin findet sich eine Protokollsymmetrie. Außerdem werden viele zusätzliche Dienste angeboten, die die einzelnen Nebenstellenteilnehmer in Anspruch nehmen können.

Weiterhin ist im Sprach-Datenmultiplexer eine ISDN-Komponente vorhanden, die den Zugang zum ISDN realisiert.

In der Zukunft können die Sprach-Datenmultiplexer auch um eine vermittlungstechnische Komponente ergänzt werden. Zur Implementierung wird dabei derzeit der QSIG-Standard bevorzugt. Dann werden Sprach-Datenmultiplexer auch die Vermittlungsfunktionen, die bisher in die Telekommunikationsanlagen eingebettet sind, übernehmen können. Dieses vereinfacht die Netzgestaltung in erheblichem Maße. Außerdem können sie extreme Belastungsspitzen und daraus resultierende Engpässe durch alternatives Routing abfangen [Wit96].

Als weiteres Leistungsmerkmal findet sich das Bandbreitenmanagement. Dabei werden einzelnen Anwendungen und Übertragungen nicht mehr feste Kanäle zugewiesen, sondern jede Anwendung erhält genau die Bandbreite, die sie benötigt. Diese Zuordnung geschieht dynamisch und automatisch. Sobald eine Ressource nicht mehr benötigt wird, wird sie den anderen Prozessen wieder zur Verfügung gestellt. Zusätzlich können den verschiedenen Anwendungen verschiedene Prioritäten zugeordnet werden. Durch das Bandbreitenmanagement wird eine optimale Ausnutzung der vorhandenen Leitungskapazität erreicht.

Die erwähnten Schnittstellen werden durch Schnittstellenkarten realisiert. Weiterhin sind Sprachkarten mit den entsprechenden Codecs sowie Faxerkennung vorhanden. Als weitere Komponente findet man ein internes Koppelfeld (Durchschaltefeld).

Das Koppelfeld kann auf der Hybridtechnik basieren. Es verfügt in diesem Fall über einen Zeitmultiplex-Anteil (TDM) für zeitkritische Anwendungen wie Sprache, Video oder Übertragungen, bei denen konstante Bitraten erforderlich sind, sowie über einen Paket-Anteil für die Übertragung paketorientierter Daten wie bei X.25, SNA oder Frame Relay.

Eine andere Realisierungsmöglichkeit ist die Verwendung der Cell-Relay-Technik (ATM-Technik). Diese basiert auf einem asynchronen Zeitmultiplexverfahren. Dabei werden Transportblöcke als Zellen konstanter Größe erzeugt. Diese Größe beträgt üblicherweise 53 Bytes. Durch dieses Verfahren wird die einheitliche Behandlung von verschiedenen Kommunikationsarten auf einer Technikplattform ermöglicht.

Sprach-Datenmultiplexer können aber auch als Kombination beider vorgestellter Techniken realisiert werden.

3.2.3 Corporate Networks auf Basis des Euro-ISDN und IDNneu.

Es besteht die Möglichkeit, Corporate Networks aufsetzend auf einer fiktiven Plattform des ISDN als Virtuelles Privates Netz zu implementieren. Wenn nun eine Telekommunikationsanlage im Rahmen einer Lösung im Corporate Network vernetzt werden soll, so hat diese Zugänge zu dieser „Corporate Network“-Plattform selbst wie auch zum öffentlichen ISDN. Dabei ist zu beachten, daß zwischen QSIG und DSS1 (Protokoll

des Euro-ISDN) erhebliche Unterschiede bestehen, so daß Kommunikationsbeziehungen zwischen beiden Protokollen nicht ohne weiteres möglich sind. Dazu muß das bereits im Netz implementierte (E)DSS1 um die entsprechenden Protokollparameter des QSIG-Protokolls erweitert werden.

Im IDNneu (IDN+) ist als zentraler Kern das Network Management System vorhanden. Dieses weist das Leistungsmerkmal Virtual Private Network auf, durch das der Kunde sein eigenes privates Netz abbilden, überwachen und (in eingeschränktem Maße) konfigurieren kann. Das Virtual Private Network kann unterteilt werden in die Virtual Backbone Networks und die Virtual Switched Networks.

Beim *Virtual Backbone Network* kann der Anwender sein „eigenes Netz“ verwalten. Außerdem kann er seine Netzwerkressourcen durch die ermöglichte flexible Konfiguration optimal nutzen. Der Anwender kann sein Netzwerk also selbst managen.

Im *Virtual Switched Network* werden nur die jeweiligen Endpunkte von Verkehrsbeziehungen dem „privaten Netz“ zugeordnet. Die Bandbreite des übergeordneten Netzes steht somit allen Anwendungen als Pool zur Verfügung, auf den dann je nach Bedarf zugegriffen wird.

Zuguterletzt bietet der Frame-Relay-Server die Möglichkeit, LAN-Kopplungen in einem Corporate Network vorzunehmen. Außerdem kann ein Bandbreitengewinn unter Berücksichtigung des statistisch verteilten Verkehrsaufkommens erzielt werden.

3.2.4 Mobilkommunikation.

Der zunehmende Gebrauch der Mobilkommunikation im privaten wie auch geschäftlichen Bereich läßt die steigende Bedeutung für den Einsatz in Corporate Networks vermuten. In den Bereich der Mobilkommunikation fallen verschiedene Techniken, auf die im folgenden kurz eingegangen werden soll.

Zum einen werden die schnurlosen Telefone steigenden Einfluß haben. Marktforscher gehen von einem Anteil von 50 % aller gekauften Telefone bereits im Jahr 2000 aus. Dementsprechend muß ihr Einsatz in Corporate Networks vorzusehen sein. Dabei bringt die Bezeichnung „schnurlos“ zum Ausdruck, daß es sich um Telefone mit geringer Funkreichweite handelt. Es ist auch eine zellulare Netzstruktur für ein Gebiet mit hoher Teilnehmerdichte vorgesehen.

Als weitere Komponente treten die LANs auf, die nicht mit einer Kabelverbindung vernetzt sind. Dabei wird die Verbindung über Funk aufgebaut. Deshalb nennt man sie auch RLAN (*Radio Local Area Network*). Ihr Vorteil liegt in der einfachen Installation und Verwaltung. Nachteilig wirkt sich der vergleichsweise geringe Datendurchsatz und demzufolge eine längere Antwortzeit sowie die Störungsempfindlichkeit aus.

Außer den beschriebenen Arten der Mobilkommunikation gibt es noch die Richtfunksysteme, die sich einteilen lassen in den digitalen und den optischen Richtfunk.

Digitale Richtfunksysteme können wegen ihrer einfachen Installation als schnelle und kurzfristige Lösung eingesetzt werden. Auch sind Kosten für die kaum anfallende Wartung sehr gering. Lediglich Genehmigungsgebühren, Frequenznutzungsentgelte und Beiträge zur Elektromagnetischen Verträglichkeit (EMV) sind zu entrichten. Als Nachteile sind die Übertragungsfehler durch extreme Witterung sowie geringe Abhörsicherheit, die durch Verschlüsselungsmechanismen ausgeglichen werden muß, zu nennen.

Optische Richtfunksysteme basieren auf der Datenübertragung mit Licht in den unsichtbaren Frequenzbereichen mittels Laser oder LED (Infrarot). Wegen der sehr starken Bündelung ist die Abhörsicherheit größer als bei den digitalen Richtfunksystemen, die Empfindlichkeit gegenüber Witterungseinflüssen ist aber deutlich höher (z.B. durch starke Niederschläge wie auch durch durchfliegende Objekte wie Vögel oder Hubschrauber). Die erreichbare Funkfeldlänge liegt zwischen 2 und 5 km.

3.3 Vorteile der Vernetzung von Telekommunikationsanlagen

Abschließend sollen hier die Vorteile, die die unternehmensweite Vernetzung der Telekommunikationsanlagen bietet, genannt werden.

Zunächst ist eine effizientere standortübergreifende Sprachkommunikation festzustellen. Dies äußert sich im beschleunigten Ablauf von Kommunikationsvorgängen wie z.B. bei Konferenzgesprächen, durch automatischen Rückruf, Anrufweiterschaltung und Anklopfen. Weiterhin wird durch einen Rufnummernplan entsprechend der Struktur oder der Zuständigkeiten im Unternehmen die Kommunikation untereinander erheblich vereinfacht. Desweiteren können die Mitarbeiter ihre Rufnummer auch bei örtlich wechselndem Einsatz behalten und sind somit einfacher und besser erreichbar. Nicht zu vernachlässigen ist auch der verbesserte Komfort, der durch Rufnummernanzeige, elektronisches Telefonbuch durch zentrale Rufnummernspeicher, Kurzwahl und Hotline-Nummern dem Nutzer geboten wird. Weiterhin kann das firmeninterne Netz durch Sprachkompressionsverfahren und Sprechpausenunterdrückung besser ausgelastet werden als das öffentliche Netz.

Doch nicht nur die interne Kommunikation wird durch die Vernetzung verbessert. Auch für die externe Sprachkommunikation ergeben sich Vorteile.

Das Least Cost Routing ermöglicht Kosteneinsparungen, indem der Ausstieg ins öffentliche Netz dem externen Zielpunkt am nächsten gewählt wird. Auch können hier Sprachkompression und Sprechpausenunterdrückung bei Anrufen ins öffentliche Netz genutzt werden. Das eigene Netz ermöglicht weiterhin die Einrichtung eines „Call Centers“ zur flexiblen Organisation von dezentralen Service-Stationen. Außerdem können Routineaufgaben unterstützt und dem Kunden ein verbesserter Zugang zum Unternehmen durch intelligente Rufbearbeitung bzw. -umleitung geboten werden. Weiterhin läßt sich der Rufnummernplan auch den Kundenbedürfnissen anpassen, so daß verschiedene Servicefunktionen wie Kundenbetreuung, Beratung, Verkauf etc. zusammengefaßt werden.

Desweiteren bringt die Vernetzung auch einen betriebswirtschaftlichen Nutzen. So kann die interne Wertschöpfung erhöht werden, indem eigene Kapazitäten Dritten als Dienstleistung angeboten werden (derzeit nach Aufhebung des Monopols in Deutschland ab 1998). Auch die Bündelung der Konzern- oder Gruppenressourcen wirkt sich vorteilig aus. Durch die interne Vernetzung wird außerdem die Abhängigkeit von öffentlichen Netzbetreibern verringert, was eine erhöhte Planungssicherheit und eine vereinfachte Implementierung neuer Leistungsmerkmale mit sich bringt. Außerdem werden Personalkosten durch zentralisierte Vermittlungsplätze eingespart. Ebenso senken einfacheres Netzwerkmanagement und die Möglichkeit des Outsourcings die Personalkosten. Zuguterletzt können auch Heimarbeitsplätze sehr einfach eingebunden werden (Stichwort virtuelles Büro).

4 Standardisierungsmöglichkeiten

Mit den Problemen von unterschiedlichen Entwicklungen, Hardware-Plattformen sowie Software-Lösungen mußte seit jeher in allen Bereichen des Technologie-Einsatzes gekämpft werden. Dieses Kapitel beschreibt die ersten Standardisierungsversuche, ausgehend von einem Vergleich vom OSI-Basisreferenzmodell und dem TCP/IP, das dem Internet zugrundeliegt. Anschließend werden zukunftsweisende Standardisierungskonzepte speziell für den Bereich der Corporate Networks vorgestellt.

Als Grundlage oder Vergleich zur Implementierung firmeneigener Netzwerke wird immer wieder das amerikanische Internet herangezogen. Doch genausogut hätte das in Europa entwickelte OSI-Modell ein gültiger Standard werden können. Wie kam es dazu, das sich TCP/IP durchgesetzt hat?

Der wesentliche Grund hierfür ist in der unterschiedlichen Entwicklung zu sehen, die beide Ansätze aufweisen. OSI wurde sehr theoretisch durchgedacht, bevor an die Implementierung gegangen wurde. Die Entwickler vom TCP/IP sind den entgegengesetzten Weg gegangen. Ausgehend vom vorhandenen wurden schnelle und lauffähige Lösungen gesucht, so daß TCP/IP inzwischen ein funktionierendes, in der Praxis bewährtes Protokoll ist, zu dem es auch entsprechend viele Anwendungen gibt. Für OSI fehlen die anwendungsbereiten Produkte. Hinzu kommt weiterhin die steigende Beliebtheit von UNIX, das TCP/IP inhärent in seinem Kernel verankert hat.

Nun zu den Standardisierungsbemühungen speziell im Bereich der Corporate Networks: Von einem Corporate Network wird die Möglichkeit verlangt, international garantiert Vermittlungs- und Übertragungseinrichtungen unterschiedlicher Hersteller zusammenschalten zu können. Weiterhin muß das Netz kurzfristig und flexibel an die potentiell schnellen Veränderungen eines Betriebes angepaßt werden können.

4.1 Ziele der Standardisierung

Idealerweise sollte ein Corporate Network den Mitarbeitern einer Organisation ein homogenes Dienstangebot zur Verfügung stellen. Grundvoraussetzung dazu ist ein geschlossener Numerierungsplan sowie eine netzweit einheitliche Verfügbarkeit der angebotenen Ressourcen. Der einheitliche Numerierungsplan orientiert sich an den Strukturen, die in der Organisation vorherrschen. Er muß leicht zu warten und vor allem für die Benutzer zu durchschauen sein. Er bildet die Unternehmensstruktur auf die firmeninternene Rufnummern ab. Im Gegensatz dazu sind die Numerierungspläne der öffentlichen Netze politisch-geographisch orientiert (Trennung nach Ländern und Städten).

4.2 Standardisierungsmaßnahmen

Zu Beginn der Standardisierungsaktivitäten setzten namhafte Hersteller zunächst ausschließlich auf ISDN-fähige Protokolle und Dienste. 1990 wurde auf Basis des Standard-Signalling-Protokolls Q.931 das bereits vorgestellte Protokoll QSIG entwickelt. Dieses Protokoll wurde von der European Computer Manufactures Association (ECMA) bestätigt.

Die ECMA behandelt und entwickelt das QSIG-Protokoll wie auch den privaten Rufnummernplan. Letzterer wurde standardisiert in der Norm ECMA 155. Für den Aufbau eines Rufnummernplans existieren verschiedene Ansätze:

- ISDN-Numbering Plan gemäß International Telecommunication Union E.164 mit Ländercode, Stadtcode und Teilnehmernummer
- Private Numbering Plan mit Struktur ähnlich dem ISDN-Numbering Plan mit Organisation hierarchisch nach Regionen, Region-Code und regionaler Teilnehmernummer
- Unknown Numbering Plan ohne erkennbare Strukturen, allerdings mit Präfixen und Escape-Codes Rufnummernplan als Kombination vorgenannter Möglichkeiten

Im Rahmen des QSIG-Protokolls lassen sich folgende Standards herausarbeiten:

Der QSIG Basic Call (nach ECMA 143) beschreibt das Herstellen, Aufrechterhalten und Abbauen einer leitungsvermittelnden Verbindung. Die Signalisierung der erforderlichen Daten erfolgt auf einem separaten Signalisierungskanal (D-Kanal).

Die QSIG Generic Functions (ECMA 165) spezifizieren ein Protokoll für die zusätzlichen Dienste und zusätzliche Netzwerk-Möglichkeiten am Referenzpunkt Q (s. oben) sowie die Mechanismen für Transit-Knoten, die Feature Transparency aufweisen müssen. Die QSIG Supplementary Services sowie QSIG Additional Network Features werden in spezifischen Standards behandelt.

Das European Telecommunications Standards Institute ETSI definiert ein privates Telekommunikationsnetzwerk als den Zusammenschluß aus mehreren Telekommunikationsanlagen. Dabei wird die Unterstützung der Vernetzung durch das öffentliche Netz in verschiedenen Szenarien durchgespielt:

- Beim „Concatenated Scenario“ werden private Netze nicht besonders berücksichtigt. Die einzige Grundlage ist das öffentliche ISDN mit Rufnummernplan gemäß E.164 und dem Euro-ISDN-Protokoll.
- Das „Overlay Scenario“ zieht die privaten Netze mit in Betracht. Dabei besteht die Vernetzung entweder aus gemieteten Standleitungen oder aber über leitungsvermittelnde Verbindungen des öffentlichen ISDN-Netzes. Dabei ist das ISDN bezüglich der B-Kanäle zum Datenaustausch (und Signalisierungsaustausch der Telekommunikationsanlagen) transparent.
- Beim „Integrated Scenario“ wird das ISDN um die Funktionalitäten der Telekommunikationsanlegen erweitert und verhält sich so gleichfalls wie eine Telekommunkationseinrichtung.

5 International Virtual Private Networks – ein Ausblick

Der Trend zu den Corporate Networks ist ungebrochen. Als Erweiterung drängen seit den frühen neunziger Jahren die International Virtual Private Networks (IVPN) [Hey95] auf den Markt. Doch was genau unterscheidet diese IVPNs von den bisher bekannten Virtual Private Networks?

Die internationalen Verbindungen der alten Virtual Private Networks wurden jeweils durch das eigene Netzwerk sowie durch den Gebrauch der öffentlichen Netze in den jeweils betroffenen Ländern hergestellt. Dieser dezentrale Aspekt eines Teils der Netzwerkanbieter (staatliche Telekommunikationsanbieter, in Europa meist durch ein Monopol geschützt) beinhaltete natürlich auch, daß es für die Organisationen viele verschiedene Ansprechpartner gab. Weiterhin gab es auch viele verschiedene Rechnungen für die in Anspruch genommenen Leistungen, teilweise auch mit verschiedenen Mehrwertsteuersätzen behaftet. Auch war die Lokalisierung von Problemen im Netzwerk schwierig, da jeder öffentliche Netzbetreiber eigene Stellen zu diesem Zweck unterhielt. Schließlich war durch das oftmals vorhandene Monopol der Wettbewerb ausgeschaltet, so daß es für die Netzbetreiber wenig Anreiz zu Verbesserungen des Leistungsangebots sowie zur kundenfreundlichen Preisgestaltung gab.

Diese Punkte entfallen bei den International Virtual Private Networks. Sie werden durch einen globalen Provider angeboten, die von öffentlichen Netzbetreibern (mehr oder weniger) unabhängig sind. Außerdem stehen sie in Konkurrenz zu anderen Anbietern, was Innovation, bessere Dienstleistungen und günstigere Tarife zur Folge hat. Durch die zentrale Verwaltung eines ganzen möglicherweise globalen Netzes gibt es für die Organisation nur einen Ansprechpartner und auch nur eine Rechnung, die von den verschiedenen Steuern der einzelnen Länder unabhängig ist.

Doch es gibt auch Nachteile. Das entscheidende Problem ist, daß sich die International Virtual Private Networks in einer sehr frühen Entwicklungsphase befinden. Es gibt erst sehr wenige Anbieter (1993 Concert Communications als joint venture von British Telecommunications PLC und MCI Communications Corp.; Phoenix als Zusammenschluß der Deutschen Telekom AG, France Telecom und Sprint Corp.; Worldpartners Co. aus u.a. AT&T, Hongkong Telecom Ltd., Korea Telecom, Unisource, Unitel Communications Inc.), die sich erst in der Entwicklungs- und Konsolidierungsphase befinden. Viele weitere Anbieter existieren erst auf dem Reißbrett. Außerdem sind trotz des Monopolwegfalls in Europa im Jahr 1998 weiterhin Restriktionen vorhanden.

Ein wesentlicher Punkt, den die Kunden vor einem Wechsel zu einem Anbieter eines International Virtual Private Networks zu bedenken haben, ist, daß dieser Wechsel möglicherweise auch ein komplett neues Denken in der Konzeption des eigenen Corporate Networks erfordert. Entscheidend ist dabei, daß es in der Organisation nur eine zentrale Stelle gibt, die Entscheidungen bezüglich des Netzes trifft.

Trotz einiger Anfangsschwierigkeiten läßt sich jedoch vermuten, daß im Rahmen der immer internationaler werdenden Geschäftsbeziehungen der Trend zu den International Virtual Private Networks anhalten wird.

6 Zusammenfassung

Nachdem Corporate Networks von ihrer Entwicklungsgeschichte bis zu einzelnen technischen Merkmalen sowie die mit den technischen Neuerungen einhergehenden Umstrukturierungen einzelner Organisationen betrachtet wurden, stellt sich nun die Frage, wann denn der Einsatz eines Corporate Networks sinnvoll ist. Zunächst läßt sich diese Frage nicht einfach auf eine Entweder-Oder-Frage reduzieren.

Grundsätzlich läßt sich sagen, daß alle mittleren und großen Firmen den Einsatz eines Corporate Networks rechtfertigen, wenn die Mitarbeiter in verschiedenen Standorten firmenintern sehr viel kommunizieren. Dieses Faktum ist bei mittleren und großen Firmen zur Koordination fast zwingend vorgegeben.

Bei der Abschätzung nach dem zu erwartenden internen Kommunikationsaufwand ist natürlich der Datenverkehr nicht zu vernachlässigen. Außerdem muß in eine Wirtschaftlichkeitsrechnung die Tatsache einbezogen werden, daß Sprachübertragung einerseits und Datenübertragung andererseits über die gleichen Leitungen abgewickelt werden.

Sollte ein Unternehmen vorwiegend mit externen Teilnehmern kommunizieren, lohnt sich in der Regel die Anschaffung eines Corporate Networks nicht, da die externen Gespräche über das öffentliche Netz abgewickelt werden müssen.

Es sind auch Lösungen denkbar, bei denen einzelne Firmenteile über ein Corporate Network miteinander verbunden sind, andere Teile jedoch nicht mit ins Netz aufgenommen werden und somit die Kommunikation über das öffentliche Netz abgewickelt wird.

Derzeit sind in den meisten Corporate Networks die Kommunikationsanlagen über Festverbindungen mit vorgeschalteten Multiplexern miteinander vernetzt. Dabei wird sich die Multiplexertechnik langsam in Richtung ATM-Lösungen entwickeln. Dies vereinfacht die vollständige Integration von Sprache, Daten und Bildern in einem Corporate Network.

Erst wenn die Anforderungen aus den Corporate Networks standardisiert und ins (B-)ISDN aufgenommen werden, kann das öffentliche Netz wieder eine Alternative zu firmeneigenen Netzen werden.

Literatur

[Hey95] P. Heywood. The Dawn of the New VPN Area. *Data Communications International* 24(12), September 1995, Seite 48B–48F. The Global Enterprise Networking Magazine of the McGraw-Hill Companies.

[Mef86] H. Meffert. *Marketing. Grundlagen der Absatzpolitik.* Gabler-Verlag, Wiesbaden. 1986.

[Val93] T. Valovic. *Corporate Networks – The Strategic Use of Telecommunications.* Artech House, Boston; London. 1993.

[Wit96] H. Wittmann. Corporate Networks. In B. Seiler (Hrsg.), *Taschenbuch der Telekom Praxis 1996*, Band 33, Seite 31–64. Schiele & Schön, Berlin, 1996.

Abbildungsverzeichnis